CÔNG TY TNHH AN NINH AN TOÀN THÔNG TIN CMC

CMC CYBER SECURITY CO. LTD.

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.cmccybersecurity.com

15th Floor, CMC Tower, Duy Tan Street, Dich Vong Hau, Cau Giay, Hanoi | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

DỊCH VỤ GIÁM SÁT AN NINH AN TOÀN THÔNG TIN BY CMC SOC

Thành viên chính thức của AVAR và ICSA

CMC CYBER SECURITY
Aspire to Inspire the Digital World

CMC CYBER SECURITY
Aspire to Inspire the Digital World

CÔNG TY TNHH AN NINH AN TOÀN THÔNG TIN CMC

Report No	2.0
Date	
Document Type	Service Description
Prepared By	

I. Mô tả dịch vụ

Dịch vụ giám sát ANATTT của CMC Cyber Security 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.

II. 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 An Toàn Thông Tin

- 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 Cyber Security 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…cũng như các ứng dụng dùng chung trong hệ thống mạng LAN/WAN nội bộ và public

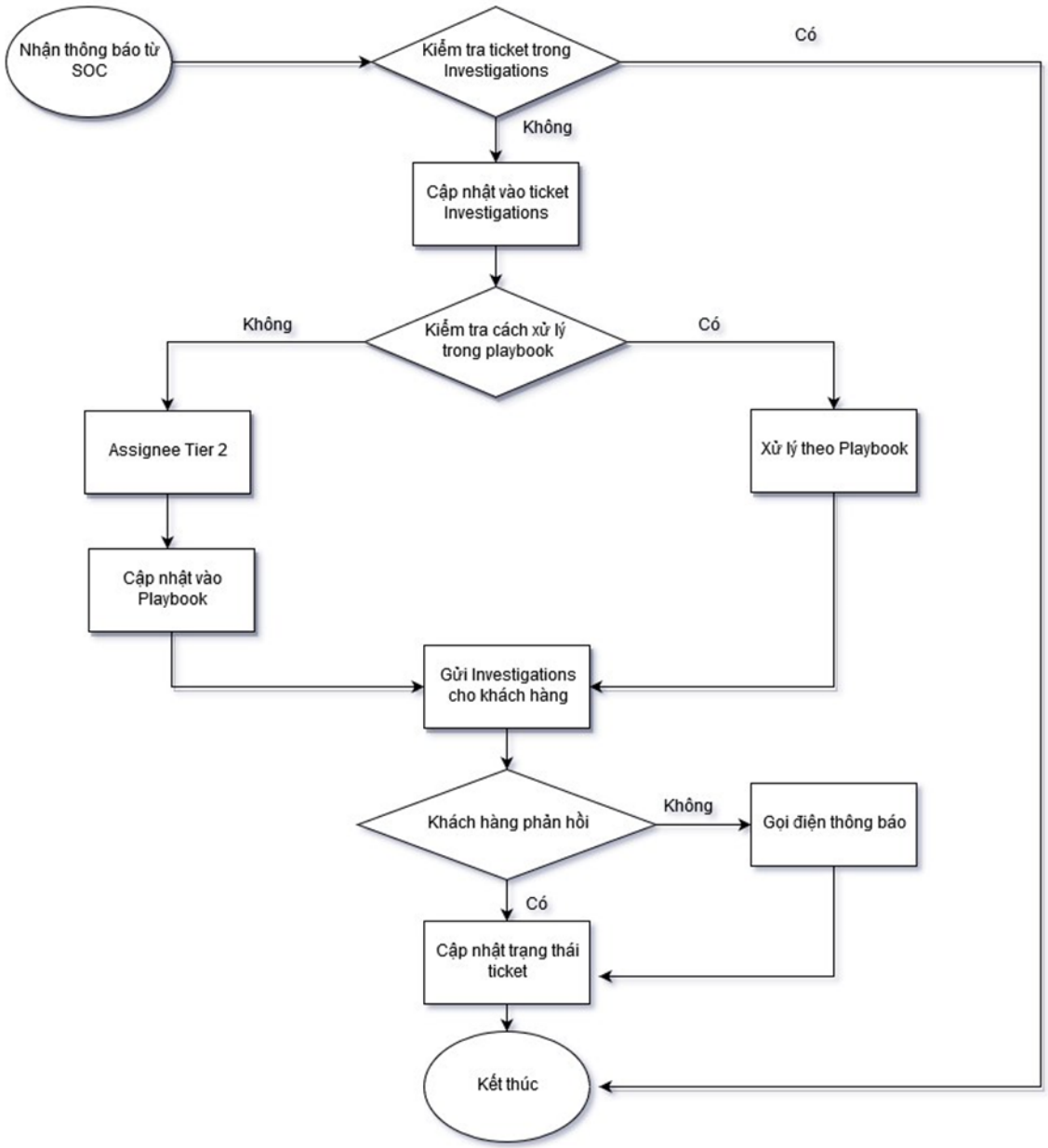
- Phát hiện các cuộc tấn công, khai thác lỗ hổng trên các thiết bị mạng thông dụng: Cisco, D-Link, TPLink, HPE, Sophos, Jupiter, Peplink… trong hệ thống mạng LAN/WAN nội bộ và public
- Phát hiện các cuộc tấn công, khai thác lỗ hổng trên nền tảng di động (Android, IOS)
- Phát hiện các cuộc tấn công từ 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, bạo lực
- 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…)
- 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 Cyber Security, OTX, Emerging Threats

3. Giám sát Thiết bị đầu cuối (Endpoint Monitor & Log Collector – bắt buộc cài CMC Endpoint Detection & Response)

- 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
- Phát hiện hoạt động liên quan tấn công APT trong hệ thống theo cơ sở dữ liệu đã biết
- Phát hiện hoạt động của các tiến trình/phần mềm độc hại/mã độc trong server Linux
- Phát hiện hoạt động của các tiến trình/phần mềm độc hại/mã độc trong máy chạy Windows
- Phát hiện hoạt động mạng (Proxy, VPN, DNS, Telegram) của các tiến trình/phần mềm độc hại/mã độc chạy trong máy Linux/Windows
- Phát hiện hoạt động khai thác, leo thang đặc quyền trong các máy Linux/Windows có sử dụng string, command nhạy cảm
- Phát hiện, thu thập các IOC liên quan tới các mối nguy hại dựa theo cơ sở dữ liệu của CMC Cyber Security, OTX.
- Phần mềm EDR Agent để giám sát thiết bị đầu cuối (Endpoint Detection and Response)

- EDR cung cấp khả năng ngăn chặn các mối đe dọa một cách đa dạng, bao gồm các trường hợp phổ biến sau:
  - Sự cần thiết phải xác định và ngăn chặn các hành động thực thi có tính độc hại
  - Kiểm soát vị trí, cách thức và ai có thể thực thi các script
  - Giám sát việc sử dụng các thiết bị USB, thiết bị không được phép sử dụng
  - Loại bỏ khả năng kẻ tấn công sử dụng kỹ thuật fileless malware attack trên các endpoints được bảo vệ
  - Ngăn chặn các tệp đính kèm độc hại trong email thực thi các payload
  - Dự đoán và ngăn chặn các cuộc tấn công zero-day
- Kết nối, chia sẻ dữ liệu giám sát với hệ thống Giám sát an toàn không gian mạng quốc gia

III. Quy trình giám sát



- **Bước 1:** Sau khi tiếp nhận thông báo ticket từ hệ thống SOC, nhân viện phụ 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 xuất hiện không? Nếu đã trùng lặp thì kết thúc quy trình. Nếu đã trùng lặp thì kết thúc quy trình. Nếu không trùng lặp thì chuyển tới bước 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 trên Investigations (chức năng Investigations giúp người dùng và đội giám sát

SOC tương tác trực tiếp hai bên với nhau thông qua giao diện Dasboard). Nhân viên giám sát Tier 1 sẽ cập nhật mức độ cảnh báo trong mục Severity của Investigations.

- **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 trong Playbook, nhân viên giám sát Tier 1 sẽ gán Assignee cho một nhân viên thuộc Tier 2 có trách nhiệm phân tích và đưa ra phương án xử lý đối với ticket. Sau khi đưa ra khuyến nghị xử lý đối với ticket nhân viên giám sát Tier 1 sẽ cập nhật vào báo cáo.
- **Bước 4:** Nhân viên giám sát Tier 1 có trách nhiệm gửi lại báo cáo cho khách hàng trong phần Investigations sau khi đã cập nhật khuyến nghị xử lý.
- **Bước 5:** Khi gửi thông tin cảnh báo cho khách hàng:
  - Nếu quá thời gian phản hồi theo SLA mà khách hàng chưa phản hồi thì CMC SOC sẽ gọi điện để thông báo.
  - Nếu khách hàng phản hồi ticket trong phần Notes của Investigations, hai bên sẽ tiến hành trao đổi và xác minh thêm các thông tin cần thiết về ticket và mức độ ảnh hưởng tới hệ thống
- **Bước 6:** Sau khi hoàn thành quá trình trao đổi xử lý giữa hai bên, nhân sự giám sát SOC sẽ cập nhật lại trạng thái của ticket và đóng quy trình thông báo sự cố.

IV. Cam kết cung cấp dịch vụ (Service Level Agreement – SLA)

Đối với dịch vụ giám sát 24/7 của CMC SOC, cam kết chung về cung cấp dịch vụ của chúng tôi sẽ như dưới đây. ***Lưu ý:*** *Cam kết này sẽ thay đổi trong quá trình hoàn tất hợp đồng:*

Sources of Alerts	Mức độ đe dọa (từ CMC SIEM)	Mức độ ưu tiên xử lý	Phương pháp thông báo	Thời gian tối đa từ khi nhận cảnh báo đến khi xử lý
SOC Alerts	HIGH	3	Thời gian thực thông qua tin nhắn và email	90 phút
	WARNING	2	Thời gian thực thông qua tin nhắn và email	24 tiếng
	INFORMATIONAL	1	N/A	
Alerts/ Notification từ khách hàng	Review Action	3	N/A	180 phút từ khi nhận được thông báo chính thức từ khách hàng