

# CORSO CLOUD SECURITY: PROTEZIONE DELLE APPLICAZIONI CLOUD-NATIVE

Durata: 20 ore

## PROGRAMMA

### MODULO 1: WEB SECURITY: TOWARDS CLOUD-NATIVE

- Same Origin Policy
- Cross-Origin Resource Sharing
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery
- API Security
- JWT Security

### MODULO 2: INTRODUCTION TO CLOUD SECURITY

- Cloud-Native security
- Examples from Real-World breaches
- Shared responsibility model
- OWASP Cloud-Native Application Security Top 10
- OWASP Top 10 CI/CD Security Risks
- DevSecOps principles

### MODULO 3: SECURING CI/CD PIPELINES

- Anatomy of a CI/CD pipeline
- Common Threats & Defenses
- Secrets management
- Code signing & artifact verification
- CI/CD tools: SAST, DAST, and SCA
- Security Gates

### MODULO 4: SOFTWARE SUPPLY CHAIN SECURITY

- Supply chain anatomy
- Threats to the supply chain
- Real-World attacks
- Secure dependency management

Scopri di più sul [corso Secure Coding](#).



# CORSO CLOUD SECURITY: PROTEZIONE DELLE APPLICAZIONI CLOUD-NATIVE

Durata: 20 ore

## MODULO 5: INCIDENT RESPONSE, MONITORING & COMPLIANCE

- Introduzione al processo di incident response
- Incidenti comuni in ambienti cloud
- Sviluppo di incident response playbooks
- Principi di osservabilità nel cloud
- Compliance in ambienti cloud

Scopri di più sul [corso Cloud Security](#).



# CORSO CLOUD SECURITY: PROTEZIONE DELLE APPLICAZIONI CLOUD-NATIVE

Durata: 20 ore

## OVERVIEW DEL CORSO

Il corso Cloud Security affronta in modo completo e pratico i principali aspetti della sicurezza negli ambienti cloud e nei moderni processi di sviluppo software.

Attraverso laboratori e casi reali, i partecipanti analizzeranno le vulnerabilità più comuni delle applicazioni cloud-native, i rischi legati alle pipeline CI/CD e alle supply chain del software, fino ad arrivare ai principi di incident response, monitoring e compliance.

Con un approccio hands-on, il corso fornisce strumenti concreti per prevenire e gestire minacce come CSRF, SSRF, API e JWT exploitation, garantire la sicurezza delle pipeline di integrazione e rilascio, gestire in modo sicuro le dipendenze di progetto e sviluppare playbook di risposta agli incidenti.

Un percorso ideale per chi lavora con tecnologie cloud e vuole acquisire competenze applicabili subito nei propri progetti e nei processi DevSecOps aziendali.

## A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Sviluppatori
- DevOps engineer
- Professionisti della sicurezza IT
- IT Manager

## COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Analizzare e prevenire vulnerabilità comuni nel contesto cloud-native.
- Comprendere il modello di responsabilità condivisa e i principali standard (OWASP Top 10 Cloud e CI/CD).
- Integrare la sicurezza nei processi DevOps (principi DevSecOps).
- Proteggere pipeline CI/CD con strumenti di analisi e security gates.
- Gestire in sicurezza segreti, dipendenze e artifact del software.
- Identificare e contrastare attacchi alla software supply chain.
- Sviluppare playbook di incident response per ambienti cloud.
- Implementare monitoring, osservabilità e compliance in contesti cloud.

