Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

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

Gói thầu: Cung cấp dịch vụ tổ chức diễn tập an toàn thông tin năm 2025;

Chủ đầu tư: Công ty Nhiệt điện Vĩnh Tân – Chi nhánh Tổng Công ty Phát điện 3 – Công ty cổ phần;

Địa điểm thực hiện: Nhà máy Nhiệt điện Vĩnh Tân 2, thôn Vĩnh Phúc, xã Vĩnh Hảo, tỉnh Lâm Đồng.

Thời gian thực hiện gói thầu: Trong vòng 05 ngày kể từ ngày hợp đồng có hiệu lực và nhà thầu nhận được thông báo của chủ đầu tư về thời gian bắt đầu công việc.

2. Mục tiêu công việc:

- Thuê đơn vị bồi dưỡng kiến thức nâng cao về ATTT và khảo sát xây dựng kích bản, tổ chức diễn tập;

- Tổ chức triển khai diễn tập cho đơn vị; họp rút kinh nghiệm từ công tác diễn tập.

3. Yêu cầu kỹ thuật của gói thầu:

Phạm vi công việc cần thực hiện như sau:

TT	Hạng mục công việc	Đơn vị tính	Khối lượng
1	Dịch vụ tổ chức diễn tập an toàn thông tin năm 2025	Trọn gói	1

Kế hoạch và kịch bản diễn tập:

STT	Nội dung	Nội dung chi tiết	Thời lượng
I. Bồi dưỡng, nâng cao kiến thức (01 ngày), số lượng tham dự: 10 người			
Ngày 1	Ứng dụng thao trường diễn tập An toàn thông tin ngành điện	- Bối cảnh an ninh mạng toàn cầu và Việt Nam. - Các lỗ hổng của tường lửa và hệ thống thông tin điện lực.	4 giờ

STT	Nội dung	Nội dung chi tiết	Thời lượng
		- Tấn công Phishing có khả năng thành công cao. - Các vụ tấn công nổi bật vào hệ thống điện. - Thực hành: ▪ Sử dụng thao trường an ninh mạng ▪ Ứng dụng thu thập thông tin ▪ Sử dụng các cộng cụ rà quét lỗ hổng ▪ Thử nghiệm khai thác lỗ hổng - Thảo luận nhóm: phân tích hiện trạng ▪ Thảo luận nhóm: phân tích hiện trạng thực tế tại NMNĐ Vĩnh Tân 2 ▪ Bảo mật mạng (Network security): o Bảo mật mạng với các tường lửa công nghiệp o Phân vùng mạng và mạng con o Bảo mật truy cập từ xa và VPN o Kiểm soát truy cập mạng (NAC) ▪ Bảo mật thiết bị đầu cuối (Endpoint security): o Danh sách ứng dụng cho phép o Quản lý bản vá cho OT o Phòng chống mã độc cho môi trường công nghiệp ▪ Giám sát và phát hiện: o Phân tích hành vi mạng o Ứng dụng SIEM công nghiệp o Honeypots trong OT o Threat Intelligence cho ICS ▪ Bảo vệ dữ liệu: o Chiến lược sao lưu và khôi phục o Mã hóa dữ liệu	

STT	Nội dung	Nội dung chi tiết	Thời lượng
	Quản lý rủi ro, giám sát và khôi phục hệ thống	- Quy trình đánh giá rủi ro cho ICS - Quản lý tài sản và thiết bị OT - Quản lý lỗ hổng/điểm yếu - Quy trình và kế hoạch phản ứng sự cố - Kế hoạch kinh doanh liên tục và khôi phục thảm họa - Đánh gia định kỳ và đảm bảo tuân thủ - Quy trình quản lý sự cố - Demo: các kỹ thuật tấn công phổ biến ▪ Tấn công Phishing và Social Engineering ▪ Tạo mã độc và lây nhiễm mã độc ▪ Kỹ thuật tấn công từ nội bộ ▪ Kỹ thuật tấn công APT - Thực hành: ▪ Xây dựng quy trình giám sát, phát hiện, phân tích và phản ứng sự cố ▪ Phân chia vai trò thực hiện khôi phục hệ thống ▪ Đánh giá và rút ra bài học sau sự cố	4 giờ
II. Diễn tập (01 ngày), số lượng tham dự: 10 người			
Ngày 2	Đội tấn công: Diễn tập tấn công Phishing và khai thác hệ thống ICS	*Môi trường diễn tập: Dùng các máy tính đã cài đặt sẵn các công cụ tấn công* - Máy ảo Kali Linux - Các công cụ và mã độc tự lập trình - Các script để khai thác tự động và tấn công Web Apps **Kịch bản diễn tập tấn công:** 1. Tấn công, khai thác điểm yếu và chiếm quyền điều khiển Firewall 2. Tấn công khai thác lỗ hổng ứng dụng Web 3. Lây nhiễm mã độc và thực hiện lan truyền từ IT sang OT network	4 giờ

STT	Nội dung	Nội dung chi tiết	Thời lượng
		4. Nhận diện thêm các ngõ ngách và leo thang đặc quyền 5. Cố gắng truy cập vào hệ thống SCADA	
	Blue Team: Diễn tập giám sát, phân tích, phản ứng sự cố và khôi phục hệ thống	*Môi trường diễn tập: Thao trường mô phỏng hệ thống điều khiển của nhà máy do đội ngũ kỹ thuật của nhà thầu thực hiện, kết hợp ý kiến chuyên môn từ bên mời thầu.* - Hệ thống mạng OT, IT - Máy chủ Historian ở DMZ (nếu cần thiết) - Máy HMI và các máy trạm giám sát - Các hệ thống OT và giám sát khác **Công cụ sử dụng để diễn tập giám sát:** - Các nền tảng SIEM (Splunk/Wazuh) - Các công cụ giám sát mạng - Tài liệu hay sổ tay hướng dẫn xử lý sự cố - Các công cụ giao tiếp nhóm diễn tập (Slack/Teams) **Kịch bản diễn tập giám sát và ứng cứu:** 1. Phát hiện các lưu lượng bất thường trong mạng ICS 2. Ghi nhận và quản lý sự cố 3. Phân loại sự cố và escalation 4. Giao tiếp ứng phó sự cố 5. Phân tích và xóa bỏ mã độc 6. Khôi phục hệ thống	

<u>Yêu cầu cụ thể</u>

a) Thành lập Ban Tổ chức và Đội diễn tập

- Ban Tổ chức diễn tập: Có nhiệm vụ chủ trì thực hiện tổ chức diễn tập thực chiến, giám sát các đội tham gia diễn tập, xử lý vi phạm, giải quyết các vướng mắc trong quá trình diễn tập và đánh giá kết quả diễn tập của các Đội Tấn công,

Đội Phòng thủ.

- Đội Tấn công: Thành viên Đội ứng cứu sự cố an toàn thông tin mạng Công ty Nhiệt Điện Vĩnh Tân phụ trách công nghệ thông tin, an toàn thông tin theo lựa chọn của Ban tổ chức thực hiện tấn công vào hệ thống theo giới hạn diễn tập của Ban tổ chức.

- Đội Phòng thủ: Dự kiến 03 đến 07 người, gồm: Lực lượng thường trực Đội ứng cứu sự cố an toàn thông tin mạng huy động lực lượng kỹ thuật hỗ trợ vận hành hệ thống SOC. Thực hiện bảo vệ mục tiêu tấn công vào hệ thống của Đội tấn công.

b) Giới hạn diễn tập

- Mục tiêu diễn tập: lựa chọn giả lập mô phỏng toàn bộ hệ thống hoặc một thành phần hệ thống điều khiển nhà máy.

- Ngưỡng tấn công:

+ Khi chiếm được quyền điều khiển mục tiêu diễn tập phải dừng cuộc tấn công hoặc chuyển phương án tấn công mới (nếu có); không tấn công leo thang đặc quyền hệ thống khi chưa có được sự chấp thuận của Ban Tổ chức.

+ Không tấn công từ chối dịch vụ; phá hủy hệ thống hoặc dữ liệu; khởi động lại hoặc tắt máy chủ dịch vụ; khai thác lỗ hổng bảo mật để phát tán mã độc; đánh cắp, chia sẻ làm lộ lọt thông tin; sử dụng các loại mã độc mã hóa dữ liệu, đòi tiền chuộc và các loại tấn công khác để lại hậu quả về sau.

c) Hình thức và địa điểm tổ chức: Cuộc diễn tập được tổ chức theo hình thức bán tập trung:

- Việc tấn công mục tiêu được các Đội Tấn công thực hiện tại địa điểm diễn tập và trực tuyến qua Internet; việc bảo vệ mục tiêu được thực hiện theo hình thức tập trung và giám sát bảo vệ từ xa.

- Địa điểm diễn tập: Do Ban Tổ chức lựa chọn đảm bảo đủ điều kiện, cơ sở vật chất triển khai thực hiện các nội dung theo Kế hoạch.

d) Nhiệm vụ của Ban Tổ chức và các Đội tham gia diễn tập

- Ban Tổ chức:

+ Phổ biến các quy định diễn tập cho các Đội tham gia diễn tập nắm và thực hiện.

+ Triển khai nhiệm vụ cho Đội Tấn công và Đội Phòng thủ thực hiện trong thời gian diễn tập.

+ Xác định giới hạn và lựa chọn hệ thống thông tin diễn tập đảm bảo tính khả thi và an toàn thông tin khi triển khai thực hiện.

+ Giám sát các Đội, xử lý vi phạm, giải quyết các vướng mắc trong quá trình diễn tập.

+ Đánh giá kết quả diễn tập của các Đội Tấn công, Đội Phòng thủ.

+ Công bố và báo cáo kết quả diễn tập cho Lãnh đạo Công ty.

- Đội Tấn công:

+ Tuân thủ ngưỡng tấn công đã được xác định trong giới hạn diễn tập.

+ Phân công vai trò, trách nhiệm mỗi thành viên trong đội thực hiện việc tấn công mục tiêu theo hướng dẫn và Quy định của Ban Tổ chức.

+ Tuân thủ theo thời gian diễn tập theo quy định của Ban Tổ chức.

+ Lưu vết hoặc đưa ra các bằng chứng tấn công.

+ Báo cáo về Ban Tổ chức phương pháp, tên công cụ và kết quả của việc tấn công theo các quy tắc: đúng thời hạn và bảo vệ kết quả báo cáo bằng việc mã hóa hoặc đặt mật khẩu.

- Đội Phòng thủ:

+ Phân công vai trò, trách nhiệm mỗi thành viên, nhóm liên quan thực hiện công tác phòng thủ theo hướng dẫn và quy định của Ban Tổ chức.

+ Được quyền sử dụng mọi biện pháp (kỹ thuật, quy trình, quy định) để bảo vệ mục tiêu, xử lý sự cố trong quá trình diễn tập.

+ Rà soát và thực thi tăng cường phương án giám sát hệ thống mục tiêu diễn tập thực chiến, phát hiện khi các hệ thống bị tấn công nằm ngoài giới hạn diễn tập.

+ Rà soát và thực thi tăng cường phương án dự phòng, sao lưu dữ liệu và hệ thống.

+ Lưu vết hoặc đưa ra các bằng chứng phòng ngừa, ngăn chặn các cuộc tấn công.

+ Báo cáo về Ban Tổ chức kết quả thực hiện phòng thủ theo các quy tắc:

đúng thời hạn và bảo vệ kết quả báo cáo bằng việc mã hóa hoặc đặt mật khẩu.

đ) Yêu cầu tổ chức diễn tập:

- Nhà thầu chịu trách nhiệm xây dựng thao trường diễn tập, cung cấp chiến thuật tấn công, khai thác lỗ hổng bảo mật trên mục tiêu diễn tập.

- Nhà thầu chịu trách nhiệm chuẩn bị hệ thống phục vụ diễn tập thực chiến trong hội trường đảm bảo quy mô 10 cán bộ tham dự trong 02 ngày, cụ thể:

+ Các Công cụ kiểm tra an toàn cho ứng dụng web; Công cụ quét lỗ hổng bảo mật; Công cụ hỗ trợ khai thác, tấn công lỗ hổng an toàn thông tin.

+ Máy chủ phục vụ đội tấn công.

+ Máy tính xách tay cho học viên (máy tính đã bao gồm các phần mềm phục vụ công tác diễn tập): tối thiểu 10 bộ/ngày.

+ Máy chiếu, màn chiếu: tối thiểu 02 máy/ngày.

- Nhà thầu chịu trách nhiệm cơ sở vật chất phục vụ diễn tập bao gồm:

+ Khu vực bồi dưỡng kiến thức, diễn tập: quy mô tối thiểu 10 người. Phòng Hội trường được thiết kế có đầy đủ ánh sáng ổn định, có bục phát biểu, biển chỉ dẫn. Nhà thầu chịu trách nhiệm về kỹ thuật trong suốt quá trình tổ chức diễn tập. Kê bàn ghế hợp lý, thuận lợi cho diễn tập.

+ Trang trí khu vực diễn tập: phông nền

+ Chi phí quà tặng các đội xuất sắc

+ Chi văn phòng phẩm: Tài liệu, giấy, bút, clear bag cho cán bộ tham dự

+ Chi nước uống, tea-break: 10 người trong 2 ngày

- Kết thúc diễn tập, nhà thầu chịu trách nhiệm xây dựng báo cáo diễn tập theo quy định.

e) Yêu cầu khác:

- Yêu cầu về địa điểm, thời gian tổ chức:

+ Địa điểm diễn tập: Chủ đầu tư lựa chọn địa điểm diễn tập.

+ Thời gian tổ chức: Thời gian diễn ra sự kiện sẽ được Chủ đầu tư cung cấp cho nhà thầu tối thiểu 05 ngày làm việc trước sự kiện được tổ chức. Trường hợp bất khả kháng phải lùi thời gian tổ chức, Chủ đầu tư sẽ thông báo cho nhà thầu tối

thiểu 03 ngày làm việc trước khi diễn ra sự kiện và 02 bên sẽ trao đổi thay đổi thời gian thực hiện, việc thay đổi thời gian này không tính là vi phạm.

Lưu ý: ***Chủ đầu tư mặc định dịch vụ trong gói thầu này có thuế suất GTGT tạm tính là 10% để có cơ sở so sánh giá chào thầu và hoàn thiện hợp đồng. Trường hợp nhà thầu chào thuế khác 10% thì Chủ đầu tư sẽ quy về cùng mặt bằng thuế tạm tính 10% để có cơ sở so sánh giá chào thầu. Thuế GTGT sẽ được điều chỉnh theo quy định của Nhà nước tại thời điểm xuất hóa đơn, thanh toán.***

4. Giấy phép tổ chức của nhà thầu

Nhà thầu phải có Giấy phép về kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng theo yêu cầu của Nghị định số 108/2016/NĐ-CP ngày 01/7/2016 về Quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng và phải đáp ứng tối thiểu điều kiện kinh doanh về dịch vụ ứng cứu sự cố an toàn thông tin mạng trong Giấy phép kinh doanh nêu trên.

5. Yêu cầu tiến độ thực hiện

Tiến độ thực hiện: Trong vòng 05 ngày kể từ ngày hợp đồng có hiệu lực và nhà thầu nhận được thông báo của chủ đầu tư về thời gian bắt đầu công việc.

6. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định nêu trên, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

7. Quy định về kiểm tra, nghiệm thu sản phẩm:

Trong vòng 15 ngày lịch kể từ ngày Bên B hoàn thành công việc theo yêu cầu mỗi đợt, các Bên ký hồ sơ nghiệm thu làm cơ sở thực hiện thủ tục thanh quyết toán theo quy định.