Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

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

1.1 Tên dự toán:

Trang bị cơ sở dữ liệu thám báo an ninh mạng Threat Intelligence

1.2. Tên gói thầu:

Trang bị cơ sở dữ liệu thám báo an ninh mạng Threat Intelligence

1.3. Đơn vị mua sắm:

Công ty Công nghệ thông tin VNPT

1.4. Mục tiêu, quy mô mua sắm:

1.4.1. Mục tiêu:

- Tăng cường hiệu quả phát hiện và ngăn chặn các cuộc tấn công vào các hệ thống cung cấp dịch vụ, phục vụ nội bộ của VNPT; giảm thời gian phản ứng trước các cuộc tấn công; hoàn thiện mô hình hệ thống giám sát an ninh mạng;

- Cập nhật kịp thời nguồn tri thức mới cho dịch vụ VNPT MSS và các dịch vụ kế thừa khác như SmarIR, DNS Protection.

1.4.2. Quy mô:

Gói Bản quyền cơ sở dữ liệu thám báo an ninh mạng Threat Intelligence trong 01 năm.

STT	Danh mục hàng hoá dịch vụ	Thời hạn	Đơn vị tính	Số lượng
1	Bản quyền cơ sở dữ liệu thám báo an ninh mạng Threat Intelligence	01 năm	Gói	01

1.5. Nguồn vốn: Chi phí SXKD

1.6. Địa điểm: Thành phố Hà Nội.

2. Yêu cầu về kỹ thuật

STT	Yêu cầu kỹ thuật
I	**Dữ liệu liên quan đến VNPT**
1	Có khả năng cung cấp thông tin về dữ liệu của các tên miền có yếu tố "vnpt" và VNPT đang quản trị, vận hành, cung cấp dịch vụ trong trường hợp phát hiện các dữ liệu này bị xâm phạm, rò rỉ trên các nguồn đóng và nguồn mở. Tối thiểu phải bao gồm: 1. vnpt.vn 2. vnptit.vn 3. vnpt.com.vn 4. vinaphone.com.vn

STT	Yêu cầu kỹ thuật
	5. vinaphone.vn 6. vnptmedia.vn 7. vnptnet.vn 8. mytv.com.vn 9. vnedu.vn 10. vnptweb.vn 11. vnptigate.vn 12. vnptioffice.vn 13. ecabinet.vn 14. vinaphoneplus.com.vn 15. onesme.vn 16. vnpt-bhxh.vn 17. vnlms.vn 18. iocvnpt.com 19. congdulieuyte.vn 20. dulieuyte.vn 21. hososuckhoe.vn 22. myhealth.vn 23. vncare.vn 24. vnpt-ca.vn 25. vnpt-invoice.com.vn 26. vnptsmartads.vn 27. smartcloud.vn Danh sách các tên miền do VNPT cung cấp và có thể cập nhật, thay đổi định kỳ theo hàng quý.
2	Có khả năng cung cấp thông tin về các dữ liệu của tối thiểu 05 tên miền hoặc thương hiệu do VNPT đang quản trị, vận hành, cung cấp dịch vụ bị xâm phạm, rò rỉ trên các nguồn đóng và nguồn mở. Danh sách các tên miền do VNPT cung cấp và có thể cập nhật, thay đổi định kỳ theo hàng quý.
3	Có khả năng cung cấp dữ liệu về các tài khoản của VNPT và khách hàng sử dụng dịch vụ VNPT MSS bị xâm phạm, rò rỉ trên các nguồn đóng và nguồn mở (bao gồm cả trong các CSDL của website khách bị rò rỉ, tối thiểu bao gồm: - Các loại tài khoản sau đây: + Tài khoản quản trị. + Tài khoản người dùng nội bộ. + Tài khoản khách hàng sử dụng dịch vụ. - Các dịch vụ do VNPT cung cấp, vận hành và phát triển: + Dịch vụ nội bộ: email, xác thực (CAS). + Dịch vụ khách hàng: MyTV, VNPT Money.
4	Có khả năng cung cấp thông tin về các dữ liệu khác liên quan đến VNPT (bao gồm nhưng không giới hạn các dữ liệu sau: lỗ hổng của dịch vụ, ứng dụng, mã nguồn, tấn công, sự kiện xâm phạm, rò rỉ/buôn bán dữ liệu liên quan đến VNPT) bị xâm phạm, rò rỉ trên các nguồn đóng và nguồn mở.
5	Có khả năng cung cấp được thông tin về các trường hợp lạm dụng thương hiệu VNPT để thực hiện việc lừa đảo, thu thập thông tin mà không được cho phép, đánh cắp thông tin cá nhân của người sử dụng (phishing).
6	Có khả năng cung cấp được thông tin, dữ liệu về các loại mã độc, tấn công có chủ đích nhắm tới VNPT và khách hàng sử dụng dịch vụ VNPT MSS.

STT	Yêu cầu kỹ thuật
7	Có phương án hỗ trợ để giảm thiểu rủi ro cho VNPT trong trường hợp phát hiện dữ liệu liên quan đến VNPT bị rò rỉ, phát tán hoặc tên miền giả mạo VNPT.
II	**Dữ liệu về IoC, URL, APT**
1	Có khả năng cung cấp các dữ liệu sau đây dưới định dạng JSON/STIX để tích hợp vào các hệ thống VNPT Cyber Threat Intelligence Platform và các hệ thống SIEM (Qradar, Splunk): - Chỉ báo xâm phạm IOC của mã độc và các nhóm tội phạm, gồm có: địa chỉ IP, tên miền, URL, mã hash. - Các liên kết (URL), tên miền và IP giả mạo hoặc có dấu hiệu giải mạo, lừa đảo. - Máy chủ chỉ huy và điều khiển (C&C) được sử dụng bởi các nhóm tội phạm. - Dữ liệu về các lỗ hổng bao gồm tối thiểu các thông tin (mã CVE, điểm CVSS, phiên bản phần mềm, hệ điều hành bị ảnh hưởng, dẫn nguồn).
2	Có khả năng cung cấp dữ liệu về các mã độc bao gồm tối thiểu các thông tin: - Phân loại mã độc. - Tên tệp tin chứa mã độc. - Nền tảng hệ điều hành hoạt động. - Các tác nhân đe dọa có liên quan đến mã độc. - Phân tích cơ chế hoạt động của mã độc. - Mã hash của tệp tin chứa mã độc. - Chỉ báo tấn công (IOC) nơi phát tán các tệp tin chứa mã độc gồm: địa chỉ IP, URL, tên miền.
3	Cung cấp các tập luật được sử dụng để phát hiện mã độc, tấn công khai thác lỗ hổng bao gồm: - YARA rule (cho mã độc). - Suritaca rule (cho lỗ hổng).
4	Cung cấp các thông tin liên quan các cuộc tấn công từ chối dịch vụ (DdoS) và tấn công thay đổi giao diện (Deface, tối thiểu bao gồm: - Các thông tin DdoS: + Thời gian phát hiện. + Thông tin C&C. + Thông tin IP mục tiêu. + Thông tin loại DdoS. - Các thông tin Deface: + Thời gian phát hiện. + Mục tiêu tấn công. + Thông tin tác nhân đe dọa - threat actor. + Thông tin IP mục tiêu.
III	**Dữ liệu về tội phạm mạng**
1	Giải pháp có khả năng cung cấp và cập nhật thường xuyên hồ sơ về các nhóm tội phạm mạng (còn gọi là các tác nhân đe dọa - threat actor), trong đó phải bao gồm cả hồ sơ về các nhóm tội phạm APT.

STT	Yêu cầu kỹ thuật
2	Giải pháp có khả năng cung cấp các thông tin sau đây trong hồ sơ các nhóm tội phạm, tối thiểu bao gồm: - Chiến thuật, kỹ thuật và quy trình (TTPs) của các nhóm tội phạm mạng và đáp ứng theo khung MITRE ATT&CK. - Công cụ, các lỗ hổng bảo mật mà các nhóm tội phạm mạng sử dụng. - Dấu hiệu nhận biết nhóm tội phạm mạng. - Quốc gia và lĩnh vực mà nhóm tội phạm nhắm đến. - Hoạt động và sự kiện liên quan đến nhóm tội phạm theo dòng thời gian.
3	Giải pháp có khả năng cung cấp dữ liệu về hoạt động của các nhóm APT, tối thiểu bao gồm: - Dữ liệu về các hoạt động tấn công của nhóm APT diễn biến theo dòng thời gian. - Dữ liệu về các chiến dịch được thực hiện bởi nhóm APT. - Dữ liệu được chọn lọc, phân tích, dẫn chứng đầy đủ bởi các chuyên gia.
4	Giải pháp có khả năng cung cấp dữ liệu về các nhóm tội phạm sử dụng mã độc tống tiền (Ransomware) và các hoạt động tấn công, cùng với nạn nhân của các nhóm tội phạm này.
5	Giải pháp có khả năng theo dõi và cung cấp dữ liệu từ Deep/Dark Web về các mối đe dọa (thông tin buôn bán dữ liệu, tấn công khai thác dữ liệu, chia sẻ dữ liệu trái phép), và có khả năng cung cấp bổ sung dữ liệu theo yêu cầu đột xuất.
6	Giải pháp có khả năng cung cấp được thông tin, dữ liệu được chia sẻ từ các cộng đồng, diễn đàn bảo mật riêng tư và từ mạng lưới quan hệ trong cộng đồng hacker được thiết lập bởi các chuyên gia, đặc biệt là khu vực Châu Á nói chung và Việt Nam nói riêng và nêu cụ thể các cộng đồng.
7	Giải pháp có khả năng cung cấp được các thông tin, phân tích các mối đe dọa theo từng tiêu chí, tối thiểu bao gồm: - Phân loại theo các lĩnh vực, bao gồm: viễn thông, tài chính ngân hàng, chính phủ. - Phân loại theo từng quốc gia/nhóm quốc gia, bao gồm Việt Nam.
IV	**Báo cáo**
1	Giải pháp có khả năng cung cấp báo cáo định kỳ theo tháng, quý, năm và báo cáo cho khoảng thời gian tùy chọn, có thể tạo báo cáo dành riêng theo yêu cầu của VNPT.
2	Giải pháp có khả năng cung cấp các báo cáo tổng hợp thông tin các mối đe dọa, các loại mã độc theo từng tiêu chí tối thiểu gồm: - Báo cáo theo các lĩnh vực, bao gồm: viễn thông, tài chính ngân hàng, chính phủ. - Báo cáo theo khu vực, bao gồm Châu Á. - Báo cáo theo từng quốc gia/nhóm quốc gia, bao gồm Việt Nam.
3	Giải pháp có khả năng cung cấp các báo cáo chiến lược về sự thay đổi bối cảnh, xu hướng của các mối đe dọa trên không gian mạng theo chu kỳ 6 tháng, 1 năm, đặc biệt là khu vực châu Á và Việt Nam.
V	**Các yêu cầu khác**
1	Giải pháp cung cấp được portal để tra cứu các dữ liệu về tội phạm mạng, các dữ liệu APT, lỗ hổng và các dữ liệu liên quan đến VNPT.
2	Giải pháp phải thể hiện được xu hướng, thông tin nổi trội trên Portal về tình hình ATTT trong ngày/tuần có khu vực ASIA hoặc Việt Nam.
3	Cung cấp ít nhất 5 tài khoản có quyền tra cứu thông tin TI và tích hợp dữ liệu TI vào các hệ thống khác.
4	Có khả năng phân tích, cung cấp dữ liệu về các nhóm tội phạm thuộc các cộng đồng ngôn ngữ khác nhau. Tối thiểu bao gồm các loại ngôn ngữ như sau: tiếng Anh, tiếng Trung, tiếng Nga, tiếng Việt.

STT	Yêu cầu kỹ thuật
5	Giải pháp tích hợp được với hệ thống VNPT Cyber Threat Intelligence Platform hoặc các hệ thống SIEM (Qradar, Splunk).
6	Có khả năng gửi cảnh báo qua một trong các phương thức sau Email/SMS.
7	Có khả năng hỗ trợ phân tích mẫu mã độc, mối đe dọa thông qua một trong các kênh bao gồm: Portal, Email, Service Desk.
8	Thời hạn sử dụng, khai thác dữ liệu thám báo an ninh mạng tối thiểu 01 năm.

3. Các yêu cầu khác

TT	Nội dung yêu cầu	
1	Dịch vụ bảo hành, hỗ trợ kỹ thuật	Nhà thầu cam kết dịch vụ bảo hành, hỗ trợ kỹ thuật 24/7 tối thiểu 12 tháng kể từ thời điểm nghiệm thu đưa vào sử dụng.
2	Điều kiện hợp đồng	Nhà thầu cam kết đáp ứng các quy định tại Chương VI. Điều kiện chung của hợp đồng và Chương VII. Điều kiện cụ thể của hợp đồng;

Lưu ý: ***<u>Tài liệu chứng minh Yêu cầu kỹ thuật của hàng hóa:</u>***

Ngoài việc giới thiệu và trình bày tổng thể, chi tiết về hàng hóa và dịch vụ, nhà thầu phải trả lời mức độ đáp ứng các yêu cầu kỹ thuật theo mẫu sau đây:

TT	Yêu cầu	Mức độ đáp ứng (chọn Đạt/Không Đạt)	Dẫn chứng trong E-HSDT
[Yêu cầu trong E-HSMT]	Yêu cầu: [đưa phần mô tả yêu cầu từ E-HSMT]		Chỉ dẫn tới dẫn chứng trong E-HSDT

Nhà thầu phải nêu rõ đã giải thích/dẫn chứng tại phần nào, mục nào, tài liệu nào của E-HSDT đáp ứng yêu cầu kỹ thuật gì trong E-HSMT, để bên mời thầu dễ dàng tham chiếu khi xem xét E-HSDT.

Trường hợp nhà thầu chỉ dẫn, dẫn chiếu không đúng, hoặc thông tin trong E-HSDT được trích dẫn không chính xác, và thông tin trong E-HSDT không được tìm thấy trên các địa chỉ chính thức của hãng sản xuất sản phẩm dự thầu đáp ứng yêu cầu kỹ thuật trong E-HSMT thì yêu cầu đó coi như trả lời không hợp lệ và chấm không đạt.

Cung cấp tài liệu kỹ thuật (catalogue, datasheet, hướng dẫn sử dụng...) để chứng minh tuyên bố đáp ứng, cũng như nêu rõ nguồn gốc của các tài liệu này. Trong trường hợp tài liệu kỹ thuật nhà thầu cung cấp có nội dung khác với tài liệu kỹ thuật trên website chính thức của Hãng sản xuất thì bên mời thầu sẽ căn cứ theo tài liệu kỹ thuật trên website chính thức của Hãng sản xuất để đánh giá về khả năng đáp ứng yêu cầu kỹ thuật của hàng hóa chào thầu.

Mục 2. Bản vẽ

Không có bản vẽ

Mục 3. Kiểm tra và thử nghiệm

Theo Chương VII. Điều kiện cụ thể của hợp đồng - Mục E_ĐKC 21.1.