Programma Academy Cybersecurity

Introduzione

Il programma di formazione in Cybersecurity sistemistica nasce con l'obiettivo di preparare giovani professionisti in grado di affrontare le sfide crescenti legate alla sicurezza informatica nelle infrastrutture IT moderne. La crescita della digitalizzazione e l'aumento delle minacce cyber rendono fondamentale formare figure specializzate in grado di operare in contesti complessi, sia in ambienti on-premise sia in cloud.

Il percorso integra conoscenze teoriche e competenze pratiche, coprendo sistemi operativi, reti, database, sicurezza, gestione identità e conformità normativa europea. Questa formazione completa prepara i partecipanti ad affrontare le moderne sfide della cybersecurity con competenza e professionalità.

READY2USE

Obiettivi del Programma

Formazione Professionale

Formare nuovi professionisti in ambito cybersecurity sistemistica, capaci di gestire, proteggere e monitorare infrastrutture IT complesse attraverso un approccio metodico e strutturato.

Percorso Pratico

Accompagnare i partecipanti in un percorso professionalizzante che unisce teoria e pratica con casi reali, esercitazioni e simulazioni per garantire un apprendimento efficace.

Opportunità di Carriera

Assunzione a tempo indeterminato dei candidati selezionati, con l'obiettivo di avviare una carriera strutturata e di lungo periodo nel settore IT e cybersecurity.

READY2USE

Modulo 1 – Fondamenti di Informatica

Durata del Modulo

1 giorno intensivo di formazione concentrata sui fondamenti essenziali dell'informatica moderna.

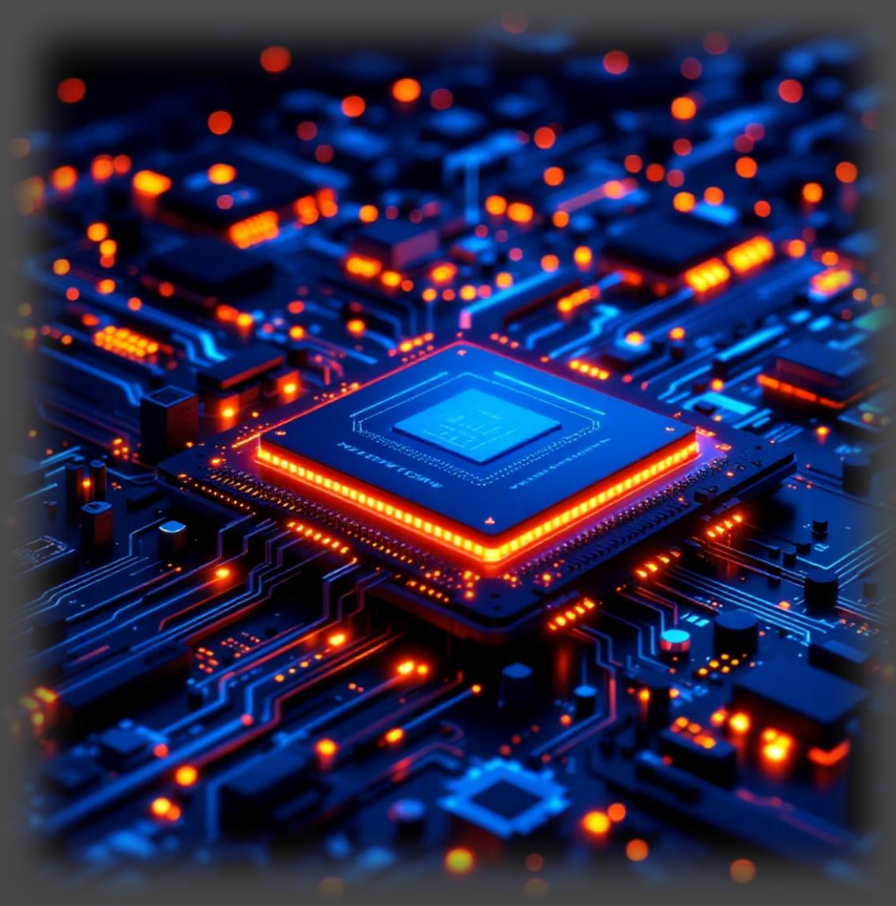
Argomenti Chiave

Architettura del calcolatore, sistemi operativi, reti, protocolli, virtualizzazione, cloud, configurazione di rete su Windows/Linux.

Questi argomenti costituiscono la base fondamentale per comprendere come funzionano le moderne infrastrutture IT e come possono essere vulnerabili agli attacchi informatici.

Finalità Formativa

Fornire basi solide di informatica e networking per comprendere l'infrastruttura IT e il contesto di sicurezza. Questo modulo prepara i partecipanti a comprendere le vulnerabilità sistemiche e le best practice di sicurezza.



Le basi dell'informatica moderna sono essenziali per comprendere le vulnerabilità e implementare soluzioni di sicurezza efficaci.

READY2USE

Modulo 2 – Linux

01

Durata: 11 giorni

Un percorso approfondito che copre tutti gli aspetti essenziali dell'amministrazione Linux per la cybersecurity.

02

Competenze Tecniche

Comandi base, gestione utenti e permessi, shell scripting avanzato, gestione pacchetti e storage, configurazione firewall e implementazione delle migliori pratiche di sicurezza.

03

Obiettivo Formativo

Sviluppare competenze nella gestione e messa in sicurezza di sistemi Linux, preparando i partecipanti a diventare amministratori Linux sicuri e competenti.

Linux rappresenta una componente fondamentale dell'infrastruttura IT moderna, specialmente in ambito server e cloud. La padronanza di questo sistema operativo è essenziale per qualsiasi professionista della cybersecurity, dato che molti strumenti di sicurezza e server critici operano su piattaforme Linux. Durante questo modulo, i partecipanti acquisiranno non solo le competenze tecniche necessarie, ma anche la mentalità di sicurezza richiesta per proteggere efficacemente i sistemi Linux da minacce interne ed esterne.

READY2USE

Modulo 3 – Windows

Durata: 8 giorni intensivi

Un modulo completo dedicato all'ecosistema Microsoft, fondamentale per la maggior parte delle infrastrutture aziendali italiane.

Windows Server

Amministrazione avanzata dei server Windows, configurazione dei ruoli e delle funzionalità per garantire prestazioni ottimali e sicurezza.

Active Directory

Gestione centralizzata di utenti, computer e risorse di rete attraverso le directory services Microsoft.

Integrazione Azure

Connessione e gestione degli ambienti ibridi cloud-on premise per massimizzare flessibilità e sicurezza.

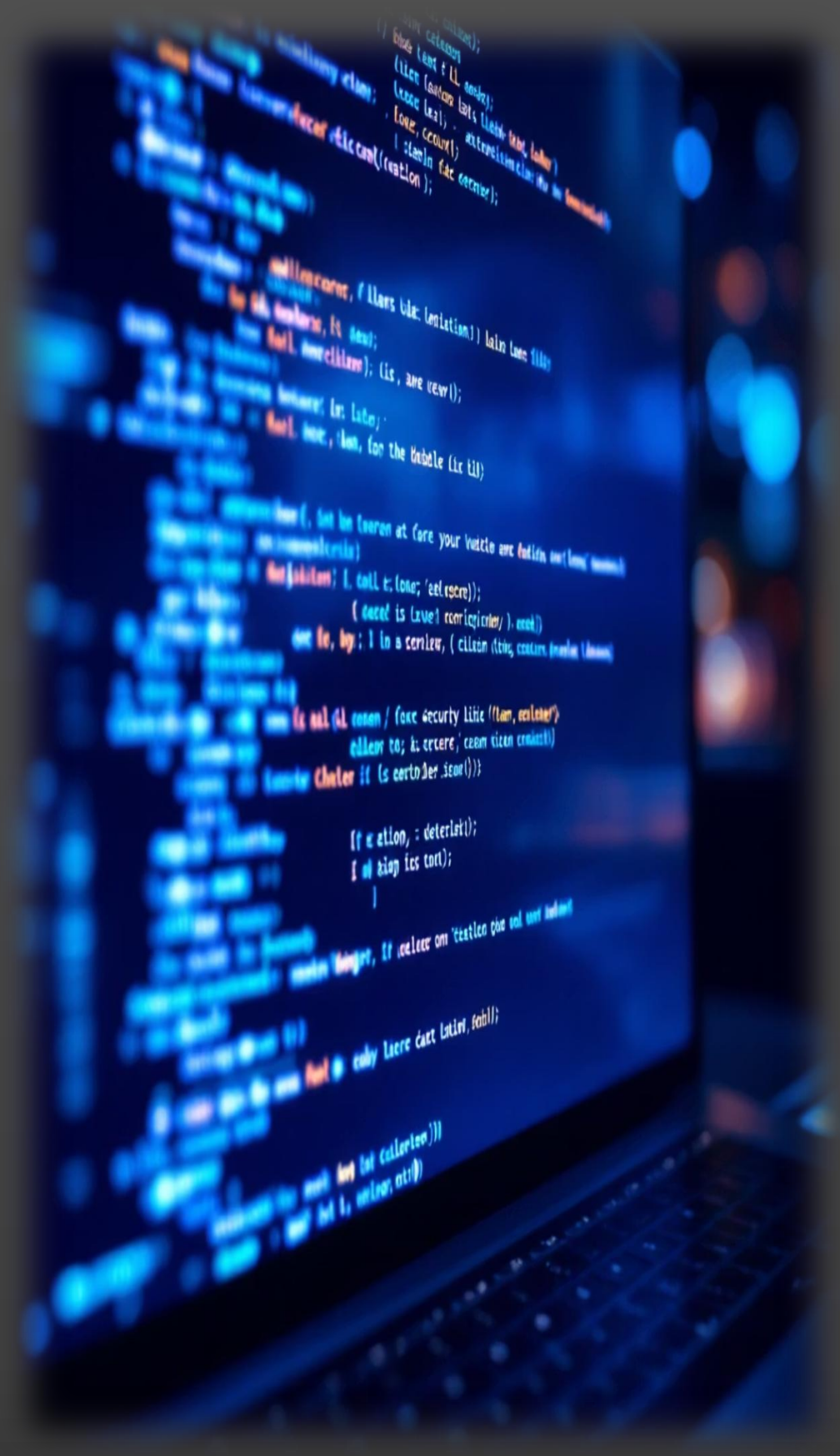
L'ecosistema Windows rimane predominante nelle aziende italiane. Questo modulo prepara i partecipanti a gestire e proteggere ambienti Microsoft complessi, integrando servizi core come IIS, virtualizzazione Hyper-V e automazione PowerShell. La finalità è formare sistemisti capaci di amministrare e proteggere ambienti Microsoft con competenza professionale, implementando politiche di sicurezza avanzate e gestendo efficacemente la transizione verso soluzioni cloud ibride.

READY2USE

Modulo 4 – SQL e Database

Durata del Modulo

6 giorni dedicati alla gestione sicura dei dati e alla protezione delle informazioni critiche aziendali.



Argomenti Fondamentali

Il modulo copre i concetti fondamentali di SQL, tecniche avanzate di query optimization, creazione e gestione di viste complesse, gestione delle transazioni per garantire l'integrità dei dati, e approfondimenti specifici su Oracle Database con focus particolare sulla sicurezza.

I partecipanti impareranno a implementare controlli di accesso granulari, tecniche di crittografia dei dati, backup sicuri e strategie di disaster recovery. La sicurezza dei database rappresenta un elemento critico nella protezione delle informazioni sensibili aziendali.

Finalità: Acquisire competenze nella gestione sicura dei dati e nella protezione dei database, preparando i partecipanti a diventare esperti nella sicurezza delle basi di dati enterprise.

READY2USE

Modulo 5 – Reti e Sicurezza

Fondamenti di Rete

Modelli OSI/TCP-IP, subnetting avanzato e tecniche di routing per comprendere il flusso dei dati nelle reti moderne.

1

Protocolli e Servizi

Analisi approfondita dei protocolli TCP/UDP, configurazione NAT e implementazione di soluzioni VPN sicure.

2

Sicurezza Perimetrale

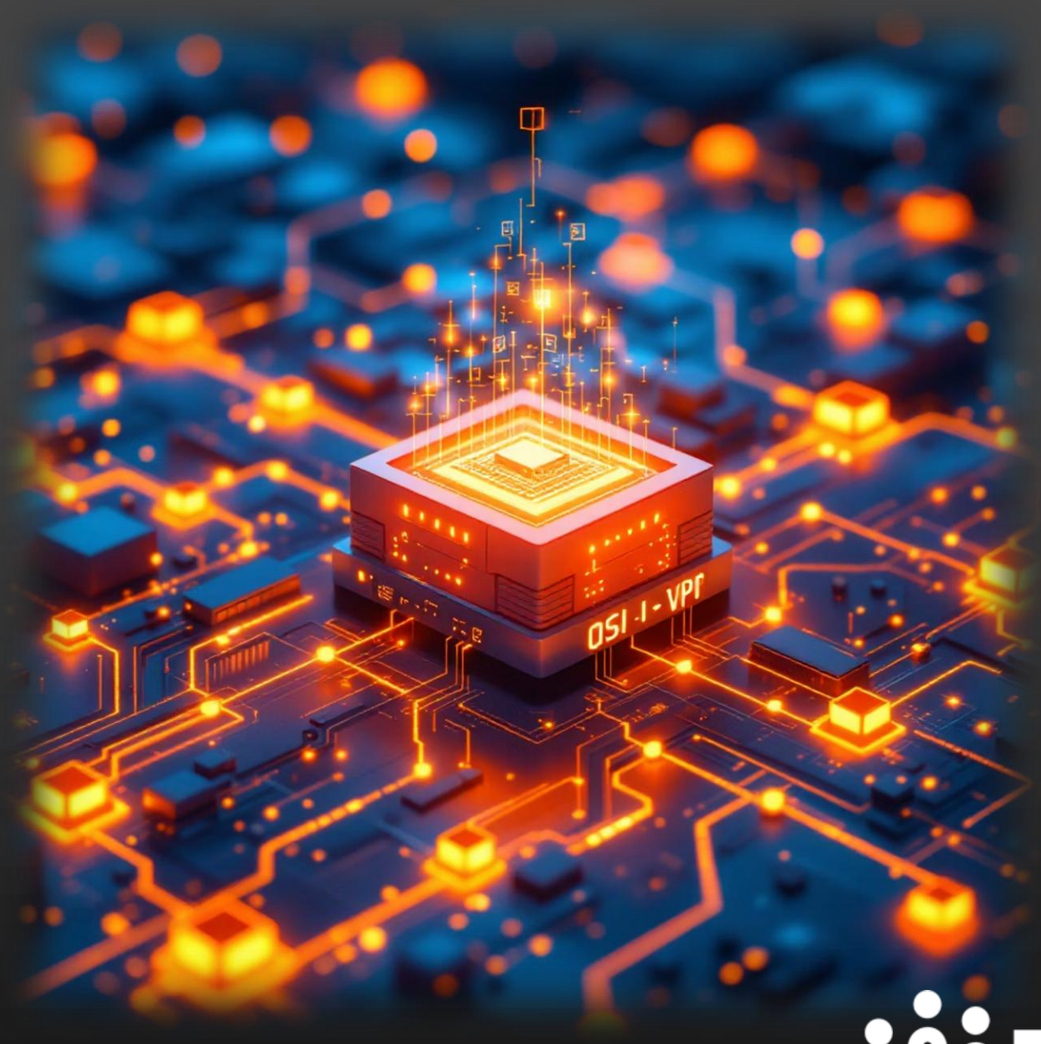
Configurazione firewall avanzata e utilizzo di strumenti di diagnostica per il monitoraggio della sicurezza di rete.

3

Durata: 6 giorni

Un modulo intensivo che combina teoria delle reti e applicazioni pratiche di sicurezza. I partecipanti acquisiranno competenze essenziali per comprendere le architetture di rete moderne e le loro potenziali vulnerabilità.

Finalità del modulo: Comprendere architetture di rete e loro vulnerabilità, con focus specifico sulla protezione delle comunicazioni aziendali. I partecipanti svilupperanno competenze per progettare, implementare e mantenere infrastrutture di rete sicure.



READY2USE

Modulo 6 – SOC e SIEM

Ruolo del SOC

Comprensione delle responsabilità e dei processi operativi di un Security Operations Center moderno.

Analisi e Detection

Tecniche di analisi log, identificazione degli Indicator of Compromise (IoC) e metodologie di threat hunting.

Response & Forensics

Incident response efficace e digital forensics per investigazioni approfondite su incidenti di sicurezza.

6

giorni di formazione

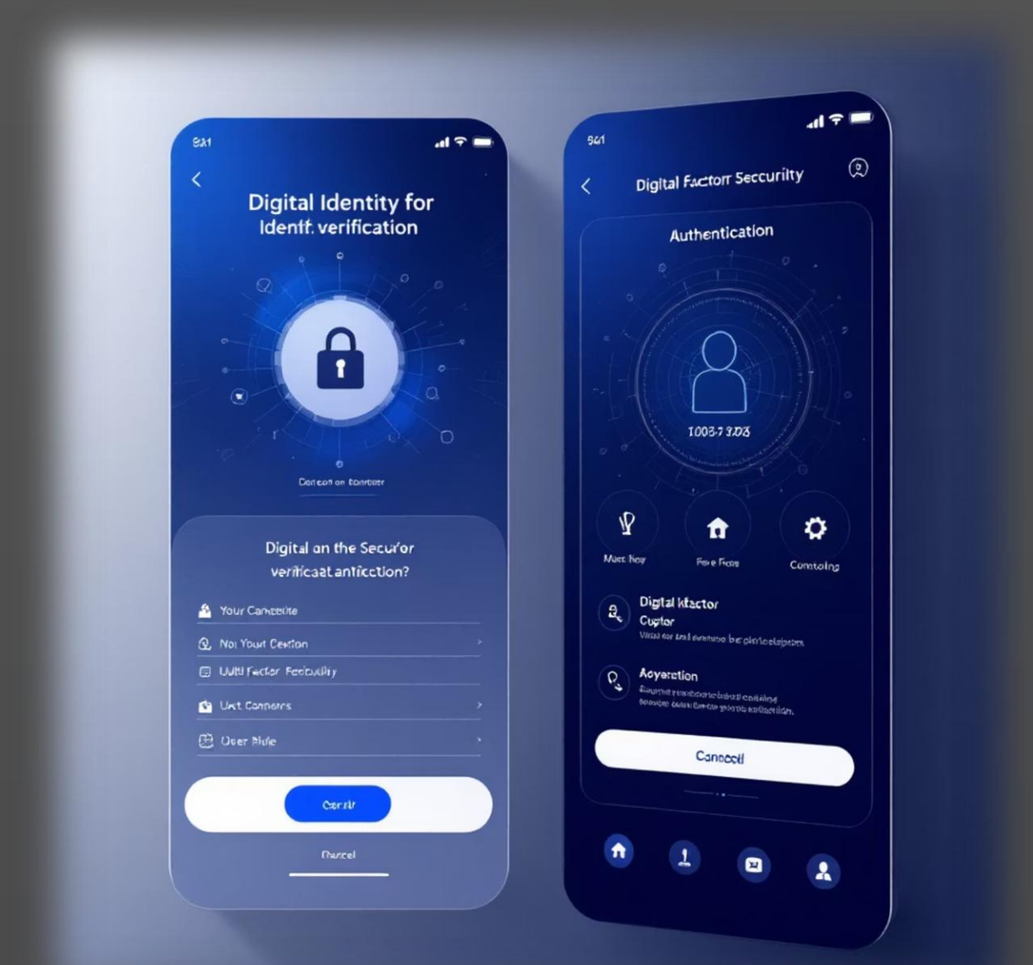
Intensiva e pratica

Questo modulo rappresenta il cuore operativo della cybersecurity moderna. I partecipanti apprenderanno l'utilizzo pratico di strumenti SIEM avanzati come Wazuh ed ELK Stack, sviluppando competenze nell'analisi dei log di sicurezza, nella correlazione degli eventi e nella creazione di dashboard per il monitoraggio continuo.

Finalità: Preparare analisti SOC qualificati in grado di rilevare tempestivamente gli incidenti di sicurezza e rispondere efficacemente alle minacce, utilizzando metodologie standardizzate e strumenti professionali del settore.

READY2USE

Modulo 7 – Identity and Access Management



Durata

3 giorni di formazione specialistica sui sistemi di gestione delle identità digitali.

Focus

Gestione sicura delle identità e degli accessi in ambienti enterprise complessi.

Principi IAM

Fondamenti dell'Identity and Access Management, architetture di autenticazione e autorizzazione per garantire accessi sicuri e controllati.

MFA e SSO

Implementazione di Multi-Factor Authentication e Single Sign-On per bilanciare sicurezza e usabilità nei sistemi aziendali.

Controlli Avanzati

Protocolli RBAC/ABAC, directory services enterprise e privileged access management per proteggere account amministrativi critici.

Finalità del modulo: Gestire identità e accessi in maniera sicura e conforme, implementando politiche granulari che proteggano le risorse aziendali critiche mantenendo al contempo efficienza operativa e compliance normativa.

READY2USE

Modulo 8 – Normativa Europea e Compliance

1

GDPR

Regolamento Generale sulla Protezione dei Dati: implementazione pratica, diritti degli interessati, valutazioni d'impatto e gestione delle violazioni di dati personali.

2

NIS2

Direttiva sulla sicurezza delle reti e dei sistemi informativi: obblighi per le entità essenziali e importanti, misure di gestione del rischio cyber.

3

DORA

Regolamento sulla resilienza operativa digitale: requisiti specifici per il settore finanziario, test di penetrazione e gestione del rischio ICT.

Durata: 3 giorni

Un modulo essenziale che completa la formazione tecnica con la comprensione del quadro normativo europeo. I partecipanti acquisiranno competenze negli obblighi di notifica degli incidenti, nelle procedure di audit e nei framework ISO/IEC 27001.

Finalità: Comprendere il quadro normativo europeo e i requisiti di compliance per operare legalmente e eticamente nel settore della cybersecurity, garantendo che le soluzioni tecniche implementate rispettino i più alti standard normativi internazionali.

Il completamento di tutti i moduli fornisce una formazione completa e bilanciata, preparando i partecipanti ad affrontare le sfide moderne della cybersecurity con competenza tecnica e consapevolezza normativa.

READY2USE