Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

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

- Chủ đầu tư: Công an tỉnh Đồng Tháp

- Tên gói thầu: Thuê dịch vụ vận hành, giám sát an toàn thông tin và đường truyền kết nối từ Hệ thống SOC của tỉnh Đồng Tháp đến nhà cung cấp dịch vụ;

- Tên dự toán: Thuê dịch vụ vận hàng giám sát an toàn thông tin;

- Địa điểm thực hiện: Tỉnh Đồng Tháp;

- Nguồn vốn: Kinh phí địa phương;

- Loại hợp đồng: Trọn gói;

- Thời gian thực hiện hợp đồng: 13 tháng, trong đó (Thời gian hoàn thành việc cài đặt, kết nối hệ thống trong vòng 01 tháng kể từ ngày hợp đồng có hiệu lực; Thời gian thuê dịch vụ 12 tháng kể từ ngày hoàn thành việc cài đặt, kết nối hệ thống)

- Quy mô: Thực hiện hỗ trợ vận hành từ xa hệ thống SOC được đặt tại tỉnh Đồng Tháp, hỗ trợ phối hợp ứng cứu các sự cố an toàn an ninh mạng xảy ra trên địa bàn tỉnh Đồng Tháp.

2. Mục tiêu công việc: Nâng cao năng lực phòng, chống tấn công mạng, bảo đảm an ninh, an toàn trong hoạt động giao dịch điện tử, ứng dụng công nghệ thông tin, chuyển đổi số, góp phần phát triển kinh tế - xã hội theo tỉnh thần Nghị quyết 57 của Trung ương, bảo đảm quy định của Luật An toàn thông tin mạng, 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, Thông tư số 12/2022/TT-BTTTT của Bộ Thông tin và truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Tính năng dịch vụ

Dịch vụ vận hành giám sát an toàn thông tin:

- Giám sát, phát hiện, cảnh báo các dấu hiệu bất thường.

- Ứng cứu, xử lý sự cố an toàn thông tin

3. Yêu cầu kỹ thuật của gói thầu:

3.1. Yêu cầu về kỹ thuật chung

Nhà thầu phải lập Bảng cam kết và đáp ứng đầy đủ các nội dung như sau:

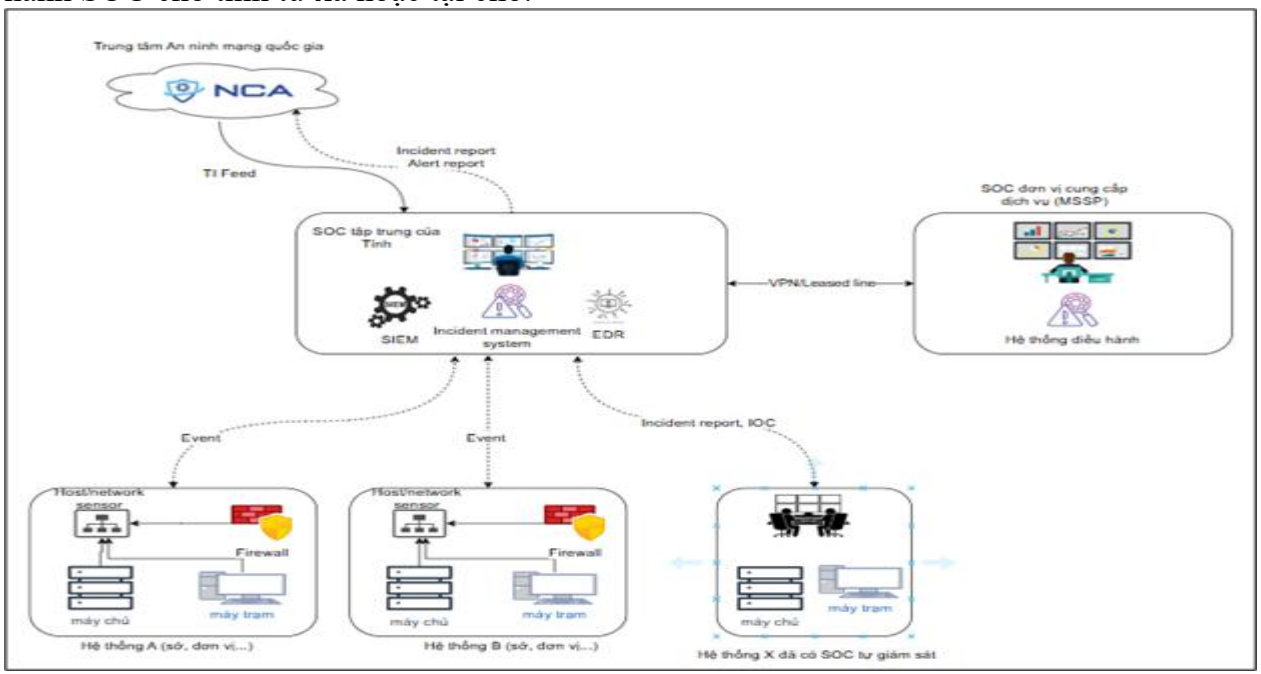
- Giải pháp, dịch vụ trung tâm giám sát điều hành an toàn, an ninh mạng (SOC) phải đáp ứng đầy đủ theo quy định tại Quyết định số 1356/QĐ-BTTTT ngày 07 tháng 7 năm 2022 của Bộ Thông tin và truyền thông;
- Cam kết khi xảy ra sự cố nhà thầu phải liên hệ khắc phục trong vòng 02 giờ ngay sau khi nhận được thông tin đơn vị sử dụng (bằng điện thoại, email) và phải khắc phục xong sự cố trong vòng 04 giờ.
- Không tiết lộ bất kỳ thông tin gì liên quan đến việc đào tạo, huấn luyện, đánh giá an toàn thông tin của hệ thống;
- Sẵn sàng trình diễn các tính năng sản phẩm trong trường hợp chủ đầu tư yêu cầu để chứng minh khả năng đáp ứng dịch vụ.
- Nghiệm thu chất lượng dịch vụ hàng tháng (Thể hiện bằng Biên bản nghiệm thu từng tháng). Căn cứ Biên bản nghiệm thu chất lượng dịch vụ, nếu nhà thầu không đảm bảo về chất lượng dịch vụ cung cấp theo yêu cầu E-HSMT và đề xuất trong E-HSDT, Chủ đầu tư sẽ chấm dứt hợp đồng với nhà thầu, toàn bộ thiệt hại của Chủ đầu tư nhà thầu phải chịu trách nhiệm, đồng thời Chủ đầu tư sẽ công bố về chất lượng sản phẩm dịch vụ cung cấp của nhà thầu trên Hệ thống mạng đấu thầu quốc gia.
- Nhà thầu phải đạt ISO/IEC 27001:2022 trong lĩnh vực vận hành giám sát và xử lý sự cố an toàn thông tin (SOC) (*Trường hợp liên danh thì từng thành viên liên danh phải đáp ứng yêu cầu này*). Trong quá trình thực hiện hợp đồng, trường hợp cần thiết Chủ đầu tư có quyền yêu cầu nhà thầu cung cấp chứng chỉ ISO/IEC 27001:2022 như đã cam kết trong E-HSDT để Chủ đầu tư kiểm tra, xác minh.
- Nhân sự có hồ sơ năng lực đảm bảo yêu cầu về tổng số lượng, chuyên ngành, chứng chỉ, kinh nghiệm (ít nhất 12 người) theo quy định tại Quyết định số 1356/QĐ-BTTTT ngày 07 tháng 7 năm 2022 của Bộ Thông tin và truyền thông, trong đó tối thiểu nhân sự phải đáp ứng đầy đủ quy định như sau:

STT	Vị trí công việc	Số lượng	Bằng cấp/chứng chỉ/ Trình độ chuyên môn được bố trí thực hiện gói thầu
1	SOC Manager	1	- Có bằng tốt nghiệp đại học trở lên thuộc chuyên ngành công nghệ thông tin/An toàn thông tin hoặc chuyên ngành gần với công nghệ thông tin theo quy định. - Có 01 trong các chứng chỉ còn hiệu lực đến thời điểm đóng thầu: CISA, CISSP, CISM, CCISO hoặc tương đương - Có kinh nghiệm ít nhất 5 năm trở lên cho vị trí tương tự
2	Nhân sự giám sát an toàn thông tin - Tier 1	6	- Có bằng tốt nghiệp đại học trở lên thuộc chuyên ngành công nghệ thông tin/An toàn thông tin hoặc chuyên ngành gần với công nghệ thông tin theo quy định. - Có 01 trong các chứng chỉ còn hiệu lực đến thời điểm đóng thầu: CEH, S+, CSA, CND hoặc tương đương - Có kinh nghiệm ít nhất 1 năm trở lên cho vị trí tương tự
3	Nhân sự xử lý sự cố - Tier 3	2	- Có bằng tốt nghiệp đại học trở lên thuộc chuyên ngành công nghệ thông tin/An toàn thông tin hoặc chuyên ngành gần với công nghệ thông tin theo quy định - Có 01 trong các chứng chỉ còn hiệu lực đến thời điểm đóng thầu: CHFI, CTIA, OSCP, OSCE, GSEC hoặc tương đương - Có kinh nghiệm ít nhất 5 năm trở lên cho vị trí tương tự

3.2. Yêu cầu kỹ thuật chi tiết:

- Nhà thầu phải lập bảng thuyết minh về nội dung công việc cung cấp dịch vụ và đáp ứng đầy đủ theo yêu cầu bên dưới.

- Bảng tóm tắt nội dung công việc yêu cầu:

STT	Danh mục dịch vụ	Mô tả dịch vụ, nội dung công việc yêu cầu
1	Dịch vụ vận hành giám sát an toàn hệ thống thông tin 24x7	**Dịch vụ Vận hành giám sát an toàn thông tin 24x7 (Monitoring), đáp ứng các yêu cầu cơ bản sau:** ***1. Mô hình chung:*** Hệ thống SOC được đặt tại hệ thống của tỉnh (Công an tỉnh hoặc Sở Khoa học và Công nghệ), do Công an tỉnh Đồng Tháp (Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao) chịu trách nhiệm quản lý, vận hành. Đơn vị cung cấp dịch vụ (MSSP) cung cấp đội ngũ chuyên gia, các giải pháp công nghệ hỗ trợ để vận hành SOC cho tỉnh từ xa hoặc tại chỗ.  ***2. Giám sát lớp mạng (NDR):*** - Giám sát hoạt động mạng của các thiết bị trong hệ thống được giám sát.

STT	Danh mục dịch vụ	Mô tả dịch vụ, nội dung công việc yêu cầu
		- Phát hiện các giao thức lớp ứng dụng (Layer 7) hoạt động trong hệ thống như: Facebook, Youtube, BitTorrent,… - Phát hiện và hiển thị thời gian thực các kết nối mạng từ hệ thống đến các vùng địa lý trên thế giới trên giao diện bản đồ (Geographic Map). - Phát hiện và thống kê thời gian thực các website được truy cập bởi người dùng, ứng dụng trong hệ thống. - Phát hiện và thống kê thời gian thực các ứng dụng hoạt động trên hệ thống (mặc định thống kê top 20 ứng dụng có hoạt động nhiều nhất). - Hỗ trợ xuất báo cáo thống kê theo các tiêu chí: Top IP trong mạng có hoạt động nhiều nhất, Top giao thức, Top quốc gia, Top website, Top IP đích,..). - Hỗ trợ xuất báo cáo thống kê hoạt động mạng đối với một thiết bị cụ thể trong hệ thống mạng được giám sát. ***3. Giám sát nhật ký, sự kiện an toàn thông tin (SIEM):*** - Phát hiện và cảnh báo các hoạt động kết nối tới các máy chủ điều khiển mạng Botnet (BotCC). - Phát hiện và cảnh báo các hoạt động kết nối tới các máy chủ, tên miền nguy hại được báo cáo và tổng hợp trong cơ sở dữ liệu của nhà thầu và các tổ chức uy tín như Emerging Threats, Virus Total, OTX, Spamhaus,… - Phát hiện và cảnh báo các hoạt động của Malware, Spyware, Ransomeware, Adware; Trojan, Worm trong hệ thống. - Phát hiện các hoạt động khai thác, lây nhiễm, của mã độc trong hạ tầng mạng LAN/WAN.

STT	Danh mục dịch vụ	Mô tả dịch vụ, nội dung công việc yêu cầu
		- Phát hiện và cảnh báo các phần mềm độc hại/mã độc được tải về từ internet. - Phát hiện và cảnh báo các cuộc tấn công, khai thác lỗ hổng của hệ điều hành: Windows, Linux, Unix trong hệ thống mạng LAN/WAN và public. - Phát hiện và cảnh báo các cuộc tấn công, khai thác lỗ hổng trong các ứng dụng quan trọng như: Web, FTP, SMTP, SQL, DNS, VOIP, TFTP, Telnet, các ứng dụng dùng chung của tỉnh,… trong hệ thống mạng LAN/WAN và public. - Phát hiện và cảnh báo các cuộc tấn công, khai thác lỗ hổng trên các thiết bị mạng: Cisco, D-Link, TPLink, HPE, Sophos, Jupiter, Peplink,… trong hệ thống mạng LAN/WAN và public. - Phát hiện và cảnh báo các cuộc tấn công, khai thác lỗ hổng trên nền tảng di động (Android, IOS,...). - Phát hiện và cảnh báo các cuộc tấn công từ chối dịch vụ DoS, DDoS. - Phát hiện và cảnh báo các hành vi dò quét, thăm dò hệ thống sử dụng các công cụ như Nessus, Acunetix, Nmap,… trong hệ thống mạng LAN/WAN và public. - Phát hiện và cảnh báo các hành vi vi phạm chính sách an ninh an toàn thông tin của pháp luật. - Phát hiện và cảnh báo việc sử dụng các phần mềm, ứng dụng Chat, IRC như: Facebook, Google Talk, ICQ,…; các phần mềm Teamview, Logmein,… - Phát hiện và cảnh báo các hành vi truy cập các website có nội dung khiêu dâm, bạo lực, cá độ. - Phát hiện và cảnh báo các hoạt động của mạng ngang hàng Peer To Peer P2P như BitTorrent, Edonkey, Gnutella,… - Phát hiện và cảnh báo các hoạt động của mạng TOR (TOR network).

STT	Danh mục dịch vụ	Mô tả dịch vụ, nội dung công việc yêu cầu
		- Phát hiện và cảnh báo các thông tin liên quan tới data breached (lộ password, password dễ đoán, password mã hóa yếu,...). - Phát hiện và cảnh báo các phần mềm độc hại/mã độc được gửi vào hệ thống mail nội bộ. - Phát hiện và cảnh báo các cuộc thăm dò, khai thác của kẻ tấn công sử dụng các payload đã có trong cơ sở dữ liệu của đơn vị cung cấp dịch vụ, OTX, Emerging Threats. Giám sát thiết bị đầu cuối (Endpoint Monitor & Log Collector): - Thu thập giám sát log của các server Window/Linux/AIX/Solaris (syslog, audit log, secure log, kern log, auth log, mail log, modsec log). - Thu thập giám sát log của các webserver: Nginx/Apache/JBoss/Tomcat/Lighttpd/LiteSpeed Web Server/IIS. - Thu thập giám sát log của các ứng dụng thông dụng sinh logs theo chuẩn syslog. - Giám sát tính toàn vẹn của các file/thư mục hệ thống Linux/Windows. - Phát hiện và cảnh báo hoạt động liên quan tấn công apt trong hệ thống theo cơ sở dữ liệu đã biết. - Phát hiện và cảnh báo hoạt động của các tiến trình/phần mềm độc hại/mã độc trong server Linux. - Phát hiện và cảnh báo hoạt động của các tiến trình/phần mềm độc hại/mã độc trong máy chạy Windows. - Phát hiện và cảnh báo hoạt động mạng (proxy, VPN, dns, telegram) của các tiến trình/phần mềm độc hại/mã độc chạy trong máy Linux/Windows. - Phát hiện và cảnh báo hoạt động khai thác, leo thang đặc quyền trong các máy Linux/Windows có sử dụng string, command nhạy cảm.

STT	Danh mục dịch vụ	Mô tả dịch vụ, nội dung công việc yêu cầu
		- Phát hiện, thu thập các IOC liên quan tới các mối nguy hại dựa theo cơ sở dữ liệu của đơn vị giám sát, OTX. - Thống kê số lượng thiết bị được giám sát (máy chủ, thiết bị mạng). ***4. Báo cáo và xử lý sự cố 24/7:*** - Báo cáo kết quả thu thập, phân tích giám sát hệ thống (đột xuất, định kỳ hàng tuần, tháng). - Hỗ trợ ứng cứu sự cố 24/7.
2	Kênh thuê riêng L2VPN 50Mbps	Đảm bảo có kênh đường truyền phù hợp để kết nối từ Hệ thống SOC tỉnh về đơn vị Nhà cung cấp dịch vụ

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: Nhà thầu cam kết thực hiện theo yêu cầu của chủ đầu tư và các quy định của pháp luật