Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**Organizzazione Aziendale**
Corso di studio	Laurea Magistrale in Sicurezza Informatica
Anno Accademico	2022/23
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	6 CFU
Settore Scientifico Disciplinare	SECS-P/08
Lingua di erogazione	Italiano
Anno di corso	primo
Periodo di erogazione	1° semestre, le date esatte sono riportate nel manifesto/regolamento
Obbligo di frequenza	La frequenza è fortemente raccomandata
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica

Docente/i

Nome e cognome	Vita Santa Barletta
Indirizzo mail	vita.barletta@uniba.it
Telefono	080-5443270
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Laboratorio SERLab, IV piano.
Sede virtuale	Piattaforma e-learning UNIBA - https://elearning.uniba.it/
Sito web del docente	https://serlab.di.uniba.it
Ricevimento (giorni, orari e modalità, es. su appuntamento)	(da confermare) Lunedì 14:00 – 15:00 (previo appuntamento)

Syllabus

Obiettivi formativi	L'insegnamento di Organizzazione Aziendale riguarda l'analisi e la gestione di un incidente di sicurezza per le organizzazioni, nonché processi metodi e tecniche per implementare controlli di sicurezza adeguati alla specifica organizzazione,

	identificare una vulnerabilità e gestire al contempo la difesa. Ciò include l'esecuzione di attività relative all'attacco (Red Team) e difesa (Blue Team), supportati da strumenti allo stato della pratica.
Prerequisiti	Prerequisiti definiti dal manifesto del corso di studi

Contenuti di insegnamento (Programma)	**Introduzione all'organizzazione aziendale**
	• L'organizzazione
	• Le principali teorie dell'organizzazione
	• Le variabili dell'organizzazione
	• Le strutture organizzative
	
	L'organizzazione, i processi e i ruoli
	• La progettazione organizzativa
	• I processi di impresa
	• I ruoli chiave
	• I sistemi di gestione di impresa
	
	Introduzione alla Sicurezza Informatica
	• Sicurezza Organizzativa
	• Sicurezza Applicativa
	• Sicurezza in Rete
	
	L'organizzazione per la sicurezza
	• Metodi di attacco
	• Tecniche di Difesa
	• Controlli di sicurezza
	• SOC: Security Operations center
	• CSIR T: Computer Security Incident Response T eam
	
	I processi per la Sicurezza
	• Processi SOC
	  ○ Incident analysis
	  ○ Security Information and Event Management
	  ○ Log Management
	  ○ Risk Management
	  ○ Vulnerability Management
	  ○ Controllo remoto delle workstation
	  ○ Analisi Forense
	  ○ Interfaccia all'Incident Analysis and Response
	  ○ Interfaccia al processo di Change Management
	• Processi CSIRT
	  ○ Incident triage
	  ○ Incident response
	  ○ Patch management
	  ○ Altri processi e funzioni del CSIRT
	
	I processi di controllo della Sicurezza
	• Verifica vulnerabilità
	• Protezione dei dati e Data Privacy
	• Altri controlli di sicurezza

Testi di riferimento	• ORGANIZZAZIONE AZIENDALE, 3ed 8838615284 · 9788838615283 di Giovanni Costa, Paolo Gubitta, Daniel Pittino. © 2015 | Data di Pubblicazione: 15 Dicembre 2015 • Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases: A condensed field guide for the Security Operations team (Volume 2). ISBN-13: 978-1726273985

	Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.
Note ai testi di riferimento	I testi di riferimento sono integrati con slide, dispense del docente e altro materiale didattico messi a disposizione degli studenti sulla piattaforma di e-learning usata dal CdS.

Organizzazione della didattica

Ore			
Totali	Didattica frontale	Esercitazione guidate + Progetto	Studio individuale
150 ore	48 ore		102 ore
CFU/ETCS			
6 CFU	6 CFU		

Metodi didattici

- Lezioni frontali con l'ausilio di slide che riportano esempi per illustrare gli argomenti trattati.
- Esercitazioni pratiche sull'utilizzo dei vari principi e tecniche presentate a lezione.
- Ricevimento e approfondimento tecnico.

Risultati di apprendimento previsti

Conoscenza e capacità di comprensione

- Lo studente deve conoscere le principali strutture organizzative aziendali e saper correttamente collocare in esse i processi connessi ad un SOC e CSIRT.
- Lo studente acquisisce tale conoscenza sia attraverso le lezioni frontali e la partecipazione a seminari tematici erogati durante il corso, sia attraverso esercitazioni che gli consente di mettere in pratica e verificare quanto appreso, acquisendo così consapevolezza della capacità di comprensione e di come migliorare l'applicazione delle tecniche apprese.

Conoscenza e capacità di comprensione applicate

- Lo studente deve saper definire ed organizzare i processi ed i servizi dell'impresa nella direzione della difesa e protezione delle proprie reti ed informazioni.
- Lo studente deve saper definire e strutturare operativamente il SOC ed il CSIRT.

Competenze trasversali

Autonomia di giudizio

- Lo studente deve saper formulare giudizi autonomi e fare valutazioni circa l'organizzazione dei processi connessi alla sicurezza di una impresa.

	• Lo studente deve saper valutare e giudicare soluzioni volte al miglioramento della sicurezza dell'organizzazione e dei suoi processi e servizi. **Abilità comunicative** • Lo studente deve saper esporre, comunicare ed esprimere in modo chiaro ed efficace le conoscenze apprese, presentare i casi applicativi e d esempi illustrativi. • Lo studente deve saper discutere le soluzioni adottate inerenti la sicurezza dell'organizzazione. • Lo studente deve saper redigere elaborati scritti chiari, sintetici e coerenti. • Lo studente deve saper comunicare con le diverse professionalità operanti in un SOC e un CSIRT. **Capacità di apprendere in modo autonomo** • Lo studente deve dimostrare attraverso lo svolgimento di piccoli esercizi pratici di saper elaborare soluzioni a problemi connessi all'organizzazione della sicurezza in una impresa. • Lo studente deve sapere elaborare e organizzare idee e soluzioni a problemi organizzativi connessi alla sicurezza.

Valutazione	
Modalità di verifica dell'apprendimento	La verifica dei risultati formativi raggiunti avviene durante l'esame finale, che prevede: • Un colloquio orale in cui si presenta e si discute il progetto sviluppato in gruppo e si verificano le competenze acquisite durante il corso e le capacità espositive dello studente. Per gli studenti frequentanti sono previste le seguenti facilitazioni: • Bonus punteggio a valere sulla valutazione del progetto per gli studenti che svolgono positivamente le esercitazioni sul progetto/caso di studio.
Criteri di valutazione	**Conoscenza e capacità di comprensione** • Conoscenze e competenze relative ai principali aspetti di organizzazione aziendale orientati alla sicurezza, ai processi di divisione e coordinamento del lavoro in un SOC (Security Operations Center) e CSIRT (Computer Security Incident Response Team) e all'organizzazione dei processi per la sicurezza dell'infrastruttura. **Conoscenza e capacità di comprensione applicate** • Saper definire ed organizzare i processi ed i servizi dell'impresa nella direzione della difesa e protezione delle proprie reti ed informazioni per poter garantire la business continuity di una organizzazione e renderla capace di rilevare attacchi di natura cibernetica e preservare, o ripristinare quando necessario, i servizi eventualmente coinvolti e danneggiati. **Autonomia di giudizio** • Capacità di formulare giudizi autonomi, nonché di esprimere valutazioni collegiali con riferimento alle politiche gestionali e scelte tecnico-progettuali degli enti nei quali potrà operare e sempre con riferimento agli aspetti connessi alla sicurezza. • Capacità di proporre, valutare e giudicare soluzioni volte al miglioramento della sicurezza dell'organizzazione e dei suoi processi e servizi **Abilità comunicative**

<table>
<tr><td></td><td>

Comunicare ed esprimere verbalmente in modo chiaro ed efficace le conoscenze apprese, presentare i casi applicativi ed esempi illustrativi.
Discutere le soluzioni adottate adeguando il contenuto al target professionale. Redigere elaborati scritti chiari, sintetici e coerenti. Lavorare in team con diverse professionalità.

Capacità di apprendere

Individuare, elaborare e organizzare informazioni appropriate per soluzioni di problemi connessi all’organizzazione della sicurezza in una impresa. Elaborare e organizzare idee e soluzioni a problemi organizzativi connessi alla sicurezza in modo critico e sistematico.

</td></tr>
<tr><td>Criteri di misurazione dell'apprendimento e di attribuzione del voto finale</td><td>
<table>
<tr><th>Voto</th><th>Descrittori</th></tr>
<tr><td>< 18 insufficiente</td><td>Conoscenze frammentarie e superficiali dei contenuti, errori nell’applicare i concetti, descrizione carente.</td></tr>
<tr><td>18 - 20</td><td>Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell’applicazione di concetti teorici.</td></tr>
<tr><td>21 - 23</td><td>Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice.</td></tr>
<tr><td>24 - 25</td><td>Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato.</td></tr>
<tr><td>26 - 27</td><td>Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta.</td></tr>
<tr><td>28 - 29</td><td>Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta.</td></tr>
<tr><td>30
30 e lode</td><td>Conoscenze dei contenuti molto ampie, complete ed approfondite, capacità ben consolidata di applicare i contenuti, ottima capacità di analisi, di sintesi e di collegamenti interdisciplinari, padronanza di descrizione.</td></tr>
</table>
</td></tr>
<tr><td>Altro</td><td>
Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:

https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea
https://www.uniba.it/it/ricerca/dipartimenti/informatica
https://elearning.uniba.it/

I programmi degli insegnamenti sono disponibili qui:

https://elearning.uniba.it/

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito:

https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non
</td></tr>
</table>

corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

- Link al corso sulla piattaforma e-learning: https://elearning.uniba.it/course/view.php?id=1786