# Gói thầu: Trang bị hệ thống giám sát an toàn thông tin vùng mạng OT

# PHẦN 2. YÊU CẦU VỀ KỸ THUẬT
# 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: Chi nhánh Tổng Công ty Điện lực Thành phố Hồ Chí Minh TNHH – Trung tâm Chăm sóc Khách hàng

- Tên dự án: Trang bị hệ thống giám sát an toàn thông tin vùng mạng OT

- Tên gói thầu: Trang bị hệ thống giám sát an toàn thông tin vùng mạng OT

- Nguồn vốn: Vay tín dụng thương mại và khấu hao cơ bản (đối ứng)

- Loại hợp đồng: Trọn gói

- Thời gian thực hiện gói thầu: 90 ngày

- Tùy chọn mua thêm (nếu có): 3.847.880.259 đồng

- Địa điểm thực hiện: Tòa nhà Green Power, Số 35 Tôn Đức Thắng, Phường Sài Gòn, Thành phố Hồ Chí Minh.

### 1.2. Yêu cầu về kỹ thuật

| STT | Tiêu chí kỹ thuật | Yêu cầu kỹ thuật chi tiết |
|---|---|---|
| **A** | **Yêu cầu chung hệ thống giám sát an toàn thông tin (ATTT) cho vùng mạng OT** | |
| **I** | **Kiến trúc và môi trường cài đặt tổng quát** | |
| 1 | Kiến trúc | Cài đặt và vận hành trong môi trường OT (On premises). |
| | | Môi trường cài đặt cách ly toàn bộ với Internet. |
| **II** | **Tính năng dành cho hệ thống quản trị mối đe dọa tập trung** | |
| 1 | Khả năng quản trị mối đe dọa | Trung tâm IoC. Nhận các kết quả IoC từ các thành phần trong mạng. |
| | | Chia sẻ các IoC này đến các thành phần bảo vệ máy trạm và máy chủ. |
| | | Cho phép import IoC từ bên ngoài vào. |
| **III** | **Tính năng dành cho hệ thống bảo vệ cho máy trạm** | |
| 1 | Hỗ trợ đa dạng hệ điều hành | Windows 10, 11..., đồng thời hỗ trợ Windows server 2008R2, 2012/2012R2, 2016, 2019, 2022... và Linux (Ubuntu, SUSE, Redhat…) |
| 2 | Hỗ trợ phát hiện mã độc | Có thể quét mã độc realtime scan, schedule scan, manual scan. |
| 3 | Hỗ trợ công nghệ quét | Signature-based. |
| 4 | Sandboxing | Có thể tích hợp và gửi file đến hệ thống sandboxing để phân tích sâu. |
| **IV** | **Tính năng dành cho hệ thống bảo vệ cho máy chủ** | |
| 1 | Hỗ trợ đa dạng hệ điều hành | Windows server 2008R2, 2012/2012R2, 2016, 2019, 2022. Linux (Ubuntu, SUSE, Redhat…) |

| | | |
|---|---|---|
| 2 | Hỗ trợ phát hiện mã độc | Có thể quét mã độc realtime scan, schedule scan, manual scan |
| 3 | Hỗ trợ công nghệ quét | Signature-based |
| 4 | Hỗ trợ host-based firewall | Hỗ trợ tính năng firewall |
| 5 | Tính năng phát hiện hoặc ngăn chặn xâm nhập mạng | Hỗ trợ tính năng IPS hoặc IDS giúp nhận diện và cảnh báo hoặc ngăn chặn các hành vi khai thác điểm yếu của máy chủ |
| 6 | Tính năng giám sát ứng dụng | Giám sát và có thể ngăn chặn bất kỳ file thực thi/ mã không nằm trong danh sách ứng dụng được biết |
| 7 | Quản trị tập trung | Có thể quản trị tập trung cho cả máy trạm và máy chủ |
| 8 | Cập nhật mẫu | Air-gap, cách ly với Internet |
| 9 | Sandboxing | Có thể tích hợp và gửi file đến hệ thống sandboxing để phân tích sâu |
| **V** | **Tính năng dành cho hệ thống sandboxing tập trung** | |
| 1 | Định dạng | Phần cứng cài đặt sẵn phần mềm hỗ trợ tính năng sandboxing, cho phép phân tích mã độc trong môi trường ảo hóa |
| 2 | Tính năng sandboxing | Cho phép tùy chỉnh sandboxing (cấu hình sandbox, driver, phần mềm …) |
| 3 | Khả năng phân tích | Hỗ trợ phân tích tối thiểu 38.000 sample/ngày |
| 4 | Số lượng Sanbox hỗ trợ | Hỗ trợ tối thiểu 50 Sandboxes trong một thiết bị phần cứng |
| 5 | Thiết bị | - Cấu hình phần cứng:<br>+ Hỗ trợ ≥ 02 ổ cứng 4TB chạy tối thiểu RAID1 hoặc cao hơn;<br>+ Có sẵn ≥ 01 cổng quản trị và ≥ 02 cổng mạng data 10/100/1000 base-T RJ45. |
| **VI** | **Tính năng dành cho hệ thống giám sát bất thường mạng** | |
| 1 | Định dạng | Phần cứng cài đặt sẵn phần mềm hỗ trợ tính năng giám sát các tấn công mạng có chủ đích, các mối đe dọa nâng cao, ransomware |
| 2 | Khả năng triển khai, tích hợp với network hiện hữu | Out-of-band monitor (SPAN/Mirror) |
| 3 | Khả năng giám sát giao thức mạng | Hỗ trợ giám sát hơn 100 giao thức mạng khác nhau |
| 4 | Hỗ trợ giao thức mạng OT | Protocol: SCADA, DNP3, MODBUS-TCP, MODBUS-UDP, IEC104,… |
| 5 | Hỗ trợ giao thức nền | HTTP, DNS, FTP, SMTP, SMB, ICMP, RDP, … |
| 6 | Thiết bị | - Cấu hình phần cứng:<br>+ RAM (Random Access Memory) ≥ 32GB;<br>+ Hỗ trợ ≥2 ổ cứng 2 TB chạy RAID1 hoặc cao hơn;<br>+ Có sẵn≥ 4 cổng 10/100/1000 base-T RJ45. |
| **VII** | **Tính năng dành cho hệ thống tương quan bất thường mạng** | |
| 1 | Định dạng | Phần mềm hoặc phần cứng có cài đặt sẵn phần mềm |
| 2 | Tính năng | Tương quan dữ liệu phát hiện bất thường mạng từ hệ thống giám sát bất thường mạng (mục VI) hoặc từ hệ thống network sensor. Cung cấp trực quan phân tích mối đe dọa theo thời gian thực. |
| 3 | Đồ thị tương quan | Hỗ trợ đồ thị trực quan (correlation graph/investigation graph) thể hiện sự tương quan giữa các sự kiện với nhau. |

| B | Bản quyền và hỗ trợ kỹ thuật |
|---|---|
| 1 | - Bản quyền hệ thống, bảo hành và hỗ trợ kỹ thuật chính hãng: ≥ 36 tháng.<br>- Tiêu chuẩn bảo hành 24x7x4.<br>- Hỗ trợ xử lý sự cố trong vòng 4 tiếng.<br>- Đối tác định kì On-site kiểm tra tình trạng thiết bị 3 tháng 1 lần của nhà cung cấp. |
| 2 | - Bản quyền phần mềm hệ thống quản trị mối đe dọa tập trung:<br>+ Số lượng: 350 thiết bị đầu cuối.<br>- Bản quyền phần mềm bảo vệ phòng chống mã độc dành cho máy trạm:<br>+ Số lượng: 310 thiết bị đầu cuối.<br>- Bản quyền phần mềm bảo vệ phòng chống mã độc dành cho máy chủ:<br>+ Số lượng: 40 thiết bị đầu cuối.<br>- Bản quyền phần mềm hệ thống tương quan bất thường mạng:<br>+ Băng thông: ≥ 1Gbps<br>+ Không giới hạn thiết bị đầu cuối.<br>- Bản quyền phần mềm dành cho hệ thống giám sát bất thường mạng:<br>+ Băng thông: ≥ 500Mbps<br>+ Không giới hạn thiết bị đầu cuối.<br>+ Số lượng: 01 thiết bị.<br>- Bản quyền phần mềm dành cho hệ thống sandboxing tập trung:<br>+ Số lượng: 01 thiết bị. |
| C | **Dịch vụ triển khai** |
| 1 | - Thực hiện trực tiếp tại Tổng công ty và 41 trạm biến áp tại TP.HCM<br>- Triển khai khảo sát, thiết kế, cài đặt và cấu hình hệ thống giám sát an toàn thông tin (phần mềm và thiết bị).<br>- Xây dựng các kịch bản tích hợp và vận hành trong hệ thống OT.<br>- Cung cấp các phụ kiện SFP, dây nhảy… và các vật tư cần thiết khác trong quá trình triển khai lắp đặt, cài đặt và cấu hình.<br>- Đào tạo hướng dẫn sử dụng toàn bộ hệ thống. |

### 1.3. Các yêu cầu khác

- Thực hiện trực tiếp tại Tổng công ty và 41 trạm biến áp tại TP.HCM.

- Triển khai khảo sát, thiết kế, cài đặt và cấu hình hệ thống giám sát an toàn thông tin (phần mềm và thiết bị).

- Xây dựng các kịch bản tích hợp và vận hành trong hệ thống OT.

- Cung cấp các phụ kiện SFP, SFP+, dây nhảy,… và các vật tư cần thiết khác trong quá trình triển khai lắp đặt, cài đặt và cấu hình.

- Đào tạo hướng dẫn sử dụng toàn bộ hệ thống.

- Khả năng đáp ứng và bảo mật an toàn thông tin:

- Đảm bảo kết nối với các hệ thống hiện tại và hoạt động ổn định.

- An toàn bảo mật thông tin: Đảm bảo cập nhật các bản vá lỗi, đảm bảo an toàn thông tin, tính bảo mật, toàn vẹn dữ liệu cho các hệ thống công nghệ thông tin của TCT.

- Bảo hành, cập nhật các bản vá: 36 tháng trong suốt thời gian của hợp đồng.

- Kiểm tra, bảo trì và tối ưu thiết bị/hệ thống định kỳ 3 tháng/1 lần.

- Cử cán bộ hỗ trợ quản lý vận hành, xử lý sự cố theo chế độ 24/7.

## Mục 2. Bản vẽ

- E-HSMT này không có bản vẽ kèm theo.

**Mục 3. Kiểm tra và thử nghiệm**

- Hàng hóa và dịch vụ phải được kiểm tra và thử nghiệm trước khi đưa vào cấu hình lắp đặt sử dụng.

- Nhà thầu phải tiến hành tất cả các thử nghiệm, kiểm tra đối với hàng hóa, dịch vụ liên quan và chịu toàn bộ chi phí thử nghiệm, kiểm tra.

- Chủ đầu tư có quyền từ chối bất kỳ hàng hóa, bộ phận hàng hóa nào không đáp ứng yêu cầu trong các buổi kiểm tra, thử nghiệm hoặc không phù hợp với đặc tính kỹ thuật theo hợp đồng.