

Viettel Endpoint Detection & Response

. .

.

=

.

.

.

.

.

-

.

.

.

.

.

.

.

. .

.

- - - - **-**

.

.

.

. .

- - - - **-**

.

.

-

.

.

.

.

.

(VCS-aJiant)

Version 3.3.0 EDR - 2021

Update date: 29 Nov. 2021

User Guide



Contents

<u>Glos</u>	<u>sary</u>		5
1.	Introdu	uction	6
1.1	Curr	ent Situation	6
1.2	2. Tech	nology Development	6
1.3	B. VCS-	aJiant	6
1.4	l. Upgı	raded Information	6
2.	Overvie	9W	7
2.1	Tech	nologies	7
2.2	2. Infra	structure Architecture	7
2.3	8. Worl	with Admin Interface	8
3.	Instruc	tion to Use	9
3.1	Logi	n	9
3.2	2. Dash	board VCS-aJiant	9
	3.2.1.	Action to Manipulating Data	10
	3.2.2.	Overview Statistic	11
	3.2.3.	Monitor Security Operation	15
	3.2.4.	Monitor Agent Monitoring	16
	3.2.5.	Monitor Risk Detection	18
3.3	8. Man	age Alerts	20
	3.3.1.	Search Alerts	21
	3.3.2.	Alert List	25
	3.3.3.	Group Alert	27
	3.3.4.	View Alert Summary	28
	3.3.5.	View Alert Details	29
	3.3.6.	Investigation Graph	31
	3.3.7.	Mark Not Dangerous for 1 Alert/Multi-Alert or Alert Group	39
	3.3.8.	Create IR Flow from 1 Alert/Multi-Alert or Alert Group	39

1



	3.3.9.	Add 1 Alert/Multi-Alert or Alert Group into Existed IR FLow	40
3.4	. IR Flo	ow Screen	41
	3.4.1.	Display List	41
	3.4.2.	Search IR FLow	41
	3.4.3.	How to Create a IR Flow	43
	3.4.4.	Steps to Perform in IR Flow	44
	3.4.5.	IRFLow - Detection	44
	3.4.6.	IRFlow - Containment	45
	3.4.7.	IRFLow - Investigation	47
	3.4.8.	IR Flow - Response	64
	3.4.9.	Close IR FLow	77
3.5	. Inves	tigation Screen	79
	3.5.1.	Investigation_Process Analysis	80
	3.5.2.	Investigation_Event Search	88
	3.5.3.	Investigation Deploy Tools	93
3.6	. Respo	onse Screen	96
	3.6.1.	Response Live Response	96
3.7.	. Settir	ng Screen	103
	3.7.1.	Agent Management	103
	3.7.2.	Policy Setting	115
	3.7.3.	Group Management	120
	3.7.4.	Account Management	131
3.8	. BLS S	Screen	143
	3.8.1.	Violation statistics	143
	3.8.2.	Software statistics	150
3.9	. Rules	Correlation	153
	3.9.1.	Display List	153
	3.9.2.	Add New Rules Correlation	158

/



3.9.	3.	Edit Correlation Rules	164
3.9.	4.	Delete Correlation Rule	165
3.10	Pro	tect & Prevention	167
3.9.	5.	Application Control	167
3.9.	6.	Display list of blocked apps/ processes	167

1



Glossary

Terms	Description			
VCS-aJiant	Trade name of the Viettel Endpoint Detection & Response product			
IR Flow	Incident Response Flow: A operational flow to handle alerts, investigations and responses			
Artifact	Alert-related investigation objects, such as path file/registry/process			
Detection	Object detection related to alerts			
Containment	Process isolation in computer, such as network isolation and process suspension			
Investigation	Investigation process: Based on event logs or active investigation using tools on the users' machine.			
	The below investigation methods with investigation tools including auto runs and listdlls are supported:			
	Process Analysis			
	Search event logs.			
Response	Response process: From the investigation results, the operator processes them in the following ways:			
	Response Scenario			
	Live Response.			
Timeline	A timeline to show activities in IR Flow, including:			
	Create IR Flow			
	Create/close Process Analysis session			
	Create/close Live Response session.			
	Close IR Flow.			

1



1. Introduction

1.1. Current Situation

Today, organizations and enterprises continue to face many difficulties with the detection, identification, investigation and minimization of advanced malware forms in the system. Traditional anti-malware technologies such as signature-based anti-virus are being intentionally bypassed by highly skilled professional attackers with attack kits and malware customized and targeted to specific objects. Many organizations have acknowledged that their traditional anti-malware defense methods have failed and a new strategy must be created to identify these breaches at the endpoint. A significant number of recent data breaches from advanced malware forms have made the customer interest increase in the Endpoint Detection and Response (EDR) Solutions, in which VCS-aJiant is one of them.

1.2. Technology Development

The technology of the VCS-aJiant Solution improves the shortcomings of signaturebased technologies that organizations are using such as anti-virus or IPS/IDS to provide the ability to detect the behavior-based anomalies and the deep insight into specific information related to endpoint to detect and minimize the advanced threats.

1.3. VCS-aJiant

VCS-aJiant is able to provide detailed information on malware infections and lateral movement behaviors of attackers as they perform scans or use information stolen in the intranet for systems and applications.

In addition, VCS-aJiant also complements the existing security technologies, such as Security Information and Event Management (SIEM) solutions, Network Forensics tools and Advanced Threat Detection devices, which means complement to an organization's portfolio of information security incident response solutions.

1.4. Upgraded Information

Version 3.3.0 provides the following new features:

- Improve Login and Process Analysis features according to new interface design
- Improve user experience and add necessary process information to support users in the investigation process
- Improve issues in the old version to ensure stability.



2. Overview

2.1. Technologies

VCS-aJiant uses Filter Driver technology (allow to run and monitor at the Kernel-based level) to collect information, including Files, Processes, Registries, Networks on user computers and servers. The file signs include Modified, Delete and Changed attribute. The registry signs include Delete key/value, Set value, Rename key/value and Create key with suspicious access. The suspicious signs of Memory are periodically scanned. The behavior identified as Suspicious is pushed to the centralized analysis back-end system.

The attack investigation workflow is designed as a closed flow according to the IR Flow scenario in order to support the detection and analysis of anomalous signs right on a single interface, provide deep investigation (Forensic) functions on Endpoint, support to get suspicious files (Get Artifact), push scanning tool (Tool Deployment), allow investigation implementation, provide evidence in real-time (Process Analysis and Live Response) and allow respond to a threat detected.

As soon as the anomaly is verified, Endpoint provides wide-ranging malware removal tools (Response Scenario), including: isolating the infected machine network (with network containment), killing process and deleting file/registry.



2.2. Infrastructure Architecture

VCS-aJiant system includes 03 main components:



- Agents: A component installed on each computer, responsible for monitoring abnormal signs on the computer and sending logs to a centralized server.
- Cluster of servers for centralized processing and storage: A data processing component, playing a key role in analyzing and processing data sent by the Agent in real time.
- Web Portal: A component for administrators, used to monitor and analyze system information.

2.3. Work with Admin Interface

The Web-portal interface includes the following functional interfaces and processing flows:

- Dashboard: Statistics and visual charts about the organization's information security situation.
- Alert management: An alert list about signs of malware appearing on the user's computer.
- IR Flow management: A list of IR Flows created by the administrator during the investigation. The flow includes a set of Detection, Containment, Investigation and Response.
- Investigation: A tool list for investigation (Process Analysis, Event search and Deploy tools).
- Response: A tool list for response and incident response (Live response)
- Protect & Prevention: A list of workstation protection and prevention features (Application control and Endpoint firewall)
- Setting: A list of system setting functions (Policy management, Agent management, Group management, Rule correlation and Account management: User, Role, Permission management).



3. Instruction to Use

3.1. Login

• Access the system at the provided address.

English
Sign in Username
Pasoword Eorgot your, password? Sign in
Version 3.8.123 (pedie: 1,2,3,4) # 2021 VetHic Cyber Security - Branch of VetHel Group

• Login with the provided user/password.

3.2. Dashboard VCS-aJiant

• Main features include as follows:

TIAILA 🚺	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting		③ EN -	root 🔔 🔹
Organization Dashboard							Export 1 کی Export 1	his Dashboard	06/06/2021 - Now	⇔
Agents •	Online 7 + -1 agents	0%	Offline 43906 † +1 agents	100%	Alerts • 4999	new 30 99940	New 30 † + 5 alerts	100%	Executing 0 ⇒ Remain uncl	0%
2	● 43913		+ + 30 alerts has been updated	erts has pdated	False Positive 0 Remain unchange	d	Closed 0 ⇒ Remain uncl	0%		
Security Operation 3 Agent Monitoring	Risk Detection 5									
ALERTS BY STATUS							🛃 Export data	ALERTS BY SEV	/ERITY	🛃 Export data
100%										
80% -										
70% -									30	
60% - 50% - 40% -									TOTAL	

- o Operations with data on Dashboard
 - Export data on Dashboard
 - Search data up to the last 90 days

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Refresh data.
- Overview: An overview statistics of the organization's information security situation (through agent and alert state).
- Security Operation: Monitor information security operation situation (through alert operation monitor).
- Agent Monitoring: Monitor installation state and agent state.
- Risk Detection: Track threats to the organization (through the statistics of the objects generating the most unprocessed alerts in the system).
- Data authorization at the features is as follows:
 - User login under root group: Display data of the entire system.
 - User login in 1 level group: Display data at all 1 level group and affiliated childlevel groups.
 - User login in 2 level group onwards: Display data at the entire 1 level group containing the group of the user login and the affiliated child-level groups of the corresponding 1 level group.

3.2.1. Action to Manipulating Data

3.2.1.1. Export Data

This function allows to export the existing data on the Dashboard interface by selecting

Export this Dashboard , in addition to adding the detailed data sheets to support reports.

- In case of connection failure or no data on all components of Dashboard, the export is not supported and the action will be hidden.
- In case of having data, support to export files in .xlsx format.

3.2.1.2. Search by Date

This function allows to adjust the time period to monitor the information security situation up to the current time with the default time from the last day.

• To select the start-time range to monitor, enable to choose absolute or relative time range as follows



Absolute time range	Relative time range
From	Last 90 days
06/06/2021	Last 60 days
Apply time range	Last 30 days
	Last 24 hours

• Absolute time range: A specific start date value and up to 90 days from the current date supported.

For example, it is currently 3 am on 7 June 2021, select start date = "06/06/2021". \rightarrow Monitoring period: 00:00 6 June 2021 to 03:00 6 July 2021.

• Relative time range: A relative time range between the start date and the current date.

For example, it is currently 3 am on 7 June 2021, select start date = "Last 30 days". The system automatically searches the last 30 days and starts counting from 00:00 of that day. \rightarrow Monitoring period: 00:00 8 May 2021 to 03:00 7 June 2021.

• After selecting the time range to monitor, select Apply time range to reload the corresponding data.

3.2.1.3. Refresh Data

This function allows to refresh manual data, select ¹ to update the latest data up to the current time.

3.2.2. Overview Statistics

This function allows to quick statistics on the information security situation at the organization according to the selected time range in the search section.



3.2.2.1. Statistics Related to Agents

Statistics	Meaning
	Include 2 numbers as follows:



Offline

2897

-898 agents



Total number of machines with agent installed in the system (regardless of search time range) Total number of new machines with agent installed during the search time range Newly installed (+: machine, Remain

unchanged: No newly installed machine during the search time range).

Include 3 numbers as follows:



Average number of online machines during the search time range (only counting working time during office hours from 08:00 - 18:00)

Average number rate of online machines compared to the whole system

Average number of online machines different from the previous cycle.

(+: Average number of online machines increased compared to the previous time range, Remain unchanged: No difference).

Include 3 numbers as follows:

Average number of offline machines in the search time range (only counting working time during office hours from 08:00 - 18:00)

Average number rate of offline machines compared to the whole system

Average number of offline machines different from the previous cycle.

(+: Average number of offline machines increased compared to the previous time range, Remain unchanged: No difference).

Include 3 numbers as follows:

Page | 12



	Total number of machines with agent installed
Suspicious	in the system (regardless of search time range)
3748	generating unprocessed alerts
↑ + 1529 agents	Rate of machines generating alerts compared
	to the number of machines in the whole system
	(regardless of search time range)
	Total number of machines generating alerts
	during the search time range
	(+: New machines generating alerts, Remain
	unchanged: No new machine generating alerts
	during the search time range).

3.2.2.2. Statistics Related to Alerts

Statistics		Meaning
\wedge	Alerts • 466354	Include 2 numbers as follows: Total number of alerts in whole system (regardless of search time range)
<u>··</u>	+ 10386 alerts has been updated	Total number of new alerts generated or updated during the search time range (+: New alerts generated, Remain unchanged: No new alert generated during the search time range).
		Include 3 numbers as follows:
		Total number of new alerts generated or updated during the search time range and in the NEW state
New 10386 ↓ -3627 alerts	100%	Rate of new alerts generated or updated during the search time range in the NEW state compared to all new alerts generated or updated during the search period time range
		Total number of new alerts generated or updated during the search time range and in

Page | 13

/

Exec "

Remain unchanged

O

0%

the NEW state different from the previous cycle.

(+: Total number of new alerts increased from the previous time range, Remain unchanged: Total number of new alerts remained unchanged from the previous time range).

Include 3 numbers as follows:

Total number of new alerts generated or updated during the search time range and in the <> (NEW, FALSE POSITIVE, CLOSED) state Rate of new alerts generated or updated during the search time range and in the <> (NEW, FALSE POSITIVE, CLOSED) state compared to all new alerts generated or updated during the search time range

Total number of new alerts generated or updated during the search time range and in the <> (NEW, FALSE POSITIVE, CLOSED) state different from the previous cycle.

(+: Total alert increased compared to the previous time range, Remain unchanged: Total number of alerts remained unchanged from the previous time range).

Include 3 numbers as follows:

Total number of new alerts generated or updated during the search time range and in the CLOSED state

Rate of new alerts generated or updated during the search time range and in the CLOSED state compared to all new alerts generated or updated during the search time range

False Positive 0 → Remain unchanged

Page | 14



Close

Remain unchanged

0

Total number of new alerts generated or updated during the search time range and in the CLOSED state different from the previous cycle

(+: Total alert increased compared to the previous time range, Remain unchanged: Total number of alerts remained unchanged from the previous time range).

Include 3 numbers as follows:

 Total number of new alerts generated or updated during the search range time and in the FALSE POSITIVE state

Rate of new alerts generated or updated during the search time range and in the FALSE POSITIVE state compared to all new alerts generated or updated during the search time range

Total number of new alerts generated or updated during the search time range and in the FALSE POSITIVE state different from the previous cycle.

(+: Total alert increased compared to the previous time range, Remain unchanged: Total number of alerts remained unchanged from the previous time range).

3.2.3. Monitor Security Operation

This function allows to monitor the information security operation situation (through alert operation monitor) according to the selected time range in the search section, including:

- Statistic of alert process state by state
- Statistic of alert by severity



• Corresponding data export in the charts.



Charts/Statistics	Meaning
Alert by state	 Domain chart: Monitor the state of newly recorded or updated alerts during the search time range, including: X-axis: Time Y-axis: Alert rate divided by 4 state groups (New, Executing, Closed and False Positive) Allow selecting to download alert lists sorted by state
Alert by severity	 Pie chart: Monitor the state of newly recorded or updated alerts by severity during the search time range, including: Rate: alert rate at each severity The total number of new or updated alerts in a time range is displayed in the middle of the chart. Allow selecting to download alert lists sorted by severity

3.2.4. Agent Monitoring

Allow statistics of agents by state and operating system information according to the selected time range in the search section, including:

Page | 16



- Agent state statistics (online and offline)
- Agent statistics by operating system and operating system version
- Agent data export.



Charts/Statistics	Meaning
Agent by state	Domain chart: Monitor the state of machine recognition by state (Online/Offline) in the report cycle up to the current time, including:
	• Y-axis: Rate of machine divided by 2 state groups (Online and Offline)
	• X-axis: statistical time
	• Display the number of machines that are not online at all (in case the machine is not online for more than 30 days, the machine is not automatically recognized).
Agent by operating system	Pie chart: Monitor the state of machine recognition by operating system (OS), including:



	Rate: Machine rate at each OS
	• The notes section lists the OS list: Windows, MacOS, Linux and other operating systems.
	• Allow selecting to download machine lists sorted by OS information.
Agent by OS version	Statistic on the top OS versions installed on the machines.
	• Allow changing the statistical period: Top 5, Top 10, Top 20, Top 50. Default is Top 5.

3.2.5. Monitor Risk Detection

This function allows to monitor threats to the organization (through the statistic of the objects that generate the most unprocessed alerts in the system), including:

- Statistic of top groups that generate the most alerts.
- Statistic of top agents that generate the most alerts.
- Statistic of the top RuleIDs and scenarios that generate the most scenes.
- Export the information data according to dangerous objects.



Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@vietteLcom.vn | W: www.viettelcybersecurity.com



Charts/Statistics	Meaning
Total groups at risk	Total number of groups containing computers with newly recorded or updated alerts (excluding false positive and closed alerts, excluding deleted groups) during the search time range. Rate of suspicious groups to the entire group in the system (excluding deleted groups).
Top groups at risk	 Column chart: Statistics of top groups containing many computers with the most newly recorded or updated alerts (excluding false positive and closed alerts, excluding deleted groups) during the search time range, including: X-axis: Number of machines generating multiple alerts in each group Y-axis: Corresponding group name Allow changing the statistical interval: Top 5, Top 10, Top 20, Top 50. Default is Top 5 Allow selecting to download computer lists that generate alerts
Total agents at risk	Total number of computers with newly recorded or updated alerts (excluding false positive and closed alerts, excluding computers that have been inactive for more than last 30 days) during the search time range. Rate of suspicious machines compared to all computers in the system (excluding computers that have been inactive for more than last 30 days).
Top agents at risk	 Column chart: Statistics of top computers with the most newly recorded or updated alerts (excluding false positive and closed alerts) during the search time range, including: X-axis: Number of alerts at each host, clearly divided by severity (Critical, High, Medium and Low) Y-axis: Corresponding machine name

Page | 19

1



	 Allow changing the statistical period: Top 5, Top 10, Top 20, Top 50. Default is Top 5. Allow selecting details to download computer lists that generate alerts.
Alerts by RuleID	 Statistics of top RuleID with the most newly recorded or updated alerts during the search time range, including: Allow changing the statistical period: Top 5, Top 10, Top 15, Top 20. Default is Top 5.
Alerts by Scenarios	 Statistics of top Scenario with the most newly recorded or updated alerts in the report cycle up to the current time, including: Allow changing the statistical period: Top 5, Top 10, Top 15, Top 20. Default is Top 5.

4. Manage Alerts

• Main features include as follows:

TIAILA 🚺	Alerts IR						
Alert Management							😗 Guidelines
Use saved query * $\int fx$ Type to search by queries							🔾 🕓 Last 7 days 🔻 🛠
Last 30 Days 405.851	STATUS New In Progress Enhanced Auto Investigated	405.424 417 0 0	SEVERITY Critical High Medium Low	11.839 5.451 699 387.861	SCENARIO Unknown Suspicious Behaviour Makware Execution	379.405 25.571 487 263	ASSIGNED TO Root 423 Admin 4
19.094 result(s)						8 1	😳 Group alerts by 🔹 View column 🔻
3 SEVERITY & TIMESTAMP_CREATE * TIMESTAMP_CLOSE & ALL	LERT_ID \$	STATUS 🖨 GROUP	♦ HOST_NAME	SCENARIO \$	IR_FLOW_NAME \$	DESCRIPTION &	ACTION
HIGH 21:09:35 09/06/2021 N/A 20	0210609_14937_484416353_379455	New default	WIN7X64-A-PC	Malware	N/A	[IOC] Detect process [nul +	J 2 O
LOW 21:03:35 09/06/2021 N/A 20	0210609_14337_829163612_488495	New default	VCS	Execution	N/A	Detect process [null] (PI »	J 2 0
HIGH 17:59:56 09/06/2021 N/A 20	0210609_105957_747552400_437443	New default	WIN7X64-A-PC	Malware	N/A	[IOC] Detect process [C:\ >	J 2 0
MEDIUM 17:59:56 09/06/2021 N/A 20	0210609_105957_745578050_476671	• New default	WIN7X64-A-PC	Malware	N/A	[T1543.003] Windows Servi »	J 2 0
0 1011 17:59:35 09/06/2021 N/A 20	0210609_105936_760363850_101257	• New default	VCS	Execution	N/A	Detect process [null] (PI >	J 2 0
01011 17:41:46 09/06/2021 N/A 20	0210609_104147_718242143_718165	New default	WIN7X86CHUYENTE	Persistence	N/A	Detect process [C:\Users\ >	J 2 0
MEDIUM 16:59:43 09/06/2021 N/A 20	0210609_95944_274342921_910924	New dattes	2 WIN10X64	Malware	N/A	[T1543.003] Windows Servi »	J 2 0
0 1017 16:59:43 09/06/2021 N/A 20	0210609_95944_271587002_374811	New dattes	2 WIN10X64	Persistence	N/A	Detect process [C:\Users\ >	J 2 0
0 16:45:43 09/06/2021 N/A 20	0210609_94544_447010947_638027	New dattes	2 WIN10X64	Defense Evasion	N/A	Detect process [C:\Window >	J 2 0
HIGH 16:45:43 09/06/2021 N/A 20	0210609_94544_446007203_502344	New dattes	2 WIN10X64	Malware	N/A	[IOC] Detect process [nul >	J 2 0
HIGH 16:16:54 09/06/2021 N/A 20	0210609_91655_554647921_686621	New default	WIN7X86CHUYENTE	Malware	N/A	[IOC] Detect process [nul >	J 2 0
16:16:44.09/06/2021 N/A 20	0210609_91646_603511667_367005	New default	WIN7X64-A-PC	Persistence	N/A	Detect process [C:\Window >	A 2 O
MED/UM 16:16:44 09/06/2021 N/A 20	0210609_91646_602927627_678933	New default	WIN7X64-A-PC	Malware	N/A	(T1547.001) Registry Run ►	J 2 O

- \circ $\,$ Search data by query and time $\,$
 - Search data by query command and use stored query commands
 - Search data by time



- Quick search
- Alert list and actions with alert
 - View alert list
 - Group alert
 - View alert summary
 - View 1 alert details
 - View Investigation Graph
 - Mark not dangerous (Set False Positive) for 1 or many alerts
 - Create IR flow from 1 or many alerts
 - Add 1 or many alerts to IR flow
- Data authorization at the following features:
 - User login under root group: Display all alerts in the system.
 - User login under default group: Display all alerts belonging to the default group.
 - User login under parent group: Display all alerts belonging to the group of the user logging in and the corresponding child-level group.
 - User login under a group with one child-level group or many child-level groups:
 Display all alerts belonging to the group of the user logging in.

4.1.1. Search Alerts

Allow creating a query command, using a stored query command or quickly searching to search for an alert by the time that the alert was generated.

4.1.1.1. Search by Time

• Default when accessing the system, search alert according to the last 7 days.







- Allow changing time value by selecting absolute time or relative time
 - Absolute time: A specific start time end time value, which allows entering or choosing from the calendar and supports dd/mm/yy, hh:mm:ss format.
 - Relative time: A relative time between the start time and current time.

For example, it is currently 3 am on 07/06/2021, select start date is "Last 30 days". The system automatically searches the last 30 days and starts from 03:00 hour of that day. \rightarrow Monitoring period: 03:00 08/05/2021 to 03:00 07/06/2021.

4.1.1.2. Quick Search

Quick Search supports quick alert search by fields:

- Time: Time to generate alert
- State: The state of the alert
- Severity: The severity of the alert
- Scenario: The scenario that generates the alert.
- Assigned to: The person assigned to handle the alert.

4.1.1.3. Search by Query

Use saved query *

This function allows to search by query in 2 below ways:

- Use the previously saved query to search
- Enter the query to search
- 4.1.1.3.1. Use Previously Saved Query to Search
- Step 1: Select the previously saved query at the Use saved query combo box.
- Step 2: Review the query content before selecting by selecting .

In case of deleting the old query, move the cursor to the record to delete and select .

• Step 3: Click on the record to use in order to query, the old query content is displayed in the query input box.

Q



Q Search name auto test 2 ▼ host_name = "ADMIN-PC" testauto ▶ test test ▶ Hello ▶ test20 ▶ test15 ▶ test13 ▶ test12 ▶ test12 ▶	Use saved query $*$ fx host_name = "ADMIN-PC"	
auto test 2 host_name = "ADMIN-PC" testauto > testauto > test > Hello > test20 > test15 > test13 > test12 > test12 > test12 >	Q Search name	
host_name = "ADMIN-PC" testauto ▶ test ▶ Hello ▶ test20 ▶ test15 ▶ test13 ▶ test12 ▶ test12 ▶	auto test 2 🔻	
testauto > □□ test > □□ Hello > □□ test20 > □□ test15 > □□ test13 > □□ test12 > □□ test12 > □□ test12 > □□	host_name = "ADMIN-PC"	
test > III Hello > III test20 > III test15 > III test13 > III test12 > III test12 > III	testauto >	111
Hello ► III test20 ► III test15 ► III test13 ► III test12 ► III -test ► III	test ⊳	111
test20 ▶ III test15 ▶ III test13 ▶ III test12 ▶ III -test ▶ III	Hello >	1
test15 ▶	test20 ►	1
test13 ▶	test15 ►	1
test12 ⊳ III -test ⊳ III	test13 ▶	
-test ▶ 🔟	test12 ▶	
	-test ▶	

In case of adding or editing the query content, enable to enter right on the query

box and select Save query to save.

Notes: The Save query button is only displayed when the query has correct structure.

4.1.1.3.2. Enter a query to search

• Step 1: Enter query into the Search textbox with the following format:

<field_name> <operator> "<value>" AND/OR <field_name> <operator> "<value>" In which:

<field name> are the following values:

- Severity: The severity of the alert.
- Alert id: Alert code.
- State: The state of the alert.
- Group: The group of the event that generates the alert.
- Hostname: Name of the workstation.
- Scenario: The scenario that generates an alert based on MITER ATT&CK.
- Ir_flow_name: The name of the IR flow to which the alert belongs to that IR flow.
- Assignee: The person assigned to handle the alert.
- Signature_id: Event code that generates the alert.



- Rule id: Code of the rules generating alerts
- Description: Describe the context information the alert generated.
- <operator> are the following values:
 - =: Find an exact value as the value
 - I=: Find a value other than the value
 - ~: Find a value including the value
 - AND/OR: Combination operators to combine 2 queries.
- Step 2: Click on Search.
 - In case there is no matched result, the system will display the notification as No data.
 - In case there is a matched result, the system defaults to display 50 records in descending order by time. To view more records, scroll the data to the bottom of the page, the system will load the next 50 records.
- Step 3: In case the query has the correct structure to save it for future usage, select

^{Save query} and enter a name to remind the query:

query 1		
4		

Notes: The

Save query button is only displayed when the query has correct structure.

4.1.2. Alert List

This function allows to view a list of alerts that meet the search condition.

3 resi	ilt(s)									🗐 😃 🔯 Group alerts by 🔻	Vie	ew colu	ımn ▼
	SEVERITY \$	TIMESTAMP_CREATE ¥	TIMESTAMP_CLOSE \$	ALERT_ID \$	STATUS \$	GROUP \$	HOST_NAME \$	SCENARIO \$	IR_FLOW_NAME \$	DESCRIPTION \$	N	CTION	
	HIGH	16:23:19 10/06/2021	N/A	20210610_92321_102926463_784417	• New	default	WIN10X64	Malware	N/A	[IOC] Detect process [nul >	2	2	0
	HIGH	16:17:32 10/06/2021	N/A	20210610_91734_461280860_412414	• New	default	ANM-BICHPT3	Malware	N/A	[IOC] Detect process [nul >	5	2	0
	LOW	15:56:16 10/06/2021	N/A	20210610_9111_314657586_582156	• New	default	WIN10X64	Privilege Escalation	N/A	Detect process [null] (PI +	5	2	0

Step 1: Select View column * to select the fields to display on the Alert List.





Here, searching information fields by field name is allowed and select/deselect all fields are supported.

- Step 2: On the list, the operations are supported as follows:
 - o Sort by data in each column

For example, to sort the data by the creation time field, click **THESTAMP_CREATE** the first time at the field name to sort by the ascending creation time, click **THESTAMP_CREATE** the second time to sort by the descending creation time, click the third time to remove the sort and return to original state **THESTAMP_CREATE** .

o Drag and drop the information field to the desired position

STATUS	GROUP 🖨	IOST_NAME 🗣	DESCRIPTION 🜩		IMESTAMP_CREATE 븆		SCENARIO 荣	
• New	default	VIN10X64	[IOC] Detect process [nul ▶		6:23:19 10/06/2021	HIGH	Malware	
• New	default	им-віснртз	[IOC] Detect process [nul ▶		6:17:32 10/06/2021	HIGH	Malware	
• New	default	VIN10X64	Detect process [null] (PI ►		5:56:16 10/06/2021	LOW	Privilege Escalation	
	1. Chọn trư	ờng muốn thay đổi vị trí		2.	Kéo đến vị trí mới			

- Click once to view summary information, view details at section 3.3.4 View Alert Summary.
- Click twice or select ⁽ⁱ⁾ to view detailed information, view details at section
 3.3.4 View Alert Summary.
- Select ⁴ to mark Not Dangerous for alert, view the marked case of 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.
- Select ² to insert alert into IR Flow, view the inserted case of 1 alert into an existed IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow or into a new IR Flow at section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert Group.

Page | 25



- Select state to view the reason for marking Not Dangerous in alerts that are in the FALSE POSITIVE state.
- Step 3: After completing the actions on the records, selecting one or more records is allowed by clicking
 at the top of each alert to continue performing next actions with the below supported actions.

Selected 3 a	alert(s)	Add to IRFlow	📳 Set false po	ositive 📃 🛃	Export selected alert(s)	Clear select	kon					
SEVER	RITY 1	TIMESTAMP_CREATE	TIMESTAMP_CLOSE	ALERT_ID		STATUS	GROUP	HOST_NAME	SCENARIO	IR_FLOW_NAME	DESCRIPTION	ACTION
MEI	DIUM	09:17:38 11/06/2021	N/A	20210611_2184	41_450884396_801941	• New	default		N/A	N/A	Test KIAN Alert	
MEI MEI	DIUM	09:17:38 11/06/2021	N/A	20210611_2184	43_451494270_398683	• New	default		N/A	N/A	Test KIAN Alert	
ME	DIUM	09:17:38 11/06/2021	N/A	20210611_2184	18_455351315_775451	• New	default		N/A	N/A	Test KIAN Alert	
ME	DIUM	09:17:38 11/06/2021	N/A	20210611_2185	52_462470354_542493	• New	default		N/A	N/A	Test KIAN Alert	

• Select Add to IRFlow to add the selected alert to the IR Flow for processing.

Notes: This action is only applied when all selected alerts are in NEW state. If there is at least one alert in state different from NEW, the action will be hidden the button. View details in case of adding 1 alert to a new IR Flow at section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert Group or add to an existing IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow.

• Select Set false positive to mark Not Dangerous for alert.

Notes: This action is only applied when all selected alerts are in NEW state. If there is at least one alert in state different from NEW, the action will be hidden the

Set false positive button. View details in case of marking Not dangerous 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.

• Select Export selected alert(s) to export the currently selected alert.

4.1.3. Group Alert

This function allows to group alerts by one or more criteria, including: hostname, scenario, group and RuleID.

• Step 1: After searching, alerts can be grouped by selecting Group alerts by to select the criteria to use as alert grouping criteria.



-	📴 Group alerts by
Q S	earch field
	Select all
	host_name
	scenario
	group
	rule_id
	Арріу

Support searching by criteria name and selecting 1 or more criteria to group

• Step 2: Select Apply to apply.

Alerts that have the same selected criteria and same state and are in the same IR Flow (if any) will be grouped into 1 row in the result list.

2	1 re	ult(s)									e	Group alerts by *	new colum	n v
		SCENARIO \$	HOST_NAME \$	GROUP \$	SEVERITY \$	TIMESTAMP_CREATE *	TIMESTAMP_CLOSE \$	ALERT_ID 🗘	STATUS 🛱	IR_FLOW_NAME \$	DESCRIPTION \$,	CTION	
		Malware	WIN10X64	default	MEDIUM	17:53:53 10/06/2021	N/A	20210610_105355_63452087_644270	In Progress	liennt_dashboard_close	[T1543.003] Windows Servi	Þ		
		Malware	WIN7X86-A-PC	default	HIGH	10:42:33 10/06/2021	N/A	20210610_34234_517154921_141482	• New	N/A	[IOC] Detect process [nul >		5	•
	0	33 allert(s) in group Malware	ANM-BICHPT3	default	нібн	09:40:59 04/06/2021	N/A	20210611_12543_444783129_799979, 20210611_12144_236343336_627307 and 31 others	• New	N/A	[T1547.001] Registry Run ≯		ş	2
		Malware	KHAITB	default	HIGH	14:02:51 03/06/2021	N/A	20210603_7252_652579214_467528	New	N/A	[IOC] Detect process [nul >		Ş	2
		Malware	ANM-CHUYENNT2	default	HIGH	06:53:42 02/06/2021	N/A	20210601_235343_653743842_344462	In Progress	HoaNN test	[IOC] Detect process [C:\ >			
	0	66 alert(s) in group Malware	WIN7X64-A-PC	default	HIGH	16:29:41 01/06/2021	N/A	20210611_22912_397509963_480283, 20210610_212644_79442733_693462 and 64 others	New	N/A	[IOC] Detect process [C:\ >		5	2
		5 alert(s) in group Malware	VUONGLVMTEST	default	HIGH	15:31:40 01/06/2021	N/A	20210602_2635_224577402_753210, 20210601_161543_266010266_987263 and 3 others	New	N/A	[IOC] Detect process [nul ►		Ş	2
	0	7 alert(s) in group Malware	TEST_SEABANK_KH	dattest2	HIGH	13:11:40 28/05/2021	N/A	20210528_6472_820898530_774157, 20210528_6438_322265580_874336	• New	N/A	[T1543.003] Windows Servi	Þ	5	A

In which:

- \circ $\;$ Fields used as grouping criteria will be bolded.
- \circ The number of grouped alerts is displayed at the selected criteria.
- Step 3: To ungroup, perform the same actions but do not select any criteria and select Apply only.



	Select all host_name	
	scenario	
	group	
	rule_id	

4.1.4. View Alert Summary

This function allows to quickly view the alert summary information.

• Step 1: Click once on the alert to view the summary, the following information is displayed:

 ARTIFACTS	 OBJECTS	00:00:46:27 TIME TO DETECT	:: TIME TO RESPONSE
Add to IR flow		🗐 Set false positive	
General information			
ASSIGNEE	Unassig	ned	
DESCRIPTION	[IOC] De	etect process [C:\Windows\explo	orer.exe] (PID: [1628]) >
SROUP	default		
HOST NAME	WIN7X6	4-A-PC	
R FLOW NAME	N/A		
LINK	N/A		
RULE ID	Window	vs_Malware_ZeroDay_Taskschee	duler
SCENARIO	Malwar	2	
SIGNATURE ID	11		

- General information group of alert, in which:
 - Artifacts: List of suspicious objects automatically/ manually marked in alert.
 - Objects: List of objects in alert.
 - Time to detect: Total time to detect and investigate alert, from when the alert is generated to when it is inserted into the IR Flow or marked FALSE POSITIVE.
 - Time to response: Total alert processing time, from when the alert is inserted into IR Flow to when IR Flow is closed.
- Group actions with alert



- Select Addustor to insert alert into IR Flow, view the case of inserting 1 alert into an existed IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow or into a new IR Flow section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert Group.
- Select setate positive to mark Not dangerous for alert, view the case of marking 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.
- Select E View related events to switch to the Event Search feature with the default time of last 4 hours and after the time the alert generated.

Notes: The action of addition of and set the positive is only displayed for the alert in the NEW state, in case the alert is different from NEW, only the following were verified events button is displayed:

 ARTIFACTS	 OBJECTS	:: TIME TO DETECT	:: TIME TO RESPONSE	
	E	View related events		
General information	ı			
ASSIGNEE	root			
DESCRIPTION	Windows	executable load a module		
GROUP	default			
HOST NAME				
IR FLOW NAME	liennt_das	hboard_close		
LINK	N/A			
RULE ID	Load Imag	e		
SCENARIO	N/A			
Advanced informati	on			~

4.1.5. View Alert Details

This function allows to view detailed alert information, support automatic information enrichment by automatically collecting information about events related to the alert that has just arisen, and provide a visual chart to quickly view the relationship between objects included in the alert.



Alert detail New Medium CREATED 26/05/2021 10:5	20210526_35922_830373607_729431 921 - RESOLVED AT -→-+	 ARTIFACTS	 OBJECTS	16:00:16:26::: TIME TO DETECT TIME TO RESPONSE	 Enhancing	Add to IRFlow	Set false positive	ः Tiew related events
Group default	Host name WINTX84_MAYAOHA	Ć	Scenario Malware	IR flow N/A		C Assignee Unassigned		Assign time N/A 1
							Unknown 📕 Clean	Suspicious 📕 Malicious
								:
								۲
								Q (*
3								÷
DESCRIPTION		General			Advanced			
	Сору	GROUP	default		AGENT ID	29B78C1C37B926E	6EA90F9E810204B5D1F682	31C
LINK	https://confluence.viettelcyber.com/display/CON/CON+- +%/SBT1543_003%/5D+-+Windows+Service	EVENT LOG ID	N/A		AJIANT EVENT ID	13		
		SIGNATURE ID	13		CLIENTID	29B78C1C37B926E	6EA90F9E810204B5D1F682	31C
		RULEID	Anomaly_Detection	_ATTCK_T1543_003_Windows_Service_Correlation	CREATE TIME	2021-05-26T03:59:	22Z	
					HOSTNAME	WIN7X64_MAYAOH	A	
					LOG CHANNEL NAME	N/A		
4					LOG PROVIDER NAME	N/A		

- General information group of alert, in which:
 - o Artifacts: List of suspicious objects automatically/ manually marked in alert
 - Objects: List of objects in alert
 - Time to detect: Total time to detect and investigate alert, from when the alert is generated to when it is inserted into the IR Flow or marked FALSE POSITIVE.
 - Time to response: Total alert processing time, from when the alert is inserted into IR Flow to when IR Flow is closed.
 - Enhancing: The completion rate of the system's automatic information enrichment process.
- Group actions with alert
 - Select Actualized to insert alert into IR Flow, view the case of inserting 1 alert into an existed IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow or into a new IR Flow at section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert Group.
 - Select set to mark Not dangerous for alert, view the case of marking 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.
 - Select vevretated events to switch to the Event Search feature with the default time of last 4 hours and after the time the alert generated.
- Investigation Graph: View details at section 3.3.5 Investigation Graph.
- Information tab related to alert: Currently only Alert Detail is supported.



4.1.6. Investigation Graph

This function allows to display the object relationship in the alert, view the object details and support the spill investigation based on the set of events collected in the system.



1 - Graph display area and graph actions

- 2 Detailed information display area of objects on the graph
- 4.1.6.1. Graph Display Area and Graph Actions
- This function allows to visually display the objects in the alert for information view and investigation.
- By default, when accessing, the graph displays information related to the original machine that generates an alert, specifically as follows:



• In the graph, there is always a flagged F machine to mark the original machine that generates the alert, and by default, each machine always comes with the objects that have a direct relationship with the original machine within 1 day from the time the alert is generated. The list of objects includes as follows:



NETWORK	DEFAULT					
USER	O DEFAULT					
REGISTRY	DEFAULT	KEY	VALUE			
FILE	DEFAULT	DOC	X EXCEL Æ	POWERPOIN	IT	
		<%> .ASP	{} .JS	 .PHP	SCPT	VBS .VBS
HOST	2	SERVICE	¢°	PROCESS	C.	
SCHEDULED TASK	Ľ _o	DNS QUERY	DNS	WMI	¢. wmi	

- Each object includes the following state:
- Among objects, the relationships are displayed, including:
 - Relationship: The relationship is defined according to the events arising within 1 day from the time the alert is generated (where the relationship name is above the solid line arrow connecting 2 objects.):



📕 Unknown 📕 Clean 📒 Suspicious 📕 Malicious

 Reference: Reference relationship, which is other objects recorded in the main event that generated the object (shown by a dashed line arrow and without a specific relationship name):

-----Þ

For example:





• Actions to support graph display, including:

Display support actions	Meaning
Hide reference	Enable to hide/show information on the graph, including:
Hide relationship name	• Reference: When selected, enable to hide/ show reference information, including dashed line arrow and reference object at all existing objects on the graph.
	• Relationship name: When selected, enable to hide/ show the relationship name information above all existing solid line arrows on the graph.
Q	Enable to zoom in/ zoom out the corresponding graph at the
Q	position of the pointed cursor.
	In addition, enable to roll the cursor the desired position to zoom in/ zoom out for quick action.
\$	Enable to return to the graph center (original machine).
25	Enable to zoom in the maximum screen in order to view graph
TE	and perform action on it.

Page | 33



• An example of a default graph as follows:



- In case each object type has more than 1 dependent object, the objects will be automatically grouped.
- Hover to view quick statistics at each object group as follows:



- From here, for further spill investigation to the objects, perform the following steps:
 - Step 1: Click on the group of objects to view, the interface is displayed as follows:

Obje	Objects in this group network X									
Q	Q Search object Q									
2 Uni	known (48) 🗹 Clean	(125) Malicious (87)				View column ▼				
ielecte	ed 1/20 node(s) 🛛 🗖 Sho	w on graph Clear selection								
	STATUS	DOMAIN ADDRESS	IP	LOCAL PORT	PROCESS NAME	ACTION				
~	• Clean	ocsp.verisign.com	240.100.28.3	N/A	SYSTEM	ę				
	• Clean	crl4.digicert.com	80.105.28.3	N/A	SYSTEM	ę				
	• Clean	crl.microsoft.com	16.87.28.3	N/A	SYSTEM	Ø				
	Malicious	www.microsoft.com	96.103.28.3	N/A	SYSTEM	Ø				
	Clean	ocsp.digicert.com	240.94.28.3	N/A	SYSTEM	Ę				
	• Clean	crl.verisign.com	224.91.28.3	N/A	SYSTEM	Ø				
	Malicious	www.msftncsi.com	0.96.28.3	N/A	SYSTEM	Ę				
	• Clean	csc3-2010-crl.verisign.com	112.89.28.3	N/A	SYSTEM	Ę				
	Clean	ocsp.globalsign.com	48.88.28.3	N/A	SYSTEM	Ę				
	Clean	crl4.digicert.com	80.105.28.3	N/A	SYSTEM	۳Q				



- Enable to filter objects in the group by state
 Unknown
 Clean
 Suspicious
 Malicious
 or quickly search by entering the data to search in all fields.
- When a suitable object selected, select
 to display 1 object on the graph or select
 to select up to 20 objects on the graph.

Notes: If the expanded object is a computer, when the object is displayed by default, the objects that have direct relationships to the computer within 1 day from the time the alert generated are also automatically displayed.



- Step 2: After displaying the objects to be investigated on the graph, the below support actions enable to expand/ collapse are displayed:
 - At the original machine/ normal computer: Support collapsing objects to the default state when displaying the machine (Only include objects that have a direct relationship with the machine and for each object type if there is more than 1 object inside, a group form is displayed) by right-clicking on the object, then selecting Group child-level objects.



 At other objects: Support collapsing by grouping by object type and relationship type with objects of the same level by right-clicking on the object, then selecting Group same-level objects.

Page | 35





 At the object is a process, allow expanding for spill investigation by rightclicking on the object,

In case it is not possible to continue the spill, the following is displayed:



In case of the spill, select Add more objects...



The interface that allows selecting the object to be spilled is displayed as follows:

Show more object			10.03.1 5.03			×
Files 1	Create Key Delete Value	Set Value				2
Network 5 Process 3	Q Search object					٩
Registry 3	Malicious (3)					View column 🔻
	🗌 STATUS 🌲	DOMAIN ADDRESS 🚔	IP 🖕	LOCAL PORT 荣	PROCESS NAME 💂	ACTION
	Malicious	N/A	127.0.0.1	1588	main.exe	ĘČ
-	Malicious	N/A	127.0.0.1	6668	main.exe	Ę
	Malicious	N/A	0.0.0	0	main.exe	۳Q
						3
1						


- Select object type
- o Select the relationship type from process to object
- Directly select the object to display. Support searching by object's Malicious or Clean state or searching by content in the object's information fields.

Select vew column to select the display information fields or use the feature to sort information in the list.

When a suitable object is selected, select a to display 1 object on the graph or select to select up to 20 objects on the graph.

• At the object which is a process, when there are objects being expanded, it is allowed to collapse by right-clicking on the object as follows:

mai	Add more objects	
	Collapse all	
ſ	Unpin	_

position. To cancel the Pin action, select

• By default, in the graph, objects automatically run and keep their distance from each other when moved. In case of using the cursor to select and drag and drop objects, after removing the cursor, the object is automatically pinned to a new

Unpin

3	
	Add more objects
(Collapse all
l	Jnpin

4.1.6.2. Detailed Information Display Area

As an additional feature of the graph, allow displaying detailed element information in the graph (including objects and relationships in the graph).



Host detail		>
General		
HOST NAME	Win7x64_MayaoHai	3 Сору
HOST ID	fe2a4ba0-b348-4a43-bd26-79995feb57e9	
STATUS	Offline	
SET UP VERSION	N/A	
GROUP	default	
UPDATE GROUP	release	
POLICY	full_features	
IP DCN	10.61.188.2	
os	windows	
FIRST PING	12/05/2021 16:02:02	
LAST PING	26/05/2021 14:23:17	1
Platform		~
CPUs		~
Network Interfaces		~
Default Gateway		<mark>2</mark> ~

- Group of general information: Including general information/identifying information of the object and always displayed when accessing.
- Detailed information group: Include detailed information of object classified into different information groups which will be closed by default, select \checkmark to expand and display the information group.

The **Copy** action supports copying the information field content.

Notes: Some object identifying information fields allow quickly linking to look up in Event Search or Agent Management.



Process detail	×
General	
PROCESS ID	1432
PROCESS NAME	main.exe
MD5	1e092a44d44c29ef8d6bfc3a74f34b73
SHA26	1941d3f261033344b22c5e9cf246e5683c17d450ac87d0af6f 3ed7a52f431bb6
PROCESS PATH	C:\users\admin\desktop\taodataloang\main.exe
FILE COMPANY	N/A
FILE DESCRIPTION	N/A
FILE VERSION	N/A
FILE PRODUCT	N/A
USER NAME	admin
COMMANDLINE	.\main.exe
INTEGRITY LEVEL	HIGH

4.1.7. Mark Not Dangerous for 1 Alert/Multi-Alert or Alert Group

This function allows to mark alert as Not dangerous and Not continue processing as follows:

- Step 1: Select 1 alert or multi-alerts to mark as Not dangerous.
- Step 2: Click on the Set False Positive button (Set False Positive button is only displayed in record with the NEW state as or all selected records are in NEW state.)



Cancel

4.1.8. Create IR Flow from 1 Alert/Multi-Alert or Alert Group

- Step 1: Select 1 alert/multi-alerts to create IR Flow.
- Step 2: Enter the information and create IR Flow.



Create New IR Fl	ow	×
IR flow name	Type IR flow name	
Assigned to	Choose assignees	
Alert(s)	20210611_34330_331623754_076066 ×	
First note	All alert(s) above will be added to IRFlow Type first note	
	Cancel	

The data displayed in the Assigned to combo box include as follows:

- \circ $\:$ User login under root group: Display all user names in the system.
- \circ User login under default group: Display the username of the current user login.
- User login under parent-level group: Display all user names belonging to the child-level group of the current user login and the own current user login.
- User login under a group of one or more child-level group: Display the username of the current user login.
- Step 3: After creating, the following window displayed to be able to undo in 10s:



- To undo: Select Undo for 10 seconds.
- To create an IR Flow immediately and switch to the IR Flow screen, select the name of the newly created IR Flow and then select New IR Flow.
- To back to the alert screen, select Alert List.

4.1.9. Add 1 Alert/Multi-Alert or Alert Group into Existed IR Flow

Same as the 3.3.5 section but do not select Add new IR Flow and select an existed IR Flow from the drop-down list only:



Q Search in dropdown list	
liennt_dashboard_inpro	
liennt_dashboard_close	11
20210607_anhnn_test	
Centos 6	11
HoaNN test	11
chuyen test UAT	
liennt centos6 6	
Add new IRFlow	
_	-



5. IR Flow Screen

5.1.1. Display List

- User login under root group: Display all IR Flow in the system.
- User login under default group: Display all IR Flow assigned to the current user login.
- User login under parent-level group: Display all IR Flow assigned to the user login and the users belonging to the respective child-level group.
- User login under a group of one or more child-level group: Display all IR Flow assigned to the current user login.

5.1.2. Search IR Flow

Only the records corresponding to the current user login can be searched.

Similar to the Search function in the Alert screen, the IR Flow screen supports searching by query as follows:

VEDR Portal		Alerts IR	Flow Investigation	on Response	Setting	③ en →	chuyennt2	- -
Search IR Flow							2	3
assignee = "hieupc4" AND status = "NEW"	1	L				Ð	Last 60 days	Q
4 result(s) 23/03/2019 17:17:53 - 22/05/2019	17:17:53						+ Add	new IRFlow
TIME	NAME	STATUS	CREATED BY	ASSIGNED TO	NOTATION			ACTION
17:34:12 02/05/2019	0205 test them artifact vào IRFLow	New	chuyennt2	hieupc4	dfdfd		C) 🕣
10:14:44 26/04/2019	2604 test4 che do multi chon 1 artifact add v ào IRFLow mới	New	chuyennt2	hieupc4	dfdff		C) 🕀
09:29:11 26/04/2019	2604 test2 multi chọn 1 artifact	 New 	chuyennt2	hleupc4	2333		C) 🕀
09:22:55 26/04/2019	2604 test multi add 1	New	chuyennt2	hleupc4	ddd		C) 🕀
Display 4/4 result(s)								

• Step 1: Enter into the Search query textbox with the following format:

<field_name> <operator> "<value>" AND/OR <field_name> <operator> "<value>" In which:

- o <field_name> are the following values:
 - Assignee: The person assigned to handle the alert.
 - Created by: Account to create IR Flow
 - Name: Name of IR Flow
 - Notation: IRFlow's note
 - State: State of IR Flow
- <operator> are the following values:

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi



- =: Find an exact value as the value
- !=: Find a value other than the value
- ~: Find a value including the value
- AND/OR: Combination operator to combine 2 queries.
- Step 2: Select the search period by clicking the Date & Time button and select an arbitrary time period. If not selected, the default is Last 7 days.
- Step 3: Click on Search.

In addition, search by history is also supported.

	VEDR Portal		Alerts	IR Flow	Investigation	Response	Setting	③ en -	chuyennt2	. .
Search IR Flow										
Type t	o search							1 👝 💿	Last 60 days	Q
Q	assignee = "hieupc4" AND status =	"NEW" AND Last 60 days	~ 2							
Q	assignee = "congnc9" AND Last 60	days							+ Add	d new IRFlow
Q	assignee = "congnc9" AND status =	"IN_PROGRESS" AND Last 60 days								ACTION
									C) Ð
Clear	history search	ào IRFLow mới		,					0) Ð
09:29:	11 26/04/2019	2604 test2 multi chọn 1 artifact	New	chuyennt2	hieupo	4	8888		C) Ð
09:22:	55 26/04/2019	2604 test multi add 1	New	chuyennt2	hieupo	4	ddd		0) Ð
Display 4	I/4 result(s)									

To view detailed information of 1 IR Flow and perform investigation and process, select IR Flow Detail.



5.1.3. How to Create a IR Flow?

• Step 1: Click Add new IR Flow.



Ð	Last	7 days	Q
		+ Add ne	w IRFlow
		ACT	ION
			i
			i

• Step 2: Enter valid information.

The data displayed in the Assigned to combo box include as follows:

- User login under root group: Display all user names in the system.
- \circ User login under default group: Display the username of the user logging in.
- User login under parent-level group: Display all usernames belonging to the child-level group of the user logging in and the user logging in.
- $\circ~$ User login under a group of one or more child-level groups: Display the username of the user logging in.

Create New IRFlow		×
IR Flow Name	IR Flow Name	
Assigned to	Choose assignees	
First Note	First Note	
	Cancel Create	

 Step 3: Click the Create button → the newly created IR Flow is displayed on the IR Flow Screen



5.1.4. Steps to Perform in IR Flow

- After creating IR Flow from alerts or pushing alerts into IR Flow, operator will go to IR Flow page to perform following actions:
 - View information to investigate: Alert list, computer with alert, related objects (file/registry/process).
 - Isolate alert generating computers: Isolate the network and process.
 - Investigate and detect alert-related objects (artifacts).
 - Response: Process the investigated results. For example, kill the malicious processes, delete malicious files, delete registry entries generated by malwares, etc.
 - Investigation close: Close IR Flow, stop isolating machine and close Process Analysis and Live Response sessions.

5.1.5. IRFLow - Detection

- Detection tab displays alert-related objects, such as:
 - Computer list with alert.
 - Alert list.
 - List of artifacts discovered during investigation.

			Detection	Containment	Investigation	Response		
Ori	ginal detection							
	Agent DESKTOP-HHN2B1Q							
	Alert							
	TIME	GROUP		HOSTNAME		SCENARIO		SEVERITY
	07:00:00 14/01/2019	no_group		DESKTOP-HHN2B1Q		Execution		High
	07:00:00 14/01/2019	no_group		DESKTOP-HHN2B1Q		Execution		High
	07:00:00 14/01/2019	no_group	,	DESKTOP-HHN2B1Q		Initial Acces	s	High
Ad	Additional detection							
	Aritfacts							
	TIME	AGENT ID		OBJECT			FROM	REFERENCE
	07:25:05 14/01/2019 9D76E75C81645C6B88E18B46961C5D75C8154752		1	c:\Users\Test\Desktop\demo.exe			WIN_EVENT_LOG	plq3SWgBTy9idpUvVJ-d
	07:25:05 14/01/2019	9D76E75C81645C6B88E18B46961C5D75C8154752		HKLM\SOFTWARE\Microsoft\Wind	ows\CurrentVersion\Run\demo		WIN_EVENT_LOG	plq3SWgBTy9idpUvVJ-d

- Objects in the Original Detection section: Be as initial alerts (Alert) and computers (Agent) when IR Flow is created.
- As for the objects in the Additional Detection section: As the alerts, computers, artifacts added at the investigation step (Investigation).
- Meaning of some fields on the Detection screen:



- Time: Time to add agent/artifact to the Detection screen.
- Object: File/registry path of artifact.
- From: Source of generating artifact (Event log or Process Analysis).
- Reference: ID of event log or ID of Process Analysis connection session.

5.1.6. IRFlow - Containment

Containment tab allows isolating 1 or more computers in the Detection or Suspend tab the process in the alert located in IR Flow.

Containment state includes as follows:

- NOT APPLIED: The command to agent is not sent.
- APPLYING: The command to agent is being sent.
- APPLIED: The isolation command is sent successfully.
- STOPPING: The isolation stop command is being sent.
- STOPPED: The stop isolation command is sent successfully.
- Step 1: Select the investigation method: Isolate the network or suspend the process and then select Next Step.

		Detection	Containment	Investigation	Response	
- 1	Rule setting Choose one rule setting to continue next step					2 Next Step
1 •	Network containment					
	Process containment					
- 2	Deploy to agent					
	Agent list Choose agent in list below and click move right button to add to apply agent list			Agent apply list Click		🕨 Start
			NOT APPLIED			
		- Detection	Containment	investigation	Response	2
1	Rule setting Choose one rule setting to continue next step					Next Step
	Network containment					
	Process containment (Create rules) Puth/PID 5678					
	Type 2 en press Enter terreste new rule					

Notes: After entering Path/PID, the Enter button must be pressed to save the configuration. The multiple processes can be suspended at the same time.

• Step 2: Select the list of Agents to isolate and select Start to start isolating.



1	Rule set	ting						Edit Setting
	۲	Network containment						
		Process containment						
2	Deploy t	o agent						
		Agent list (1 agent selected) Choose agent in list below and click move	e right button to add to apply agent list		4	Agent apply list Click Start button to apply rule for list agent below	_5 →	► Start
		DESKTOP-J1VS222 Agent_id: 2A29678CD57CEC904C85D414E5382288F6F876E5	no_group	NOT APPLIED	»			
3-	> 🛛	WIN7-CONGNC Agent_id: 4CE4695ED33F65799C1EF9666452765077642A83	no_group	NOT APPLIED	«			
		DESKTOP-HHN2B1Q Agent_id: 9D76E75C81645C6B68E18B46961C5D75C8154752	no_group	NOT APPLIED				

• Step 3: To stop isolating, click Stop or select agent in the Agent apply list button and switch back to Agent List.

Agent apply list				(Stop
DESKTOP-EGANUBQ Agent_id: B2A03630B8EEA76B1D5B7105B70DD4F4	DE5E593E		no_group		APPLIED •
2 Deploy to agent Agent list			igent apply list		Stop
DESKTOP-HHN2B1Q Agent, de 807667503144506886138446810507508154752 nbandid-PC	no_group NOT APPL		ESKTOP-EGANUBQ gent_id: 8240585088EEA76810587105870004F4DE3E583E	no_group	APPLIED •
Agent, id: B0677B363962C77626887C5988657B080C3285 Win7-CongNC9 Agent, id: 4C54690203766709C18596664027607764D485	no_group NOT APPL	ED • Edit			
		1			
2 Deploy to agent					
Agent list Choose agent in list below and click move right button to add to apply agent list			Agent apply list (1 agent selected) Click Start button to apply rule for list age	ant below	Stop
DESKTOP-HHN2B1Q Agent_id: 9076675C31645C6888E18846961C5075C8154752	no_group NOT APPLIE		DESKTOP-EGANUBQ Agent_id: B2403650886EA7681D587105870DD4F4DE5E583E	no_group	APPLIED .
hhandt4-PC Agent_id: BotFT8559EECT762688TCC968655FBDe5DC5265 WIN7-CongNC9	no_group NOT APPLE	see 2	2		
Agent_id: 4CE-A605ED35F65T99C1EF9666452T65CT7642A83					
		4			

In case the administrator does not actively stop the isolation on the Portal, after the default time (24h), the Agent will also automatically remove the isolation under the Agent.

5.1.7. IRFLow - Investigation

5.1.7.1. Process Analysis

5.1.7.1.1. View Process Information

This is the process of analyzing the processes on the user's machine in the Detection tab in real time to look for anomalies.

Step 1: Select the agent to connect, then click Start. Agent List is Agents in IR Flow.



Choose Agent to
 DESKTOP-HHN2B1Q (9D76E75C81645C6B88E18B46961C5D75C8154752) nhandt4-PC (B0EF7B3E39EEC77626B87CC988653FBD63DC8285)
 DESKTOP-EGANUBQ (B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E)
Win7-CongNC9 (4CEA695ED33F65799C1EF96664527650776A2A83)

Notes:

٠

- Timeout to create a connection is 60s. After 60 seconds, if the Agent cannot be connected, it needs to be reconnected.
- At a time in 1 IR Flow, only 1 connection to the Agent can be created. In case there is another account connecting to the Agent in the same IR Flow, an error notification will be displayed.





• Step 3: Select the process in the process list to view detailed information



Process Analysis	Q Event Search			🖓 Tools		□ Investigation result
SELECT AGENT Choose Agent to	PROCESS VESSVC.exe	Nomal Alert	Refresh 🛈	Agent Info	© STARTED 18:10 23/05/2019	C DURATION C STATE 0011115 Europine
			#	PROCESS INFO	LOADED MODULES	FILE HANDLE KEY HANDLE THREAD LIST S
			<u> </u>	USER	SYSTEM	
				COMPANYNAME	Viettel Corporation	
				PRODUCTNAME	Viettel Endpoint Detectio	n & Response
				FILEVERSION	0.1.0.756	3
				PROCESSPATH	C:\Program Files\VEDR\V	ESSvc.exe
				COMMANDLINE	C:\Program Files\VEDR\\	/ESSvc.exe*
				PPID	936	
	VESS/vc.exe			MDS	4dcde72caf86954738022	504bd50a433
				SHA256	9d4c4d07a568ca3abfbee	35d89d4c3a0772792f693c643135fc31e052a6cc962
				PROCESSENV	ALLUSERSPROFILE=C:\Pr	ogramData; APPDATA=C:\Windows\system32\config\systemprofil
		xà		PID	5976	
VESConfiager.exe VESConneager.exe	VESUpdater.exe VESCollector.exe VESResp	ponselexe				

- Area 1: Select agent and process.
- Area 2: Display process tree information. The default displays 1 parent level and 1 child level. Allow expanding/collapsing the levels when clicking on a process in the tree. Processes that is focused in the tree will display an icon different from the process that is not focused.
- Area 3: Display focused process information in the tree, including information on tabs: Process info, Modules (loaded dll), File handles, Key handles, Thread List, Section handles and Network Connection.
- Step 4: To get the latest information of the process, click the Refresh icon on each tab.

Agent Info					
HOST DESKTOP-EGANUBQ	STARTED 18:10 23/05/2019	OURATION 00:26:31	受	STATE Running	
PROCESS INFO C	LOADED MODULES	FILE HANDLE	KEY HANDLE	THREAD LIST	S 🕨
USER	SYSTEM				
COMPANYNAME	Viettel Corporation				
PRODUCTNAME	Viettel Endpoint Detectio	n & Response			
FILEVERSION	0.1.0.756				
PROCESSPATH	C:\Program Files\VEDR\VI	ESSvc.exe			
COMMANDLINE	C:\Program Files\VEDR\\	/ESSvc.exe"			
PPID L	936				
MD5	4dcde72caf86954738022	504bd50a433			
SHA256	9d4c4d07a568ca3abfbee	35d89d4c3a0772792	f693c643135fc31e0)52a6cc962	
PROCESSENV	ALLUSERSPROFILE=C:\Pr	ogramData; APPDAT	A=C:\Windows\syst	em32\config\system	nprofil
PID L	5976				

Notes:



- When switching sub-tabs in Investigation, such as Event Search, Tools and Investigation Result, the connection session with Agent is kept and no need to reconnect.
- When switching to other tabs, such as Detection, Containment, Response, Alert, Setting, etc. or F5, Logout, etc., the connection session with Agent needs to be reconnected.
- The Process Analysis connection session in IR Flow only closes when the administrator closes IR Flow. That is, if the IR Flow is not closed, every time when entering IR Flow and connecting to the Agent, the ID of the connection session does not change.

5.1.7.1.2. Marking/Get Artifact

- Marking artifact function allows marking the artifact to be tracked. The following data can be marked:
 - Process Info: Process Path
 - Loaded module: Path
 - o File Handle: Path
 - Key Handle: Key path and Value
- Step 1: Select any record and hover over that record. Click on the Marking artifact button.

Agent Info					
B HOST DESKTOP	eganubo 14	ARTED 1:34 24/05/2019	OURATION 00:41:42	STATE Runn	ing
∢ IFO LO	ADED MODULES 😋	FILE HANDLE	KEY HANDLE	THREAD LIST	SECTION LIST
NAME	PATH	MD	5	SHA256	COMPANY NAME
VESSvc.exe	📙 C:\Program F	R\VESSvc.exe 🛛 🏥	4dcde72caf869547	. 🕒 9d4c4 Marking art	ifact t Get Artifact
ntdll.dll	🕒 C:\Windows\S	.32\ntdll.dll 🏻 [87f19276e5f6f799b	. 🍺 1c37cca54a534aac	I Microsoft Corpo
KERNEL32.DLL	🕒 C:\Windows\s	KERNEL32.DLL 뱐	038b10c8e735fe66	. 뱐 9d9d6fa334aa40b1	Microsoft Corpo
KERNELBASE.dll	📙 C:\Windows\s	.RNELBASE.dll 🌓	e202b8613c3e9171	.🍺 632e8ce10f414153	Microsoft Corpo
msvcrt.dll	🕒 C:\Windows\s	.2\msvcrt.dll 🛛 🏥	42e3a19087cca1f6	🌔 628ae302e49726fc	Microsoft Corpo
WS2_32.dll	📙 C:\Windows\s	.2\WS2_32.dll 📗	0e49b1e08df84848	. 🎒 8e56e5e0c3986223	3Microsoft Corpo
sechost.dll	📙 C:\Windows\s	\sechost.dll 🛛 🏥	2a6b77a72aea0c20	.🅒 86d38fc561acb046	Microsoft Corpo

• Step 2: Click the Accept button, enable to edit the file path when clicking on the Edit icon.



Agent Info HOST DESKTOP-	O STARTED EGANUBQ 14:34 24/05/2019	OURATION 00:44:11	STATE Running	:
∢ IFO LOA	DED MODULES G	E KEY HANDLE	THREAD LIST	SECTION LIST
NAME	PATH	MD5 S	HA256	COMPANY NAME
VESSvc.exe	C:\Program FR\VESSvc.exe	比 4dcde72caf869547 🛽	9d4c4d07a568ca3a	Viettel Corporat
ntdll.dll	E:\Windows\S32\ntdll.dll	🍺 87f19276e5f6f799b	1c37cca54a534aad	Microsoft Corpo
KERNEL32.DLL	C:\Windows\sKERNEL32.DLL	🌔 038b10c8e735fe66 🛽	9d9d6fa334aa40b1	Microsoft Corpo
KERNELBASE.dll	C:\Windows\sRNELBASE.dll	🍺 e202b8613c3e9171🌡	632e8ce10f414153	Microsoft Corpo
msvcrt.dll	C:\Windows\s2\msvcrt.dll	🌔 42e3a19087cca1f6 📗	628ae302e49726fc	Microsoft Corpo
WS2_32.dll	C:\Windows\s2\WS2_32.dll	🌔 0e49b1e08df84848	8e56e5e0c3986223	Microsoft Corpo
sechost.dll	📙 C:\Windows\s\sechost.dll	🍺 2a6b77a72aea0c20🌡	86d38fc561acb046	Microsoft Corpo
RPCRT4.dll	C:\Windows\s2\RPCRT4.dll	🍺 015b50451c5503fd 🛽	13e5d9833bde390	Microsoft Corpo
NSI.dll	C:\Windows\sem32\NSI.dll	🍺 dd1e88bc0333756 🛽	🖡 e3b794df433bd349	Microsoft Corpo
WINMM.dll	C:\Windows\S32\WINMM.dll	🍺 04b150189dce3afe 🛽	98b6eb826644cd5	Microsoft Corpo
Marking artifact PATH C:\Program Files\	VEDRIVESSVC.exe	And the later of	2 Accept	Cancel 🗙

In case of selecting a record with an Agent that does not exist in Detection, there will be an Add Agent to IR Flow check box. When performing Accept, the corresponding Agent will be added to Detection.

ILA 🚺	IANT		IR Flow	Investigat						ତ∂ EN •	root	
IRFlow Detail	- liennttesst5.5											
	💱 Process Analysis		Q Event S	earch			Tools			Investigation I	Result	
Search Log	Search Log									La	st 7 days	Q
POPULAR		≡ 210.621 result	is 18/05/2020 17:42:39 - 2	25/05/2020 17:42:39						V	iew column	~
AgentID		AGENTID				EVENTID	COMPUTER	LOGTYPE	SYSTEMTIMESTAMP	TIMESTAM	P	
Channel		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06		1	DESKTOP-EGANUBQ	EventLog	17:42:03 25/05/2020	17:20:56	25/05/2020	
CommandLine		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06		1	DESKTOP-EGANUBQ	EventLog	17:41:28 25/05/2020	17:20:21	25/05/2020	
Computer		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06		1	DESKTOP-EGANUBQ	EventLog	17:41:26 25/05/2020	17:20:19	25/05/2020	
EventID		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06		1	DESKTOP-EGANUBQ	EventLog	17:41:20 25/05/2020	17:20:13	25/05/2020	
EventRecordID		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06		1	DESKTOP-EGANUBQ	EventLog	17:40:57 25/05/2020	17:19:50	25/05/2020	
Image		7849229EFD1784DF6	SCF104722BD4EE0E27C36AD	06 M	larking art	ifact(s)					05/2020	
Keywords		7849229EFD1784DF6	SCF104722BD4EE0E27C36AD	D6	\CHUYEN	NT2 🖉					05/2020	
Level		7849229EFD1784DF6	SCF104722BD4EE0E27C36AD	06	C-\Windo	welevetam32					05/2020	
LogType		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06	- c. (mildo	anglystemsz v					05/2020	
OTHERS		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06	C:\Windo	ws\Microsoft.NET\	Framework\v4.0.30319\regasm.exe	0			05/2020	
Company		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06	C:\Windo	ws\Microsoft.NET\	Framework\v4.0.30319\RegAsm.exe	0			05/2020	
CurrentDirectory	v	7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06				-			05/2020	
Description		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06	Account	Cancel	~~~ ^		6	Add Agent To IR Flow	/05/2020	
FileVersion		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06		cancer				Add Agent To IR Flow	/05/2020	
Cuid		7849229EFD1784DF6	CF104722BD4EE0E27C36AD	06		1	DESKTOP-EGANUBQ	EventLog	17:39:26 25/05/2020	17:18:19	25/05/2020	
Guid		Display 50/210.621 n	esult(s)									

• After marked successfully, the notification is displayed. Click the View all artifacts in Investigation Result button to go to the Investigation Result screen. Artifact marked will be displayed on this screen.



Agent Info HOST DESKTOP-	-EGANUBQ	STARTED 14:34 24/05/2019	OURATION 00:45:22	्र STATE Runni	ng
∢ IFO LOA	ADED MODULES Ġ	FILE HANDLE	KEY HANDLE	THREAD LIST	SECTION LIST
NAME	PATH	ME)5	SHA256	COMPANY NAME
Marked artifact	C:\Windows\S	32\ntdll.dll	3 87†19276e5†6†799b.	View all Artifacts in Inv	restigation Result
KERNEL32.DLL	C:\Windows\s	KERNEL32.DLL	038b10c8e735fe66.	🏓 9d9d6fa334aa40b1	Microsoft Corpo
KERNELBASE.dll	C:\Windows\s	RNELBASE.dll 🍺	e202b8613c3e9171.		Microsoft Corpo
msvcrt.dll	C:\Windows\s	2\msvcrt.dll	42e3a19087cca1f6	. 🏥 628ae302e49726fc.	Microsoft Corpo
WS2_32.dll	C:\Windows\s	2\WS2_32.dll 🏼 🏥	0e49b1e08df84848.	🏓 8e56e5e0c3986223	Microsoft Corpo
IRFlow Detail - 2305 test1 ← IRFlow List TIMELINE ← 60 Create IR Flow	Containment Tool Deployed Agent (U Agent (U	Tool Depicyed Aren 10	las/	4004	Cicce Hillion
121 Process A	nalysis	Q Event Search	nment Nestigation	Kesponse	investigation result
Result DESKTOP-EGANUBQ DESKTOP-HIN2BLQ Marked Artifact TIME	Success (2/2) Success (0/1) OBJECT				
10:35:00 24/05/2019 10:35:00 24/05/2019	DESKTOP-EGANUBQ\0 C:\Windows\System33	HUYENNT2 taskhostw.exe			Added to IRFlow 🖌
14:21:57 24/05/2019 15:19:21 24/05/2019	C:\Windows\System32 C:\Program Files\VEDF	wbem\WmiPrvSE.exe \VESSvc.exe			Added to IRFlow 🖌
Search the web and Windows	0 🔳 👰	I V 4 8			▲ ⑨ Ř ● 図 〒 4 - 岡 B6 323M

- Get Artifact function allows getting file/registry information under Agent for investigation.
- Select a record and hover over that record. Click Get artifact button → Select artifact type (File/Registry) → Click Accept. Then check the result of performing Get artifact on the Investigation Result screen.



Agent Info					
	P-FGANUBO	STARTED 4:34 24/05/2019	OURATION 00:41:42	STATE Runn	ing
∢ IFO LC	DADED MODULES 😋	FILE HANDLE	KEY HANDLE	THREAD LIST	SECTION LIST
NAME	PATH	MI	D5	SHA256	
VESSvc.exe	📋 C:\Program F	R\VESSvc.exe 🛛 🌔	4dcde72caf869547.	🕒 9d4c4 Marking art	tifact t Get Artifact
ntdll.dll	📙 C:\Windows\S.	32\ntdll.dll 🛛 🌓	87f19276e5f6f799b.	🌔 1c37cca54a534aad	dMicrosoft Corpo
KERNEL32.DLL	📙 C:\Windows\s.	KERNEL32.DLL 뱐	038b10c8e735fe66.	뱐 9d9d6fa334aa40b:	1Microsoft Corpo
KERNELBASE.dl	l 뱐 C:\Windows\s.	RNELBASE.dll 🏾 🌔	e202b8613c3e9171.	🌔 632e8ce10f414153	Microsoft Corpo
msvcrt.dll	📙 C:\Windows\s.	2\msvcrt.dll 🛛 🌓	42e3a19087cca1f6	. 뱐 628ae302e49726fc	Microsoft Corpo
Get Artifact				3 Accept	Cancel 🗙
PATH	_				
C:\Program Files	\VEDR\VESSvc.exe	FILE ~ 2			

5.1.7.2. Event Search

This is the process of finding objects based on event logs. Unlike other tabs in IR Flow that only display information about Agents added to IR Flow, this tab displays all events of all Agents in the system.

5.1.7.2.1. Event Search



🕑 VEDR Portal - Event Search 🛛 🗙 🔛 VEDR Portal - IR Fi	low Detail 🗙 🚯 User-Role-Permit	ision - Viettel En 🗙 📔 🕂					- σ ×
← → C (m) ▲ Not secure 10.30.161.37/#/ir-flow	w/ir-flow-detail/27ac440795d30aa522	494d184a7e1389?tab=2					⊘☆♥ 🕫 😫 🕒 🛓 😂
		IR Flow					😚 EN 👻 chuyennt2 🕒 👻
Create IR Flow Containmen	nt						
		Detection	Containment	Investigation	Response		
Process Analysis		Q Event Search			다. Tools		Investigation result
					0		
Search Log AgentID = "B2A03630B8EEA76B1D5B710	05B70DD4F4DE5E593E" AND Channel = "	Microsoft-Windows-Sysmon/Op	erational" 1				2 Last 7 days Q 3
POPULAR	= 711 results 17/05/2019 08:	29:19 - 24/05/2019 09:29:19					View column 🗸 🗸
AgentID	AGENTID		EVENTID	COMPUTER	LOGTYPE	PLATFORM	CHANNEL
Channel	B2A03630B8EEA76B1D5B7105B70D0	WF4DE5E593E	11	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Computer	B2A03630B8EEA76B1D5B7105B70D0	MF4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
EventID	B2A03630B8EEA76B1D5B7105B70D0	04F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
EventRecordID	B2A03630B8EEA76B1D5B7105B70DD	MF4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Image	B2A03630B8EEA76B1D5B7105B70D0	4F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Keywords	B2A03630B8EEA76B1D5B7105B70D0	4F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Level	B2A03630B8EEA76B1D5B7105B70D0	04F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
LogType	B2A03630B8EEA76B1D5B7105B70DD	04F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
CommandLine	B2A03630B8EEA76B1D5B7105B70D0	04F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
OTHERS	B2A03630B8EEA76B1D5B7105B70D0	04F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Guid	B2A03630B8EEA76B1D5B7105B70D0	04F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Name	B2A03630B8EEA76B1D5B7105B70D0	04F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Oprode	B2A03630B8EEA76B1D5B7105B70D0	MF4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/ Marking artifact Get artifact ①
ProcessGuid	B2A03630B8EEA76B1D5B7105B70D0	MF4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
ProcessID	B2A03630B8EEA76B1D5B7105B70D0	MF4DE5E593E	3	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Processid	B2A03630B8EEA76B1D5B7105B70D0	WF4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
TargetFilename	B2A03630B8EEA76B1D5B7105B70D0	MF4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Task	B2A03630B8EEA76B1D5B7105B70D0	WF4DE5E593E	1	DESKTOP-EGANUBQ	EventLog		Microsoft-Windows-Sysmon/Operational
Search the web and Windows	o 📄 💽 S 🕽	1 10 10 10 10 10 10 10 10 10 10 10 10 10					∧ 🌃 🕢 🕅 💿 🕅 😨 🚛 🖪 ENG 🛛 \$30 AM \$/24/2019

• Step 1: Enter query into the Search textbox with the following format:

<field_name> <operator> "<value>" AND/OR <field_name> <operator> "<value>" In which:

- <field name> are the following values:
 - AgentID: ID of the agent
 - EventID: ID of the event
 - Computer: Name of the computer
 - LogType: Type of log
 - Channel: Channel of the event.
- <operator> are the following values:
 - =: Find an exact value as the value
 - !=: Find a value different from the value
 - ~: Find a value including the value
 - AND/OR: Combination operator to combine 2 queries.
- Step 2: Select the search range by clicking the Date & Time button and choosing an arbitrary time. If no time is selected, the system defaults to Last 7 days.
- Step 3: Click on Search.



- $\circ~$ In case there are no matching results, the system will display the notification: No data.
- In case there is a match, the system will default to 50 records in descending order of time with 5 default display columns, including: AgentID, EventID, Computer, LogType, Channel.
- To add a display column, click on View Column and tick to select the necessary fields.



- In addition, users can search for fields in the Popular and Others section by showing the values of the fields and hovering over the value in Popular/Others, that record will display 2 icons: "=" and "!=".
 - If the user selects "=", the Search textbox will display the query corresponding to the "=" operator.
 - If the user selects "!=", the Search textbox will display the query corresponding to the "!=" operator.
 - If there is data in the Search textbox and the user chooses to add values in the Popular/Others section, the two sides of the query are connected by the AND operator.



POPULAR
AgentID ^
B2A03630B8EEA76B1D5B7105B7(Add to search = z
Channel
Computer
EventID
EventRecordID
Image
Keywords
Level
LogType
CommandLine
OTHERS
DestinationHostname
DestinationIp
DestinationIsIpv6

- In the Others section, all fields of the log are displayed.
- When performing show/hide 1 field, 5 fields with the highest number of records sorted from highest to lowest will be displayed.
- When the user loads more, each record of field will be updated according to the number of records displayed on the screen.
 - \circ In the Popular section, 10 popular fields of the most searched log are displayed.
 - If there are >= 10 fields, the 10 fields with the highest number of searches will be displayed, if there are less than 10 fields, all those fields will be displayed.
- When performing show/hide 1 field, 5 fields with the highest number of records sorted from highest to lowest will be displayed.
- When the user loads more, each record of field will be updated according to the number of records displayed on the screen.
- When double-clicking on a record, the detailed information of that record will be displayed.
 - $\circ~$ The detailed information tab is displayed as a Table type, the data is displayed in the form of a table
 - \circ When selecting the JSON tab, the data is displayed as .JSON format.

5.1.7.2.2. Event Handle

Marking artifact: The artifact is marked.



🔄 VEDR Portal - Event Search 🛛 🗙 🔛 VEDR Portal - IR I	Flow Detail 🗙 🚯 User-Role-Permission - Viettel Er 🗴 🕂				- σ ×
\leftarrow \rightarrow C \bigcirc \land Not secure 10.30.161.37/#/ir-flo	ow/ir-flow-detail/27ac440795d30aa522494d184a7e1389?tab=2				⊘☆♥ 🤊 名 ⊖ 🛓 🥃
VEDR Portal	Alerts IR Flow	Investigation	Response Setting		🕃 EN 👻 chuyennt2 😩 💌
IRFlow Detail - 2305 test1 ← IRFlow List					
TIMELINE 66 Create IR Flow Containme	int				Close INflow
	<u></u> Detection	Containment	Investigation Res	oonse	
Process Analysis	Q Event Search		🖸 Tools		Investigation result
Search Log AgentiD = "B2A03630B8EEA76B1D5B7	105B70DD4F4DE5E593E" AND Channel = "Microsoft-Windows-SysmoniOpera	ational'			Last 7 days
POPULAR	= 738 results 17/05/2019 09:40:03 - 24/05/2019 09:40:03				View column 🗸
Agentu	AGENTIO	EVENTID	COMPUTER	LOGTYPE	
B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E (100)	B2403630B8EE476B1D3B7105B700D4F4DE5E593E B3403630B8EE476B1D5B7105B700D4E4DE5E593E	3	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon Operational
Channel	B2A03630B8EEA76B1D5B7105B70D04F4DE5E593E	1	DESKTOP-EGANUBO	EventLog	Microsoft-Windows-Sysmon/Operational
Computer	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
EventID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
EventRecordID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
image Koswords	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
Nejworas	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
Lever	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
Command ins	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
Communicatione	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
OTHERS	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
DestinationHostname	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
DestinationIp	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
DestinationIsIpv6	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	3	DESKTOP-EGANUBQ	EventLog	Microsoft-Windows-Sysmon/Operational
Search the web and Windows	o 🛤 💿 S 🍉 📑 😚 🐗				∧ 10.21 AM N S S Log Log ENG 5/24/2015

• Step 1: Select any record and hover over that record. Click on the Marking artifact button. A popup will appear on the screen as follows:

VEDR Portal - Event Search x VEDR Portal - IR R ↔ → ○ ↔ ▲ Not secure 10.30.161.37/#/ir-flox	Now Detail X X Y + w/rir-flow-detail/27ac440795d30aa522494d184a7e13897tab=2 + + +					– ଟ × ମନ୍ତ ହ ହ ⊨ କ ↓ §
VEDR Portal	Alerts IR Flow	w Investigation	Response	Setting	⊙ en	• chuyennt2 •
IRFlow Detail - 2305 test1 ← IRFlow List						
TIMELINE 60 Create IR Flow Containmer	nt					Close IRFlow
	<u>Detection</u>	Containment	Investigation	Response		
Process Analysis	Q Event Search	h		Tools	□ Inve	stigation result
Search Log AgentID = "B2A03630B8EEA76B1D5B71	105B70DD4F4DE5E593E" AND Channel = "Microsoft-Windows-Sysmon/O	perational"				Last 7 days
POPULAR AgentID	T38 results 17/05/2019 09:40:03 - 24/05/2019 09:40:03	e	WENTID COMPUTER	LOGTYPE	CHANNEL	View column 🗸
B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E (100)	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGAN	UBQ EventLo	g Microsoft-Windows-Sysmon/Operatio	onal
Channel	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	N	larking artifact(s)			
Computer	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	P	ATH			
EventID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E		DESKTOP-EGANUBQ\CHUYENN	T2 0 2		
EventRecordID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E		C:\Windows\System32\taskhos	tw.exe 🖉		
Image	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E					
Keywords	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E					
Level	B240363088EE476B1D587105B70DD4F4DE5E593E					
LogType	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593F	3	Accept Cancel			
CommandLine	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E		DESKTOP-EGAN	UBQ EventLo	og Microsoft-Windows-Sysmon/Operatic	onal
OTHERS	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGAN	UBQ EventLo	g Microsoft-Windows-Sysmon/Operatio	onal
DestinationHostname	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGAN	UBQ EventLo	g Microsoft-Windows-Sysmon/Operatio	onal
DestinationIp	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGAN	UBQ EventLo	Microsoft-Windows-Sysmon/Operatio	onal
DestinationIsIpv6	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	3	DESKTOP-EGAN	UBQ EventLo	g Microsoft-Windows-Sysmon/Operatio	onal
Search the web and Windows	o 📑 💿 S Þ 🖬 🕅 🛷				^ 🛽	🦅 🔀 💿 💟 💭 d∎ 🐻 ENG 10:19 AM S/24/2019

In case of selecting the event of the Agent that is not part of IR Flow, there will be an option for the user to add the Agent to IR Flow. Agent will be added to the Detection screen of the active IR Flow.



Marking artifact(s) PATH	1
TCP/IP Route Command 2	
□ NT AUTHORITY\SYSTEM 🖉	
C:\Program Files\VEDR\AgentInfo.exe 🔗	
C:\Windows\system32	
C:\Windows\System32\ROUTE.EXE 🖉	
Accept Cancel	Add Agent To IR Flow

• Step 2: Choose a suitable path for marking artifact. Then click Accept to perform marking. If Cancel is selected, the marking artifact will be delayed.

When the marking artifact is successful, the screen will display a notification. Click on View in investigation result to go to the Investigation Result screen and the marked event will be moved to this tab.

☑ VEDR Portal - Event Search X ☑ VEDR Portal - IF ← → C ▲ Not secure 10.30.161.37/#/ir-1	R Flow Detail x 🔯 User-Role-Permission - Viettel E x flow/ir-flow-detail/27ac440795d30aa522494d184a7e13897tz	+ ab=2				- 8 × 0☆당 9 월 8 보 8
VEDR Portal	Alerts	R Flow Investigation	Response	Setting	⊙ en *	chuyennt2 🔹 👻
IRFlow Detail - 2305 test1 ← IRFlow List						
TIMELINE 66 Create IR Flow Containm	nent 0					Close IRFlow
	<u>- <u> </u></u>	Containment	Investigation	Response		
1©1 Process Analysis	Q. Event	Search		🖸 Tools	🗋 investiga	ation result
Search Log AgentID = "B2A03630B8EEA76B1D5B	17105B70DD4F4DE5E593E" AND Channel = "Microsoft-Windows-Sys	mon/Operational*				Last 7 days
POPULAR AgentiD	T38 results 17/05/2019 09:40:03 - 24/05/2019 09:40: Marked artifact! 17/05/2019 09:40:03 - 24/05/2019 09:40:	03				View column ~ View in investigation result ×
B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E (100)	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	3	DESKTOP-EGANUE	IQ EventLog	Microsoft-Windows-Sysmon/Operational	
Channel	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	3Q EventLog	Microsoft-Windows-Sysmon/Operational	
Computer	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	Q EventLog	Microsoft-Windows-Sysmon/Operational	
EventID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	Q EventLog	Microsoft-Windows-Sysmon/Operational	
EventRecordID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	Q EventLog	Microsoft-Windows-Sysmon/Operational	
Image	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	3	DESKTOP-EGANUE	IQ EventLog	Microsoft-Windows-Sysmon/Operational	
Keywords	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	IQ EventLog	Microsoft-Windows-Sysmon/Operational	
Level	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	Q EventLog	Microsoft-Windows-Sysmon/Operational	
LogType	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	3Q EventLog	Microsoft-Windows-Sysmon/Operational	
CommandLine	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	3Q EventLog	Microsoft-Windows-Sysmon/Operational	
ATLEDS	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	3Q EventLog	Microsoft-Windows-Sysmon/Operational	
Destinationklostname	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	3Q EventLog	Microsoft-Windows-Sysmon/Operational	
DestinationIn	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	SQ EventLog	Microsoft-Windows-Sysmon/Operational	
DestinationIsIpv6	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DESKTOP-EGANUE	IQ EventLog	Microsoft-Windows-Sysmon/Operational	• • •
Search the web and Windows	0 📄 💿 S 🎾 🖲 🕅	ø			^ 🚺 👽	🕅 💿 💟 完 🚛 📑 ENG 10:35 АМ 5/24/2019

Get artifact: Perform get file/registry under Agent to server to serve the investigation process.

• Step 1: Select any record and hover over that record. Click on the Get artifact button, a popup will be appeared on the screen as follows:



🔄 VEDR Portal - Event Search 🛛 🗙 😔 VEDR Portal - IR Fi	low Detail 🗙 🦃 User-Role-Permission - Viettel Er: 🗙 📔 🕂					- σ ×
← → C (A) A Not secure 10.30.161.37/#/ir-flow	w/ir-flow-detail/27ac440795d30aa522494d184a7e1389?tab=2					⊘☆♥ ၈ 8 Ө ± §
VEDR Portal	Alerts IR Flow	Investigation				🚱 EN 👻 chuyennt2 💶 👻
IRFlow Detail - 2305 test1 ← IRFlow List						
TIMELINE 00 Create IR Flow Containmer	nt					Close IRHow 0
	Detection	Containment	10 Investigation	Response		
ইট্টি Process Analysis	Q Event Search			C Tools		Investigation result
Search Log Search Log						4) Last 7 days
POPULAR	= 11877 results 17/05/2019 10:49:37 - 24/05/2019 10:49:37					View column 🗸 🗸
AgentID	AGENTID	EVENTID	COMPUTER	LOGTYPE PLATFORM	CHANNEL	
Channel	D5403030D05541001030110301000454053535	4000	UESTION-EGHINODQ	Evencog	security	
Computer	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	4688	DESKTOP-EGANUBQ	EventLog	Security	
EventID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	4689	DESKTOP-EGANUBQ	EventLog	Security	
EventRecordID	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	4688	DESKTOP-EGANUBQ	EventLog	Security	
Keywords	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	4688	DESUTOR COMULDO	Eventline .	Contribu	
Level	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	1	DE: Get artifact(s)			
LogType	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	4689	DE:	the State of		2
CommandLine	B2A03630B8EEA76B1D5B7105B70DD4F4DE5E593E	4688	DE: C:(Windows(sy	stemszybackground lasknost.exe		Z PILE
Image	82A0363088EEA7681D587105870D04F4DE5E593E	4089	DE			
OTHERS	B2A03030B8EEA70B1D387103870D04F4DE55593E	5001	DE:			
Guid	B24026308655476810587105870004540555335	louc	DE			
Name	B240303086EEA10B103B103B100B4F4DE3E353E	5058	DE:			
Opcode	21020200000000100010001000000000000000	5050	Accept Canc	el		
ProcessID	D240262000000000000000000000000000000000	4680	DESKTOR EGANURO	Evention	Security	
Processid	B2403630B8EE476B105B7105B700D4E40E5E503E	4689	DESKTOP-EGANUBO	Eventing	Security	U
Search the web and Windows		4007	Scotton Controlog	erences.	occorry	へ 📙 🐨 🌠 💿 💟 🖅 🗤 🐻 ENG 5/24/2019

• Step 2: Select artifact, then select artifact type (File/Registry) and click Accept.

When the marking artifact is successful, the screen will display a notification. Click on View in investigation result to go to the Investigation Result screen. The result of Get artifact will be displayed on this tab.

🔛 VEDR P	fortal - Event Search X	VEDR Portal - IR Flow Detail	× 🚯 User-Role-Permission - Viett	el En 🗙 🕂						- a ×
\leftrightarrow \rightarrow (C 🞧 🔺 Not secure	10.30.161.37/#/ir-flow/ir-flow-de	tail/27ac440795d30aa522494d184a	7e1389?tab=2					0 1	ଟ 🔊 🙆 \varTheta 날 🧕
	VEDR Portal		Alerts	IR Flow	Investigation	Response	Setting		⊙ en +	chuyennt2 🔹 🔹
	Detail - 2305 test1 List									
TIMELINE	Create IR Flow	Containment Agent: (s)								Close IRFlow
			- <u>````</u>	etection	Containment	Investigation	Response			
	18 Proc	ess Analysis		Q, Event Search			Tools		Investigation re	sult
Result										
~	DESKTOP-EGANUBQ	Success (1/1)								
	TIME	GET BY						STATUS	DO	WINLOAD ACTION
	10:49 24/05/2019	Get Artifact Type: FILE	Path: C:\Windows\System32\Backgroi	indTaskHost.Exe				Successed		¥ 0
Marked	Artifact									
	TIME	OE	UECT							
	10:35:00 24/05/2019	DE	SKTOP-EGANUBQ\CHUYENNT2							<u>1</u> ×
	10:35:00 24/05/2019	C:)Windows\System32\taskhostw.exe							<u>10</u> ×
										0
Sea		s (0)	🗖 💁 😓 📬	V 🐢					^ 🚺 💔 🕺 🍕	V 💭 do 🕞 ENG 5/24/2019

View event details: Select any record and hover on that record, click on the View details icon.





5.1.7.2.3. Deploy Tools

This is the process of pushing the tool down to the Agent to get information for investigation. Information about some tools available on the system as follows:

For a Windows agent:

- Listdlls: Get information about processes and dlls being loaded.
- Autorunsc: Get information about processes and services that start with the system.

For a Linux agent:

• ListService: Get the list of services under the agent machine.

The flow that implements this function is as follows:

Make tool selection \rightarrow Select agent \rightarrow Click Deploy tools.

To choose the appropriate tool, there are two ways:

◦ Method 1: Click on the Search tool textbox → Click the tool to deploy → Click Choose tool.



VEDR board - Agile Board - Your × ◆ Test Manageme → C ☆ ▲ Not secure 10.30.161.37/#/ir-fi	nt for JIRA - Your 🗙 🛛 🔷 ow/ir-flow-detail/813bl	Test Management for 00d7389b01fe3fdba	JIRA - Your 🗙 💠 T 2ebd55562ff?tab=2	iest Management for JIRA - You	× 📶 AJIANT - Gro	ips Management 🗙 🔃 AJIA	NT - IR Flow Detail	x 🗙 Test Design - a/iant - VCS Conflux x + - の ② む ☆ ② 盤 ◎ ⊕ 上
TI AJIANT			IR Flow					🕄 EN 👻 root 💶 👻 🛩
Flow Detail - 2003_test win server								
🖏 Process Analysis		Q Event Search		(김 Tools		🕄 Autoruns	Investigation Result
Add tool Add tool Multi select agents online	·····> O Click De	play Tool button to						
Tools	Agents	Type to search		c	2			
O Type to search tool Add tool	HOSTNAME		PLATFORM	TOOLS				STATUS
	DESKTOP-E	GANUBQ	8	Test_Tool_40s_2.E	te V1			Offline
WINDOWS	WINSERVER	_2008_R2	•	Test_Tool_40s_2.E	e V1			Online
Iest_Iool_40s_2.exe U1 Hash: 7959405740052554785c75a6Hedddsbeetaecf	WIN7-32BIT-	PC	0					Offline
autorunsc 2 usia.s.a.i euri: terteseecabic.effectiteseiseasees. unins000.exe Vijieuri.tetteseerttaseaseasettaseitasettasettase Java.exe Java.exe			-					
V1/Hahr:1513954953377909c13059853976431209 nginx.exe V1/Hahr:151849053274600c2345344c1354497363479 procexp.exe								
We Heah: 0019173710883040893218817e304662e4c577 Agentinfo.exe Vi Heah: 01249329713883447508248954e6cb466954								
Iogonsessions.exe VsjHash: 7c782275d5c7H36657se2a+755855bafb5b/H								
See all tools 3 Choose tool								
Deploy tools								C
Search the web and Windows	0 5	6	🛤 😚 🛹	🔣 😷 🔽	15 🐻 🐖			∧ (5) 💯 🐹 🍙 💟 🖽 de) 📰 ENG 🏾 🕺

◦ Method 2: Click on the Search tool textbox → Click See all tools → Display the full tool list screen → Search and select the tool to deploy → Click Add tool.

Q Type to search tool	Add tool								
WINDOWS Test_Tool_40s_2.exe V1 Hash: 79b9e657e80525b478bc7f3a	5f49ddd3b998a9cf								
autorunsc V15.82.0.0 Hash: 3a75018edd9fbc3eff84f8f959b9c95045b									
Unins000.exe	if9564ff17da7ba4								
java.exe ↑ Vi Hash: 781a95a4b1a57790a9c1b0e5	☐ java.exe								
nginx.exe ∴ V1 Hash: 8864806926f46b00a28458f4c	155649073fc8a79								
procexp.exe Ve Hash: de91737fc8815b408a512f881	.7e1b9f8d2e9c57f								
AgentInfo.exe V1 Hash: 071493367d189a547faed75081898348cbafd95e									
logonsessions.exe	75b8b5bafb5bf84f								
See all tools	Choose tool								



List	3 All	~	Tool selected	6 Add tool
ListService	4	Owner: root	Listdlls V3.20.0.0 Hash: fbac538166d8154f10db834bd4bc1b86c81e56fb	G Owner: root
ListService2	Icc8013	Owner: root		
			5	
		•		

• After searching for tools, select an agent and click Deploy tools.

 ♦ VEDR board - Agile Board - Your × ◆ Test Management I ← → C ∩ ∩ ▲ Not secure 10.30.161.37/#/ir-flow 	for JIRA - You: × A Test Management for J w/ir-flow-detail/813bb0d7389b01fe3fdba2e	RA - Your 🗙 🔷 T ebd55562ff?tab=2	est Management for JIRA - Your 🗦	K AJIANT - Groups	i Management 🗙 🔃 AJIA	NT - IR Flow Detail	x X Test Design - aliant - VCS Conflux + - ♂ X
📶 ΔΙΙΔΝΤ	Alerts	IR Flow	Investigation	Response	Protect & Prevention	Setting	ⓒ EN 🕶 root 🕒 👻
IRFlow Detail - 2003_test win server ← IRFlow List							
101 Process Analysis	Q. Event Search		ď	Tools		🕄 Autoruns	Investigation Result
Add tool ····· > Ø Multi select agents online	····· 🐌 🔞 Click Deploy Tool button to						
Tools	Agents Type to search		Q				
O Type to search tool Add tool	HOSTNAME	PLATFORM	TOOLS				STATUS
	DESKTOP-EGANUBQ	8	Test_Tool_40s_2.Exe	V1			Offline
 Windows 	WINSERVER_2008_R2	0	Autorunsc V13.82.0.0	Test_Tool_40s_2.	Exe V1		Online
autorunsc	WIN7-32BIT-PC	8					Online
V15.82.0.0 Healt: 3a73016edd9fbc34ff84f8959b9c86045ba90b3	THANHLN-PC	•					Online
Listdlis							
V320.0.0 Hark (backStatedets-H100b80-bod4bc1b86c81a98b)							
∧ Linux							
Deploy tools 8							0

• After deploying the tool, view the results in the Investigation Result and Tools Result tab.



VEDR bo	xard - Agile 🗙 💠 Te	est Management i 🗙 📔 💠 Test M	anagement fi 🗙 🛛 💠 Test Man	agement fi 🗙 📶 AJIANT -	Deploy To: 🗙 📶 AJIAI	NT - IR Flow D e 🗙 😫	Test Design - aJiant 🗙 🛛 🔂 [Rel	ease][[BBXNTK] \ 🗙 👲	Downloads 🛛 🗙 🗎	CS-aJiant Portal - × +	- σ ×
$\epsilon \rightarrow c$	🗅 🍙 🔺 Not secur	re 10.30.161.37/#/ir-flow/ir-fl	ow-detail/813bb0d7389b01fe	3fdba2ebd55562ff?tab=2						0 🕄 🏠 🔊	ଥ । 🗢 😁 👱 💈
N	AJIANT			IR Flow							root 🚊 🝷
IRFlow [Detail - 2003_tes ist	t win server									
TIMELINE	Response Scen Agent: (1)	ario Containment Agent: (s)	Containment Agent: (0)	Containment Agent: (1)	Containment Agent: (2)	Tool Deployed	Response Scenario Agent: (i)	Tool Deployed Agent: (1)	Tool Deployed Agent: (3)	Tool Deployed Agent: (3)	Close IRFlow
				Detection	Containme	nt 🥰 I	westigation	Response			
	193 Process	Analysis	Q Event	Search		Tools		🕄 Autoruns		🗍 Investigatio	n Result
	⊻	Tools Result									
	Got Artifact	Autorunsc	Agents (1)	Success (1/1)							
		TIME	PLATFORM AGENT ID				HOSTNAME		STATUS	ACTION	
		15:36 25/03/2020	6BBCD23F	D1BB16E4B13E549126ED244	3BF0707F		Win7-32bit-PC		 Success 	* 0	
		✓ Listdlls	Agents (1)	Success (1/1)							
		✓ Autorunsc	Agents (1)	Success (0/1)							
	Iarked Artifact	√ Test_Tool_40s_2.Ex	a Agents (1)	Success (1/1)							
		v Test_Tool_40s_2.Ex	e Agents (1)	Success (1/1)							
											0
Sear	ch the web and Wind	dows	0 🔯 📄 🔗	🍋 🙉 😚 "	×8 🔀 🖬	e 🔍 🐝 🎽	Ø			^ 🖻 🖲 🔣 🕗 🔽	및 4) 🖳 ENG 456 PM

5.1.7.2.4. Handle Event

This is the screen displaying information about Deploy tool, Marking/Get Artifact results in 3 tabs: Process Analysis, Event search and Tools.

- Got Artifact: The result of executing the Get Artifact command.
- Tool Results: The results of executing the Deploy tools command.
- Marked Artifact: The artifacts are marked.
- In the Got Artifact and Tool Results tabs, the following actions can be performed:
 - View the detailed content of the taken artifact or the result of running the tool under the agent. If the data is text, it can be viewed directly on the interface. If the data is an executable file (.exe), it needs to be downloaded to the local machine to check.
 - Download the artifact or tool run results. There are 2 ways to download: Click the Download icon on the interface or click the View details icon → Click the Download icon on this screen.



	泣 Detection 🔛 Containment 💘 Investigation 🕼 Response	
131 Process Analys	is Q. Event Search [? Tools 🔅 Autorur	ns 🛛 Investigation Result
,↓, Go	t Artifact	
Got Artifact	A WINSERVER_2008_R2 Agents (1) Success (1/1)	
T	IME TYPE OBJECT	STATUS ACTION
14	127 20/03/2020 FILE C:\Windows\System32\notepad.exe	• Success 🛃 🛈
Tools Result		
\checkmark		
Marked Artifact		
	Preview	× Ł
	Error opening System(4):	
	Access is denied.	
	smss.exe pid: 280	
	Command line: \SystemKoot\System32\smss.exe	
	Base Size Path	
	0x48070000 0x13000 C:\Windows\System32\smss.exe	
	Verified: Microsoft Windows	
	Publisher: Microsoft Corporation	
	Description: Windows Session Manager	
	Product: Microsoft® Windows® Operating System	
	Version: 0.1.7000.10385	
	Create time: Tue Jul 14 06:11:12 2009	
	0x77620000 0x13c000 C:\Windows\SYSTEM32\ntdll.dll	
	Verified: Microsoft Windows	
	Publisher: Microsoft Corporation	
	Description: NT Layer DLL	
	Product: Microsoft® Windows® Operating System	
	Version: 0.1./001.1/514	
	Create time: Sat Nov 20 19:05:02 2010	

• In the Marked artifact tab, select the artifact to add to the Detection screen as follows:

Select an artifact and click Add to detection:

Marked Artifact		
TIME	OBJECT	
10:35:00 24/05/2019	DESKTOP-EGANUBQ\CHUYENNT2	Add to detection > 11 ×
10:35:00 24/05/2019	C:\Windows\System32\taskhostw.exe	<u>1</u> ×

Select multiple artifacts and click Add to detection:



Marked	d Artifact		
Selec	ted (2)	2 Add to detection	
	TIME	OBJECT	
1	10:35:00 24/05/2019	DESKTOP-EGANUBQ\CHUYENNT	2
	10:35:00 24/05/2019	C:\Windows\System32\taskhostv	/.exe
	Marked Artifact		3
	Added artifacts to detection 10:35:00 24/05/2019	DESKTOP-EGANUBQ/CHUYENNT2	View all artifacts Detecti Added to IRFI
	10:35:00 24/05/2019	C:\Windows\System32\tashostv.exe	Added to IRFin

After adding successfully, a notification will be displayed, click on View all artifacts in Detection phase to go to Detection screen. The artifacts are added to Additional detection on the Detection screen.

		Alerts	IR Flow Investigation					chuyennt2 😩
		Detection	Containment	investigation	Response			
al detection								
nt ESKTOP-EGANUBQ								
rt TIME	GROL	P	HOSTNAME		SCENARIO		SEVERITY	
10:13:37 22/05/2019	unkr	own	DESKTOP-EGANUBQ		Initial Access		High	
onal detection								
nt ESKTOP-HHN2B1Q rt TIME	nhandt4-PC X Win7-CongNC9 X GROUP		HOSTNAME	SCENUS	ARIO	SEVERITY		
Int ESKTOP-HHN2B1Q rt TIME 11:09:41 22/05/2019	nhands4-PC X Win7-CongNCS X GROUP unknown		HOSTIKAME nhandt4-PC	scow Execu	ario	SEVERITY High		×
nt ESKTOP-HHN2B1Q rt TIME 11:09:41 22/05/2019 14:07:50 15/05/2019	nhandsEPC X WinT-CongNCS X GROUP unknown no_group		HOSTMAKE nhand14-PC Win7-CongNC9	schw Execu	ARIO ution	SEVERITY High High		×
nt ESKTOP-HHN2B1Q (1 rt 11:08:41 22/05/2019 14:07:50 15/05/2019 14:39:29 17/05/2019	nhandsEPC X Wint-CongleG X caoup unknown no_group unknown		HOSTINAME Inhandt4-PC Win7-CongNC9 DESKTOP-HHN28LQ	SCEN Dieco Initia Electric	ARIO ution Il Access ution	SEVERTY High High		×
nt ESKTOP-HHN2B1Q 1 tt TIME 11:08:41 22/05/2019 14:07:50 15/05/2019 14:39:29 17/05/2019 facts TIME	nhandi&PC X Win7-CongNG X CROUP CROUP Unknown congroup Unknown	OBJECT	HODTNAKE nhandt4-PC Win7-CongNC9 DESKTOP-HHN281Q	SCDW Exec Initia Execu	ABIO ution I Access ution	SEVERTY High High High FROM	REFERENCE	×
nt ESKTOP-HHNI2B1Q tr TIME 11:0904122/05/2019 14:09:29 17/05/2019 facts TIME 10:03:500 24/05/2019	Abundik-PC X Winit-CongRG X GROUP unknown no_group unknown Aburt 0 Bundissbestehroeb159710567004440555585	OBJECT	HODTNAKE mhandt4-PC Win7-CongNC9 DESKTOP-HHN281Q OP-EGMNUBQ(CHUYENNT2	SCDW Exect Initia Exect	ution (fAccess ution	SEVERTY High High FROM WINLEVENT_LOG	REFERENCE (PC1320BE3(gbypWIA)	× × ×
nt ESKTOP-HH4281Q 7 t t 11:08-41 22/05/2019 14:07:50 15/05/2019 14:39:29 17/05/2019 14:39:29 17/05/2019 16:35:00 24/05/2019 10:35:00 24/05/2019	MandsEPC X Wint-CongRG X COUP Unknown C	OBJECT DESKT C(Win	HODTNAHE mhandt4-PC Win7-CongNC9 DESKTOP-HHN281Q OP-EGNUDBQICHUTEINT2 dowl/System22(taskhostnuxxe	SCDW Exec Initia Execu	ABIO ution If Access ution	SCREATY HID HID HID HID HID HID HID HID HID HID	REFERENCE IPC1520688/gbypNLX0 IPC152088/gbypNLX0	× × ×

5.1.8. IR Flow - Response

5.1.8.1. Live Response

The Live response function provides the ability to process a set of remote commands according to the working session to provide information or handle requests on the host.

Steps to implement Live Response function in IR Flow as follows:



- Step 1: Click the IR Flow tab.
- Step 2: Click duplicate on a record in the list of records (Notes: Select the correct IR Flow record containing the Agent that needs to perform the Live Response.)

VEDR Portal - IR Flow List X	+					- σ ×
\leftrightarrow \rightarrow C \textcircled{A} Not secure	10.30.161.37/#/ir-flow/ir-flow-managem	ent?search=eyJxdWVyeVNIYXJjaCl	l6lilsInNvcnRDb2x1bW4iOjAsInI	NvcnREaXJIY3Rpb24iOiJkZXNjliwibGlta	XQiOjIsInRpdGxlX2RhdGVwaWNrZXIiOiJ	BTEVSVC5MQVNUX1NFVkVOX0RBWSIsImtleV ⊘ 🏠 👽 🧔 😝 👱 😫
VEDR Portal		Alerts	IR Flow Inve	stigation Response	Setting	🕃 EN 👻 nhandt4 😩 👻
Search IR Flow		-	K	(1)		
Type to search				0.0		Last 7 days Q
2 result(s) 13/05/2019 10:25:14 - 2	20/05/2019 10:25:14					+ Add new IRFlow
TIME	♥ NAME	STATUS	CREATED BY	ASSIGNED TO	NOTATION	ACTION
10:22:43 15/05/2019	phuocnm3 0515 1	New	phuocnm3	phuocnm3	laksdf	© €
09:24:01 15/05/2019	phuocnm3 test	Closed	phuocnm3	phuocnm3	abc	Ū Đ
		(2)				

• Step 3: Click the Response sub-tap.

VEDR Portal - IR Flow Detail × +								- σ ×
\leftarrow \rightarrow C \bigcirc Not secure 10.30.161.37/#/ir-flow/ir-flow-detail/697e2583af4	add1bf4a42ba4805b1b	!0?tab=3						⊘☆♥ 🥬 🖰 👱 🥞
VEDR Portal	Alerts	IR Flow	Investigation	Response	Setting		© EN ₹	nhandt4 👱 👻
IRFlow Detail - phuocnm3 0515 1 ← IRFlow List								
TIMELINE 68 Create IR Flow						(3)		Close IRFlow
	<u>- </u> Detect	on 🗗	Containment	Investigation	Response			
🖾 Live response						Response scenario		
					C ₂			
			₩ ×					
	AGENTI	D		SESSION LEN	IGTH			
	Choos	e Agent to		Choose tim	ie to live 🗸 🖌			
			Start Live Re	isponse				
								U

• Step 4: Select Agent and time range (5 minutes/ 15 minutes/ 1 hour/ 3 hours) to perform Live Response and press the Start Live Response button.

The list of Agents displayed in the combo box is all the agents displayed in the Detection tab.



😔 VEDR Portal - IR Flow Detail 🛛 🗙 🔛 VEDR Portal - Live Response 🛛 🗙 🕂								- a ×
← → C ⋒ ▲ Not secure 10.30.161.37/#/ir-flow/ir-flow-detail/bf43ffa2b55	33e35a36649ed366edcb9?	ab=3					Ģ	D A 🕄 🤌 🖯 👱 😫
VEDR Portal		IR Flow						nhandt4 🔔 👻
RFlow Detail - IRFlow_test_2019 ← IRFlow List								
TIMELINE 08 Create IR Flow								Close IRFlow
	<u>Detection</u>	Cont	ainment 🥳	investigation	Response			
C Live response						Response scenario		
	AGENT ID nhandl4	PC (1)	Sart Live Response	SESSION LENGTH 15 minutes	<u>َنَ</u> (2)			0

After that, the user needs to wait 1 minute for the system to connect to the agent. The system state is Connecting.

VEDR Portal - IR Row Detail x	2a25a36649art266ard-h92tah=3				- 5 ×
VEDR Portal	Alerts IR Fi	ow Investigation	Response	Setting	3 EN • nhandt4 🔄 •
L ₂	Detection	Containment	investigation	Response	
Live response				Response scenario	
Remote session list	+ Add New Remote	Agent ID: B0EF7B3E39EEC77626	iB87CC988653FBD63DC8285		
STATUS AGENT ID TIME STARTED	TIME STOPPED	HOSTNAME nhandt4-PC	STARTED	O DURATION	C TIME TO LIVE 15m
		Remote session start (Please wait while connection	ed ng)		
				485	
					• Connecting
		 Attachment Log 			0

• Step 5: When the connection is successful, the system displays a record in the Remote Session List and the console screen has information about the connection and displays the Running state.

(Remote Session List: Display a list of IR Flow's Live response sessions that have been performed.)

Notes: Each agent at a time has only 1 working session of Live response.





VEDR Portal - IR Flow	Detail X VEDR Portal - Live Re	esponse X +	12a35a35640ard366ard+h07tah==					0	- o x
VEDR Port	al	n non octany bi sonacooo	Alerts IR	Flow Investigation	Response	Setting		③ EN ▼	nhandt4
	R		Detection	Containment	100 Investigation	Response	_		
		Live response					Response scenario		
Remote session	list		+ Add New Remote	Agent ID: BOEF7B3E39EEC7762	26B87CC988653FBD63DC8285			() TIME TO LIVE	
STATUS	AGENTID	TIME STARTED	TIME STOPPED	nhandt4-PC	11:17:07 2	20/05/2019	00:12:28	15m	
				[Penday, 20-80y-19 1.17 [Penday, 20-80y-19 11:17 Cia Cia	:07 +07] Agent Connected :07 +07] Agent info: Agent	t jafé here			• Ruming

Users can execute commands at the console screen as follows:

No.	Commands	Parameters	Description
1	cd	cd <dirpath></dirpath>	Change current working folder
2		cd or cd	Switch back to parent-level folder
3	pwd		Print current working folder
4	dir		List files/sub-level folders in the current folder
5	delete	delete -file <path> For example: delete -file "c:\temp\run path.exe"</path>	Delete 1 file
		delete -folder <folderpath> For example: delete -folder temp\axvers</folderpath>	Delete 1 folder

1



		delete -all <folderpath> For example: delete -all c:\temp</folderpath>	Delete all files/sub-folders in the folder (but do not delete the folder)
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Display data in file (file size limit)
7	get	<filepath></filepath>	Upload 1 file from host to server
8	put	<url><folderpath></folderpath></url>	Download 1 file to host machine
9	mkdir	<dir name=""></dir>	Create 1 folder
10	reg		Commands related to Registry
		query <keyname>-v<valuename>For example:-queryreg-query-query"HKLM\Software\abc xyz" -v-v"run path"-v</valuename></keyname>	Query the value data of a key
		query <keyname> -s For example: reg -query "HKLM\Software\abc xyz" -s</keyname>	Query all sub keys, values and data
		add <keyname> For example: reg -add "HKLM\software\abc xyz"</keyname>	Add 1 key
		add <keyname> -v <valuename> -t <type> -d <data> For example: reg -add "HKLM\software\abc xyz" -v</data></type></valuename></keyname>	Add 1 value



		"run path" -t REG_SZ -d "c:\temp\bin.exe"	
		delete <keyname> For example: reg -delete HKU\S-1-5-21- 3791698801-2327923109- 636705026- 2080\Software\Test</keyname>	Delete 1 key and all sub keys and value
		delete <keyname> -v <valuename></valuename></keyname>	Delete 1 key value
		import <filename></filename>	Import 1 file .reg
		export <keyname> <filename></filename></keyname>	Export 1 file .reg
11	process		Commands related to process
		-t <processid></processid>	Turn off a running process by process ID
		-s <processid></processid>	Pause a process
		-r <processid></processid>	Recover a previously paused process
		-l -a	List all processes of all users
		-l -u <username></username>	List all processes of an user
12	service		Commands related to service
		-query	List the services running on the host machine
		-start <servicename></servicename>	Start 1 service
		-stop <servicename></servicename>	Stop 1 service



13	user	-list	List the users on the machine
		-sid <username></username>	Get sid of username
14	cls		Delete the console screen
15	help		Help command

Some notes when working with commands on the console screen as follows:

 Clear command: After executing the Clear command, the system will support the user to download the entire log made on the previous console screen, by clicking on the here link.

	🖸 VDR ford - R Jow Cesal x 🖄 VDR ford - Los Response x + +										
VEDR Porcial Addity Ref Nov meetingation Response Satisty Nov medded & 2 Nov	← → C A A Not secure 1030.161.37/#/r-flow.fetal/b43/fit2b5533e3549ed366edcb9ttab=3									⊘☆♥ 🥬 🖰 ≟	
	VEDR PO			Alerts	IR Flow	Investigation					nhandt4 🔹 👻
Clip Version Add Nove Result Add Nove Resu				- Detection	•	Containment	Investigation	Response			
Rends session list + Add New New April 0 Third Standtell			Live response						Response scenario		
Status Addriño Tite Statuto Tite Statuto O controleva	Remote sessi	on list		+ Add New R	temote Age	ent ID: BOEF7B3E39EEC776	26B87CC988653FBD63DC8285				
• Running • BortFREUENECCTREASBRCCORB • Add BortFREUENECCTREASBRCCORB • Lastad 200/2019 • Halad 200/	STATUS	AGENT ID	TIME STARTED	TIME STOPPED	٢	HOSTNAME nhandt4-PC	STARTED 14:37:56 20	0/05/2019	COUNTDOWN 00:03:29	Тиєтоц 15m	
Strapped	Running	B0EF7B3E39EEC77626B87CC988	14:37:56 20/05/2019	N/A		*Repote session star	rted***				
900prd B0F783E84ECT7826887C088 1012/07 20 05/2019 1022/07 20 05/2019 • Stopped B0F783E84ECT7826887C088 111/07 20 05/2019 1022/07 20 05/2019 • Attachment Log * Attachment Log * Introduction possepare 2019/2021/11448tm ^b Class 2011/1448tm ^b * Attachment Log * Attachment Log * Class 2011/1448tm ^b * Stopped 2019/2021/114445tm ^b * Stopped 2019/2021/114445tm ^b * Stopped * Stopped	 Stopped 	B0EF7B3E39EEC77626B87CC988	14:33:03 20/05/2019	14:34:07 20/05/2019	Cl C:	ick here to get log	file to view all command				
Stopped BisF7RELEXEKCT/REASER/CCS88 111/37/20(5)/2019 1122/97/20(5)/2019 Image: Comparison of the	Stopped	B0EF7B3E39EEC77626B87CC988	14:30:31 20/05/2019	14:31:23 20/05/2019							
Attachment Log Attachment Log Ret Mild THE OSERTE DRECTORY Procespece 2018-05-20714.08.344-02:00 Cl ja	 Stopped 	B0EF7B3E39EEC77626B87CC988	11:17:07 20/05/2019	11:32:07 20/05/2019							
^ Attachment Log Fill duit Tell duit							l	lu I			• Punning
PLE LUNE THE CALLETS DESCRIPTION procespiere 2019-05-2011.432.8149-05.00 Clair Image: Clair Clai					^	Attachment Log					
poccepere 2019-05-2011.438.264+07:00 C/a 2 2 E 2019-05-2011.438.264+07:00 C/a Soor all					FILET	NAME		TIME CR	IEATED	DIRECTORY	
■ 201953011164436_tmc ^ Seew all					proc	exp.exe		2019-0	5-20T14:38:36+07:00	C:\a	<u>ت</u> ±
■ 201965011164436tot ^											
	2019052011164	436txt ^									Show all

 Get <filepath> command: For example, get procexp.exe in the console screen, the result of getting the file is displayed in the Attachment Log screen at the bottom right corner of the screen. Users are allowed to download files to the browser or delete the downloaded files to the server.



	VEDR Portal - IR Flow D	tall X 🕑 VEDR Portal - Live Re	esponse X +							-	σ×
	VEDR Portal	201 secure [10.30.161.37/#/II-110W/	n-now-detai/pl43ma205555	Alerts IR	Flow Investigation	Response	Setting		⊙ en v	nhandt4	• <u>•</u> •
				Detection	Containment	Netigation	Response				
			Live response					Response scenario			
ß	Remote session lis	t		+ Add New Remote	Agent ID: B0EF7B3E39EEC77626	887CC988653FBD63DC8285					
	STATUS	AGENT ID	TIME STARTED	TIME STOPPED	HOSTNAME nhandt4-PC	STARTED 14:37:56 20	05/2019	COUNTDOWN 00:14:07	 TIMETOLI 15m 		
	 Running 	B0EF7B3E39EEC77626B87CC988	14:37:56 20/05/2019	N/A	14/ 7/2009 10:20 <0IR>	0 Program Files (x06) 0 ProgramData 0 Prython27 0 Recovery 0 Ruby24-x54					
	 Stopped 	B0EF7B3E39EEC77626B87CC988	14:33:03 20/05/2019	14:34:07 20/05/2019	14/ 7/2009 10:20 <0IR> 11/ 8/2016 15:50 <0IR>						
	 Stopped 	B0EF7B3E39EEC77626B87CC988	14:30:31 20/05/2019	14:31:23 20/05/2019	29/ 1/2016 10:31 <0IR> 14/ 6/2018 16:59 <0IR>						
	 xopped 			122201-0003,013	14 77,000 1::0 colin 14 71,010 1::0 colin 14 1::0 2:0 i:0 15 1::0 2:0 i:0 17 1:0 1::0 i:0 i:0 17 1:0	14/ 77000 10:02 4000 4000 0 00445 14/ 77000 10:02 4000 0 00445 14/ 77000 10:02 4000 0 0 00407 12/ 12/ 12/ 12/ 12/ 12/ 12/ 12/ 12/ 12/		ek realt ar try again. urto Järtulaisteitaa	percoav C(a	• Ru	Lunning_

- Step 6: The Live Response session ends when:
 - Time of session expires: When the time of Duration field is equal to the time of Time to Live field.

🗧 -> 🔿 🙆 🔥 Vet secure 10.30.161.37///r-flow/hr-flow-detail/b403/1625553.85649ed366edcb97tab=3 🖉 🏠 😫								
		IR Flow Investigation					nhandt4 🕒 👻	
	Detection	Containment	Investigation	Response				
Live response					Response scenario			
Remote session list	+ Add New Rem	Agent ID: B0EF7B3E39EEC77	626B87CC988653FBD63DC8285				-	
DTATUS ACCIVITIO TIME STATED	TIME STOPPED	nhandt4-PC	G STARTED 11:17:07 2	0/05/2019	00:15:00	15m	ε	
Stoped BEFFBIISHECTROBERCOSE., LL17672005019	11:32:07 20:50/24:9	Helpente session tat (Redy, 2049):31 hit (Redy, 2049):31 hit (R	1707-071 Agent Cennected 1707-071 Agent Lennected 1707-071 Agent Lenge 1707-071 Agent Lenge 1707-071 Agent Lenge 1707-071 Agent Lenge 1707-071 Section 1D 201000	info here exiti 200116443000A (Lood		÷	• Stopped	
		 Attachment Log 						

 \circ $\;$ The user actively requests to close the connection with the Close command.


				22 X X X X X X X X X X X X X X X X X X	100	22.44			-
VEDR P	Portal		Alerts IR	Flow Investigation	Response	Setting		⊙ EN -	nhandt4 😩 🔹
			·	Containment	investigation	Response			
		Uve response		1			Response scenario		
Remote sess	ion list		+ Add New Remot	Agent ID: B0EF7B3E39EEC77626B	87CC988653FBD63DC8285				
STATUS	AGENTIO	TIME STARTED	TIME STOPPED	Inhandt4-PC	STARIED 14:30:31 20	W05/2019	OURATION 00:00:52	C TIME TO LI	
Stopped	B0EF7B3E39EEC77626B87CC988	14:30:31 20/05/2019	14:31:23 20/05/2019	NAME OF ADDRESS OF ADDRESS OF					
 Stopped 	B0EF7B3E39EEC77626B87CC988	11:17:07 20/05/2019	11:32:07 20/05/2019	TYPE: 16 STATE: 4 (1 = STOPPED, 2 3	5 6 = PENDING, 4 = RUNN	ING, 7 = PAUSE)			
				PROCESS_ID: 2348 WIN32_EXIT_CODE: 0					
				SERVICE_EXIT_CODE: 0 CHECKPOINT: 0					
				SERVICE_NAME: Woodews Under	te.				
				TYPE: 32 STATE: 4 (1 = STOPPED, 2 3	5 6 = PENDING, 4 = RUNNC	ING, 7 = PAUSE)			
				PROCESS_ID: 544 WIN32_EXIT_CODE: 0					
				SERVICE_EXIT_CODE: 0 CHECKPOINT: 0					
				WAIT_HIND: 0 SERVICE_NAME: wudfsvc					
				DISPLAY_NAME: Windows Drive TYPE: 32	er Foundation - User-mod	e Driver Framework			
				PROCESS_ID: 456	5 0 = PENDEND, 4 = Home	ING. 7 - PHOSE)			
				SERVICE_EXIT_CODE: 0 CHECKPOINT: 0					
				WAIT_HIND: 0 SERVICE_NAME: WwwnSvc					
				DISPLAY_NAME: WWAN AutoCon TYPE: 32	fig				
				ETATE, 3 (3 - ETOBER 3 3	5.6 = PENDING, 4 = RENE	ING, 7 - PAUSE)			
				PROCESS_ID: 0					
				PROCESS_ID: 0 WIN32_EXIT_CODE: 1077 SERVICE_EXIT_CODE: 0					
				PROCESSID: 0 WIN32 EXIT_CODE: 1077 SERVICE_EXIT_CODE: 0 CHECKPOINT: 0 NAIT_HIND: 0					

When the connection with the agent is lost, the server performs ping/pong failed more than 3 times.

VEDR Portal - IR Pie ← → C 向	ow Detail X VEDR Portal - Live Response X A Not secure 10.30.161.37/#/r-flow/ir-flow-detail/	+ bf43ffa2b5533e35a36649ed366edcb9?tab	ä			- 0 × 040 0 0±1
VEDR Po	rtal	Alerts I	R Flow Investigation	Response Se	tting	🕄 EN + nhandt4 😩 +
		Detection	Containment	K Investigation	Response	
R	@ u	ve response			Response scenario	
Remote sessio	on list	+ Add New Remo	te Agent ID: B0EF7B3E39EEC7762	687CC988653FBD63DC8285		
STATUS	AGENTID THREE STARTED	I IME STOPPED	Mostnume nhandt4-PC	STARTED 14:33:03 20/05/2019	OURATION 00:01:04	O TIME TO LIVE
 Stopped 	B0EF7B3E39EEC77026B87CC988 34:33:03 20/	05/2019 14:34:07 20/05/2019	were a second to personal a			
Stopped	B0EF7B3E39EEC77626B87CC988 14:30:3120/	05/2019 14:31:23 20/05/2019	Pid: 4928 Image: C:\Program Files\V	EDR\collector\VESCallector.exe		
Stopped	B0EF7B3E39EEC77626B87CC988 11:17:07 20/	05/2019 11:32:07 20/05/2019	Pid: 4160			
			ber: N. Allinearthy The State of the Stat	K SKYUCL 2)taskeng.exe 2)taskeng.exe 2)stuiree 2)ubentwaipruse.exe 7)ubentwaipruse.exe 3)ubentwaipruse.exe 3)stylic 2)tashoet.exe 3)stylic 2)ubentwaipruse.exe 5, 30%/CL 2)Ubentwaipfuse.exe 4) 40%/Ping Agent Lineset ! 4) 40%/Ping Agent Lineset !	8.690	

In addition, users can click the + Add New Remote button to create a new live response session:

/



VEDR Port	rtal		Alerts	IR Flow	Investigation	Response	Setting		😚 EN 👻 nhandt4 📿	•
			- <u>Detec</u>	tion 🗗	Containment	Investigation	Response			
~		Elive response						Response scenario		
Remote session	n list		+ Add Net	w Remote Agent	ID: BOEF7B3E39EEC7762	6B87CC988653FBD63DC8285				
STATUS	AGENTID	TIME STARTED	SI OPPED	i Hilling Hilling	OSTNAME handt4-PC	STARTED 11:17:07	20/05/2019	OURATION 00:15:00	TIME TO LIVE 15m	
Stopped	B0EF7B3E39EEC77626B87CC988	11:17:07 20/05/2019	11:32:07 20/05/201	19 ***Re [Mond [Mond [Mond [Mond [Mond	emote session start lay, 20-May-19 11:17: lay, 20-May-19 11:17: lay, 20-May-19 11:32: lay, 20-May-19 11:32: lay, 20-May-19 11:32:	ed*** 07 +07] Agent Connected 07 +07] Agent info: Agen 107 +07] Sessien timeout. 07 +07] Sessien to 20196 07 +07] Sessien 10 20196	it info here exit! 52011164436660A Closed			
		Ad	ld New Remote					×		
			Agent Id			Sessi	on length			
			nhandl4-PC			15	minutes	~		
					Cancel	Create				
		_								
										opped
				^	Attachment Log					

5.1.8.2. Response Scenario

The Response scenario function provides the ability to set up a Response scenario and execute the response on one or more Agents.

Steps to implement Response Scenario function in IR Flow as follows:

• Step 1: Click the IR Flow tab.

EVEDR Portal - IR Flow List × X	VEDR Portal - Live Response × + 10.30.161.37/#/ir-flow/ir-flow-management	+ nt?search=eyJxdWVyeVNIYXJjaCl6	lilsInNvcnRDb2x1bW4iOji	AsInNvcnREaXJIY3Rpb24iOi	JkZXNjliwibGltaXQiOjMsInRpdGxlX2RhdGVw	aWNrZXIIOUBTEVSVC5MQVNUX1NFVkVOX0RBWSIsImtie 🖉 ş	- 2010	σ × Θ ≟ §
VEDR Portal		Alerts	IR Flow	Investigation	Response Setting	③ EN ▼	nhandt4	•
> Search IR Flow								
Type to search						Last 7	r days	Q
3 result(s) 13/05/2019 16:07:14 - 20	/05/2019 16:07:14						+ Add ne	w IRFlow
TIME	 NAME 	STATUS	CREATED BY	ASSIGNED TO	NOTATION		ACT	NOI
11:02:49 20/05/2019	IRFlow_test_2019	New	nhandt4	nhandt4	IRFlow_2019		0	€
10:22:43 15/05/2019	phuocnm3 0515 1	New	phuocnm3	phuocnm3	laksdf		0	€
09:24:01 15/05/2019	phuocnm3 test 1	Closed	phuocnm3	phuocnm3	abc		0	€

• Step 2: Click duplicate on a record in the list of records (Notes: Select the correct IR Flow record containing the Agent that needs to perform Response Scenario.).



	VEDR Portal - IR Flow List ×	VEDR Portal - Live Response X +						-	σ×
<	$- \rightarrow \mathbb{C}$ (ii) A Not secure 10.3) VEDR Portal	0.161.37/#/ir-flow/ir-flow-management?sea	rch=eyJxdWVyeVNIYXJjaCl Alerts	IR Flow	V4iOjAsInNvcnREaXUIY3Rpb24# Investigation	Response Set	adX2RhdrGVwaWNrZXIIOUBTEVSVC5MQVNUX1NEVkVOX0RBWSIsImtie	이 값 🕤 🤪 nhandt4	• <u>•</u> •
2	Search IR Flow		_						_
	Type to search							Last 7 days	Q
	3 result(s) 13/05/2019 16:07:14 - 20/05/2	1019 16:07:14						+ Add n	ew IRFlow
	TIME	NAME	STATUS	CREATED BY	ASSIGNED TO		NOTATION	AC	TION
	11:02:49 20/05/2019	IRFlow_test_2019	New	nhandt4	nhandt4	1	IRFlow_2019	0	€
	10:22:43 15/05/2019	phuocnm3 0515 1	New	phuocnm3	phuocnm3	1	laksdf	0	€
	09:24:01 15/05/2019	phuocnm3 test 1	Closed	phuocnm3	phuocnm3	-	abc	0	€

Notes: To perform the reaction scenarios, the administrator must add the Artifacts in the Detection section as shown below:

\leftrightarrow \rightarrow \bigcirc \bigcirc \land Not see	ure 10.30.161.37/#/ir-flow/ir-flow-detail/bf43ffa2b553	3e35a36649ed366e	icb9?tab=0					0	습 🐨 🔊 \varTheta 🛓 💈
			IR Flow						nhandt4 😩 -
IRFlow Detail - IRFlow_	_test_2019								
TIMELINE 66 Create IR FI	low								E Close SRFlow
		<u>iii</u> De	tection	Containment	Nvestigation	Response			
Original detection									
Agent nhandt4-PC									
Alert									
TIME		GROUP		HOSTICAME		SCENARIO		SEVERITY	
14:39:29 17/05/2019		unknown		nhandt4-PC		Execution		High	
Additional detection									
Aritfacts									
TIME	AGENTID		OBJECT				FROM	REFERENCE	
14:38:53 24/05/2019	B0EF7B3E39EEC77626B87CC988653FBD63DC8285		C:\Windows\regedit.exe				WIN_EVENT_LOG	UvC06GoB89lgfaypzLk4	×
14:39:05 24/05/2019	B0EF7B3E39EEC77626B87CC988653FBD63DC8285		C:\Windows\system32\S	nippingTool.exe			WIN_EVENT_LOG	DPC56GoB89lgfaypMbot	×
14:42:40 24/05/2019	B0EF7B3E39EEC77626B87CC988653FBD63DC8285		C:\Users\nhandt4\AppDa	sta\Local\Temp\procexp64	exe		WIN_EVENT_LOG	D_C56GoB89lgfaypQLr8	×
17:24:51 24/05/2019	B0EF7B3E39EEC77626B87CC988653FBD63DC8285		HKLM\SOFTWARE\Micro 75BD40A59C0A]\DateLas	soft\Windows NT\CurrentV tConnected	ersion\NetworkList\Profiles\[4	034A037-3505-4974-804E-	WIN_EVENT_LOG	V_BC6WoB89lgfayp6c8o	×

• Step 3: Click Response Tab \rightarrow Response Scenario.

1



$\leftrightarrow \to C$	Not secure 10.30.161.37/#/ir-flow/ir-flo	w-detail/bf43ffa2b5533e35a36649ed36	6edcb9?tab=3				Ģ) A 🕄 🔊 🕒 👱 😫
VE			IR Flow					nhandt4 👱 🗸
IRFlow D	etail - IRFlow_test_2019							
TIMELINE	O O Create IR Flow							Close IRFlow
		<u>-````</u>	Detection Conta	ainment 🥳 I	nvestigation	ponse		
		Live response				Response scenario		
	Add action to artifact (Choose artifacts have same type to ad	d action! Drag and Drop artifact in table to chang	e position)					
	Containment Integration							
				Add artifacts from detection	phase			
	Dapley to anost							
•	Agent list Choose ONLINE agent in list below and click sa	button to add to apply agent list			Agent apply list Click Deployments	anniv rule for arent list below	_	► Deploy

- Step 4: Perform detailed configurations as follows:
 - Add action to Artifact
 - Click the Add artifacts from detection phase button to start adding Artifacts to Response scenario.
 - Artifact List visible from the Detection tab

	Artifacts from detection (4 artifact(s) selected)		Artifacts adde	d to response			
~	C:\Windows\system32\SnippingTool.exe						
~	C:\Windows\regedit.exe	»					
~	C:\Users\nhandt4\AppData\Local\Temp\procexp64.exe						
~	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profile s\{4034A037-3505-4974-804E-75BD40A59C0A}\DateLastConnected						
						Canc	el

Click the button to switch to the Artifact section in the Response scenario.

Artifacts from detection	Artifacts added to response
	C:\Windows\system32\SnippingTool.exe
	C:\Windows\regedit.exe
	C:\Users\nhandt4\AppData\Local\Temp\procexp64.exe
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList s\\4034A037-3505-4974-804E-75BD40A59C0A}\DateLastConnected





Click Save to save the selected Artifact List or Cancel to cancel the above selection.

Centalment Integration Centalment Integratio	TIPE	ACTIONS	
ORE O	TIPE	ACTIONS	
Chilledowskowstanting			
C. (minoras falacenas fundamilia por exe	Add Type		×
C/Windows/regedit.exe	Add Type		×
C: Users\nhandt4 AppDatalLocal Templprocexp84.exe	Add Type		×
HKLM(SOFTWARE)Microsoft;Windows NT;CurrentVersion) NetworkList(Profiles)[40344037-3505-4974-804E-758D40A59C0A][DateLastConnected	Add Type		×

• Select Type for Artifacts

The system supports assigning 1 Type/Action to 1 Artifact or 1 Type/Action to many Artifacts. There are 3 types, including: File, Process, Registry. Each Type has its own Action.

		+ Add artifacts	Save & Next Step
Containment Integration			
08/67	TYPE	ACTIONS	
C:(Windows\system32)(SnippingTool.exe	PROCESS	Terminate	×
C:/Windows/regadit.ese	PROCESS	Suspend	×
C:(Usersinhandsi/AppDatai)Locali/Tempi procesp64.exe	FILE	Delete	×
HKLM/SOFTWARE/Microsoft/Windows NT/CurrentVersion/NetworkList/Profiles/(40344037-3505-4974-804E-758D40A59C0A)(DateLastConnected	REGISTRY	Delete	×

After completing the assignment of Type and Action, Click Save & Next Step to save and move to the next step or Click + Add artifacts to continue adding Artifact.

• Deploy to Agent

Agent List is obtained from the Detection tab

 Tick to select the Agent that is online in the Agent List of IR Flow to switch to the List of agents that execute the Response scenario.

2	Deploy to agent		
	Agent list (1 agent(s) selected) Choose GNUNII agent in list below and click >> button to add to apply agent list	30 Agent apply list Click Deploy button to apply rule for agent list below Deploy	
	Agent_cill Softmassescontexesmocrases Online		

- Tick to select Agent to deploy.

Deploy
Deploy
° U



Successes

2	Deploy to agent				
	Agent list Choose ONLINE agent in list below and click >> button to add to apply agent list	»	Agent apply list Click Deploy button to apply rule for agent list below		Deploy
			nhandt4-PC Agent_id: 805F783E59EEC77628867C088853F8D63DC6285	Online •	17:56:49 24/05/2019 successed

Click on the details to view the scenario implementation results

Deploy result				
Object	Туре	Action	Result	
C:\Windows\system32\SnippingTool.exe	PROCESS	Terminate	successed	
C:\Windows\regedit.exe	PROCESS	Suspend	Error: Incorrect function.	
C:\Users\nhandt4\AppData\Local\Temp\procexp64.exe	FILE	Delete	Error: The request is not supported.	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{4034A037-35	0 REGISTRY	Delete	successed	

5.1.9. Close IR Flow

- Close IR Flow after investigation and process is complete.
- To close IR Flow click Close IR Flow on IR Flow List screen.

		Alerts	IR Flow	Investigation	Response S	etting	© en ▼	chuyennt2	- (
Search IR Flow									
Type to search							-9	Last 30 days	Q
7 result(s) 27/04/2019 17:20:31 - 27/05/2	019 17:20:31							+ Add new	IRFlow
тіме	NAME	STATUS	CREATED BY	ASSIGNED TO		NOTATION		ACTIO	NN .
11:31:24 23/05/2019	2305 test1	New	chuyennt2	congnc9		XXXXX		Close IRFlow	•Ð
11:02:49 20/05/2019	IRFlow_test_2019	New	nhandt4	nhandt4		IRFlow_2019		0	€
10:22:43 15/05/2019	phuoenm3 0515 1	New	phuocnm3	phuocnm3		laksdf		0	€
09:24:01 15/05/2019	phuocnm3 test 1	Closed	phuocnm3	phuocnm3		abc		i	€
16:46:42 07/05/2019	thi test 0705	New	thild1	phuocnm3, th	anhin9	qu'eqweqweqwe		0	€
14:50:30 03/05/2019	TheDV1 test	New	thedv1	chuyennt2		test		0	€
17:34:12 02/05/2019	0205 test them artifact vào IRFLow	New	chuyennt2	hieupc4		dfdfd		()	€
Display 7/7 result(s)									

• Or click Close IR Flow on the timeline at any phase in IR Flow, such as Detection, Containment, Investigation, Response.

VEDR Portal		A	Alerts	IR Flow	Investigation	Response	Setting	⊙ en -	chuyennt2 🕒 👻
IRFlow Detail - 2305 test1 ← IRFlow List									
Create IR Flow	Containment Agent: (1)	Tool Deployed	Tool Deployer Agent: (1)	d					Close IRFlow
			Detecti	-	Containment	Investigation	Response		

 If when selecting Close IR Flow, there are unfinished tasks, such as: Containment, Live Response, Response Scenario, Deployment tool, etc., a notification will be displayed to ask the user as follows:



🖸 Trang chủ 🗙 🔛 VEDR Portal - IR Flow D 🗙 🔛 VEDR I	Portal - Event Sea 🗙 🛛 🚯 Containment - Viet	ttel E 🗙 📔 🕱 VEDR - Your Company 🗙 📔 🙀 [VEDR-18] Đóng IR flow: 🗙 🗌	🕱 (VEDR-311) Thèm api x 🛛 🕱 (VEDR-312) Thèn	napix: X 🙀 [VEDR-238] Agent Poli: X + - 🗗 X
\leftarrow \rightarrow \bigcirc \bigcirc \land Not secure 10.30.161.37/#/ir-flow/ir-flow-de	tail/27ac440795d30aa522494d184a7e138	89?tab=0		⊘☆♥ 🤉 😢 🕂 😫
	Alerts	IR Flow Investigation Response		🔄 EN 👻 chuyennt2 😩 👻
IRFlow Detail - 2305 test1 ← IRFlow List				
TIMELINE 08 O	Tool Deployed Agent: (1)	d		Close IRFlow
	Detecti	on Containment ² C investigation	Response	
Original detection				
Agent			×	
DESKTOP-EGANUBQ		🛆 Cannot close IR Flow		
Alert		1. ProcessAnalysis phase is pending ! 2. Containment phase is pending !		
TIME	GROUP		SCENARIO	SEVERITY
10:13:37 22/05/2019	unknown	Do you want to force close IR How Cancel OK	Initial Access	High
Additional detection				
Agent DESKTOP-HH412B1Q nhands4-PC X Win7-CongNC9 X Alert				
TIME	GROUP	HOSTNAME	SCENARIO	SEVERITY
11:09:41 22/05/2019	unknown	nhandt4-PC	Execution	High ×
14:07:50 15/05/2019	no_group	Win7-CongNC9	Initial Access	High ×
14:39:29 17/05/2019	unknown	DESKTOP-HHN2B1Q	Execution	High ×
Aritfacts				
TIME AGENT ID		IECT	FROM	REFERENCE
Search the web and Windows	. v S 🗭 🕅 I	💆 🐠 🚚 🍋 📴 🐻 🖉 🛄		^ (7) 🐜 🙆 💟 💭 d _a 📮 ENG 5/27/2019

- \circ $\;$ When the user selects OK, it will close all connections to the Agent in IR Flow.
- When entering the closed IR Flow, information in only 2 tabs of Detection and Investigation Result can be viewed, other tabs with different function will be disabled or will not display data.

🔒 Trang ch	ů 🗙 ⊡ VEDR Portal	- IR Flow D 🗙 🔛 VEDR F	Portal - Event Sei 🗙 🦃 Cor	ntainment - Viettel E 🗙 🃋	😵 VEDR - Your Company 🛛 🗙 📗	YEDR-	18] Đóng IR flov 🗙 🏻 🗣	[VEDR-311] Thêm api 🛛 🗙 🏻 😭 [V	/EDR-312] Thêm api 🛛 🗙 📔 😭 [VEDR-2	38] Agent Polic × 🛛 +	- ø ×
\leftrightarrow \rightarrow C	C 🕞 🔺 Not secure 10.30.16	51.37/#/ir-flow/ir-flow-de	tail/27ac440795d30aa52249	4d184a7e1389?tab=1						⊘☆€ 🦸	8 0 ± 6
٧	ÆDR Portal		Alerts	IR Flow	Investigation		Response	Setting	1	③ EN ▼ chuyer	int2 😩 👻
	Detail - 2305 test1 🔒										
TIMELINE	Create IR Flow	Containment Agent: (3)	Tool Deployed Agent: (1)	Tool Deployed	Close IR Flow						• •
			j	Detection	Containment	YQ.	Investigation	Response			
0	Rule setting Choose one rule setting to	a continue next step									
- 2	Deploy to agent										
	Agent list Choose agent in list be						Agent apply list				Start
					NOT APPLIED						
					NOT APPLIED						
					STOPPED .						
					NOT APPLIED						



And Barban				GHATE IS GOVERNOUN					0	0
				IR Flov	w Investigation				🕙 EN 👻 chuyennt2 (۲
	w Detail - 2305 test1	ê		_						
	w List									
	•	•	×	×						-
	Create IR Flow	W Containment Agent (I)	Agent: (1)	Agent: (3)	Close IR Flow					
				Detection	FO contributed		28% Bornanta			
Image: marrow marro			111	belection	Lei containment	investigation	- Nesponse			
LEXENDELANCE AND	131 P	Process Analysis		Q Event Searc	h		C ^M Tools		Investigation result	
					6	2				
					IDElow	is closed				
					IRFlow	is closed				
					Go to investigation	Result to view data!				
N N <td></td>										
col N 100 Model - R.Morel X N 100 M										
a) *										
 										
a) VDRA but Aller Nein X VDRA but Aller Nein X <td< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></td<>										
a) x) URD Runder Lever (x) (2) Containeet (x) (2)										
A for the start in 133.131.21/00/ theory: 64400/35240422343418124321 C (1) C (1) <thc (1)<="" th=""> <thc (1)<="" th=""> C</thc></thc>										
	chủ X 🖂	VEDR Portal - IR Flow D 🗴 🕓 VEDR P	Portal - Event Sei 🗙 🛛 🕅 Contain	ment - Viettel E 🗙	VEDR - Your Company X	VEDR-181 Đóng IR flor ×	👻 IVEDR-3111 Thêm api x 🖌 😜	IVEDR-3121 Thêm api : X 9 IVEDR-	2381 Agent Polic X + -	-
Acts R Flow Receiption <	chủ 🗙 🖸	VEDR Portal - IR Flow 🛙 🗴 🕑 VEDR F	Portal - Event See 🗙 🚱 Contain	ment - Viettel E 🗙	👻 VEDR - Your Company 🗙	😵 [VEDR-18] Đóng IR flov 🗙	👰 [VEDR-311] Thêm api x 🗶 🏾 🙀	[VEDR-312] Thêm api = 🗙 🍟 [VEDR-	238] Agent Polic X + -	-
VDDR Pots Adds IR Bow Intestigation Response Setting It is a closed It Containeet Containeet It Containeet It It<	chù x 🖂 C 🎧 🔺 Not secure	VEDR Portal - IR Flow D x VEDR F 10.30.161.37/#/ir-flow/ir-flow/det	Portal - Event Se: 🗙 🚺 Contain tail/27ac440795d30aa522494d1	ment - Viettel E × 84a7e1389?tab=2	😤 VEDR - Your Company 🗙	😤 [VEDR-18] Đóng IR flor 🗴	🏆 [VEDR-311] Thèm api 🛛 🗙 🏻 🙀	[VEDR-312] Thêm api x 🕴 😭 [VEDR-	238] Agent Poli: x + - 	
Patial 2205 test il	chù x 🖻 C 🎧 🛦 Not secure	VEDR Portal - IR Flow D x VEDR F 10.30.161.37/#/ir-flow/ir-flow-det	Portal - Event Se: 🗙 🎲 Contain tail/27ac440795d30aa522494d1	ment - Viettel E 🗙 84a7e1389?tab=2	👻 VEDR - Your Company . 🗙 🏻	🕱 [VEDR-18] Đảng IR flor 🗙	👷 [VEDR-311] Thêm api : 🗙 🔗	[VEDR-312] Thêm api x 🕴 😭 [VEDR-	238] Agent Poli: x + - 	
	e chu x 열 C 슈 A Not secure VEDR Portal	VEDR Portal - IR Flow D × 🖂 VEDR F 10.30.161.37/#/ir-flow/ir-flow-det	Portal - Event Sei × 🚱 Contain tail/27ac440795d30aa522494d1 Alerts	ment - Viettel E × 84a7e1389?tab=2 IR Flov	YEDR - Your Company ×	🍷 [VEDR-18] Dång IR flor: 🗴	♀ [VEDR-311] Thêm *pi = × ♀ Setting	[VEDR-312] Thêm api = 🗙 😵 [VEDR-	238) Agent Polis X + - ② ☆ � ② 2 8 ③ EN マ churyennt2 (
And a	chi x 😫 C 🍙 🛦 Not secure VEDR Portal	VEDR Portal - IR Flow D × 🔐 VEDR F t 10.30.161.37/#/ir-flow/ir-flow-det	Portal - Event Sei X 🎲 Contain tail/27ac440795d30aa522494d1 Alerts	ment - Viettel E 🗙 84a7e1389?tab=2 IR Flow	YEDR - Your Company X	Ŷ [VEDR-18] Đáng IR filo∷ × n Response	🗣 [VEDR-311] Thêm api = 🗙 😭 Setting	[VEDR-312] Thêm api ::: 🗙 😭 [VEDR-	238) Agent Poli X + 2 ☆ � � 와 銘 ⓒ EN - chuyennt2 (θ
Create ill Filow Containent Tool Deployed Tool Deployed Close R Row Create ill Filow Containent Coll Deployed Coll R Row Coll R Row Coll Percess Analysis C. Event Search Coll R Row Coll R Row Coll R Row PESKTOP FEGMURQ Soccess (2) Coll Event Search Coll R Row Coll R Row PESKTOP FEGMURQ Soccess (2) Coll Event Search Coll R Row Coll R Row PESKTOP FEGMURQ Soccess (2) Coll Event Search Coll R Row Coll R Row PESKTOP FEGMURQ Soccess (2) Coll Event Search Coll R Row Coll R Row PESKTOP FEGMURQ Soccess (2) Soccess (2) Coll R Row Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Coll R Row PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) Soccess (2) PESKTOP FEGMURQ Soccess (2) Soccess (2) Soccess (2) So	ebú x ⊡ C ∩ ▲ Not secure VEDR Portal	VEDR Portal - IR Row D × 🛛 VEDR F 10.30.161.37/#/ir-flow/ir-flow-det	Portal – Event Sel 🗙 🔞 Contain tail/27ac440795d30aa522494d1 Alerts	ment - Viettel E 🗙 84a7e1389?tab=2 IR Flov	♥ VEDR - Your Company × w Investigation	Y [VEDR-18] Doing IR flow x Response	Ŷ [VEDR-311] Them api∞ × Ŷ Setting	[VEDR-312] Them api = 🗙 😵 [VEDR-	238] Agent Pole: X + 승규 후 우 유 요 중 EN + chuyenni2 (•
Observed	chú x 2 C A Not secure VEDR Portal w Detail - 2305 test1 w List	VEDR Portal - IR Flow D × VEDR P 10.30.161.37/#/ir-flow/ir-flow-det	Portal - Event Sei 🗙 🔯 Contain tail/27ac440795d30aa522494d1 Alerts	ment - Viettel E x 84a7e1389?tab=2 IR Flow	♥ VEDR - Your Company × w Investigation	😧 [VEDR-18] Dáng IR Ro: 🗴 n Response	Ŷ [VEDR-311] Thèm api⇒ x Ŷ Setting	[VEDR-312] Them age = X 😭 [VEDR-	238] Agent Poli: X +	0
Create it River Containment Agentic Tool Deployed Agentic Tool Deployed Agentic Close River Liver Containment Agentic Containm	A Not secure C A Not secure VEDR Portal v Detail - 2305 test1 wList	VEDR Portel - IR Rew C x VEDR Portel - IR Rew C x VEDR Portel - IR Rew C x VEDR Portel - IR Rew C + I = I = I = I = I = I = I = I = I = I	Portal - Event Sei X 🕼 Contain tail/27ac440795d30aa522494d1 Alerts	ment - Viettel E 🗙 84a7e1389?tab=2 IR Flow	Ŷ VEDR - Your Company x w Investigation	😧 (VEDR-18) Dong ilk filo: 🗴 n Response	♀ [VEDR-311] Them api ⇒ × ♀ Setting	[PEDR-312] Them age = X 😵 [PEDR-	238] Agent Polis X + ② ☆ � @ Ø Ø Ø ③ EN + chuyennt2 (•
Create IR Pow Containment Aperticit Tool Deployed Aperticit Close IR Pow Aperticit	ebé x 🛛 🕰 C 🖳 🛦 Not secure VEDR Portal v Detail - 2305 test1 with	VEDR Ronal - IR Row C X VEDR Ronal - IR Row C X VEDR Ronal - IR Row C X VEDR Roman - IR Row - det	Portal - Event Se : x 😰 Contain Lail/27ac440795430aas522494d1 Alerts	ment - Viettel E × B4a7e1389?tab=2 IR Flov	♀ VEDR - Your Company x w Investigation	Ŷ [VEDR-18] Dong IR no∷ x D Response	♀ [VEDR-311] Them api = × ♀ Setting	(NEDR-312) Theim age = X 😧 (NEDR-	238] Agent Pelli X + -	•
Line Line <thline< th=""> Line Line</thline<>	Abi X Image: Constraint of the secure C Image: Abid of the secure VEDR Portal VEDR Portal Vectail - 2305 test1 w List	VEDR Portal - IR Rew C x VEDR A	Portal - Evert Sr. X 🛛 🕲 Contain call(273:oc440795:d30as522494d1 Atorts	ment - Viettei [x 84a7e1389?tab=2 IR Flow	 VEDR - Your Company × Investigation 	🖗 [rtDR-18] Dong iR Ro 🗴	Image:	[VEDR-312] Them agin → X 😨 [VEDR-	238] Agent Poli: x + -	•
Image: Description Image: Description Image: Description Image: Description Image: Description Image: Description Image: Description Image: Description Image: Description Image: Description Image	chù x ⊇ C m ▲ Not secure VEDR Portal w Detail - 2305 test1 w List Create IR Flow	VEDR Ponal - IR Row C x VEDR J 1 03.03.161.37/#/ir-flow/ir-flow-det	Portal - Event Sir: X 🕼 Contain Itali/27ac440795d30aa5524M4d1 Alerts	ment - Viettel I × 84a7e1389?tab=2 IR Flow Tool Deployed	VIDR - Your Company ×	Ŷ [VEDR-18] Deng IR fi∞ x n Response	🕱 (MEOR-311) Them api :: 🛪 🕏 Setting	: [9408-312] Telm api - × 😧 [9408-	238) Agent Polit X + -	•
Image: Containment Image:	del x C A Not secure VEDR Portal V Detail - 2305 test1 w Lite Create IR Flow	VER Portal - IR Row D x VER A 1 0.03.0161.37/#/ir-flow/ir-flow-det w Containment spert (s)	Portal - Event Sex X V Contain cui/(27.ac.440/195.d1)0aa.522.494.d1 AlcertS V Tool Deployed agent (a)	ment - Viettel I × 84a7e1389?tab=2 IR Flow Tool Deployed Agent (0)	VEDR - Your Company X	PrtDR-18) Deng ill fic x Response	😨 (p154-311) Them api । 🗴 😨 Setting	PIEDR-312] Delm agis - X 😭 PIEDR-	238] Agent Polis X + - ② ☆ 한 ② 월 양 EN + chuyennt2 (- 0 (1)
Image: Second Analysis Image: Control of Control	(d) X Q C Image: Comparison of the secure VEDR Portal VEDR Portal v Detail - 2305 test1 w Lat Create IR Flow	VEDR Ponal - IR Row C X VEDR J 1 0.30.161.37/#/ir-flow/ir-flow-det w Containment rgent (a)	Portal - Event Sr: X 🕼 Contain Init/27ac440795d30aas52484d1 Alorts	Ment - Viettel : x 84a7e1389?tab=2 IR Flow R Flow Tool Deployed Agent (t)	VEDR - Your Company X Investigation Close IR Flow	Present	(M206-311) Them april: x Y Setting Setting APTION	: [HERE-312] Them age : × 😧 [HERE	238) Aguen Puli: x + -	- -
DESKTOP-EGANUAR DESKTOP-EGANUARD DESKTOP-EGANU	(dù x C ∩ A Not secure VEDR Portal V Detail - 2305 test1 itat Create IR Flow	VEDR Ronal - IR Row C X VEDR R 1 03.0161.37/#/ir-flow/ir-flow-det w Containment April 10	Portal - Event Sr: X & Contain call(27ac440795430aa55249441 Aterts Tool Deployed Agent (i)	ment - Viettel : × 84a7e1389?tab=2 IR Flow Tool Deployed Aeret (0) Detection	VEDR - Your Company X w Investigation Close IR Flow Containment	(M2DR-18) Dong ill film: x Response Investigation	(M104-311) Them apt : X Setting	: [NED#-312] Telm api - X ♀ [NED#-	238] Agent Poli: x + - ⊘ ☆ ♥ 의 원 ⓒ EN - chuyennt2 (- 0 2
• DESKTOP-FGANURQ Soccess 20.7) Trice 0ETF Stotus Domiculo Action 1548 24/05/2019 GeEArtificat Type:/FLIC Type:/FLIC Type:/FLIC Type:/FLIC Domiculo Action 1548 24/05/2019 GeEArtificat Type:/FLIC Type:/FLI	eki x C A Not secure VEDR Portal VEDR Portal VETail - 2305 test1 rote Create IR Flor Create IR Flor	VEDR Ronal - IR Row D x VEDR R 1 03.03.161.37/#/ir-Row/Ir-Row-det w Containment Agent 1.0 Tocess Analysis	Portal - Event Sr: X & Contain Instituti / 2744407954310aa55249441 Afterts Tool Deployed Agent 10	Ment - Viettel 1 x 84a7e13897tab=2 IR Flow Tool Deployed Apent (0) Detection	VEDR - Your Company X N N N N N N N N N N N N N	(VEDR-18) Dong ill for x Response Response Investigation	(MESR-311) Them apt: X Setting Kesponse Response	: (NED#-312) Them age: - X 🗣 (NED#-	238) Agent Petit × + - ⊘ ☆ ♥ Ø Ø ③ EN + chuyennt2 (- 0 1 1
DESITION EGANUING Success (2,0) Titlet GET PF Status Dominuluu Actioner 1348 24/05/2039 Gef Antflakt Type FLE Type FLE Type FLE Status Dominuluu Actioner 1348 24/05/2039 Gef Antflakt Type FLE Type FLE Status Eggind Image: Comparison of Compari	eki x 2 A Not secure VEDR Portal V Detail - 2305 test1 stat Create IR Flow (2 P	VEDR Ronal - IR Row C X VEDR J 1 0.30.161.37/#/ir-flow/ir-flow-det w Containment Agent (1) VTOCESS Analysis	Portal - Event Sr: X & Contain Ital/27ac440795d30aa352494d1 Aferts	ment - Viettel (x) 64a7e13897bab=2 IR Flow Reflowed Agent III Detection Q, Event Search	VEDR - Your Company X VeDR - Your Company X Ventors (R Flow Close (R Flow Containment C	PEDR-18[Dong ill fic: x Response Response Investigation	(MESR-311) Them apt: X Setting Setting Response Tools	: (NED#-312) Them age:- X ♀ (NED#-	238) Agent Pall × + - ⊘ ☆ ♥ Ø Ø Ø ③ EN + chuyennt2 (prestigation result	- 0 (1)
init diff control status control status 1348 40%2020 Get Anthick Type FLE Type FLE<	chá x C A Not secure VEDR Fortal V Detail - 2305 test1 cuar Create IR Flow	VEDR Ronal - IR Row D x VEDR 6 1 0.30.161.37/#/ir-Row/ir-Row-det w Containment Agent (1) Toccess Analysis	Portal - Event Sr: X & Contain Intel/272ac440795d30aa352494d1 Aferts	ment - Vetter (x) 844/e13897tab=2 IR Flow Tool Deployed Apert () Detection Q Event Search	VEDR - Your Company X V VEDR - Your Company X V V V V V V Close IR Flow Containment Containment	PEDR-18] Dong IR for x Response Response Investigation	(MESR-311) Them apt: X Setting Setting Response Tools	: (NED#-312) Them age:- X ♀ (NED#-	238) Agent Pati × + - ⊘ ☆ ♥ Ø Ø ③ EN + chuyennt2 (prestigation result	- - -
1348 4249203 0 et Attitut: 1 ppe FUL Patric (Program Files)UDR/V[SSucDe 0 ppe FUL Success (Program	chá x C A Not secure VEDR Fortal V Detail - 2305 test1 clas Create IR Fion (3 P DESKTOP-EGANUBQ	VEDR Ronal - IR Row D x VEDR 7 1 03.01.161.37/#/ir-flow/ir-flow-det w Containment Apert 1.0 Trocess Analysis Success (2/3)	Notal - Event Sr. X & Contain Intel/27ac440795d30aa552494d1 Aterts Tool Opployed Agent III	ment - Vetter (x) R Flow R Flow Tool Deployed Apent III Detection Q Event Search	VEDR - Your Company X w Investigation Close IR Flow Containment a	(VEDR-18) Dong IR file: x Response Response Investigation	(MEDR-311) Them api: X Setting Setting Response Tools	: (NDR-312) Them age: x 😧 (NDR-	238) Agent Pati: x + - ⊘ ☆ ♥ Ø Ø ③ EN - chuyennt2 (☐ investigation result	- ⊖ ●
1152 24/03/2039 106 06 Autownice [13.82.0.0 6. doccesed	A Mor secure VEDR Pontal W Detail - 2305 test1 w Ust Create in Fion Q P VESKTOP-EGANUEQ THE	VUDR Penel - IR Row C × VUDR F 10.30.161.37/#/ir-Row/Ir-Row-det w Containment Aprel 10 Success (2/3) GET Br	Potel - Svert Ser X 😰 Contain tail(27ac440795530as522494dt Atorts Totol Deployed Apert (0)	ment-Vettell X 84a7e13097tats=2 R Flow R Flow Tool Deployed Apent () Detection Q, Event Search	VEDR-Your Company X Investigation Close IR Flow Containment	(MDR-18) Dong IR file: X Response Response Investigation	(M10R-311) Them spin X Setting Setting Response Tools	: (MDR-312) Thim age - × ♀ (MDR- 12)	238) Agent Poli: x + - ⊘ ☆ ♥ ∞ @ ③ EN + chuyennt2 (prestigation result	- -
1048 24/05/2033 Get Auflickt Type: FAL Patric: Virridon's System 32/06400.0000 Soccessal C O CBXKTOP-HHN2B102 Soccessa (0/1) Soccessa (0/1) <t< td=""><td>(du) x C A Not secure VEDR Pontal W Detail - 2305 test1 w Las Create IR Prov Create IR</td><td>VEDR Ponel - IR Rise: C X VEDR J 1 10.30.161.37/#/ir-Rise/Ir-Rise-det w Containment Agent (3) Success (2/3) GET #7 Get Antifact Type FILE 7</td><td>Portal - Event Ser X Cartain tau(27ac440795d30aa522494d1 Alerts X Tool Deployed Agent (8)</td><td>Refet - Vietkel X X R Flow B4a7e13897bab-2 IR Flow Totol Deployed Agent 30 Detection Q Event Search</td><td>VEDR-Your Company X M Investigation Close IR Flow Containment N</td><td>IVEDR-18) Dong ik fic: x Response Investigation</td><td>Yolds 311] Them set: X Setting Setting Tools</td><td>: (MER4-312) Them age - ×</td><td>238) Agent Put:: x + ② ☆ ⑦ ③ ⑥ ③ EN + chuyennt2 (□ Investigation result</td><td>- - - - - - - - - - - - - -</td></t<>	(du) x C A Not secure VEDR Pontal W Detail - 2305 test1 w Las Create IR Prov Create IR	VEDR Ponel - IR Rise: C X VEDR J 1 10.30.161.37/#/ir-Rise/Ir-Rise-det w Containment Agent (3) Success (2/3) GET #7 Get Antifact Type FILE 7	Portal - Event Ser X Cartain tau(27ac440795d30aa522494d1 Alerts X Tool Deployed Agent (8)	Refet - Vietkel X X R Flow B4a7e13897bab-2 IR Flow Totol Deployed Agent 30 Detection Q Event Search	VEDR-Your Company X M Investigation Close IR Flow Containment N	IVEDR-18) Dong ik fic: x Response Investigation	Yolds 311] Them set: X Setting Setting Tools	: (MER4-312) Them age - ×	238) Agent Put:: x + ② ☆ ⑦ ③ ⑥ ③ EN + chuyennt2 (□ Investigation result	- - - - - - - - - - - - - -
DESRUP 4498280 Sicces (01) DESRUP 4498280 Sicces (01) Arbite Sicces (01) TM OLICI 105500 2405/201 OLISYO 400400[(AV12MT2] Addet to 1990 105500 2405/201 Olisyo 400400[(AV12MT2] Addet to 1990 105500 2405/201 Olindowis (System2) (Sostema) Addet to 1990 12122 2405/2015 Olindowis (System2) (Sostema) Addet to 1990	(c) A Not secure (c) A Not secure VEDR Portal Vectail - 2305 test1 Not secure (c) DESKTOP-EGANUBQ R Post (c) DESKTOP-EGANUBQ Thet 15:48 34(65/2019 11:52 24(65/2019 11:52 24(65/2019	VEDR Ponel - IR Row C X VEDR J 1 (0.30.161.37/#//r-flow/ir-flow-det w Containment Apert (1) Success (2/3) GET W Get Artifact Type: FILE / Tools Autorunce [13	Portal - Event Se: X Contain tai/(27ac440795d30as522494d1 Alorts X Contain Tool Deployed Agent (8)	Refet-Verter x B4a7e13897bab-2 IR Flow Tool Geployed Agent 10 Detection Q. Event Search vc.De	VEDR - Your Company X VEDR - Your Company X V Close IR Flow Close IR Flow Containment b	IVEDR-18) Dong ill flor - X Response Response Investigation	(VEDR-311) Them spin + x Setting Setting Tools	INTER-312] Them apr → X ♀ NEOF Status • Expired • Successed	238) Agent Nui: x + ⊘ ☆ ♥ 𝔅 𝔅 ③ EN + chuyennt2 (prestigation result DownLOAD ACTI & ©	
Artifact OBJECT TIME OBJECT 105500240502310 DESKTOP-EGANLBQC(rAVI2NT2] 105500240502310 DESKTOP-EGANLBQC(rAVI2NT2] 105500240502310 Cl/Indows/System32(Jaskhostuk.ee 126257240502310 Cl/Indows/System32(Jaskhostuk.ee 126254040502310 Cl/Indows/System32(Jaskhostuk.ee	(chi) × □ (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) <	VEDR Ponel - IR Row C X VEDR J 1 0.30.161.37/#/ir-flow/ir-flow-det w Containment rocess Analysis Success (2/3) GET B' Get Antifact Type: FILE F Tools Autorunis [13] Get Antifact Type: FILE F	Portal - Event Sr: X Contain Ini/272ac440795d30as22484d1 Alorts	Here - Vater (X) 543/e1309/tab-2 IR Flow Tool Operand Agent () Detection Q Event Search vc.De poundTaskHest.Exe	VEDR - Your Company X N N Investigation Close IR Flow Containment S	(VEDR-18) Obry (II fig: - x Response Response Investigation	Setting Construction Response Construction Tools	I (MERK-312) Them apin × STATUS STATUS STATUS Status	238) Agent Ruit x + ⊘ ☆ ♥ Ø Ø ③ EN + Chuyennit2 (Presstigston result Domis.ch0 ACTII & ©	
DLCT 105500 2405/2519 DESTOP-EGANLBQC/AVJENTI2 Added to IPPior 105500 2405/2519 DESTOP-EGANLBQC/AVJENTI2 Added to IPPior 1025500 2405/2519 Ci/Indows/System32/Laskhostw.ee Added to IPPior 1242517 2405/2519 Ci/Indows/System32/Laskhostw.ee Added to IPPior 12526 2405/2519 Ci/Indows/System32/Laskhostw.ee Added to IPPior	chi x ₽ C A A lot secure VEDR Portal VEDR Portal Create IR Fox Create IR Fox Create IR Fox Create IR Fox Create IR Fox 15.48 24(5)/2019 15.48 24(5)/2019 15.49 24(5)/2019 15.49 24(5)/2019	VEDR Portal - IR Row C x VEDR 3 1 0.30.161.37/#/ir-flow/ir-flow-det w Containment special in vocess Analysis Success (2/3) GET Br Get Antiact Type: FILE F Success (0/1)	Portal - Event Sr: X Contain Intel/27ac440795d30aa522484d1 Alerts Tool Deployed sern II Portal - Electropy of the service	mere - Vatter (x) 544/re1309/tab-2 IR Flow Tool Opployed gent 1 Detection Q Event Search vc.Dae poundTaskHost.Dae	VEDR - Your Company X V Investigation Close IR Flow Containment	INTER-18) Obry III file: x Response Investigation	Setting Constraints Response Constraints Response Constraints Response Response Re	STATUS Status	238) Agent Ruit × + ⊘☆ ? ? ? ? ? 3 EN + Chuyenni2 (Investigation result DoenLOAD ACTI ± C ± C	
10550024/05/2019 DESKTOP-EGANUEQC/cN/YEINT2 Added to IPFlow 10550024/05/2019 Cl/Wndows/System2/Laskhostw.ee Added to IPFlow 14215724/05/2019 Cl/Wndows/System2/Laskhostw.ee Added to IPFlow 15152124/05/2019 Cl/Program File/UER/VESN-case Added to IPFlow 15152124/05/2019 Cl/Program File/UER/VESN-case Added to IPFlow 15152124/05/2019 Cl/Program File/UER/VESN-case Added to IPFlow 1515212405/2019 Cl/Program File/UER/VESN-case Added to IPFlow 1515212405/2019 Cl/Program File/UER/VESN-case Added to IPFlow 1512242405/2019 Cl/Program File/UER/VESN-case Added to IPFlow	A Mot secure VEDR Portal Vental Zaos Create IR Fion DeskTOP-ECANUEQ That Isse 2405/2019 Isse 2405/2019 Secure 2405/2019 Sec	VEDR Portal - IR Row C x VEDR 3 1 0.30.161.37/#/ir-flow/ir-flow-det w Containment special success (2/3) Get Eur Get Antifact Type: PILE F Success (0/1)	Portal - Event Sr: X Contain Intel/27ac440795d30aa522494d1 Aferts	mere - Vetter (X) 5447e13097hab-2 IR Flow X Tool Deployed gen () Detection Q Event Search vc.Dae proundTaskHost.Exe	VEDR - Your Company X V Investigation Close IR Plow Containment Containment	INTER-18) Cong ill fic: x Response Response Investigation	Setting	Status Status	238) Agent Rei: x + - ⊘ ☆ ♥ Ø Ø ③ EN + chuyennt2 (Investigation result Dotestubei Actri	
10:3500 24/05/2019 C/(Windows) System32 (askhotthu.exe Added to IPFlow	(a) × ≥ (c) (a) Not secure VEDR Portal Verall v Detail -2305 test1 v Verall (b) (c) v Detail -2305 test1 v Detail -2405/2019	VICR Penel - IR Rive: X VICR 1 10.30.161.37/#/ir-Rive/Ir-Rive-det Count of the second of the secon	Partiel - Event Ser: X P Contain tail(27)ac440795530as522494d1 Atorts Totol Deployed Apent (0) Apent (0) Attr: C:(Program Files)/VEDRI/VESS 820.0 Attr: C:(Windows)System32(Back buckt	ment-Vettell X X B437e13097tats=2 RF how RF	VEDR - Your Company X V V V V Cover IR Flow Containment Containment	INTER-18] Corry IR for: x Response Response Investigation	(M1504-311) Them apt: X Setting C Tools	STATUS ■ Discressed ■ Successed	238) Agent Pati × + - ⊘ ☆ ♥ Ø Ø ③ EN + chuyennt2 (Investigation result DOSTLOAD ACTI ± C ± C	
14/2157 24(95/2019 Cl(Windows/System/Zim/beril/Mill/Pir/SE.see Added to IPFlow 151922 14(95/2019 Cl/Program Files/USDRI/SSG-cae	(a) X Image: Comparison of the secure (C) (a) Not secure VEDR Portal VEDR Portal (c) (a) Not secure (c) (a) (b) (c) (a) (c) (c) (a) (c) (c) (a) (c) (c) (c) (c) (c) <td< td=""><td>VECR Ponel - IR Rise: 2 X VECR VICRA 1 10.30.161.37/#/ir-Rise/Ir-Rise-vector w Containment April 10 Success (2/3) GET Br Get Antifact Tools Autorums (13 Get Autorums</td><td>Portal - Event Ser X R Contain tax1/27ac440795430aa522494d1 Alorts Totol Diployed Agent (II) Totol Diployed Agent (II) Alorts Totol Diployed Agent (II) Alorts Alorts Alorts Contained Alorts Alorts Contained Alorts Contained Co</td><td>Refet - Vietkell X X X X X X X X X X</td><td>VEDR-Your Company X</td><td>IVEDR-16) Dong ill fici X Response Investigation</td><td>IVEDR-311] Them set: X Setting C Tools</td><td>International production of the second s</td><td>228) Agent Nui: × + ⊘ ☆ ♥ ♪ & ③ EN + chuyennt2 (□ Investigation result □ 00000.0.00 ACTI ↓ C ↓ C ↓ C</td><td></td></td<>	VECR Ponel - IR Rise: 2 X VECR VICRA 1 10.30.161.37/#/ir-Rise/Ir-Rise-vector w Containment April 10 Success (2/3) GET Br Get Antifact Tools Autorums (13 Get Autorums	Portal - Event Ser X R Contain tax1/27ac440795430aa522494d1 Alorts Totol Diployed Agent (II) Totol Diployed Agent (II) Alorts Totol Diployed Agent (II) Alorts Alorts Alorts Contained Alorts Alorts Contained Alorts Contained Co	Refet - Vietkell X X X X X X X X X X	VEDR-Your Company X	IVEDR-16) Dong ill fici X Response Investigation	IVEDR-311] Them set: X Setting C Tools	International production of the second s	228) Agent Nui: × + ⊘ ☆ ♥ ♪ & ③ EN + chuyennt2 (□ Investigation result □ 00000.0.00 ACTI ↓ C ↓ C ↓ C	
15192124/05/2019 Ci/Program Files/UE/RIVESSoc.exe 171226324/05/2019 Ci/Program Files/UE/RIVESConnectionNanager.exe Added to IRFilow 171226324/05/2019 Ci/Windows(system2)/(ERRVES2.0LL Added to IRFilow	(a) × • (a) A Not secure VEDR Portal • w Detail - 2305 test1 • w Detail - 2305 test3 • • • •	VEDR Ponel - IR Row C X VEDR J 1 (0.3.0.161.37/#/ir-flow/ir-flow-det Containment Apert (0) VEDR Ponel - IR Row C X VEDR Ponel - IR Row C X VE	Portal - Event Ser X Contain tai/(27ac440795d30as522494d1 Alorts Xent Service Tool Deployed Agent Service Agent Se	ment-Vestel X X B437e13897bab-2 IR Flow Tool Geployed Aren 10 Detection Q. Event Search vc.Dre groundTaskHost.Dre	VEDR-Your Company X W Investigation Close IR Flow Containment a	Internet interne	(VEDR-311) Them spin + x Setting C Tools	INTER-312] Them apr ×	238) Agent Poli: x + ⊘ ☆ ♥ ♥ ♥ ♥ ③ EN + chuyennt2 (Poweligston result	
17:12:26 34/05/2019 CL/Program Files/VEDR/USConnectionManager.exe Added to 19Flow 17:12:26 34/05/2019 CL/Windows(system2)/KERNEL32.0LL Added to 19Flow	chi x 2 C A Not secure VEDR Fortal VEDR Fortal V Petall - 2305 test1 v Crastel IR Fox C B DESKTOP-EGANUBQ Tiste 15:42 4/05/2019 15:42 24/05/2019 DESKTOP-HOHN2B1Q CARTIFICE TIME 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019 10:43 24/05/2019	VEDR Ponel - IR Row C X VEDR J 1 (0.30.161.37/#/ir-flow/ir-flow-det w Containment Agent (c) Success (2/3) GET 8* Get Artifact Type: FILE F Success (0/1) Get C (c) C (c)	Portal - Event Sr: X Contain Int/272ac440795d30ab22494d1 Atorts Tool Deployed Apert (0) Tool Deployed Apert (0) Attric Ci(Program Files)/EDRIVESS 82.0.0 Table: Ci(Windows)(System32(Back B2CH StrOP-CAMUBQ(CHUTENT22 Windows)(System32(Backbothus))	erent - Verter x B42/e1309/tab-2 IR Flow D42/e1309/tab-2 IR Flow Detection Detection Detection Q Event Search w.c.De erent eren	VEDR-Vour Company X VEDR-Vour Company X V Close IR Flow Containment N	Investigation		INTER-312] Them apr ×	238) Agent Noi: x + ⊘ ☆ ♥ ♥ Ø Ø ③ EN + Chuyennit2 (Porestigation result	
17:12:28 24/05/2019 C:\Windowskystem32/KERNEL32.DLL Added to IRFlow 🗸	chi X Image: Chi and the secure VEDR Fortal VEDR Fortal VDEtail - 2305 test1 Image: Chi and the secure VDESKTOP-EGANUBQ Image: Chi and the secure DESKTOP-EGANUBQ Image: Chi and the secure 15:48 24/05/2019 Image: Chi and the secure 16:58:5124/05/2019 Image: Chi and the secure 16:58:5124/05/2019 Image: Chi and the secure	VEDR Portel - IR Row C x VEDR 3 1 0.30.161.37/#/ir-flow/ir-flow-det	Portal - Event Se: X Contain Intel/27ac440795d30aa522484d1 Alerts Tool Deployed agent II For Clifford Section 2010 For Clif	ment - Vettell X X B4a7e13097tata-2 IR Flow Tool Deployed Apertion Detection Q Event Search v.r.De groundTaskHost.De	VEDR-Vour Company X V V Close IR Flow Containment	INVESTIGATION	Setting Constant Themapic X	STATUS Status	238) Agent Rei: x + ⊘ ☆ ♥ Ø Ø ③ EN + chuyenni2 (EN + chuyenni2 (EN + chuyenni2 (S EN + chuyenni2 (C C C C C C C C C C C C C C C C C C	
	chi X 2000 C A Not secure VEDR Portal VEDR Portal VEDR Portal VEDR Portal VEDR Portal VEDR Portal VEDR Portal VEDR Portal VEDR Portal (2) P (2)	VEOR Ponel - IR Rise: 2 × v VOR 1 1 10.30.161.37/#/ir-Rise:-det w Containment April 10 Success (2/3) GET Br GET Artifact Type: FILE F Success (2/3) GET C GET Artifact Type: FILE F Success (2/3) GET C GET Artifact Type: FILE F Success (2/3) GET C GET C	Abrial - Event Ser X R Contain tal/27ac440795430as52249441 Alorts Totol Diployed Apent (II) Totol Diployed Apent (II) Tath: CL/Program Files//EDRI/VESS 82.0.0 Tath: CL/Program Files//EDRI/	ment - Vettell X X B4a7e13097bab-2 R Flow Tool Deployed Agent III Detection Q Event Search CDE poundTaskHost.Exe a m m SEnse	VEDR-Your Company X Investigation Close IR Flow Containment	IVEOR-16) Dong ill fici X Response Investigation	IVEDR-3111] Them serie: X Setting Setting Tools	International and a second design of the second	228) Agent Rui: × + ⊘ ☆ ♥ ♥ Ø Ø Investigation result Dotations Added to IRFlow Added to IRFlow Added to IRFlow	

1

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



6. Investigation Screen

The Investigation screen includes a number of small tabs, which are Process Analysis, Event Search, and Deploy Tools. In terms of operation, these two functions are not much different from those in IR Flow, however, there are some other points that will be described in details as follows:

6.1.1. Investigation Process Analysis

The function allows the user to create a connection and check the process state under the user's machine. In which:



- List of user machines:
 - \circ User login under root group: Display all Agents in the active system < 30 days.
 - User login under default group: Display all Agents in the default group.
 - User login under parent-level group: Display all Agents in the group of the user logging in and the corresponding child-level group.
 - User login under a child-level group or many child-level groups: Display all Agents belonging to the group of the user logging in.
- Step 1: Search and select Agent to connect (Notes: To make sure to connect, the list only displays the online machines.)



Choose agent 🗸		I
Q Search agent		
DESKTOP-NPLF9RK (35674DFE640571E950A0FEEF7		
• VCS (07DC8C7154AB47371E9595AF52F88E43478F8C		
Win10x64DRE (F513995917335DEF78C30E3B792ED4		
Win7x64-A-3-PC (0A58A9926F37E92F7F8A7C9CACE		
Win7x64-A-PC (E7240263DA88051ABB0CD78E201FD		
• phula-ubuntu-18 (ED8369ED38DE994B35E383D227A		

Select 1 machine and click to make the connection (connection can take up to 60 seconds.)



• Step 2: View the list of active processes at the user's machine.



Process Analysis				Win7x64-A-3-	°C	× 🕨 0 H	low to use this function
HOST NAME Win7x64-A-3-PC (0A58A9926F3)	7E92F7FBA7C9CACEBFC304DC540FE)	CONNECTED TIME 27/10/2021 10:29:57	DURATION 00:00:56	STATUS Running			
Q Type to search							Q O Refresh
4 results Last updated: 27/10/2021	1 10:30:02				Verify signature	V Filter by signature	Show columns 🔻
Name	PID	Path	User name	Command line	Signature		Action
smss.exe	300	C:\Windows\System32\smss.exe	SYSTEM	\SystemRoot\System32\sms	.exe N/A		
csrss.exe	376	C:\Windows\System32\csrss.exe	SYSTEM	%SystemRoot%\system32\csi	ss.exe Obje N/A		
wininit.exe	416	C:\Windows\System32\wininit.exe	SYSTEM	wininit.exe	N/A		
w services.exe	516	C:\Windows\System32\services.exe	SYSTEM	C:\Windows\system32\servic	es.exe N/A		
▼ svchost.exe	644	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\system32\svcho	st.exe -k DcoN/A		
unsecapp.exe	1620	C:\Windows\System32\wbem\unsecapp.e	SYSTEM	C:\Windows\system32\wbem	unsecapp.eN/A		
prevhost.exe	3384	C:\Windows\System32\prevhost.exe	AnhNN	C:\Windows\system32\prevh	ost.exe (914 N/A		3
slui.exe	5952	C:\Windows\System32\slui.exe	AnhNN	C:\Windows\System32\slui.er	e -Embedding N/A		
WmiPrvSE.exe	12636	C:\Windows\System32\wbem\WmiPrvSE.	NETWORK SERVICE	C:\Windows\system32\wbem	\wmlprvse.eN/A		
VBoxService.exe	704	C:\Windows\System32\VBoxService.exe	SYSTEM	C:\Windows\System32\VBox	Service.exe Oracle Corporati	ion	
svchost.exe	772	C:\Windows\System32\svchost.exe	NETWORK SERVICE	C:\Windows\system32\svcho	st.exe -k RP N/A		
svchost.exe	832	C:\Windows\System32\svchost.exe	LOCAL SERVICE	C:\Windows\System32\svcho	st.exe -k Loc N/A		
▼ svchost.exe	920	C:\Windows\Svstem32\svchost.exe	SYSTEM	C:\Windows\Svstem32\svcho	st.exe -k Loc N/A		

In which, the interface is divided into below information groups:

- (1) The information group related to the connection, including: The connecting machine, the time of creating the connection, the duration of the connection to the present and the connection state.
- (2) The information group supports searching/refreshing and filtering data in the list, including the following actions:

^Q: Allow searching by keyword of the data currently displayed in all fields on the list.

• Refresh : Allow refreshing data (still hold the the search conditions and filter conditions in use, only get the latest data from the user's machine to display).

• Verify signature : Enable/disable to obtain digital signature information for processes. In case this configuration is enabled, the progress data by digital signature is enabled to filter.

Filter by signature
Select all
Verified
Not verified
🗹 Not available

The digital signature states will specify the color of the corresponding record.



CRYPTSP.dll	C:\Windows\system3d0c2fbb6d97416b01 7eab6c37f0a845e64 Microsoft Corporation	Microsoft Windows
GDI32.dll	C:\Windows\system31084aa52ccc324ea5 6e972cf624f7c0de81 Microsoft Corporation	Microsoft Windows
IMM32.DLL	C:\Windows\system3aa2c08ce85653b1a0 83dfd0c119b20aedb Microsoft Corporation	Microsoft Windows
KERNELBASE.dll	C:\Windows\system3da68c291b4ef2dec9c21aa4779fc21e7621 Microsoft Corporation	Microsoft Windows
LPK.dll	C:\Windows\system3d202223587518b13d9db971b866d058adb Microsoft Corporation	Microsoft Windows
MSCTF.dll	C:\Windows\system3c431eaf5caa1c82cacaddf850128dc675e6 Microsoft Corporation	Microsoft Windows
NSI.dll	C:\Windows\system3044fe45ffd6ad40e3b a1688a5e6e0f7037c Microsoft Corporation	Microsoft Windows
PerfCtrl.dll	C:\Program Files\Ajia a8a221af714077ec8 e11aec935d0a34766 Viettel Corporation	Viettel Group
RPCRT4.dll	C:\Windows\system30611473c1ad9e2d9990afcc2a60350ece27Microsoft Corporation	Microsoft Windows
USER32.dll	C:\Windows\system3 fe70103391a64039a f7d219d75037bc98f6 Microsoft Corporation	Microsoft Windows
USP10.dll	C:\Windows\system32f8b1e3ee3545d3b5 2a3ec01f3bafe7d7d6 Microsoft Corporation	Microsoft Windows
VESSvc.exe	C:\Program Files\Ajia e381c58f04dae8f2a2 c6510091a2433f918fN/A	N/A
advapi32.dll	C:\Windows\system36df46d2bd74e3da1b 2dc945f6f2c4a82189Microsoft Corporation	Microsoft Windows

- Verified: Green with digital signature and still valid
- Not verified: Red no digital signature or expired digital signature
- N/A: White no digital signature information found.

show columns **•** : Allow adjusting the display field on the progress list.

On the list, except the Name field, which is always displayed permanently, the remaining fields can be optionally displayed or not displayed.





 (3) Process list: Display current progress data on user machine with selected information fields in Show column section. At each record, double click to view progress details.

2	Pro	ocess detail						~ ×
<	c	Loaded modules	File handles	Key handles	Threads		Sections	Network cc ゝ
	Q	Type to search				Q	6	View all artifacts (10)
F	Path							Action
\	REGI	STRY\USER\.DEFAULT\S	OFTWARE\Microsoft\Wi	ndows NT\CurrentVersion				
١	REGI	STRY\USER\.DEFAULT\C	Control Panel\Internationa	al				
١	REGI	STRY\MACHINE\SYSTE	M\ControlSet001\service	s\WinSock2\Parameters\P	rotocol_Catalog9			
1	REGI	STRY\MACHINE\SYSTE	M\ControlSet001\service	s\WinSock2\Parameters\N	lameSpace_Catalog	5		
۲١	REGI	STRY\MACHINE\SYSTE	M\ControlSet001\Control	SESSION MANAGER				
r ۱	REGI	STRY\MACHINE\SYSTE	M\ControlSet001\Control	\NIs\Sorting\Versions				
r١	REGI	STRY\MACHINE\SOFTW	/ARE\Microsoft\Windows	NT\CurrentVersion\Image	File Execution Optio	ns		
r١	REGI	STRY\MACHINE\SOFTW	/ARE\Microsoft\Windows	NT\CurrentVersion\AppCo	ompatFlags			
r١	REGI	STRY\MACHINE						
г								
г								
N								
r								
	_							
	9 resi	JITS						

Progress details are divided into tabs. For each tab, a corresponding list of information is displayed.

• Step 3: Marking artifact

Similar to the Process Analysis function in IR Flow, this screen also provides marking of artifacts for investigation.

User can select progress outside the list to mark.



Name		PID	Path	User name	Command line	Signature	Action
smss.ex	ce	300	C:\Windows\System32\smss.exe	SYSTEM	\SystemRoot\System32\smss.exe	N/A	
csrss.ex	(e	376	C:\Windows\System32\csrss.exe	SYSTEM	%SystemRoot%\system32\csrss.exe Obje.	N/A	
▼ wininit.e	exe	416	C:\Windows\System32\wininit.exe	SYSTEM	wininit.exe	N/A	
▼ serv	ices.exe	516	C:\Windows\System32\services.exe	SYSTEM	C:\Windows\system32\services.exe	N/A	D D
	svchost.exe	644	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\system32\svchost.exe -k Dco	Mark artifact	
	unsecapp.exe	1620	C:\Windows\System32\wbem\unsecapp.e	SYSTEM	C:\Windows\system32\wbem\unsecapp.e	N/A	
	prevhost.exe	3384	C:\Windows\System32\prevhost.exe	AnhNN	C:\Windows\system32\prevhost.exe {914.	N/A	
	slui.exe	5952	C:\Windows\System32\slui.exe	AnhNN	C:\Windows\System32\slui.exe -Embeddir	ng N/A	

Or mark suspicious objects in process details.

Path	Action
\REGISTRY\USER\S-1-5-21-3949336984-4152371306-1276221334-1000_CLASSES	
\REGISTRY\USER\S-1-5-21-3949336984-4152371306-1276221334-1000	Mark artifact
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER	
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NIs\Sorting\Versions	
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	
\REGISTRY\MACHINE	

For each selected object, select Mark with edit - mark the current content directly.

C:\Windows\system32\Dwm.exe	Mark without edit
C:\Windows\System32\dwm.exe	
C:\Windows\System32\svchost.exe	

Or users can edit object content before marking.



After marking, to review the list by clicking

Notes: This button is only displayed when at least 1 artifact is marked.



1	Marked Artifact						\times
	Time	Agent ID	Object	From	Reference	Action	
	27/10/2021 11:08:53	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Windows\System32\services.exe	PROCESS_ANALYSIS	83A5DAAD		
	27/10/2021 11:08:54	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajiant\VESSvc.exe	PROCESS_ANALYSIS	83A5DAAD		
	27/10/2021 11:08:56	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajiant\autoscan\VESAuto	PROCESS_ANALYSIS	83A5DAAD		
	27/10/2021 11:08:58	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajiant\VESUpdater.exe	PROCESS_ANALYSIS	83A5DAAD		
	27/10/2021 11:09:01	0A58A9926F37E92F7F8A7C9CACE8FC304DC540FE	C:\Program Files\Ajiant\propre\VESProPre	PROCESS_ANALYSIS	83A5DAAD		
	27/10/2021 11:09:05	0A58A9926F37F92F7F8A7C9CACF8FC304DC540FF	C:\Program Files\Aiiant\propre\BLS\Securi	PROCESS ANALYSIS	83A5DAAD		
10) results			0.1111001101010101010102			

• Step 4: Add artifact to IR Flow

On the Marked artifact tab, click Add to IR Flow on a record or select multiple artifacts in multi-select mode and click Add to IR Flow.

		YSIS	83A5DAAD	
Marked Artifact	to IB Flow	YSIS	83A5DAAD	
■ Time Agent I 27/10/2021 11:08:53 0A58A	ID 9926F37E92F7F8A7C9CACE8FC304DC540FE	sis	83A5DAAD	T <u>+</u> ⊗
 27/10/2021 11:08:54 0A58A 27/10/2021 11:08:56 0A58A 	9926F37E92F7F8A7C9CACE8FC304DC540FE	S Add	to IR Flow	
27/10/2021 11:08:58 0A58A	9926F37E92F7F8A7C9CACE8FC304DC540FE			

Choose from a ready-made IR Flow or create a new IR Flow.



(1) Ready-made IR Flow list:

• User login under root group: Display all IR Flow in the system.



- User login under default group: Display all IR Flow assigned to the user logging in.
- User login under parent-level group: Display all IR Flow assigned to the user logging in and the users belonging to the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all IR Flow assigned to the user logging in.

Add to IR Flo	W	DOIGHOIT		×	
IR Flow name	Centos637				
Assignee(s)	o root				
Note (optional)	- may that				
List of artifacts	vstem32\services.exe				
C:\Program File	es\Ajiant\VESSvc.exe				
			Cancel	Add to IR Flow	

The assigned to list when creating a new IR Flow

- User login under root group: Display all usernames in the system.
- \circ User login under default group: Display the username of the user logging in.
- User login under parent-level group: Display all usernames belonging to the child-level group of the user logging in and the user logging in.
- User login under a child-level group or many child-level groups: Display the name of user logging in.
 - If choose to add into an existed IR Flow, when moving to the Detection artifact screen, it will be added to the Additional detection section.
 - If choose to add a new IR Flow, when moving to the Detection artifact screen, it will be added to the Original detection section.



			IR Flow						chuyennt2 😩
al detection									
int									
ESKTOP-EGANUBQ									
rt									
TIME		GROUP		HOSTNAME		SCENARIO		SEVERITY	
10:13:37 22/05/2019		unknown		DESKTOP-EGANUBQ		nitial Access		High	
onal detection									
ESKTOP-HHN2BIQ n rt TIME	handt4-PC X Win7-CongNC9 X	GROUP	HOSTN	м	SCENARIO		SEVERITY		
11:09:41 22/05/2019		unknown	nhandt	4-PC	Execution		High		×
14:07:50 15/05/2019		no_group	Win7-C	ongNC9	Initial Access		High		×
14:39:29 17/05/2019		unknown	DESKT	DP-HHN2B1Q	Execution		High		×
facts									
TIME	AGENT ID		OBJECT			FROM		REFERENCE	
10:35:00 24/05/2019	B2A03630B8EEA76B1D5B7105B70DD4F	4DE5E593E	DESKTOP-EGANI	IBQ\CHUYENNT2		WIN_EVE	NT_LOG	fPC152oB89lgfaypWJx0	×
10:35:00 24/05/2019	B2A03630B8EEA76B1D5B7105B70DD4F	4DE5E593E	C:\Windows\Syst	em32\taskhostw.exe		WIN_EVE	NT_LOG	fPC152oB89lgfaypWJx0	×
14:21:57 24/05/2019	B2A03630B8EEA76B1D5B7105B70DD4F	4DE5E593E	C:\Windows\Sys	em32\wbem\WmiPrvSE.exe		WIN_EVE	NT_LOG	hPC16GoB89lgfayp-rm3	, ×
17:12:26 24/05/2019	B2A03630B8EEA76B1D5B7105B70DD4F	4DE5E593E	C:\Program Files	VEDR\VESConnectionManager.exe		PROCES	_ANALYSIS	962D2A61	×
17:12:26 24/05/2019	B2A03630B8EEA76B1D5B7105B70DD4F	4DE5E593E	C:\Windows\syst	em32\KERNEL32.DLL		PROCES:	_ANALYSIS	962D2A61	×

Notes:

Artifact data will not be lost if the connection is transferred to different machines or in case the current machine loses connection, the user reloads the page or navigates to another page, the system asks for confirmation as follows:

Reload site?		
Changes you made may not be saved.		
	Reload	Cancel

6.1.2. Investigation Event Search

6.1.2.1. Event Search

This function is similar to the IR Flow's Event Search.

• Step 1: Enter the query \rightarrow Select a time range \rightarrow Click Search.



VEDR Portal	- Event Search	× +												-
$\in \rightarrow G$	🙃 🔺 Not secur	re 10.30.161.37/#	/investigation/eve	nt-search									2 Cr	👽 🤌 l 🖰 🕹 😫
VED	OR Portal			,	llerts	IR Flow	Investigation	Respo	nse	Setting			③ EN ▼	None 😐 👻
Event Sear	rch													🗭 Guide line
					Q EV	ent Search							🗍 Marked Artifact	
Search Log	AgentiD = "5E4A	60F26D38D9647A7D6	56AE532B4DD8A0D5	1323"	1								1 Last	7 days
4 results	11/04/2019 09:36:13	18/04/2019 09:36:13												Hide graph 🛠
20,000 7														
15,000 -														
10.000 -														
										_				
5,000 -														
0	09:36 11/04/19 - 18:59 11/04/19	19:00 11/04/19 - 06:59 12/04/19	07:00 12/04/19 18:59 12/04/19	19:00 12/04/19 - 06:59 13/04/19	07:00 13/04/19 18:59 13/04/19	19:00 13/04/19 - 06:59 14/04/19	07:00 14/04/19 - 18:59 14/04/19	19:00 14/04/19 - 06:59 15/04/19	07:00 15/04/19 - 18:59 15/04/19	19:00 15/04/19 - 06:59 16/04/19	07:00 16/04/19 - 18:59 16/04/19	19:00 16/04/19 - 06:59 17/04/19	07:00 17/04/19 - 18:59 17/04/19	19:00 17/04/19 - 09:36 18/04/19
POPULAR			= Vie	v column 🗸 🗸										_
AgentID			AGENTID							EVENTIO	COM	PUTER	LOGTYPE	
Channel			5E4A60F2	6D38D9647A7D66AE5328	34DD8A0D61323					3	hair	ov-PC	EventLog	
Computer			5E4A60F2	6D38D9647A7D66AE5328	34DD8A0D61323					4689	haij	ov-PC	EventLog	
EventID			5E4A60F2	6D38D9647A7D66AE5328	54DD8A0D61323					4689	haij	ov-PC	EventLog	
EventRecord	diD		5E4A60F2	6D38D9647A7D66AE5328	54DD8A0D61323					4689	haij	IV-PC	EventLog	
LogType			Display 4	4 result(s)										
onur ne														
Guid														
Keywords														
Name														
Opcode														
C Ask	me anything		4 O	🗮 🛍 📂	🤹 🔮 (ø 🧧 🕅	I S C	n 🔁 🧰 🖤	5 💋 🖉	🔤 👲 🎍			^ T	4() ENG 4/18/2019

• Step 2: Add search fields to the query with Popular and Others fields.





6.1.2.2. Chart

Viettel Mail System: Inbox x VEOR Portal - Event ← → C	: Search × +								Ø ģ	- a × 8 0 0 ± 8
VEDR Portal	Alerts	IR Flow	Investigation	Res	ponse	Setting			⊙ en +	None 🕒 🔹
Event Search										📮 Guide line
		Q Event Search							Marked Artifact	
Search Log Search Log									Last 7	'days Q
51819 results 12/04/2019 08:40:28 - 19/04/2019 08:40:28										Hide graph 余
20,000]										
15,000 -										
10,000 -										
5 000 -										
5,600 -									-	
0 - 08:40 12/04/19 - 19:00 12/04/19 - 07:01 18:59 12/04/19 06:59 13/04/19 18:5	0 13/04/19 - 19:00 13/04/19 - 07:00 14 59 13/04/19 06:59 14/04/19 18:59 1	/04/19 - 19:00 14/04/19 - 4/04/19 06:59 15/04/19	07:00 15/04/19 - 18:59 15/04/19	19:00 15/04/19 06:59 16/04/19	07:00 16/04/19 - 18:59 16/04/19	19:00 16/04/19 - 06:59 17/04/19	07:00 17/04/19 - 18:59 17/04/19	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
POPULAR	View column									
AgentID	AGENTID			EVENTID	COMPUTER	LOGTYPE	CHANNEL			1
Channel	931ECF82E655629579A6AB6D001183B559DC0	0408		4689	win7x64-PC	EventLog	Security			
Computer	931ECF82E655629579A6AB6D001183B559DC0	0408		4689	win7x64-PC	EventLog	Security			
EventID	931ECF82E655629579A6AB6D001183B559DC0	9405		1	win7x64-PC	EventLog	Microsoft-Windo	ws-Sysmon/Operation	al	
EventRecordID	931ECF82E655629579A6AB6D001183B559DCI	9408		4689	win7x64-PC	EventLog	Security			
Level	931ECF82E655629579A6AB6D001183B559DC	0408		4688	win7x64-PC	EventLog	Security			
LogType	931ECF82E655629579A6AB6D001183B559DC	0408		4688	win7x64-PC	EventLog	Security			
CommandLine	931ECF82E655629579A6AB6D001183B559DC0	9408		4688	win7x64-PC	EventLog	Security			
Image	931ECF82E655629579A6AB6D001183B559DC	9408		1	win7x64-PC	EventLog	Microsoft-Windo	ws-Sysmon/Operation	al	
OTHERS	931ECF82E655629579A6AB6D001183B559DC0	9408		4688	win7x64-PC	EventLog	Security			
Guid	931ECF82E655629579A6AB6D001183B559DC0	9408		4689	win7x64-PC	EventLog	Security			
Keywords	931ECF82E655629579A6AB6D001183B559DC	2408		4688	win7x64-PC	EventLog	Security			
Ask me anything	0 🛢 🛱 🖻 🍕 📢) 🖉 🚺 💱	×I S C	¶ 1	1 🖉 🖉	🔤 🙆 🎦	2		~ E	¢i) ENG 8-40 AM €

- Step 1: Perform a search same with the Event Search. •
- Step 2: The chart displays statistics according to the search time range. The way to ٠ divide the time range corresponding to the columns on the chart is as follows:
 - Statistics for >= 90 days: Divide into 30 statistical intervals. 0
 - Statistics of events in the last 60 days: Divide into 20 intervals, 3 days/each 0 interval.
 - Statistics for 30 days: Divide into 15 intervals, 2 days/each interval. 0
 - Statistics for 7 days: Divide into 14 intervals, 12 hours/ each interval. 0
 - Statistics for 1 day: Divide into 24 intervals, 1 hour/ each interval. 0
 - Statistics for 12 hours: Divide into 12 intervals, 1 hour/ each interval. 0
 - Statistics for 6 hours: Divide into 12 intervals, 30 minutes/ each interval.
 - Statistics for 1 hour: Divide into 12 intervals, 5 minutes/ each interval.
 - Statistics for 30 minutes: Divide into 15 intervals, 2 minutes/ each interval. 0
 - Statistics for under 30 minutes: Divide into 1-minute intervals. 0

When hovering over each column, the time range and the number of records searched during that period will be will displayed.



Notes: The timelines on the chart are the timelines calculated in round days/hours/minutes to suit the long or short statistical period.

- 6.1.2.3. Event Handle
- View event details: Double click on a record or hover over a record and click the View details icon.



• Marking artifact: Hover over a record and select Marking artifact.



• Select path and click Accept.

VEDR Portal - Event Search × +											
- → C 🛱 🔺 Not secure 10.30.161.37	7/#/investigation/event-search									<mark>0</mark> රු	€ २ Ө ±
				Investigation							None 🕒 -
Event Search											📮 Guide li
		QD	vent Search							Marked Artifact	
Search Log Search Log										Last	7 days
51819 results 12/04/2019 08:40:28 - 19/04/2019 0	08:40:28										Hide graph 🛠
20,000]											
15,000 -											
10,000											
5,000 -											
5,000 -											
5,000 - 0 - 08140 12/04/19 - 19:00 12/04/19 18:59 12/04/19 - 06:59 13/04/19	- 07:00 13/04/19 - 19:00 13/04/ 9 18:59 13/04/19 06:59 14/04	19 - 07:00 14/04/19 /19 18:59 14/04/19	- 19:00 14/04/19 - 06:59 15/04/19	07:00 15/04/19 - 18:59 15/04/19	19:00 15/04/ 06:59 16/04	9 · 07:00 16/04/19 19 18:59 16/04/19	· 19:00 16/04/19 - 06:59 17/04/19	07:00 17/04/19 - 18:59 17/04/19	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
5,000 0 0 08:40 12/04/19 - 18:59 12/04/19 06:59 13/04/19	- 07:00 13/04/19 - 19:00 13/04/ 9 18:59 13/04/19 06:59 14/04 = Wiew column	19 - 07:00 14/04/19 /19 18:59 14/04/19	- 19:00 14/04/19 - 9 06:59 15/04/19	07:00 15/04/19 - 18:59 15/04/19	19:00 15/04/ 06:59 16/04	9 · 07:00 16/04/19 19 18:59 16/04/19	- 19:00 16/04/19 - 06:59 17/04/19	07:00 17/04/19 - 18:59 17/04/19	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
5,000 08440 12/04/19 - 19:00 12/04/19 0855 12/04/19 2000UAR AgenttD	- 07:00 13/04/19 - 19:00 13/04/ 18:59 13/04/19 - 06:59 14/04	19 - 07:00 14/04/19 /19 18:59 14/04/19	- 19:00 14/04/19 - 9 06:59 15/04/19	07:00 15/04/19 - 18:59 15/04/19	19:00 15/04/ 06:59 16/04	9 - 07:00 16/04/19 19 18:59 16/04/19	- 19:00 16/04/19 - 06:59 17/04/19	07:00 17/04/19 - 18:59 17/04/19	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
5,000 08440 12/04/19 - 19:00 12/04/19 06:59 12/04/19 PORVLAR AgentID Channel	- 07:00 13/04/19 - 19:00 13/04/ 2 13:59 13/04/19 - 06:59 14/04	19 - 07:00 14/04/19 19 18:59 14/04/19 *	- 19:00 14/04/19 - 9 06:59 15/04/19	07:00 15/04/19 - 18:59 15/04/19	19:00 15/04/ 06:59 16/04	9 - 07:00 16/04/19 19 18:59 16/04/19 COMPUTER	- 19:00 16/04/19 - 06:59 17/04/19 LOGTYPE	07:00 17/04/19 - 18:59 17/04/19 CHANNEL	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
15,000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	- 07:00 13:04/19 - 19:00 13:04/ 18:99 13:04/19 00.59 14:04 Wew column Activitio 9110CF82655628578A6ABB	19 - 07:00 14/04/19 18:59 14/04/19 V	- 19:00 14/04/19 - 9 06:59 15/04/19	07:00 13/04/19 - 18:59 15/04/19	19:00 15/04/ 06:59 16/04/ EVENTID 4689	9 - 07:00 16/04/19 18:59 16/04/19 COMPUTER Win7x84-PC	19:00 16/04/19 - 06:59 17/04/19 LOGTYPE LOGTYPE EventLog	07:00 17/04/19 18:59 17/04/19 CHAVINEL Security	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
15,000 0 0 0 0 0 0 0 0 0 0 0 0	- 07:00 13:04/19- 19:00 13:04/ 18:59 13:04/19 06:59 14/04 Wew column ACENTO 931ECF82E555628578AA688 931ECF82E555628578AA688	19 - 07:00 14/04/19 18:59 14/04/19 v D00118385590CD408 D00118385590CD408	- 19:00 14/04/19 - 9 06:59 15/04/19	07:60 13/04/19 - 18:59 15/04/19	19:00 15/04/ 06:59 16/04/ EVENTID 4689 Marking artifa	9 - 07:00 16/04/19 18:59 16/04/19 18:59 16/04/19 COMPUTER Win7x64-PC tt(s)	 19:00 16/04/19 - 05:59 17/04/19 LOGTYPE EventLog 	07:00 17/04/19 - 18:59 17/04/19 CHAMREL Security	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
15,000 0 0 0 0 0 0 0 0 0 0 0 0	27:00 13/04/19 19:00 13/04/19 19:00 13/04/19 06:59 14/04 E Wew column Aconto 031ECF821655629578A6A86 931ECF821655629578A6A86 931ECF8216555629578A6A86 931ECF8216555629578A6A86 931ECF8216555629578A6A86 931ECF8216555629578A6A86 931ECF8216555629578A6A86 931ECF8216555695784686 931ECF8216555695784686 931ECF821655569578486 931ECF8216555695784686 931ECF8216555695784686 931ECF82165555695784686 931ECF8216555569 931ECF821655569 931ECF821655569 931ECF821655569 931ECF821655569 931ECF821655569 931ECF821655569 931ECF821655569 931ECF821655569 931ECF821655569 931ECF82165556 931ECF82165556 931ECF8216555 931ECF8216555 931ECF821655 931ECF821655 931ECF821655 931ECF82165 931ECF82165 931ECF8216 931ECF8 931ECF8 931ECF8 931ECF8 931ECF8	19- 07:00 14/04/19 19 18:59 14/04/19 00011838559DCD408 D0011838559DCD408 D0011838559DCD408	- 19:00 14/04/19- 06:59 15/04/19	07:00.13/04/19 18:59.15/04/19	19:00 15/04/ 06:59 16/04/ EVENTIO 4689 Marking artifa	9 - 07/00 16/04/19 18 - 18:59 16/04/19 COMPUTER WIN7X64-PC t(9)	19:00 14/04/19 - 06:59 17/04/19 LOGTYPE EventLog	07:00 17/04/19 - 18:59 17/04/19 CHAMEL Security	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
1,5,00 0,5,00 1,5,00		19 - 07:00 14/04/19 18:55 14/04/15 000118385590CD408 000118385590CD408 000118385590CD408 000118385590CD408	- 19-00 14/04/19- 06:59 13/04/19	07:00 13/04/19 18:59 13/04/19	19:00 15/04/ 06:59 16/04/ EVENTID 4689 Marking artifa XTH 2 C:\Windows\	 97.00 16/04/19 18:59 16/04/19 сонелитея win7x64-РС x(s) 	 19:00 16/04/19 - 06:59 17/04/19 LOGTIPE LOGTIPE EventLog 	07-00 17/04/19- 18:59 17/04/19 CHAMEL Security	19:00 17/04/19 06:59 18/04/19	07:00 18/04/19 18:59 18/04/19	19-00 18/04/19 - 06-40 19/04/19
15,000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	87:00 13/04/19- 19:00 13/04/ 06:59 13/04/19 19:00 13/04/ 06:59 14:04 E Wew column Addrtt0 0310CF82055523578AAABB 9310CF82055523578AAABB 9310CF82055523578AAABB 9310CF82055523578AAABB 9310CF8205578AABB 9310CF82055523578AABB 9310CF8205578AABB	19- 07:00 14/04/19 18:59 14/04/13 000118185590CD408 000118385590CD408 000118385590CD408 000118385590CD408	- 19:00 14/04/19 9 06:59 15/04/19	07:00-18/04/19 - 38:59 15/04/19	19:00 15/04/ 06:59 16/04/ EVENTID 4689 Aarking artifa ATH 2 C:\Windows\	9 - 07;00 16/04/19 18:59 16:04/19 COMPUTER Win7x64-PC t(s) bystem32\ROUTE.EXE c	- 19:00 14/04/19 - 06:59 17/04/19 LOCTIFE EventLog	07-00 17/04/19- 18:59 17/04/19 CHAMEL Security	19:00 17/04/19 06:59 18/04/19	07:00 18/04/19 18:59 18/04/19	19:00 18/04/19 - 08:40 19/04/19
15,000 0 0 0 0 0 0 0 0 0 0 0 0		19- 07:00 14/04/19 18-59 14/04/11 000118885590CD408 000118885590CD408 000118885590CD408 000118885590CD408 000118885590CD408	- 19:00 14/04/19 9 06:59 15:04/19	07:00 13/04/19 - 18:59 15/04/19	19:00 15/04/ 06:59 16/04/ EVENTIO 4689 Aarking artifa ATH 2 C:\Windows\	9 - 07,00 16/04/19 18:59 16/04/19 comPUTER win7x64-PC t(s) bystem32\ROUTE EXE _ c	 19:00 14/04/19 - 06:59 17/04/19 LOGTYPE EventLog 	07:00 17/04/19- 18:59 17/04/19 CHM/REL Security	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18:59 18/04/19	19-00 16/04/19
15,000 13,000 15,155 12/04/19 15,155 12/04/19 PORMUR AgentiD Channel Computer EventB EventB EventB EventB CommandLine Image	- 07:00 13(04/19- 18:59 13(04/19- 18:59 13(04/19) ■ Vew column ACD/110 031CCF82E5552057bAAAB 931CCF82E5552057bAAAB 931CCF82E5552057bAAAB 931CCF82E5552057bAABB 931CCF82E5552057bAABB 931CCF82E5552057bAABB 931CCF82E5552057bAABB	19 - 07:00 14/04/19 18:59 14/04/19 000118385590CD408 000118385590CD408 000118385590CD408 000118385590CD408 000118385590CD408 000118355590CD408 000118355590CD408	- 19:00 14/04/19 06:59 15:04/19	07:00 13/04/19 - 38:59 35/04/19	19:00 15/04/ 06:59 16/04/ EVENTID 4689 Marking artifa ATH 2 C:\Windows\	9. 07,00 16/04/19 18:59 16:04/19 COMPUTER Win7x64-PC t(s) Jystem32\ROUTE.EXE c	 19:00 16/04/19- 66:59 17/04/19 LOCTYPE EventLog 	07:00 17/04/19- 18:59 17/04/19 CHANNEL Security	19:00 17/04/19 - 06:59 18/04/19	07:00 18/04/19 - 18/59 18/04/19	19-00 16/04/19- 06-40 15/04/19-
1,000 0,440 12/04/3 - 19:00 12:04/3 16:59 12/04/3 - 19:00 12:04/3 10:004/4 Agentia Computer Eventio Computer Eventio CommandLine CommandLine CommandLine CommandLine CommandLine CommandLine		19 - 07:00 14/04/19 18:59 14/04/13 000118385590CD408 000118385590CD408 000118385590CD408 000118385590CD408 000118385590CD408 000118385590CD408 000118385590CD408	- 19:00 14/04/19 9 06:59 15:04/19	07:00 13/04/19 - 38:59 15/04/19	18:00 15/04/ 06:59 16/04/ EVENTID 4689 Aarking artifa ATH 2 C:\Windows\	9. 07,0016/04/19 18:3916/04/19 COMPUTER WM7268-PC π(s) System:32\ROUTE.EXE δ	• 15:00 1694/15 06:59 17/04/15 LOGTINE EventLog	07:00 17/04/19 - 18:59 17/04/19 CHANREL Security	19:00 17/04/19 06:59 18/04/19	07:00 18/04/19 - 15:59 18/04/19	19/00/18/00/19 19/00/18/00/19
1,5,00 0,146 13/54/19 15:59 12/64/19 10:00.4/1 Agent/D Computer EventO	87:00 13:04/19* 19:00 13:04/ 18:59 13:04/19 06:59 14:04 E View column Addrifto 011CFR2:6554205 70AAAB 011CFR2:6554205 70AAAB 011CFR2:6554205 70AAAB 011CFR2:6554205 70AAAB 011CFR2:6554205 70AAAB 011CFR2:6554205 70AABB 011CFR2:6554205 70AABB 011CFR2:6554205 70AABB 011CFR2:6554205 70AABB 011CFR2:6554205 70AABB 011CFR2:6554205 70AABB 011CFR2:6554205 70ABB 011CFR2:6554205 70AABB 011CFR2:6554205 70ABB 011CFR2:6554205 70ABBB 011CFR2:6554205 70ABB 011CFR2:6554205 70ABBB 011CFR2:6554205 70ABBB 011CFR2:6554205 70ABBB	97.00 14/04/19 18:59 14/04/19 18:59 14/04/19 00118885590C0408 000118885590C0408 000118885590C0408 000118885590C0408 000118885590C0408 000118885590C0408 000118885590C0408 000118885590C0408	- 19:00 14/04/19 06:59 15/04/19	07:00 13/04/19 38:59 13/04/19	18:00 15/04/ 06:59 16/04/ EVENTID 4689 Marking artifa ATH 2 C:\Windows\	** 07,003,46,4419 ***********************************	* 19:00 36:04/19: 06:59 37:04:19 LOOTIFE EventLog	CHANNEL CHANNEL	19:00 17:04/19 06:59 18:04:19	07100 18/04/19 -	140.003 800043 -
5,000 014:05 12/04/19 18:59 12/04/19 Pomul/A Agent/A Agent/A Computer EventD EventD EventD EventD EventD CommandLine Image Crimess Could Keypords	■ 107:00 13/04/19 19:00 13/04/ 06:59 14:04 ■ 107:00 13/04/19 19:00 13/04/ 06:59 14:04 ■ Wew column 4:00:10 ■ 011CFR265592297304ABB 931CFR265592397304ABB 931CFR265592397304ABB 931CFR265592397304ABB 931CFR265592397304ABB 931CFR265592397304ABB 931CFR265592397304ABB 931CFR265592397304ABB 931CFR265592397304ABB 931CFR26559237304ABB 931CFR26559237304ABB 931CFR26559237304ABB 931CFR26559237304ABB 931CFR26559237304ABB	19 - 07:00 14/04/19 18:59 14/04/19 000118385590C0408 000118385590C0408 000118385590C0408 000118385590C0408 000118385590C0408 000118385590C0408 000118385590C0408	- 19:00 14/04/19 - 06:59 13/04/19	07:00 18/04/19 - 38:59 18/04/19	19:00 15/04/ 06:59 16/04 EVENTID 4689 4689 4689 2 CtWindows C CtWindows	 сото за/дания сончочтвя сончочтвя міплов4-РС ttp: 	 19:00 16:04/19- 06:59 17:04/19 LOGTIPE EventLog 	07:00 17:04/15- 18:05 17:04/15 CHARMEL Security	10.00 17.0415	0700 1300-130	1 00 1 2004 1 1



Page | 92





• Select IR Flow and add that artifact to IR Flow.

			Investigation	ivesi/011se	Setting			
VEDR Portal		1 10 10			Setting		G" EN ₹	None
Search								
		Q, Event	Search			4	Marked A	rtifact
t(s)								
TIME	AGENTID	OBJECT			FROM	REFERENCE		
10/04/2019 06:00:31	931ECF82265542357544AB6000118385500CD4	08 C:WindowsiSystem	N37,ROUTE.EXE		WHI_EVENT_LOG	MotM26884gbpD Search uster2 tester2 hu a id 1122 thi 8b thi 8b th	mby in dropdown list 1 8 8 8 9 8 8 9 8 8 9 8 8 8 8 8 8 8 8 8	م م
Ask me anything	र ा 🛤 🛱	<u>in 8</u> 8 10	o 🕅 🕅 🗧 e	만 💿 🔨 💋	* 🖻 😆 🛓	W U	,	^ 및 Φ) ENG <u>9:</u> 10 4/19/
Ask me anything I Portal - IR Pow Detail C A Not second VEDR Portal al detection	X VEDR Portal - Process Analysis X 😨 4	nvestigation - Viettal Endpoint (- X 1995d30aas524844.184a7e13897tz Alerts	VIDR - Your Company JIRA X 🛠	만 한 한 Ø	X R (MDR-60) Process Analyse	■ ■ ■	() 슈 () 년 N +	へ 知 中 ENG 約0 4/19/ - - - - - - - - - - -
Ask me anything Portal - IR Now Desail C Anot seen VEDR Portal Idetection	X VEDR Portal - Process Analysis X 20 H	x Kettel Endpoint (X) Nestigation - Viettel Endpoint (X) 2955330as5224944184a7e13897tr Alerts	YUDR - Your Company JRA X	PF DE-31] Artifact Marking - You Response	 Model Process Analyst Setting 	2 3 - You X +	() () ปี () ค. +	ヘ 卯 Φ ENG 4/19/ - - - - - - - - - - - - - - - - - - -
Ask me anything Portal - IR flow Detail C A to t seen VEDR Portal at detection nt ssr0r0P.EGANURD	X VEDR Portal - Process Analysis X 20 L	x C C C C C C C C C C C C C C C C C C C	Image: Second	Le Contract Marking - You Response	 Model Process Analyst Setting 	∎ ₽ s-¥e x +	⊘☆ ⓒ EN +	ヘ 卾 む ENG 4/19/
Ast me anything LPortal - IR Plow Detail C C C C C C C C C C C C C C C C C C C	X VLDR Portel - Process Analysis X X 1	Nestigation - Viettel Endpoint (* 14) 1795d30aa522494d184a7e13897tr Alerts	Image: Second	Le Contract Marking - You Response	X R MDR-60 Process Analys Setting	₩ 1-%:: X +	⊘ ≙ ि स•	へ 切 ゆ: ENG 910 4/19/ - - - - - - - - - - - - - - - - - - -
Ask me anything Portal - IR Pow Detail Portal - IR Pow Detail Portal at detection nt t t t t t t t t t t t t t t t t t	X VLDR Portel - Process Analysis X X 10 A	Vette Englore : X 1795d30aa52494d184a7e13897t Alerts	VEDR-Your Company JRA X X VEDR-Your Company JRA X X NabeO IRR How Investigation	Le Contract Marking - You (VEDR-31] Artifact Marking - You Response	Control of the second sec	■ ■ •-*e. × +	⊘☆ ③ BN •	へ 切 ゆ: DNG 910 4/19/ - - - - - - - - - - - - - - - - - - -
Ask me anything Portal - Ift Flow Detail Portal - Ift Flow Detail Portal Portal Not see VEDR Portal It detection nt t t Tass: Detail 2006/2008	X VEDR Portal - Process Analysis X 2 4 10.30.161.37/#/r-flow/in-flow-detail/27ac440	Alerts	Image: Second	VEDE-313 Antifact Marking - Yes: Response	COLLING SECLING ENTER LEASE SECLING ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE ENTER LEASE	■ ■ s-% ₀ x +	⊘☆ ③ EN + SUGRIT	- 〒 0 Bic 419/
Ask me anything Portal - IR Row Detail Portal - IR Row Detail Portal - IR Row Detail Portal I detection It t t t t t t t t t t t t t t t t t t	X VEDR Partal - Process Analysis X X 1	Alerts	VEDR - Your Company JRA X X VEDR - Your Company JRA X X Reflow Investigation HOSTIGATE DESKTOP-EGANUBQ	UPEDE-31] Antifact Marking - Yeu Response	CODARD C	■ ■ u-%0. × +	⊘ ф ⊙ ви • Блаят нар	∧ ເຼີ ψ mic ∳n ເບີ ເວ ເຊ chuyennt2
Ask me anything Portal - IR Row Detail Portal - IR Row Detail Portal Por	X VEDR Partal - Process Analysis X X 1	Alerts Bour unknown	Image: Second	UPEDE-313 Antifact Marking - Yes: Response	K K	■ ■ u-%0. × +	⊘́ф ⊙ ви• Боват Нер	∧ ເຼີ ψ ms ຢາຊີ - ເບັດ chuyann2 ເ
Ask me anything Portal - IR Flow Detail Portal - IR Flow Detail Portal P	X VEDR Partal - Process Analysis X X 1	Alerts soup	Image: Second	VEDE-31) Artitect Marking - Yes: Response	CDUARO CONTRACTOR CONTRACTOR	■ ■ s-%c. x +	⊘ д ⊙ ви • Бобят Нур	∧ ເ]ູ (+ nic ∳n) - ເບັດ & & € chuyennt2
Ask me anything Porsal - IR Pow Detail C Porsal - IR Pow Detail C Porsal - IR Pow Detail C Porsal Net section nt t t t t c c c c c c c c c c c c c c	X VLDR Partal - Process Analysis X 2 A	verter Endpoint : x verter Endpoint : x Alerts secon unknown	Image: Second	IVEDR-31) Artifact Marking - Ye: Response	COUMO Instal Access	► ■	⊘ ☆ ♂ EN + SDERIT (TEE)	∧ (ີ) ψ mic ຟາມ – ເບິ່ງ ອີເຊີ € chuyennt2
Ask me anything Portal - III. Flow Detail Portal - III. Flow Detail Portal - III. Flow Detail Portal	X VEDR Partal - Process Analyss X X III X VEDR Partal - Process Analyss X III UR 10.30.161.37/#/u- Row/in-Row-detail/27.ac440	verteglation - Verted Endpoint (; x) verteglation - Verted Endpoint (; x) Alerts escoure unknown	Image: Second	DP 💿 🧐 🥬		▶ ♥ ♥ h • %0: × +	⊘ ☆ ⊘ EN + SOBBIT Hem	N (C) (+) ING (400) - P (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)
Ack me anything Partal - IR Rew Detail Partal - IR Rew Detail Partal - IR Rew Detail Partal P	x VLDR Partsi - Process Analysis X x VLDR Partsi - Process Analysis X tre 10.30.1613.7/#/r=flow/in-flow-detail/27.ac440	verteglation - Verted Endpoint (* x) verteglation - Ve	Image: Second	PEDE-31) Artifect Marking - Yec Response		► ►	⊘ ≙ ⊘ en • stertt reen	∧ ∏ ψ nic 400 4000 ♥ Ø Ø Ø € chuyennt2 €
Asic me anything Portal - II, Pow Detail Portal - II, Pow Detail Portal - II, Pow Detail Portal Portal	VEDR Partsi - Process Analysis X VEDR Partsi - Process Analysis X VEDR Partsi - Process Analysis X VER 10.30.161.37/#/r- flow/in-flow-detail/27ac440 mhandts-PC X Win7-CongNCS X scours unkno	nextiguition - Vietral Endpoint (* x) 7755430as522494410437e13097br Alcrts	HOSTNAKE hostnake hostnake hostnake	PEDE-ST) Antiset Making - Yeu Response		№	⊘ ≙ ⊘ en ↓ soent	N ♥ I I I I I I I I I I I I I I I I I I
Ack me anything Persial - III. Plow Detail Persial - III. Plow Detail Persial - III. Plow Detail Persial detection Int EsstTOP-ECANUBQ Int EsstTOP-HENRI2B1Q Int EsstTOP-HENRI2B1Q Int EsstTOP-HENRI2B1Q Int Int EsstTOP-HENRI2B1Q Int Int EsstTOP-HENRI2B1Q Int			Note: Section of the section of th	PEDIC-31) Areface Masking - You Response			© ☆ ⊙ EN ↓ SOBRITY RED	 N □ ↓ n6 ⁴³/₄₁₆ - • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • <lp>• </lp> <lp>• </lp> <
Ask me anything Postal - III. Plow Detail Postal - III. Plow Detail Postal Postal Postal Postal Post			Image: Section 2000 and 20000 and 2000 and	PEDR-31) Areface Masking - You Response			⊘ д 3 рн • seenr	
Ask me anything Pertal - IR Pow Detail C □ □ □ □ ▲ Not sec VEDR Portal Al detection nt tsskröp#GANUBQ t tsskröp#GANUBQ t tsskröp#GANUBQ t tsskröp#GANUBQ t tsskröp#GANUBQ t tsskröp#Henu281Q			Image: Second	DEDE-313 Antilect Marking - You Response		severy (1995) (1995) (1995) (1995) (1995)	⊘ ∰ 3 EN • MIERIT ENERT	
Adc me anything Portal - III Pow Detail Portal - IIII Pow Detail Portal - III Pow Detail Portal - III Pow Detail Por			NOSTNAME HOSTNAME	VEDR-31) Artifact Marking - You Response			© ☆ © EN • EDERIT ENERT	 <!--</td-->
Adc me anything Persia - IR Pow Detail Int Escrop Ecanuage rt rt rt Inte Inte Inte Inte Inte Inte Inte	VEDR Partsi - Process Analysis X VEDR Partsi - Process Analy			PEDR-31) Artifact Marking - Yes Response		EVIENT E	© ☆ © EN + SCRET7 ••••••••••••••••••••••••••••••••••••	N ♥ ↓ nG
Ack me anything Ack me anything C				PEDE-311 Artifact Marking - Yeu Response		EUUEIT7	⊘ ☆ © ☆ © N → SUBRITY EFFEELCE EFFEELCE EFFEELCE PCL35068888597978200 PCL3506888597978200 PCL35068885597978200	N ♥ ↓ nG
Asc. me anything C 0 al centre anything C 0 al centre anything C 0 al cetection Int ESKTOP-EGANUBQ rt IDUI:03722/05/2019 IDUI:03722/05/2019 Idui:050122/05/2019 Idui:050022/05/2019 Idui:05002/05/2019 Idui:05002/05002/05/2019 Idui:05002/05002/05002/05002/05000	VEDR Partial - Process Analysis VEDR Partial - Process An		Image: Section Company MRA Image: Section Company MRA <td< td=""><td>PEDIC-31) Areface Massing - Yeu Response</td><td>COUNTO COUNTO COUNTO</td><td>EXTERT EXTERT</td><td>С № 1 К № 1 К № 1</td><td>\(\begin{aligned} \begin{aligned} \begin{aligned} & \mathcal{P} & \mathcal & \mathcal{P} & \mathcal{P} & \mathcal{P} & \mathcal{P} & \m</td></td<>	PEDIC-31) Areface Massing - Yeu Response	COUNTO COUNTO	EXTERT EXTERT	С № 1 К № 1 К № 1	\(\begin{aligned} \begin{aligned} \begin{aligned} & \mathcal{P} & \mathcal & \mathcal{P} & \mathcal{P} & \mathcal{P} & \mathcal{P} & \m
Asic me anything Cevial - IR Flow Detail al detection Int Eskrop-schwidzelog rt rt rt rt rt rt rt rt rt r	VEDR Partsi - Process Analysis VEDR Partsi			DEDE-313 Antifact Marking - You Response	CENARD C	EXTERT EXTERT	② 合 ③ 合 ③ 日 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	へ ① 4 m6 400
Act. m.e. anything Rousi - IR Pow Detail	VDR Partal - Process Analysis V				COUNDO COUNDO COUNDO COUNDO CO		⊘ ☆ ⊘ ☆ EN - ENERTY	

- Similar to the Process Analysis function, there are also some notes as follows:
 - If switching tabs between Event Search and Marked artifact, the data in Marked artifact screen will not be lost.
 - If switching to the big tabs, such as Alert, IR Flow, Response and Setting, the data in Marked artifact screen will be lost.



6.1.3. Investigation Deploy Tools

6.1.3.1. Tool Management

Purpose: Manage all tools of the system. Users can add/delete tools on this screen. Features on this screen include as follows:

- Display tool list with detailed information of the tool, including: Name, Parameter, Version, Architecture, Upload User, Platform and Hash code.
- Search tool: Search by many criteria, such as All (all data fields), Name (tool name), Tool ID, Version, SHA1, Upload User and Platform.
- Upload tool: Upload tool running on Windows and Linux agents with a maximum capacity of 10MB.

For the Upload tool feature, perform the following steps:

• Click Upload tool → Select the path to the tool to upload or drag and drop the tool into the interface → Enter information in the Tool info popup → Click Upload tool.

🚺 AJIANT				Setting	
oy Tools					📮 Guide
	Tools Management		C ² Deploy tool		💭 Result
ols 56 result(s)		Q Type and enter to search tool	All 🗸	X Upload Tool	
Listdlis Parameter: accepteula	C/F Parameter: Scoopt EXT Ver: 13.82.0.0 0.M8 Arbitecture: N I	eula-a *	ListService Parameter : Ver : 1.0.0 0 MB Architecture (M / h	ф	Drop file to attach or browse 2
C/ Test_Tool_1.exe Parameter:	Tool info Name	linux_sleep_30s.sh		C:/ Linux_sleep_3	.0s.sh
Ver: 1.0 2 MB Architecture : N/A 2019/11/13 14:33:29 by : root	Parameter Platform	Input parameter			
rest_tool_Linux_1 Parameter:1 Ver:1.0 2MB Architecture:N/A 2019/11/13 14:35:51 by:root	Type Architecture Version	exe msi bat ps1 elf x86 x64 ON/A	baah 3		
Test, Tool3 Parameter : 1 Ver: 1.0 Ver: 1.0 2MB Architecture : N/A 2019/11/14 17:34:30 by : root	2M8 Ver:1.0.0 Architecture:N/A 2019/11/14 17:40:29	Cancel L	2MB Ver: 1.0 Architecture : N/A 2019/11/15 14:57:41 by : root		
C/h Test, Tool. 2, 32bit.exe Brameter: 0 2140 Ver: 1.0 Architecture: N/A 2019/11/15 14:57:54 by : root	C/P Test_Tool_3_22bit. Parameter: Parameter: 2M6 Ver: 1.0 2M6 Architecture: N/A Q19/11/15 14:58:15 2019/11/15 14:58:15	exe : by : root	hello_word.bat Parameter : 2538 Archtecture : N/A C1 2019/11/18 09:46:09 by : root		
C:/ Test_Tool_4.exe	C/b Test_Tool_32bit_40	is_2.exe	C:/ Parameter :		

For the Delete tool feature, hover the mouse over the tool to delete \rightarrow Select Delete.



🔷 VEDR board - Agile Boi 🗙 🔷 Te	st Management for J 🗙 📔 💠 Test Management	t for JI 🗙 📔 💠 Test Management fo	e J 🗙 🔃 AJIANT - Deploy Tools 🗙	AJIANT - IR Flow Detail	🗙 📔 🗮 Test Design - aliant	t - 🗸 🗙 💽 [Release][BBX	NTK] VCS 🗙 📔 🛓 Downloads	$\times + - \sigma \times$
\leftarrow \rightarrow C \bigcirc A Not secure	10.30.161.37/#/settings/group/it_departme	ent					00	습 🔊 🙆 । 🗢 😁 👱 😂
📶 ΔΙΙΔΝΤ		Alerts IR Flow	Investigation	Response	Protect & Prevention	Setting	© (N - root 💶 -
Deploy Tools								📮 Guide line
	🕄 Tools Manage	ement			🖸 Deploy tool			Result
Tools 57 result(s)			Q Type and enter to search to	IIA Io	~	X Upload Tool	Upload Tool	×
C/ BX3 Ver: 3.20.0.0 0 MB Architecture: N/A 2018/12/28 15:13:5	euta -v	autorunsc Parameter: -accepte Ver: 13.82.0.0 0 M8 Architecture: N/A 1 2018/12/28 15:14:53	ula -a * by : root	ListSer Parame Ver : 1.4 O MB Archite 2019/0	vice eter : .0 cture : N/A 9/19 14:36:53 by : root		C Drop file to	attach or browse
C/P Test_Tool_1.exe Parameter : 1 2M8 Architecture : N/A 2019/11/13 14:39:2	by:root	Test_Tool_2.exe Parameter: Ver: 1.0 2MB Architecture: N/A 10 2019/11/13 14:34:07	by : root	C:/ Test_T Parame 2 M8 Archite 1 2019/1	bol_3.exe eter : 111 0 cture : N/A 1/13 14:34:26 by : root		iinux_sleep_30s.sh 2020/03/25 15:58:41 by rc 19 8	ot
Test_Tool_Linux_1 Parameter : 1 Ver : 1.0 2 MB Architecture : N/A 2019/11/13 14:35:5	by : root	Test_Tool_Linux_2 Parameter: Ver:1.0 2MB Architecture: N/A 2019/11/13 14:36:05	by : root	Bash_l Paramy S1B Archite 2019/1	Linux_2.sh eter : 1 0 cture : N/A 1/13 14:37:55 by : root			
Test_Tool3 Parameter : Ver : 1.0 2 MB Architecture : N/A 2019/11/14 17:34:3	by : root	Test_Tool2 Parameter: Ver:1.0.0 2MB Architecture: N/A 2019/11/14 17:40:29	by : root	C:/ Test_T Paramy 2 MB Archite 2019/1	ool_1_32bit.exe eter: 1 o cture : N/A 1/15 14:57:41 by : root			
C:/ Test_Tool_2_32bit. Parameter: 1 2 MB Architecture: N/A 2 019/11/15 14:57:5 2019/11/15 14:57:5	exe by : root	Test_Tool_3_32bit.e Parameter: Ver:1.0 2MB Architecture: N/A 2019/11/1514:58:15	xe by : root	hello_n Paramo 253 B Archite 2019/1	word.bat eter : 3 cture : N/A 1/18 09:46:09 by : root			
C:/ Test_Tool_4.exe Parameter :		C/ Test_Tool_32bit_40	:_2.exe	C:/ Test_To Parame	ool_32bit_50s_2.exe ater :			
Display 50/57 result(s)								
Search the web and Windo	vs 🛛 🔯 🚦	3 💫 🔍 🖇) 🐴 📧 🔽 🗃	🤗 🚺 应			^ 🍺 💔	₩ 💿 💟 🔛 dı) 🐺 ENG 🕺 3/25/2020

6.1.3.2. Deploy tool

The actions are similar to the Deploy tool function in IR Flow in section 3.4.4.3. However, there are a few other points as follows:

- User login under root group: Display all Agents in active system < 30 days.
- User login under default group: Display all Agents in the default group.
- User login under parent-level group: Display all Agents in the group user logging in and the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Agents belonging to the group of the user logging in.

Enable to filter online agents, then search for agents.



📶 AJIANT						ତ EN 👻 root 💶 🕙
ploy Tools						📮 Guid
	Tools Management			🖸 Deploy tool		Result
Add tool	·····> S Click Deploy Tool button to					
ools	Agents Type and enter t	o search	Q			ſ
	HOSTNAME T	PLATFORM	TOOLS T			STATUS
Q Type to search tool Add tool	WIN-LCEP3B4853K	•	ListService V1.0.0	Autorunsc V13.82.0.0 Listdils V3.20.0.0		Online
	WIN-4EBDUC0L7SK	•				Offline All
	WIN7X64	•				Offline
	ANM-NHANDT4	•				Offline
	THANHLN9	•				Offline
	WIN-D8U54D510EL	•	ConfigReader.Exe V1	.0		Offline
	THANHLN9-PC	•	Autorunsc V13.82.0.0	Listdlls V3.20.0.0		Offline
	DESKTOP-2L169U5	•				Offline
~	CHUYENNT2-VIRTUALBOX	<u>₽</u>				Offline
Search && Add tools	HUYHV-PC	•	Listdlls V3.20.0.0 ListService V1.0.0	TestScriptLinux_03.5h V2.5.6 Test_Tool_40s View more	2.Exe V1 Logonsessions.Exe V5 CFF Explo	er.Exe V1 Online
	DESKTOP-4HA8UHH	•				Offline
	TESTONEAGENT-PC	•				Offline
	DESKTOP-U808HAB	•				Offline
	THEDV1W7-PC	•				Offline
	DESKTOP-J1VS222					Offline
	DESKTOP-1L66CDG	•				Offline
	WIN-4DI87RP96PL	8	the second second	state to burne a second state of	and the second	Offline
	THANHLN9-VIRTUALBOX		ListService2 V1.1.1	ListService V1.0.0 Procexp.Exe V6 Te	25t_100t_405_2.Exe V1	Offline
Deptoy tools	WIN7-CONGNC9	•				e utiline

After selecting the tool and agent to deploy, check the results on the Result tab. On this screen, the results of running the tool under the agent also can be viewed or downloaded to the local machine similar to IR Flow.

 ♦ VEDR board - Agile: x ◆ Test Management (: x \bullet Test	agement i: 🗙 💠 Test Mana ools?tab=1	igement fi 🗙 🚺 AJIANT - De	eploy To 🗙 🚺 AJIANT - IR I	Flow D : 🗙 🎇 Test D	Design - aliant 🗙 💽 [Release]]	[BBXNTK] \ 🗙 🛓 Downloads	🗙 🗮 VCS-aliant Portal - : 🗙	+ - 3908 0	- ʊ ×
	Alerts	IR Flow	Investigation	Response	Protect & Prevention	Setting	G EN	• root	. .
Deploy Tools									📮 Guide line
\$	Tools Management				🖸 Deploy tool		C Re	sult	
Add tool Add tool Multi select agents online	Click Deploy Tool button to	h							
Tools Agen	Type and e	nter to search	Q						
Q Type to search tool Add tool	HOSTNAME	PLATFORM T	Listdlis V3.20.0.0	TestScriptLinux_03.5	h V2.5.6 Test_Tool_40s_2.1	Exe V1 Logonsessions.Exe V	/5 CFF Explorer.Exe V1	Online	8
autorunsc 1	WIN7-32BIT-PC	•	ListService V1.0.0 V Autorunsc V13.82.0.0 Test Tool 4.Exe V1.0	Test_Tool_40s_2.	Exe V1 ListService V1.0.0	0 Procexp.Exe V6 Test_Te	ool_Linux_1 V1.0	Online	
VISSE 0.0 Harb: Sa1355eedeebectoffsetbilsseecedoebeetbal	THANHLN-PC	•	Autorunsc V13.82.0.0 Listdlls V3.20.0.0 Vi	Procexp.Exe V6	Test_Tool_40s_2.Exe V1	ListService V1.0.0 Config	Reader.Exe V1.0	Online	
0	THILD1-PC	<u>@</u>	Test_Tool_40s_2.Exe	V1 Listdlis V3.20	1.0.0 ListService V1.0.0			Online	
G Deploy tools							✓ Deploy tool	successfully!	x



🚺 ΔΙΙΔΝΤ						③ EN ≠ root 🔔
ov Tools						P Gu
.,		Tools Management		[계 Deploy tool		Result
ls Result	279 result(s)					
Autorunsc	Agents (1)	Success (1/1)				
ИЕ	Platform T	Agent ID 🛛 🗑		Hostname 🏼 🗑	Status 🗑	ACTION
15 25/03/2020	•	6BBCD23F7D1BB16E4B13E549126ED24	43BF0707F	Win7-32bit-PC	Success	⊻ ③
 Autorunsc 	Agents (1)	Success (1/1)				
 Autorunsc 	Agents (1)	Success (1/1)				
 ListService 	Agents (1)	Success (0/1)				
 Autorunsc 	Agents (1)	Success (1/1)				
 Autorunsc 	Agents (1)	Success (1/1)				
 ListService 	Agents (1)	Success (0/1)				
- Autorunsc	Agents (1)	Success (1/1)				
 Autorunsc 	Agents (1)	Success (1/1)				
Autorunsc	Agents (1)	Success (1/1)				
Test_Tool_40s_2.6	Exe Agents (1)	Success (1/1)				
Sleep_10s_linux.5	Sh Agents (1)	Success (0/1)				
lav 15/279 result(s)						4 5 6 7 9 10 5

7. Response Screen

7.1.1. Response Live Response

Purpose: The Live Response function provides the ability to process a set of remote commands according to the working session to provide information or process requests on the host.

Steps to implement Live Response function as follows:

• Step 1: Click the Response tab and select Live Response.



😐 VEDR Portal - Live Response 🛛 X 🔛 VEDR Portal - Live Response 🛛 X 📔							- a ×
← → C 🞧 🔺 Not secure 10.30.161.37/#/response/live-response							⊘☆♥ 🤊 ⊖ 👱 😫
VEDR Portal	Alerts	IR Flow	Investigation	Response	Setting	③ EN •	nhandt4 😐 👻
Live Response							🟳 Guide line
GNOODE ACENT TO LIVE RESPOnse ***Click Add New Remote to start remote***	v	Time (Choose time to Liv	n Respons	Start Law Hingdon			
							^

• Step 2: Create a new Live Response session

Select Agent: Display the list of agents:

- \circ User login under root group: Display all Agents in active system < 30 days.
- User login under default group: Display all Agents in the default group.
- User login under parent group: Display all Agents in the group of the user logging in and the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Agents belonging to the group of the user logging in.

Users can only perform Live Response command with agents that are online (

- Select Time: There are intervals of 5 minutes, 15 minutes, 1 hour and 3 hours.
- Click Start Live Response button.



 ・ → C	0 4 5
VEDR Portal Alerts IR Flow Investigation Response Setting 😚 EN + nhand14	•
	•
Live Response	🟳 Guide line
GIODS AGINT TO LIVE RESPONDE Agent's Choose agent to Live Response V Time : Choose time to Live Response V Star Live Response	
***Clask Add New Remote It Search agent is dropdown list Q	
 choyennt2-Vettel05 (biox0000004/c3b5004/c2b8/310/c2b8/300/c2b8/310/c2b8/300/c2b8	
nhand#4PC(INCETRESINGCTRENDETCOMMOS/EDUIDCENS)	
DESKTOP HERZELQ DOKESKELMAGURARELIMANKI COSTCELL.	
• Thankin PC (2006)FEBRC1159-LANNE22911ATRETHIND)	
Win7-CongNCS (ictAmSt03IV03794CE199646231007740343)	
• hajp+PC [\$e440/73033094737364253286034603123]	
DESRIDP FEMILIEQ [IDARISHMEZATREIDS97100770047425	
thanthirds VistualBox (6:CRBAALU-MBAACPC-0BB377299-2271963	
Ø Attachment log	^

• Step 3: Wait for 1 minute for the system to connect to the agent, the system state is Connecting.

VEDR Portal - Live Response 🛛 🗙	☑ VEDR Portal - Live Response × +								- σ ×
\leftrightarrow \rightarrow \bigcirc \bigcirc \land Not secure	10.30.161.37/#/response/live-response								⊘☆\$ 🥄 👂 🕂 🥵
VEDR Portal		Alerts	IR Flow	Investigation	Response	Setting		⑤ EN ▼	nhandt4 🕒 👻
Live Response									🟳 Guide line
CHOOSE AGENT TO LIVE RESPONSE	Agent : nhandt4-PC(B0EF7B3E39EEC77626B	387CC988653FBD63DC8285) 🗸	Time : 3 hours	~	Start Live Response				
Hostname nhandt4-PC		Started N/A			Duration 3h		Time to live 3h		
**Hemato session started (Place with lic conscipul) (Mendy, 20 May 10 15:24-42 (Mendy, 20 May-10 15:24-42	+e71 Creating Session 201905201524554 +e71 Connecting	59840							
				<u>(</u> 8)					
Attachment Log									• Connecting

• Step 4: When the connection is successful, the user is allowed to execute commands at the console screen and the state of the Live Response session is Running.

Notes: Each agent at a time has only 1 working session of Live Response.



😔 VEDR Portal - Live Response 🛛 🗙 🔛 VEDR Portal - Live Response	× +						- σ ×
\leftarrow \rightarrow C (a) A Not secure 10.30.161.37/#/response/live-resp	onse					(2 🕁 👽 👂 😝 👱 😫
VEDR Portal	Alerts	IR Flow Investigatio	n Response	Setting		③ EN •	nhandt4 👱 👻
Live Response							🟳 Guide line
CHOOSE AGENT TO LIVE RESPONSE Agent : nhandt4-PC(B0EF7B3E39)	EC77626B87CC988653FBD63DC8285) 🗸	Time:3 hours 🗸	Start Live Response				
Hostname nhandt4-PC	Started 15:25:42 20/05/2019		Countdown 02:40:45		C Time to live 3h		
06.mstg.scsilon tis/tdd Imnedy, 26.Msy19 1552442 4971 Crating Sessins 201005 Imnedy, 26.Msy19 1552442 4971 Cranteling (mody, 26.Msy19 152527 4971 Agent Cimencial Imnedy, 26.Msy19 152527 4971 Agent Cimencial Imnedy, 26.Msy19 152527 4971 Agent Cimencial Imnedy, 26.Msy19 152527 4971 Agent Links 27.1772010 14:40 4971b 0 27.1772010 14:40 4971b 0 27.1772010 14:40 4971b 100 5 27.1772010 10:55 471L5 1009536 MousiefithoutBurderst 27.1772010 10:55 471L5 1009536 MousiefithoutBurderst 27.1772010 10:55 471L5 1009536 MousiefithoutBurderst 27.1772010 10:55 471L5 102 -450012 proceeding and 27.1772010 10:55 471L5 102 -450012 horest 27.1772010 102 -450000 horest 27.1772010 102 -450000 horest 27.177200 horest 27.177200 horest 27.177200 horest 27.177200 horest 27.177200 horest 27.177200 horest 27.177200 horest 27.177200 horest 27.17700 horest 27.17700 horest 27.17700 horest 27.1770 horest 2	015245559840 ere etup.assi						 Rutming
& Attachment Log							^

Users can execute commands at the console screen as follows:

No.	Commands	Parameters	Description
1	cd	cd <dirpath></dirpath>	Change current working folder
2		cd or cd	Switch back to parent-level folder
3	pwd		Print current working folder
4	dir		List files/sub-level folders in the current folder
5	delete	delete -file <path> For example: delete -file "c:\temp\run path.exe"</path>	Delete 1 file
		delete -folder <folderpath> For example: delete -folder temp\axvers</folderpath>	Delete 1 folder

/



		delete -all <folderpath> For example: delete -all c:\temp</folderpath>	Delete all files/sub-folders in the folder (but do not delete the folder)
6	viewfile	<filepath><sizeinbytes></sizeinbytes></filepath>	Display data in file (file size limit)
7	get	<filepath></filepath>	Upload 1 file from host to server
8	put	<url><folderpath></folderpath></url>	Download 1 file to host machine
9	mkdir	<dir name=""></dir>	Create 1 folder
10	reg		Commands related to Registry
		query <keyname>-v<valuename>For example:-queryreg-query-query"HKLM\Software\abc xyz" -v-v"run path"-v</valuename></keyname>	Query the value data of a key
		query <keyname> -s For example: reg -query "HKLM\Software\abc xyz" -s</keyname>	Query all sub keys, values and data
		add <keyname> For example: reg -add "HKLM\software\abc xyz"</keyname>	Add 1 key
		add <keyname> -v <valuename> -t <type> -d <data> For example: reg -add "HKLM\software\abc xyz" -v</data></type></valuename></keyname>	Add 1 value

Page | 101

1



		"run path" -t REG_SZ -d "c:\temp\bin.exe"	
		delete <keyname> For example: reg -delete HKU\S-1-5-21- 3791698801-2327923109- 636705026- 2080\Software\Test</keyname>	Delete 1 key and all sub keys and value
		delete <keyname> -v <valuename></valuename></keyname>	Delete 1 key value
		import <filename></filename>	Import 1 file .reg
		export <keyname> <filename></filename></keyname>	Export 1 file .reg
11	process		Commands related to process
		-t <processid></processid>	Turn off a running process by process ID
		-s <processid></processid>	Pause a process
		•	•
		-r <processid></processid>	Recover a previously paused process
		-r <processid> -l -a</processid>	Recover a previously paused process List all processes of all users
		-r <processid> -l -a -l -u <username></username></processid>	Recover a previously paused process List all processes of all users List all processes of an user
12	service	-r <processid> -l -a -l -u <username></username></processid>	Recover a previously paused process List all processes of all users List all processes of an user Commands related to service
12	service	 -r <processid></processid> -l -a -l -u <username></username> -query 	Recover a previously paused process List all processes of all users List all processes of an user Commands related to service List the services running on the host machine
12	service	 -r <processid></processid> -l -a -l -u <username></username> -query -start <servicename></servicename> 	Recover a previously paused process List all processes of all users List all processes of an user Commands related to service List the services running on the host machine Start 1 service

1



13	user	-list	List the users on the machine
		-sid <username></username>	Get sid of username
14	cls		Delete the console screen
15	help		Help command

Some notes when working with commands on the console screen as follows:

- Clear command: After executing the Clear command, the system will support the user to download the entire log made on the previous console screen, by clicking on the here link.
- Get <filepath> command: For example, get procexp.exe in the console screen, the result of getting the file is displayed in the Attachment Log screen at the bottom right corner of the screen. Users are allowed to download files to the browser or delete the downloaded files to the server.

😟 VEDR Portal - Live Response 🛛 🗙 🔛 VEDR Portal - Live	ve Response X +						- a ×
← → C (2) ▲ Not secure 10.30.161.37/#/resp	ponse/live-response					Ø	🗘 🕄 🤌 😓 😫
VEDR Portal	Alerts	IR Flow Investigation	Response	Setting		⊙ en +	nhandt4 👱 👻
Live Response							📮 Guide line
CHOOSE AGENT TO LOF DESDONSE Amont - phonded 6	Dr/865570252055777626887/r088652500520r82853 v	Time: 3 bours	Shart I has Romonea				
Hostname nhandt4-PC	© Started 15:52:48 20/05/2019		Countdown 02:59:39		C Time to live		
<pre>***Remote session started** Penday, 20-bwy/10 joslis3 ed7) consting 56 penday, 20-bwy/10 joslis3 ed7) consting jos penday, 20-bwy/10 joslis32 ed7 Apet Conse Penday, 20-bwy/10 joslis32 ed7 Apet Conse Penday, 20-bwy/10 joslis32 ed7 def file precap.ses seccessfully i def file precap.ses secces</pre>	nsien 20100520155140#531CB cred Agent info here ay still processed. please check result or try ag	nin.					
							Running
FILE NAME		TIME CREATED		DIRECTORY			
procexp.exe		2019-05-20715:52:50+	07:00	C:\a			± 8

- Step 6: The Live Response session ends when:
 - \circ $\,$ Time of session expires: When the time of Duration field is equal to the time of the Time to Live field.



😔 VEDR Portal - Live Response 🛛 🗙 🔛 VEDR Portal - Live Response	× +					- σ ×
← → C ⋒ A Not secure 10.30.161.37/#/response/live-resp	onse					⊘☆♥ 🤉 🖯 💆 👱 😫
			gation Response	Setting		EN - nhandt4 🚊 -
Live Response						📮 Guide line
CHOOSE AGENT TO LIVE RESPONSE Agent : nhandt4-PC(B0EF7B3E39E	EC77626B87CC988653FBD63DC8285) 🗸	Time : 5 minutes	✓ Start Live Response			
Ø Hostname nhandt4-PC	Started 15:56:10 20/05/2019		Duration 00:05:00		Time to live 5m	
Remote session started [Monday, 20-May-19 15:55:04 +07] Creating Session 20190520 [Monday, 20-May-19 15:55:04 +07] Connecting	01555EFFB7AD6					
[Monday, 20-May-13 15:55:55 +07] Agent Connected [Monday, 20-May-19 15:55:55 +07] Agent info: Agent info he [Monday, 20-May-19 16:00:55 +07] Session timeout, exit!	re					
[Monday, 20-May-19 16:00:55 +07] agent closed						
						Stopped
Attachment Log						^

- \circ The user actively requests to close the connection with the Close command.
- $\circ~$ When the connection with the agent is lost, the server performs ping/pong failed more than 3 times.

VEDR Portal - Live Response X	VEDR Portal - Live Response × +					- 0 ×
\leftrightarrow \rightarrow \bigcirc \bigcirc \land Not secure	10.30.161.37/#/response/live-response					⊘ ☆ 🏵 👂 ! \varTheta 👱 🧕
VEDR Portal	Alerts	IR Flow Investigation	Response	Setting	⊙ en •	nhandt4 🕒 👻
Live Response						🟳 Guide line
CHOOSE AGENT TO LIVE RESPONSE	$eq:agent:handt4-PC(B0EF7B3E39EEC77626B87CC988653FBD63DC8285) \checkmark$	Time : 15 minutes 🗸 🗸	Start Live Response			
Hostname nhandt4-PC	Started 16:04:30 20/05/2019		Duration 00:00:16		Time to live 15m	
Attachment Log	** 07) Creating Session 20190030160023A0002 09) Conventing					• Stopped

Ι



8. Setting Screen

8.1.1. Agent Management

Agent Management function supports administrators to manage installed agents, including:

- View Agent List and general information
- View details of Agent
- Quickly select Agents and set some settings (policy, update group).

	Portal - IR Flow Detail X	VEDR Portal - Agent Manageme: × 30.161.37/#/settings/agent-manage	VEDR Portal - Agent Manageme	r × │ + IjaCl6lilsImxpbWl0ljozNSwidGl0b0	GVfZGF0ZXBpY2tlcif6lkFMRVJULkxBU1RfU0V	WRU5fREFZliwia2V5X3RpbWUiOiJsYXN0X3NIc	dmVuX2RheSlsImIudGVydmFsX3Rpb	- ଅ ୦ନ୍ତ ନ 🖯 🛓
	VEDR Portal		Alerts	IR Flow Inv	restigation Response	Setting	© en *	nhandt4 👱 👻
gent M	Management		(2	2)				@ Q
5 resu	lt(s)	(5)					View col	umn 🗸
· •	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY
<u> </u>	DESKTOP-EGANUBQ	Online	No_group	Release	20/05/2019 16:47:07	17/04/2019 10:16:46	192.168.4.222,192.168.4.111	test_sample
	ThanhLN-PC	Online	No_group	Release	20/05/2019 16:47:01	13/03/2019 13:30:45	192.168.4.222,192.168.4.111	test_sample
	Nhandt4-PC	Online	No_group	Release (1)	20/05/2019 16:46:45	13/03/2019 13:05:22	192.168.4.111	test_sample
4	Chuyennt2-ViettelOS	Offline	No_group	Release	20/05/2019 16:35:19	22/04/2019 16:56:49	192.168.4.222,192.168.4.11	(4)
	DESKTOP-HHN2B1Q	 Offline 	No_group	Release	20/05/2019 13:43:08	05/11/2018 14:21:48	192.168.4.111,192.168.4.2	best_sample
	W(3) gNC9	Offline	No_group	Release	16/05/2019 18:41:25	25/03/2019 17:38:14	192.168.129.2	test_sample
0	Harpy-PC	 Offline 	No_group	Release	14/05/2019 15:27:58	01/04/2019 17:11:43	192.168.253.2	test_sample
	Thanhln9-VirtualBox	Offline	No_group	Test	03/05/2019 15:48:57	11/03/2019 14:30:07	192.168.4.222,192.168.4.111	N/A
	Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10	29/01/2019 04:57:35	192.168.4.222	test_sample
	Chuyennt2-ViettelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52	22/04/2019 15:36:41	192.168.4.222,192.168.4.111	N/A
	Thanhin9-VirtualBox	 Offline 	No_group	Test	20/04/2019 10:36:54	13/03/2019 09:01:48	192.168.4.222,192.168.4.111	N/A
	DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/2019 18:51:50	05/11/2018 14:42:16	192.168.11.2	test_sample
	Halpv-PC	Offline	No_group	Release	01/04/2019 16:00:13	13/03/2019 11:50:06	192.168.253.2	test_sample
	DESKTOP-U808HAB	Offline	No_group	Release	29/03/2019 15:48:06	12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample
	ThanhLN9-PC	Offline	No_group	Release	26/03/2019 17:48:49	21/03/2019 13:31:53	192.168.4.222,192.168.4.111	N/A
	DESKTOP-J1VS222	Offline	No_group	Release	02/03/2019 22:54:03	19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample
	DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14	22/02/2019 10:53:15	192.168.4.111	test_sample
	ANM-THANHLN9	Offline	No_group	Test	15/02/2019 08:35:41	29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample
	WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41	08/11/2018 10:55:46	192.168.129.2	test_sample
	ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35	19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample

The system support performing the following features:

(1) View the Agent List installed on the system:

- User login under root group: Display all Agents in active system < 30 days.
- User login under default group: Display all Agents in the default group.
- User login under parent-level group: Display all Agents in the group of the user logging in user and the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Agents belonging to the group of the user logging in user.
- Each agent is displayed general information, including: Name, State, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, Platform, Platform Version, Architecture, DNS and Version.

Page | 105



(2) Support searching for Agent by AgentID, ComputerName, OS, Architecture, Platform, Policy, IPDCN, Online, Update Group, Group ID, IP, Mac and Version. For each search criteria, search operators "=", "!=", and "~" are supported.

	VEDR	Portal - IR Flow Detail 🗙 🔛	VEDR Portal - Agent Managemer 🗙	😟 VEDR Portal - Agent Manageme	- × +					-	o x
~	7	C 🕞 🔺 Not secure 10.3	0.161.37/#/settings/agent-manag	ement/search=ey/xdWVyeVNIYX	jaCl6lilsImxpbWl0ljozNSwidGl0b	GV1ZGF0ZX8pY2tIci6lk	FMRVJULIodBU1R#UUV	WRU5fREFZIwna2V5X3RpbWUrOUsYXN0X31	NidmVuX2RheSIsImludGVydmFsX3Rpb.	-020 0	⊌ ≟ ⊌
							Response	Setting	③ EN +	nhandt4	9 -
Ag	gent M	lanagement									
I	Type to	search agent								0	Q
	@	AgentID			Agent ID						_
	Ð	ComputerName			Agent Computer Name						~
	Ð	os			Agent Operating System						
		Architecture			Amont Architectum						
		Activectore			Agencochitecture	G					
	ຍ	Platform			Agent Platform						
		Nhandt4-PC	Offline	No_group	Release	20/05/2019 17:02:46		13/03/2019 13:05:22	192.168.4.111	test_sample	-
		Chuyennt2-ViettelOS	Offline	No_group	Release	20/05/2019 16:35:19		22/04/2019 16:56:49	192.168.4.222,192.168.4.111	N/A	- 1
		DESKTOP-HHN2B1Q	Offline	No_group	Release	20/05/2019 13:43:08		05/11/2018 14:21:48	192.168.4.111,192.168.4.222	test_sample	
		Haipy-PC	Offline	No_group	Release	14/05/2019 15:27:58		01/04/2019 17:11:43	192.168.253.2	test_sample	
		ThanhIn9-VirtualBox	Offline	No_group	Test	03/05/2019 15:48:57		11/03/2019 14:30:07	192.168.4.222,192.168.4.111	N/A	
		Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10		29/01/2019 04:57:35	192.168.4.222	test_sample	
		Chuyennt2-ViettelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52		22/04/2019 15:36:41	192.168.4.222,192.168.4.111	N/A	
		ThanhIn9-VirtualBox	Offline	No_group	Test	20/04/2019 10:36:54		13/03/2019 09:01:48	192.168.4.222,192.168.4.111	N/A	
		DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/2019 18:51:50		05/11/2018 14:42:16	192.168.11.2	test_sample	
		Haipv-PC	Offline	No_group	Release	01/04/2019 16:00:13		13/03/2019 11:50:06	192.168.253.2	test_sample	_
		DESKTOP-U808HAB	Offline	No_group	Release	29/03/2019 15:48:06		12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample	
		ThanhLN9-PC	Offline	No_group	Release	26/03/2019 17:48:49		21/03/2019 13:31:53	192.168.4.222,192.168.4.111	N/A	
		DESKTOP-J1VS222	Offline	No_group	Release	02/03/2019 22:54:03		19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample	
		DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14		22/02/2019 10:53:15	192.168.4.111	test_sample	
		ANM-THANHLN9	Offline	No_group	Test	15/02/2019 08:35:41		29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample	
		WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41		08/11/2018 10:55:46	192.168.129.2	test_sample	
		ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35		19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample	
Dis	splay 3	5/35 result									

Examples of search statements as follows:

Search by the condition "=":

$\in \rightarrow$	C 🕞 🔺 Not secure 10.3	0.161.37/#/settings/agent-manage	ement?search=eyJxdWVyeVNIYXUj	aCl6lkFnZW50SUQgPSBclj8BO	TE2NTY4QjQ4RUQyNDZF	MjBFOTYwNjBGRjID	ODJERjdFND	lorMjhcliAiLCJsaW1pdCl6MSwid	GIOBGV	fZGF0ZXBpY2tlcil6lk	kfmrvju	uk Ø	☆ 👽 💡	•	э 🛓 🥫
							Sett	ing					nhandt4		
Agent M	Management														
Agentic	D = "0A913568B48ED246E20E96060F	F9C82DF7E49128*												9	Q
1 result	(5)										View	column			~
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING		FIRST	PING		DNS		PO	LICY		
	ANM-NHANDT4	Offline	No_group	Test	18/12/2018 10:37:10		12/12	2018 09:06:04		192.168.4.222		tes	t_sample		
Display 1	/1 result														

Search by the condition "!=":

\rightarrow	C 🞧 🔺 Not secure 10	0.30.161.37/#/settings/age	nt-management?search=eyJxdWVyeVN	YXJjaCl6lkFnZW50SUQgIT	0gXCIwQTlotMzU2OEI0OEVEMj0	2RTIwRTk2MDYwRk	Y5QzgyREY3RTQ5MTI4XCIgliwib0	iltaXQiOjM0LCJ0a	XRsZV9kYXRlcGljaZVyljoiQl	JxFUL 🛛 合 🕄 🤌 🛛 🖯 🖯
							Setting			EN - nhandt4 🚨
ent	Management									
Agent	D != "0A913568848ED246E20E960	60FF9C82DF7E49128"								Ð
1 res	ult(s)									/iew column
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING		FIRST PING		DNS	POLICY
	DESKTOP-EGANUBQ	Online	No_group	Release	24/05/2019 10:42:43		17/04/2019 10:16:46		192.168.4.222,192.168.4.111	test_sample
	Thanhin9-VirtualBox	Offline	No_group	Test	24/05/2019 09:17:22		11/03/2019 14:30:07		192.168.4.222,192.168.4.111	N/A
	Nhandt4-PC	Offline	No_group	Release	23/05/2019 16:44:37		13/03/2019 13:05:22		192.168.4.111	test_sample
	Thanhin9-VirtualBox	© Offline	No_group	Test	22/05/2019 14:32:06		13/03/2019 09:01:48		192.168.4.222,192.168.4.111	N/A
	ThanhLN-PC	Offline	No_group	Release	22/05/2019 09:26:27		13/03/2019 13:30:45		192.168.4.222,192.168.4.111	test_sample
	Win7-CongNC9	Offline	No_group	Release	21/05/2019 18:19:26		25/03/2019 17:38:14		192.168.129.2	test_sample
	Chuyennt2-ViettelOS	© Offline	No_group	Release	21/05/2019 16:04:51		22/04/2019 16:56:49		192.168.4.222,192.168.4.111	N/A
	DESKTOP-HHN2B1Q	Offline	No_group	Release	21/05/2019 15:18:40		05/11/2018 14:21:48		192.168.4.111,192.168.4.222	test_sample
	Haipv-PC	Offline	No_group	Release	14/05/2019 15:27:58		01/04/2019 17:11:43		192.168.253.2	test_sample
	Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10		29/01/2019 04:57:35		192.168.4.222	test_sample
	Chuyennt2-ViettelOS-Test	© Offline	No_group	Release	22/04/2019 16:46:52		22/04/2019 15:36:41		192.168.4.222,192.168.4.111	N/A
	DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/2019 18:51:50		05/11/2018 14:42:16		192.168.11.2	test_sample
	Hajpy-PC	Offline	No_group	Release	01/04/2019 16:00:13		13/03/2019 11:50:06		192.168.253.2	test_sample
	DESKTOP-U808HAB	Offline	No_group	Release	29/03/2019 15:48:06		12/03/2019 18:29:01		192.168.4.222,192.168.4.111	test_sample
	ThanhLN9-PC	Offline	No_group	Release	26/03/2019 17:48:49		21/03/2019 13:31:53		192.168.4.222,192.168.4.111	N/A
	DESKTOP-J1VS222	Offline	No_group	Release	02/03/2019 22:54:03		19/02/2019 16:09:27		192.168.4.111,192.168.4.222	test_sample
	DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14		22/02/2019 10:53:15		192.168.4.111	test_sample
	ANM-THANHLN9	Offline	No_group	Test	15/02/2019 08:35:41		29/01/2019 04:45:08		192.168.4.222,192.168.4.111	test_sample
	WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41		08/11/2018 10:55:46		192.168.129.2	test_sample
	ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35		19/01/2019 09:45:19		192.168.4.111,192.168.4.222	test_sample

Page | 106

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Search by the condition "~":

							Setting			nhandt4	
gent I	lanagement										
Compu	erName ~ "ANM"									9	Q
repult	el.								View co	lumn	~
C	-)	6747110	00018	URDATE (BOUR	LAST BINS	~	DIDET DING	-	DWE	BOLICY	
	ANM-THANHLN9	© Offline	No_group	Test	15/02/2019 08:35:41		29/01/2019 04:45:08		192.168.4.222.192.168.4.111	test_sample	
	ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35		19/01/2019 09:45:19		192.168.4.111,192.168.4.222	test_sample	
	ANM-NHANDT4	Offline	No_group	Test	18/12/2018 10:37:10		12/12/2018 09:06:04		192.168.4.222	test_sample	
	ANM-CONGNC9	Offline	No_group	Alpha	03/12/2018 15:01:10		30/11/2018 16:13:13		192.168.4.222,192.168.4.111	test_sample	
	ANM-PHUOCNM2	Offline	No_group	Alpha	03/12/2018 14:31:13		30/11/2018 16:12:38		192.168.4.222,192.168.4.111	test_sample	
	ANM-CONGNC9	Offline	N/A	N/A	N/A		N/A.		192.168.129.2	N/A	

Search by AND match criteria:

\leftrightarrow	C 🝙 🔺 Not secure	10.30.161.37/#/settings/ag	ent-management?search=eyJxdl	WVyeVNIYXJjaCl6lkNvbX81dGV	yTmFtZSB%2BIFwiQU5NXClgQU5EIFBs	YXRmb3JtlD0gXCJI	NaWNyb3NvZnQgV2luZ	G93cyAxMCBQcm9cliAiLCJsaW1p	dC16MiwidG10bGVE	ZGFOZ 🤇) ch 😨 👂	Θ 🛓 🧯
							Setting			N ₹	nhandt4	. .
Agent M	lanagement											
Comput	terName ~ "ANM" AND Platfo	rm = "Microsoft Windows 10 Pro"									9	Q
												_
2 result	s)									/iew column		~
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING		DNS	POLICY		PLATFORM	
	ANM-CONGNC9	Offline	No_group	Alpha	03/12/2018 15:01:10	30/11/2018 16:	13:13	192.168.4.222,192.168.4.111	test_sample		Microsoft Windo	ws 10 Pro
	ANM-CONGNC9	 Offline 	N/A	N/A	N/A	N/A		192.168.129.2	N/A		Microsoft Windo	ws 10 Pro
Display 2	/2 result											

Search by OR match criteria:

								Sett	ling			nhandt4 🕒	
ent I	lanagement												
Compu	erName ~ "ANM" OR Platforr	n = "Microsoft Windows 10 I	Pro"									Ð	C
resu	lt(s)										View colur	nn	~
	NAME	STATUS	GROUP	UPDATE GROUP	LAST P	ING	FIRST PING	E	DNS	POLICY	PLATFORM	м	
	DESKTOP-EGANUBQ	 Online 	No_group	Release	24/05/	2019 10:50:45	17/04/2019 10:	16:46	192.168.4.222,192.168.4.111	test_sample	Microsoft	Windows 10 Pro	
	DESKTOP-HHN2B1Q	Offline	No_group	Release	21/05/	2019 15:18:40	05/11/2018 14:	21:48	192.168.4.111,192.168.4.222	test_sample	Microsoft	Windows 10 Pro	
	DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/	2019 18:51:50	05/11/2018 14:	12:16	192.168.11.2	test_sample	Microsoft	Windows 10 Pro	
	DESKTOP-U808HAB	Offline	No_group	Release	29/03/	2019 15:48:06	12/03/2019 18:	19:01	192.168.4.222,192.168.4.111	test_sample	Microsoft	Windows 10 Pro	
	DESKTOP-J1VS222	Offline	No_group	Release	02/03/	2019 22:54:03	19/02/2019 16:	09:27	192.168.4.111,192.168.4.222	test_sample	Microsoft	Windows 10 Pro	
	ANM-THANHLN9	Offline	No_group	Test	15/02/	2019 08:35:41	29/01/2019 04:	15:08	192.168.4.222,192.168.4.111	test_sample	Microsoft	Windows 10 Enterprise	
	WIN10-CONGNC9	Offline	No_group	Release	25/01/	2019 09:35:41	08/11/2018 10:	55:46	192.168.129.2	test_sample	Microsoft	Windows 10 Pro	
	ANM-HIEUPC4	Offline	No_group	Release	22/01/	2019 11:25:35	19/01/2019 09>	15:19	192.168.4.111,192.168.4.222	test_sample	Microsoft	Windows 7 Enterprise Se	ervio
	ANM-NHANDT4	Offline	No_group	Test	18/12/	2018 10:37:10	12/12/2018 09:	06:04	192.168.4.222	test_sample	Microsoft	Windows 10 Enterprise	
	ANM-CONGNC9	Offline	No_group	Alpha	03/12/	2018 15:01:10	30/11/2018 16:	13:13	192.168.4.222,192.168.4.111	test_sample	Microsoft	Windows 10 Pro	
	ANM-PHUOCNM2	Offline	No_group	Alpha	03/12/	2018 14:31:13	30/11/2018 16:	12:38	192.168.4.222,192.168.4.111	test_sample	Microsoft	Windows 10 Enterprise	
	DESKTOP-OMETRIE	Offline	No_group	Release	30/11/	2018 14:10:30	30/11/2018 14:	04:16	192.168.4.111,192.168.4.222	test_sample	Microsoft	Windows 10 Pro	
	DESKTOP-3QTIL7P	Offline	No_group	Release	26/11/	2018 15:31:19	17/11/2018 17:	11:19	8.8.8.8,8.8.4.4	test_sample	Microsoft	Windows 10 Pro	
	ANM-CONGNC9	Offline	N/A	N/A	N/A		N/A		192.168.129.2	N/A	Microsoft	Windows 10 Pro	

(3) Quickly select 1 agent/ 1 group of agents to set policy as follows:

1



Ĩ	U AJIANT			Investigation			evention Setting		(§) EN ▼	root 👱 👻
Agent Management										
Type t	o search agent								First Ping 📋	Last Ping 🖨 🛛 🔾
33 results)										
Select	ed (3) Set Policy Move to group	Set update group Can	cel							
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING		FIRST PING		IP DCN	POLICY
2	DESKTOP-4C6V54I	Offline	Test_scan_ip	Test	22/05/2020 15:46:14		15/05/2020 17:38:55		10.61.188.2	Agent Performance
1	ThanhLN9-PC	Offline	Liennt_group1	Alpha	25/05/2020 15:05:57		21/03/2019 13:31:53		10.61.188.2	bls_test
2	HuyHV-PC	Offline	Test_scan_ip	Test	25/05/2020 14:40:55		31/01/2020 17:23:19		10.61.188.2	Agent Performance
	Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10		22/04/2020 17:00:46		10.61.188.2	huyhv-2211
	WIN-MM956VNPD90	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40		07/05/2020 09:39:04		10.61.188.2	N/A
	Chuyennt2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13		18/05/2020 11:16:38		10.61.188.2	default
	DESKTOP-BGH8QIG	Offline	Default	Alpha	07/05/2020 14:28:53		24/07/2019 13:44:07		10.61.188.2	full_features
	DESKTOP-LRT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55		17/01/2020 18:39:40		10.61.188.2	huyhv_15.01.ProPre
	LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29		21/05/2020 11:42:22		10.61.188.2	N/A
	Ubuntu18x64chuyennt	Offline	Default	Beta	18/05/2020 15:32:16		29/10/2019 10:50:34		10.61.188.2	Agent Performance
	WIN-OH33SL4BBRJ	Offline	Test_scan_ip	Beta	19/05/2020 15:20:57		17/12/2019 13:36:53		10.61.188.2	hieupc4
	Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53		25/02/2020 17:38:33		10.61.188.2	Agent Performance
	Ubuntuhyperv-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39		25/02/2020 17:03:22		10.61.188.2	test
	ThanhLN-PC	Offline	Default	Test	18/05/2020 13:29:01		13/03/2019 13:30:45		10.61.188.2	Agent Performance
	Localhost.Localdomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29		01/04/2020 14:38:38		10.61.188.2	centos
	DESKTOP-EGANUBO	Online	Test_scan_ip	Test	25/05/2020 15:30:51		08/05/2020 22:16:52		10.61.188.2	full_features
	DESKTOP-315SAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40		19/08/2019 17:18:19		10.61.188.2	huyhv_15.01.ProPre

- Tick to select 1 agent or multiple agents to enter the Multi-selected session.
- Perform Set Policy.

Select	ed (1)	Set Policy Cancel	
	NAME	Policy	UP
	Nhand	test_sample \lor	grout
	<u>Win7-C</u>	Set Policy	group
	<u>Thanh</u>		group

• Result after setting policy:

).2	test_sample	
^{11,19} ~	Set Policy successfully!	×
		٦

 \circ $\;$ Delete the action on the Multi-selected screen

(4) View Column: Configure the display of columns at will:




(5) View details of an agent by clicking duplicate the mouse on any row

The system supports users to perform Set Policy, Update Group and Move to group for Agent quickly.

- User login under root group: Display all Groups in the system.
- User login under default group: Display default Group.
- User login under parent-level group: Display all the Groups belonging to the user logging in and the users belonging to the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Groups belonging to the user logging in.
- General Info Tab

The system displays general information about the agent, including: General information, CPUs, Network Interfaces, Default Gateway and DNS Server.



Î	U AJIANT			Agent ANM-CHUYE	10 Maria - Norman - Nama - N		🛞 EN 🖛 root 主 👻			
Agent	management			Agent ID 4030C72A3525D	0B939BC065533A18B6F6A5B006E	- ONLINE VIIIISAN	Guidelines			
Versio	a = "3.0.30"			First ping: 24/05/2021 03	:47:46 Last ping: 09/06/2021 14:56:58	First Ping 🖨 Last Ping 🛱 🔾				
				Agent properties						
13 res	ult(s)			SET POLICY	exhause shed shows		🛃 Vie	w column 🗸		
	Imagement Verses - 38 30* Search1 Imagement Search1 Imagement Search1 Imagement Status Imagement Im				ennance_auer_cruyen		ROUCY	VERSION		
	VCS	a Offine	Def	SET UPDATE GROUP	release	default	3,0,30			
	Nextcloud	© Offline	Dat	MOVE TO GROUP	default	-	default	3.0.30		
	Win7x86chuventest	Online	Def		Save	enhance_alert_chuyen	3.0.30			
ANM-CHUYENNT2 Online Def Ger							enhance_alert_chuyen	3.0.30		
	Ubuntu18x64chuyennt	© Offline	Dat	General info Installatio	on Hies Version Installed Certificates Scheduled lasks	full_features_centos	3.0.30			
	Test SeaBank khaitb v1	Offline	Def	General info		Network Interfaces	full_features	3.0.30		
	Allant tmanagement se - 33.50' NAME STATUS V2S 0.00me Name 0.0me Name 0.0me Name 0.0me Name 0.0me Name 0.0me Name 0.0me Districture 0.0me V2S 0.0me V2District 0.0me V2Districture 0.0me V2Districture 0.0me	Def	HOST NAME	ANM-CHUYENNT2	IPV4 192.168.56.1 IPV6 5680*eda1*11cdvda1*201e	enhance_alert_chuyen	3.0.30			
	DESKTOP-RUMB3Q9	© Offline	Def	HOSTID	495db28b-db32-4a1e-bb6c-f21a787391e7	MAC 0a:00:27:00:00:0e	anhnn19_test_load_image	3.0.30		
	Win7x86-A-PC	© Offline	Def	SETUP VERSION	N/A	NAME VirtualBox Host-Only Network	full_features	3.0.30		
	VCS	Online	Def	Agent ANI-CHUYENN First pre-24/05/20130-77 Agent properties SIT POLOY en SIT POLOY	windows	IP V4 109.294.197.94 IP V6 fe80::618d:cd15:12b0:c554	full_features	3.0.30		
	ThanhLN-PC	Online Def Offline Def	Def		Microsoft Windows 10 Enterprise	MAC 90:odb6:51:31:4/	full_features_thanhin9	3.0.30		
	Win10x64	a Diffice and a Office and a Office and a Office and and		PLATEORM VERSION	10.0.19041 Build 19041	IPV4 169.254.98.5	full_features_server	3.0.30		
	VLS O titine D ThanhULPC 0 Offine D Win10x64 0 Offine D Win2x64A-PC 0 Online D		Def	DI ATEMBA RAMIN	Standalone Workstation	IPV6 fe80::149f:a428:11ce:6205	anhnn19_test_load_image	3.0.30		
Display	13/13 result					MMC 12/08/06/51/31/4F				
				ARCHITECTORE	ama94	Default Gateway				
				PHYSICAL MEMORY	16,777,216	192.168.8.1				
				CPUs		DNS Server				
				CORES	8 3408.000000	192.168.4.222				
				MODEL NAME	Intel(R) Core(TM) 17-6700 CPU @ 3.40GHz	192.168.4.111				
				VENDORID	Venuineintei					

• Installation Files Version Tab

Statistics of all agent installation files, including the following information: Name of folder containing installation file, File name and Version.

Support quick search by File name, Version in search text box.

۵ì	AJIANT		Agent VCS		(3 EN * root 📤 *			
Agent ma	anagement		Agent ID 07DC8C7154	AB47371E9595AF52F88E43478F8CC4		•		
Version =	"3.0.30"		First ping: 31/05/2021	121:42:51 Last ping: 04/06/2021 09:52:08	First Ping 🖨 Last Ping 🖨 Q			
			Agent properties					
13 result(13 result(s)			default	🛃 Vie	w column 🗸		
	NAME	STATUS	GRI SET LIPOATE CONLID			POLICY	VERSION	
	VCS	Offline	Def	release		default	3.0.30	
	Nextcloud	Offline	MOVE TO GROUP Dat	default \checkmark	default	3.0.30		
	Win7x86chuyentest	Online	Def	Save		enhance_alert_chuyen	3.0.30	
	ANM-CHUYENNT2	Online	Def General info Install	lation Files Version Installed Certificates Scheduled Tasks Disks & nartitions	enhance_alert_chuyen	3.0.30		
	Ubuntu18x64chuyennt	Offline	Dat	adon mea veranti i maanea ceremeatea i denedatea marea i dana a particiona	full_features_centos	3.0.30		
	<u>Test SeaBank khaitb v1</u>	Offline	Def Search by file name or ver	sion	٩	full_features	3.0.30	
	DESKTOP-EGANUBQ	Offline	Def 🚍 AJIANT	VEDRDrvSetup.exe	VEDRDrvSetup.exe			
	DESKTOP-RUMB3Q9	Offline	Def propre	VERSION 1.0.0.85	anhnn19_test_load_image	3.0.30		
	Win7x86-A-PC	Offline	Def collector	VESConfigurationManager.exe		full_features	3.0.30	
	VCS	Online	Def response	VERSION 3.0.0.1210		full_features	3.0.30	
	ThanhLN-PC	Offline	Def drivers	Agentinfo.exe		full_features_thanhin9	3.0.30	
	Win10x64	Offline	Dat colector	VERSION 3.0.0.1050		full_features_server	3.0.30	
	Win7x64-A-PC	Online	Def	Parifett di		anhnn19_test_load_image	3.0.30	
Display 13/	13 result			VERSION 3.0.0.1213				
				RWorker.exe VERION 3.0.0.1154				
				VESUpdater.exe VERSION 3.0.0.1194				
				VESConnectionManagerok.exe VERSION 1.0.0.1168				

• Installed Certificates Tab

Statistics of all certificates on the machine with the agent installed, including the following information: List of certificates on the machine, Issued by, Issued to, Expiration date and State.



Ĩ	J AJIANT		- (1	Agent VCS	met	lanna Mandra Manana Manaka di Biban na bi		() E	N 🕶 root 💶 👻
Agent n	nanagement						• OFFEINE Uninstall		Guidelines
Version	- 13.0.307			First ping; 31/05/2021	21:42:51 Last ping: 04/0	First Plans C. Last Plans C.			
13	18(a)			Agent properties					w column
10 160	(L(3)	_	SET POLICY	default					
	NAME		GRO	SET UPDATE GROUP	release	~		POLICY	VERSION
	VCS	Offline	Def	MOVE TO GROUP	default			default	3.0.30
	Nextcloud	Offline	Dat					default	3.0.30
	Win7x86chuyentest	Online	Def		Save			enhance_alert_chuyen	3.0.30
	ANM-CHUYENNT2	Online	Def	General info Installa	ation Files Version Instal	lled Certificates Scheduled Tasks Disks & partitions Environ	ment variables Installed software Required software	enhance_alert_chuyen	3.0.30
	Ubuntu18x64chuyennt	Offline	Date	Continue (and	1 Marchine	D. Married Data Configurate Industry		full_features_centos	3.0.30
	Test SeaBank khaitb v1	Offline	Def	Cerunicates - Local	i Machine	Issued by Microsoft Root Certificate Authority	EXPIRATION DATE 10/05/2021 06:28:13	full_features	3.0.30
	DESKTOP-EGANUBQ	Offline	Def	му		R Thawte Timestamping CA ISSUED BY Thawte Timestamping CA		enhance_alert_chuyen	3.0.30
	DESKTOP-RUMB3Q9	Offline	Def	MOOt			EXPRATION DATE 01/01/2021 06:59:59	anhnn19_test_load_image	3.0.30
	Win7x86-A-PC	Offline	Def	Certificates				full_features	3.0.30
	VCS	Online	Def	- Trust R		R repolvisc.com	0000000000 00/04/0119 00/09/56	full_features	3.0.30
	Win10x64	 Online 	Def	CA		R Microsoft Root Authority	EXPRATION DATE 29/04/2110 09:36:30	N/A	3.0.30
	ThanhLN-PC	Offline	Def	TrustedPublish	ier			full_features_thanhin9	3.0.30
	Win7x84-A-PC	Online	Def	Disallowed		ISSUED BY Microsoft Root Authority	EXPIRATION DATE 31/12/2020 14:00:00	full_features	3.0.30
Display 1	3/13 result			TrustedPeople	AuthRoot R Symantec Enterprise Mobile Root for Microsoft Insted People Issued er: Symantec Enterprise Mobile Root for Microsoft		EXPRATION DATE 15/03/2032 06:59:59		
				ClientAuthissuer		R Microsoft Root Certificate Authority 2011 ISSUED BY Microsoft Root Certificate Authority 2011	EXPRATION DATE 23/03/2036 05:13:04		
				AAD Token Issuer	ion Authorities	R Microsoft Authenticode(tm) Root Authority	EXPIRATION DATE 01/01/2000 06:59:59		
				-E3 esiM Certhicati	on Autoonties	180 m			

In case of viewing details with more information, select ⁽¹⁾, the screen is displayed as follows:

Certificate

FRIENDLY_NAME	Microsoft Root Certificate Authority
ISSUER	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
KEY_USAGE	Digital Signature, Non-Repudiation, Certificate Signing, Off-line CRL Signing, CRL Signing (c6)
SIGNATURE_ALGORITHM	sha1RSA
STATUS	R
SUBJECT	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
VALID_FROM	10/05/2001 06:19:22

• Scheduled Tasks Tab

Statistics of all scheduled tasks on the agent installed machine, including information: List of scheduled tasks, Name, State, Trigger, Next time run, Last time run, Author and Created.

- Select or to customize the display of additional information for each task.
- Select Show or Hide to customize the display of additional information for each task.

 \times



Î	🚺 AJIANT		Agent	tVCS	10, et ;	terrestenten Brenzen Brenzen Brenzen Brenzen (* Brenzen 1975) er	and second	@ 1	n = root 🖭 =		
Agent	management		Agent 1	0.0700607154	4847371E9595AF33FME4	ISAT8FBCC4	Uninstan X		Guidelines		
Versid	m = "3.0.30"		First pir	First ping: 31/05/2021 21:42:51 Last ping: 04/06/2021 09:52:08					First Pine Ci Last Pine Ci		
			Agent	properties							
13 re	13 result(s)			UCY	default	~		± Ve	sv column 🗸 🗸		
	NAME	STATUS	GRI SETURO	MATE GROUP				POLICY	VERSION		
	YCS	Offline	Def	Receiver Y			default	3.0.30			
	Nextcloud	© Offline	Dat MOVE TO	O GROUP	default	~	default	3.0.30			
	Win7x86chuyentest	Online	Def		Save			enhance_alert_chuyen	3.0.30		
	ANM-CHUYENNT2	Online	Def	info bostalla	aking Eller Massion ha	defined Conditionals - Exclusion of Tables - Disks & and House - Exclusion - Exclusion	dunishing industry and and and	enhance_alert_chuyen	3.0.30		
	Ubuntu18x64chuyennt	@ Offline	Dat	inito inistalia	Subminies version and	sulleu ceruncates "acheuneu raska" urais a parcourta Environniter	ic variables installed soldware negulied soldware	full_features_centos	3.0.30		
	Test SeaBank khaitb v1	tb_v1 © Offline Def 📮 Task Schedules Lib	lules Library diffiff			full_features	3.0.30				
	DESKTOP-EGANUBQ	Offline	Def			 Ready 	Hide 3	enhance_alert_chuyen	3.0.30		
	DESKTOP-RUMB3Q9	Offline	Def • •			TRIGERS N/A		anhnn19_test_load_image	3.0.30		
	Win7x86-A-PC	@ Offline	Def			NERTRUNTIME N/A	NEITRUNTIME N/A				
	VCS	Online	Def			LAST PUN TIME 00:00:00 30/11/1999		full_features	3.0.30		
	Win10x64	Online	Def			LAST RUN RESULT The task has not yet run. (0X41303)		N/A	3.0.30		
	ThanhLN-PC	Offline	Def			AUTHOR WCS(Administrator		full_features_thanhin9	3.0.30		
	Win7x64-A-PC	Online	Def			18:36569 09/03/2021		full_features	3.0.30		
Display	13/13 small					folipoloci a Ready Holisoff a Ready දුර්ගිද a Ready	Show 3 Show 3 Show 2				

• Hover over the task and select into view the complete information of the task in .xml format.

XML Detail

 \times

xml version="1.0" encoding="UTF-16"?	
<task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"></task>	
<registrationinfo></registrationinfo>	
<date>2021-03-09T18:36:49.6502882</date>	
<author>VCS\Administrator</author>	
<uri>\dfffff</uri>	
<triggers></triggers>	
<principals></principals>	
<principal id="Author"></principal>	
<userid>S-1-5-21-3942219608-2782901308-3935319899-500</userid>	
<logontype>InteractiveToken</logontype>	
<runl evel="">1 eastPrivilege</runl>	
<settings></settings>	
<pre><multipleinstancespolicy>IgnoreNew<!--/-->/MultipleInstancesPolicy></multipleinstancespolicy></pre>	
ChisallowStarthforBatteries>true	
<pre>StonlfGningOnBatteries>true</pre> /StonlfGningOnBatteries>	
<	
<start available="" when="">false</start>	
<runoniyinvetworkavallable>ialse</runoniyinvetworkavallable>	
<pre>concerned.com/accord/acco</pre>	
<pre><suponialeend>aude</suponialeend></pre> /suponialeEnd> <destatoethessates< pre="">/DestatOetHes</destatoethessates<>	
<kestartonidie>taise</kestartonidie>	

🛃 Export to XML



- Select Export to XML to download scheduled task information. The .xml format is supported.
- Disks & Partitions Tab

Statistics of all disks & partitions on the agent installed machine, including the following information: List Disks, Partition, Volume name, Serial, Drive type, File system, Capacity and Available.

 \circ Select $^{\circ}$ or $^{\vee}$ to customize the display of additional information for each disk.

				Agent VCS	ID Plant Teachadh Bhann Rann ann Readaidh Bhantaidh a		© EN	- root 主 -
Agent management Version = "3.0.30"				Agent ID 07DC8C7154	847371E9595AF52F88E43478F8CC4			🔞 Guidelines
Versio	m = "3.0.30"			First ping: 31/05/2021	21:42:51 Last ping: 04/06/2021 09:52:08	First Ping 🖨 Last Ping 🖨 Q		
	-			Agent properties				_
13 result(s)				SET POLICY	default	📩 View column 🗸		
NAME STATUS GR				SET UPDATE GROUP			POLICY	VERSION
□ <u>VCS</u> © Offline Def					release		default	3.0.30
	Nextcloud Offline Dat				default ~		default	3.0.30
Win7x86chuyentest Online Def					Save		enhance_alert_chuyen	3.0.30
ANM-CHUYENNT2 Online Def				General info	tion Files Version Installed Certificates Scheduled Tasks Disks & partitions Emissionment vari	ablas Installed onfluera Required onfluera	enhance_alert_chuyen	3.0.30
	Ubuntu18x64chuyennt	Offline	Date		territines readent installed certification obsoluted reads brance participants careful territines for a		full_features_centos	3.0.30
	Test SeaBank khaitb v1	Offline	Def	ST500DM002-1BD142		^	full_features	3.0.30
	DESKTOP-EGANUBQ	Offline	Def	PARTITION	E		enhance_alert_chuyen	3.0.30
	DESKTOP-RUMB3Q9	Offline	Def	VOLUME NAME			anhnn19_test_load_image	3.0.30
	Win7x86-A-PC	Offline	Def	SERIAL	60138EF2		full_features	3.0.30
	VCS	Online	Def	DRIVE TYPE	Fixed		full_features	3.0.30
	Win10x64	Online	Def	FILE SYSTEM	FAT32		N/A	3.0.30
	ThanhLN-PC	Offline	Def	AVAILABLE	Se MD		full_features_thanhin9	3.0.30
	Win7x64-A-PC	Online	Def		04 MD		full_features	3.0.30
Display	53/35 result			Apacer A5350 51268				

• Environment Variables Tab

Statistics of all environment variables on the machine where the agent is installed, including the following information: List of system and users, variable name and values belonging to system or users.

 \circ Select $^{\circ}$ or $^{\sim}$ to customize the display of additional information for each disk.



Î	🗓 АЈІАНТ			Agent VCS	In Plans Includent Announce Parked & Rescaled Ref.	() E	i = root 主 =			
Agent	management			Agent ID 07DC8C7154	AB47371E9595AF52F88E43478F8CC4	 Guidelin 				
Versio	n = "3.0.30"			First ping: 31/05/2021	21:42:51 Last ping: 04/06/2021 09:52:08	First Ping 🗀 Last Ping 🗀 🔾				
13				Agent properties						
13 result(s) NAME STATUS VZS © Office				SET POLICY		🛃 Vie	w column 🗸 🗸			
	NAME		GR		0eianit	POLICY	VERSION			
	VCS	a Offine	Def	SET UPDATE GROUP	release V	default	3.0.30			
	Nextcloud	o Offine	Dat	MOVE TO GROUP	default ~	default	3.0.30			
	Win7x86chuventest	Online	Def		Save	enhance_alert_chuven	3.0.30			
	ANM-CHUYENNT2	Online	Def			enhance_alert_chuyen	3.0.30			
	Ubuntu18x64chuyennt	© Offline	Dat	General info Installi	ation Files Version Installed Certificates Scheduled lasks Disks & partitions Environment variables Installed software Required software	full_features_centos	3.0.30			
	Test SeaBank khaitb v1	Offine	Def	System	×	full_features	3.0.30			
	DESKTOP-EGANUBQ	Offline	Def	Administrator	^	enhance_alert_chuyen	3.0.30			
	DESKTOP-RUMB309	Offline	Def	Path		anhnn19_test_load_image	3.0.30			
	Win7x86-A-PC	© Offline	Def	%USERPROFILE%\Ap	pData\Local\Microsoff(WindowsApps;	full_features	3.0.30			
	VCS	Online	full_features	3.0.30						
	Win10x64	Online	Def	96USERPROFILE96\App	pData\Local\Temp	N/A	3.0.30			
	ThanhLN-PC	Offline		full_features_thanhin9	3.0.30					
	Win7x64-A-PC	Online	Def	%USERPROFILE%	pData)Local(Temp	full_features	3.0.30			
Display	13/13 result			OneDrive C:\Users\visc_admin\/	OneDrive					

• Installed Software Tab

Statistics of all software installed in the agent, including information: Software name, installed version and installed date.

• Support quick search for installed Antivirus software or enter the software name in the search text box.

Î	🚺 Δ.ΙΙΔΝΤ			Agent ANM-CHUYENNT2					() EN	- root 主 -	
Agent	management			Agent ID 4030C72A35	25D0B939BC065533A18B6F6A5B006E		 Guideline 				
Versic	m = "3.0.30"			First ping: 24/05/2021	03:47:46 Last ping: 09/06/2021 14:56:58	First Ping	Last Ping 🖨 🔍				
				Agent properties							
13 res	13 result(s)			SET POLICY	enhance_alert_chuyen	🛃 View column					
	NAME	STATUS	GR	SET UPDATE GROUP release v			POLICY	VERSION			
	VCS	 Offline 	Def		1 CIRCULAR				default	3.0.30	
	Nextcloud	Offline	Dat	MOVE TO GROUP default					default	3.0.30	
	Win7x86chuyentest	Online	Def		Save				enhance_alert_chuyen	3.0.30	
	ANM-CHUYENNT2	Online	Def	General info Install	ation Files Version Installed Certificates Sche	eduled Tasks Disks & partitions	Environment variables Installe	nd software Required software	enhance_alert_chuyen	3.0.30	
	Ubuntu18x64chuyennt	Offline	Date						full_features_centos	3.0.30	
	Test SeaBank khaitb v1	Offline	Def	59 result(s)	All Anti Virus		Type software name to search	Q	full_features	3.0.30	
	DESKTOP-EGANUBQ	Offline	Def			enhance_alert_chuyen	3.0.30				
	DESKTOP-RUMB3Q9	Offline	Def	Version 13.2.1	nents installer	04/08/2020	anhnn19_test_load_image	3.0.30			
	Win7x86-A-PC	Offline	Def	7-Zip 19.00 (x64)		full_features	3.0.30				
	VCS	 Online 	Def	Version 19.00				100	full_features	3.0.30	
	ThanhLN-PC	Offline	Def	Ajiant Version 1.0.1				11/03/2021	full_features_thanhin9	3.0.30	
	Win10x64	Offline	Dat	Version 1.0.1					full_features_server	3.0.30	
	Win7x64-A-PC	 Online 	Def	Version 2.0.4.0		05/01/2021	anhnn19_test_load_image	3.0.30			
Display	13/13 result			Foxit Reader Version 9.6.0.25114				03/08/2020			
				Google Chrome Version 89.0.4389.114				01/04/2021			
				Google Update Helpe Version 1.3.99.3	r			05/08/2020			
				HP LaserJet Pro M404 Version 48.4.4585.208	-M405 Basic Device Software			05/01/2021			
				Display 10/59 result(s	a						

• Required Software Tab

Statistics of all required software installed or not installed in the agent, including information: Software name, installed version and installed state.

• Support quick search for required software that is not installed on the machine or enter the name of the software in the search text box.



Ĩ	📶 AJIANT			rti-da In Maria Tanadastra Rassan Rassa Rassa Agent ANIA-CHUYENNT2 • ONLINE Unicetal I ×				~	🕃 EN 👻 root 😩 💌					
Agent	management			Agent ID 4030C72A35:	:5D0B939BC065533A18B6F6	A58006E			* UNLINE	Chinistan	\sim	Guidelines		
Version	n = "3.0.30"			First ping: 24/05/2021 03:47:46 Last ping: 09/06/2021 14:56:58							First Ping 🛱 Last Ping 🛱 🔾			
			Agent properties											
13 result(s)			SET POLICY	and an all all all and all all all all all all all all all al								📩 Vier	v column 🗸 🗸	
NAME STATUS GR USS ● Offline Def				ermande_arer (_crivyer							POLI		VERSION	
	VCS	© Offline	Def	SET UPDATE GROUP	release		~					defa	ult	3.0.30
	Nettland	e Office	Dat	MOVE TO GROUP	default		~					defa	ult	3.0.30
	Win7x86chuventest	Online	Def		Save							enha	ance alert chuven	3.0.30
	ANM-CHUYENNT2	Online	Def									enha	ance alert chuven	3.0.30
	Ubuntu18x64chuvennt	© Offline	Dat	Installation Files Versi	on Installed Certificates	Scheduled Tasks	Disks & partitions	Environment variables	Installed software	Required software Us	er list	full f	features centos	3.0.30
	Test SeaBank khaitb v1	Offline	Def	5 result(s)	All Not Installed	0		Туре з	oftware name to search		a	full_f	features	3.0.30
	DESKTOP-EGANUBQ	Offline	Def									enha	ance_alert_chuyen	3.0.30
	DESKTOP-RUMB3Q9	Offline	Def	Ajiant Version 1.0.1						 Installe 	d	anhn	n19_test_load_image	3.0.30
	Win7x86-A-PC	Offline	Def	SFive								full_f	features	3.0.30
	VCS	Online	Def	Version 64.0.3282.204						 Installe 	d	full_f	features	3.0.30
	ThanhLN-PC	Offline	Def	SecurityAgent						Installe	d	full_f	features_thanhIn9	3.0.30
	Win10x64	Offline	Dat	Version 1.2.19								full_f	features_server	3.0.30
	Win7x64-A-PC	Online	Def	SecurityAgentHotFix						 Not Installe 	d	anhn	n19_test_load_image	3.0.30
Display 1	13/13 result			VEDR						Not Installe	d			
				-							1			
											- 8			
				Display 5/5 result(s)										
											_			

• User List Tab

Statistics of all logged in users in the agent, including information: Username, active and administrator.

Μαιία 🔟	Allele Institut Institution Researce Researce Researce Researce Institution Researce Institutio Researce Institution Researce Institution Researce Instituti				
Agent management	Agent ID 07DCI8C7154AB47371E9595AF52F68E43478F8CC4	Guidelines			
Version = "3.0.30"	First ping: 31/05/2021 21:42:51 Last ping: 04/06/2021 09:52:08	First Ping 🖨 Last Ping 🛱 📿			
	Agent properties				
13 result(s)	SET POUCY default V	🛓 View column 🗸			
NAME STATUS	GRI SET LIBRATE CANUE	POLICY VERSION			
UCS Offline	Def	default 3.0.30			
Nextcloud © Offline	MOVE TO GROUP default	default 3.0.30			
Win7x86chuyentest Online	Def	enhance_alert_chuyen 3.0.30			
ANM-CHUYENNT2 Online	Def Installation Files Version Installed Certificates Scheduled Tasks Disks & partitions Environment variables Installed software Required software User Lit	enhance_alert_chuyen 3.0.30			
Ubuntu18x64chuyennt © Offline	Dat	full_features_centos 3.0.30			
□ <u>Test SeaBank khaitb v1</u> Offline	Der USER ACTIVE ADMINISTRATOR	full_features 3.0.30			
DESKTOP-EGANUBQ Offline	Def admin No No	enhance_alert_chuyen 3.0.30			
DESKTOP-RUMB3Q2 Offline	Det Administrator Yes Yes	anhnn19_test_load_image 3.0.30			
□ <u>Win7x86-A-PC</u> © Offline	Def DefaultAccount No No	full_features 3.0.30			
VCS Online	Def Guest No No	full_features 3.0.30			
<u>ThanhLN-PC</u> Offline	Det khaitb Yes No	full_features_thanhin9 3.0.30			
□ <u>Win10x64</u> © Offline	Dat WDAGUtilityAccount No No	full_features_server 3.0.30			
Win7x64-A-PC Online	Det	anhnn19_test_load_image 3.0.30			
Digglay 13/13 vessil					

(6) Quickly select 1 agent/ 1 group of agents to set up Move to group

• Select 1 agent/multiple agents to enter the Multi-selected session



Ĩ	U AJIANT			Investigation		evention Setting		§ EN -	root 👱 👻	
Agent	Management									
Type t	o search agent							First Ping 🗒	Last Ping 📋 🔾	
										1
33 resi	ilt(s)							*	View column 🗸 🗸	
Selecte	ed (3) Set Policy Move to grou	up Set update group Can	cel							í.
	NAME Groups			UPDATE GROUP	LAST PING	FIRST PING	E IP	DCN	POLICY	1
	DESKTOP-4C6V54I Select	an Option	~	Test	22/05/2020 15:46:14	15/05/2020 17:38:55	10	.61.188.2	Agent Performance	П
	ThanhLN9-PC Set Grou	P		Alpha	25/05/2020 15:05:57	21/03/2019 13:31:53	10	.61.188.2	bls_test	
	HuyHV-PC			Test	25/05/2020 14:40:55	31/01/2020 17:23:19	10	.61.188.2	Agent Performance	
	Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/2020 17:00:46	10	.61.188.2	huyhv-2211	L
	WIN-MM956VNPD90	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40	07/05/2020 09:39:04	10	.61.188.2	N/A	L
	Chuyennt2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/2020 11:16:38	10	.61.188.2	default	L
	DESKTOP-BGH8QIG	 Offline 	Default	Alpha	07/05/2020 14:28:53	24/07/2019 13:44:07	10	.61.188.2	full_features	L
	DESKTOP-LRT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/2020 18:39:40	10	.61.188.2	huyhv_15.01.ProPre	L
	LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29	21/05/2020 11:42:22	10	.61.188.2	N/A	U
	Ubuntu18x64chuyennt	Offline	Default	Beta	18/05/2020 15:32:16	29/10/2019 10:50:34	10	.61.188.2	Agent Performance	
	WIN-OH33SL4BBRJ	Offline	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/2019 13:36:53	10	.61.188.2	hieupc4	
	Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/2020 17:38:33	10	.61.188.2	Agent Performance	
	Ubuntuhyperv-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/2020 17:03:22	10	.61.188.2	test	
	ThanhLN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/2019 13:30:45	10	.61.188.2	Agent Performance	
	Localhost.Localdomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/2020 14:38:38	10	.61.188.2	centos	
	DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/2020 22:16:52	10	.61.188.2	full_features	
	DESKTOP-315SAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40	19/08/2019 17:18:19	10	.61.188.2	huyhv_15.01.ProPre	

• Perform Move to group

Group list in the Move to group combo box

- User login under root group: Display all Groups in the system.
- User login under default group: Display default Group.
- User login under parent-level group: Display all the Groups belonging to the user logging in and the users belonging to the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Groups belonging to the user logging in.
- $\circ~$ Quickly select 1 agent/ 1 group of agents to set up Set update group
 - Select 1 agent/multiple agents to enter the Multi-selected session.



6	JIANT			Investigation		vention Setting	😚 EN 🕶	root 🔔 👻
Agent I	Management							
Type b	search agent						First Ping 🗎	Last Ping 📋 🔾
33 resu	ilt(s)						ٹ	View column 🗸
Selecto	d (3) Set Policy Move to group	Set update group Can	cel					
	NAME	STAT Update Groups		OUP	LAST PING	FIRST PING	IP DCN	POLICY
	DESKTOP-4C6V54I	Of Select an Option		~	22/05/2020 15:46:14	15/05/2020 17:38:55	10.61.188.2	Agent Performance
	ThanhLN9-PC	Of Set Update Group			25/05/2020 15:05:57	21/03/2019 13:31:53	10.61.188.2	bls_test
	HuyHV-PC	● Of			25/05/2020 14:40:55	31/01/2020 17:23:19	10.61.188.2	Agent Performance
	Win7-32bit-PC	 Offline 	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/2020 17:00:46	10.61.188.2	huyhv-2211
	WIN-MM956VNPD90	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40	07/05/2020 09:39:04	10.61.188.2	N/A
	Chuyennt2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/2020 11:16:38	10.61.188.2	default
	DESKTOP-BGH8QIG	Offline	Default	Alpha	07/05/2020 14:28:53	24/07/2019 13:44:07	10.61.188.2	full_features
	DESKTOP-LRT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/2020 18:39:40	10.61.188.2	huyhv_15.01.ProPre
	LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29	21/05/2020 11:42:22	10.61.188.2	N/A
	Ubuntu18x64chuyennt	Offline	Default	Beta	18/05/2020 15:32:16	29/10/2019 10:50:34	10.61.188.2	Agent Performance
	WIN-OH33SL4BBRJ	 Offline 	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/2019 13:36:53	10.61.188.2	hieupc4
	Win7-32bit-PC	 Offline 	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/2020 17:38:33	10.61.188.2	Agent Performance
	Ubuntuhyperv-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/2020 17:03:22	10.61.188.2	test
	ThanhLN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/2019 13:30:45	10.61.188.2	Agent Performance
	Localhost.Localdomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/2020 14:38:38	10.61.188.2	centos
	DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/2020 22:16:52	10.61.188.2	full_features
	DESKTOP-315SAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40	19/08/2019 17:18:19	10.61.188.2	huyhv_15.01.ProPre

Perform Set update group.

Notes:

- Move to group: Move the agent to the groups in the Group Management screen
- Update group: Move the agent into groups that store files running under the agent, each group has different running files defined in the server.

8.1.2. Policy Setting

Purpose: Support users to manage the list of policies set up for Agents.

Interface screen when users access Setting >> Policy Setting as follows:

	ings/policy-s	ettings				⊘☆♥	≥ ⊝ ± 1
		Alerts		Response Settin	ng	ତ EN ≠ nhandt4	•
Policy List	•	1)				(2)	ireate New Policy
NAME	¥	NUMBER OF AGENT	CREATE TIME	UPDATE TIME	APPLIED TIME	APPLY STATUS	
default		1	28/01/2019 14:11:52	19/04/2019 17:06:17	26/03/2019 17:33:51	Not applied (3)	1
test		0	02/03/2019 14:13:28	25/04/2019 17:13:57	25/04/2019 17:19:07	Applied	ØÛ
test_sample		25	04/03/2019 11:07:09	21/05/2019 13:43:57	21/05/2019 13:44:03	 Applied 	0 Ū
test_sample 1		0	04/03/2019 13:53:51	04/03/2019 13:53:51	N/A	 Not applied 	e û
test2		0	04/03/2019 17:53:51	04/03/2019 17:54:23	05/03/2019 09:23:02	Applied	(4)
hieupc4		0	05/03/2019 15:44:15	05/03/2019 15:44:15	05/03/2019 15:44:20	 Applied 	a a
0503_test1		• (5)	05/03/2019 17:19:27	06/03/2019 14:10:13	06/03/2019 15:03:18	Applied	Ø Û
0703_policy		0	07/03/2019 09:04:29	07/03/2019 09:04:29	07/03/2019 09:04:33	Applied	Ø Û
2003_test core service		0	20/03/2019 10:14:49	20/03/2019 15:34:56	20/03/2019 15:35:28	Applied	a û
2003 test plugin Response		0	20/03/2019 10:37:48	20/03/2019 15:36:07	20/03/2019 15:38:33	Applied	@ Ü
2003_test du plugin		0	20/03/2019 10:53:16	20/03/2019 10:53:39	20/03/2019 10:57:55	 Applied 	@ û
2003_test collector chua module		0	20/03/2019 17:35:34	20/03/2019 17:35:43	20/03/2019 17:35:46	 Applied 	í ū
uisulav 12/12 resuluisi		•		#4/ *** #** # * ************************	201 001 001 00 X 1000 100		

(1) Display the list of Policies that have been created on the system. Each Policy includes the following information: name, number of Agents to which the Policy is applied, creation time, update time, time of Policy application and state (there are 2 states: Applied and Not Applied).



(2) Create a new Policy: Click on the + create New Policy button, the system displays a popup to create a new Policy as follows:

	+ Create New Policy
NAME OF POLICY	
Enter name of policy	
Cannot edit name of policy after create policy	

Notes: When creating a new Policy, the Policy name cannot be the same as previously created Policy.

After creating a new Policy successfully, the system will display a detailed screen of a Policy as follows:

← → C 🞧 🔺 Not secure 10.30.161.37/#)	/settings/policy-settings-detail/d5d-	1357ab68fa4e6fd5debe	2a9ea8a7666e1eea9			2	0 A 8 🧕 🖯 🛓 🖻
VEDR Portal					Setting		nhandt4 😩 👻
Policy Detail - New Policy ← Back to list							Apply Policy
Config Policy Tree							Edit Config
AGENT		SERVICE LIST		PLUQIN LIST		MODULES	
	Config	unstionManager) ectionManager) Updater)					
Config guidelines - Change mode of Policy tree: Press Edit Config buttor - In Edit Mode: Press Check/Uncheck button to Add/Re	in to edit lemove a node						
- After editing complete: Press Save Config button to s	save Config or Cancel button to comeb	ack previous Config					

Each created Policy usually has 3 default core services, including: ConfigurationManager, ConnectionManager and Updater. Note that these 3 services are not allowed to be deleted from the system. Steps to configure a Policy as follows:

- Step 1: Click the Edit Config button to change the Policy tree.
- Step 2: When in Edit mode, users are allowed to Check/Uncheck to Add/Remote other services.



← → C @ ▲ Not secure 10.30.161.37/*/s	ettings/policy-settings-detail/d5d4357ab68fa4e6fd5d	ebe2a9ea8a7666e1eea9				0 A 8 9 8 ±
				Setting		nhandt4 🔳 👻
Policy Detail - New Policy						Apply Patry
Config Policy Tree						Cancel Save Config
AGENT	SERVICE LIST		PLUGIN LIST		MODULES	
()	ConfigurationManager ConnectionManager Updater B Collector B Collector B Response	*	WindowsEventLog Antikeykogor ProcessAnalysis		CventSubcite VentFulig	
Config guidelines - Change mode of Policy tree: Press Edit Config button	to edit					
In Edit Mode: Press Check/Uncheck button to Add/Ren	nove a node					

• Step 3: After completing the Edit mode: Users click the Save config button to save the changes or click the Cancel button to return to the previous configuration.

← → C @ ▲ Not secure 10.30.161.37/	e/settings/policy-settings-detail/d5d4357ab68fa4e6fd5debe	2a9ea8a7666e1eea9			(ටරා ව 👂 🕹 😫
				Setting		nhandt4 😩 -
Policy Detail - New Policy ← Racktolist						Αρφίγ Ροίκην
Config Policy Tree						Gancel Save Config
AGENT	SERVICE LIST		PLUGIN LIST		MODULES	
.	ConfigurationManager ConnectionManager Updater Collector Response		WindowsEventLe AntikeySogger ProcessAnalysi		CventSubciber (CventFiblicy d CventFiblicy d CventFiblicy d CventFiblicy d CventFiblicy d CventFiblicy d	
Config guidelines - Change mode of Policy tree: Press Edit Config butto - In Edit Mode: Press Check/Uncheck button to Add/P - After editing complete: Press Save Config button to	on to edit temove a node save Config or Cancel button to comeback previous Config					

- Step 4: Click the 🔯 icon to perform detailed configuration for each Module/Plugin of the Services.
 - WindowsEventLog: Configure the log sources obtained under Agent.
 - EventSubscriber: Specify channels to get log.

Data request:

• Event filter field (filter by Event ID): Substrings separated by comma (,)

For example:

"4": filter events with EventID = 4



"-689": filter events with EventID #689

- Providers field: Substrings separated by semicolons (;)
- Fields require to have subs type and channel.
- Channel: A log source
- o Sub_type:

PUSH: When there is a new event \rightarrow call the function of VCS-aJiant to handle it.

POLLING: VCS-aJiant after a time period of actively taking the log.

PULL: VCS-aJiant actively takes the log after a time.

After the configuration is complete, it is required to be saved.

						2		
Event Subscriber Config								
	SUBSCRIBER TYPE	CHANNEL	EVENT FILTER	LEVEL	PROVIDERS			
	Select 🗸	Type to	Multi value separate by ,	Select 🗸	Multi value separate by ;	Add new		
	PUSH	Microsoft-Windows-Sysmon/Operational				û		
	POLLING	Microsoft-Windows-WMI-Activity/Trace				ū		
	PUSH	Microsoft-Windows-PowerShell/Operational				û		
	PUSH	Security	-4703			ŵ		

• EventPolicy: Set Policy to enable/disable some log types that the system does not have by default.

Requirement: At least 1 field selected.

E	vent Policy Config		2 Save
A	IDIT POLICIES	GROUP POLICIES	
C	Account Logon	Powershell	
e	Account Management	Process Create Command Line	
E	Detail Tracking		Vpdate config successfully

• EventChannel: Detailed configuration of some log sources as follows:

Retention: Whether to save the log rotation or not (If the Retention is selected, when the log file is full, the new log will overwrite the oldest log.)

Log file path: A log file path

Log file size: A log file size

Requirements: All data must be filled in.

				3
Event Channel Config				Clear Save
CHANNEL	RETENTION	LOG FILE PATH	LOG FILE SIZE (BYTES)	1
Type to 2		Type to	Note: max 52428800(50MB) min 10485760(10MB)	Add new
Microsoft-Windows-Bits-Client/Operational	0	%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Bits-Clien t%40perational.evtx	10485760	Û
Microsoft-Windows-WMI-Activity/Trace		%SystemRoot%System32\Winevt\Logs\Microsoft-Windows-WMI-Activit v%4Trace.etl	20971520	Û

 SysmonConfig: Enable/disable sysmon tool on Agent to get a sysmon log: Microsoft-Windows-Sysmon/Operational



Sysmon Config	2 Save
1 😰 Swith On Security System Config	

- Antikeylogger: Be as a SelfRun Plugin of VCS-aJiant, has the task that periodically scans the entire machine to find out the KeyLogger running on the machine if any.
- Scan settings: Configure the types of KeyLogger to scan

Requirements:

Scan cycle: Min is 1 minute and max is 180 minutes.

Choose at least 1 type of KeyLogger

• Whitelist setting: Configure the whitelist of some software according to the file path on the drive or according to the digital signature (cert) of the file running the KeyLogger.

Requirement: Fill out all fields.

After entering, the configuration is required to be saved.

White list setting							
WLTYPE	SCAN TYPE	DATA					
Select 🗸	Select 🗸	Type to	Add new				
WhiteListCer	Rawinput	Microsoft Corporation	ū				
WhiteListPath	HookMessage	C:\users\win 10 64\desktop\unikev40rc2-1101-win64\unikevnt.exe	ŵ				

- Step 5: Click the Apply Policy button to set the newly configured Policy for Agent.
 - Clone new Policy: Click the
 button, the system copies all details of the cloned Policy, except for the Policy name.

Clone from policy: test_sample							
NAME OF POLICY							
Enter name of policy							
Cannot edit name of policy after create policy Create Create							

 Delete Policy: Click on the $\frac{1}{2}$ button, the system displays a popup for the user to make a decision whether to delete Policy or not.

security		
Delete Policy		×
	Do you want to delete policy: 0503_test1	
	Cancel Accept	

In case the Policy already has an applied agent, after deleting it, the system automatically assigns default policy to that agent.

Delete Policy	×
Do you want to delete policy: <i>hieupc4</i> This policy has been assigned to agent(s). If this policy is deleted, agent(s) will be reset to default policy!	
Cancel Accept	-

• When clicking duplicate on each record, the system will forward to the detail page of a Policy for users to view/change the configuration for the Policy.

8.1.3. Group Management

Configure the rule to automatically switch the Policy and group to the agents if the rule is satisfied on the Portal, reduce the time to switch the Policy and group for each agent and synchronize the Policy for the agents that satisfy the configured rule. Key features on this monitor include as follows:

- (1) Manage groups by tree
- (2) Search group
- (3) Add a new group:
- Create rules to automatically switch groups for agents
- Options for group switch (All existing agents, New agents only, All existing and new agents) and Policy assignment (assign immediately, not assign).

(4) Monitor the agents belonging to the group and the total number of agents belonging to the group

- (5) Edit group
- (6) Delete group and agent belonging to the group.

8.1.3.1. Manage groups by tree

• User login under root group: Display all groups in the system.



- User login under default group: Display default group.
- User login under parent-level group: Display the group belonging to the group of the user logging in and the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all groups belonging to the group of the user logging in.

The list of groups displayed in a tree form includes the root groups, and each root group includes child-level groups at level 1, level 2, etc.

Each group includes the group name, the group's configuration information (rule, policy and apply to), and a list of agents belonging to the group.

Group rules are independent among groups (no parent-child level group inheritance).

The group management by tree is for easier management when the number of agents is large and there is a hierarchy of agent management by company, department, etc.

When the user belongs to a child-level group, if selecting a parent-level group, the group detail popup will not be seen.

8.1.3.2. Search group

Method 1: Click on the Search textbox \rightarrow A scrollable list of groups corresponding to the user logging in will be displayed \rightarrow Select the group in the displayed list.

Method 2: Click on the Search textbox \rightarrow Enter the search character into the textbox \rightarrow The system automatically searches for records containing the entered characters \rightarrow Select a suitable record in the suggested list or click Search or Enter, the list of satisfying records will be displayed.



Viettel Web Client Sign In	K 🔄 AJIANT - Groups Management 🗙	💶 Triệu đoá hoa hông * Ái Văn 🔹 🗙	VEDR-478] [Group managemer	< × +				- a ×
\leftarrow \rightarrow C \bigcirc A Not secure	10.30.161.37/#/settings/group/						2 2 3	ခု ၊ \varTheta 날 😫
TIAILA					Setting		ⓒ EN → havn2	•
Group Management	new	1	2 •	Delete Add new				
🗅 new_grouha	new_grouphin							
new_group67787	new_groups							
new_group1234	new_group4							
C asdasdaa	new_group3							
	new_group2							
asasdasd	new_group121							
ewedwedwed	new_group67787							
123123123								
🗅 hhhh								
🗅 new_group1								
new_groupddd								
new_groupasdasd	>							
🗅 new_group	>							
🗅 default								
Ask me anything		n n n s		🔿 💵 🔂 🕚		Image:	م 🗉 do) Pi	9:43 AM
- A Pak me unyunng			V 🖬 V 💼	u .				6/27/2019
		Alorte IB Flow	Investigation	Bosnonco Droi	toct E. Drougation S	otting	0.00	
		AICIO	incogation	Response i Ho		comp		
Group Management	al					×		Delete Add new
Search results								
🗅 all_exist		Go to group						1
		Delete group						

- Double-clicking on a record will display detailed information of that record.
 - Detailed information tab is displayed as Detail and the data of that group is Rule, Policy and Apply to.
 - $\circ~$ When selecting the Agent List tab, the agent information data matches that group.
- When right-clicking on a record, it will display 2 options: Go to group and Delete group.
 - $\circ~$ If selecting Go to group, then the user is taken to the location of that group on the tree
 - If selecting Delete group, a confirmation popup to delete the group will be displayed.
- When clicking on the menu in the right corner, each record also displays 2 options: Go to group and Delete group.

8.1.3.3. Add a new group

• User login under root group: Enable to add all new groups.



- User login under default group: Unable to add a new group.
- User login under parent-level group: Enable to add a new corresponding child-level group of the group belonging to the user logging in.
- User login under a child-level group or many child-level groups: Enable to add a new corresponding child-level of the group belonging to the user logging in.
 - Step 1: Select the group location to create.

If creating a new group in the original group list, click the Add new button on the right corner of the screen or hover over the bottom of the original group list on the screen and click Add new.

VEDR board - Agile Board - Your 🗙 🛛 🔷 Te	est Management for JIRA - Your 🗙 💠 Test Manage	ement for JIRA - You: 🗙 💠 Test Mar	nagement for JIRA - Your 🗙	AJIANT - Agent Ma	inagement 🗙 🔃 AJIANT -	Groups Management 🗙	AJIANT - Login	× +	- a ×
← → C ⋒ ▲ Not secure 10.30.1	161.37/#/settings/group/							0 🕄 🟠 👂	යි 🔉 🖯 👱 😫
📶 ΑJIANT					Protect & Prevention	Setting			root 😩 👻
Group Management	Type group to search						٩		Delete Add new
server_computer									
It_department									
hr_department									
🗅 os_linux									
□ test >									
🗅 hdsds									
new_and_exsit_os									
add_group									
phuocnm3_0722_1									
C cpu_modelname									
🗅 hostname_anm									
🗅 all_exist									
🗅 all_3									
🗅 ip_dcn									
C ip_192.168.8									
🗅 ip_dai									
🗅 default									
Add new									
Search the web and Windows	• 🔹 🗟 🖇	🍋 🧔 😵 😘 🛔	×8 🔀 📲 🌠	눧 🤿 🧉	6		,	N 🍺 🕖 🔣 💿 🔽	도 4) 💭 ENG 🔐 6:30 PM 3/25/2020

If creating a new group is a chil-level group in an original group or a group at level 1, level 2, etc, click on the parent-level group, then click Add new on the screen or hover over the bottom of the group list at the same level and click Add new.



VEDR board	rd - Agile Board - Your X 🔷 1	fest Management for JIRA - Your X	Test Management for JIRA - Your X	Test Management for JIRA - Your	K 🔃 AJIANT - Agent Mana	agement 🗙 🔃 AJIANT - Grou	aps Management 🗙 🔃 AJIANT - Login	x + - o x
<u>ر</u>		ron <i>ary=</i> /secongs/group/test	Alerts IR Flow	Investigation	Response P	Protect & Prevention	Setting	S EN + root
Group Ma	anagement Type	group to search		Q	Delete Add new	test		×
□ serv	ver_computer	khcl_department				D	etail	Agent list
🗅 it_di	department	Add new				p.d.		0
🗅 hr_d	department					Noving agent to this group if	All T following conditions matched	V
C 05_1	linux					05		
C test	• >							
🗅 hdso	ids					Policy		
C new	v_and_exsit_os						\sim	
add,	i_group					Apply policy now when rule m	satched	
D phu	Jocnm3_0722_1							
	toame anm					Apply to		
	exist					All existing and new agents	5 ×	
🗅 all_3	3							
C ip_d	den							
□ ip_1	192.168.8							
□ ip_d	dai							
🗅 defa	ault							
							Apply	
Search	the web and Windows	0 🕵	🖬 🖇 🍋 😵	🐚 🗷 🔀	诸 🗭 🎻 🍕			へ 🦕 🕖 👯 😋 💟 🔛 di) 💭 ENG 🛛 🔐 25/2020

• Step 2: Enter the group name and configure the rule.

Notes: The name and configuration rule cannot be the same as the existing name and rule.

If the All operator is selected: The rule is satisfied when both fields are satisfied.

If the Any operator is selected: The rule is satisfied when one of the two or both fields is satisfied.

VEDR board - Agile Board - Your	× 🛛 💠 Test Management for JIRA - Your 🗙	Test Management for JI	RA - Your 🗙 💠 Test Mi	anagement for JIRA - Your 🗙	AJIANT - Agent Manag	ernent 🗙 🔃 AJIANT - Groups Management 🗙 🔃 AJIANT - Logi	× +	- a ×
\leftrightarrow \rightarrow C \bigcirc A Not secu	re 10.30.161.37/#/settings/group/test						0 C 🌣 🔊 🖻	S 🛛 🕹 S
📶 ΔΙΔΝΤ		Alerts	IR Flow	Investigation	Response Pr	otect & Prevention Setting	© EN + r	bot 主 🝷
Group Management	Type group to search			Q	Delete Add new	KHCL_department		
server_computer	KHCL_department	× 2			1	Detail	Agent list	
L it_department						Rula		
hr_department						Moving agent to this group if All T following conditions matche	3	
🗅 os_linux						IP 192.168.8.*	×	
🗅 test						OS Platform V "Windows"	×	
🗅 hdsds						Add rule		
new_and_exsit_os								1
add_group						Policy		
phuocnm3_0722_1						default \checkmark		
C cpu_modelname						Apply policy now when rule matched		
hostname_anm						Analy to		
all_exist						nggary co		
C all_3						All existing and new agents		
🗅 ip_dcn								
□ ip_192.168.8								
🗅 ip_dai								
🗅 default								
						Αροί		
Search the web and Win	dows 🔲 🔯	📄 S 🐳	🛛 🖇 🛸	xii 🔀 📓 🏹	🕨 🧔 🗣		^ 🍺 🖗 🐹 💿 💟 🚍	(1) ENG 6:13 PM 3/25/2020



• Step 3: Select the policy and the agent type to apply the policy if the rule is satisfied.

	Detail		Age	ent list	
Rule					ć
Moving agent to	o this group if All 🔹 fol	lowing conditions matched :			
IP	192.168.8.*				
OS	*Windows*				
Policy					
test		~ Ç			
test Apply policy n	ow when rule matched	~ 5			
test	ow when rule matched	~ 5			
Apply policy n	iow when rule matched	<u> </u>			
test Apply policy n Apply to All existing ag	ow when rule matched	~ 5			
test Apply policy n Apply to All existing ag	ow when rule matched	× 5			
test Apply policy n Apply to All existing ag	iow when rule matched	× 5			
test Apply policy n Apply to All existing ag	iow when rule matched	× 5 × 6			
test Apply policy n Apply to All existing ag	ow when rule matched	× 5			
test Apply policy n Apply to All existing ag	ow when rule matched	× 5			

After clicking Apply, check the agent switched to new group in the Agent List tab: The list of agents meets the rules and is switched to the newly added group. Depending on the option in the Apply to section to switch the group for agents in the system as follows:

- All existing agents: Switch groups for all existing agents in the system. For new agents installed after Apply, if they match the rule, groups are NOT switched.
- New agents only: Only switch groups for newly installed agents after Apply. For the existing agents on the system, if they match the rule, groups are NOT switched.
- All existing and new agents: Switch groups for all existing agents in the system and the newly installed agents after Apply if the rule is matched.

Notes:



- If select the Apply policy now when rule matched checkbox, and click Apply, those selected agents will be checked the values. If they match the configured rule, they will switch the policy for the agent to the selected policy at the Policy section, and switch groups.
- In case the above checkbox is not selected, after Apply, those selected agents will be switched the group but not the policy. That is, the agents will keep the same policy while switching to the group with another policy. For newly installed agents, if the rule is matched, the group is switched and the default policy is applied. Because the checkbox is not selected, the default policy is applied.
- If the new agent matches the rules of many groups, it is prioritized to switch to the newly created group without counting the time to edit the group.

8.1.3.4. Edit group

Enable to choose to edit 1 or 2 or all 3 elements in a group, including: Rule, Policy and Apply to.

- User login under root group: Enable to edit all groups in the system.
- User login under default group: Unable to edit the default group.
- User login under parent-level group: Enable to edit all groups belonging to the user logging in/ and the child-level group whose role is also in the child-level role group of the user role logging in.
- User login under a child-level group or many child-level groups: Enable to edit all groups belonging to the user logging in.

To edit a Rule of a group, click the Edit icon.

khcl_dep	partment					×
	D	etail			Agent list	
Rule Moving agent	to this group if	All v followin	g conditions m	atched :		· 1
IP	192.	168.8.*				
OS	*Wir	dows*				

Edit the group rule then click Save.



	1	Detail	Agent list						
ule			Can	cel Save					
oving agent to t	this group i	if All following conditions matched :							
oving agent to t	this group i	f All following conditions matched :	×						

Then enable to edit in the Policy and Apply to sections, and click Apply.



Notes:

- In case of editing the elements of the group (Rule, Policy or Apply to) and do not click Apply, the edited content has been saved, but the Agent List is not updated. For newly installed Agents, perform the following:
 - Switch group: Depend on whether the new Agent is selected in the Apply to section. If selected, the Agent will be checked. If the rule of the group is matched, it will be switched to the group.
 - Apply policy: A policy of an agent depending on selecting the Apply policy now when rule matched checkbox. If the checkbox is selected, the group's policy will be applied. If it is not selected, the default policy will be applied. Because if the checkbox is not selected, the default policy will be applied.
- In case the components of the group are edited and then Apply is clicked, the edited content is saved. And if the All existing agents button in the Apply to section is selected, perform a scan of the entire agent information in the system and switch the group for the agent, then update the Agent List.

For new Agent, perform the same process as above.



- 8.1.3.5. Delete group or remove agent from group
- User login under root group: Enable to delete all groups in the system.
- User login under default group: Unable to delete the default group
- User login under parent-level group: Enable to delete all groups belonging to the user logging in and the child-level group whose role is also in the child-level role group of the user role logging in.
- User login under a child-level group or many child-level groups: Enable to delete all groups belonging to the user logging in.

To delete a group, click on the group to delete, click Delete \rightarrow OK on the confirmation screen.

After deleting a group, the agents belonging to the group will be switched to the default group, while their policies will still remain.



To remove the agent from the group, click on the Agent List tab, click the x icon to remove the agent from the group.

After removing the agent from the group, the agent is switched to the default group, while its policy still remains.



os_	linux					×
	Detai	l			Agent list	
7 ag	gent(s)	Type to	filter agent		View column	~
NO.	AGENT ID		HOSTNAME	STATUS	POLICY	# <mark>]</mark>]
1	CFF901BC683AE08EA40	77690	thedv1-VirtualBox	Offline	default	×
2	68555CF02D2580563A8	F12B4	ubuntu18x64chuyennt	Offline	thanhln0910	×
3	B6900069868F655D59F	4C2B8	chuyennt2-ViettelOS	Offline	thanhln_demo	×
4	EA3892E4CBB2887FB04	DF59E	chuyennt2-ViettelOS-test	Offline	default	×
5	8C7C096A104B60A07FC	4BB87	thanhln9-VirtualBox	Offline	thanhln_demo	×
6	C9FFB3E6991525CE5EA	6D360	test-windows7	 Offline 	thanhln0910	×
7	C8B5960DEF7C9E83253	6930F	chuyennt2-VirtualBox	Offline	default	×

Notes: For deleting a parent-level group:

- Delete all child-level groups
- Switch all agents of the parent-level group and child-level groups to default group
- Maintain policy of agents in parent and child-level groups.
- 8.1.3.6. Add a new user to the group





User av	ilable to add into gro	μр		User in group
N	D. USERNAME	FULLNAME	EMAIL	
1	admin	Supper Admin	admin@viettel.com	
2	ajiant	ajiant	ajiant@viettel.com	
3	ajiant_dev	ajiant_dev	ajiant_dev@viettel.com	
4	chuyennt2	chuyennt2	chuyennt2@viettel.com	
5	datnt88	datnt88	datnt88@viettel.com	
6	hieupc4	hieupc4	hieupc4@viettel.com.vn	»
7	liennt1	liennt1 5556668899665547	liennt18899665544112233@gmail.com	
8	liennt_alert	liennt alert	lienntalert@gmail.com	
9	liennt_inves	liennt investigation	lienntinvestigation@gmail.com	
10	liennt_irflow	liennt irflow	lienntirflow@gmail.com	
11	liennt_test1	liennt_test1	liennt_test1@gmail.com	
12	root	Supper Admin	admin@viettel.com	
13	siem	siem	siem@viettel.com	
14	thanhln9	Lê Như Thành	thanhln@viettel.com.vn	
19	thild1	Lưu Đình Thi	thild1@viettel.com.vn	

List of Users:

- User login under root group: Display all Users in the system.
- User login under default group: Display User only belonging to default group
- User login under parent-level group: Display the user logging in and the user belonging to the child-level group whose role is also in the child role group of the user role logging in.
- User login under a child-level group or many child-level groups: Display the user logging in.

																-	_
📶 ΔΙΙΔΝΤ												Setting		🕄 EN 🔫	root	•	
Group Management	Type grou	p to sea	rch			٩	Delete	e Add new	test								×
🗅 anm	>		bussiness_solution	>	🗅 test_ip					Detail			Agent list		Userlí	ist	
🗅 default			liennt_group	>					5 us	er(s)		Type to filter	user			Update use	er
			vcs_anm						NO.	USERNAME	FULLNAME		EMAIL		STATUS		
			test	>					1	admin	Supper Adr	nin	admin@viettel.com		 Active 	<	×
			group_test						2	ajiant	ajiant		ajiant@viettel.com		Active		×
			unknown						4	chuyennt2	chuyennt2		chuyennt2@viettel.co	m	Active		×
									5	datnt88	datnt88		datnt88@viettel.com		• Active		×

8.1.3.7. Delete user



8.1.4. Account Management

Manage accounts, permission and permission group of the portal system.

8.1.4.1. Permission management

Manage access permission to system resources (APIs). A permission is access permission to a specific resource (API) of the system.

The main functions on this screen, including:

- (1) Manage permission
- (2) Search permission
- (3) Delete permission

8.1.4.1.1. Manage permission

Display all system permission. In case the permission is deleted on this screen, when performing functions on the portal without permission, the deleted permission will automatically be added on the Permission Management screen.

8.1.4.1.2. Search permission

Enter the search character in the Search textbox \rightarrow Click Enter or Search \rightarrow A list of satisfied permission is displayed.

← → C									ଛା 🗢 \varTheta 날 💈
📶 AJIANT			Investigation		Protect & Prevention	Setting		ତ∂ en +	root 😐 👻
Permission search									2
alert 1									×Q
2 result(s)									
ND. PERMISSION NAME		DESCRIPTION			ROLE LIST				ACTION
1 alerts_manage					manage_alert, root				Ø 11
2 alerts_read					root, view_alert				0 Î
Display 2/2 result(s)									

8.1.4.1.3. Delete permission

Click the Delete icon \rightarrow Click OK on confirmation screen to delete successfully.



🔹 🔷 VEDR board - Agile Board - Your 🗙 🔷 [VEDR-650] [Portal] Hỗ trợ hiển 🗉 🗙 🔷 [VEDR-434] UserRoles	- Your Con 🗙 🔃 AJIANT - Permission Managemen 🗙	AJIANT - Alert List	🗙 🌻 Insti	ances - OpenStack Dashboar: 🗙 📔 🕂		- σ	×
← → C 🎧 🔺 Not secure 10.30.161.37/#/settings/account/permission					0 🗣 🟠 🔊	🛚 🗢 🖯 🕹	5
	IR Flow Investigation	Response Protect &	k Prevention	Setting	© εn τ	root 😦 👻	
Permission search							
Type permission to search						Q	
43 result(s)							
ND. PERMISSION NAME DE	SCRIPTION		ROLE LIST			ACTION	E
1 agent_management_manage			manage_agent_	management, manage_containment, manage_deploy_t	ool, root	/ 🗊 1	
2 agent_management_read			manage_investig	gation_result, root, view_agent_management, view_dep	loy_tool,View	Ø 🗓	
3 agent_policy_manage			manage_policy_	management, root		0 Î	
4 agent_policy_read			root, view_policy	y_management		0 Û	
5 agent_read						Ø Ü	
6 alerts_manage			×	sot		0 Ü	
7 alerts_read	Do you want to remove permissio	n : agent_management_manage ?				0 Î	
8 appctrl_handler_manage				_handler, root		0 Î	
9 appctrl_handler_read	Cancel	ок 2		trl_handler		0 D	
10 artifact_handler_manage			monoge_erent_	search, manage_investigation_result, manage_process_	analysis, root	Ø 11	
11 artifact_handler_read			root, view_inves	tigation_result, view_irflow, view_process_analysis		0 Î	
12 artifact_manage			manage_detecti	on, root		0 Î	
13 auto_runs_handler_manage			manage_auto_n	uns, root		0 Î	
14 auto_runs_handler_read			root, view_auto_	runs		0 Ü	
15 containment_manage			manage_contain	nment, manage_irflow, root		0 Î	
16 containment_read			root, view_conta	inment, view_irflow		0 Î	
17 deploy_tool_handler_manage			manage_deploy	_tool, manage_investigation_tool, manage_irflow, root		0 Î	
18 deploy_tool_handler_read			manage_investig	gation_result, root, view_deploy_tool, view_investigatio	_result,View	Ø 11	
19 endpointfw_handler_manage			manage_endpoi	ntfw_handler, root		0 Î	
20 endpointfw_handler_read			root, view_endp	ointfw_handler		0 Î	
21 event_manage			manage_event_s	search, manage_irflow, root		0 Î	
Display 25/43 result(s)							
🗄 Search the web and Windows 🕕 📴 📑 🤗 🗮	S 🐹 🖬 🛷 🔍 🗖	1			^ ▷ 🥑 🐹 🙆 🔽	🗊 de) 💭 ENG 🔐 2007/0	AM

8.1.4.2. Role Management

Manage roles (permission group) of the system.

Functions on this screen includes a set of as follows:

(1) Manage list of role

- User login under root Role: Display all Roles in the system.
- User login under default Role: Display default Role.
- User login under parent-level Role: Display all the Roles belonging to the user logging in and the corresponding child-level group.
- User login under a child-level Role or many child-level Roles: Display all Roles belonging to the role of the user logging in.
- (2) Search role
- (3) Add a new role
- (4) Delete role

8.1.4.2.1. Manage list of role

Manage the role list in the tree form. There are 2 built-in default root roles: Default and Root.

Default role: User with Default permission only has permission to access to Portal, no permission to view data or perform the function.



Root role: Include all system roles. The user with Root role has full permission to use all functions on Portal.

Clicking on a role, the detailed information of the role will be displayed. A role will include information: role name, list of permission, list of users (accounts) containing role, parent-level role or list of child-level roles (if any).

8.1.4.2.2. Search role

- Method 1: Click on the Search textbox → The list of roles in the system is displayed and can be scrolled → Select the role in the list that is displayed.
- Method 2: Click on the Search textbox → Enter the search character in the textbox
 → The system filters out the roles containing the search character → Select the role in the filtered list or click Enter or click the Search button.

🔷 VEDR board - Agile Boi 🗙 🔷 [VEDR-650] [Portal] Hồ 🗙 🏻	🔷 [VEDR-434] UserRoles - 🗙	AJIANT - Role Manager 🗙	AJIANT - Groups Mana	x AJIANT - Login	🗙 🛛 💠 Test Management fo	or J 🗙 📶 AJIANT - Rules Manage 🗙	🔶 Instances - OpenStack 🗙 🕂	- σ ×
\leftrightarrow \rightarrow \bigcirc \bigcirc \land Not secure 10.30.16	51.37/#/settings	/account/role/manage_contai	nment					O 🕄 🏠 🔊	🛚 🗢 🕒 🕹 😫
📶 ΔΙΙΔΝΤ		Alerts	IR Flow	Investigation	Response	Protect & Prevention	Setting	© en -	root 😐 👻
Role Management		mana		1			×Q	2	
C default	🗅 manag	manage_agent_manageme manage_alert	nt						
🗅 root >	🗅 manag	manage_appctrl_handler							
	🗅 manag	manage_auto_runs							
	🗅 manag	manage_containment							
	~	manage_deploy_tool							
	🗆 manag	manage_detection manage_endpointfw_band	er						
	🗅 manag	manage_event_search							
	🗅 manag	e_detection							
	🗅 manag	e_endpointfw_handler							
	🗅 manag	e_event_search							
	🗅 manag	e_group_management							
	🗅 manag	e_investigation_result							
	🗅 manag	e_investigation_tool							
	🗅 manag	e_irflow							
	🗅 manag	e_live_response							
	🗅 manag	e_permission_management							
	🗅 manag	e_policy_management							
	🗅 manag	e_process_analysis							
	🗅 manag	e_response_scenario							
	🗅 manag	e_role_management							
Search the web and Windows		0 🔯 🗎 S	💌 😵 🌃	🖲 🛷 🍕 🗷	()			^ 🍺 🖗 💆 🔽	및 (4) 및 ENG 2:16 PM 3/27/2020

- When double-clicking on a record, the detailed information of that record will be displayed.
 - Detailed information tab is displayed as Detail. The role data includes role information and permission of that role.
 - When selecting the User List tab, it means the user list containing the role is selected.
- When right-clicking on a record, it will display Go to role. Click on Go to role to return to the original tree role list.



- When clicking on the menu in the right corner, each record also displays the option: Go to role.
- 8.1.4.2.3. Add a new role
- User login under root group: Enable to add all new roles in the data tree.
- User login under default group: Unable to add new.
- User login under parent-level group: Enable to add a new corresponding child-level role of the group belonging to the user logging in. Unable to add a new role at the same level.
- User login under a child-level group or many child-level group: Enable to add a new corresponding child-level group of the group belonging to the user logging in.
 - Step 1: There are ways to create a new role as follows:
 - Click on a role then hover over the end of the role list and select Add new to create a role with the same level as the selected role.
 - Click Add new on the screen to create a child-level role of the selected role
 - Right click on a column in the tree and select Add new role.

Then, enter the role name that does not match the role name existed in the system.



- Step 2: Click the Edit icon to add permission information for the role → Select permission to add to the role → Click Save.
- User login under root group: Enable to edit all roles in the system.



- User login under default group: Unable to edit default role.
- User login under parent-level group: Enable to edit all the roles belonging to the user logging in and its child-level roles.
- User login under a child-level group or many child-level group: Enable to edit all roles belonging to the user logging in.

Notes: The permission list of child-level role is the parent-level role's subset. That is, when choosing the permission to assign to the child-level role, that role must belong to the permission list of the parent-level role.



test					>
Detail		_	User list		П
Detail role information				1	Ŷ
NAME	test (test)				
DOMAIN					
DESCRIPTION	test				
Permission					
test				×	
Detail			User list		
Detail role information			Cano	cel Save	3
Name	test				
Domain					
Description	test				
Permission					
agent_management_read ×	deploy_tool_handler_manage ×				
auto_runs_handler_manage		2			
auto_runs_handler_read		2			
containment_manage					
containment_read					
deploy_tool_handler_read					
endpointfw_handler_manage					

- \circ Step 3: Switch to the User List tab to add a role to the User's role list.
 - User login under root group: Display all users in the system.
 - User login under default group: Display user only belongs to the default.



- User login under parent-level group: Display the user logging in and the user in the child-level group whose role is also in the child-level role group of the user logging in.
- User login under a child-level group or many child-level groups: Display the user logging

🔷 VED	R boar	d - Agile Ba	or × ♦ [VEDR-65	0] [Portal] Hỗ 🗙 💠 [VEDR-434] UserRoles - 🗄	K AJIANT - Role Manager X	AJIANT - Groups Mana	🗙 📶 AJIANT - Login	🗙 🛛 💠 Test Management fo	er J 🗙 🔃 AJIANT - Rules Manage 🗙 1	🔶 Instances - OpenStack 🗙 🕂 🦳 🗕	$a \times$
\leftarrow \rightarrow	C	<u>م</u>	Not secure 10.30	0.161.37/#/settings/account/role/test						🖉 🕄 🏠 🖉 🙆	θ 🕹 😫
í	N	مالم	NT					Protect & Prevention	Setting	③ EN ♥ root	•
Role	Man	ageme	nt Type	role to search			Delete Add new	test			×
									Detail	User list	1
				manage_permission_management				0 user(s)	Type to filter user		Update user
A	dd u:	ser into	role								×
	U	lser availat	ble to add into role (2	selected)			User in role				
	C] NO.	USERNAME	FULLNAME	EMAIL						
	C	1	admin	Supper Admin	admin@ajiant.com						
2		2	chuyennt2	Chuyên	chuyennt2@viettel.com.vn		2				
	E	3	chuyennt3	chuyên	test@gmail.com		S				
	_ C	4	hieupc4	hieupc4	hieupc4@viettel.com.vn		<u> </u>				
	C	5	ngant	Nguyễn Thị Nga	ngant@rikkeisoft.com						
	C	6	ngant123	Nguyễn Thị Nga	nganguyen.nuce@gmail.com						
	C	7	root	Supper Admin							
	C	8	thanhln9	Lê Như Thành	thanhln@viettel.com.vn						
		9	thild1	Lưu Đình Thi	thild1@viettel.com.vn						
	- C	10	viewer	viewer	viewer@viettel.com.vn						
										Cancel Save	
				view_endpointfw_handler				_			
				D view awat coard							
				view_group_management							
				view_investigation_result							
				Pa view investigation tool							
	Search	h the web	and Windows	0 🙋 🚍	S 🔺 🕅 🔣 I	🔹 🛷 🗵 🌖	>			^ 🍃 🕼 🙀 💿 🔽 📰 փ) 💷 E	NG 3/27/2020

8.1.4.2.4. Delete role





Click on the role to delete, select Delete \rightarrow Click OK on the confirmation screen.

Notes: After deleting a role, all users using this role are changed: If user X is in the deleted role and user X has only 1 role, user X is switched to the default role. Otherwise, if user X has many roles, only the deleted role is removed from user X's role list.

8.1.4.3. User Management

Manage accounts logged into Portal VCS-aJiant system.

The main functions on this screen include a set of as follows:

- (1) Search account
- (2) Add new account
- (3) Edit account
- (4) Delete account

8.1.4.3.1. Search account

Click on the Search textbox \rightarrow The list of accounts in the system is displayed \rightarrow Select the account to search in the list or enter the <text> character in the textbox to filter out the accounts \rightarrow Click Search or select the account to search from the list of filtered accounts.



Tìm kiếm tài khoản				
nd				×Q
ngant				
ngant123				'hêm tài khoản
STT. TÊN ĐĂNG NHẬP	HQ VÀ TÊN	EMAIL	TRẠNG THẢI	THAD TÁC
1 admin	Supper Admin	admin@ajiant.com	🔲 Hoạt động	0
2 chuyennt2	Chuyển	chuyennt2@viettel.com.vn	🗾 Hoạt động	0 🗊
3 hieupc4	hleupc4	hleupc4@viettel.com.vn	🗾 Hoạt động	0
4 ngant	Nguyễn Thị Nga	ngant@rikkeisoft.com	🚺 Hoạt động	0
5 ngant123	Nguyễn Thị Nga	nganguyen.nuce@gmail.com	🚺 Hoạt động	0
6 root	Supper Admin		🗾 Hoạt động	0
7 thanhin9	Lê Như Thành	thanhln@viettel.com.vn	Hoạt động	0
8 thild1	Lưu Đình Thi	thild1@viettel.com.vn	🗾 Hoạt động	0
9 viewer	viewer	viewer@viettel.com.vn	Hoạt động	0 🗊
Hiển thị 9/9 kết quả				

8.1.4.3.2. Add new account

Click Add user \rightarrow Enter information in the form that is displayed \rightarrow Click Next.

📶 ΔJIANT				Setting			liennt_irflow	
User search								
Type to search								Q
16 result(s)								
NO. USERNAME	Add user				×	STATUS		ACTION
1 admin	Information Role Group) Active	
2 ajiant) Active	
3 ajiant_dev	Username	Type userna	ame) Active	
4 chuyennt2	Fullmanne) Active	
5 datnt88	romane	Type tulinar	me) Active	
6 hieupc4	Email	Type email) Active	
7 liennt1	Password	Type pass	word) Active	
8 liennt_alert	Status	 Active 	 Inactive) Active	
9 liennt_inves) Active	
10 liennt_irflow	1) Active	0 11
11 liennt_test1			Cancel No) Active	0 11
12 root	Supper Admin			admin@viettel.com) Active	
13 siem	siem			siem@viettel.com) Active	
14 thanhin9	Lê Như Thành			thanhln@viettel.com.vn			Inactive	
15 thild1	Lưu Đình Thi			thild1@viettel.com.vn) Active	
Display 16/16 result(s)								

- Select the role (permission group) to assign to the account, then click Next.
- When clicking on the check box, each role will display the permission corresponding to that role:
 - User login under root role: Display all roles in the system.
 - User login under default role: Display default role.
 - User login under parent-level role: Display all the roles belonging to the user logging in and the corresponding child-level group.
 - User login under a child-level role or many child-level roles: Display all roles belonging to the role of the user logging in.



ก	Edit user						×) -
Liser sea	Information	Role	Group	Type role to search Q	2 role selected			
Type to :	🗅 default				default Permissions:	read		٩
16 result	🗅 root		>		liennt_prote	et agent management manage agent manag	×	Add user
NO. U					Permissions	agent_policy_manage View more		CTION
1 a								
2 a								
3 a								
4 c								
5 d								
6 h								
7 6								
8 li								
9 li								
10 li								2
11 6								2 🗇
12 rc								
13 si								
14 tł								
15 tł								
Display 16				Back Next				

• On the Add role screen for user, the roles can be searched similar to the account search. After entering the search characters in the Search textbox → Click the Search icon or Enter to display the role screen that meets the search criteria.

	Add user inves		×				×
	Search results			2 role selected			
	manage_investigation_result	⁷⁰⁰ Go to role		default			
	manage_ inves tigation_tool	root		Permissions:	read		
	view_investigation_result	root		manage_invest	igation_result		×
	view_investigation_tool	root		Permissions:	agent_management_read	artifact_handler_manage	
					deploy_toor_nandier_read		
1							

• Click the checkbox corresponding to the role to be added, and click Go to role to return to the original role list screen, then click Create to create an account.

Notes: The account that is logged in to create a new account can only create accounts containing child-level roles in the list of roles that the account logging in is granted.

- Select the group to assign to the account, then click Create.
- When clicking on the check box, each role will display the permission corresponding to that role.
 - User login under root group: Display all groups in the system.
 - User login under default group: Display default group.
 - User login under parent-level group: Display the group belonging to the group of the user logging in and the corresponding child-level group.
 - User login under a child-level group or many child-level groups: Display all groups belonging to the group of the user logging in.



ก	Edit user			×) -
User sea	Information Role Group	Type group to search Q	1 group selected		
Type to r	🗅 anm 🔸		Lient_group1 anm/lient_group	×	۹
16 result					Add user
NO. U					CTION
1 a					
2 a,					
3 а					
4 c					
5 d					
6 h					
7 li					
8 li					
9 li					
10 li					2
11 li					2 🗊
12 rc					
13 si					
14 tł					
15 tł					
Display 16		Back Cancel Save			

• Click the checkbox corresponding to the group to be added, and click Go to role to return to the original group list screen, then click Create to create an account.

ัก	Edit user				×	
Liser see	Information Role Group	nga ×	1 group selected			
Usersea	Search results	nga123	liennt_group1	×		
Type to s	C nga123	2	anm/liennt_group			~
16 result					- 1	
NO. U					c	TION
1 a					- 1	
2 a,					- 1	
3а,						
4 ci						
5 d						
6 h						
7 li-						
8 li-						
9 li-						-
10 6						-
11 6						-
12 R						
13 si 14 th						
15 tł						
Display 16					-	
Unspilay 16		Back Cancel Save			. 1	

8.1.4.3.3. Delete account

Click on the Delete icon, then click OK on confirmation screen.

Check the display of the Delete icon as follows:

- User login under root group: Display all users in the system.
- User login under default group: Display user only belongs to default.
- User login under parent-level group: Display the user logging in and the user in the child-level group whose role is also in the child-level role group of the user logging in.



• User login under a child-level group or many child-level groups: Display the user logging in.

🔷 VEDR board - Agile Board - Your 🗙 🛛 🔷 [VEDR-1381] [HDSD] Viilt tái liệu 🗙	AJIANT - User Managem	ent X 🔃 AJIANT -	Alert List X	G regeneratorRuntim	e is not define 🗙 🛛 🗛 "reg	eneratorRuntime is not defin 🗙 📔 🏄	javascript - Babel 6 regener	atorR: × +	- o :	×
\leftarrow \rightarrow C (a) A Not secure 10.30.161.37/#/settings/account/use	r						Ģ	0 🕄 🕁 🔊	8 🛛 🗢 \varTheta 🐇	5
📶 ΔJIΔΝΤ	Alerts	IR Flow	Investigation	Response	Protect & Prevention	Setting		⊙ en *	root 😦 -	
User search										
Type to search									Q	
10 result(s)									Adduser	
NO. USERNAME	FULLNAME				EMAIL			STATUS	ACTION	
1 admin	Supper Admin				admin@ajiant.co	m		Active	0 🗓	1
2 chuyennt2	Chuyên				chuyennt2@viet	tel.com.vn		Active	/ 11	
3 chuyennt3	chuyên				test@gmail.com			Active	0 11	
4 hieupc4	hieupc4				hleupc4@viettel.	.com.vn		Active	0 11	
5 ngant	Nguyễn Thị Nga	-			nrant@rikkeienf	t.com		Active	0 11	
6 ngant123	Nguyễn Thị Nga		Do you want to remove	user : Supper Admin ?		@gmail.com		Active	0 🗓	
7 root	Supper Admin		Cancel	ov 2				Active	0 11	
8 thanhin9	Lê Như Thành		Cancer	2		.com.vn		Active	0 11	
9 thild1	Lưu Đình Thi				unioacovieweived	m.vn		Active	0 11	
10 viewer	viewer				viewer@viettel.o	iom.vn		Active	0 11	
Ditplay 10/15 result())										
Search the web and Windows	🖬 S 🍽	V 🔣 🗐 4	ý 🤻 🍺				^	Þ 🕅 🐹 💿 🔽	토미 (10:44 A) 💭 ENG 3/27/20	M 20

1


9. BLS Screen

9.1.1. Violation statistics

The function of Violation statistics supports the administrator to make statistics about the violations of the installed agent, including:

- Top base line violations and top baseline violation units
- View the list of violations and the list of violation agents in each unit
- View the list of violation units and the list of violations in each unit
- View details of Agent
- Export violation
- Report violation.

Click on the BLS tab >> Violation statistics.

3.9.1.1 Violation Statistics Screen

📶 ΔΙΙΔΝΤ	Cảnh báo	IR Flow	Điều tra	Phản ứng	Bảo vệ & Ngăn chặn	BLS	Cài đặt	© vi -	root 🔹 👻
Thống kê vi phạm		<u> </u>							🏳 Hướng dẫn sử dụng
Q Tìm kiếm theo nhóm			Q. Loại vi phạ	m				30 ngày trước	٩
Top vi phạm baseline				٦. ٢	Top Đơn vị vi phạm baselin	e			
Quy định bắt buộc cài đặt và sử dụng phần n	nëm diệt virus		20	1	¹ anm				42
Quy dịnh kiếm tra cài đặt và sử dụng phần m	ềm diệt virus Kaspersky		16		² dev_test_group				12
³ Quy định cấu hình cập nhật Hệ điều hanh			16		³ attt				10
⁴ Quy định máy tính phải join domain, và sử d	ụng tài khoản domain để đăng nh	hập máy tính	14		4 TTPP				2
⁵ Quy định cài đặt và sử dụng phần mềm			12	2	5 hgg				2
⁶ Quy định bắt buộc sử dụng phần mềm tường	ş lửa		•		⁶ kpt				2
7 Quy định làm việc không quá 20h			9		⁷ oələb1				2
⁸ Quy định cấm sử dụng thiết bị USB			8		⁸ root				2
9 [KPI] Proxy Firefox, IE			7		⁹ vi_mach				2
¹⁰ Quy định tự động khóa màn hình sau 5 phút			7		¹⁰ vtpost				2

The system supports performing the following features:

(1) Statistics of Top 10 most base line violations arranged in descending order

Each record is displayed with information, including: violation content and number of violation machines.

Select any record in the Top baseline violation, the system will move to the detail screen corresponding to the selected violation.

(2) Statistics of Top 10 units violating the most base-line arranged in descending order

Page | 145



Each record is displayed with information, including: name of violation unit and number of violation machines.

Select any record in the Top unit violating the baseline, the system will move to the detail screen corresponding to the selected unit.

(3) Search

Individual search:

- Search by unit
 - Top violation units: Display the units entered and the list of corresponding childlevel units (if any).
 - Top violations: Display the violations of the unit and corresponding child-level unit (if any).
- Violation type
 - Top violation units: Display a list of violation units and selected violation type.
 - Top violations: Display the selected violation.
- Violated time

Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

3.9.1.2 Violation Type Tab

TIAILA 🔟	Cảnh báo	IR Flow	Điều tra	Phản ứng	Bảo vệ & Ngăn chặn	BLS Cài đặ	t ⊡ vi -	root 💶 👻
Thống kê vị phạm		4						🏳 Hướng dẫn sử dụng
Q. Tìm kiếm theo nhóm			Q. Quy định b	sắt buộc cài đặt và sứ dụn	g phần mềm diệt virus		× 30 ngày trước	٩
🗖 root	Thống kê vi phạm baseline	•						
test	Loại vi phạm	Đơn vị						
server	LOAI VI PHAM		ĐÃ XỬ LÝ		CHƯA XỬ LÝ	MÁY VI PHẠM	DCIN Vị VI PHẠM	
- kdl	Quy định bắt buộc cài đặt và sử vírus	dụng phần mềm diệt	3 (21%)	1	11 (79%)	14 (64%)	17	0
- kpt								
anm			1	3				
default								
	Hiển thị 1/1 kết quả							



📶 ΔΙΙΔΝΤ					BLS	Cài đặt			root 主 👻
Thống kê vi phạm ← Top vi phạm									🏳 Hưởng dẫn sử dụng
Q Tìm kiếm theo nhóm			Q. Loại vi phạm					30 ngày trước	٩
🗖 root	Thống kê vi phạm basel	ine							
test	Loại vi phạm	Đơn vị							
no group	ĐƠN VỊ		ONLINE TRONG NGÀY	ONLINE TRONG 30 NGÀY GẦN NHẤT	ĐÃ XỬ LÝ	CHƯA XỬ LÝ	MÁY VI PHẠM	LUÂT VI PHAM	
kdl	root		0 (0%)	0	0 (0%)	0 (0%)	0 (096)	2	
kpt	default		1 (996)	11	2 (17%)	10 (83%)	12 (109%)	0	
thi_truong	anm		2 (50%)	4	0 (0%)	4 (100%)	4 (100%)	12	
anm	unknown		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
default	liennt_group2.1		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	ajiant_dev		0 (0%)	2	0 (0%)	2 (100%)	2 (100%)	0	
	dev_test_group		1 (50%)	2	0 (0%)	3 (100%)	3 (150%)	10	
	kpt		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	2	
	vtt		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	vtt_khoi_khcn_hgd_tt_kh_v	a_marketing	0 (0%)	0	0 (0%)	0 (0%)	0 (096)	1	
	OS31		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	vtt_cskh-dng		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	okv2		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	vtt_vdi_normal		0 (0%)	0	0 (096)	0 (0%)	0 (096)	1	
	vtt_khoi_cntt		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	ybi		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	has		0 (054)	٨	0.(004)	0.000	0.00543		
	Hiển thị 50/68 kết quả								

The system supports performing the following features:

(1) Select the Top violation links

Move to the Dashboard screen, the list of top violations and top violating units.

(2) The unit data tree of system

Display all system units with the parent-child hierarchy.

Enable to select units on the unit data tree to filter violations.

(3) Violation Type tab

Each Violation Type is displayed with general information, including: Violation type, Resolved, Unresolved, Violation Computer and Violation unit.

Select the Violation Type record on the list: Display a list of computers in each violation unit.

Select computer: Display detailed computer information and the corresponding violation list of the computer.



📶 ΔΙΙΔΝΤ						ion BLS		root 😐 👻
Violation statistic						List computers and units	baseline violation	Collapse all 🙍 🗙
Q Search for group			Q Violatio	n type		anm		^
📮 root	Violation statistic bas	seline				WIN7-32BIT-PC 5EF765BF9 3 violation	CE6221DA50F787ACB52C48AE32FBD0C	Hide list »
test	Violation type	Unit				Quy định bắt buộc cài đ 11:59:26 23/06/2020	iặt và sử dụng phần mềm diệt virus	Not resolved yet
	VIOLATION TYPE		RESOLVED		UNRESOLVED			· · · · ·
- C kdi	Quy định bắt buộc cài đặt virus	t và sử dụng phần mềm diệt	3 (25%)		9 (75%)	Quy định bắt buộc cài đ 12:37:09 16/06/2020	ặt và sử dụng phần mềm diệt virus	Resolved
- thi_truong	Quy dịnh kiểm tra cài đặt virus Kaspersky	và sử dụng phần mềm diệt	4 (31%)		9 (69%)	Quy định bắt buộc cài đ	iặt và sử dụng phần mềm diệt virus	
anm	Quy định cấu hình cập nh	ật Hệ điều hanh	1 (11%)		8 (89%)	12:37:09 16/06/2020		Resolved
default	Quy định máy tính phải jo khoản domain để đăng n	bin domain, và sử dụng tài hập máy tính	1 (1196)		8 (89%)	dev_test_group		^
	Quy định cài đặt và sử dụ	ng phần mềm	1 (13%)		7 (88%)	HUYHV-PC 1D15A98115CD	FEBBB1DAD9BB1D0575221BF95BD3	
	Quy định làm việc không	quá 20h	0 (0%)		3 (100%)	1 violation		Hide list »
	Quy định bắt buộc sử dụn	ıg phần mềm tường lửa	0 (0%)		5 (100%)	Quy định bắt buộc cài đ	ất và sử dụng phần mềm diệt virus	
	Quy định cấm sử dụng thi	iết bị USB	2 (40%)		3 (60%)	08:39:11 23/06/2020		Not resolved yet
	[KPI] Praxy Firefax, IE		1 (33%)		2 (67%)	thanking Virtual Roy 90700	00EA104BE0A07EC4BB977300C33710E20EEA	
	Quy định tự động khóa m	àn hình sau 5 phút	3 (50%)		3 (50%)	 1 violation 		Hide list »
	Quy định nghiêm cấm kết Internet.	t nối trực tiếp mạng	2 (100%)		0 (0%)	Quy định bắt buộc cài đ	iặt và sử dụng phần mềm diệt virus	
			0 (0%)		3 (100%)	10:38:35 09/06/2020		Not resolved yet
	Quy định nghiêm cấm lưu duyệt	i trữ mật khẩu trên trình	1 (50%)		1 (50%)	ybi		^
	Quy định bắt buộc cập nh	iật phần mềm diệt virus	1 (50%)		1 (50%)	DESKTOP-HHN2B1Q 59221	LA0A9179C465DCD95A4E6F38D2E78E2126DF	
	Display 16/16 result(s)					 1 violation 		Hide list »

Select a computer on the Computer List popup: Display a popup with detailed computer information, including: Computer, AgentID, IP Address, Domain, Group, Resolved and Detail (all types of violations of the machine).

📶 ΔΙΙΔΝΤ			ise Protect & Prevention	BLS	Setting	😚 EN 👻 root 主 👻
Violation statistic		List computers and units baseline violation	Collapse	e all 🙊	Detail information	×
Q Search for group		anm		^	COMPUTER	WIN7-32BIT-PC
		WIN7-32BIT-PC 5EF765BF9CE6221DA50F787ACB52C48AE32F	BD0C		AGENT ID	5EF765BF9CE6221DA50F787ACB52C48AE32FBD0C
🗖 root	Violation statistic bas	 3 violation 	Hi	ide list »	IP ADDRESS	
test	Violation type	Ouv định bắt buộc cài đặt và sử dụng phần mềm diệt viru:			DOMAIN	
		11:59:26 23/06/2020	Not reso	olved yet	GROUP	anm
no_group	VIDEATION TYPE				RESOLVED	Not yet
kdl	Quy dịnh bất buộc cái dật virus	Quy dinn bat buộc cai đặt và sử dụng phản mêm diệt viru: 12:37:09 16/06/2020	5 F	Resolved	DETAIL	Anne Mark Isla book a Al Mittada and down a bline address of Mittada an
kpt						Quy dinn bac buộc cai dặt và sử dụng phản mêm diệt virus DESCRIPTION
thi_truong		Quy định bắt buộc cài đặt và sử dụng phần mềm diệt viru: 12:37:09 16/06/2020	·	Resolved		N/A
anm						TIME
default		dev_test_group		~		12:37:09 16/06/2020
			D2			CONTENT Antivirus installation rule ("enabled": 0. "installed": 0)
		1 violation	Hi	ide list »		Quu định bắt huậc củi địt và cử dụng nhận mặm địệt vàoir.
						Quy dini bac buye car uae va su uqing pran men uier virus
		Quy định bắt buộc cài đặt và sứ dụng phần mềm diệt viru: 08:39:11 23/06/2020	Not resc	olved yet		N/A
						TIME
		thanhln9-VirtualBox 8C7C096A104B60A07FC4BB877299C221	19639FFA			12:37:09 16/06/2020
		 1 violation 	Hi	ide list »		CONTENT Antivirus installation rule ("enabled": 0. "installed": 0}
		Quy định bắt buộc cài đặt và sử dụng phần mềm diệt viru:	5			Anne alle the first of a shift of a shift of the section of the section of the section
		10:38:35 09/06/2020	Not reso	olved yet		Quy dinn bac bugc cai dạt và sử dựng phản mem diệt virus
						N/A
		уы		^		TIME
		DESKTOP-HHN2B1Q 59221A0A9179C465DCD95A4E6F38D2E	78E2126DF			11:59:26 23/06/2020
	Display 1/1 result(s)	 1 violation 	Hi	ide list »		CONTENT Antivirus installation rule ("enabled": 0, "installed": 0)
		where the part of the street of a second build of the street of the				

(4) Search

Individual search:

- Search by Unit: Display the entered unit and the list of corresponding child-level units.
- Violation type: Display the selected violation.
- Violated time



Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

3.9.	1.3U	nit	Tab

📶 АЛАНТ	Cảnh báo	IR Flow	Điều tra	Phản ứng Bảo vệ & Ngăn chặn	BLS	Cài đặt		© vi •	root 🚊 🔹
Thống kê vị phạm		4 \							🟳 Hưởng dẫn sử dụng
Q Tìm kiếm theo nhóm		-0-	Q. Loại vi phạm					30 ngày trước	٩
📮 root	Thống kê vi phạm baseling								
test	Loại vi phạm	Đơn vị							
	ĐƠN VỊ		ONLINE TRONG NGÂY	ONLINE TRONG 30 NGÀY GẦN NHẤT	ĐÃ XỬ LÝ	CHƯA XỮ LÝ	MÁY VI PHẠM	LUÂT VI PHAM	
kd	root		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	2	
- t kpt	default		1 (996)	11	2 (17%)	10 (83%)	12 (109%)	0	
thi_truong	anm		2 (50%)	4	0 (0%)	4 (100%)	4 (100%)	12	
anm	unknown		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
default	liennt_group2.1		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	ajiant_dev		0 (0%)	2	0 (0%)	2 (100%)	2 (100%)	0	
	dev_test_group		1 (50%)	2	0 (0%)	3 (100%)	3 (150%)	10	
	kpt		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	2	
0	vtt		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
3 —	vtt_knot_khcn_hgd_tt_kh_va_r	narketing	0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	OS31		0 (0%)	0	0 (0%6)	0 (0%)	0 (0%)	1	
	vtt_cskh-dng		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	okv2		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	vtt_vdi_normal		0 (0%)	0	0 (096)	0 (0%)	0 (0%)	1	
	vtt_khoi_cntt		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	ybi		0 (0%)	0	0 (0%)	0 (0%)	0 (0%)	1	
	Jame		0.0053	٨	0.(004)	0.000	0.0055		
	Hiển thị 50/68 kết quả								

The system supports performing the following features:

(1) Select the Top unit links

Move to Dashboard screen, list of top violations and top violation units

(2) The unit data tree of system

Display all system units with the parent-child hierarchy.

Enable to select units on the unit data tree to filter parent-child violation units.

(3) Unit Tab

Each type of violation is displayed with general information, including: Unit, Online in day, Online in last 30 days, Resolved, Unresolved, Violation computer and Violation rule.

Select the detail icon of the violation computer column on the list: A list of computers in each violation unit is displayed, including: unit name, computer name|Agent ID, violation list of each machine, violation time, violation state (violation fixed or not fixed).



📶 AJIANT	Alerts	IR Flow		Response	Protect & Prevention	BLS	Setting	🕃 EN 👻 root 😩 👻
Violation statistic		Violation inform	ation				Detail informatio	n X
Q. Search for group		anm					COMPUTER	ANM-CHUYENNT
	_	Violation rule	Violation computer				AGENT ID	E65744E6BCF118C7D9AF21C7A0893D744B9A8F05
🔲 root	Violation statistic bas						IP ADDRESS	
test	Violation type	Quy định cấu l	hình cập nhật Hệ điều hanh				DOMAIN	
		11:59:26 23/06	5/2020			Not resolved yet	GROUP	anm
no_group	UNIT	ANIM CHUVENNT I	F65744F6BCE118C7D0AE21	1074080307448048505			RESOLVED	Not vet
🖾 kdl	root	 14 violation 	200794200CP118C709AP21	LC19003301940380F03		Hide list »	DETAIL	
	default	02-08-26 22/0/	12020			Networkedust		Quy định nghiêm câm kết nôi trực tiếp mạng Internet.
thi_truong	anm	02:08:36 22/06	5/2020			Not resolved yet		Quy định nghiêm cấm kết nối trực tiếp mạng Internet
anm	unknown							TIME
default	liennt_group2.1	Quy định nghi	iêm cấm kết nối trực tiếp mạ	ang Internet.		Beechund		10:58:22 19/06/2020
	ajiant_dev	03:51:40 17/00	5/2020			Resolved		CONTENT
	dev_test_group	Ouv định nghị	êm cấm kết nối trực tiếp mạ	ang Internet.				Direct internet access: IP: 10.30.161.3780
	kpt	10:58:22 19/06	5/2020			Resolved		Quy định làm việc không quá 20h
	vtt							DESCRIPTION
	vtt_khoi_khcn_hgd_tt_kh	Quy định nghi 02:08:36 22/06	iêm câm kết nối trực tiếp mạ 5/2020	ang Internet.		Resolved		TIME
	vtt_cskh-dng							09:14:57 18/06/2020
	vtt vdi normal	[KPI] Proxy Fir	refox, IE			Perchand		CONTENT
	vtt khoi cntt	02140133 22/00	5/2020			Resolved		Do not work over 8PM I
	vbi	[KPI] Proxy Fir	efox, IE					[KPI] Proxy Firefox, IE
	ybi	06:27:48 19/06	5/2020			Resolved		DESCRIPTION
	bgg							N/A
	tbh	Quy định bắt t 01:24:02 23/06	buộc cập nhật phần mềm di 5/2020	iệt virus		Resolved		TIME 05/27-48 19/05/2020
	.hat		-					CONTENT
	Display 50/62 result(s)	Quy định làm 11:23:26 19/06	việc không quá 20h 5/2020			Resolved		IE proxy configuration: Proxy: Firefox proxy configuration: Proxy: Ty pe: 0

Select a computer on the Computer List popup: A popup with detailed computer information is displayed, including: Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (all types of violations of the machine).

📶 ΔΙΙΔΝΤ			Protect & Prevention BLS	Setting	🔇 EN 👻 root 😩 👻				
Violation statistic		Violation Information		Detail information	×				
Q Search for group		anm		COMPUTER	ANM-CHUYENNT				
		Violation rule Violation computer		AGENT ID	E65744E6BCF118C7D9AF21C7A0893D744B9A8F05				
📮 root	Violation statistic bas			IP ADDRESS					
test	Violation type	Quy định cấu hình cập nhật Hệ điều hanh		DOMAIN					
		11:59:26 23/06/2020	Not resolved yet	GROUP	anm				
no_group	UNIT	ANM.CHIVENNT F65744F6BCE118C7D04E21C740803D744B048E05		RESOLVED	Not vet				
- 🖸 kdl	root	• 14 violation	Hide list »	DETAIL					
E kpt	default	02-08-26 22 (06 2020	Networkedust		Quy dinh nghiem cam ket noi trực tiếp mặng Internet.				
thi_truong	anm	02308:36 22/06/2020	Not resolved yet		Quy định nghiêm cấm kết nối trực tiếp mạng internet				
anm	unknown				TIME				
default	liennt_group2.1	Quy định nghiêm cấm kết nối trực tiếp mạng Internet.	Developed		10:58:22 19/06/2020				
	ajiant_dev	03:51:40 17/06/2020	Resolved		CONTENT Direct internet access: IP-10.20.161.27-80				
	dev_test_group	Ouv đinh nghiêm cấm kết nối trực tiếp mang Internet.			Direct internet access: IP: 10.30.101.3780				
	kpt	10:58:22 19/06/2020	Resolved		Quy định làm việc không quá 20h				
	vtt				DESCRIPTION				
	vtt_khoi_khcn_hgd_tt_kh	Quy định nghiêm cấm kết nối trực tiếp mạng Internet. 02:08:36 22/06/2020	Resolved		TIME				
	vtt_cskh-dng				09:14:57 18/06/2020				
	vtt vdi normal	[KPI] Proxy Firefox, IE	Product.		CONTENT				
	vtt khoi cott	02340:35 22/06/2020	Resolved		Do not work over 8PM !				
	vhi	[KPI] Proxy Firefox, IE			[KPI] Proxy Firefox, IE				
	you	06:27:48 19/06/2020	Resolved		DESCRIPTION				
	DSS				N/A The				
	tbh	Quy định bắt buộc cập nhật phần mềm diệt virus 01:24:02 23/06/2020	Resolved		06:27:48 19/06/2020				
	had				CONTENT				
	Display 50/62 result(s)	Quy định làm việc không quá 20h 11:23:26 19/06/2020	Resolved		IE proxy configuration: Proxy: Firefox proxy configuration: Proxy: Ty pe: 0				

Select the icon detail of the rule violation column on the list: A violation list of the unit is displayed.



📶 AJIANT				vention BLS Setting 🕃 EN 🕶 root 🕒 👻
Violation statistic				Violation information X
Q Search for group		Q. Violation ty	ype	anm
				Violation rule Violation computer
C root	Violation statistic baseline			Const Rade Damastick Indiana and Athle
🖸 test	Violation type Unit			Quy olim ram việc không dùa zon
	UNIT	ONLINE IN DAY	ONLINE IN 30 DAYS RECENT	Quy định tắt cấu hình Remote Desktop
no_group	root	0 (0%)	0	Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus
Kol	default	0 (0%)	10	
-El thi truong	anm	2 (50%)	4	Quy định nghiêm cẩm kết nổi trực tiếp mạng Internet.
anm	unknown	0 (0%)	0	(KPI) Proxy Firefox, IE
default	liennt_group2.1	0 (0%)	0	Quy định cấu hình cận nhật Hệ điệu hạnh
	ajiant_dev	0 (096)	2	de la alcunata de contra como como como como como como como com
	dev_test_group	1 (50%)	2	Quy định cải đặt và sử dụng phần mềm
	kpt	0 (096)	0	Quy định nghiêm cấm lưu trữ mặt khẩu trên trình duyệt
	vtt	0 (0%)	0	
	vtt_khoi_khcn_hgd_tt_kh_va_marketing	0 (0%)	0	Quy định bắt buộc cập nhật phần mêm diệt virus
	vtt_cskh-dng	0 (0%6)	0	Quy dịnh kiểm tra cài đặt và sử dụng phần mềm diệt virus Kaspersky
	vtt_vdi_normal	0 (096)	0	Cuu định mấu tính nhải loin damain và cứ dụng tài khoản damain để đặng nhận máy tính
	vtt_khoi_cntt	0 (0%)	0	Quy ujini may unin pharjuni dumani, va su ujing tarkuluan uunani ue uang imppi may unin
	ybi	0 (096)	0	
	bgg	0 (0%)	0	
	tbh	0 (0%)	0	
	heri Display 50/82 result(s)	0.70551	0	
	Tubuh ani an unantial			

(4) Search

Individual search:

- Search by Unit: Display the entered unit and the list of corresponding child-level units.
- Violation time: Display the selected violation.
- Violated time

Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

9.1.2. Software statistics

The function of Software Statistics supports administrators to make statistics of installed software in a unit, including:

- View a list of installed software in a selected unit
- View details of Agent
- Export software.



🚺 AJIANT			otect & Prevention	BLS Setting		EN 🕶 root 📥 👻
Software statistic 4						📮 Guide line
Q Search for group	Q Search for	software	Installed		~	Date & Time
root test no.group kd kd thi_truong anm default	SOFTWARE NAME 7-Zip 16.04 Version 18.04 7-Zip 16.04 7-Zip 15.00 Version 18.00,00,0 7-Zip 19.00 (sf4) Version 19.00 Adobe Acrobat Reader DC Version 20.00.20042 Adobe Acrobat Reader DC (11 Version 20.00.20042 Adobe Acrobat Reader DC (12 Version 20.00.20042 Adobe Acrobat Reader DC (11 Version 20.00.20042 Adobe Acrobat Reader DC (11 Version 20.00.20042	0.012.20036) 0.012.20040)		NUMBER OF COMPUTERS 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	3 NUMBER OF UNITS 1 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	
	Version 20.006.20042 Adobe Acrobat Reader DC (19)	9.021.20049)		11 15	2 5	
	Version 20.006.20042 Adobe Acrobat Reader DC (19)	9.021.20056)		15 16	5	
	Display 50/388 result(s)					-

The system supports performing the following features:

(1) The unit data tree of system

Display all system units with the parent-child hierarchy.

Enable to select units on the unit data tree to filter software.

(2) Software list

Each software is displayed with general information, including: Software name, computer number and unit number.

TIAILA 🚺	Alerts	IR Flow	Investigation	Response	Protect & Preve	ention	BLS	Setting		③ EN ▼	root 🚊) -
Software statistic											P	Guide line
Q Search for group		Q Search for software				Installed			¥	Date & Time		٩
📮 root												
🖸 test											🖄 Export	
	SOFTWARE NAM	4E					NUMBER (OF COMPUTERS	NUMBER OF UNITS			
no_group	7-Zip 16.04						1		1			
	Version 16.04	1					1		1			
	7-Zip 19.00						17		5		°0	
thi_truong	Version 19.00	0.00.0					17		5			
anm	7-Zip 19.00 (x64	\$)					1		1			
default	Version 19.00)					1		1			
	Adobe Acrobat	Reader DC					12		5			
	Version 20.00	06.20042					12		5			
	Adobe Acrobat	Reader DC (19.012.20036)					15		5			
	Version 20.00	06.20042					15		5			
	Adobe Acrobat	Reader DC (19.012.20040)					15		4			
	Version 20.00	06.20042					15		4			
	Adobe Acrobat	Reader DC (19.021.20048)					11		2			
	Version 20.00	06.20042					11		2			
	Adobe Acrobat	Reader DC (19.021.20049)					15		5			
	Version 20.00	06.20042					15		5			
	Adobe Acrobat	Reader DC (19.021.20056)					16		5			
	Display 50/388 resu	lt(s)										

Select the icon detail of the violation computer column on the list: Display a list of computers in each unit, including: Unit Name, Computer Name/Agent ID and Version.



11ΔΙΙΔΝΤ	Alerts			ntion BLS	Setting	root 😩 👻
Software statistic				Software statistic (in:	stalled) - 7-Zip 19.00	×
Q Search for group		Q Search for software		ajiant_dev (display 1/1 e	computer)	^
root				ThanhLN-PC 73056DEFF - Version 19.00.00.0	E88EC1E5842A8081123911A7767E5EBD	
				anm (2 computer)		~
no_group	SOFTWARE N 7.7in 16.04	IAME		default (11 computer)		~
kdl	Version 16	1.04		dev_test_group (2 com	puter)	~
kpt	7-Zip 19.00			no.group (1 computer)		~
thi_truong	Version 19	1.00.00.0				
anm	7-Zip 19.00 (:	x64)				
default	Version 19	.00				
	Adobe Acrob	at Reader DC				
	Version 20	.006.20042				
	Adobe Acrob	at Reader DC (19.012.20036)				
	Version 20	1.006.20042				
	Adobe Acrob	at Reader DC (19.012.20040)				
	Version 20	1.006.20042				
	Adobe Acrob	at Reader DC (19.021.20048)				
	Version 20	0.006.20042				
	Adobe Acrob	at Reader DC (19.021.20049)				
	Version 20	1.006.20042				
	Adobe Acrob	at Reader DC (19.021.20056)				
	Display 50/388 re	esult(s)				

Select a computer on the Computer List popup: Display a popup with detailed computer information, including: Computer, AgentID, IP Address, Domain, Group and Software information (software name, version).

📶 ΔJIANT		Investigation Response Protect & Prevention	BLS Set	tting 🚯 EN 👻 root 🔔 👻
Software statistic		Software statistic (installed) - 7-Zip 19.00		Detail information ×
Q Search for group	Q. Search for softwar	ajiant_dev (display 1/1 computer)	^	Agent information
E mat		ThanhLN-PC 73056DEFE88EC1E5842A8081123911A7767E5EBD		AGENT ID 56F90482EFE7C27CBF15166CF7B0FB52683F0B4B
		- Version 13:00:000		GROUP anm
test		anm (display 2/2 computer)	^	DOMAIN (none)
no_group	SOFTWARE NAME 7-Zip 16.04	localhost.localdomain 56F90482EFE7C27CBF15166CF780FB52683F0B4B		IP ADDRESS 127.0.0.1 192.168.48.130
- E kdl	Version 16.04	- Version 19.00.00.0		192.168.187.130
E kpt	7-Zip 19.00	localhost.localdomain 6557920AF22389E3D45B38DC67C21BBF0DE7518F		COMPUTER NAME localdomain
thi_truong	Version 19.00.00.0	- Version 19.00.00.0		Colturas information
anm	7-Zip 19.00 (x64)	default (11 computer)	~	Solware mormation
default	Version 19.00			SOFTWARE 7-ZIP 19.00
	Adobe Acrobat Reader DC	dev_test_group (2 computer)	Ŷ	VERSION - Version 19.00.00.0
	Version 20.006.20042	no_group (1 computer)	~	List softwares in computer »
	Adobe Acrobat Reader DC (19.012.20			
	Version 20.006.20042			
	Adobe Acrobat Reader DC (19.012.20			
	Version 20.006.20042			
	Adobe Acrobat Reader DC (19.021.20			
	Version 20.006.20042			
	Adobe Acrobat Reader DC (19.021.20			
	Version 20.006.20042			
	Adobe Acrobat Reader DC (19.021.20			
	Display 50/388 result(s)			

Select the link [Software list in computer]: The system goes to the Agent Management screen and the popup of corresponding computer details is displayed.

Page | 153



TIAILA 🔟	Alerts IR F	ow Investigation	Response	Protect & Prevention	BLS	Setti	ing	③ EN ▼	root 😩 🔹
Software statistic		Software statistic (installed)) - 7-Zip 19.00				Detail informatio	n	×
Q Search for group	Q. Search for so	ajiant_dev (display 1/1 compute	er)			^	Agent information		
C root		ThanhLN-PC 73056DEFE88EC1E - Version 19.00.00.0	5842A8081123911A7767E5E	8D			AGENT ID	73056DEFE88EC1E5842A	8081123911A7767E5EBD
test		anm (2 computer)				~	GROUP DOMAIN	ajiant_dev	
no_group	SOFTWARE NAME 7-Zip 16.04	default (11 computer)				~	IF ADDRESS	10.0.2.15 127.0.0.1	
-O kdl	Version 16.04	dev_test_group (2 computer)				~	COMPUTER NAME	ThanhLN-PC	
th_truong	7-Zip 19.00	no_group (1 computer)				~	Software information	on	
anm	7-Zip 19.00 (x64)						SOFTWARE	7-Zip 19.00	
default	U Version 19.00						VERSION	- Version 19.00.00.0	
	Adobe Acrobat Reader DC						List softwares in con	anutar a	
	Version 20,006.20042						List soltwares in con	aputer »	
	Adobe Acrobat Reader DC (19.0	2.20							
	Version 20.006.20042								
	Adobe Acrobat Reader DC (19.0	2.20							
	U Version 20.006.20042								
	Adobe Acrobat Reader DC (19.0	1.20							
	U Version 20.006.20042								
	Adobe Acrobat Reader DC (19.0	1.20							
	Version 20.006.20042								
	Adobe Acrobat Reader DC (19.0)	1.20							
	Display 50/388 result(s)								

(3) Search

Individual search:

- Search by Unit: Display the installed software in the unit.
- Software name: Display the list of entered software.
- Search by state: Installed and uninstalled.
- Installation time.

Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

(4) Export

Select Export: The system will download the Export file with the same data as the one displayed on the screen.



10. Rules Correlation

10.1.1.Display List

The function allows users to enter or select search conditions to search for existing rules on the system and quickly deploy/undeploy/delete with rules.

- FILTER
- FILTER includes:
 - 6 Engines: Whitelist, Agg Trigger, Agg Action, Filter, Indicator and False-Positive.
 - Search textbox by fields: Name, content and description.
 - Update time
 - \circ Created by me
- 10.1.1.1. Filter by Engine
- Step 1: Choose 1 or more default Engines as follows:

TIAILA 🔟			IR Flow					Setting	G EN ≁ root	
earch rules	Agg Trigge	s 🔄 Agg Action »	CREATOR: Only me Se	arch name, content, description					Last 7 days	Cuide li
View column 👻 🛛 2	result(s) 01/	10/2020 10:57:18 - 08/10/2020 10:57:18								+ Add nev
 	PRIORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	
08/10/2020 10:48:02	1	rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	000
08/10/2020 10:42:26	1	liennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	a 0 â
splay 2/2 result(s)										
				Screer	h: Sear	rch rule				

• Step 2: Select Expand to add the Engine to filter.

TIAILA 🔟	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	☉ EN v ro	ot 😐 🗸
Search rules				_ /					📮 Guide line
ENGINE : White List	Agg Trigger Agg Action	Filter Indicator	False Positiv	e « CREATOR: (Only me Search name, c	content, description		Last 7 days	Q
View column ~ 2	result(s) 01/10/2020 10:49:53 - 08/10/2020 10:4	19:53							+ Add new
UPDATED TIME	PRIORITY NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	=
08/10/2020 10:48:02	1 rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	0 / ū
08/10/2020 10:42:26	1 liennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	8 / ū
Display 2/2 result(s)									
		Scree	n: Expa	nd seai	rch condi	tions			



When 2 or more Engines are selected, the display screen returns results filtered by the AND operation.

• Step 3: Check the Rule creator who is the user logging in the system.

arch rules										F	Guid
int : 📋 White List	 Agg Trigger 	🗋 Agg Action 🚿 CREATOR	: Only me Search	name, content, description					Last 7 days		Q
/iew.column 👻 🛛 2	result(s) 01/1	0/2020 10:57:18 - 08/10/2020 10:57:18								E	+ Add
	PRIORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	BULE TIPE Q	OPTIONAL TYPE Q	STATUS		
08/10/2020 10:48:02	1	rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	Ø	0 0
08/10/2020 10:42:26	1	liennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	ø	0 0
slay 2/2 result(s)											

Screen: Filter by Creator

• Step 4: Enter the name, content and description to search into the textbox.

TIAILA 🔟		Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	③ EN ★ ro	oot	. (
Search rules										F	Guide line
ENGINE : 🗍 White List	 Agg Trigger 	Agg Action	CREATOR: 🗌 Only me	Search name, content, description					Last 7 days		Q
View column 👻 🛛 2	result(s) 01/10/2	2020 10:57:18 - 08/10/2020 10:5	7:18								- Add new
	PRIORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	BULE TIPE Q	OPTIONAL TYPE Q	STATUS		
08/10/2020 10:48:02	1	rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	Ø	0 11
08/10/2020 10:42:26	1	llennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	ø	0 11
Display 2/2 result(s)											

- Step 5: Enter the information to search.
- Step 6: Click Search to display search results.

10.1.1.2. Select Column

Allow users to select the columns to display on the correlation screen.

Perform the following steps:

- Step 1: Click the View column combo box. The screen displays a list of selected columns in the form of a check box.
- Step 2: Click Select to the column names to display.



ĩ	J AJIANT	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	③ EN ▼	root 😐 👻
Search	rules									📮 Guide line
ENGINE :	White List Agg Trigger	□ Agg Action >>	CREATOR : Only me S	earch name, content, descriptio	n				Last 7 days	Q
View c	olumn V Z result(s) 01/10/2020 1	10:57:18 - 08/10/2020 10:57:18								+ Add new
Sea	rch in dropdown list		TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	1
	Updated time			Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	67 / ū
	Priority			Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	đ) / Ū
	Name									
	Tag									
	Category									
	Sub category									
	Creator									
	Rule type									
	Optional type									
	Status									

Screen: Options to add more columns

10.1.1.3. Quick Search Support

📶 ΔΙΙΔΝΤ		Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	③ EN ≠ roc	x 😩 -
Search rules										📮 Guide line
ENGINE : D White List	 Agg Trigge 	Agg Action 3	CREATOR: 🗌 Only me	Search name, content, description	R _{eete}				Last 7 days	Q
View column 👻 2	result(s) 01/3	0/2020 10:57:18 - 08/10/2020 10:5	7:18							+ Add new
UPDATED TIME	PRIORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	BULE TYPE Q	OPTIONAL TYPE Q	STATUS	
08/10/2020 10:48:02	1	rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	00
08/10/2020 10:42:26	1	liennt		Windows	MITRE_ATTACK	root	builder	custom	Undeployed	@ 0 D
Display 2/2 result(s)										
				Search	n by ru	le name				

• Step 1: Click the 🔍 icon to display the search bar.

📶 AJIANT	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	⊙ EN + roo	t 😐 -
Search rules									📮 Guide line
ENGINE : White List Agg Trigger	🗌 Agg Action 🚿 CREA	TOR: Only me	Search name, content, description					Last 7 days	Q
View column View loss of the view of the v	2020 11:05:32 - 08/10								+ Add new
UPDATED TIME PRIORITY	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	÷
08/10/2 pype to filter ×	Apply		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	0 / î
08/10/2020 10:42:26 1	liennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	6) / û
Display 2/2 result(s)									
		Scre	en: Quick	search	h by rule	name			

- Step 2: Enter the rule name to search.
- Step 3: Click Enter to display the search results.



10.1.1.4. Search by Category

Support quick search with 3 default types: Windows, Linux, and MacOS.

• Step 1: Click the 🔍 icon to display a list of Category.

Search rules Lister: In Mite List: Agg Trigger Agg Action W of Kinger (Mite Colspan) List 7 days View colspan List 7 days 2 result(s) oussociesticus: -enspanse List 7 days 3 urbic/tots Triel: Piloter Invie: Q Total Unix: Invie: Q Output: Invie: Q Output: Invie: Q Output: Invie: Q Output: Invie: Q List 7 days View colspan 2 result(s) output: Invie: Q Search name, content, description: C List 7 days View colspan Search name, content, description: Q Clast 7 days List 7 days View colspan= Q Output: Invie Q Search name, content, description: Q List 7 days View colspan= Q View colspan= Q Search name, content, description: Q List 7 days View colspan Divide Total													
Note: White Lut: Agg Action Agg Action Augr Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action Agg Action 	_												arch rules
Ver column v 2 reutici autosses -			Last 7 day					ition	Search name, content, descri	CREATOR: 📋 Only me	Agg Action	Agg Trigger	SINE : White List
View column V 2 result(s) allascass Llasks2 - wassassas Llasks2 - 4 industs TME PRORTY NAME Q Tag Cattoorr Q Matchine Q RLa THPE Q orrightLarke Q status - 0 #100/2020 0x4eb22 1 NaME Image Linux Matchine Builder custom Differiord Undeployed - 0#100/2020 0x4eb23 1 Image Linux Matchine Builder custom Differiord Undeployed - 0#100/2020 0x4eb24 1 Image Linux Matchine Builder custom Differiord Undeployed	-	1						/					
• 4 4564555 Tries #R08.177 FLAG TAG CATGODIF Q CREADOR Q RULT FRE Q BPRIDUIL TRE Q SSATURE • 04710/2020 1044502 1 mkle1 Image: Classical Control Contro	+									5:32	020 11:05:32 - 08/10/2020 11:0	result(s) 01/10/2	View column 👻 2
0k102020104802 1 rule1 Windows Linux MacOS builder custom Dudeployed 0k102020104226 1 lient Clear Apply builder custom Dudeployed	- 9			STATUS	OPTIONAL TYPE Q	BULETIPE Q	CREATOR Q	a sub caregory a	CATEGORY	TAG	NAME Q	PRIORITY	4 UPDATED TIME
08/10/2020 10:4226 1 lient Clear Apply builder custom Undeployed	00	ſ	Undeployed		custom	builder	cOS	Ом	C) Unux	Windows	rule1	1	08/10/2020 10:48:02
ter (m. 17) seculity)	0	F	Undeployed		custom	builder	Clear Apply				liennt	1	08/10/2020 10:42:26
spay 2/2 reducia										-			play 2/2 result(s)

Screen: Quick search by Category

- Step 2: Select the category to search.
- Step 3: Click Apply.

10.1.1.5. Search Sub Category

Support quick search by deployment type, including 3 default types: Metre ATT&CK, Malware, and Suspicious Behavior.

- Step 1: Click the 🔍 icon to display the search bar.
- Step 2: Select the sub category to search.
- Step 3: Click Apply.

10.1.1.6. Search Creator

- Step 1: Click the 🔍 icon to display the search bar.
- Step 2: Enter the creator name to search.
- Step 3: Click Apply.



10.1.1.7. Search Rule type

Search rules DHGNE: White List Agg Trigger Agg Action 🛞 c	REATOR : Only me	Search name, content, description						📮 Guide line
ENGINE: White List Agg Trigger Agg Action » c	REATOR : Only me	Search name, content, description						
							Last 7 days	Q
View column View								+ Add new
UPDATED TIME PRIORITY NAME Q	TAG	↑ CATEGORY Q	SUB CATEGORY	Q CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	
08/10/2020 10:42:26 1 liennt		Windows	MITRE_ATT&	O Advanced	O Builder	🥏 AIL	Undeployed	0 / ū
08/10/2020 10:48:02 1 rule1		Windows	MITRE_ATT&				Apply Dundeployed	D / Ū
08/10/2020 11:12:00 2 rules2		Windows	Malware	root	builder	custom	Undeployed	0/0
Display 3/3 result(s)								

Support quick search with 3 default types: Advanced, Builder and All.

- Step 1: Click the 🔍 icon to display the list of Rule types.
- Step 2: Click on the Rule type to search.
- Step 3: Click Apply.

10.1.1.8. Search Optional Type

Quick search support includes 3 default types: Built-in, Custom, All.

irch rules										1	🗖 Gu
NE: 📄 White List	 Agg Trigger 	Agg Action	CREATOR: 🗌 Only me	Search name, content, description					Last 7 da	ys	3
ew column 👻 3		2020 11 22 28 . 08/10/2020 11 2	3-20								+ 4
	PRIORITY	NAME O	TAG	★ CATEGORY Q	SUB CATEGORY Q	CREATOR Q	BULETIPE Q	OPTIONAL TYPE	STATUS		-
08/10/2020 10:42:26	1	liennt		Windows	MITRE_ATT&CK	root	O Built-in	C) Custom	IIA 🔕		0
08/10/2020 10:48:02	1	rule1		Windows	MITRE_ATT&CK	root				Apply	0
08/10/2020 11:12:00	2	rules2		Windows	Malware	root	builder	custom	Undeployed	9	0

- Step 1: Click the *c* icon to display the list of Optional types.
- Step 2: Click Optional type to search.
- Step 3: Click Apply.

10.1.1.9. Support Deploy/Undeploy for Multiple Rules

Search rules Last 7 digs Agg 7 tiggs Agg 7 tiggs Agg 7 tiggs Casch 0 m/m Search nume, content, description Last 7 digs Q Vere colum 3 result() 01502020 112323-045172020112323-045172020112323-045172020112323-0451720200112323-045172020112323-045172020112323-045172020112323-045172020112323-045172020112323-045172020112323-045172020112323-045172020112323-045172020112323-045172020112323-04517202011232-045172010-04 Rult rive Q Profer Vere colum Vere c	τιαίζα 🔟	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	🕙 EN 🔹 🛛 🔹 💌
DUDINE: In Mile Luit: Agg Trigger Agg Action Cascoli In Augus - Main Content, description Verer colum: 3 result() 010502000 1123204 - MAIN 20200 1123204 Seach name, content, description Image: Cascoli In Augus - Main 20200 1123204 Image: Cascoli In Augus - Main 20200 112304 Image: Cascoli In Augus - Main 20200 112304 </td <td>Search rules</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>📮 Guide line</td>	Search rules								📮 Guide line
View colum 3 result(s) 01362020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.02 - 04192020 1122.00 - 0419200 - 0419	ENGINE : White List Agg	Trigger Agg Action	>> CREATOR: Only me Sea	irch name, content, description					Last 7 days
1 Selected rule(s) 0 televel	View column ~ 3 result(s)	01/10/2020 11:23:29 - 08/10/2020 11:2	23:29					_	+ Add new
UPSATED TIME PROBITY NAME Data PLATESON Q DALESSON Q CREATING Q RALE FIRE Q OPTIONAL FIRE Q OPTIONAL FIRE Q 0 01/03/2020 10-42/20 1 Bernet Windows MITRE_ATTACK Rod Builder Custom Deployed 0 01/03/2020 10-46/20 1 rule1 Windows MITRE_ATTACK Rod Builder Custom Deployed 0 01/02/2020 11:250 2 rule2 Windows Mitree_ATTACK Rod builder Custom Duddployed 0 01/02/2020 11:250 2 rule2 Windows Mahware root builder Custom Duddployed	1 Selected rule(s)							6	Deploy Undeploy Delete Cancel
Image: Construction of the construction of	UPDATED TIME PRIOR	TY NAME Q	TAG	↑ CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE	STATUS
OR/10/2020 10448-02 1 rule1 Windows MITRE_ATT&CK root builder custom Om Undeployed 0 08/10/2020 11:12:00 2 rules2 Windows Mailware root builder custom Om Undeployed Spagby 1/2 result(s)	08/10/2020 10:42:26 1	liennt		Windows	MITRE_ATT&CK	root	builder	custom	Deployed
OB/10/2020 11:12:00 2 rules2 Windows Malware root builder Custom Om Undeployed Steploy 1/3 result(s)	08/10/2020 10:48:02 1	rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed
Display 3/3 result(s)	08/10/2020 11:12:00 2	rules2		Windows	Malware	root	builder	custom	Undeployed
	Display 3/3 result(s)								





- Step 1: Click on multiple check boxes with the same state as Deploy or Undeploy.
- Step 2: Click the Deploy/Undeploy button.
- Step 3: Select Deploy/Undeploy on the popup displayed to perform Deploy/Undeploy.

📶 ΔJIANT	Alerts IR Flow	Investigation	Response P	rotect & Prevention	BLS S	Setting	🕃 EN 👻 root 主 👻
Search rules							📮 Guide line
ENGINE : O White List O Agg Trigger	Agg Action 🚿 CREATOR : 🗌 Only me	Search name, content, description.					Last 7 days
View column V 3 result(s) 01/10/202	20 11:23:29 - 08/10/2020 11:23:29						+ Add new
1 Selected rule(s)						Deploy	Undeploy Delete Cancel
UPDATED TIME PRIORITY NAM	IME Q TAG	↑ CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS
2 08/10/2020 10:42:26 1 lier	nnt	Windows	MITRE_ATT&CK	root	builder	custom	C Deployed
08/10/2020 10:48:02 1 rule	le1	Windows	MITRE_ATT&CK	root	builder	custom	Undeployed
08/10/2020 11:12:00 2 rul	les2	UnDeploy Rule			× ^{jer}	custom	Undeployed
Display 3/3 result(s)		•					
		Do you want	to undeploy: : All rule	s selected ?			
		c	ancel				

10.1.2.Add New Rules Correlation

The function allows the user to configure a complete new correlation rule.

10.1.2.1. Overview

- * Engine: It includes 6 engines with detailed information respectively as follows:
 - Whitelist is a Stateless Engine to quickly remove events that the system does not need to handle. Events that match the whitelist rule will be dropped from the traffic.
 - Agg_trigger and Agg_action is a Stateful Engine that performs group of similar events. Each aggregate rule contains information about the clustering condition (similar event definitions) and aggregation interval (e.g. 30s, 1 minute, 2 minutes, etc.). Events that match the group condition are stored and only return an event with the quantity after a time interval. Events that do not match the group condition are returned immediately with a quantity of 1.
 - \circ ~ Filter is a Stateless Engine that filters the conditions to input into the indicator.
 - Indicator is a Stateful Engine that performs checks and statistics on events that satisfy the Filter. Indicator inputs are events that satisfy the Filter, and outputs are Indicator Events or Alert Events. Indicator supports operation of count



statistics in a unit of time (time. windows) of the same object, without repeating alerts for the same object in a predefined period of time. Each rule indicator only considers conditions of the same type, on the same system.

- FalsePositive engine is a Stateless Engine that eliminates false alerts. Each alert that matches the FalsePositive rule will be dropped.
- Debug/ Not Debug are two states of the engine. When performing a debug action, the returned log that is satisfied with the engine condition will be displayed on the Debug Correlation screen.
- Conditions: Each engine will support different conditions of Event, not Event, Alert Event, not Alert Event, Accumulate, Function and not Function. Details of conditions and use as follows:
 - Event: Used for event fields.
 - Not Event: Only created if there is an event.
 - Alert: Used for alert fields.
 - Not Alert: Consider how long there is no alert event.
 - Accumulate: Perform grouping of event conditions that satisfy the number of events which can create an alert.
 - Function: Be as functions. Notes: For boolean functions, the return value is True or False.
 - Not Function: For Not Function, the functions used are the same as Function.
 However, the return value will have True/False opposition results.
- Operator:
 - Basic operators include: =, !=, >, <, >=, <= .
 - Print: Check if a field's value is in the list.
 - On the left side of the operator: Name of field to be checked.
 - On the right side of the operator: List of values to be checked is separated by ",".
 - \circ $\,$ Contains: Check the value of a field that contains the value to be checked.
 - On the left side of the operator: Name of the field to be checked (this field needs to have an array or string value).
 - On the right side of operator: Value to be checked.
 - Assign: Assign the value of a field to a variable.
 - On the left side of the operator: Name of the field to be assigned.
 - On the right side of the operator: Name of the variable to be assigned.
 - Matches: Check if the value of a field matches a regex string.

Page | 161



- On the left side of the operator: Name of the field to be checked.
- On the right side of the operator: Regex string.
- Time configuration: Check the condition for a time interval, only in the Agg trigger, Agg action and Indicator engines.
- Count: Check if the number of events counted in a time interval satisfies the condition.
- Group/Ungroup: Allow user to quickly group or ungroup conditions in an AND or OR operator.

Instruction to Group/Ungroup:

- Group
 - Step 1: Click on the field to be grouped
 - Step 2: Select Group to detailed screen of the steps to perform grouping.
- Ungroup
 - Step 1: Click on the items to be groupe
 - Step 2: Select Ungroup to detailed screen of the steps to perform ungrouping.
- Restore: Automatically reset to the latest SAVE.
- Reset: Reset conditions (to the original state).
- Delete: Delete Condition that is in focus.
- 10.1.2.2. Instruction to add new correlation rule:
- Step 1: At the Correlation screen, select the Add New button → System displays the new rule creation screen.



τιαία 🔟	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	© en ▼	root 😩 🔹
Add new rule							Preview	Save & Deploy	Save
Category" Sub category" Windows V MITRE ATTAC Rule name" Type rule name RuleND Windows_MITRE_ATTACK_	κ Υ	Description" Type description					Priority" Tags		1
ENGINE Condition White Lat WINGROUF White Lat WINGROUF Age Action Fater	• Event							\$	Debug

Figure 1: Screen of new Rule correlation creation

• Step 2: Enter the information of the rule.

ory* Sub category*	Description*	Priority*
dows 🗸 MITRE ATT&CK 🗸	Type description	1
name*		Tags
e rule name		
EID Windows_MITRE_ATT&CK_		

Notes: Fields with the mark \ddagger are required fields.

• Step 3: Select Engine, enter conditions for Event, Not Event, Alert, Not Alert, Accumulate and Function respectively.

ENGINE	Condition 5. Chon	trạng thái debug	
🗐 White List			
🖭 Agg Trigger	uncadup 4. Add group/item hoặc xóa group		
≣් Agg Action	CELETE 1. Chon toán tử 2. Chọn điều kiện 🛄 Add Group + Add Item 🔋 Reiste		
T Filter			
ជា Indicator	6. Chọn Save 3. Chọn toàn tử		
False positive	RESTORE		
	C. Sector		
	Action 7.Chon action (nếu có)		

Figure 2: Detailed screen of new rule creation

- Step 4: Click on Save to save the condition or click on Cancel to return right after the newly saved step.
- Step 5: At Action, select the action to take on that engine.

Instruction to perform additional actions corresponding to each engine.



When the user completes the steps of condition creation and clicks Save, the screen will show the actions for each engine. Each engine will include corresponding actions. Agg_trigger engine will have no action.

Whitelist: Include 4 actions in the form of a check box, such as Drop, Switch to aggregate, Alert and Active List. The user is required to select 1 of these 4 actions. When the push log meets the condition, it will perform 1 of 4 actions that the user has selected. Function details of 4 actions as follows:

- Drop: Push logs that satisfy the condition will be dropped from the traffic.
- Switch to aggregate: Push logs that meet the conditions will be transferred to the aggregate engine for further processing.
- Alert: When adding key and value fields for alert, the push logs that meet the condition will display the alert in the Alert Management screen.
- Active list: The values of the active list will be added to the list displayed on the Active List screen.

Instruction to add fields for Alert/Active List action:

- Step 5.1: Click to select the action to add.
- Step 5.2: Click on the Edit button to enter the value for the field.
- Step 5.3: Enter a value for the field
- Step 5.4: Click on Save
- Step 5.5: Click on the Add icon to add a new field to the alert.

Add i	new rule ck to list					Preview Save & Deploy	Save
	Agg Trigger Agg Action	DELETE	AND Event		🔁 Add Group + Add Item 🗿 Delete		
T	Filter			= source_log ×	l≋ ∞ logon_type	×	
ងរែ	Indicator	SAVE					
0	False positive	RESTORE C RESET					
		Action					
		O Drop					
		O Move to a 1. Chọn acti	on			Chọn icor	n thêm/xóa bàn ghi
		Alert					Add Delete
			KEY		VALUE	1.01-01	ACTION
			severity	3. Nhập gia trị mong muon	1	4. Chộn lợc	on Save 🖻 ×
			object		27 28	2. 010	
			organization_group				0
		 Active ale 	rt				



Figure 3: Screen of new action creation for rule correlation

To delete the action just created, click on the Delete icon.

To edit the action, click on the Edit icon.

Notes: It is possible to create multiple actions with different fields depending on the purpose of the user.

Agg ation: At this engine, user can perform actions to add code.

Instruction to add a field for the actions of adding code:

- Step 5.1: Enter all conditions and operators. Click Save.
- Step 5.2: In the Action section, click the Enable action icon.
- Step 5.3: Enter the code content.
- Step 5.4: Select the Clear button \rightarrow The input of the code will be deleted totally.

Add new rule ← Back to list						Preview Sav	e & Deploy	Save
White List	UNGROUP				••••			
Bå Agg Action	DELETE						٢	
T Filter		Accumulate 👻	= agent_id	×	== v agent_id		×	
ដ្ឋា Indicator	SAVE							
False positive	RESTORE							
	() RESET							
	Action					Click icon enable action	Disable a	action Clear
	1							

Figure 4: Screen of new Code creation by Agg_action engine

Filter: Consist of 3 actions: Alert, Enrichment and Active List. The user can have one or more actions in the same engine. Function details of 3 actions as follows:

- Enrichment: Add field to Alert.
- \circ $\;$ Alert and Active List (same with Whitelist engine).

The Add, Edit and Delete actions for the Filter engine actions are similar to new addition of fields for the Whitelist engine.



Indicator: Be as Alert action. The Add, Edit and Delete actions for the Indicator engine actions are similar to new addition of fields for the Whitelist engine.

FalsePositive: Be as Enrichment Action. The Add, Edit and Delete actions for the FalsePositive engine actions are similar to new addition of fields for the Whitelist engine.

• Step 6: Click Save to save rule on the system. When the user wants to save on the system and deploy to correlation engine at the same time, click Save & Deploy.

Notes: When there is an error, user can click on Preview to view it.

10.1.3. Edit Correlation Rules

It allows user to edit the created rules with below implementation steps:

• Step 1: At the Rule Management screen, click on the Edit icon of the rule to edit.



• Step 2: At the Edit screen, enter the information to be edited.



📶 AJIANT		Alerts	IR Flow Inv	estigation	Response	Protect & Prevention	BLS	Setting	③ EN ▼	root 🛓 🔹
Search rules							_			📮 Guide line
ENGINE : 🗌 White List	Agg Trigger	Agg Action	Filter Indicator	False Positi	ve < CREATOR:	Only me Search name, o	ontent, description		Last 7 days	Q
View column 🗸 1	result(s) 01/10/2020 1	10:44:11 - 08/10/2020 10:44:11								+ Add new
↓ UPDATED TIME	PRIORITY NAME	E Q.	TAG	CATEGORY C	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE	STATUS	
08/10/2020 10:42:26	1 lienr	nt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	6) / Î
										/
		Fi	qure 6: De	tailed	inform	ation scr	een of ri	ule		

Notes: The fields of rule name, category and subcategory are non-editable fields.

• Step 3: Click on Save to save the rule on the system. When the user wants to save on the system and deploy to correlation engine at the same time, click on Save & Deploy.

For edit rules but only Save, user must click on Redeploy at the Rule Management screen for the new rule to take effect on the system.

Notes: When there is an error, user can click on Preview to view it.

10.1.4. Delete Correlation Rule

📶 ΔJIΔΝΤ		Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	③ EN ▾ ro	ot 😩 🗸
Search rules										📮 Guide line
ENGINE : Utite List	Agg Trigger	Agg Action	CREATOR: Only me Sea	arch name, content, description					Last 7 days	٩
View column 🗸 🖌 re	esult(s) 01/10/202	20 10:46:59 - 08/10/2020 10:46	:59							+ Add new
↓ UPDATED TIME	PRIORITY NA	AME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	
08/10/2020 10:42:26	1 lie	ennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	đ / ū
Unpoy (A result)										7

Instructions to delete a rule as follows:

Page | 167

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Step 1: Click on the Delete icon at the rule to delete.
- Step 2: The screen displays a confirmation notification to delete, select CANCEL/OK.

📶 ΔΙΙΔΝΤ	Alerts IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	© en ▼	root 😦 👻
Search rules								📮 Guide line
ENGINE : White List Agg Trigger	Agg Action 🔉 CREATOR : 🗌 Only me	Search name, content, descripti	on				Last 7 days	Q
View column V 1 result(s) 01/10/2020 10:465	i9 - 08/10/2020 10:46:59							+ Add new
UPDATED TIME PRIORITY NAME Q	TAG	CATEGORY C	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	<i>x</i>
08/10/2020 10:42:26 1 liennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	8 / ū
		Delete Rule	u want to remove rul	e : liennt ?	×			

Figure 7: Confirmation popup to delete rule

If OK is selected, the selected rule will disappear from the display screen.

📶 AJIANT		Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	😚 EN 🔹 🛛 🔹 💌
Search rules									📮 Guide line
ENGINE : O White List	Agg Trigger	Agg Action	CREATOR : Only me	Search name, content, description	h				Last 7 days
View column	result(s) 01/10/20	020 10:49:53 - 08/10/2020 10:49	:53						+ Add new
2 Set and rule(s)								•	sploy 💿 Undeploy 👔 Delete Cancel
UPDATED TIME	PRIORITY P	NAME Q	TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS
08/10/2020 10:48:02	1 1	rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed
08/10/2020 10:42:26	1 (liennt		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed
	_		•						

Figure 8: Screen of function to delete multiple rules at the same time

Instructions to delete multiple rules:

• Step 1: Click on the rules to delete (It is possible to delete all by clicking on Select all rules).



• Step 2: The screen displays a confirmation notification to delete, select CANCEL/OK.

11ΔΝΤ	Alerts IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	⊙ EN ≠ root	t 😩 -
Search rules								📮 Guide line
ENGINE: O White List O Agg Trigger	🗌 Agg Action 🚿 CREATOR: 🗌 Only me	Search name, content, description					Last 7 days	Q
View column View column O1/10/2020 10	0:49:53 - 08/10/2020 10:49:53							+ Add new
2 Selected rule(s)								Cancel
UPDATED TIME PRIORITY NAME	Q TAG	CATEGORY Q	SUB CATEGORY Q	CREATOR Q	RULE TYPE Q	OPTIONAL TYPE Q	STATUS	
🔽 08/10/2020 10:48:02 1 rule1		Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	
2 08/10/2020 10:42:26 1 liennt	t	Windows	MITRE_ATT&CK	root	builder	custom	Undeployed	
		Detet Kue De you want to	remove Multi-rule : / Cancel Debrt	II rules selected ?				

Figure 9: Confirmation screen to delete

Select OK, all rules will be removed from the display screen. Select CANCEL, the selected action will be cancelled.

3.10 Protect & Prevention

10.1.5. Application Control

The Application Control function allows configuring apps/ processes that will be blocked under the user's machine and do not allow executing. The app/process is identified based on the hash (MD5, SHA1 and SHA256) or the path.

10.1.6.Display list of blocked apps/ processes

Click on the Protect & Prevention tab \rightarrow select Application control to display all applications/processes under the user's machine and not allowed to be used.



TIAILA 🚺			Protect & Prevention				root 😩 👻
Application Control							📮 Guide line
Agent updated: 0 Time updated: 2020/10/12 10:04:45	5			Q Type an	d enter to filter	① Import	✓ + Add new
OBJECT		TYPE		DESCRIPTION		CREATED TIME	
Haitest		PATH		Nguyễn Thị Duyên	hải thêm ngày 25/09	2020/09/25 18:42:22	ŵ
notepad.exe		PATH		tttt		2020/09/23 10:21:34	Û
*procmon.exe		PATH		test		2020/09/23 10:21:20	Û
procmon.exe		PATH		test		2020/09/23 10:20:52	ŵ
B5486691F78A935A222C1BB8ABB800AF		HASH		chrome		2020/09/22 17:48:28	ŵ
C:\Program Files (x86)\Google\Chrome\Applic	cation\chrome.exe	PATH		chrome		2020/09/22 17:42:27	ŵ
C:\Program Files\Google\Chrome\Application	n\chrome.exe	PATH		chrome		2020/09/18 18:52:13	û
6B6BE7FC1360B8E70525459BB9AA91E9		HASH		chrome		2020/09/18 18:51:45	ŵ
*chrome.exe		PATH		ttt		2020/09/18 18:44:33	ŵ
nga		PATH		123123123123		2020/09/09 15:20:28	û
test22		PATH		1		2020/08/20 11:01:11	ŵ
test21		PATH		1		2020/08/20 11:00:53	ŵ
test20		PATH		1		2020/08/20 11:00:47	ŵ
test19		PATH		1		2020/08/20 11:00:41	ŵ
test18		PATH		1		2020/08/20 11:00:34	Û
test17		PATH		17		2020/08/20 10:57:25	ŵ
test16		PATH		16		2020/08/20 10:57:17	Û
test15		PATH		15		2020/08/20 10:56:53	ŵ
test14		PATH		14		2020/08/20 10:56:46	Û
test13		PATH		13		2020/08/20 10:56:38	Û
test12		PATH		12		2020/08/20 10:56:27	ŵ
test11		PATH		11		2020/08/20 10:55:43	ΰ

Screen of blocked app/ process list

10.1.6.1. Search for blocked apps/processes

User can search by hash code or path of blocked apps.

Application Control				🟳 Guide line
Agent updated: 0 Time updated: 2020/10/12 10:04:45		Q notepad	× 🛧 Import V	+ Add new
OBJECT	TIPE	DESCRIPTION	CREATED TIME	1.0
notepad.exe	PATH	tttt	2020/09/23 10:21:34	Û

Screen of searching for blocked apps/ processes

10.1.6.2. Add new blocked apps/ processes

Click on Add new to add a new blocked app/ process. The user can choose to block by path or hash code (MD5, SHA1, SHA256).

Application Control				📮 Gui	de line
Agent updated: 0 Time updated: 2020/10/12 10:04:45			Q Type and enter to filter		anew
OBJECT		TYPE	DESCRIPTION	CREATED TIME	1
Haitest		PATH	Nguyễn Thị Duyên hải thêm ngày 25/09	2020/09/25 18:42:22	ŵ
*notepad.exe		PATH	tttt	2020/09/23 10:21:34	ŵ
procmonJexe				2020/09/23 10:21:20	ŵ
procmon.exe	Add New		×	2020/09/23 10:20:52	Û
B5486691F78A935A222C1BB8ABB800AF				2020/09/22 17:48:28	Û
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	Object Ty	rpe value object		2020/09/22 17:42:27	ŵ
C:\Program Files\Google\Chrome\Application\chrome.exe	Туре	PATH HASH		2020/09/18 18:52:13	ŵ
6B6BE7FC1360B8E70525459BB9AA91E9	Description Ty	pe description		2020/09/18 18:51:45	ŵ.
C *chrome.exe				2020/09/18 18:44:33	ŵ.
🗆 nga				2020/09/09 15:20:28	ŵ
test22				2020/08/20 11:01:11	ŵ
test21				2020/08/20 11:00:53	ŵ
test20				2020/08/20 11:00:47	Û.
test19		Cancel		2020/08/20 11:00:41	ŵ
test18		PATH	1	2020/08/20 11:00:34	ŵ

Screen of adding new blocked apps/ processes



10.1.6.3. Add new app/ process from existing file

Users can add new blocked applications/processes from the .csv file according to the available template to the current application list.

Click Import, select the path to the file to upload and click Open, the system will automatically add a list of applications to block on the system.

Application Control				📮 Guide line
Agent updated: 0 Time updated: 2020/10/12 10:04:45		Q Type and enter to filter	1 import V	+ Add new
OBJECT	TYPE	DESCRIPTION	Import 🗘	
procmon.exe	РАТН	test	Download template	û
B5486691F78A935A222C1BB8AB8800AF	HASH	chrome	2020/09/22 17:48:28	ũ 📗

Screen of adding new apps/ processes from the existing file

10.1.6.4. Remove blocked apps/ processes from the list

The system supports deleting 1 or more blocked applications.

Click on each application to delete and click the Delete icon, or click the checkbox at the top of each application and click the Delete button.

Application Control	Application Control							
Agent updated: 0 Time updated: 2020/10/12 10:04:45	Q Type and enter to filter	1 Import	+ Add new					
Selected application (3) Pelete Cancel								
08JECT	TVPE		DESCRIPTION	CREATED TIME				
procmon.exe	PATH		test	2020/09/23 10:20:52				
B5486691F78A935A7 C1BBBABB800AF	HASH		chrome	2020/09/22 17:48:28				
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	РАТН		chrome	2020/09/22 17:42:27				
C:\Program Files\Google\Chrome\Application\chrome.exe	РАТН		chrome	2020/09/18 18:52:13				
6868E7FC136088E705254598B9AA91E9	Delete Object		×	2020/09/18 18:51:45				
C *chrome.exe				2020/09/18 18:44:33				
🗌 nga		D	123	2020/09/09 15:20:28				
test22	Do you want to remove Objects ?			2020/08/20 11:01:11				
test21				2020/08/20 11:00:53				
test20	Cancel Delete			2020/08/20 11:00:47				
test19	rain a		1	2020/08/20 11:00:41				

Screen of removing blocked apps/ processes

10.1.6.5. Update stream to the number of agent machines with the new list successfully updated

After the user adds/modifies/deletes the list of processes on the interface, the system will update this list below agents according to the agent file update stream (every 3-minute interval). The agent receives the new configuration, generates a log with eventID = 101 and pushes it to the server, displayed on the Event Search screen. Then the system will automatically update the number of agents that have updated the new configuration list on the Application Control screen.





10.1.6.6. Endpoint Firewall

Purpose: The Endpoint Firewall function allows configuring connections that will be blocked under the user's machine, including blocking by ip, port, or both ip and port, supports TCP, UDP and ICMP protocols, IPv4, IPv6, inbound and outbound connection.

10.1.6.7. Display list of blocked connections

Click on the Protect & Prevention tab \rightarrow Select Endpoint Firewall to display the entire list of blocked connections.

Endpoint Firewa	II						📮 Guide line
94 result(s)	Agent updated: 0 Time updated: 2020/10/01 14:01:06				Q Type and enter to filter	⊥ Import v	+ Add new
□ P	PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION		
1.1.1.82	33	INBOUND	тср	2020/04/16 09:21:35	import from file		û
1.1.1.92	33	ALL	ICMPV6	2020/04/16 09:21:35	import from file		Û
1.1.1.94	33	INBOUND	TCP	2020/04/16 09:21:35	Import from file		ŵ
1.1.1.95	33	INBOUND	UDP	2020/04/16 09:21:35	import from file		Û
1.1.1.99	33	OUTBOUND	ALL	2020/04/16 09:21:35	import from file		û
1.1.1.3	33	INBOUND	UDP	2020/04/16 09:21:35	import from file		Û
1.1.1.23	33	ALL	ICMPV6	2020/04/16 09:21:35	import from file		ŵ
1.1.1.37	33	INBOUND	TCP	2020/04/15 13:23:37	import from file		û
1.1.1.69	33	OUTBOUND	ALL	2020/04/15 13:23:37	import from file		û
1.1.1.74	33	ALL	ICMPV6	2020/04/15 13:23:37	import from file		û
1.1.1.80	33	ALL	ICMPV6	2020/04/15 13:23:37	import from file		û
1.1.1.18	33	OUTBOUND	ALL	2020/04/15 13:23:37	Import from file		ŵ
1.1.1.21	33	INBOUND	UDP	2020/04/15 13:23:37	import from file		û
1.1.1.33	33	INBOUND	UDP	2020/04/15 13:23:37	Import from file		ŵ
1.1.1.70	33	INBOUND	TCP	2020/04/15 13:23:37	import from file		Û
1.1.1.7	33	INBOUND	TCP	2020/04/15 13:23:37	Import from file		ŵ
1.1.1.63	33	OUTBOUND	ALL	2020/04/15 13:23:37	import from file		ŵ
1.1.1.93	33	OUTBOUND	ALL	2020/04/15 13:23:37	import from file		ŵ
1.1.1.68	33	ALL	ICMPV6	2020/04/15 13:23:37	import from file		û
1.1.1.72	33	INBOUND	UDP	2020/04/15 13:23:37	import from file		ŵ
1.1.1.77	33	INBOUND	UDP	2020/04/15 13:23:37	import from file		Û
1.1.1.78	33	INBOUND	UDP	2020/04/15 13:23:37	import from file		ŵ
httpBIoplay060/947660lt(s)							Back to top 🔨

Screen of blocked connection list

10.1.6.8. Search blocked connections

Users can search by IP address and built-in port.

τιαίζα 🔟	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting	0	EN 👻	root	• •
Endpoint Firewall											🟳 Guide line
1 result(s) Agent updated: 0 Time	updated: 2020/10/01 14:01:06					Q 172		×	1 Import	~	+ Add new
□ P	PORT	DIRECTION	PROTOCOL	CREATED TIME		DESCRIPTIC	DN				
203.113.172.0	0	ALL	ALL	2020/03/30 18:2	23:25	g					û
Display 1/1 result(s)											

Screen of searching for blocked connections

10.1.6.9. Add new blocked connections

Click the Add new button, enter the information on the popup to add a new blocked connection with the following:

- IP: IP address to block
- Port: Port to block, if blocking all ports, enter 0



Direction: Inbound, outbound and All (block both directions) Protocols: ICMP, TCP, UDP, ICMPV6 and ALL.

Endpoint Firew	all					📮 📮 Guide line
94 result(s)	Agent updated: 0 Time updated: 2020/10/01 14:0	01:06			Q Type and enter to filter	🟦 Import 🗸 🕂 Add new
D IP	D PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION	-
1.1.1.123	33	INBOUND	TCP	2020/09/25 18:06:40	Hål test	ū
4.6.7.8	0	Add New			×	ū
1.3.5.9	13					ŵ
1.1.1.34	33	IP	Tuno in			ŵ
1.1.1.66	33		Type Ip			ŵ
1.1.1.64	33	Port	Type port			Ē
1.1.1.82	33	Direction	ALL		~	ũ
1.1.1.92	33	Protocol	ALL		~	ŵ
1.1.1.94	33	Description of				ŵ
1.1.1.95	33	Description	Type description			ŵ
1.1.1.99	33					ŵ
1.1.1.3	33	1				ŵ
1.1.1.23	33					ũ
1.1.1.37	33					ŵ
1.1.1.69	33	1		Cancel Add		ū
	22		LATING R	55557521121555555	in and here the	÷

Screen of adding new blocked connection address

10.1.6.10. Add new blocked connection from existing file

Users can add new blocked apps/ processes from the .csv file according to the available template to the current application list.

Click Import, select the path to the file to upload and click Open, the system will automatically add a list of applications to block on the system.

Endpoint Firewa	u		P 01					
94 result(s)	Agent updated: 0 Time updated: 2020/10/01 14:01:06				Q Type and enter to filter	1 import	• •	+ Add new
D IP	PORT	DIRECTION	PROTOCOL	CREATED TIME	DESCRIPTION	Import	£	-
1.1.1.123	33	INBOUND	TCP	2020/09/25 18:06:40	Hål test	Download template	Ð	û

Screen of adding new apps/ processes from existing file

10.1.6.11. Delete blocked connection from the list

The system supports deleting 1 or more blocked connections.

Click on each connection to delete and click the Delete icon, or click on the checkbox at the top of each connection and click the Delete button.

	Endp	oint Firewall										🟳 Guide line
3	94 res	ult(s)	Agent updated: 0	Time updated: 2020/10/01 14:01:06					Q Tyr	be and enter to filter	⊥ Import ~	+ Add new
	Selec	Selected item(s) (3) Eleter Cancel										
1	0	IP		PORT	DIRECTION	PROTOCOL	CREATED TIME			DESCRIPTION		1
		1.1.1.123		33	INBOUND	TCP	2020/09/25 18:06:40			Håi test		
		4.6.7.8		0	ALL	ALL	2020/09/18 18:44:55			h		
		1.3.5.9		13	ALL	ALL	2020/08/12 09:35:21			Add new application auto		
Ľ	- 0-	1.1.1.34		33	ALL	ICMP	2020/04/16 09:21:35			import from file		
		1.1.1.66		33	INBOUND	Delete Object		3	×	import from file		
		1.1.1.64		33	INBOUND	•				import from file		
		1.1.1.82		33	INBOUND		Do you want to remove objects ?			import from file		
		1.1.1.92		33	ALL		bo you want to remove objects :			Import from file		
		1.1.1.94		33	INBOUND				-	Import from file		
		1.1.1.95		33	INBOUND		Cancel Delete			import from file		
		1.1.1.99		33	OUTBOUND	ALL	2020/04/16 09:21:35		-	import from file		

Screen of deleting blocked connection



10.1.6.12. Update stream to the number of agent machines with the new list successfully updated

After the user adds/modifies/deletes the list of connections on the interface, the system will update this list below agents according to the agent file update stream (every 3-minute interval). The agent receives the new configuration, generates a log with eventID = 201 and pushes it to the server, displayed on the Event Search screen. Then the system will automatically update the number of agents that have updated the new configuration list on the Application Control screen.