TỔNG CÔNG TY QUẢN LÝ BAY VIỆT NAM
TRUNG TÂM ĐÀO TẠO - HUẤN LUYỆN NGHIỆP VỤ QUẢN LÝ BAY

Số: 1533 /TTĐTHL-ĐT
V/v mời báo giá gói đào tạo Nâng cao an ninh mạng và quản trị hệ thống

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 12 tháng 8 năm 2025

Kính gửi: Quý công ty

Trung tâm Đào tạo - Huấn luyện nghiệp vụ Quản lý bay (Trung tâm Đào tạo - Huấn luyện) có nhu cầu mời báo giá gói đào tạo Nâng cao an ninh mạng và quản trị hệ thống (Chi tiết tại phụ lục kèm theo).

Kính mời các Công ty quan tâm gửi báo giá gói dịch vụ trên để làm cơ sở xem xét.

Thời gian tiếp nhận: Trước 9h30 ngày 15/8/2025.

Hình thức gửi báo giá: Bản cứng (đóng dấu đỏ).

Địa chỉ nhận báo giá:

- Trung tâm Đào tạo - Huấn luyện nghiệp vụ Quản lý bay; Số 5 ngõ 200 đường Nguyễn Sơn, Phường Bồ Đề, TP Hà Nội.

- Người liên hệ: Bà Tạ Thu Trang; Số điện thoại: 0906655623

Mong nhận được sự hợp tác của Quý công ty.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: VT, ĐT (hm02b).

GIÁM ĐỐC

M.S.C.N:0100108624-013-C.T.N.H.H
TRUNG TÂM ĐÀO TẠO-HUẤN LUYỆN NGHIỆP VỤ QUẢN LÝ BAY- -CHI NHÁNH TỔNG CÔNG TY QUẢN LÝ BAY VIỆT NAM - CÔNG TY TNHH
THÀNH PHỐ HÀ NỘI

Nguyễn Đình Tuấn

Phụ lục

(Kèm theo Văn bản số: 1533 /TTĐTHL-ĐT ngày 12 tháng 8 năm 2025)

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
1	Chi phí đào tạo: **1. Thông tin chung khoá đào tạo nâng cao an ninh mạng và quản trị hệ thống:** **1.1 Khoá đào tạo Quản trị hệ thống Linux -LPIC-1 (Linux Professional Institute Certification Level 1)** **a. Tên khoá học:** Khoá đào tạo Quản trị hệ thống Linux -LPIC-1 (Linux Professional Institute Certification Level 1) **b. Quy mô lớp học:** 01 lớp, dự kiến 15-20 người. **c. Thời lượng:** 05 ngày **d. Thời gian thực hiện:** Quý 3, 4/2025 **e. Hình thức đào tạo:** Trực tiếp kết hợp trực tuyến **f. Địa điểm đào tạo:** Tại Thành phố Hồ Chí Minh và nền tảng đào tạo trực tuyến **g. Nội dung đào tạo:** 1. Module 01: Kiến Trúc Hệ Thống • Xác định và cấu hình cài đặt phần cứng • Khởi động hệ thống • Thay đổi mức chạy / mục tiêu khởi động và tắt hoặc khởi động lại hệ thống 2. Module 02: Quản Lý Gói Và Cài Đặt Linux • Thiết kế bố cục đĩa cứng • Cài đặt trình quản lý khởi động • Quản lý thư viện được chia sẻ • Sử dụng quản lý gói Debian • Sử dụng quản lý gói RPM và YUM • Linux như một khách ảo hóa 3. Module 03: Các Lệnh GNU Và Unix • Làm việc trên dòng lệnh • Xử lý luồng văn bản bằng bộ lọc	01	khoá		

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	• Thực hiện quản lý tệp cơ bản • Sử dụng luồng, đường ống và chuyển hướng • Tạo, giám sát và tiêu diệt các quy trình • Sửa đổi các ưu tiên thực hiện quy trình • Tìm kiếm tệp văn bản bằng cách sử dụng cụm từ thông dụng • Chỉnh sửa tệp cơ bản 4. Module 04: Thiết Bị, Hệ Thống Linux, Tiêu Chuẩn Hierarchy Của Hệ Thống Lọc • Tạo phân vùng và hệ thống tệp • Duy trì tính toàn vẹn của hệ thống tệp • Kiểm soát việc gắn và ngắt kết nối hệ thống tập tin • Quản lý quyền và quyền sở hữu tệp • Tạo và thay đổi các liên kết cứng và tượng trưng • Tìm tệp hệ thống và đặt tệp vào đúng vị trí 5. Module 05: Shells And Shell Scripting • Tùy chỉnh và sử dụng môi trường shell • Tùy chỉnh hoặc viết các tập lệnh đơn giản 6. Module 06: Giao Diện Và Mô Tả Của Người Dùng • Cài đặt và cấu hình X11 • Máy tính để bàn đồ họa • Khả năng tiếp cận 7. Module 07: Administrative Tasks • Quản lý tài khoản người dùng và tài khoản nhóm và các tệp hệ thống liên quan • Tự động hóa các tác vụ quản trị hệ thống bằng cách lên lịch công việc • Bản địa hóa và quốc tế hóa 8. Module 08: Các Dịch Vụ Hệ Thống Cơ Bản • Duy trì thời gian hệ thống • Ghi nhật ký hệ thống • Thông tin cơ bản về Mail Transfer Agent (MTA)				

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	• Quản lý máy in và in ấn 9. Module 09: Các Cơ Sở Mạng • Các nguyên tắc cơ bản về giao thức internet • Cấu hình mạng ổn định • Khắc phục sự cố mạng cơ bản • Định cấu hình DNS phía máy khách 10.Module 10: Bảo Mật • Thực hiện các nhiệm vụ quản trị bảo mật • Thiết lập bảo mật máy chủ lưu trữ • Bảo mật dữ liệu bằng mã hóa				
	1.2 Khoá đào tạo Quản trị Oracle (Oracle Database 19c SQL Tuning Workshop) **a. Tên khoá học:** Khoá đào tạo Quản trị Oracle (Oracle Database 19c SQL Tuning Workshop) **b. Quy mô lớp học:** 01 lớp, dự kiến 15-20 người. **c. Thời lượng:** 05 ngày **d. Thời gian thực hiện:** Quý 3, 4/2025 **e. Hình thức đào tạo:** Trực tiếp **f. Địa điểm đào tạo:** Tại Thành phố Hồ Chí Minh **g. Nội dung đào tạo:** Module 1: Introduction to SQL Tuning • SQL Tuning Session • SQL Tuning Strategies • SQLTXPLAIN (SQLT) Diagnostic Tool Module 2: Using Application Tracing Tools • Overview Using the SQL Trace Facility • Steps Needed Before Tracing • Overview Available Tracing Tools	01	khoá		

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	• The trcsess Utility • Overview Formatting SQL Trace Files Module 3: Understanding Basic Tuning Techniques • Developing Efficient SQL statement • Scripts Used in This Lesson • Table Design • Index Usage • Transformed Index • Data Type Mismatch • NULL usage • Tune the ORDER BY Clause Module 4: Optimizer Fundamentals • SQL Statement Representation • SQL Statement Processing • Why Do You Need an Optimizer? • Components of the Optimizer • Query Transformer • Cost-Based Optimizer • Adaptive Query Optimization • Optimizer Features and Oracle Database Releases Module 5: Generating and Displaying Execution Plans • Execution Plan? • The EXPLAIN PLAN Command • Plan Table • AUTOTRACE • SQL_PLAN View • Automatic Workload Repository • SQL Monitoring				

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	Module 6: Optimizer: Table and Index Access Paths • Row Source Operations • Main Structures and Access Paths • Full Table Scan • Indexes • Common Observations Module 7: Optimizer Operations • Join Methods • Join Types • SQL operators • Other N-Array Operations • Result Cache operators • Optimizer Statistics • Types of Optimizer Statistics • Gather and Manage Optimizer Statistics: Overview Module 8: Using Bind Variables • Cursor Sharing and Different Literal Values • Cursor Sharing and Bind Variables Module 9: SQL Plan Management • Maintaining SQL Performance • SQL Plan Management Module 10: Intro Partitioning in Oracle • Partition Strategies • Range • Hash • List • Interval and Automatic partition Module 11: Useful tip & techniques				

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	• Some tip for SQL Tuning: hint plan, index choice, trick Module 12: Workshops and Practical Exercises • Hands-on workshops designed to apply learned concepts in real-world scenarios. • Summary of practice sessions to reinforce learning.				
	1. 3 Khoá đào tạo Quy trình phát hiện, xử lý và phòng chống mã độc Malware **a. Tên khoá học:** Khoá đào tạo Quy trình phát hiện, xử lý và phòng chống mã độc Malware **b. Quy mô lớp học:** 01 lớp, dự kiến 15-20 người. **c. Thời lượng:** 05 ngày **d. Thời gian thực hiện:** Quý 3, 4/2025 **e. Hình thức đào tạo:** Trực tiếp **f. Địa điểm đào tạo:** Tại Thành phố Hồ Chí Minh **g. Nội dung đào tạo:** 1. Tổng quan về mã độc (Malware Fundamentals) 1.1 Giới thiệu về mã độc: • Định nghĩa và lịch sử của mã độc. • Mục tiêu và động cơ của kẻ tấn công. 1.2 Các loại mã độc phổ biến: • Virus, Worm, Trojan. • Ransomware, Spyware, Adware. • Rootkit, Botnet, Fileless malware. • Phân biệt các loại mã độc và cách thức lây nhiễm. 1.3 Vòng đời của mã độc: • Tạo ra, lây nhiễm, kích hoạt, lan truyền, duy trì quyền truy cập. 1.4 Các phương thức lây nhiễm: • Email phishing, drive-by download, USB, lỗ hổng phần mềm. 2. Phát hiện mã độc (Malware Detection) 2.1 Các kỹ thuật phát hiện:	01	khoá		

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	• Phát hiện dựa trên chữ ký (Signature-based detection). • Phát hiện dựa trên hành vi (Behavioral-based detection). • Phát hiện dựa trên heuristics (Heuristic-based detection). • Phân tích tĩnh và phân tích động. 2.2 Công cụ phát hiện mã độc: • Phần mềm diệt virus (Antivirus software). • Hệ thống phát hiện xâm nhập (IDS/IPS). • Công cụ giám sát hệ thống (SIEM, EDR). • Sử dụng các dịch vụ phân tích trực tuyến (VirusTotal, Hybrid Analysis). 2.3 Kỹ thuật né tránh phát hiện của mã độc: • Che dấu (Obfuscation), đóng gói (Packing), mã hóa (Encryption). • Polymorphism, Metamorphism. 3. Phân tích mã độc (Malware Analysis) 3.1 Môi trường phân tích an toàn: • Sử dụng máy ảo (Virtual Machines), Sandbox. • Thiết lập phòng lab phân tích mã độc. 3.2 Phân tích tĩnh cơ bản: • Sử dụng công cụ xem thông tin file (PEStudio, ExifTool). • Phân tích chuỗi (Strings), hàm API (API Calls). • Kiểm tra Packed/Unpacked file. 3.3 Phân tích động cơ bản: • Sử dụng Process Monitor, Process Explorer. • Giám sát network traffic (Wireshark). • Giám sát thay đổi Registry, File System. 3.4 Phân tích mã độc nâng cao (Giới thiệu): • Disassembly (IDA Pro, Ghidra). • Debugging (x64dbg, WinDbg). • Kỹ thuật Reverse Engineering cơ bản.				

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	4. Xử lý và gỡ bỏ mã độc (Malware Incident Response and Removal) 4.1 Quy trình xử lý sự cố an ninh mạng: • Chuẩn bị (Preparation). • Phát hiện và phân tích (Identification and Analysis). • Ngăn chặn (Containment). • Gỡ bỏ (Eradication). • Khôi phục (Recovery). • Bài học kinh nghiệm (Post-incident Activity). 4.2 Kỹ thuật gỡ bỏ mã độc: • Gỡ bỏ thủ công. • Sử dụng công cụ chuyên dụng. • Khôi phục hệ thống từ bản sao lưu. 4.3 Điều tra pháp y kỹ thuật số (Digital Forensics) cơ bản: • Thu thập và bảo toàn bằng chứng. • Phân tích log, memory dump. 5. Phòng chống mã độc (Malware Prevention) 5.1 Các biện pháp kỹ thuật: • Cập nhật phần mềm và hệ điều hành thường xuyên. • Sử dụng tường lửa (Firewall), phần mềm diệt virus. • Hệ thống kiểm soát truy cập (Access Control). • Sao lưu dữ liệu định kỳ (Backup). • Triển khai Endpoint Detection and Response (EDR). • Sử dụng Zero Trust Architecture. 5.2 Biện pháp phi kỹ thuật và nâng cao nhận thức: • Đào tạo nhận thức về an ninh mạng cho người dùng. • Chính sách mật khẩu mạnh. • Kiểm tra email phishing giả lập. • Lập kế hoạch ứng phó sự cố.				

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	5.3 Xu hướng và thách thức mới: • AI và Machine Learning trong phòng chống mã độc. • Malware-as-a-Service (MaaS). • Tấn công chuỗi cung ứng (Supply Chain Attacks). 6. Bài tập thực hành và tình huống thực tế • Thực hành phân tích mã độc trên môi trường sandbox. • Xử lý các tình huống giả định về lây nhiễm mã độc. • Xây dựng checklist phòng chống mã độc cho tổ chức.				
	1.4. Khoá đào tạo Giám sát bảo mật hệ thống mạng và thu thập phương thức tấn công của tin tặc **a. Tên khoá học:** Khoá đào tạo Giám sát bảo mật hệ thống mạng và thu thập phương thức tấn công của tin tặc **b. Quy mô lớp học:** 01 lớp, dự kiến 15-20 người. **c. Thời lượng:** 05 ngày **d. Thời gian thực hiện:** Quý 3, 4/2025 **e. Hình thức đào tạo:** Trực tiếp **f. Địa điểm đào tạo:** Tại Thành phố Hồ Chí Minh **g. Nội dung đào tạo:** 1. Quản lý và vận hành bảo mật thông tin • Tìm hiểu các nguyên tắc cơ bản của hệ thống SOC • Trình bày về các thành phần của SOC: Con người, Quy trình và Công nghệ • Tìm hiểu cách triển khai hệ thống SOC 2. Trình bày các mối đe dọa mạng, IoC và phương pháp tấn công • Trình bày các thuật ngữ về các mối đe dọa, và tấn công mạng • Hiểu rõ các cuộc tấn công cấp độ mạng • Hiểu rõ các cuộc tấn công ở cấp độ máy chủ	01	khoá		

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	• Hiểu rõ các cuộc tấn công ở cấp độ ứng dụng • Hiểu các chỉ số thỏa hiệp (IoCs) • Thảo luận về phương pháp tấn công của tin tặc 3. Hiểu rõ các nguyên tắc cơ bản của Sự cố, Sự kiện và Ghi nhật ký • Giải thích các khái niệm về ghi nhật ký cục bộ • Giải thích các khái niệm về ghi nhật ký tập trung 4. Phát hiện sự cố với hệ thống giám sát quản lý sự kiện và thông tin bảo mật (SIEM) • Giới thiệu hệ thống quản lý sự kiện và thông tin bảo mật (SIEM) • Hiểu rõ các khái niệm cơ bản về bảo mật • Thảo luận về các giải pháp SIEM khác nhau • Tìm hiểu việc triển khai SIEM • Tìm hiểu các ví dụ về trường hợp sử dụng khác nhau để phát hiện sự cố ở cấp độ ứng dụng • Tìm hiểu các ví dụ về trường hợp sử dụng khác nhau để phát hiện sự cố nội bộ • Tìm hiểu các ví dụ về trường hợp sử dụng khác nhau để phát hiện sự cố cấp mạng • Tìm hiểu các ví dụ về trường hợp sử dụng khác nhau để phát hiện sự cố ở cấp độ máy chủ • Tìm hiểu các ví dụ về trường hợp sử dụng khác nhau để đáp ứng tính tuân thủ. 5. Phát hiện sự cố nâng cao với thông tin về mối đe dọa • Tìm hiểu các khái niệm cơ bản về thông tin mối đe dọa • Tìm hiểu các loại thông tin về mối đe dọa khác nhau • Hiểu cách phát triển chiến lược thông tin về mối đe dọa • Tìm hiểu các thông tin về mối đe dọa khác nhau thu được từ các nguồn thông tin tình báo • Tìm hiểu nền tảng thông tin mối đe dọa khác nhau Threat Intelligence Platform (TIP) • Tìm hiểu nhu cầu về SOC dựa trên thông tin về mối đe dọa				

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
	6. Hiểu rõ các khái niệm cơ bản về ứng phó sự cố • Tìm hiểu các giai đoạn khác nhau trong quá trình ứng phó sự cố • Tìm hiểu cách ứng phó với sự cố an ninh mạng • Tìm hiểu cách ứng phó với các sự cố bảo mật ứng dụng • Tìm hiểu cách ứng phó với sự cố bảo mật email • Tìm hiểu cách ứng phó với sự cố nội bộ • Tìm hiểu cách ứng phó với sự cố phần mềm độc hại 7. Xây dựng mô hình và triển khai cài đặt hệ thống giám sát • Cài đặt và cấu hình Suricata trên PfSense để phát hiện và phòng chống tấn công • Cài đặt và cấu hình Logtash để giám sát VPN (Log Access VPN) • Cài đặt và cấu hình Wazuh và Zabbix để giám sát hiệu năng máy chủ, CPU, RAM dung lượng ổ cứng theo thời gian thực • Cài đặt và cấu hình hệ thông SOAR: The Hive và COrcex (hệ thống phản hồi tự động) • Cài đặt và cấu hình các chức năng trong hệ thống giám sát: Malware Detection, Security Analytics, Intrusion Detection (IDS), Log Data Analysis, File Integrity Monitoring (FIM), Vulnerability Detection, Configuration Assessment, Ticket System • Tìm hiểu cách ứng phó với sự cố phần mềm độc hại 8. Diễn tập về ứng phó sự cố • Diễn tập kịch bản vận hành hệ thống giám sát và ứng cứu sự cố mã độc tấn công đánh cắp dữ liệu • Diễn tập kịch bản vận hành hệ thống giám sát và ứng cứu sự cố tấn công hệ thống Web.				
	Tổng cộng **Giá: …… (Bằng chữ:……..……)** Giá trên là giá trọn gói đã bao gồm thuế, phí, lệ phí (nếu có) và các chi phí liên quan	04	khoá		

Yêu cầu nhà cung cấp phải đáp ứng:

1. Tài liệu đào tạo: Mỗi học viên được cung cấp tài liệu 01 bản cứng (kèm bản mềm nếu có).

2. Giáo viên:

a. Đối với Khoá đào tạo Quản trị hệ thống Linux -LPIC-1 (Linux Professional Institute Certification Level 1) và Khoá đào tạo Quản trị Oracle (Oracle Database 19c SQL Tuning Workshop):

- Có 01-02 giáo viên có ít nhất 07 năm kinh nghiệm.
- Tốt nghiệp Đại học chuyên ngành CNTT hoặc điện tử viễn thống, hệ thống thông tin, máy tính, khoa học máy tính.
- Có kinh nghiệm đào tạo từ 02 lớp LPI trở lên
- Có các chứng chỉ quốc tế sau:

+ Chứng chỉ về VMware: VCAP – DCV Design 2021;

+ Chứng chỉ về Linux Professional Institute: LPIC-1, LPIC-2

+ Chứng chỉ về Kubernetes: Certified Kubernetes Administrato

b. Đối với Khoá đào tạo Quy trình phát hiện, xử lý và phòng chống mã độc Malware và Khoá đào tạo Giám sát bảo mật hệ thống mạng và thu thập phương thức tấn công của tin tặc

- Có 01-02 giáo viên có ít nhất 10 năm kinh nghiệm
- Có bằng Thạc sĩ Khoa học máy tính/Điện tử/ Công nghệ thông tin.
- Có kinh nghiệm đào tạo từ 04 lớp Bảo mật an toàn thông tin trở lên
- Có các chứng chỉ quốc tế như sau:

+ CEI – Certified EC-Council Instructor

+ CompTIA Network +

+ CEH - Certified Ethical Hacker

+ CHFI - Computer Hacking Forensic Investigator

+ CySA+ - Cybersecurity Analyst+

3. Hồ sơ năng lực của nhà cung cấp

+ Có đăng ký doanh nghiệp/đăng ký hoạt động hợp pháp, là đơn vị ủy quyền EC-Council, CompTIA, CSA (Cloud Security Alliance).

+ Có giấy tờ chứng minh phòng LAB đạt tiêu chuẩn. Hệ thống Lab được xây dựng trên môi trường điện toán đám mây, các server phục vụ hệ thống Lab được đặt tại Data Center ở Việt Nam và chỉ cần kết nối Internet là có thể truy cập được. Học viên có thể truy cập hệ thống Lab ở nhà nếu muốn, chỉ cần có Internet. Học viên có quyền truy cập 2 tuần để luyện tập sau khi khóa học kết thúc.

+ Có giấy tờ chứng minh là đơn vị đào tạo chuyên nghiệp, hợp pháp về lĩnh vực CNTT chuyên sâu (Giấy đăng ký kinh doanh, quyết định thành lập, quyết định bổ nhiệm lãnh đạo…)