SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH VĨNH LONG
TRUNG TÂM CNTT VÀ TRUYỀN THÔNG

Số: 32/CNTTTT
V/v báo giá thẩm định giá Duy trì hệ thống và dịch vụ giám sát an toàn thông tin mạng (SOC)

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

Vĩnh Long, ngày 07 tháng 06 năm 2024

Kính gửi: Quý Cơ quan, đơn vị doanh nghiệp cung cấp dịch vụ thẩm định giá dịch vụ Công nghệ thông tin

Nhằm thực hiện nhiệm vụ được giao thường xuyên Trung tâm Công nghệ Thông tin và Truyền thông hiện tại cần triển khai việc Duy trì hệ thống và dịch vụ giám sát an toàn thông tin mạng (SOC).

Kính mời Quý Công ty/Doanh nghiệp cung cấp báo giá thẩm định giá Duy trì hệ thống và dịch vụ giám sát an toàn thông tin mạng (SOC).

(Thông tin cụ thể theo phụ lục đính kèm)

Đề nghị Quý Công ty/Doanh nghiệp phản hồi trước ngày 12/6/2024.

Nơi nhận: Phòng Hành chính - Trung tâm Công nghệ Thông tin và Truyền thông. Địa chỉ: Tầng 13 - Số 88F, đường Võ Văn Kiệt, Khóm 3, Phường 9, Tp.Vĩnh Long, Tỉnh Vĩnh Long. Số điện thoại: 02703.836.768

Trân trọng./.

Nơi nhận:
- Như trên;
- BGĐ Trung tâm;
- https://vlict.vn/
- Lưu VT, HC.

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH VĨNH LONG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Võ Văn Phước

PHỤC LỤC 1

YÊU CẦU VỀ HỆ THỐNG GIÁM SÁT AN TOÀN THÔNG TIN (SOC)

STT	Diễn giải	Số lượng	Đơn vị tính
1	Phần mềm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối – EDR (Endpoint Detection & Response) (Thời gian sử dụng 36 tháng)	1	License
2	Phần mềm Phòng chống xâm nhập lớp mạng NIPS (Network Intrusion Prevention) (Thời gian sử dụng 36 tháng)	1	License
3	Phần mềm Giám sát an ninh mạng -Security Information & Event Management (Thời gian sử dụng 36 tháng)	1	License
4	Dịch vụ Giám sát an toàn thông tin mạng 24/7 cho hệ thống Công nghệ thông tin trong Trung tâm Tích hợp dữ liệu của tỉnh Vĩnh Long với quy mô 100 máy chủ (Thời gian thực hiện 36 tháng)	1	Gói
	Tổng cộng		

Ghi chú yêu cầu Báo giá:

- Bảng báo giá sử dụng 01 tháng;
- Hiệu lực của báo giá;
- Giá thẩm định hàng hóa/sản phẩm bằng tiền Việt Nam, thuế GTGT (nếu có);
- Chi tiết tính năng chi tiết các phần mềm, dịch vụ.

PHỤ LỤC 2

CHI TIẾT NỘI DUNG DUY TRÌ HỆ THỐNG VÀ DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN MẠNG (SOC)

(Kèm theo công văn số 32../CNTTTT, ngày 7/ 6/2024)

Đơn vị tính: đồng

STT	SẢN PHẨM/DỊCH VỤ	ĐƠN VỊ	SỐ LƯỢNG	ĐƠN GIÁ	THÀNH TIỀN	VAT	THÀNH TIỀN *(ĐÃ BAO GỒM VAT)*
I	**DUY TRÌ HỆ THỐNG VÀ DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN MẠNG (SOC)**						
1	**Phần mềm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối – EDR (Endpoint Detection & Response)** - Giám sát các hành vi ở mức nhân hệ điều hành Windows Server 2008 R2 trở lên, CentOS 7 m2 - Phân tích hành vi và xử lý tập trung. - Theo dõi tình hình cài đặt, trạng thái hoạt động của máy chủ - Cảnh báo kịp thời các bất thường phát hiện trên máy chủ. - Phát hiện dấu hiệu tấn công nâng cao APT theo MITRE ATT&CK - Cung cấp giao diện khép kín điều tra các cuộc tấn công (IR Flow): Detection – Investigation - Response. - Hỗ trợ cô lập (network, process) tạm thời các máy phục vụ điều tra.	License	1				

STT	SẢN PHẨM/DỊCH VỤ	ĐƠN VỊ	SỐ LƯỢNG	ĐƠN GIÁ	THÀNH TIỀN	VAT	THÀNH TIỀN *(ĐÃ BAO GỒM VAT)*
	- Đáp ứng yêu cầu Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; - Thời gian sử dụng: 36 tháng (bao gồm hỗ trợ kể từ ngày kích hoạt)						
2	**Phần mềm Phòng chống xâm nhập lớp mạng NIPS (Network Intrusion Prevention)** - 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 các dấu hiệu IoC của mã độc APT - Phát hiện các kỹ thuật tấn công theo khung MITRE ATT&CK - Phát hiện dấu hiệu rà quét thông tin mạng. - Phát hiện dấu hiệu khai thác dịch vụ. - Thời gian sử dụng: 36 tháng (bao gồm hỗ trợ kể từ ngày kích hoạt)	License	1				
3	**Phần mềm giám sát an ninh mạng - Security Information & Event Management** - Agent thu thập Log trên Windows; Agent thu thập Log trên Linux; Thu thập Windows Event; Thu thập Log qua Syslog. - Giám sát tuân thủ chính sách trên hệ điều hành máy chủ theo TCVN 11930:2017.	License	1				

STT	SẢN PHẨM/DỊCH VỤ	ĐƠN VỊ	SỐ LƯỢNG	ĐƠN GIÁ	THÀNH TIỀN	VAT	THÀNH TIỀN *(ĐÃ BAO GỒM VAT)*
	- Chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ log, các sự kiện ATTT mạng; - Cung cấp ngôn ngữ tìm kiếm thân thiện, hỗ trợ tìm kiếm các event, alert dưới dạng biểu đồ trực quan - Hệ thống lưu trữ dữ liệu được đánh chỉ mục, sao lưu đảm bảo không mất mát dữ liệu, phục vụ cho quá trình điều tra, truy vết - Cung cấp giao diện giám sát cảnh báo theo thời gian thực - Cung cấp giao diện quản trị trực quan, thân thiện, đa dạng về thông tin và có thể tùy chỉnh theo nhu cầu sử dụng thực tế của khách hàng; - Phân quyền người dùng quản trị theo nhóm máy chủ, giải pháp giám sát; - Tạo các biểu đồ thống kê dữ liệu; - Phân tích tương quan sự kiện nhật ký theo thời gian thực. - Kết nối chia sẻ tình hình giám sát với NCSC. - Thời gian sử dụng: 36 tháng (bao gồm hỗ trợ kể từ ngày kích hoạt)						
4	**Dịch vụ giám sát ATTT mạng 24/7 cho hệ thống Công nghệ Thông tin trong Trung tâm Tích hợp dữ liệu của tỉnh tỉnh Vĩnh Long với quy mô 100 máy chủ. Các công việc bao gồm:** - Giám sát ATTT 24/7 (cho máy chủ/thiết bị đầu cuối, giám sát lớp mạng, giám sát ứng dụng), tiếp	Gói	1				

STT	SẢN PHẨM/DỊCH VỤ	ĐƠN VỊ	SỐ LƯỢNG	ĐƠN GIÁ	THÀNH TIỀN	VAT	THÀNH TIỀN *(ĐÃ BAO GỒM VAT)*
	nhận cảnh báo mới, phân tích và xử lý theo hướng dẫn với công cụ điều phối và xử lý sự kiện an toàn thông tin (SOAR). - Hỗ trợ chuyên sâu - Phân tích mã độc và Điều tra nâng cao/khắc phục sự cố. - Phân tích tối ưu Content Analysis (Tự động hoá workflow; Tối ưu hoá cảnh báo; Cải tiến và nâng cao chất lượng hệ thống; Tối ưu tập luật phù hợp với tổ chức). - Phân tích nguy cơ Threat Analysis (Cập nhật tri thức security từ bên ngoài; Xác minh và cảnh báo các nguy cơ mới; Phân tích và cập nhật các tri thức mới vào hệ thống). - Quản lý điều hành trung tâm SOC Manager (Báo cáo/đánh giá hiệu quả của hệ thống định kỳ hàng tháng và đột xuất khi có sự cố; Quản lý quá trình vận hành; Đề ra quy trình, chiến lược và kế hoạch dài hạn). - Kênh truyền kết nối phục vụ vận hành, viết tập luật (rule), tối ưu cảnh báo điều tra/ứng cứu sự cố. - Thời gian thực hiện: 36 tháng.						
TỔNG CỘNG/36 THÁNG							