Số và ký hiệu: 193/KT-NB
Ngày ban hành: 14/05/2025

TỔNG CÔNG TY
ĐIỆN LỰC DẦU KHÍ VIỆT NAM - CTCP
BAN KỸ THUẬT

Số: /KT-NB
V/v: Đăng thông báo nhu cầu báo giá mua sắm, triển khai.

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

Hà Nội, ngày tháng năm 2025

Kính gửi: Văn phòng Tổng công ty

Hiện nay Tổng công ty Điện lực Dầu khí Việt Nam – CTCP (PV Power) đang có nhu cầu về việc thuê dịch vụ kiểm tra đánh giá, đảm bảo ATTT và hỗ trợ ứng cứu sự cố an ninh mạng. Ban Kỹ thuật kính đề nghị Văn phòng đăng thư mời quan tâm dịch vụ như sau:

(Phụ lục đính kèm)

Trân trọng cảm ơn./.

***Nơi nhận*:**
- Như trên;
- PTGĐ Phan Ngọc Hiền (để b/c);
- Trưởng Ban KT (để b/c);
- Lưu: KT (NTCT-01b).

***Đính kèm*:**
- Thư mời quan tâm.

KT. TRƯỞNG BAN KỸ THUẬT
PHÓ TRƯỞNG BAN

Nguyễn Xuân Thành

Số và ký hiệu: 193/KT-NB
Ngày ban hành: 14/05/2025

THƯ MỜI QUAN TÂM

(Kèm theo Công văn số /KT-NB ngày tháng 05 năm 2025)

I. Mô tả nhu cầu:

Tổng công ty Điện lực Dầu khí Việt Nam – CTCP (PV Power) hiện có nhu cầu về việc thuê dịch vụ kiểm tra đánh giá, đảm bảo ATTT và hỗ trợ ứng cứu sự cố an ninh mạng.

II. Phạm vi công việc và yêu cầu:

1. Phạm vi công việc:

STT	Hạng mục công việc	Đơn vị tính	Số lượng	Thời gian triển khai
I	**Thuê dịch vụ kiểm tra đánh giá, đảm bảo ATTT và hỗ trợ ứng cứu sự cố an ninh mạng.**	**Gói**	**01**	**01 năm**
1	Cung cấp 05 chuyên gia tham gia Đội ứng cứu sự cố ATTT của PV Power trong 01 năm đáp ứng tiêu chuẩn theo quy định.			
2	Trực sẵn sàng hỗ trợ PV Power ứng cứu sự cố an toàn thông tin 24/7, có cam kết SLA.			
3	Kiểm tra, đánh giá việc đảm bảo ATTT cho các hệ thống thông tin tại các đơn vị.			
4	*Rà quét lỗ hổng điểm yếu thiết bị mạng, bảo mật; Đánh giá điểm yếu, kiểm thử xâm nhập (Pentest) cho các ứng dụng; Đánh giá xâm nhập và săn tìm mối nguy hại trên hệ thống máy chủ.* Các nội dung mục 4.1 và 4.3 định kỳ 06 tháng/lần (02 lần), mục 4.2 (1			

	lần) tại CQ TCT, Trung tâm dữ liệu đặt tại Viettel IDC để phát hiện mã độc, lỗ hổng, điểm yếu tuân thủ theo Chỉ thị 18/CT-TTg ngày 13/10/2022.			
5	Tư vấn, thiết kế đảm bảo đáp ứng tối thiểu ATTT theo cấp độ đề xuất tại đơn vị bao gồm hệ thống IT và OT			

2. Yêu cầu kỹ thuật cụ thể:

STT	Hạng mục công việc	Yêu cầu kỹ thuật
1	Cung cấp 05 chuyên gia tham gia Đội ứng cứu sự cố ATTT của PV Power trong 01 năm đáp ứng tiêu chuẩn theo quy định.	Các chuyên gia đảm bảo đáp ứng hạng 2 trở lên hoặc tương đương theo tiêu chuẩn quy định theo Thông tư số 12/VBHN-BTTTT ngày 26/9/2022 Quy định chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp. Tiêu chí hạng 2 bao gồm: - Đáp ứng yêu cầu kiến thức cơ bản về CNTT ở trình độ đại học, hoặc tốt nghiệp ngành đào tạo về CNTT trình độ đại học trở lên. - Đáp ứng các mục yêu cầu về kiến thức, kỹ năng chuyên sâu của hạng 2 tương ứng với Chuẩn kỹ năng An toàn thông tin. - Có khả năng phụ trách một nhóm cán bộ kỹ thuật từ 10 người trở lên thuộc lĩnh vực phù hợp với chuẩn kỹ năng tương ứng. - Có thời gian làm công việc tương ứng 6 năm liên tục trở lên ở hạng 3. Việc đáp ứng được thể hiện qua các tiêu chí như bên dưới:
		Trình độ chuyên môn: Chuyên gia tham gia đội ứng cứu phải đáp ứng: - Tốt nghiệp Đại học chuyên ngành Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin hoặc tương đương với số năm kinh nghiệm tính từ thời điểm tốt nghiệp Đại học ≥ 06 năm.
		Kinh nghiệm trong lĩnh vực an toàn thông tin: - Đã tham gia ít nhất 01 dự án trong 03 năm gần nhất (2024, 2023 và 2022) về việc cung cấp các dịch vụ an toàn thông tin như kiểm tra đánh giá an toàn thông tin hoặc giám sát an toàn thông tin hoặc

		tương đương.
		Chứng chỉ chuyên môn: - Vị trí trưởng nhóm: Tốt nghiệp Đại học chuyên ngành Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin hoặc tương đương với số năm kinh nghiệm tính từ thời điểm tốt nghiệp Đại học ≥ 06 năm. Có 02 trong các chứng chỉ sau: CISSP (Certified Information Systems Security Professional), CCIE Security, OSCE3 hoặc tương đương. - Mỗi chuyên gia phải có tối thiểu 01 chứng chỉ quốc tế về an toàn thông tin phổ biến, còn thời hạn tới thời điểm nộp thầu gồm Microsoft Certified: Cybersecurity Architect Expert, CEH (Certified Ethical Hacker), CHFI (Computer Hacking Forensic Investigator), OSWE (Offensive Security Web Expert), OSCP (Offensive Security Certified Professional), OSEP (Offensive Security Experienced Pentester) hoặc tương đương.
2	Trực sẵn sàng hỗ trợ PV Power ứng cứu sự cố an toàn thông tin 24/7, có cam kết SLA.	Hỗ trợ PV Power ứng cứu sự cố an toàn thông tin 24/7 trong 1 năm, phạm vi ứng cứu sự cố bao gồm: - Tiếp nhận, phân tích các cảnh báo/thông báo nghi ngờ mất an toàn thông tin để nhận định là sự cố an toàn thông tin hoặc không. + Kênh tiếp nhận thông tin: điện thoại, email, OTT (Zalo, Telegram). + Thời gian phản hồi kể từ khi tiếp nhận yêu cầu: tối đa 01 ngày. + Thời gian đưa ra nhận định là sự cố an toàn thông tin hoặc không: tối đa 02 ngày. - Phối hợp cùng Đội ứng cứu sự cố PV Power điều tra nguyên nhân sự cố xảy ra, các tác động có liên quan tới sự cố, đưa ra khuyến nghị xử lý sự cố và hỗ trợ, phối hợp với PV Power trong suốt quá trình khắc phục sự cố. + Thời gian phản hồi tối đa kể từ khi nhận được yêu cầu hỗ trợ của PV Power qua điện thoại: 03 tiếng. + Thời gian tối đa bố trí nhân sự sẵn sàng tham gia hỗ trợ: 12 tiếng. - Hỗ trợ tư vấn trong quá trình PVPower xử lý sự cố. +Hỗ trợ tư vấn trong quá trình PV Power xử lý sự cố, tối thiểu qua các kênh sau: điện thoại, email, OTT (Zalo, Telegram)
3	Kiểm tra, đánh giá việc đảm bảo ATTT	Tần suất thực hiện: 01 lần/năm thực hiện trực tiếp tại 10 đơn vị trực thuộc, thành viên của PV Power như sau:

	cho các hệ thống thông tin tại các đơn vị.	1. Công ty Điện lực Dầu khí Cà Mau; 2. Công ty Điện lực Dầu khí Nhơn Trạch; 3. Công ty Cung ứng Nhiên liệu Điện lực Dầu khí; 4. Trung tâm dịch vụ kỹ thuật; 5. Ban Quản lý Dự án Điện; 6. Công ty CP Điện lực Dầu khí Nhơn Trạch 2; 7. Công ty Điện lực Dầu khí Hà Tĩnh; 8. Công ty CP Thủy điện Hủa Na; 9. Công ty CP Thủy điện ĐakĐrinh; 10. Công ty CP Dịch vụ Kỹ thuật Điện lực Dầu khí Việt Nam;
		- Nội dung kiểm tra, đánh giá việc tuân thủ bảo đảm an toàn hệ thống thông tin theo cấp độ đề xuất bao gồm: + Kiểm tra hiện trạng việc lập, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống IT, OT (nếu có) tại đơn vị; + Kiểm tra, đánh giá việc đáp ứng các **yêu cầu về quản lý, yêu cầu về kỹ thuật** đối với hệ thống thông tin IT, OT (nếu có) theo cấp độ đề xuất tại đơn vị (**quy định chi tiết tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022**); + Kiểm tra, đánh giá việc thực hiện trách nhiệm của đơn vị chủ quản (nếu là chủ quản hoặc được ủy quyền chủ quản), đơn vị vận hành, đơn vị chuyên trách an toàn thông tin. - Nội dung rà quét lỗ hổng bao gồm: + Thực hiện rà quét bảo mật để phát hiện điểm yếu kỹ thuật, lỗ hổng đã biết (CVE) hoặc sai sót cấu hình (misconfiguration) trên hệ thống máy chủ và thiết bị mạng trọng yếu hệ thống IT. + Đưa ra phương án khuyến nghị đối với các nội dung kiểm tra được đánh giá là chưa đạt. + Sử dụng một trong các tiêu chuẩn hoặc kết hợp: Technical Guide to Information Security Testing and Assessment (SP 800-115) của Viện tiêu chuẩn và công nghệ Hoa Kỳ (NIST), Penetration Testing Execution Standard (PTES), OSSTMM (The Open Source Security Testing Methodology Manual) v3.0.

+ Phương pháp: Blackbox cho máy chủ, thiết bị mạng.

STT	Bước thực hiện	Mô tả
I	**Dò quét lỗ hổng, điểm yếu cho máy chủ**	
1	Bước 1: Thu thập thông tin	- Xác định mục tiêu. - Khảo sát hiện trạng hệ thống, đối tượng cần đánh giá: ✓Thu thập thông tin địa chỉ IP, hostname, hệ điều hành, cổng dịch vụ public ✓Xác định sự tồn tại của các thiết bị filter: Firewall, IPS… ✓Xác định dịch vụ đang chạy, phiên bản của dịch vụ ✓Xác định phiên bản hệ điều hành.
2	Bước 2: Dò quét lỗ hổng	- Dò quét và phân tích các nguy cơ rủi ro có khả năng xảy ra: ✓Sử dụng các công cụ tự động để rà quét lỗ hổng trên hệ thống ✓Tiến hành xác minh thủ công các lỗ hổng nghiêm trọng để loại bỏ cảnh báo sai (false positives), đánh giá mức độ ảnh hưởng thực tế đến hệ thống.
3	Bước 3: Phân tích rủi ro	- Thực hiện phân tích rủi ro để xác định mức độ rủi ro của các lỗ hổng được tìm thấy. - Tham vấn quản trị hệ thống để hiệu chỉnh mức độ rủi ro thực tế, có xét đến các biện pháp bảo vệ hiện hữu (bảo mật nhiều lớp, cách ly mạng, cơ chế giám sát...) và chính sách nội bộ của TCT.
4	Bước 4: Báo cáo kết quả đánh giá	- Sau khi kết thúc quá trình đánh giá (lần 1) nhà thầu tiến hành lập "Báo cáo tổng thể kết đánh giá (lần 1)" bao gồm bao gồm: danh sách lỗ hổng/điểm yếu, mức độ rủi ro, minh chứng kỹ thuật và đề xuất biện pháp khắc phục chi tiết cho từng lỗ hổng.
5	Bước 5: Khắc phục các lỗ	- Hỗ trợ thực hiện khắc phục theo hướng dẫn trong báo cáo đánh giá.

				hổng gây mất ATTT	
			6	Tái đánh giá	- Thực hiện tái đánh giá đối với các hệ thống/lỗ hổng đã được xác nhận khắc phục, nhằm xác minh hiệu quả vá lỗi và đảm bảo không còn tồn tại lỗ hổng hoặc lỗi cấu hình tương tự.
			7	Bước 7: Báo cáo kết quả tái đánh giá	- Báo cáo kết quả tái đánh giá (lần 2). Nội dung báo cáo kết quả tái đánh giá: ✓Danh sách hệ thống đã được xử lý lỗ hổng, kèm hình ảnh/bằng chứng kỹ thuật xác nhận. ✓Đối chiếu các điểm yếu mới nếu có phát sinh thêm trong quá trình khắc phục. ✓Nhận định về trạng thái an toàn hiện tại và khả năng tiếp tục vận hành ổn định.
			II	**Dò quét lỗ hổng, điểm yếu cho thiết bị mạng, bảo mật**	
			1	Bước 1: Thu thập thông tin	- Xác định mục tiêu đánh giá và phạm vi hệ thống. - Khảo sát hiện trạng các thiết bị trong phạm vi đánh giá (tên thiết bị, địa chỉ IP, đơn vị quản lý, vai trò trong hệ thống). - Phân loại nền tảng hệ điều hành, firmware, phiên bản thiết bị (nếu có) để lựa chọn công cụ và kỹ thuật quét phù hợp.
			2	Bước 2: Dò quét lỗ hổng	- Dò quét và phân tích các nguy cơ rủi ro có khả năng xảy ra:. ✓Sử dụng công cụ tự động để thực hiện rà quét lỗ hổng đối với các thiết bị mạng và bảo mật nhằm phát hiện các điểm yếu đã biết (CVE), lỗi cấu hình phổ biến (misconfiguration), hoặc giao thức lỗi thời (insecure protocols). ✓Phân tích và xác minh thủ công các lỗ hổng tiềm ẩn được công cụ phát hiện, nhằm loại bỏ cảnh báo sai (false positives), đặc biệt với các thiết bị quan trọng.

				✓Kết quả được ghi nhận kèm theo thông tin về: mã CVE, mô tả kỹ thuật, ảnh hưởng, khả năng khai thác và điều kiện khai thác.
		3	Bước 3: Phân tích rủi ro	- Đánh giá mức độ rủi ro của từng lỗ hổng dựa theo tiêu chuẩn CVSS (v3.x) hoặc khung đánh giá nội bộ. - Tham vấn cán bộ quản trị hạ tầng để hiệu chỉnh mức rủi ro thực tế, có xét đến các yếu tố giảm thiểu như: kiểm soát truy cập, segment mạng, firewall chặn port, giám sát hành vi,… - Xếp loại các rủi ro thành: Nghiêm trọng / Cao / Trung bình / Thấp để ưu tiên khắc phục.
		4	Báo cáo kết quả đánh giá	- Sau khi kết thúc quá trình đánh giá (lần 1) nhà thầu tiến hành lập Báo cáo tổng thể kết đánh giá (lần 1): ✓Danh sách đầy đủ các thiết bị đã kiểm tra. ✓Lỗ hổng/điểm yếu đã phát hiện, kèm mức độ rủi ro. ✓Hình ảnh minh chứng (nếu có) và phân tích kỹ thuật. ✓Đề xuất biện pháp khắc phục tương ứng theo từng nhóm lỗ hổng.
		5	Bước 5: Khắc phục các lỗ hổng gây mất ATT	- Hỗ trợ khắc phục theo hướng dẫn trong báo cáo đánh giá.
		6	Bước 6: Tái đánh giá	- Sau khi đơn vị xác nhận đã thực hiện đầy đủ khắc phục, nhà thầu tiến hành tái đánh giá lần 2 để xác minh tính hiệu quả của các biện pháp xử lý. - Nội dung tái đánh giá tập trung vào: ✓Các lỗ hổng đã tồn tại ở lần đánh giá trước. ✓Các thiết bị đã có thay đổi cấu hình hoặc cập nhật.
		7	Bước 7: Báo cáo kết quả tái đánh giá	- Báo cáo kết quả tái đánh giá điểm yếu an ninh cho các thiết bị mạng (lần 2). Nội dung báo cáo kết quả tái đánh giá: ✓Danh sách và minh chứng các thiết bị đã được xử lý thành công.

				✓Phát hiện các điểm yếu mới phát sinh (nếu có) trong quá trình tái rà soát. ✓Khẳng định mức độ an toàn hiện tại của từng thiết bị, và khuyến nghị bổ sung nếu vẫn còn tồn tại rủi ro.
4	*Rà quét lỗ hổng điểm yếu thiết bị mạng, bảo mật; Đánh giá điểm yếu, kiểm thử xâm nhập (Pentest) cho các ứng dụng; Đánh giá xâm nhập và săn tìm mối nguy hại trên hệ thống máy chủ.* Các nội dung 4.1 và 4.3 định kỳ 06 tháng/lần (02 lần), mục 4.2 (1 lần) tại CQ TCT, Trung tâm dữ liệu đặt tại Viettel IDC để phát hiện mã độc, lỗ hổng, điểm yếu tuân thủ theo Chỉ thị 18/CT-TTg ngày 13/10/2022.	4.1. Rà quét lỗ hổng điểm yếu thiết bị mạng, bảo mật: theo mục 03 - II			
		4.2. Kiểm tra, đánh giá điểm yếu, kiểm thử xâm nhập (Pentest) đối với ứng dụng nội bộ tại CQ TCT, Trung tâm dữ liệu đặt tại Viettel IDC cụ thể: (Email, Voffice, Histaff, Cmms, Ecat, SAP, Power Monitoring).			

- Nội dung thực hiện đánh giá điểm yếu, kiểm thử xâm nhập (Pentest):
  + Thực hiện rà quét, phân tích điểm yếu và tiến hành kiểm thử xâm nhập có kiểm soát đối với từng ứng dụng mục tiêu nhằm xác định khả năng bị khai thác thực tế.
  + Đề xuất biện pháp khắc phục chi tiết cho từng lỗ hổng, bao gồm hướng dẫn kỹ thuật, phương án giảm thiểu tạm thời (nếu chưa thể vá ngay) và kiến nghị cải tiến quy trình nếu liên quan tới lỗi logic nghiệp vụ. Sử dụng một trong các tiêu chuẩn hoặc kết hợp tùy theo loại ứng dụng được đánh giá:
  ✓ Web App: OWASP Web Security Testing Guide v4.2, OWASP Top 10, PTES, NIST SP 800-115.
  ✓ Desktop App: OWASP Desktop App Security Project.
  ✓ Mobile App: OWASP Mobile Top 10, Mobile App Security Testing Guide.
  ✓ Tổng quát: PTES, OSSTMM v3.0 – dùng để xác định cách tiếp cận theo từng lớp và từng pha đánh giá.
  ✓ Phương pháp: Graybox

STT	Bước thực hiện	Mô tả
1	Bước 1: Thu thập thông tin	- Khảo sát mục tiêu và thu thập thông tin ứng dụng: tên, phiên bản, nền tảng (Web/Desktop/Mobile/API), mô hình triển khai, endpoint, các dịch vụ liên quan. - Nhận tài khoản kiểm thử (nếu có), phân quyền user/admin để đánh giá phân quyền logic. - Ghi nhận phạm vi, giới hạn kiểm thử và khung thời gian thực hiện.
2	Bước 2: Dò quét lỗ hổng, điểm yếu	- Sử dụng các công cụ tự động (Burp Suite, OWASP ZAP, Nuclei, Nikto...) để rà soát điểm yếu kỹ thuật: lỗi cấu hình, injection, XSS, CSRF, authentication flaws... - Tìm kiếm endpoint hoặc thông tin nhạy cảm bị lộ bằng wordlist, thư mục ẩn, API. enumeration.

				- Xác định điểm đầu vào có thể bị khai thác.
		3	Bước 3: Xác minh lỗ hổng, điểm yếu, kiểm thử xâm nhập	- Thực hiện kiểm thử có kiểm soát đối với các lỗ hổng nguy cơ cao nhằm xác minh khả năng khai thác. - Sử dụng kỹ thuật phù hợp (manual payload, công cụ hỗ trợ, custom script) để xây dựng PoC. - Ghi lại kết quả, hình ảnh minh họa và mức độ ảnh hưởng thực tế. - Không phá hoại hệ thống hoặc gây gián đoạn dịch vụ.
		4	Bước 4: Đánh giá mức độ nguy hiểm của các lỗ hổng, điểm yếu và Báo cáo kết quả đánh giá	- Phân loại lỗ hổng theo tiêu chí chuẩn (CVSS v3.1 hoặc tương đương): Nghiêm trọng / Cao / Trung bình / Thấp. - Lập báo cáo cho từng ứng dụng, bao gồm: ✓ Mô tả lỗ hổng và cách phát hiện. ✓ Hình ảnh minh chứng. ✓ Đánh giá mức rủi ro. ✓ Khuyến nghị khắc phục chi tiết.
		5	Bước 5: Khắc phục các lỗ hổng gây mất ATT	- Hỗ trợ khắc phục theo hướng dẫn trong báo cáo đánh giá.
		6	Bước 6: Tái đánh giá	- Thực hiện tái đánh giá sau khi có thông báo đã khắc phục, vá lỗi thành công sau lần đánh giá đầu tiên (lần 1).
		7	Bước 7: Báo cáo kết quả tái đánh giá	- Báo cáo kết quả tái đánh giá lỗ hổng, điểm yếu (lần 2). Nội dung báo cáo kết quả tái đánh giá: ✓ Danh sách các lỗi đã khắc phục thành công. ✓ Minh chứng kỹ thuật. ✓ Ghi nhận lỗi mới phát sinh (nếu có).

		✓ Kết luận mức độ an toàn hiện tại
		4.3. Đánh giá xâm nhập và săn tìm mối nguy hại trên hệ thống máy chủ
		- Săn tìm mối nguy hại định kỳ 06 tháng/lần để phát hiện mã độc, lỗ hổng, điểm yếu trên hệ thống máy chủ tại CQ TCT, Viettel IDC, hệ thống máy chủ được quản trị bởi PV Power (website TCT), máy tính quản trị hệ thống. - Phát hiện sự hiện diện của các mối đe dọa hoặc các dấu hiệu xâm phạm trong hệ thống CNTT mà hệ thống tự động không thể phát hiện. Nhanh chóng nhận biết những hoạt động đáng ngờ trước khi chúng gây ra hậu quả nghiêm trọng hoặc nhận diện những mối đe dọa đang hiện hữu trong hạ tầng. - Cung cấp khả năng phát hiện các cuộc tấn công tiềm ẩn chủ động, thay vì chỉ phản ứng khi sự cố đã xảy ra. - Cung cấp báo cáo chi tiết về kết quả đánh giá, khuyến nghị thực tiễn để cải thiện hệ thống bảo mật, giúp tăng cường khả năng phòng chống và ứng phó với các mối đe dọa tương lai. - Đối tượng thực hiện: Hệ thống máy chủ tại CQ TCT, Viettel IDC, hệ thống máy chủ được quản trị bởi PV Power (website TCT), máy tính quản trị hệ thống như danh sách dưới đây.

STT	Thiết bị	Số lượng	Ghi chú
1	Máy chủ, máy tính quản trị hệ thống	<= 60	Bao gồm cả máy chủ vật lý (Hosts) và máy chủ ảo (VMs)

Nội dung thực hiện:

- Đánh giá xâm nhập, xác định các dấu hiệu bị xâm phạm, hoạt động độc hại hoặc rủi ro bảo mật trong cơ sở hạ tầng (nếu có).
- Quy trình, kết hợp giữa công nghệ tiên tiến và đội ngũ chuyên gia kinh nghiệm, nhằm cung cấp kết quả chi tiết, nhận diện nguy cơ nhanh chóng và đưa ra khuyến nghị triển khai các biện pháp ứng phó kịp thời.

Yêu cầu kỹ thuật:

- Săn tìm nguy cơ chủ động bằng cách truy cập trực tiếp vào máy tính (máy chủ/máy trạm), thực hiện chạy các công cụ đánh giá nhằm xác định các dấu hiệu bị tấn công, phát hiện các mối đe dọa

nâng cao mà hệ thống tự động không thể phát hiện.

- Công cụ đánh giá dựa theo các giả thuyết được xây dựng với các chiến thuật, kỹ thuật, và quy trình (TTPs) đã biết sử dụng frameworks như MITRE ATT&CK, các nguồn Threat Intelligence và kinh nghiệm xử lý sự cố.

TT	**Công việc thực hiện**	**Chi tiết công việc**
1	Khảo sát hiện trạng	Khảo sát thu thập thông tin về môi trường và các hệ thống cần thực hiện đánh giá (bao gồm OS, version OS, IP, Hostname, chi tiết dịch vụ đang chạy trên các máy tính, webroot).
2	Chuẩn bị công cụ	- Thực hiện truy cập thử (onsite hoặc remote) vào các các máy tính (máy chủ/máy trạm) cần đánh giá của Khách hàng trước khi tiến hành để nhận biết đã đủ quyền hạn thực hiện hay chưa. - Thực hiện chạy test công cụ trên mỗi loại Hệ điều hành để đánh giá hiệu năng, độ tương thích. - Gửi danh sách các công cụ sẽ sử dụng để thực hiện đánh giá (mô tả công cụ, link đối chiếu)
3	Thực hiện đánh giá	- Thực hiện kết nối với quyền Administrator/root qua RDP/SSH,… vào các máy tính (máy chủ/máy trạm) cần đánh giá. - Copy và chạy công cụ đánh giá. - Sau khi chạy xong công cụ, trích xuất log ra một máy tính (máy chủ/máy trạm) và thực hiện đánh giá trên các log này. - Xóa công cụ đánh giá trên các máy tính (máy chủ/máy trạm) sau khi hoàn than - Hình thức đánh giá: • Onsite: Kết nối máy tính, phiên kết nối để thực hiện đánh giá. • Remote: Hỗ trợ kênh truy cập, xuất log.

		4	Báo cáo kết quả	*<u>Báo cáo bao gồm các nội dung:</u>* - Tổng hợp danh sách các đối tượng và kỹ thuật đã thực hiện săn tìm và kết quả tương ứng. - Đối với các mối nguy hại săn tìm được, nêu rõ mức độ nghiêm trọng và các dấu hiệu bị tấn công, xâm phạm, bao gồm: thông tin sơ bộ; thông tin về điểm bị xâm phạm, dấu hiệu tìm được (đường dẫn mẫu mã độc, registry, process,…); thông tin các chỉ số xâm phạm (IOCs - Indicators of Compromise) hoặc chỉ số tấn công (IOAs - Indicators of Attack) tìm thấy được. - Khuyến nghị (không tác động) về cách xác định, gỡ bỏ các dấu hiệu tìm được và phương án, giải pháp khắc phục để ngăn ngừa các sự cố như vậy trong tương lai và cách cải thiện tính bảo mật của các hệ thống (không bao gồm điều tra chuyên sâu và xử lý sự cố).
5	Tư vấn, thiết kế đảm bảo đáp ứng tối thiểu ATTT theo cấp độ đề xuất tại đơn vị bao gồm hệ thống IT và OT	Thực hiện việc tư vấn, thiết kế đảm bảo đáp ứng tối thiểu ATTT theo cấp độ tại 11 đơn vị bao gồm hệ thống IT và OT (nếu có), danh sách các đơn vị: 1. Công ty Điện lực Dầu khí Cà Mau; 2. Công ty Điện lực Dầu khí Nhơn Trạch; 3. Công ty Cung ứng Nhiên liệu Điện lực Dầu khí; 4. Trung tâm dịch vụ kỹ thuật; 5. Ban Quản lý Dự án Điện; 6. Công ty CP Điện lực Dầu khí Nhơn Trạch 2; 7. Công ty Điện lực Dầu khí Hà Tĩnh; 8. Công ty CP Thủy điện Hủa Na; 9. Công ty CP Thủy điện ĐakĐrinh; 10. Công ty CP Dịch vụ Kỹ thuật Điện lực Dầu khí Việt Nam; **Nội dung thực hiện:** 1. Khảo sát, đánh giá hiện trạng hệ thống IT và OT (nếu có) tại đơn vị:	

		- Khảo sát thu thập tài liệu hiện trạng: sơ đồ mạng, cấu hình thiết bị, dịch vụ đang hoạt động… - Đánh giá hệ thống hiện hữu: + Xác định ranh giới mạng IT và OT (nếu có), điểm giao tiếp và kết nối bên ngoài. + Đánh giá hiện trạng kiểm soát truy cập, backup, chống mã độc, giám sát nhật ký... 2. Tư vấn, thiết kế đảm bảo an toàn thông tin cho hệ thống IT và hệ thống OT (nếu có) đáp ứng tối thiểu theo cấp độ đề xuất tại đơn vị: - Đề xuất kiến trúc bảo mật đối với IT, OT (nếu có); - Lập hồ sơ thiết kế, bản vẽ kỹ thuật cho hệ thống IT, OT (nếu có) đáp ứng tối thiểu theo cấp độ đề xuất, cụ thể: + Sơ đồ mạng bảo mật cho hệ thống IT và hệ thống OT. + Bản vẽ sơ đồ phân vùng mạng. - Tư vấn mô hình kết nối an toàn giữa IT ↔ OT (nếu có kết nối IT và OT). - Đối chiếu yêu cầu kỹ thuật theo các Phụ lục tại Thông tư 12/2022/TT-BTTTT. 3. Tư vấn danh mục trang thiết bị, giải pháp cần trang bị. - Đề xuất danh mục trang thiết bị, giải pháp cần trang bị kèm theo mô tả tính năng kỹ thuật.

3. Yêu cầu đề xuất:

Đơn vị cung cấp dịch vụ cần có kinh nghiệm triển khai hợp đồng tương tự.

Nội dung đề xuất bao gồm:

- Giới thiệu năng lực, kinh nghiệm của đơn vị.
- Lý lịch chuyên gia thực hiện công việc.
- Báo giá đối với dịch vụ.

Số và ký hiệu: 193/KT-NB
Ngày ban hành: 14/05/2025

Kính mời các đơn vị cung cấp dịch vụ quan tâm gửi nội dung đề xuất đến địa chỉ: Ban Kỹ thuật, Tổng công ty Điện lực Dầu khí Việt Nam - CTCP, 167 Trung Kính, Yên Hòa, Cầu Giấy, Hà Nội và gửi bản mềm qua email: nguyenthicamtu@pvpower.vn trước 09h00 ngày 22/05/2025.