Chương V. Yêu cầu về kỹ thuật

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự án, gói thầu

- Tên dự án: Trang bị bổ sung license giải pháp tự động phát hiện và phản hồi EDR;
- Mục tiêu: Đảm bảo hiệu năng của hệ thống EDR phục vụ bảo vệ các máy chủ, máy ảo cung cấp dịch vụ của VNPT;
- Quy mô: 01 máy chủ master (cấu hình tối thiểu: CPU 32 Cores, RAM 256 GB; Lưu trữ 500GB SSD); 04 máy chủ minion (cấu hình tối thiểu: CPU 32 Cores, RAM 256 GB; Lưu trữ khả dụng 11TB SSD); 1800 license;
- Chủ đầu tư: Công ty Công nghệ thông tin VNPT;
- Tên gói thầu: Cung cấp lắp đặt hàng hóa;
- Hình thức, phương thức lựa chọn nhà thầu: Chào hàng cạnh tranh trong nước; một giai đoạn một túi hồ sơ, áp dụng lựa chọn nhà thầu qua mạng;
- Thời gian thực hiện gói thầu: 128 ngày;
- Loại hợp đồng: Trọn gói.

1.2. Yêu cầu về kỹ thuật

STT	Yêu cầu
I	**Yêu cầu kỹ thuật**
A	**Phần mềm cho hệ thống EDR**
1	Có sẵn tính năng phát hiện hành vi, kết nối bất thường dựa trên tập luật định sẵn.
2	Có sẵn tính năng phát hiện hành vi, kết nối bất thường dựa trên tập luật tùy chỉnh.
3	Có sẵn tính năng phát hiện hành vi, kết nối bất thường dựa trên dữ liệu Threat Intelligence.
4	Có tính năng quản lý với điểm cuối thông qua giao diện quản lý tập trung.
5	Có tính năng tương tác với điểm cuối phục vụ ứng cứu sự cố.
6	Có tính năng chặn lọc file, binary
7	Có tính năng cách ly và ngắt cách ly điểm cuối trên toàn mạng qua giao diện tập trung
8	Có tính năng tìm kiếm dữ liệu trên điểm cuối với tối thiểu các tham số sau: process name, ID, hash, command, alert level, IP
9	Có tính năng ghi log hành vi, kết nối đã thực hiện trên điểm cuối và đối chiếu với các dữ liệu tương quan trên các điểm cuối khác nhằm xây dựng biểu đồ lây lan, kết nối
10	Có khả năng phát hiện và cảnh báo toàn trình của các cuộc tấn công mạng bao gồm: khai thác, cài đặt mã độc, lây lan, kết nối với máy chủ C&C và thực hiện hành vi bất thường

STT	Yêu cầu
11	Có khả năng phát hiện và cảnh báo lateral movement
12	Có khả năng Thu thập dữ liệu về các sự kiện khởi tạo, mở, kết thúc tiến trình
13	Có khả năng Thu thập dữ liệu về các kết nối mạng
14	Có khả năng Thu thập các thông tin thay đổi registry
15	Có khả năng Thu thập sự kiện thay đổi quyền hạn của file, tiến trình
16	Có khả năng Thu thập dữ liệu theo thời gian thực
17	Có khả năng trích xuất báo cáo, phân loại, thống kê về các hành vi, cảnh báo
18	Tương thích với hệ điều hành Windows và Linux
19	Thời hạn sử dụng phần mềm tối thiểu 36 tháng
B	**Phần cứng**
B.1	**Máy chủ Loại 1**
1	Có tối thiểu 02 CPU vật lý, tổng số tối thiểu 32 core vật lý
2	Bộ vi xử lý có tốc độ tối thiểu 2.0 GHz
3	Có sẵn tối thiểu 256 GB RAM, có khả năng nâng cấp lên 512 GB RAM
4	Dung lượng các thanh RAM bằng nhau và tối thiểu 32 GB
5	Tối thiểu 16 khe cắm RAM
6	Có sẵn tối thiểu 02 ổ SSD, dung lượng mỗi ổ tối thiểu 500GB, DWPD ≥ 1
7	Có sẵn RAID Controller hỗ trợ các cấu hình RAID0, RAID1, Non-RAID/pass-through, có cache battery
8	Có tối thiểu 02 port Ethernet quang tốc độ tối thiểu 10Gb/s, có sẵn transceiver SR Multimode
9	Có tối thiểu 01 port quản trị remote tốc độ tối thiểu 100Mb/s
10	Nguồn điện AC, hoạt động được ở điện áp 220V, tần số 50Hz
11	Có module nguồn dự phòng N+1 (N≥1), cho phép thay thế nóng.
12	Module nguồn đạt chứng chỉ 80 Plus Platinum hoặc 80 Plus Titanium
13	Dạng rackmount cho tủ rack kích thước rộng 19 inch
14	Có sẵn cổng quản trị cho phép cài đặt, bật tắt máy từ xa, kết nối Virtual Media
15	Có sẵn giải pháp/phần mềm cho phép quản trị, cài đặt máy chủ và nâng cấp firmware tất cả các thành phần phần cứng của máy chủ tập trung với đầy đủ bản quyền hợp pháp, không giới hạn thời gian sử dụng
16	Hỗ trợ Hyper-threading hoặc tương đương
17	Hỗ trợ các công nghệ ảo hoá như VMware, Hyper-V, KVM-based Hypervisor
18	Tương thích tối thiểu một trong số các hệ điều hành sau: - Linux Ubuntu (20.04LTS trở lên)

STT	Yêu cầu
	- Red Hat Enterprise Linux 8.8 trở lên - Windows Server 2022 trở lên
B.2	**Máy chủ Loại 2**
1	Có tối thiểu 02 CPU vật lý, tổng số tối thiểu 32 core vật lý
2	Bộ vi xử lý có tốc độ tối thiểu 2.0 GHz
3	Có sẵn tối thiểu 256 GB RAM, có khả năng nâng cấp lên 512 GB RAM
4	Dung lượng các thanh RAM bằng nhau và tối thiểu 32 GB
5	Tối thiểu 16 khe cắm RAM
6	Có sẵn tối thiểu 02 ổ SSD, dung lượng mỗi ổ tối thiểu 500GB, DWPD ≥ 1
7	Có sẵn tối thiểu 6 ổ cứng SAS SSD Enterprise, dung lượng mỗi ổ cứng tối thiểu 3.8 TB hoặc dung lượng lưu trữ khả dụng tối thiểu 11TB (cấu hình RAID10)
8	Hỗ trợ cấu hình RAID10
9	Có tối thiểu 02 port Ethernet quang tốc độ tối thiểu 10Gb/s, có sẵn transceiver SR Multimode
10	Có tối thiểu 01 port quản trị remote tốc độ tối thiểu 100Mb/s
11	Nguồn điện AC, hoạt động được ở điện áp 220V, tần số 50Hz
12	Có module nguồn dự phòng N+1 (N≥1), cho phép thay thế nóng.
13	Module nguồn đạt chứng chỉ 80 Plus Platinum hoặc 80 Plus Titanium
14	Dạng rackmount cho tủ rack kích thước rộng 19 inch
15	Có sẵn cổng quản trị cho phép cài đặt, bật tắt máy từ xa, kết nối Virtual Media
16	Có sẵn giải pháp/phần mềm cho phép quản trị, cài đặt máy chủ và nâng cấp firmware tất cả các thành phần phần cứng của máy chủ tập trung với đầy đủ bản quyền hợp pháp, không giới hạn thời gian sử dụng
17	Hỗ trợ Hyper-threading hoặc tương đương
18	Hỗ trợ các công nghệ ảo hoá như VMware, Hyper-V, KVM-based Hypervisor
19	Tương thích tối thiểu một trong số các hệ điều hành sau: - Linux Ubuntu (20.04 LTS trở lên) - Red Hat Enterprise Linux 8.8 trở lên - Windows Server 2022 trở lên

1.3. Các yêu cầu khác

STT	Yêu cầu
1	Năm sản xuất của máy chủ (loại 1, loại 2): Từ năm 2024 trở về sau
2	- Có hỗ trợ kỹ thuật 24x7 tối thiểu 03 năm kể từ thời điểm nghiệm thu hợp đồng

STT	Yêu cầu
	- Hỗ trợ nâng cấp các phiên bản phần mềm, OS mới trong ít nhất 03 năm - Thay thế phần cứng lỗi trong 12h kể từ thời điểm báo lỗi.
3	Đáp ứng các quy định tại Chương VI. Điều kiện chung của hợp đồng và Chương VII. Điều kiện cụ thể của hợp đồng
4	Thời gian thực hiện hợp đồng ≤ 128 ngày kể từ ngày hợp đồng có hiệu lực

Mục 2. Bản vẽ: Không có bản vẽ.

Mục 3. Kiểm tra và thử nghiệm:

Các kiểm tra và thử nghiệm cần tiến hành gồm có: Theo quy định tại mục 21.1 E-ĐKCT.