

“Giải pháp phát hiện và xử lý nhanh chóng, chủ động trước các nguy cơ tấn công mạng giúp các tổ chức, doanh nghiệp đảm bảo an toàn thiết bị đầu cuối một cách toàn diện.”

THÁCH THỨC

Ngày nay, các tổ chức, doanh nghiệp liên tục gặp khó khăn với việc phát hiện, xác định, điều tra và giảm thiểu các cuộc tấn công nâng cao vào hệ thống. Các công nghệ phòng chống mã độc truyền thống như antivirus dựa trên chữ ký đang bị vượt qua một cách cố ý bởi những kẻ tấn công chuyên nghiệp có trình độ cao với các bộ công cụ tấn công, phần mềm độc hại được tùy chỉnh và hướng mục tiêu cụ thể.

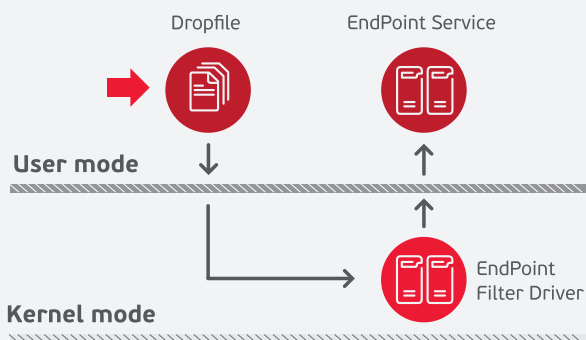
GIẢI PHÁP

Viettel Endpoint Detection & Response (VCS-aJiant) là giải pháp phát hiện và chống tấn công có chủ đích lớp endpoint được xây dựng dựa trên các công nghệ mới nhất trên thế giới, phù hợp với mọi mô hình tổ chức và doanh nghiệp, đảm bảo loại bỏ tất cả các nguy cơ bị khai thác và chiếm quyền điều khiển.

TÍNH NĂNG CHÍNH

Giám sát hành vi mức driver

Sử dụng công nghệ Filter Driver giám sát tất cả các hành vi liên quan đến File, Process, Memory, Registry, Network,... trên máy tính người dùng và máy chủ. Các hành vi nghi ngờ được đẩy về thành phần backend phân tích tập trung.



Phân tích tập trung

Sử dụng nhiều công nghệ như phát hiện bất thường theo IOC/IOAs, mô hình hóa hành vi, xâu chuỗi các mối quan hệ giữa các đối tượng nghi ngờ và làm nổi bật bất thường, mã độc chưa từng được biết trên thế giới.

Thiết lập chính sách ATTT

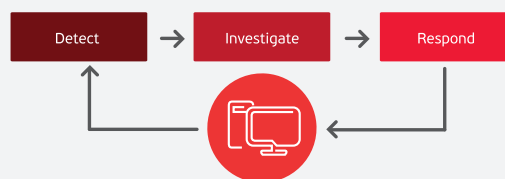
Máy tính được thiết lập chính sách An toàn thông tin sẽ giảm thiểu nguy cơ bị lây nhiễm mã độc. Giải pháp hỗ trợ một số chính sách An toàn thông tin như: kiểm soát thiết bị ngoại vi, cung cấp kênh remote an toàn (Security Helpdesk...).

GIÁ TRỊ MANG LẠI

- Giám sát các hành vi bất thường theo chuẩn MITRE & ATT&CK.
- Phân tích & truy vết chuyên sâu bằng khả năng biểu diễn kill chain map trực quan.
- Giám sát tuân thủ chính sách của tổ chức.
- Phản ứng nhanh chóng, chủ động, tự động.
- Nắm bắt trực quan tình hình an ninh mạng của tổ chức ở lớp thiết bị đầu cuối.
- Tiết kiệm thời gian xử lý sự cố, giảm thiểu tỷ lệ cảnh báo sai (false positive).
- Quản trị hiệu quả quy trình xử lý sự cố thông qua các chỉ số thời gian.

Phản ứng sự cố nhanh chóng, kịp thời

Luồng nghiệp vụ điều tra tấn công được thiết kế khép kín, hỗ trợ phát hiện và phân tích các dấu hiệu bất thường trên giao diện điều khiển. Cung cấp chức năng Forensic sâu trên endpoint. Ngay khi xác minh được bất thường, cung cấp các công cụ gỡ bỏ mã độc diện rộng



Giao diện quản trị thân thiện

Giao diện điều khiển được thiết kế tối ưu nhất cho đội ngũ vận hành dễ dàng giám sát được hệ thống mà không phải thực hiện nhiều thao tác.



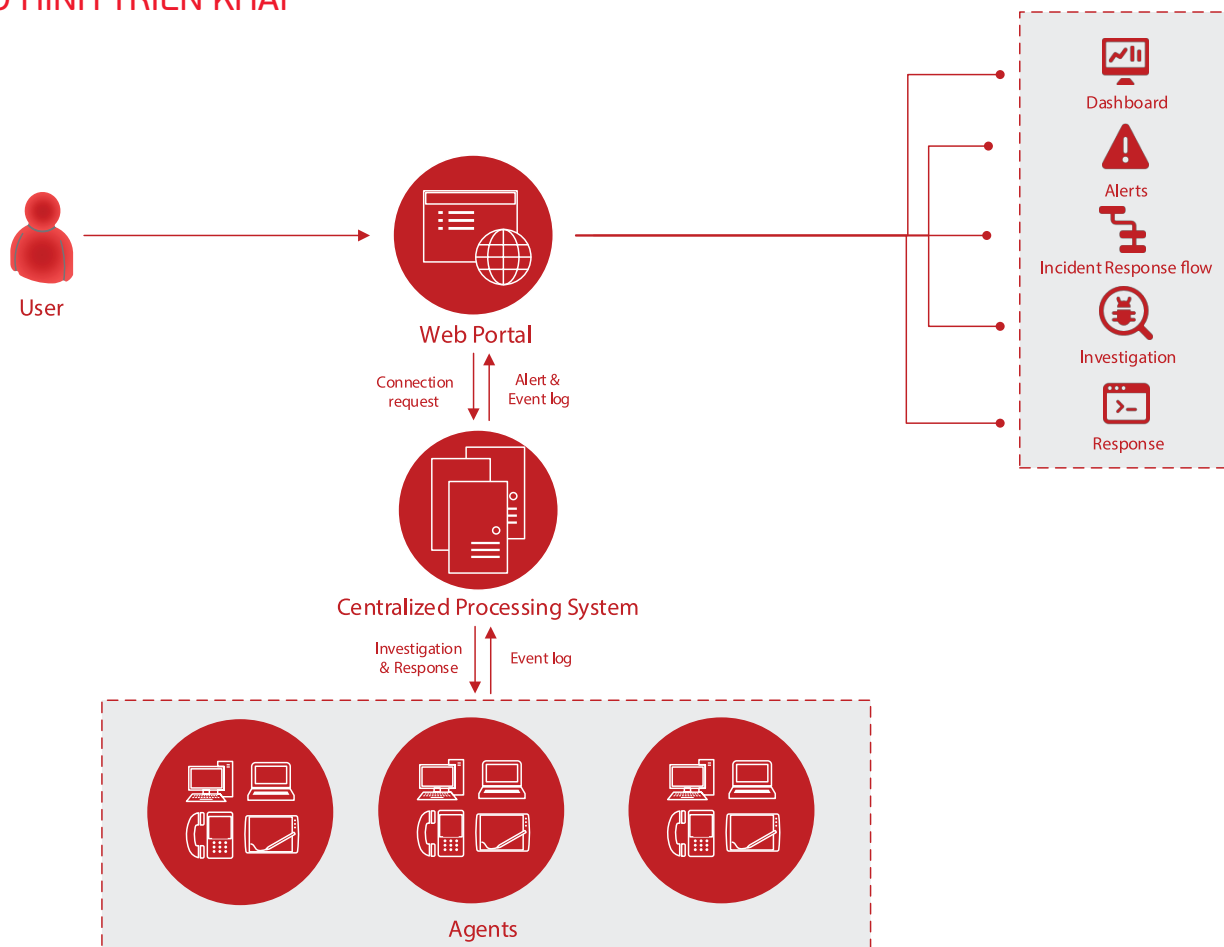
Hoạt động nhẹ nhàng

Thiết kế tối ưu với người dùng, hoạt động nhẹ nhàng và hoàn toàn trong suốt

Tích hợp và hỗ trợ đa nền tảng

Tích hợp với các nguồn tri thức bên thứ ba như Threat Intelligence, Advanced Malware Analysis, SOAR, SIEM. Hỗ trợ đa nền tảng: Windows, Linux, MacOS.

► MÔ HÌNH TRIỂN KHAI



Hệ thống VCS-aJiant bao gồm 03 thành phần chính:

- 

Agents
Là thành phần được cài đặt trên từng máy tính, có nhiệm vụ giám sát các dấu hiệu bất thường trên máy tính, gửi log về server tập trung.
- 

Cụm máy chủ xử lý tập trung và lưu trữ
Là thành phần xử lý dữ liệu do Agent gửi về, đóng vai trò chính trong việc phân tích và xử lý dữ liệu theo thời gian thực.
- 

Web Portal
Là thành phần người quản trị sẽ sử dụng để theo dõi, giám sát và phân tích các thông tin của hệ thống.

GIẢI PHÁP

VCS-aJiant kết hợp đầy đủ tính năng của Giải pháp phát hiện & chống tấn công có chủ đích lớp endpoint (Endpoint Detection & Response - EDR) và Giải pháp bảo vệ & phòng chống mã độc trên toàn bộ hệ thống (Endpoint Protection Platform - EPP). Được xây dựng dựa trên công nghệ tiên tiến trên thế giới, phù hợp với mọi mô hình tổ chức & doanh nghiệp, VCS - aJiant đảm bảo loại bỏ tất cả nguy cơ bị khai thác & chiếm quyền điều khiển cũng như đáp ứng đầy đủ nhu cầu phòng chống mã độc tại doanh nghiệp & tổ chức, nhằm phản ứng, ngăn chặn, bảo vệ một cách triệt để toàn bộ hệ thống mà không ảnh hưởng đến người dùng. Đồng thời, tự động hóa tác vụ, từ đó tiết kiệm thời gian & giảm thiểu thao tác điều hành trong hệ thống.

TÍNH NĂNG CHÍNH	MÔ TẢ TÍNH NĂNG	PHIÊN BẢN ĐÁP ỨNG		
		EDR	EPP	EDP
1. Tính năng hỗ trợ theo dõi, thống kê				
Agent Management	Quản lý thông tin máy trạm, hỗ trợ gỡ cài đặt agent từ xa	✓	✓	✓
Group Management	Cho phép tạo nhóm và phân loại máy trạm theo nhóm định nghĩa	✓	✓	✓
Account Management	Hỗ trợ tạo tài khoản người dùng, phân quyền theo vai trò	✓	✓	✓
2. Tính năng ngăn chặn sự cố				
Application IOCs Block	Cấu hình chặn ứng dụng độc hại hoạt động trên máy trạm	✓		✓
Network IOCs Block	Cấu hình chặn kết nối độc hại từ máy trạm	✓		✓
3. Tính năng cảnh báo và xử lý cảnh báo				
Detection	Phát hiện dấu hiệu tấn công nâng cao APT theo MITRE ATT&CK	✓		✓
Alert Management	Theo dõi và quản lý cảnh báo	✓		✓
Incident Response Flow	Cho phép điều tra phản ứng trên một giao diện duy nhất	✓		✓
4. Tính năng điều tra				
Process Analysis	Phân tích tiến trình đang chạy từ xa trên máy mục tiêu	✓		✓
Event Search	Tìm kiếm log event trên toàn bộ máy trạm	✓		✓
Deploy Tools	Quản lý & triển khai công cụ điều tra/xử lý sự cố trên máy trạm trong tổ chức	✓		✓
Containment	Hỗ trợ cô lập (network, process) tạm thời các máy phục vụ điều tra	✓		✓
5. Tính năng phản ứng nhanh				
Live Response	Thực hiện remote console từ xa tới máy mục tiêu để điều tra xử lý	✓		✓
Response Scenario	Cho phép định nghĩa kịch bản xử lý sự cố trên diện rộng một cách tự động	✓		✓
6. Tính năng Diệt mã độc				
Real-time Protection	Tự động phát hiện và tiêu diệt mã độc trên máy trạm		✓	✓
Scan OnDemand	Cho phép người dùng chủ động quét mã độc bằng quét nhanh, quét toàn bộ, quét thư mục theo nhu cầu		✓	✓
Anti Ransomware	Phát hiện và tiêu diệt mã độc mã hóa tổng tiền		✓	✓
Endpoint Firewall	Thiết lập chính sách để kiểm soát truy cập mạng trong tổ chức		✓	✓
Scan Scheduler	Thiết lập lịch quét mã độc dưới các máy trạm từ xa		✓	✓
Device Control	Kiểm soát, bảo vệ dữ liệu quan trọng thông qua thiết bị ngoại vi: USB, CD, DVD, thiết bị Bluetooth		✓	✓