SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SERICS
CYBERSECURITY
ACADEMY

PIANO DIDATTICO

ATTIVITÀ DI PROMOZIONE
E SUPPORTO DI MASTER UNIVERSITARI


Finanziato
dall'Unione europea
NextGenerationEU


Ministero
dell'Università
e della Ricerca


Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA

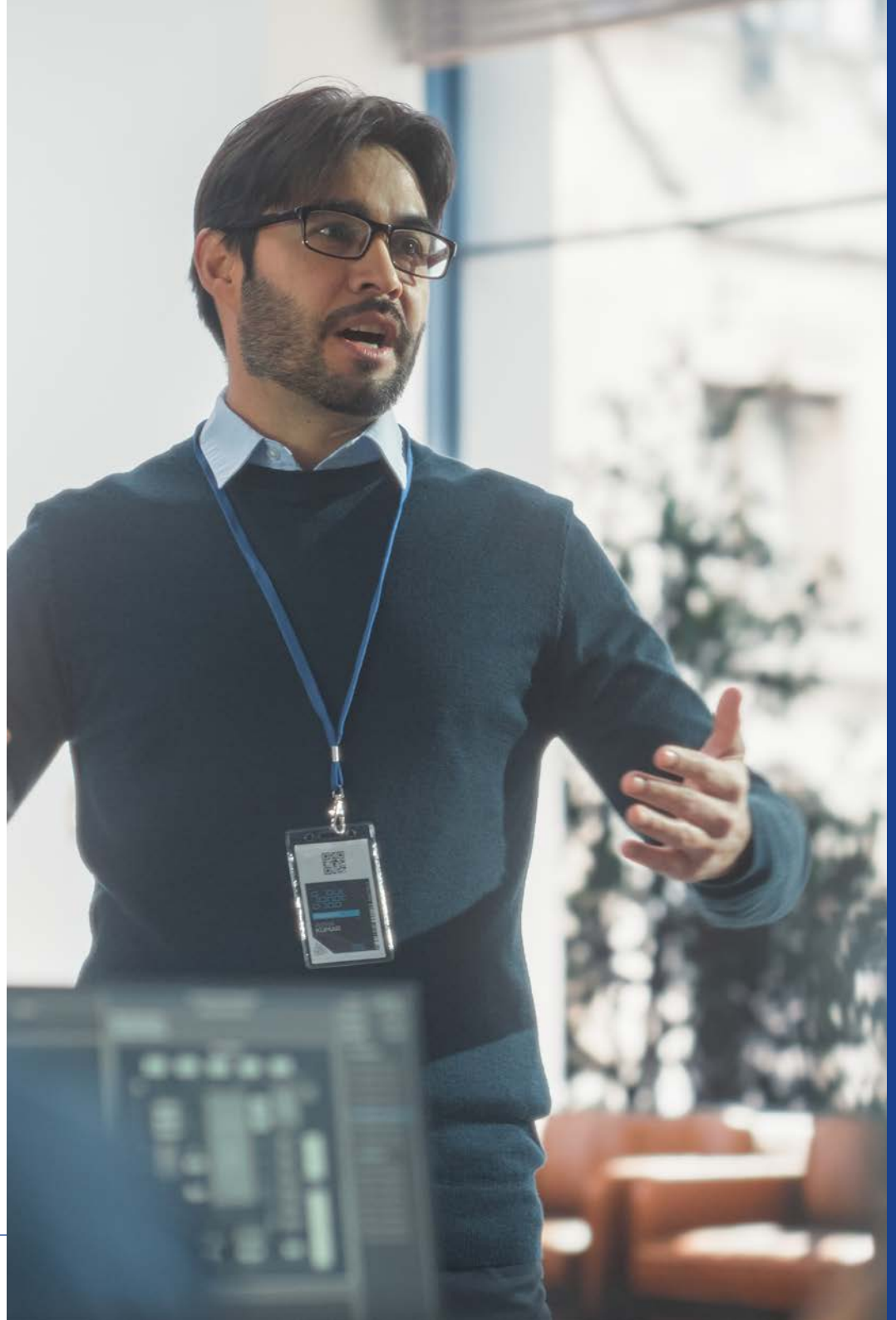

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

I NOSTRI DOCENTI

Per la progettazione e l'erogazione della formazione, la SERICS Cybersecurity Academy si avvale di docenti, tutor ed esperti di altissimo profilo.

Nello specifico:

- Docenti con esperienza pluriennale in ricerca e insegnamento sulla cybersecurity presso università o centri di ricerca accreditati ANVUR;
- Tutor specializzati in percorsi formativi sulla cybersicurezza;
- Progettisti didattici, esperti nella creazione di materiali formativi per la cybersecurity;
- Specialisti nella preparazione di test e competizioni di cybersecurity;
- Esperti nella progettazione e realizzazione di attività formative con esperienza specifica in ambito aziendale e pubblico.



SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

INDICE

modulo 01	Elementi avanzati per la gestione della Cybersecurity	8
modulo 02	Elementi di Cybersecurity	10
modulo 03	Secure Software Engineering	12
modulo 04	Web Security	14
modulo 05	Network attacks and security strategies	16
modulo 06	From Cryptography to Stenography	18

modulo 01

ELEMENTI AVANZATI PER LA GESTIONE DELLA CYBERSECURITY

argomento 01

ELEMENTI DI CRITTOGRAFIA AVANZATI ED APPLICAZIONI

4 ORE

Il modulo avanzato sulla crittografia si concentra sulle applicazioni pratiche e sulle sfide moderne della sicurezza digitale, approfondendo il ruolo cruciale dei certificati digitali e della firma digitale nel garantire autenticità, integrità e riservatezza delle informazioni nel cyberspazio. Dopo una panoramica sulle tecniche crittografiche più avanzate, come l'uso delle curve ellittiche e degli algoritmi asimmetrici, il corso esplora l'applicazione di queste tecnologie nella creazione e gestione dei certificati digitali, utilizzati per l'autenticazione sicura dei servizi online. La firma digitale, analizzata sia dal punto di vista teorico che pratico, è presentata come una soluzione fondamentale per garantire l'integrità dei dati e la non ripudiabilità nelle transazioni elettroniche. Le esercitazioni pratiche offrono agli studenti l'opportunità di applicare le conoscenze acquisite nella generazione, gestione e verifica di certificati digitali e firme digitali, approfondendo le loro implicazioni nell'ambito delle comunicazioni sicure, del commercio elettronico e della protezione della privacy.

argomento 02

L'INTEGRAZIONE DELLA NIS2 CON LA ISO9001

12 ORE

Il modulo esplora l'integrazione tra la ISO 9001, standard per la gestione della qualità, e la NIS2, direttiva europea sulla sicurezza informatica. Dopo una panoramica sui principi della ISO 9001, come la gestione dei processi e il miglioramento continuo, si analizza l'allineamento con i requisiti di sicurezza della NIS2, con particolare attenzione a controlli, gestione del rischio e processi. Si evidenzia la differenza tra il monitoraggio di prodotti e di processi per garantire qualità e sicurezza. Il modulo si conclude con un'esercitazione pratica sull'applicazione combinata degli standard.

argomento 03

ORGANIZZAZIONE DELLE ATTIVITÀ DI INCIDENT RESPONSE TEAM PER SISTEMI IT ED OT

12 ORE

Il modulo illustra le attività operative da svolgere in caso di incidente informatico, con un focus su tecniche di reazione e contrasto e sulla collaborazione con le autorità competenti. Vengono approfonditi i processi di Incident Response, dall'identificazione e analisi degli eventi alla gestione delle evidenze digitali, con particolare riferimento alla raccolta e all'analisi di Memory Dump. L'approccio pratico include la classificazione degli artefatti digitali, essenziale per distinguere informazioni rilevanti e supportare le indagini, garantendo al contempo la corretta gestione dei dati secondo le normative e le procedure richieste per affrontare minacce informatiche in modo coordinato e sistematico. Il modulo prevede inoltre esercitazioni pratiche su scenari virtualizzati realizzati in ambiente GNS3, per simulare situazioni reali e consolidare le competenze operative acquisite.

argomento 04

OPEN SOURCE INTELLIGENCE - STRUMENTI E TECNICHE

12 ORE

L'introduzione alle tecniche di OSINT (Open Source Intelligence) offre un panorama completo sull'uso di strumenti e metodi per raccogliere informazioni da fonti aperte, come social network, motori di ricerca e piattaforme online. Il documento approfondisce l'uso di API, dork Google, e software specializzati per analisi su Facebook, Instagram, Twitter, LinkedIn, YouTube e Telegram. Evidenzia le peculiarità di ciascuna piattaforma e le strategie per estrarre dati utili, sottolineando l'importanza di comprendere i limiti imposti dalle policy e i rischi di privacy legati all'utilizzo di questi strumenti.

modulo 02 ELEMENTI DI CYBERSECURITY

argomento 01

ANALISI DEL RISCHIO

7.30 ORE

Si propone di fornire ai partecipanti una comprensione approfondita dei concetti legati all'analisi del rischio valutando la presenza di incertezza nel processo decisionale, focalizzandosi sulla riduzione dell'incertezza attraverso tecniche avanzate di analisi del rischio. Verrà esplorata la dimensione temporale nell'analisi del rischio, evidenziando come le decisioni possano evolvere nel tempo e come l'incertezza influisca sulle scelte future. Il primo modulo si concentrerà sulle principali tecniche di analisi del rischio, con particolare attenzione alla comprensione delle barriere e del loro degrado nel contesto operativo, nonché all'importanza delle barriere organizzative nel mitigare i rischi. Il secondo modulo si focalizzerà su approcci sistematici e sistemici, esplorando il concetto di affidabilità e sicurezza come pilastri fondamentali per la gestione dei rischi. Infine, il programma tratterà gli esiti dell'analisi del rischio, permettendo ai partecipanti di acquisire gli strumenti necessari per valutare e interpretare i risultati dell'analisi, così da prendere decisioni informate e consapevoli.

argomento 02

ELEMENTI DI PROGRAMMAZIONE

22.30 ORE

Fornisce le competenze fondamentali per la programmazione e la sicurezza del software. I partecipanti esploreranno concetti base di programmazione, come controllo di flusso, funzioni, gestione degli errori, e strutture dati, con particolare attenzione alla scrittura di codice sicuro. Verranno introdotti anche i concetti di programmazione orientata agli oggetti (OOP) e la gestione degli ambienti virtuali, essenziali per mantenere un codice efficiente e protetto. Il programma prevede esercitazioni che integreranno le competenze acquisite in programmazione e cybersecurity, permettendo ai partecipanti di sviluppare software sicuro e resiliente. Questo corso è ideale per chi desidera acquisire una solida base nella programmazione e nel rafforzamento della sicurezza informatica.

argomento 03

INTRODUZIONE AI DATI

11.30 ORE

Fornisce una formazione completa sulla gestione sicura dei dati, esplorando le normative, la governance e le migliori pratiche per garantire la protezione e l'integrità delle informazioni. I partecipanti apprenderanno i concetti fondamentali sui dati, il loro ciclo di vita e le tipologie, e approfondiranno le politiche e le normative europee e nazionali, come il GDPR, che regolano la protezione dei dati e la cybersecurity. Saranno trattati anche gli aspetti pratici della governance dei dati, tra cui i ruoli e le responsabilità, e l'importanza della qualità dei dati attraverso framework internazionali come il DAMA DMBoK. Il corso esamina inoltre la protezione dei dati e le tecniche di cybersecurity necessarie per gestire e mitigare i rischi legati alla sicurezza delle informazioni. Verranno analizzati i requisiti per un sistema di gestione dei dati sicuro e l'importanza di una corretta valutazione di impatto sulla privacy. Questo programma è ideale per professionisti e responsabili aziendali che desiderano acquisire competenze avanzate nella gestione sicura dei dati e nella protezione delle informazioni personali, assicurando conformità alle normative e sostenibilità a lungo termine.

argomento 04

I DATABASE

7 ORE

Fornisce una formazione completa sulla progettazione e gestione sicura dei database, integrando aspetti fondamentali come la modellazione tramite diagrammi ER, l'esecuzione di query, l'interazione tra interfacce web e database, e le migliori pratiche di sicurezza. I partecipanti apprenderanno a progettare database robusti utilizzando diagrammi Entità-Relazione (ER), comprendendo la definizione di entità, attributi e relazioni, e applicando principi di progettazione sicura. Saranno esplorate le tecniche per scrivere query efficienti e sicure, minimizzando i rischi di SQL injection e garantendo l'integrità dei dati. Il corso approfondirà anche la configurazione sicura delle interfacce tra applicazioni web e database, includendo l'uso di HTTPS, autenticazione forte e gestione delle sessioni.

argomento 05

LE RETI INFORMATICHE

17 ORE

Analisi dei concetti di base relativi alle reti informatiche con attenzione alla descrizione delle caratteristiche principali dello stack ISO-OSI nell'ottica di fornire competenze di base utili per una comprensione completa del traffico di rete. Il modulo analizzerà le caratteristiche fondamentali del traffico generato in reti simulate durante attività pratiche di laboratorio. Durante le lezioni, inoltre saranno fornite le competenze necessarie per impostare moduli avanzati sul tema del filtraggio del traffico e l'identificazione di minacce.

modulo 03

SECURE SOFTWARE ENGINEERING

argomento 01

SECURE SOFTWARE FUNDAMENTALS

1.40 ORE

L'argomento introduce i principi base della sicurezza del software, concentrandosi su come prevenire vulnerabilità sin dalle prime fasi dello sviluppo.

argomento 02

SECURE DESIGN PRINCIPLES

1.30 ORE

Tratta le linee guida per progettare sistemi sicuri, come il principio del minimo privilegio e la difesa in profondità.

argomento 03

SECURE DESIGN PRINCIPLES VULNERABILITIES

1.30 ORE

Approfondisce le buone pratiche di progettazione e le principali vulnerabilità che possono compromettere la sicurezza applicativa.

argomento 04

SECURE SOFTWARE GOVERNANCE AND ACCEPTANCE

2 ORE

Analizza le politiche e i processi di gestione della sicurezza del software, inclusa la verifica e la validazione prima del rilascio.

argomento 05

SOFTWARE ASSURANCE MATURITY MODEL (SAMM)

1.40 ORE

Descrive il modello SAMM come strumento per misurare e migliorare la maturità dei processi di sicurezza nel ciclo di vita del software.

argomento 06

THREAT MODELING

1.40 ORE

Illustra le tecniche per identificare, analizzare e mitigare le minacce in fase di progettazione, anticipando possibili attacchi informatici.

modulo 04 WEB SECURITY

argomento 01

INFORMATION GATHERING

1.30 ORE

Introduzione al ciclo completo: identificazione, contenimento, eradicazione, recupero, post-mortem. Allineamento con NIST SP 800-61 e ISO/IEC 27035.

argomento 02

AUTENTICAZIONE

1.30 ORE

Riguarda il processo che verifica l'identità di un utente o di un sistema, assicurando che solo soggetti autorizzati possano accedere alle risorse.

argomento 03

AUTORIZZAZIONE

2 ORE

Definizione di quali azioni un utente autenticato può compiere, regolando l'accesso alle risorse secondo ruoli e privilegi.

argomento 04

GESTIONE SESSIONE

3 ORE

In questo argomento si tratta del controllo e protezione delle sessioni utente attive per prevenire furti di sessione, hijacking e abusi di credenziali.

argomento 05

DATA VALIDATION

2 ORE

Illustra la garanzia che i dati inseriti in un sistema siano corretti e sicuri, prevenendo attacchi come SQL injection o cross-site scripting (XSS).

modulo 05

NETWORK ATTACKS AND SECURITY STRATEGIES

argomento 01

CYBERSECURITY IS A PROCESS, NOT A PRODUCT

2 ORE

La sicurezza informatica non è un risultato statico, ma un processo continuo di prevenzione, monitoraggio e miglioramento contro le minacce.

argomento 02

SECURITY GOALS: THE CIA TRIAD

2 ORE

Descrive i tre obiettivi fondamentali della sicurezza: Confidenzialità, Integrità e Disponibilità dei dati e dei sistemi.

argomento 03

ATTACK SURFACE ANALYSIS

2 ORE

Analizza tutti i punti di un sistema che possono essere attaccati, aiutando a ridurre le vulnerabilità e rafforzare le difese.

argomento 04

THE SWISS CHEESE MODEL

2 ORE

Rappresenta la sicurezza come una serie di livelli di difesa: anche se ogni strato ha delle falle, la loro combinazione crea una protezione efficace.

modulo 06

FROM CRYPTOGRAPHY TO STENOGRAPHY

argomento 01

STEGANOGRAFIA CONCETTO E PRINCIPI

1.30 ORE

Spiegazione della tecnica che consiste nel nascondere informazioni all'interno di altri dati o file, rendendo invisibile la presenza stessa del messaggio.

argomento 02

STEGANOGRAFIA DIGITALE - DATI IN FORMATO LOSSLESS

1.30 ORE

Utilizzo dei file senza perdita di qualità (come BMP o WAV) per inserire dati nascosti, mantenendo intatta l'informazione originale.

argomento 03

STEGANOGRAFIA DIGITALE - DATI IN FORMATO LOSSY

1.30 ORE

L'argomento tratta di come nascondere le informazioni in file compressi (come JPEG o MP3), sfruttando le aree meno percettibili per l'occhio o l'orecchio umano.

argomento 04

STEGANALISI

1.30 ORE

Insieme di tecniche per rilevare, estrarre o analizzare dati nascosti all'interno di file attraverso la steganografia.

argomento 05

WATERMARKING E FINGERPRINT

2 ORE

Metodi per incorporare informazioni identificative nei contenuti digitali: il watermarking protegge i diritti d'autore, mentre il fingerprinting traccia l'origine o l'uso dei file.

serics.eu

serics.eu/academy

academy@serics.eu

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE