ITLABTHUDUC

LAB THỰC - VIỆC THẬT

GIỚI THIỆU KHÓA
SOC TIER 1

Giới thiệu khóa SOC Tier 1

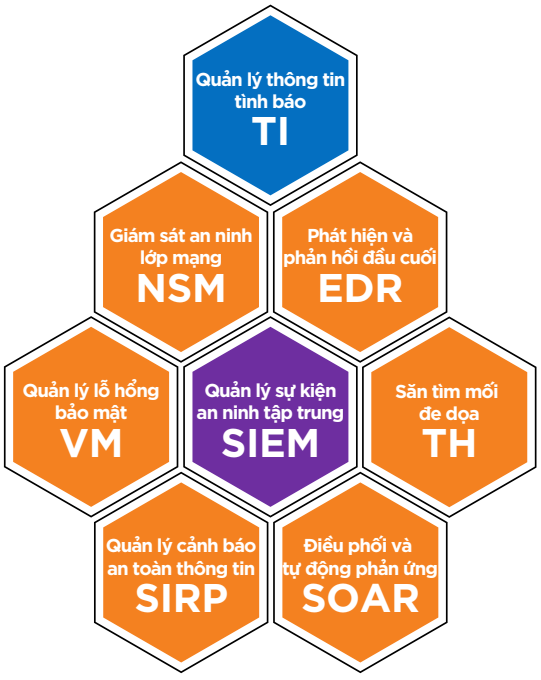
Khóa SOC Tier 1 – Căn bản cho Chuyên viên SOC (Security Operations Center)

Đây là khóa học nền tảng dành cho sinh viên và người mới định hướng nghề nghiệp trong lĩnh vực Security Operations Center (SOC). Khóa học kéo dài 40 giờ (10 buổi trong 8 tuần) với hơn 10 nội dung thực hành chiếm > 50% thời lượng đào tạo.

Nội dung khóa học không chỉ bao gồm các kiến thức thiết yếu như nhận diện và phân loại mối đe dọa, tình báo mạng, SIEM, EDR/XDR, SOAR, mà còn chú trọng vào thực hành qua các lab thực chiến: từ cấu hình Firewall, triển khai SIEM Elastic Security, đến mô phỏng tấn công và phòng thủ bằng DVWA, Metasploit hay NSM monitoring,..... trên nền tảng thiết bị thực tế kết hợp với hệ thống đang vận hành. Bên cạnh đó, học viên cũng được tiếp cận tư duy quản trị rủi ro, tuân thủ (GRC) – một kỹ năng ngày càng quan trọng với chuyên viên SOC.

Mục tiêu hướng đến của khóa học:

- ✓Cung cấp kiến thức căn bản về SOC và vai trò SOC Tier 1.
- ✓Hiểu và thực hành các kỹ thuật SOC: SIEM, EDR, XDR, Threat Intel, SOAR.
- ✓Nắm vững các loại mối đe dọa, phương pháp phân loại, kỹ thuật phát hiện và ứng phó.
- ✓Thực hành lab với hệ thống thiết bị như: Firewall, SIEM Elastic Security, DVWA Attack, Metasploit, NSM monitoring... trên các nền tảng vật lý và ảo hóa đang được vận hành.
- ✓Trang bị kỹ năng thực tế, sẵn sàng đảm nhận công việc SOC Tier 1 Analyst hoặc Kỹ sư bảo mật.



Tại sao nên học SOC – Tier 1?

Khóa học này sẽ đưa học viên từ zero đến SOC Analyst tuyến đầu, trang bị kỹ năng thực chiến và kiến thức nền tảng để bắt đầu sự nghiệp trong lĩnh vực An ninh mạng.

01 – Career Readiness (Sẵn sàng nghề nghiệp)

Khám phá xu hướng việc làm trong ngành SOC, hiểu công việc hằng ngày của SOC Tier 1 Analyst, và chuẩn bị hành trang để bước vào lĩnh vực đang có nhu cầu nhân lực cao.

02 – Practical Upskill (Nâng cấp kỹ năng thực chiến)

Học viên được thực hành trên các hệ thống SOC thực tế, theo dõi cảnh báo, phân tích Log, nhận diện mối đe dọa, xử lý sự cố ban đầu. Sử dụng công nghệ SIEM, EDR/XDR, SOAR,.... Từ đó phát triển kỹ năng phân tích và phản ứng An ninh Mạng.

03 – Job Opportunities (Cơ hội nghề nghiệp rộng mở)

Ngành an ninh mạng là lĩnh vực đang khát nhân lực, đặc biệt ở vị trí SOC Tier 1 Analyst. Sau khóa học, bạn có thể ứng tuyển vào các vai trò như: SOC Analyst Tier 1, Network Security Engineer hoặc tiếp tục phát triển lên SOC Tier 2, Tier 3, Incident Responder.

Vì sao chọn học SOC – Tier 1 tại ITLabThuDuc?

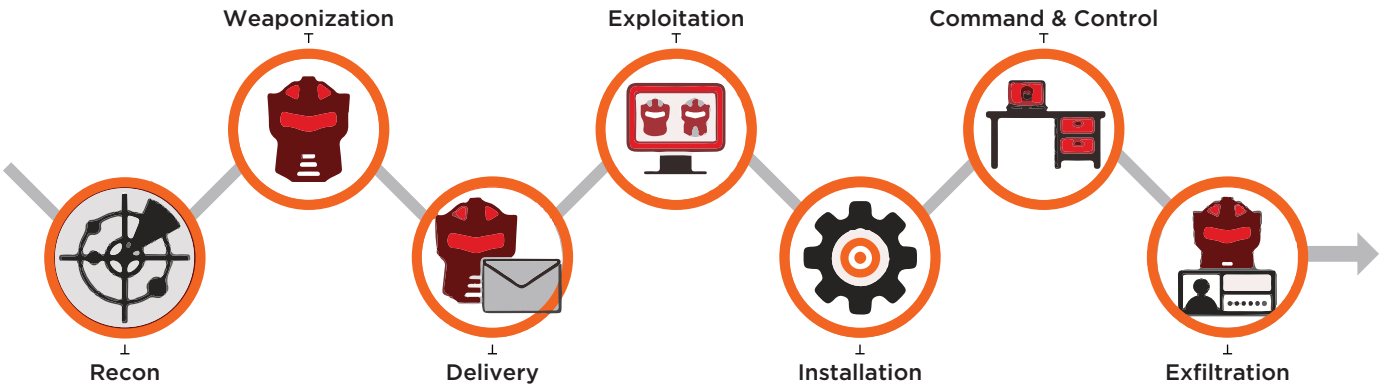
ITLabThuduc là đơn vị đào tạo chuyên sâu về Network – System – Cybersecurity, với phương pháp lab thực chiến **"Lab thực – Việc thật"** giúp học viên học đi đôi với làm. Những ưu điểm nổi trội khi học viên chọn học khóa SOC Tier1 tại tại ITLabThuduc gồm:

1. Có thời lượng thực hành > 50% với thiết bị thật, tình huống thực tế
2. Giảng viên là các chuyên gia thực thụ, đang làm việc tại các doanh nghiệp và đã có chứng chỉ quốc tế
3. Chất lượng luôn được đảm bảo với số lượng không qua 5 học viên cho mỗi lớp
4. Môi trường học thân thiện, chú trọng thực tế và thực hành
5. Được hỗ trợ giới thiệu các cơ hội thực tập, việc làm sau mỗi khóa học

Khóa học SOC Tier1 dành cho đối tượng nào?

- Sinh viên ngành An toàn thông tin, CNTT, Điện tử – Viễn thông tại các trường Đại học, Cao đẳng.
- Người mới bắt đầu sự nghiệp trong An ninh mạng
- Các bạn chuyên viên đã làm trong ngành IT (System, Network, Helpdesk) nhưng muốn chuyển hướng sang SOC/ Security.
- Nhân sự yêu thích Cybersecurity và muốn xây dựng lộ trình nghề nghiệp từ vị trí SOC Analyst.

Yêu cầu chuyên môn cần có trước khi tham gia khóa SOC Tier1



1 Cơ bản về mạng

Một chuyên viên Phân tích SOC cần có sự hiểu biết sâu sắc về giao thức, kiến trúc và thiết bị mạng. Điều này bao gồm kiến thức về TCP/IP, DNS, DHCP và các giao thức định tuyến.

2 Kiến thức về hệ điều hành

Cần phải quen thuộc với nhiều hệ điều hành khác nhau, bao gồm Windows, Linux và Unix, để phân tích nhật ký hệ thống và hiểu được tác động của các mối đe dọa bảo mật.

3 Công nghệ bảo mật

Kiến thức về công nghệ bảo mật, chẳng hạn như tường lửa, hệ thống phát hiện xâm nhập (IDS) và hệ thống quản lý thông tin và sự kiện bảo mật (SIEM) , là rất quan trọng đối với một Nhà phân tích SOC.

4 Kỹ năng phân tích và giải quyết vấn đề

Chuyên viên phân tích SOC cần phân tích khối lượng lớn dữ liệu, xác định các mô hình và khắc phục sự cố liên quan đến bảo mật. Kỹ năng phân tích và giải quyết vấn đề vững chắc là điều cần thiết cho vai trò này.

5 Kỹ năng giao tiếp

Kỹ năng giao tiếp hiệu quả là cần thiết để Nhà phân tích SOC có thể phối hợp với nhiều bên liên quan, bao gồm kỹ sư an ninh, người ứng phó sự cố và nhóm quản lý.

6 Kiến thức về Khung và Quy định An ninh

Sự quen thuộc với các khuôn khổ bảo mật, chẳng hạn như Khuôn khổ an ninh mạng NIST và các quy định, chẳng hạn như HIPAA và PCI-DSS, là điều quan trọng đối với một Nhà phân tích SOC.

Chi tiết nội dung chương trình học:

Thời gian	Chủ đề	Nội dung đào tạo	Lab
		Phần 1: SOC Overview	
02 buổi	. SOC definition . SOC as service	• Giới thiệu phòng SOC • Những vai trò, thực tiễn, lý do, lợi ích xây dựng SOC • Con người, quy trình, công nghệ • Mô hình SOC as a service/MSSP • Những vai trò, thực tiễn, lý do, lợi ích và so sánh điểm khác biệt của SOC as a service/MSSP • SOC-tier1-2-3 • SOC vs NOC • Defense in depth - Phòng thủ đa lớp, theo chiều sâu • NIST csf v2 - Khung tiêu chuẩn giám sát & xử lý sự cố an toàn thông tin Mitre att&ck framework • Bách khoa toàn thư ghi chép kỹ thuật tấn công của hacker	- Thiết kế và cấu hình Mạng - Hệ thống CNTT doanh nghiệp - Tìm hiểu về windows audit policy. Tìm hiểu những event thường gặp của windows 4625, 4624, 4776, 4688, ..., sysmon, powershell - Những loại log cơ bản của linux (Ubuntu, Centos), đường dẫn lưu trữ các loại log
		Phần 2: SOC technique	
04 buổi	. Event, incident . SIEM . VA/VM . EDR and XDR . Threat Intel . Soar, automate -response . Ticket System (ITOM, ITSM, CRM ...) . External Attack Surface Management (EASM)	• Giới thiệu vòng đời của các sự kiện ATTT, các loại sự kiện ATTT • Thế nào là sự cố ATTT, các loại sự cố ATTT • Giải pháp SIEM: giới thiệu, tính năng, công nghệ lõi, một số hãng, platform và xu hướng NG-SIEM/Cloud-SIEM • Giải pháp VA/VM: giới thiệu, tính năng, công nghệ lõi, một số hãng, platform • Giải pháp EDR: giới thiệu, tính năng, công nghệ lõi, một số hãng, platform và mở rộng lên XDR • Giải pháp Threat Intel: giới thiệu, tính năngi, một số hãng, platform • Giải pháp SOAR: giới thiệu, tính năngi, một số hãng, platform và xu hướng chuyển dịch sang automate-response • Giải pháp EASM: giới thiệu, tính năng, công nghệ lõi, một số hãng, platform	- Lab SIEM Elastic-Securirty và viết rule SIEM detect tấn công cơ bản - DVMA Attack lab - Khai thác lỗ hổng (VA) Lab
		Phần 3: Threats	
04 buổi	. Threats classification . Kill chain/MITRE ATT&CK/TTP . IOC . Some popular attacks definition: malware, ransomware, web, unauthorized	• Giới thiệu, phân loại các mối đe dọa: rủi ro, đối tượng, ảnh hưởng, nguyên nhân... • Giới thiệu kill chain: Lock heel, MITRE ATT&CK, ứng dụng thực tiễn, hiểu chuỗi tấn công và mapping hành vi • Trình bày một số dạng tấn công kinh điển: malware, ransomware, web attack, unauthorized access - đối tượng, ảnh hưởng, nguyên nhân, rủi ro, hành vi, vết	- Test tấn công 2 loại theo danh sách trong DVWA và làm Dash-board, viết rule detect tấn công, giám sát các test case - Exploit lỗ hổng và compromise hệ thống. Viết rule detect LFI, RFI - Lab tấn công Network Exploit bằng Metasploit và quan sát log, viết rule detect trên SIEM, giám sát bảo mật trên NSM

Hình thức học:

Thời lượng: 40 giờ (10 buổi trong 8 tuần)
Hình thức: Part-time | Học Online thông qua nền tảng MS Teams | Lịch học Thứ 7 hoặc Chủ Nhật hàng tuần.
Giảng dạy: Trực tiếp giảng dạy bởi kỹ sư SOC & kỹ sư bảo mật nhiều kinh nghiệm, kết hợp lý thuyết & lab thực chiến.

Học phí:

Hình thức đăng ký	01 học viên	Nhóm 2 học viên	Nhóm 3-5 học viên
Mức học phí	4.300.000 vnđ/ 01 học viên	4.085.000 vnđ/ 01 học viên	3.870.000 vnđ/ 01 học viên

Cảm nhận của học viên tiêu biểu sau khóa học

"Qua khóa SOC Tier 1 em hiểu rõ con đường nghề nghiệp của mình hơn: không chỉ nắm được kiến thức về mạng và hệ thống ở mức sâu, mà còn biết cách ứng dụng để tiến xa hơn trong lĩnh vực bảo mật - chứ không chỉ dừng ở bề nổi của các công cụ. Khóa học SOC Tier1 còn trang bị cho em kỹ năng tấn công có kiểm soát để kiểm tra và khẳng định hiệu quả các lớp phòng thủ; đó chính là phần 'thực chiến' giúp em thấy được điểm mạnh, điểm yếu của hệ thống thay vì chỉ học phòng thủ một chiều."

Nguyễn Trung Nguyên D22 (HVBCVT)

"Điều em ấn tượng nhất ở khóa SOC Tier 1 là được trực tiếp trải nghiệm trên hệ thống và thiết bị thật như firewall, SIEM và các công cụ giám sát. Thay vì chỉ nghe lý thuyết khô khan, em được thực sự nhập vai một SOC Analyst, quan sát cảnh báo, phân tích log và xử lý tình huống ngay tại lab. Nhờ vậy, dù khả năng học lý thuyết của em chưa tốt lắm, em vẫn tiếp thu rất nhanh và hiểu sâu hơn qua đó giúp em tự tin để theo đuổi con đường An ninh mạng chuyên nghiệp"

Đinh Tuấn Dương D22 (HVBCVT)

LIÊN HỆ TƯ VẤN & ĐĂNG KÝ HỌC:
Hotline: 0833 052 299
Email: support@itlabthuduc.com
https://www.facebook.com/itlabthuduc
Website: ITLabThuduc.COM

ITLABTHUDUC
LAB THỰC - VIỆC THẬT