CORSO BLUE TEAM ADVANCED: THREAT HUNTING, FORENSICS E MALWARE ANALYSIS

Durata: 2 giorni

PROGRAMMA

MODULO 1: FONDAMENTI DELLE SECURITY OPERATIONS (SECOPS)

Security Operations: fondamenti e modello CIA

- Introduzione alle Security Operations
- Principi fondamentali della sicurezza informatica e triade CIA

Security Operations Center (SOC): panoramica e modelli di implementazione

- Introduzione ai Security Operations Center (SOC)
- Proteggere il business attraverso un SOC efficace
- Modelli di SOC: dedicato e virtuale
- Quando implementare un SOC

Componenti tecnologiche di un SOC

- Network Firewall: protezione delle comunicazioni e dei dati
- Network Intrusion Detection e Prevention System (NIDS/NIPS)
- Host Intrusion Detection e Prevention System (HIDS/HIPS)
- Web Application Firewall (WAF): protezione delle applicazioni web
- Endpoint Detection and Response (EDR/XDR)
- Web Proxy Server
- Processo di Vulnerability Management
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Malware Analysis: analisi statica, dinamica e sandboxing
- Honeypot e sistemi di deception
- Cloud Computing e Cloud Access Security Broker (CASB)
- Threat Intelligence per la difesa delle infrastrutture
- Machine Learning e Deep Learning applicati alla cybersecurity
- Sistemi di ticketing per la gestione degli incidenti
- Asset Inventory e gestione degli asset aziendali

Persone e organizzazione nel SOC

- Organigramma e ruoli all'interno di un SOC
- Pianificazione efficace della formazione cybersecurity
- Sfide operative e criticità dei team SOC
- Strategie per prevenire il burnout degli analisti

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO BLUE TEAM ADVANCED: THREAT HUNTING, FORENSICS E MALWARE ANALYSIS

Durata: 2 giorni

Processi e governance

- Policy di sicurezza e protezione del business
- Procedure operative di un SOC
- Standard di sicurezza e conformità
- Linee guida e benchmark di sicurezza
- Valutazioni di sicurezza Windows con CIS-CAT Lite

MODULO 2: DIFESA DEL PERIMETRO - EMAIL SECURITY

Email Spoofing

- Prevenzione degli attacchi di spoofing e ruolo del DMARC
- SPF: Sender Policy Framework
- DKIM: autenticazione tramite firme digitali
- Implementazione e utilizzo del DMARC

Allegati malevoli

- Rischi associati agli allegati malevoli
- Buone pratiche per la gestione sicura degli allegati

URL malevoli

- Le minacce basate su URL malevoli
- Tecniche di protezione degli utenti
- Laboratorio: rilevamento di domini lookalike

Controlli avanzati di protezione

- Formazione degli utenti come misura di sicurezza
- Simulazioni di phishing e misurazione della consapevolezza
- Laboratorio: deploy di GoPhish
- Rilevamento precoce del phishing tramite token esca
- Laboratorio: deploy di Canary Tokens
- Multi-Factor Authentication (MFA)
- Conditional Access basato sulla posizione geografica
- Email reconnaissance e raccolta informazioni da parte degli attaccanti
- Hardening dei mail server secondo benchmark DISA e CIS
- Laboratorio: valutazione degli header email esposti

Risposta agli attacchi email

- Validazione, mitigazione e remediation degli attacchi email

MODULO 3: RACCOLTA DELLE EVIDENZE FORENSI

- Acquisizione della memoria su sistemi live e offline
- Acquisizione dei dischi: cifratura e write blocking
- Triage image e raccolta rapida delle evidenze
- Acquisizione di immagini disco su sistemi Windows e Linux
- Montaggio e analisi delle immagini forensi

CONTATTI info@nexsys.it www.nexsys.it

CORSO BLUE TEAM ADVANCED: THREAT HUNTING, FORENSICS E MALWARE ANALYSIS

Durata: 2 giorni

MODULO 4: DISK FORENSICS

- Struttura e analisi dei Windows Event Log
- Struttura e analisi del Windows Registry
- Profilazione di sistemi Windows
- Raccolta delle connessioni di rete e dei dispositivi collegati
- Analisi delle attività degli utenti
- NTFS Forensics e attività sui file
- Correlazione tra utenti e file/cartelle
- Rilevamento di dispositivi USB collegati
- Analisi delle applicazioni installate
- Analisi delle attività di esecuzione

MODULO 5: MEMORY FORENSICS

- Raccolta delle informazioni del sistema operativo
- Analisi dei processi in esecuzione
- Analisi degli artefatti di rete
- Identificazione delle tecniche di persistenza
- Raccolta e analisi degli artefatti NTFS

MODULO 6: NETWORK FORENSICS

- Statistiche del traffico di rete
- Analisi delle conversazioni e degli stream
- Estrazione di file dal traffico di rete

MODULO 7: THREAT HUNTING ED EMULATION

Tecniche avanzate di Threat Hunting

- Threat Hunting proattivo guidato dall'analista
- Importanza dell'approccio proattivo
- Requisiti per un programma efficace di Threat Hunting
- Fasi operative del processo di Threat Hunting

Microsoft Defender XDR e Sentinel per SOC Operations

- Microsoft Defender portal come console SOC unificata
- Incidents & alerts
- Advanced Hunting
- Microsoft Sentinel workspace
- Data connectors
- Analytics rules
- Hunting queries
- Workbooks
- Automation rules / playbook

Threat Hunting sugli endpoint

- Tecniche di hunting sugli endpoint
- Ricerca di meccanismi di persistenza
- Individuazione di movimenti laterali
- Rilevamento di attività di credential dumping

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO BLUE TEAM ADVANCED: THREAT HUNTING, FORENSICS E MALWARE ANALYSIS

Durata: 2 giorni

Threat Hunting di rete
- Fondamenti del network threat hunting
- Individuazione di movimenti laterali in rete
- Rilevamento di attività di data exfiltration

Threat Hunting su identità e Microsoft 365
- Analisi sign-in sospetti
- Impossible travel
- Password spray
- MFA fatigue
- Token theft
- OAuth consent abuse
- Inbox rule abuse
- Mailbox compromise
- Risky users e risky sign-ins
- Conditional Access bypass/misconfiguration
- Correlazione Entra ID + Defender XDR + Exchange Online

MODULO 8: MALWARE ANALYSIS

Analisi statica
- Fingerprinting dei malware tramite hash
- Utilizzo di antivirus per la verifica della natura malevola
- Analisi di malware packed
- Analisi di stringhe offuscate
- Automazione delle attività di malware analysis

Analisi dinamica
- Tecniche di esecuzione controllata dei malware
- Monitoraggio delle attività dei processi
- Monitoraggio delle attività sui file
- Monitoraggio delle modifiche al Registry
- Monitoraggio delle comunicazioni di rete
- Utilizzo delle sandbox

Analisi dei file Microsoft Office
- Analisi di macro VBA
- Analisi di macro XML
- Analisi di documenti RTF con contenuti attivi
- Automazione del processo di analisi malware su documenti Office

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO BLUE TEAM ADVANCED: THREAT HUNTING, FORENSICS E MALWARE ANALYSIS

Durata: 2 giorni

OVERVIEW DEL CORSO

Il corso Blue Team Advanced è il naturale proseguimento del percorso Blue Team ed è rivolto a professionisti della sicurezza che vogliono sviluppare competenze avanzate in detection, analisi e risposta alle minacce informatiche. Nelle due giornate vengono approfonditi processi, strumenti e metodologie dei moderni Security Operations Center (SOC), con focus su threat hunting, digital forensics e malware analysis. I partecipanti acquisiscono una visione completa delle tecnologie e dei processi di sicurezza, imparando a raccogliere e analizzare evidenze digitali da sistemi Windows e Linux, memoria, traffico di rete ed endpoint compromessi.
Il corso include anche le principali tecniche di email security contro spoofing, phishing e allegati malevoli. Ampio spazio è dedicato alle attività pratiche di threat hunting (Defender XDR / Sentinel), analisi forense e malware analysis, con l'obiettivo di identificare indicatori di compromissione, tecniche di persistenza, movimenti laterali ed esfiltrazione dei dati attraverso un approccio strutturato alle investigazioni di sicurezza.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Security Analyst e SOC Analyst.
- System Administrator
- Cybersecurity Specialist
- IT Manager e responsabili della sicurezza che desiderano approfondire le attività operative di detection e investigazione.

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Comprendere struttura, processi, ruoli e tecnologie di un moderno Security Operations Center (SOC).
- Rafforzare la sicurezza del perimetro email attraverso SPF, DKIM, DMARC, MFA, Conditional Access e strumenti di simulazione phishing.
- Acquisire, preservare e analizzare evidenze digitali provenienti da sistemi Windows e Linux utilizzando tecniche di digital forensics.
- Effettuare attività di memory forensics e network forensics per individuare indicatori di compromissione e tecniche di persistenza.
- Svolgere attività avanzate di threat hunting su endpoint, rete e SIEM utilizzando Defender XDR e il framework MITRE ATT&CK.
- Analizzare malware tramite tecniche di analisi statica e dinamica, identificandone comportamento, capacità e indicatori di compromissione.

CONTATTI

info@nexsys.it

www.nexsys.it