Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về gói thầu

- Tên gói thầu: Thuê dịch vụ giám sát và đảm bảo an toàn mạng cho hệ thống thông tin của Bộ Công Thương
- Chủ đầu tư: Cục Thương mại điện tử và Kinh tế số.
- Nguồn vồn: Sự nghiệp kinh tế
- Thời gian thực hiện: 120 ngày
- Hình thức hợp đồng: Trọn gói.

2. Mục tiêu công việc

- Nâng cao tính chủ động và hiệu quả xử lý, giảm thiểu tấn công nhằm vào các hệ thống thông tin tại Bộ đặc biệt là các hệ thống thông tin quan trọng, qua đó, giảm thiểu hậu quả và góp phần duy trì tính khả dụng của thông tin và sự hoạt động liên tục của hệ thống thông tin khi bị tấn công. Nâng cao năng lực phát hiện các hình thức tấn công mạng Internet; đáp ứng việc tuân thủ các quy định, chỉ thị của Chính phủ về giám sát an toàn thông tin (ATTT), đảm bảo ATTT theo mô hình 4 lớp và tăng cường khả năng theo dõi, giám sát trung tâm dữ liệu theo đúng Chỉ thị 14/CT-TTg ngày 07/6/2019 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. Qua đó, sẽ thực hiện thuê đơn vị thực hiện tại lớp thứ 2 của mô hình: "Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ".
- Giám sát, cảnh báo các cuộc tấn công, rà quét vào hệ thống ứng dụng, mạng, máy chủ của Bộ cho các hệ thống: Hệ thống thư điện tử, Hệ thống Quản lý văn bản, Hệ thống Quản lý người dùng Active directory và hệ thống tường lửa Bộ Công Thương.
- Giám sát, cảnh báo sớm các nguy cơ an ninh mạng, có biện pháp khắc phục, phòng ngừa, giảm thiểu rủi ro mất ATTT cho các hệ thống: Hệ thống thư điện tử, Hệ thống Quản lý văn bản, Hệ thống Quản lý người dùng Active directory và hệ thống tường lửa Bộ Công Thương.

3. Yêu cầu kỹ thuật

3.1. Phạm vi công việc: Thực hiện các công việc cho các hệ thống: Hệ thống thư điện tử, Hệ thống Quản lý văn bản, Hệ thống Quản lý người dùng Active directory và hệ thống tường lửa Bộ Công Thương.

- Khảo sát, cấu hình danh mục endpoint cần giám sát. Thiết lập cài đặt hệ thống giám sát.

- Trực vận hành, theo dõi, giám sát hệ thống, thu thập thông tin từ hệ thống giám sát trung tâm.

- Nghiên cứu phân tích log hệ điều hành, ứng dụng, phân tích các sự kiện, nhật ký có dấu hiệu nguy cơ mất an toàn mạng để phát hiện kịp thời các tấn công, sự cố, các điểm yếu, lỗ hổng bảo mật trong hệ thống được giám sát và các xu hướng tấn công, các khuyến nghị phòng ngừa để cảnh báo cho khách hàng.

- Cảnh báo, phối hợp xác minh, đề xuất cách thức khắc phục tấn công được phát hiện.

- Nghiên cứu, cập nhật, điều chỉnh hệ thống giám sát phù hợp điều kiện thực tế và kỹ thuật tấn công mới

+ Nghiên cứu, tối ưu hóa hệ thống giám sát trung tâm.

+ Phối hợp cập nhật thông tin thay đổi, nâng cấp tại điểm giám sát.

- Tổng hợp, hoàn thiện báo cáo định kỳ hàng tuần, tháng.

3.2. Yêu cầu cụ thể

3.2.1. Yêu cầu về kỹ thuật, công nghệ với giải pháp giám sát lớp mạng

Phương án giám sát lớp mạng phải đảm bảo thực hiện các yêu cầu:

- Hỗ trợ phân tích lưu lượng mạng tối thiểu 5Gbps và hỗ trợ nhiều cổng giám sát để đảm bảo giám sát được toàn bộ hệ thống mạng

- Hỗ trợ phân tích mạng theo mô hình phân tán, mỗi hệ thống có sensor phân tích riêng, được quản trị tập trung nhằm đảm bảo khả năng mở rộng của hệ thống

- Thường xuyên giám sát, phát hiện và cảnh báo sớm các hành vi, cụ thể:

+ 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) bằng cách giải mã giao thức, bóc tách dữ liệu dạng file, URL đưa vào các hệ thống phân tích tự động;

+ Các Shellcode, payload tấn công khai thác lỗ hổng 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…

3.2.2. Yêu cầu về kỹ thuật, công nghệ với giải pháp giám sát các máy chủ dịch vụ

Phương án giám sát các máy chủ dịch vụ phải đảm bảo thực hiện các yêu cầu:

- 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;

- Sự thay đổi trái phép của các tệp tin hệ thống;

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

3.2.3. Yêu cầu về kỹ thuật, công nghệ với giải pháp giám sát ứng dụng

Giải pháp giám sát lớp ứng dụng phải đảm bảo thực hiện các yêu cầu:

- Các dạng tấn công vào lớp ứng dụng phổ biến gồm SQLi, XSS...;

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

- Tấn công thay đổi giao diện;

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

- Tấn công từ chối dịch vụ.

- Có khả năng tích hợp log với các hệ thống SIEM để phục vụ việc giám sát tập trung

3.2.4. Yêu cầu về quy trình trình thực hiện:

Bước	**Mô tả công việc**	**Xử lý chính**

1	Thông tin cảnh báo: - Từ hệ thống giám sát ATTT - Từ email, điện thoại của các Phòng/Ban, nhân sự vận hành về sự cố ATTT Chuyển bước 2	Tier 1
2	Thực hiện xác minh thông tin cảnh báo: - Cảnh báo đúng: Chuyển bước 2a. Phân loại, đánh giá cấp độ sự cố - Cảnh báo sai: Cảnh báo nhầm nghiệp vụ quản trị, nghiệp vụ đơn vị, tác động có kế hoạch… Chuyển bước 2b. Cập nhật trạng thái ticket REJECT – False Positive.	Tier 1
2a	- Phân loại cấp độ sự cố, gồm 2 mức độ: Thông thường và Nghiêm trọng. - Dựa vào phân loại cấp độ sự cố ATTT và hướng dẫn xử lý, Tier 1 thực hiện 1 trong các lựa chọn sau: + Sự cố trong phạm vi do Tier 1 xử lý được: Chuyển bước 3a. + Sự cố do Tier 2 xử lý: Chuyển bước 3b. + Sự cố do Tier 3 xử lý: Trong trường hợp xác định cấp độ sự cố Nghiêm trọng. Chuyển bước 3c.	Tier 1
3a	Cập nhật thông tin xử lý ticket. Tier 1 thực hiện xử lý ticket sự cố theo hướng dẫn - Cập nhật trạng thái ticket CLEAR - Chuyển bước 14: Xác minh kết quả xử lý	Tier 1
3b	Tạo ticket sự cố cho Tier 2: - Trạng thái ticket ANALYSING - Gán ticket cho Tier 2. Chuyển bước 4 cho Tier 2 xác minh thông tin	Tier 1
3c	Tạo ticket sự cố cho Tier 3 xử lý Trong trường hợp Tier 1 xác định cấp độ sự cố là Nghiêm trọng. Tier 1 thực hiện: Tạo ticket sự cố cho Tier 3 xử lý. Chuyển bước 11	Tier 1

4	Xác minh thông tin của ticket sự cố: Thông tin ticket nhầm nghiệp vụ quản trị, nghiệp vụ đơn vị, tác động có kế hoạch… Cập nhật trạng thái ticket REJECT - False Positive (bước 2b). - Thông tin cảnh báo đúng: Chuyển bước 5	Tier 2
5	Xử lý ticket sự cố theo hướng dẫn: - Xử lý xong ticket sự cố: Tier 2 xử lý xong ticket sự cố theo hướng dẫn. Chuyển bước 5a. - Cần System Owner xử lý: Ticket sự cố cần System Owner xác minh thông tin nghiệp vụ. Chuyển bước 5b gán tiket cho System Owner. - Cần Tier 3 hỗ trợ: Ticket sự cố đã xử lý theo hướng dẫn nhưng không triệt để, cần Tier 3 hỗ trợ. Chuyển bước 5c tạo sub-ticket cho Tier 3.	Tier 2
5a	Cập nhật thông tin xử lý cho ticket: - Tier 2 thực hiện cập nhật các thông tin đã xử lý cho ticket. - Chuyển bước 14: Xác minh kết quả xử lý	Tier 2
5b	Gán ticket cho System Owner: Tier 2 gán ticket cho System Owner với các thông tin: - Thông tin cho System Owner cần xử lý - Trạng thái ticket là ANALYSING Chuyển bước 6.	Tier 2
5c	Tạo sub-ticket cho Tier 3: Tier 2 tạo sub-ticket cho Tier 3 khi cần hỗ trợ với các thông tin: - Các thông tin, hành động đã xử lý theo hướng dẫn. - Vấn đề cần Tier 3 hỗ trợ - Trạng thái sub-ticket là ANALYSING - Gán ticket cho nhóm Tier 3 Chuyển bước 8	Tier 2
6	Xử lý ticket theo hướng dẫn + System Owner xử lý ticket sự cố theo hướng dẫn. + Chuyển bước 7	System Owner

7	Cập nhật thông tin đã xử lý vào ticket: + Ticket gán sai cho nhóm vận hành System Owner. Cập nhật thông tin và trạng thái ticket là REJECT – Wrong Assignment, gán ticket cho Tier 2 xử lý tiếp. + System Owner xác minh thông tin trong ticket nhầm nghiệp vụ quản trị, nghiệp vụ đơn vị, tác động có kế hoạch… Cập nhật thông tin và trạng thái ticket là REJECT – False Positive, gán ticket cho Tier 2 nắm thông tin. + Xử lý thành công theo hướng dẫn. Cập nhật thông tin và trạng thái ticket là CLEAR. + Xử lý không thành công, cần hỗ trợ. Cập nhật thông tin cần hỗ trợ và gán ticket lại cho Tier 2. - Chuyển bước 4: Cho Tier 2 xác minh thông tin và xử lý tiếp	System Owner
8	Xử lý yêu cầu hỗ trợ trong sub-ticket: - Tier 3 hỗ trợ Tier 2, System Owner xử lý vấn đề đang gặp khó khăn trong quá trình xử lý ticket sự cố theo hướng dẫn. - Cập nhật đầy đủ thông tin xử lý vào sub-ticket - Chuyển bước 11	Tier 3
9	Cập nhật lại các tài liệu hướng dẫn: - Bổ sung thêm tài liệu hướng dẫn cho Tier 1, Tier 2, System Owner có thế xử lý được. - Chuyển bươc 10	Tier 3
10	Thông báo lại kết quả cho Tier 2: Chuyển bước 4 cho Tier 2 xác minh thông tin	Tier 3
11	Xử lý ticket sự cố: - Thực hiện các biện pháp nghiệp vụ điều tra nhanh, khắc phục sự cố kịp thời, đảm bảo các hoạt động CNTT. - Tier 2, System Owner hỗ trợ Tier 3 khi cần - Chuyển bước 12	Tier 3
12	Cập nhật ticket các thông tin về sự cố: - Thông tin điều tra - Thông tin việc khắc phục sự cố - Đề xuất, kiến nghị Chuyển bước 13	Tier 3

13	Báo cáo kết quả: Báo cáo kết quả tổng hợp quá trình xử lý sự cố cho cấp lãnh đạo Sở TTTT, đồng gửi Tier 2.	Tier 3
14	Xác minh kết quả xử lý: Thực hiện xác minh kết quả toàn bộ quá trình xử lý của ticket có trạng thái CLEAR, REJECT xem đã thực hiện đúng theo hướng dẫn, đã triệt để chưa: - Nếu đối tượng, thiết bị có cảnh báo phát sinh hoặc chưa đầy đủ theo hướng dẫn, kết quả xử lý chưa triệt để, thực hiện mở lại ticket với trạng thái ANALYSING, chuyển Tier 2 xử lý. (bước 4) - Nếu đối tượng, thiết bị không có cảnh báo phát sinh, quá trình xử lý đầy đủ theo hướng dẫn, thực hiện chuyển ticket từ trạng thái CLEAR sang CLOSE, đóng ticket.	Tier 1

3.2.5. Yêu cầu về đơn vị thực hiện:

- Nhà thầu thực hiện phải là tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc tổ chức được cấp có thẩm quyền cấp phép theo Nghị định số 108/20216/NĐ-CP ngày 01/7/2016 *(Nhà thầu cung cấp tài liệu chứng minh).*

3.2.6. Yêu cầu về nhân sự thực hiện:

- Chuyên gia trực vận hành hệ thống giám sát, số lượng 02 người: Tốt nghiệp Đại học đại học trở lên được đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư 08/2022/TT-BTTTT hoặc tương đương đối với các bằng tốt nghiệp tại nước ngoài. Có kinh nghiệm tương tự 03 năm hoặc 01 hợp đồng giám sát ATTT. Có chứng chỉ quốc tế cơ bản về an ninh mạng – ECSS *(Nhà thầu cung cấp các tài liệu chứng minh)*.

- Chuyên gia phân tích sự kiện, sự cố an toàn thông tin mạng chuyên sâu số lượng 01 người: Tốt nghiệp Đại học đại học trở lên được đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư 08/2022/TT-BTTTT hoặc tương đương đối với các bằng tốt nghiệp tại nước ngoài. Có kinh nghiệm tương tự 03 năm hoặc 01 hợp đồng về giám sát. Có đồng thời các chứng chỉ quốc tế về điều tra số - CHFI và kiểm thử xâm nhập hỗ trợ công tác phân tích điều tra – OSCP và OSEP *(Nhà thầu cung cấp các tài liệu chứng minh)*.

- Chuyên gia phân tích sự kiện, sự cố an toàn thông tin mạng cho ứng dụng số lượng 01 người: Tốt nghiệp Đại học đại học trở lên được đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư

08/2022/TT-BTTTT hoặc tương đương đối với các bằng tốt nghiệp tại nước ngoài. Có kinh nghiệm tương tự 03 năm hoặc 01 hợp đồng. Có chứng chỉ quốc tế về kiểm thử xâm nhập web hỗ trợ công tác phân tích điều tra – OSWA và OSWE *(Nhà thầu cung cấp các tài liệu chứng minh)*.

- Chuyên gia hỗ trợ ứng cứu sự cố, số lượng: 02 người: Tốt nghiệp Đại học đại học trở lên được đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư 08/2022/TT-BTTTT hoặc tương đương đối với các bằng tốt nghiệp tại nước ngoài. Có kinh nghiệm tương tự 03 năm hoặc 01 hợp đồng. Có chứng chỉ quốc tế về điều tra số - CHFI *(Nhà thầu cung cấp các tài liệu chứng minh).*

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị 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. Kế hoạch công tác.

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

Mục này quy định về quy trình kiểm tra, nghiệm thu sản phẩm, trình tự giao nộp sản phẩm (nếu có)... để phục vụ công tác thanh, quyết toán hợp đồng.