Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

- Chủ đầu tư: Công ty TNHH MTV Tổng công ty Tân Cảng Sài Gòn (TCT).

- Nguồn vốn: Vốn chủ sở hữu của Tổng công ty Tân Cảng Sài Gòn.

- Địa điểm thực hiện: Tại Cảng Tân Cảng Cát Lái - 1295B Đường Nguyễn Thị Định – Phường Cát Lái – Tp. Hồ Chí Minh

Để có cơ sở cho việc lập hồ sơ dự thầu, nhà thầu được bố trí, sắp xếp đi khảo sát hiện trường để nắm bắt thực trạng hiện có. Chủ đầu tư sẽ hướng dẫn Nhà thầu khảo sát hiện trường.

Người liên hệ đi khảo sát : Ông Lê Viết Kiên – SĐT 0901 770 100.

1.1.1. Phạm vi cung cấp

Thông tin trong Bảng phạm vi và tiến độ cung cấp hàng hóa là cơ sở để nhà thầu lập bảng chào giá. Phạm vi và tiến độ cung cấp hàng hóa được mô tả theo Bảng dưới đây:

Bảng số 1. Phạm vi cung cấp hàng hóa

Stt	Danh mục hàng hóa	Đơn vị tính	Khối lượng	Ghi chú
1	Thiết bị giám sát, phát hiện tấn công xâm nhập có chủ đích qua mạng.	Cái	01	
2	Bản quyền thời hạn 03 năm phần mềm giám sát và phát hiện tấn công xâm nhập có chủ đích qua mạng (tính theo băng thông, 1 Gói = 1 Mbps).	Gói	350	
3	Bản quyền phần mềm quản lý tập trung.	Gói	01	
4	Mô đun quang 1G/10G.	Cái	02	

Bảng số 2. Dịch vụ liên quan

Stt	Mô tả dịch vụ	Khối lượng	Đơn vị tính	Địa điểm thực hiện dịch vụ	Ngày hoàn

		mời thầu			**thành dịch vụ[(2)]**
1	Triển khai, cài đặt hệ thống APT, tối ưu hệ thống, kiểm thử, đánh giá hiệu quả và đào tạo vận hành.	01	Lần	Tại Cảng Tân cảng Cát Lái - 1295B Đường Nguyễn Thị Định – Phường Cát Lái – Tp. Hồ Chí Minh.	84

1.1.2. Tiến độ cung cấp

Bảng số 3. Tiến độ cung cấp

Stt	Danh mục hàng hóa	Đơn vị	Số lượng	Tiến độ cung cấp	Địa điểm cung cấp
1	Toàn bộ hàng hóa và dịch vụ liên quan theo yêu cầu của HSMT.	Gói	01	Tối đa 84 ngày kể từ ngày HĐ có hiệu lực.	Tại Cảng Tân cảng Cát Lái - 1295B Đường Nguyễn Thị Định – Phường Cát Lái – Tp. Hồ Chí Minh.

1.2. Yêu cầu về kỹ thuật

Tóm tắt thông số kỹ thuật của hàng hóa, dịch vụ liên quan. Hàng hóa, dịch vụ liên quan phải tuân thủ các thông số kỹ thuật và tiêu chuẩn sau đây:

Bảng số 4. Yêu cầu kỹ thuật

Stt	Mô tả chi tiết thông số kỹ thuật	
	Thiết bị giám sát, phát hiện tấn công xâm nhập có chủ đích qua mạng.	
1	**Yêu cầu chung**	
	- Thiết bị phần cứng chuyên dụng. - Phải tương thích, đồng bộ chia sẻ IoC (Indicator of compromise) với hệ thống giám sát, phát hiện APT hiện có của TCT TCSG.	
2	**Yêu cầu năng lực xử lý**	
	Kiểu thiết kế phần cứng	Rackmount
	Nguồn điện	Tối thiểu 02 nguồn

	Đĩa cứng	Tối thiểu 2x 10TB HDD RAID 1
	Giao diện mạng	Tối thiểu: - 04 cổng 1GE/10GE Bypass - 06 cổng 10GE SFP+ - 02 cổng 40 GE QSFP+
	Năng lực xử lý	- Tối thiểu 350 Mbps và có khả năng nâng cấp lên 5 Gbps bằng bản quyền.
	Khả năng duy trì dịch vụ khi bị lỗi	- Bao gồm mô-đun hoặc card mạng bypass.
3	**Yêu cầu về tính năng**	
- Phát hiện ngăn chặn các cuộc tấn công tiên tiến, có chủ đích và các cuộc tấn công né tránh khác thông qua truy cập internet.		
- Triển khai được ở chế độ: In-line monitor, fail- open, fail-close (HW bypass) hoặc TAP/ SPAN.		
- Có tính năng giải mã SSL Decryption hoặc SSL Interception.		
- Giải pháp phải phân tích được các kết nối web từ máy người dùng nhằm phát hiện và cảnh báo các hành vi nguy hiểm, các trang web độc hại có chứa tập tin mã độc được tải về thông qua các truy cập web/ internet.		
- Có khả năng phát hiện các kỹ thuật lẩn tránh môi trường phân tích của mã độc: sử dụng công nghệ phân tích trên môi trường ảo hoá không dựa theo mẫu (signatureless) để phát hiện tấn công zero-day, multi-flow và các kỹ thuật lẩn tránh.		
- Phát hiện và ngăn chặn các kiểu tấn công: làm rối mã (obfuscated), chủ đích (targeted), tùy chỉnh (customized attacks).		
- Có khả năng phát hiện và ngăn chặn các kết nối C&C (command & control).		
- Giải pháp hỗ trợ phát hiện mã độc và tổng hợp dựa theo nhiều môi trường khác nhau như Windows, Linux, MacOS với nhiều phiên bản khác nhau.		
- Giải pháp có khả năng phát hiện và cảnh báo đối với các hành vi tấn công qua mạng nội bộ như: Internal Reconnaissance, Privilege Escalation, Credentials Access, Lateral Movement, Schedule Task Execution, Data Exfiltration Detection.		

- Tích hợp sẵn công nghệ môi trường giả lập Virtual Enviroment/ sandboxing, phân tích động, signature-less và signature-based IPS (dựa theo mẫu) để phát hiện và ngăn chặn các mối hiểm hoạ.
Cung cấp báo cáo phân tích chi tiết về hành vi của mã độc phát hiện được: + Dạng danh sách thống kê chi tiết hành vi của mã độc theo trình tự các bước thực thi của mã độc. + Biểu đồ hoá dưới dạng hình cây trực quan để hiển thị các hành vi của mã độc bao gồm: process, files, registry, network apicall.
- Tự động lưu lại các kết nối mạng dưới dạng pcap khi thực hiện phân tích mã độc trong môi trường sandbox, đồng thời cho phép người quản trị có thể tải về để phân tích.
- Có tính năng kiểm tra, đánh giá rủi ro (riskware) của các tập tin đính kèm có hành vi của mã độc nhưng không nhằm mục đích độc hại như: các chương trình cài đặt không mong muốn, các phần mềm sửa đổi cài đặt gây ảnh hưởng hoặc giảm hiệu suất của hệ thống, phần mềm adware.
- Công nghệ phân tích động được xây dựng trên nền tảng ảo hoá (hypervisor) riêng, không sử dụng các giải pháp ảo hoá phổ biến như VMware, HyperV, KVM ,…
- Hỗ trợ phân tích tối thiểu 160 định dạng file khác nhau: portable executables (PEs), active web content, archives, images, Java, Microsoft, Adobe applications & multimedia…
- Giải pháp phải có tính năng quản trị cấu hình tập trung, chia sẻ dữ liệu IoC đã phát hiện trên hệ thống APT Email, APT Network đang sử dụng tại TCT TCSG thông qua trung tâm quản lý tập trung.
- Có khả năng gửi các thông báo qua Syslog, SNMP, HTTP, SMTP.
- Giải pháp hỗ trợ nhiều định dạng báo cáo như XML,CSV,JSON,TEXT,…
- Sử dụng các YARA Rules để phát hiện mã độc.
- Có hỗ trợ đảm bảo tính sẵn sàng cao, không phát sinh thêm giải pháp bổ sung.
4 Yêu cầu về bảo hành
- Bảo hành chính hãng. - Thời gian bảo hành: Tối thiểu 03 năm cho phần cứng và phần mềm.

1.3. Các yêu cầu khác

1.3.1. Các yêu cầu về triển khai và giải pháp kỹ thuật:

1.3.1.1. Yêu cầu chung:

- Nhà thầu đề xuất phương án nâng cấp (phần mềm firmware, hệ điều hành) và các tính năng cần thiết theo khuyến nghị của hãng sản xuất thiết bị trước khi tích hợp vào hệ thống.

- Nhà thầu đề xuất kịch bản kiểm thử theo các tính năng và cam kết thực hiện kiểm thử để đảm bảo thiết bị đáp ứng đúng những yêu cầu về tính năng và năng lực xử lý như mô tả tại mục 1.2 chương V "Yêu cầu kỹ thuật".

1.3.1.2. Yêu cầu cụ thể:

- Nhà thầu đề xuất thiết kế, giải pháp và mô hình triển khai cho thiết bị, đảm bảo khả năng bypass nếu xảy ra sự cố với thiết bị trong khi vận hành, có phương án sao lưu dự phòng và kịch bản xử lý khi có sự cố từng trường hợp.

- Nhà thầu xây dựng phương án và triển khai thực hiện đồng bộ chia sẻ IoC với các hệ thống giám sát APT hiện có nhằm đảm bảo không ảnh hưởng hoặc không gây sự cố nghiêm trọng đến hoạt động của hệ thống, cam kết không phát sinh thêm bất kỳ chi phí nào khác ngoài giá trị gói thầu.

- Nhà thầu xây dựng và thực hiện kiểm thử kịch bản mô phỏng tấn công có chủ đích (APT), bao gồm: khai thác lỗ hổng (CVE), chiếm quyền điều khiển hệ thống, kết nối đến máy chủ điều khiển (C2) và thực hiện hành vi trích xuất dữ liệu ra ngoài. Đánh giá hiệu quả, đề xuất cải tiến hiện trạng sau khi kiểm thử.

- Nhà thầu đề xuất phương án và quy trình các bước để chuyển đổi, tích hợp thiết bị giám sát, phát hiện tấn công xâm nhập có chủ đích mới vào hệ thống mạng một cách nhanh nhất và phải cam kết đảm bảo không làm gián đoạn hoạt động giám sát của hệ thống.

- Nhà thầu đề xuất xây dựng, tùy chỉnh các báo cáo tổng hợp (theo ngày, tuần, tháng).

1.3.2. Các yêu cầu về huấn luyện và đào tạo:

- Nhà thầu đề xuất kế hoạch, phương án huấn luyện đào tạo triển khai, vận hành, thực hiện kịch bản dự phòng, xử lý sự cố, tối ưu thiết bị và tài liệu liên quan.

- Nhà thầu cam kết chuyển giao tài liệu mô tả mô hình và thiết kế; tài liệu triển khai, vận hành; tài liệu mô tả các bước xử lý sự cố, tối ưu thiết bị và tài liệu liên quan khác.

1.3.3. Các yêu cầu khác về dịch vụ bảo hành, hỗ trợ kỹ thuật:

Trong thời gian bảo hành chính hãng, nhà thầu phải đảm bảo các yêu cầu sau:

- Thời gian bảo hành và hỗ trợ kỹ thuật 24/7 tối thiểu 3 năm.
- Được hỗ trợ mở support case từ hãng khi cần hỗ trợ về kỹ thuật hay lỗi phát sinh trong quá trình vận hành.
- Hỗ trợ thay thế linh kiện (sau khi xác định được lỗi) tận nơi.
- Khi có yêu cầu của chủ đầu tư qua kênh hotline được cung cấp thì nhà thầu phải cam kết phản hồi trong vòng 2 giờ.
- Hỗ trợ kiểm tra hệ thống, đề xuất cải tiến hiệu quả định kỳ hằng quý.