

# CORSO CYBERSECURITY BLUE TEAM: DALLA DETECTION AL THREAT HUNTING OPERATIVO

Durata: 10,5 ore



## PROGRAMMA

### MODULO 1: FONDAMENTI DI DIFESA E VISIBILITY

- Ruoli e operatività: Triage, escalation, investigazione e contenimento all'interno di un SOC moderno.
- Superfici di attacco moderne: Monitoraggio di Identity, Endpoint, Email/Cloud e DNS.
- Logging essenziale: Quali sorgenti e quali eventi servono realmente per indagini efficaci.
- Analisi della baseline: Distinguere la normalità dall'anomalia su utenti, host e autenticazioni.

### MODULO 2: PHISHING & BUSINESS EMAIL COMPROMISE (BEC)

- Deep Header Analysis: Analisi forense degli header, salti SMTP e validazione SPF/DKIM/DMARC.
- BEC & Financial Fraud: Rilevare pattern di Invoice Manipulation e social engineering senza payload malevolo.
- Evoluzione delle minacce: Analisi di attacchi AiTM (Adversary-in-the-Middle), QR-phishing e tecniche di evasione sandbox.
- Incident Response per E-mail: Automazione della pulizia tenant (Search & Purge) su M365 e gestione di inoltri malevoli.


### MODULO 3: ACTIONABLE THREAT INTELLIGENCE

- Oltre l'IOC: Focus sulle TTPs (Tactics, Techniques, Procedures) tramite la Piramide del Dolore.
- MISP & Threat Sharing: Gestione dei feed, correlazione automatica e ciclo di vita degli indicatori.
- OSINT Enrichment: Utilizzo di sandbox (Any.run, JoeSandbox) per arricchire l'analisi in tempo reale.
- Mapping MITRE ATT&CK: Utilizzo della matrice per misurare l'effettiva capacità di rilevazione.

### MODULO 4: METODOLOGIE DI THREAT HUNTING

- L'ipotesi di hunting: Formulare domande basate sulla Threat Intelligence per scovare minacce silenti.
- Analisi Pivot: Ricostruire la Kill Chain muovendosi tra User, Process, Network e Registry.
- Query Design pratico: Introduzione a KQL (Kusto) o SPL (Splunk) per estrarre segnali da moli di dati complesse.
- Feedback Loop: Trasformare l'attività di hunting in nuove regole di detection permanente.

**CONTATTI**

 [info@nexsys.it](mailto:info@nexsys.it)

 [www.nexsys.it](http://www.nexsys.it)

# CORSO CYBERSECURITY BLUE TEAM: DALLA DETECTION AL THREAT HUNTING OPERATIVO

Durata: 10,5 ore



## MODULO 5: IDENTITY HUNTING & PASSWORD ATTACKS

- Advanced password attacks: Rilevare Brute Force, Password Spraying e Credential Stuffing nei log Azure/AD.
- Hunting on Identity: Investigazione su Kerberoasting, AS-REP Roasting e accessi da location insolite.
- Post-Compromise check: Analisi dei log dopo un takeover, app registrations anomale e persistenza cloud.
- Hardening operativo: Priorità per bloccare l'attaccante tramite revoca token e MFA enforcement.

## MODULO 6: DNS HUNTING & NETWORK TUNNELING

- DNS as a Weapon: Approfondimento su DNS Tunneling e Beaconing per canali di Command & Control (C2).
- Analisi statistica: Identificare anomalie tramite entropia dei sottodomini e record type insoliti.
- NXDOMAIN Monitoring: Rilevamento di algoritmi DGA (Domain Generation Algorithm) tipici dei malware.
- Network Containment: Tecniche di Sinkholing e isolamento a livello di risoluzione DNS.

## MODULO 7: ENDPOINT TRIAGE & INCIDENT RESPONSE

- Living off the Land (LotL): Hunting di processi legittimi abusati (PowerShell, Certutil, Wmic).
- Persistence & PrivEsc: Identificare tracce di escalation e persistenza (servizi, task, autorun).
- Rapid Triage: Cosa verificare prioritariamente su un endpoint senza complessità forense.
- IR "Light": Gestione dello scope, contenimento, recovery e lessons learned per prevenire ricorrenze.

**CONTATTI**

 [info@nexsys.it](mailto:info@nexsys.it)

 [www.nexsys.it](http://www.nexsys.it)

# CORSO CYBERSECURITY BLUE TEAM: DALLA DETECTION AL THREAT HUNTING OPERATIVO

Durata: 10,5 ore



## OVERVIEW DEL CORSO

Il corso Cybersecurity Blue Team ti fornisce un metodo concreto per illuminare le zone d'ombra della tua infrastruttura. Superiamo la teoria classica per concentrarci su ciò che conta davvero: Identity, Cloud e Detection avanzata.

Attraverso scenari reali, imparerai a smascherare attacchi all'identità, frodi email evolute e tecniche di movimento silenzioso degli attaccanti. Non solo riceverai strumenti per analizzare i log, ma acquisirai una vera metodologia di Threat Hunting per trasformare i dati in decisioni rapide e difese permanenti.

## A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a sistemisti e amministratori di rete, responsabili IT, aspiranti security analyst, tecnici IT, security consultant.

Per ottenere il massimo dal corso è consigliabile possedere: conoscenza base delle reti TCP/IP, familiarità con l'ambiente Windows e Active Directory, comprensione generale dei concetti di sicurezza, orientamento alla risoluzione dei problemi.

## COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Identificare le zone d'ombra della tua infrastruttura per capire esattamente dove manca visibilità e quali eventi monitorare.
- Smascherare attacchi evoluti di Phishing e BEC, analizzando header, bypass dell'MFA e frodi finanziarie senza malware.
- Utilizzare la Threat Intelligence operativa per mappare le minacce sulla matrice MITRE ATT&CK e prendere decisioni rapide.
- Adottare un metodo di Threat Hunting guidato per cercare proattivamente tracce di intrusione attraverso query e analisi pivot.
- Difendere l'Identity e il Cloud, rilevando attacchi alle password e tentativi di takeover nei log di Azure e Active Directory.
- Intercettare il traffico DNS sospetto, identificando tunnel e comunicazioni silenziose utilizzate dai malware per esfiltrare dati.
- Gestire l'Incident Response ed il Triage, analizzando i processi abusati sugli endpoint e applicando procedure di contenimento rapide.

**CONTATTI**

 [info@nexsys.it](mailto:info@nexsys.it)

 [www.nexsys.it](http://www.nexsys.it)