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

Số: 2010 /TTTD-QLĐT
V/v mời báo giá dịch vụ trung tâm giám sát điều hành an toàn, an ninh mạng (SOC)

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

Hà Nội, ngày 11 tháng 12 năm 2024

Kính gửi:

Trung tâm Thông tin tín dụng Quốc gia Việt Nam (CIC) có nhu cầu thuê dịch vụ trung tâm giám sát điều hành an toàn, an ninh mạng (SOC). CIC mời Quý đơn vị cung cấp báo giá đối với dịch vụ nói trên, yêu cầu kỹ 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 10 Quang Trung, phường Quang Trung, quận Hà Đông, Hà Nội) đồng thời gửi bản mềm về địa chỉ email: qldt@creditinfo.org.vn. Báo giá của Quý đơn vị là cơ sở để CIC xây dựng dự toán và thực hiện thủ tục đấu thầu theo đúng quy định hiện hành.

Thời hạn gửi báo giá: chậm nhất ngày 20/12/2024.

Xin trân trọng cảm ơn./.

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

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

TỔNG GIÁM ĐỐC

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

Cao Văn Bình

PHỤ LỤC

(Kèm theo công văn mời báo giá số 2010 /TTTD-QLĐT ngày 11 /12/2024)

YÊU CẦU KỸ THUẬT TRUNG TÂM GIÁM SÁT ĐIỀU HÀNH AN TOÀN, AN NINH MẠNG (SOC)

STT	Tên hạng mục	Yêu cầu kỹ thuật tối thiểu
I	**Yêu cầu chung của hệ thống SOC được cung cấp dịch vụ**	
	Chức năng quản trị	Chức năng phân tích tương quan (Correlation)
		Chức năng lọc (Filters)
		Tạo các luật (Rules)
		Chức năng hiển thị (Dashboards)
		Chức năng cảnh báo và báo cáo (Alerts and Reports)
		Chức năng cảnh báo thời gian thực (Real Time Alert)
	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
	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…
		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
	Yêu cầu về lưu trữ	Yêu cầu lưu trữ đối với hệ thống quản lý tập trung cần bảo đảm thời gian tối thiểu để lưu trữ nhật ký hệ thống của hệ thống thông tin được triển khai giám sát, bảo vệ, cụ thể: tối thiểu 03 tháng
	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
	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
	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
	Đơn vị vận hành hệ thống SOC cần tổ chức và bố trí nhân sự thực hiện quản lý, vận hành hệ thống và giám sát an toàn thông tin bao gồm các nhóm:	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)
II	***Phần mềm Giám sát an ninh mạng SIEM***	

	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
	Kết nối chia sẻ tình hình giám sát với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)	Có khả năng kết nối chia sẻ tình hình giám sát với NCSC
	Yêu cầu về hãng sản xuất	Hãng sản xuất phần mềm 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	***Phần mềm Điều phối phản ứng an ninh mạng***	
	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	***Phần mềm Giám sát bất thường lớp mạng NSM***	
		Phát hiện tấn công rà quét mật khẩu trong mạng
		Phát hiện dấu hiệu tấn công từ chối dịch vụ...

	Tính năng kỹ thuật	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**	
	Quy mô	Giám sát 200 thiết bị quan trọng (máy chủ vật lý và ảo hóa, mạng, bảo mật …) trong thời gian 01 năm.
	Trung tâm vận hành SOC	Nhà cung cấp dịch vụ SOC phải có trung tâm vận hành giám sát đặt tại Việt Nam.
	Giấy phép cung cấp dịch vụ	Nhà cung cấp phải được cấp "Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng" trong đó có các 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
	Tích hợp	Thực hiện triển khai, tích hợp hệ thống giám sát ATTT với hạ tầng hiện có của CIC.
	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.
	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.

		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.
	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.
	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.
	Kết nối giữa CIC và SOC	Yêu cầu kết nối được mã hóa

VI	Yêu cầu nhân sự	
	Nhân sự trực giám sát 24/7 (Tier 01)	+ Số lượng: tối thiểu 8 người + 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. + Yêu cầu năng lực của nhân sự: ▪ Số năm kinh nghiệm: tối thiểu 01 năm kinh nghiệm. ▪ Chứng chỉ chuyên môn: 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.
	Nhân sự phân tích, xử lý sự cố nâng cao (Tier 03)	+ Số lượng: tối thiểu 03 người + 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, … + Yêu cầu năng lực của nhân sự: ▪ Số năm kinh nghiệm: tối thiểu 05 kinh nghiệm ▪ Chứng chỉ chuyên môn: 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.
	Content Analysis	+ Số lượng: tối thiểu 02 người + 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. + Yêu cầu năng lực của nhân sự: ▪ Số năm kinh nghiệm: tối thiểu 03 năm. ▪ Chứng chỉ chuyên môn: 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
	Threat Analysis	+ Số lượng: tối thiểu 02 người + 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 cho 200 thiết bị quan trọng (máy chủ vật lý và ảo hóa, mạng, bảo mật …) ít nhất 01 lần trong 01 năm. + Yêu cầu năng lực của nhân sự: ▪ Số năm kinh nghiệm: tối thiểu 03 năm. ▪ Chứng chỉ chuyên môn: 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 01 trong các chứng chỉ CHFI, OSCP hoặc GREM.
	SOC Manager	+ Số lượng: tối thiểu 01 người + 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. + Yêu cầu năng lực của nhân sự: ▪ Số năm kinh nghiệm: tối thiểu 05 năm kinh nghiệm ▪ Chứng chỉ chuyên môn: 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 01 trong các chứng chỉ: CISA, CISSP, CISM, CCISO hoặc tương đương.
VII	**Yêu cầu khác**	

	Đào tạo	+ Số lượng: 10 học viên + 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 03 ngày. + Đào tạo quy trình phối hợp xử lý sự kiện, sự cố an toàn thông tin. Thời lượng tối thiểu 01 ngày.
	Bản quyền	+ Các phần mềm được sử dụng cho CIC phải tuân thủ sử dụng bản quyền, không được sử dụng các phần mềm vi phạm bản quyền và đảm bảo hạn cập nhật, hỗ trợ trong thời gian thực hiện hợp đồng dịch vụ.
	Kết nối với hệ thống log tập trung của CIC	+ Nhà cung cấp dịch vụ có trách nhiệm kết nối hệ thống SOC với hệ thống log tập trung của CIC khi có yêu cầu.
VIII	**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**	
	Yêu cầu về quản lý, chuyển giao dữ liệu trong quá trình thuê	- Đơn vị thuê dịch vụ có quyền sử dụng dịch vụ đã thuê để phục vụ công việc của đơn vị và có quyền tải về thông tin, dữ liệu do chính đơn vị tạo lập trong thời gian sử dụng dịch vụ. - Nhà cung cấp dịch vụ có trách nhiệm đảm bảo tính an toàn bảo mật thông tin, dữ liệu do đơn vị thuê dịch vụ 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 cung cấp dịch vụ có trách nhiệm cung cấp công cụ quản lý, giám sát hệ thống dịch vụ cho đơn vị thuê dịch vụ sau khi đã hoàn tất thủ tục cung cấp dịch vụ cho bên thuê. - Nhà cung cấp dịch vụ có trách nhiệm chuyển giao toàn bộ thông tin trong quá trình sử dụng phần mềm, dữ liệu phát sinh cho đơn vị thuê dịch vụ khi hết hạn thuê dịch vụ mà bên thuê không gia hạn sử dụng dịch vụ nữa hoặc khi có yêu cầu bằng văn bản của bên thuê dịch vụ.
	Sở hữu thông tin, dữ liệu	- Đơn vị thuê dịch vụ có quyền sở hữu, tải về phần dữ liệu do chính đơn vị tạo lập trong suốt quá trình sử dụng. - Nhà cung cấp có trách nhiệm bảo mật mọi thông tin về dữ liệu của đơn vị thuê dịch vụ 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. - Nhà cung cấp dịch vụ có trách nhiệm chuyển giao toàn bộ thông tin, dữ liệu phát sinh cho đơn vị thuê dịch vụ khi

		hết hạn thuê dịch vụ khi bên thuê không gia hạn sử dụng dịch vụ nữa hoặc khi có yêu cầu bằng văn bản của bên thuê dịch vụ.
	Phương án sau quá trình thuê	- Nhà cung cấp dịch vụ thông báo cho đơn vị thuê dịch vụ bằng hình thức văn bản, email, điện thoại, nhắn tin nhắc nhở trước 60 ngày khi hợp đồng thuê kết thúc để tiếp tục duy trì phương án thuê. - Nếu như đơn vị thuê dịch vụ không tiếp tục thuê thì nhà thầu phải hỗ trợ đơn vị thuê dịch vụ tối đa trong việc sao chép hệ thống và back up dữ liệu về máy chủ của đơn vị thuê dịch vụ chỉ định. - Tài sản hình thành trong quá trình sử dụng 100% thuộc quyền sở hữu hợp pháp của đơn vị thuê dịch vụ. Nhà cung cấp có trách nhiệm bảo mật mọi thông tin về dữ liệu của đơn vị thuê dịch vụ 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.
IX	**Thời gian thuê dịch vụ**	12 tháng