

# Roadmap corsi Cybersecurity

Livello

Corsi di formazione Cybersecurity

Beginner



Cybersecurity Fundamentals

Intermediate



Cybersecurity Specialist

Advanced



Defense

Cybersecurity Blue Team



Attack

CEH Ethical Hacking



Integrato

Cybersecurity Purple Team

Specialist



Defense

Incident Responder  
Ransomware Attack



Attack

Red Team: Attack and Defense  
Penetration Test on Azure

Che tu sia un professionista in cerca di specializzazione o un utente aziendale desideroso di migliorare le tue conoscenze in ambito cybersecurity, abbiamo il corso perfetto per te.

I nostri corsi di formazione sono progettati per trasformare le tue ambizioni in competenze concrete, offrendo la massima flessibilità con opzioni sia online che in aula e soluzioni dedicate oppure interaziendali.

La formazione in cybersecurity non è solo un investimento nelle tue competenze: è una necessità per stare al passo con l'evoluzione tecnologica e garantire la sicurezza dei dati aziendali.

# Un corso per ogni esigenza

In Nexsys, abbiamo l'obiettivo è soddisfare ogni esigenza dei nostri clienti. Verifica le tue necessità e scegli il corso più adatto!

Se desideri...

Scegli

- Acquisire conoscenze di base in cybersecurity

**Cybersecurity  
Fundamentals**

- Imparare come proteggere reti, endpoint e cloud aziendali
- Gestire la sicurezza in infrastrutture ibride

**Cybersecurity  
Specialist**

- Difendere reti e sistemi aziendali in modo avanzato
- Configurare e utilizzare sistemi SIEM per il rilevamento di minacce
- Eseguire indagini forensi per raccogliere e analizzare prove digitali

**Cybersecurity  
Blue Team**

- Sviluppare competenze offensive in cybersecurity
- Eseguire Vulnerability Assessment e Penetration Test
- Imparare tecniche di evasione dei firewall e antivirus

**CEH  
Ethical Hacking**

- Rafforzare la collaborazione tra team difensivi e offensivi

**Cybersecurity  
Purple Team**

- Creare e implementare piani di risposta agli incidenti
- Gestire incidenti di sicurezza in tempo reale

**Incident  
Responder**

# Un corso per ogni esigenza

In Nexsys, abbiamo l'obiettivo è soddisfare ogni esigenza dei nostri clienti. Verifica le tue necessità e scegli il corso più adatto!

Se desideri...

Scegli

- Capire come funzionano gli attacchi ransomware
- Applicare tecniche di risposta agli incidenti e analisi forense per raccogliere ed esaminare i dati.

**Ransomware Attack**

- Difendere reti e sistemi aziendali in modo avanzato
- Configurare e utilizzare sistemi SIEM per il rilevamento di minacce
- Eseguire indagini forensi per raccogliere e analizzare prove digitali

**Red Team: Attack and Defense**

- Identificare e mitigare le vulnerabilità nel cloud su Microsoft Azure
- Simulare movimenti laterali e attacchi su identità e risorse cloud su Azure

**Penetration Test on Azure**

# Portfolio corsi Cybersecurity

Qui puoi trovare l'elenco completo dei nostri corsi sulla cybersecurity, clicca sul nome del corso per visitare la pagina web dedicata.

Corso	Competenze	Step successivi
<a href="#">Cybersecurity Fundamentals</a>	<ul style="list-style-type: none"><li>• Difendere reti e sistemi aziendali in modo avanzato</li><li>• Configurare e utilizzare sistemi SIEM per il rilevamento di minacce</li><li>• Eseguire indagini forensi per raccogliere e analizzare prove digitali</li></ul>	Corso Cybersecurity: Network, Endpoint & Cloud
<a href="#">Cybersecurity Specialist</a>	<ul style="list-style-type: none"><li>• Creare un programma di sicurezza</li><li>• Strategia di difesa</li><li>• Difesa contro ransomware</li><li>• Architettura di rete difendibile</li><li>• Metodologia IAM</li><li>• Differenze tra fornitori di cloud</li><li>• Punti deboli di un sistema</li><li>• Mappa di visibilità della rete</li></ul>	Corso Cybersecurity Blue Team Corso CEH Ethical Hacking Corso Cybersecurity Purple Team
<a href="#">Cybersecurity Blue Team</a>	<ul style="list-style-type: none"><li>• Rispondere ad attacchi di phishing</li><li>• Indagini forensi su prove digitali</li><li>• Utilizzo di piattaforme SIEM</li><li>• Analisi di log e traffico di rete</li><li>• Ricerca sugli attori delle minacce</li><li>• Implementazione di sistemi di logging</li><li>• Best practices per soluzioni di sicurezza</li></ul>	Corso CEH Ethical Hacking Corso Cybersecurity Incident Responder
<a href="#">CEH Ethical Hacking</a>	<ul style="list-style-type: none"><li>• Raccolta di informazioni di intelligence</li><li>• Scansione di reti e computer</li><li>• Sfruttamento di vulnerabilità software e web</li><li>• Evasione dei firewall</li><li>• Evasione degli antivirus</li><li>• Attacchi su reti wireless</li><li>• Analisi della sicurezza nell'IoT</li><li>• Sviluppo di security policy aziendali</li></ul>	Corso Cybersecurity: Blue Team Corso Red Teaming AD: Attack and Defense Corso Penetration Test on Azure: Cloud Security
<a href="#">Cybersecurity Purple Team</a>	<ul style="list-style-type: none"><li>• Analisi tattiche di attacco e contromisure</li><li>• Utilizzo del framework MITRE ATT&amp;CK</li><li>• Implementazione di strategie di difesa attiva con MITRE D3FEND</li><li>• Utilizzo di strumenti come SIEM e Threat Intelligence</li><li>• Metodologie di test di sicurezza (Exploitation e Detection)</li></ul>	Corso Cybersecurity Blue Team Corso CEH Ethical Hacking
<a href="#">Incident Responder</a>	<ul style="list-style-type: none"><li>• Gestire incidenti di sicurezza e risposte</li><li>• Creare piani di risposta su Windows</li><li>• Eseguire analisi forensi di memoria e dischi</li><li>• Analizzare server web compromessi e log</li><li>• Analizzare log e attività di navigazione</li><li>• Redigere rapporti e piani di gestione delle crisi</li></ul>	Corso CEH Ethical Hacking

# Portfolio corsi Cybersecurity

Qui puoi trovare l'elenco completo dei nostri corsi sulla cybersecurity, clicca sul nome del corso per visitare la pagina web dedicata.

## Corso

## Competenze

## Step successivi

Red Teaming:  
Attack and  
Defense

- Introduzione ad AD e Powershell
- Autenticazione e Domain Controllers
- Recon nelle infrastrutture AD
- Metodi di attacco
- Kerberos e NTLM
- Privilege Escalation
- Password e Hash
- Attacchi Kerberos e mimikatz
- Persistence
- Modelli di difesa
- Modelli di logging
- Detection degli attacchi
- Miglioramenti della security di Windows Server e di AD

Corso Cybersecurity: Blue Team  
Corso Penetration Test on Azure: Cloud Security

Penetration Test  
on Azure

- Gestire tecniche di enumerazione di Azure
- Identificare configurazioni di sicurezza errate
- Sfruttare lacune nel controllo degli accessi
- Padroneggiare il Lateral Movement su Azure
- Sfruttare attacchi di phishing per compromissione iniziale
- Condurre controlli di sicurezza nel cloud di Azure

Corso Cybersecurity Blue Team  
Corso Red Teaming AD: Attack and Defense

Ransomware  
Attack

- Acquisire una comprensione delle fasi di un attacco ransomware e delle tecniche di difesa.
- Eseguire simulazioni di attacco in un ambiente di laboratorio cloud.
- Applicare tecniche di incident response per la raccolta e l'analisi dei dati.
- Comprendere le migliori pratiche per prevenire e rispondere efficacemente agli attacchi ransomware.

OSINT  
Fundamentals

- Comprendere il ciclo OSINT
- Utilizzare strumenti di ricerca Open
- Raccogliere e valutare la rilevanza delle informazioni
- Comunicare risultati con report e dashboard
- Applicare una metodologia di lavoro integrata