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 dự án, gói thầu

- Bên mời thầu: Ngân hàng Liên doanh Việt – Nga.
- Tên gói thầu: Gia hạn bản quyền hệ thống database firewall.
- Tên dự án: Gia hạn bản quyền hệ thống database firewall.
- Địa điểm thực hiện dự án: Hội sở chính (HO), Trung tâm dữ liệu (DC) của Ngân hàng Liên doanh Việt – Nga.
- Nguồn vốn: Nguồn kinh phí hoạt động của Ngân hàng Liên Doanh Việt – Nga.
- Thời gian cung cấp giấy chứng nhận license: 30 ngày kể từ ngày hợp đồng có hiệu lực
- Thời hạn license: 01 năm.

1.2. Yêu cầu về kỹ thuật

1.2.1. Yêu cầu chung

Yêu cầu chung về hàng hóa cung cấp

- Phần mềm cung cấp theo gói thầu phải có bản quyền hợp lệ, không vi phạm luật sở hữu trí tuệ;

- Nhà thầu tham gia dự thầu phải chào đúng và đủ chủng loại, khối lượng hàng hoá nêu tại Bảng Phạm vi cung cấp hàng hóa;

- Hàng hóa được cung cấp tới địa điểm yêu cầu của E-HSMT phải trong dạng đóng gói của Nhà sản xuất; các thông số bên trong phải phù hợp với đặc tính kỹ thuật được cam kết tại E-HSDT. Bất kỳ sự thay đổi nguồn gốc, chủng loại, quy cách kỹ thuật nào sẽ không được chấp thuận nếu không có sự đồng ý của Đơn vị trực tiếp sử dụng tài sản.

- Nhà thầu phải đảm bảo có hàng hóa thay thế sẵn sàng trong trường hợp hàng hóa cung cấp có sự cố, đảm bảo việc sử dụng không gián đoạn.

1.2.2. Yêu cầu kỹ thuật cụ thể

a) Yêu cầu kỹ thuật cụ thể về hàng hoá:

STT	Yêu cầu	Thông số kĩ thuật	Thời gian license
1	**Tính năng**		
1.1	**Phần mềm Database Firewall Impervar**		**12 tháng**
		Audit/giám sát các hoạt động trên CSDL (các lệnh DML, DDL, DCL, SELECT), bao gồm hoạt động của người dùng có đặc quyền (privileged users) truy cập trực tiếp trên CSDL	
		Cung cấp chính sách audit ghi lại các truy cập CSDL sau:: - Database configuration changes - Database connections - New Databases - New Users Account - Privilege Manipulation - Privilege Operations - New Users Account - Users and Privileges Management Commands	
		Có sẵn phân tích, hiển thị các thông tin nguồn truy cập sau mà không cần cấu hình thêm: - Shared DB User, - Most Active Users, - Source Applications, - Source Host, OS Users, - Source IPs,	

STT	Yêu cầu	Thông số kĩ thuật	Thời gian license
		- User Groups, - Login Analysis - Performance by Source.	
		Có sẵn các hiển thị các thông tin về hành động người dùng đặc quyền sau mà không cần cấu hình thêm: - Privileged Query Overview - Table drops/truncates - Stored Procedures Changes - Changes to DB/Schemas - DCL Commands - DDL Commands - Native Auditing Changes - Newly Created Users	
		Có khả năng tự động phát hiện (discover) các máy chủ CSDL	
		Phát hiện, cảnh báo, ngăn chặn các truy cập SQL trái quyền, chống tấn công SQL injection trên CSDL (áp dụng đối với CSDL quan hệ)	
		Cung cấp signature phát hiện/chống tấn công, và Signature bảo vệ điểm yếu đã biết (gắn theo mã CVE), các mẫu được cập nhật liên tục	
		Cho phép người dùng tùy biến, tự viết Signature sử dụng ngôn ngữ Regular Expressions	
		Các chính sách Audit và Security được định nghĩa và áp dụng một cách độc lập với nhau	

STT	Yêu cầu	Thông số kĩ thuật	Thời gian license
		Cung cấp các chính sách bảo vệ (Security Policy) nhiều mức, gồm mức mạng (Network Security Policies), mức dịch vụ CSDL (Database Service Level Security Policies), và mức ứng dụng CSDL (DB Application Level Policies) Cung cấp các mẫu chính sách được định nghĩa sẵn, cho phép tùy biến chính sách	
		- Kiểm tra giao thức mạng TCP/IP tuân thủ theo chuẩn RFC (Network Protocol Validation) - Kiểm tra hợp lệ giao thức CSDL/SQL (SQL protocol validation, DB protocol Validation) như kiểm tra độ dài, kích thước header, giá trị tham số có hợp lệ. - Phát hiện tấn công ứng dụng CSDL qua nhiều giai đoạn (multi-stage database application attacks)	
		Cung cấp chính sách bảo mật có sẵn xử lý các vấn đề bảo mật sau: - SQL Protocol Validation - Oracle SQL Protocol Validation - SQL Correlation Policy - SQL Protocol Signatures	
		Có tính năng phát hiện các truy cập bất thường từ phân tích log thông qua machine-learning, tính năng với bản quyền cho tối thiểu 8 DB server Có khả năng phát hiện các truy cập bất thường điển hình sau từ các phân tích: - Người dùng sử dụng tài khoản dịch vụ DB dành cho ứng dụng để truy cập CSDL (Database Service Account Abuse) - Người dùng truy cập vùng dữ liệu chỉ dành cho ứng dụng (Suspicious Application Data Access) - Sử dụng máy tính khác để truy cập DB, dấu hiệu tài khoản DB bị đánh cắp (Machine Takeover)	

STT	Yêu cầu	Thông số kĩ thuật	Thời gian license
		- Truy cập số lượng lớn bản ghi DB quá mức bình thường (Excessive Database Record Access) - Truy cập nhiều CSDL quá mức bình thường (Excessive Multiple Database Access) - Login sai nhiều lần (Excessive Failed Logins) - Login sai nhiều lần từ máy chủ ứng dụng (Excessive Failed Logins from Application Server) - Truy cập DB vào thời gian bất thường (Database Access at Non-standard Time) - Sử dụng lệnh DB đáng ngờ (Suspicious Database Command Execution) - Sử dụng các dynamic SQL queries bất thường - Suspicious Dynamic SQL Activity	
		Phát hiện tấn công brute force attack, nỗ lực login nhiều lần trong một thời gian ngắn, nhiều người dùng từ cùng một host/IP address login sai vượt quá số lần được định nghĩa	
		Đánh giá điểm yếu trên CSDL. Đánh giá dựa theo chuẩn DISA STIG, CIS và CVSS (Common Vulnerability Scoring System)	
		Đánh giá rủi ro bằng việc kết hợp điểm yếu và dữ liệu nhạy cảm liên quan	
		Hỗ trợ mô hình triển khai host based, cài đặt Agent trên các CSDL	
		Agent cài trên máy chủ CSDL thu thập các hoạt động trên Shared Memory, IPC, TCP local, BEQ,..	
		Cho phép cấu hình mức sử dụng CPU của agent, nếu vượt ngưỡng nào đó sẽ tạm dừng hoặc bypass agent để tránh gây ảnh của tới máy chủ DB	

STT	Yêu cầu	Thông số kĩ thuật	Thời gian license
		Hỗ trợ triển khai các gateway trong chế độ cluster N+1, cho phép chia tải giữa các thành viên trong cluster	
		Hỗ trợ các DB bao gồm Oracle, Microsoft SQL Server, MySQL, PostgreSQL, Progress OpenEdge, MariaDB	
1.2	**Quản trị tập trung**		
		Hỗ trợ SNMP, SMTP/Email, syslog, real-time monitoring cho giám sát	
		Hỗ trợ quản lý, lưu trữ dữ liệu audit: - Encrypt audit archives - Data signing - FTP archive, SCP archive	
		Áp dụng chính sách theo đối tượng DB bảo vệ (máy chủ/service) mà không phải áp chính sách theo DBF gateway	
		Định nghĩa chính sách an ninh tập trung áp dụng cho toàn bộ hệ thống DB, với các loại DB khác nhau (MSSQL, Oracle, MySQL), không yêu cầu định nghĩa cùng chính sách lặp lại nhiều lần cho từng hệ thống CSDL khác nhau	
		Cung cấp quản trị tập trung cho phép cấu hình chính sách, tạo báo cáo, hiển thị log và giám sát sự kiện trong thời gian thực cho tất cả các thiết bị DB Firewall và agent trên cùng một giao diện duy nhất.	
		Dữ liệu báo cáo tổng hợp từ nhiều DBF gateway có thể được cấu hình lịch lấy dữ liệu nhật ký theo phút và giờ (như là lấy dữ liệu nhật ký trong 15 phút qua, trong 1 giờ qua,..)	

STT	Yêu cầu	Thông số kĩ thuật	Thời gian license
		Dữ liệu nhật ký/Audit phải được lưu trong flat file được mã hóa, không lưu trong CSDL quan hệ để đảm bảo tính bảo mật và nguyên vẹn	