Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

1.1. Giới thiệu chung về dự án, gói thầu

1.1.1. Giới thiệu chung về dự án:

Dự án "Nâng cấp, mở rộng Hệ thống điều hành an toàn thông tin (SOC)" là dự án bổ sung nâng cấp các phần cứng, giải pháp phần mềm nhằm nâng cao năng lực xử lý, lưu trữ, mở rộng tính năng điều tra, tương quan, xử lý sự cố và tự động hóa ngăn chặn tấn công của phân hệ SOC quản lý vùng biên và khi hoàn thành triển khai dự án định hướng phân hệ SOC quản lý vùng biên chuyển về thành hệ thống điều hành an toàn thông tin (SOC) tập trung để tối ưu công nghệ và quản trị vận hành hệ thống. Sau khi hoàn thành dự án giải pháp có khả năng ứng dụng trí tuệ nhân tạo (AI), học máy (machine learning) và tích hợp thông tin tình báo (Threat Intelligence) để phát hiện hành vi bất thường theo thời gian thực, khả năng hỗ trợ mở rộng (scalable) và tích hợp với các nguồn nhật ký, sự kiện (log/event) phức tạp (log phi cấu trúc), tích hợp với hạ tầng đám mây, hạ tầng đám mây lai (hybrid cloud) giúp phát hiện sớm các mối đe dọa an ninh, đưa ra phản ứng nhanh chóng với các sự cố bảo mật, tấn công vào hệ thống CNTT của Agribank và đảm bảo tuân thủ, đáp ứng đầy đủ các quy định của Ngân hàng Nhà nước về hoạt động giám sát và ứng cứu xử lý sự cố an toàn thông tin trong hoạt động ngân hàng.

- Tên dự án: Nâng cấp, mở rộng Hệ thống điều hành an toàn thông tin (SOC).

- Tên chủ đầu tư: Ngân hàng Nông nghiệp và Phát triển Nông thôn Việt Nam (Agribank)

- Mục tiêu đầu tư:

+ Nâng cấp năng lực xử lý phần mềm lõi về giám sát, tìm kiếm, phân tích; Mở rộng tính năng phần mềm điều tra, tương quan, xử lý sự cố; Mở rộng tính năng phần mềm tự động hóa ngăn chặn tấn công để đáp ứng yêu cầu về hoạt động giám sát và ứng cứu xử lý sự cố an toàn thông tin trong tình hình hiện nay;

+ Nâng cấp các thiết bị phần cứng để đáp ứng nâng cao năng lực xử lý, lưu trữ cho hệ thống SOC;

+ Đảm bảo tuân thủ, đáp ứng đầy đủ các quy định của Ngân hàng Nhà nước và Agribank về an toàn bảo mật.

- Quy mô đầu tư:

Nâng cấp, mở rộng tại phân hệ SOC quản lý vùng biên bao gồm:

+ Đầu tư phần mềm cho cả Trung tâm dữ liệu chính (PDC) và Trung tâm dữ liệu dự phòng (BDC) trong thời gian 05 năm (kể từ ngày nghiệm thu hợp

đồng):

✓ Đầu tư phần mềm lõi về giám sát, tìm kiếm, phân tích để nâng cao năng lực xử lý, giám sát, tìm kiếm, phân tích với dung lượng xử lý 150GB/ngày hoặc 6000 EPS;

✓ Đầu tư phần mềm điều tra, tương quan, xử lý sự cố để mở rộng tính năng điều tra, cảnh báo sự kiện an ninh với dung lượng xử lý 50 GB/ngày hoặc 2000 EPS;

✓ Đầu tư phần mềm tự động hóa ngăn chặn tấn công để mở rộng tính năng tự động hóa ngăn chặn tấn công, cô lập phạm vi tấn công, phân loại, phối hợp xử lý và khôi phục hệ thống;

+ Trang bị các thiết bị phần cứng để đáp ứng nâng cao năng lực xử lý, lưu trữ cho phân hệ SOC quản lý vùng biên tại PDC;

+ Tổ chức triển khai, tích hợp hệ thống, đào tạo.

- Địa điểm:

Tại các Trung tâm dữ liệu của Agribank gồm:

+ Trung tâm dữ liệu tại tòa nhà C3, phường Phương Liệt, Thành phố Hà Nội;

+ Trung tâm dữ liệu tại khu đất A5-THCT2, Khu đô thị mới Lê Trọng Tấn, xã An Khánh, Thành phố Hà Nội.

- Thời gian thực hiện hợp đồng gói thầu: Tối đa là 06 tháng (bao gồm cả ngày nghỉ, ngày lễ) kể từ ngày hợp đồng có hiệu lực.

- Tổng quan giải pháp:

Nâng cấp, mở rộng hệ thống điều hành an toàn thông tin hoàn chỉnh bao gồm hệ thống chính, hệ thống dự phòng, cụ thể như sau:

+ Hệ thống chính và hệ thống dự phòng được triển khai, cấu hình các phần mềm lõi về giám sát, tìm kiếm, phân tích; phần mềm điều tra, tương quan, xử lý sự cố; phần mềm tự động hóa ngăn chặn tấn công.

+ Hệ thống được thiết kế tại 02 trung tâm dữ liệu chính và dự phòng tương ứng. Các máy chủ, thiết bị trong hệ thống đặt tại các phân vùng mạng phù hợp, các phân vùng đảm bảo an toàn bảo mật theo đúng quy định của Agribank. Ngoài ra, hệ thống được đồng bộ dữ liệu đồng thời đảm bảo tính sẵn sàng, ổn định có thể chuyển site khi có lỗi, sự cố theo mô hình Active/Active hoặc Active/Standby. Các thiết bị đảm bảo tích hợp tương thích với hạ tầng sẵn có của Agribank.

+ Tài nguyên hệ thống chính tại trung tâm dữ liệu chính sẽ đầu tư mới, tài nguyên hệ thống dự phòng sử dụng tài nguyên máy chủ ảo hóa sẵn có của Agribank.

+ Hệ thống phải đảm bảo hiệu năng cao, đáp ứng được tăng trưởng thu thập log trong tối thiểu 05 năm tiếp theo. Đồng thời khả năng tích hợp với các hệ thống log source của Agribank, third-party (Virustotal,Threat Inteligence, v.v…), Cloud (AWS, GCP, Azure, v.v…), v.v… cung cấp mở rộng mà không làm thay

đổi mô hình thiết kế.

1.1.2. Giới thiệu về gói thầu

- Tên gói thầu: Nâng cấp, mở rộng Hệ thống điều hành an toàn thông tin (SOC)
- Nguồn vốn: Sử dụng nguồn vốn đầu tư mua sắm tài sản cố định của Agribank.
- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi, trong nước, qua mạng.
- Loại hợp đồng: Trọn gói.
- Thời gian thực hiện gói thầu: Tối đa là 06 tháng (bao gồm cả ngày nghỉ, ngày lễ) kể từ ngày hợp đồng có hiệu lực.

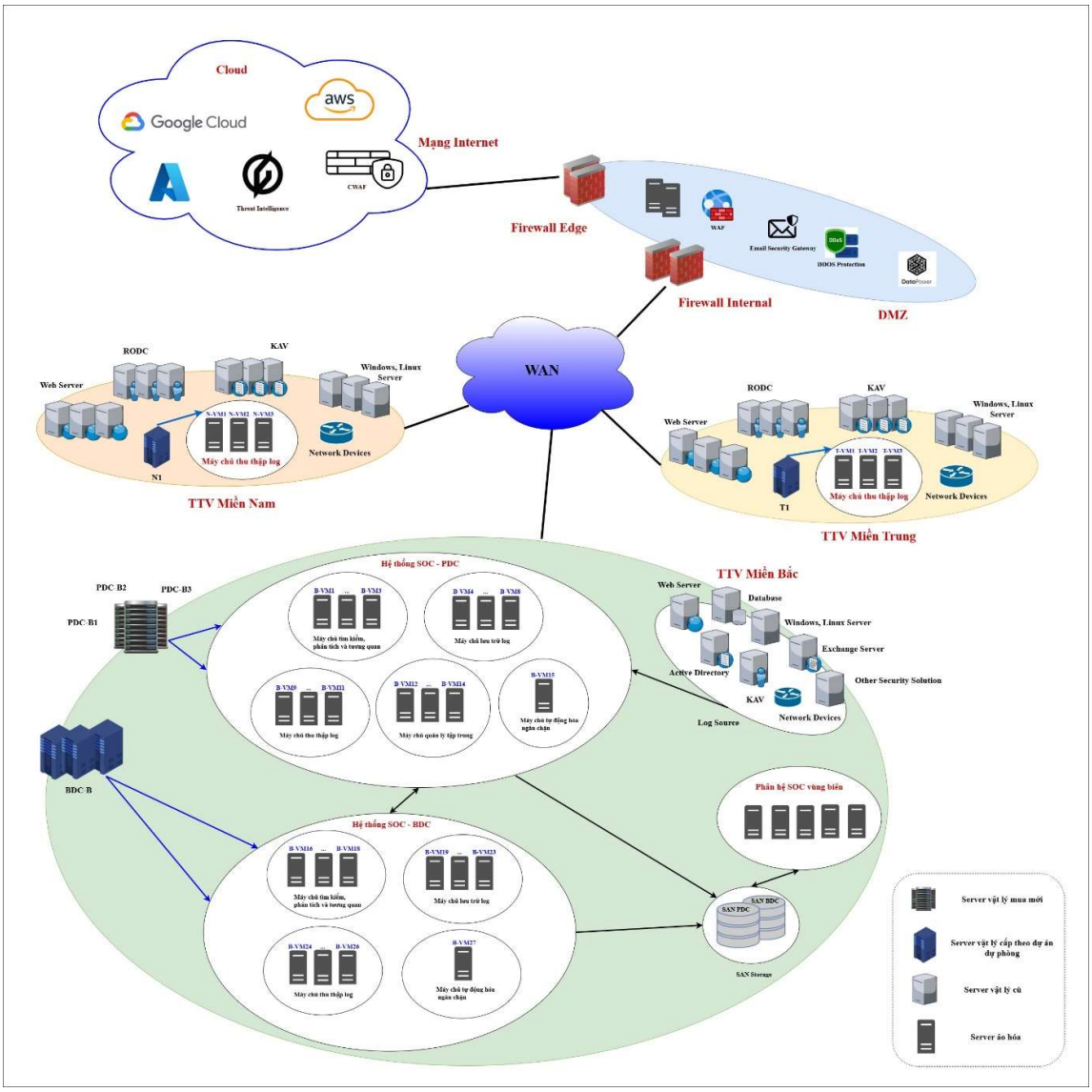
1.2. Yêu cầu về kỹ thuật

1.2.1. Yêu cầu đối với mô hình thiết kế

1.2.1.1. Mô hình thiết kế được đề xuất sẽ phải đảm bảo các nguyên tắc sau:

- Đảm bảo có khả năng khai thác kết nối thu thập dữ liệu từ các Trung tâm dữ liệu chính, Trung tâm dữ liệu dự phòng, Trung tâm vùng Miền Trung, Trung tâm vùng Miền Nam và các thành phần hạ tầng khác của Agribank (như hạ tầng đám mây, hạ tầng đám mây lai (hybrid cloud), v.v…) về lưu trữ tập trung tại PDC và BDC.
- Đảm bảo khả năng vận hành các quy tắc (rule) dựa trên chức năng nhiệm vụ của các nhóm giám sát level 1,2,3, nhóm quản trị, xây dựng content/playbook tham gia vào giám sát, xử lý điều tra các cảnh báo an ninh.
- Đảm bảo khả năng lưu trữ theo yêu cầu và theo quy định của nhà nước.
- Dễ dàng mở rộng bản quyền (license).
- Dễ dàng mở rộng năng lực hệ thống theo bề ngang: Bổ sung dễ dàng các thành phần vào các cụm máy chủ mà không cần phải thay thế thành phần đang có.

1.2.1.2. Mô hình triển khai tổng thể của hệ thống SOC sau khi nâng cấp, mở rộng



Hình 1: Mô hình triển khai tổng thể Hệ thống điều hành An toàn thông tin nâng cấp, mở rộng

Về mặt tổng thể, hệ thống SOC được đặt tại Trung tâm dữ liệu chính và Trung tâm dữ liệu dự phòng (đóng vai trò trung tâm giám sát và xử lý dữ liệu an ninh từ toàn bộ hệ thống mạng của Agribank) bao gồm các thành phần thu thập, lưu trữ, xử lý dữ liệu, giám sát, tìm kiếm, phân tích; điều tra tương quan, xử lý sự cố và tự động hóa ngăn chặn tấn công (Tham chiếu mục 2.4 mô hình thiết kế hệ thống SOC chi tiết).

Các vùng mạng của Agribank:

- Hệ thống điều hành an toàn thông tin sẽ đặt tại Trung tâm dữ liệu chính và Trung tâm dữ liệu dự phòng. Thu thập toàn bộ log source tại trung tâm dữ liệu chính và dự phòng như: trang thiết bị Network/Network Security, thiết bị an ninh bảo mật, ứng dụng, cơ sở dữ liệu, log audit máy chủ, v.v...

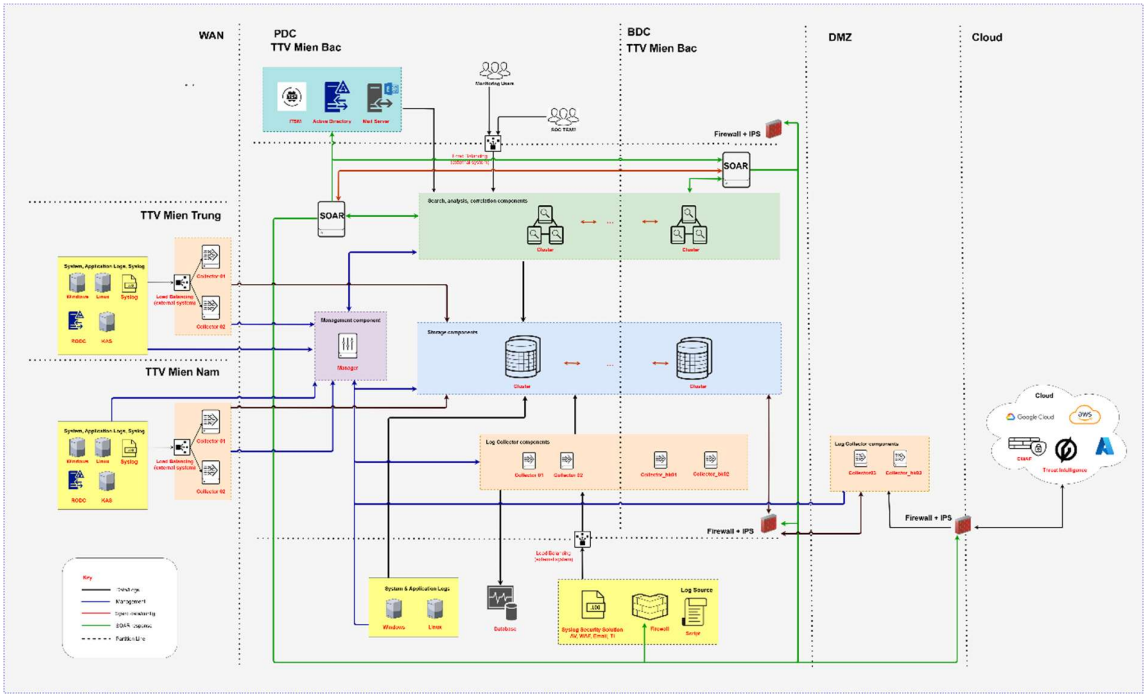
- Trung tâm vùng Miền Nam và Miền Trung: Triển khai các máy chủ thu thập log để tích hợp các nguồn log source tại các trung tâm vùng Miền Trung và Miền Nam: Hệ thống máy chủ, AD/RODC, Network Device, KAS, Email, v.v…và gửi về TTDL chính và TTDL dự phòng. Thành phần Load balancing dùng để cân bằng tải hai máy chủ thu thập log thông qua cấu hình Load balancing mềm. Trong tương lai khi nâng cấp hệ thống mạng lên SD-WAN sẽ loại bỏ các máy chủ thu thập log tại các Trung tâm vùng Miền Trung, Miền Nam này.

- Thành phần thu thập và chuyển tiếp dữ liệu log tại vùng mạng DMZ. Thành phần này đóng vai trò thu thập log/data từ các hệ thống bên ngoài mạng Agribank như: Google Cloud, AWS, Azure; các dịch vụ như Threat Intelligence, CWAF - Cloud Web Application Firewall, v.v...

Sơ đồ tổng thể trên đáp ứng đầy đủ khả năng của một hệ thống điều hành an toàn thông tin trong thu thập dữ liệu, giám sát tại các Trung tâm dữ liệu chính, Trung tâm dữ liệu dự phòng, Trung tâm vùng Miền Trung, Trung tâm vùng Miền Nam, hạ tầng đám mây, hạ tầng đám mây lai (hybrid cloud).

Mô hình triển khai sử dụng kiến trúc cluster cho các thành phần trọng yếu nhằm hỗ trợ khả năng mở rộng theo chiều ngang (horizontal scaling) và đảm bảo tính sẵn sàng cao (HA). Mô hình đảm bảo luồng dữ liệu được thu thập, xử lý và lưu trữ xuyên suốt, đồng thời duy trì khả năng truy vấn, phân tích và tương quan sự kiện một cách liên tục.

1.2.1.3. Mô hình triển khai chi tiết các thành phần nâng cấp, mở rộng hệ thống điều hành an toàn thông tin của Agribank



Hình 2: Mô hình triển khai chi tiết các thành phần hệ thống điều hành an toàn thông tin SOC nâng cấp, mở rộng

Chi tiết các thành phần Hệ thống SOC trong mô hình:

- Thành phần máy chủ giám sát, tìm kiếm, phân tích và điều tra, tương quan, xử lý sự cố: Thực hiện giám sát, phân tích và điều tra truy vết. Các máy chủ này hoạt động trong một cluster đồng bộ được đặt tại 2 site PDC và BDC sử dụng mô hình active – active, cho phép người dùng truy cập dashboard, report và dữ liệu truy vấn từ bất kỳ node nào trong cụm thông qua cơ chế Load Blancer. Điều này đảm bảo tính sẵn sàng và liên tục, ngay cả khi một node gặp sự cố. Bên cạnh đó với cấu hình cluster, toàn bộ các máy chủ sẽ được quản trị tập trung và tự động chia tải.

+ Thành phần máy chủ lưu trữ dữ liệu log: Phụ trách lưu trữ log của toàn hệ thống, bao gồm cả log giám sát từ hệ thống Agribank và log nội bộ từ hệ thống SIEM. Dữ liệu được lưu phân tán qua nhiều node, với mỗi bản ghi log (raw data và search data) được nhân bản ba lần và phân phối ngẫu nhiên trong cluster. Điều này bảo đảm dữ liệu vẫn có thể truy cập và phục hồi kể cả khi một hoặc nhiều node bị lỗi. Hệ thống cũng đảm bảo tối thiểu 1 bản ghi log được lưu trữ trên site BDC ứng phó sự cố, dự phòng thảm hoạ.

+ Thành phần máy chủ quản trị (Manager): Quản lý và điều phối toàn bộ hoạt động của hệ thống SIEM – SOC, bao gồm cấu hình, giám sát trạng thái và vận hành hệ thống.

+ Thành phần thu thập log (Collectors): Bao gồm các máy chủ Collector (đặt tại Trung tâm dữ liệu chính, Trung tâm dữ liệu dự phòng, Trung tâm vùng Miền Trung, Trung tâm vùng Miền Nam), chịu trách nhiệm thu thập nhật ký, sự kiện (log/event) toàn bộ Trung tâm dữ liệu chính, Trung tâm dữ liệu dự phòng: các thiết bị an ninh, thiết bị Network/Network Security, máy chủ, ứng dụng, cơ sở dữ liệu,v.v…; thu thập nhật ký, sự kiện (log/event) hạ tầng đám mây, đám mây lai: CWAF, Threat Intelligence,v.v…; thu thập nhật ký, sự kiện (log/event) Trung tâm vùng Miền Trung và Trung tâm vùng Miền Nam: Email, AD, RODC, Antivirus,v.v…

+ Thành phần tự động hóa ngăn chặn tấn công: máy chủ SOAR (Security Orchestration, Automation and Response) để thực thi các playbook tự động, hỗ trợ tối ưu hóa quy trình xử lý sự cố trong SOC. Hệ thống này được tích hợp với ITSM, mail server và Active Directory, giúp tạo và phân phối ticket, đồng thời thực hiện xác thực người dùng thông qua LDAP.

- Giải pháp Dự phòng Thảm họa (Disaster Recovery – DR):

+ Yêu cầu các máy chủ đầu tìm kiếm và lưu trữ log được phân bổ tại hai site PDC/BDC theo tỉ lệ tối thiểu 1:1 để đảm bảo hiệu suất xử lý theo mô hình active active, đảm bảo ngay cả khi một site gặp sự cố, hệ thống vẫn có thể hoạt động với tối thiểu 1/3 năng lực.

+ Yêu cầu dữ liệu log (raw và search) trong cụm lưu trữ được cấu hình sao

cho luôn có tối thiểu 01 bản sao trên các node khác nhau thuộc các site khác nhau, bảo đảm tính toàn vẹn, tối ưu nguồn tài nguyên và khả năng phục hồi khi có sự cố.

+ Dữ liệu tìm kiếm được đồng bộ và nhân bản trên tất cả các máy chủ tìm kiếm, luôn sẵn sàng kể cả trên hệ thống dự phòng BDC.

+ Các thành phần quản trị và Collector do không yêu cầu tính liên tục cao sẽ được sao lưu cấu hình định kỳ và chuẩn bị sẵn máy chủ dự phòng tại site BDC để thực hiện chuyển đổi khi cần thiết, không ảnh hưởng đến hoạt động kết nối chung.

- Yêu cầu hạ tầng bổ sung:

+ Load Balancer cho cụm đầu giám sát, tìm kiếm, phân tích: sử dụng hạ tầng Load Balancer cứng của Agribank thông qua tích hợp thiết bị F5.

+ Load Balancer cho cụm thu thập dữ liệu tại trung tâm vùng Miền Trung, Miền Nam: sử dụng Load Balancer mềm và đặt Load Balancer trước các thành phần thu thập nhằm phân phối đồng đều đến các đầu collector thu thập, đảm bảo khả năng thu thập ổn định, sẵn sàng.

- Yêu cầu thiết kế workflow Level/Tier 1,2,3,4 tham gia vận hành:

SOC Leader, Tier 1,2,3,4 và tuân thủ (Compliance) & báo cáo (Reporting) SOC.

1.2.2. Yêu cầu chi tiết về phần cứng

1.2.2.1. Danh mục phần cứng cần thiết đầu tư

TT	Danh mục phần cứng	Đơn vị tính	Số lượng
1	Máy chủ	Node	03
2	Switch kết nối nội bộ	Chiếc	02

1.2.2.2. Yêu cầu chi tiết

TT	Tiêu chí	Thông số kỹ thuật tối thiểu hoặc tương đương	Số lượng
I	**Hệ thống máy chủ**		**01 hệ thống**
1	Thông số kỹ thuật của mỗi node tại PDC		03 node
1.1	Form factor	Rack-mount	
1.2	Processor	2 x Intel Gold 5rd Generation 32 core 2.8 GHz	
1.3	Memory	- 256 GB - Up to 8TB	
1.4	Internal Storage	- 10 x 3,84TB SSD Disk - Up to 24 disk	
1.5	Boot Storage	2 x 960GB SSD, RAID 1	

TT	Tiêu chí	Thông số kỹ thuật tối thiểu hoặc tương đương	Số lượng
1.6	Network	- 2 x 10/25Gb port - Including 02 x 25Gb transceiver	
		1 x 1GbE RJ45 port (mgmt)	
1.7	Power Supply	Dual redundant power supply	
1.8	Fan	Redundant cooling fans	
1.9	Bản quyền phần mềm hệ thống được tích hợp với máy chủ có đầy đủ tính năng	- Clustering and scaling: Có khả năng mở rộng tới 16 nodes cho mỗi cluster - Có khả năng thêm (add) node để mở rộng cluster - Có khả năng thêm (add) disk để mở rộng dung lượng - Hỗ trợ đồng bộ synchronous and asynchronous - Có khả năng kết nối tới tủ đĩa ngoài	
		Tính năng ảo hóa lưu trữ: - Có khả năng quản lý các thiết bị/phân vùng lưu trữ khác nhau và tạo ra một không gian lưu trữ ảo (virtual storage space) mà các máy tính khác có thể truy cập và sử dụng như một đơn vị lưu trữ duy nhất - Cơ chế bảo vệ dữ liệu: mirror - Mã hóa dữ liệu tại lớp lưu trữ - Deduplication tại lớp lưu trữ: có khả năng thiết lập deduplication tại mức Volume - Thin provisioning: có khả năng thiết lập Thin provisioning tại mức Volume	
		Tính năng ảo hóa máy chủ: - Tạo máy chủ ảo trên cluster - Hỗ trợ hệ điều hành trên máy chủ ảo: Windows Server, Red Hat Enterprise Linux, Oracle Linux, CentOS, FreeBSD	
		Management: - Onpremise Dashboard quản lý, giám sát trạng thái và tài nguyên của Cluster gồm VM, Storage, Network và quản lý Update phần mềm	

TT	Tiêu chí	Thông số kỹ thuật tối thiểu hoặc tương đương	Số lượng
		- Hỗ trợ khả năng tích hợp quản lý, giám sát Cluster trên Cloud của chính hãng phần mềm - Một đầu mối hỗ trợ kỹ thuật duy nhất cho cả phần cứng và phần mềm	
2	Thông số kỹ thuật của mỗi chiếc Switch kết nối nội bộ tại PDC (Cùng hãng sản xuất với hệ thống máy chủ tại PDC)		02 Chiếc
2.1	Form factor	Rack Mount	
2.2	Interface	24 x 10/25Gbps port	
		4 x 40/100Gbps port	
2.3	Transceiver and Cable	4 x 25GbE Transceiver	
		2 x 10GbE Transceiver	
		4 x OM4 Optical LC-LC 3m	
		2 x OM4 Optical LC-LC 30m	
2.4	Management Port	1 x 1Gbps RJ45	
2.5	Protocol	Support RDMA protocol	
2.6	Performance	Switching capacity: 2Tbps	
		Memory: 8GB	
		Package Buffer: 32MB	
2.7	Power	Hot swappable redundant power	

1.2.3. Yêu cầu chi tiết về phần mềm

1.2.3.1. Danh mục các phần mềm cần thiết đầu tư

TT	Danh mục các phần mềm	Đơn vị tính	Số lượng
1	Phần mềm lõi về giám sát, phân tích và tìm kiếm (dung lượng 150 GB/ngày hoặc 6000 EPS, thời hạn sử dụng 05 năm)	Bộ	01
2	Phần mềm điều tra, tương quan và xử lý sự cố (dung lượng 50 GB/ngày hoặc 2000 EPS, thời hạn sử dụng 05 năm)	Bộ	01
3	Phần mềm tự động hóa ngăn chặn tấn công (thời hạn sử dụng 05 năm)	Bộ	01

1.2.3.2. Yêu cầu cấu hình kỹ thuật chi tiết

1.2.3.2.1. Phần mềm lõi về giám sát, phân tích và tìm kiếm

- Yêu cầu về bản quyền/ quyền sử dụng phần mềm (license): Dung lượng 150 GB/day hoặc tương đương 6000 EPS đảm bảo hệ thống hoạt động bình

thường khi vượt ngưỡng license ở một số thời điểm cao điểm mà không gây ra mất log, không bị khóa tính năng tìm kiếm.

- Yêu cầu về mô hình triển khai:

+ Giải pháp hỗ trợ triển khai On-Premises và On-Cloud SaaS;

+ Giải pháp nằm trong nhóm Leader bảng xếp hạng của các bên đánh giá như Gartner, Forrester,... theo báo cáo đánh giá mới nhất; Nhà cung cấp phải cung cấp bằng chứng kết quả đánh giá để chứng minh cho giải pháp của mình.

- Yêu cầu về quản trị hệ thống:

+ Hệ thống có chức năng phân quyền người dùng hệ thống theo vai trò (Role-based access control);

+ Hệ thống có khả năng xác thực người dùng thông qua LDAP, Active Directory, eDirectory, SAML, two-factor authentication.

- Khả năng thu thập và chuẩn hóa dữ liệu:

+ Có khả năng thu thập log từ nhiều nguồn dữ liệu máy khác nhau như: các máy chủ, các ứng dụng, các dữ liệu mạng bao gồm cả dữ liệu log, dữ liệu về các giao dịch, nhật ký cuộc gọi, dữ liệu từ điện thoại di động,v.v...

+ Có khả năng thu thập dữ liệu của các ứng dụng tùy chỉnh (ứng dụng tự phát triển và opensource);

+ Có khả năng che các thông tin nhạy cảm (masking) trong dữ liệu raw trước khi hiển thị lên dashboard, đảm bảo tính bí mật của thông tin (như thông tin tài khoản người dùng, thông tin mật khẩu…).

- Khả năng tìm kiếm và phân tích dữ liệu:

+ Cho phép tự động phát hiện các bất thường hoặc dữ liệu ngoại lệ thông qua các mẫu dữ liệu lịch sử;

+ Có khả năng tạo biểu đồ về xu hướng kết quả bằng time-based charts, histograms, sparklines và summaries;

+ Có khả năng sử dụng Data Model để tăng tốc hiệu suất tìm kiếm, phân tích dữ liệu từ nhiều loại dữ liệu khác nhau;

+ Có khả năng giới hạn tài nguyên sử dụng của người dùng theo vai trò.

- Khả năng bổ sung tri thức để làm giàu dữ liệu:

+ Có khả năng cho phép hệ thống và người dùng tự động thêm các nguồn tri thức để làm giàu dữ liệu;

+ Có khả năng cho phép gán thẻ vào các trường thông tin nhằm nhóm các sự kiện có liên quan với nhau, hỗ trợ hiệu quả việc tìm kiếm, phân tích dữ liệu;

+ Có khả năng áp dụng các câu lệnh học máy (machine learning commands) cho dữ liệu máy để hỗ trợ việc tìm kiếm, phân tích dữ liệu hiệu quả.

- Khả năng giám sát, cảnh báo:

+ Có khả năng cảnh báo theo thời gian thực thông qua Email, Script, RSS, SNMP;

- Khả năng phân tích và báo cáo:

+ Có khả năng hỗ trợ phân tích, thống kê bằng cách kết hợp các câu lệnh tìm kiếm nâng cao trong một câu lệnh tìm kiếm duy nhất;

+ Cho phép cài đặt/tùy chỉnh để có chức năng tùy biến báo cáo theo các dạng khác nhau: time-based charts, histograms, sparklines, line, bar, pie, map charts;

- Khả năng tạo và tùy chỉnh Dashboard:

+ Có khả năng tạo và chỉnh sửa dashboard bằng cách kết hợp các kết quả tìm kiếm, báo cáo, bảng và biểu đồ;

+ Có khả năng chia sẻ các panel đã tạo sẵn để xây dựng dashboard một cách nhanh chóng;

+ Có khả năng phân quyền cho người dùng đối với từng dashboard;

- Khả năng xây dựng và phát triển ứng dụng:

+ Có khả năng cho phép xây dựng và triển khai các ứng dụng trên nền tảng của giải pháp cho các trường hợp sử dụng cụ thể;

+ Có khả năng cho phép tạo các ứng dụng thông qua việc đóng gói các dashboard và các file cấu hình khác nhau;

+ Có khả năng mở rộng hoặc hạn chế quyền theo vai trò người dùng cho từng ứng dụng;

+ Có khả năng xây dựng các dashboard, báo cáo về giám sát vận hành ứng dụng, giám sát bảo mật và giám sát business trên cùng một nền tảng/hệ thống dựa trên các dữ liệu sẵn có của hệ thống kết hợp với các dữ liệu bổ sung.

- Triển khai và mở rộng hệ thống:

+ Cho phép hỗ trợ các hệ điều hành Linux, Windows, Solaris, AIX;

+ Cho phép khả năng triển khai theo mô hình tập trung hoặc phân tán;

+ Hỗ trợ khả năng dự phòng HA (High Availability), cân bằng tải;

+ Có khả năng lưu trữ và khôi phục dữ liệu đã đánh chỉ mục theo yêu cầu.

- Yêu cầu về bảo mật hệ thống:

+ Có khả năng phân quyền người dùng trong hệ thống theo vai trò;

+ Cho phép cấu hình hạn chế truy cập vào các nguồn dữ liệu, loại dữ liệu, khoảng thời gian, view, báo cáo hoặc dashboard cụ thể;

+ Cho phép xác nhận tính toàn vẹn của dữ liệu index theo nhu cầu để đảm bảo tính an toàn và tuân thủ.

1.2.3.2.2. Phần mềm điều tra, tương quan và xử lý sự cố

- Yêu cầu về bản quyền/ quyền sử dụng phần mềm (license): Dung lượng

50 GB/day hoặc tương đương 2000 EPS.

- Khả năng giám sát bảo mật tổng thể:

+ Tăng khả năng phát hiện và điều tra sự cố thông qua các phương thức phân tích nâng cao;

+ Có khả năng cài đặt/tùy chỉnh, phân loại các thông tin trên giao diện giám sát bảo mật theo location, host;

- Khả năng phân tích, điều tra sự cố:

+ Có khả năng tương quan dữ liệu để hiển thị các thông tin điều tra (hiển thị tất các hoạt động có liên quan) của một IP nào đó trong hạ tầng mạng;

+ Cung cấp các dashboard xây dựng sẵn để phát hiện các hành vi bất thường và giao thức bất thường, các dashboard này được tự động cấu hình thresholds và baselines;

+ Cung cấp Workflow/Case Management để quản lý các sự kiện an ninh bất thường/tấn công được định danh;

+ Hỗ trợ công cụ phân loại và đánh giá sự cố theo trạng thái, mức độ, phân quyền xử lý đến thành viên có liên quan, v.v…;

+ Sử dụng các công cụ điều tra để phát hiện các hành vi bất thường trên các hệ thống bị xâm nhập (Advanced Threat Detection);

+ Cho phép phân tích tương quan các hành vi bất thường trong toàn bộ hạ tầng mạng liên quan đến người dùng như: authentications, endpoint changes, threat list activity, IDS attacks, malware attacks, risk modifiers, v.v...;

+ Cung cấp sẵn giao diện Workbench để phân tích điều tra sự cố và cung cấp trải nghiệm phân tích chi tiết đơn giản, giảm số lượng tab đang mở và giúp xác định xu hướng sự kiện đáng chú ý dễ dàng.

- Khả năng phản ứng sự cố:

+ Có khả năng ghi nhớ các câu lệnh tìm kiếm, các bước đã thực hiện, các gợi ý cho việc xử lý, ứng phó sự cố;

+ Có khả năng xâu chuỗi các sự kiện liên quan đến sự cố theo thời gian (kill chain) để hiểu rõ về vòng đời của cuộc tấn công (attack lifecycle);

+ Cho phép tích hợp với các hệ thống SOAR (Security Orchestration, Automation and Response) thực hiện quá trình tự động phản ứng lại các dấu hiệu bất thường như thu thập thông tin chuyên sâu, cho phép kết nối tới các hãng thứ ba để thực hiện ngăn chặn, cách ly.

- Khả năng quản lý rủi ro:

+ Cho phép áp dụng Risk score tới các tài sản, hành vi hoặc người dùng dựa trên độ quan trọng hay mức độ ảnh hưởng tới tổ chức;

+ Hỗ trợ dễ dàng track hiện trạng bảo mật từ đó hiểu và chủ động quản lý rủi ro tổng thể.

- Khả năng quản lý lỗ hổng tổng thể: Cho phép thu thập thông tin lỗ hổng bảo mật của hệ thống từ các giải pháp quản lý lỗ hổng bảo mật như Tenable, Rapid7, v.v...để lấy được các kết quả rà quét và đưa vào hệ thống giám sát tổng thể.

- Các tính năng nâng cao:

+ Cho phép tích hợp thêm các nguồn thông tin về threat intelligence ở bên ngoài để hỗ trợ điều tra, phân tích sự cố;

+ Cung cấp thư viện các use case trong việc phát hiện, phân tích và xử lý các mối nguy hại bảo mật;

+ Hỗ trợ tính năng cho phép thực thi một số hành động ra lệnh (chặn IP, thực thi scripts, ping, Nbtstat, v.v...) cho các máy chủ/thiết bị mạng/bảo mật của các hãng như Cisco, Fortinet, CyberArk, Palo Alto Networks, Gigamon, v.v…;

+ Có ứng dụng mobile trên App Store và Google Play, cho phép người quản trị giám sát Dashboard và nhận cảnh báo ngay trên thiết bị di động.

1.2.3.2.3. Phần mềm tự động hóa ngăn chặn tấn công

- Tạo và thực thi các luồng tự động hóa quy trình bảo mật;
- Xây dựng playbook bằng giao diện kéo-thả dễ sử dụng;
- Theo dõi, phân loại và xử lý sự cố bảo mật toàn diện;
- Quản lý cơ sở dữ liệu thông tin tình báo;
- Tích hợp nhiều công cụ 3rd-party và hỗ trợ nhiều hành động;
- Tích hợp chặt chẽ với giải pháp SIEM để hợp nhất điều tra;
- Giao tiếp và tích hợp ngoài với hệ thống qua REST API;
- Quy trình điều tra tiêu chuẩn, hỗ trợ hướng dẫn theo bước và tự động hóa;
- Kiểm soát truy cập hệ thống theo vai trò người dùng;
- Theo dõi chỉ số thời gian phát hiện sớm (Mean Time To Detect), thời gian phản ứng sớm (Mean Time To Response) từ các hoạt động phản ứng tự động;
- Quản lý và vận hành theo nhóm/team phân cấp.

1.2.4. Yêu cầu cung cấp và triển khai

1.2.4.1. Yêu cầu về cung cấp

1.2.4.1.1.Yêu cầu chung

Đơn vị cung cấp chịu trách nhiệm cung cấp giải pháp đáp ứng các yêu cầu sau:

- Bàn giao đầy đủ các thiết bị dự án cho Agribank tại các địa điểm triển khai dự án và chịu mọi rủi ro, chi phí liên quan trong quá trình vận chuyển;
- Lắp đặt thiết bị; cài đặt thiết bị và phần mềm; kiểm tra, hiệu chỉnh thiết bị và phần mềm;
- Cung cấp các phụ kiện (như cáp điện, cáp mạng, cáp quang, mô đun

quang, v.v...) và chịu mọi chi phí liên quan để lắp đặt, kết nối, tích hợp các thiết bị vào hệ thống mạng của Agribank;

- Bồi thường cho Agribank mọi thiệt hại phát sinh (nếu có) do lỗi của cá nhân hay đơn vị cung cấp gây ra.
- Phần mềm SIEM nằm trong nhóm bảng xếp hạng của các bên đánh giá như Gartner, Forrester,... theo báo cáo đánh giá mới nhất và phù hợp với Agribank.

1.2.4.1.2. Đối với các thiết bị

- Các thiết bị phần cứng khi cung cấp phải có giấy chứng nhận chất lượng của nhà sản xuất và giấy tờ chứng minh nguồn gốc xuất xứ của hàng hóa bao gồm cả đơn vận chuyển hải quan, packinglist (bản gốc hoặc bản sao công chứng trường hợp hàng hóa nhập khẩu). Thiết bị phải đảm bảo mới 100%, nguyên đai nguyên kiện và được sản xuất trước ngày hợp đồng có hiệu lực tối đa 08 tháng;
- Các thiết bị phần cứng cung cấp phải kèm các tài liệu xác định tính phù hợp của thiết bị như: Các catalog hoặc địa chỉ các website của nhà sản xuất thiết bị giới thiệu về công nghệ tính năng kỹ thuật của thiết bị phần cứng chào bán;
- Đơn vị cung cấp phải đảm bảo Agribank không phải trả thêm bất kỳ khoản chi phí nào liên quan đến bản quyền, các bí mật công nghệ, các sáng chế liên quan đến thiết bị phần cứng được chế tạo hoặc sử dụng chúng mà không có một điều khoản ràng buộc nào khác;
- Đơn vị cung cấp phải bồi thường cho Agribank về mọi thiệt hại do khiếu nại của bên thứ ba (nếu có) đối với việc vi phạm bản quyền sáng chế, nhãn hiệu thương mại hoặc thiết kế hàng hoá.

1.2.4.1.3. Đối với các phần mềm

- Phần mềm phải là phiên bản mới nhất, có chứng nhận (chứng nhận điện tử) bản quyền cấp cho Agribank; Có tài liệu hướng dẫn cài đặt, quản trị, tài liệu kỹ thuật kèm theo;
- Đơn vị cung cấp phải chịu trách nhiệm cung cấp và chi trả mọi chi phí đối với các phần mềm khác có liên quan (nếu có) để cài đặt, triển khai và vận hành hệ thống;
- Đơn vị cung cấp phải hoàn toàn chịu trách nhiệm về mọi thiệt hại phát sinh do việc khiếu nại của bên thứ ba về việc vi phạm bản quyền sở hữu trí tuệ liên quan tới phần mềm cung cấp cho Agribank.

1.2.4.2. Yêu cầu về tổ chức triển khai

1.2.4.2.1. Yêu cầu về công việc triển khai

a) Khảo sát, phương án triển khai

- Đề xuất danh sách các công việc chính cần thực hiện, thống nhất các công việc của từng bên tham gia cùng các mốc thời gian thực hiện chi tiết;
- Thực hiện khảo sát hiện trạng Hệ thống điều hành an toàn thông tin SOC

đang sử dụng và các hệ thống đã tích hợp liên quan; các hệ thống log source cấp độ 2,3; các log source về ứng dụng, cơ sở dữ liệu của Agribank;

- Thực hiện báo cáo hiện trạng Hệ thống điều hành an toàn thông tin SOC đang sử dụng và đề xuất phương án triển khai;
- Đề xuất kiến trúc tổng thể của hệ thống điều hành an toàn thông tin SOC nâng cấp, mở rộng. Thực hiện đề xuất thiết kế và phương án triển khai hệ thống. Sau đó, làm việc với Agribank thống nhất kiến trúc tổng thể, thiết kế và phương án triển khai của hệ thống;
- Lên phương án kiểm tra, bàn giao thiết bị, license phần mềm và nghiệm thu hàng hóa.

b) Lắp đặt, cài đặt, cấu hình hạ tầng

- Lắp đặt thiết bị phần cứng, kết nối vào hệ thống mạng của Agribank tại hệ thống chính, hệ thống dự phòng;
- Cài đặt, cấu hình hệ điều hành và các phần mềm hạ tầng liên quan tại hệ thống chính, hệ thống dự phòng và hệ thống thử nghiệm;
- Cài đặt, cấu hình các phần mềm của hãng thứ ba (nếu có) tại hệ thống chính, hệ thống dự phòng và hệ thống thử nghiệm;
- Phối hợp cập nhật phiên bản sử dụng trên hạ tầng dùng chung của Agribank sử dụng cho hệ thống chính, dự phòng và hệ thống thử nghiệm lên phiên bản mới, ổn định nhất;
- Đưa ra phương án, phối hợp cấu hình cân bằng tải cho các máy chủ của hệ thống tại hệ thống chính, hệ thống dự phòng;
- Đưa ra phương án, phối hợp cấu hình máy chủ theo các tiêu chuẩn bảo mật của Agribank.

c) Cài đặt các phần mềm của hệ thống điều hành an toàn thông tin SOC nâng cấp, mở rộng tại hệ thống chính, hệ thống dự phòng và hệ thống thử nghiệm.

- Kiểm tra cấu hình các thành phần hệ thống điều hành an toàn thông tin SOC và các phần mềm liên quan đảm bảo hoàn thành trước khi thực hiện triển khai, cài đặt phần mềm của hệ thống điều hành an toàn thông tin tại hệ thống chính, hệ thống dự phòng và hệ thống thử nghiệm;
- Thực hiện đề xuất các rule kết nối mạng, kiểm tra kết nối mạng giữa các máy chủ của hệ thống chính, hệ thống dự phòng và hệ thống thử nghiệm để đảm bảo các phần mềm, thiết bị giao tiếp được với nhau;
- Lên phương án; thực hiện kiểm tra, kiểm thử thông luồng đầy đủ nghiệp vụ (workflow) với dữ liệu mẫu tại hệ thống chính, hệ thống dự phòng, hệ thống thử nghiệm;
- Yêu cầu triển khai và tích hợp thu thập log tối thiểu toàn bộ hệ thống cấp độ 3 tại thời điểm triển khai về hệ thống SOC;
- Thực hiện chuyển đổi xây dựng lại cấu hình Rule/Dashboard/Alert đang sử dụng hiện tại sang hệ thống mới.

- Tham gia triển khai với các nhiệm vụ cụ thể như sau:

+ Triển khai, cài đặt:

✓ Thiết kế và lên phương án triển khai;

✓ Cài đặt, cấu hình phần mềm

✓ Kiểm tra, hiệu chỉnh phần mềm: Kiểm tra, hiệu chỉnh tham số cài đặt phần mềm;

+ Xây dựng các màn hình giám sát an ninh cho Agribank như sau:

✓ Nguyên tắc thiết kế UseCase: Việc xây dựng các Use-Case sẽ phụ thuộc vào nguồn Log hiện đang có tại Agribank. Từ những thông tin này, nhà thầu sẽ đánh giá và lên các Use-Case phù hợp với hệ thống Agribank. Mỗi một Use-Case sẽ cần làm rõ các thông tin bao gồm:

- Tên Use-Case
- ATT&CK ID
- MITRE ATT&CK Technique
- MITRE ATT&CK Tactic
- Description (mô tả Use-Case)
- Source Log (thông tin các nguồn Log cần có để thực hiện Use-Case)

Các thông tin Use-Case sẽ phải matching với thông tin theo framework MITRE ATT&CK để đối chiếu mức độ bao quát.

✓ Kết quả các màn hình giám sát dựa trên UseCase đã được triển khai:

- 01. Màn hình giám sát tình hình an ninh tổng thể chung: Phân loại các mức độ sự cố an ninh theo các mức Nghiêm trọng, Cao, Trung Bình, Thấp
- 02. Playbook ngăn chặn tự động tấn công phishing vào email
- 03. Playbook ngăn chặn tự động tấn công Bruteforce dò đoán mật khẩu
- 04. Playbook ngăn chặn tự động dò quét mạng & enumerate hệ thống mạng nội bộ
- 05. Playbook ngăn chặn tự động dò quét web tự động hoặc dò tìm entry point (Directory Traversal / Fuzzing)
- 06. Cảnh báo tấn công phát hiện upload mã độc/ webshell
- 07. Cảnh báo thay đổi User-Agent, Header bất thường gọi vào cơ sở dữ liệu
- 08. Cảnh báo lưu lượng C2 Beacon hoặc Payload download qua HTTP
- 09. Cảnh báo Remote Excution bằng PsExec
- 10. Cảnh báo Phát hiện Mimikatz hoặc LSASS Memory Access

1.2.4.2.2. Yêu cầu về bảo hành và hỗ trợ kỹ thuật

- Thời gian bảo hành: Đơn vị cung cấp chịu trách nhiệm bảo hành cho các thiết bị phần cứng trong 3 năm, phần mềm trong 5 năm (không tính phí) theo tiêu

chuẩn, chất lượng của Hãng sản xuất (kể từ ngày nghiệm thu hợp đồng).

- Địa điểm bảo hành và hỗ trợ kỹ thuật: Tại 02 Trung tâm dữ liệu của Agribank tại Hà Nội.

- Thiết bị/ phần mềm hệ thống điều hành an toàn thông tin SOC được bảo hành (không tính phí) theo tiêu chuẩn dịch vụ bảo hành nâng cao từ chính Hãng trong suốt thời gian bảo hành, cụ thể:

+ Hỗ trợ liên tục 24 giờ trong ngày, 7 ngày trong tuần;

+ Thời gian phản hồi sự cố nghiêm trọng là 2 giờ, thời gian phản hồi sự cố mức cao là 4 giờ;

+ Gửi yêu cầu hỗ trợ trên trang Web hoặc điện thoại;

+ Tất cả các bản cập nhật, bản vá của phần mềm, firmware được cung cấp không tính phí.

- Thời gian có mặt xử lý và khắc phục sự cố: Trong vòng tối đa 02 (hai) giờ kể từ khi nhận được thông báo sự cố qua một trong các hình thức sau: Văn bản, Fax, Email hoặc điện thoại đơn vị cung cấp phải có mặt để đánh giá, xây dựng phương án và xử lý sự cố phát sinh.

- Agribank được cấp tài khoản trên trang của chính hãng và thông qua nhà phân phối để mở case hỗ trợ xử lý kỹ thuật đảm bảo việc xử lý sự cố nhanh chóng và kịp thời.

- Đơn vị cung cấp phải đảm bảo thiết bị, vật tư mới 100%. Đồng thời, đơn vị cung cấp phải đảm bảo Agribank không phải trả thêm bất kỳ một khoản chi phí nào khác đối với trang thiết bị, linh kiện thay thế trong thời gian bảo hành. Đơn vị cung cấp phải cung cấp đầu mối liên lạc cũng như để tiếp nhận thông tin sự cố 24/7.

- Trong thời gian bảo hành, Đơn vị cung cấp phải thực hiện việc kiểm tra, tổ chức nâng cấp, hiệu chỉnh hệ thống theo định kỳ ít nhất 06 tháng một lần hoặc khi có yêu cầu từ Agribank. Đơn vị cung cấp phải đảm bảo Agribank không phải trả thêm bất kỳ một khoản chi phí nào đối với việc hỗ trợ và tổ chức nâng cấp hệ thống. Các công việc nâng cấp, hiệu chỉnh hệ thống bao gồm:

+ Kiểm tra hoạt động của thiết bị/phần mềm;

+ Nâng cấp phiên bản và vá lỗi thiết bị/phần mềm (nếu có);

+ Tổ chức hiệu chỉnh, tối ưu hóa hoạt động thiết bị/phần mềm.

1.2.5. Yêu cầu về đào tạo

1.2.5.1. Yêu cầu chung

- Đơn vị cung cấp lập kế hoạch chi tiết và tổ chức 02 khóa đào tạo cho các cán bộ quản trị, vận hành hệ thống của Agribank;

- Các chi phí đào tạo bao gồm: Tài liệu, các thiết bị phục vụ đào tạo, hội trường, khánh tiết, v.v... do đơn vị cung cấp chịu trách nhiệm chi trả.

1.2.5.2. Tổ chức lớp đào tạo phần mềm

1.2.5.2.1. Lớp đào tạo phần mềm cơ bản

- Số lượng lớp: 01 lớp;
- Số lượng học viên: Tối thiểu 20 cán bộ;
- Thời gian đào tạo: Tối thiểu 03 ngày;
- Giảng viên: Yêu cầu có chứng chỉ Quản trị (Administrator) của Hãng phần mềm;
- Môi trường đào tạo: Nhà thầu phải chuẩn bị đầy đủ cơ sở vật chất, trang thiết bị, tài liệu cho đào tạo, sẵn sàng và đảm bảo chất lượng;
- Nội dung đào tạo phần mềm yêu cầu tối thiểu như sau:

+ Giới thiệu kiến trúc tổng thể phần mềm;

+ Các tính năng chính của các phần mềm điều tra, tương quan, xử lý sự cố và phần mềm tự động hóa ngăn chặn tấn công;

+ Hướng dẫn vận hành, quản trị người dùng.

- Địa điểm đào tạo: Do đơn vị cung cấp đề xuất.

1.2.5.2.2. Lớp đào tạo phần mềm nâng cao

- Số lượng lớp: 01 lớp;
- Số lượng học viên: Tối thiểu 10 cán bộ;
- Thời gian đào tạo: Tối thiểu 05 ngày;
- Giảng viên: Yêu cầu có chứng chỉ Kiến trúc (Architecture) của Hãng phần mềm;
- Môi trường đào tạo: Nhà thầu phải chuẩn bị đầy đủ cơ sở vật chất, trang thiết bị, tài liệu cho đào tạo, sẵn sàng và đảm bảo chất lượng.
- Nội dung đào tạo phần mềm yêu cầu tối thiểu như sau:

+ Đào tạo về Troubleshooting nâng cao liên quan đến vận hành, quản trị hệ thống, v.v...;

+ Đào tạo tối ưu (tuning) nâng cao về tối ưu Rule/Alert/Dashboard/Playbook; nâng cao săn lùng (hunting) điều tra dấu hiệu sự cố bảo mật dựa trên các rule theo tư vấn của Hãng.

+ Xây dựng mẫu kịch bản tấn công trên SOAR theo phương thức tự động, bán tự động. Hướng dẫn tích hợp một trong các hệ thống của Agribank: Firewall, WAF, Email Gateway, Antivirus,v.v... để thực hiện các playbook ngăn chặn tấn công tự động.

+ Hướng dẫn tích hợp trí tuệ nhân tạo/ học máy (AI/Machine) để cảnh báo các dấu hiệu tấn công bất thường vào hệ thống.

- Địa điểm đào tạo: Do đơn vị cung cấp đề xuất.

Mục 2. Bản vẽ

Không có.

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có:

- Kiểm tra trực tiếp trên thiết bị, qua catalog, qua giao diện quản trị của thiết bị và các kịch bản thử nghiệm khác để đảm bảo hàng hóa có cấu hình và tính năng đáp ứng yêu cầu trong HSMT và HSDT.
- Các chi phí liên quan (nếu có) đến việc kiểm tra, thử nghiệm hàng hóa do nhà thầu chịu trách nhiệm chi trả.

THUẬT NGỮ VÀ CÁC TỪ VIẾT TẮT

STT	Từ viết tắt/Thuật ngữ	Giải thích
1	Agribank	Ngân hàng Nông nghiệp và Phát triển Nông Thôn Việt Nam
2	AI/ML (Artificial Intelligence/ Machine Learning)	Trí tuệ nhân tạo/ Học máy
3	ATTT	An toàn thông tin
4	BDC (Backup Data Center)	Trung tâm dữ liệu dự phòng
5	CNTT	Công nghệ thông tin bao gồm phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng.
6	DMZ (Demilitarized Zone)	Là vùng mạng trung gian giữa mạng nội bộ (LAN) và mạng bên ngoài (Internet), được thiết kế để cách ly và bảo vệ hệ thống nội bộ khỏi các mối đe dọa từ bên ngoài, đồng thời vẫn cho phép truy cập đến một số dịch vụ công cộng (web, mail, DNS, v.v…)
7	EPS (Event Per Second)	Số sự kiện trong 1 giây
8	Firewall	Tường lửa
9	Gbps (Gigabits Per Second)	Là đơn vị đo **băng thông** hoặc **tốc độ truyền dữ liệu** trong mạng máy tính hoặc thiết bị truyền dẫn
10	HA (High Availability)	Mức độ sẵn sàng cao
11	PDC (Primary Data Center)	Trung tâm dữ liệu chính
12	SIEM (Security Information & Event Management)	Quản lý sự kiện và thông tin an ninh bảo mật
13	SOAR (Security Orchestration, Automation, and Response)	Phần mềm tự động hóa ngăn chặn tấn công
14	SOC (Security Operation Center)	Hệ thống điều hành An toàn Thông tin của Agribank
15	TTDL	Trung tâm dữ liệu của Agribank, bao gồm trung tâm dữ liệu chính PDC tại C3 Phương Liệt và trung tâm dữ liệu dự phòng BDC tại Tòa nhà Agribank, Khu đất A5-THCT2, Khu đô thị mới Lê Trọng Tấn, Xã An Khánh, Thành phố Hà Nội
16	WAN (Wide Area Network)	Hệ thống mạng diện rộng