

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Giới thiệu chung về Gói thầu

Tên gói thầu	Giải pháp giảng dạy và phát hiện tấn công nâng cao
Nguồn vốn	Vốn đầu tư, mua sắm tài sản cố định của Ngân hàng TMCP Việt Nam.
Tên chủ đầu tư	Ngân hàng TMCP Công Thương Việt Nam
Thời gian thực hiện gói thầu	150 ngày kể từ ngày Hợp đồng có hiệu lực
Loại hợp đồng	Trọn gói
Mục tiêu công việc	Triển khai Giải pháp giảng dạy và phát hiện tấn công nâng cao

Mục 2. Yêu cầu về kỹ thuật

2.1. Biểu mẫu phạm vi cung cấp

Đáp ứng theo yêu cầu tại mẫu số 01A Phạm vi cung cấp hàng hóa, Chương IV

2.2. Yêu cầu kỹ thuật chi tiết

Thiết bị chào thầu phải có cấu hình/thành phần tương đương hoặc cao hơn các yêu cầu như sau:

STT	Hạng mục	Yêu cầu tối thiểu	Số lượng	Đơn vị
I	Hệ thống phòng thủ chủ động dựa trên công nghệ Deception – giải pháp dạng Appliance (phần cứng tích hợp sẵn phần mềm – được cung cấp từ một hãng sản xuất).			
1	Thông số phần cứng			
1.1	Thiết bị triển khai tại DC		1	Thiết bị
	Yêu cầu về bộ nhớ RAM	DDR4-2400 48 GB ECC RDIMM (16 GB*3)		
	Yêu cầu về cổng kết nối	4 x GE (RJ45) 4 x GE (SFP)		

STT	Hạng mục	Yêu cầu tối thiểu	Số lượng	Đơn vị
	Yêu cầu về bộ lưu trữ sử dụng được (Sau khi RAID)	1 TB		
	Kích thước tiêu chuẩn	1 RU Rackmount		
	Nguồn điện	100-240 VAC, 60-50 Hz, 650W Redundant PSU		
	Năm sản xuất	2025 trở về sau		
	Số lượng Decoy VM tối đa	20 Decoy		
	Số địa chỉ IP tối đa cho mỗi Decoy	24		
	Số lượng Decoy tối đa	480		
	Hỗ trợ các nền tảng Decoy VM	Windows 7 / 10 / 11, Win 10 / 11 (customizable, BYOL), Win Server 2016/2019/2022 (customizable, BYOL), Ubuntu 16.04 / 18.04, Redhat (customizable, BYOL), CentOS 7.9, SSL-VPN, ESXI Decoy, IoT (Routers, Switch, Printers and IP-Camera), Medical devices, (PACS, Infusion pump), SWIFT, SCADA, ERP, POS, SAP, Elastic Search, Tomcat, MySql MariaDB, SIP, XMPP, MQTT, 4G/5G 3GPP, MacOS, Webmin, Citrix, Nginx, EV-CPO		
	Hỗ trợ các dịch vụ Decoy	ARP, BACNET, B.BRAUN (port 8080), CAN Bus Protocol, CDP, CoAP, CWMP, DICOM Serve, Elastic Search, ENIP, ERP-WEB, FTP, GIT, GTP-U, Guardian-AST, HoneyDoc, HTTP, HTTP (APACHE), HTTPS, ICMP, IEC104, IIS (HTTP), IIS (HTTPS), Infusion Pump (FTP), Infusion Pump (Telnet), IP Camera-WEB, IPMI, Jetdirect, KAMSTRUP, Lantronix Discovery Protocol, LOGON, MariaDB, MOXA, MQTT WEB, MSSQL, MYSQL, NBNSSpoofSpotter, NextEPC WEB, PACS, PACS-WEB, POS-WEB, Printer-		

STT	Hạng mục	Yêu cầu tối thiểu	Số lượng	Đơn vị
		WEB, PROFINET, RADIUS, RARP, RDP, RTSP, SAMBA, SAP DISPATCHER, SAP ROUTER, SAP WEB, SAP WEB HTTPS, ScadaBR, SCTP and GTP-C, SIP, SMB, SMTP, SNMP, SRTP, SSH, SSLVPN, SWIFT Lite2, TCPListener, Telnet, TFTP, TOMCAT (HTTP), TOMCAT (HTTPS), TP-LINK WEB, TRICONEX, UPnP, vnc, XMPP, XMPP, WEB		
	Các chứng chỉ an toàn	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB		
1.2	Thiết bị triển khai tại DR		1	Thiết bị
	Yêu cầu về bộ nhớ RAM	4G		
	Yêu cầu về cổng kết nối	10 x GE RJ45		
	Hỗ trợ các nền tảng Decoy VM	Windows 7 / 10 / 11, Win 10 / 11 (customizable, BYOL), Win Server 2016/2019/2022 (customizable, BYOL), Ubuntu 16.04 / 18.04, Redhat (customizable, BYOL), CentOS 7.9, SSL-VPN, ESXI Decoy, IoT (Routers, Switch, Printers and IP-Camera), Medical devices, (PACS, Infusion pump), SWIFT, SCADA, ERP, POS, SAP, Elastic Search, Tomcat, MySql MariaDB, SIP, XMPP, MQTT, 4G/5G 3GPP, MacOS, Webmin, Citrix, Nginx, EV-CPO		
	Hỗ trợ các dịch vụ Decoy	ARP, BACNET, B.BRAUN (port 8080), CAN Bus Protocol, CDP, CoAP, CWMP, DICOM Serve, Elastic Search, ENIP, ERP-WEB, FTP, GIT, GTP-U, Guardian-AST, HoneyDoc, HTTP, HTTP (APACHE), HTTPS, ICMP, IEC104, IIS (HTTP), IIS (HTTPS), Infusion Pump (FTP), Infusion Pump (Telnet), IP Camera-WEB, IPMI, Jetdirect, KAMSTRUP, Lantronix Discovery Protocol, LOGON, MariaDB, MOXA, MQTT WEB, MSSQL, MYSQL,		

STT	Hạng mục	Yêu cầu tối thiểu	Số lượng	Đơn vị
		NBNSSpoofSpotter, NextEPC WEB, PACS, PACS-WEB, POS-WEB, Printer-WEB, PROFINET, RADIUS, RARP, RDP, RTSP, SAMBA, SAP DISPATCHER, SAP ROUTER, SAP WEB, SAP WEB HTTPS, ScadaBR, SCTP and GTP-C, SIP, SMB, SMTP, SNMP, SRTP, SSH, SSLVPN, SWIFT Lite2, TCPLListener, Telnet, TFTP, TOMCAT (HTTP), TOMCAT (HTTPS), TP-LINK WEB, TRICONEX, UPnP, vnc, XMPP, XMPP, WEB		
	Các chứng chỉ an toàn	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB, USGv6/IPv6		
2	Tính năng phần mềm – tích hợp sẵn trên phần cứng		1	Gói
2.1	Bản quyền phần mềm: có thời hạn 15 tháng kể từ ngày hoàn thành triển khai			
2.2	Các tính năng bắt buộc			
	Asset Discovery	Hệ thống phải hỗ trợ quét và phát hiện tài sản trong hệ thống		
	Deploy Decoy dễ dàng	Hệ thống phải hỗ trợ triển khai Decoy theo wizard hướng dẫn		
		Hệ thống phải hỗ trợ thêm danh sách tài khoản tùy chỉnh để làm mồi nhử		
		Hệ thống phải hỗ trợ kết nối về máy chủ LDAP để thu thập danh sách tài khoản làm mồi nhử		
	Triển khai Decoy chân thực, giống hệ thống thật	Hệ thống phải có khả năng khám phá thông tin của hệ thống mạng thật và xây dựng các bẫy phù hợp với các hệ thống này		
	Phát hiện các hành vi do thám mạng nội bộ	Hệ thống phải có khả năng phát hiện sớm các hành vi do thám mạng nội bộ như quét ICMP, quét cổng. Đây là chức năng cảnh báo sớm giai đoạn reconnaissance của nhóm tin tặc trong hệ thống – một yêu cầu tối thiểu để ngăn hàng phát hiện tấn công từ sớm.		

STT	Hạng mục	Yêu cầu tối thiểu	Số lượng	Đơn vị
	Phát hiện và cảnh báo Malware/Ransomware trên Decoy	Hệ thống phải có khả năng phát hiện Malware/Ransomware được gửi vào Decoy.		
	Giám sát hành động Attacker	Hệ thống phải có khả năng phát hiện và ghi lại các hành động của tin tặc khi tương tác với Decoy như đăng nhập, đăng xuất, thay đổi file trong hệ thống, điều chỉnh registry, ...		
	Phân tích sự kiện, cung cấp thông tin chi tiết về kỹ thuật, chiến thuật của tin tặc	Hệ thống phải có khả năng ghi nhận các sự kiện xảy ra trên Decoy, với đầy đủ các thông tin như: thời gian sự kiện, mức độ nghiêm trọng, giao thức sử dụng để kết nối, thông tin địa chỉ IP, MAC của tin tặc, ...		
	Tích hợp với SIEM	Hệ thống phải có khả năng kết nối với các hệ thống SIEM qua các giao thức thông dụng như Syslog, CEF		
2.3	Yêu cầu về tính năng nâng cao			
	Phát hiện đến các kết nối URL độc hại thông qua cơ sở dữ liệu Web Filtering	Hệ thống phải có khả năng phát hiện các kết nối đến URL độc hại, giám sát các kết nối ra ngoài Internet của các Decoy. Cơ sở dữ liệu Web Filtering phải hỗ trợ hơn 500M các website được phân loại vào các danh mục khác nhau.		
	Phát hiện các kết nối ICMP bất thường	Hệ thống phải có khả năng phát hiện, và ghi nhận các kết nối ICMP bất thường.		
3	Dịch vụ bảo hành và hỗ trợ kỹ thuật		1	Gói
	Dịch vụ hỗ trợ kỹ thuật	- Hỗ trợ phản hồi khi có sự cố kỹ thuật (24x7x365): phản hồi trong vòng 1h đối với các sự cố nghiêm trọng và trong ngày làm việc kế tiếp với các sự cố không nghiêm trọng. - Cung cấp dịch vụ hỗ trợ, giải đáp các vấn đề kỹ thuật, quản trị vận hành sản phẩm qua các công cụ web, điện thoại, và chat.		

STT	Hạng mục	Yêu cầu tối thiểu	Số lượng	Đơn vị
		- Hỗ trợ thay thế các thiết bị, linh kiện hỏng lỗi. - Thực hiện nâng cấp firmware khi có phiên bản mới. - Cung cấp Portal quản trị thiết bị để khách hàng có thể tự quản lý, theo dõi các thiết bị đang sử dụng. - Thời hạn cung cấp dịch vụ hỗ trợ kỹ thuật: 12 tháng từ thời điểm hoàn thành triển khai và nghiệm thu hệ thống đối với Thiết bị phần cứng và 15 tháng từ thời điểm hoàn thành triển khai và nghiệm thu hệ thống đối với Bản quyền phần mềm tích hợp sẵn trên phần cứng		
	Dịch vụ bảo hành	Dịch vụ Bảo hành giải pháp chính hãng: 12 tháng đối với Thiết bị phần cứng và 15 tháng đối với Bản quyền phần mềm tích hợp sẵn trên phần cứng .		
4	Dịch vụ triển khai		1	Gói
	Triển khai	Thực hiện các công việc triển khai: giao hàng, lắp đặt, cài đặt, kết nối với các hệ thống liên quan, đưa giải pháp vào vận hành hoạt động theo đúng chức năng yêu cầu. Đảm bảo công việc triển khai hoàn thành trước thời hạn. Thời gian triển khai: 90 ngày kể từ ngày ký hợp đồng.		
5	Dịch vụ đào tạo, chuyển giao		1	Gói
	Đào tạo hướng dẫn vận hành hệ thống	Giảng viên có chứng chỉ do hãng chứng nhận. Số lượng học viên: tối thiểu 03 cán bộ của VietinBank. Nội dung: quản trị, vận hành, tối ưu hệ thống.		