E-HSMT gói thầu: Giải pháp quản lý bảo mật cho các hệ thống Container Platform, subscription 3 năm

Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về gói thầu

- Tên gói thầu: Giải pháp quản lý bảo mật cho các hệ thống Container Platform, subscription 3 năm

- Thời gian thực hiện gói thầu: 180 ngày kể từ ngày Hợp đồng có hiệu lực

- Địa điểm đầu tư: Trung tâm dữ liệu chính và Trung tâm dữ liệu dự phòng của ngân hàng TMCP Công thương Việt Nam

- Phạm vi, quy mô triển khai Gói thầu cụ thể như sau:

TT	Danh mục	Đơn vị tính	Số lượng
I	**Giải pháp quản lý bảo mật cho các hệ thống Container Platform, subscription 3 năm**	**Gói**	**01**
I.1	Giải pháp quản lý bảo mật cho các hệ thống Container Platform, subscription 3 năm		
I.2	Dịch vụ triển khai giải pháp		

1.2. Yêu cầu về kỹ thuật

Hàng hóa phải có cấu hình tương đương, hoặc cao hơn, hoặc tổng hiệu năng (khi quy đổi về tốc độ, dung lượng, số lượng, các tiêu chuẩn đáp ứng, bản quyền sử dụng...) của hệ thống/thành phần, tương đương hoặc cao hơn các yêu cầu sau:

TT	HẠNG MỤC	YÊU CẦU TỐI THIỂU
1	Yêu cầu chung về giải pháp	- Giải pháp quản lý bảo mật các Container: tối thiểu 200 Worker Nodes. - Thời hạn: quyền sử dụng trong 03 năm kể từ ngày hoàn thành dịch vụ triển khai - Cung cấp các khả năng mở rộng trong một nền tảng duy nhất để bảo vệ các workloads bằng cách sử dụng phương pháp bảo vệ đa lớp bao gồm nhưng không giới hạn trong số: + Quản lý lỗ hổng bảo mật + Bảo vệ Runtime + Bảo mật ứng dụng web và API
2	Các tính năng	
2.1.	Tổng quan	- Có các khả năng bảo vệ các Container workload hoạt động trên các nền tảng như sau: + OpenShift + Kubernetes (k8s) + Elastic Kubernetes Service (EKS) + Elastic Container Service (ECS) + Oracle Container Engine for Kubernetes (OKE) + Google Kubernetes Engine (GKE) + Google Kubernetes Engine (GKE) autopilot + Azure Kubernetes Service (AKS) + Lightweight Kubernetes (k3s) + VMware Tanzu Application Service (TAS) - Có khả năng triển khai thành phần bảo vệ xuống các worker node hoạt động như một DaemonSet trên các Container orchestrator

2.2.	Tính tuân thủ	- Hỗ trợ giám sát và bảo đảm tính tuân thủ cho các máy chủ, Container và serverless + CIS Docker + CIS Kubernetes + CIS Openshift + CIS Linux + NIST SP 800-190 + PCI - Hỗ trợ quét VM image trong môi trường đám mây để phát hiện các lỗ hổng sau đây: + Cấu hình máy chủ: Những lỗ hổng trong việc thiết lập VM image. + Cấu hình Docker daemon: Những lỗ hổng phát sinh từ việc cấu hình sai Docker daemon. + Tập tin cấu hình Docker daemon: Những lỗ hổng phát sinh do thiết lập quyền truy cập không chính xác trên các tập tin cấu hình quan trọng. + Vận hành bảo mật Docker: Gợi ý và nhắc nhở để mở rộng các quy tắc bảo mật tốt nhất hiện tại bao gồm cả các Container. + Cấu hình Linux: Tuân thủ của các máy chủ Linux. - Có kiểm tra các tuân thủ trên các máy ảo MS Windows - Hỗ trợ phát hiện thông tin nhạy cảm không được bảo mật đúng cách trong image và Container. Quá trình quét có thể phát hiện các mật khẩu, login token và các thông tin mật bí mật khác được nhúng trong đó
2.3.	Quản lý lỗ hổng bảo mật	- Có cơ chế cập nhật các cơ sở dữ liệu các lỗ hổng bảo mật, threat intelligence liên tục - Có cơ chế định danh các lỗ hổng bảo mật trước khi chúng được gán các CVE ID cụ thể - Sử dụng các Risk Factor của môi trường để đánh giá mức độ rủi ro thực tế của lỗ hổng bảo mật như: Remote execution, Exploit PoC, Exploit in the wild, Reachable from the internet, Container is running as root...

2.4.	Bảo vệ Workload	- Giải pháp cho phép quét image để phát hiện lỗ hổng, phần mềm độc hại và dữ liệu nhạy cảm. - Giải pháp có khả năng chặn image không tuân thủ được triển khai - Giải pháp có khả năng bảo mật runtime cho các host, Container và serverless. - Giải pháp có khả năng tự động học cho tất cả các image mới trong môi trường để quan sát hoạt động của tập tin hệ thống, mạng và process của image và tự động áp dụng vào trong các chính sách policy để phát hiện và ngăn chặn các hành vi bất thường - Giải pháp có khả năng phát hiện và ngăn chặn các malware - Giải pháp có khả năng ngăn chặn các hành vi như Crypto miners, Reverse shell attacks, Processes used for lateral movement - Giải pháp có khả năng ngăn chặn tiến trình (process) bất thường hoặc thậm chí xóa Container khi xảy ra các vi phạm - Giải pháp có khả năng phát hiện các hành vi Port scanning và có thể xóa Container nếu phát hiện vi phạm - Giải pháp có khả năng chặn hoặc cho phép Container kết nối đến các domain cụ thể - Giải pháp có khả năng chặn hoặc cho phép Container lắng nghe hoặc kết nối ra các PORT cụ thể - Giải pháp có khả năng phát hiện và ngăn chặn các hành vi như encrypted/packed binaries, Binaries with suspicious ELF headers. - Giải pháp có khả năng tự động ngăn chặn các hành vi bất thường liên quan đến file system - Giải pháp hỗ trợ quản lý việc chèn khóa bí mật (secret key) vào các Container - Giải pháp hỗ trợ vá ảo lỗ hổng (Virtual Patching) bằng các chính sách tùy chỉnh (custom rule) - Giải pháp hỗ trợ điều tra và phản ứng sự cố, cung cấp các thông tin chi tiết về các tiến trình trên Container - Giải pháp hỗ trợ giám sát / theo dõi traffic đi vào / đi ra thời gian thực giữa các Container và host - Giải pháp có thể kết nối với môi trường sandboxing của cùng một nhà cung cấp bên ngoài để phân tích malware.

2.5.	Bảo mật ứng dụng Web và API	- Giải pháp có khả năng thiết lập tính năng bảo mật cho web và API service trên từng Container, host. - Giải pháp có thể tự động phát hiện các ứng dụng web và hiển thị một bảng các ứng dụng web chưa được bảo vệ. - OWASP Top- 10: Bảo vệ chống lại những rủi ro bảo mật quan trọng nhất đối với ứng dụng web, bao gồm các lỗi injection, xác thực hỏng, kiểm soát truy cập hỏng, cấu hình bảo mật không chính xác, v.v. - API Protection: Có thể thực thi bảo mật cho kết nối API dựa trên các định nghĩa/quy định được cung cấp dưới dạng tệp Swagger hoặc OpenAPI. - Access Control: Kiểm soát quyền truy cập vào các ứng dụng được bảo vệ bằng cách sử dụng các hạn chế do người dùng xác định dựa trên địa lý, địa chỉ IP hoặc HTTP header. - File Upload Control: Bảo mật quá trình tải lên tập tin trong ứng dụng bằng cách áp dụng quy tắc quản lý loại tập tin - Penalty Box: Hỗ trợ cấm IP trong 5 phút đối với những IP vi phạm một trong những biện pháp bảo vệ, nhằm làm chậm quá trình quét lỗ hổng và các tấn công khác vào ứng dụng. - Bot Protection: Phát hiện các bot nổi tiếng và các bot khác, trình duyệt không có giao diện (headless) và các framework tự động hóa khác, cũng có thể chống lại cookie dropper... - DoS Protection: Có khả năng thiết lập giới hạn tần suất truy cập cao (high rate) và "low and slow" để bảo vệ chống lại các cuộc tấn công DoS layer 7 - Hỗ trợ các giao thức: + HTTP 1.0, 1.1, 2.0 + hỗ trợ đầy đủ các HTTP methods + TLS 1.0, 1.1, 1.2 và 1.3 + gRPC + WebSockets Passthrough + Hỗ trợ Message Parser và Decoder + GZip, deflate content encoding + HTTP Multipart content type + URL Query, x- www- form- urlencoded, JSON và XML parameter parsing

		+ URL, HTML Entity, JS, BASE64 decoding + Overlong UTF- 8
2.6.	Yêu cầu quản trị và giám sát	- Có quản trị qua Web - Hỗ trợ tính năng xác thực đa nhân tố với các tài khoản quản trị - Tích hợp xác thực với + Active Directory +ADFS + Tích hợp với Azure Active Directory - Hỗ trợ role-based gán quyền cho tài khoản người dùng dựa trên vai trò của người dùng - Cảnh báo: + Giải pháp có khả năng cung cấp bảng điều khiển ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) để hiển thị thông tin về các chiến thuật và kỹ thuật mà những kẻ tấn công sử dụng để tấn công ứng dụng và cơ sở hạ tầng. + Hỗ trợ xuất báo cáo ra file CSV
2.7.	Yêu cầu tích hợp	- Cung cấp việc truy xuất log theo hai dạng là chủ động đẩy log ra nơi lưu trữ ngoài hoặc cho hệ thống SIEM kéo log từ nhà cung cấp về. Có khả năng đẩy log đến các hệ thống IBM Qradar, ElasticSearch, AWS S3 - Có khả năng gửi cảnh báo qua email
2.8.	Cam kết	- Đơn vị cung cấp dịch vụ cam kết về thời gian uptime 99%. - Đơn vị cung cấp công bố các lỗi sự cố đã xảy ra đối với dịch vụ cung cấp để khách hàng có thể nắm bắt thông tin và phối hợp
3	Triển khai	
3.1	Khảo sát	- Lên phương án, lập kế hoạch, thực hiện khảo sát
3.2	Thiết kế hệ thống	- Thiết kế tổng quan/sơ bộ - Thiết kế chi tiết (tối thiểu bao gồm: sơ đồ và thuyết minh giải pháp; quy hoạch IP; thông số kỹ thuật; triển khai tích hợp log với các hệ thống SIEM) - Triển khai download/đồng bộ log truy cập về hệ thống on-premise của VietinBank

3.3	Triển khai	- Lập phương án triển khai - Lập kế hoạch triển khai tổng thể và chi tiết - Thực hiện triển khai và chuyển đổi hệ thống
3.4	Kiểm thử tính năng hệ thống	- Thực hiện kiểm tra chức năng các thành phần sau triển khai, đảm bảo các chức năng hoạt động đúng theo thiết kế
3.5	Hỗ trợ tinh chỉnh, theo dõi hệ thống sau triển khai	- Theo dõi, hiệu chỉnh, tối ưu, giám sát hệ thống
3.6	Tài liệu cung cấp	- Tài liệu khảo sát - Tài liệu Thiết kế hệ thống - Tài liệu hướng dẫn cài đặt hệ thống - Tài liệu kiểm thử hệ thống - Tài liệu hướng dẫn giám sát hệ thống. - Tài liệu hướng dẫn quản trị, vận hành hệ thống - Tài liệu danh mục lỗi, nguyên nhân và biện pháp xử lý - Tài liệu hướng dẫn sao lưu, khôi phục hệ thống.

1.3. Yêu cầu về bảo hành:

- Bảo hành: Thời gian bảo hành là 1095 ngày kể từ ngày hoàn thành dịch vụ triển khai, bảo hành theo tiêu chuẩn chính hãng, có xác nhận bảo hành bằng văn bản hoặc gửi qua email từ hãng cung cấp hoặc có thông tin bảo hành trên website của chính hãng.

- Với nhà thầu liên danh: Xác nhận bảo hành phải được cấp cho liên danh hoặc được cấp cho thành viên liên danh mà thành viên đó chịu trách nhiệm cung cấp dịch vụ bảo hành cho gói thầu này.

- Khi thực hiện bảo hành/xử lý sự cố: nhà thầu có mặt tại địa điểm triển khai trong vòng 2h và thực hiện khắc phục các lỗi, xử lý sự cố trong vòng tối đa 4 giờ kể từ khi nhận được yêu cầu bảo hành từ chủ đầu tư; Nhà thầu chịu toàn bộ chi phí cho việc khắc phục các lỗi, sự cố khi hệ thống/phần mềm vẫn đang trong thời gian bảo hành. Trong trường hợp không khắc phục được ngay nhà thầu có phương án thay thế để đảm bảo tính hoạt động liên tục của hệ thống.

1.4. Yêu cầu khác:

Nhà thầu phải cam kết:

- Không có thông tin vi phạm về kết quả thực hiện hợp đồng của nhà thầu theo quy định tại

Điều 19 và Điều 20 của Nghị định số 214/2025/NĐ-CP.

Mục 2. Quy định trả lời yêu cầu kỹ thuật:

- Nhà thầu cần cung cấp câu trả lời riêng biệt 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.

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.