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

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

Số: 1346 /TTĐTHL-ĐT
V/v mời báo giá gói đào tạo chuyên gia an toàn thông tin

Hà Nội, ngày 21 tháng 7 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 chuyên gia an toàn thông tin (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 14h00 ngày 23/7/2025.

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 Nguyễn Thị Hồng Minh; Số điện thoại: 0916712008

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:0100108624-014-C.T.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: 1346 /TTĐTHL-ĐT ngày 21 tháng 7 năm 2025)

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
1	Chi phí đào tạo: **1. Thông tin chung các khoá học về đào tạo chuyên gia an toàn thông tin:** **1.1 Khoá Chuyên gia bảo mật hệ thống thông tin - Certified Information Systems Security Professional (CISSP Security)** a. Tên khoá học: Khoá Chuyên gia bảo mật hệ thống thông tin - Certified Information Systems Security Professional (CISSP Security): b. Thời lượng đào tạo: 5 ngày c. Thời gian thực hiện: dự kiến Quý III/2025 d. Quy mô lớp học: 01 lớp, dự kiến 15-20 người. e. Hình thức đào tạo: Trực tuyến f. Nội dung đào tạo: Bài 1: Quản lý Bảo mật - Trách nhiệm về quản lý bảo mật - Phân biệt giữ kiểm soát vật lý, kỹ thuật và quản trị - Ba nguyên lý bảo mật chính - Quản lý và phân tích rủi ro - Chính sách bảo mật - Phân loại thông tin - Đào tạo nâng cao nhận thức về bảo mật Bài 2: Kiểm soát truy cập - Các phương pháp và kỹ thuật định danh - Các phương pháp, mô hình xác thực - Phân biệt các mô hình kiểm soát truy cập - Kiểm toán và giám sát - Hệ thống phát hiện xâm nhập - Các mối nguy hiểm đối với kiểm soát truy cập	1	gói		

	Bài 3: Các mô hình và kiến trúc bảo mật - Kiến trúc phần cứng của máy tính - Các kiến trúc của hệ điều hành - Các cơ chế bảo mật cơ bản - Các cơ chế bảo mật trong hệ điều hành - Các mô hình bảo mật - Các khu vực kiểm thử và đánh giá - Quy trình chứng nhận và bổ nhiệm - Các phương pháp tấn công Bài 4: Bảo mật vật lý - Phân biệt về kiểm soát vật lý, kỹ thuật và quản trị - Vị trí các thiết bị và quản lý - Các rùi ro bảo mật vật lý, mối nguy hiểm và phương pháp phòng chống - Các vấn đề liên quan đến nguồn điện và phương pháp phòng chống - Phát hiện và Ngăn chặn cháy nổ - Hệ thống phát hiện xâm nhập Bài 5: Bảo mật mạng và viễn thông - Mô hình OSI - TCP/IP và các giao thức khác - Các công nghệ LAN, WAN, MAN, Intranet, Extranet - Phân loại dây mạng và các phương pháp truyền dữ liệu - Các dịch vụ và thiết bị mạng - Quản lý bảo mật trong truyền thông - Các thiết bị viễn thông - Các kỹ thuật và phương pháp truy cập từ xa - Các kỹ thuật sử dụng trong mạng không dây Bài 6: Mật mã - Lịch sử của Mật mã - Các thành phần của Mật mã và mối liên hệ - Sự tham gia của chính phủ đề phát triển mật mã - Các thuật toán mã hóa đối xứng và bất đối xứng - Các khái niệm và cơ chế sử dụng trong PKI				

	- Thuật toán Băm và ứng dụng - Các phương pháp tấn công vào các hệ thống mật mã Bài 7: Lập kế hoạch đảm bảo tính liên tục của doanh nghiệp và khôi phục sau thảm họa - Các bước khởi tạo dự án - Các yêu cầu lập kế hoạch đảm bảo tính liên tục và khôi phục sau thảm họa - Các phân tích sự ảnh hưởng đến doanh nghiệp - Lựa chọn, phát triển và triển khai các kế hoạch đã vạch - Sao lưu - Thử nghiệm Bài 8: Các điều luật, sự điều tra và tính đạo đức - Tính đạo đứuc gắn với các chuyên gia bảo mật thông tin - Tội phạm máy tính và các điều luật về máy tính - Động cơ và hồ sơ kẻ tấn công - Tiến trình điều tra tội phạm máy tính và thu thập dấu vết - Các bước xử lý sự cố - Các kiểu dấu vết - Các điều luật ảnh hưởng đến tội phạm mát tính Bài 9: Bảo mật trong quá trình phát triển ứng dụng và hệ thống - Các phương pháp kiểm soát và triển khai phần mềm - Khái niệm về cơ sở dữ liệu và các vấn đề bảo mjaat - Kho dữ liệu và khai thác dữ liệu - Tiến trình phát triển và việc khai thác dữ liệu - Tiến trình phát triển chu kỳ sống của phần mềm - Các khái niệm về kiểm soát sự thay đổi - Các thành phần của chương trình đối tượng - Các hệ thống chuyên dụng và trí tuệ nhân tạo Bài 10: Bảo mật trong hệ vận hành - Các trách nhiệm về quản lý các công việc quản trị - Thử nghiệm sản phẩm và đảm bảo vận hành - Quản lý cấu hình - Các bước trong quá trình khôi phục - Các hệ thống có khả năng chống lỗi				

	- Bảo mật cho thư điện tử - Các mối nguy hiểm liên quan đến bảo mật trong vận hành **1.2 Khoá đào tạo CompTIA Security+ theo chương trình** a. Tên khoá học: Khoá đào tạo CompTIA Security+ theo chương trình b. Thời lượng đào tạo: 4 ngày c. Thời gian thực hiện: dự kiến Quý III/2025 d. Quy mô lớp học: 01 lớp, dự kiến 20 người. e. Hình thức đào tạo: Trực tiếp tại Hồ Chí Minh f. Nội dung đào tạo: **Chương 1: Tổng quan về ATTT-Rủi ro, Các hình thức tấn công** – Các sự kiện an ninh mạng gần đây – Các khái niệm cơ bản về an ninh mạng – Các hình thức tấn công mạng phổ biến – Chính sách bảo mật – Demo một số hình thức tấn công: – Tấn công password, tấn công dos lan, dos qua lỗ hổng IIS, tấn công qua lỗ hổng ứng dụng Apache, tấn công HĐH **Chương 2: Giám sát, rà soát lỗ hổng và một số kỹ thuật đảm bảo ATTT** – Tổng quan về Scan – Scan mạng – Scan Port – Scan lỗ hổng bảo mật – Demo: Dùng nmap scan, Nesus, Security Baseline, snort trên kali **Chương 3: Tìm hiểu về các thiết bị và hạ tầng mạng** – Mô hình TCP/IP – Ipv4 và Ipv6 – Các giao thức phổ biến – Các thiết bị mạng – Một số khái niệm: DMZ, Subnet, VLAN, NAT, Remote access, NAC – Các kiểu FireWall				

	– Load Balancers – VPN – IDS và IPSd – UMT – Demo: Cấu hình NAP cho DHCP, cấu hình RDP, cấu hình VPN client to site, cấu hình squid Proxy firewall, cấu hình snort **Chương 4: Các khái niệm Access Control, Authentication, and Authorization** –Access control list, truy cập nguồn tài nguyên và các permision –Xác thực login các HĐH, Xác thực Keberos, LDAP, PAP CHAP, Trắc sinh học, CA, presharekey, Single Site On **Demo:** –Cấu hình NAP cho VPN –Nghe lén các giao thức xác thực clear text, VPN L2tP/ipsec xác thực CA, VPN xác thực RADIUS, Trust Domain, Cấu hình account Policy, password Policy **Chương 5: Protecting Wireless Networks** –Các chuẩn bảo mật wireless –Các mô hình thiết kế mạng wireless –Các lỗ hổng và các cách tấn công mạng wireless –Demo một vài hình thức tấn công wireless: **Chương 6: Cloud** – Cloud computing: Private Cloud, Public Cloud, Community Cloud, Hybrid Cloud – Ảo hóa – Bảo mật cho Cloud **Chương 7: Host, Data, and Application Security** –Bảo mật xác thực máy, gia cố lỗ hổng các HĐH, các lỗ hổng mới, firewall host base –Mã hóa bitlocker, EFS, NTFS security –Gia cố các lỗ hổng trên App zero day –Gia cố DHCP, DNS, FTP..AD –Các cơ chế dự phòng: Backup (các kiểu), RAID, Cluster FailOVer, NLB –**Demo**: tấn công chiếm quyền máy thông qua 1 số lỗ hổng, cấu hình firewall ngăn chặn wanna cryp				

	(Ms17-010), cấu hình mã hóa EFS và bitlocker, tấn công qua lỗ hổng trên app (CVE 2015 8562), **Chương 8: Mã hóa:** – Mã hóa Hash – Mã hóa đối xứng – Mã hóa bất đối xứng – CA **Chương 9: Malware, Vulnerabilities, và ThreatsMalware** – Virus – Trojan Horse – Malicious Mobile Code – Tracking Cookie – Attacker Tool – Backdoor – Keylogger – Rootkits **Chương 10: Social Engineering** –SE phi kỹ thuật –SE có kỹ thuật: fake login, trojan –Demo: beef, chiếm quyền thông qua shell update flash, fake login **Chương 11: Security Administration** – Third-Party Integration – Classifying Information – Mobile Device: – Demo attack Mobile và cách phòng chống **Chương 12: Disaster Recovery** – Tổng quan Backup và Restore – Lập kế hoạch và thực thi Backup & Restore – Demo Backup Windows Server 2012 **1.3 Khóa đào tạo tấn công và phòng thủ bảo mật Windows** a. Tên khoá học: Khóa đào tạo tấn công và phòng thủ bảo mật Windows				

	b. Thời lượng đào tạo: 4 ngày c. Thời gian thực hiện: dự kiến Quý III/2025 d. Quy mô lớp học: 01 lớp, dự kiến 20 người. e. Hình thức đào tạo: Trực tiếp tại Hồ Chí Minh f. Nội dung đào tạo: **Phần 1: Kiến trúc bảo mật Windows, kỹ thuật khai thác ban đầu.** **Tổng quan về kiến trúc bảo mật Windows:** o Kernel, LSASS, Winlogon, Registry. o User Account Control (UAC), Credential Manager. Active Directory & Kerberos Essentials. Attack Surface: o Misconfigurations & Patch Gaps. **Kỹ thuật do thám và rà quét lỗ hổng bảo mật trên Windows** o Sử dụng NMAP o Sử dụng Metasploit o Sử dụng Nessus o Sử dụng AI Shell GPT **Quản lý về lỗ hổng bảo mật trên Windows: Nist, Fist, Mitre ATT** **Quản lý tiến trình Update** **Kỹ thuật tấn công ban đầu**: o Phishing & Malicious Attachments. o Exploiting SMB & RDP. o Exploiting Windows Services (PrintNightmare update). o Sử dụng AI để khai thác và tấn công tự động Windows. **Công cụ**: o Metasploit, Cobalt Strike (Beacon Simulation), PowerShell Empire, Shell GPT AI **Lab thực hành:** Lab 1: Khai thác RDP Brute-force + Detect với Event ID. Lab 2: Tạo Payload với Metasploit và thực hiện Initial Access. Lab 3: Bypass UAC bằng PowerShell. Lab 4: Khai thác Windows 11, Server 2025 bằng AI **Phần 2: Credential Access & Lateral Movement**				

	(Ăn cắp thông tin đăng nhập và di chuyển ngang trong hệ thống) **Credential Dumping**: o Mimikatz và kỹ thuật trích xuất LSASS. o SAM & NTDS.dit Extraction. o Credential Guard & LSA Protection. **Pass-the-Hash / Pass-the-Ticket (PtH/PtT)**: o Kerberos TGT Forging (Golden Ticket). **Lateral Movement**: o PsExec, WMI, Remote PowerShell. o Exploiting SMB Relay. **Persistence**: o Registry Autoruns, Scheduled Tasks. o WMI Event Subscription. **Lab thực hành:** Lab 5: Dùng Mimikatz lấy NTLM Hash + Pass-the-Hash. Lab 6: Kerberos Attack – Golden Ticket. Lab 7: Di chuyển ngang với PsExec và phát hiện bằng Sysmon. Lab 8: Dùng AI lấy NTLM Hash của Windows Lab 9: Password Responder Attack **Phần 3: Detection & Defense** *(Phát hiện tấn công & triển khai phòng thủ)* Windows Logging Essentials: o Event Logs, Sysmon, PowerShell Logging. Giải pháp EDR trên WIndows o CrowdStrike, Microsoft Defender for Endpoint. Security Baselines & Hardening: o LAPS (Local Administrator Password Solution). o Credential Guard, Attack Surface Reduction (ASR). Giải pháp Zero Trust trên Windows: o Just Enough Administration (JEA). o Conditional Access. Phòng thủ với PowerShell Defensive Mode:				

	○ Constrained Language Mode. ○ AMSI (Antimalware Scan Interface). **Lab thực hành:** Lab 10: Cài Sysmon + Viết Rule phát hiện Credential Dumping. Lab 11: Bật LAPS và triển khai ASR Rules. Lab 12: Tạo Script phát hiện hoạt động của Mimikatz trong Event Logs. **Phần 4: Incident Response & Disaster Recovery** *(Xử lý sự cố & và phục hồi dữ liệu)* Quy trình xử lý và ứng cứu sụ cố trên Windows (NIST): ○ Identification → Containment → Eradication → Recovery → Lessons Learned. Memory Forensics với **Volatility**. **Phòng chống Ransomeware và mã độc trên Windows** **Các giải pháp Backup & Recovery trên Windows** **Tabletop Exercise & Attack Simulation**: ○ Red Team mô phỏng chuỗi tấn công thực tế (Initial Access → Lateral Movement → Exfiltration). ○ Blue Team thực hiện điều tra & phản ứng. **Lab thực hành:** Lab 13: Phân tích dump bộ nhớ phát hiện credential dumping. Lab 14: Cấu hình Windows Defender, Registry, GPo để phòng chống và phát hiện mã độc Lab 15: Cấu hình sao lưu và phục hồi dữ liệu **2. Tài liệu khoá học:** Tài liệu bằng bản cứng **3. Yêu cầu giáo viên:** - Có bằng đại học trở lên một trong các chuyên ngành: CNTT, hệ thống thông tin, khoa học máy tính, toán – tin ứng dụng. - Có kinh nghiệm tối thiểu 03 năm tham gia giảng dạy về CNTT hoặc tối thiểu 01 hợp đồng đào tạo với vai trò là giáo viên về nội dung của khoá học mà giáo viên sẽ tham gia giảng dạy. **4. Hồ sơ năng lực của nhà cung cấp**				
	Giá: ..... (Bằng chữ:.....) Giá trên là giá trọn gói đã bao gồm thuế, phí, lệ phí (nếu có) và các chi phí liên quan				