Datasheet

Viettel Endpoint Detection & Response

(VCS - aJiant)

viettel security

"Giải pháp toàn diện bảo vệ, phát hiện và xử lý chủ động trước các nguy cơ tấn công mạng, đảm bảo an toàn cho thiết bị đầu cuối của doanh nghiệp và tổ chức."

THÁCH THỨC

Các cuộc tấn công mạng ngày nay ngày một đa dạng về quy mô và mục đích, không chỉ đơn thuần là những hành vi xâm nhập hệ thống, khai thác thông tin, trục lợi vì mục đích cá nhân mà còn là những cuộc tấn công có tổ chức, có động cơ kinh tế và chính trị.

Các cuộc tấn công có thể kéo dài hàng tháng, tới hàng năm; các loại mã độc được tạo ra, dành riêng để vượt qua các hệ thống bảo vệ của tổ chức, chiếm quyền và thực hiện tấn công leo thang gây ra những thiệt hại nặng nề đến tổ chức, doanh nghiệp.

GIẢI PHÁP

VCS-aJiant là giải pháp đảm bảo an toàn thiết bị đầu cuối một cách toàn diện, kết hợp trọn vẹn tính năng của Endpoint Detection & Response (EDR) và Endpoint Protection Platform (EPP). Giải pháp đáp ứng nhu cầu bảo vệ và phòng chống mã độc tại các doanh nghiệp và tổ chức; phản ứng, ngăn chặn, gỡ bỏ chương trình độc hại một cách triệt để trên toàn bộ hệ thống.

Bên cạnh đó, phát hiện các dấu hiệu tấn công sớm nhất với độ chính xác cao có thể điều tra, loang rộng để đánh giá quy mô, hậu quả của chiến dịch tấn công; tự động hóa các công việc một cách tối đa để tiết kiệm thời gian và giảm thiểu các thao tác vận hành với hệ thống.

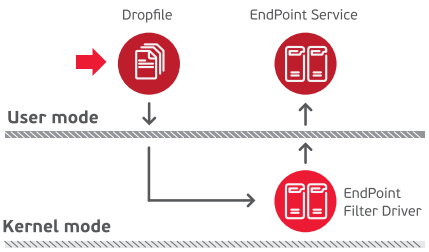
GIÁ TRỊ MANG LẠI

- Bảo vệ toàn diện các thiết bị đầu cuối.
- Giám sát các hành vi bất thường theo chuẩn MITRE ATT&CK.
- Bảo vệ chủ động và toàn diện đối với tấn công nâng cao có chủ đích APT (EDR) và tự động diệt mã độc thông thường (EPP)
- Phản ứng nhanh, chủ động, tự động.
- Phân tích & truy vết chuyên sâu bằng khả năng biểu diễn kill chain map trực quan.
- Tiết kiệm thời gian xử lý sự cố.
- Quản trị hiệu quả quy trình xử lý sự cố thông qua các chỉ số thời gian.

TÍNH NĂNG CHÍNH

Phòng chống mã độc toàn diện, chủ động

Cung cấp cơ chế cho phép thành phần agent giám sát chủ động dưới kernel mode, bắt các sự kiện khi mã độc xâm nhập và tiêu diệt tự động và ngay lập tức



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.

Tích hợp với các giải pháp bên thứ ba

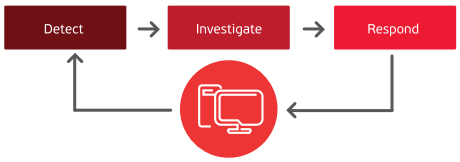
Tích hợp với các nguồn tri thức bên thứ ba như Threat Intelligence, Advanced Malware Analysis (Phân tích mã độc chuyên sâu), SOAR, SIEM.

Báo cáo theo thời gian thực

Hiển thị trực quan tình hình an toàn thông tin trên toàn hệ thống và trên từng máy người dùng.

Phản ứng sự cố nhanh chóng, chủ động

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 điều tra truy vết (Forensic) chuyên sâu trên thiết bị endpoint. Ngay khi xác minh được bất thường, cung cấp các công cụ gỡ bỏ mã độc diện rộng.



Tích hợp và hỗ trợ đa nền tảng

Hỗ trợ đa nền tảng: Windows, Linux, MacOS.

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.

Thiết lập chính sách ATTT

Hỗ trợ các chính sách An toàn thông tin như: Kiểm soát thiết bị ngoại vi, cung cấp remote an toàn (Security Helpdesk) giảm thiểu nguy cơ lây nhiễm mã độc

Phân tích tập trung

Áp 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.

Hoạt động nhẹ nhàng

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

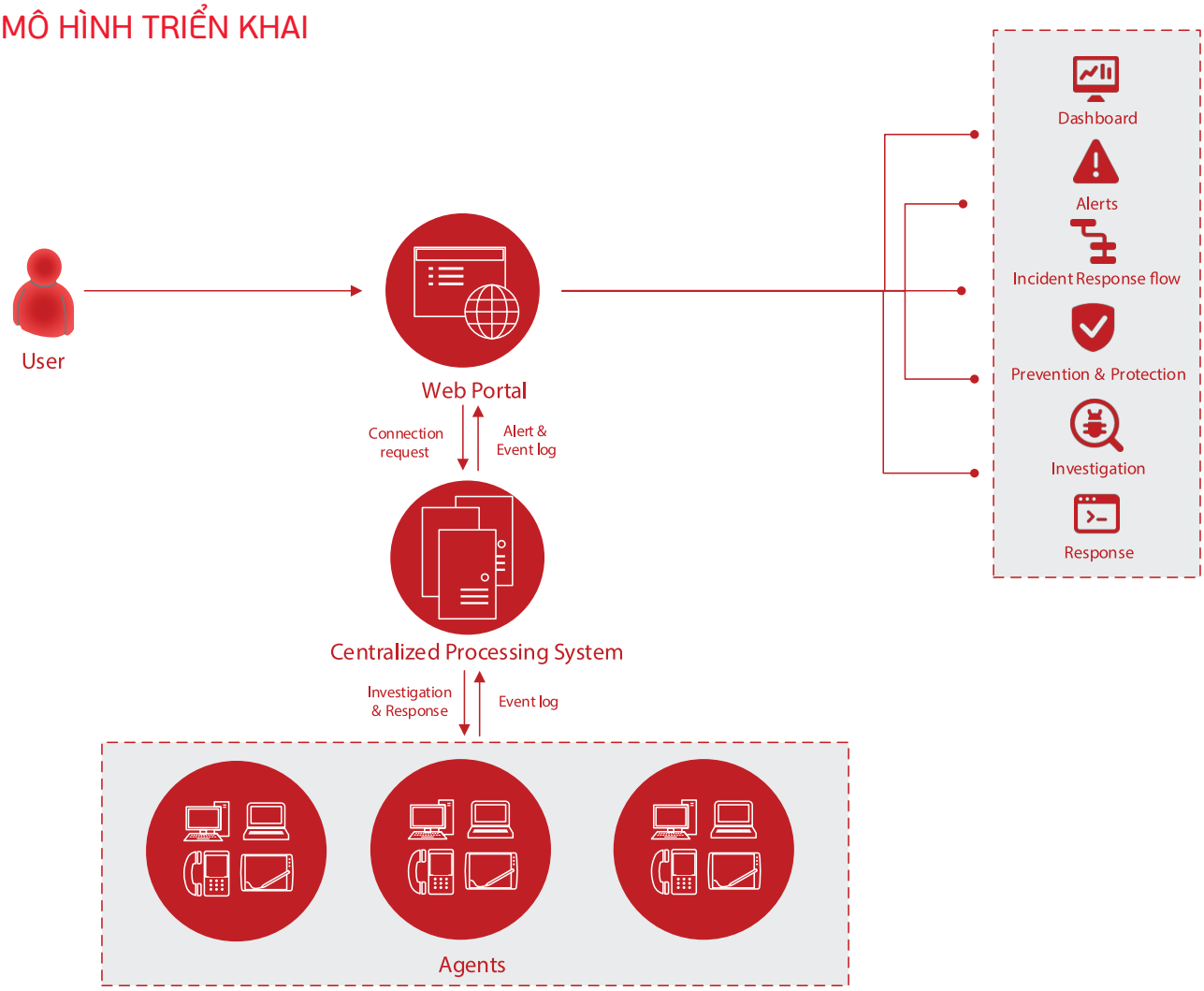
Datasheet

Viettel Endpoint Detection & Response

(VCS - aJiant)

viettel security

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

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.