Phần 2

CHƯƠNG V. YÊU CẦU KỸ THUẬT

1. Phạm vi triển khai:

STT	Hạng mục mua sắm	Số lượng	Đơn vị
1.	Thuê Giải pháp Digital Risk Protection trong 2 năm	1	Gói

Địa điểm triển khai: Khối CNTT – Ngân hàng TMCP Công thương Việt Nam

2. Yêu cầu kỹ thuật Thuê Giải pháp Digital Risk Protection trong 2 năm:

STT	Nội dung yêu cầu
1	**Yêu cầu chung**
1.1	Có khả năng tận dụng nhiều nguồn dữ liệu để phân tích, quản lý nhiều nguồn dữ liệu tình báo về mối đe dọa và xác minh mức độ liên quan và chính xác của dữ liệu
1.2	Có khả năng tự động phân tích các thông tin thu thập được để xác định nội dung có độc hại hay không và/hoặc gây rủi ro cho khách hàng bằng việc sử dụng kĩ thuật fingerprinting, heuristics,…
1.3	Giải pháp sử dụng honeypots để thu thập nội dung lừa đảo và spam
1.4	**Giải pháp cung cấp cho khách hàng khả năng** tự thêm các mối đe dọa/nghi ngờ về website, tên miền, truyền thông xã hội, di động và web mở có liên quan tới thương hiệu của khách hàng để theo dõi/phân tích
1.5	Giải pháp có khả năng phá vỡ toàn bộ hệ sinh thái tội phạm mạng bằng cách thực hiện một hoặc nhiều hành động sau: - Triệt phá các điểm rút dữ liệu (data drops) và công cụ phát tán email lừa đảo (mailers) - Ngăn chặn các kênh phân phối bộ công cụ phishing (phishing kit distribution) - Điều tra và phân tích các hoạt động rút tiền phi pháp (cash out operations) - Thực hiện giám sát liên tục để phát hiện và theo dõi các mối đe doạ tiềm tàng (ongoing reconnaissance)
1.6	Giải pháp sẽ phản hồi yêu cầu không quá 1 giờ
1.7	Giải pháp hỗ trợ gỡ bỏ/ngăn chặn nội dung độc hại và/hoặc trái phép trong vòng 72 giờ
2	**Yêu cầu liên quan đến Trang web Đánh cắp Thông tin xác thực**
2.1	Giải pháp có khả năng thu thập các thông tin sau: URL mối đe dọa, địa chỉ IP của trang web, công ty Webhosting và ASN lưu trữ trang web, các bộ công cụ lừa đảo được sử dụng cho cuộc tấn công, vị trí thả dữ liệu/địa chỉ email bị đánh cắp

2.2	Giải pháp có thể thu thập các thông tin sau từ các bộ công cụ lừa đảo: - Các địa chỉ email được liên kết với trang web đánh cắp thông tin xác thực - Vị trí của dữ liệu bị đánh cắp - Các lỗ hổng tiềm ẩn trong mã trang web có thể được sử dụng để hỗ trợ gỡ xuống hoặc phát hiện ra các tác nhân đe dọa
2.3	Giải pháp sử dụng beacon phát hiện để cảnh báo khách hàng khi nội dung web của họ bị sao chép và tiến hành phân tích rủi ro độc hại
2.4	Giải pháp cho phép khách hàng mở rộng tìm kiếm của họ để tìm kiếm nội dung độc hại được lưu trữ trên cùng một dải IP
2.5	Giải pháp hỗ trợ khách hàng khôi phục danh tính bị đánh cắp
2.6	Giải pháp sẽ vô hiệu hóa các số điện thoại Vishing
2.7	Giải pháp sẽ cung cấp API hỗ trợ Khách hàng trong việc tích hợp với các giải pháp TI khác để gỡ bỏ Trang web đánh cắp thông tin đăng nhập
3	**Yêu cầu liên quan đến tên miền**
3.1	Giải pháp có thể giám sát việc tạo ra các tên miền mới cụ thể
3.2	Giải pháp có thể giám sát Chứng chỉ SSL mới đăng ký
3.3	Giải pháp có thể xác định xem miền có độc hại và/hoặc trái phép hay không dựa trên các thông tin sau: Ảnh chụp màn hình, URL mối đe dọa, Bản ghi MX, Dữ liệu WHOIS
3.4	Giải pháp có thể thông báo cho khách hàng khi các tên miền độc hại và/hoặc trái phép đang được theo dõi có bất kỳ thay đổi nào
4	**Yêu cầu liên quan đến Truyền thông xã hội**
4.1	Giải pháp có thể phát hiện nội dung độc hại được liên kết sai với thương hiệu của khách hàng
4.2	Giải pháp có thể phát hiện mã nguồn thuộc quyền sở hữu của khách hàng đang được sử dụng cho mục đích xấu
4.3	Giải pháp sử dụng Web Crawler với các nguồn như: Các trang web truyền thông xã hội, Blog/Diễn đàn; Trang web Paste, Gripe và tin tức để tìm các kết quả trùng khớp với các nội dung độc hại.
4.4	Giải pháp có khả năng thu thập các thông tin sau: Ảnh chụp màn hình, trang web nguồn, URL mối đe dọa, chi tiết về tác nhân đe dọa
5	**Yêu cầu liên quan đến Di Động**
5.1	Giải pháp có thể phát hiện các loại mối đe dọa trên di động như: Ứng dụng có rủi ro bảo mật, ứng dụng nhân bản và ứng dụng bị sử dụng trái phép
5.2	Giải pháp có thể thu thập được các thông tin sau: Ảnh chụp màn hình, URL tải xuống ứng dụng, mô tả ứng dụng

5.3	Giải pháp sử dụng trình thu thập dữ liệu web để tìm các ứng dụng có sử dụng thương hiệu của khách hàng trong các ứng dụng có sẵn trên cả cửa hàng ứng dụng chính và phụ của các hệ điều hành sau: - Apple iOS - Blackberry Android - Google Android - Microsoft Windows dành cho điện thoại di động
6	**Yêu cầu liên quan đến Web Mở**
6.1	Giải pháp có thể thu thập được các thông tin sau: Ảnh chụp màn hình, URL mối đe dọa
6.2	Giải pháp sẽ sử dụng trình thu thập thông tin web để xác định xem nội dung có khả năng sử dụng trái phép thương hiệu của khách hàng hay không
7	**Yêu cầu liên quan đến Dark Web**
7.1	Giải pháp có thể thu thập thông tin từ các nguồn trong Dark Web, bao gồm: - Các trang trên Dark Web - Diễn đàn - Nhóm thảo luận - Nơi mua bán
7.2	Giải pháp có thể thu thập được các thông tin sau: - Ảnh chụp màn hình - URL mối đe dọa - Nguồn nội dung - Thông tin về Tác nhân đe dọa
7.3	Giải pháp có thể tìm kiếm thông tin độc hại và bị xâm phạm, bao gồm: - Bộ công cụ lừa đảo - Công cụ gian lận - Tài khoản nhân viên - Dữ liệu người tiêu dùng - Dữ liệu tài chính bị đánh cắp (thẻ tín dụng và thông tin đăng nhập khác) - Các nguồn PII bị rò rỉ khác

- Nhà thầu cần cung cấp câu trả lời giải thích/dẫn chứng cho mỗi yêu cầu kỹ thuật chi tiết.
- Đối với mỗi yêu cầu, Nhà thầu cần giải thích chi tiết, rõ ràng và cung cấp thông tin, dẫn chứng để tuyên bố đáp ứng (như catalogue, datasheet, hướng dẫn sử dụng, …).
- Trong trường hợp Nhà thầu cung cấp tham chiếu đến các thông tin chi tiết, thông tin tham chiếu phải xác định rõ tên tài liệu, số trang và đoạn tài liệu.
- Để trả lời đối với từng yêu cầu, đề nghị Nhà thầu sử dụng Bảng mẫu Trả lời dưới đây:

Stt	Yêu cầu	Mức độ đáp ứng (Chọn Đáp ứng/Không đáp ứng)	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. Trong trường hợp tài liệu có giải thích/dẫn chứng bằng tiếng nước ngoài, nhà thầu phải cung cấp bản dịch sang tiếng Việt và chịu trách nghiệm về tính chính xác của bản dịch.

Trường hợp E-HSDT thiếu các tài liệu theo yêu cầu, hoặc nhà thầu chỉ dẫn, dẫn chiếu không đúng, hoặc thông tin trong E-HSDT được trích dẫn không chính xác, hoặc thông tin trong E-HSDT không được tìm thấy trên các địa chỉ của chính hãng cung cấp sản phẩm, dịch vụ, hoặc không có cơ sở để cho rằng sản phẩm, dịch vụ dự thầu có cấu hình tương đương hoặc đáp ứng yêu cầu kỹ thuật trong E-HSMT thì Chủ đầu tư sẽ yêu cầu nhà thầu làm rõ E – HSDT trên cơ sở tuân thủ quy định tại Mục 23 E – CDNT.