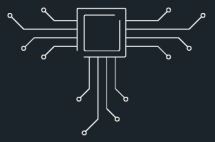
LEONARDO

Leonardo Cyber & Security Solutions

Cybersecurity Summer course 2024 @ DIETI

Aprile 2024



Electronics

Helicopters

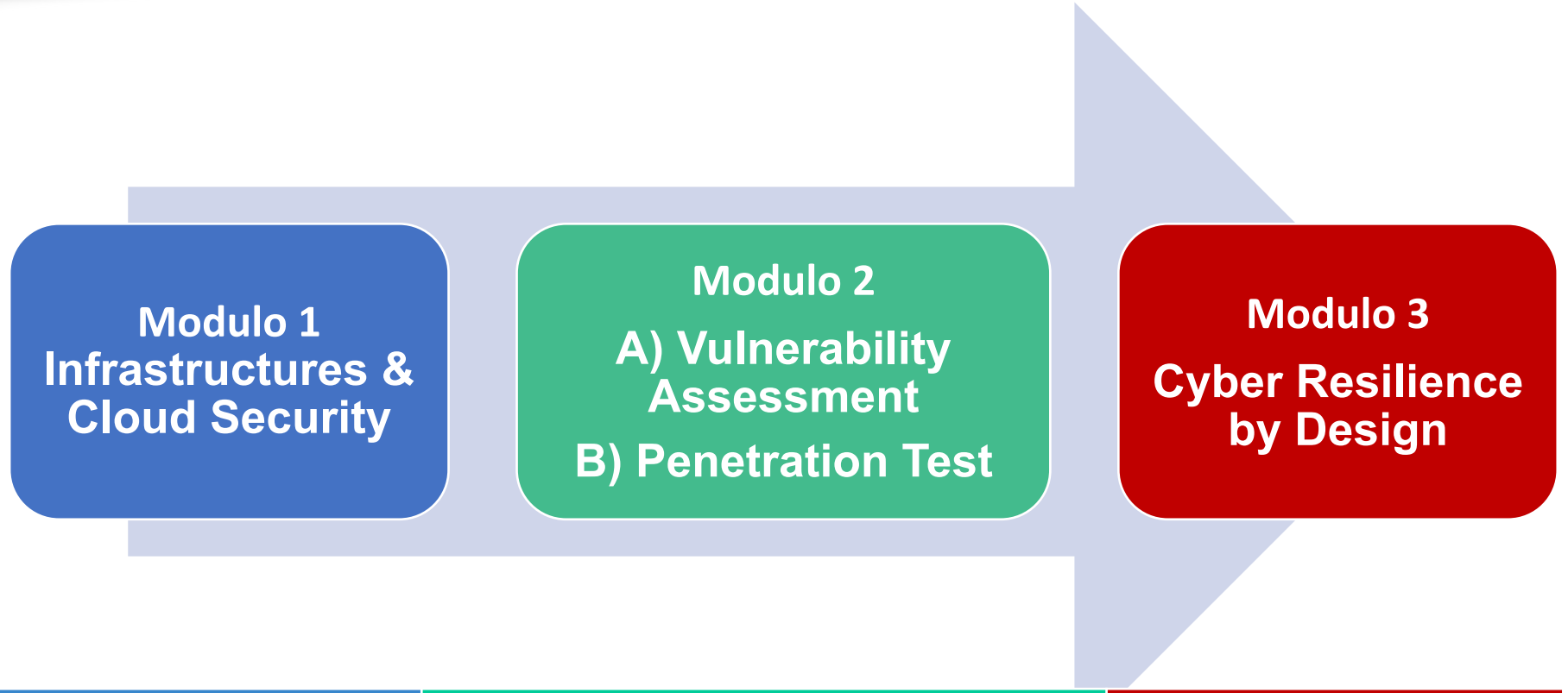
Aircraft

Cyber &
Security

Space

Aerostructures

Percorso formativo «*LDO-CYS Summer Course 2024*»



Giugno		Giugno/Luglio			Luglio	
2^ Sett.	3^ Sett.	4^ Sett.	1^ Sett.	2^ Sett.	3^ Sett.	4^ Sett.
3 gg x 5 h	2 gg x 5 h	3 gg x 5 h	3 gg x 4 h	2 gg x 4 h	3 gg x 5 h	3 gg x 5 h
25 ORE		35 ORE			30 ORE	

Modulo 1: Infrastructures & Security Cloud

(A. Busà, D. Roggero, P. D’Ambrosio)

Infrastructures & Cloud Security : obiettivi del Modulo

- Il Modulo di «Infrastructures & Security Cloud» ha lo scopo di rappresentare i principi fondamentali su cui si basano le infrastrutture Cloud, illustrando sia le fasi di progettazione che implementazione dell'ambiente Cloud. In tale ambito verranno esplorate le soluzioni di sicurezza applicate al cloud computing quale ad esempio «Confidential Computing».
- L'obiettivo è fornire le competenze base di:
  - Cloud computing e i servizi offerti dai CSP (Cloud Service Provider)
  - Implementazione e gestione delle risorse di base in Azure, come Macchine Virtuali, Risorse di Rete e Archiviazione
  - Concetti di sicurezza e affidabilità di una Piattaforma Cloud
  - Fondamenti di tecnologie correlate come DevOps e IaC (Infrastructure As Code)
- Il Modulo è organizzato in 5 argomenti per una durata complessiva di 25 ore distribuite su cinque giorni.

Infrastructures & Cloud Security [Totale 25 ore]

#	Argomento	Contenuti	Durata (h)	Data Inizio
1	**Introduzione Leonardo Divisione Cyber & Security** **Confidential Computing & Cloud**	**Overview Azienda Leonardo – Divisione Cyber & security:** • Chi siamo • Mission della divisione Cyber Security • Mercato • Network Accademico **Confidential Computing** • Cos'è e da dove nasce l'esigenza • Hyperscalers e Confidential Computing **Use Case – Polo Strategico Nazionale** • Strategia Cloud Italia • Polo Strategico Nazionale: principi e servizi offerti	3h (1 g)	TBD
2	**Secure Public Cloud**	**Approfondimento Servizio Secure Public Cloud e relativa architettura:** • Gestione delle chiavi • Governance Model • Soluzioni Hub & Spoke • Soluzione di Backup	4h (1 g)	TBD
3	**Confidential Computing & Cloud**	**Confidential Computing & Cloud – Requisiti e Tecnologie** • Tecnologie attualmente disponibili • Approfondimento su CYSEC - ArcaTrusted OS • Remote Attestation	4h (1 g)	TBD
4	**Automation & Provisioning**	• Azure DevOps • Infrastructure As Code & Scripting (SLZ Microsoft + Custom Leonardo) • Step di automazione che portano alla creazione di un tenant dell'SPC	5h (1 g)	TBD
5	**Azure Secure Public Cloud (Hands-on)**	**Sessione pratica di configurazione di servizi cloud utilizzando il portale Azure Cloud**: • Governance: Policy Dashboard, creazione/assegnazioni policy • Gestione utenze Cloud Native (EntraID) • Creazione Confidential VM (disk Encryption Set) • Creazione cluster RH Openshift Container Platform	9h (2 gg)	TBD

Modulo 2: Ethical Hacking

(P. Mantenuto, U. Mosca)

Ethical Hacking: obiettivi del Modulo

- **Il Modulo di «Ethical Haking» ha lo scopo di rappresentare le varie fasi del processo di hacking etico partendo dalle principali metodologie, per esplorare strumenti e tecniche comunemente utilizzati dagli ethical hacker per individuare e sfruttare vulnerabilità. L'approccio che si vuole adottare prevede la presentazione di esempi pratici e hands-on, attraverso esercizi e laboratori che consentano agli studenti di applicare le conoscenze acquisite in scenari realistici, ma controllati.**

- **L'obiettivo è fornire le competenze tecniche con riferimento a:**
  - **Servizi erogati da un SOC e come è strutturato**
  - **Servizi erogati da un Red Team e come è strutturato**
  - **Fasi di un Vulnerability Assessment**
  - **Analisi vulnerabilità**
  - **Principali framework di un Penetration Test**
  - **Payloads, moduli ausiliari, exploit e moduli di post exploitation**
  - **Penetration Test infrastrutturale e Applicativo (Web Application Penetration Test)**
  - **Produzione di report e presentazione dei risultati**

- Il Modulo è organizzato in 4 argomenti per una durata complessiva di 35 ore distribuite su sei giorni.

VA/PT [Totale 35 ore]

#	Argomento	Contenuti	Durata (h)	Data Inizio
1	**Introduzione**	**Cosa è un SOC**	5 (1 g)	TBD
		Cosa è un RedTeam		
2	**Vulnerability Assessment**	**Information gathering**	10 (2 gg)	TBD
		Scanning		
		Enumeration		
		Analisi delle vulnerabilità		
3	**Penetration Test**	**Metodologia e fasi di un PT**	16 (4 gg)	TBD
		Metasploit		
		Payloads, moduli ausiliari, moduli post exploitation		
		Password cracking		
		Attacchi alle web applications		
		Attacchi client side		
		Privilege escalation		
4	**Test Finale**	**Presentazione risultati PT**	4 (1 g)	TBD

Modulo 3: Cyber Resilience by Design

(E. Angelitti, F. Varriale)

CR by Design: obiettivi del Modulo

- Il Modulo ha lo scopo di far comprendere che il miglior modo per proteggere l'informazione o un sistema d'informazione è integrare la sicurezza e la cyber resilienza in tutto il ciclo di vita del prodotto/servizio/sistema.
- L'obiettivo è fornire le competenze necessarie a comprendere i principi di «cyber resilience by design» e ad avviare gli studenti laureandi ad un percorso nel mondo del lavoro in tema di sicurezza

- Il Modulo è organizzato in 5 Argomenti della durata complessiva di 30 ore distribuite su sette giorni.

- di **sei (6)** giorni per un totale di 30 ore nella 2^ e 3^ settimana di Luglio 2024
  - Il corso è indirizzato a studenti universitari con specializzazione informatica e di sicurezza, che abbiamo completato almeno il primo anno del 2° ciclo universitario (laurea magistrale)
  - Il corso sarà in italiano ma si consiglia la conoscenza della lingua inglese almeno di livello B2

CR by Design: Scheda del Corso (1/2)

#	Argomento	Contenuti	Durata (h)	Data Inizio
1	Modulo 1: Concetti base	• Introduzione al concetto di Security by Design • Considerare la sicurezza nel processo di sviluppo di prodotti e servizi • Panoramica delle linee guida e dei framework di Security by Design	2 (1° g)	Q2/2025
2	Modulo 2: Il Rischio di Sicurezza	• Cos'è il Rischio di sicurezza • Principi e fasi del Rischio di Sicurezza nel processo di sviluppo di prodotti e servizi • Panoramica sulle linee guida e standard del rischio di sicurezza • Il Threat Modeling • Definizione e gestione dei requisiti di sicurezza (Security Requirements Engineering, SRE) • Applicazione dei requisiti su sistemi complessi: definizione della superficie di attacco • Deviazioni e deroghe: relazione con l'analisi dei rischi e re-engineering	8 (1° e 2° gg)	Q2/2025

CR by Design: Scheda del Corso (2/2)

#	Argomento	Contenuti	Durata (h)	Data Inizio
3	Modulo 3 **Standard e progettazione sicura**	DevOps e DevSecOps Gestione dei cambi (Change Management) e della configurazione del prodotto (Configuration Management) Utilizzo di strumenti per la progettazione sicura Sicurezza e segregazione degli ambienti di progettazione, produzione e test Principi di certificazione e accreditamento	8	Q2/2025
4	Modulo 4 **Verifica di sicurezza e supply chain security**	Integrazione e Verifica della sicurezza: approccio generale Identificazione e gestione di eventuali vulnerabilità Processi di security auding interni e gestione della comunicazione Il ruolo della supply chain nel security by design Monitoraggio e controllo di sicurezza nelle fasi operative del prodotto o servizio Supporto al cliente: risposta agli incidenti di sicurezza e ripristino delle attività Sensibilizzazione e formazione (Awareness and Training)	8	Q2/2025
5	Modulo 5 **Esercitazione**	Esercitazioni di riepilogo	4	Q2/2025

Modulo di paretcipazione

https://forms.office.com/e/TyBzXitGAH

Leonardo "Cybersecurity Deep Dive" Summer course @ DIETI

Form di iscrizione al Summer Course sulla Cybersecurity **"LDO-CYS Summer Course 2024"** organizzato da Leonardo SPA in collaborazione con il DIETI

Hi, SIMON PIETRO. When you submit this form, the owner will see your name and email address.

* Required

1. Cognome e Nome *

Enter your answer

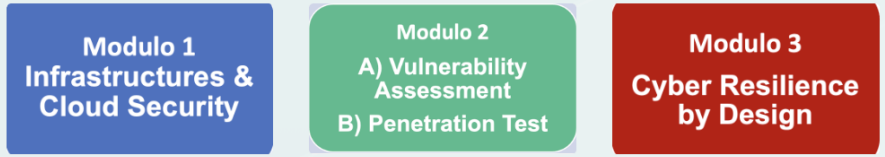
2. Corso di Laurea Magistrale al quale sei iscritto/a *

Enter your answer

3. Email *

Enter your answer

4. Indica i moduli ai quali sei interessato/a (**NB: almeno 2 su 3!**) *



- [ ] **Modulo 1**: *"Infrastructures & Cloud Security"*, **25** ore (**10/06-21/06**)
- [ ] **Modulo 2**: *"Vulnerability Assessment & Penetration Testing"*, **35** ore (**24/06-12/07**)
- [ ] **Modulo 3**: *"Cyber Resilience by Design"*, **30** ore (**15/07-26/07**)

Submit