Datasheet

Viettel Endpoint Detection & Response

(VCS-aJiant phiên bản EDR)

viettel security

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

THÁCH THỨC

Ngày nay, các tổ chức, doanh nghiệp liên tục gặp khó khăn với việc phát hiện, xác đ ịnh, đ iều tra và giảm thiểu các cuộc tấn công nâng cao vào hệ thống. Các công nghệ phòng chống mã đ ộc 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 đ ộ cao với các bộ công cụ tấn công, phần mềm đ ộc 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 đ ược 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.

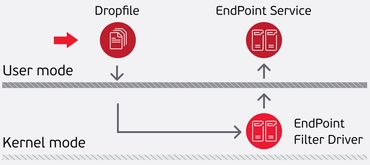
HIGHLIGHT VALUES

- 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

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 server 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 đ ộc. 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...).

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 đ iều 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 đ ộng nhẹ nhàng và hoàn toàn trong suốt.

Tích hợp và hỗ trợ đa nền tảng

Có khả năng tích hợp với giải pháp Threat Intelligence, SIEM, SOAR.
Hỗ trợ đa nền tảng Windows, Linux, MacOS.

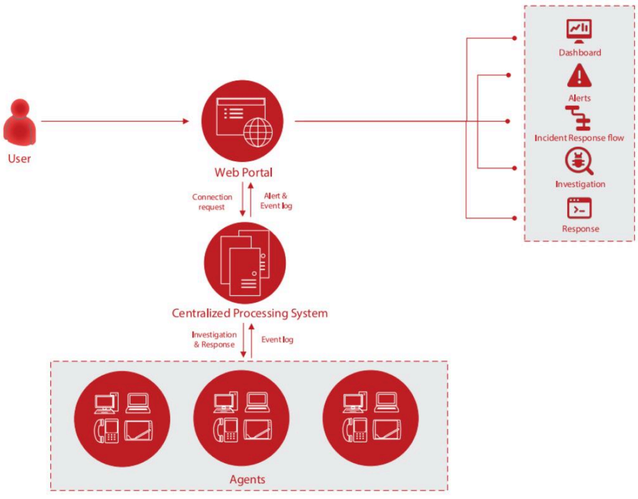
Datasheet

Viettel Endpoint Detection & Response

(VCS-aJiant phiên bản EDR)

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 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.

Viettel Cyber Security
For more information go to ▸ www.viettelcybersecurity.com
viettel security