CÔNG TY CỔ PHẦN AN NINH AN TOÀN THÔNG TIN CMC – CMC INFOSEC
Tầng 15 tòa nhà CMC, phố Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmcinfosec.com
15th Floor, CMC Tower, Duy Tân Street, Dịch Vọng Hậu, Cầu Giấy, Hà Nội | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmcinfosec.com

DỊCH VỤ GIÁM SÁT VÀ CẢNH BÁO ANAT TT

(MONITORING SERVICE)

Thành viên chính thức của AVAR và ICSA

CMC INFOSEC

CÔNG TY CỔ PHẦN AN NINH AN TOÀN THÔNG TIN CMC INFOSEC

Report No	**V1.0**
Date	03/01/2019
Document Type	Service Description

MỤC LỤC

Định nghĩa các hoạt động giám sát và cảnh báo sự cố

Dịch vụ giám sát ANATTT của CMC Infosec có nhiệm vụ theo dõi, thu thập, tổng hợp, phân tích, xác minh thông tin về các rủi ro, sự cố ATTT, các cuộc tấn công vào đối tượng giám sát; chịu trách nhiệm về mức độ an toàn của toàn bộ hệ thống thông tin của tổ chức với tần suất giám sát, hoạt động 24/7.

Nội dung giám sát

1. **Giám sát mạng**
   - Giám sát hoạt động mạng của các thiết bị trong hệ thống được giám sát.
   - Phát hiện các giao thức lớp ứng dụng (Layer 7) hoạt động trong hệ thống như: Facebook, Youtube, BitTorrent,…
   - Phát hiện và hiển thị thời gian thực các kết nối mạng từ hệ thống đến các vùng địa lý trên thế giới trên giao diện bản đồ (Geographic Map)
   - Phát hiện và thống kê thời gian thực các website được truy cập bởi người dùng, ứng dụng trong hệ thống
   - Phát hiện và thống kê thời gian thực các ứng dụng hoạt động trên hệ thống (mặc định thống kê top 20 ứng dụng có hoạt động nhiều nhất)
   - Hỗ trợ xuất báo cáo thống kê theo các tiêu chí: Top IP trong mạng có hoạt động nhiều nhất, Top giao thức, Top quốc gia, Top website, Top IP đích,..)
   - Hỗ trợ xuất báo cáo thống kê hoạt động mạng đối với một thiết bị cụ thể trong hệ thống mạng được giám sát.

2. **Giám sát ATTT**
   - Phát hiện các hoạt động kết nối tới các máy chủ điều khiển mạng Botnet (BotCC)
   - Phát hiện các hoạt động kết nối tới các máy chủ, tên miền nguy hại được báo cáo và tổng hợp trong cơ sở dữ liệu của CMC Infosec và các tổ chức uy tín như Emerging Threats, Virus Total, OTX, Spamhaus,…

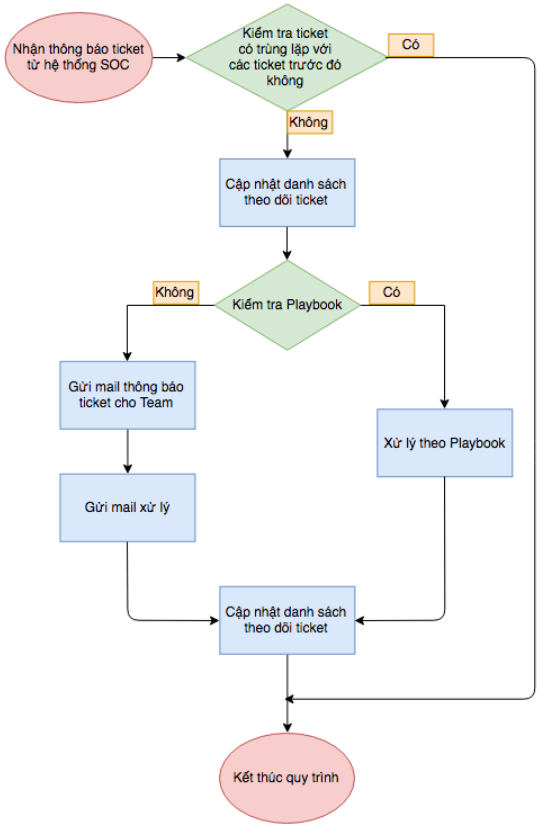
- Phát hiện các hoạt động của Malware, Spyware, Ransomeware, Adware; Trojan, Worm trong hệ thống
    - Phát hiện các hoạt động khai thác, lây nhiễm, của mã độc trong hạ tầng mạng LAN/WAN nội bộ
    - Phát hiện các phần mềm độc hại/mã độc được tải về từ internet.
- Phát hiện các cuộc tấn công, khai thác lỗ hổng của hệ điều hành: Windows, Linux, Unix trong hệ thống mạng LAN/WAN nội bộ và public
- Phát hiện các cuộc tấn công, khai thác lỗ hổng trong các ứng dụng quan trọng như: Web, FTP, SMTP, SQL, DNS, VOIP, TFTP, Telnet,… trong hệ thống mạng LAN/WAN nội bộ và public
- Phát hiện các cuộc tấn công, khai thác lỗ hổng trên các thiết bị mạng thông dụng: Cisco, D-Link, TPLink trong hệ thống mạng LAN/WAN nội bộ và public
- Phát hiện các cuộc tấn công, khai thác lỗ hổng trên nền tảng di động (Android, IOS)
- Phát hiện các cuộc tấn công từ chối dịch vụ DoS, DDoS
- Phát hiện các hành vi dò quét, thăm dò hệ thống sử dụng các công cụ như Nessus, Acunetix, Nmap,… trong hệ thống mạng LAN/WAN nội bộ và public
- Phát hiện các hành vi vi phạm chính sách ANATTT của tổ chức như:
    - Phát hiện việc sử dụng các phần mềm, ứng dụng Chat, IRC như: Facebook, Google Talk, ICQ,…; các phần mềm Teamview, Logmein,…
    - Phát hiện các hành vi truy cập các website có nội dung khiêu dâm
    - Phát hiện các hoạt động của mạng ngang hàng Peer To Peer P2P như BitTorrent, Edonkey, Gnutella,…
    - Phát hiện các hoạt động của mạng TOR (TOR network)
- Phát hiện các thông tin liên quan tới data breached (lộ password, password dễ đoán, password mã hóa yếu, .etc)
- Phát hiện các phần mềm độc hại/mã độc được gửi vào hệ thống mail nội bộ.

- Phát hiện các cuộc thăm dò, khai thác của kẻ tấn công sử dụng các payload đã có trong cơ sở dữ liệu của CMC Infosec, OTX, Emerging Threats

3. Giám sát thiết bị đầu cuối (Endpoint Monitor & Log Collector)

- Thu thập giám sát log của các server Window/Linux/AIX/Solaris (syslog, audit log, secure log, kern log, auth log, mail log, modsec log)
- Thu thập giám sát log của các webserver: Nginx/Apache/Tomcat/Lighttpd/LiteSpeed Web Server/IIS
- Thu thập giám sát log của các ứng dụng thông dụng sinh logs theo chuẩn syslog.
- Giám sát tính toàn vẹn của các file/thư mục hệ thống Linux/Windows (theo phụ lục)
- Phát hiện hoạt động liên quan tấn công apt trong hệ thống theo cơ sở dữ liệu đã biết (theo phụ lục)
- Phát hiện hoạt động của các tiến trình/phần mềm độc hại/mã độc trong server Linux (theo phụ lục)
- Phát hiện hoạt động của các tiến trình/phần mềm độc hại/mã độc trong máy chạy Windows (theo phụ lục)
- Phát hiện hoạt động mạng (proxy, VPN, dns, telegram) của các tiến trình/phần mềm độc hại/mã độc chạy trong máy Linux/Windows (theo phụ lục)
- Phát hiện hoạt động khai thác, leo thang đặc quyền trong các máy Linux/Windows có sử dụng string, command nhạy cảm (theo phụ lục)
- Phát hiện, thu thập các IOC liên quan tới các mối nguy hại dựa theo cơ sở dữ liệu của CMC Infosec, OTX.

Quy trình vận hành và cảnh báo sự cố



1. Định nghĩa tên gọi:

+ Danh sách theo dõi ticket: là danh sách theo dõi các thông tin về ticket được lưu và cập nhật trên Google Docs để toàn bộ Team có thể theo dõi. Danh sách ticket phải được kiểm tra, theo dõi và cập nhật hàng ngày. Các nội dung của danh sách theo dõi ticket bao gồm:
- IP nguồn: Địa chỉ IP nguồn trong thông báo ticket
- IP đích: Địa chỉ IP đích trong thông báo ticket
- Tên Threat: Tên đầy đủ của Threat tương ứng trong thông báo ticket
- Thời gian bắt đầu: Thời điểm nhận được thông báo ticket có nội dung Threat tương ứng lần đầu tiên trong ngày.
- Thời gian kết thúc: Thời điểm không còn nhận được thông báo ticket có nội dung Threat tương ứng hoặc tại thời người giám sát check thông báo.
- Số lần: Số lượng tương tác giữa IP nguồn và IP đích trong khoảng thời gian từ Thời gian bắt đầu đến Thời gian kết thúc trong thông báo ticket.
- Đánh giá: Xác nhận nội dung ticket là False positive hay không?
- Trạng thái xử lý: Tình hình xử lý ticket với các mức là: (chưa xử lý; đã gửi mail nhưng chưa gọi điện, đã gọi điện nhưng vẫn chưa xử lý; đang xử lý; xử lý xong)

+ Playbook: là tuyển tập các ticket và cách xử lý ticket tương ứng. Playbook sẽ thường xuyên được cập nhật và bổ sung theo các trường hợp thực tế để đảm bảo tính chính xác và hiệu quả

2. Mô tả nội dung:

+ Bước 1: Sau khi tiếp nhận thông báo ticket từ hệ thống SOC, nhân viên phục trách giám sát có trách nhiệm kiểm tra ticket có trùng lặp không: là việc kiểm tra và xác định ticket xuất hiện trên hệ thống giám sát SOC đã có tồn tại hay chưa? các IP đích và IP nguồn có thường xuyên xuất hiện không? Nếu đã trùng lặp thì kết thúc quy trình. Nếu không trùng lặp thì chuyển tới bước kế tiếp theo quy trình.

+ Bước 2: Nhân viên giám sát cập nhật các thông tin về ticket theo Mẫu của Danh sách theo dõi ticket. Sau đó chuyển tới bước xử lý kế tiếp.

+ Bước 3: Nhân viên giám sát kiểm tra xem thông báo tiếp nhận đã có trong Playbook chưa? Nếu đã có thì xử lý theo hướng dẫn trong Playbook. Nếu chưa có, nhân viên giám sát gửi thông báo tới cho các thành viên trong Team để tiến hành kiểm tra, đánh giá và xử lý ticket. Công việc gửi mail như sau:
- Gửi mail thông báo cho Team: Người nhận là Nhân viên phân tích Tier 2 và CC cho các thành viên trong Team SOC gồm: Giám đốc Trung tâm, Trưởng phòng phân tích, các thành viên mức Tier 1, Tier 2 và Tier 3.
- Gửi mail thông báo xử lý cho đội xử lý: Trường hợp có người xử lý, mail thông báo và hướng dẫn xử lý sẽ được gửi cho đội xử lý với Người nhận là Đội xử lý và CC cho toàn bộ các thành viên trong Team SOC
- Gửi mail thông báo xử lý cho khách hàng: Trường hợp cần phối hợp với Khách hàng để xử lý sự cố, mail thông báo và hướng dẫn xử lý sẽ được gửi cho Khách hàng với Người nhận là Đại diện đầu mối tiếp nhận thông tin phía Khách hàng và CC cho các thành viên Tier 2, Tier 3, Trưởng phòng Phân tích, Đầu mối thông tin và Phụ trách dự án.

+ Bước 4: Nhân viên cập nhật trạng thái xử lý sau khi đã gửi mail phối hợp xử lý để tiếp tục theo dõi trạng thái xử lý của ticket.

+ Bước 5: Sau khi hoàn thành việc cập nhật trạng thái xử lý vào Danh sách theo dõi ticket, quy trình xử lý ticket được coi là kết thúc.

Mức cam kết của nhà cung cấp dịch vụ

Nguồn thông tin	Mức độ nguy hiểm (Threat Level)	Mức độ ưu tiên xử lý	Hình thức CMC cảnh báo tới khách hàng	Thời gian CMC gửi báo cáo đánh giá tiền xử lý
SOC Alerts	Khẩn cấp	5	Real-time (qua Message và Email)	90 phút (tính từ thời điểm phát sinh cảnh báo)

	Nghiêm trọng	4	Real-time (qua Message và Email)	120 phút (tính từ thời điểm phát sinh cảnh báo)
	Cao	3	Email	24 tiếng
	Cảnh báo	2	N/A	N/A
	Lộ thông tin	1		
Kết quả thực hiện điều tra số (Cyber Forensic)	Có sự cố	4	Ngay khi bắt đầu cuộc điều tra	Ngay sau khi có kết quả của cuộc điều tra
	Chưa có kết luận / Cần thêm thông tin	2	N/A	N/A
Các cảnh báo từ phía khách hàng	Nghiêm trọng	5	N/A	120 phút (tính từ thời điểm nhận yêu cầu từ khách hàng)