Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

I. Giới thiệu chung về chương trình, gói thầu

1. Tên chương trình: Thuê dịch vụ giám sát và xử lý sự cố ATTT tại TTDL EVNCPC giai đoạn 2026-2028.
2. Tên gói thầu: 01.PTV: Dịch vụ giám sát và xử lý sự cố ATTT tại TTDL EVNCPC giai đoạn 2026-2028.
3. Chủ đầu tư: Công ty Công nghệ thông tin Điện lực miền Trung - Tổng công ty Điện lực miền Trung (CPCIT).
4. Thời gian thực hiện gói thầu: Tính từ ngày hợp đồng có hiệu lực đến ngày nghiệm thu hoàn thành gói thầu, trong đó:

   Thời gian thực hiện dịch vụ giám sát và xử lý sự cố ATTT là 36 tháng (Bắt đầu từ ngày 01/01/2026 đến 31/12/2028), không bao gồm thời gian chuẩn bị trước khi triển khai dịch vụ: Tối đa 01 tháng
5. Quy mô hạng mục chương trình: Thuê 01 gói dịch vụ giám sát và xử lý sự cố ATTT tại TTDL EVNCPC giai đoạn 2026-2028 (từ ngày 01/01/2026 đến 31/12/2028), gồm: cấp độ 1 (Tier 1) và cấp độ 3 (Tier 3).

II. Mục tiêu công việc:

- Đảm bảo các hệ thống thông tin (HTTT) tại TTDL EVNCPC được giám sát và xử lý sự cố về ATTT;
- Phát hiện sớm các nguy cơ, sự cố mất ATTT trên toàn bộ các HTTT tại TTDL EVNCPC. Thực hiện xử lý các cảnh báo, sự cố, sự kiện an ninh mạng (ANM) xảy ra đối với hệ thống;
- Chủ động phát hiện sớm và gỡ bỏ các loại mã độc, webshell và các lỗ hổng, nguy cơ tồn tại trên các hệ thống máy chủ, phần mềm, ứng dụng;
- Đảm bảo cho các HTTT hoạt động liên tục phục vụ quá trình sản xuất kinh doanh (SXKD), quản lý điều hành (QLĐH) của Tổng công ty.

III. Yêu cầu kỹ thuật của gói thầu:

1. Địa điểm triển khai*:*

Site chính TTDL EVNCPC, địa chỉ: 393 Trưng Nữ Vương, TP Đà Nẵng và site dự phòng TTDL EVNCPC, địa chỉ: 02 Quang Trung, TP Đà Nẵng.

2. Quy mô thực hiện*:*

TT	Nội dung chi tiết	Yêu cầu	Nhà thầu chào
I	**Yêu cầu kỹ thuật dịch vụ**		
1	**Yêu cầu kỹ thuật với cấp độ 1 (Tier 1)**	**Đáp ứng**	

TT	Nội dung chi tiết	Yêu cầu	Nhà thầu chào
	Thực hiện hoạt động giám sát ATTT 24/7 theo mô hình 3 ca, 4 kíp cho các HTTT của EVNCPC bằng hình thức kết nối từ xa thông qua kênh truyền Metrowan. Mỗi ca tối thiểu 01 nhân sự.		
	Hoạt động giám sát được thực hiện từ xa trên các công cụ, hệ thống giám sát ATTT hiện hữu tại EVNCPC (*). Tiếp nhận cảnh báo mới, phân tích và xử lý theo hướng dẫn. Các tác vụ thay đổi, cấu hình hệ thống do cán bộ EVNCPC thực hiện.		
	Chịu trách nhiệm về việc giám sát, phân tích sơ bộ nhằm nhận diện và phân loại các sự kiện ATTT được cung cấp từ hệ thống các công cụ và từ các bộ phận, quy trình hoạt động khác.		
	Thực hiện các hành động được định nghĩa sẵn nhằm ngăn chặn nhanh chóng các sự cố, tránh gây thiệt hại về mặt kinh tế, dữ liệu, hình ảnh của EVNCPC.		
	Theo dõi quá trình xử lý, kiểm tra kết quả và đóng các ticket xử lý xong.		
	Xử lý các cảnh báo, sự kiện ATTT đúng hạn theo các chỉ tiêu KPI tại **Phụ lục 1** đính kèm.		
2	**Yêu cầu kỹ thuật với cấp độ 3 (Tier 3)**	**Đáp ứng**	
	Phân tích mã độc.		
	Phân tích điều tra chuyên sâu, nâng cao về nguồn tấn công, phát hiện đề phòng tấn công.		
	Phân tích, xử lý các cảnh báo phức tạp, chưa có hướng dẫn hoặc đã có hướng dẫn nhưng Tier 1, Tier 2 xử lý không thành công.		
	Phối hợp Tier 1, Tier 2 và Đơn vị liên quan (do EVNCPC đề xuất) ứng cứu sự cố, khôi phục hệ thống, đưa dịch vụ trở lại hoạt động bình thường.		
	Xử lý các sự cố, cảnh báo ATTT chưa có hướng dẫn đúng hạn theo các chỉ tiêu KPI tại **Phụ lục 1** đính kèm.		
	Cán bộ cấp độ Tier 3 (tối thiểu 01 nhân sự) của Đơn vị cung cấp dịch vụ hỗ trợ xử lý sự cố thông qua kết nối mạng riêng (sử dụng kênh truyền metrowan) hoặc trực tiếp tại EVNCPC khi cần thiết hoặc khi được EVNCPC yêu cầu.		

TT	Nội dung chi tiết	Yêu cầu	Nhà thầu chào
3	**Yêu cầu kỹ thuật đối với phân tích nội dung (Content Analysis)**	**Đáp ứng**	
	Thực hiện tối ưu cảnh báo vận hành đang có trên hệ thống giám sát ATTT của EVNCPC (*) để tăng hiệu quả của việc vận hành, giảm thiểu tối đa cảnh báo sai.		
	Phân tích thông tin sự cố nội bộ, bên ngoài xảy ra có liên quan đến EVNCPC để tạo cảnh báo mới (nếu cần) và tối ưu hóa tập luật (rule) hiện tại.		
	Cán bộ Content Analysis (tối thiểu 01 nhân sự) của Đơn vị cung cấp dịch vụ tối ưu cảnh báo từ xa thông qua kết nối mạng riêng (sử dụng kênh truyền metrowan).		
4	**Yêu cầu kỹ thuật đối với phân tích lỗ hổng ATTT (Threat Analysis)**	**Đáp ứng**	
	Thực hiện theo dõi trên các nguồn thông tin công khai và cảnh báo về các lỗ hổng ANM mức nghiêm trọng (theo thang đo CVSS 3.0 điểm từ 7 đến 10) có thể liên quan đến các công nghệ đang được sử dụng trong hệ thống EVNCPC như Microsoft, Google, Cisco, Adobe, Oracle, VMware, Apache, IBM,…		
	Cập nhật tri thức security từ các nguồn công khai, thực hiện phân tích, xác minh các nguy cơ (đặc biệt là lộ lọt tài khoản người dùng, mã nguồn ứng dụng EVNCPC nếu có), lỗ hổng bảo mật, dấu hiệu tấn công (IoC) mới và thông báo để EVNCPC cập nhật vào hệ thống phòng thủ, xử lý nguy cơ, lỗ hổng có ảnh hưởng.		
	Cán bộ Threat Analysis (tối thiểu 01 nhân sự) của Đơn vị cung cấp dịch vụ thực hiện công việc tại văn phòng của đơn vị cung cấp dịch vụ, cảnh báo cho chủ đầu tư thông qua hệ thống/công cụ giám sát và/hoặc bằng email.		
5	**Yêu cầu kỹ thuật đối với quản lý SOC (SOC Manager)**	**Đáp ứng**	
	Quản lý điều hành việc xử lý các cảnh báo, sự cố theo KPI, đảm bảo chất lượng dịch vụ theo SLA.		
	Trực tiếp hoặc trực tuyến trao đổi công việc định kỳ với Chủ đầu tư (hàng quý hoặc theo yêu cầu của Chủ đầu tư) để: - Báo cáo, đánh giá các công tác hoạt động của SOC.		

TT	Nội dung chi tiết	Yêu cầu	Nhà thầu chào
	- Trình bày, hướng dẫn Chủ đầu tư các trường hợp xử lý cảnh báo điển hình, phức tạp (bao gồm các case Tier 3) trong quá trình cung cấp dịch vụ, bao gồm tối thiểu: chi tiết cảnh báo, sự cố; các công cụ sử dụng để thu thập log, điều tra, phân tích, rà soát, nhận diện các mối đe dọa ATTT và xử lý mã độc; quy trình các bước thực hiện; … - Rà soát, theo dõi và thống nhất với Chủ đầu tư các vướng mắc, vấn đề phát sinh trong quá trình cung cấp dịch vụ để đề xuất quy trình, giải pháp ngắn hạn, kế hoạch dài hạn để xử lý các vấn đề tồn tại, nâng cao chất lượng dịch vụ. - Đề xuất các biện pháp kỹ thuật, giải pháp công nghệ nhằm nâng cao hiệu quả, tối ưu hoạt động của hệ thống SOC EVNCPC (nếu có).		
	Cán bộ SOC Manager (01 nhân sự) của Đơn vị cung cấp dịch vụ thực hiện công việc tại văn phòng của đơn vị cung cấp dịch vụ, thực hiện các báo cáo tháng hoặc quý hoặc năm (theo thỏa thuận) bằng văn bản cho Chủ đầu tư.		
6	**Yêu cầu kỹ thuật đối với dịch vụ săn tìm mối nguy (Threat Hunting)**	**Đáp ứng**	
	Đơn vị cung cấp dịch vụ thực hiện Threat Hunting cho 1.392 máy chủ/năm.		
7	**Yêu cầu về quy trình, báo cáo định kỳ**	**Đáp ứng**	
	Đơn vị cung cấp dịch vụ biên soạn, thống nhất với Chủ đầu tư để ban hành "Quy trình phối hợp giám sát và xử lý sự cố ATTT 24/7 tại TTDL EVNCPC" để áp dụng trong quá trình cung cấp dịch vụ.		
	Đơn vị cung cấp dịch vụ: - Thực hiện báo cáo toàn diện về các vấn đề ATTT trong quá trình cung cấp dịch vụ (kèm theo bằng chứng chứng minh các số liệu trong báo cáo) cho Chủ đầu tư định kỳ hàng tháng, gửi vào ngày 01-05 của tháng tiếp theo thông qua văn bản và/hoặc bằng email.		

TT	Nội dung chi tiết	Yêu cầu	Nhà thầu chào
	- Thực hiện báo cáo bổ sung trong giai đoạn cần tăng cường giám sát; xác nhận của Đơn vị cung cấp dịch vụ trong dịp Lễ, Tết, … và khi có yêu cầu từ Chủ đầu tư thông qua văn bản và/hoặc bằng email.		
	Đơn vị cung cấp dịch vụ tổng hợp các hướng dẫn xử lý cảnh báo của Tier 3 xây dựng cho Tier 1, Tier 2 và chia sẻ với Chủ đầu tư thông qua đường dẫn (link) được phân quyền đầy đủ để Chủ đầu tư làm cơ sở xác minh lại quá trình xử lý cảnh báo của Tier 1.		
8	**Yêu cầu về đường truyền giám sát**	**Đáp ứng**	
	Đơn vị cung cấp dịch vụ kéo đường truyền kênh trắng (Metrowan), tốc độ tối thiểu 5 Mbps kết nối từ TTDL EVNCPC về đơn vị giám sát		
	Đơn vị cung cấp dịch vụ thực hiện giám sát, vận hành, duy trì chất lượng đường truyền để phục vụ công tác giám sát, xử lý sự cố ổn định, thông suốt 24/7 (có khả năng dự phòng khi đường giám sát chính bị mất kết nối).		
9	**Thời gian cung cấp dịch vụ:** 03 năm (từ 01/01/2026 đến 31/12/2028)	**Đáp ứng**	
II	**Điều kiện kinh doanh dịch vụ an toàn thông tin mạng**	**Đáp ứng**	
1	Nhà thầu có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng do Cơ quan nhà nước có thẩm quyền cấp; hoặc Quyết định giao nhiệm vụ của Cơ quan nhà nước có thẩm quyền để cung cấp dịch vụ an toàn thông tin tương ứng (Giấy phép/Quyết định còn hiệu lực)		
2	Nhà thầu có Giấy chứng nhận ISO 9001 – Hệ thống quản lý chất lượng và Giấy chứng nhận hệ thống quản lý an toàn thông tin ISO 27001 còn hiệu lực.		

Ghi chú (*): *Công cụ, hệ thống giám sát ATTT tại EVNCPC*

- Phần mềm phát hiện tấn công lớp mạng (NSM/NDR):

+ Giám sát và phát hiện tấn công lớp mạng Core tại TTDL: Hỗ trợ băng thông tối thiểu 2,5 Gbps.

+ Giám sát và phát hiện tấn công lớp mạng WAN và Internet tại TTDL: Hỗ trợ băng thông tối thiểu 1,0 Gbps.

- Phần mềm điều phối và phản ứng sự kiện ATTT (SOAR).

- Phần mềm quản lý, phân tích sự kiện ATTT (SIEM): Có license thu thập log tập trung và xử lý các sự kiện an ninh bảo mật

Lưu ý: *Một nhân sự chỉ được bố trí cho 01 vị trí theo yêu cầu gói thầu*

4. Kế hoạch triển khai gói thầu:

STT	Nội dung yêu cầu của gói thầu	Thời gian thực hiện
I	**Chuẩn bị trước khi thực hiện dịch vụ**	**Từ khi Hợp đồng có hiệu lực và hoàn thành trước 03 ngày bắt đầu triển khai dịch vụ**
1	Triển khai đường truyền giám sát	
2	Tạo tài khoản và cấp quyền truy cập cho nhân sự của đơn vị cung cấp dịch vụ trên các hệ thống giám sát ATTT của EVNCPC để thực hiện giám sát và xử lý sự cố ATTT 24/7.	
3	Chuyển tất cả dữ liệu, sự kiện, ticket, case... từ hệ thống giám sát của nhà cung cấp dịch vụ SOC EVNCPC hiện hữu sang hệ thống giám sát của EVNCPC để nhà cung cấp dịch vụ SOC giai đoạn 2026-2028 thực hiện giám sát liên tục, không bị gián đoạn.	
4	Tối ưu cảnh báo từ các công cụ, hệ thống giám sát để giảm thiểu các cảnh báo giả.	
II	**Thực hiện dịch vụ giám sát và xử lý sự cố ATTT tại TTDL EVNCPC giai đoạn 2026-2028**	**03 năm (Từ ngày 01/01/2026 đến ngày 31/12/2028)**

5. 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 tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

Phụ lục 1:

Chỉ tiêu KPI của việc giám sát và xử lý các cảnh báo ATTT

Bảng dưới đây sẽ mô tả các chỉ số KPI, mốc cam kết dịch vụ và tính toán số Service Credit khấu trừ hoặc thanh toán bổ sung theo các hoạt động chính của dịch vụ.

Service Credit tính cho bên chịu trách nhiệm chính (R) theo mô hình RASCI dưới đây:

+ R – Responsible: Trách nhiệm thực hiện chính.
+ A – Approval: Trách nhiệm phê duyệt, đồng ý nội dung thực hiện.
+ S – Support: Trách nhiệm hỗ trợ Bên thực hiện chính.
+ C – Consulted: Trách nhiệm dựa vào kiến thức, kinh nghiệm chuyên môn tư vấn giải pháp thực hiện.
+ I – Informed: Trách nhiệm được cung cấp thông tin.

Nội dung chi tiết bảng đánh giá dịch vụ:

<table>
<tr><th>TT</th><th>Hạng mục công việc</th><th>Mô tả</th><th>Cách tính thời gian xử lý</th><th>Service Credit</th><th>Trách nhiệm của Đơn vị cung cấp dịch vụ</th><th>Trách nhiệm của Chủ đầu tư</th><th>Mục tiêu cam kết</th></tr>
<tr><td>1</td><td>Tỷ lệ xử lý cảnh báo đúng hạn</td><td>- Là tỉ lệ giữa số lượng cảnh báo ATTT đã hoàn thành xử lý với Tổng số lượng cảnh báo trên hệ thống giám sát ATTT (SOAR) của EVNCPC.
- Thời gian xử lý cảnh báo ATTT đúng hạn, cụ thể như sau:<table><tr><td>Loại cảnh báo ATTT</td><td>Thời gian xử lý</td></tr><tr><td>NGHIÊM TRỌNG</td><td><= 30 phút</td></tr><tr><td>BÌNH THƯỜNG</td><td><= 1 giờ</td></tr></table></td><td>Từ thời điểm cảnh báo được tạo trên hệ thống đến khi cảnh báo được gán vào 1 Case (hoặc chuyển trạng thái False Positive)</td><td>1</td><td>R</td><td></td><td>98% (Với cảnh báo mức Nghiêm trọng)

92% (Với cảnh báo mức Bình thường)</td></tr>
<tr><td>2</td><td>Tỉ lệ sự cố ATTT</td><td>- Là tỷ lệ giữa số lượng sự cố ATTT chưa có</td><td>Từ thời điểm</td><td>1</td><td>R</td><td>S</td><td>98% (Với</td></tr>
</table>

<table>
<tr><th>TT</th><th>Hạng mục công việc</th><th>Mô tả</th><th>Cách tính thời gian xử lý</th><th>Service Credit</th><th>Trách nhiệm của Đơn vị cung cấp dịch vụ</th><th>Trách nhiệm của Chủ đầu tư</th><th>Mục tiêu cam kết</th></tr>
<tr><td></td><td>chưa có hướng dẫn hoàn thành xử lý trong hạn</td><td>hướng dẫn hoàn thành xử lý trong thời gian quy định với Tổng số sự cố ATTT chưa có hướng dẫn.
- Sự cố ATTT chưa có hướng dẫn được quản lý trên hệ thống SOC (của Bên B) được tạo và gắn cho Tier 3 (01 sự cố ATTT tương ứng với 01 case)
- Thời gian xử lý sự cố ATTT quy định theo loại sự cố ATTT, cụ thể như sau:
<table>
<tr><td>Loại sự cố ATTT</td><td>Thời gian xử lý</td></tr>
<tr><td>NGHIÊM TRỌNG</td><td><= 4 giờ</td></tr>
<tr><td>BÌNH THƯỜNG</td><td><= 48 giờ</td></tr>
</table></td><td>case sự cố có trạng thái OPEN đến khi case chuyển trạng thái CLOSE</td><td></td><td></td><td></td><td>Case mức Nghiêm trọng)

92% (Với Case mức Bình thường)</td></tr>
</table>