Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**Organizzazione Aziendale**
Corso di studio	Laurea Magistrale in Sicurezza Informatica
Anno Accademico	2023/24
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.
- Utilizzo della piattaforma di e-learning del Dipartimento di Informatica per la distribuzione del materiale e per le interazioni tra docenti e studenti durante e dopo il corso.

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

- 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.

Criteri di misurazione dell'apprendimento e di attribuzione del voto finale

Voto	Descrittori
< 18 insufficiente	Conoscenze frammentarie e superficiali dei contenuti, errori nell'applicare i concetti, descrizione carente.
18 - 20	Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell'applicazione di concetti teorici.
21 - 23	Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice.
24 - 25	Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato.
26 - 27	Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta.
28 - 29	Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta.
30 30 e lode	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.

Altro

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 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=2061

Main information on the course

Course name	**Business Organization**	
Degree	Master Degree in Computer Science	
Academic year	2023/24	
European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU)	6 CFU	
Settore Scientifico Disciplinare	SECS-P/08	
Course language	Italian	
Course year	First	
Course period	First Semester - exact dates can be found in the didactic regulations	
Course attendance requirement	None, but it is highly recommended to attend classes	
Website of the Degree	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica	

Teacher(s)

Name and Surname	Vita Santa Barletta
email	vita.barletta@uniba.it
phone	080-5443270
office	Department of Computer Science, Via Orabona 4, 70125 Bari. Laboratory SERLab, 4th floor
e-learning platform	E-LEARNING Platform - https://elearning.uniba.it/
Teacher's homepage	https://serlab.di.uniba.it
Office hours	(To be confirmed) Monday 14:00 – 15:00 (by appointment)

Syllabus

Course goals	The Business Organization course covers the analysis and management of a security incident for organizations, as well as processes methods and techniques for implementing security controls appropriate to the specific organization, identifying a vulnerability while managing the defense. This includes performing activities related to attack (Red Team) and defense (Blue Team), supported by state-of-the-art tools.
Prerequisites/requirements	Prerequisites defined by the course manifesto.
Course program	**Introduction to Business Organization** - Organization - The main theories of organization - The variables of organization - The organizational structures **The organization, processes and roles** - Organizational design - Business processes - The key roles - Enterprise management systems **Introduction to Information Security** - Organizational Security

	- Application Security
	- Network Security
	
	The Security Organization
	- Methods of Attack
	- Defense Techniques
	- Security Controls
	- SOC: Security Operations Center
	- CSIRT: Computer Security Incident Response Team Network Security
	
	Processes for Security
	- SOC Processes
	  ○ Incident analysis
	  ○ Security Information and Event Management
	  ○ Log Management
	  ○ Risk Management
	  ○ Vulnerability Management
	  ○ Remote control of workstations
	  ○ Forensic Analysis
	  ○ Interface to Incident Analysis and Response
	  ○ Interface to the Change Management process
	- CSIRT Processes
	  ○ Incident triage
	  ○ Incident response
	  ○ Patch management
	  ○ Other CSIRT processes and functions
	
	Security control processes
	- Vulnerability testing
	- Data protection and data privacy
	- Other security controls

Books of reference	• 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 Students can borrow these texts from the library. It is advisable to check availability through the University Library System (https://opac.uniba.it/easyweb/w8018/index.php?) and contact the library for lending.
Notes to the books	The reference texts are supplemented with slides, teacher's notes, and other teaching materials made available to students on the e-learning platform used by the degree program.

Organization of the didactic activities

Hours				
Total	Lectures	Practice sessions	Project work	Individual study
150 hours	48 hours			102 hours
CFU/ETCS				
6 CFU	6 CFU			

Teaching methods	
	• Lectures with the aid of slides illustrating the discussed topics with examples. • Practical exercises on using the various principles and techniques presented during the lectures through individual exercises. • In-depth technical study. • Use of the Department of Computer Science's e-learning platform for distributing materials and facilitating interactions between teachers and students during and after the course.

Expected learning outcomes	
Knowledge and understanding	• Students must know the main business organizational structures and be able to correctly place the processes associated with a SOC and CSIRT within them. • Students acquire this knowledge through lectures and thematic seminars during the course and through practical exercises that allow them to practice and verify what they have learned, gaining awareness of their understanding and how to improve the application of learned techniques.
Applying knowledge and understanding	• Student must know how to define and organize the processes and services of the enterprise in the direction of defending and protecting its networks and information. • Student must know how to define and operationally structure the SOC and CSIRT.
Other skills	*Making judgements* • The student must be able to make independent judgments and make assessments about the organization of processes related to the security of an enterprise. • The student must be able to evaluate and judge solutions aimed at improving the security of the organization and its processes and services. *Communication* • The student must be able to clearly express the knowledge learned, present application cases and illustrative examples. • The student must be able to discuss the solutions adopted inherent to the security of the organization. • The student must be able to write clear, concise and coherent written papers. • The student must be able to communicate with the various professionals working in a SOC and a CSIRT. *Learning skills* • The student must demonstrate through the execution of practical exercises that he/she can work out solutions to problems related to the security organization in an enterprise. • The student must know how to develop and organize ideas and solutions to organizational problems related to security.

Assessment	

<table>
<tr><td>Assessment methods</td><td>The assessment of the achieved learning outcomes occurs during the final exam, which includes:
An oral interview presenting and discussing the group-developed project, verifying the knowledge acquired during the course and the student's presentation skills.
For attending students, the following benefits are provided:
Score bonus for the project evaluation for students who positively complete the project/case study exercises.</td></tr>
<tr><td>Evaluation criteria</td><td>Knowledge and Understanding
The student must be knowledgeable about the main aspects of security-oriented business organization, the processes of division and coordination of work in a SOC (Security Operations Center) and CSIRT (Computer Security Incident Response Team), and the organization of processes for infrastructure security.
Applied Knowledge and Understanding
The student must know how to define and organize the processes and services of the enterprise in the direction of defending and protecting its networks and information. The goal is to guarantee the business continuity of an organization and make it capable of detecting cyberattacks and preserving, or restoring when necessary, services that may be involved and damaged.
Autonomy of Judgment
Ability to make independent judgments as well as evaluations with reference to the management policies and technical and design choices of the entities in which he/she may work and always with reference to security-related aspects.
Ability to propose, evaluate and judge solutions aimed at improving the security of the organization and its processes and services.
Communication Skills
Explain clearly and effectively the knowledge learned, present application cases and illustrative examples.
Discuss solutions adopted by adapting the content to the professional target audience. Produce clear documentation. Work in teams with diverse professional backgrounds.
Learning Ability
Identify, process and organize appropriate information for problems solutions related to security organization in an enterprise. Develop and organize ideas and solutions to safety-related organizational problems critically and systematically.</td></tr>
<tr><td>Measurements and final grade</td><td><table><tr><th>Grade</th><th>Descriptors</th></tr><tr><td>< 18
insufficient</td><td>Fragmentary and superficial content knowledge, errors in applying concepts, poor description.</td></tr><tr><td>18-20</td><td>Sufficient but general content knowledge, simple description, uncertainties in applying theoretical concepts.</td></tr><tr><td>21-23</td><td>Appropriate but not deep content knowledge, ability to apply theoretical concepts, ability to present content simply.</td></tr><tr><td>24-25</td><td>Appropriate and broad content knowledge, fair ability to apply knowledge, ability to present content articulately.</td></tr><tr><td>26-27</td><td>Precise and complete content knowledge, good ability to apply knowledge, clear and correct description.</td></tr></table></td></tr>
</table>

	28-29	Broad, complete, and deep content knowledge, good content application, good analysis and synthesis ability, confident and correct description.
	30 30 e lode	Very broad, complete, and deep content knowledge, well-established content application ability, excellent analysis, synthesis, and interdisciplinary connections, mastery of description.

Further information

Students are advised to rely exclusively on information/communications provided on the official websites of the Department of Computer Science or on social groups only if formed and administered exclusively by the lecturers of the related courses:

- 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/

The course programs are available here:

- https://elearning.uniba.it/

The information that all students should know is written in the Teaching Regulations and study posters available on the site:

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

Students are advised to be cautious of information and materials circulating on unofficial sites or social groups as they are often unreliable, incorrect, or incomplete. For any doubts, request a meeting with the instructor according to the office hour arrangements.

Link to the course on the e-learning platform of the University E-Learning Center:

- https://elearning.uniba.it/course/view.php?id=2061