Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Giới thiệu chung về dự toán mua sắm, gói thầu:

1.1. Tên gói thầu: Thuê dịch vụ quản lý, giám sát, điều phối xử lý sự cố an ninh mạng và hỗ trợ quản lý vận hành hạ tầng CNTT của Ủy ban Chứng khoán Nhà nước giai đoạn 2026-2029

1.2. Chủ đầu tư: Ban Công nghệ và Chuyển đổi số - Ủy ban Chứng khoán Nhà nước.

1.3. Thời gian thực hiện

- Thời gian thực hiện việc cài đặt, tích hợp các giải pháp an toàn thông tin với hệ thống giám sát (thời gian thiết lập, xây dựng hệ thống/giải pháp): trong vòng 30 ngày.

- Thời gian cung cấp dịch vụ: 1095 ngày liên tục.

- Tổng thời gian thực hiện hợp đồng: 1125 ngày kể từ ngày hợp đồng có hiệu lực.

1.4. Nội dung, quy mô, phạm vi, địa điểm thuê dịch vụ CNTT

1.4.1. Nội dung thuê dịch vụ

Nhiệm vụ Thuê dịch vụ quản lý, giám sát, điều phối xử lý sự cố an ninh mạng và hỗ trợ quản lý vận hành hạ tầng CNTT của Ủy ban Chứng khoán Nhà nước giai đoạn 2026-2029 gồm các dịch vụ sau:

Stt	Nội dung chi tiết thuê dịch vụ CNTT	Đơn vị	Số lượng	Thời gian thực hiện
1	Dịch vụ quản lý, giám sát, điều phối xử lý sự cố an ninh mạng 24/7	Gói dịch vụ	01	1095 ngày liên tục
2	Dịch vụ hỗ trợ quản lý vận hành hạ tầng CNTT của UBCKNN	Gói dịch vụ	01	1095 ngày liên tục

1.4.2. Quy mô thuê dịch vụ

Thuê dịch vụ quản lý, giám sát, điều phối xử lý sự cố an ninh mạng và hỗ trợ quản lý vận hành hạ tầng CNTT của Ủy ban Chứng khoán Nhà nước bao gồm các nội dung sau:

1. Dịch vụ quản lý, giám sát, điều phối xử lý sự cố an ninh mạng 24/7

Triển khai dịch vụ giám sát, phát hiện, điều tra, cảnh báo và hỗ trợ xử lý các hiện tượng bất thường, mã độc, tấn công có chủ đích (Advanced Persisten Threat-APT) và các mối đe dọa, tấn công mạng khác trên hệ thống mạng nội bộ và toàn bộ hệ thống máy chủ, máy trạm của UBCKNN thông qua:

- Triển khai hệ thống giám sát an toàn thông tin mạng tập trung trên cơ sở tận dụng các giải pháp hiện có của UBCKNN để phù hợp với phạm vi giám sát và đáp ứng các yêu cầu đảm bảo an toàn thông tin cho hệ thống cấp độ 3 theo quy định của pháp luật nhà nước. Hệ thống giám sát của đơn vị cung cấp dịch vụ đáp ứng các yêu cầu:

+ Tích hợp thông tin sự kiện an ninh từ các thiết bị mạng, bảo mật, thiết bị quản trị và các máy chủ của UBCKNN vào hệ thống SIEM, đảm bảo việc lưu trữ các sự kiện đáp ứng theo các yêu cầu của UBCKNN và Bộ Tài chính; triển khai mô hình hoạt động giám sát an ninh mạng tập trung (Security Operation Center-SOC);

+ Triển khai bổ sung các thành phần hỗ trợ cho hệ thống giám sát an ninh mạng tập trung gồm thành phần: (1) Quản lý và phân tích sự kiện an toàn thông tin tập trung (SIEM – Ngoài hệ thống SIEM của UBCKNN (nếu có)) (2) Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR); (3) Cung cấp tri thức phòng ngừa mối đe dọa an toàn thông tin Threat Intelligence; (4) Giám sát, phát hiện và phản ứng với nguy cơ tấn công cho máy chủ, máy trạm; (5) Thu thập dữ liệu, phát hiện tấn công lớp mạng tại Core Switch của Địa điểm đặt hosting các hệ thống CNTT của UBCKNN và trụ sở UBCKNN

+ Triển khai đặt, cấu hình, tích hợp hệ thống giám sát an toàn thông tin mạng tập trung đáp ứng các yêu cầu đảm bảo an toàn thông tin cho hệ thống cấp độ 3.

+ Triển khai chia sẻ dữ liệu với Trung tâm giám sát an ninh mạng Quốc gia của Bộ Công an theo quy định.

- Triển khai nhân sự thực hiện quản trị, giám sát, điều phối xử lý sự cố an ninh mạng cho hệ thống công nghệ thông tin của Ủy ban Chứng khoán Nhà nước. Đội ngũ nhân sự (tối thiểu 08 nhân sự giám sát an ninh mạng mức 1; 03 nhân sự giám sát an ninh mạng mức 2; 02 nhân sự giám sát an ninh mạng mức 3 ; 01 nhân sự SOC manager) thực hiện các dịch vụ sau:

+ Dịch vụ quản trị vận hành các giải pháp an toàn thông tin 24/7

+ Dịch vụ theo dõi và cảnh báo các nguy cơ về an ninh mạng 24/7

+ Dịch vụ phân tích và phối hợp xử lý các cảnh báo về an ninh mạng 24/7

+ Dịch vụ săn tìm chủ động các mối đe dọa (Threat Hunting) và phân tích cảnh báo sớm các mối đe dọa an ninh mạng (Threat Intelligence)

+ Dịch vụ điều phối và xử lý sự cố về an ninh mạng

+ Dịch vụ điều tra và phân tích chuyên sâu các sự cố về an ninh mạng

+ Xây dựng quy trình vận hành hệ thống giám sát an toàn thông tin tập trung

+ Lập báo cáo giám sát an ninh mạng theo quy định của nhà nước về hoạt động giám sát an toàn hệ thống thông tin, bao gồm: Báo cáo ngày, Báo cáo tuần (báo cáo trực tiếp cho cán bộ chuyên trách của UBCKNN), Báo cáo hoạt động giám sát định kỳ theo tháng, quý, năm (báo cáo bằng văn bản theo quy định).

2. Triển khai Dịch vụ hỗ trợ quản lý vận hành hạ tầng CNTT của UBCKNN:

Thuê dịch vụ nhân sự hỗ trợ quản trị vận hành hạ tầng CNTT cho Ủy ban Chứng khoán Nhà nước. Đội ngũ nhân sự (tối thiểu 03 chuyên gia) thực hiện các dịch vụ sau:

- Hỗ trợ kỹ thuật, và quản trị vận hành các trang thiết bị phần cứng được nêu tại Tiểu mục 1.4 Mục 1 Chương V của E-HSMT liên tục 24/7.

- Hỗ trợ thực hiện sao lưu hàng ngày, khôi phục các máy chủ (sử dụng phần mềm Backup có sẵn tại UBCKNN như VEEAM/ Veritas/ Commvault/ Dell...(nếu có) hoặc cấu hình dịch vụ sao lưu, khôi phục ở mức hệ điều hành theo yêu cầu của Chủ đầu tư);

- Hỗ trợ khắc phục, xử lý sự cố liên quan đến máy chủ, thiết bị mạng được nêu tại Tiểu mục 1.4 Mục 1 Chương V của E-HSMT liên tục 24/7(không bao gồm dịch vụ hỗ trợ thay thế, sửa chữa các máy chủ bị hỏng hóc phát sinh (nếu có));

- Quản trị, vận hành hệ thống thư điện tử tại UBCKNN (Máy chủ hệ thống Mail Exchange Server, hệ thống Active Directory Server của UBCKNN) và kết nối dịch vụ thư điện tử public ra Internet và người dùng;

- Báo cáo công tác quản trị, vận hành và xử lý sự cố (nếu có) của hệ thống.

1.4.3. Phạm vi thuê dịch vụ

Triển khai dịch vụ giám sát, điều phối xử lý sự cố an ninh mạng và hỗ trợ quản trị vận hành hạ tầng CNTT của UBCKNN cho toàn bộ các máy chủ, thiết bị mạng bảo mật, ứng dụng và thiết bị đầu cuối bao gồm:

+ Các máy chủ vật lý và ảo hóa: tối thiểu 110 máy chủ.

+ Các thiết bị người dùng tại Trụ sở UBCKNN: tối thiểu 500 thiết bị.

+ Các thiết bị mạng (Switch, router...) và thiết bị bảo mật (firewall, IPS/IDS...) của UBCKNN: tối thiểu 50 thiết bị.

+ Các hệ thống thông tin kèm cơ sở dữ liệu hiện có của UBCKNN vào thời điểm ký kết hợp đồng.

+ Trong quá trình triển khai dịch vụ, số lượng máy chủ, thiết bị mạng và thiết bị bảo mật có thể thay đổi theo nhu cầu thực tế vận hành hệ thống. Trường hợp số lượng tăng hoặc giảm trong phạm vi không quá 10% so với quy mô nêu trên thì vẫn được coi là phù hợp với phạm vi cung cấp dịch vụ theo hợp đồng đã ký kết.

1.4.4. Địa điểm triển khai:

- Trụ sở Ủy Ban Chứng khoán Nhà nước – Số 164 Trần Quang Khải, Phường Hoàn Kiếm, Thành phố Hà Nội;

- Địa điểm đặt hosting các hệ thống CNTT của Ủy Ban Chứng khoán Nhà nước (Hiện nay là Công ty Cổ phần Truyền thông Quốc tế INCOM, tòa nhà IC, 82 Duy Tân, Cầu Giấy, Hà Nội).

Mục 2. Mục tiêu công việc

Thuê đơn vị chuyên nghiệp cung cấp dịch vụ giám sát, điều phối xử lý sự cố an ninh mạng 24/7 và hỗ trợ quản trị vận hành hạ tầng CNTT cho Ủy ban Chứng khoán Nhà nước nhằm đáp ứng các yêu cầu của (1) Luật An ninh mạng; (2) Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; (3) Các tiêu chuẩn quốc gia gồm: 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, TCVN 14423:2025 Yêu cầu đối với hệ thống thông tin quan trọng; (4) Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông (hiện nay là Bộ Khoa học và Công nghệ) quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ; (5) Quyết định số 1690/QĐ-TTg ngày 26/12/2023 của Thủ tướng Chính phủ về việc phê duyệt Đề án "Kiện toàn tổ chức bộ máy, nâng cao năng lực quản lý Nhà nước và thực thi pháp luật về chuyển đổi số từ Trung ương đến địa phương năm 2025, định hướng đến năm 2030; (6) Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; (7) Thực hiện Công điện số 33/CĐ-TTg ngày 07/4/2024 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn thông tin mạng; (8) Quyết định số 03/QĐ-TBATANMBTC ngày 21/01/2026 của Tiểu ban An toàn An ninh mạng của Bộ Tài chính về Kế hoạch bảo đảm an toàn, an ninh mạng tổng thể của Bộ Tài chính năm 2026, cụ thể như sau:

- Triển khai hệ thống giám sát an toàn thông tin mạng tập trung và thực hiện giám sát an toàn an ninh mạng, điều phối xử lý sự cố an ninh mạng cho hệ thống thông tin của UBCKNN (24 giờ/7 ngày)

- Hỗ trợ quản lý vận hành hạ tầng CNTT của UBCKNN (24 giờ/7 ngày) đảm bảo hệ thống vận hành liên tục, ổn định.

Mục 3. Yêu cầu kỹ thuật của gói thầu:

3.1. Yêu cầu chất lượng dịch vụ

3.1.1. Các tiêu chí về chức năng của hệ thống

- Hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung cần đáp ứng toàn bộ các yêu cầu theo các tiêu chí công nghệ và tiêu chí về chất lượng dịch vụ được quy định theo Quyết định số 1356/QĐ-BTTTT ngày 07/7/2022 của Bộ Thông tin và Truyền thông (hiện nay là Bộ Khoa học và Công nghệ) về Tiêu chí đánh giá giải pháp, dịch vụ Trung tâm giám sát điều hành an toàn, an ninh mạng (SOC). Các chức năng của hệ thống phải đảm bảo hoạt động ổn định và đem lại hiệu quả trong việc giám sát an toàn thông tin, đáp ứng yêu cầu về chất lượng dịch vụ. Hệ thống cần có đầy đủ các hệ thống/cấu phần bao gồm: hệ thống/cấu phần Quản lý và phân tích sự kiện an toàn thông tin tập trung (SIEM-có tích hợp với hệ thống SIEM hiện có của UBCKNN), hệ thống/cấu phần Phòng chống xâm nhập lớp mạng (NIPS), hệ thống/cấu phần phòng chống mã độc (Anti-Virus), Hệ thống/cấu phần phát hiện và phản ứng sự cố an toàn thông tin trên endpoint (EDR), Hệ thống/cấu phần tường lửa ứng dụng web (WAF), Hệ thống/cấu phần Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR), Hệ thống/cấu phần tri thức mối đe dọa an toàn thông tin (Threat Intelligence). '

- Các quy trình giám sát, điều phối xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT cần được lập trước các biểu mẫu và thống nhất với chủ quản hệ thống thông tin trước khi đưa vào triển khai. Quy trình cần phù hợp với Quyết định số 2405/QĐ-BTC ngày 08/7/2025 của Bộ trưởng Bộ Tài chính ban hành Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính;

- Hoạt động giám sát, điều phối xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT phải được thực hiện phù hợp với các quy định của pháp luật chuyên ngành có liên quan.

3.1.2. Đáp ứng về hiệu năng vận hành:

- Hiệu năng của hệ thống phải đáp ứng các yêu cầu kỹ thuật, công nghệ và đáp ứng được theo phạm vi, quy mô giám sát, điều phối xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT được nêu tại Tiểu mục 1.4 Mục 1 Chương V của E-HSMT.

- Các dịch vụ và giải pháp cung cấp bổ sung (nếu có) phải được tài liệu hóa để chứng minh khả năng triển khai dịch vụ ở mức độ tốt, phù hợp với mong muốn của người dùng, đúng cấu hình yêu cầu và không gây ra chi phí phát sinh không cần thiết. Hiệu năng của hệ thống cần soát xét, truy vấn được và phù hợp với kiến trúc kỹ thuật của hệ thống CNTT của UBCKNN.

- Khả năng mở rộng của dịch vụ: Hệ thống của Nhà thầu có khả năng mở rộng quy mô giám sát, điều phối, xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT theo yêu cầu của Chủ đầu tư trong suốt quá trình, thời gian thuê dịch vụ. Nhà thầu cung cấp dịch vụ phải thực hiện kết nối các hệ thống CNTT mà chủ trì thuê dịch vụ yêu cầu mà không phát sinh thêm kinh phí thực hiện.

3.1.3. Đáp ứng các tiêu chí về an toàn thông tin mạng, an toàn dữ liệu

- Hệ thống giám sát an toàn an ninh mạng phải được đặt trong VLAN riêng của hệ thống CNTT nhằm phục vụ hoạt động giám sát.

- Hệ thống giám sát an toàn an ninh mạng phải được thiết lập, cấu hình đáp ứng cấp độ 3 theo quy định tại mục 2.2 Phụ lục III Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) 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; Các tiêu chuẩn quốc gia gồm: 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, TCVN 14423:2025 Yêu cầu đối với hệ thống thông tin quan trọng.

- Việc thu thập, lưu trữ, xử lý, khai thác và chia sẻ dữ liệu giám sát phải tuân thủ quy định của Luật An ninh mạng và Nghị định số 13/2023/NĐ-CP; bảo đảm dữ liệu được quản lý tập trung, bảo mật, kiểm soát truy cập và phục vụ công tác quản lý nhà nước theo quy định.

- Dữ liệu của hệ thống giám sát chỉ được lưu trữ trong phạm vi hệ thống và cung cấp cho các cơ quan quản lý theo quy định. Nhà thầu cung cấp dịch vụ giám sát không được lấy dữ liệu ra khỏi hệ thống để phục vụ cho các hoạt động khác ngoài các hoạt động thuộc phạm vi dịch vụ cung cấp.

- Dữ liệu giám sát phải được sao lưu và sẵn sàng khôi phục nếu có sự cố.

- Có quy chế vào ra phòng giám sát tại trụ sở của đơn vị cung cấp dịch vụ.

3.1.4. Các tiêu chí phi chức năng của hệ thống

3.1.4.1. Đáp ứng các tiêu chí về độ tin cậy và khả dụng:

- Hệ thống giám sát, điều phối xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT cần được vận hành đáp ứng theo các tiêu chuẩn về vận hành tương tự Trung tâm dữ liệu, đảm bảo hệ thống hoạt động 24/7.

- Hệ thống giám sát, điều phối xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT phải được thực hiện nhằm đáp ứng mô hình an toàn thông tin cấp độ 3 tại Thông tư số 12/2022/TT-BTTTT của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) ban hành ngày 12/08/2022 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.

- Hoạt động giám sát, điều phối xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT phải được đáp ứng theo Công văn số 2973/BTTTT-CATTT ban hành ngày 04/9/2019 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước; Công văn số 2596/BTTTT-CATTT ban hành ngày 02/07/2024 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) về việc Hướng dẫn bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý cấp bộ, tỉnh và có các tiêu chí cụ thể đánh giá.

3.1.4.2. Đáp ứng các tiêu chí về khả năng tích hợp, kết nối, liên thông của hệ thống

- Hệ thống phải tuân thủ các tiêu chuẩn kỹ thuật, quy chuẩn hiện hành về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

- Hệ thống phải bảo đảm sự tương thích về nền tảng công nghệ, phù hợp với hiện trạng ứng dụng công nghệ thông tin của UBCKNN;

- Hệ thống cần cho phép tùy chỉnh các chính sách giám sát, ngưỡng cảnh báo và báo cáo phù hợp với nhu cầu cụ thể của UBCKNN;

- Hệ thống giám sát an toàn, an ninh mạng tập trung phải triển khai đồng bộ, áp dụng các công nghệ mới và có khả năng mở rộng trong tương lai, trong đó:

+ Đối với các phần mềm nhà thầu đề xuất sử dụng để cung cấp dịch vụ: là các phần mềm phiên bản mới nhất, có bản quyền hợp pháp, có khả năng mở rộng; bảo đảm kết nối an toàn và tránh xung đột với các phần mềm hiện có của UBCKNN; bảo đảm khi triển khai hệ thống giám sát an toàn, an ninh mạng thì các hệ thống khác vẫn hoạt động bình thường. Nhà thầu phải cung cấp kèm theo E-HSDT văn bản xác nhận của hãng sản xuất (hoặc đại diện hợp pháp của hãng sản xuất tại Việt Nam) xác nhận về tính hiệu lực của phần mềm hoặc Nhà thầu phải có cam kết đáp ứng nội dung này trong E-HSDT là sẽ thực hiện cung cấp văn bản xác nhận của hãng sản xuất (hoặc đại diện hợp pháp của hãng sản xuất tại Việt Nam) xác nhận về tính hiệu lực của phần mềm cho Chủ đầu tư trong quá trình đối chiếu tài liệu (nếu được mời đối chiếu tài liệu) với tối thiểu các nội dung sau: Phần mềm cung cấp cho gói thầu đang trong thời gian hãng sản xuất cho phép bán ra thị trường, chưa có kế hoạch ngừng bán hàng (end of sale), hãng sản xuất cam kết đảm bảo dịch vụ hỗ trợ kỹ thuật trong thời gian triển khai dịch vụ.

3.1.4.3. Đáp ứng các tiêu chí về khả năng nâng cấp, mở rộng của hệ thống

- Hệ thống có khả năng mở rộng quy mô giám sát theo yêu cầu của Chủ đầu tư trong suốt quá trình, thời gian thuê dịch vụ. Nhà thầu cung cấp dịch vụ phải thực hiện kết nối với các hệ thống CNTT mà Chủ đầu tư yêu cầu mà không phát sinh thêm kinh phí thực hiện.

- Hệ thống được cập nhật hoặc cải tiến các thành phần phần mềm và phần cứng mà không làm gián đoạn hoạt động hoặc ảnh hưởng đến dữ liệu hiện tại. Cho phép hệ thống tăng hoặc giảm quy mô để đáp ứng khối lượng công việc hoặc nhu cầu giám sát mà không ảnh hưởng đến hạ tầng CNTT hiện có UBCKNN;

- Nhà thầu cung cấp dịch vụ phải có phương án triển khai đảm bảo hợp lý, hiệu quả không gây ảnh hưởng đến việc hoạt động thường xuyên của chủ quản hệ thống.

- Đảm bảo hệ thống hoạt động 24/7 và khắc phục các sự cố (nếu có).

3.1.4.4. Đáp ứng các tiêu chí về khả năng bảo trì, quản trị, vận hành

- Kiến trúc triển khai module hóa giúp dễ dàng sửa chữa hoặc thay thế từng thành phần mà không làm ảnh hưởng đến toàn bộ hệ thống.

- Có cơ chế tự động phát hiện lỗi, ghi nhật ký sự cố (log) chi tiết và cung cấp cảnh báo kịp thời;

- Cung cấp hướng dẫn chi tiết về bảo trì, từ việc nâng cấp phần mềm, thay thế phần cứng đến quản lý sự cố;

- Dashboard hiển thị trạng thái hệ thống theo thời gian thực, dễ dàng theo dõi thông tin về hiệu suất và các sự kiện bất thường;

- Hệ thống cho phép quản trị tất cả các thành phần từ một điểm duy nhất (Centralized Management);

- Phân quyền chi tiết cho các vai trò khác nhau (quản trị viên, nhân viên giám sát, chuyên gia phân tích) để đảm bảo chỉ những người được ủy quyền mới có quyền truy cập dữ liệu nhạy cảm;

- Hệ thống có khả năng tạo báo cáo chi tiết theo yêu cầu, giúp đánh giá tình hình bảo mật và hỗ trợ ra quyết định nhanh chóng;

- Hệ thống cần duy trì giám sát và phản ứng 24/7 kịp thời với các mối đe dọa mà không bị gián đoạn;

- Hỗ trợ tích hợp với các công cụ SIEM, IPS, Firewall, AV, EDR, PAM và các hệ thống an toàn thông tin khác của UBCKNN;

- Nhà thầu cung cấp dịch vụ phải đảm bảo nguồn nhân lực CNTT để duy trì, theo dõi, giám sát và khắc phục sự cố ATTT (nếu có) trong suốt thời gian cung cấp dịch vụ giám sát ATTT. Đồng thời có trách nhiệm chuyển giao đầy đủ thông tin, cơ sở dữ liệu phục vụ công tác giám sát an ninh thông tin hệ thống CNTT sau khi kết thúc hợp đồng để bảo đảm đơn vị Chủ quản vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả khi thay đổi Nhà thầu cung cấp dịch vụ;

- Nhà thầu cung cấp dịch vụ phải có "Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng " trong đó có nội dung "Cung cấp dịch vụ giám sát an toàn thông tin mạng" do Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) cấp còn hiệu lực trong thời gian thực hiện dịch vụ để đảm bảo khả năng cung cấp dịch vụ liên tục trong thời gian hợp đồng có hiệu lực; và có chứng nhận ISO/IEC 27001:2022 về "Cung cấp giải pháp, dịch vụ về an ninh mạng, an toàn thông tin" còn hiệu lực trong thời gian thực hiện dịch vụ.

- Nhà thầu cung cấp dịch vụ có cam kết bảo đảm an toàn, bảo mật và tính riêng tư về thông tin, dữ liệu của cơ quan nhà nước; tuân thủ quy định của pháp luật về an toàn, an ninh thông tin, cơ yếu và Luật Bảo vệ bí mật nhà nước số 117/2025/QH15 ban hành ngày 10/12/2025. Máy chủ lưu trữ thông tin, dữ liệu của cơ quan nhà nước phải được đặt trên lãnh thổ Việt Nam.

- Nhà thầu cung cấp dịch vụ cam kết trách nhiệm đào tạo, hướng dẫn sử dụng, chuyển giao công nghệ cho đội ngũ chuyên trách về an toàn thông tin của UBCKNN để từng bước nâng cao trình độ năng lực, có thể vận hành hệ thống đảm bảo toàn bộ hệ thống thông tin của UBCKNN hoạt động ổn định thông suốt.

3.1.5. Tiêu chí về sự hài lòng của người sử dụng

Nhà thầu phải định kỳ (Tối thiểu 6 tháng/lần) thực hiện khảo sát đánh giá về các sản phẩm, dịch vụ đối với người sử dụng sử dụng (Nhân sự quản lý hạ tầng và an toàn an ninh mạng của UBCKNN và một số cán bộ quản trị hệ thống thông tin của UBCKNN) đối với dịch vụ giám sát, điều phối xử lý sự cố an ninh mạng và quản trị vận hành hạ tầng CNTT.

3.1.6. Tiêu chí về quản lý dịch vụ.

3.1.6.1 Tiêu chí chung để quản lý dịch vụ

- Giám sát, hỗ trợ xử lý sự cố ATTT liên quan đến việc tấn công, xâm nhập, khai thác lỗ hổng, vi phạm tuân thủ về chính sách ATTT đối với hệ thống của UBCKNN liên tục 24/7.

- Hỗ trợ kỹ thuật, và xử lý sự cố các trang thiết bị được nêu tại Tiểu mục 1.4 Mục 1 Chương V của E-HSMT liên tục 24/7.

- Có quy trình xử lý sự cố nhằm phối hợp giữa Ban CĐS – UBCKNN và nhà cung cấp dịch vụ.

- Nhà thầu phải có bản mô tả, đề xuất quy trình phối hợp, kênh liên lạc trong trường hợp xử lý sự cố khẩn cấp.

- Có chuyên gia xử lý sự cố onsite trong vòng 01 giờ đối với các sự cố tấn công có mức độ ảnh hưởng nghiêm trọng hoặc khi có yêu cầu, xử lý trực tiếp tại UBCKNN đối với các sự cố mới chưa có hướng dẫn hoặc phức tạp.

- Thực hiện báo chi tiết đầy đủ thông tin về sự cố, nguyên nhân, phạm vi và ảnh hưởng của cuộc tấn công, cũng như các kết quả phân tích chuyên sâu.

- Định kỳ hàng tháng, nhà cung cấp gửi báo cáo giám sát, quản lý, vận hành hệ thống xử lý sự cố trong tháng.

- Định kỳ 3 tháng thực hiện tìm kiếm chủ động (threat-hunting) trên hệ thống SIEM để phát hiện các nguy cơ mất ATTT có thể xảy ra với hệ thống của UBCKNN

- Định kỳ 6 tháng thực hiện lập Báo cáo dịch vụ tổng thể, đánh giá các quá trình thực hiện, điều chỉnh và cải thiện chất lượng.

3.1.6.2 Tiêu chí quản lý chất lượng dịch vụ giám sát, điều phối xử lý sự cố an ninh mạng như sau:

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
A	**Dịch vụ giám sát an toàn thông tin**			
I	**Theo dõi và cảnh báo an toàn thông tin (hoạt động 24/7)**			
1	Theo dõi cảnh báo trên màn hình giám sát; kiểm tra và phân loại cảnh báo; tạo ticket và gán yêu cầu xử lý	R	I	Tính từ thời điểm cảnh báo ghi nhận được trên hệ thống đến khi chuyển cho Tier 2 hoặc chuyển sang trạng thái cảnh báo sai (fault positive): + Nghiêm trọng: ≤ 30 phút + Thông thường: ≤ 01h Tỉ lệ xử lý đúng hạn ≥ 90%

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
2	Số lượng sự cố xảy ra mà hệ thống không phát hiện, cảnh báo được trong quý	R	I	- Số sự cố không có cảnh báo: <= 1
II	**Phân tích cảnh báo và hướng dẫn xử lý sự cố thông thường (hoạt động 24/7)**			
1	Phân tích, xác định các hành động xử lý	R	I, S	Tính từ thời điểm tiếp nhận cảnh báo từ Tier 1 đến khi đưa ra kết quả và hành động: - Thực hiện gửi thông tin cảnh báo để UBCKNN xác nhận hành vi trong cảnh báo: ≤ 01h - Thực hiện đóng cảnh báo (đối với cảnh báo Fault Positive): ≤ 01h - Thông báo cho UBCKNN và chuyển sang Quy trình cảnh báo đối sự cố: + Nghiêm trọng: ≤ 30 phút + Thông thường: ≤ 01h

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
				Tỉ lệ xử lý đúng hạn ≥ 90%
2	Hướng dẫn xử lý ứng cứu, ngăn chặn khi có dấu hiệu sự cố	R	I, S	Tính từ thời điểm sự cố được xác định đến khi UBCKNN nhận được phương án xử lý, ngăn chặn: ≤ 4h + Sự cố xử lý không đúng hạn ≤ 02 sự cố/ tháng
3	Thực hiện các hành động theo quy trình nhằm ngăn chặn nhanh chóng các sự cố	S	R	Tính từ thời điểm đưa ra được phương án xử lý, ngăn chặn đến khi thực hiện tác động hệ thống ≤ 72h - Sự cố xử lý không đúng hạn ≤ 02 sự cố/ tháng
4	Phân tích nguồn gốc, nguyên nhân để xác định phương án, thiết lập các tập luật khắc phục không bị lặp lại	R	S	Tính từ thời điểm sự cố được xác định đến khi có kết quả phân tích và báo cáo về sự cố. + Thực hiện điều tra sự cố trên hệ thống SIEM hoặc UBCKNN hỗ trợ truy cập trực tiếp vào hệ thống để trực tiếp rà

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
				soát máy chủ bị ảnh hưởng (trong quá trình điều tra có thay đổi, mở rộng phạm vi sự cố). + Thực hiện lập báo cáo tổng quan về sự cố, khuyến nghị khắc phục. *Thời gian điều tra và phân tích sự cố* được mô tả chi tiết bên dưới.
5	Báo cáo sự cố và đề xuất, khuyến nghị, khắc phục nhằm hạn chế, giảm thiểu rủi ro có thể gặp phải trong tương lai.	R	I	Tính từ thời điểm khắc phục xong sự cố đến khi hoàn thành báo cáo: ≤ 21 ngày Tỉ lệ xử lý không đúng hạn ≤ 01 sự cố
III	**Tối ưu, chuẩn hóa hệ thống**			
1	Thực hiện tối ưu hoạt động hệ thống SIEM của Nhà thầu (nếu có), SOAR, logsource (Nguồn lấy log), content analysis (Phân tích nội dung), alert analys (Phân tích cảnh báo), rule (tập luật)	R	I, A	- Định kỳ: 1 tháng/lần - Theo yêu cầu: ≤ 6 ngày - Tỉ lệ xử lý đúng hạn ≥ 90%

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
2	Thực hiện whitelist, chỉnh sửa luật để loại bỏ cảnh báo sai (fault positive), nhận diện nhầm	R	I, S	Tính từ thời điểm được xác định là cảnh báo sai đến khi hoàn thành cấu hình whitelist - Thời gian ≤ 24h - Tỉ lệ xử lý đúng hạn ≥ 90%
IV	**Tìm kiếm nguy cơ mất an toàn thông tin (Threat Hunting)**			
1	Thực hiện rà soát, phát hiện các nguy cơ mất an toàn thông tin từ log thu thập được trên SIEM	R	I	- Tần suất thực hiện: hàng ngày.
2	Phân tích để cập nhật chính sách trên các giải pháp được triển khai	R	I	Tính từ thời điểm được phát hiện nguy cơ (hoặc theo yêu cầu) đến khi có báo cáo phân tích. - Thời gian ≤ 7 ngày - Tỉ lệ xử lý đúng hạn ≥ 90%
V	**Quản lý, điều hành giám sát**			

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
1	Báo cáo việc theo dõi, giám sát, phân tích cảnh báo và xử lý sự cố thông thường	R	I	Báo cáo tháng: 1 tháng/lần Báo cáo quý: 3 tháng/lần Báo cáo năm: 12 tháng/lần Tỷ lệ gửi báo cáo đúng hạn ≥ 90% (Tính trên thời gian quy định tại hợp đồng)
2	Báo cáo việc tối ưu, chuẩn hóa hệ thống	R	I	Báo cáo tháng: 1 tháng/lần Báo cáo quý: 3 tháng/lần Báo cáo năm: 12 tháng/lần Tỷ lệ gửi báo cáo đúng hạn ≥ 90% (Tính trên thời gian quy định tại hợp đồng)
3	Báo cáo việc tìm kiếm nguy cơ mất an toàn thông tin (Threat Hunting)	R	I	- Báo cáo tháng: 1 tháng/ lần - Báo cáo quý: 3 tháng/lần - Báo cáo năm: 12 tháng/lần

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
				Tỷ lệ gửi báo cáo đúng hạn ≥ 90% (Tính trên thời gian quy định tại hợp đồng)
4	Báo cáo về nguy cơ, đe dọa an toàn thông tin (Threat Intelligence Platform - TIP)	R	I	- Báo cáo tháng: 1 tháng/lần - Báo cáo quý: 3 tháng/lần - Báo cáo năm: 12 tháng/lần Tỷ lệ gửi báo cáo đúng hạn ≥ 90% (Tính trên thời gian quy định tại hợp đồng)
5	Báo cáo phát hiện và phản ứng sự cố an toàn thông tin trên máy chủ			- Báo cáo tháng: 1 tháng/lần - Báo cáo quý: 3 tháng/lần - Báo cáo năm: 12 tháng/lần Tỷ lệ gửi báo cáo đúng hạn ≥ 90% (Tính trên thời gian quy định tại hợp đồng)

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
6	Báo cáo, đánh giá các công tác hoạt động của SOC	R	I	- Báo cáo tháng: 1 tháng / lần - Báo cáo quý: 3 tháng/lần - Báo cáo năm: 12 tháng/lần Tỷ lệ gửi báo cáo đúng hạn ≥ 90% (Tính trên thời gian quy định tại hợp đồng)
7	Đảm bảo chất lượng dịch vụ trong việc giám sát và xử lý các cảnh báo, sự cố	R	I	Số sự cố thông thường không phát hiện được ≤ 1 sự cố/ tháng Số sự cố nghiêm trọng không phát hiện được ≤ 0 sự cố Số sự cố không xử lý được ≤ 0 sự cố - Số sự cố xử lý không đúng hạn ≤ 02 sự cố trong tháng
VI	**Cung cấp thông tin nguy cơ, đe dọa an toàn thông tin (Threat Intelligence Platform - TIP)**			

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
1	Thực hiện cung cấp thông tin và phân tích nguy cơ, đe dọa an toàn thông tin ảnh hưởng đến hệ thống của UBCKNN (lỗ hổng bảo mật, các cuộc tấn công APT mức độ Nghiêm trọng/Cao, các mẫu mã độc mới, các hành vi mới của các tác nhân đe dọa...)	R	I	- Thực hiện: hàng ngày
VII	**Phát hiện và phản ứng sự cố an toàn thông tin trên máy chủ**			
1	Thực hiện cung cấp thông tin và phân tích phát hiện, phản ứng sự cố an toàn thông tin trên máy chủ			- Thực hiện: hàng ngày
B	**Dịch vụ điều phối xử lý sự cố nghiêm trọng**			

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
1	Thực hiện xử lý các sự cố mới, phức tạp, nghiêm trọng	R	S	- Thời gian xử lý ≤ 2h từ thời điểm ghi nhận sự cố xuất hiện đến khi UBCKNN nhận được phương án phương án ngăn chặn sự cố khẩn cấp từ đơn vị cung cấp dịch vụ. - 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 khẩn cấp thời cho hệ thống của khách hàng. - Số lượng sự cố xử lý không đúng hạn ≤ 0 sự cố
2	Thực hiện bóc gỡ mã độc	I, S	R, A	- Tính từ thời điểm đưa ra được phương án xử lý đến khi thực hiện các tác động xử lý: ≤ 24h - Số lượng sự cố xử lý không đúng hạn ≤ 0 sự cố

STT	Nội dung	ĐV Giám sát	UBCKNN	KPI áp dụng cho với đơn vị giám sát
3	Thực hiện điều tra sự cố, phân tích chuyên sâu	R	S	Tính từ thời điểm sự cố được xác định đến khi có kết quả điều tra, phân tích và báo cáo về sự cố. + Thực hiện điều tra sự cố trên hệ thống SIEM của Nhà thầu (nếu có) hoặc UBCKNN hỗ trợ truy cập trực tiếp vào hệ thống để trực tiếp rà soát máy chủ bị ảnh hưởng (trong quá trình điều tra có thay đổi, mở rộng phạm vi sự cố). + Thực hiện lập báo cáo tổng quan về sự cố, khuyến nghị khắc phục. *Thời gian điều tra và phân tích sự cố* được mô tả chi tiết bên dưới.
4	Báo cáo sự cố và đề xuất, khuyến nghị, khắc phục nhằm hạn chế, giảm thiểu rủi ro có thể gặp phải trong tương lai.	R	I	Tính từ thời điểm khắc phục xong sự cố đến khi hoàn thành báo cáo: ≤ 7 ngày Tỉ lệ xử lý không đúng hạn ≤ 01 sự cố

Trong đó:

- ✓ 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

❖ **Phân loại mức độ nghiêm trọng của cảnh báo**

Phân loại mức độ cảnh báo ATTT: Được chia thành 2 loại NGHIÊM TRỌNG & THÔNG THƯỜNG tùy theo 'Mức độ ảnh hưởng' và 'Khả năng tấn công thành công'

Mức độ ưu tiên

Mục đích của việc phân chia mức độ ưu tiên là để: phân loại cảnh báo ATTT từ đó xác định thời gian cam kết xử lý tương ứng.

Có các mức độ ưu tiên được xác định theo bảng sau:

MA TRẬN THIẾT LẬP GIÁ TRỊ ƯU TIÊN CỦA CẢNH BÁO			
Mức độ cảnh báo = Mức độ ảnh hưởng X Khả năng tấn công thành công		**Khả năng tấn công thành công**	
		Cao (1)	**Trung bình (2)**
Mức độ ảnh hưởng	**Nghiêm trọng (1)**	1	2
	Cao (2)	2	4
	Trung bình (3)	3	6
	Thấp (4)	4	8

Dựa trên bảng ưu tiên như trên, cảnh báo ATTT sẽ được phân loại thành 02 loại:

- Cảnh báo NGHIÊM TRỌNG: là cảnh bảo có mức 1, 2.
- Cảnh báo THÔNG THƯỜNG: là cảnh báo có mức 3, 4, 6, 8

Mức độ ảnh hưởng

Mức độ ảnh hưởng của cảnh báo sử dụng để đánh giá phạm vi ảnh hưởng, tính chất nghiêm trọng của cảnh báo. Mức độ ảnh hưởng của một cảnh báo ATTT được phân làm 04 (bốn) mức sau:

Mức độ ảnh hưởng	**Điều kiện phân loại mức độ ảnh hưởng**
Nghiêm trọng	Cảnh báo ATTT phát sinh từ hệ thống ứng dụng phục vụ người dân, doanh nghiệp được public ra internet: ví dụ như các cấu phần sau: Cổng dịch vụ công trực tuyến, Cổng thông tin điện tử, Công bố thông tin,..
Cao	Cảnh báo ATTT phát sinh từ các ứng dụng nghiệp vụ: ví dụ như Giám sát giao dịch trên thị trường chứng khoán, CSDL Quản lý các đối tượng như: Công ty Chứng khoán, Công ty quản lý quỹ và quỹ đầu tư chứng khoán, Nhà đầu tư nước ngoài, thư điện tử công vụ….
Trung bình	Cảnh báo ATTT phát sinh từ hệ thống cung cấp các ứng dụng phục vụ nội bộ: ví dụ CSDL Phục vụ công tác thống kê nội bộ; cấu phần Quản lý Văn bản và Điều hành; cấu phần kết nối trao đổi thông tin giữa UBCK và Cục thuế và các đơn vị khác,…
Thấp	Cảnh báo ATTT phát sinh từ máy tính người dùng của UBCKNN

<u>Khả năng tấn công thành công</u>

Khả năng tấn công thành công	**Điều kiện phân loại khả năng tấn công thành công**
Cao	Cảnh báo ATTT phát sinh từ các luật (rule) phát hiện tấn công sau: - Phát hiện các tấn công thông qua dấu hiệu IOC (Indicator Of Compromise) trên tất cả các giải pháp ATTT

Khả năng tấn công thành công	Điều kiện phân loại khả năng tấn công thành công
	- Phát hiện các hành vi bất thường trên máy chủ, máy trạm mức cao.
Trung bình	Cảnh báo ATTT phát sinh từ các luật (rule) còn lại, bao gồm: - Phát hiện các hành vi bất thường khác mức Cao - Phát hiện thay đổi tài nguyên quan trọng trên máy chủ (User, File trong thư mục Website, Port, Service,...)

❖ **Phân loại mức độ nghiêm trọng của sự cố**

- **Sự cố nghiêm trọng được định nghĩa** là các cảnh báo về an ninh mạng xảy ra trên hệ thống thông tin tại UBCKNN, sau khi được bộ phận giám sát phân tích và đánh giá mức độ ảnh hưởng rơi vào một trong các trường hợp sau:

+ Đánh giá có thể làm hệ thống bị gián đoạn dịch vụ;

+ Đánh giá ảnh hưởng đến các dữ liệu trên hệ thống là bảo mật hoặc tuyệt mật;

+ Đánh giá ảnh hưởng đến các dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được;

+ Đánh giá có thể làm hệ thống bị mất quyền điều khiển;

+ Đánh giá sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin khác.

- Sự cố thông thường được định nghĩa là những sự cố không phải sự cố nghiêm trọng.

+ Phân loại mức độ nghiêm trọng của sự cố theo các tiêu chí sau:

Số lượng máy chủ/máy tính bị ảnh hưởng	**Khả năng truy cập**	**Biện pháp phòng thủ**	**Mức độ ảnh hưởng**	**Lộ lọt dữ liệu**
Mức độ 1: Nhỏ (1 máy)	Người dùng không có quyền truy cập đến các thông tin đặc quyền, các truy cập được giám sát chặt chẽ	Các biện pháp bảo vệ và phát hiện hoạt động hiệu quả	Dữ liệu hoặc hệ thống quan trọng sẽ không bị ảnh hưởng	Không có khả năng lộ lọt dữ liệu
Mức độ 2: Trung Bình (<10 máy)	Người dùng không có quyền truy cập đến các thông tin đặc quyền, nhưng các truy cập không được giám sát chặt chẽ	Các biện pháp bảo vệ hoạt động hiệu quả, các biện pháp phát hiện không hiệu quả	Dữ liệu hoặc hệ thống quan trọng có thể bị ảnh hưởng	Có khả năng lộ lọt dữ liệu
Mức độ 3: Lớn (từ 10 đến 20 máy)	Người dùng có quyền truy cập đến các thông tin đặc quyền, các truy cập được giám sát	Các biện pháp bảo vệ hoạt động không hiệu quả, các biện pháp phát hiện có hiệu quả	Dữ liệu hoặc hệ thống quan trọng sẽ bị ảnh hưởng	Có khả năng cao lộ lọt dữ liệu

Số lượng máy chủ/máy tính bị ảnh hưởng	Khả năng truy cập	Biện pháp phòng thủ	Mức độ ảnh hưởng	Lộ lọt dữ liệu
Mức độ 4: Rất lớn (>20 máy)	Người dùng có quyền truy cập đến các thông tin đặc quyền, các truy cập không được giám sát	Các biện pháp bảo vệ và phát hiện hoạt động không hiệu quả	Dữ liệu hoặc hệ thống quan trọng đã bị ảnh hưởng	Dữ liệu đã bị lộ lọt và đang tiếp tục
(0-3)	(0-3)	(0-3)	(0-3)	(0-3)

+ Phạm vi bị ảnh hưởng được xác định như sau:

Phạm vi	Mô tả
Nhỏ	01 máy chủ/máy tính
Trung bình	< 10 máy chủ/máy tính
Lớn	Từ 10 đến 20 máy chủ/máy tính
Rất lớn	> 20 máy chủ/máy tính

Mỗi tiêu chí sẽ có 4 mức điểm đánh giá từ 0 đến 3, Đơn vị cung cấp dịch vụ sẽ dựa vào sự cố và tính điểm trên từng tiêu chí. Tổng điểm của các tiêu chí sẽ quyết định mức độ nguy hiểm của sự cố như sau:

Mức độ nguy hiểm	Điểm
Nghiêm trọng	10-15
Thông thường	0-9

❖ **Thời gian điều tra và phân tích sự cố**

Thời gian trên được ước lượng theo thời gian trung bình của công việc xử lý sự cố thông thường. Đối với các sự cố đặc biệt phức tạp sẽ phụ thuộc theo tình hình thực tế

Thời gian Đơn vị cung cấp dịch vụ thực hiện quá trình phân tích và điều tra sự cố nhằm tìm ra nguyên nhân gốc và đưa ra các phương án, khuyến nghị để khắc phục các sự cố tương tự được xác định như sau:

Mức độ nghiêm trọng	**Phạm vi**	**Thời gian điều tra sự cố**
Nghiêm trọng	Nhỏ	3 ngày
	Trung bình	7 ngày
	Lớn	12 ngày
	Rất lớn	Phụ thuộc tình hình thực tế
Thông thường	Nhỏ	< 14 ngày
	Trung bình	
	Lớn	
	Rất lớn	Phụ thuộc tình hình thực tế

Thời gian điều tra sự cố: là thời gian từ khi đơn vị chủ quản gửi thông tin hỗ trợ điều tra sự cố cho Đơn vị cung cấp dịch vụ đến khi Đơn vị cung cấp dịch vụ 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.

3.1.7 Tiêu chí quản lý chất lượng dịch vụ quản trị, hỗ trợ kỹ thuật hệ thống CNTT

- Thời gian tiếp nhận và xử lý lỗi: 24/7 (24 giờ/ ngày, 7 ngày/ tuần).

- Xử lý CSR (Customer Service Request): Tất cả các CSR phải được xử lý theo tiến trình xử lý CSR, bao gồm các bước:

+ Đăng ký, tiếp nhận CSR: Khách hàng gửi email, gọi điện để yêu cầu dịch vụ hỗ trợ.

+ Cập nhật CSR - Xác định mức độ nghiêm trọng của CSR.

+ Phân tích CSR.

+ Trả lời CSR bao gồm cả các hoạt động đề xuất.

+ Thời gian phản hồi các CSR các mức theo quy định như sau:

Hạng mục	Mức độ CSR	Thời gian đáp ứng	Thời gian phản hồi	Thời gian khôi phục tạm thời, hoặc giải pháp khôi phục tạm thời
CSR handling	Nghiêm trọng	24X7	120 min	1CD
	Trung bình	8X7	240 min	3CD
	Ít nghiêm trọng	8X5	NBD	5CD
Tỉ lệ xử lý sự cố đúng thời hạn cam kết không ít hơn 90% (tính trên tổng số lượng CSR được xử lý trong 1 quý)				

+ Trong đó

- CD: Calendar Day – ngày theo lịch
- NBD: Next Business Day – ngày làm việc tiếp theo
- Thời gian đáp ứng: Là thời gian Đơn vị cung cấp dịch vụ đảm bảo sẵn sàng tiếp nhận yêu cầu hỗ trợ kỹ thuật (CSR).
- Thời gian Phản hồi: Là khoảng thời gian từ khi nhận một CSR và lần đầu tiên Đơn vị cung cấp dịch vụ liên hệ với UBCK.

❖ **Phân loại mức độ CSR**

Nghiêm trọng: Là các sự cố ảnh hưởng tới dịch vụ, năng lực thiết bị, mất khả năng thực hiện các chức năng vận hành quan trọng và đòi hỏi phải có phản ứng ngay lập tức bất kể vào thời gian nào, bao gồm:

+ Hệ thống hoặc thiết bị bị lỗi hoàn toàn và hệ thống, thiết bị mất dịch vụ;

+ Các lỗi gây suy giảm dịch vụ, phạm vi rộng, lặp lại nhiều lần;

+ Không thể login vào thiết bị hoặc không thể điều khiển được thiết bị;

+ Sự cố gây nguy cơ mất dịch vụ trên diện rộng nếu không xử lý kịp thời.

Trung bình: Có thể thực hiện các chức năng vận hành, nhưng hiệu suất/ khả năng bị suy giảm hoặc bị hạn chế nghiêm trọng:

+ Các lỗi gây ảnh hưởng đến một vùng chức năng cụ thể, 1 dịch vụ cụ thể trên hệ thống, thiết bị nhưng không ảnh hưởng tới toàn bộ hệ thống và dịch vụ.

+ Sự cố ảnh hưởng đến hiệu năng của hệ thống hoặc một phần của hệ thống gây ra ảnh hưởng nhỏ tới hệ thống.

Mức Ít nghiêm trọng: Không ảnh hưởng đến quá trình vận hành hoặc nghiệp vụ.

+ Các sự cố không gây ảnh hưởng hoặc gây mất dịch vụ;

+ Các lỗi trong quá trình vận hành và khai thác, khai báo dịch vụ chưa chính xác;

❖ **Thời gian xử lý các yêu cầu và xử lý sự cố:**

- Đơn vị cung cấp dịch vụ sẽ thực hiện hỗ trợ từ xa, trong trường hợp hỗ trợ từ xa không xử lý được yêu cầu, Đơn vị cung cấp dịch vụ sẽ cử kỹ thuật thực hiện hỗ trợ trực tiếp (onsite support)

- Đưa giải pháp khắc phục tạm thời:

+ Trong thời gian xử lý CSR, Đơn vị cung cấp dịch vụ sẽ đưa ra phương án xử lý tạm thời trước (phương án đưa ra các hành động cần thiết để hạn chế ảnh hưởng của lỗi).

+ Trong trường hợp CSR được xác định có mức độ CSR là Nghiêm trọng, Đơn vị cung cấp dịch vụ sẽ thực hiện hỗ trợ khẩn cấp và ứng cứu thông tin, cung cấp các biện pháp hỗ trợ từ xa hoặc onsite tại trạm để phục hồi hệ thống một cách nhanh chóng nhất, Đơn vị cung cấp dịch vụ sẽ thực hiện dịch vụ hỗ trợ 24/7 cho đến khi tình trạng nghiêm trọng được xử lý tạm thời.

- Đưa giải pháp khắc phục hoàn toàn: Giải pháp khắc phục hoàn toàn là một giải pháp cần thiết để ngăn chặn sự cố xảy ra lại. Khi giải pháp này được thực hiện, hệ thống sẽ được khôi phục về trạng thái trước khi sự cố xảy ra. Trong một số trường hợp, giải pháp này có thể được thực hiện bằng việc sử dụng những bản software/ firmware vá lỗi có sẵn hoặc hãng cung cấp thiết bị phải phát triển một bản software/firmware mới để khắc phục hoàn toàn lỗi xảy ra.

- Đóng CSR: Sau khi đã giải quyết CSR, Đơn vị cung cấp dịch vụ sẽ đưa ra trả lời chính thức với các thông tin tóm tắt sự kiện lỗi, các hành động đã thực hiện trong quá trình xử lý và giải pháp để giải quyết vấn đề và gửi trả lời chính thức cho

Khách hàng. Khách hàng sẽ phản hồi việc chấp thuận hoặc từ chối câu trả lời cho CSR (trong 1 ngày làm việc với CSR mức nghiêm trọng và 3 ngày làm việc với CSR mức trung bình, ít nghiêm trọng):

+ Nếu được chấp nhận, CSR sẽ được đóng lại.

+ Nếu bị từ chối, Đơn vị cung cấp dịch vụ sẽ tiếp tục phân tích sâu hơn và cung cấp câu trả lời mới. Nếu trả lời mới vẫn bị từ chối thì CSR sẽ được xử lý ngoài quy trình CSR thông thường và theo các cuộc họp đánh giá dịch vụ.

- Hỗ trợ hỏi đáp kỹ thuật (Technical Query): Đơn vị cung cấp dịch vụ phản hồi các vấn đề về kỹ thuật khi có yêu cầu:

Hạng mục	**Thời gian đáp ứng**	**Thời gian phản hồi**
Hỗ trợ hỏi đáp kỹ thuật (Technical Query)	8x5	Trong vòng 1H

3.2. Yêu cầu về kỹ thuật, công nghệ đối với dịch vụ giám sát, điều phối xử lý an toàn thông tin cho hệ thống CNTT của UBCKNN

3.2.1. Yêu cầu về dịch vụ triển khai tích hợp hệ thống giám sát

- Triển khai hệ thống giám sát an toàn thông tin mạng tập trung trên cơ sở tận dụng các giải pháp hiện có của UBCKNN để phù hợp với phạm vi giám sát và đáp ứng các yêu cầu đảm bảo an toàn thông tin cho hệ thống cấp độ 3 theo quy định của pháp luật nhà nước. Hệ thống giám sát của đơn vị cung cấp dịch vụ đặt tại UBCKNN (trang thiết bị, phần mềm), đáp ứng các yêu cầu:

+ Triển khai bổ sung các thành phần hỗ trợ cho hệ thống giám sát an ninh mạng tập trung gồm thành phần: : (1) Quản lý và phân tích sự kiện an toàn thông tin tập trung (SIEM – Ngoài hệ thống SIEM của UBCKNN (nếu có)) (2) Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR); (3) cung cấp tri thức phòng ngừa mối đe dọa an toàn thông tin Threat Intelligence; (4) Phát hiện và phản ứng với nguy cơ tấn công cho máy chủ máy trạm (EDR) cho tối thiểu 110 máy chủ, 500 máy tính trạm; (5) Thu thập dữ liệu, phát hiện tấn công lớp mạng tại Core Switch của Địa điểm đặt hosting các hệ thống CNTT của UBKCNN và trụ sở UBCKNN.

+ Triển khai cài đặt, cấu hình, tích hợp hệ thống giám sát an toàn thông tin mạng tập trung đáp ứng các yêu cầu đảm bảo an toàn thông tin cho hệ thống cấp độ 3.

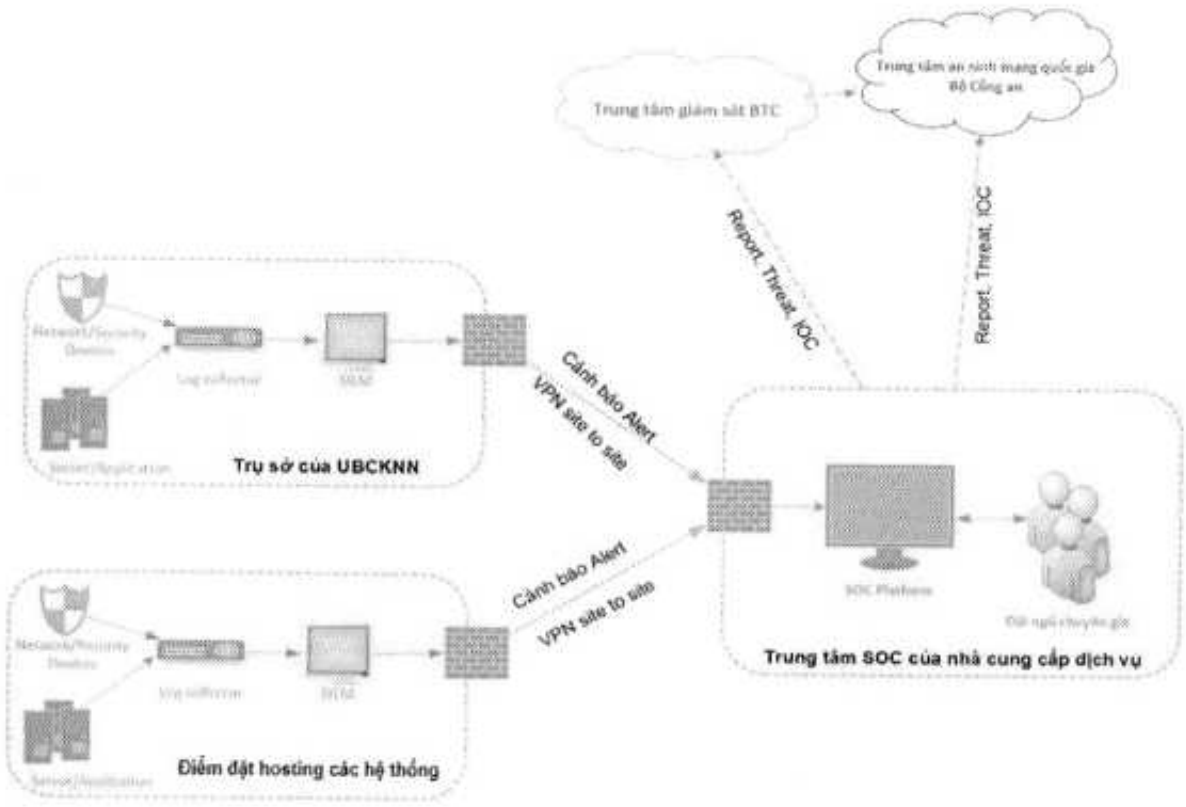
+ Triển khai chia sẻ dữ liệu với Trung tâm giám sát an ninh mạng Quốc gia của Bộ Công an theo quy định

- Tích hợp các hệ thống ATTT có sẵn tại UBCKNN và SOC Platform của đơn vị cung cấp dịch vụ, hệ thống không đẩy log trực tiếp từ UBCKNN mà chỉ đẩy các thông tin cảnh báo và liên quan đến cảnh báo về hệ thống SOC Platform: Đơn vị cung cấp dịch vụ phải có phương án chi tiết tích hợp hệ thống SIEM của UBCKNN, hệ thống SIEM của Nhà thầu (nếu có) và SOC Platform của đơn vị cung cấp dịch vụ bao gồm: phương án kết nối, băng thông kênh truyền, các thiết bị cần thiết để phục vụ việc lưu trữ và bảo vệ dữ liệu, các phần mềm bổ sung để phục vụ cho việc giám sát.

- Tối ưu log source cho hệ thống SIEM: review cấu hình lấy log đưa ra đề xuất, hỗ trợ UBCKNN thực hiện parser logsource đối với các ứng dụng mới;

- Tối ưu rule hệ thống lưu trữ log tập trung để nhận biết sớm cảnh báo tấn công, tăng cường khả năng giám sát và bảo vệ cho hệ thống: từ log source của các hệ thống gửi về, thực hiện xây dựng và tối ưu Rule để nhận biết sớm cảnh báo tấn công, tăng cường khả năng giám sát và bảo vệ cho hệ thống.

a) Mô hình kiến trúc giải pháp giám sát:



Hình 1. Mô hình tổng quan phương án giám sát

Hệ thống SIEM: Hệ thống thu thập và phân tích log tập trung đặt tại trung tâm dữ liệu của UBCKNN. Toàn bộ dữ liệu được lưu trữ trong hạ tầng của UBCKNN .

Hệ thống SOC của đơn vị cung cấp dịch vụ: nhận cảnh bảo từ hệ thống SIEM của đơn vị, thực hiện giám sát 24/7 và phản ứng sự cố an toàn thông tin.

Khi có có sự cố ATTT, đơn vị cung cấp dịch vụ giám sát SOC phối hợp chặt chẽ với đội ngũ ATTT của UBCKNN để xử lý triệt để sự cố. Việc xử lý theo đúng quy trình, quy định của UBCKNN.

b) Phạm vi, đối tượng giám sát

- Phạm vi: Toàn bộ hệ thống, thiết bị được lnêu tại Tiểu mục 1.4.3, Mục 1, Chương V của HSMT.

- Đối tượng giám sát:

+ Giám sát lớp mạng: Thiết bị mạng và thiết bị, giải pháp bảo mật thông tin

+ Giám sát lớp máy chủ (cả vật lý, ảo hóa)

+ Giám sát lớp ứng dụng: Các hệ thống, ứng dụng CNTT.

+ Giám sát lớp thiết bị đầu cuối: Máy tính trạm, máy tính xách tay.

c) Triển khai hệ thống giám sát

Triển khai cài đặt, cấu hình, tích hợp hệ thống, thu thập log (sự kiện) tại 4 lớp: mạng, máy chủ, ứng dụng, thiết bị đầu cuối bao gồm:

+ Cung cấp giải pháp Giám sát, phát hiện và phản ứng với nguy cơ tấn công cho máy chủ, máy trạm của UBCKNN (tối thiểu hai nền tảng hệ điều hành Windows và Linux). Hệ thống cần đáp ứng các tính năng:

- Thu thập và tương quan các dữ liệu từ nhiều nguồn khác nhau gồm có email, web, endpoint, server, cloud workload, network, mobile.
- Cảnh báo và thông báo về incident xảy ra trong hệ thống
- Cung cấp Detection Model (mô hình phát hiện - cảnh báo): kết hợp nhiều quy tắc và bộ lọc bằng cách sử dụng các kỹ thuật như học máy và xếp chồng dữ liệu giúp phát hiện các hành vi hoặc sự kiện đáng ngờ, có khả năng tùy biến phù hợp với kiến trúc hạ tầng của UBCKNN.
- Phân tích nguyên nhân của tấn công, rủi ro (Root-Cause analysis) và phản hồi cảnh báo: điều tra cảnh báo thông qua giao diện đồ hoạ phân tích root-cause và đánh giá ảnh hưởng, cho phép hiểu sự nghiêm trọng của cảnh báo và đưa ra các quyết định tương ứng với cảnh báo đó.
- Hỗ trợ định kỳ quét và tìm kiếm dấu hiệu xâm nhập
- Hỗ trợ quét sandboxing: Cho phép submit File, URL. Hỗ trợ quét sử dụng sandboxing
- Hỗ trợ thời gian lưu trữ dữ liệu tối thiểu 90 ngày
- Kiểm soát truy cập quản trị: Giới hạn địa chỉ IP được phép truy cập vào giao diện quản trị, giới hạn số phiên trình duyệt cho một account quản trị
- Áp dụng AI (Artificial Intelligence) và phân tích chuyên sâu để đưa ra kết quả có độ tin cậy cao
- Hỗ trợ liên kết với dịch vụ điều tra và phản hồi mở rộng (XDR) cho máy chủ và các thành phần khác gồm có: Email security, Endpoint security, Network Sensor, IPS, Mobile security, ...

- Hỗ trợ phản hồi nhanh chóng (Response): Thêm /bỏ đối tượng nguy hiểm vào/ra khỏi block list, Gửi vào sandbox phân tích, Thu thập file để điều tra, Dump process memory, Isolate endpoint, Chạy custom script (powershell hoặc shell), Remote shell
- Cung cấp thông tin mapping với MITRE ATT&CK: Ánh xạ các phát hiện với MITRE ATT&CK framework cho phép tổ chức nhanh chóng hiểu được tình huống sự cố đang xảy ra trong mạng. Các phát hiện được liên kết với tài liệu chính thức của MITRE ATT&CK framework
- Hỗ trợ khả năng tích hợp với giải pháp Quản lý rủi ro bề mặt tấn công (Attack Surface Risk Management), và tính năng truy cập bảo mật theo Zero Trust (Zero Trust Secure Access) trong cùng một hệ quản trị tập trung
- Hỗ trợ đa dạng endpoint sensor cho các hệ điều hành: Tối thiểu các hệ điều hành Windows 10/11, Windows server 2012/2012R2, 2016, 2019, 2022, Centos, CloudLinux, Debian, Oracle Linux, Redhat Enterprise Linux, SUSE, Ubuntu…
- Thu thập và hiển thị các thông tin về tấn công có chủ đích trên toàn cầu. Các thông tin tình báo này được cập nhật về các mối đe doạ (APT) đang diễn ra. Cung cấp các thông tin về tấn công APT dựa trên các trường thông tin như: Ứng hợp tên (Matched result), Kiểu (Type), Nhắm vào phân khúc nào (targeted industry), Nhắm vào vùng địa lý nào (targeted region)
- Cho phép làm giàu thông tin tình báo (custom intelligence) bằng cách nhập thông tin thủ công (import) hoặc tự động từ bên thứ ba. Các loại thông tin được hỗ trợ gồm có: Domain, File (SHA-1, SHA-256, MD5), File name, IP address, Sender address (email address), URL, Command line, User account

+ Thu thập dữ liệu, phát hiện tấn công lớp mạng tại Core Switch của địa điểm đặt hosting các hệ thống CNTT của UBCKNN và trụ sở UBCKNN. Hệ thống thu thập, phát hiện tấn công lớp mạng đáp ứng các tính năng:

- Cho phép gom dữ liệu từ các hệ thống phân tích lưu lượng mạng khác để đẩy về trung tâm
- Cho phép bóc tách các nguồn dữ liệu để phân tích hoặc để loại bỏ không phân tích bao gồm: ứng dụng, dải IP. Cho phép xác định và loại bỏ các gói tin trùng lặp trong lưu lượng mạng.

- Phân tích cú pháp của các nguồn syslog đẩy về từ các hệ thống ATTT khác tại địa điểm giám sát
- Có sẵn nguồn thông tin tình báo mối đe doạ ATTT đến từ nhiều nguồn. Cho phép tích hợp thêm với Threat Intelligence bên ngoài
- Có sẵn công nghệ phân tích mối đe doạ APT, zero-day, mã độc chưa biết. Cho phép tải file mã độc lên để phân tích
- Có công nghệ phân tích gói sâu giúp nhận diện ứng dụng trong mạng
- Triển khai quản trị tập trung và không giới hạn các điểm thu thập dữ liệu.
- Có khả năng tích hợp phản ứng với các thiết bị bảo mật như AD, Firewall và các giải pháp bảo mật khác.
- Hỗ trợ khả năng tạo Dashboard với các biểu đồ mô tả bằng Tiếng Việt

+ Cung cấp công cụ Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR) đáp ứng các yêu cầu sau:

- Cung cấp cho UBCKNN tối thiểu 05 tài khoản truy cập hệ thống SOAR để đọc thông tin, phối hợp điều tra và xử lý sự cố.
- Tích hợp thông tin từ các thiết bị mạng, bảo mật, thiết bị quản trị bảo mật trên hệ thống mạng nội bộ UBCKNN (các loại thiết bị này UBCKNN có thể thay thế hoặc thay đổi về số lượng thiết bị trong quá trình cung cấp dịch vụ) .
- Có khả năng phản ứng đồng thời xuống Email, Active Directory, firewall, Endpoint,....
- Có khả năng phân tích các rủi ro bảo mật liên quan đến các thiết bị bên trong hệ thống, thống kê các cảnh báo, sự kiện bảo mật xảy ra trên thiết bị đó, cũng như các lỗ hổng bảo mật, các câu lệnh được gõ, số lần login, số file được truyền đi

+ Cung cấp thông tin tình báo và thông báo chủ động các cuộc tấn công có thể xảy ra trên nền tảng Threat Intelligence của hãng/ nhà sản xuất có uy tín

- Có khả năng quản lý dấu hiệu tấn công và xâm phạm trên cơ sở thời gian thực và các thuộc tính, sử dụng mô hình AI (Artificial Intelligence) / ML (Machine Learning).
- Cung cấp các dấu hiệu tấn công (IOC Lookup), trong đó có thể nhận được điểm rủi ro của IOC (IOC Risk Score), điểm tin cậy (Confidence Score), thông tin

nguồn (Source details), hồ sơ tác nhân đe dọa (TA profile) và các chỉ báo tấn công (IOA - Indicators of Attack).

- Có khả năng gửi cảnh báo qua email, qua ứng dụng trên điện thoại;
- Cung cấp các thông tin chuyên sâu về các mối đe dọa, các chiến dịch tấn công APT, cảnh báo về dữ liệu của UBCKNN bị đánh cắp, rò rỉ trên các nền tảng chia sẻ dữ liệu

- Triển khai thu thập log phục vụ giám sát lớp mạng

+ Triển khai giám sát lớp mạng 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 hổng phần mềm, dịch vụ trong dữ liệu truyền tải trên mạng thông qua phân tích các dấu hiệu đặc trưng, nhận biết từ log của các hệ thống phòng chống tấn công Web Application Firewall;
- 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:

- Log của hệ thống Firewall
- Log của IPS/IDS
- Log của hệ thống Webproxy
- Log của hệ thống IPS/IDS
- Log của hệ thống Network Detection & Response/Network Traffic Analysis
- 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 (NAC)
- Log của thiết bị tối ưu chính sách bảo mật

- Triển khai thu thập log phục vụ giám sát lớp máy chủ.

+ Việc triển khai giám sát ở lớp máy chủ 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 kết nối mạng tới máy chủ (Firewall log);
- 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.

- Triển khai thu thập log phục vụ 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 hệ thống bảo mật như Firewall, Web Application Firewall, NAC;
- Log của hệ thống IPS/IDS;
- Log của hệ thống Network Detection & Response/Network Traffic Analysis;

+ 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;
- Thông tin thay đổi cấu hình ứng dụng.

- Triển khai thu thập log phục vụ giám sát lớp thiết bị đầu cuối

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

- Phát hiện sớm các dấu hiệu của phần mềm độc hại và ngăn chặn chúng trước khi gây thiệt hại: các phần mềm độc hại, virus, trojan, ransomware, và các loại mã độc khác
- Giám sát hành vi người dùng giúp phát hiện các hành động bất thường hoặc không phù hợp, chẳng hạn như cố gắng truy cập dữ liệu nhạy cảm, thay đổi quyền truy cập, hoặc truy cập hệ thống không đúng
- Phát hiện các cuộc tấn công khai thác lỗ hổng của hệ điều hành, phần mềm hoặc các ứng dụng đang chạy trên thiết bị.
- Giám sát thiết bị p phát hiện các dấu hiệu của cuộc tấn công APT, như truy cập trái phép kéo dài hoặc sự thay đổi bất thường trong hành vi của hệ thống (các cuộc tấn công APT thường khởi phát từ các thiết bị đầu cuối)

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

- System logs
- Security Logs
- Authentication & Access Logs
- File and Directory Logs
- EDR Logs
- Anti Virus Logs

+ Nguồn log tối thiểu gồm các thông tin:

- Thông tin liên quan đến việc cài đặt, cập nhật hoặc gỡ bỏ phần mềm hệ thống và ứng dụng
- Thông tin đăng nhập, đăng xuất, thay đổi mật khẩu, hoặc quyền truy cập của người dùng vào hệ thống
- Thông tin cảnh báo từ các phần mềm AV và EDR

- Triển khai kết nối, chia sẻ dữ liệu và đảm bảo các yêu cầu triển khai khác:

+ Thiết lập, duy trì đường truyền kết nối trụ sở làm việc của đơn vị cung cấp dịch vụ tới Địa điểm hosting các hệ thống CNTT của UBCKNN và trụ sở UBCKNN để phục vụ hoạt động giám sát từ xa (gửi các alert để phân tích). Băng thông kênh truyền phải đảm bảo đáp ứng yêu cầu đối với dịch vụ giám sát (Tối thiểu 02 Mb). Toàn bộ dữ liệu hệ thống giám sát đặt tại UBCKNN, không truyền về trụ sở làm việc của đơn vị cung cấp dịch vụ.

+ Triển khai đặt, cấu hình, tích hợp hệ thống giám sát an toàn thông tin mạng tập trung đáp ứng các yêu cầu đảm bảo an toàn thông tin cho hệ thống cấp độ 3.

+ Quá trình triển khai hệ thống giám sát không làm ảnh hưởng hoạt động của các hệ thống thông tin của UBCKNN trong giờ hành chính.

+ Đảm bảo cung cấp đầy đủ phần cứng và bản quyền phần mềm cho hoạt động hệ thống giám sát trong suốt thời gian cung cấp dịch vụ. Nhà thầu có trách nhiệm cập nhật phiên bản phần mềm cho hệ thống giám sát triển khai tại UBCKNN (Trong vòng 60 ngày kể từ khi công bố phát hành).

+ Trong quá trình giám sát hệ thống mà UBCKNN thay thế, cài đặt, cấu hình lại thiết bị nhà thầu có trách nhiệm triển khai công cụ/phần mềm phục vụ giám sát (thu thập, ngăn chặn, phát hiện tấn công) trên các thiết bị cần thay thế, cài đặt, cấu hình lại.

+ Triển khai chia sẻ dữ liệu với Trung tâm giám sát an ninh mạng Quốc gia của Bộ Công an theo quy định.

+ Thiết lập hệ thống tiếp nhận thông tin kết nối, chia sẻ với hệ thống giám sát an ninh mạng của Bộ Tài chính.

+ Theo dõi, đảm bảo việc kết, chia sẻ thông tin giữa hệ thống giám sát của UBCKNN và các hệ thống giám sát thực hiện thông suốt trong thời gian hợp đồng

có hiệu lực (trừ trường hợp phát sinh lỗi từ các hệ thống giám sát không phải của UBCKNN).

+ Xây dựng và thống nhất quy trình phối hợp xử lý sự cố giữa hai bên.

3.2.2. Yêu cầu về dịch vụ giám sát, điều phối xử lý sự cố 24/7

- Quản trị và vận hành hệ thống SOC 24/7: Đảm bảo hoạt động ổn định, liên tục, khắc phục các sự cố liên quan đến phần cứng, phần mềm của hệ thống SOC. Thực hiện việc tối ưu hệ thống bao gồm:

• Tối ưu SIEM (của Nhà thầu (nếu có)) rules nhằm nâng cao khả năng nhận biết và cảnh báo khi có sự cố;

• Rà soát và tối ưu cấu hình nhận log, nguồn log. Đưa ra đề xuất, hỗ trợ UBCKNN thực hiện parser logsource đối với các ứng dụng mới.

• Tối ưu Playbook, Contents Analysis: tiến hành nghiên cứu, áp dụng tự động hoá workflow; Tối ưu hoá cảnh báo; Cải tiến và nâng cao chất lượng hệ thống

- Theo dõi và cảnh báo các nguy cơ về an ninh mạng 24/7: Giám sát liên tục các sự kiện về an toàn thông tin phát sinh trên hệ thống SOC của UBCKNN từ trụ sở Nhà thầu trong thời gian 24 giờ/ngày và 7 ngày/tuần (bao gồm cả ngày lễ, tết);

- Phân tích và phối hợp xử lý các cảnh báo về an ninh mạng 24/7: Phân tích, điều tra sự kiện, xác định các vấn đề về an toàn thông tin cần phải xử lý (mã độc, tấn công, điểm yếu bị khai thác...), từ đó đưa ra các cảnh báo và khuyến nghị xử lý;

- Săn tìm chủ động các mối đe dọa (Threat Hunting) và phân tích cảnh báo sớm các mối đe dọa an ninh mạng (Threat Intelligence): Xây dựng danh mục (checklist) săn tìm (hunting) định kỳ hàng ngày dựa trên nguồn log source trên hệ thống SIEM để phát hiện các hành vi bất thường trên hệ thống để ngăn chặn kịp thời; Cung cấp thông tin tình báo và thông báo chủ động các cuộc tấn công có thể xảy ra, những thay đổi trong TTPs (Tactics, Techniques, Procedures) và các hành vi mới của các tác nhân đe doạ, cung cấp thông tin về việc rò rỉ dữ liệu nhạy cảm trong hệ thống của UBCKNN (nếu có).

+ Điều phối xử lý sự cố về an ninh mạng: Hỗ trợ ứng cứu, điều phối, xử lý sự cố an toàn thông tin mạng nhằm đối phó hiệu quả, điều phối xử lý, ngăn chặn sự cố trong thời gian ngắn nhất, không để sự cố lan rộng thêm qua đó góp phần giảm thiểu

tác động và mức độ ảnh hưởng thiệt hại do sự cố gây ra cho hệ thống thông tin. Cam kết có chuyên gia xử lý sự cố onsite trong vòng 01 giờ đối với các sự cố tấn công có mức độ ảnh hưởng nghiêm trọng hoặc khi có yêu cầu. Xử lý trực tiếp tại UBCKNN đối với các sự cố mới chưa có hướng dẫn hoặc các sự cố mà UBCKNN thực hiện không thành công theo hướng dẫn hoặc các sự cố khẩn cấp về ATTT theo yêu cầu của UBCKNN

- Điều tra và phân tích chuyên sâu các sự cố về an ninh mạng: Thực hiện bóc gỡ mã độc đối với các trường hợp hệ thống phòng chống mã độc của UBCKNN không xử lý được; xác định nguyên nhân đối các trường hợp mã độc sau khi bị diệt vẫn tái xuất hiện nhiều lần và khuyến nghị phương án xử lý, phối hợp theo dõi kết quả xử lý và điều chỉnh phương án xử lý trong trường hợp cần thiết.

- Hỗ trợ xây dựng, tối ưu quy trình vận hành hệ thống giám sát an toàn thông tin tập trung: Xây dựng các quy trình cung cấp dịch vụ giám sát; điều chỉnh quy trình trong quá trình thực hiện hợp đồng để phù hợp với thực tế nếu cần thiết. Tối thiểu các quy trình sau:

- Quy trình theo dõi cảnh báo sự cố an toàn thông tin: Mô tả các bước thực hiện theo dõi, giám sát an toàn thông tin trong hệ thống và vai trò các bộ phận tham gia trong quá trình giám sát.
- Quy trình quản lý sự cố an toàn thông tin: Mô tả các bước thực hiện và mô tả vai trò của các bộ phận tham gia.
- Quy trình thông báo, báo cáo sự cố: Mô tả các bước thực hiện và vai trò các bộ phận tham gia trong quá trình thông báo, báo cáo sự cố cho khách hàng.
- Quy trình xử lý sự cố an toàn thông tin: Mô tả các bước thực hiện xử lý và vai trò các bộ phận tham gia trong quá trình xử lý sự cố an toàn thông tin phát hiện được

- Lập báo cáo giám sát an ninh mạng theo quy định của nhà nước về hoạt động giám sát an toàn hệ thống thông tin, bao gồm: Báo cáo ngày, Báo cáo tuần (báo cáo trực tiếp cho cán bộ chuyên trách của UBCKNN), Báo cáo hoạt động giám sát định kỳ theo tháng, quý, năm (báo cáo bằng văn bản theo quy định):

- Định kỳ hàng tháng, nhà cung cấp gửi báo cáo giám sát, xử lý sự cố trong tháng, nội dung báo cáo bao gồm tối thiểu:Cảnh báo, bất thường, sự cố trong tháng,

số lượng đã xử lý; Các lỗ hổng bảo mật phát hiện; Tiến độ và tình trạng xử lý các sự cố; Khuyến nghị và phối hợp xử lý cũng như tối ưu bảo mật cho hệ thống

- Báo cáo nhanh sự cố an toàn thông tin: thực hiện gửi khi nghi ngờ có sự cố xảy ra hệ thống; đánh giá và phân tích nhanh các thông tin đã điều tra, ghi nhận (các cảnh báo liên quan, bằng chứng); nhận định sự cố và khuyến nghị xử lý nhanh.
- Định kỳ 6 tháng/lần, nhà cung cấp thực hiện báo cáo giám sát tổng thể, đánh giá các quá trình thực hiện, điều chỉnh và cải thiện chất lượng

- Thiết lập và điều chỉnh kết nối, chia sẻ thông tin giữa hệ thống giám sát an toàn hệ thống thông tin của UBCKNN với Trung tâm giám sát do Bộ Khoa học và Công nghệ hoặc Bộ Công an quản lý;

- Theo dõi, đảm bảo việc kết, chia sẻ thông tin giữa hệ thống giám sát của UBCKNN với các hệ thống giám sát đảm bảo thông suốt trong thời gian hợp đồng có hiệu lực (trừ trường hợp phát sinh lỗi từ các hệ thống giám sát không phải của UBCKNN).

3.3. Yêu cầu về kỹ thuật, công nghệ đối với dịch vụ quản trị, hỗ trợ kỹ thuật hệ thống CNTT

- Hỗ trợ kỹ thuật, và quản trị vận hành các trang thiết bị phần cứng được nêu tại Tiểu mục 1.4 Mục 1 Chương V của E-HSMT liên tục 24/7.

- Hỗ trợ thực hiện sao lưu hàng ngày, khôi phục các máy chủ (sử dụng phần mềm Backup có sẵn tại UBCKNN như VEEAM/ Veritas/ Commvault/ Dell...(nếu có) hoặc cấu hình dịch vụ sao lưu, khôi phục ở mức hệ điều hành theo yêu cầu của Chủ đầu tư);

- Hỗ trợ khắc phục, xử lý sự cố liên quan đến máy chủ, thiết bị mạng được nêu tại Tiểu mục 1.4 Mục 1 Chương V của E-HSMT liên tục 24/7(không bao gồm dịch vụ hỗ trợ thay thế, sửa chữa các máy chủ bị hỏng hóc phát sinh (nếu có));

- Quản trị, vận hành hệ thống thư điện tử tại UBCKNN (Máy chủ hệ thống Mail Exchange Server, hệ thống Active Directory Server của UBCKNN) và kết nối dịch vụ thư điện tử public ra Internet và người dùng;

- Bố trí nhân sự quản trị vận hành và hỗ trợ kỹ thuật cho hệ thống đáp ứng yêu cầu sau:

- Giám sát hệ thống 24/7: Theo dõi hiệu suất máy chủ, lưu trữ, mạng, cơ sở dữ liệu, ứng dụng để phát hiện lỗi kịp thời
- Đảm bảo hệ thống không bị gián đoạn: Quản lý uptime/downtime, duy trì hoạt động liên tục của hệ thống CNTT.
- Tối ưu hóa tài nguyên hệ thống: Điều chỉnh CPU, RAM, Storage, Bandwidth để tối ưu hóa hiệu suất.
- Cập nhật phần mềm, vá lỗi bảo mật: Đảm bảo hệ thống luôn chạy phiên bản mới nhất, giảm nguy cơ bị tấn công.
- Kiểm tra và bảo trì định kỳ: Đánh giá tình trạng hệ thống, dự đoán lỗi phần cứng, phần mềm, hạn chế sự cố bất ngờ.
- Quản lý tài nguyên & cấp quyền truy cập: Kiểm soát các user, quyền hạn truy cập hệ thống để đảm bảo an toàn
- Phát hiện & khắc phục sự cố nhanh chóng: Khi hệ thống gặp lỗi, cần tìm nguyên nhân và xử lý ngay để tránh downtime kéo dài
- Hỗ trợ điều phối xử lý sự cố an toàn thông tin: Khi bị tấn công mạng, rò rỉ dữ liệu, mất quyền truy cập, chuyên gia sẽ phục hồi hệ thống.
- Hỗ trợ xác minh và xử lý các cảnh báo về an toàn thông tin và cảnh báo lỗi hệ thống: Xác minh các thông tin cảnh báo từ đội ngũ giám sát, xử lý các lỗi phát sinh xuất hiện trên hệ thống quản trị tập trung.
- Xử lý yêu cầu hỗ trợ kỹ thuật: Hướng dẫn & hỗ trợ khi gặp vấn đề về hệ thống

3.4. Yêu cầu, điều kiện về khả năng kết nối, liên thông với ứng dụng, hệ thống thông tin khác

Yêu cầu về kết nối, chia sẻ thông tin giữa hệ thống giám sát an toàn hệ thống thông tin của UBCKNN với Hệ thống giám sát an toàn không gian mạng quốc gia:

- Thiết lập và điều chỉnh kết nối, chia sẻ thông tin giữa hệ thống giám sát an toàn hệ thống thông tin của UBCKNN với Trung tâm giám sát An ninh mạng Quốc gia (Bộ Công An).

- Thiết lập kết nối, chia sẻ thông tin giữa hệ thống giám sát an toàn hệ thống thông tin của UBCKNN với hệ thống giám sát an ninh thông tin của Bộ Tài chính.

- Theo dõi, đảm bảo việc kết, chia sẻ thông tin giữa hệ thống giám sát của UBCKNN và các hệ thống giám sát thực hiện thông suốt trong thời gian hợp đồng có hiệu lực (trừ trường hợp phát sinh lỗi từ các hệ thống giám sát không phải của UBCKNN)

3.5. Yêu cầu về an toàn thông tin, dữ liệu

- Hoạt động giám sát phải tuân thủ các quy định của Nhà nước và Bộ Tài chính về an toàn thông tin mạng, an ninh mạng, bảo vệ bí mật nhà nước và dữ liệu cá nhân.

- Ban Công nghệ và chuyển đổi số thực hiện kiểm tra định kỳ hoặc đột xuất việc tuân thủ các quy đinh của Bộ Tài chính và UBCKNN về an toàn thông tin mạng, an ninh mạng, bảo vệ bí mật nhà nước và dữ liệu cá nhân trong hoạt động giám sát của đơn vị cung cấp dịch vụ..

- Nhà cung cấp dịch vụ chịu trách nhiệm quản lý, vận hành đảm bảo hệ thống giám sát hoạt động thông suốt trong suốt thời gian cung cấp dịch vụ.

- Kết thúc thời gian thuê dịch vụ: Nhà cung cấp dịch có trách nhiệm: bàn giao thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ. Sau khi bàn giao, nhà cung cấp dịch phải hủy các thông tin, dữ liệu liên quan, không được lưu trữ, phát tán, làm lộ thông tin, dữ liệu thuộc sở hữu của UBCKNN.

3.6 Yêu cầu về nhân sự

Năng lực kinh nghiệm của nhân sự đáp ứng yêu cầu sau:

TT	Mô tả yêu cầu nhân sự	
1	**Trưởng nhóm quản lý, giám sát an ninh mạng**	
1.1	Số lượng	01 nhân sự
1.2	Nội dung công việc đảm nhận	Chịu trách nhiệm tổ chức, quản lý điều phối và giám sát triển khai dịch vụ giám sát an toàn an ninh mạng; đảm bảo đúng yêu cầu kỹ thuật, tiến độ, chất lượng; phối hợp nghiệm thu, bàn giao và chuyển giao kỹ thuật cho Chủ đầu tư.

TT	Mô tả yêu cầu nhân sự	
1.3	Bằng cấp	Có bằng tốt nghiệp đại học trở lên chuyên ngành CNTT (CNTT bao gồm các ngành đúng đào tạo về CNTT và các ngành gần đào tạo về CNTT thuộc Hệ thống ngành nghề đào tạo Máy tính và công nghệ thông tin theo quy định tại Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 của Bộ Thông tin và Truyền thông (hiện nay là Bộ Khoa học và Công nghệ)). Bằng cấp có thể do các trường đại học trong nước hoặc nước ngoài cấp.
1.4	Chứng chỉ	- Có ít nhất 1 chứng chỉ chuyên môn về quản trị an toàn thông tin còn hiệu lực thuộc danh sách sau: CISA, CISSP, CISM, CCISO hoặc tương đương - Có ít nhất 1 chứng chỉ chuyên môn về kiểm thử bảo mật (Penetration Testing) còn hiệu lực thuộc danh sách sau: GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN). - Có ít nhất 1 chứng chỉ chuyên môn về xử lý sự cố (Incident Handler) còn hiệu lực thuộc danh sách sau: GIAC Certified Incident Handler Certification (GCIH), EC-Council Certified Incident Handler (ECIH). - Trường hợp chứng chỉ có thông tin về thời gian hiệu lực thì chứng chỉ phải còn hiệu lực tối thiểu đến hết thời điểm đóng thầu. Trường hợp trên chứng chỉ không có thông tin về thời hạn hiệu lực, nhà thầu phải cung cấp đường dẫn từ website chính thức của đơn vị cung cấp có thể hiện nội dung chứng chỉ và được coi là đáp ứng.
1.5	Kinh nghiệm làm việc	- Tổng số năm kinh nghiệm: Có tối thiểu 10 năm kinh nghiệm tính từ ngày tốt nghiệp đại học (1 năm = 12 tháng).

TT	Mô tả yêu cầu nhân sự	
		- Kinh nghiệm trong các công việc tương tự: Đã tham gia làm việc ở vị trí tương tự trong tối thiểu 10 năm hoặc tối thiểu 03 hợp đồng cung cấp Dịch vụ giám sát an ninh thông tin hệ thống CNTT
1.6	Tài liệu chứng minh	Nếu được mời vào đối chiếu tài liệu, Nhà thầu phải nộp các loại tài liệu sau (bản gốc hoặc bản sao công chứng hoặc bản sao của Nhà thầu): - Bằng cấp; chứng chỉ chuyên môn. - Tài liệu chứng minh kinh nghiệm làm việc: + Bảng kinh nghiệm chuyên môn theo mẫu số 06C của E-HSMT; + Hợp đồng hoặc văn bản có xác nhận của chủ đầu tư thể hiện nhân sự có kinh nghiệm trong các công việc tương tự kèm theo biên bản nghiệm thu hợp đồng hoặc biên bản thanh lý hợp đồng.
2	**Cán bộ giám sát an ninh mạng mức 1**	
2.1	Số lượng	08 nhân sự
2.2	Nội dung công việc đảm nhận	- Thực hiện theo dõi, giám sát các cảnh báo sự cố 24/7; - Chịu trách nhiệm giám sát các cảnh báo bảo mật từ hệ thống SIEM và các công cụ giám sát khác (Firewall, IDS/IPS, EDR, v.v.); - Xử lý các sự cố đơn giản (ví dụ: xử lý các cảnh báo từ phần mềm chống virus hoặc tường lửa). - Tạo các ticket để thực hiện xử lý sự cố và phối hợp với các cấp cao hơn, theo dõi quá trình xử lý cảnh báo và sự cố

TT	Mô tả yêu cầu nhân sự	
2.3	Bằng cấp	- Có bằng tốt nghiệp đại học trở lên chuyên ngành CNTT (CNTT bao gồm các ngành đúng đào tạo về CNTT và các ngành gần đào tạo về CNTT thuộc Hệ thống ngành nghề đào tạo Máy tính và công nghệ thông tin theo quy định tại Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 của Bộ Thông tin và Truyền thông (nay là Bộ KH&CN)). Bằng cấp có thể do các trường đại học trong nước hoặc nước ngoài cấp.
2.4	Chứng chỉ	- Có tối thiểu 04 cán bộ khác nhau có một trong các chứng chỉ sau: CEH, S+, CSA, CND hoặc tương đương. - Trường hợp chứng chỉ có thông tin về thời gian hiệu lực thì chứng chỉ phải còn hiệu lực tối thiểu đến hết thời điểm đóng thầu. Trường hợp trên chứng chỉ không có thông tin về thời hạn hiệu lực, nhà thầu phải cung cấp đường dẫn từ website chính thức của đơn vị cung cấp có thể hiện nội dung chứng chỉ và được coi là đáp ứng.
2.5	Kinh nghiệm làm việc	- Tổng số năm kinh nghiệm: Có tối thiểu 1 năm kinh nghiệm tính từ ngày tốt nghiệp đại học (1 năm = 12 tháng). - Kinh nghiệm làm việc trong các công việc tương tự: Đã tham gia làm việc ở vị trí tương tự tối thiểu 01 năm hoặc 01 hợp đồng cung cấp Dịch vụ giám sát an ninh thông tin hệ thống CNTT
2.6	Tài liệu chứng minh	Nếu được mời vào đối chiếu tài liệu, Nhà thầu phải nộp các loại tài liệu sau (bản gốc hoặc bản sao công chứng hoặc bản sao của Nhà thầu): - Bằng cấp; chứng chỉ chuyên môn. - Tài liệu chứng minh kinh nghiệm làm việc:

TT	Mô tả yêu cầu nhân sự	
		+ Bảng kinh nghiệm chuyên môn theo mẫu số 06C của E-HSMT; + Hợp đồng hoặc văn bản có xác nhận của chủ đầu tư thể hiện nhân sự có kinh nghiệm trong các công việc tương tự kèm theo biên bản nghiệm thu hợp đồng hoặc biên bản thanh lý hợp đồng.
3	**Cán bộ giám sát an ninh mạng mức 2**	
3.1	Số lượng	03 nhân sự
3.2	Nội dung công việc đảm nhận	- Thực hiện phân tích, đánh giá và xử lý các cảnh báo an toàn thông tin được chuyển tiếp từ cán bộ giám sát mức 1; - Phân tích chuyên sâu các sự kiện, nhật ký hệ thống (log), dấu hiệu bất thường và nguy cơ tấn công trên các hệ thống CNTT; - Thực hiện điều tra, xác định nguyên nhân, phạm vi ảnh hưởng của các sự cố an toàn thông tin; đề xuất biện pháp xử lý, khắc phục và ngăn chặn tái diễn; - Theo dõi, giám sát quá trình xử lý sự cố, phối hợp với các đơn vị kỹ thuật, quản trị hệ thống và cán bộ giám sát mức 3 khi cần thiết; - Thực hiện tinh chỉnh (tuning) luật cảnh báo trên hệ thống SIEM, EDR và các công cụ giám sát an toàn thông tin nhằm giảm cảnh báo giả, nâng cao hiệu quả phát hiện; - Cập nhật, xây dựng quy trình xử lý sự cố, kịch bản ứng cứu và cơ sở tri thức phục vụ công tác giám sát an toàn thông tin;

TT	Mô tả yêu cầu nhân sự	
3.3	Bằng cấp	- Có trình độ đại học chuyên ngành Công nghệ thông tin hoặc các ngành gần đào tạo về công nghệ thông tin *(Theo quy định tại Điều 2-Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học & Công nghệ));*
3.4	Chứng chỉ	Có ít nhất 02 nhân sự có một trong các chứng chỉ sau: GIAC Reverse Engineering Malware (GREM), CREST Registered Threat Intelligence Analyst (CRTIA), Offensive Security Experienced Certification 3 (OSCE3), eLearnSecurity Certified Reverse Engineer (eCRE), Certified Reverse Engineering Analyst (CREA), Certified Malware Analyst and Penetration Tester (CMWAPT), CompTIA PenTest+, EC-Council Computer Hacking Forensic Investigator (CHFI) hoặc tương đương. - Trường hợp chứng chỉ có thông tin về thời gian hiệu lực thì chứng chỉ phải còn hiệu lực tối thiểu đến hết thời điểm đóng thầu. Trường hợp trên chứng chỉ không có thông tin về thời hạn hiệu lực, nhà thầu phải cung cấp đường dẫn từ website chính thức của đơn vị cung cấp có thể hiện nội dung chứng chỉ và được coi là đáp ứng.
3.5	Kinh nghiệm làm việc	- Tổng số năm kinh nghiệm: Có tối thiểu 3 năm kinh nghiệm tính từ ngày tốt nghiệp đại học (1 năm = 12 tháng). - Kinh nghiệm làm việc trong các công việc tương tự: Đã làm việc ở vị trí tương tự tối thiểu 03 năm hoặc 01 hợp đồng cung cấp Dịch vụ giám sát an ninh thông tin hệ thống CNTT

TT	Mô tả yêu cầu nhân sự	
3.6	Tài liệu chứng minh	Nếu được mời vào đối chiếu tài liệu, Nhà thầu phải nộp các loại tài liệu sau (bản gốc hoặc bản sao công chứng hoặc bản sao của Nhà thầu): - Bằng cấp; chứng chỉ chuyên môn. - Tài liệu chứng minh kinh nghiệm làm việc: + Bảng kinh nghiệm chuyên môn theo mẫu số 06C của E-HSMT; + Hợp đồng hoặc văn bản có xác nhận của chủ đầu tư thể hiện nhân sự có kinh nghiệm trong các công việc tương tự kèm theo biên bản nghiệm thu hợp đồng hoặc biên bản thanh lý hợp đồng.
4	**Cán bộ giám sát an ninh mạng mức 3**	
4.1	Số lượng	02 nhân sự
4.2	Nội dung công việc đảm nhận	- Phân tích và điều tra các sự cố phức tạp nhất . Tiếp nhận và đưa ra các giải pháp xử lý cảnh báo ở mức phức tạp; - Điều phối xử lý các sự cố và tiến hành điều tra phân tích chuyên sâu để đưa ra các phương án ứng phó với các mối đe dọa mới, nâng cao khả năng phòng vệ của hệ thống; - Thực hiện điều tra số, phân tích mã độc, phân tích hành vi tấn công, truy vết nguyên nhân và đánh giá phạm vi ảnh hưởng của sự cố.
4.3	Bằng cấp	Có bằng tốt nghiệp đại học trở lên chuyên ngành CNTT (CNTT bao gồm các ngành đúng đào tạo về CNTT và các ngành gần đào tạo về CNTT thuộc Hệ thống ngành nghề đào tạo Máy tính và công nghệ thông tin theo quy định tại Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 của Bộ

TT	Mô tả yêu cầu nhân sự	
		Thông tin và Truyền thông (hiện nay là Bộ Khoa học và Công nghệ)). Bằng cấp có thể do các trường đại học trong nước hoặc nước ngoài cấp.
4.4	Chứng chỉ	- Có ít nhất 01 nhân sự có chứng chỉ còn hiệu lực về xử lý dịch ngược mã độc như GIAC Reverse Engineering Malware (GREM), CREST Registered Threat Intelligence Analyst (CRTIA), Offensive Security Experienced Certification 3 (OSCE3), eLearnSecurity Certified Reverse Engineer (eCRE), Certified Reverse Engineering Analyst (CREA), Certified Malware Analyst and Penetration Tester (CMWAPT), CompTIA PenTest+, EC-Council Computer Hacking Forensic Investigator (CHFI) hoặc tương đương. - Có ít nhất 01 nhân sự có chứng chỉ còn hiệu lực về phân tích phòng thủ bảo mật như Offensive Security Defensive Analyst (OSDA), GIAC Certified Incident Handler (GCIH), GIAC Certified Detection Analyst (GCDA), Cybersecurity Analyst (CompTIA CySA+) hoặc tương đương - Trường hợp chứng chỉ có thông tin về thời gian hiệu lực thì chứng chỉ phải còn hiệu lực tối thiểu đến hết thời điểm đóng thầu. Trường hợp trên chứng chỉ không có thông tin về thời hạn hiệu lực, nhà thầu phải cung cấp đường dẫn từ website chính thức của đơn vị cung cấp có thể hiện nội dung chứng chỉ và được coi là đáp ứng.
4.5	Kinh nghiệm làm việc	- Tổng số năm kinh nghiệm: Có tối thiểu 5 năm kinh nghiệm tính từ ngày tốt nghiệp đại học (1 năm = 12 tháng). - Kinh nghiệm làm việc trong các công việc tương tự: Đã làm việc ở vị trí tương tự tối thiểu 05 năm hoặc 02 hợp

TT	Mô tả yêu cầu nhân sự	
		đồng cung cấp Dịch vụ giám sát an ninh thông tin hệ thống CNTT
4.6	Tài liệu chứng minh	Nếu được mời vào đối chiếu tài liệu, Nhà thầu phải nộp các loại tài liệu sau (bản gốc hoặc bản sao công chứng hoặc bản sao của Nhà thầu): - Bằng cấp; chứng chỉ chuyên môn. - Tài liệu chứng minh kinh nghiệm làm việc: + Bảng kinh nghiệm chuyên môn theo mẫu số 06C của E-HSMT; + Hợp đồng hoặc văn bản có xác nhận của chủ đầu tư thể hiện nhân sự có kinh nghiệm trong các công việc tương tự kèm theo biên bản nghiệm thu hợp đồng hoặc biên bản thanh lý hợp đồng.
5	**Cán bộ hỗ trợ quản trị, vận hành hệ thống**	
5.1	Số lượng	03 nhân sự
5.2	Nội dung công việc đảm nhận	- Thực hiện hỗ trợ quản trị, vận hành và hỗ trợ kỹ thuật hoạt động của hạ tầng hệ thống CNTT, bao gồm: máy chủ, hệ thống ảo hóa, thiết bị mạng, thiết bị bảo mật, hệ thống lưu trữ, hệ thống thư điện tử và các dịch vụ hạ tầng liên quan. - Theo dõi hiệu suất máy chủ, lưu trữ, mạng, cơ sở dữ liệu, ứng dụng để phát hiện lỗi kịp thời; - Tiếp nhận, xử lý hoặc phối hợp xử lý các sự cố kỹ thuật liên quan đến hạ tầng hệ thống, mạng và dịch vụ thư điện tử;

TT	Mô tả yêu cầu nhân sự	
		- Thực hiện cấu hình, tối ưu, cập nhật đối với hệ thống máy chủ, hệ điều hành, thiết bị mạng khi được yêu cầu. - Hỗ trợ xác minh và xử lý các cảnh báo về an toàn thông tin và cảnh báo lỗi hệ thống; - Thực hiện sao lưu, phục hồi dữ liệu khi được yêu cầu; - Theo dõi hiệu năng hệ thống, dung lượng lưu trữ, tài nguyên xử lý; đề xuất phương án nâng cấp, mở rộng khi cần thiết; - Cấu hình tối ưu hệ thống nếu được yêu cầu để đảm bảo an toàn thông tin và vận hành. - Xử lý yêu cầu hỗ trợ kỹ thuật, hướng dẫn và hỗ trợ khi gặp vấn đề về hệ thống;
5.3	Bằng cấp	Có bằng tốt nghiệp đại học trở lên chuyên ngành CNTT (CNTT bao gồm các ngành đúng đào tạo về CNTT và các ngành gần đào tạo về CNTT thuộc Hệ thống ngành nghề đào tạo Máy tính và công nghệ thông tin theo quy định tại Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 của Bộ Thông tin và Truyền thông (hiện nay là Bộ Khoa học và Công nghệ)). Bằng cấp có thể do các trường đại học trong nước hoặc nước ngoài cấp.
5.4	Chứng chỉ	- Có ít nhất 01 nhân sự có chứng chỉ về quản trị hạ tầng mạng hoặc thiết bị mạng (switch, router) của các hãng Cisco/Juniper/Dell/HPE/Array/Fortinet hoặc tương đương. - Có ít nhất 01 nhân sự có chứng chỉ về về quản trị hệ thống thư điện tử, hệ điều hành máy chủ hoặc dịch vụ hạ tầng Microsoft như Microsoft 365 Administrator, Messaging

TT	Mô tả yêu cầu nhân sự	
		Administrator, Windows Server Hybrid Administrator Associate, Azure Administrator Associate hoặc tương đương. - Có ít nhất 01 nhân sự có chứng chỉ về quản trị, vận hành máy chủ hoặc hệ thống lưu trữ hoặc hệ thống ảo hóa hoặc hạ tầng CNTT của các hãng như VMware, Microsoft, Red Hat, HPE, Dell, Fujitsu hoặc tương đương. - Trường hợp chứng chỉ có thông tin về thời gian hiệu lực thì chứng chỉ phải còn hiệu lực tối thiểu đến hết thời điểm đóng thầu. Trường hợp trên chứng chỉ không có thông tin về thời hạn hiệu lực, nhà thầu phải cung cấp đường dẫn từ website chính thức của đơn vị cung cấp có thể hiện nội dung chứng chỉ và được coi là đáp ứng.
5.5	Kinh nghiệm làm việc	- Tổng số năm kinh nghiệm: Có tối thiểu 3 năm kinh nghiệm tính từ ngày tốt nghiệp đại học (1 năm = 12 tháng). - Kinh nghiệm làm việc trong các công việc tương tự: Đã triển khai tối thiểu 01 năm hoặc 01 hợp đồng cung cấp Dịch vụ hỗ trợ kỹ thuật hệ thống CNTT.
5.6	Tài liệu chứng minh	Nếu được mời vào đối chiếu tài liệu, Nhà thầu phải nộp các loại tài liệu sau (bản gốc hoặc bản sao công chứng hoặc bản sao của Nhà thầu): - Bằng cấp; chứng chỉ chuyên môn. - Tài liệu chứng minh kinh nghiệm làm việc: + Bảng kinh nghiệm chuyên môn theo mẫu số 06C của E-HSMT; + Hợp đồng hoặc văn bản có xác nhận của chủ đầu tư thể hiện nhân sự có kinh nghiệm trong các công việc tương tự

TT	Mô tả yêu cầu nhân sự	
		kèm theo biên bản nghiệm thu hợp đồng hoặc biên bản thanh lý hợp đồng.

3.7. Uy tín nhà thầu

a. Uy tín của nhà thầu thông qua việc thực hiện các hợp đồng tương tự trước đây.

Nhà thầu cam kết đầy đủ nội dung sau trong E-HSDT:

- Nhà thầu không có hợp đồng tương tự chậm tiến độ hoặc bỏ dở do lỗi của nhà thầu.

- Nhà thầu không có hợp đồng không thực hiện các cam kết về bảo hành, bảo trì, dịch vụ sau bán hàng.

b. Uy tín của nhà thầu về việc đảm bảo tình trạng pháp lý lành mạnh khi tham dự gói thầu

Có cam kết nội dung sau trong HSDT:

- Nhà thầu, Đại diện pháp luật của nhà thầu, các nhân sự tham gia thực hiện gói thầu không đang trong tình trạng thụ lý điều tra, khởi tố hoặc tranh chấp, kiện tụng mà thời gian xử lý tranh chấp kiện tụng nằm trong thời gian dự kiến thực hiện gói thầu

- Cam kết mọi cá nhân được giao nhiệm vụ liên hệ, nhiệm vụ thực hiện các công việc thuộc gói thầu đều có lý lịch tư pháp rõ ràng, không có tiền án tiền sự và nhà thầu sẵn sàng cung cấp lý lịch tư pháp đầy đủ nếu chủ đầu tư có yêu cầu.

- Nhà thầu hoàn thành đầy đủ nghĩa vụ theo quy định của pháp luật trong việc sử dụng lao động (Sử dụng nhân sự trong độ tuổi lao động theo quy định, có ký hợp đồng lao động trong trường hợp phải ký hợp đồng lao động và hoàn tất các nghĩa vụ trả lương, thù lao, đóng bảo hiểm bắt buộc và các chế độ khác đầy đủ và đúng thời hạn theo quy định của Pháp luật…)

- Nhà thầu có cam kết không có các hành vi vi phạm qui định về mua, bán trái phép hóa đơn, gian lận thuế hoặc trốn thuế theo quy định của pháp luật trong 3 năm

gần nhất.

- Nhà thầu có cam kết tuân thủ các quy định của pháp luật về trụ sở chính và địa điểm kinh doanh theo quy định của pháp luật.

- Cam kết tuân thủ trách nhiệm đền bù đối với mọi thiệt hại đối với Chủ đầu tư và các bên liên quan gây ra do lỗi của Nhà thầu trong quá trình thực hiện gói thầu.

c. Uy tín của nhà thầu trong quá trình tham gia hoạt động đấu thầu

- Cam kết không bị kết luận vi phạm quy định về đấu thầu ở bất kỳ gói thầu nào trong vòng 3 năm gần nhất trước thời điểm đóng thầu;

- Cam kết không đang bị bất kỳ Chủ đầu tư, Chủ đầu tư nào cấm tham gia hoạt động đấu thầu trong vòng 3 năm gần nhất trước thời điểm đóng thầu; (Trường hợp các kết luận công khai trên hệ thống mạng đấu thầu quốc gia chưa kịp xử lý đính chính trước thời điểm dự thầu nhà thầu có thể cung cấp xác nhận đính chính của đơn vị Chủ đầu tư có kết luận vi phạm để chứng minh)

d. Uy tín của nhà thầu trong việc sử dụng các tài liệu thông tin trong hồ sơ dự thầu

Nhà thầu có cam kết các nội dung sau:

- Cam kết các thông tin kê khai và các tài liệu đính kèm trong hồ sơ dự thầu là chính xác và trung thực, nhà thầu đã xác minh tính chính xác và chân thực của thông tin, tài liệu trước khi dự thầu và sẵn sàng cung cấp thông tin, tài liệu chứng minh tính xác thực theo yêu cầu của Chủ đầu tư.

- Cam kết có đầy đủ bản gốc của các tài liệu đính kèm hồ sơ dự thầu và các tài liệu chứng minh nội dung thông tin kê khai tại E-HSDT, sẵn sàng cung cấp đối chiếu nếu có yêu cầu của Chủ đầu tư.

Mục 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.

Mục 5. Quy định về kiểm tra, nghiệm thu sản phẩm, trình tự giao nộp sản phẩm (nếu có)... được nêu trong hợp đồng giữa hai bên: Không yêu cầu.