Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

I. Giới thiệu chung về Dự án, gói thầu:

- Tên Dự án: Mua sắm trang bị giải pháp bảo mật API Security chuyên dụng.
- Tên gói thầu: Mua sắm trang bị giải pháp bảo mật API Security chuyên dụng.
- Nội dung công việc chính của gói thầu: Mua sắm trang bị giải pháp bảo mật API Security chuyên dụng trong 3 năm đáp ứng bảo vệ 190 APIs hoặc 270 API Endpoints hoặc 70 triệu API requests/tháng.
- Lĩnh vực LCNT: Mua sắm hàng hóa
- Thời gian thực hiện gói thầu: 44 tháng.
- Tên Chủ đầu tư: Ngân hàng TMCP Đầu tư và Phát triển Việt Nam

II. Yêu cầu về kỹ thuật:

1. Yêu cầu chung:

− Địa điểm thực hiện: Các Trung tâm dữ liệu (TTDL) của BIDV tại Hà Nội (TTDL chính Duy Tân, TTDL DP IDC Viettel Hòa Lạc).

− Hạng mục cung cấp:

TT	Hạng mục	Số lượng	Đơn vị tính	Ghi chú
1	Giải pháp bảo vệ API Security chuyên dụng trong 03 năm	01	Gói	Đáp ứng bảo vệ 190 APIs hoặc 270 API Endpoints hoặc 70 triệu API requests/tháng Bao gồm dịch vụ hỗ trợ kỹ thuật trong 36 tháng
2	Dịch vụ triển khai	01	Gói	

− Thời gian thực hiện hợp đồng: 44 tháng kể từ ngày hợp đồng có hiệu lực, trong đó:

+ Thời gian bàn giao, nghiệm thu hàng hóa và triển khai cấu hình hệ thống: 06 tháng kể từ ngày Hợp đồng có hiệu lực.
+ Thời gian hiệu lực bản quyền phần mềm: 36 tháng kể từ ngày hoàn thành triển khai và kích hoạt bản quyền phần mềm.
+ Thời gian hỗ trợ kỹ thuật theo bản quyền phần mềm: 36 tháng kể từ ngày hoàn thành triển khai và kích hoạt bản quyền phần mềm.
+ Thời gian nghiệm thu hợp đồng: 02 tháng

2. Yêu cầu về tiêu chuẩn kỹ thuật chi tiết

Tiêu chí kỹ thuật	Yêu cầu/Mô tả chi tiết
1. YÊU CẦU CHUNG	
1.1. Cam kết về tiêu chuẩn kỹ thuật	
1.1.1. Cam kết tuân thủ	Nhà thầu cam kết giải pháp cung cấp cho BIDV tuân thủ chứng chỉ PCI DSS 4.0.
1.2. Yêu cầu triển khai	

Tiêu chí kỹ thuật	Yêu cầu/Mô tả chi tiết
1.2.1. Hỗ trợ đa dạng mô hình	Hỗ trợ triển khai on-premises, container hoá (K8s, Openshift, VMware Tanzu…) và có thể hỗ trợ chuyển đổi sang các mô hình: Public cloud; và hybrid theo nhu cầu của BIDV
1.2.2. Phương thức triển khai	Hỗ trợ một trong số các phương thức triển khai sau: inline (proxy), out-of-band (qua traffic mirroring/TAP), agent-based (trên API gateway, application server, container), agentless (qua log, network)
1.2.3. Hỗ trợ môi trường container hóa	Hỗ trợ triển khai và bảo vệ API trong các môi trường container hóa (Docker, Kubernetes, OpenShift) và môi trường private cloud/ảo hoá sử dụng VMWare.
1.3 Tính sẵn sàng	
1.3.1. Hỗ trợ hoạt động liên tục	Có hỗ trợ các cơ chế/ phương án để đảm bảo hoạt động liên tục của giải pháp.
1.4. Bản quyền (Licensing)	
1.4.1. Thông tin bản quyền	Yêu cầu cung cấp bản quyền đảm bảo triển khai đủ cho 190 APIs hoặc 270 API Endpoints hoặc 70 triệu API requests/tháng của BIDV
1.5. Hỗ trợ kỹ thuật và tài liệu	
1.5.1. Lộ trình sản phẩm rõ ràng	Sản phẩm còn được hỗ trợ, đảm bảo đến thời gian nộp hồ sơ dự thầu, sản phẩm chưa có thông báo ngừng hỗ trợ từ hãng (End of Support).
1.5.2. Cập nhật thường xuyên	Cung cấp thường xuyên các bản cập nhật, cơ sở dữ liệu nhận diện mối đe dọa (threat intelligence), các dữ liệu huấn luyện dựa trên các mối đe doạ mới cho cấu phần AI (nếu có).
1.6. Yêu cầu về hiệu năng	
1.6.1. Throughput	Giải pháp có thông lượng xử lý tổng thể đáp ứng tối thiểu 01Gbps.
1.6.2. Số lượng request/ngày	Giải pháp đáp ứng xử lý tối thiểu 2,5 triệu request/ngày.
1.6.3. Hiệu năng xử lý RPS	Giải pháp đáp ứng tối thiểu 20,000 RPS (Request-Per-Second) trên một node cài đặt; tổng số request giải pháp có thể xử lý trên tất cả các node có thể hỗ trợ lên tới 200,000 RPS.
2. YÊU CẦU VỀ KHẢ NĂNG KHÁM PHÁ VÀ QUẢN LÝ API	
2.1. Khám phá và quản lý API	
2.1.1. Phát hiện toàn diện API	Có khả năng tự động phát hiện và lập danh mục tất cả các API đang hoạt động trong hệ thống, bao gồm cả các API theo phạm vi quản lý và mức độ kiểm soát: API nội bộ, API công khai, API của bên thứ ba, shadow APIs (API không được quản lý) và zombie APIs (API lỗi thời); theo giao thức và định dạng API: REST, SOAP, XML, GraphQL.
2.1.2. Hỗ trợ đa dạng nguồn API	Có thể khám phá API từ nhiều nguồn: traffic mạng, log từ API Gateway/server, tích hợp với CI/CD, đặc tả API (OpenAPI, Swagger, WSDL, GraphQL,…).
2.2. Phân loại và đặc tả API	
2.2.1. Thu thập chi tiết thông tin API	Có thể tự động thu thập thông tin chi tiết về mỗi API: endpoints, HTTP methods, request/response header&body bao gồm: IP Client, User-Agent, Timestamp, version, authentication type,

Tiêu chí kỹ thuật	Yêu cầu/Mô tả chi tiết
2.2.2. Nhận diện định dạng dữ liệu API	Có khả năng nhận diện và phân tích các định dạng dữ liệu phổ biến trong API (JSON, XML, form-data, plain text) và các định dạng đặc thù nếu có.
2.2.3. Hỗ trợ các chuẩn đặc tả API	Có hỗ trợ import và phân tích các file đặc tả API theo chuẩn OpenAPI, Swagger, WSDL, GraphQL Schema.
2.2.4. Phân loại API theo mức độ rủi ro/ độ quan trọng của dữ liệu	Có khả năng tự động hoặc hỗ trợ người dùng phân loại API dựa trên loại dữ liệu mà API xử lý (ví dụ: PII, thông tin hệ thống, PCI-DSS, dữ liệu tài chính nhạy cảm: thông tin định danh khách hàng, thông tin tài khoản, thông tin tiền gửi ...).
2.2.5. Gắn nhãn (tagging) và nhóm API	Cho phép người dùng tự định nghĩa nhãn (tags) và nhóm các API theo (ít nhất) các tiêu chí: high-risk, low risk; unauthenticated; new api/recently updated…
2.3. Quản lý vòng đời API	
2.3.1. Theo dõi thay đổi phiên bản API	Có thể theo dõi sự thay đổi và các phiên bản khác nhau của API, API phiên bản cũ, hoặc các API không còn được sử dụng (Đối với Zombie API: không có lượt truy cập nào trong vòng tối đa 90 ngày – có thể tuỳ chỉnh ngắn hơn cho phù hợp với BIDV).
2.3.2. So sánh sự khác biệt giữa các phiên bản API	Có hỗ trợ so sánh request/response thực tế với schema được định nghĩa trong đặc tả API, cảnh báo các sai lệch.
3. YÊU CẦU VỀ ĐÁNH GIÁ VÀ QUẢN LÝ TRẠNG THÁI BẢO MẬT API	
3.1. Đánh giá lỗ hổng bảo mật và cấu hình sai	
3.1.1. Phát hiện lỗ hổng theo Top 10 OWASP API	Có khả năng quét, phân tích và phát hiện các lỗ hổng API phổ biến theo danh sách OWASP API Security Top 10 (ví dụ: BOLA/IDOR, Broken Authentication, Data Exposure, Rate Limiting, Mass Assignment, Injection, etc.) và các API chưa được xác thực/ xác thực không đúng cách.
3.1.2. Phân tích an ninh dựa trên đặc tả API	Có khả năng phân tích file đặc tả API để tìm kiếm các vấn đề bảo mật liên quan đến tối thiểu các nội dung: cấu hình bảo mật, xác thực và uỷ quyền trước khi golive API mới
3.2. Xác định và phân loại dữ liệu nhạy cảm	
3.2.1. Tự động phát hiện dữ liệu quan trọng trong API traffic	Có khả năng tự động xác định và phân loại các loại dữ liệu gửi qua API (ví dụ: PII, thông tin hệ thống, PCI-DSS, dữ liệu tài chính nhạy cảm: thông tin định danh khách hàng, thông tin tài khoản, thông tin tiền gửi ...) trong request và response của API.
3.2.2. Hỗ trợ tùy chỉnh mẫu dữ liệu	Có thể cho phép người dùng định nghĩa các mẫu (patterns/regex) hoặc các policy/rule để phát hiện các loại dữ liệu đặc thù của tổ chức.
3.3. Quản lý rủi ro và ưu tiên khắc phục	
3.3.1. Chấm điểm rủi ro API	Có thể cung cấp cơ chế chấm điểm rủi ro cho từng API và từng lỗ hổng dựa trên nhiều yếu tố (mức độ nghiêm trọng/khả năng khai thác/…). dựa trên ma trận chấm điểm rủi ro bảo mật của OWASP
3.3.2. Ưu tiên hóa các hành động khắc phục	Có tính năng đưa ra các khuyến nghị và cho phép ưu tiên các hành động cần thực hiện để giảm thiểu rủi ro an ninh API. Cụ thể: - Thứ tự ưu tiên hành động: dựa trên Mức độ ưu tiên khắc phục các lỗ hổng/điểm yếu bảo mật.

Tiêu chí kỹ thuật	Yêu cầu/Mô tả chi tiết
	- Các thông tin khuyến nghị cung cấp bao gồm : Tham chiếu kĩ thuật tới thông tin lỗ hổng/điểm yếu cùng với các biện pháp khắc phục, giảm thiểu tương ứng.
3.4. Tích hợp với quy trình phát triển (DevSecOps)	
3.4.1. Tích hợp CI/CD	Giải pháp có khả năng tích hợp vào các pipeline CI/CD (Jenkins, GitLab CI, Azure DevOps, ...)
4. YÊU CẦU VỀ BẢO VỆ VÀ PHÁT HIỆN MỐI ĐE DOẠN API THEO THỜI GIAN THỰC	
4.1. Phòng chống tấn công theo OWASP API Security Top 10	
4.1.1. Bảo vệ chống BOLA/IDOR (Broken Object Level Authorization)	Có khả năng phát hiện, cảnh báo và phối hợp thực thi chính sách ngăn chặn (có thể dựa trên các hệ thống tích hợp – tham chiếu mục 7) đối với các truy cập trái phép vào tài nguyên dữ liệu (object) do thiếu hoặc sai kiểm soát phân quyền ở cấp đối tượng
4.1.2. Bảo vệ chống lỗi xác thực (Broken User Authentication)	Có khả năng phát hiện, cảnh báo và thực thi chính sách ngăn chặn (có thể dựa trên các hệ thống tích hợp) các tấn công liên quan đến xác thực yếu, quản lý session không an toàn, lộ thông tin xác thực.
4.1.3. Bảo vệ chống lộ lọt dữ liệu quá mức (Excessive Data Exposure)	Có khả năng phát hiện, cảnh báo và thực thi chính sách ngăn chặn (có thể dựa trên các hệ thống tích hợp) API trả về nhiều dữ liệu hơn mức cần thiết.
4.1.4. Bảo vệ chống thiếu kiểm soát tài nguyên và giới hạn (Lack of Resources & Rate Limiting)	Có khả năng phát hiện, cảnh báo và thực thi chính sách ngăn chặn (có thể dựa trên các hệ thống tích hợp) các tấn công DoS/DDoS ở tầng ứng dụng, request bombing, lạm dụng tài nguyên API.
4.1.5. Bảo vệ chống lỗi kiểm soát quyền mức chức năng (Broken Function Level Authorization)	Có khả năng phát hiện, cảnh báo và thực thi chính sách ngăn chặn (có thể dựa trên các hệ thống tích hợp) người dùng truy cập vào các chức năng API mà họ không được phép.
4.1.6. Bảo vệ chống Mass Assignment	Có khả năng phát hiện, cảnh báo và thực thi chính sách ngăn chặn (có thể dựa trên các hệ thống tích hợp) việc kẻ tấn công sửa đổi các thuộc tính đối tượng không được phép thông qua việc gán tham số đầu vào.
4.1.7. Bảo vệ chống cấu hình sai an ninh (Security Misconfiguration)	Có khả năng phát hiện các cấu hình sai trên API endpoints, server (ví dụ: HTTP verb không cần thiết, thiếu Security Header).
4.1.8. Bảo vệ chống tấn công Injection (Injection)	Có khả năng phát hiện, cảnh báo và thực thi chính sách ngăn chặn (có thể dựa trên các hệ thống tích hợp) các loại tấn công injection (SQLi, NoSQLi, Command Injection, XXE, etc.) qua các tham số API.
4.1.9. Bảo vệ chống quản lý tài sản API không đúng cách (Improper Assets Management)	Có khả năng phân tách các API theo các môi trường, hoặc mục đích sử dụng (tuỳ theo mô hình triển khai); lập danh mục và quản lí vòng đời các API đang hoạt động, API phiên bản cũ hoặc không còn sử dụng
4.1.10. Hỗ trợ giám sát và ghi log đầy đủ (Insufficient Logging & Monitoring)	Đảm bảo giải pháp tạo ra log chi tiết và có thể tích hợp với hệ thống giám sát, hệ thống quản lý thông tin và sự kiên bảo mật (SIEM: QRadar) của BIDV để phát hiện tấn công.
4.2. Phát hiện hành vi bất thường và mối đe dọa nâng cao	
4.2.1. Phân tích hành vi người dùng và thực thể	Có thể xây dựng baseline hành vi sử dụng API bình thường cho từng API/ứng dụng/token và phát hiện các hành vi bất thường, sai

Tiêu chí kỹ thuật	Yêu cầu/Mô tả chi tiết
	lệch (ví dụ: truy cập API bất thường, tần suất lạ, lượng dữ liệu bất thường).
4.2.2. Phát hiện tấn công zero-day	Có khả năng phát hiện các mối đe dọa mới, chưa có dấu hiệu (signature) dựa trên phân tích hành vi.
4.2.3. Chống bot và lạm dụng API	Có khả năng phát hiện và ngăn chặn các truy cập tự động độc hại (bots)
4.3. Hành động phản ứng (Response Actions)	
4.3.1. Đa dạng hành động phản ứng (Tham chiếu các mục 6.2; 7; 8.3)	Có khả năng phối hợp với các hệ thống bảo mật khác của BIDV để cung cấp nhiều tùy chọn phản ứng khi phát hiện mối đe dọa: ghi log (log) , cảnh báo (alert), chặn (block request)
5. YÊU CẦU VỀ TUÂN THỦ	
5.1. Ngăn chặn thất thoát dữ liệu (DLP for APIs)	
5.1.1. Phát hiện và kiểm soát dữ liệu quan trọng trong API	Có khả năng giám sát và kiểm soát việc truyền dữ liệu (đã được định nghĩa ở mục 2.2) qua API.
5.1.2. Che giấu/mã hóa dữ liệu (Data Masking/Encryption)	Có khả năng che giấu (masking) hoặc mã hóa một phần dữ liệu nhạy cảm trong log, báo cáo hoặc trên giao diện dashboard quản trị. Cơ chế masking/mã hoá có thể đáp ứng các tiêu chuẩn như PCI DSS
5.2. Ghi log và kiểm toán (Auditing and Logging)	
5.2.1. Ghi nhận API Traffic Log	Có cơ chế ghi nhận log dạng API Traffic với tối thiểu các trường thông tin sau: Headers, body, IP Client, User-Agent, Timestamp, HTTP Status Code
5.2.2. Ghi log quản trị	Có khả năng ghi log các thay đổi cấu hình, hoạt động của quản trị viên trong ít nhất 03 tháng và sao lưu log tối thiểu 01 năm; Có hỗ trợ gửi log tới các hệ thống tích hợp khác thông qua Syslog.
5.2.3. Đảm bảo tính toàn vẹn của log	Có cơ chế bảo vệ log chống sửa đổi trái phép.
6. YÊU CẦU VỀ KHẢ NĂNG TÍCH HỢP	
6.1. Tích hợp với API Gateway	Có khả năng tích hợp với các giải pháp API Gateway mà BIDV sử dụng, bao gồm tối thiểu các API Gateway sau: IBM API Connect (OpenAPI), Kong, Apigee.
6.2. Tích hợp với hệ thống SIEM, SOAR	Có khả năng tích hợp, gửi sự kiện an ninh, log (Syslog) tới hệ thống Quản lý sự kiện và thông tin bảo mật (SIEM :QRadar) và Hệ thống điều phối, tự động hoá phản hồi bảo mật (SOAR: xSOAR hay Cortex XSOAR) của BIDV.
6.3. Tích hợp với WAF	Có thể tích hợp với một số giải pháp Web Application Firewall (WAF), bao gồm tối thiểu: Imperva và F5.
6.4. Tích hợp công cụ Monitor giám sát bên thứ ba	Có khả năng, hỗ trợ tích hợp với 1 trong các công cụ giám sát hiệu năng bên ngoài: Prometheus & Grafana, Telemetry, Manage Engine thông qua tối thiểu 1 trong các phương thức: syslog, webhook hoặc SNMP, API.
7. YÊU CẦU VỀ QUẢN TRỊ, VẬN HÀNH	
7.1. Quản lý tập trung	
7.1.1. Giao diện trực quan, dễ sử dụng	Có khả năng cung cấp giao diện quản lý web tập trung, trực quan, và quản lý toàn bộ các tính năng của giải pháp.
7.1.2. Dashboard tùy chỉnh	Có cho phép tùy chỉnh dashboard theo nhu cầu người dùng liên quan tới tình trạng theo dõi, tình trạng bảo mật API.

Tiêu chí kỹ thuật	Yêu cầu/Mô tả chi tiết
7.2. Quản lý người dùng và phân quyền	
7.2.1. Hỗ trợ Role-Based Access Control (RBAC)	Có hỗ trợ quản lý người dùng và phân quyền chi tiết (RBAC) cho các vai trò quản trị khác nhau, đảm bảo chỉ những người có thẩm quyền mới truy cập được các chức năng/dữ liệu tương ứng.
7.2.2. Tích hợp với LDAP/AD	Có thể tích hợp với hệ thống quản lý người dùng tập trung của BIDV (AD/AD FS) thông qua LDAP/SAML để xác thực người dùng quản trị.
7.3. Cảnh báo và thông báo (Alerting and Notifications)	
7.3.1. Cảnh báo thời gian thực	Có khả năng cung cấp cơ chế cảnh báo thời gian thực khi phát hiện các sự kiện an ninh, hành vi bất thường hoặc vi phạm chính sách.
7.3.2. Thông báo đa kênh	Có hỗ trợ gửi cảnh báo qua nhiều kênh khác nhau: Email của BIDV hoặc qua API tới hệ thống ticketing: Jira
7.3.4. Quản lý phát hiện sai (false positive)	Có khả năng gán nhãn/đánh dấu các phát hiện, điểm yếu hay rủi ro bảo mật là an toàn hoặc không, đưa vào danh sách nhận diện tương tự trên từng API
8. YÊU CẦU VỀ BÁO CÁO	
8.1. Tùy chỉnh báo cáo	Có cung cấp cho người dùng các mẫu báo cáo: Compliance, Security và trích xuất sang một trong các định dạng thông dụng: CSV, JSON, PDF,...
8.2 Quyền tạo báo cáo	Hỗ trợ tạo báo cáo theo phân quyền (RBAC)

3. Yêu cầu về dịch vụ triển khai

- Thời gian triển khai:
  + Thời gian bàn giao hàng hoá: Trong vòng 30 ngày kể từ ngày hợp đồng có hiệu lực.
  + Thời gian triển khai tích hợp, cài đặt và cấu hình hệ thống: Trong vòng 180 ngày kể từ ngày hợp đồng có hiệu lực.
- Trách nhiệm của nhà thầu:
  + Nhà thầu chịu trách nhiệm triển khai cài đặt phần mềm do nhà thầu cung cấp theo đúng yêu cầu tính năng kỹ thuật của sản phẩm.
  + Cài đặt, cập nhật các phiên bản phần mềm mới nhất của sản phẩm, phù hợp với hệ thống BIDV.
  + Nhà thầu đề xuất mô hình triển khai phù hợp với hạ tầng của BIDV.
  + Đảm bảo triển khai không ảnh hưởng tới các hệ thống tích hợp của BIDV trong trường hợp giải pháp API Security gặp sự cố/downtime.
- Quy trình triển khai: Nhà thầu phải đề xuất kế hoạch triển khai chi tiết, bao gồm nhưng không giới hạn các bước sau:

1. Khảo sát hiện trạng hệ thống hiện tại.
2. Đề xuất mô hình triển khai.
3. Lập kế hoạch triển khai.
4. Bàn giao hàng hóa.
5. Triển khai cài đặt, tích hợp.
6. Nghiệm thu hàng hóa và nghiệm thu hoàn thành triển khai.

- Nhà thầu phải cung cấp đủ nguồn lực để triển khai các hạng mục sau đây:
  + Thiết kế kiến trúc của hệ thống: phân tích yêu cầu của hệ thống và đưa ra giải pháp phù hợp. Bản thiết kế phải thể hiện được các thành phần chính và liên quan, cách thức kết nối và tương tác với nhau.
  + Thiết kế mô hình, phương án triển khai cho các môi trường của BIDV bao gồm: Môi trường triển khai thật (Production DC1 và DC2), môi trường dự phòng (DR), môi trường test (UAT).
  + Triển khai trên môi trường: Production (DC1 và DC2), môi trường dự phòng (DR).
  + Cung cấp nhân sự hỗ trợ (trực tiếp tại BIDV và từ xa) trong quá trình triển khai và tích hợp hệ thống; bao gồm cả các nội dung cài đặt, cấu hình, kiểm tra các thành phần và các nội dung cập nhật bản vá, health check, tuning, tối ưu cấu hình, kể cả cài đặt sau triển khai.

4. Yêu cầu về dịch vụ hỗ trợ kỹ thuật

- Hỗ trợ kỹ thuật chính hãng 24/7 (khắc phục sự cố, nâng cấp, cập nhật phần mềm) trong thời gian bản quyền sử dụng còn hiệu lực và tương ứng với số bản quyền đã mua hàng năm.

- Hình thức hỗ trợ: Tại chỗ (On-site) hoặc từ xa (Off-site) qua điện thoại, email, kênh trao đổi thông tin, chương trình hỗ trợ kỹ thuật từ hãng, nhà cung cấp tại Việt Nam phụ thuộc vào mức độ cấp thiết và khẩn cấp của tình huống cần hỗ trợ (chi tiết tham chiếu bảng yêu cầu về thời gian phản hồi bên dưới).

- Yêu cầu chung:
  + Đảm bảo duy trì hoạt động liên tục, ổn định của hệ thống bảo mật cho các hệ thống nhằm cung cấp dịch vụ với chất lượng cao, ổn định, thuận tiện và an toàn.
  + Đảm bảo ngăn ngừa lỗi, hạn chế phát sinh sự cố đối với hệ thống, góp phần nâng cao tính bảo mật, an toàn trong công tác vận hành hệ thống.
  + Đảm bảo khả năng sửa chữa nhanh những hỏng hóc, khắc phục kịp thời sự cố phát sinh nhằm khôi phục và đảm bảo khả năng sẵn sàng hoạt động một cách nhanh nhất cho hệ thống đảm bảo an toàn cho hệ thống.

- Được cung cấp tài khoản và có thể truy cập vào trang web hỗ trợ của hãng để tìm kiếm, tải về các tài liệu, tài nguyên, liên quan đến sản phẩm, và có thể tạo yêu cầu hỗ trợ.

- Được phép cập nhật miễn phí tất cả các phiên bản phần mềm (software/firmware), model AI mới nhất của thiết bị được hãng phát hành.

- Các chi phí phát sinh trong thời gian thực hiện dịch vụ hỗ trợ kỹ thuật do nhà thầu chi trả.

- Hỗ trợ kỹ thuật định kỳ:
  + Định kỳ 03 tháng/lần vào tuần đầu tiên của kì kiểm tra, nhà thầu thực hiện kiểm tra tình trạng hoạt động của đưa ra những khuyến nghị nhằm đảm bảo và nâng cao hiệu quả hoạt động.
  + Các yêu cầu kiểm tra cụ thể:

- Thực hiện phân tích đánh giá các vấn đề kỹ thuật của hệ thống định kỳ dựa trên file log của hệ thống, có báo cáo đầy đủ về các vấn đề phát sinh và nội dung thực hiện.
- Thực hiện phân tích đánh giá mức tăng trưởng dữ liệu của hệ thống định kỳ có báo cáo đề xuất thiết lập tham số và tối ưu hệ thống.
- Thực hiện cập nhật bản vá lỗi của hệ thống định kỳ và có báo cáo kết quả thực hiện.

– Hỗ trợ kỹ thuật đột xuất:

+ Kênh hỗ trợ: Tùy theo tính chất và mức độ của sự cố phát sinh, các yêu cầu hỗ trợ có thể được tiếp nhận thông qua các kênh sau:
  - Thông qua websites hỗ trợ của hãng.
  - Thông qua email tới bộ phận tiếp nhận yêu cầu hỗ trợ từ hãng, hoặc đầu mối nhà thầu.
  - Thông qua điện thoại trực tiếp tới đầu mối tiếp nhận hỗ trợ của nhà thầu.
+ Thời gian hỗ trợ trực tuyến: 24x7x365.
+ Thời gian phản hồi: Đối với các yêu cầu kỹ thuật và xử lý sự cố được tạo trên website của hãng sẽ được phản hồi trong khoảng thời gian theo tiêu chuẩn của từng hãng. Đối với các yêu cầu kỹ thuật và xử lý sự cố khác, thời gian phản hồi và hình thức hỗ trợ tùy theo mức độ cần đáp ứng như sau:

Cấp độ nghiêm trọng	**Mô tả**	**Thời gian đáp ứng**	**Phương thức hỗ trợ**
1	Lỗi gây cho sản phẩm không hoạt động, hoặc gây ảnh hưởng nghiêm trọng như ảnh hưởng toàn hệ thống, hoặc hệ thống bị dừng.	0.5 giờ	Tại chỗ 24x7
2	Lỗi làm giảm hiệu năng của sản phẩm, hoặc hạn chế các dịch vụ kinh doanh như ảnh hưởng nhẹ đến hệ thống, làm treo hệ thống.	04 giờ	Tại chỗ 24x7
3	Lỗi gây ra ảnh hưởng nhỏ đến việc sử dụng sản phẩm, các ảnh hưởng nhẹ đến hệ thống, các ảnh hưởng đến hiệu năng và chức năng.	04 giờ	Từ xa 8x5
4	Lỗi liên quan đến phần mềm mà không ảnh hưởng nhiều đến việc sử dụng chức năng sản phẩm để thực hiện hoạt động kinh doanh.	04 giờ	Từ xa 8x5

+ Yêu cầu hỗ trợ kỹ thuật cho giải pháp bao gồm (tối thiểu):
+ Hỗ trợ BIDV tích hợp vào hệ thống OpenAPI, đảm bảo triển khai bảo vệ đầy đủ cho các APIs trên Open API của BIDV..
  - Thực hiện hỗ trợ đột xuất theo thực tế các phát sinh của hệ thống trong quá trình vận hành.
  - Thực hiện hỗ trợ BIDV trong quá trình khai báo tham số theo yêu cầu của nghiệp vụ.

5. Yêu cầu về đào tạo, chuyển giao kỹ thuật:

- Sau khi hoàn thành triển khai, nhà thầu phải cung cấp các tài liệu đầy đủ và dễ hiểu về tất cả các mặt của các hệ thống được đề xuất, bao gồm nhưng không chỉ giới hạn ở:
  + Tài liệu hướng dẫn chi tiết các bước thực hiện trong quá trình triển khai các nội dung cài đặt, cấu hình, tích hợp các thiết bị.
  + Tài liệu hướng dẫn quản trị vận hành.
- Nhà thầu thực hiện đào tạo, hướng dẫn sử dụng, chuyển giao công nghệ về quản trị và vận hành với các yêu cầu sau:
  + Nội dung: Quản trị, vận hành giải pháp bảo mật API Security chuyên dụng
  + Địa điểm: TTCNTT BIDV số 7 Duy Tân, Cầu Giấy, Hà Nội
  + Số lượng cán bộ tham gia của BIDV: tối thiểu 5 người/lớp đào tạo.
  + Thời gian (số lớp đào tạo): 2 lớp đào tạo, tối thiểu 02 giờ/ lớp.

6. Yêu cầu bàn giao, nghiệm thu hàng hóa

- Nhà thầu phải bàn giao đầy đủ bản quyền phần mềm của giải pháp và các bản quyền phần mềm liên quan khác nếu có, đảm bảo có thể tra cứu thông qua hồ sơ bàn giao bản quyền dạng bản cứng hoặc thông tin tra cứu trên giao diện quản trị của giải pháp.
- Nhà thầu phải bàn giao đầy đủ các tài liệu theo quy định.

  Danh mục tài liệu/báo cáo cần cung cấp:

STT	**Tài liệu/Báo cáo**	**Thời điểm thực hiện** (Trong vòng khoảng thời gian yêu cầu tính từ ngày hợp đồng có hiệu lực)
1	Tài liệu thiết kế (mô hình triển khai) trên cơ sở các nội dung đã được BIDV thống nhất .	180
2	Tài liệu hướng dẫn cài đặt, triển khai dịch vụ, vận hành hệ thống	180
3	Quy trình nâng cấp sản phẩm, hỗ trợ kỹ thuật, xử lý sự cố	180
4	Báo cáo kiểm thử tải từ nhà thầu	180
5	Báo cáo kết quả đánh giá bảo mật, xử lý các lỗ hổng bảo mật (nếu có) từ nhà thầu	180
6	Tài liệu hướng dẫn chuyển đổi dự phòng DC-DC, DC-DR	180