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

- Tên dự án: Hệ thống phát hiện sớm hành vi, các mối nguy hại và phòng chống tấn công.

- Tên gói thầu: Hệ thống phát hiện sớm hành vi, các mối nguy hại và phòng chống tấn công.

- Địa điểm thực hiện dự án: Thiết bị, phần mềm của dự án được triển khai lắp đặt tại Trung tâm dữ liệu (DC) 72 Hai Bà Trưng, phường Sài Gòn, TP.HCM

STT	Tên VTTB	Mô tả	Đơn vị tính	Số lượng	Thời gian thực hiện gói thầu	Ghi chú
I	**HỆ THỐNG PHÁT HIỆN SỚM HÀNH VI, CÁC MỐI NGUY HẠI VÀ PHÒNG CHỐNG TẤN CÔNG**					
1	Hệ thống phát hiện sớm hành vi và các mối nguy hại	**Phần cứng chuyên dụng Hệ thống phát hiện sớm hành vi và các mối nguy hại phát hiện sớm các cuộc tấn công, hỗ trợ:** - Tối thiểu 48GB RAM, 2x 1TB HDD. - Hỗ trợ tối thiểu 20 máy ảo mồi nhử (bao gồm sẵn bản quyền Windows cho 10 máy ảo). - Hỗ trợ các loại máy ảo mồi nhử trên các hệ điều hành sau: Windows (các phiên bản 7, 10, 11,..), Windows Server (2016, 2019, 2022,..), Ubuntu, CentOS, Red Hat, macOS,... - Hỗ trợ các loại dịch vụ chạy trên máy ảo mồi nhử: SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, Telnet, FTP, TFTP, SNMP, RTSP, UPnP, CDP, TCP port listener, SMTP, RADIUS, MySQL, MQTT, SIP, XMPP, 3GPP, B.BRAUN, VNC, IP Camera-WEB. - Giải pháp phải có khả năng tích hợp với Hệ thống phòng	Bộ	01	Trong vòng 90 ngày kể từ ngày hợp đồng có hiệu lực, trong đó: •Thời gian cung cấp, nghiệm thu hàng hóa: trong vòng 60 ngày kể từ ngày hợp đồng có hiệu lực. •Thời gian triển khai, nghiệm thu bàn giao sản phẩm: trong vòng 90 ngày kể từ ngày hợp đồng có hiệu lực	

		chống tấn công nâng cao chào tại mục II để phân tích các phần mềm độc hại. - Tích hợp với thiết bị Tường lửa hiện có để cách ly, cấm IP và khả năng cách ly tùy thuộc vào mức độ nghiêm trọng của sự kiện. - Bản quyền phần mềm các tính năng mồi nhử để phát hiện sớm các cuộc tấn công và phòng chống khai thác (Anti-Reconnaissance & Anti-Exploit, AntiVirus, IPS, Web Filtering) cho 40 VLAN hoặc 10.000 địa chỉ IP trong 03 năm. - Bảo hành và hỗ trợ kỹ thuật 24x7 chính hãng trong 03 năm.				
2	Hệ thống phòng chống tấn công nâng cao	**Phần cứng chuyên dụng Sandbox phòng chống các cuộc tấn công nâng cao:** - Có khả năng phân tích mã độc dựa trên Sandbox Engine và AI Engine. - Hỗ trợ lên tới 14 máy ảo Sandbox với ít nhất 10 máy có sẵn bản quyền Windows. - Tích hợp với giải pháp Hệ thống phát hiện sớm hành vi và các mối nguy hại trong cùng dự án để phân tích các phần mềm độc hại chưa được biết đến để phát hiện sớm các cuộc tấn công nâng cao. - Bản quyền phần mềm các tính năng Sandbox Engine, AI Engine, Threat Intelligence (IOC), Industrial Security (OT), Anti-Phishing theo thời gian thực, các tính năng phòng chống tấn công (Antivirus, IPS, Web Filtering) trong 03 năm. - Bảo hành và hỗ trợ kỹ thuật 24x7 chính hãng trong 03 năm.	Bộ	01		
Hệ thống trọn gói bao gồm: Phụ kiện để kết nối vào hệ thống hiện hữu của EVNSPC (Các module quang, dây nhảy quang, dây cáp mạng…). Công tác triển khai lắp đặt thiết bị và cấu hình, tối ưu hóa chính sách, hoạch định chính sách cho các thiết bị và giải pháp được trang bị trong dự án, Đào tạo chuyển giao công nghệ, hướng dẫn quản trị vận hành, troubleshoot hệ thống.						

1.2. Yêu cầu về kỹ thuật: Thông số kỹ thuật của hàng hóa và dịch vụ liên quan phải đáp ứng theo Tập 3 – Yêu cầu kỹ thuật

1.3. Các yêu cầu khác

- Đáp ứng theo Hồ sơ yêu cầu kỹ thuật đính kèm.

- Đánh giá chất lượng VTTB trong giai đoạn vận hành: các VTTB sau khi được mua sắm, lắp đặt sẽ tiếp tục được đánh giá chất lượng theo quy định của EVN trong quá trình vận hành, bao gồm cả giai đoạn bảo hành và sau bảo hành.

Mục 2. Bản vẽ: Không có

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có: Theo E-ĐKC 21.1 – Điều kiện cụ thể hợp đồng

TẬP 3 – YÊU CẦU KỸ THUẬT

I. PHẠM VI CUNG CẤP:

STT	Tên VTTB	Mô tả	Đơn vị tính	Số lượng
I	**HỆ THỐNG PHÁT HIỆN SỚM HÀNH VI, CÁC MỐI NGUY HẠI VÀ PHÒNG CHỐNG TẤN CÔNG**			
1	Hệ thống phát hiện sớm hành vi và các mối nguy hại	**Phần cứng chuyên dụng Hệ thống phát hiện sớm hành vi và các mối nguy hại phát hiện sớm các cuộc tấn công, hỗ trợ:** - Tối thiểu 48GB RAM, 2x 1TB HDD. - Hỗ trợ tối thiểu 20 máy ảo mồi nhử (bao gồm sẵn bản quyền Windows cho 10 máy ảo). - Hỗ trợ các loại máy ảo mồi nhử trên các hệ điều hành sau: Windows (các phiên bản 7, 10, 11,..), Windows Server (2016, 2019, 2022,..), Ubuntu, CentOS, Red Hat, macOS,... - Hỗ trợ các loại dịch vụ chạy trên máy ảo mồi nhử: SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, Telnet, FTP, TFTP, SNMP, RTSP, UPnP, CDP, TCP port listener, SMTP, RADIUS, MySQL, MQTT, SIP, XMPP, 3GPP, B.BRAUN, VNC, IP Camera-WEB. - Giải pháp phải có khả năng tích hợp với Hệ thống phòng chống tấn công nâng cao chào tại mục II để phân tích các phần mềm độc hại. - Tích hợp với thiết bị Tường lửa hiện có để cách ly, cấm IP và khả năng cách ly tùy thuộc vào mức độ nghiêm trọng của sự kiện. - Bản quyền phần mềm các tính năng mồi nhử để phát hiện sớm các cuộc tấn công và phòng chống khai thác (Anti-Reconnaissance & Anti-Exploit, AntiVirus, IPS, Web Filtering) cho 40 VLAN hoặc 10.000 địa chỉ IP trong 03 năm.	Bộ	01

		- Bảo hành và hỗ trợ kỹ thuật 24x7 chính hãng trong 03 năm.		
2	Hệ thống phòng chống tấn công nâng cao	**Phần cứng chuyên dụng Sandbox phòng chống các cuộc tấn công nâng cao:** - Có khả năng phân tích mã độc dựa trên Sandbox Engine và AI Engine. - Hỗ trợ lên tới 14 máy ảo Sandbox với ít nhất 10 máy có sẵn bản quyền Windows. - Tích hợp với giải pháp Hệ thống phát hiện sớm hành vi và các mối nguy hại trong cùng dự án để phân tích các phần mềm độc hại chưa được biết đến để phát hiện sớm các cuộc tấn công nâng cao. - Bản quyền phần mềm các tính năng Sandbox Engine, AI Engine, Threat Intelligence (IOC), Industrial Security (OT), Anti-Phishing theo thời gian thực, các tính năng phòng chống tấn công (Antivirus, IPS, Web Filtering) trong 03 năm. - Bảo hành và hỗ trợ kỹ thuật 24x7 chính hãng trong 03 năm.	Bộ	01
Hệ thống trọn gói bao gồm: Phụ kiện để kết nối vào hệ thống hiện hữu của EVNSPC (Các module quang, dây nhảy quang, dây cáp mạng...). Công tác triển khai lắp đặt thiết bị và cấu hình, tối ưu hóa chính sách, hoạch định chính sách cho các thiết bị và giải pháp được trang bị trong dự án, Đào tạo chuyển giao công nghệ, hướng dẫn quản trị vận hành, troubleshoot hệ thống.				

II. YÊU CẦU VỀ ĐẶC TÍNH KỸ THUẬT:

STT	Mô tả	Yêu cầu kỹ thuật
A	**Yêu cầu chung:**	
1	Yêu cầu về Phương án triên khai	Sau khi ký hợp đồng nhà thầu khảo sát hiện trạng phần cứng, phần mềm hiện hữu, xây dựng phương án triển khai dự án trình cho Chủ đầu tư phê duyệt để triển khai.
2	Yêu cầu về triển khai	Nhà thầu kiểm tra hiện trạng hệ thống, thực hiện cấu hình triển khai Hệ thống phát hiện sớm hành vi, các mối nguy hại và phòng chống tấn công, đảm bảo an toàn ổn định khi tích hợp vào hệ thống hiện hữu của EVNSPC. Nhân sự của nhà thầu thực hiện cài đặt cấu hình triển khai cho Hệ thống phát hiện sớm hành vi, các mối nguy hại và

		phòng chống tấn công cho Tổng công ty Điện lực miền Nam phải có chứng chỉ của hãng về thiết bị bảo mật.
3	Yêu cầu về Bảo hành	Các đơn vị cung cấp sản phẩm và dịch vụ cần có trung tâm bảo hành trên lãnh thổ Việt Nam; Các đơn vị cung cấp sản phẩm và dịch vụ cần phải có cam kết chi tiết về thời gian bảo hành như sau: cam kết có mặt tại trụ sở, nơi có sự cố (trong trường hợp không thể giải quyết từ xa) trong vòng 04 giờ làm việc khi nhận được yêu cầu về sự cố kỹ thuật; Các đơn vị cung cấp sản phẩm và dịch vụ cần phải luôn có đội ngũ kỹ thuật riêng của mình để thực hiện việc bảo hành (có cung cấp số điện thoại nóng và địa chỉ để liên hệ).
4	Yêu cầu cho hãng sản xuất thiết bị	Có cam kết của hãng sản xuất về việc tiếp tục cung cấp dịch vụ hỗ trợ theo tiêu chuẩn sau thời gian kết thúc bảo hành và sẵn sàng cung cấp cho Chủ đầu tư khi có yêu cầu.
		Cam kết của nhà sản xuất thiết bị cung cấp trong gói thầu không chứa mã độc.
5	Yêu cầu về đào tạo và chuyển giao công nghệ	+ Tổ chức đào tạo hướng dẫn vận hành các hệ thống liên quan trong dự án cho 08 học viên trong 02 ngày (Lý thuyết 01 ngày, Thực hành 01 ngày). + Nhà thầu cung cấp thiết bị sẽ lập kế hoạch đào tạo cho các đối tượng do chủ đầu tư cung cấp danh sách các cán bộ quản trị, vận hành hệ thống. + Nhà thầu có trách nhiệm xây dựng tài liệu các quy trình cài đặt, triển khai hệ thống, quy trình quản trị vận hành hệ thống. + Nhà thầu sẽ cung cấp nội dung và tài liệu hướng dẫn cài đặt/ sử dụng cho các đối tượng tham gia đào tạo. + Nội dung đào tạo: Nhà thầu soạn thảo tài liệu đào tạo và trình cho Chủ đầu tư xem xét trước khi tổ chức đào tạo. Phạm vi đào tạo về các thiết bị được đầu tư trong dự án (quản trị, vận hành, trouble shoot, …).
6	Điều kiện nghiệm thu	+ Có biên bản xác nhận các thiết bị trong dự án vận hành ổn định trong vòng 72 giờ; + Hoàn thành đào tạo theo yêu cầu của chủ đầu tư. + Cung cấp tài liệu hoàn công cho chủ đầu tư.
B	**Yêu cầu chi tiết**	

I	**Hệ thống phát hiện sớm hành vi và các mối nguy hại:**	
1	Mã hiệu	Nhà thầu khai báo
2	Nhà sản xuất	Nhà thầu khai báo
3	Số lượng cổng kết nối	Tối thiểu 4 cổng GE RJ45 hoặc 4 cổng GE SFP
4	Ổ cứng	Tối thiểu 2 x 1TB
5	Bộ nhớ	Tối thiểu 48GB DDR4
6	Nguồn điện	Tối thiểu 02 nguồn
7	Số lượng máy ảo mồi nhử	Tối thiểu 20 máy ảo (bao gồm sẵn bản quyền Windows cho 10 máy ảo) hoặc 512 mồi nhử
8	Các loại máy ảo mồi nhử	Hỗ trợ các loại máy ảo mồi nhử trên các hệ điều hành sau: - Windows: 7, 10, 11,.. - Windows Server: 2016, 2019, 2022,.. - Linux: Ubuntu, CentOS, Redhat - MacOS - SSL-VPN, ESXI Decoy, IoT (Routers, Switch, Printers and IP-Camera), ERP, POS, SAP, Elastic Search, Tomcat, MySQL, MariaDB, SIP, XMPP, MQTT, 4G/5G 3GPP, Webmin, Citrix, Nginx…
9	Các loại dịch vụ chạy trên máy ảo mồi nhử	Hỗ trợ các loại dịch vụ chạy trên máy ảo mồi nhử: SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, Telnet, FTP, TFTP, SNMP, RTSP, UPnP, CDP, TCP port listener, SMTP, RADIUS, MySQL, MQTT, SIP, XMPP, 3GPP, B.BRAUN, VNC, IP Camera-WEB.
10	Thu thập dữ liệu mồi nhử	Giải pháp phải thu thập đầy đủ dữ liệu từ hệ thống mồi nhử (Decoy), bao gồm địa chỉ IP nguồn, thông tin đăng nhập được sử dụng để kết nối, các tiến trình khởi tạo và toàn bộ lịch sử lệnh CLI.
11	Đặt lại mồi nhử (Decoy Reset)	Giải pháp phải cho phép người dùng cấu hình chức năng tự động đưa máy ảo mồi nhử về trạng thái mặc định sau khi phát hiện sự cố và cho phép thiết lập được khoảng thời gian tự động reset
12	Phát hiện phần mềm độc hại	Mồi nhử phải có khả năng phát hiện phần mềm độc hại bị thả vào và gửi cảnh báo kịp thời.

13	Phát hiện phần mềm (ransomware)	Giải pháp cần có khả năng dẫn dụ ransomware mã hóa các tệp giả lập, qua đó kích hoạt cơ chế tự động cô lập và chặn hoạt động của điểm cuối bị nhiễm
14	Các tính năng ghi nhật ký sự kiện và báo cáo	Hỗ trợ hiển thị sự cố trong dòng thời gian
		Hỗ trợ nhóm các sự kiện thành chiến dịch (campaign)
		Hỗ trợ SYSLOG, Common Event Format (CEF)
15	Các tính năng tích hợp với các giải pháp an ninh mạng	Giải pháp phải có khả năng tích hợp với Hệ thống phòng chống tấn công nâng cao chào tại mục II để phân tích các phần mềm độc hại.
		Giải pháp phải có khả năng tích hợp với các giải pháp SIEM
		Giải pháp phải có khả năng tích hợp với thiết bị Tường lửa hiện có của EVNSPC (các hãng Checkpoint, Palo Alto, Fortinet) để cách ly thiết bị đầu cuối hoặc lưu lượng (traffic) độc hại
		Giải pháp phải có khả năng tích hợp với các giải pháp NAC để cách ly thiết bị đầu cuối
		Giải pháp hỗ trợ tích hợp với các công cụ của bên thứ ba thông qua API
		Giải pháp phải có khả năng xuất ra các chỉ dấu tấn công IOC (Indicators of Compromise) theo định dạng CSV và STIX
16	Các tính năng quản trị	Giải pháp phải có khả năng tùy chỉnh Dashboard quản trị
		Giải pháp phải có khả năng xác thực cho tài khoản quản trị với Radius
		Giải pháp phải có khả năng phần quyền cho tài khoản quản trị theo vai trò (RBAC)
		Hỗ trợ Mail service để gửi cảnh báo và report
17	Bản quyền phần mềm	Bản quyền phần mềm các tính năng mồi nhử để phát hiện sớm các cuộc tấn công và phòng chống khai thác (Anti-Reconnaissance & Anti-Exploit, AntiVirus, IPS, Web Filtering) cho 40 VLAN hoặc 10,000 địa chỉ IP/asset trong 03 năm.
18	Bảo hành và hỗ trợ kỹ thuật	Dịch vụ Bảo hành và hỗ trợ kỹ thuật chính hãng 24x7 trong 03 năm

19	Triển khai và đào tạo	Hệ thống trọn gói bao gồm: – Các vật tư thiết bị đấu nối đến hệ thống hiện hữu (Bao gồm tất cả module cần thiết để kết nối vào hệ thống hiện hữu). – Thực hiện, lắp đặt thiết bị, cài đặt, cấu hình, tích hợp và tối ưu hóa cho hệ thống. Triển khai các tính năng đã mua bản quyền kèm theo trong dự án. – Thực hiện đào tạo chuyển giao công nghệ, hướng dẫn vận hành đối với các thiết bị trong dự án.
II	**Hệ thống phòng chống tấn công nâng cao:**	
1	Mã hiệu	Nhà thầu khai báo
2	Nhà sản xuất	Nhà thầu khai báo
3	Số lượng cổng kết nối	Tối thiểu 4 cổng GE RJ45
4	Ổ cứng	Tối thiểu 960 GB
5	Nguồn	100 - 240V Nguồn AC
6	Số lượng máy ảo (VM) hỗ trợ	Tối thiểu 12 (bao gồm sẵn bản quyền Windows cho ít nhất 05 máy ảo)
7	Thông lượng bộ lọc Sandbox (file/giờ)	Tối thiểu 10,000
8	Yêu cầu về tính năng Sniffer	Thông lượng Sniffer tối thiểu 500 Mbps
		Phát hiện mối đe dọa mạng trong Chế độ Sniffer (Tính năng có sẵn của thiết bị hoặc tích hợp giải pháp cùng hãng, hoặc tích hợp giải pháp của hãng thứ 3): xác định các hoạt động và tấn công mạng của Botnet, truy cập URL độc hại.
9	Các tính năng phòng chống tấn công có chủ đích (Advance Threat Protection)	Phát hiện và bảo vệ trước các mối đe dọa, phần mềm độc hại chưa được biết đến bao gồm Ransomware
		Nhận dạng theo thời gian thực các trang web lừa đảo Zero-day bao gồm các trang web lưu trữ thư rác và phần mềm độc hại
10	Các tính năng bảo mật nâng cao	Tích hợp với bên thứ ba để kiểm tra thêm theo Yara rule
		Trích xuất URL được nhúng trong mã QR

		Cho phép quản lý file theo danh mục an toàn (whitelist) và danh mục cấm (blacklist) dựa vào checksum
		Quét URL được nhúng bên trong tập tin tài liệu
		Quét URL từ email và tập tin gửi lên
		Quét song song để chạy nhiều loại máy ảo riêng biệt
		Hỗ trợ AI/Machine Learning trong việc phân tích hành vi của mẫu Malware và Ransomware mới
11	Hỗ trợ quét loại tập tin	Windows Executables: .bat, .cmd, .dll, .exe, .msi, .ps1, .vbs, wsf Microsoft Office: Word, Excel, Powerpoint, Publisher Document/Email files: .eml, .pdf Android files: .apk Linux files: .elf MacOS files: .dmg Web files: .htm, html, .lnk Compress files: .7z, .ace, .arj, .bz2, .gz, .iso, .kgb, .lzh, .rar, .swf, .tar, .tgz, .upx, .xz, .z, .zip
12	Tính năng dự phòng	Hỗ trợ HA để tăng tính dự phòng
13	Các tính năng giám sát và báo cáo	Các tiện ích theo dõi cho việc kết nối và dịch vụ, trạng thái bản quyền, hiệu suất quét, tài nguyên hệ thống. Tiện ích theo dõi thời gian thực: hoạt động quét (theo thời gian); Top danh sách các máy chủ bị nhắm tới, phần mềm độc hại, lây nhiễm URL, tên miền được trả về nhiều nhất. Hiển thị sự kiện chi tiết: tên phần mềm độc hại, xếp hạng, loại malware, nguồn, đích, thời gian phát hiện và đường dẫn tải xuống
		Có thể tải báo cáo ở định dạng pdf. Hỗ trợ thiết lập để hệ thống tự động gửi báo cáo hàng tuần gửi tới danh sách email được chỉ định. Cập nhật nhật ký thường xuyên về trạng thái và hiệu suất hệ thống. Gửi Email thông báo khi phát hiện tập tin độc hại.
		Hỗ trợ MITRE ATT&CK. Hỗ trợ PCAP và các chỉ báo ở định dạng STIX 2.0.
14	Các tính năng quản trị	Hỗ trợ cấu hình GUI và CLI

		Tạo nhiều tài khoản quản trị Sao lưu và khôi phục cấu hình Tự động cập nhật signatures thường xuyên Tự động kiểm tra và tải xuống các bản VM mới Giám sát trạng thái máy ảo Xác thực cho tài khoản quản trị với Radius Kiểm tra tình trạng hệ thống và cảnh báo
15	Khả năng tích hợp	Tích hợp được với giải pháp "Hệ thống phát hiện sớm hành vi và các mối nguy hại" đã chào tại mục I.
16	Bản quyền phần mềm	Bản quyền phần mềm các tính năng Sandbox Engine, AI Engine, Threat Intelligence (IOC), Anti-Phishing theo thời gian thực, các tính năng phòng chống tấn công (Antivirus, IPS, Web Filtering) trong 03 năm.
17	Bảo hành và hỗ trợ kỹ thuật	Bảo hành và hỗ trợ kỹ thuật 24x7 chính hãng trong 03 năm.
18	Triển khai và đào tạo	Hệ thống trọn gói bao gồm: – Các vật tư thiết bị đấu nối đến hệ thống hiện hữu (Bao gồm tất cả module cần thiết để kết nối vào hệ thống hiện hữu). – Thực hiện, lắp đặt thiết bị, cài đặt, cấu hình, tích hợp và tối ưu hóa cho hệ thống. Triển khai các tính năng đã mua bản quyền kèm theo trong dự án. – Thực hiện đào tạo chuyển giao công nghệ, hướng dẫn vận hành đối với các thiết bị trong dự án.

III. TIÊU CHÍ ĐÁNH GIÁ VỀ MẶT KỸ THUẬT:

STT	Nội dung yêu cầu		Đánh giá		
	Mô tả	Yêu cầu tối thiểu	Đạt	Chấp nhận được	Không đạt
A	**Yêu cầu chung:**				
1	Yêu cầu về phương án triển khai	Sau khi ký hợp đồng nhà thầu khảo sát hiện trạng phần cứng, phần mềm hiện hữu, xây dựng phương án triển khai dự án trình cho Chủ đầu tư phê duyệt trước khi triển khai.	Có văn bản cam kết đáp ứng của Nhà thầu kèm theo hồ sơ dự thầu.		Không có văn bản cam kết đáp ưng của Nhà thầu kèm theo hồ sơ dự thầu.
2	Yêu cầu về triển khai	Nhà thầu kiểm tra hiện trạng hệ thống, thực hiện cấu hình triển khai Hệ thống phát hiện sớm hành vi, các mối nguy hại và phòng chống tấn công, đảm bảo an toàn ổn định khi tích hợp vào hệ thống hiện hữu của EVNSPC.	Có văn bản cam kết đáp ứng của Nhà thầu kèm theo hồ sơ dự thầu.		Không có văn bản cam kết đáp ưng của Nhà thầu kèm theo hồ sơ dự thầu.
		Nhân sự của nhà thầu thực hiện cài đặt cấu hình triển khai cho Hệ thống phát hiện sớm hành vi, các mối nguy hại và phòng chống tấn công cho Tổng công ty Điện lực miền Nam phải có chứng chỉ của hãng về thiết bị bảo mật.	Nhà thầu khai báo nhân sự triển khai và xuất trình chứng chỉ theo yêu cầu HSMT		Nhân sự triển khai của Nhà thầu không có chứng chỉ theo yêu cầu HSMT
3	Yêu cầu về bảo hành	Các đơn vị cung cấp sản phẩm và dịch vụ cần có Trung tâm bảo hành trên lãnh thổ Việt Nam; Các đơn vị cung cấp sản phẩm và dịch vụ cần phải có cam kết chi tiết về thời gian	Có văn bản cam kết đáp ứng của Nhà thầu kèm theo hồ sơ dự thầu.		Không có văn bản cam kết đáp ưng của Nhà thầu kèm theo hồ sơ dự thầu.

		bảo hành như sau: cam kết có mặt tại trụ sở, nơi có sự cố (trong trường hợp không thể giải quyết từ xa) trong vòng 04 giờ làm việc khi nhận được yêu cầu về sự cố kỹ thuật; Các đơn vị cung cấp sản phẩm và dịch vụ cần phải luôn có đội ngũ kỹ thuật riêng của mình để thực hiện việc bảo hành (có cung cấp số điện thoại nóng và địa chỉ để liên hệ).			
4	Yêu cầu cho hãng sản xuất thiết bị	Hãng sản xuất cam kết sẽ tiếp tục cung cấp dịch vụ hỗ trợ theo tiêu chuẩn khi Chủ đầu tư có nhu cầu mua bản quyền phần mềm và dịch vụ bảo hành cho thiết bị sau khi kết thúc thời gian bảo hành.	Có văn bản cam kết đáp ứng của hãng sản xuất kèm theo hồ sơ dự thầu.		Không có văn bản cam kết đáp của hãng sản xuất kèm theo hồ sơ dự thầu.
		Hãng sản xuất cam kết thiết bị cung cấp trong gói thầu không chứa mã độc.	Có văn bản cam kết đáp ứng của hãng sản xuất kèm theo hồ sơ dự thầu.		Không có văn bản cam kết đáp của hãng sản xuất kèm theo hồ sơ dự thầu.
5	Đào tạo	+ Tổ chức đào tạo hướng dẫn vận hành các hệ thống liên quan trong dự án 08 học viên trong 02 ngày (Lý thuyết 01 ngày, Thực hành 01 ngày). + Nhà thầu cung cấp thiết bị sẽ lập kế hoạch đào tạo cho các đối tượng do chủ đầu tư cung cấp danh sách các cán bộ quản trị, vận hành hệ thống.	Có văn bản cam kết đáp ứng của Nhà thầu kèm theo hồ sơ dự thầu.		Không có văn bản cam kết đáp ưng của Nhà thầu kèm theo hồ sơ dự thầu.

		+ Nhà thầu có trách nhiệm xây dựng tài liệu các quy trình cài đặt, triển khai hệ thống, quy trình quản trị vận hành hệ thống. + Nhà thầu sẽ cung cấp nội dung và tài liệu hướng dẫn cài đặt/ sử dụng cho các đối tượng tham gia đào tạo. + Nội dung đào tạo: Nhà thầu soạn thảo tài liệu đào tạo và trình cho Chủ đầu tư xem xét trước khi tổ chức đào tạo. Phạm vi đào tạo về các thiết bị được đầu tư trong dự án (quản trị, vận hành, trouble shoot, …).			
6	Điều kiện nghiệm thu	+ Có biên bản xác nhận các thiết bị trong dự án vận hành ổn định trong vòng 72 giờ; + Hoàn thành đào tạo theo yêu cầu của chủ đầu tư. + Cung cấp tài liệu hoàn công cho chủ đầu tư.	Có văn bản cam kết đáp ứng của Nhà thầu kèm theo hồ sơ dự thầu.		Không có văn bản cam kết đáp ưng của Nhà thầu kèm theo hồ sơ dự thầu.
A	**Yêu cầu chi tiết**				
I	**Hệ thống phát hiện sớm hành vi và các mối nguy hại**				
1	Mã hiệu	Nhà thầu khai báo	Như yêu cầu		Nhà thầu không khai báo

2	Nhà sản xuất	Nhà thầu khai báo	Như yêu cầu		Nhà thầu không khai báo
3	Số lượng cổng kết nối	Tối thiểu 4 cổng GE RJ45 và 4 cổng GE SFP	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
4	Ổ cứng	Tối thiểu 2 x 1TB	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
5	Bộ nhớ	Tối thiểu 48GB DDR4	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
6	Nguồn điện	Tối thiểu 02 nguồn	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
7	Số lượng máy ảo mồi nhử	Tối thiểu 20 máy ảo (bao gồm sẵn bản quyền Windows cho 10 máy ảo) hoặc 512 mồi nhử	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
8	Các loại máy ảo mồi nhử	Hỗ trợ các loại máy ảo mồi nhử trên các hệ điều hành sau: - Windows: 7, 10, 11,.. - Windows Server: 2016, 2019, 2022,..	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)

		- Linux: Ubuntu, CentOS, Redhat - MacOS - SSL-VPN, ESXI Decoy, IoT (Routers, Switch, Printers and IP-Camera), ERP, POS, SAP, Elastic Search, Tomcat, MySQL, MariaDB, SIP, XMPP, MQTT, 4G/5G 3GPP, Webmin, Citrix, Nginx…			
9	Các loại dịch vụ chạy trên máy ảo mồi nhử	Hỗ trợ các loại dịch vụ chạy trên máy ảo mồi nhử: SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, Telnet, FTP, TFTP, SNMP, RTSP, UPnP, CDP, TCP port listener, SMTP, RADIUS, MySQL, MQTT, SIP, XMPP, 3GPP, B.BRAUN, VNC, IP Camera-WEB.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
10	Thu thập dữ liệu mồi nhử	Giải pháp phải thu thập đầy đủ dữ liệu từ hệ thống mồi nhử (Decoy), bao gồm địa chỉ IP nguồn, thông tin đăng nhập được sử dụng để kết nối, các tiến trình khởi tạo và toàn bộ lịch sử lệnh CLI.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
11	Đặt lại mồi nhử (Decoy Reset)	Giải pháp phải cho phép người dùng cấu hình chức năng tự động đưa máy ảo mồi nhử về trạng thái mặc định sau khi phát hiện sự cố và cho phép thiết lập được khoảng thời gian tự động reset	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
12	Phát hiện phần mềm độc hại	Mồi nhử phải có khả năng phát hiện phần mềm độc hại bị thả vào và gửi cảnh báo kịp thời.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)

13	Phát hiện phần mềm (ransomware)	Giải pháp cần có khả năng dẫn dụ ransomware mã hóa các tệp giả lập, qua đó kích hoạt cơ chế tự động cô lập và chặn hoạt động của điểm cuối bị nhiễm	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
14	Các tính năng ghi nhật ký sự kiện và báo cáo	Hỗ trợ hiển thị sự cố trong dòng thời gian	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
		Hỗ trợ nhóm các sự kiện thành chiến dịch (campaign)			
		Hỗ trợ SYSLOG, Common Event Format (CEF)			
15	Các tính năng tích hợp với các giải pháp an ninh mạng	Giải pháp phải có khả năng tích hợp với Hệ thống phòng chống tấn công nâng cao chào tại mục II để phân tích các phần mềm độc hại.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
		Giải pháp phải có khả năng tích hợp với các giải pháp SIEM			
		Giải pháp phải có khả năng tích hợp với thiết bị Tường lửa hiện có của EVNSPC (các hãng Checkpoint, Palo Alto, Fortinet) để cách ly thiết bị đầu cuối hoặc lưu lượng (traffic) độc hại			
		Giải pháp phải có khả năng tích hợp với các giải pháp NAC để cách ly thiết bị đầu cuối			
		Giải pháp hỗ trợ tích hợp với các công cụ của bên thứ ba thông qua API			
		Giải pháp phải có khả năng xuất ra các chỉ dấu tấn công IOC (Indicators of			

		Compromise) theo định dạng CSV và STIX			
16	Các tính năng quản trị	Giải pháp phải có khả năng tùy chỉnh Dashboard quản trị Giải pháp phải có khả năng xác thực cho tài khoản quản trị với Radius Giải pháp phải có khả năng phân quyền cho tài khoản quản trị theo vai trò (RBAC) Hỗ trợ Mail service để gửi cảnh báo và report	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
17	Bản quyền phần mềm	Bản quyền phần mềm các tính năng mồi nhử để phát hiện sớm các cuộc tấn công và phòng chống khai thác (Anti-Reconnaissance & Anti-Exploit, AntiVirus, IPS, Web Filtering) cho 40 VLAN hoặc 10,000 địa chỉ IP/asset trong 03 năm.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
18	Bảo hành và hỗ trợ kỹ thuật	Dịch vụ Bảo hành và hỗ trợ kỹ thuật chính hãng 24x7 trong 03 năm	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
19	Triển khai và đào tạo	Hệ thống trọn gói bao gồm: – Các vật tư thiết bị đấu nối đến hệ thống hiện hữu (Bao gồm tất cả module cần thiết để kết nối vào hệ thống hiện hữu).	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)

		– Thực hiện, lắp đặt thiết bị, cài đặt, cấu hình, tích hợp và tối ưu hóa cho hệ thống. Triển khai các tính năng đã mua bản quyền kèm theo trong dự án. – Thực hiện đào tạo chuyển giao công nghệ, hướng dẫn vận hành đối với các thiết bị trong dự án.			
II	**Hệ thống phòng chống tấn công nâng cao**				
1	Mã hiệu	Nhà thầu khai báo	Như yêu cầu		Nhà thầu không khai báo
2	Nhà sản xuất	Nhà thầu khai báo	Như yêu cầu		Nhà thầu không khai báo
3	Số lượng cổng kết nối	Tối thiểu 4 cổng GE RJ45	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
4	Ổ cứng	Tối thiểu 960 GB	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
5	Nguồn	100 - 240V Nguồn AC	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)

6	Số lượng máy ảo (VM) hỗ trợ	Tối thiểu 12 (bao gồm sẵn bản quyền Windows cho ít nhất 05 máy ảo)	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
7	Thông lượng bộ lọc Sandbox (file/giờ)	Tối thiểu 10,000	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
8	Yêu cầu về tính năng Sniffer	Thông lượng Sniffer tối thiểu 500 Mbps Phát hiện mối đe dọa mạng trong Chế độ Sniffer (Tính năng có sẵn của thiết bị hoặc tích hợp giải pháp cùng hãng, hoặc tích hợp giải pháp của hãng thứ 3): xác định các hoạt động và tấn công mạng của Botnet, truy cập URL độc hại.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
9	Các tính năng phòng chống tấn công có chủ đích (Advance Threat Protection)	Phát hiện và bảo vệ trước các mối đe dọa, phần mềm độc hại chưa được biết đến bao gồm Ransomware Nhận dạng theo thời gian thực các trang web lừa đảo Zero-day bao gồm các trang web lưu trữ thư rác và phần mềm độc hại	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
10	Các tính năng bảo mật nâng cao	Tích hợp với bên thứ ba để kiểm tra thêm theo Yara rule Trích xuất URL được nhúng trong mã QR Cho phép quản lý file theo danh mục an toàn (whitelist) và danh mục cấm (blacklist) dựa vào checksum	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)

		Quét URL được nhúng bên trong tập tin tài liệu			
		Quét URL từ email và tập tin gửi lên			
		Quét song song để chạy nhiều loại máy ảo riêng biệt			
		Hỗ trợ AI/Machine Learning trong việc phân tích hành vi của mẫu Malware và Ransomware mới			
11	Hỗ trợ quét loại tập tin	Windows Executables: .bat, .cmd, .dll, .exe, .msi, .ps1, .vbs, wsf Microsoft Office: Word, Excel, Powerpoint, Publisher Document/Email files: .eml, .pdf Android files: .apk Linux files: .elf MacOS files: .dmg Web files: .htm, html, .lnk Compress files: .7z, .ace, .arj, .bz2, .gz, .iso, .kgb, .lzh, .rar, .swf, .tar, .tgz, .upx, .xz, .z, .zip	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
12	Tính năng dự phòng	Hỗ trợ HA để tăng tính dự phòng	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)

13	Các tính năng giám sát và báo cáo	Các tiện ích theo dõi cho việc kết nối và dịch vụ, trạng thái bản quyền, hiệu suất quét, tài nguyên hệ thống. Tiện ích theo dõi thời gian thực: hoạt động quét (theo thời gian); Top danh sách các máy chủ bị nhắm tới, phần mềm độc hại, lây nhiễm URL, tên miền được trả về nhiều nhất. Hiển thị sự kiện chi tiết: tên phần mềm độc hại, xếp hạng, loại malware, nguồn, đích, thời gian phát hiện và đường dẫn tải xuống	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
		Có thể tải báo cáo ở định dạng pdf. Hỗ trợ thiết lập để hệ thống tự động gửi báo cáo hàng tuần gửi tới danh sách email được chỉ định. Cập nhật nhật ký thường xuyên về trạng thái và hiệu suất hệ thống. Gửi Email thông báo khi phát hiện tập tin độc hại.			
		Hỗ trợ MITRE ATT&CK. Hỗ trợ PCAP và các chỉ báo ở định dạng STIX 2.0.			
14	Các tính năng quản trị	Hỗ trợ cấu hình GUI và CLI Tạo nhiều tài khoản quản trị	Như yêu cầu (Có viện dẫn chương,		Không như yêu cầu (Không viện dẫn

		Sao lưu và khôi phục cấu hình Tự động cập nhật signatures thường xuyên Tự động kiểm tra và tải xuống các bản VM mới Giám sát trạng thái máy ảo Xác thực cho tài khoản quản trị với Radius Kiểm tra tình trạng hệ thống và cảnh báo	trang, mục tham chiếu)		chương, trang, mục tham chiếu)
15	Khả năng tích hợp	Tích hợp được với giải pháp "Hệ thống phát hiện sớm hành vi và các mối nguy hại" đã chào tại mục I.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
16	Bản quyền phần mềm	Bản quyền phần mềm các tính năng Sandbox Engine, AI Engine, Threat Intelligence (IOC), Anti-Phishing theo thời gian thực, các tính năng phòng chống tấn công (Antivirus, IPS, Web Filtering) trong 03 năm.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
17	Bảo hành và hỗ trợ kỹ thuật	Bảo hành và hỗ trợ kỹ thuật 24x7 chính hãng trong 03 năm.	Như yêu cầu (Có viện dẫn chương, trang, mục tham chiếu)		Không như yêu cầu (Không viện dẫn chương, trang, mục tham chiếu)
18	Triển khai và đào tạo	Hệ thống trọn gói bao gồm: – Các vật tư thiết bị đấu nối đến hệ thống hiện hữu (Bao gồm tất cả	Như yêu cầu (Có viện dẫn chương,		Không như yêu cầu (Không viện dẫn

		module cần thiết để kết nối vào hệ thống hiện hữu). – Thực hiện, lắp đặt thiết bị, cài đặt, cấu hình, tích hợp và tối ưu hóa cho hệ thống. Triển khai các tính năng đã mua bản quyền kèm theo trong dự án. – Thực hiện đào tạo chuyển giao công nghệ, hướng dẫn vận hành đối với các thiết bị trong dự án.	trang, mục tham chiếu)		chương, trang, mục tham chiếu)

IV.PHƯƠNG PHÁP ĐÁNH GIÁ YÊU CẦU KỸ THUẬT

- Phương pháp đánh giá chi tiết là sử dụng Tiêu chí Đạt/Không đạt
- Theo đó :
    - Một Nhà thầu được đánh giá là "ĐẠT" nếu : "ĐẠT" và/hoặc "CHẤP NHẬN ĐƯỢC" tất cả các tiêu chí.
    - Một Nhà thầu được đánh giá là "KHÔNG ĐẠT" nếu : "KHÔNG ĐẠT" một tiêu chí.