NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
TRUNG TÂM THÔNG TIN TÍN DỤNG QUỐC GIA VIỆT NAM

Số: 1169 /TTTD-QLĐT
V/v mời báo giá dịch vụ trung tâm Giám sát, điều hành an toàn, an ninh mạng

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 07 tháng 07 năm 2026

Kính gửi:

Trung tâm Thông tin tín dụng Quốc gia Việt Nam (CIC) có kế hoạch thuê dịch vụ trung tâm Giám sát, điều hành an toàn, an ninh mạng. CIC mời Quý đơn vị cung cấp báo giá đối với dịch vụ nêu trên, yêu cầu kĩ thuật chi tiết gửi kèm công văn này.

Đề nghị Quý đơn vị gửi báo giá về Trung tâm Thông tin tín dụng Quốc gia Việt Nam (Địa chỉ: số 45 Lý Thường Kiệt, phường Cửa Nam, thành phố Hà Nội) đồng thời gửi bản mềm về địa chỉ email: qldt@creditinfo.org.vn, phongketoan@creditinfo.org.vn. Báo giá của Quý đơn vị là cơ sở để CIC xây dựng dự toán và thực hiện thủ tục mua sắm theo quy định hiện hành.

Thời hạn gửi báo giá: chậm nhất ngày 12/07/2026. Báo giá có hiệu lực tối thiểu 60 ngày.

Xin trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- P. NCPT, P.TCKT (Để đăng tải);
- Lưu VT, QLĐT.LTNhung.

Gửi kèm:
- Yêu cầu kỹ thuật của dịch vụ.

KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM
TRUNG TÂM THÔNG TIN TÍN DỤNG QUỐC GIA VIỆT NAM

Lê Anh Tuấn

YÊU CẦU KỸ THUẬT

(Đính kèm công văn số: 1169..../TTTD - QLĐT ngày 07/7/2026)

1. Yêu cầu kỹ thuật của gói thầu

1.1 Yêu cầu chi tiết về kỹ thuật

Dịch vụ Trung tâm giám sát, điều hành an toàn, an ninh mạng có yêu cầu tối thiểu như sau:

STT	Tên hạng mục	Yêu cầu kỹ thuật tối thiểu
I	**Yêu cầu chung của hệ thống SOC được cung cấp dịch vụ**	
1	Chức năng quản trị bao gồm tối thiểu các chức năng sau:	Chức năng phân tích tương quan (Correlation): Chức năng này cho phép phân tích tương quan thông tin giữa các log nhận được từ các đối tượng giám sát khác nhau;
		Chức năng lọc (Filters): Cho phép lọc ra log cần truy vấn dựa theo nội dung của từng trường thông tin mà nguồn log đã được chuẩn hóa và lưu trữ;
		Tạo các luật (Rules): Cho phép người quản trị thiết lập các luật kết hợp giữa chức năng Filter và các luật tương quan để phát hiện ra tấn công mạng hay hành vi bất thường của người sử dụng;
		Chức năng hiển thị (Dashboards): Cung cấp giao diện quản trị hệ thống, thông tin thống kê và quản lý sự kiện nhận được theo thời gian thực;
		Chức năng cảnh báo và báo cáo (Alerts and Reports): Cho phép quản lý thông tin cảnh báo và tạo báo cáo;
		Chức năng cảnh báo thời gian thực (Real Time Alert): Cho phép gửi thông tin cảnh báo thời gian thực từ hệ thống ngay khi có sự cố xảy ra;
2	Chức năng nhận log	Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng
		Định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng;
		Nhận log trực tiếp qua các giao thức mạng như: Syslog, Netflow, SNMP và các giao thức có chức năng tương đương theo thiết kế của từng hãng cụ thể;
		Giao thức truyền, nhận log qua môi trường mạng cần hỗ trợ chức năng mã hóa dữ liệu, nén dữ liệu;
		Tải các tệp tin log theo các định dạng khác nhau lên hệ thống để chuẩn hóa và phân tích;
3	Yêu cầu về chức năng giám sát hệ thống	Giám sát lớp mạng: thu thập, quản lý và giám sát các sự kiện từ các thiết bị mạng, thiết bị bảo mật như: Router, Switch, Firewall/IPS/IDS, WAF...
		Giám sát lớp máy chủ: thu thập, quản lý và giám sát các sự kiện từ các máy chủ hệ thống (cả máy chủ vật lý và ảo hóa) trên các nền tảng khác nhau như: Windows, Linux, AIX…

		Giám sát lớp ứng dụng: thu thập, quản lý và giám sát các sự kiện từ các ứng dụng như: Ứng dụng phục vụ hoạt động của hệ thống: DNS, AD…
		Ứng dụng cung cấp dịch vụ: Web, Mail, FPT và các hệ quản trị cơ sở dữ liệu Oracle, SQL ...
		Có khả năng hỗ trợ giám sát lớp thiết bị đầu cuối: thu thập, quản lý và giám sát các sự kiện từ các thiết bị như: Thiết bị mạng, bảo mật, máy chủ, Máy tính người sử dụng …
		Giám sát trên đường truyền: thu thập, quản lý và giám sát các sự kiện từ điểm giám sát biên tại giao diện kết nối của thiết bị định tuyến biên với các mạng bên ngoài; điểm giám sát tại mỗi vùng mạng của hệ thống
4	Năng lực xử lý của Trung tâm giám sát, điều hành an toàn, an ninh mạng	Đáp ứng đủ khả năng xử lý, phân tích liên tục các thông tin được thu thập từ tối thiểu 250 thiết bị quan trọng (máy chủ vật lý và ảo hóa, mạng, bảo mật …) của CIC.
5	Yêu cầu về lưu trữ	Thời gian lưu trữ log hệ thống SOC thu thập từ CIC: tối thiểu 03 tháng
6	Chức năng mở rộng	Tích hợp, cập nhật cơ sở dữ liệu nền tảng tri thức mối đe dọa ATTT
		Hỗ trợ và tích hợp các công nghệ Bigdata & Machine learning, AI
7	Quy trình quản lý, vận hành bảo đảm an toàn thông tin cho hệ thống SOC	Khởi động và tắt hệ thống giám sát
		Thay đổi cấu hình và các thành phần của hệ thống giám sát
		Quy trình xử lý các sự cố liên quan đến hoạt động của hệ thống giám sát
		Quy trình sao lưu, dự phòng cấu hình hệ thống và log của hệ thống
		Quy trình bảo trì, nâng cấp hệ thống giám sát
		Quy trình khôi phục hệ thống sau sự cố
8	Quy trình giám sát, bảo vệ hệ thống thông tin của khách hàng	Giám sát quản lý các sự kiện và cảnh báo an toàn thông tin
		Xử lý sự cố an toàn thông tin
		Tối ưu cảnh báo trên hệ thống giám sát để tăng hiệu quả của việc vận hành, giảm thiểu tối đa cảnh báo sai
		Điều tra, phân tích các nguy cơ mất an toàn thông tin
9	Đơn vị vận hành hệ thống SOC cần tổ chức và bố trí nhân sự thực hiện quản lý, vận hành hệ	Nhóm quản lý vận hành hệ thống giám sát (Soc Manager)
		Nhóm theo dõi và cảnh báo (Tier 01)
		Nhóm xử lý sự cố (Tier 02, 03)
		Nhóm điều tra, phân tích (Content Analysis, Threat Analysis)

	thống và giám sát an toàn thông tin bao gồm các nhóm:	
10	Kết nối chia sẻ tình hình giám sát với Trung tâm giám sát An ninh mạng Quốc gia.	Có khả năng kết nối chia sẻ tình hình giám sát với Trung tâm giám sát An ninh mạng Quốc gia, thuộc Bộ Công An
11	Yêu cầu của dịch vụ Trung tâm giám sát, điều hành an toàn, an ninh mạng.	Dịch vụ cung cấp đáp ứng các tiêu chí đánh giá SOC tham chiếu theo quyết định số 1356/QĐ-BTTTT ngày 07/07/2022 của Bộ Thông tin truyền thông.
II	***Hệ thống Giám sát an ninh mạng SIEM***	
1	Tính năng kỹ thuật	Khả năng phát hiện sớm các tấn công có chủ đích nhờ giám sát hệ thống một cách toàn diện theo thời gian thực
		Cấu trúc dữ liệu được chuẩn hoá, dễ hiểu và có thể tích hợp với các hệ thống sẵn có khác
		Kiến trúc triển khai mềm dẻo, dễ dàng mở rộng theo quy mô của hệ thống
		Khả năng lưu trữ và tìm kiếm phạm vi rộng, theo hướng phục vụ tối đa cho việc điều tra số, xử lý sự cố
2	Yêu cầu về hãng sản xuất	Hãng sản xuất hệ thống Giám sát an ninh mạng SIEM phải nằm trong nhóm Leader của một trong các báo cáo sau: - Báo cáo Magic Quadrant for Security Information and Event Management năm 2022 hoặc 2024.
III	***Hệ thống Điều phối phản ứng an ninh mạng***	
1	Tính năng kỹ thuật	Tự động thu thập cảnh báo và sự kiện từ SIEM
		Phân loại mức độ ưu tiên của cảnh báo
		Lập lịch và xuất báo cáo qua giao diện trực quan
		Quản lý ticket xử lý, gán đơn vị/người xử lý theo tổ chức
		Định nghĩa các thỏa thuận mức dịch vụ (service-level agreement - SLA) phù hợp với tính chất của tổ chức, tính chất của yêu cầu
		Thông báo ticket mới, ticket sắp hết hạn
		Thống kê chỉ số đánh giá thực hiện công việc (Key

		Performance Indicator -KPI) ticket xử lý theo từng đơn vị
IV	***Hệ thống Giám sát bất thường lớp mạng NSM***	
1	Tính năng kỹ thuật	Phát hiện tấn công rà quét mật khẩu trong mạng
		Phát hiện dấu hiệu tấn công từ chối dịch vụ...
		Phát hiện dấu hiệu tấn công rà quét lỗ hổng
		Phát hiện dấu hiệu tấn công ứng dụng Web (SQL Injection, XSS....)
		Phát hiện tấn công APT
		Phát hiện dấu hiệu rà quét thông tin mạng
		Phát hiện dấu hiệu khai thác dịch vụ.
V	**DỊCH VỤ ATTT MẠNG**	
1	Quy mô giám sát của CIC	Giám sát tối thiểu 250 thiết bị quan trọng (máy chủ vật lý và ảo hóa, mạng, bảo mật …) của CIC trong thời gian 12 tháng.
2	Trung tâm vận hành SOC	Nhà thầu phải có trung tâm vận hành giám sát đặt tại Việt Nam.
3	Giấy phép cung cấp dịch vụ	Nhà thầu phải có "Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng" còn hạn đến 31/8/2027 trong đó có các hạng mục: - Cung cấp dịch vụ giám sát an toàn thông tin mạng. - Cung cấp dịch vụ ứng cứu sự cố an toàn thông tin mạng. Trường hợp Nhà thầu liên danh thì từng thành viên liên danh phải có "Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng" đáp ứng các yêu cầu nêu trên. Nhà thầu nộp kèm theo E-HSDT bản scan bản gốc hoặc bản sao chứng thực giấy phép kinh doanh
4	Thời gian thành lập SOC	≥ 3 năm tính đến thời điểm chào thầu.
5	Kết nối giữa CIC và SOC	Yêu cầu kết nối được mã hóa.
6	Tích hợp	Thực hiện triển khai, tích hợp hệ thống giám sát ATTT với hạ tầng hiện có của CIC. Khi CIC nâng cấp hạ tầng (máy chủ, ảo hóa), nhà thầu có trách nhiệm phối hợp, triển khai tích hợp lại hệ thống giám sát ATTT.
7	Chuyển giao công nghệ	- Cung cấp quy trình giám sát ATTT và quy trình xử lý sự cố ATTT trong quá trình phối hợp cung cấp dịch vụ cho CIC. - Thực hiện đào tạo kiến thức quản trị, vận hành hệ thống giám sát ATTT cho nhân sự của CIC.

8	Giám sát ATTT 24/7	Cung cấp số điện thoại hotline SOC 24/7.
		Bố trí nhân sự có chuyên môn thực hiện giám sát ATTT 24/7, thực hiện cảnh báo, phối hợp với nhân sự chuyên trách của CIC để phản ứng kịp thời với các cảnh báo, sự cố ATTT xảy ra.
		Giám sát ATTT 24/7 từ các cảnh báo sinh ra từ hệ thống giám sát; phát hiện đưa ra cảnh báo; phân tích, điều tra sự cố.
		Thực hiện công tác báo cáo định kỳ hoạt động giám sát an toàn thông tin, bao gồm các báo cáo: + Báo cáo định kỳ công tác giám sát ATTT (hàng tháng, quý, năm). + Báo cáo đột xuất khi có sự cố. Nội dung báo cáo bao gồm đầy đủ các thông tin sau: thời gian giám sát; danh mục đối tượng bị tấn công cần chú ý (địa chỉ IP, mô tả dịch vụ cung cấp, thời điểm bị tấn công); kỹ thuật tấn công đã phát hiện được và chứng cứ liên quan; các đối tượng thực hiện tấn công; các thay đổi trong hệ thống được giám sát và hệ thống giám sát; v.v...;
		Giám sát, phân tích các cảnh báo nhằm nhận diện và phân loại các sự kiện ATTT được cảnh báo từ hệ thống đáp ứng tối thiểu các yêu cầu sau: + Ứng dụng (ứng dụng web, email, CSDL…): phát hiện tấn công bruteforce, truy cập bất thường… + Bất thường lớp mạng: + Bất thường lớp Endpoint cho các máy chủ quan trọng. + Các cảnh báo từ hệ thống Antivirus, EDR của CIC + Hệ thống và dịch vụ vùng biên: phát hiện các tấn công từ Internet, WAN.
9	Điều tra và xử lý sự cố	Thực hiện điều tra, xử lý các sự cố phức tạp bao gồm các công việc cơ bản sau: + Phân tích mã độc, phân tích điều tra sâu về nguồn tấn công, phát hiện đề phòng tấn công trong trường hợp xác định có sự cố ATTT hoặc khi có yêu cầu dựa trên quy trình đã được thống nhất. + Thực hiện xử lý sự cố theo 4 bước theo chuẩn NIST gồm:

		▪ Preparation ▪ Detection & Analysis ▪ Containment, Eradication & Recovery ▪ Post-incident Activity + Cam kết có chuyên gia xử lý sự cố onsite tại CIC tối đa trong vòng 04 giờ đối với các sự cố tấn công có mức độ ảnh hưởng nghiêm trọng hoặc khi có yêu cầu của CIC dựa trên quy trình giám sát/xử lý sự cố được hai bên thống nhất khi thực hiện hợp đồng. + Thực hiện báo cáo 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. + Săn tìm các mối nguy ATTT cho tối thiểu 250 thiết bị quan trọng (máy chủ vật lý và ảo hóa, mạng, bảo mật …) ít nhất 01 lần trong 01 năm hoặc khi có yêu cầu xử lý các sự cố về ATTT đột xuất của CIC.
10	Cam kết điều tra, xác minh các sự cố ATTT được cảnh báo từ hệ thống giám sát ATTT 24/7	+ Cảnh báo mức nghiêm trọng trong vòng 1 giờ. + Cảnh báo mức cao trong vòng 4 giờ. + Cảnh báo mức trung bình trong vòng 12 giờ. + Cảnh báo mức thấp trong vòng 24 giờ.
VI	**Yêu cầu kỹ thuật khác**	
1	Bản quyền	+ Đối với hệ thống/giải pháp nhà thầu tự xây dựng, nhà thầu cần cung cấp giấy chứng nhận đăng ký bản quyền tác giả của Cơ quan có thẩm quyền cấp + Đối với hệ thống/giải pháp nhà thầu không phải là nhà sản xuất, nhà thầu cần cung cấp hoặc cam kết cung cấp giấy phép sử dụng bản quyền hệ thống/giải pháp trong phạm vi cung cấp dịch vụ cho CIC và đảm bảo thời gian cung cấp dịch vụ giám sát ATTT của gói thầu này
2	Kết nối với hệ thống log tập trung của CIC	+ Nhà thầu có trách nhiệm kết nối hệ thống SOC với hệ thống log tập trung của CIC khi có yêu cầu.
VII	**Quyền sở hữu thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ công nghệ thông tin, yêu cầu về quản lý, chuyển giao dữ liệu sau quá trình thuê**	
1	Yêu cầu về quản lý, chuyển giao dữ liệu trong quá trình thuê	+ CIC có quyền sử dụng dịch vụ đã thuê để phục vụ công việc của CIC và có quyền tải về thông tin, dữ liệu do chính CIC tạo lập trong thời gian sử dụng dịch vụ. + Nhà thầu có trách nhiệm đảm bảo tính an toàn bảo mật thông tin, dữ liệu do CIC tạo lập, đảm bảo hệ thống có thể khôi phục lại dữ liệu khi xảy ra các sự cố ngoại trừ những trường hợp bất khả kháng.

		+ Nhà thầu có trách nhiệm cung cấp công cụ quản lý, giám sát hệ thống dịch vụ cho CIC sau khi đã hoàn tất thủ tục cung cấp dịch vụ cho CIC. + Nhà thầu có trách nhiệm chuyển giao toàn bộ thông tin trong quá trình sử dụng phần mềm, dữ liệu phát sinh cho CIC khi hết hạn thuê dịch vụ mà CIC không gia hạn sử dụng dịch vụ nữa hoặc khi có yêu cầu bằng văn bản của CIC.
2	Sở hữu thông tin, dữ liệu	+ CIC có quyền sở hữu, tải về phần dữ liệu do chính CIC tạo lập trong suốt quá trình sử dụng. + Nhà thầu có trách nhiệm bảo mật mọi thông tin về dữ liệu của CIC và không được phép tiết lộ cho bất kỳ bên thứ 3 nào khác ngoại trừ yêu cầu của cơ quan có thẩm quyền của nhà nước, đảm bảo thời gian bảo mật mọi thông tin về dữ liệu của CIC trong và sau quá trình thuê dịch vụ. + Nhà thầu có trách nhiệm chuyển giao toàn bộ thông tin, dữ liệu phát sinh cho CIC khi hết hạn thuê dịch vụ khi CIC không gia hạn sử dụng dịch vụ nữa hoặc khi có yêu cầu bằng văn bản của bên thuê dịch vụ.
3	Phương án sau quá trình thuê	+ Nhà thầu có trách nhiệm thông báo cho CIC bằng hình thức văn bản, email, điện thoại, nhắn tin nhắc nhở trước 60 ngày khi hợp đồng thuê dịch vụ kết thúc để CIC lên phương án thuê dịch vụ sau khi hết hợp đồng. + Nếu như CIC không tiếp tục thuê thì nhà thầu phải hỗ trợ CIC tối đa trong việc sao chép hệ thống và back up dữ liệu về máy chủ của CIC chỉ định. + Tài sản hình thành trong quá trình sử dụng 100% thuộc quyền sở hữu hợp pháp của CIC.
VIII	**Thời gian thuê dịch vụ**	12 tháng
IX	**Yêu cầu bố trí nhân sự**	
IX.1	**Phân công công việc**	
1	Nhân sự trực giám sát 24/7 (Tier 01)	+ Thực hiện hoạt động giám sát 24/7. + Chịu trách nhiệm về việc giám sát, phân tích sơ bộ nhằm nhận diện và phân loại các sự kiện ATTT được cung cấp từ hệ thống các công cụ và từ các bộ phận, quy trình hoạt động khác. + Thực hiện các hành động được định nghĩa sẵn nhằm ngăn chặn nhanh chóng các sự cố, tránh gây thiệt hại về mặt kinh tế, dữ liệu, hình ảnh... của Khách hàng. + Theo dõi quá trình xử lý, đóng các ticket xử lý xong.
2	Nhân sự phân tích, xử lý sự cố nâng cao (Tier 03)	+ Tiếp nhận, xử lý sự cố mới, phức tạp, nghiêm trọng, sự cố xử lý không thành công theo hướng dẫn và sự cố mới chưa có hướng dẫn. + Thực hiện viết bổ sung hướng dẫn xử lý cho các sự

		cố mới, đào tạo cho các nhóm nhân sự liên quan để có khả năng xử lý những lần sau. + Khi nghi ngờ có tấn công hay có các sự cố, thực hiện phân tích và gỡ bỏ mã độc. + Thực hiện xử lý sự cố cần chuyên môn sâu về: Phân tích, xử lý, điều tra sâu khi phát hiện tấn công, nguồn tấn công và ngăn chặn tấn công, …
3	Content Analysis	+ Tối ưu cảnh báo ATTT phù hợp với nghiệp vụ các hệ thống của khách hàng để tăng hiệu quả của việc vận hành, giảm thiểu tối đa cảnh báo sai. + Vận hành hàng ngày, phân tích cảnh báo sai, thực hiện điều chỉnh/tối lưu luật để tăng hiệu quả của việc vận hành, giảm thiểu tối đa cảnh báo sai. + Phân tích thông tin sự cố đã xảy ra trong nội bộ và bên ngoài, rà soát các hành vi độc hại hệ thống không phát hiện được & tiến hành nghiên cứu, bổ sung, tối ưu luật cảnh báo.
4	Threat Analysis	+ Theo dõi các nguồn tin về lỗ hổng mới (CVE, các nguồn thông tin về lỗ hổng khác: website của hãng, thế giới ngầm...) để đánh giá ảnh hưởng đến hệ thống của Khách hàng. + Phân tích để cập nhật tri thức trên các giải pháp triển khai cho Khách hàng để phát hiện, ngăn chặn các lỗ hổng mới. + Săn tìm các mối nguy cơ ATTT theo định kỳ hoặc khi có yêu cầu xử lý các sự cố về ATTT đột xuất của CIC.
5	SOC Manager	+ Quản lý điều hành việc xử lý các cảnh báo, sự cố theo KPI, đảm bảo chất lượng dịch vụ theo SLA. + Báo cáo, đánh giá các công tác hoạt động của SOC.
IX.2	**Yêu cầu về chất lượng nhân sự**	
1	Nhân sự trực giám sát 24/7 (Tier 01)	+ Số lượng tối thiểu 8 nhân sự. Mỗi nhân sự đáp ứng đầy đủ các yêu cầu sau: + Kinh nghiệm tối thiểu 01 năm hoặc tối thiểu 01 hợp đồng thực hiện các công việc tương tự. + Trình độ đại học trở lên, được đào tạo một trong các ngành đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư 08/2022/TT-BTTTT. Có tối thiểu một trong các chứng chỉ CEH, S+, CSA, CND hoặc tương đương
2	Nhân sự phân tích, xử lý sự cố nâng cao (Tier 03)	+ Số lượng tối thiểu 3 nhân sự. Mỗi nhân sự đáp ứng đầy đủ các yêu cầu sau: + Kinh nghiệm tối thiểu 5 năm hoặc tối thiểu 3 hợp đồng thực hiện các công việc tương tự. + Trình độ đại học trở lên, được đào tạo một trong các ngành đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều

		2, Thông tư 08/2022/TT-BTTTT. Có tối thiểu một trong các chứng chỉ CHFI, CTIA, OSCP, CHFI, OSCE, GSEC hoặc tương đương.
3	Content Analysis	+ Số lượng tối thiểu 02 nhân sự. Mỗi nhân sự đáp ứng đầy đủ các yêu cầu sau: + Kinh nghiệm tối thiểu 3 năm hoặc tối thiểu 3 hợp đồng thực hiện các công việc tương tự. + Trình độ đại học trở lên, được đào tạo một trong các ngành đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư 08/2022/TT-BTTTT. Có tối thiểu một trong các chứng chỉ OSCP, OSWE, CEH, CHFI hoặc tương đương.
4	Threat Analysis	+ Số lượng tối thiểu 02 nhân sự. Mỗi nhân sự đáp ứng đầy đủ các yêu cầu sau: + Kinh nghiệm tối thiểu 3 năm hoặc tối thiểu 3 hợp đồng thực hiện các công việc tương tự. + Trình độ đại học trở lên, được đào tạo một trong các ngành đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư 08/2022/TT-BTTTT. Có tối thiểu một trong các chứng chỉ CHFI, OSCP hoặc GREM.
5	SOC Manager	+ Số lượng tối thiểu 01 nhân sự. Mỗi nhân sự đáp ứng đầy đủ các yêu cầu sau: + Kinh nghiệm tối thiểu 01 năm hoặc tối thiểu 01 hợp đồng thực hiện các công việc tương tự. + Trình độ đại học trở lên, được đào tạo một trong các ngành đào tạo về công nghệ thông tin và ngành gần đào tạo về công nghệ thông tin theo quy định tại Điều 2, Thông tư 08/2022/TT-BTTTT. Có tối thiểu một trong các chứng chỉ CISA, CISSP, CISM, CCISO hoặc tương đương.

1.2 Yêu cầu khác

1.2.1 Yêu cầu về triển khai:

- Nhà thầu phải thực hiện khảo sát xây dựng phương án, kế hoạch triển khai, khởi tạo, cài đặt, cấu hình, tích hợp các giải pháp cung cấp cho CIC.
- Nhà thầu chịu trách nhiệm cài đặt, cấu hình, tích hợp các giải pháp cung cấp khi CIC có thay đổi các thiết bị quan trọng (máy chủ vật lý và ảo hóa, mạng, bảo mật …) trong thời gian thực hiện hợp đồng dịch vụ.
- Nhà thầu cung cấp, xây dựng các quy trình phục vụ công tác giám sát, xử lý sự kiện, sự cố an toàn thông tin để phối hợp với chủ đầu tư triển khai hoạt động giám sát.

1.2.2 Yêu cầu về đào tạo:

- Số lượng: 10 học viên

- Địa điểm đào tạo: trụ sở của CIC tại Số 45 Lý Thường Kiệt, Phường Cửa Nam, TP.Hà Nội.
- Trang bị cho học viên những kiến thức về quản lý, sử dụng, quản trị, vận hành hệ thống SOC đảm bảo cán bộ của CIC có thể vận hành ở vị trí Tier 02. Thời lượng tối thiểu 01 ngày.
- Đào tạo quy trình phối hợp xử lý sự kiện, sự cố an toàn thông tin. Thời lượng tối thiểu 01 ngày.
- Nhà thầu phải đảm bảo có đầy đủ tài liệu hướng dẫn, máy chiếu và máy tính (nếu cần), … cho các học viên tham gia đào tạo.

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

- Nhà thầu phải cung cấp đầy đủ các tài liệu sau quá trình triển khai:
  + Tài liệu mô tả mô hình triển khai, tích hợp hệ thống.
  + Tài liệu về quy trình giám sát, xử lý sự cố dành riêng cho CIC.
- Nhà thầu phải gửi Báo cáo định kỳ công tác giám sát ATTT (hàng tháng, quý, năm) để làm cơ sở nghiệm thu và thanh toán hợp đồng.