1. A. PHẠM VI CÔNG VIỆC

1.1 I. Đối tượng dịch vụ SOC

Triển khai trọn gói thuê dịch vụ triển khai hệ thống giám sát ATTT Tập trung 24/7 của Tổng công ty Điện lực Dầu khí Việt Nam – CTCP (PV Power), áp dụng đối với các hệ thống CNTT trọng yếu (máy chủ, thiết bị mạng, thiết bị bảo mật chính...) tại các địa điểm:

- Trung tâm dữ liệu của PV Power tại Viettel IDC, Hòa Lạc, Hà Nội;
- Trụ sở cơ quan Tổng công ty PV Power tại Hà Nội (địa chỉ hiện tại: 167 Trung Kính, Yên Hòa, Cầu Giấy, Hà Nội và dự kiến sẽ chuyển địa điểm vào cuối năm 2025);
- Công ty Điện lực Dầu khí Cà Mau;
- Công ty Điện lực Dầu khí Hà Tĩnh;
- Công ty Điện lực Dầu khí Nhơn Trạch.

Với phạm vi thiết bị cần được giám sát và khối lượng sự kiện được thu thập:

- Thiết bị máy chủ/mạng: Giám sát an toàn thông tin cho khoảng 100 máy chủ, 80 thiết bị mạng, bảo mật, lưu trữ trên hệ thống;
- Tổng khối lượng sự kiện ATTT cần phân tích, giám sát và xử lý là khoảng 2000 EPS hoặc quy đổi tương đương.

Lưu ý: Hệ thống SIEM tập trung PV Power sẽ kết nối thu thập dữ liệu SIEM (LogRhythm) của Công ty Điện lực Dầu khí Cà Mau đã được trang bị.

1.2 II. Phạm vi công việc và thời gian cung cấp dịch vụ Soc PV Power

1.2.1 1. Phạm vi công việc

STT	Sản phẩm/Dịch vụ	Số lượng	ĐVT	Yêu cầu kỹ thuật
I	**Bộ giải pháp phần mềm thu thập giám sát ATTT 24/7 cho 2000 EPS tối thiểu các thành phần sau:**	**01**	**Gói**	
	- Quản lý và phân tích sự kiện ATTT (SIEM - Security Information & Event Management)			Chi tiết tại B.II.1
	- Phát hiện và phản ứng sự cố ATTT trên thiết bị đầu cuối (EDR - Endpoint Detection and Response)			Chi tiết tại A.II.2
	- Sản phẩm Điều phối, tự động hóa và phản ứng ATTT (SOAR - Security Orchestration, Automation and Response)			Chi tiết tại B.II.3
	- Sản phẩm tri thức mối đe dọa an toàn thông tin (TI – Threat Intelligence)			Chi tiết tại B.II.4
II	**Thiết bị phần cứng**			
	- Máy chủ vật lý bao gồm các bản quyền cần thiết như hệ điều hành, phần mềm ảo hóa…			Chi tiết tại B.III.1
	- Các trang thiết bị hỗ trợ việc đấu nối, giám sát (nếu có).			Chi tiết tại B.III.2
III	**Dịch vụ triển khai ban đầu**			
	Bao gồm các công việc sau: - Khảo sát hệ thống hiện hữu; - Đề xuất phương án triển khai; - Lắp đặt, cấu hình hệ thống (bao gồm phần cứng, phần mềm liên quan);			Chi tiết tại B.IV

STT	Sản phẩm/Dịch vụ	Số lượng	ĐVT	Yêu cầu kỹ thuật
	- Tinh chỉnh các tập luật trên các hệ thống SIEM, SOAR, EDR…phù hợp với hệ thống hiện hữu. - Đào tạo nhân sự phối hợp vận hành hệ thống của PV Power. - Vận hành thử nghiệm hệ thống và bàn giao đưa vào cung cấp dịch vụ. - Kiểm tra, nghiệm thu sản phẩm.			
IV	**Dịch vụ giám sát và phản ứng ATTT**			
	- Dịch vụ giám sát và phản ứng ATTT cho PV Power.			Chi tiết tại B.V
V	**Chấm dứt dịch vụ**			
	- Trường hợp chấm dứt sử dụng dịch vụ, nhà thầu có trách nhiệm: - Gỡ toàn bộ các thành phần của hệ thống SOC được cài đặt trên các máy chủ vật lý/ảo hoá của chủ đầu tư. Thiết lập lại cấu hình tự động gửi log trên các thiết bị phần cứng. - Thu hồi các phần cứng của nhà thầu đặt tại địa điểm của chủ đầu tư. - Sao lưu toàn bộ các log đang được lưu trữ và gửi lại chủ đầu tư. - Các công việc nêu trên phải đảm bảo không gây ảnh hưởng đến hệ thống của chủ đầu tư.			
VI	**Kênh truyền riêng (nếu có)**			
	- Kênh truyền riêng để đảm bảo băng thông dịch vụ Soc			Do đơn vị cung cấp dịch vụ đề xuất giải pháp nếu cần thiết

1.2.2 2. Thời gian cung cấp dịch vụ:

- 12 tháng;

- Sau 12 tháng sử dụng, dựa trên kết quả thực hiện hợp đồng và các điều kiện quy định trong hợp đồng, chủ đầu tư sẽ xem xét gia hạn thời gian sử dụng dịch vụ thêm 12 hoặc 24 tháng.

2. B. YÊU CẦU KỸ THUẬT

2.1 I. Yêu cầu chung và tiêu chí đánh giá hiệu quả.

2.1.1 1. Yêu cầu chung

STT	Nội dung	Mô tả chi tiết
1	Thu thập và phân tích sự kiện ATTT	Tổng hợp và phân tích đầy đủ các sự kiện liên quan đến an toàn, an ninh thông tin từ các nguồn log tập trung trong hệ thống.
2	Giám sát an ninh mạng từ xa 24/7	Theo dõi hệ thống liên tục, phát hiện kịp thời các sự cố và hành vi tấn công mạng nhằm đảm bảo phản ứng sớm.
3	Xây dựng và tối ưu hệ thống SOAR	- Điều phối và quản lý ticket; - Giám sát tiến độ xử lý sự cố;

		- Triển khai playbook và tự động hóa các tác vụ; - Cung cấp giao diện cảnh báo và hệ thống báo cáo tập trung.
4	Cung cấp dịch vụ Threat Intelligence	- Cập nhật thông tin về các mã độc có chủ đích (Targeted Malware); - Cung cấp thông tin về các lỗ hổng bảo mật; - Tổng hợp mối đe dọa và sự cố ATTT mới phát sinh trên toàn cầu.
5	Triển khai giải pháp EDR	Tích hợp phần mềm EDR trong gói dịch vụ SOC để nâng cao năng lực phát hiện, làm giàu dữ liệu phục vụ giám sát và điều tra sự cố.
6	Hỗ trợ ứng phó sự cố	Cung cấp lực lượng chuyên gia sẵn sàng phối hợp, xử lý khi có sự cố an ninh mạng xảy ra tại hệ thống của PV Power.
7	Cập nhật liên tục quy tắc phát hiện và quy trình ứng phó	Thường xuyên cập nhật hệ thống phát hiện và quy trình xử lý để kịp thời đối phó với các hình thức tấn công mới.
8	Tối ưu hệ thống log và các rule/use case	Xây dựng, tinh chỉnh các rule và use case nhằm phát hiện bất thường và mối đe dọa từ sớm, tối ưu hóa việc sử dụng log.
9	Báo cáo định kỳ và đột xuất	Cung cấp báo cáo định kỳ hoặc theo yêu cầu đột xuất về tình hình an ninh mạng, sự cố và khuyến nghị cải thiện.
10	Dữ liệu	Dữ liệu log và sự kiện ATTT chỉ được lưu trữ trong hệ thống SIEM đặt tại PV Power. Không được sao lưu, sao chép hoặc di chuyển ra ngoài dưới bất kỳ hình thức nào.

2.1.2 2. Tiêu chí đánh giá hiệu quả đối với hệ thống Soc hoàn chỉnh

STT	Tiêu chí/Nội dung đánh giá	Yêu cầu đáp ứng
1	**Giải pháp**	
1.1	**Hiệu quả của các thành phần trong hệ thống**	
1.1.1	Thu thập, xử lý, phân tích log.	Có khả năng tiếp nhận log của tối thiểu 04 nguồn log thiết yếu (thiết bị mạng (Router, Switch), thiết bị bảo mật (Firewall, NIDS, Endpoint server), hệ điều hành (Linux, Windows), ứng dụng (Mail, DNS, DHCP)).
1.1.2	Phân tích phát hiện tấn công dựa vào phân tích lưu lượng mạng.	- Có khả năng phát hiện tấn công cơ bản lớp mạng; - Khả năng phát hiện kết nối đến máy chủ điều khiển của mã độc.
1.1.3	Phân tích phát hiện tấn công Endpoints, Server.	Có khả năng phát hiện các hành vi bất thường như: - Tập tin bị thay đổi, thêm mới trên đường dẫn cụ thể; - Chạy các lệnh nguy hiểm; - Có các hành vi như: thay đổi Registry, tự động khởi chạy; - Ngăn chặn từ trung tâm khi cần thiết.

1.1.4	Phát hiện, ngăn chặn tấn công lớp ứng dụng.	Tối thiểu có giải pháp bảo vệ Web hoặc tích hợp được với giải pháp có sẵn.
1.1.5	Quản lý, phân tích, cảnh báo.	Có hệ thống phần mềm hỗ trợ khách hàng đảm bảo có các thông tin: chi tiết về sự cố, tương quan giữa các sự kiện, mức độ, tình trạng xử lý.
1.2	**Chức năng cơ bản của SOC**	
1.2.1	Tùy chỉnh giao diện giám sát	Giải pháp có thể tùy chỉnh giao diện giám sát
1.2.2	Gửi cảnh báo đến các thành phần thứ 3 (MAIL, SMS, APP…)	Gửi được cảnh báo đến tối thiểu 01 thành phần.
1.2.3	Truy xuất dữ liệu phục vụ phân tích tấn công.	Có thể truy xuất log network, security của Endpoint
1.2.4	Ngăn chặn tấn công	Tối thiểu có khả năng chặn tấn công theo IP.
1.2.5	Tích hợp với các giải pháp/hệ thống cung cấp, chia sẻ thông tin tấn công mạng.	Hệ thống có khả năng tích hợp với hệ thống Threat Intelligence hoặc dễ dàng tùy biến.
1.3	**Chức năng nâng cao của SOC**	
1.3.1	Threat Intelligence	Có hệ thống Threat Intelligence tự phát triển hoặc mua của hãng thứ 3.
1.3.2	SOAR	Hệ thống có playbook (hướng dẫn xử lý các tình huống điển hình) để xử lý các trường hợp: phát hiện mã độc, hành vi dò quét.
2	**Khả năng làm chủ giải pháp**	
2.1	Mức độ làm chủ giải pháp - Mức độ làm chủ các giải pháp thương mại (nếu có); - Mức độ làm chủ các giải pháp tự phát triển, mã nguồn mở (nếu có)	Tự làm chủ giải pháp, hoặc có khả năng tùy biến theo yêu cầu của khách hàng.
2.2	Khả năng tùy chỉnh hệ thống đáp ứng yêu cầu đặc thù khách hàng.	Chứng minh được khả năng tùy biến qua một số yêu cầu cụ thể.
3	**Tuân thủ các các quy định, hướng dẫn về an toàn thông tin**	
3.1	Kết nối, chia sẻ thông tin với Trung tâm giám sát an toàn không gian mạng quốc gia, Tập đoàn Công nghiệp – Năng lượng Quốc gia Việt Nam… theo yêu cầu, quy định hiện hành. - Khả năng kết nối chia sẻ dữ liệu; - Chất lượng dữ liệu chia sẻ.	

3.2	Tuân thủ các quy định, quy trình hiện hành về bảo đảm an toàn thông tin của nhà nước.	

2.2 II. Yêu cầu kỹ thuật giải pháp phần mềm (yêu cầu về công nghệ).

2.2.1 1. Yêu cầu kỹ thuật của thành phần Quản lý và phân tích sự kiện an toàn thông tin (SIEM - Security Information & Event Management)

1.1. Yêu cầu về tài liệu

SIEM có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

1.2. Yêu cầu về quản trị hệ thống

1.2.1. Quản lý vận hành

SIEM cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

b) Cho phép thay đổi thời gian hệ thống;

c) Cho phép thay đổi thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,…);

e) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;

g) Cho phép xóa log;

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

1.2.2. Quản trị từ xa

SIEM cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

1.2.3. Quản lý xác thực và phân quyền

SIEM cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

1.2.4. Quản lý báo cáo

SIEM cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau: a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML;

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra.

1.2.5. Quản lý tập luật bảo vệ

SIEM cho phép quản lý tập luật bảo vệ bao gồm các thao tác sau:

a) Thêm luật mới;

b) Tinh chỉnh luật;

c) Tìm kiếm luật;

d) Xóa luật;

đ) Kích hoạt/vô hiệu hóa luật;

e) Xuất tập luật ra tệp tin;

g) Khôi phục tập luật từ tệp tin;

h) Cập nhật tập luật được phát hành bởi nhà sản xuất.

1.2.6. Cập nhật tập luật bảo vệ

SIEM cho phép cập nhật tập luật bảo vệ đáp ứng các yêu cầu sau:

a) Cho phép tự động thông báo có bản cập nhật mới cho quản trị viên;

b) Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới.

1.2.7. Quản lý đối tượng được giám sát và nguồn gửi log

SIEM cho phép quản lý đối tượng được giám sát và nguồn gửi log đáp ứng các yêu cầu sau:

a) Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo các nhóm được định nghĩa bởi quản trị viên;

b) Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo địa chỉ vật lý, địa chỉ mạng và vị trí địa lý.

1.2.8. Quản lý và giám sát tập trung các thành phần tích hợp bên trong

SIEM cho phép quản lý và giám sát tập trung thông qua giao diện đồ họa các thông số hiệu năng sau của các thành phần tích hợp bên trong:

a) Receiver;

b) Parser;

c) Indexer;

d) Storage;

đ) Correlator.

1.2.9. Chia sẻ dữ liệu

SIEM cho phép kết nối với các loại hệ thống sau để chia sẻ dữ liệu:

a) Hệ thống giám sát an toàn không gian mạng quốc gia;

b) Hệ thống giám sát SOC của Tập đoàn;

b) Hệ thống SIEM khác.

1.3. Yêu cầu về kiểm soát lỗi

1.3.1. Bảo vệ cấu hình

Trong trường hợp SIEM phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SIEM đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình tập luật bảo vệ.

1.3.2. Bảo vệ dữ liệu log

Trong trường hợp SIEM phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SIEM đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

1.3.3. Đồng bộ thời gian hệ thống

Trong trường hợp SIEM phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SIEM đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

1.4. Yêu cầu về log

1.4.1. Log quản trị hệ thống

a) SIEM cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i) Đăng nhập, đăng xuất tài khoản;

ii) Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii) Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

iv) Kích hoạt lệnh khởi động lại, tắt hệ thống;

v) Thay đổi thủ công thời gian hệ thống.

b) SIEM cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i) Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy trạm;

iii) Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,…);

iv) Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,…);

v) Kết quả thực hiện hành vi (thành công hoặc thất bại).

vi) Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,…).

1.4.2. Log cảnh báo

SIEM cho phép ghi log cảnh báo được sinh ra bởi việc thực thi tập luật bảo vệ.

1.4.3. Định dạng log

SIEM cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

1.4.4. Quản lý log

SIEM cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,…).

b) Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép phân nhóm log thành các nhóm sự kiện theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng, các dạng tấn công, các nguồn log,…);

d) Cho phép truy xuất dữ liệu thô của log thông qua kết quả tìm kiếm và cảnh báo;

e) Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra log.

1.4.5. Cách thức tiếp nhận log

SIEM cho phép tiếp nhận log gửi từ Collector thông qua các cách thức sau:

a) Tiếp nhận log qua kết nối UDP;

b) Tiếp nhận log qua kết nối TCP không mã hóa;

c) Tiếp nhận log qua kết nối TCP có mã hóa như TLS hoặc tương đương.

1.4.6. Chuẩn hóa log

SIEM cho phép tiếp nhận và chuẩn hóa log gửi từ Collector theo tối thiểu 10 loại log khác nhau đáp ứng các yêu cầu sau:

a) Chuẩn hóa được log theo các định dạng tệp tin cơ bản tối thiểu với 01 trong các định dạng bao gồm: SYSLOG, JSON, CSV, CEF, NETFLOW;

b) Chuẩn hóa được log của hệ điều hành Windows và Unix;

c) Chuẩn hóa được log của tối thiểu 02 loại tường lửa khác nhau;

d) Chuẩn hóa được log của tối thiểu 04 loại thiết bị mạng khác nhau.

1.4.7. Đồng bộ hóa thời gian log

SIEM cho phép đồng bộ hóa thời điểm log được tiếp nhận tại Receiver và thời điểm log được thu thập tại Collector dựa trên cài đặt về múi giờ đã được thiết lập.

1.4.8. Lưu trữ log dưới dạng dữ liệu thô

SIEM cho phép lưu trữ tất cả log dưới dạng dữ liệu thô bất kể có thể phân tích cú pháp được hay không.

1.4.9. Làm giàu thông tin

SIEM cho phép làm giàu thông tin cho log (ví dụ: phân giải chuỗi ký tự định danh thành tên tài khoản người dùng; lưu lại mốc thời gian sinh log theo múi giờ cục bộ tại máy trạm;…).

1.4.10. Giám sát hiệu năng quá trình tiếp nhận log

SIEM cho phép giám sát thông qua giao diện đồ họa các thông số hiệu năng sau của quá trình tiếp nhận log:

a) Số lần thử kết nối lại đến Collector;

b) Thông báo về kết nối không thành công đến Collector;

c) Số lượng tác vụ tiếp nhận log mà không được thực hiện thành công.

1.4.11. Giám sát log tiếp nhận được theo thời gian thực

SIEM cho phép giám sát thông qua giao diện đồ họa log gửi từ Collector đáp ứng các yêu cầu sau:

a) Cho phép tạo thống kê dữ liệu theo thời gian thực;

b) Cho phép tìm kiếm và tạo thống kê dữ liệu theo khoảng thời gian xác định.

1.4.12. Xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP

SIEM cho phép xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP tối thiểu theo định dạng IPv4 (ví dụ: xử lý truy vấn tìm kiếm dữ liệu bằng dải địa chỉ IP,…).

1.4.13. Truyền dữ liệu an toàn

SIEM cho phép mã hóa dữ liệu hoặc sử dụng giao thức có mã hóa để trao đổi dữ liệu giữa Collector và Receiver.

1.5. Yêu cầu về hiệu năng xử lý

SIEM được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất phải đảm bảo đáp ứng các yêu cầu sau:

SIEM cho phép xử lý và lưu trữ dữ liệu đồng thời 2000 EPS sự kiến.

Đảm bảo việc giữ nguyên, không thay đổi dữ liệu gốc nhận được. Có khả năng xây dựng index của dữ liệu mà không cần tuân theo lược đồ dữ liệu (schema).

Có khả năng tìm kiếm cùng lúc trên nhiều nguồn dữ liệu, nhiều định dạng.

1.6. Yêu cầu về chức năng tự bảo vệ

1.6.1. Phát hiện và ngăn chặn tấn công hệ thống

SIEM có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm tối thiểu các dạng sau:

a) SQL Injection;

b) OS Command Injection;

c) XPath Injection;

d) Remote File Inclusion (RFI);

đ) Local File Inclusion (LFI);

e) Cross-Site Scripting (XSS);

g) Cross-Site Request Forgery (CSRF).

1.6.2. Cập nhật bản vá hệ thống

SIEM có chức năng cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật. 1**.7. Yêu cầu về chức năng phân tích tương quan sự kiện và cảnh báo**

1.7.1. Phân tích tương quan sự kiện theo thời gian thực

SIEM cho phép phân tích tương quan sự kiện theo thời gian thực đối với dữ liệu log thu thập được.

1.7.2. Phân tích tương quan sự kiện sử dụng danh sách động

SIEM cho phép phân tích tương quan sự kiện sử dụng thông tin trong danh sách động (ví dụ: tạo luật để so khớp địa chỉ IP, tên miền hoặc giá trị hàm băm đối với một danh sách có thể được cập nhật tự động từ phía nhà sản xuất,…).

1.7.3. Cảnh báo theo thời gian thực

SIEM cho phép tự động cảnh báo tới người dùng theo thời gian thực đối với các loại sự kiện sau:

a) Cảnh báo về việc hệ thống ngừng lưu trữ thêm dữ liệu mới khi Storage đã đạt ngưỡng giới hạn lưu trữ mà không thể lưu được dữ liệu mới;

b) Cảnh báo về dấu hiệu, nguy cơ, sự cố, cuộc tấn công và các hành vi gây mất an toàn thông tin khác dựa trên kết quả thực thi luật phân tích tương quan sự kiện.

1.7.4. Cảnh báo về các nhóm đối tượng được giám sát

SIEM cho phép sinh cảnh báo chứa các thông tin thuộc nhóm đối tượng được giám sát (ví dụ: cảnh báo về việc có truy cập vào máy chủ email; cảnh báo có truy cập từ xa vào dải địa chỉ IP dành cho các máy chủ,…).

1.7.5. Cảnh báo theo nhiều phương thức

SIEM cho phép tự động cảnh báo theo các phương thức sau:

a) Hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo;

b) Cảnh báo qua phương thức gửi thư điện tử hoặc tin nhắn SMS.

1.8. Các yêu cầu khác

STT	Tiêu chí
1	Giải pháp SIEM sử dụng trong Soc nằm trong Top Leader bảng xếp hạng uy tín về SIEM như Forrester, Gartner hoặc tương đương.
2	Có khả năng sử dụng Data Model để tăng tốc hiệu suất tìm kiếm, phân tích dữ liệu từ nhiều loại dữ liệu khác nhau
3	Có khả năng che các thông tin nhạy cảm (masking) trong dữ liệu raw trước khi hiển thị lên dashboard, đảm bảo tính bí mật của thông tin (như thông tin tài khoản người dùng, thông tin mật khẩu…)
4	Trường hợp phát sinh lượng dữ liệu lớn hơn số lượng license hiện có của PVPOWER là 2000 EPS hoặc tương đương, hệ thống sẽ không drop đối với dữ liệu bị vượt quá mà vẫn đảm bảo tính toàn vẹn của dữ liệu thu thập
5	Có khả năng xâu chuỗi các sự kiện liên quan đến sự cố theo thời gian (kill chain) để hiểu rõ về vòng đời của cuộc tấn công (attack lifecycle)
6	Phát hiện mối đe dọa tiên tiến sử dụng mô hình học sâu (Deep Learning)
7	Sử dụng mô hình học máy được huấn luyện trước (Pre-trained ML Models)
8	Khả năng phát hiện tiến trình độc hại bằng mạng nơ-ron hồi tiếp (RNN)
9	Phân tích ngôn ngữ tự nhiên (NLP) cho cảnh báo và truy vấn rủi ro

2.2.2 2. Yêu cầu kỹ thuật của thành phần Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối (EDR - Endpoint Detection and Response).

2.1. Yêu cầu về tài liệu

Sản phẩm EDR có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

2.2. Yêu cầu về quản trị hệ thống

2.2.1. Quản lý vận hành

Sản phẩm EDR cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

b) Cho phép thay đổi thời gian hệ thống;

c) Cho phép thay đổi thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,…);

đ) Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;

e) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;

g) Cho phép xóa log; Lập lịch xóa log định kỳ để tối ưu hóa hệ thống là tiêu chí điểm cộng.

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất;

i) Cho phép gửi cảnh báo qua thư điện tử hoặc tin nhắn.

2.2.2. Quản trị từ xa

Sản phẩm EDR cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

2.2.3. Quản lý xác thực và phân quyền

Sản phẩm EDR cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu. Hệ thống đã được thiết lập trước, hoặc cho phép thiết lập độ phức tạp của mật khẩu để đảm bảo an toàn.

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm quyền và từng nhóm máy tính để phân vùng quản lý.

2.2.4. Quản lý báo cáo

Sản phẩm EDR cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML, CSV.

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra.

2.2.5. Quản lý tập luật bảo vệ

Sản phẩm EDR cho phép quản lý tập luật bảo vệ bao gồm các thao tác sau:

a) Thêm luật mới;

b) Tinh chỉnh luật;

c) Tìm kiếm luật;

d) Xóa luật;

đ) Kích hoạt/vô hiệu hóa luật;

e) Xuất tập luật ra tệp tin;

g) Khôi phục tập luật từ tệp tin;

h) Cập nhật tập luật được phát hành bởi nhà sản xuất.

2.2.6. Cập nhật tập luật bảo vệ

Sản phẩm EDR cho phép cập nhật tập luật bảo vệ đáp ứng các yêu cầu sau:

a) Cho phép tự động thông báo hoặc tự động tải về bản cập nhật mới cho quản trị viên;

b) Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới.

2.2.7. Quản lý tập trung các máy chủ/máy trạm

Sản phẩm EDR cho phép quản lý tập trung các máy chủ/máy trạm thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép quản lý tập trung các máy chủ/máy trạm trên tối thiểu hai nền tảng Window và Linux.

b) Quản lý thông tin trên máy chủ/máy trạm bao gồm các thông tin sau:

i. Địa chỉ IP, MAC, Tên máy, Hệ điều hành, Phiên bản của hệ điều hành;

ii. Trạng thái kết nối đến máy chủ quản trị;

iii. Thông tin phần cứng (CPU, RAM, Disk Capcity/Free)

iv. Thông tin bản vá trên máy chủ/máy trạm;

v. Trạng thái cập nhật thông tin từ máy chủ EDR;

vi. Chính sách được thiết lập và các vi phạm trên agent.

c) Có khả năng điều khiển agent tối thiểu bao gồm các chức năng sau:

i. Cho phép phân tích, xóa, sửa tệp tin lây nhiễm mã độc trên máy chủ/máy trạm;

ii. Cho phép điều khiển thay đổi các chính sách phát hiện, ngăn chặn mã độc trên các agent;

iii. Cho phép sửa giá trị thanh ghi để ngăn chặn mã độc tự khởi động trên máy chủ/máy trạm sau khi khởi động lại.

2.2.8. Đồng bộ dữ liệu với các hệ thống khác

Sản phẩm EDR cho phép kết nối với tối thiểu một trong các loại hệ thống sau để đồng bộ dữ liệu:

a) Tích hợp với hệ thống quản lý và phân tích sự kiện an toàn thông tin (SIEM);

b) Hệ thống Nền tảng tri thức mối đe dọa an toàn thông tin (TI);

c) Tích hợp hệ thống phân tích mã độc tự động.

2.2.9. Chia sẻ dữ liệu

Sản phẩm EDR cho phép kết nối, chia sẻ dữ liệu với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền theo hướng dẫn tại Văn bản số 2290/BTTTT- CATTT ngày 17/07/2018 của Cục An toàn thông tin.

2.3. Yêu cầu về kiểm soát lỗi

2.3.1. Bảo vệ cấu hình

Trong trường hợp EDR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), EDR đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình tập luật bảo vệ.

2.3.2. Bảo vệ dữ liệu log

Trong trường hợp EDR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), EDR đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

2.3.3. Đồng bộ thời gian hệ thống

Trong trường hợp EDR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), EDR đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

2.4. Yêu cầu về log

2.4.1. Log quản trị hệ thống

a) Sản phẩm EDR cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i. Đăng nhập, đăng xuất tài khoản;

ii. Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii. Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

iv. Kích hoạt lệnh khởi động lại, tắt hệ thống;

v. Thay đổi thủ công thời gian hệ thống.

b) Sản phẩm EDR cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i. Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii. Địa chỉ IP hoặc định danh của máy chủ/máy trạm;

iii. Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,…);

iv. Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, 7 xóa, cập nhật, hoàn tác,…);

v. Kết quả thực hiện hành vi (thành công hoặc thất bại);

vi. Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,…).

2.4.2. Log cảnh báo

Sản phẩm EDR cho phép ghi log cảnh báo được sinh ra khi thực thi tập luật bảo vệ.

2.4.3. Định dạng log

Sản phẩm EDR cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

2.4.4. Quản lý log

Sản phẩm EDR cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,…);

b) Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép phân nhóm log thành các nhóm sự kiện theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng, các dạng tấn công, các nguồn log,…);

d) Cho phép truy xuất dữ liệu thô của log thông qua kết quả tìm kiếm và cảnh báo;

đ) Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra log.

2.4.5. Lưu trữ log dưới dạng dữ liệu thô

Sản phẩm EDR cho phép lưu trữ tất cả log dưới dạng dữ liệu thô bất kể có thể phân tích cú pháp được hay không.

2.5. Yêu cầu về tài nguyên xử lý

a) Agent cài trên máy chủ/máy trạm sử dụng tài nguyên tối đa, đáp ứng yêu cầu sau:

i. CPU < 20% ; ii. RAM < 500 MB;

iii. Tốc độ truyền tải qua mạng: Tốc độ nhận < 2,7 KB/s, Tốc độ gửi < 0,4 KB/s.

b) Độ phủ phát hiện tấn công: Đối với các dạng tấn công được công bố từ các nguồn công khai, EDR bảo đảm độ phủ phát hiện tấn công đáp ứng trên 85% với tỷ lệ cảnh báo đúng >= 80%.

2.6. Yêu cầu về tính khả dụng của hệ thống

Sản phẩm EDR hỗ trợ phương án triển khai đáp ứng các yêu cầu về tính khả dụng sau:

a) Kênh kết nối giữa agent và máy chủ quản lý được mã hóa và có cơ chế xác thực;

b) Hỗ trợ triển khai theo mô hình High Availability (HA) hoặc Clustering;

c) Hỗ trợ cơ chế cân bằng tải (Load Balancing).

2.7. Yêu cầu về chức năng phát hiện và phản ứng (đáp ứng cơ bản theo quy định)

2.7.1. Phát hiện sự cố

Sản phẩm EDR có chức năng phát hiện sự cố đáp ứng các yêu cầu sau:

a) Cho phép phát hiện tấn công, mã độc dựa theo thông tin địa chỉ IP, tên miền, giá trị băm và theo hành vi;

b) Cho phép người dùng chủ động thực hiện quét tại các tệp tin và thư mục khả nghi tại máy của mình;

c) Cho phép quản lý cảnh báo; xem chi tiết thông tin cảnh báo; bổ sung, làm giàu thông tin cảnh báo;

d) Cho phép điều tra phản ứng trên một giao diện tập trung duy nhất.

2.7.2. Điều tra và phản ứng sự cố

Sản phẩm EDR có chức năng điều tra và phản ứng sự cố đáp ứng các yêu cầu sau:

a) Cho phép phân tích các tiến trình đang chạy từ xa trên máy chủ/máy trạm;

b) Cho phép tìm kiếm log trên máy chủ/máy trạm;

c) Cho phép thiết lập chính sách chặn các ứng dụng độc hại hoạt động trên máy chủ/máy trạm bằng cách định nghĩa đường dẫn/giá trị băm;

d) Cho phép chặn kết nối độc hại từ máy chủ/máy trạm bằng cách điều khiển tường lửa hệ điều hành trên máy chủ/máy trạm hoặc tường lửa được tích hợp trên EDR.

2.8. Các yêu cầu khác

2.8.1. Yêu cầu về điều tra phân tích chuyên sâu:

a) Thu thập dữ liệu điều tra chuyên sâu: Hỗ trợ thu thập dữ liệu phục vụ điều tra chuyên sâu trên máy chủ, máy trạm. Các loại dữ liệu có thể thu thập bao gồm tối thiểu: Agent Event, Browser, Drivers, Event Log, File System, Network, Persistence, Process, System Information, Task, Shell History, System Log

b) Thu thập bộ thông tin điều tra:

i. Hỗ trợ tự động thu thập bộ thông tin điều tra (triage collection/package) là ảnh chụp hệ thống quanh thời điểm diễn ra cảnh báo.

ii. Có thể tùy chỉnh để thu thập nhiều dữ liệu hơn phục vụ điều tra, bao gồm: User accounts, Disk listing, Volume listing, Registry hive list, Prefetch entries, System restore point.

c) Các loại khai thác có thể phát hiện: Các loại khai thác có thể ngăn chặn tối thiểu trên hệ điều hành Windows là: Return-oriented programming (ROP) attack, Reverse shell, Heap spray attack, Structured Exception Handling Overflow Protection (SEHOP) corruption, Null page exploit, Microsoft Office macro-based exploit, Access token privilege escalation detection

d) Giám sát, phát hiện các hành vi nghi ngờ dựa trên các dấu hiệu tấn công (Indicators): Hỗ trợ giám sát dựa trên các bộ luật các dấu hiệu tấn công (Indicators) theo thời gian thực bao gồm cả hệ điều hành Windows và Mac OSX, Linux để phát hiện các hành vi:

i. Truy cập trái phép vào các tài khoản

ii. Theo dõi chứng cứ và các tập tin thành phần

iii. Hoạt động C&C (command and control)

iv. Mã độc đã biết hoặc chưa biết

v. Dữ liệu mạng bất thường

vi. Các chương trình hợp lệ bị sử dụng bởi các mục đích độc hại

vii. Truy cập trái phép vào các tập tin

e) Cho phép cấu hình thêm các dấu hiệu bị tấn công: Cho phép tạo thủ công thêm các dấu hiệu bị tấn công (IOC - Indicator of compromised) để phát hiện các mối hiểm họa đặc thù trong hệ thống.

f) Săn tìm các mối nguy: Hỗ trợ trợ tìm kiếm nhanh các hành vi nghi ngờ và nhận diện và xác định mức độ của các mối nguy hại cho hàng chục nghìn máy tính trong thời gian tình bằng phút.

g) Hệ điều hành hoạt động: Hỗ trợ các hệ điều hành: Windows, Windows Server, Linux, Ubuntu, MacOS

2.8.2. Yêu cầu về phát hiện mối nguy và chủ động phản ứng cụ thể và nâng cao

a) Thu thập thông tin, phân tích phát hiện mối nguy liên tục, quan trắc và phát hiện các mối đe dọa, cung cấp ngữ cảnh

b) Trợ giúp điều tra bằng trí tuệ nhân tạo: Trợ giúp dẫn hướng điều tra sử dụng sức mạnh của máy học hoặc trí tuệ nhân tạo để thu thập các mảnh thông tin, các dòng sự kiện, …

c) Dẫn hướng điều tra: Sử dụng trí tuệ nhân tạo (AI) để dẫn hướng dạng hỏi đáp, hiển thị các thông tin phát hiện chính, trợ giúp điều tra tập trung vào các thông tin quan trọng, nhanh chóng

d) Các thông tin khi tìm kiếm thời gian thực: Tìm kiếm theo thời gian thực tối thiểu các thông tin sau: thông tin về các tiến trình, file, kết nối mạng, Registry của Windows, thông tin của các máy, thông tin của Browser, ..

e) Hành động ứng phó: Có sẵn các công cụ/hành động cho phép thực hiện các hành động khắc phục, phản ứng nhanh như kill process, xóa file hoặc cách ly máy tính.

f) Các hành động phản ứng: Công cụ phản ứng có sẵn tối thiểu gồm: loại bỏ cây tiến trình, tiến trình theo has, tên, đường dẫn, xóa file, xóa thư mục, xóa giá trị của register, cách lý máy tính, ngừng cách ly, Dump tiến trình ra file, thực thi đăng xuất, khởi động hoặc shutdown hệ thống

g) Các thông tin khi tìm kiếm thời gian thực: Tìm kiếm theo thời gian thực tối thiểu các thông tin sau: thông tin về các tiến trình, file, kết nối mạng, Registry của Windows, thông tin của các máy, thông tin của Browser, ..

2.8.4. Yêu cầu về quản lý tập trung

a) Tính năng quản lý tập trung:

i. Xử lý thông tin liên lạc với Agent thu thập và lưu trữ dữ liệu trong cơ sở dữ liệu

ii. Chức năng quản lý, áp dụng chính sách theo cấu trúc quản lý của doanh nghiệp, theo sites, đơn vị phòng ban hoặc theo cấu trúc của active directory.

b) Hành động khắc phục nhanh: Người quản trị có thể thực hiện các hành động khắc phục, ứng cứu tự động theo các điều kiện và hành động cấu hình sẵn, hoặc gán nhãn cho máy tính đang điều tra để áp dụng các chính sách thắt chặt an ninh

c) Giám sát hành động phản ứng: Ghi lại lịch sử các hành động phản ứng, ứng phó của các cán bộ vân hành

d) Thống kê hiệu quả hoạt động: Thống kê các trường hợp phân tích, các phát hiện, thời gian làm việc trên hệ thống, điều tra phân tích.

2.2.3 3. Yêu cầu kỹ thuật của thành phần Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR – Security Orchestration, Automation and Response).

3.1. Yêu cầu về tài liệu

SOAR có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

3.2. Yêu cầu về quản trị hệ thống

3.2.1. Quản lý vận hành

SOAR cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình thu thập cảnh báo, cấu hình kịch bản, cấu hình thành phần tích hợp;

b) Cho phép thay đổi thời gian hệ thống;

c) Cho phép thay đổi thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,…);

đ) Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;

e) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;

g) Cho phép xóa log;

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

3.2.2. Quản trị từ xa

SOAR cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

3.2.3. Quản lý xác thực và phân quyền

SOAR cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

3.2.4. Quản lý báo cáo

SOAR cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm cảnh báo, sự kiện để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML.

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra;

e) Cho phép đặt lịch gửi báo cáo định kỳ tới email được cấu hình;

g) Cho phép tạo báo cáo hiệu năng hoạt động của SOAR thông qua tối thiểu 02 thông số sau: thời gian trung bình để xác nhận một sự cố an toàn thông tin, thời gian trung bình để xử lý một sự cố an toàn thông tin kể từ lúc xác nhận;

h) Cho phép tạo báo cáo hiệu quả công việc của từng người tham gia xử lý cảnh báo thông qua tối thiểu 02 thông số sau: số lượng cảnh báo được xử lý trên mỗi người, số lượng cảnh báo được xử lý đúng hạn trên mỗi người.

3.3. Yêu cầu về kiểm soát lỗi

3.3.1. Bảo vệ cấu hình

Trong trường hợp SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình thu thập cảnh báo;

đ) Cấu hình kịch bản;

e) Cấu hình thành phần tích hợp.

3.3.2. Bảo vệ dữ liệu log, cảnh báo, tình huống và bằng chứng

Trong trường hợp SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR đảm bảo dữ liệu log, cảnh báo, tình huống và bằng chứng đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

3.3.3. Đồng bộ thời gian hệ thống

Trong trường hợp SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), SOAR đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

3.4. Yêu cầu về log

3.4.1. Log quản trị hệ thống

a) SOAR cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i) Đăng nhập, đăng xuất tài khoản;

ii) Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii) Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình thu thập cảnh báo, cấu hình kịch bản;

iv) Kích hoạt lệnh khởi động lại, tắt hệ thống;

v) Thay đổi thủ công thời gian hệ thống;

b) SOAR cho phép ghi log quản trị hệ thống bao gồm các trường thông tin sau:

i) Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy trạm;

iii) Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,…);

iv) Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,…);

v) Kết quả thực hiện hành vi (thành công hoặc thất bại);

vi) Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,…).

3.4.2. Định dạng log

SOAR cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

3.4.3. Quản lý log

SOAR cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,…).

b) Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra log.

3.5. Yêu cầu về hiệu năng xử lý

SOAR được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất phải đảm bảo đáp ứng các yêu cầu sau:

3.5.1. Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu

SOAR đảm bảo rằng độ trễ thời gian tìm kiếm log, cảnh báo và tình huống với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 01 phút.

3.5.2. Thu thập đồng thời nhiều cảnh báo

SOAR cho phép thu thập, xử lý và lưu trữ dữ liệu đồng thời 100 cảnh báo trong khoảng thời gian là 01 phút.

3.6. Yêu cầu về chức năng điều phối xử lý và giám sát

3.6.1. Điều phối xử lý cảnh báo

SOAR cho phép điều phối xử lý cảnh báo đáp ứng các yêu cầu sau:

a) Cho phép thiết lập cấu hình thu thập cảnh báo từ các giải pháp an toàn thông tin, công nghệ thông tin khác (ban đầu các cảnh báo được gán trạng thái là mới);

b) Cho phép tìm kiếm cảnh báo theo từ khóa trên tất cả các trường thông tin của cảnh báo bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép lưu trữ và phân nhóm cảnh báo theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng của cảnh báo, nguồn gửi cảnh báo,…);

d) Cho phép thực hiện xử lý cảnh báo, trong đó bao gồm tối thiểu các thao tác xử lý sau: cập nhật trạng thái xử lý, cập nhật bằng chứng thu thập được, cập nhật kết quả xử lý;

đ) Cho phép cập nhật trạng thái xử lý cảnh báo, trong đó bao gồm tối thiểu các giá trị trạng thái xử lý sau: mới, đang xử lý, đã xử lý;

e) Cho phép cập nhật kết quả xử lý cảnh báo, trong đó bao gồm tối thiểu các giá trị kết quả xử lý sau: cảnh báo thật, cảnh báo giả;

g) Cho phép cập nhật bằng chứng thu thập được, trong đó bao gồm tối thiểu các thao tác sau: tải lên tệp tin bằng chứng, nhập nội dung text;

h) Cho phép xem lại lịch sử xử lý cảnh báo, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm thực hiện, người thực hiện, nội dung thực hiện;

i) Cho phép thiết lập thời hạn xử lý cảnh báo;

k) Cho phép xác định thời gian xử lý cảnh báo có bị quá hạn hay không;

l) Cho phép áp dụng thực hiện một kịch bản với cảnh báo.

3.6.2. Điều phối xử lý tình huống

SOAR cho phép điều phối xử lý tình huống đáp ứng các yêu cầu sau:

a) Cho phép tạo một tình huống bằng việc nhóm một hoặc nhiều cảnh báo thành tình huống đó (ban đầu các tình huống được gán trạng thái là mở);

b) Cho phép tìm kiếm tình huống theo từ khóa trên tất cả các trường thông tin của tình huống bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép lưu trữ và phân nhóm tình huống theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng của tình huống, nguồn tạo tình huống,…);

d) Cho phép thực hiện xử lý tình huống, trong đó bao gồm tối thiểu các thao tác xử lý sau: cập nhật trạng thái xử lý, cập nhật kết quả xử lý;

đ) Cho phép cập nhật trạng thái xử lý tình huống, trong đó bao gồm tối thiểu các giá trị trạng thái xử lý sau: mở, đóng;

e) Cho phép cập nhật kết quả xử lý tình huống, trong đó bao gồm tối thiểu các giá trị kết quả xử lý sau: phát hiện đúng, phát hiện sai;

g) Cho phép xem lại lịch sử xử lý tình huống, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm thực hiện, người thực hiện, nội dung thực hiện;

h) Cho phép thiết lập thời hạn xử lý tình huống;

i) Cho phép xác định thời gian xử lý tình huống có bị quá hạn hay không;

k) Cho phép áp dụng thực hiện một kịch bản với tình huống;

l) Cho phép gán một hoặc nhiều người xử lý cho tình huống.

3.6.3. Giám sát và phân tích sự cố an toàn thông tin

SOAR cho phép giám sát và phân tích sự cố an toàn thông tin thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép hiển thị thông tin trực quan thể hiện mối liên kết giữa các đối tượng liên quan trong sự cố bằng đường đi và kèm thông tin của liên kết (nếu có), trong đó bao gồm tối thiểu các đối tượng sau: địa chỉ IP, địa chỉ email, tên miền;

b) Cho phép xem dòng thời gian của các sự kiện trong sự cố, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm xuất hiện, nội dung, các đối tượng có liên quan (nếu có), các bằng chứng thu thập được (nếu có);

3.7. Yêu cầu về chức năng tích hợp và tự động hóa

3.7.1. Quản lý thành phần tích hợp

SOAR cho phép quản lý cấu hình thành phần tích hợp thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại, cập nhật và xóa thành phần tích hợp đã được tạo;

b) Cho phép phát triển thành phần tích hợp thông qua tối thiểu 01 ngôn ngữ lập trình dạng thông dịch (ví dụ: Python, Javascript,…).

3.7.2. Hỗ trợ tích hợp nhiều nền tảng khác nhau

SOAR cho phép kết nối và tương tác với các nền tảng khác nhau, trong đó tối thiểu bao gồm:

a) Security Information and Event Management (SIEM) - Quản lý và phân tích sự kiện an toàn thông tin;

b) Threat Intelligence Platform (TIP) - Nền tảng tri thức mối đe dọa an toàn thông tin;

c) Endpoint Security - Đảm bảo an toàn thông tin cho thiết bị đầu cuối (ví dụ: Endpoint Detection and Response (EDR) - Phát hiện và ứng phó các mối đe dọa an toàn thông tin tại thiết bị đầu cuối; Endpoint Protection Platform (EPP) - Nền tảng bảo vệ thiết bị đầu cuối;…);

d) Network Security - Đảm bảo an toàn thông tin mạng (ví dụ: Network-based Intrusion Prevention System (NIPS) - Phòng, chống xâm nhập lớp mạng; Web Application Firewall (WAF) - Tường lửa ứng dụng web;…);

đ) Malware Analysis - Phân tích mã độc;

e) Ticketing System - Quản lý các yêu cầu cần giải quyết;

g) Identity and Access Management (IAM) - Quản lý định danh và truy cập.

3.7.3. Hỗ trợ tích hợp nhiều API

SOAR cho phép thiết lập cấu hình một hoặc nhiều API trên các thành phần tích hợp để ứng dụng nhiều nhất có thể các chức năng, tính năng mà nền tảng tích hợp cung cấp.

3.7.4. Hỗ trợ tích hợp API theo hai chiều

SOAR cho phép thiết lập cấu hình API trên các thành phần tích hợp để tương tác hai chiều với các nền tảng tích hợp:

a) Cho phép truy vấn dữ liệu từ nền tảng tích hợp để làm giàu thông tin cho các dữ liệu được xử lý và lưu trữ trên SOAR;

b) Cho phép thực thi lệnh tác động đến nền tảng tích hợp để thực hiện việc ứng phó sự kiện, cố an toàn thông tin.

3.7.5. Quản lý kịch bản

SOAR cho phép quản lý cấu hình kịch bản thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại, cập nhật và xóa kịch bản đã được tạo;

b) Cho phép xây dựng kịch bản với tối thiểu các thành phần sau: khối thực thi, đường đi giữa các khối, điều kiện rẽ nhánh;

c) Cho phép xây dựng kịch bản thông qua tối thiểu các thao tác sau để tương tác với loại thành phần trên: tạo mới, xem lại, cập nhật, xóa;

d) Cho phép xuất một kịch bản ra tệp tin và tải về tệp tin đã xuất;

đ) Cho phép tải lên tệp tin chứa một kịch bản và nhập kịch bản từ tệp tin đó;

e) Cho phép đưa một kịch bản đã được xây dựng trước đó vào một kịch bản.

3.7.6. Hỗ trợ thực hiện kịch bản tự động

SOAR cho phép thực hiện kịch bản tự động đáp ứng các yêu cầu sau:

a) Cho phép cấu hình kịch bản dựa theo các điều kiện, quy tắc tìm kiếm cảnh báo, tình huống để thực hiện tất cả các bước trong kịch bản mà không cần con người tương tác;

b) Cho phép thiết lập thời hạn thực hiện kịch bản;

c) Cho phép xác định thời gian thực hiện kịch bản có bị quá hạn hay không;

d) Cho phép xem lại lịch sử thực hiện của từng bước trong kịch bản, trong đó bao gồm tối thiểu các trường thông tin sau: tập dữ liệu đầu vào, tập dữ liệu đầu ra, thời điểm bắt đầu thực hiện, thời điểm kết thúc thực hiện, trạng thái thực hiện (thành công hoặc thất bại).

3.7.7. Hỗ trợ thực hiện kịch bản bán tự động

SOAR cho phép thực hiện kịch bản bán tự động đáp ứng các yêu cầu sau:

a) Cho phép thực hiện kịch bản dựa vào dữ liệu người dùng đưa vào, thông qua một hoặc một số các thao tác sau: nhập giá trị (số hoặc chuỗi ký tự), chọn một hoặc một số trong các giá trị có sẵn, tải lên tệp tin, thiết lập thời điểm bắt đầu tự động thực hiện, thiết lập thời hạn thực hiện;

b) Cho phép thiết lập thời hạn thực hiện kịch bản;

c) Cho phép xác định thời gian thực hiện kịch bản và từng bước trong kịch bản có bị quá hạn hay không;

d) Cho phép xem lại lịch sử thực hiện của từng bước trong kịch bản, trong đó bao gồm tối thiểu các trường thông tin sau: tập dữ liệu đầu vào, tập dữ liệu đầu ra, thời điểm bắt đầu thực hiện, thời điểm kết thúc thực hiện, trạng thái thực hiện (thành công hoặc thất bại), tài khoản người dùng có tương tác;

đ) Cho phép sử dụng kết quả thực hiện của bước trước đó làm dữ liệu đầu vào cho bước tiếp theo trong kịch bản;

e) Cho phép gán một hoặc nhiều người tương tác cho những bước trong kịch bản cần con người tương tác.

2.2.4 4. Yêu cầu kỹ thuật của thành phần Sản phẩm tri thức mối đe dọa an toàn thông tin (TI – Threat Intelligence).

4.1. Yêu cầu về tài liệu

TI có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

4.2. Yêu cầu về quản trị hệ thống

4.2.1. Quản lý vận hành

TI cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng;

b) Cho phép cấu hình thời gian hệ thống;

c) Cho phép cấu hình thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,...);

đ) Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;

e) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;

g) Cho phép xóa log;

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

4.2.2. Quản trị từ xa

TI cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

4.2.3. Quản lý xác thực và phân quyền

TI cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi dược độ phức tạp của mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

4.2.4. Quản lý báo cáo

TI cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML;

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra.

4.2.5. Chia sẻ dữ liệu

a) TI cho phép kết nối với các loại hệ thống sau để chia sẻ dữ liệu:

i) Các giải pháp và nền tảng khác loại (tối thiểu là SIEM);

ii) Hệ thống TI khác được phát triển bởi chính nhà sản xuất.

b) TI cho phép chia sẻ dữ liệu log thông tin mối đe dọa theo tối thiểu 01 trong các cách thức sau:

i) Chuẩn quốc tế STIX/TAXII;

ii) Đường dẫn URL (API).

4.3. Yêu cầu về kiểm soát lỗi

4.3.1. Bảo vệ cấu hình

Trong trường hợp TIP phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), TIP đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng.

4.3.2. Bảo vệ dữ liệu log

Trong trường hợp TI phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), TI đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

4.3.3. Đồng bộ thời gian hệ thống

Trong trường hợp TI phải khởi động lại do có lỗi phát sinh (ngoại trừ lồi phần cứng), TIP đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

4.4. Yêu cầu về log

4.4.1. Log quản trị hệ thống

a) TI cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i) Đăng nhập, đăng xuất tài khoản;

ii) Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii) Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng;

iv) Kích hoạt lệnh khởi động lại, tắt hệ thống;

v) Thay đổi thủ công thời gian hệ thống.

b) TI cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i) Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy trạm;

iii) Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,...);

iv) Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,...);

v) Kết quả thực hiện hành vi (thành công hoặc thất bại);

vi) Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,...).

4.4.2. Log thông tin mối đe dọa

a) TI cho phép thu thập và lưu trữ log thông tin mối de dọa từ phía nhà cung cấp sản phẩm TI.

b) TI cho phép thu thập và lưu trữ log thông tin mối đe dọa có các loại thông tin sau:

i) Mô tả tổng quan mối đe dọa;

ii) Mức độ nguy hiểm của mối đe dọa (severity level);

iii) Mức độ tin cậy về dữ liệu của mối đe dọa (confidence level);

iv) Các phân nhóm được gán cho mối đe dọa;

v) Các thuộc tính mô tả chi tiết mối đe dọa.

b) TI cho phép thu thập log thông tin mối đe dọa qua hai cách thức thủ công và tự động.

4.4.3. Log cảnh báo

TI cho phép ghi log cảnh báo được sinh ra bởi việc thực thi các thiết lập cảnh báo mối đe dọa.

4.4.4. Định dạng log

TI cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

4.4.5. Quản lý log

TI cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,...);

b) Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép tìm kiếm log thông tin mối đe dọa theo thời gian, giá trị băm của mã độc và phân nhóm;

d) Cho phép truy xuất log thông tin mối đe dọa thông qua cảnh báo;

đ) Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào TIP khác hoặc giải pháp khác về quản lý, phân tích, điều tra log.

4.4.6. Phân nhóm log thông tin mối đe dọa

TI cho phép phân loại và gắn nhãn tên phân nhóm cho log thông tin mối đe dọa theo các phân nhóm sau phục vụ cho mục đích tìm kiếm:

a) Điểm yếu, lỗ hổng an toàn thông tin đã được công bố;

b) Họ mã độc;

c) Kỹ thuật tấn công;

d) Chiến dịch tấn công;

d) Mục đích tấn công;

e) Loại đối tượng, tổ chức bị tấn công;

g) Đối tượng, tổ chức thực hiện tấn công;

h) Tên miền, địa chỉ IP của khách hàng có kết nối đến cơ sở hạ tầng của đối tượng, tổ chức thực hiện tấn công;

i) Điểm yếu, lỗ hổng an toàn thông tin đối với hệ thống của khách hàng.

4.5. Yêu cầu về hiệu năng xử lý

TI được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất phải đảm bảo đáp ứng các yêu cầu sau:

a) TI đảm bảo rằng độ trễ thời gian tìm kiếm log với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 02 phút;

b) Dữ liệu tri thức các mối đe dọa của TI có tối thiểu 100.000 bản ghi.

4.6. Yêu cầu về chức năng tự bảo vệ

4.6.1. Phát hiện và ngăn chặn tấn công hệ thống

TI có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm tối thiểu các dạng sau:

a) SQL Injection;

b) OS Command Injection;

c) XPath Injection;

d) Remote File Inclusion (RFI);

đ) Local File Inclusion (LFI);

e) Cross-Site Scripting (XSS);

g) Cross-Site Request Forgery (CSRF).

4.6.2. Cập nhật bản vá hệ thống

TI có chức năng cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật.

4.7. Yêu cầu về chức năng thống kê xu hướng và cảnh báo mối de dọa

4.7.1. Thống kê xu hướng mối đe dọa trên thế giới

TI có chức năng cho phép thống kê các mối đe dọa trên thế giới thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép thống kê xu hướng mối đe dọa dưới dạng biểu đồ;

b) Cho phép tìm kiếm dữ liệu xu hướng mối đe dọa theo thời gian (tối thiểu theo 04 mức: năm, quý, tháng, ngày).

4.7.2. Quản lý thiết lập cảnh báo

TI có chức năng cho phép quản lý thiết lập cảnh báo mối đe dọa đến người dùng đáp ứng các yêu cầu sau:

a) Cho phép nhận cảnh báo theo các phân nhóm được mô tả ở 4.6;

b) Cho phép thiết lập thời gian nhận cảnh báo;

c) Cho phép tải nội dung cảnh báo dưới dạng tập tin;

d) Cho phép hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo;

đ) Cho phép nhận cảnh báo qua phương thức gửi thư điện tử hoặc tin nhắn SMS.

2.3 II. Yêu cầu kỹ thuật phần cứng

Nhà thầu cần đề xuất phương án, cấu hình phần cứng và hạ tầng phù hợp để đảm bảo triển khai, vận hành ổn định các hệ thống SIEM, SOAR, EDR…theo các yêu cầu sau:

2.3.1 1. Máy chủ vật lý triển khai

Nhà thầu đề xuất máy chủ vật lý với cấu hình đủ mạnh để triển khai các máy ảo (VM) phục vụ các thành phần hệ thống SOC (theo mô hình giải pháp của nhà thầu) như: SIEM (phân tích và lưu trữ log), EDR Server, Forwarder/Collector (nếu có) v.v...

Các máy chủ phải hỗ trợ nền tảng ảo hóa (VMware ESXi, Hyper-V...) theo thiết kế triển khai của nhà thầu.

Bao gồm đầy đủ bản quyền phần mềm cần thiết để vận hành như:

- Hệ điều hành máy chủ (nếu cần).
- Bản quyền ảo hóa (nếu áp dụng).
- Các license quản trị hoặc giám sát phần cứng (nếu có).

2.3.2 2. Thiết bị và phụ kiện phụ trợ.

Nhà thầu có tránh nhiệm khảo sát hệ thống, lập danh mục và cung cấp đầy đủ các thiết bị, phụ kiện cần thiết để đảm bảo khả năng triển khai, kết nối và giám sát hệ thống, bao gồm:

- Module quang/RJ45 tốc độ xử lý tối thiểu 10Gb tương thích với switch hiện hữu của PVPOWER (switch EXTREME X590).
- Cáp quang/cáp mạng phục vụ kết nối với switch hoặc thiết bị giám sát.

- Thiết bị phục vụ sao chép lưu lượng mạng (Network TAP hoặc thiết bị tách lưu lượng) trong trường hợp switch, máy chủ không hỗ trợ port mirroring, logging.
- Các thiết bị phụ trợ khác nếu cần thiết để đảm bảo hệ thống hoạt động đầy đủ theo thiết kế (nguồn dự phòng, rail kit, shelf…)

2.3.3 3. Khả năng đáp ứng hiệu năng xử lý.

- Hạ tầng đề xuất phải đủ năng lực xử lý phù hợp với quy mô hệ thống, đảm bảo khả năng thu thập, xử lý, lưu trữ và phân tích log/sự kiện an toàn thông tin từ toàn bộ hệ thống CNTT theo yêu cầu đầu bài.

2.3.4 4. Đảm bảo độ tin cậy và sẵn sàng hoạt động.

- Hạ tầng phải hỗ trợ các cơ chế bảo vệ mức hệ thống, đảm bảo tính liên tục dịch vụ và giảm thiểu thời gian gián đoạn.
- Ưu tiên thiết kế giải pháp có tính sẵn sàng cao (High Availability) và khả năng khôi phục khi xảy ra sự cố.

2.3.5 5. Khả năng tích hợp, tương thích, mở rộng.

- Phần cứng và kiến trúc triển khai phải đảm bảo khả năng tích hợp tốt với các giải pháp bảo mật hiện có và các nền tảng CNTT khác nhau của đơn vị. Máy chủ và thiết bị phụ trợ phải đảm bảo khả năng mở rộng tài nguyên (CPU, RAM, ổ cứng, cổng mạng…) trong tương lai khi khối lượng log và event tăng lên;
- Hỗ trợ triển khai linh hoạt: có thể triển khai trên nền tảng vật lý, ảo hóa hoặc container tùy theo điều kiện hạ tầng hiện hữu.
- Đảm bảo tương thích với các thiết bị mạng, giải pháp bảo mật và hệ thống hiện có của PV Power.

2.3.6 6. An toàn và bảo mật.

- Đáp ứng các yêu cầu bảo mật vật lý và bảo mật truy cập đối với thiết bị hạ tầng.
- Có khả năng phân vùng bảo mật, kiểm soát truy cập, và theo dõi nhật ký hoạt động của các thành phần phần cứng.
- Cách ly các thành phần triển khai khỏi các mạng sản xuất hoặc mạng ngoài (Internet) tại PV Power bằng các biện pháp như VLAN, Firewall, DMZ…
- Truy cập từ bên ngoài vào mạng PV Power phải sử dụng kết nối an toàn (VPN, kênh truyền riêng…).
- Tất cả các máy chủ, thiết bị lưu trữ log (SIEM), thiết bị thu thập log (Collector, Agent) và các công cụ phân tích phải được cập nhật bản vá định kỳ.
- Các máy chủ cài của hệ thống Soc phải được cài đặt phần mềm chống mã độc và được kiểm soát quyền truy cập.
- Tất cả các đăng nhập vào hệ thống phải được ghi lại và giám sát.

- Sử dụng mô hình quyền tối thiểu cần thiết đối với các tài khoản quản trị của các thành phần hệ thống. Không để một người có toàn quyền kiểm soát toàn bộ hệ thống.
- Dữ liệu log, event..phải được mã hóa khi lưu trữ và truyền tải.
- Nhân viên vận hành SOC phải được kiểm tra lý lịch và cam kết bảo mật.
- Có quy trình rõ ràng cho dịch vụ giám sát, xử lý sự cố, ứng cứu khẩn cấp và phục hồi sau tấn công.
- Định kỳ kiểm tra, rà soát và cập nhật chính sách bảo mật SOC.

2.4 II. Yêu cầu kỹ thuật dịch vụ triển khai ban đầu

Đơn vị cung cấp dịch vụ cần thực hiện đầy đủ các bước triển khai hệ thống Trung tâm Điều hành An toàn thông tin (SOC) ban đầu theo trình tự dưới đây. Từng bước phải đảm bảo đáp ứng yêu cầu kỹ thuật, tính khả thi, an toàn và hiệu quả trong thực tế vận hành tại PV Power.

2.4.1 1. Khảo sát hệ thống hiện hữu.

Nhà thầu phải tiến hành khảo sát toàn bộ hệ thống CNTT hiện hữu của PV Power để:

- Đánh giá hiện trạng hạ tầng mạng, máy chủ, hệ thống bảo mật, ứng dụng.
- Xác định phạm vi cần giám sát an toàn thông tin (log source, sự kiện, thiết bị...).
- Kiểm tra khả năng tích hợp và gửi log từ hệ thống hiện hữu đến hệ thống SOC.
- Thống nhất các ràng buộc kỹ thuật và chính sách nội bộ (nếu có).

2.4.2 2. Đề xuất phương án triển khai.

Căn cứ trên kết quả khảo sát, nhà thầu thực hiện:

- Đề xuất giải pháp triển khai hệ thống SOC phù hợp với quy mô, mô hình vận hành và yêu cầu bảo mật của PV Power.
- Thiết kế kiến trúc tổng thể bao gồm các thành phần SIEM, SOAR, EDR, TI...
- Xác định phương án thu thập log phù hợp: trực tiếp, qua agent, qua thiết bị tách lưu lượng mạng (network TAP)...
- Đề xuất danh mục phần cứng, phần mềm, bản quyền và hạ tầng cần cung cấp.

Yêu cầu: Phương án phải đảm bảo khả năng mở rộng, tính sẵn sàng cao và tính tương thích với hệ thống hiện hữu.

2.4.3 3. Lắp đặt, cấu hình hệ thống (phần cứng, phần mềm liên quan).

a. Phần cứng.

Nhà thầu thực hiện:

- Lắp đặt máy chủ vật lý, thiết bị mạng và các thiết bị phụ trợ.
- Triển khai nền tảng ảo hóa (vCenter, KVM, Hyper-V…) để cài đặt các máy chủ ảo phục vụ SOC.

- Cài đặt các máy chủ ảo cho từng thành phần: SIEM, EDR Server, Dashboard, v.v.
- Cấu hình tài nguyên phù hợp cho từng máy chủ (CPU, RAM, Storage, NIC…).

b.Phần mềm.

Nhà thầu thực hiện:

- Cài đặt và cấu hình đầy đủ các thành phần phần mềm SOC, bao gồm:
  + SIEM: thu thập log, correlation rule, dashboard, cảnh báo.
  + SOAR: tích hợp hệ thống và xây dựng playbook xử lý sự cố.
  + EDR: triển khai agent, giám sát endpoint, tích hợp SIEM/SOAR.
  + Threat Intelligence: đồng bộ IOC và enrich dữ liệu.
- Tối ưu hệ thống để đảm bảo hiệu suất và độ tin cậy.

2.4.4 4. Tinh chỉnh các tập luật trên các hệ thống SIEM, SOAR, EDR…phù hợp với hệ thống hiện hữu.

Nhà thầu thực hiện:

- Xây dựng và tinh chỉnh các tập lệnh, rule và kịch bản vận hành phù hợp hệ thống của PV Power, bao gồm:
  + Correlation rule trong SIEM;
  + Playbook phản ứng trong SOAR;
  + Chính sách phân quyền truy cập, lọc log, IOC whitelist.
- Cập nhật cấu hình nhằm giảm false positive, nâng cao khả năng cảnh báo đúng.

2.4.5 5. Đào tạo.

Nhà thầu có trách nhiệm:

- Tổ chức đào tạo cho nhân sự PV Power về luồng quy trình phối hợp; phân tích, tổng hợp thông tin cảnh báo; sử dụng các công cụ, giải pháp được trang bị để điều tra, xác định nguyên nhân sự cố bao gồm:
  + Cách tiếp nhận cảnh báo, báo cáo từ hệ thống SOC.
  + Quy trình phản hồi, cung cấp thông tin phục vụ điều tra sự cố.
  + Cách truy cập dashboard theo dõi cảnh báo (nếu được phân quyền).
  + Đào tạo về các Module liên quan như:

STT	Module	Nội dung
1	Cài đặt hệ thống giám sát	Nắm được kiến trúc tổng thể của hệ thống giám sát SIEM
2	Tích hợp các thành phần hệ thống	Giới thiệu, hướng dẫn tích hợp các thành phần của hệ thống SIEM

STT	Module	Nội dung
3	Tích hợp LogSources	Giới thiệu, hướng dẫn tích hợp LogSources của hệ thống vào SIEM
4	Giám sát và phân tích sự cố ATTT	Hướng dẫn sử dụng chức năng Offense để giám sát và phân tích sự cố ATTT
5	Quản lý Event và Flows	Giới thiệu Event và Flows trong hệ thống giám sát SIEM
6	Quản lý Dashboard, Reports	Hướng dẫn cách theo dõi trên Dashboard và cách xuất báo cáo
7	Giới thiệu và vận hành SOAR	Hướng dẫn vận hành Playbook tự động hóa xử lý sự cố bằng nền tảng SOAR
8	Giám sát và vận hành EDR	Giới thiệu chức năng giám sát Endpoint, cách phát hiện và phản ứng với hành vi bất thường

- Cung cấp đầy đủ các tài liệu đào tạo liên quan:
  + Tài liệu liên quan đến các Module đào tạo;
  + Sơ đồ hệ thống SOC đã triển khai;
  + Tài liệu mô tả quy trình xử lý sự cố, mô hình vận hành SOC theo TIER;
  + Các biểu mẫu phối hợp, biểu mẫu yêu cầu hỗ trợ kỹ thuật, mẫu báo cáo định kỳ.

2.4.6 6. Vận hành thử nghiệm hệ thống và bàn giao đưa vào sử dụng chính thức.

- Nhà thầu phải thực hiện giai đoạn vận hành thử dịch vụ SOC tối thiểu 30 ngày, để đánh giá:
  + Tính ổn định của hệ thống.
  + Khả năng phát hiện và cảnh báo các sự kiện an toàn thông tin thực tế.
  + Quy trình phối hợp giữa PV Power và đội ngũ vận hành SOC của nhà thầu.
- Trong giai đoạn này, nhà thầu phải:
  + Chủ động phân tích, phân loại và phản ứng với các sự kiện an ninh, tiếp tục tinh chỉnh rule, kịch bản để lọc bớt false positive.
  + Phối hợp với PV Power để điều tra và xử lý các sự cố phát sinh (nếu có).
- Sau khi kết thúc giai đoạn vận hành thử và đáp ứng đầy đủ các yêu cầu kỹ thuật, nhà thầu tiến hành bàn giao:
  + Biên bản nghiệm thu kỹ thuật hệ thống SOC.
  + Tài liệu hướng dẫn vận hành, báo cáo thử nghiệm.

+ Các tài khoản truy cập dashboard (nếu có), mẫu biểu báo cáo, phương án duy trì dịch vụ chính thức.

2.5 III. Yêu cầu dịch vụ giám sát và phản ứng ATTT

Dịch vụ giám sát và phản ứng an toàn thông tin 24/7 (SOC Managed Security Service) giúp giám sát, xử lý các vấn đề về an toàn thông tin để phát hiện, phân tích, phản ứng, ngăn chặn và điều tra truy vết với các sự cố về an toàn thông tin, đảm bảm an toàn, an toàn thông tin cho một tổ chức.

Dịch vụ là tổng hòa của ba yếu tố: **Quy trình**, **Con người** và **Công nghệ**.

- **Con người:** Là những chuyên gia trong lĩnh vực an toàn thông tin, được đào tạo bài bản để để giám sát, phát hiện sự cố, ngăn chặn sự số, điều tra truy vết và phục hồi tổn thất mà một cuộc tấn công mạng gây ra.
- **Quy trình:** Là những quy trình chính sách, quy định, quy chế, khuyến nghị về công tác đảm bảo an toàn thông tin được một tổ chức ban hành.
- **Công nghệ:** Là những giải pháp kỹ thuật, công cụ chuyên môn, hỗ trợ việc giám sát, phát hiện, ngăn chặn và điều tra truy vết các sự cố về an toàn thông tin.

2.5.1 1. Yêu cầu về quy trình

- Xây dựng quy chế quản lý SOC (quy định chung bao gồm quyền hạn, trách nhiệm của cá nhân, tổ chức liên quan).
- Xây dựng quy trình, tài liệu liên quan đến vận hành SOC (thiết kế, thiết lập, vận hành, nâng cấp…): Quy trình, tài liệu đảm bảo có đủ các mục như mô hình, vận hành, giám sát, phối hợp xử lý, quy trình xử lý sự cố, báo cáo định kỳ. Tất cả các quy trình cần được lập thành tài liệu, trình bày rõ vai trò đầu vào, đầu ra, công cụ sử dụng, biểu mẫu đính kèm.
- Bàn giao toàn bộ quy trình và hướng dẫn triển khai thực tế, phục vụ kiểm tra, đánh giá hoặc Audit.

a.Quy trình tiếp nhận và xử lý cảnh báo an toàn thông tin.

- Quy định cụ thể cách tiếp nhận cảnh báo từ SIEM, EDR…hoặc hệ thống cảnh báo khác.
- Hướng dẫn phân loại mức độ nghiêm trọng (severity) của từng cảnh báo.
- Phân công nhân sự theo TIER để xử lý phù hợp với mức độ rủi ro.
- Đảm bảo ghi log toàn bộ quá trình xử lý, từ tiếp nhận đến phản hồi.

b. Quy trình điều tra và phân tích sự cố.

- Xác định rõ các bước điều tra sự cố (triage, log collection, timeline…).
- Phân tích nguyên nhân, mức độ ảnh hưởng, đối tượng bị tác động.
- Truy vết, phân tích IOC, dấu hiệu tấn công (TTP) liên quan.
- Kết luận bằng văn bản, gửi báo cáo sự cố kỹ thuật.

c.Quy trình ứng phó và khắc phục sự cố.

- Có playbook hoặc hướng dẫn xử lý cho từng loại sự cố phổ biến (phishing, malware, ransomware, brute force...).
- Xác định vai trò của từng TIER trong phản ứng sự cố.
- Quy định cách cô lập hệ thống, xử lý tạm thời và khôi phục dịch vụ.
- Phân biệt xử lý tự động (qua SOAR) và xử lý bán tự động/phê duyệt thủ công.

d. Quy trình phân tích và xử lý log.

- Quy định về chuẩn định dạng log, thời gian lưu giữ, phân loại nguồn log.
- Phân tích log để phát hiện hành vi bất thường, đánh giá rủi ro tiềm ẩn.
- Lập nhật ký truy vết log theo từng sự kiện để phục vụ điều tra.

e. Quy trình cập nhật IOC và quản lý Threat Intelligence.

- Cập nhật IOC từ nguồn TI (internal/external).
- Tích hợp IOC vào hệ thống SIEM/SOAR để phát hiện và phản ứng.
- Đánh giá độ tin cậy (confidence level) của IOC và xác định thời gian sử dụng.

f. Quy trình quản lý tài khoản và phân quyền.

- Quản lý tài khoản người dùng truy cập vào hệ thống SOC, SIEM, SOAR.
- Quy định phân quyền theo vai trò (RBAC): analyst, admin, viewer…
- Ghi nhận toàn bộ log truy cập và thao tác người dùng.

g. Quy trình bảo trì, cập nhật và backup hệ thống.

- Lập kế hoạch định kỳ cập nhật phần mềm, hệ điều hành, rule, IOC.
- Kiểm tra định kỳ hiệu suất hệ thống, tối ưu hóa alert rule, log storage.
- Quy định tần suất backup dữ liệu và kiểm tra phục hồi.

h. Quy trình đánh giá hiệu quả vận hành SOC.

- Theo dõi các chỉ số vận hành (KPI) như:
    + Tỷ lệ xử lý cảnh báo đúng.
    + Tỷ lệ false positive.
    + Thời gian phản ứng (MTTR).
- Đánh giá định kỳ hệ thống cảnh báo, playbook, báo cáo.

i. Quy trình phối hợp với PV Power.

- Hướng dẫn xử lý khi cần yêu cầu hỗ trợ từ phía PV Power (phê duyệt hành động, cung cấp log...).
- Biểu mẫu yêu cầu hỗ trợ, báo cáo sự cố, cảnh báo vượt quyền xử lý.
- Cơ chế liên lạc, phân cấp thẩm quyền phản ứng sự cố theo kịch bản.

j. Quy trình kiểm tra, rà soát và cải tiến hệ thống.

- Đánh giá định kỳ chất lượng cảnh báo, hiệu suất hệ thống.
- Cập nhật playbook theo sự kiện mới, hành vi tấn công mới (APT, zero-day...).
- Rà soát vai trò, phân quyền, kết nối hệ thống định kỳ để giảm thiểu rủi ro.

2.5.2 2. Yêu cầu về công nghệ

- Yêu cầu về công nghệ đã được nêu cụ thể, chi tiết tại mục A, II: Yêu cầu kỹ thuật phần mềm và A, III: Yêu cầu kỹ thuật phần cứng.
- Có cộng đồng người dùng rộng lớn, hỗ trợ kỹ thuật đầy đủ, roadmap phát triển rõ ràng.
- Trong trường hợp phát sinh lưu lượng log vượt quá giấy phép hiện tại (2000 EPS hoặc tương đương):
    + Hệ thống vẫn tiếp tục thu thập, ghi nhận và lưu trữ đầy đủ dữ liệu.
    + Tuyệt đối không được làm mất (drop) log, đảm bảo toàn vẹn dữ liệu để phục vụ giám sát và điều tra.

2.5.3 3. Yêu cầu về con người

Nhân sự tối thiểu 13 người đảm bảo vận hành hệ thống SOC cho PV Power (nhân sự trực 24/7, nhân sự hỗ trợ khách hàng xử lý các vấn đề phát sinh), cụ thể như sau:

Nhóm nhân sự	Số lượng tối thiểu	Trực ca
Tier 1 (Giám sát cơ bản)	06 người	02 người/ca, trực 24/7
Tier 2 (Phân tích sự cố)	03 người	Theo ca hoặc theo sự kiện
Tier 3 (Chuyên gia nâng cao)	02 người	Theo ca hoặc on-call
SOC Manager	01 người	Giám sát toàn bộ hoạt động
Threat Intelligence Analyst	01 người	Chuyên trách phân tích TI

Nhân sự phải có hồ sơ năng lực rõ ràng, bằng cấp và chứng chỉ phù hợp với từng vai trò, đảm bảo yêu cầu cụ thể như sau:

a. Tier 1 – nhân sự giám sát cơ bản.

- Tốt nghiệp ĐH chuyên ngành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định;
- Có kinh nghiệm ít nhất 1 năm trở lên;
- Có 1 trong các chứng chỉ CEH, Security+, CSA, CND hoặc tương đương;
- Có khả năng và năng lực giám sát Tier 1, chứng minh bằng việc nhân sự đã tham gia ít nhất 02 dự án Soc với vai trò Tier 1.
- Tiêu chí tính điểm cộng: Nhân sự có chứng chỉ OSCP, OSWE hoặc tương đương.

b. Tier 2 – nhân sự phân tích sự cố.

- Tốt nghiệp ĐH chuyên nghành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định;
- Có kinh nghiệm ít nhất 03 năm trở lên;
- Có ít nhất 01 trong các chứng chỉ: ECIH, CHFI, CEH, OSCP, OSWE hoặc tương đương;
- Tiêu chí tính điểm cộng: Có khả năng điều tra phân tích sự cố và mức độ ảnh hưởng của sự cố chứng minh bằng việc có tối thiểu 01 nhân sự có chứng chỉ tương ứng với giải pháp SIEM được cung cấp.

c. Tier 3 – nhân sự chuyên gia phân tích nâng cao.

- Có kinh nghiệm ít nhất 05 năm trở lên;
- Có 01 trong các chứng chỉ: CHFI, CTIA, OSCP, CHFI, OSCE, GSEC, OSCE3, GCFA, CISSP hoặc tương đương;
- Tiêu chí chấm điểm cộng khi đáp ứng các yêu cầu sau:

  + Có kinh nghiệm ít nhất 08 năm trở lên;

  + Có tối thiểu 02 trong các chứng chỉ nêu trên hoặc tương đương;

  + Có khả năng điều tra phân tích chuyên sâu, xây dựng và tinh chỉnh các use case, alerting rule, tích hợp các nguồn log, tối ưu hiệu suất hệ thống và hỗ trợ điều tra các sự cố nâng cao chứng minh bằng việc có tối thiểu 01 nhân sự có các chứng chỉ tương ứng với giải pháp SIEM được cung cấp;

d. Soc Manager.

- Tốt nghiệp đại học trở lên chuyên nghành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định;
- Có kinh nghiệm ít nhất 05 năm trở lên;
- Có 01 trong các chứng chỉ: CISA, CISSP, CISM, CCISO, ITIL Expert hoặc tương đương;
- Tiêu chí tính điểm cộng đối khi đáp ứng các yêu cầu sau:

  + Có kinh nghiệm ít nhất 10 năm trở lên.

  + Có khả năng quản lý dịch vụ/dự án và kiến thức bảo mật để đảm bảo khả năng giám sát đúng mục tiêu gói thầu chứng minh bằng việc nhân sự có chứng chỉ quản lý dự án.

e. Threat Intelligence Analyst.

- Tốt nghiệp đại học trở lên chuyên nghành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định;
- Có kinh nghiệm ít nhất 05 năm trở lên;
- Am hiểu hành vi tấn công của Hacker, có khả năng phân tích mối đe dọa và đề xuất biện pháp phòng chống;
- Nhân sự phải có tối thiểu 1 chứng chỉ quốc tế trong nhóm sau: CEH, ECIH, ECSA, SSCP, OSCP, OSEP, OSWE hoặc tương đương.

- Tiêu chí tính điểm cộng: khi nhân sự có tối thiểu 2 chứng chỉ quốc tế trong nhóm nêu trên.

2.5.4 4. Yêu cầu về chất lượng dịch vụ (SLA).

a. Thời gian hoạt động của dịch vụ

- Hệ thống SOC phải duy trì hoạt động giám sát an toàn thông tin **24/7/365**, bao gồm cả ngày nghỉ, ngày lễ.
- Trung tâm SOC của nhà cung cấp p- hải có nhân sự trực theo ca liên tục, đảm bảo khả năng phát hiện và xử lý cảnh báo mọi thời điểm.

b. Chỉ tiêu sẵn sàng và toàn vẹn dữ liệu

TT	Chỉ tiêu	Định mức tiêu chuẩn
1	Thời gian dịch vụ được khôi phục cơ bản khi xảy ra thảm họa	1 giờ
2	Thời gian dịch vụ khôi phục hoàn toàn khi xảy ra thảm họa	4 giờ
3	Thời gian lưu trữ dữ liệu PVPOWER	Lưu trữ dữ liệu trong vòng 12 tháng nếu PV POWER còn hợp đồng

c. Chỉ tiêu thời gian phản hồi và phối hợp xử lý sự cố

Mức độ sự cố	Định nghĩa	Thời gian phản hồi	Thời gian phối hợp xử lý
Mức 1 (nghiêm trọng)	Sự cố gây gián đoạn toàn bộ hệ thống, gây tổn thất nghiêm trọng, có dấu hiệu tấn công APT, mã độc lây lan rộng. Tấn công xảy ra, gây mất dịch vụ và ảnh hưởng nghiêm trọng, lan rộng, không thể phục hồi nếu không có kế hoạch khẩn cấp.	≤ 15 phút	≤ 2 giờ
Mức 2 (Cao)	Sự cố gây gián đoạn nghiêm trọng, phục hồi khó khăn, tổn thất đáng kể. Gián đoạn dịch vụ chính, mất dữ liệu quan trọng. Sự cố ảnh hưởng 1 phần hệ thống, có rủi ro cao nhưng chưa ảnh hưởng trực tiếp đến sản xuất. Mối đe dọa cao, có nguy cơ lan rộng hoặc ảnh hưởng lớn.	≤ 30 phút	≤ 4 giờ
Mức 3 (Trung bình)	Sự cố gây ảnh hưởng tới một phần hoạt động, có thể phục hồi trong thời gian cho phép. Suy giảm hiệu suất hệ thống, mất dữ liệu cục bộ. Mối đe dọa nghi ngờ hoặc cảnh báo chưa xác thực. Sự cố tiềm ẩn, có thể gây ảnh hưởng nếu không xử lý kịp thời.	≤ 2 giờ	≤ 24 giờ
Mức 4 (Thấp)	Cảnh báo dạng thông tin, sự kiện nghi ngờ, yêu cầu hỗ trợ kỹ thuật không khẩn cấp. Ảnh hưởng nhỏ, không gây gián đoạn đáng kể.	≤ 4 giờ	≤ 72 giờ

d. Chỉ tiêu mức độ phát hiện cảnh báo và xử lý

TT	Chỉ tiêu	Định mức tiêu chuẩn
	Độ khả dụng	≥ 99.7%
	Tỷ lệ xử lý lỗi đạt	≥ 99.5%
	Tỷ lệ không xảy ra sự cố nghiêm trọng	≥ 99,0%
	Tỷ lệ phát hiện cảnh báo đúng (True Positive)	≥ 90%
	Tỷ lệ cảnh báo sai (False Positive)	≤ 15%
	Tỷ lệ cảnh báo được xử lý trong thời gian SLA quy định	≥ 95%

e. Thời gian cung cấp báo cáo dịch vụ

Nhà thầu có trách nhiệm lập mẫu và thực hiện công tác báo cáo công việc như sau:

Loại báo cáo	Tần suất	Thời gian cung cấp
1. Báo cáo tháng		
- Báo cáo tổng hợp các sự vụ trong tháng, biện pháp và kết quả khắc phục; - Lưu lượng log hàng tháng và giải pháp tối ưu hệ thống; - Tình trạng phòng, chống mã độc trên hệ thống, hành vi tấn công trên hệ thống.	Hàng tháng (qua email)	Trước ngày 05 mỗi tháng
2. Báo cáo quý, năm		
- Báo cáo tổng hợp các sự vụ trong quý, năm biện pháp và kết quả khắc phục; - Lưu lượng log hàng quý, năm và giải pháp tối ưu hệ thống; - Tình trạng phòng, chống mã độc trên hệ thống, hành vi tấn công trên hệ thống.	Quý, năm (email, văn bản)	Trước ngày 30 tháng cuối cùng của Quý
3. Báo cáo sự cố		
- Báo cáo chi tiết về sự cố, nguyên nhân (nếu có), báo cáo tình trạng xử lý, đề xuất phương án xử lý.	Ngay khi xử lý xong sự cố mức 1, 2 (email, văn bản)	Trong vòng 05 ngày kể từ ngày xử lý xong sự cố.
4. Báo cáo đột xuất theo yc		
- Báo cáo đột xuất theo yêu cầu của PV Power.	(Email, văn bản)	Nhà thầu cần thống nhất tiêu chí thực hiện với PV Power, cam kết thời hạn hoàn thành báo cáo. Trong trường hợp thời hạn hoàn thành báo cáo không được PV Power xác định cụ thể, nhà thầu có trách nhiệm phản hồi và hoàn thiện báo cáo trong vòng 05 ngày làm việc

f. Khả năng hỗ trợ PV Power

- Nhà thầu có nghĩa vụ phối hợp với PV Power trong các trường hợp cần hỗ trợ điều tra sự cố, truy vết hành vi tấn công, hoặc chuẩn bị tài liệu kiểm tra.

- Kênh hỗ trợ chính thức: email, điện thoại, hệ thống ticket.
- Phản hồi hỗ trợ kỹ thuật thông thường: ≤ 4 giờ làm việc.

g. Đảm bảo dữ liệu và tính liên tục dịch vụ

- Không được để mất dữ liệu log, event trong quá trình vận hành hệ thống.
- Đảm bảo dữ liệu được mã hóa khi lưu trữ và truyền tải.
- Có phương án backup, khôi phục hệ thống SOC trong trường hợp gián đoạn/hỏng hóc thiết bị.

h. Chế tài vi phạm SLA

- Nếu nhà thầu không đáp ứng SLA đã cam kết, PV Power có quyền yêu cầu:
  + Giải trình nguyên nhân bằng văn bản.
  + Khắc phục trong vòng 3 ngày làm việc.
  + Trừ điểm đánh giá dịch vụ định kỳ, hoặc áp dụng hình thức chế tài theo hợp đồng (nếu có).

2.5.5 5. Yêu cầu về tiến độ, thời gian thực hiện

- Thời gian thực hiện gói thầu là 14 tháng, trong đó:
  + 02 tháng triển khai cài đặt, tích hợp hệ thống, tính từ thời điểm hai bên ký kết hợp đồng và hoàn thành các thủ tục đảm bảo bí mật, an toàn thông tin;
  + 12 tháng thuê dịch vụ giám sát và phản ứng ATTT 24/7, tính từ thời điểm bàn giao hệ thống;

2.5.6 6. Yêu cầu kiểm tra, nghiệm thu sản phẩm

- Kiểm tra, đánh giá chất lượng dịch vụ trong giai đoạn chuẩn bị cung cấp dịch vụ. Việc kiểm tra, đánh giá chất lượng dịch vụ được thực hiện thông qua vận hành thử và các phương pháp kiểm tra, đánh giá (nếu có).
- Kết quả kiểm tra, đánh giá chất lượng dịch vụ là cơ sở nghiệm thu, bàn giao dịch vụ để đưa vào sử dụng. Các tài liệu làm căn cứ nghiệm thu bao gồm:
  + Báo cáo kết quả vận hành thử;
  + Báo cáo kết quả kiểm tra, đánh giá (nếu có);
  + Các biên bản, tài liệu khác có liên quan.
- Chủ đầu tư và nhà cung cấp dịch vụ thống nhất, ký biên bản nghiệm thu, bàn giao dịch vụ để đưa vào sử dụng theo mẫu số 1 Phụ lục V của Thông tư số 16/2024/TT- BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông.

2.5.7 7. Yêu cầu về bảo mật thông tin.

Trong quá trình thực hiện việc quản trị vận hành hệ thống Soc PV Power, nhà thầu cam kết tuân thủ các nội dung sau:

a. Tuân thủ quy định của pháp luật và chính sách bảo mật

- Tuân thủ các quy định về an toàn, bảo mật thông tin theo các quy định pháp luật hiện hành của Việt Nam liên quan đến an toàn thông tin, an ninh mạng, bảo vệ dữ liệu.
- Tuân thủ tất cả các chính sách, quy định nội bộ về bảo mật thông tin và vận hành hệ thống do PV Power ban hành.

b. Cam kết bảo mật thông tin

- Nhà thầu và toàn bộ nhân sự tham gia dự án phải ký cam kết bảo mật thông tin (NDA) với PV Power trước khi bắt đầu triển khai.
- Cam kết bảo mật có hiệu lực trong suốt thời gian thực hiện hợp đồng và duy trì sau khi hợp đồng kết thúc.

c. Tuân thủ theo tiêu chuẩn bảo mật dịch vụ

- Dịch vụ được cung cấp phải đáp ứng các tiêu chuẩn bảo mật quốc tế, ưu tiên theo ISO/IEC 27001 hoặc tương đương.
- Đảm bảo đầy đủ ba nguyên tắc bảo mật cơ bản:
    + Tính sẵn sàng (Availability)
    + Tính toàn vẹn (Integrity)
    + Tính bảo mật (Confidentiality)

d. Quản lý nhân sự và truy cập hệ thống

- Chuyên gia của nhà thầu khi thực hiện công việc phải tuân thủ đầy đủ quy trình kiểm soát truy cập, ghi log thao tác, và phân quyền theo nguyên tắc "quyền tối thiểu cần thiết".
- Mọi thay đổi nhân sự trực tiếp tham gia dự án (bao gồm cả quản trị, giám sát và khắc phục sự cố) phải được thông báo bằng văn bản và được PV Power chấp thuận trước khi triển khai.

e. Sở hữu và sử dụng dữ liệu

- Toàn bộ dữ liệu, thông tin kỹ thuật, cấu hình hệ thống, log sự kiện và tài liệu phát sinh trong quá trình cung cấp dịch vụ được coi là tài sản tuyệt đối thuộc sở hữu của PV Power.
- Nhà thầu không được sử dụng, sao chép, trích xuất, chia sẻ hay chuyển giao bất kỳ thông tin nào nói trên nếu không có sự chấp thuận bằng văn bản của PV Power.

f. Nghĩa vụ bảo mật sau khi kết thúc hợp đồng

- Sau khi kết thúc hợp đồng, nhà thầu vẫn phải tiếp tục giữ bí mật mọi thông tin, dữ liệu liên quan đến hệ thống, thiết kế, vận hành, hợp đồng và dịch vụ.
- Tuyệt đối không được tiết lộ hoặc tái sử dụng thông tin cho bất kỳ mục đích nào, trừ khi có sự đồng ý chính thức của PV Power.

2.5.8 8. Yêu cầu về tích hợp với thành phần của hệ thống

- Cung cấp dịch vụ Điều phối bảo mật, tự động hóa và ứng phó (SOAR), bao gồm các tính năng tổng quan như:
  + Có hệ thống quản lý ticket đảm bảo có các thông tin chi tiết về sự cố, sự kiện.
  + Cho phép điều phối xử lý cảnh báo đáp ứng các yêu cầu của người quản trị.
  + Cho phép điều phối xử lý cảnh báo đáp ứng các yêu cầu của người quản trị.
  + Cho phép giám sát và phân tích sự cố an toàn thông tin thông qua giao diện đồ họa.
  + Có khả năng tích hợp với hệ thống Threat Intelligence.
- Cung cấp dịch vụ Điều phối bảo mật, tự động hóa và ứng phó (SOAR) cho phép quản lý báo cáo thông qua giao diện đồ họa:
  + Cho phép tạo, xem báo cáo đã được tạo.
  + Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước.
  + Cho phép áp dụng các quy tắc tìm kiếm cảnh báo, sự kiện để thêm, lọc, tinh chỉnh nội dung cho báo cáo.
  + Cho phép lựa chọn định dạng tệp tin báo cáo
  + Cho phép đặt lịch gửi báo cáo định kỳ tới email được cấu hình
  + Cho phép hiển thị thông tin trực quan thể hiện mối liên kết giữa các đối tượng liên quan trong sự cố bằng đường đi và kèm thông tin của liên kết (nếu có).
  + Cho phép xem dòng thời gian của các sự kiện trong sự cố, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm xuất hiện, nội dung, các đối tượng có liên quan, các bằng chứng thu thập được.
- Cung cấp dịch vụ Threat Intelligence phục vụ cho việc cung cấp thông tin tri thức tình báo hỗ trợ cho việc giám sát:
  + Có khả năng cung cấp thông tin về mối đe dọa mới nhất trong thời gian thực hoặc gần thời gian thực, xác minh thông tin từ các nguồn đáng tin cậy để giảm thiểu nguy cơ false positives hoặc false negatives
  + Có khả năng tích hợp tự động hoặc tích hợp với các hệ thống như SIEM, EDR và các công cụ phòng thủ khác để tối ưu hóa việc phát hiện và phản ứng với các mối đe dọa.
  + Cung cấp thông tin về các loại mối đe dọa, các phương thức tấn công và phân tích về mức độ nghiêm trọng của các mối đe dọa đó.
  + Đảm bảo tuân thủ các quy định về bảo mật và quyền riêng tư, thông tin tình báo được bảo mật cao, tránh bị rò rỉ hoặc bị khai thác.
- Nhà thầu cung cấp dịch vụ EDR phải có khả năng giám sát liên tục các endpoint (máy chủ, máy trạm) để phát hiện hành vi bất thường, mã độc, và các hoạt động tấn công có chủ đích (APT):
  + Hỗ trợ cả phương pháp phát hiện dựa trên dấu hiệu (signature-based) và hành vi

(behavior-based).

+ Ghi nhận toàn bộ dữ liệu hoạt động trên thiết bị: tiến trình, file, kết nối mạng, registry, quyền truy cập,...
+ Cho phép truy xuất dữ liệu phục vụ điều tra và phân tích sau sự cố.
+ Tích hợp với nền tảng SOAR để tự động hóa quy trình xử lý và phản ứng với sự cố.
+ Tích hợp với hệ thống Threat Intelligence (TI) để đối chiếu với IOC, phát hiện các mối đe dọa mới theo thời gian thực.
+ Hỗ trợ phân tích nguyên nhân gốc (Root Cause Analysis) của các cuộc tấn công.
+ Có khả năng cô lập endpoint khỏi mạng để ngăn chặn lây lan.
+ Cho phép thực hiện các hành động phản ứng như: kết thúc tiến trình, chặn kết nối, phục hồi hệ thống,...
+ Cung cấp giao diện quản trị tập trung.
+ Đáp ứng với các hệ điều hành phổ biến: Windows, Linux, macOS.
+ Sinh cảnh báo tự động khi phát hiện dấu hiệu xâm nhập hoặc hành vi bất thường.
+ Hỗ trợ tạo dashboard và báo cáo tùy biến theo thời gian thực hoặc định kỳ.

2.5.9 9. Yêu cầu về giám sát sự kiện ATTT và ANM

- Giám sát sự kiện bất thường, các cảnh báo sinh ra từ hệ thống SIEM đảm bảo 24 giờ/ngày.
- Hệ thống giám sát có khả năng xây dựng, tùy biến Dashboard, định dạng báo cáo theo yêu cầu thực tế của PV Power.
- Cung cấp phương án, công cụ quản lý luồng công việc để đội ngũ giám sát của nhà thầu có thể phối hợp công việc cùng cán bộ của PV Power.
- Giám sát màn hình cảnh báo, kiểm tra, xác minh và phân loại các cảnh báo, tạo ticket và gán yêu cầu xử lý cho các bộ phận tương ứng.
- Xử lý các tickets theo quy trình có sẵn hoặc xử lý sơ bộ trước khi yêu cầu tăng cấp (escalate) xử lý.
- Phương thức cảnh báo: Cảnh báo sự kiện bất thường, sự cố qua điện thoại và email theo thứ tự ưu tiên người nhận, trong đó ưu tiên cảnh báo qua điện thoại đối với những sự cố được phân cấp từ mức “Cao” (High) trở lên.
- Báo cáo định kỳ hàng tháng/quý/năm.
- Cán bộ ngồi trực thực hiện giám sát, hỗ trợ và làm việc theo yêu cầu của PVPOWER từ xa qua kênh kết nối an toàn. Luôn có 1 đầu mối sẵn sàng hỗ trợ onsite tại PVPOWER trong trường hợp cần thiết.
- Phân loại mức độ của sự cố dựa trên mức độ rủi ro cũng như các cấp độ như:
  + Nghiêm trọng (Critical): Priority 1

+ Cao (High): Priority 2
+ Trung bình (Medium): Priority 3
+ Thấp (Low): Priority 3

- Thực hiện giám sát toàn diện 24/7/365 sự kiện ATTT xuất hiện trên hệ thống, mục tiêu giúp phát hiện sớm các tấn công vào hệ thống.
- Phối hợp cùng các bộ phận liên quan xây dựng Quy trình vận hành giám sát ATTT hiệu quả.
- Tổ chức thực hiện theo mô hình 3 ca-4 kíp, đảm bảo khả năng giám sát 24/7 (kể cả cuối tuần và ngày nghỉ lễ, Tết).

2.5.10 10. Yêu cầu về xử lý sự cố

- Phối hợp cùng các bộ phận liên quan xây dựng Quy trình xử lý sự cố.
- Đảm bảo sẵn sàng xử lý sự cố 24/7, giảm thiểu tối đa thiệt hại, gián đoạn dịch vụ, tối ưu hóa quá trình khôi phục sau sự cố.
- Thực hiện các biện pháp nghiệp vụ điều tra số và phân tích mã độc: thu thập, phân tích các dữ liệu số trên nhiều nền tảng, dịch ngược, phân tích mã độc, mã khai thác chuyên sâu để xác định (bao gồm & không hạn chế):
  + Thời điểm, nguồn gốc, nguyên nhân lây nhiễm.
  + Chủng loại mã độc, hành vi lạ.
  + Máy chủ điều khiển, hạ tầng tấn công.
  + Nhóm, chiến dịch tấn công liên quan.
  + Phương án phát hiện, ngăn chặn tấn công tương tự.
- Tuân thủ theo tiêu chuẩn xử lý sự cố của NIST và quy trình của PV Power.

2.5.11 11. Yêu cầu về đánh giá, tối ưu nguồn logs và xây dựng tập luật phát hiện (Content Services)

- Tối ưu cảnh báo ATTT phù hợp với nghiệp vụ trên các hệ thống CNTT. Thực hiện tối ưu trên giải pháp SIEM.
- Phân tích cảnh báo sai, thực hiện hiệu chỉnh luật để giảm thiểu tối đa cảnh báo sai, tăng hiệu quả công tác vận hành giám sát.
- Bổ sung luật phát hiện các kỹ thuật tấn công mới, dấu hiệu khai thác lỗ hổng mới, dấu hiệu lây nhiễm mã độc, công cụ mới của các nhóm APT.
- Xây dựng các kịch bản (playbook) tự động hóa công tác vận hành giám sát giúp tăng chất lượng và tối ưu chi phí.
- Tần suất thực hiện: Thực hiện công tác tối ưu định kỳ hàng tháng, và thực hiện ngay khi có yêu cầu tối ưu đối với lỗ hổng, chiến dịch tấn công mới.
- Thực hiện tối ưu chủ động, rà soát các tập luật cảnh báo sai.

Các công việc thực hiện bao gồm:

a. Khảo sát hiện trạng thu thập logs và các bộ luật đang áp dụng

- Khảo sát danh mục hệ thống, ứng dụng của khách hàng từ các hệ thống quản lý tập trung (Asset Management, Antivirus tập trung, …).
- Thu thập danh mục logs đang được thu thập trên hệ thống SIEM:
  + Lập danh sách những loại logs đang được thu thập.
  + Rà soát các loại logs không sử dụng, logs trùng.
  + Lập danh sách nhưng loại logs còn thiếu phục vụ phát hiện nguy cơ.
- Xác định và xây dựng các usecase giám sát phù hợp với hiện trạng log và hệ thống của khách hàng hoặc bản đồ nguy cơ có thể ảnh hưởng đến hệ thống khách hàng dựa vào các tiêu chí:
  + Kỹ thuật tấn công phổ biến được các nhóm APT, nhóm hacker sử dụng tại Việt Nam.
  + Các hệ thống, ứng dụng khách hàng đang sử dụng.
- Khảo sát hiện trạng tập luật đang được áp dụng:
  + Lập danh sách tập luật đang được áp dụng.
  + Rà soát tập luật không sử dụng, luật trùng.
  + Rà soát logic rule.
  + Rà soát rule phát sinh ít và nhiều cảnh báo.
  + Rà soát rule tốn hiệu năng hệ thống.
- Báo cáo về hiện trạng, đề xuất tối ưu nguồn log và tập luật.

b. Xây dựng tập luật phát hiện và ngăn chặn các nguy cơ

- Dựa trên tri thức từ Framework MITRE ATT&CK và các kỹ thuật tấn công phổ biến được các nhóm APT sử dụng tại Việt Nam – Tham chiếu theo các giải pháp Threat Intelligence.
- Hệ thống tri thức về tích lũy trong quá trình xử lý sự cố về ATTT
- Thực hiện phát triển tập luật trên các hệ thống giải pháp SIEM
- Phối hợp giám sát vận hành thử và tối ưu cho phù hợp với nghiệp vụ.

c. Tổng hợp báo cáo đề xuất xây dựng kịch bản giám sát ATTT (usecase) và và báo cáo tối ưu định kỳ

- Báo cáo về các kịch bản giám sát ATTT (usecase) triển khai.
- Khuyến nghị về các loại logs cần thiết, các giải pháp cần bổ sung để phát hiện nguy cơ tương ứng.
- Chỉ số hóa về chất lượng tập luật và độ trưởng thành về phát hiện nguy cơ đối với hệ thống.

d. Định kỳ rà soát, đánh giá và tối ưu hệ thống lưu trữ logs tập trung

- Định kỳ thực hiện bổ sung tập luật phát hiện lỗ hổng mới công bố trên ứng dụng quan trọng.
- Bổ sung tập luật phát hiện hình thức tấn công, lỗ hổng trong quá trình phân tích và xử lý sự cố.
- Định kỳ thực hiện rà soát tối ưu tập rule phát sinh cảnh báo sai, cảnh báo nhiều giảm mức độ nhiễu và hiệu năng hệ thống.

2.5.12 12. Yêu cầu về trách nhiệm các bên

Trách nhiệm các bên theo các cấp độ và kết quả cần đạt được theo (RACI), cụ thể như sau:

STT	Ký hiệu	Mô tả nhiệm vụ
1	R	**Thực hiện:** Đóng vai trò thực thi gói công việc nhằm đảm bảo gói công việc đó được hoàn thành
2	A	**Phê duyệt:** Chịu trách nhiệm cuối cùng đối với việc hoàn thành công việc
3	C	**Đánh giá, khuyến nghị:** Người/nhóm chịu trách nhiệm thực thi có thể tham vấn ý kiến, tham vấn chuyên gia đối với người/nhóm có vai trò C để có thể thực thi công việc
4	I	**Được biết thông tin:** Người/nhóm cần được thông báo thông tin về một công việc

Bảng quy định công việc theo các cấp độ và kết quả cần đạt được (RACI) như sau:

STT	Công việc	Mô tả công việc	Yêu cầu kết quả đầu ra	Đơn vị cung cấp dịch vụ	Đơn vị sử dụng dịch vụ
I	**TIER 1: Giám sát, xử lý cảnh báo**				
1	Giám sát 24/7, phối hợp và phản ứng sự cố	- Thực hiện giám sát liên tục, toàn bộ các cảnh báo (SIEM, Firewall, Router, IDS/IPS, EDR, Windows event log, UNIX/Linux log, web application, database...) và các nguồn từ khách hàng, nội bộ, cá nhân, public, mail/telegram, … - Thực hiện truy vấn tìm kiếm thông tin trên các hệ thống SIEM và các hệ thống khác.	Đảm bảo giám sát toàn bộ, liên tục trong ca trực. Đảm bảo xử lý toàn bộ các cảnh báo, không bỏ sót các cảnh báo...	A, R	I
2	Phân tích cảnh báo, truy vấn tìm kiếm, tạo Ticket	Đối với các cảnh báo Mã độc: - Xác định rõ tên mã độc, tên file, hành động (xóa bỏ, cách	Tạo Ticket điều phối xử lý sự cố, cập nhật thông tin	A, R	I

STT	Công việc	Mô tả công việc	Yêu cầu kết quả đầu ra	Đơn vị cung cấp dịch vụ	Đơn vị sử dụng dịch vụ
	điều hành xử lý sự cố: - Đánh giá cảnh báo True/False, xác định phạm vi mức độ ảnh hưởng (như số lượng hệ thống, thời gian bị tấn công...) - Sử dụng công cụ quản lý sự kiện, sự cố để phân loại sự cố: Đảm bảo sự cố được phân loại, cập nhật, đóng theo đúng quy trình và trong SLA thỏa thuận - Thông báo cho các bên liên quan - Thực hiện chuyển Tier 2 xử lý (nếu cần)	ly, chặn,...) nguồn lây nhiễm (nếu có) Đối với các cảnh báo Scan/Exploit/Web: - Đánh giá mức độ ảnh hưởng. - Kiểm tra đã khai thác thành công hay chưa. Phối hợp các đơn vị chủ quản để điều tra thêm - Đưa rõ nguồn tấn công, vector, entry khai thác trước khi tạo Ticket xử lý - Nếu chỉ dừng ở mức scan hệ thống (chưa khai thác thành công), đưa ra các biện pháp khuyến nghị (block IP trong khoảng thời gian, rà soát lại hệ thống) Đối với các cảnh báo về hành vi, tiến trình, account: Xác định mức độ ảnh hưởng Tiến trình thực thi Điều tra thêm các thông tin liên quan (tiến trình cha, kết nối, user, các hành vi tương tự) Kiểm tra thông tin trên CTIP, google (ip/domain, hash file, command line,...) Kết hợp Mitre Att &Ck Đối với các cảnh báo về Hạ tầng hệ thống: Xác định thời gian, mức độ ảnh hưởng Kiểm tra các sự kiện trong khoảng thời gian gần nhất Xác định nguyên nhân - Tổ chức kiểm tra hệ thống (nếu cần thiết, chuyển lên Tier 2)	XLSC lên hệ thống, đóng Ticket khi hoàn thành XLSC		
3	Phân tích sự cố, thu thập dữ liệu	Kết hợp nhiều nguồn dữ liệu và hệ thống để phân tích sự cố, bước đầu xác định đánh giá mức độ sự cố	Bổ sung thông tin chi tiết vào Ticket sự cố	A, R	I

STT	Công việc	Mô tả công việc	Yêu cầu kết quả đầu ra	Đơn vị cung cấp dịch vụ	Đơn vị sử dụng dịch vụ
4	Phối hợp cập nhật và tối ưu các rule cảnh báo	Phối hợp đội viết rule thêm/sửa/xóa/tối ưu các rule cảnh báo	Báo cáo kết quả	A, R	I
5	Báo cáo	- Tổng hợp báo cáo định kỳ/ đột xuất. - Cung cấp, bổ sung thông tin phục vụ công tác xử lý sự cố ATTT	Báo cáo tháng Báo cáo định kỳ/ đột xuất File số liệu tổng hợp	A, R	I
II	**TIER 2: Thực hiện tiếp nhận thông tin, phân tích sơ bộ, xác minh nghiệp vụ và xử lý các tấn công theo hướng dẫn của Tier 1**				
1	Xử lý các sự cố được assign bởi tier 1 theo quy trình: - Tiếp nhận sự cố từ Tier 1 - Đánh giá và xử lý sự cố	Đối với sự cố liên quan đến tấn công Web/Exploit/Mã độc: Xác minh các hành vi với quản trị. Đưa ra hướng xử lý mã độc theo khuyến nghị (nếu có). Phân tích các hành vi tấn công nâng cao.	Phản hồi lại Tier 1 kết quả xử lý. Sự cố được xử lý và Resolve Ticket đúng hạn theo quy định. Báo cáo kết quả XLSC (nếu có)	A, R	C, I
2	Xử lý các sự cố được assign bởi tier 1 theo quy trình: - Tiếp nhận sự cố từ Tier 1 - Đánh giá và xử lý sự cố	Đối với các yêu cầu liên quan đến quản trị hệ thống: - Hỗ trợ xác minh thông tin nghiệp vụ nếu có yêu cầu. - Cung cấp thông tin về người dùng, thiết bị, ứng dụng. - Phản hồi, xác minh hành vi bất thường. - Thực thi các thay đổi trên hệ thống, cung cấp truy cập/log hệ thống nếu cần điều tra chuyên sâu.	Phản hồi lại Tier 1 kết quả xử lý. Sự cố được xử lý và Resolve Ticket đúng hạn theo quy định. Báo cáo kết quả XLSC (nếu có)	C, I	A, R
III	**TIER 3: Điều tra số, phân tích chuyên sâu các sự cố nghiêm trọng, tấn công APT, Khai thác lỗ hổng; Săn tìm mối nguy hại trong hệ thống.**				
1	Xử lý các sự cố được assign bởi tier 2 theo quy trình: - Tiếp nhận sự cố từ Tier 2	- Tiếp nhận thông tin các sự cố từ Tier 2 - Phân tích chuyên sâu, điều tra xác định nguồn gốc tấn công, các hành vi và mức độ ảnh hưởng	Báo cáo phân tích sự cố (IOCs, TTPs, khuyến nghị, ...)	A, R	I

STT	Công việc	Mô tả công việc	Yêu cầu kết quả đầu ra	Đơn vị cung cấp dịch vụ	Đơn vị sử dụng dịch vụ
	- Đánh giá và phân tích sự cố	- Đưa ra các biện pháp khắc phục, khuyến nghị phòng tránh.	- Sự cố được xử lý và Resolve Ticket đúng hạn theo quy định - Báo cáo kết quả XLSC		
2	Điều tra số	- Thu thập thông tin, dữ liệu và đảm bảo tính xác thực và toàn vẹn của dữ liệu đã thu thập - Xác định nguồn gốc, phạm vi, mức độ ảnh hưởng của sự cố. - Đưa khuyến nghị khắc phục giảm thiểu rủi ro, các biện pháp phát hiện trong tương lai Đưa ra các dấu hiệu tấn công, sự kiện bất thường Nguồn, vector tấn công, dữ liệu bị đánh cắp (nếu có) Xác định phạm vi, mức độ bị ảnh hưởng - Các biện pháp phát hiện trong tương lai	- Báo cáo kết quả điều tra, phân tích - Ticket	A, R	C, I
3	Phân tích mã độc	Phân tích tĩnh và phân tích động mã độc: Nguồn mã độc từ các Ticket được tạo bởi Tier 1 và mã độc phát hiện trong quá trình săn tìm mối nguy tại hệ thống của khách hàng: Đưa ra báo cáo chi tiết các hành vi của mã độc Nguồn gốc tấn công, mức độ ảnh hưởng Các dữ liệu bị đánh cắp (nếu có) Cập nhập IOCs, TTPs vào cơ sở dữ liệu Threat Intelligence Đưa ra khuyến nghị khắc phục, biện pháp xử lý và phòng tránh mã độc Phân loại các sự cố mã độc theo cấp độ	Báo cáo kết quả phân tích Đưa ra các kỹ thuật mã độc sử dụng, các biện pháp phát hiện và ngăn ngừa Khuyến nghị khắc phục Ticket	A, R	C

STT	Công việc	Mô tả công việc	Yêu cầu kết quả đầu ra	Đơn vị cung cấp dịch vụ	Đơn vị sử dụng dịch vụ
		- Đối với sự cố nghiêm trọng có thể chuyển lên Tier 3 phân tích đảm bảo đánh giá, phân tích nhanh, chính xác, khắc phục sự cố đúng hạn theo quy định			
4	Săn tìm mối nguy hại	Điều tra, truy tìm nguồn gốc các cuộc tấn công, săn tìm các mối đe dọa tiềm ẩn trong hệ thống và trên Không gian mạng,	- Báo cáo kết quả săn tìm mối nguy - Cảnh báo các sự cố phát hiện	A, R	I
5	Phối hợp rà soát kiểm tra hệ thống theo các target thu thập được từ các nguồn TI, Threat hunting…	Nhận dữ liệu cảnh báo từ TI (entry, payload khai thác, signature), các đơn vị khác tiến hành rà soát toàn bộ hệ thống.	- Báo cáo kết quả rà soát các hệ thống theo nguồn dữ liệu từ TI	A, R	I

3. C. YÊU CẦU VỀ NĂNG LỰC KINH NGHIỆM

3.1 I. Yêu cầu đối với đơn vị cung cấp dịch vụ

- Đơn vị cung cấp phải có xác nhận kết nối, chia sẻ thông tin với trung tâm giám sát an toàn an ninh mạng quốc gia
- Đơn vị cung cấp dịch vụ phải có giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng của Bộ Thông tin Truyền thông tối thiểu 5 năm trong lĩnh vực an toàn thông tin. Giấy phép đồng thời có các loại hình sản phẩm dịch vụ:
  + Dịch vụ Giám sát an toàn thông tin mạng.
  + Dịch vụ ứng cứu xử lý sự cố an toàn thông tin mạng.
  + Dịch vụ khôi phục dữ liệu.
  + Sản xuất các sản phẩm về giám sát ATTT
- Đơn vị cung cấp dịch vụ phải có giấy chứng nhận ISO: ISO/IEC 27001:2013 hoặc ISO/IEC 27001: 2022.
- Đơn vị cung cấp thêm chứng chỉ ISO 9001: 2015 sẽ là tiêu chí điểm cộng.
- Đơn vị cung cấp dịch vụ phải đạt chứng nhận CREST về SOC.

- Đơn vị cung cấp dịch vụ phải cam kết bảo đảm hỗ trợ kỹ thuật trong thời gian cung cấp dịch vụ.
- Đơn vị cung cấp dịch vụ có nhân lực cho Tier 1, Tier 2, Tier 3 với các chứng chỉ vận hành hệ thống SIEM được cung cấp tương ứng hãng SIEM đơn vị chào hoặc của các hãng thuộc Top Gartner SIEM cấp theo yêu cầu về nhân sự các Tier nêu trên.

3.2 II. Yêu cầu đối với nhân sự giám sát

- Thời gian giám sát: 24/7/365 (bao gồm cả ngày lễ, tết). Đội ngũ giám sát Tier 1 thực hiện giám sát theo 3 ca/1 ngày (8 tiếng 1 ca) và 4 kíp trực, đảm bảo khả năng liên tục giám sát 24/7/365.
- Thực hiện hoạt động giám sát 24/7 từ xa cho hệ thống CNTT PV Power thông qua kênh Internet VPN hiện có của PV Power hoặc qua kênh truyền riêng do đơn vị cung cấp dịch vụ đề xuất. Đơn vị cung cấp dịch vụ đảm bảo kênh truyền bảo mật, ổn định, đáp ứng các yêu cầu giám sát ATTT cho PV Power.
- Chịu trách nhiệm về việc giám sát, phân tích sơ bộ nhằm nhận diện và phân loại các sự kiện ATTT được cung cấp từ hệ thống các công cụ và từ các bộ phận, quy trình hoạt động khác. Nội dung giám sát cơ bản gồm:
  + Giám sát lớp mạng: Phát hiện kết nối C&C và Shellcode/payload tấn công trong traffic mạng thuộc phân vùng mạng; Phát hiện các bất thường từ log của thiết bị mạng của PV Power trang bị như Firewall, IPS,...
  + Giám sát lớp máy chủ và Giám sát lớp đầu cuối: Phát hiện máy chủ (Windows, Linux, Unix, Ứng dụng hệ thống như DNS,.., Computer, Laptop) nhiễm mã độc APT.
  + Giám sát lớp ứng dụng: Phát hiện các bất thường, tấn công vào ứng dụng Web, Email, hệ quản trị cơ sở dữ liệu dựa trên log của các ứng dụng cùng các giải pháp hiện có của PV Power và với các giải pháp WAF, Database Firewall, ... nếu sau này PV Power đầu tư triển khai.
- Theo dõi quá trình xử lý, đóng các ticket xử lý xong.
- Cán bộ của đơn vị cung cấp dịch vụ thực hiện công việc giám sát tại văn phòng của đơn vị cung cấp dịch vụ và chỉ thực hiện tác vụ giám sát. Các tác vụ thay đổi, cấu hình hệ thống do cán bộ của PV Power hoặc phối hợp với cán bộ PV Power lên phương án cụ thể để thực hiện.