Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

I. Giới thiệu chung về dự án/dự toán mua sắm:

1. Tên dự toán/Hạng mục

Thuê dịch vụ giám sát an toàn thông tin mạng cho các hệ thống thông tin của Sở.

2. Chủ đầu tư

Tên đơn vị: Sở Giao dịch Chứng khoán Thành phố Hồ Chí Minh

Địa chỉ: 16 Võ Văn Kiệt, phường Bến Thành, Thành phố Hồ Chí Minh

3. Địa điểm thực hiện

- Trung tâm dữ liệu (DC) – Địa chỉ tại số 16 Võ Văn Kiệt, phường Bến Thành, Thành phố Hồ Chí Minh;

- Trung tâm dữ liệu dự phòng (DR): Địa chỉ tại Lô 32A, khu Công viên Phần mềm Quang Trung.

4. Thời gian thực hiện:

Thời gian thực hiện: 365 ngày (Tính từ thời điểm 02 bên ký biên bản nghiệm thu đưa dịch giám sát vào sử dụng).

5. Nguồn vốn đầu tư

Chi phí thường xuyên tại doanh nghiệp.

6. Hình thức lựa chọn nhà thầu

Đấu thầu rộng rãi, qua mạng, trong nước.

7. Phương thức lựa chọn nhà thầu:

Một giai đoạn một túi hồ sơ.

8. Loại hợp đồng:

Hợp đồng trọn gói.

II. Mục tiêu công việc:

1. Mục tiêu công việc

Mục tiêu của hạng mục "Thuê dịch vụ giám sát an toàn thông tin mạng cho các hệ thống thông tin của Sở" là đảm bảo toàn bộ hệ thống CNTT của HOSE được giám sát an ninh mạng 24/7, phát hiện và ứng phó kịp thời các rủi ro an toàn thông tin, đáp ứng đầy đủ yêu cầu pháp lý cấp độ 3, và duy trì hoạt động ổn định, tin cậy, an toàn cho các hệ thống thông tin của Sở.

Thực hiện mục tiêu giám sát an toàn thông tin mạng (ATTT) cho các hệ thống thông tin của Sở (SOC/SIEM) là một chiến lược toàn diện nhằm chuyển từ mô hình phòng thủ bị động sang mô hình phòng thủ chủ động và liên tục, cho hệ thống thông tin cấp độ 3 của HOSE, được tóm tắt như sau:

- Mục tiêu cốt lõi là thiết lập khả năng quan sát và ứng phó tức thì (Visibility & Incident Response) trên toàn bộ hệ thống:

+ Phát hiện và Cảnh báo Sớm: Thiết lập một hệ thống SIEM (Security Information and Event Management) tập trung để thu thập và phân tích log từ toàn bộ 29 VLAN, 25 dải mạng, 153 máy chủ (bao gồm cả DMZ và DR) và các thiết bị bảo mật (Firewall Cisco Firepower, WAF F5 ASM,…) nhằm sớm phát hiện các sự cố ATTT theo thời gian thực, bao gồm các cuộc tấn công đang diễn ra, hành vi bất thường của người dùng, và các dấu hiệu xâm nhập.

+ Phân tích Chuyên sâu (Threat Hunting): Áp dụng các quy tắc tương quan và phân tích hành vi để phát hiện các mối đe dọa phức tạp, đặc biệt là các cuộc tấn công logic nhắm vào hệ thống nghiệp vụ cốt lõi và 2 loại CSDL (Oracle & SQL Server).

+ Ứng phó và Khắc phục Nhanh: Rút ngắn tối đa Thời gian Phát hiện (MTTD - Mean Time to Detect) và Thời gian Phản hồi (MTTR - Mean Time to Respond) đối với các sự cố bảo mật.

III. Yêu cầu kỹ thuật của gói thầu:

1. Hình thức thực hiện

- Thuê dịch vụ SOC chuyên nghiệp giám sát và bảo đảm ATTT 24/7.

2. Thời gian và tiến độ thực hiện

- Thực hiện trong 365 ngày, không kể thời gian nhà thầu chuẩn bị, cụ thể như sau:

+ Khảo sát, cài đặt cấu hình và tích hợp hoàn thành: Tối đa 60 ngày.

+ Thực hiện cung cấp dịch vụ: 365 ngày (Tính từ thời điểm 02 bên ký biên bản nghiệm thu đưa dịch giám sát vào sử dụng).

3. Phạm vi thực hiện

TT	Nội dung	Phạm vi thực hiện
1	**Máy chủ**	Tại DC & DR **có 153 máy chủ vật lý và ảo hóa**, được phân bố cụ thể như sau: - Tại Trung tâm dữ liệu (TTDL): + 32 máy chủ vật lý; + 116 máy chủ ảo hóa được triển khai ảo hóa trên hạ tầng VMware/Hyper-V. - Tại Trung tâm dữ liệu dự phòng (TTDLDP): + 02 máy chủ vật lý; + 03 máy chủ ảo hóa.
3	Thiết bị mạng tại DC	**Có 45 thiết bị mạng cần giám sát tại DC gồm:** - Có 06 thiết bị định tuyến (Router); - Có 09 thiết bị đảm bảo ATTT; - Có 29 thiết bị chuyển mạng (Switch); - 01 Wireless controller;
4	Thiết bị mạng tại DR	Tại **DR có 11 thiết bị** cần giám sát ATTT: - Hệ thống có 06 thiết bị định tuyến (Router); - Hệ thống có 02 thiết bị tường lửa (Firewall); - Hệ thống có 02 thiết bị chuyển mạng lõi (Core switch); - Hệ thống có 01 thiết bị chuyển mạng biên (Access switch);
5	Ứng dụng nghiệp vụ	Có 8 ứng dụng nghiệp vụ;

TT	Nội dung	Phạm vi thực hiện
6	Hệ thống lưu trữ	Lưu trữ tại chỗ (On premises) – Lưu trữ trên NAS và SAN;
7	Ứng dụng web cần giám sát	1) Trang thông tin điện tử của HOSE: hsx.vn; 2) Cổng công bố thông tin: ecm.hsx.vn.
8	Ứng dụng cài đặt trên máy trạm	Có 23 ứng dụng cần giám sát ATTT
9	Tổng số máy trạm (desktop) cần giám sát	HOSE có 239 máy;

4. Nội dung thực hiện

4.1. *Giám sát, quản lý các sự kiện ATTT và cảnh báo ATTT*

Thực hiện giám sát, quản lý các sự kiện ATTT và cảnh báo ATTT cho toàn bộ hệ thống công nghệ thông tin bao gồm máy chủ, máy trạm và thiết bị mạng của SGDCK tại TTDL Dịch vụ bao gồm các nội dung sau:

- Triển khai công cụ giám sát ATTT mạng đáp ứng Quyết định số 1356/QĐ-BTTTT ngày 07/7/2022 của Bộ Thông tin và Truyền thông về tiêu chí đánh giá giải pháp, dịch vụ trung tâm giám sát điều hành an toàn, an ninh mạng (SOC) (không bao gồm các hệ thống đã được SGDCK trang bị). Cụ thể bao gồm: hệ thống SIEM, NIPS, EDR, SOAR và TIP (Threat Intelligence Platform).

- Triển khai hệ thống và giải pháp phòng, chống thất thoát dữ liệu(DLP) qua mỗi trường mạng đáp ứng tiêu chuẩn TCVN 11930:2017 (Mục 7.2.1.1.b: Có phương án phòng, chống thất thoát dữ liệu).

- Triển khai phòng chống tấn công từ chối dịch vụ (DDoS) cho 02 đường truyền mạng.

- Mức độ giám sát: Giám sát mức cơ bản (lớp mạng và vành đai); giảm sát mức lớp hệ điều hành; giám sát lớp ứng dụng và giám sát lớp cơ sở dữ liệu;

- Số lượng máy chủ, máy trạm và thiết bị mạng hiện tại:

+ Số lượng máy chủ, máy trạm và thiết bị mạng tại TTDL: 148 máy chủ (32 máy chủ vật lý, 116 máy chủ ảo hóa), 225 máy trạm và 45 thiết bị mạng;

+ Số lượng máy chủ, máy trạm và thiết bị mạng tại TTDLDP (kết nối với TTDL bằng đường truyền thuê riêng - leased line): 05 máy chủ (2 máy chủ vật lý, 3 máy chủ ảo hóa), 14 máy trạm và 11 thiết bị mạng;

+ Trường hợp số lượng máy chủ, máy trạm và thiết bị mạng tăng thêm (tối đa 10% so với phạm vi) do SGDCK triển khai hệ thống mới không phát sinh chi phí.

- Yêu cầu nhân sự:

+ Phân công giám sát: tối thiểu 02 nhân sự/ca, 24 giờ/ngày và 7 ngày/tuần kể cả các ngày tết/lễ.

- Thu thập và phân tích sơ bộ dữ liệu về ATTT, dấu hiệu tấn công, truy cập trái phép vào hệ thống công nghệ thông tin của SGDCK để đưa ra các cảnh báo về sự kiện, sự cố liên quan đến ATTT;

- Việc cảnh báo về sự kiện, sự cố liên quan đến ATTT phải thực hiện trên hệ thống, bao gồm tạo thẻ cảnh báo, phối hợp và hướng dẫn xử lý đối với các cảnh báo phức tạp, theo dõi quá trình xử lý và đóng các the cảnh báo sau khi hoàn thành việc xử lý,

- Tối ưu cảnh báo về ATTT để hạn chế các cảnh báo giá, cảnh báo trùng lập về các sự kiện, sự cố ATTT.

- Kết nối, chia sẻ thông tin giám sát ATTT với hệ thống SOC của Bộ Tài chính. Nội dung kết nối, chia sẻ thông tin theo công văn số 308/THTK-ATTT ngày 22/4/2021 của Cục Tin học và Thống kê Tài chính - Bộ Tài chính về việc kết nối, chia sẻ thông tin giảm sát ATTT mạng (đường truyền kết nối chia sẻ thông tin giám sát ATTT: Sử dụng đường truyền thuê riêng có sẵn của Bộ Tài chính):

- Kết nối, chia sẻ thông tin giám sát với các cơ quan quản lý khác trong trường hợp được yêu cầu và có hướng dẫn cụ thể:

- Báo cáo kết quả Giám sát, quản lý các sự kiện ATTT và cảnh báo ATTT trong Báo cáo hàng tuần và hàng tháng về Dịch vụ giám sát an toàn thông tin mạng cho các hệ thống thông tin của Sở.

4.2 Xử lý sự cố ATTT

Nhà thầu trúng thầu phải thực hiện hạng mục SOC phối hợp với HOSE xử lý các sự cố về ATTT (nếu có) toàn bộ hệ thống công nghệ thông tin của Sở Giao dịch Chứng khoán Thành phố Hồ Chí Minh. Công việc bao gồm các nội dung như sau:

- Phân tích dữ liệu về ATTT, dấu hiệu tấn công, truy cập trái phép vào hệ thống công nghệ thông tin của SGDCK để nhận diện và phát hiện mức độ của sự cố ATTT;

- Xác định các hành động cần thiết và hướng dẫn SGDCK thực hiện ngăn chặn ngay các sự có ATTT và/hoặc xử lý ATTT;

- Thực hiện ứng cứu, trực tiếp xử lý tại SGDCK đối với các sự cố ATTT nghiêm trọng, sự cố ATTT mới (chưa có hướng dẫn) các sự cố ATTT phức tạp cần phân tích mã độc, điều tra truy vết, phân tích điều tra sâu về nguồn tấn công, phát hiện để phòng các tấn công, tấn công DDOS và hoặc các sự cố mà nhân viên SGDCK thực hiện không thành công;

- Phân tích sâu, khoanh vùng, điều tra nguyên nhân gốc, xác định phương án và thực hiện khắc phục triệt để sự cố;

- Nhân sự thực hiện xử lý sự cố: Cung cấp 05 chuyên gia đáp ứng yêu cầu tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về việc đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam để SGDCK thành lập đội ứng cứu sự cố.

- Báo cáo kết quả xử lý sự cố ATTT (nếu có) trong Báo cáo hàng tháng về Dịch vụ giám sát và bảo đảm an toàn thông tin cho các hệ thống thông tin của HOSE.

4.3. Cảnh báo nguy cơ về ATTT

Cập nhật và cung cấp thông tin cảnh báo nguy cơ về ATTT đối với hệ thống công nghệ thông tin (phần cứng, phần mềm....) của SGDCK ngay khi phát hiện các nguy cơ mất ATTT mới (không gửi các cảnh báo ngoài phạm vi, cảnh báo trùng lặp): Dịch vụ bao gồm các nội dung như sau:

- Việc cảnh báo nguy cơ về ATTT phải thực hiện trên hệ thống, bao gồm tạo thẻ cảnh báo, phối hợp và hướng dẫn xử lý đối với các cảnh bảo phức tạp, theo dõi quá trình xử lý và đóng các thẻ cảnh báo sau khi hoàn thành việc xử lý;

- Tối ưu cảnh báo nguy cơ về ATTT nhằm tránh các cảnh báo ngoài phạm vi, cảnh báo trùng lập về các nguy cơ ATTT;

- Báo cáo kết quả cảnh báo nguy cơ về ATTT trong Báo cáo hàng tháng về Dịch vụ giám sát và bảo đảm an toàn thông tin cho các hệ thống thông tin của HOSE.

4.4. Tìm kiếm chủ động các nguy cơ về ATTT

Thực hiện việc tìm kiếm chủ động các nguy cơ về ATTT đối với hệ thống công nghệ thông tin của SGDCK; Dịch vụ bao gồm các nội dung như sau:

- Định kỳ 03 tháng thực hiện tìm kiếm chủ động (threat-hunting) nhằm phát hiện các nguy cơ mất ATTT có thể xảy ra đối với các máy chủ của SGDCK: số lượng máy chủ cụ thể sẽ được hai Bên thống nhất trước mỗi kỳ thực hiện tìm kiếm chủ động;

- Phối hợp xử lý ATTT (vá lỗi, gỡ bỏ mã độc,...) nếu quá trình tìm kiếm chủ động các nguy cơ về ATTT phát hiện các bất thường;

- Báo cáo Dịch vụ tìm kiếm chủ động các nguy cơ về an toàn thông tin mạng trong Báo cáo hàng tháng về Dịch vụ giám sát và bảo đảm an toàn thông tin cho các hệ thống thông tin của HOSE.

4.5. Địa điểm thực hiện dịch vụ:

1) Trung tâm dữ liệu (DC) – Địa chỉ tại số 16 Võ Văn Kiệt, phường Bến Thành, Thành phố Hồ Chí Minh;

2) Trung tâm dữ liệu dự phòng (DR): Địa chỉ tại Lô 32A, khu Công viên Phần mềm Quang Trung.

4.6. Yêu cầu kỹ thuật thực hiện

4.6.1 Yêu cầu kỹ thuật công cụ giám sát ATTT

4.6.1.1 *Yêu cầu về hệ thống SIEM*

Giải pháp SIEM đóng vai trò lõi của nền tảng SOC và triển khai trực tiếp tại hệ thống thông tin của HOSE, cung cấp khả năng giám sát và quản lý toàn bộ sự kiện, cảnh báo của hệ thống. Do đó phần mềm SIEM cần đảm bảo đáp ứng đầy đủ các tính năng sau:

STT	Yêu cầu	Mô tả
1	**Phát hiện sự cố và lỗ hổng**	Hệ thống ứng dụng công nghệ AI và ML trong việc phát hiện các mối đe dọa đã biết cũng như các hình thức tấn công tinh vi và chưa từng được nhận diện trước đó. Trong đó, mô hình phân tích hành vi thiết lập các ngưỡng hành vi chuẩn (baseline) dựa trên quá trình quan sát và học tập từ hoạt động thông thường của người dùng, thiết bị và hệ thống. Khi một hành vi mới xuất hiện, hệ thống sẽ tự động so sánh hành vi đó với các mẫu hành vi chuẩn đã học được. Nếu sự sai lệch giữa hành vi hiện tại và baseline vượt quá một ngưỡng xác định trước, hệ thống sẽ đánh dấu đó là hành vi bất thường và khởi tạo cảnh báo tương ứng.
		Hệ thống hỗ trợ thu thập chủ động và thụ động các thông tin bao gồm: phần mềm đã cài đặt, lỗ hổng bảo mật, và sự kiện hoạt động từ nhiều nguồn khác nhau trong hạ tầng CNTT.
		Hệ thống được trang bị sẵn các quy tắc chuẩn hóa sự kiện, quy tắc tương quan và hỗ trợ nhận diện 280 kỹ thuật tấn công theo khung MITRE ATT&CK
		Hệ thống cho phép lưu trữ lịch sử trạng thái của từng tài sản tại các thời điểm cụ thể. Đồng thời, theo dõi và ghi nhận mọi thay đổi của tài sản theo thời gian, bao gồm, phần mềm, thiết lập bảo mật và hành vi sử dụng. Dữ liệu lịch sử này được dùng làm cơ sở phục vụ phân tích sự cố, truy vết tấn công và kiểm toán bảo mật. Hệ thống được cập nhật liên tục qua gói chuyên môn từ Cơ sở Tri thức, hỗ trợ phát hiện sớm các TTPs của kẻ tấn công
		Dùng giao diện kéo-thả (rule constructor), không cần lập trình

STT	Yêu cầu	Mô tả
2	**Khả năng hiển thị**	Hệ thống cung cấp bảng hiển thị tập trung các thông tin về sự kiện, sự cố, lỗ hổng và các quy tắc bảo mật đã được kích hoạt. Người dùng có thể thực hiện các thao tác sau trực tiếp trên giao diện: - Xem dữ liệu phân tích, lưu thông tin dưới dạng tệp; - Chỉ định khoảng thời gian để xem thông tin (là mặc định và mỗi số liệu thống kê là trong 24 giờ); - Chỉ định khoảng thời gian làm mới tự đông cho dữ liệu mỗi 15 phút hoặc cập nhật thủ công;
		Menu chính của hệ thống cung cấp quyền truy cập tập trung đến các chức năng cốt lõi, giúp người dùng dễ dàng điều hướng và quản lý toàn bộ hệ thống. Giao diện menu hiển thị rõ tên hệ thống và bao gồm các thành phần chính sau: - Truy cập cơ sở dữ liệu sự kiện: Cho phép xem, tìm kiếm và phân tích log/sự kiện từ các nguồn dữ liệu khác nhau. - Truy cập trang chính (home) với bảng điều khiển: Cung cấp cái nhìn tổng quan theo thời gian thực về tình trạng an ninh, các sự kiện nổi bật, cảnh báo và thống kê hệ thống. - Các mục chức năng khác: Bao gồm quản lý cảnh báo, quản lý người dùng, cấu hình hệ thống, báo cáo và phân quyền truy cập.
		Hệ thống hiển thị trạng thái hoạt động của SIEM theo thời gian thực, giúp người dùng nhanh chóng đánh giá tình trạng tổng thể. Các trạng thái có thể bao gồm: - Hệ thống đang hoạt động bình thường, không phát hiện lỗi. - Hệ thống đang hoạt động, nhưng có cảnh báo cần được kiểm tra. - Hệ thống đang hoạt động nhưng có lỗi xảy ra, yêu cầu xử lý. - Hệ thống không thể thực hiện chẩn đoán hoặc quá trình chẩn đoán thất bại.
		Bảng điều khiển (dashboard) có thể được tùy chỉnh linh hoạt bằng cách sử dụng các tiện ích (widget) có sẵn hoặc tạo mới các tiện ích tùy chỉnh theo nhu cầu giám sát và phân tích cụ thể của người dùng
3	**Tối ưu hoá và giảm thiểu báo động giả**	Cho phép cấu hình ngoại lệ vào các quy tắc phát hiện mối đe doạ để ngăn chăn các báo động giả lặp đi lặp lại
		Cho phép chỉ định các tiêu chí cụ thể như địa chỉ IP máy chủ, tên người dùng hoặc các đặc điểm sự kiện, để hệ thống tự động bỏ qua (loại trừ) các sự kiện phù hợp với những tiêu chí này trong

STT	Yêu cầu	Mô tả
		quá trình áp dụng quy tắc phát hiện, nhằm giảm cảnh báo không cần thiết.
4	**Quản lý bảng thông tin và tiện ích**	Bảng điều khiển cung cấp thống kê sự kiện và cho phép người dùng tùy chỉnh loại thông tin hiển thị theo nhu cầu giám sát.
		Người dùng có thể tạo mới, đổi tên, chỉnh sửa nội dung, di chuyển vị trí và xóa các bảng thông tin tùy chỉnh cũng như các tiện ích (widget) trên bảng điều khiển.
		Hệ thống cho phép xuất dữ liệu từ các tiện ích sang tệp hình ảnh định dạng PNG, và xuất dữ liệu từ các tiện ích dạng bảng sang các định dạng CSV, XLSX, JSON hoặc XML.
5	**Quản lý thông báo**	Thông báo của hệ thống phải bao gồm các thông tin liên quan đến: các thay đổi trong cơ sở hạ tầng CNTT; trạng thái và hoạt động của các tác vụ thu thập dữ liệu; các sự kiện đã được ghi nhận; tham số luồng sự kiện; các sự cố bảo mật được phát hiện; và tình trạng vận hành tổng thể của hệ thống.

Yêu cầu kỹ thuật hệ thống SIEM

4.6.1.2 *Yêu cầu về hệ thống SOAR*

Giải pháp SOAR của Nhà thầu kết nối với SIEM đặt tại HOSE, cho phép quản lý các ticket, case sự cố, cảnh báo và khả năng tự động phản ứng với kịch bản tấn công đã định nghĩa. Phần mềm SOAR cung cấp đảm bảo các tính năng:

STT	Yêu cầu	Mô tả
1	**Quản lý xác thực**	Cho phép đăng nhập bằng Tên đăng nhập và Mật khẩu, xác thực OTP qua email
		Cho phép thiết lập mật khẩu mới qua email trong trường hợp quên mật khẩu
		Có thể tích hợp với các hệ thống xác thực tập trung như LDAP/AD, SAML
2	**Trang chủ**	Cho phép tạo sự cố từ Trang chủ, điều hướng vào màn hình sự cố

STT	Yêu cầu	Mô tả
		Cho phép xem thống kê số liệu sự cố, công việc - Sự cố mới trong tuần - Sự cố đã đóng trong tuần - Công việc mới trong tuần
		Cho phép xem sự cố đang xử lý của tôi ở trạng thái Mở, Mới, Đang Hoãn, Đang xử lý,..
		Cho phép xem các biểu đồ tương ứng với sự cố, công việc
		Giao diện kéo thả (Low-code/No-code) thân thiện. Hỗ trợ các hành động logic phức tạp (rẽ nhánh, vòng lặp).
		Cho phép thiết lập 1 số thông tin về cấu hình thông báo, quy tắc đổi mật khẩu mặc định, nguồn tích hợp của thông tin liên quan
3	**Công việc**	Cho phép tạo công việc theo các trường thông tin như sau: Tên công việc, Mã công việc, Loại công việc, Thuộc sự cố, Người thực hiện, Đơn vị thực hiện, SLA, Độ ưu tiên, Mô tả, File đính kèm
		Cho phép sửa công việc, tùy theo vai trò là người tạo hay thực hiện công việc
		Cho phép tìm kiếm công việc theo tiêu chí: Mã công việc, Tên công việc, Loại công việc, Độ ưu tiên, SLA, Đơn vị thực hiện, Người thực hiện, Người tạo, Khách hàng, Ngày tạo
		Cho phép xem danh sách công việc gồm: STT, Mã công việc, Tên công việc, Loại công việc, Mã sự cố của công việc, SLA, Trạng thái
		Cho phép xem chi tiết công việc với nội dung sau: Thông tin chung, Mô tả, File đính kèm
4	**Quản lý sự cố**	Cho phép tạo sự cố theo các trường thông tin như sau: Tên sự cố, Mã sự cố, Loại sự cố, Phân loại, Mức độ nguy hiểm, Trạng thái, Phương án xử lý, Người thực hiện, Đơn vị thực hiện, SLA, Thời gian xảy ra, Thời gian phát hiện, Mô tả, Thông tin thêm, File đính kèm
		Cho phép sửa sự cố, tùy theo vai trò là người tạo hay thực hiện sự cố

STT	Yêu cầu	Mô tả
		Cho phép tìm kiếm sự cố theo tiêu chí: Tên sự cố, Mã sự cố, Loại sự cố, Phân loại, Mức độ nguy hiểm, Trạng thái, Phương án xử lý, Người thực hiện, Đơn vị thực hiện, Người tạo, SLA, Thời gian xảy ra, Thời gian phát hiện, Thời gian đóng, Thời gian tạo
		Cho phép xem danh sách sự cố gồm: STT, Mã, Tên sự cố, Khách hàng, Mức độ nguy hiểm, Số công việc, Nạn nhân, Phương án xử lý, Người thực hiện, Người tạo, SLA, Đóng lúc, Ngày tạo
		Cho phép xem chi tiết sự cố với các nội dung sau: - Xem thông tin chung - Xem thông tin quy trình - Xem thông tin công việc - Xem thông tin liên quan: Người theo dõi, Dán nhãn, Thông tin chỉ báo/ nhóm/ nạn nhân - Xem thông tin ghi chú của công việc tương ứng với sự cố - Xem lịch sử xử lý liên quan sự cố, công việc
		Cho phép hiển thị đồng thời thông tin chi tiết về sự cố và các hành động khắc phục tương ứng trên cùng một giao diện
		Cho phép đổi người thực hiện sự cố, cụ thể là đổi đơn vị thực hiện hoặc đổi người thực hiện
		Tự động hóa việc tạo, phân loại, gán mức độ ưu tiên, theo dõi và quản lý toàn bộ vòng đời của sự cố bảo mật.
		Có khả năng làm giàu dữ liệu (Data Enrichment) cho sự cố bằng cách thu thập thông tin bổ sung từ các nguồn Threat Intelligence hoặc hệ thống khác.
5	**Quản lý quy trình**	Cho phép tìm kiếm quy trình theo tiêu chí: Tên quy trình
		Cho phép xem quy trình gồm: Tên quy trình, phiên bản
6	**Quản lý người dùng**	Cho phép tạo người dùng theo các trường thông tin như sau: Phân loại, Tên tài khoản, Họ và tên, Email, Số điện thoại, Trạng thái, Phòng ban, Quyền

STT	Yêu cầu	Mô tả
		Cho phép sửa tài khoản theo các trường thông tin như sau: Họ và tên, Email, Số điện thoại, Trạng thái, Phòng ban, Quyền. Không cho sửa các thông tin như Phân loại, Tên tài khoản
		Cho phép xóa người dùng khỏi hệ thống
		Cho phép đặt lại mật khẩu người dùng theo mật khẩu mặc định hệ thống
		Cho phép tìm kiếm người dùng theo tiêu chí: Tên tài khoản, Họ và tên, Email, Số điện thoại, NHóm quyền, Phòng ban, Phân loại, Trạng thái mật khẩu, Trạng thái
		Cho phép xem danh sách người dùng gồm: STT, Tên tài khoản, Họ và tên, Nhóm quyền, Phòng ban, Phân loại, Trạng thái mật khẩu, Trạng thái
		Cho phép xem lịch sử chỉnh sửa người dùng, ghi lại các thao tác tạo mới, chỉnh sửa tại các ngày cụ thể
7	**Quản lý nhóm quyền**	Cho phép thiết lập vai trò (Role-based Access Control - RBAC) và phân quyền chi tiết cho người dùng và nhóm người dùng đối với các chức năng và dữ liệu khác nhau.
		Cho phép tạo nhóm quyền theo các trường thông tin như sau: Tên nhóm quyền, Phân loại, Danh sách quyền, Mô tả
		Cho phép sửa nhóm quyền Không cho sửa thông tin như Phân loại
		Cho phép xóa tài khoản khỏi hệ thống
		Cho phép tìm kiếm nhóm quyền theo tiêu chí: Tên nhóm quyền, Họ và tên
		Cho phép xem danh sách nhóm quyền gồm: STT, Tên nhóm quyền, Phân loại, Số lượng quyền, Phòng ban áp dụng, Người tạo, Ngày tạo, Trạng thái
		Cho phép xem lịch sử chỉnh sửa nhóm quyền, ghi lại các thao tác tạo mới, chỉnh sửa tại các ngày cụ thể

STT	Yêu cầu	Mô tả
8	**Quản lý Thông báo**	Cho phép nhận thông báo về sự cố, công việc, cảnh báo SLA qua Email
		Cho phép nhận thông báo về sự cố, công việc, cảnh báo SLA qua thông báo đẩy
		Cho phép nhận thông báo về sự cố, công việc, cảnh báo SLA qua biểu tượng quả chuông trên hệ thống
9	**Quản lý Danh mục**	Cho phép tạo, sửa, tìm kiếm, xem danh sách, xem lịch sử chỉnh sửa dán nhãn
		Cho phép tạo, sửa, tìm kiếm, xem danh sách, xem lịch sử chỉnh sửa mức độ nguy hiểm
		Cho phép tạo, sửa, tìm kiếm, xem danh sách, xem lịch sử chỉnh sửa loại sự cố
		Cho phép tạo, sửa, tìm kiếm, xem danh sách, xem lịch sử chỉnh sửa độ ưu tiên
		Cho phép tạo, sửa, tìm kiếm, xem danh sách, xem lịch sử chỉnh sửa phương án xử lý
10	**Quản lý SLA**	Cho phép tạo, sửa, tìm kiếm, xem danh sách, xem lịch sử chỉnh sửa SLA
		Cho phép tạo, sửa, tìm kiếm, xem danh sách, xem lịch sử chỉnh sửa cảnh báo SLA
		Xử lý job gửi cảnh báo định kỳ SLA theo sự cố, công việc
		Cung cấp API mở để tích hợp hai chiều với các giải pháp an toàn thông tin khác (SIEM, Firewall, EDR, Sandboxing, TIPs...).
11	**Quản lý Báo cáo**	Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo
		Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước

STT	Yêu cầu	Mô tả
		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 xem danh sách số lượng thành viên theo các đơn vị tham gia xử lý ứng cứu theo sự cố và công việc
		Cho phép đặt lịch gửi báo cáo định kỳ tới email được cấu hình
		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

Yêu cầu kỹ thuật hệ thống SOAR

4.6.1.3 *Yêu cầu về hệ thống NIPS*

Giải pháp NIPS giám sát và bảo vệ lớp của TTDL và TTDLDP của HOSE, cần cung cấp đảm bảo các tính năng:

STT	Yêu cầu	Mô tả
1	**Bóc tách và phân tích gói tin**	Sử dụng công nghệ kiểm tra gói sâu (Deep packet inspection - DPI) bóc tách các gói tin, phân tích và phát hiện các bất thường trong mạng kết hợp với bộ giải mã các giao thức phổ biến.
2	**Phát hiện tấn công mạng**	Thông qua theo dõi lưu lượng mạng để xác định các cuộc tấn công có chủ đích, các mối đe dọa nâng cao, ngụy trang, ẩn mình như APT, các tính năng chính bao gồm: - Phát hiện tấn công rà quét mật khẩu trong mạng. - Phát hiện dấu hiệu tấn công từ chối dịch vụ. - Phát hiện dấu hiệu tấn công rà quét lỗ hổng. - Phát hiện dấu hiệu tấn công ứng dụng Web (SQL Injection, XSS,…). - Phát hiện các dấu hiệu IoC của mã độc APT. - Phát hiện các kỹ thuật tấn công theo khung MITRE ATT&CK. - Phát hiện dấu hiệu rà quét thông tin mạng. - Phát hiện dấu hiệu khai thác dịch vụ.
3	**Bộ luật**	Phát hiện nhóm hành vi bất thường khác nhau trên lớp mạng, liên tục được cập nhật để có thể phát hiện được những dấu hiệu tấn công mới nhất, bao gồm các nhóm hành vi bất thường như: Network Scan, Trojan Activities, Shellcode Detect, Web Application Attack, Suspicious Login,…
4		Rà soát các kết nối liên quan đến một dấu hiệu tấn công mạng.

STT	Yêu cầu	Mô tả
	Hỗ trợ điều tra, phân tích chuyên sâu	Rà soát các kết nối liên quan đến một địa chỉ IP trong mạng.
		Hỗ trợ tái tạo các kết nối, truy vấn trong mạng dưới dạng PCAP để phục vụ điều tra, phân tích chuyển sâu.
		Có khả năng tích hợp với các giải pháp khác như SIEM thông qua các để gửi log qua giao thức syslog hoặc gửi cảnh báo qua API.
5	**Quản lý vận hành**	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, danh sách trắng địa chỉ IP, danh sách đen địa chỉ IP
		Cho phép thay đổi thời gian hệ thống, thời gian duy trì phiên kết nối
		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, …)
		Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực
		Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại
		Cho phép xóa log
		Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.
6	**Quản trị từ xa**	Sử dụng giao thức có mã hóa như TLS hoặc tương đương
		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.
7	**Quản lý xác thực và phân quyền**	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;
		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.

STT	Yêu cầu	Mô tả
8	**Quản lý các giao diện mạng**	Cho phép thiết lập một hoặc một số giao diện giám sát ở chế độ giám sát chủ động hoặc chế độ giám sát thụ động hoặc kết hợp cả hai chế độ
		Cho phép thiết lập tối thiểu một giao diện quản trị (khác với giao diện giám sát) để thực hiện
9	**Quản lý báo cáo**	Cho phép tạo mới, xem lại và xóa 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 thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;
		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;
		Cho phép tải về tệp tin báo cáo đã được xuất ra.
10	**Quản lý tập luật bảo vệ**	Cho phép thêm luật mới, tinh chỉnh, tìm kiếm, xóa, kích hoạt / vô hiệu hóa, xuất tệp tin, khôi phục và cập nhật luật.
11	**Quản lý danh sách trắng địa chỉ IP và danh sách đen địa chỉ IP**	Thêm, xóa, sửa, tìm kiếm địa chỉ/dải địa chỉ IP
		Thiết lập hành động kiểm soát lưu lượng mạng với địa chỉ/dải địa chỉ IP
		Kích hoạt/vô hiệu hóa hành động kiểm soát lưu lượng mạng đang được áp dụng đối với địa chỉ/dải địa chỉ IP
		Xuất danh sách địa chỉ/dải địa chỉ IP ra tệp tin
		Khôi phục danh sách địa chỉ/dải địa chỉ IP từ tệp tin.
12	**Quản lý tập các địa chỉ IP đang bị chặn kết nối**	Tìm kiếm các địa chỉ IP đang bị chặn kết nối theo địa chỉ IP, từ khóa
		Xem các thông tin về một địa chỉ IP đang bị chặn kết nối (tối thiểu bao gồm: thời điểm bắt đầu chặn kết nối, khoảng thời gian chặn chặn kết nối có hiệu lực tính từ thời điểm bắt đầu, số hiệu định danh của luật gây ra việc chặn chặn kết nối);

STT	Yêu cầu	Mô tả
		Hủy chặn kết nối đối với một hoặc nhiều địa chỉ IP cùng lúc đang bị chặn kết nối.
13	**Chia sẻ kết nối**	Cho phép kết nối với các loại hệ thống SIEM để chia sẻ dữ liệu
14	**Bảo vệ dữ liệu log**	Đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

Yêu cầu kỹ thuật hệ thống NIPS

4.6.1.4 *Yêu cầu về hệ thống EDR*

Giải pháp EDR giám sát và bảo vệ thiết bị điểm cuối của HOSE, cần cung cấp đảm bảo các tính năng:

STT	Nội dung	Mô tả
1	**Phát hiện mối nguy và chủ động phản ứng**	Thu thập thông tin và giám sát liên tục, quan trắc và phát hiện các mối đe dọa, cung cấp ngữ cảnh
		Hiển thị các mối nguy theo phân loại mức độ nguy hiểm, thời điểm phát hiện giúp các bộ vận hành nhanh chóng nhận diện và ưu tiên xử lý các mối nguy nghiêm trọng
		Hiển thị đầy đủ thông tin liên quan tới mối nguy như thời điêm xuất hiện đầu tiên, các máy tính có xuất hiện, các chuỗi hành vi bất thường và hành động phản ứng có thể thực hiện để xử lý mối nguy, cách ly các máy bị nhiễm
		Hệ thống chỉ thu nhận các thông tin như snapshot hệ thống khi có yêu cầu của cán bộ vận hành cho các máy tính đang nằm trong một trường hợp điều tra cụ thể
		Phát hiện dựa trên hành vi và tham chiếu vào khung MITRE ATT&CK giúp xác định giai đoạn tấn công và ưu tiên phản ứng
		Phân tích mức độ rủi ro và hiển thị thông tin trực quan giúp cán bộ điều tra nhanh chóng hiểu và quyết định hành động tiếp theo như bỏ qua hoặc phản ứng hoặc điều tra thêm
		Cho phép tạo các case điều tra đối với các mối nguy cần phân tích thêm, thiết lập mức độ ưu tiên, trạng thái xử lý, giao việc xử lý
		Tìm kiếm trong lịch sử các thông tin tối thiểu nhưng không hạn chế: hành vi truy nhập, tài khoản người dùng, các tiến trình, File, Script, công cụ hack, các services bị thay đổi, kết nối mạng, thay đổi schedule task, DNS request, các phát hiện và cảnh báo

		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,...
		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.
		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
		Cho phép cán bộ quản trị tạo thêm các công cụ thu thập dữ liệu, hành động phản ứng theo yêu cầu, sử dụng các ngôn ngữ và công cụ có sẵn như lệnh của hệ điều hành, Bash Script, Powershell, VBScript, Python Script
2	**Chống virus, mã độc, phần mềm gián điệp, độc hại**	Sử dụng công nghệ Machine Learning để phát hiện, ngăn chặn các tấn công phức tạp, các malicious payloads/malware
		Sử dụng công nghệ ngăn chặn hành vi độc hại của file mới để đảm bảo an toàn cho máy chủ kể cả khi file lạ được thực thi trên máy chủ
3	**Chống tấn công thâm nhập**	Công nghệ định danh tấn công và ngăn chặn: Signature-based & behavior-based
		Cho phép tự viết luật phát hiện (detection rule)
		Cung cấp sẵn cơ chế bảo vệ chủ động Startup firewall protection: Chỉ cho phép kết nối outgoing cho tới khi Firewall khởi động và enforce xong chính sách.
4	**Quản lý ứng dụng**	Kiểm kê các ứng dụng đã và đang có trên các máy tính / máy chủ hệ thống Cho phép xem thông tin ứng dụng đã kiểm kê trên toàn hệ thống hoặc trên một máy tính/máy chủ nào đó
		Sử dụng công nghệ bảo mật nâng cao cho Memory, phòng chống các tấn công khai thác vùng nhớ máy chủ.
5	**Quản lý thiết bị cắm ngoài và thiết bị ngoại vi**	- Disk storage (HDD), USB removable disk, CD/DVD, FireWire Storage - Printer, Bluetooth Device, Smart card reader, Imaging Device - Modem, LPT/COM port, Portable Device - Hỗ trợ các loại thiết bị ngoại vi
		Cho phép thiết lập cấu hình quét thiết bị ngoại vi
		Cho phép thiết lập danh sách các thiết bị cắm ngoài được phép sử dụng dựa trên thông số hãng, model, serial

6	**Quản lý tập trung**	Phần mềm phải có khả năng tập trung hóa quy trình quản lý, triển khai, báo cáo
		Có khả năng phân chia nhóm theo điều kiện (Dynamic Group)
		Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn hệ thống
		Hỗ trợ cập nhật cấu hình cho nhiều máy trạm từ máy chủ quản lý
		Hỗ trợ lập lịch tự động tải các phiên bản cập nhật
		Hỗ trợ tải các phiên bản cập nhật từ các mirror server, HTTP Proxy Server hoặc trực tiếp từ Internet
		Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn mạng

Yêu cầu kỹ thuật hệ thống EDR

4.6.1.5 *Yêu cầu về hệ thống TIP (Threat Intelligence Platform)*

Giải pháp TIP cung cấp các thông tin tình báo, nguy cơ ATTT chủ động cho HOSE, cần cung cấp đảm bảo các tính năng:

STT	Yêu cầu	Mô tả
1	**Quản trị hệ thống**	Hỗ trợ quản lý cấu hình tài khoản xác thực và phân quyền chi tiết
		Có khả năng tích hợp với các hệ thống xác thực tập trung như LDAP/AD, SAML
		Cung cấp chức năng quản lý, sao lưu (backup) và phục hồi (restore) cấu hình và dữ liệu TIP.
		Cung cấp giao diện tổng hợp, đa chiều về các mối đe doạ, cảnh báo kịp thời qua Email/ SMS/Điện thoại trực tiếp.
		Cung cấp bộ lọc linh hoạt, tiện dụng. Tra cứu, truy vấn thông tin
2	**Yêu cầu về tính năng Thu thập, Xử lý và Lưu trữ dữ liệu**	Hỗ trợ thu thập dữ liệu TI từ nhiều nguồn (mở, thương mại, nội bộ) qua nhiều giao thức
		Cung cấp và cập nhật thông tin hàng ngày về các chỉ dấu mã độc (IOC) bao gồm: domain, Hash, IP, Host name, URI, URL…
		Cung cấp thông tin về các nhóm tội phạm mạng bao gồm các quốc gia, lĩnh vực mà nhóm tội phạm nhắm tới; các kỹ thuật, chiến thuật tấn công (TTPs), công cụ, mã độc, lỗ hổng CVE… được sử dụng cho các hoạt động tấn công; các tập luật phát hiện các mối nguy
		Thông tin về các cuộc tấn công của Ransomware, Botnet
		Cung cấp thông tin về các cuộc nói chuyện/trao đổi liên quan tới tổ chức trên Forum/ Deep web và trên Telegram/Discord

		Hỗ trợ các định dạng dữ liệu chuẩn để nhập (ví dụ: STIX/TAXII, CSV, JSON)
		Có khả năng chuẩn hóa (Normalization) dữ liệu thu thập được về một định dạng thống nhất
		Cung cấp chức năng tự động làm giàu thông tin (Data Enrichment) cho IOCs
		Có cơ chế tự động loại bỏ các chỉ số đe dọa trùng lặp
		Có chức năng phân loại mức độ nghiêm trọng/độ tin cậy của dữ liệu TI
		Hỗ trợ lưu trữ dữ liệu TI có cấu trúc, cho phép truy vấn nhanh chóng, và đảm bảo tuân thủ chính sách lưu trữ
		Có khả năng phân tích và liên kết các chỉ số đe dọa, chiến dịch tấn công, nhóm tấn công
		Hỗ trợ liên kết mối đe dọa với các kỹ thuật tấn công theo mô hình chuẩn (ví dụ: MITRE ATT&CK)
		Nhận diện các lỗ hổng CVE, ports, và các thông tin khác liên quan đến Domain/ sub Domain/ IP address.
		Nhận diện các vấn đề về chứng chỉ SSL/TLS.
		Nhận diện các lỗ hổng, cấu hình sai với ứng dụng Web công khai của tổ chức.
3	**Yêu cầu về tích hợp**	Tích hợp đẩy các thông tin IoC cho các giải pháp bảo mật như SIEM, SOAR, TIP…
4	**Yêu cầu về Báo cáo**	Cho phép tạo báo cáo với mỗi khách hàng: chiến dịch tấn công, sự cố bảo mật, phân tích mã độc, danh sách IoC, danh sách tài khoản bị lộ lọt…
		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 thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;
		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;
		Cho phép tải về tệp tin báo cáo đã được xuất ra.

Yêu cầu kỹ thuật hệ thống Threat Intelligence Platform – TIP

4.6.1.6 *Xây dựng giải pháp và phương án phòng, chống thất thoát dữ liệu (DLP)*

- Hiện nay, HoSE có 03 phân vùng cần áp dụng giải pháp và quy trình phòng, chống thất thoát dữ liệu gồm: (1) Phân vùng máy chủ; (2) Phân vùng máy vi tính vận hành; (3) Phân vùng thiết bị mạng.

- Tương thích của chương trình với hệ thống bảo mật đầu cuối được đề nghị bởi nhà thầu.

- Nhận diện và ngăn chặn các dữ liệu được HOSE chỉ định thông qua URL, export hoặc tạo ra chương trình pdf, excel, words, file csv…

- Nhận diện các file có cấu trúc hoặc phi cấu trúc

- Cảnh báo khi có vi phạm cũng như có lưu đồ xử lý cho các trường hợp ngoại lệ và phê duyệt cụ thể

- Xây dựng quy trình, quy định truy cập và sử dụng dữ liệu, phù hợp với hiện trạng và giải pháp do nhà thầu cung cấp.

1	**Giải pháp phòng, chống thất thoát dữ liệu (DLP)**	**1**	**Gói/Năm**
	- Phạm vi: - Tại DC & DR có 153 máy chủ vật lý và ảo hóa, được phân bố cụ thể như sau: - Tại Trung tâm dữ liệu (TTDL): + 32 máy chủ vật lý & 116 máy chủ ảo hóa. + 45 thiết bị mạng; - Tại Trung tâm dữ liệu dự phòng (TTDLDP): + 02 máy chủ vật lý & 03 máy chủ ảo hóa. + 11 thiết bị mạng; - Tổng số máy trạm (desktop): 239 máy;		
	- Yêu cầu tính năng tối thiểu như sau:		
	+ Tương thích của chương trình với hệ thống bảo mật đầu cuối được đề nghị bởi nhà thầu.		
	+ Nhận diện và ngăn chặn các dữ liệu được HoSE chỉ định thông qua URL, export hoặc tạo ra chương trình pdf, excel, words, file csv…		
	+ Nhận diện các file có cấu trúc hoặc phi cấu trúc.		
	+ Cảnh báo khi có vi phạm cũng như có lưu đồ xử lý cho các trường hợp ngoại lệ và phê duyệt cụ thể.		
	+ Xây dựng quy trình, quy định truy cập và sử dụng dữ liệu, phù hợp với hiện trạng và giải pháp do nhà thầu. cung cấp.		

Yêu cầu kỹ thuật hệ thống giải pháp DLP

4.6.1.7 *Yêu cầu kỹ thuật phòng chống tấn công từ chối dịch vụ (DDOS)*

Giải pháp Anti DDOS cho 02 đường truyền cần đảm bảo các tính năng sau:

- Băng thông xử lý khi có tấn công là 5Gb.

- Giám sát lưu lượng thời gian thực, tự động phát hiện bất thường và kích hoạt biện pháp ngăn chặn.

- Lọc bỏ lưu lượng độc hại, đảm bảo duy trì hoạt động ổn định cho hệ thống và ứng dụng hợp lệ.

- Tự động mở rộng năng lực xử lý khi tấn công tăng cao, đảm bảo không gián đoạn dịch vụ.

- Cho phép tích hợp linh hoạt với hạ tầng hiện hữu và các thiết bị bảo mật khác (nếu có).

4.6.1.8 *Yêu cầu triển khai giám sát lớp mạng và vành đai*

Việc triển khai giám sát ở lớp mạng và vành đai cho phép phát hiện:

+ Các kết nối, truy vấn tới các máy chủ điều khiển mạng botnet (C&C Server);

+ Các file mã độc, URL nguy hiểm được truyền qua môi trường mạng (với các giao thức không mã hóa) thông qua log của hệ thống Webproxy hoặc Firewall Internet;

+ Các Shellcode, payload tấn công khai thác lỗ hỗng phần mềm, dịch vụ trong dữ liệu truyền tải trên mạng thông qua phân tích các dấu hiệu đặc trưng

+ Các hành vi bất thường như dò quét mạng, dò quét tài khoản mật khẩu mặc định, mật khẩu yếu ...

Thông tin log lấy tối thiểu từ các hệ thống sau (nếu có):

+ Log của hệ thống Firewall

+ Log của thiết bị Router, switch

+ Log của hệ thống IPS/IDS

+ Log của hệ thống phòng chống tấn công từ chối dịch vụ (DDoS)

+ Log của thiết bị phòng chống tấn công có chủ đích (APT)

+ Log hệ thống quản lý truy cập

+ Log của hệ thống EDR

4.6.1.9 *Triển khai giám sát lớp máy chủ và hệ điều hành*

Việc triển khai giám sát ở lớp máy chủ và hệ điều hành cho phép phát hiện:

+ Các hành vi vi phạm chính sách truy cập, quản lý, thiết lập cấu hình hệ điều hành, các dịch vụ hệ thống;

+ Các kết nối của máy chủ ra các địa chỉ IP độc hại;

+ Các hình thức tấn công mạng như tấn công khai thác điểm yếu, tấn công dò quét và các dạng tấn công tương tự khác;

+ Các tiến trình có dấu hiệu bất thường về hành vi và việc sử dụng tài nguyên máy chủ.

Thông tin log lấy tối thiểu từ các hệ thống sau:

+ Log hệ điều hành máy chủ;

+ Log hệ thống dịch vụ AD/DNS, KMS, NTP;

+ Log Web Server, App Server.

+ Log các hệ thống an toàn thông tin (IPS, EDR, Endpoint Security, PAM ....).

Nguồn log tối thiểu gồm các thông tin:

+ Thông tin đăng nhập vào máy chủ;

+ Lỗi phát sinh trong quá trình hoạt động (nhật ký trạng thái hoạt động của máy chủ);

+ Thông tin về các tiến trình hệ thống;

+ Thông tin thay đổi cấu hình máy chủ ..

4.6.1.10 *Triển khai giám sát lớp ứng dụng*

Việc triển khai giám sát lớp ứng dụng cho phép phát hiện:

+ Các dạng tấn công vào lớp ứng dụng như SQLi, XSS ...;

+ Tấn công dò quét, vét cạn mật khẩu, thư mục và khai thác thông tin;

+ Tấn công Phishing và cài cắm mã độc trên ứng dụng;

+ Tấn công từ chối dịch vụ.

Thông tin log lấy từ các hệ thống sau (bao gồm nhưng không giới hạn):

+ Access log

+ Log của các ứng dụng phục vụ hoạt động của hệ thống: DHCP, DNS, NTP, VPN, Proxy Server ...

+ Ứng dụng cung cấp dịch vụ: Web, Mail, FPT, TFTP và các hệ quản trị cơ sở dữ liệu Oracle, SQL, MySQL ...

+ Log hệ thống bảo mật như Firewall, Web Application Firewall

+ Log của hệ thống IPS/IDS;

Nguồn log tối thiểu gồm các thông tin:

+ Thông tin truy cập ứng dụng;

+ Thông tin đăng nhập khi quản trị ứng dụng;

+ Thông tin các lỗi phát sinh trong quá trình hoạt động;

Triển khai giám sát lớp cơ sở dữ liệu

Việc triển khai giám sát lớp cơ sở dữ liệu cho phép phát hiện:

+ Truy cập bất thường hoặc trái phép vào cơ sở dữ liệu, đặc biệt từ các tài khoản đặc quyền.

+ Hành vi truy vấn hoặc chỉnh sửa dữ liệu nhạy cảm vượt ngoài phạm vi được phép.

+ Thao tác nghi ngờ khai thác lỗ hổng SQL hoặc thực thi mã độc trong câu lệnh truy vấn.

+ Thay đổi cấu hình hoặc phân quyền không hợp lệ trong hệ thống cơ sở dữ liệu

Thông tin log lấy từ các hệ thống sau (bao gồm nhưng không giới hạn):

+ Nhật ký truy cập và truy vấn cơ sở dữ liệu (Query log, Access log).

+ Nhật ký hệ thống và dịch vụ quản trị cơ sở dữ liệu (Audit log, Error log).

+ Log hệ thống bảo mật như Firewall, Database Firewall.

+ Log của hệ thống IPS/IDS;

Nguồn log tối thiểu gồm các thông tin:

+ Thông tin truy cập co sở dữ liệu;

+ Thông tin đăng nhập khi quản trị cơ sở dữ liệu;

+ Thông tin các lỗi phát sinh trong quá trình hoạt động;

4.6.2 Yêu cầu chất lượng dịch vụ thực hiện

Nhà thầu đảm bảo tiêu chí chất lượng dịch vụ giám sát và ứng cứu sự cố an toàn thông tin mạng như sau:

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm Nhà thầu	Trách nhiệm HOSE	Mục tiêu cam kết
I	**Quản lý các sự kiện ATTT**					
	Giám sát cảnh báo ATTT					
1	Tỷ lệ xử lý cảnh báo đúng hạn	- Là tỉ lệ giữa số lượng cảnh báo ATTT đã hoàn thành xử lý với Tổng số lượng cảnh báo trên hệ thống SOC. - Thời gian xử lý cảnh báo ATTT đúng hạn, cụ thể như sau: + Nghiêm trọng: ≤ 30 phút + Thông thường: ≤ 01 giờ	Từ thời điểm cảnh báo được tạo trên hệ thống đến khi cảnh báo được đóng hoặc gửi thông báo xác nhận cảnh báo với nhân sự HOSE	R		90%
II	**Xử lý sự cố ATTT**					
	Phân tích xử lý sự cố theo hướng dẫn					
1	Thời gian đưa ra giải pháp ngăn chặn sự cố khẩn cấp	Là thời gian từ khi xác định là sự cố theo quy trình giám sát ATTT cho đến khi đưa ra được các khuyến nghị ngăn chặn sự cố, được xác định như sau: + Nghiêm trọng: ≤ 2 giờ + Thông thường: ≤ 4 giờ	Từ thời điểm ghi nhận sự cố xuất hiện đến khi HOSE nhận được phương án phương án ngăn chặn sự cố khẩn cấp từ Nhà thầu	S	R	90%
	Phân tích và xử lý sự cố chưa có hướng dẫn					
2	Thời gian đưa ra giải pháp	Là thời gian từ khi xác định là sự cố theo quy trình giám sát ATTT cho đến	Từ thời điểm ghi nhận sự cố xuất hiện đến khi HOSE	R	S	90%

	ngăn chặn sự cố khẩn cấp	khi đưa ra được các khuyến nghị ngăn chặn sự cố khẩn cấp thời cho hệ thống của khách hang, được xác định như sau: + Nghiêm trọng: ≤ 3 giờ + Thông thường: ≤ 5 giờ	nhận được phương án phương án ngăn chặn sự cố khẩn cấp từ Nhà thầu			
3	Phân tích và điều tra sự cố	Nhà thầu sẽ thực hiện điều tra sự cố trên hệ thống SIEM, trong trường hợp không thể điều tra trên hệ thống SIEM, HOSE hỗ trợ Nhà thầu được truy cập trực tiếp vào hệ thống để thực hiện rà soát các máy chủ bị ảnh hưởng. Nhà thầu sẽ thực hiện phân tích và điều tra tuỳ thuộc vào từng loại sự cố khác nhau. Sau khi hoàn thành việc phân tích và điều tra sự cố, đối tác sẽ lập báo cáo sơ bộ (tổng quan về sự cố, khuyến nghị khắc phục). *Thời gian phân tích và điều tra sự cố* được mô tả chi tiết bên dưới.	Là thời gian từ khi phát hiện sự cố đến khi Nhà thầu đưa ra kết quả phân tích và báo cáo sơ bộ về sự cố. Trong quá trình điều tra, nếu có thay đổi về phạm vi sự cố thì thực hiện mở rộng phạm vi sự cố.	R	S	90%
III	**Tối ưu cảnh báo**					
1	Tỷ lệ ticket tối ưu xử lý đúng hạn	- Là tỷ lệ giữa số lượng ticket tối ưu hoàn thành xử lý trong thời gian quy định với Tổng số lượng tickets tối ưu được tạo, gán cho	Từ thời điểm ticket tối ưu có trạng thái OPEN đến khi ticket chuyển trạng thái CLOSE	R	S	90%

		nhóm Content Analyst trên hệ thống SOC. - Thời gian xử lý ticket tối ưu quy định theo loại ticket tối ưu, cụ thể như sau: + Cao: ≤ 24 giờ + Trung bình: ≤120 giờ + Thấp: ≤ 360 giờ Trong đó: - Mức CAO: với các yêu cầu chỉnh sửa tối ưu cảnh báo gấp do các cảnh báo phát sinh sai, hoặc lặp lại nhiều gây nhiễu, ảnh hưởng gây gián đoạn việc vận hành giám sát ATTT. - Mức TRUNG BÌNH: với các yêu cầu chỉnh sửa tối ưu cảnh báo nhằm nâng cao tính chính xác dù hiện tại việc vận hành giám sát chưa bị ảnh hưởng trực tiếp, whitelist các trường hợp ngoại lệ. - Mức THẤP: Các góp ý, yêu cầu bổ sung các tính năng công cụ hỗ trợ việc vận hành giám sát, phân tích, xử lý cảnh báo ATTT.				
IV	**Các hoạt động liên quan việc vận hành cung cấp dịch vụ**					
1	Tỷ lệ báo cáo tháng toàn diện	- Là tỷ lệ báo cáo hàng tháng gửi HOSE đúng hạn với Tổng số báo cáo tháng gửi HOSE.	Tỷ lệ báo cáo hàng tháng gửi HOSE đúng hạn với Tổng số báo cáo	R	I	90%

	công tác ATTT của HOSE đúng hạn	- Thời gian báo cáo đúng hạn, gửi vào ngày thống nhất giữa hai bên.	tháng gửi HOSE (Thời gian báo cáo đúng hạn, gửi vào ngày thống nhất giữa hai bên)			
V	**Chất lượng của hệ thống giám sát cảnh báo**					
1	Số lượng cảnh báo mức Nghiêm trọng mà hệ thống không phát hiện được	Số lượng cảnh báo mức Nghiêm trọng được gửi từ Tier 2 – SOC (HOSE) mà hệ thống không phát hiện được và được Tier 1 xác minh chính xác trong tháng	Đo bằng số lượng cảnh báo được Tier 2 HOSE gửi đến Nhà thầu theo đúng "Quy trình phối hợp xử lý sự cố ATTT" và được Tier 1 xác minh chính xác là sự cố mức Nghiêm trọng và hệ thống không phát hiện được. Việc đo lường số lượng cảnh báo mà hệ thống không phát hiện được sẽ được tính nếu các thông tin sự kiện liên quan đến cảnh báo đó được thu thập và lưu trữ trên hệ thống SIEM	R	I	0 cảnh báo
2	Số lượng cảnh báo mức Thông thường mà hệ thống	Số lượng cảnh báo mức Thông thường được gửi từ Tier 2 – SOC (HOSE) mà hệ thống không phát hiện được và được Tier 1 xác minh	Đo bằng số lượng cảnh báo được Tier 2 HOSE gửi đến Nhà thầu và được Tier 1 xác minh chính xác là sự	R	I	5 cảnh báo

	không phát hiện được	chính xác trong tháng	cố mức Thông thường và hệ thống không phát hiện được. Việc đo lường số lượng cảnh báo mà hệ thống không phát hiện được sẽ được tính nếu các thông tin sự kiện liên quan đến cảnh báo đó được thu thập và lưu trữ trên hệ thống SIEM			

Yêu cầu cam kết chất lượng dịch vụ

- Phân loại trách nhiệm theo mô hình RASCI:

+ R - Responsible: Trách nhiệm thực hiện chính.

+ A - Approval: Trách nhiệm phê duyệt, đồng ý nội dung thực hiện.

+ S - Support: Trách nhiệm hỗ trợ bên thực hiện chính.

+ C - Consulted: Trách nhiệm dựa vào kiến thức, kinh nghiệm chuyên môn tư vấn giải pháp thực hiện.

+ I - Informed: Trách nhiệm được cung cấp thông tin.

4.7. Kết quả thực hiện

Sản phẩm tư vấn của hạng mục "Thuê dịch vụ giám sát an toàn thông tin mạng cho các hệ thống thông tin của Sở" bao gồm bộ báo cáo, hệ thống SOC 24/7, quy trình ứng phó, hồ sơ kỹ thuật và kết quả đánh giá an toàn thông tin, đảm bảo tuân thủ pháp lý, nâng cao năng lực giám sát, phát hiện và ứng phó sự cố, phục vụ quản lý vận hành hệ thống CNTT cấp độ 3 của HOSE.

Việc triển khai Dịch vụ giám sát ATTT mạng (SOC) mang lại các kết quả và giá trị pháp lý – kỹ thuật cụ thể như sau:

- Nâng cao năng lực bảo đảm an toàn thông tin mạng ở cấp độ 3, đáp ứng đầy đủ yêu cầu quy định tại:

+ Luật An toàn thông tin mạng số 86/2015/QH13;

+ Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

+ Thông tư số 12/2022/TT-BTTTT của Bộ Thông tin và Truyền thông hướng dẫn chi tiết về kiểm tra, giám sát, và đánh giá hệ thống thông tin cấp độ 3.

- Tăng cường năng lực giám sát, phát hiện và ứng phó sự cố an toàn thông tin một cách chủ động, toàn diện, bảo đảm:

+ Giám sát 24/7 đối với toàn bộ hạ tầng CNTT của HOSE;

+ Phát hiện sớm các hành vi tấn công, xâm nhập, rò rỉ dữ liệu;

+ Triển khai các biện pháp phòng ngừa, ứng cứu và khắc phục sự cố kịp thời, hạn chế tối đa thiệt hại;

+ Bảo đảm an toàn tuyệt đối cho hạ tầng công nghệ và hoạt động giao dịch chứng khoán quốc gia, góp phần duy trì tính liên tục, ổn định và minh bạch của thị trường chứng khoán Việt Nam;

- Tăng cường khả năng tuân thủ pháp luật và kết nối an toàn với các hệ thống trọng yếu, bao gồm:

+ Hệ thống Hệ thống công nghệ thông tin cho thị trường chứng khoán Việt Nam;

+ Sở Giao dịch Chứng khoán Hà Nội (HNX);

+ Trung tâm Lưu ký Chứng khoán Việt Nam (VSDC);

+ Các ngân hàng thanh toán và tổ chức thành viên thị trường.

- Đáp ứng đầy đủ các yêu cầu pháp lý và tiêu chuẩn kỹ thuật quốc gia về an toàn thông tin cấp độ 3, là cơ sở để:

+ Cơ quan quản lý nhà nước (Bộ KHCN, Bộ Tài chính, Ủy ban Chứng khoán Nhà nước) công nhận kết quả đánh giá;

+ Làm căn cứ pháp lý phục vụ nghiệm thu, thẩm định, phê duyệt và báo cáo định kỳ về bảo đảm an toàn thông tin cho toàn hệ thống của HOSE.

4.8 Sản phẩm dịch vụ (nhà thầu bàn giao cho HOSE)

Sản phẩm tư vấn chính của hạng mục Thuê dịch vụ Giám sát An toàn Thông tin mạng (ATTT) cho các Hệ thống Thông tin của Sở (SOC) là các tài liệu báo cáo mang tính định kỳ và tổng hợp về tình trạng ATTT, kết quả giám sát, và các khuyến nghị.

Dựa trên bản chất của dịch vụ SOC và mục tiêu tuân thủ của HOSE (Hệ thống Cấp độ 3), các sản phẩm bàn giao (Deliverables) chính sẽ bao gồm:

5.9.1. Hệ thống giám sát an toàn thông tin hoạt động 24/7

- Thiết lập kết nối giám sát giữa HOSE và SOC thuê ngoài.

- Tích hợp log từ các nguồn: Firewall, IDS/IPS, WAF, Endpoint, Server, Database, Application, AD, Proxy, Mail, v.v.

- Bảng điều khiển (Dashboard) hiển thị tình trạng an toàn thời gian thực, phân loại cảnh báo (Critical – High – Medium).

- Hệ thống SOC vận hành liên tục, đảm bảo SLA ≥ 99.9%.

5.9.2. Sản phẩm Báo cáo Định kỳ (Operational Reports)

Đây là các báo cáo được cung cấp liên tục, phản ánh hiệu quả giám sát và tình trạng ATTT theo thời gian thực:

- Báo cáo kết quả Giám sát, quản lý các sự kiện ATTT và cảnh báo ATTT trong Báo cáo hàng tuần và hàng tháng về Dịch vụ giám sát an toàn thông tin mạng;

- Báo cáo kết quả xử lý sự cố ATTT (nếu có) trong Báo cáo hàng tháng về Dịch vụ giám sát an toàn thông tin mạng;

- Báo cáo kết quả cảnh báo nguy cơ về ATTT trong Báo cáo hàng tháng về Dịch vụ giám sát an toàn thông tin mạng;

- Báo cáo Dịch vụ tìm kiếm chủ động các nguy cơ về an toàn thông tin mạng trong Báo cáo hàng tháng về Dịch vụ giám sát an toàn thông tin mạng.

5.9.3. Các hồ sơ tài liệu khác:

- Quy trình phối hợp giám sát ATTT.

5. Yêu cầu dịch vụ

Yêu cầu dịch vụ đối với hạng mục Thuê dịch vụ giám sát an toàn thông tin mạng (ATTT) cho các hệ thống thông tin của Sở (SOC) là rất chi tiết và tập trung vào hiệu suất hoạt động 24/7, khả năng phân tích chuyên sâu (tương quan), và cam kết về chất lượng ứng phó sự cố (SLA).

6.1. Yêu cầu về Phạm vi Giám sát và Tích hợp Log

Dịch vụ phải đảm bảo khả năng thu thập và phân tích log từ toàn bộ hệ thống trọng yếu của HOSE.

6.1.1. Phạm vi Bao phủ Log Source:

- Máy chủ: Giám sát log ATTT và log hệ thống từ các máy chủ (bao gồm cả máy vật lý và máy ảo hóa) chạy các HĐH Windows Server và Red Hat Linux/Ubuntu…

- Thiết bị Mạng & Bảo mật: Giám sát log và cảnh báo từ các thiết bị (Router, Switch, 10 Firewall Cisco Firepower, WAF F5 ASM) và các giải pháp bảo mật đầu cuối (Endpoint như Symantec, Trend Micro, McAfee).

- Ứng dụng & CSDL: Bắt buộc phải tích hợp và phân tích log từ 8 hệ thống nghiệp vụ cốt lõi và 02 hệ thống CSDL (Oracle, SQL Server) để phát hiện các truy vấn bất thường và tấn công logic.

- Bảo phủ Mạng Lưới: Đảm bảo khả năng thu thập log từ tất cả 29 VLAN và 25 dải mạng, đặc biệt là các khu vực nhạy cảm: DMZ (máy chủ công khai), Dải mạng Máy chủ Nội bộ, và Trung tâm Dữ liệu Dự phòng (DR).

6.1.2. Yêu cầu về Hiệu suất Giám sát và Phân tích (SOC Platform)

Nhà thầu phải đảm bảo nền tảng công nghệ và quy trình vận hành SOC đạt hiệu suất cao:

- Phân tích Tương quan: Bắt buộc phải xây dựng và duy trì các bộ quy tắc tương quan (Custom Correlation Rules) được tùy chỉnh để liên kết các sự kiện đơn lẻ từ nhiều nguồn log khác nhau, nhằm phát hiện các cuộc tấn công nhiều giai đoạn (Multi-stage Attacks) và tấn công Logic Nghiệp vụ.

- Khả năng Phân tích Hành vi: Giải pháp phải có khả năng áp dụng phân tích UEBA (User and Entity Behavior Analytics) để nhận diện các hành vi bất thường, đặc biệt là các hành vi của người dùng quản trị nội bộ.

- Quản lý Log: Đảm bảo khả năng Normalize (chuẩn hóa) và Parse (phân tích cú pháp) log một cách chính xác, đồng thời cung cấp khả năng lưu trữ log theo yêu cầu tuân thủ pháp lý (thường là 6 tháng đến 1 năm).

- Hoạt động 24/7: Cung cấp dịch vụ Giám sát liên tục 24 giờ/ngày, 7 ngày/tuần bởi đội ngũ chuyên gia SOC.

6.1.3. Yêu cầu về Ứng phó Sự cố (Incident Response - IR) và SLA

- Quy trình Ứng phó: Thiết lập và tuân thủ Quy trình Ứng phó Sự cố (IR Playbook) đã được phê duyệt, bao gồm cả việc Phân loại Mức độ Nghiêm trọng của sự cố (Critical, High, Medium, Low).

- Báo cáo và Chuyển giao: Cung cấp các báo cáo định kỳ (Tuần/Tháng/Quý) chi tiết về sự cố, phân tích xu hướng, và Báo cáo Tổng kết Tình trạng ATTT (Security Posture), bao gồm cả khuyến nghị khắc phục chiến lược.

6. Yêu cầu về năng lực của nhà thầu cung cấp dịch vụ:

6.1 *Yêu cầu chung*

- Dịch vụ SOC phải đảm bảo năng lực triển khai, vận hành, giám sát và phân tích sự kiện an toàn thông tin (ATTT) cho toàn bộ hệ thống CNTT của Sở Giao dịch Chứng khoán TP. Hồ Chí Minh.

- Nhà thầu phải là đơn vị chuyên nghiệp trong lĩnh vực an toàn thông tin, có năng lực kỹ thuật, hệ thống SOC hoạt động thực tế tại Việt Nam, đáp ứng đầy đủ các quy định pháp luật hiện hành.

- Dịch vụ được cung cấp theo mô hình SOC-as-a-Service, kết nối giám sát từ xa qua đường truyền bảo mật (VPN/MPLS), hoạt động liên tục 24 giờ/ngày, 7 ngày/tuần (24/7).

- Mục tiêu: đảm bảo hệ thống CNTT của HOSE được giám sát tập trung, phát hiện – cảnh báo – ứng phó kịp thời, duy trì tuân thủ an toàn thông tin cấp độ 3.

6.2 *Yêu cầu năng lực nhà thầu*

Là doanh nghiệp được thành lập hợp pháp tại Việt Nam, có đăng ký ngành nghề kinh doanh liên quan đến dịch vụ an toàn thông tin mạng.

- Có Giấy phép kinh doanh hoặc Giấy chứng nhận đăng ký doanh nghiệp do cơ quan có thẩm quyền cấp;

- Có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng do Bộ Thông tin và Truyền thông cấp (theo Nghị định 108/2016/NĐ-CP) hoặc theo quy định được Bộ Khoa học Công nghệ công nhận tại thời điểm triển khai.

- Có tư cách pháp nhân độc lập, không trong thời gian bị đình chỉ hoặc xử phạt vi phạm hành chính trong lĩnh vực ATTT.

- Có cam kết bảo mật thông tin và chịu trách nhiệm pháp lý về toàn bộ kết quả đánh giá, thử nghiệm, báo cáo.

- Có Trung tâm SOC đáp ứng tối thiểu chứng nhận:

  + ISO/IEC 27001:2022 (An toàn thông tin);

- Có khả năng kết nối, chia sẻ IOC/Threat Intel với các SOC cấp bộ/ngành liên quan.

6.3 *Năng lực pháp chế và cam kết bảo mật*

Nhà thầu cung cấp cam kết bảo mật thông tin bao gồm tối thiểu các nội dung sau:

- Ký Thỏa thuận bảo mật thông tin (NDA) với chủ đầu tư: Nhà thầu cam kết không tiết lộ bất kỳ thông tin, dữ liệu hoặc tài liệu nào có chứa các thông tin, dữ liệu như sau:

+ Thông tin, dữ liệu của Chủ đầu tư và của các hệ thống trong phạm vi triển khai của dự án.

+ Thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ.

- Nhà thầu cam kết chịu trách nhiệm nếu để xảy ra việc lộ lọt thông tin dữ liệu trong quá trình thuê dịch vụ do lỗi của nhà thầu và của các nhân sự tham gia vào dự án theo đề xuất của nhà thầu.

- Nhà thầu cam kết chỉ sử dụng các các nhân sự tham gia vào dự án theo đề xuất của nhà thầu, cam kết không sử dụng các nhân sự khác khi chưa được sự đồng ý của chủ đầu tư.

- Có chính sách xử lý sự cố và vi phạm bảo mật nội bộ rõ ràng.

- Có cơ chế lưu trữ, bàn giao, tiêu hủy dữ liệu sau khi hoàn thành kiểm tra.

7. Yêu cầu tiêu chuẩn, quy chuẩn cần áp dụng

- Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;
- Nghị định số 147/2024/NĐ-CP ngày 09/11/2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;
- Nghị định số 25/2014/NĐ-CP ngày 07/4/2014 của Chính phủ quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao;
- Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ;
- Chỉ thị số 14/CT-TTg ngày 07/06/2019 của Thủ tướng chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;
- Tiêu chuẩn TCVN ISO/IEC 27001:2019 ISO/IEC 27001:2013: Hệ thống quản lý an toàn thông tin;
- Tiêu chuẩn TCVN 10295:2014 & ISO/IEC 27005:2011: Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin;
- Tiêu chuẩn TCVN 9801-3:2014 & ISO/IEC 27033-3:2010: Kỹ thuật an toàn - An toàn mạng;
- Tiêu chuẩn quốc gia TCVN 11930:2017 về công nghệ thông tin - Các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;
- Thông tư số 13/2017/TT-BTTTT ngày 23/6/2017 của Bộ Thông tin và Truyền thông về quy định các yêu cầu kỹ thuật về kết nối các hệ thống thông tin, cơ sở dữ liệu với cơ sở dữ liệu quốc gia;
- Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;
- Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;
- Quyết định 1356/QĐ-BTTTT ngày 07/07/2022 của Bộ Thông tin và Truyền thông Ban hành tiêu chí đánh giá giải pháp, dịch vụ trung tâm giám sát điều hành án toàn, an ninh mạng (SOC);
- Các tiêu chuẩn theo quy định của pháp luật hiện hành, và tại thời điểm triển khai.

8. Quyền sở hữu, bảo mật thông tin, dữ liệu

Thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ công nghệ thông tin thuộc sở hữu của Chủ đầu tư. Nhà cung cấp dịch vụ có trách nhiệm bảo đảm an ninh, an toàn thông tin, chuyển giao đầy đủ cho cơ quan, đơn vị thuê các thông tin, dữ liệu khi kết thúc hợp đồng thuê dịch vụ công nghệ thông tin.

9. Yêu cầu khác

- Nhà thầu cam kết cung cấp Đội ngũ chuyên gia ứng cứu sự cố, số lượng 05 chuyên gia trong số 12 nhân sự chốt do nhà thầu đề xuất.
- Nhà thầu cung cấp giải pháp, công cụ và thiết bị (phần cứng, phần mềm, thiết bị mạng,…) phục vụ cho dịch vụ giám sát an toàn thông tin mạng.

IV. Giải pháp và phương pháp luận:

Nhà thầu đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Có kế hoạch triển khai, giải pháp công cụ giám sát trong vòng tối đa 60 ngày.

V. Quy định về kiểm tra, nghiệm thu sản phẩm:

- Báo cáo kết quả Giám sát, quản lý các sự kiện ATTT và cảnh báo ATTT trong Báo cáo hàng tuần và hàng tháng về Dịch vụ giám sát an toàn thông tin mạng
- Báo cáo kết quả xử lý sự cố ATTT (nếu có) trong Báo cáo hàng tháng về Dịch vụ giám sát an toàn thông tin mạng
- Báo cáo kết quả cảnh báo nguy cơ về ATTT trong Báo cáo hàng tháng về Dịch vụ giám sát an toàn thông tin mạng.
- Báo cáo Dịch vụ tìm kiếm chủ động các nguy cơ về an toàn thông tin mạng trong Báo cáo hàng tháng về Dịch vụ giám sát an toàn thông tin mạng.
- Biên bản nghiệm thu dịch giám sát ATTT mạng 3 tháng/lần.
- Báo cáo đột xuất khi có yêu cầu.