Datasheet

Dịch vụ Săn tìm mối nguy An toàn thông tin (Threat Hunting)

viettel security

Sự cần thiết của việc dịch vụ săn tìm mối nguy An toàn thông tin

Trong những năm gần đây, các cuộc tấn công an ninh mạng ngày càng gia tăng về cả số lượng và mức độ tinh vi. Những rủi ro bảo mật và mã độc có thể gây thiệt hại không nhỏ đến uy tín và tài chính của doanh nghiệp.

Các doanh nghiệp và tổ chức đều nỗ lực xây dựng hệ thống an toàn thông tin có tính bảo mật chặt chẽ, phát hiện các cuộc tấn công sớm. Tuy nhiên, một khảo sát gần đây đã chỉ ra rằng phần lớn các mối nguy cơ an ninh mạng vẫn diễn ra bên trong mạng lưới nhưng không được phát hiện.

Do đó, dịch vụ Săn tìm mối nguy An toàn thông tin (Threat Hunting) ra đời nhằm tìm kiếm phát hiện và loại bỏ mã độc cũng như những mối đe dọa an ninh mạng tiềm ẩn trong mạng lưới của doanh nghiệp.

Dịch vụ săn tìm mối nguy An toàn thông tin

Dịch vụ Săn tìm mối nguy An toàn thông tin (Threat Hunting) của Công ty An ninh mạng Viettel là dịch vụ được tiến hành bởi những chuyên gia an ninh mạng giàu kinh nghiệm, sử dụng những công cụ tiên tiến. Dịch vụ đem lại các lợi ích:

- Chủ động phát hiện mã độc và những rủi ro an ninh mạng tiềm ẩn trong mạng, kể cả khi các mối nguy vượt qua được sự kiểm soát của các phần mềm, giải pháp bảo mật, hạn chế rủi ro xảy ra các sự cố
- Tăng tốc độ phản ứng với các nguy cơ bảo mật, giảm chi phí, thời gian điều tra số.
- Thường xuyên cập nhật, bổ sung, tăng cường an ninh các hệ thống bảo mật.
- Tăng cường tri thức về hệ thống mạng của tổ chức cho đội ngũ nhân sự CNTT, ATTT.
- Tăng cường tri thức, kỹ năng chuyên môn cho đội ngũ an ninh mạng in-house.

Những điểm chính của dịch vụ

Thu thập, phân tích nguy cơ toàn cầu

Hệ thống Viettel Threat Intelligence thường xuyên thu thập thông tin về các mối nguy an ninh mạng trên toàn cầu, bao gồm mạng Internet, các cộng đồng underground, cũng như từ các hệ thống giám sát của Viettel. Các thông tin này được sử dụng để đánh giá mức độ rủi ro bảo mật của hệ thống. Các nguy cơ bao gồm:

- Các nhóm, chiến dịch tấn công mạng
- Các loại mã độc
- Các lỗ hổng bảo mật
- Các nguy cơ lộ lọt dữ liệu
- Các nguy cơ bảo mật khác

Thu thập dữ kiện mạng

Các chuyên gia Viettel thực hiện thu thập các dữ kiện mạng, trực tiếp trên các hệ thống hoặc thông qua các giải pháp SIEM sẵn có, phục vụ phân tích phát hiện mã độc và các nguy cơ bảo mật. Các dữ kiện bao gồm:

- Log trên host (Event Log, audit log, file list...)
- Log network (NSM, netflow...)
- Log các giải pháp bảo mật (Firewall, IDS/IPS, Antivirus...)
- Log ứng dụng (Web, Database, DNS, LDAP...)

Rà soát phát hiện mã độc, mối nguy hại

Dựa trên các dữ kiện mạng đã thu thập, các thông tin nguy cơ toàn cầu, kết hợp với hệ thống phân tích thông minh Viettel iML, các chuyên gia Viettel rà soát phát hiện mã độc, các mối nguy hại trong mạng:

- Rà soát theo các kỹ thuật tấn công mạng, chuẩn hóa theo framework MITRE ATT&CK
- Rà soát theo các dấu hiệu nhận biết xâm nhập do hệ thống Viettel Threat Intelligence xác định
- Rà soát theo các dấu hiệu đặc trưng của tấn công APT
- Rà soát theo kết quả học máy của giải pháp Viettel iML

Phân tích chuyên sâu, điều tra số

Khi phát hiện mã độc, mối nguy hại, chuyên gia Viettel thực hiện phân tích mã độc, mã khai thác chuyên sâu, điều tra số trên các máy tính nghi nhiễm, các log đã thu thập, xác định:

- Thời điểm, nguồn gốc, nguyên nhân lây nhiễm
- Chủng loại mã độc, hành vi độc hại
- Máy chủ điều khiển, hạ tầng tấn công
- Nhóm, chiến dịch tấn công liên quan

Xử lý sự cố, phản ứng nhanh

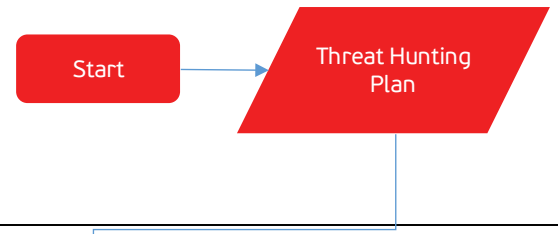
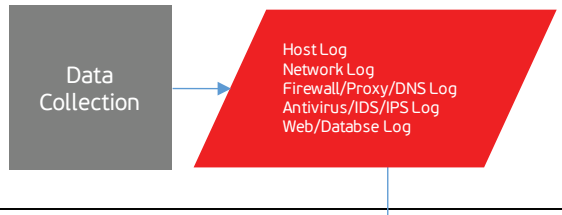
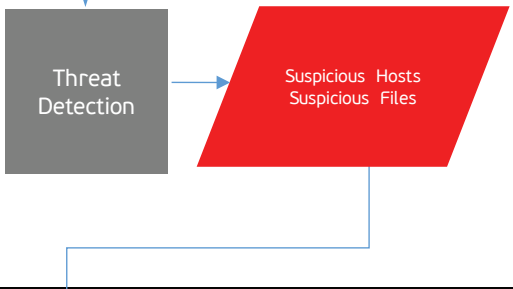
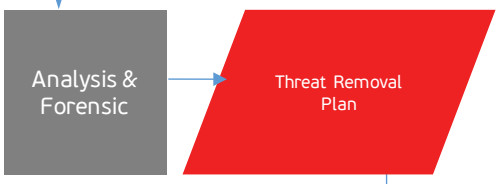
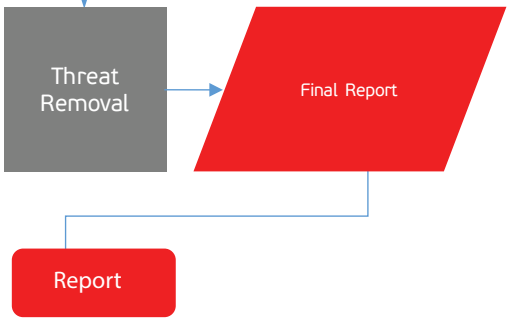
Sau khi phân tích sâu, chuyên gia Viettel đề xuất phương án xử lý sự cố, phản ứng nhanh với các mã độc, mối nguy phát hiện được:

- Gỡ bỏ, làm sạch mã độc
- Cập nhật, cài đặt các bản vá nghiêm trọng
- Siết chặt cấu hình bảo mật các hệ thống

Dịch vụ Săn tìm mối nguy An toàn thông tin (Threat Hunting)

viettel security

Quy trình thực hiện

Quy trình	Nội dung chi tiết
	**Viettel** đề xuất kế hoạch thực hiện Threat Hunting, **Khách hàng** phê duyệt kế hoạch, các nội dung bao gồm nhưng không giới hạn: - Log list (Host, FW/Proxy/DNS, AV...) - Cách thu thập từng loại log - Nơi lưu trữ, review: Tại máy tính KH/Qua hệ thống VCS iML - Phương thức thực hiện: On-site/Remote - Thời gian thực hiện - Nhân sự thực hiện, nhân sự phối hợp
	**Khách hàng** chuẩn bị các điều kiện cần thiết: - Máy tính thực hiện (nếu KH lựa chọn thực hiện trên máy tính KH) - Kết nối mạng sẵn sàng đến các máy tính, hệ thống cần thiết **Viettel** thực hiện, **KH** giám sát: - Host log (tool rà soát): **Viettel** thực hiện trực tiếp trên máy hoặc **Khách hàng** đẩy công cụ qua AD/SCCM/AV/SE/EDR... - FW/Proxy/DNS/AV/Network/Web/Database...: qua SIEM hoặc **Khách hàng** lấy qua console quản trị
	**Viettel** thực hiện, **Khách hàng** giám sát: - Host log: qua iML hoặc trực tiếp trên máy chủ - FW/Proxy/DNS/AV/Network/Web/Database...: trực tiếp trên laptop Analyst/ PC KH hoặc qua hệ thống SIEM/SOC của KH Phương pháp phát hiện các mối nguy: - Theo các kỹ thuật tấn công mạng (chuẩn ATT&CK Framework) - Theo các dấu hiếu nhận biết xâm nhập do hệ thống Viettel Threat Intelligent xác định - Theo các dấu hiệu đặc trưng của tấn công APT do Viettel nghiên cứu xây dựng - Theo kết quả học máy của hệ thống iML (nếu sử dụng phương án hunting trên hệ thống iML)
	**Viettel** thực hiện Forensics, **Khách hàng** giám sát: - Forensics trực tiếp trên các máy nghi nhiễm - Forensics qua tra cứu các loại log đã thu thập - Dịch ngược, phân tích sample trên laptop analyst **Viettel** đề xuất Threat Removal Plan, **Khách hàng** phê duyệt: - Phương án gỡ bỏ mã độc - Phương án hardening các giải pháp hiện có Phương án triển khai bổ sung các giải pháp ATTT
	**Khách hàng /Viettel** thực hiện gỡ bỏ mã độc, thực hiện các biện pháp ngắn hạn đơn giản, không ảnh hưởng hệ thống: - Gỡ bỏ mã độc - Hardening đơn giản (cài bản vá, cấu hình đơn giản...) **Viettel** báo cáo Threat Hunting: - Các nội dung đã thực hiện và kết quả - Đề xuất các nội dung tiếp theo cho KH