

10. Tecnologie dell'informazione, della comunicazione e dei dati
10.2 Architetture e Sistemi
10.2.2 Tecnico superiore System Cybersecurity
- Cyber Security Specialist -
Biennio 2026/2028

Fasi / Unità Formative / Argomenti / Saperi	Ore	Descrizione UF
COMPETENZE TRASVERSALI		
Approfondimenti didattici e Orientamento		
Avvio corso		
Avvio prima annualità, accoglienza gruppo-classe		
La Fondazione ITS Academy ICT		
Strumenti didattici della Fondazione		
Rapporto con gli uffici e modalità		
Gestione del piano lezioni	**16**	Lo scopo dell'Unità Formativa è supportare gli studenti durante tutto il percorso formativo: dalla fase iniziale di accoglienza, al monitoraggio, organizzato con appuntamenti a cadenza regolare in itinere durante tutto il biennio formativo, al fine di verificare l'avanzamento della didattica e la gestione di eventuali criticità, fino al termine del percorso, con una simulazione di prova d'esame. Parte delle ore sarà dedicata a orientare gli studenti rispetto alla Fondazione ITS Academy ICT stessa, rendendoli consapevoli di tutti gli strumenti e opportunità che offre loro, inclusa la strutturazione degli uffici e la gestione del piano lezioni.
Scelta Rappresentanti di Classe		
Monitoraggio corso		
Monitoraggio avanzamento della didattica		
Gestione eventuali criticità		
Simulazione prova esame		
Simulazione prova scritta esame finale		
Governance, Risk and Compliance (GRC)		
IT & Cyber Security Governance		
Definizione di Governance (Modelli organizzativi, ruoli (CISO, DPO, CIO) e responsabilità aziendali).		
Struttura e applicazione dei framework COBIT, NIST Cyber Security Framework (CSF) e ISO/IEC 27001.		
Redazione di procedure, linee guida e politiche di sicurezza (es. password policy, data retention).		
Indicatori chiave di prestazione (KPI) e di rischio (KRI) per misurare l'efficacia della sicurezza.		
Risk Management (Gestione del Rischio)		
Introduzione alle metodologie di Risk Assessment (Standard ISO 31000, ISO/IEC 27005 e NIST SP 800-30).		
Classificazione e inventario dei beni aziendali (hardware, software, dati).		
Calcolo del rischio intrinseco e residuo (Probabilità x Impatto), approcci qualitativi e quantitativi.		
Strategie di mitigazione, trasferimento (assicurazioni cyber), accettazione o evitamento.		
Piani di continuità operativa (BCP) e Disaster Recovery (DRP), analisi dell'impatto sul business (BIA).		
Information Compliance (Conformità Normativa)		
Normative di Settore (Standard PCI-DSS (pagamenti elettronici), Direttiva NIS 2 (infrastrutture critiche) e Regolamento DORA (settore finanziario)).		
Responsabilità Giuridica: Cenni al D.Lgs. 231/01 (responsabilità amministrativa d'impresa) e reati informatici.		
Tutela dei dati personali – le leggi dell'information security – i reati informatici	**50**	Questa Unita Formativa analizza la sicurezza informatica da una prospettiva strategica, organizzativa e normativa. Gli studenti imparano a tradurre gli obiettivi di business in politiche di sicurezza stabili, valutando l'impatto dei rischi e garantendo il rispetto delle leggi vigenti. Lo scopo è quello di fornire le competenze necessarie per allineare la sicurezza IT alle strategie aziendali. Il corso abilita lo studente a mappare i processi organizzativi, identificare le minacce normative e implementare framework di controllo per proteggere il patrimonio informativo aziendale. Durante questa unità formativa verranno inoltre fornite le nozioni base di diritto d'autore, dei brevetti, dei marchi, della privacy e delle comunicazioni applicate alle reti digitali. Verranno supportati gli studenti nella fase di comprensione dei termini giuridici dei dibattiti in corso in materia di riforma del diritto applicato alle reti digitali e dei rischi connessi all'uso e condivisione di materiale e contenuti sul web e nelle varie fasi del compravendita on-line.
Normativa in materia di dati personali - il Reg. UE 679/2016 (GDPR) e la normativa italiana		
Comprensione e redazione delle informative privacy		
Policy aziendali di tutela dei dati personali.		
Data breach		
Privacy by design e by default		
Decreto 70/2003, e-commerce e ISPs		
Direttiva NIS e la sua implementazione italiana		
Reati informatici		
Proprietà industriale e intellettuale		
Diritto d'autore		
Tutela del software		
Licenza del software e software as a service		
Comprensione dei termini delle licenze e l'impatto sulla sicurezza dei prodotti informatici		
Open Source, licenze libere e garanzie degli sviluppatori		
Contratti per reti, servizi e sistemi informatici		
Fornitura di servizi, IAAS-SAAS, consulenza informatica, distribuzione software e hardware		
SLA e requisiti tecnici dei contratti		
Data processing agreements e obblighi in caso di incidenti informatici		
Blockchain e smart contracts		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
Inglese		
Grammatica		
Percorso di miglioramento personalizzato		
Alternanza dei tempi verbali		
Grammatica come uso vs Grammatica come regole		
Conversazione		
Crowdfunding settoriale		
Panoramica tecnica globale		
Rapporti su incidenti e procedure		
Descrizioni funzionali e operative		
Processi e sistemi	**72**	L'Unità Formativa Inglese ha l'obiettivo di trasmettere allo studente una competenza linguistica di livello B2 (detto anche post intermedio), finalizzata al conseguimento del First Certificate in English (FCE). In conformità a quanto prescritto dal Quadro Comune di Riferimento Europeo stabilito dal Consiglio d'Europa, il livello B2 corrisponde ad una conoscenza specifica di strutture sintattico-grammaticali, fonetica avanzata, vocabolario adeguato per esprimersi nelle situazioni di vita quotidiana e lavorativa, competenze avanzate di lettura, ascolto e comprensione sulla base di supporti audiovisivi e multimediali. Inoltre in relazione al percorso di studi e alla futura professione, si studierà la terminologia tecnica riferita al futuro settore professionale.
Interpretazione di testi e dati tecnici		
Linguaggio digitale		
Colloquio di lavoro (CV e profilo LinkedIn)		
Terminologia tecnica in lingua inglese		
Vocabolario settoriale		
Comprensione di termini e conversazioni specifici del settore		
Gergo professionale		
Valutazione		
Valutazione intermedia		
Valutazione finale		
Orientamento al lavoro		
Tematiche e orientamenti ambientali previsti a livello UE, nazionale, regionale e locale		
Rifiuti e risorse materiali		
Neutralità climatica		
Ambiente e salute		
Idrogeno e mobilità elettrica		
Il Green Deal europeo e le strategie UE ad esso correlate		
Vulnerabilità degli ambienti naturali		
Cambiamenti climatici e impatto sui territori		
Biodiversità		
Tecniche di ricerca delle informazioni negli ambienti digitali		
Tecniche e strumenti finalizzati all'avvio di una ricerca efficace di un potenziale candidato in risposta a una job description aziendale		
Elementi di cittadinanza digitale		
Elementi chiave della Carta della cittadinanza digitale		
Concetti di sicurezza, trattamento dell'identità digitale		
Formazione sui diritti/doveri dell'utente e la comunità di utenti in correlazione all'impatto delle azioni on-line e off-line		
Disposizioni aziendali in materia di privacy		
Elementi di base del Regolamento Generale Sulla Protezione Dei Dati – RGPD o GDPR da osservare in un contesto organizzativo aziendale		
Le caratteristiche personali		
acquisire e consolidare fiducia in se stessi e consapevolezza		
esplorare ad ampio raggio le esperienze dei partecipanti		
analizzare il proprio presente di vita e lavorativo		L'unità formativa Orientamento intende proporre attività per lo sviluppo dell'autonomia di obiettivi personali e sociali degli studenti con la progressiva maturazione delle competenze necessarie per governare le scelte connesse alle transizioni formative e lavorative. Per una preparazione completa, oltre alla competenza tecnica e professionale, acquisibile durante il biennio, lo studente necessita di acquisire competenze personali, capacità cognitive, relazionali, manageriali, attitudini al lavoro e comprensione

apprendere definizione e proprietà delle competenze: sapere, saper fare, saper essere		della figura professionale. L'Unità formativa proporrà attività formative dall'inizio del percorso di studi fino al termine dello stage curriculare. Gli obiettivi che si intendono perseguire con le azioni di orientamento sono i seguenti: - Accoglienza e orientamento al percorso formativo professionale - Rilevazione del livello delle soft skills dell'allievo - Potenziamento delle competenze - Favorire lo sviluppo di capacità progettuali e di scelta consapevole negli studenti - Sostenere il processo di costruzione del progetto professionale individuale - Orientamento all'organizzazione e al ruolo professionale - Facilitare l'inserimento lavorativo - Orientamento al mercato del lavoro, ai servizi per l'incontro Domanda/Offerta, alla ricerca attiva del lavoro Tramite attività propedeutiche utilizzate per analizzare e potenziare le soft skills e i profili di personalità, giochi di ruolo, ore in piccolo gruppo e attività individuali e laboratoriali si cercherà di sostenere e garantire l'efficacia del percorso formativo, monitorando l'andamento sia dell'individuo sia del gruppo classe. Durante l'UF si lavorerà sullo sviluppo del profilo professionale e delle capacità e competenze relazionali degli studenti in aula. Saranno organizzate delle attività sui profili di personalità (estroversione-introversione, gradevolezza-sgradevolezza, coscienziosità-negligenza, nevroticismo-stabilità emotiva, apertura-chiusura mentale). L'esperienza formativa nasce dall'idea di utilizzare specifiche metodologie per lavorare in gruppo al fine di migliorare la capacità degli studenti a lavorare in team (team working) e di conseguenza migliorare i risultati conseguiti dal team di lavoro e creare un clima positivo utile anche a evitare la dispersione scolastica. Saranno organizzate attività ludiche, formative ed esperienziali le quali serviranno per costruire un gruppo di lavoro affiatato, creare relazione, incrementare la collaborazione, aumentare il livello di fiducia nei compagni, motivare il gruppo di lavoro e creare coesione e integrazione. Tali attività possono facilitare la comunicazione, stimolare la creatività, far emergere la leadership, educare alla delega e al lavoro per obiettivi, sviluppare l'empatia e l'ascolto, veicolare vision, mission e valori aziendali, valutare il potenziale e le attitudini, avvicinare management e personale operativo. Per la peculiarità dell'Unità Formativa vengono inserite qui le misure di accompagnamento dedicate alle azioni di riallineamento delle competenze, al riconoscimento dei crediti, alla sperimentazione nei percorsi formativi di alta formazione in apprendistato e alla flessibilità degli orari per adulti occupati. Queste misure saranno sviluppate comunque trasversalmente durante tutto il percorso a seconda delle necessità riscontrate. Inoltre, con riferimento al settore professionale d'appartenenza, verranno affrontati i valori di base della parità di trattamento e della lotta alla discriminazione nella vita sociale e nel mercato del lavoro. In questa unità formativa saranno sviluppate le conoscenze essenziali "Tematiche e orientamenti ambientali previsti a livello UE, nazionale, regionale e locale" per la durata di un'ora e "Vulnerabilità degli ambienti naturali" per la durata di due ore relative all'Obiettivo "Contribuire allo sviluppo sostenibile e alla difesa dell'ambiente. Verranno inoltre affrontate le conoscenze essenziali "Tecniche di ricerca delle informazioni negli ambienti digitali", "Elementi di cittadinanza digitale", "Concetti di sicurezza, trattamento dell'identità digitale" e "Disposizioni aziendali in materia di privacy" relative all'Obiettivo "Competenze digitali trasversali"
identificare le competenze possedute, anche quelle tacite o inespresse o da potenziare		
sapere individuare, riconoscere, descrivere le proprie conoscenze, capacità, abilità e competenze		
monitorare la propria esperienza (formativa e non), la propria evoluzione, crescita, cambiamento, durante tutto l'arco del percorso		
aumentare e consolidare in itinere le acquisizioni e gli apprendimenti in via di sviluppo		
condividere e valorizzare gli apprendimenti acquisiti e sviluppati nell'intero arco del corso		
favorire autonomia attraverso una piena presa in carico da parte dei partecipanti del proprio apprendimento successivo al termine del corso		
Il contesto di riferimento del percorso formativo		
aprire le attività del corso/percorso formativo (obiettivi, contenuti, modalità, metodologie, regole, vincoli etc. per la partecipazione)		
conoscere e valorizzare le opportunità offerte dal percorso e dalla struttura proponente (presentazione del gruppo dei partecipanti, conoscenza reciproca dei partecipanti, stipula patto formativo)		
motivare all'apprendimento e riflettere sull'apprendere (apprendiamo ad apprendere)		
riflettere sul proprio stile di apprendimento (come apprendo, che cosa, cosa mi fa paura, cosa mi aiuta, cosa voglio portare, cosa vorrei trovare)		
riconoscere il ruolo dell'apprendimento nella propria vita professionale		
creare buone relazioni con lo staff docente e con i compagni di corso		
costituire le premesse per un buon apprendimento individuale e collettivo		
costituire il gruppo di/in apprendimento		
imparare a utilizzare il gruppo come moltiplicatore dell'apprendimento, come opportunità di scambio e confronto, come luogo di sinergie per la propria crescita professionale	**20**	
sviluppare capacità personali insieme agli altri, con/sul gruppo e sul benessere organizzativo, per lo sviluppo delle capacità relazionali, sociali e professionali		
acquisire e consolidare capacità e competenze di comprensione, osservazione, lettura e relazione con e nelle diverse realtà organizzative in cui le persone opereranno nelle loro future esperienze professionali e di vita lavorativa		
sviluppare conoscenza e capacità di agire in organizzazioni moderne nelle loro diverse taglie, misure e contesti (impresa artigianale, piccolissime, piccole e medie imprese e/o società di servizi, grandi imprese italiane e multinazionali)		
chiudere le attività e prendere commiato dai compagni d'esperienza e dallo staff		
Definizione e valutazione dei propri progetti: personale e professionale		
preparazione allo stage		
predisposizione di strumenti e attenzioni utili a valorizzare e potenziare l'opportunità di sperimentarsi in un contesto lavorativo reale (diario di stage etc.)		
analisi della domanda delle aziende/imprese		
approfondire la domanda di lavoro del territorio - scenari e opportunità per valorizzare l'offerta di lavoro dei partecipanti		
mettere a fuoco gli strumenti offerti dal territorio per valorizzare, promuovere e divulgare la candidatura dei partecipanti nel mercato del lavoro - i servizi per l'impiego, ruolo delle strutture pubbliche e private per il lavoro e servizi offerti ai cittadini, Garanzia Giovani		
cosa vorrei essere (il cv immaginario) per far emergere le proprie potenzialità e le possibilità ("I have a dream")		
cosa posso essere (il CV - I can do)		
sviluppare la conoscenza e l'utilizzo delle principali tecniche utilizzabili nella ricerca del lavoro		
approfondire la ricerca delle informazioni e l'analisi del mercato del lavoro		
scrivere lettere di presentazione o/e risposta alle inserzioni di lavoro		
come scrivere un curriculum vitae		
prepararsi a sostenere un colloquio con un datore di lavoro		
definire progetti coerenti alle proprie aspettative/desideri, realistici e adeguati al proprio profilo professionale e alle proprie potenzialità		
elaborare un piano di azione individuale		
Valorizzazione dei propri progetti: personale e professionale		
identificare i principali desideri dei partecipanti		
ricostruire le motivazioni e gli elementi di fondo di tali desideri/stimoli/aspettative		
riconoscere e appropriarsi delle potenzialità personali collegate a tali desideri/stimoli/aspettative		
implementare e consolidare capacità e competenze di sense-making organizzativo, di motivazione e stimolo personale e professionale nelle organizzazioni moderne, di orientamento agli obiettivi specifici di ruolo e/o di funzione org. e di bilanciamento con gli obiettivi generali dell'organizzazione stessa, di visione sistemica e di relazione funzionale nelle organizzazioni del nostro tempo		
approfondire la definizione di organizzazione, la sua natura e i suoi paradossi; input, elaborazione/trasformazione output e ciclo aziendale; il sistema impresa e le sue componenti/variabili; strategia, strutture e meccanismi org.		
acquisire conoscenze e competenze di base sul ruolo organizzativo: definizione, aree, obiettivi, funzionalità e relazioni; area prescritta, discrezionale, innovativa; relazioni gerarchiche e funzionali		
sviluppare capacità di condivisione, collaborazione, orientamento agli obiettivi, raggiungimento dei risultati, nel lavoro in staff/team/squadra/gruppo nei contesti organizzativi		
matching tra le competenze personali e professionali raggiunte dallo studente con le posizioni aperte dalle aziende		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
Parità fra uomini e donne e non discriminazione		
Interculturalità e Pari Opportunità		Le tematiche riferite alla parità fra uomini e donne e non discriminazione vengono trattate sia in questa U.F. dedicata, sia in modo trasversale in tutto il percorso formativo. Con riferimento al settore professionale d'appartenenza, al fine di diffondere i valori di base della parità di trattamento e della lotta alla discriminazione nella vita sociale e nel mercato del lavoro, si esamineranno in un'ottica di parità per tutti: - modalità per il riconoscimento e la valorizzazione delle competenze che tutti, indipendentemente da genere, origine etnica, religione o credo, disabilità, età o orientamento sessuale possono fornire al mercato del lavoro; - presenza femminile e maschile; - ruoli/funzioni/differenze salariali e progressione di carriera; - problematiche collegate all'integrazione e alla coesione di diversi gruppi sociali in ambito lavorativo (giovani-anziani, immigrati-nativi, etc); - ambiente e clima di lavoro; - prevenzione e salute. Per ciò che riguarda i destinatari del percorso, partendo dalla loro esperienza lavorativa e/o di vita, si privilegerà la trattazione degli aspetti relativi a: - le dinamiche relazionali in un'ottica di parità fra uomini e donne e non discriminazione sul lavoro e nella formazione; - segregazione orizzontale e verticale ed altre forme di discriminazione nel mercato del lavoro. All'interno di questa unità formativa verranno in particolare trattati i seguenti argomenti: - principi fondamentali delle pari opportunità; - parità di genere: -Strumenti di conciliazione-Condivisione delle responsabilità; - valorizzazione e armonizzazione delle differenze: età, orientamento sessuale ed identità di genere, religione, razza ed etnia, disabilità; - identità, stereotipi e adeguamento del linguaggio; - elementi normativi e Istituzioni di parità. Le tematiche relative alla parità fra uomini e donne e non discriminazione verranno svolte trasversalmente nelle seguenti unità formative dedicate all'Orientamento al lavoro, alla Sicurezza sul lavoro, Parità fra uomini e donne e non discriminazione, Learning by Project - Soft Skill, Learning by Project - Tech e Laboratorio integrato. Inoltre, in questa U.F. verrà applicata la metodologia del "Social Hub" che consentirà agli allievi di condividere saperi, informazioni e domande e i docenti potranno utilizzare questa risorsa per condividere materiale, esercitazioni e informazioni.
Origine della distinzione di genere. Affermazione del concetto di pari opportunità.		
Le dinamiche del panorama legislativo comunitario in materia di Pari Opportunità.		
Principi fondamentali delle Pari Opportunità.		
Parità di genere: -Strumenti di conciliazione -Condivisione delle responsabilità		
Valorizzazione ed armonizzazione delle differenze: età, orientamento sessuale ed identità di genere, religione, razza ed etnia, disabilità.		
Identità, stereotipi e adeguamento del linguaggio.		
Elementi normativi e Istituzioni di parità.		
Il sostegno della donna come soggetto di diritto privato, come studente e come madre.		
Cenni del panorama legislativo italiano, strumenti e attori: gli organismi di parità, i consiglieri di Parità, L.125/91.		
La disciplina giuridica del rapporto di lavoro e dell'attività sindacale, finalizzata all'acquisizione di una maggiore consapevolezza del contenuto del contratto di lavoro subordinato in particolare tenendo in considerazione l'appartenenza ad un sesso piuttosto che ad un altro.		
Le esperienze maturate all'interno delle azioni positive promosse dall'Unione Europea (ad esempio progetti NOW) attraverso la diffusione delle BUONE PRASSI.		
La legislazione vigente in materia di imprenditorialità femminile (L.215/92).		
Verifica finale		
Valutazione sulle competenze apprese durante il corso	**8**	
Percorso di sviluppo soft skills		
Technical Writing & Executive Reporting		
Tecniche di redazione per differenziare i report operativi dettagliati (per specialisti e tecnici) dai documenti di sintesi direzionale (Executive Summary) focalizzati su impatti economici, rischi di business e decisioni strategiche.		
Metodologie per convertire indicatori complessi (tecnologici, finanziari o di processo) in metriche di rischio aziendale, costi/benefici e ritorno sull'investimento (ROI), comprensibili a stakeholder non tecnici.		
Progettazione di grafici, tabelle riassuntive e dashboard aziendali per presentare dati complessi in modo visivamente immediato, evidenziando trend, criticità e aree di miglioramento.		
Linee guida per la stesura di report professionali, policy interne e procedure operative (SOP), curando la precisione terminologica, l'assenza di ambiguità e la conformità alle normative aziendali e di settore.		
Gestione dello Stress, Incident Escalation e Comunicazione di Crisi		
Definizione di criteri e soglie di gravità per attivare correttamente i flussi comunicativi aziendali, dal supporto di primo livello fino al coinvolgimento del top management e dei comitati di crisi		L'unità formativa ha l'obiettivo di trasmettere agli studenti gli strumenti per governare i flussi informativi sia in condizioni di normale operatività — redigendo report d'impatto e documentazione tecnica — sia sotto pressione, strutturando escalation efficaci e gestendo la comunicazione in scenari critici. In conformità a quanto raccomandato dalle disposizioni regionali novellate in materia di "Standard di progettazione dei percorsi " mediante ATTO DD 491 del 28/09/2023, al fine di promuovere e favorire -per
Strategie organizzative e psicologiche per gestire picchi di lavoro elevati, mitigare il burnout del team e mantenere la lucidità decisionale e la concentrazione durante scenari di emergenza o scadenze critiche.		
Gestione dei flussi informativi interni ed esterni durante un disservizio o un'emergenza aziendale, inclusi i protocolli di notifica a clienti, partner commerciali ed eventuali autorità competenti.		

Conduzione di sessioni di revisione post-crisi e stesura del report delle "lezioni apprese" (Lessons Learned) per analizzare le dinamiche umane, organizzative e tecniche, ottimizzando i processi aziendali futuri.	**48**	la popolazione adulta- lo sviluppo e il potenziamento di competenze chiave per la cittadinanza e l'occupabilità, fra cui anche l'Educazione finanziaria e l'Imprenditorialità, la presente UF recepisce e prevede la trattazione di tematiche essenziali (evincibili dai "saperi" collegati alle conoscenze essenziali) relative l'imprenditoria innovativa giovanile e tematiche essenziali correlate a un'Educazione Finanziaria di base. L'obiettivo di questa caratterizzazione consiste principalmente nel rendere i giovani consapevoli, attraverso momenti formali e informali, del significato e valore del voler essere e diventare un imprenditore nell'era contemporanea.
Autoimprenditorialità		
Business Planning e Analisi di Mercato		
Gestione Finanziaria		
Ricerca fondi e finanziamenti		
Project Management		
Metodologie di sviluppo progettuale: Metodologia Agile e Scrum		
Come valutare l'andamento dell'esecuzione del progetto		
Elementi di base di educazione finanziaria		
Cosa significa fare startup		
Il BM - Business model Canvas		
Struttura organizzativa delle startup		
Variabili economico/numeriche della gestione		
Modello previsionale per le startup		
Service Design		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
Sicurezza sul lavoro		
Organizzazione della sicurezza aziendale		
Concetti di rischio		
Danno		
Prevenzione		
Protezione		
Organizzazione della prevenzione aziendale		
Diritti doveri e sanzioni per i vari soggetti aziendali		
Organi di vigilanza, controllo e assistenza		
Fattori di rischio generali e specifici		
rischi infortuni		
meccanici generali		
elettrici generali		
macchine		
attrezzature		
cadute dall'alto		
rischi fisici		
microclima ed illuminazione		
videoterminali		
ambienti di lavoro		
stress lavoro-correlato		
movimentazione manuale dei carichi		
incidenti e infortuni mancati		
Misure e procedure di prevenzione e protezione		
etichettatura		
DPI e organizzazione del lavoro		
segnaletica		
emergenze		
procedure di sicurezza con riferimento al profilo di rischio specifico		
procedure esodo ed incendi		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
COMPETENZE BASE		
Fondamenti Programmazione, Basi di Dati e Scripting per la Sicurezza		
Legislazioni ambientali e incentivazioni economiche di settore		
La normativa RAEE		
Principali strumenti e tecniche di osservazione		
L'impronta ambientale delle organizzazioni produttive in ambito IT		
I fattori che influiscono sulla sostenibilità dei processi		
Il monitoraggio degli asset IT in ottica di consumo energetico		
Legame di causa/effetto delle azioni umane sull'ambiente		
L'efficienza energetica delle soluzioni hardware e software utilizzate		
Buone prassi per l'utilizzo eco-compatibile delle tecnologie informatiche		
Principi di elaborazione testi		
Elementi teorici e pratici di formattazione e struttura per l'elaborazione di Report di carattere tecnico-scientifico		
Elementi di foglio elettronico		
Elementi teorici e pratici di formattazione e struttura per l'elaborazione di fogli elettroni da utilizzare in contesti di project management al fine di elaborare piani di azione progettuali per garantire cronoprogrammi in coerenza fra l'organizzazione interna del contesto lavorativo e i requirements/desiderata della committenza		
Elementi di presentazione multimediale		
Elementi teorici e pratici di formattazione e struttura per l'elaborazione di presentazioni multimediali da utilizzare in contesti di project management al fine di elaborare pitch finali di progetto efficaci termini di comunicazione e presentazione degli output finali di progetto in coerenza ai requirements di alto livello, deliverables e risultati attesi		
Fondamenti della tecnologia dell'informazione		
ICT: storia e utilizzi		
Tipologia di trasporto flussi di dati		
Funzioni di base del sistema operativo		
Tipologie di OS: Windows, Apple, Linux		
Elementi di basi dati		
Organizzazione dati in Database relazionali e Tabelle		
Concetti e termini relativi ad Internet		
Internet: storia e nascita		
Evoluzione dei sistemi online		
Logica di Programmazione e Algoritmi		
Sintassi del linguaggio Python e ambienti di sviluppo (IDE)		
Variabili, costanti e tipi di dati primitivi (interi, stringhe, booleani)		
Operatori aritmetici, di confronto e logici per l'algebra di Boole		
Costruzione di diagrammi di flusso e pseudocodice per la risoluzione di problemi		
Strutture di Controllo e Flusso di Esecuzione		
Costrutti condizionali annidati (if, elif, else) per la deviazione del flusso		
Cicli iterativi definiti (for) per l'elaborazione di sequenze e collezioni		
Cicli iterativi indefiniti (while) e controllo delle condizioni di uscita		
Istruzioni di interruzione prematura dei cicli (break, continue)		
Strutture Dati Complesse e Manipolazione Stringhe		
Gestione di liste e tuple per l'indicizzazione ordinata dei dati		
Utilizzo dei dizionari (chiave-valore) per la mappatura di informazioni strutturate		
Metodi nativi per la ricerca, formattazione e slicing delle stringhe di testo		
Conversione e parsing di formati di interscambio standard (JSON, CSV, XML)		
Modularità del Codice e Funzioni		
Definizione di funzioni personalizzate, parametri di input e valori di ritorno		
Ambito di visibilità delle variabili (scope globale vs scope locale)		
Importazione e utilizzo di moduli e librerie dalla libreria standard		
Gestione strutturata delle eccezioni (try, except) per prevenire crash del codice		
Modellazione dei Dati e Database Relazionali		
Architettura dei sistemi di gestione di basi di dati (DBMS)		
Progettazione concettuale (Modello Entità-Relazione) e chiavi (primarie, esterne)		
Processo di normalizzazione delle tabelle per l'eliminazione della ridondanza		
Vincoli di integrità referenziale e strutture di memorizzazione del dato		
Linguaggio SQL e Interrogazione dei Dati		
Comandi DDL (Data Definition Language) per la creazione di tabelle e schemi		
Comandi DML (Data Manipulation Language) per inserimento, modifica e cancellazione		
Scrittura di query di selezione (SELECT) con filtri complessi (WHERE, LIKE)		
Funzioni di aggregazione (COUNT, SUM) e raggruppamenti di dati (GROUP BY)		
Operazioni Avanzate su Database e Sistemi NoSQL		
Utilizzo delle operazioni di JOIN per correlare tabelle differenti		
Scrittura di sottoquery (subquery) e viste per interrogazioni nidificate		
Introduzione ai database non relazionali orientati ai documenti (es. MongoDB)		
Differenze strutturali e casi d'uso in cybersecurity tra approccio SQL e NoSQL		
Sicurezza e Hardening dei Database		
Implementazione del controllo degli accessi basato sui ruoli (RBAC) in SQL		
Tecniche di crittografia dei dati a riposo (at-rest) e in transito (in-transit)		

8

L'unità formativa ha lo scopo di esplicitare gli argomenti relativi alle conoscenze della sicurezza sul lavoro.L'obiettivo è di rendere esplicito all'utente come lavorare in un'ottica di sicurezza. Secondo quanto definito dalla circolare regionale 13591 del 3 marzo 2014, verranno erogate 4 ore di formazione generale e 8 ore di formazione specifica rispetto al livello di rischio medio per quanto riguarda il settore ateco 2007 "Istruzione". In particolare per la formazione specifica in questa Unità Formativa si tratteranno le possibili situazioni di rischio legate alle mansioni d'ufficio, i rischi connessi all'utilizzo delle apparecchiature munite di VDT e le procedure per la gestione dell'emergenza. Inoltre, verranno affrontati i temi legati alla sicurezza relativa alla figura professionale di riferimento del percorso e al settore di appartenenza delle aziende future sedi di stage.Con riferimento al settore professionale d'appartenenza, verranno affrontati i valori di base della parità di trattamento e della lotta alla discriminazione nella vita sociale e nel mercato del lavoro.

136

Questa Unita Formativa fornisce le competenze logiche e pratiche per sviluppare script di automazione, interrogare database e comprendere il codice software. Il percorso parte dalle basi della logica di programmazione (utilizzando principalmente Python e Bash) e della gestione dei dati (SQL e NoSQL), applicandole direttamente a scenari di cybersecurity.
Lo scopo è quello di abilitare lo studente ad automatizzare i compiti ripetitivi di gestione sistemistica, estrarre e correlare log da database, e riconoscere vulnerabilità elementari a livello di codice (es. SQL Injection) per collaborare efficacemente alle attività di difesa e analisi.

In questa unità formativa saranno sviluppate le conoscenze essenziali "Legislazioni ambientali e incentivazioni economiche di settore" per la durata di un'ora, "Principali strumenti e tecniche di osservazione" per la durata di due ore e "Legame di causa/effetto delle azioni umane sull'ambiente" per la durata di due ore relative all'Obiettivo "Contestualizzare i principi dello sviluppo sostenibile nelle attività economico-produttive del settore di riferimento".

Verranno inoltre affrontate le conoscenze essenziali "Principi elaborazione testi", "Elementi di foglio elettronico", "Elementi di presentazione multimediale", "Fondamenti della tecnologia dell'informazione", "Funzioni di base del sistema operativo", "Elementi di basi di dati", "Concetti e termini relativi ad Internet" relative all'Obiettivo "Tecnologie informatiche"

Configurazione dei log di audit del DBMS per il tracciamento delle operazioni		
Meccanismi di backup e ripristino sicuro delle basi di dati aziendali		
Vulnerabilità del Codice e OWASP Top 10 (Database)		
Meccanismo teorico della vulnerabilità SQL Injection (SQLi)		
Tecniche di attacco pratiche (In-band, Inferential/Blind, Out-of-band SQLi)		
Utilizzo di Prepared Statements e query parametrizzate per la mitigazione		
Sanificazione e validazione dell'input utente a livello applicativo		
Fondamenti di Bash Scripting su Sistemi Linux		
Architettura della shell Linux, variabili d'ambiente e permessi di esecuzione		
Scrittura di script .sh con costrutti condizionali e cicli nativi di Bash		
Uso dei canali standard (stdin, stdout, stderr) e reindirizzamento dei flussi		
Automazione di comandi di sistema tramite schedulazione cron (Crontab)		
Automazione Sistemistica e Parsing dei Log		
Utilizzo dei comandi di filtraggio e manipolazione del testo (grep, awk, sed)		
Scrittura di script Bash/Python per l'ispezione automatica dei log di sistema		
Identificazione di pattern sospetti (es. tentativi di brute force) nei file di log		
Generazione di report di sicurezza automatizzati e invio di alert via email		
Scripting per l'Analisi di Rete e Sicurezza Operativa		
Utilizzo della libreria Python subprocess per eseguire comandi di sistema		
Interazione con protocolli web tramite librerie dedicate (es. requests in Python)		
Sviluppo di script elementari per il network scanning e la verifica delle porte		
Gestione sicura delle credenziali negli script (evitando l'hardcoding delle password)		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
Reti, Protocolli e Architetture di Sicurezza		
Modelli di Rete e Architetture di Comunicazione		
Struttura e comparazione dei modelli di riferimento OSI (7 livelli) e TCP/IP (4 livelli)		
Flusso di incapsulamento e decapsulamento dei dati attraverso i diversi livelli del modello		
Funzionamento dei dispositivi di rete fondamentali: Hub, Switch (Layer 2) e Router (Layer 3)		
Standard IEEE 800 (Ethernet) e gestione degli indirizzi fisici (MAC Address)		
Indirizzamento di Rete e Routing (IPv4 e IPv6)		
Struttura degli indirizzi IPv4, classi di indirizzi, subnet mask e calcolo delle sottoreti		
Meccanismi di allocazione dinamica (DHCP) e traduzione degli indirizzi di rete (NAT/PAT)		
Concetti di routing statico e dinamico (cenni su protocolli come OSPF e BGP)		
Transizione a IPv6: struttura dell'indirizzo, vantaggi di sicurezza e differenze con IPv4		
Protocolli di Trasporto e Sessione		
Protocollo TCP: meccanismo di Handshake a 3 vie, gestione dei flag e controllo del flusso		
Protocollo UDP: caratteristiche del trasporto non orientato alla connessione e casi d'uso		
Porte logiche standard (well-known ports) e mappatura dei servizi di rete principali		
Analisi delle vulnerabilità di livello trasporto (es. SYN Flood, Port Scanning)		
Introduction to Networks		
Pile protocollari		
Tipologie di apparati di rete		
Protocolli di indirizzamento		
Planning delle reti		
Routing and Switching Essentials		
LAN switching		
Basi di routing		Questa Unità Formativa approfondisce il funzionamento delle reti di calcolatori, l'analisi dei protocolli di comunicazione e la progettazione di infrastrutture di rete protette. Gli studenti imparano a comprendere come viaggiano i dati, a identificare le vulnerabilità architetturali e a implementare le difese perimetrali e logiche. Lo scopo è abilitare lo studente a configurare, monitorare e proteggere un'architettura di rete aziendale. Al termine dell'Unità Formativa, il tecnico superiore sarà in grado di analizzare il traffico di rete per rilevare anomalie, segmentare le infrastrutture in sicurezza e applicare i principali protocolli crittografici a tutela dei dati.
Servizi di rete		
Scaling Networks		
Meccanismi di gestione delle reti	**100**	
Routing avanzato		
Analisi protocollo OSPF		
Concetti avanzati sui protocolli di rete		
Access Control List		
Protocolli Applicativi e Servizi di Rete		
Funzionamento del protocollo HTTP/HTTPS e struttura delle richieste/risposte web		
Il sistema DNS (Domain Name System): gerarchia, record (A, AAAA, MX, TXT) e sicurezza		
Protocolli per il trasferimento file (FTP, SFTP) e per la posta elettronica (SMTP, IMAP, POP3)		
Servizi di gestione remota sicura e non sicura (Telnet vs SSH)		
Crittografia di Rete e Virtual Private Network (VPN)		
Fondamenti di crittografia applicata: algoritmi simmetrici, asimmetrici e funzioni di hash		
Protocollo TLS/SSL: funzionamento del protocollo di cifratura per il traffico web e gestione certificati		
Tecnologie VPN: protocollo IPsec (modalità Transport e Tunnel, architettura AH/ESP)		
Soluzioni VPN SSL/TLS (es. OpenVPN, WireGuard) per l'accesso remoto sicuro dei lavoratori		
Sicurezza delle Reti Locali (Layer 2 Security)		
Segmentazione logica delle reti tramite VLAN (Virtual LAN) e protocollo di trunking 802.1Q		
Vulnerabilità intrinseche del Layer 2: attacchi di ARP Spoofing/Poisoning e MAC Flooding		
Contromisure di sicurezza sugli switch: Port Security, DHCP Snooping e Dynamic ARP Inspection (DAI)		
Protocolli per la prevenzione dei loop di rete (Spanning Tree Protocol - STP) e relativa messa in sicurezza		
Sicurezza delle Reti Wireless e Nuovi Paradigmi Architetturali		
Standard di trasmissione wireless (IEEE 802.11) e vulnerabilità delle reti Wi-Fi aperte		
Evoluzione dei protocolli di sicurezza wireless: limiti di WEP/WPA e implementazione di WPA3		
Autenticazione centralizzata aziendale tramite standard 802.1X e server RADIUS/TACACS+		
Introduzione ai modelli architetturali moderni: approccio Zero Trust e architetture SASE (Secure Access Service Edge)		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
COMPETENZE CORE		
Application Security & DevSecOps		
Metodologia DevSecOps e approccio "Shift Left"		
Evoluzione delle metodologie di sviluppo software: dal modello Waterfall ad Agile, DevOps e DevSecOps		
Principio dello Shift Left: integrare la sicurezza fin dalle prime fasi di design e pianificazione		
Modelli di maturità per la sicurezza applicativa (es. OWASP SAMM o BSIMM)		
Condivisione delle responsabilità e superamento dei silos tra team di Sviluppo (Dev), Sicurezza (Sec) e Operations (Ops)		
Vulnerabilità Applicative e Mitigazioni (OWASP Top 10)		
Analisi teorica e pratica delle principali minacce web secondo la classifica OWASP Top 10 corrente		
Meccanismi di attacco applicativo diffusi: Broken Access Control, Injection, e Cryptographic Failures		Questa Unità Formativa introduce i principi della sicurezza del software lungo tutto il suo ciclo di vita. Gli studenti apprendono come integrare controlli di sicurezza automatizzati all'interno delle pipeline di sviluppo moderno (CI/CD), superando il vecchio approccio della sicurezza intesa come fase finale e isolata. Lo scopo è quello di abilitare lo studente a identificare, analizzare e mitigare le vulnerabilità applicative e infrastrutturali nel software. Al termine del modulo, la figura professionale saprà collaborare con i team di sviluppo applicando la filosofia "Shift Left", automatizzando i test di sicurezza e garantendo il rilascio di codice protetto e conforme.
Tecniche di programmazione sicura (Secure Coding), validazione rigorosa degli input e sanificazione dell'output		
Gestione sicura delle sessioni utente, dei token di autenticazione e delle credenziali applicative		
Sicurezza della Software Supply Chain e Analisi Strumentale	**48**	
Concetto di Software Supply Chain e mappatura dei rischi legati alle dipendenze open-source		
Strumenti SAST (Static Application Security Testing) per l'analisi statica del codice sorgente alla ricerca di falle		
Strumenti DAST (Dynamic Application Security Testing) per il testing dinamico dell'applicazione in esecuzione		
Strumenti SCA (Software Composition Analysis) per l'inventario delle librerie (SBOM) e il rilevamento di vulnerabilità note (CVE)		
Automazione della Pipeline CI/CD e Sicurezza dell'Infrastruttura		
Struttura di una pipeline di Continuous Integration e Continuous Deployment (CI/CD) e relativi strumenti (es. GitLab CI, GitHub Actions, Jenkins)		
Integrazione e configurazione di gate di sicurezza automatizzati (Security Quality Gates) nel processo di build		
Sicurezza della tecnologia dei container (es. Docker): hardening delle immagini e scansione delle vulnerabilità		
Principi di Infrastructure as Code (IaC) e scansione automatica dei file di configurazione (es. Terraform, Ansible) per prevenire misconfiguration		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
Cloud Infrastructure Security		
Architetture Cloud e Modello di Responsabilità Condivisa		
Caratteristiche dei modelli di servizio cloud (IaaS, PaaS, SaaS) e di deployment (Pubblico, Privato, Ibrido, Multi-Cloud)		
Il Modello di Responsabilità Condivisa (Shared Responsibility Model) tra Cloud Provider e cliente aziendale		
Concetti di isolamento logico multi-tenancy e sicurezza dell'ipervisore (Hypervisor) e dell'infrastruttura fisica		
Framework di riferimento per la sicurezza del cloud (es. CSA Cloud Controls Matrix, CIS Cloud Benchmarks)		
Cloud Identity & Access Management (IAM)		
Gestione delle identità nel cloud: utenti, gruppi, ruoli IAM, policy di accesso e principio del minimo privilegio		
Meccanismi di autenticazione forte (MFA/2FA) e politiche di accesso condizionale (Conditional Access)		
Federazione delle identità aziendali tramite protocolli standard (SAML 2.0, OIDC, OAuth 2.0) e Single Sign-On (SSO)		
Gestione, rotazione automatica e protezione dei segreti (Secret Management), chiavi API e credenziali programmatiche		
Sicurezza delle Reti Cloud (Cloud Networking Security)		
Configurazione sicura di reti virtuali isolate (VPC/VNet) e relative regole di routing		
Implementazione di filtri di rete a livello di risorsa e di sottorete (Security Groups e Network ACL)		
Connessioni sicure tra data center on-premises e cloud (VPN IPsec site-to-site e connessioni dedicate esterne)		
Protezione del perimetro cloud da attacchi volumetrici tramite servizi DDoS Protection e Web Application Firewall (WAF)		
Protezione e Crittografia dei Dati nel Cloud		Questa Unità Formativa esplora i modelli di sicurezza specifici per gli ambienti cloud (pubblici, privati e ibridi), analizzando le sfide legate alla decentralizzazione delle risorse. Gli studenti imparano a configurare
Strategie di classificazione e protezione dei dati a riposo (at-rest) nei servizi di storage a blocchi e ad oggetti		

Tecniche di cifratura dei dati in transito (in-transit) verso e all'interno dell'infrastruttura cloud		ibridi), analizzando le sfide legate alla decentralizzazione delle risorse. Gli studenti imparano a configurare
Utilizzo e gestione dei servizi di gestione delle chiavi crittografiche (KMS) e moduli HSM dedicati nel cloud		in sicurezza le infrastrutture dei principali Cloud Provider, gestendo l'identità, la protezione dei dati e la
Protezione del dato in uso tramite tecnologie di Confidential Computing e ambienti di esecuzione protetti (TEE)	**80**	conformità architetturale.
Cloud Security Posture Management (CSPM) e Compliance		Lo scopo è quello di abilitare lo studente a progettare, implementare e monitorare architetture cloud
Identificazione automatizzata di configurazioni errate (Misconfigurations) e vulnerabilità negli asset cloud		protette. Al termine del percorso, il tecnico superiore sarà in grado di applicare il modello di responsabilità
Utilizzo di strumenti di CSPM per la verifica continua della conformità agli standard (GDPR, PCI-DSS, ISO 27001)		condivisa, isolare le risorse di rete nel cloud, governare gli accessi e rilevare tempestivamente incidenti o
Definizione e applicazione di regole di governance automatizzate (Cloud Policies/Guardrails) a livello di organizzazione		configurazioni errate.
Gestione dei rischi legati all'effetto "Shadow IT" e monitoraggio dell'inventario degli asset cloud (Asset Discovery)		
Sicurezza dei Servizi Cloud Avanzati (PaaS e Serverless)		
Hardening e sicurezza dei database gestiti dal cloud provider (es. SQL e NoSQL as a Service)		
Modelli di sicurezza per l'architettura Serverless e le funzioni as a Service (FaaS, es. AWS Lambda, Azure Functions)		
Gestione dei permessi granulari e dei timeout per mitigare i rischi di attacchi Denial of Service (DoS) sulle funzioni		
Analisi delle minacce specifiche per gli ambienti serverless (es. iniezione di eventi, configurazioni IAM errate)		
Sicurezza di Container e Orchestratori nel Cloud (Cloud-Native Security)		
Architettura di sicurezza dei servizi di orchestrazione gestiti (es. Amazon EKS, Azure AKS, Google GKE)		
Controllo degli accessi all'API Server di Kubernetes tramite meccanismi di RBAC (Role-Based Access Control)		
Implementazione di Network Policies per l'isolamento del traffico tra Pod ed esecuzione di container non-root		
Scansione automatica e firma crittografica delle immagini dei container all'interno dei registri cloud (Container Registries)		
Policy accessi virtuali in LAN ed esterni		
Terminali Fisici (Thin Client)		
Machine Learning e AI		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
FIREWALL		
Evoluzione e Architettura dei Sistemi Firewall		
Classificazione storica dei firewall: Packet Filtering (stateless), Stateful Inspection e Proxy/Application Gateway		
Architettura e funzionalità distintive dei Next-Generation Firewall (NGFW) rispetto ai firewall tradizionali		
Posizionamento strategico dei firewall nella rete: Edge (perimetrale), Internal/Segment Filter e Host-based		
Concetto di architettura ad alta affidabilità (High Availability - HA) in modalità Active-Passive e Active-Active		
Installazione, Inizializzazione e Gestione degli Accessi		
Tecniche di installazione del firewall in modalità Routed (Layer 3), Transparent/Bridge (Layer 2) o Virtual Wire		
Configurazione iniziale delle interfacce fisiche e logiche (LAN, WAN, DMZ) e assegnazione degli indirizzi IP		
Hardening del dispositivo: configurazione degli accessi amministrativi sicuri (SSH, HTTPS) e integrazione con sistemi AAA (RADIUS/TACACS+)		
Gestione dei backup della configurazione, aggiornamento dei firmware e delle firme di sicurezza		
Logica e Definizione delle Security Policies		
Struttura e logica di elaborazione sequenziale delle regole di sicurezza (dall'alto verso il basso)		
Criteri di corrispondenza delle regole: Zone di origine/destinazione, IP/Sottoreti, Porte/Protocolli e Utenti/Gruppi		
Gestione delle azioni di una policy: Allow (Permetti), Deny (Rifiuta in modo silenzioso) e Reject (Rifiuta inviando una notifica)		
Applicazione del principio del minimo privilegio e gestione della regola finale implicita di blocco (Implicit Deny)		
Gestione avanzata del NAT (Network Address Translation)		
Implementazione del Source NAT (SNAT) statico e dinamico (IP Masquerading) per l'accesso a Internet		
Configurazione del Destination NAT (DNAT) e del Port Forwarding per la pubblicazione in sicurezza di servizi interni		
Logica di elaborazione del traffico sul firewall: precedenza tra le regole di NAT e le regole di Security Policy		
Risoluzione delle problematiche legate al NAT per i protocolli complessi tramite moduli helper (Application Layer Gateway - ALG)		
Integrazione con l'Identità Utente (User-ID / Identity-Awareness)		Questa Unità Formativa offre un percorso verticale e specialistico sui sistemi di difesa perimetrale e
Limiti del controllo degli accessi basato unicamente sugli indirizzi IP in ambienti aziendali dinamici		interna. Gli studenti approfondiscono l'evoluzione tecnologica dei firewall, dalle origini basate sul
Meccanismi di mappatura IP-Utente tramite l'integrazione del firewall con Active Directory o server LDAP		filtraggio dei pacchetti fino ai moderni sistemi di Next-Generation Firewall (NGFW), analizzandone
Configurazione di regole di accesso personalizzate in base al ruolo organizzativo dell'utente o al gruppo di appartenenza	**94**	l'installazione, la configurazione delle policy, la manutenzione e il monitoraggio.
Implementazione di portali di autenticazione (Captive Portal) per il controllo dei dispositivi ospiti o non aziendali		Lo scopo è quello di abilitare lo studente a progettare, implementare e gestire l'architettura dei firewall
Ispezione Applicativa (App-ID) e URL Filtering		all'interno di reti aziendali complesse. Al termine del modulo, il tecnico superiore sarà in grado di scrivere
Tecniche di Deep Packet Inspection (DPI) per l'identificazione delle applicazioni indipendentemente dalla porta logica utilizzata		regole di sicurezza efficaci, configurare canali cifrati, implementare ispezioni applicative profonde e
Configurazione di policy basate sulle applicazioni per bloccare o limitare software a rischio (es. P2P, proxy di evasione)		rispondere tempestivamente alle anomalie di traffico segnalate dai dispositivi.
Implementazione del filtraggio dei contenuti web (URL Filtering) basato su categorie di reputazione e blacklist		
Controllo e limitazione della banda passante (Quality of Service - QoS) per specifiche applicazioni o categorie web		
Ispezione SSL/TLS (Decryption)		
L'impatto del traffico cifrato sulla visibilità della sicurezza e i rischi legati ai canali nascosti (Evasion techniques)		
Architettura dell'ispezione SSL: meccanismo di proxying e generazione/distribuzione dei certificati CA subordinati		
Configurazione di policy di decifratura selettiva (Inbound Inspection per i server, Outbound/Forward Proxy per gli utenti)		
Gestione delle eccezioni di decifratura per motivi di privacy o requisiti tecnici (es. servizi bancari, sanitari o applicazioni con Certificate Pinning)		
Servizi di Threat Prevention Integrati		
Configurazione dei moduli antivirus e antimalware a livello di firewall per il blocco dei file infetti in transito		
Attivazione delle funzionalità IPS (Intrusion Prevention System) sul firewall per la protezione da exploit noti e vulnerabilità		
Protezione dagli attacchi DoS (Denial of Service) tramite l'impostazione di soglie massime di connessioni simultanee (Flood Protection)		
Integrazione con sistemi di Sandbox basati su cloud per l'analisi comportamentale dei file sospetti non ancora censiti (Zero-day)		
Virtual Private Network (VPN) sul Firewall		
Configurazione di tunnel VPN Site-to-Site (IPsec) per l'interconnessione sicura di sedi aziendali remote		
Implementazione di VPN Remote Access (Client-to-Site) tramite SSL o IPsec per i lavoratori in modalità smart working		
Configurazione di meccanismi di autenticazione forte (MFA) per l'accesso alle connessioni VPN remote		
Gestione delle politiche di routing del traffico VPN: modalità Split-Tunneling vs Full-Tunneling		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
Offensive Security		
Introduzione all'Ethical Hacking e Aspetti Legali		
Differenze e confini operativi tra Vulnerability Assessment, Penetration Testing e Red Teaming		
Il quadro normativo italiano ed europeo sui reati informatici e l'importanza del "Perimetro del Test" (Scope)		
Codice deontologico dell'Ethical Hacker, gestione del consenso (Rules of Engagement) e clausole di riservatezza (NDA)		
Metodologie standard internazionali di riferimento per i test di sicurezza (es. OSSTMM, OWASP, PTES, NIST SP 800-115)		
Configurazione del Laboratorio d'Attacco e OS per Pentesting		
Architettura e funzionalità delle principali distribuzioni Linux per la sicurezza offensiva (Kali Linux, Parrot OS)		
Configurazione di ambienti di laboratorio isolati tramite Hypervisor per evitare la propagazione di exploit sulla rete reale		
Utilizzo di piattaforme e macchine virtuali vulnerabili per l'addestramento pratico (es. Hack The Box, VulnHub, OWASP Juice Shop)		
Gestione della sicurezza operativa dell'operatore: utilizzo di VPN, nodi Tor, proxy e tecniche di anonimizzazione del traffico		
Raccolta Informazioni Passiva (OSINT & Reconnaissance)		
Tecniche di Information Gathering passivo tramite motori di ricerca e operatori avanzati (Google Dorking)		
Raccolta di record DNS, informazioni Whois, identificazione dei blocchi IP aziendali e record storici		
Utilizzo di strumenti per la mappatura dell'esposizione pubblica e delle informazioni sui dipendenti (es. Maltego, TheHarvester, Shodan)		
Analisi dei metadati dei file pubblici per l'estrazione di nomi utente, software utilizzati e strutture di directory interne		
Scansione di Rete e Identificazione dei Servizi (Active Scanning)		
Logica e funzionamento della scansione delle porte TCP e UDP mediante l'utilizzo avanzato di Nmap		
Interpretazione dei flag TCP durante le scansioni (SYN scan, FIN scan, Xmas scan) e tecniche di evasione dei firewall		
Tecniche di Banner Grabbing e fingerprinting per identificare con precisione sistemi operativi e versioni dei servizi in ascolto		
Utilizzo degli script Nmap (NSE - Nmap Scripting Engine) per l'automazione della scoperta di configurazioni errate		
Analisi e Valutazione delle Vulnerabilità (Vulnerability Assessment)		
Configurazione e utilizzo di scanner di vulnerabilità automatizzati di livello enterprise e open-source (es. Nessus, OpenVAS)		
Interpretazione dei report di scansione, classificazione delle criticità ed eliminazione dei falsi positivi		
Comprensione del sistema di punteggio standard CVSS (Common Vulnerability Scoring System) per la prioritizzazione dei rischi		
Consultazione di database pubblici di vulnerabilità note ed exploit documentati (es. CVE, NVD, Exploit-DB)		
Tecniche di Attacco e Sfruttamento delle Vulnerabilità (Exploitation)		
Architettura del framework Metasploit: moduli d'attacco (Exploit), carichi utili (Payload), ausiliari (Auxiliary) ed encoder		
Differenza tecnica tra i payload di tipo "Bind Shell" (connessione in ingresso) e "Reverse Shell" (connessione in uscita)		
Ricerca, compilazione, personalizzazione ed esecuzione manuale di exploit pubblici (es. scritti in C, Python)		
Gestione e stabilizzazione della sessione di accesso iniziale sul sistema target (es. upgrade della shell a TTY)		
Password Attacking e Cracking delle Credenziali		
Differenza teorica e pratica tra attacchi alle credenziali di tipo Online (es. Brute Force su protocolli SSH, HTTP) e Offline		
Strumenti per l'automazione degli attacchi online basati su dizionari di password (es. Hydra, Medusa)		
Tecniche di estrazione di hash di password da sistemi operativi compromessi (SAM/LSASS in Windows, /etc/shadow in Linux)		
Utilizzo di strumenti di cracking offline basati su CPU e GPU (John the Ripper, Hashcat) e utilizzo delle Rainbow Tables		
Attacchi Web Application (Server-Side)	**120**	Questa Unità Formativa introduce gli studenti alle metodologie, alle tecniche e agli strumenti utilizzati dagli esperti di sicurezza offensiva (Ethical Hacker) per identificare e sfruttare le vulnerabilità dei sistemi. Attraverso un approccio prevalentemente pratico in ambiente di laboratorio controllato, il corso copre l'intero ciclo di un Penetration Test e di un'attività di Red Teaming. Lo scopo è quello di abilitare lo studente a condurre verifiche di sicurezza e attività di simulazione d'attacco in modo etico e professionale. Al termine della materia, il tecnico superiore sarà in grado di adottare la mentalità di un attaccante per scovare falle di sicurezza in reti, sistemi e applicazioni, documentando i risultati in un report tecnico finalizzato alle attività di rimedio (Remediation).
Sfruttamento pratico di vulnerabilità di iniezione di codice e comandi sul server di backend (OS Command Injection)		
Vulnerabilità di inclusione di file locali e remoti (Local/Remote File Inclusion - LFI/RFI) ed esecuzione di codice arbitrario		
Sfruttamento avanzato della SQL Injection (SQLi) per l'estrazione manuale e automatizzata (es. sqlmap) di interi database		
Analisi delle vulnerabilità di caricamento file non sicuro (Unrestricted File Upload) per l'esecuzione di Web Shell		
Attacchi Web Application (Client-Side e Logica di Business)		
Meccanismo degli attacchi Cross-Site Scripting (XSS) nelle varianti Reflected, Stored e DOM-based		
Sfruttamento di XSS per il furto di cookie di sessione, session hijacking e reindirizzamenti malevoli degli utenti		
Attacchi di tipo Cross-Site Request Forgery (CSRF) per l'esecuzione di azioni non autorizzate per conto della vittima		
Identificazione di falle nella logica di business dell'applicazione (es. manipolazione dei parametri di prezzo, bypass dell'autenticazione)		
Post-Exploitation e Privileges Escalation su Linux		
Tecniche di enumerazione locale del sistema operativo Linux alla ricerca di vettori di elevazione dei privilegi		

Sfruttamento di configurazioni errate nei permessi dei file, cronjob insicuri e file con permessi speciali SUID		
Sfruttamento di vulnerabilità del Kernel Linux dovute alla mancata applicazione delle patch di sicurezza		
Tecniche di persistenza sul sistema target (es. creazione di utenti nascosti, backdoor nei servizi o chiavi SSH)		
Post-Exploitation e Privileges Escalation su Windows		
Enumerazione locale di Windows: identificazione di patch mancanti, privilegi dell'utente corrente e software vulnerabili		
Sfruttamento di debolezze strutturali del sistema (es. servizi con percorsi non tra virgolette - Unquoted Service Paths)		
Utilizzo di strumenti avanzati per l'analisi della memoria e l'estrazione di credenziali (es. Mimikatz)		
Tecniche di elusione elementari dei sistemi di protezione antivirus (AV Evasion) mediante offuscamento del codice		
Attacchi alle Infrastrutture di Rete e Active Directory Pentesting		
Tecniche di attacco sui protocolli di rete locali: ARP Spoofing, DHCP Starvation e attacchi LLMNR/NBT-NS (Responder)		
Comprensione dei vettori d'attacco specifici per ambienti Active Directory: attacchi di tipo Pass-the-Hash e Pass-the-Ticket		
Tecniche di sfruttamento dei protocolli di autenticazione Microsoft: attacchi Kerberoasting e AS-REP Roasting		
Mappatura delle relazioni di fiducia e dei percorsi di attacco complessi in un dominio AD tramite lo strumento BloodHound		
Ingegneria Sociale e Attacchi di Phishing		
Principi psicologici della persuasione e della manipolazione applicati alla cybersecurity (urgenza, autorità, riprova sociale)		
Progettazione e configurazione di campagne di simulazione di Phishing e Spear-Phishing aziendali		
Utilizzo di framework per l'ingegneria sociale (es. Social-Engineer Toolkit - SET, GoPhish) per la clonazione di portali web		
Tecniche di attacco tramite supporti fisici infetti (es. USB Rubber Ducky, attacchi di BadUSB)		
Reporting, Scrittura della Relazione e Remediation Plan		
Struttura standard di un report di Penetration Test professionale per il committente (Executive Summary vs Technical Report)		
Modalità di documentazione accurata delle prove di vulnerabilità (Proof of Concept - PoC) e dei passi per riprodurre l'attacco		
Mappatura delle vulnerabilità riscontrate sui framework globali di classificazione delle minacce (es. MITRE ATT&CK)		
Definizione di raccomandazioni tecniche chiare ed efficaci (Remediation) per supportare il team di difesa nella risoluzione delle falle		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
OT and IoT Security		
Introduzione all'OT, IoT e Modelli Architetturali	**44**	Questa Unità Formativa esplora le sfide di sicurezza legate al mondo della tecnologia operativa (OT), degli ambienti industriali (ICS/SCADA) e dei dispositivi IoT (Internet of Things). Gli studenti analizzano le differenze radicali tra il mondo IT tradizionale e i sistemi fisici cyber-sociali, studiandone i protocolli nativi, i vettori di attacco e le strategie di difesa dedicate. Lo scopo è quello di abilitare lo studente a identificare e mitigare i rischi cyber all'interno di reti industriali e infrastrutture IoT. Al termine del percorso, il tecnico superiore sarà in grado di mappare gli asset fisici, applicare modelli di segmentazione sicura e monitorare il traffico di rete per proteggere la continuità operativa ed evitare danni fisici a impianti o persone.
Differenze tra sicurezza IT (priorità alla riservatezza/CIA triad) e sicurezza OT (priorità a disponibilità e sicurezza fisica/Safety)		
Componenti fondamentali dei sistemi ICS: PLC (Programmable Logic Controller), RTU, sistemi SCADA e interfacce HMI		
Il Modello di Purdue (Purdue Reference Model) per la segmentazione e la gerarchia logica delle reti industriali		
Caratteristiche dell'ecosistema IoT ed evoluzione verso l'Industrial IoT (IIoT) e i sistemi cyber-fisici		
Protocolli di Comunicazione e Vulnerabilità Specifiche		
Funzionamento e analisi dei protocolli industriali legacy non cifrati (es. Modbus TCP, Profinet, EtherNet/IP)		
Protocolli di messaggistica leggeri specifici per l'IoT e la telemetria (es. MQTT, CoAP)		
Vettori di attacco comuni negli ambienti OT/IoT: firmware non aggiornabili, credenziali hardcoded e canali di manutenzione remota non protetti		
Analisi di casi storici di attacchi cyber-industriali (es. Stuxnet, Industroyer) per comprendere l'impatto sul mondo fisico		
Strategie di Difesa e Segmentazione in Ambito Industriale		
Tecniche di segmentazione di rete tramite l'implementazione di "Celle e Zone" secondo lo standard internazionale IEC 62443		
Configurazione di canali di accesso remoto sicuro dedicati alla manutenzione degli impianti (es. Industrial VPN e Jump Host)		
Utilizzo di sistemi IDS industriali basati sull'analisi del comportamento e sulla comprensione dei protocolli OT (Deep Packet Inspection)		
Limitazioni delle soluzioni IT tradizionali (es. patch management aggressivo, network scanning attivo) negli ambienti industriali critici		
Sicurezza dei Dispositivi IoT e Standard di Riferimento		
Linee guida per l'hardening dei dispositivi IoT: disattivazione dei servizi non necessari (es. Telnet) e gestione sicura del ciclo di vita		
Architetture di sicurezza IoT basate su crittografia leggera e gestione delle identità dei dispositivi (Device Identity)		
Panoramica sulle normative e standard di sicurezza rilevanti per il settore (es. direttive europee Cyber Resilience Act e NIS 2)		
Framework del NIST per la cybersecurity IoT e buone pratiche per la Supply Chain dei componenti hardware e software		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
Sistemi Operativi, Amministrazione di Sistema, Elementi di virtualizzazione		
Soluzioni e tecnologie per il risparmio di risorse e l'efficientamento energetico	**156**	Questa Unità Formativa fornisce le competenze fondamentali per l'installazione, la configurazione, la gestione e il consolidamento dei sistemi operativi client e server (Linux e Windows), unendo le pratiche di amministrazione di sistema con le moderne tecnologie di virtualizzazione hardware e isolamento a container. Lo scopo è quello di abilitare lo studente a gestire l'infrastruttura sistemistica di un'azienda in modo sicuro ed efficiente. Al termine del modulo, il tecnico superiore sarà in grado di configurare servizi di rete essenziali, applicare criteri stringenti di hardening sui sistemi operativi, amministrare ambienti virtualizzati e monitorare le risorse per garantire la continuità dei servizi. In questa unità formativa saranno sviluppate le conoscenze essenziali "Soluzioni e tecnologie per il risparmio di risorse e l'efficientamento energetico" per una durata di due ore e "Principi fondamentali della gestione dei rifiuti e di materiali da riciclo, in un'ottica di circolarità" per la durata di un'ora relative all'Obiettivo "Contestualizzare i principi dello sviluppo sostenibile nelle attività economico-produttive del settore di riferimento".
Smart working: tecnologie e ambiti di applicazione nel comparto IT		
Smart grid: la gestione IT delle reti di distribuzione dell'energia		
La diffusione dei sensori in rete per il monitoraggio ambientale		
Principi fondamentali della gestione dei rifiuti e di materiali da riciclo, in un'ottica di circolarità		
Estendere la vita utile di prodotti, componenti e materiali		
Gestione e smaltimento dei rifiuti e dei componenti elettrici ed elettronici (RAEE)		
Architettura dei Sistemi Operativi e Avvio del Sistema		
Componenti core di un sistema operativo: Kernel (Monolitico vs Microkernel), moduli e spazio utente (User Space)		
Gestione della memoria (RAM, Swap, Memoria Virtuale) e allocazione delle risorse hardware		
Processo di boot del sistema: differenze tra BIOS/MBR e UEFI/GPT, e funzionamento del bootloader (es. GRUB, Windows Boot Manager)		
Architetture della CPU (x86, x64, ARM) e loro impatto sulla gestione del sistema operativo		
Amministrazione della linea di comando Linux (Bash CLI)		
Navigazione del File System gerarchico standard di Linux (FHS) e manipolazione di file e directory		
Comandi fondamentali per la gestione del testo, visualizzazione ed editing (cat, less, nano, vi/vim)		
Utilizzo delle variabili d'ambiente, alias di sistema e personalizzazione dei file di configurazione della shell (.bashrc)		
Concatenazione di comandi tramite operatori logici, reindirizzamento dei flussi (pipe, >, >>) e gestione dei job in background		
Gestione di Utenti, Gruppi e Permessi su Linux		
Struttura dei file di sistema per l'autenticazione locale e le identità (/etc/passwd, /etc/shadow, /etc/group)		
Comandi per la creazione, modifica ed eliminazione di account utente e gruppi (useradd, usermod, groupadd)		
Modello dei permessi POSIX standard (Read, Write, Execute) per proprietario, gruppo e altri (chmod, chown)		
Permessi speciali (SUID, SGID, Sticky Bit) e impostazione delle maschere di default tramite umask		
Amministrazione e Sicurezza di Windows Server		
Architettura di Windows Server, gestione tramite interfaccia grafica (GUI) e console Server Manager		
Fondamenti di Windows PowerShell: sintassi basata sui cmdlet, pipeline di oggetti e script di base		
Gestione di utenti e gruppi locali, e controllo dei permessi sul file system tramite ACL (Access Control Lists) e NTFS permissions		
Configurazione del Registro di Sistema di Windows (Registry) e monitoraggio tramite Visualizzatore Eventi (Event Viewer)		
Servizi di Directory e Gestione Centralizzata (Active Directory)		
Architettura logica di Active Directory Domain Services (AD DS): Domini, Alberi, Foreste e Unità Organizzative (OU)		
Installazione di un Domain Controller (DC) e configurazione dei servizi infrastrutturali integrati (DNS, DHCP)		
Gestione centralizzata di utenti, computer, gruppi di sicurezza (Security Groups) e logiche di autenticazione Kerberos		
Creazione, collegamento e applicazione di Criteri di Gruppo (Group Policy Objects - GPO) per l'hardening dei client aziendali		
Gestione del File System, Storage e Dischi		
Tipologie di file system nativi e loro caratteristiche di sicurezza (ext4, XFS su Linux; NTFS, ReFS su Windows)		
Partizionamento dei dischi logici, formattazione e procedure di montaggio manuale e automatico (file /etc/fstab)		
Configurazione di volumi logici dinamici tramite LVM (Logical Volume Manager) in ambienti Linux		
Concetti di archiviazione ridondante (RAID software e hardware) e partizionamento sicuro per l'isolamento dei dati applicativi		
Gestione dei Processi e Schedulazione delle Attività		
Ciclo di vita di un processo, stati del processo (Running, Sleeping, Zombie) e gerarchia padre-figlio		
Monitoraggio in tempo reale dei processi e delle risorse tramite utility CLI (ps, top, htop, taskmgr)		
Invio di segnali ai processi per la gestione del ciclo di vita e la terminazione forzata (kill, pkill, sigterm, sigkill)		
Automazione e pianificazione di task periodici tramite il demone Cron (Linux) e l'Utilità di pianificazione (Windows Task Scheduler)		
Gestione dei Pacchetti, Aggiornamenti e Servizi di Sistema		
Architettura dei gestori di pacchetti software nativi e dei repository ufficiali (APT per Debian/Ubuntu, YUM/DNF per RHEL/Rocky)		
Gestione del ciclo di vita dei servizi di sistema tramite il sistema di init moderno Systemd (systemctl, journalctl)		
Gestione delle funzionalità e dei ruoli su Windows Server tramite PowerShell e strumenti di configurazione dedicati		
Pianificazione delle policy di patch management e aggiornamento dei sistemi operativi per la mitigazione delle vulnerabilità note		
Configurazione dei Servizi di Rete di Base		
Configurazione statica e dinamica delle interfacce di rete sui sistemi Linux (Netplan, NetworkManager, ifconfig/ip)		
Risoluzione dei nomi di rete locali e configurazione dei client DNS (file /etc/resolv.conf e file hosts)		
Installazione e configurazione base di server Web (Apache, Nginx, IIS) e monitoraggio delle porte in ascolto (netstat, ss)		
Configurazione di protocolli per la condivisione sicura di file in rete locale (SSH/SFTP, Samba, NFS)		
Hardening e Messa in Sicurezza dei Sistemi Operativi		
Configurazione del controllo degli accessi amministrativi delegati su Linux tramite il file dei privilegi sudoers (sudo)		
Implementazione di firewall locali integrati nel sistema operativo (UFW, Firewalld, Windows Defender Firewall)		
Introduzione ai sistemi di controllo degli accessi obbligatori (MAC) per il confinamento dei processi (SELinux o AppArmor)		
Disattivazione dei servizi non necessari, chiusura delle porte inutilizzate e applicazione dei benchmark di sicurezza (es. CIS Benchmarks)		
Fondamenti di Virtualizzazione Hardware (Type-1 e Type-2 Hypervisor)		
Principi teorici della virtualizzazione, astrazione dell'hardware ed evoluzione dei data center moderni		
Caratteristiche e casi d'uso degli Hypervisor di Tipo 1 / Bare-Metal (es. VMware ESXi, Proxmox VE, Microsoft Hyper-V)		
Caratteristiche e casi d'uso degli Hypervisor di Tipo 2 / Hosted (es. Oracle VirtualBox, VMware Workstation)		
Tecniche di estensione della virtualizzazione della CPU nativa (Intel VT-x, AMD-V) e allocazione delle risorse virtuali (vCPU, vRAM) [1, 2]		
Creazione, Configurazione e Gestione di Macchine Virtuali (VM)		
Creazione guidata di una macchina virtuale: allocazione delle risorse, provisioning del disco (Thin vs Thick) e installazione dell'OS guest		
Configurazione delle schede di rete virtuali nelle diverse modalità di rete: NAT, Bridged, Host-Only e Internal LAN		
Utilizzo e gestione degli snapshot (punti di ripristino) delle VM: vantaggi operativi, impatto sulle performance e rischi correlati		
Tecniche di migrazione delle macchine virtuali, esportazione/importazione in formati standard (OVA/OVF) e clonazione [1]		
Virtualizzazione a Livello di Sistema Operativo: I Container (Docker)		
Differenze architetturali, vantaggi e overhead computazionale tra una Macchina Virtuale tradizionale e un Container		
Architettura di Docker: il demone Docker, il client CLI, le immagini (Images) e i container in esecuzione (Containers)		

Scrittura di file di configurazione Dockerfile per la creazione di immagini personalizzate e gestione del registro locale/remoto (Docker Hub)		
Gestione del ciclo di vita dei container, mappatura delle porte di rete e persistenza dei dati tramite i volumi (Volumes)		
Orchestrazione Base e Sicurezza degli Ambienti Virtuali		
Utilizzo di Docker Compose per la definizione, configurazione e l'avvio coordinato di applicazioni multi-container [1]		
Sicurezza nell'architettura dei container: esecuzione dei processi come utente non-root e isolamento tramite Namespace e Cgroups		
Hardening dell'ambiente di virtualizzazione: protezione dell'accesso all'interfaccia di gestione dell'hypervisor e cifratura dei dischi virtuali		
Strategie di backup e disaster recovery per infrastrutture virtualizzate (backup dei file di configurazione e dei dischi virtuali completi)		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
VAPT Defensive Side	**74**	Questa Unirà Formativa introduce i principi fondamentali della sicurezza difensiva (Blue Teaming), concentrandosi sulla visibilità e sul controllo delle infrastrutture IT. Gli studenti apprendono come raccogliere e centralizzare i log di sistema, configurare strumenti di monitoraggio in tempo reale, rilevare minacce complesse e strutturare una risposta tempestiva agli incidenti informatici. Lo scopo è quello di abilitare lo studente a progettare e gestire un'architettura di monitoraggio e difesa aziendale. Al termine del percorso, il tecnico superiore sarà in grado di analizzare i dati di tracciamento per identificare indicatori di compromissione (IoC), configurare sistemi di allarmistica e supportare le attività operative di un Security Operations Center (SOC).
Architettura del Logging e Centralizzazione dei Dati		
Configurazione delle sorgenti di log native nei sistemi operativi Linux (Syslog, Journald) e Windows (Event Logs).		
Protocolli e agenti di trasporto dei log per la raccolta remota sicura (es. Rsyslog, Winlogbeat, Filebeat).		
Standardizzazione, formattazione (JSON, CEF) e tecniche di parsing dei log per l'indicizzazione efficiente dei dati.		
Politiche di conservazione dei log (Data Retention), requisiti di integrità (hashing) e conformità normativa (es. GDPR).		
Sistemi SIEM (Security Information and Event Management)		
Architettura fondamentale di una piattaforma SIEM (es. Elastic Stack/Wazuh, Splunk, Microsoft Sentinel).		
Tecniche di ingestion dei dati, creazione di indici, cruscotti (Dashboard) e visualizzazioni grafiche per gli analisti SOC.		
Scrittura di regole di correlazione logica tra eventi provenienti da fonti eterogenee (es. firewall + Active Directory).		
Gestione dei falsi positivi, ottimizzazione delle soglie di allarme e prioritizzazione degli avvisi di sicurezza (Alerting).		
Endpoint Detection and Response (EDR) e Monitoraggio Host		
Limiti dei software antivirus tradizionali basati su firme rispetto ai sistemi EDR/XDR moderni.		
Monitoraggio avanzato dei processi, delle modifiche al registro e delle connessioni di rete tramite Sysmon su Windows.		
Configurazione e deployment di agenti di monitoraggio degli endpoint aziendali per il rilevamento di comportamenti anomali.		
Funzionalità di isolamento dell'host compromesso e raccolta automatizzata di telemetria forense da remoto.		
Monitoraggio della Rete e Network Traffic Analysis (NTA)		
Implementazione di sistemi IDS/IPS open-source basati su regole per l'ispezione del traffico di rete (es. Suricata, Snort).		
Raccolta e analisi dei metadati di rete e sessione tramite strumenti di Network Security Monitoring (es. Zeek/Bro).		
Identificazione di pattern di traffico malevoli (es. comunicazioni di Command & Control - C2, tentativi di esfiltrazione dati).		
Integrazione degli avvisi di rete all'interno della pipeline di monitoraggio centralizzata.		
Threat Intelligence e Indicatori di Compromissione (IoC)		
Definizione di Threat Intelligence e utilizzo dei feed di minacce (open-source, commerciali e standard STIX/TAXII).		
Utilizzo di piattaforme di condivisione delle informazioni sulle minacce (es. MISP - Malware Information Sharing Platform).		
Ricerca sistematica (Threat Hunting) di Indicatori di Compromissione (IoC) come hash di file malevoli, IP o domini sospetti nella rete.		
Applicazione della "Piramide del Dolore" (Pyramid of Pain) per colpire le tattiche e le procedure degli attaccanti.		
Gestione degli Incidenti e Incident Response (IR)		
Fasi del ciclo di vita di gestione di un incidente informatico secondo gli standard internazionali NIST SP 800-61 e SANS.		
Procedure operative standard (Playbook/Runbook) per scenari comuni (es. infezione da Ransomware, Phishing, violazione account).		
Tecniche di contenimento iniziale, eradicazione della minaccia e ripristino sicuro dei servizi aziendali (Recovery).		
Redazione del report post-incidente e analisi delle "lezioni apprese" per il miglioramento continuo delle difese.		
Automazione della Difesa e Piattaforme SOAR		
Architettura e scopo dei sistemi SOAR (Security Orchestration, Automation, and Response) nell'ecosistema difensivo.		
Automazione dei processi ripetitivi di arricchimento degli allarmi (es. controllo automatico degli IP su VirusTotal).		
Configurazione di azioni di risposta automatica guidata (es. blocco automatico di un IP sul firewall in caso di attacco DoS).		
Mappatura degli eventi rilevati e delle risposte difensive sul framework globale MITRE ATT&CK.		
Verifica finale		
Valutazione sulle competenze apprese durante il corso		
LABORATORI		
Laboratorio di preparazione project work	**18**	Il Project work rappresenta per lo studente la sperimentazione attiva di competenze tecniche (hard skill) acquisite in formazione e l'occasione di transfer di alcune fondamentali competenze trasversali (soft skill), indispensabili per avere successo nel mondo lavorativo e considerate sempre più determinanti nei processi di selezione del personale da parte dei recruiter aziendali (a titolo esemplificativo: autonomia, imprenditività, decision making, team working, public speaking, leadership, problem solving e orientamento ai risultati). Caratteristica principale del presente modello metodologico consiste nell'assegnare allo studente la realizzazione di un progetto relativo a obiettivi e a contesti organizzativi reali mediante l'elaborazione di un piano di azione anche in collegamento e coerenza rispetto al contesto formativo di riferimento. Il progetto può coinvolgere lo studente a titolo individuale o prevedere la sua partecipazione ai lavori di un team precostituito, richiedendo allo studente di sviluppare la parte di lavoro di sua competenza avendo la possibilità di essere coinvolto attivamente in tutte o in alcune fasi progettuali (ideazione, pianificazione/sviluppo, realizzazione e closing). Per quanto concerne la presente UF, oggetto del modulo è costituito da un'analisi delle attività e delle complessità operative legate all'esecuzione del progetto reale assegnato allo studente nell'ambito dello svolgimento dello stage curriculare (II annualità) presso l'azienda ICT in cui è stato inserito nell'ultima parte (integrante) del suo percorso formativo. In tal senso, il Tutor aziendale individuato dalla sede stage è chiamato a garantire una committenza chiara e coinvolta, fornendo allo studente feedback circostanziati rispetto all'avanzamento della commessa, organizzando meeting di gruppo (nel caso in cui lo studente faccia parte di una business unit) e momenti di confronto e restituzione tecnica one to one. Le ore di questa UF sono pianificate in aula e preventivamente comunicate allo studente dal Coordinamento didattico in concomitanza con l'avvio del periodo di stage. Un docente esperto del settore produttivo di riferimento è a disposizione per supervisionare e supportare lo studente nel lavoro di scrittura e presentazione finale del progetto (corredato da un pitch sintetico da illustrare alla commissione valutatrice in occasione della terza prova orale prevista dall'Esame finale per il conseguimento del titolo di Diploma di Tecnico superiore), verificando la congruenza tra gli obiettivi formativi del corso e i requisiti tecnici richiesti dal committente per la realizzazione a regola d'arte di un progetto reale, stante il contesto formativo di realizzazione.
Project work		
Rielaborazione dell'esperienza di stage		
individuare le opportunità di inserimento lavorativo		
Ricerca del materiale e delle fonti		
Linguaggio tecnico da utilizzare		
La stesura		
Presentazione finale		
Costruzione e presentazione della relazione di fine progetto		
Laboratorio Integrato	**32**	Il laboratorio integrato è concepito non solo come setting esperienziale mediante il quale consentire allo studente di misurare e mettere in pratica quanto appreso a livello teorico nel corso della formazione d'aula, ma altresì come metodologia innovativa di trasferimento soft skill, considerate sempre più determinanti nei processi di selezione del personale nel mondo del lavoro. Il laboratorio come metodologia di apprendimento, già sperimentato dallo studente durante lo svolgimento dell'UF "Learning by project" (svolta nella prima annualità) si intensifica in questa fase formativa in termini di dimensione del progetto commissionato e per la complessità di realizzazione. In tal senso, il raggiungimento dell'obiettivo finale non è più determinato dall'alto grado di collaborazione di un team composto da figure che svolgono mansioni diverse nell'ambito di una stessa verticalizzazione specialistica, bensì dalla cooperazione di un team che vede al suo interno la presenza di figure professionali tra loro distinte e complementari. Caratteristica principale è infatti la creazione di business unit all'interno delle quali gli studenti di diverse specializzazioni ICT sperimentano - come nella prassi aziendale - il team working e la valorizzazione della complementarità tra profili professionali che agiscono ruoli e possiedono competenze distinte nell'ambito di una stessa filiera produttiva o di filiere distinte chiamate a coordinarsi per il raggiunto di un obiettivo progettuale comune. Con la presente UF si intende formare lo studente a quelle che risultano essere le prerogative essenziali di un cross-functional team chiamato a ideare, sviluppare e prototipare un bene/servizio IT nella fattispecie corsuale della scrivente Fondazione, ma di utilizzo e funzionalità in altri settori produttivi. La prerogativa di questo tipo di organizzazione di lavoro in gruppo è quella di sfruttare l'esposizione dei diversi componenti a molteplici e diversificate prospettive, conoscenze e approcci, con la finalità di arricchire il processo creativo collettivo tramite il fenomeno di condivisione della conoscenza. L'obiettivo di un team cross-funzionale è quello di aumentare il livello del risultato creativo del progetto, aumentando esponenzialmente il livello di innovazione e creatività dell'entità in questione. In occasione di un briefing iniziale, un soggetto committente presenta a tutti i team di lavoro i principali requisiti tecnici e le modalità di esecuzione del prodotto/servizio richiesto. Un referente messo a disposizione dell'azienda è chiamato a garantire una committenza chiara e coinvolta, fornendo agli studenti feedback circostanziati rispetto all'avanzamento della commessa, organizzando meeting di gruppo, momenti di confronto e restituzione con i Team Leader individuati in autonomia dagli studenti all'interno di ogni team. Nel corso delle ore di attività svolte in ITS, i team si avvalgono della consulenza di un Mentor d'aula (uno di competenza per ogni profilo di specializzazione) che ha il compito di supportare gli studenti da un punto di vista tecnico e organizzativo e di garantire, stante il contesto formativo, la
KickOff/Brainstorming		
Finding, Insight e sfide di progetto		
Concept idea, selezione e sviluppo delle idee		
Applicazione delle Soft Skill		
Public Speaking		
Leadership		
Time management		
Project/Team management		

Realizzazione della componente Digital e Visual		realizzazione a regola d'arte del prodotto/servizio IT richiesto. La realizzazione del progetto commissionato impegna gli studenti per circa 120 ore, di cui soltanto 30 ore pianificate in aula in presenza del Mentor. Per raggiungere i risultati attesi, gli studenti lavorano in alternanza e in autonomia fuori dalle ore calendarizzate dal piano didattico ordinamentale. Al termine del Laboratorio tutti i Team sono invitati a presentare i risultati raggiunti partecipando a un pitch finale di presentazione del progetto. Contestualmente, trattandosi di un'unità formativa curriculare, ogni studente ottiene una valutazione finale attribuita dal Mentor d'aula di competenza del preciso corso di appartenenza. In tal senso, l'interdisciplinarietà del team si concretizzerà nella composizione dei team mediante la sinergica collaborazione fra gli studenti di seconde annualità. Inoltre, con riferimento al settore professionale d'appartenenza, verranno affrontati i valori di base della parità di trattamento e della lotta alla discriminazione nella vita sociale e nel mercato del lavoro.
Studio e realizzazione della parte Visual (Wireframes, UX, UI)		
Strutturazione strategia Digital Marketing (SEO, SEM, SEA) per la sponsorizzazione del progetto		
Presentazione finale		
Costruzione e presentazione della relazione di fine progetto		
Learning by Project - Soft Skill		
Modalità di gestione delle risorse ambientali ed energetiche		
Efficienza energetica		
Sfruttamento del Suolo		
Utilizzo sostenibile delle risorse idriche		
Nuovi modelli di consumo e di mobilità a basso impatto ambientale		
L'economia circolare		
Nuove forme di mobilità per le persone e le merci		
Problematiche sociali e sanitarie		
Impatto dell'inquinamento sulla salute dei cittadini		
Comunicazione e Interazione Interpersonale	**12**	La presente Unità formativa offre un'importante occasione in cui valorizzare la connessione tra il sapere acquisito in contesti applicativi e il sapere teorico-astratto, riuscendo di fatto a coniugare conoscenze tecniche con abilità e capacità personali, sociali e/o metodologiche, in situazioni di lavoro o di studio e nello sviluppo professionale e/o personale. Assegnato un prodotto/servizio IT da un'azienda committente, la caratteristica principale è la creazione di business unit all'interno delle quali ogni studente sperimenta la collaborazione di figure professionali dello stesso profilo in un team complementare in termini di competenze e abilità da mettere in campo. Nell'u.f. in oggetto, le soft skills ricoprono un ruolo centrale. Pertanto, a fianco di una quota di ore dedicate e affidate all'aspetto tecnico, la presente u.f. si focalizza nell'approfondimento delle competenze trasversali, in particolare delle competenze riferite alla comunicazione e interazione interpersonale e alla creatività e innovazione, considerate più strategiche nell'ottica del lavoro in team e della gestione di un progetto. In tal senso, sono organizzati appositi incontri -ex-ante, in itinere ed ex-post l'esecuzione delle attività- in presenza di un esperto della materia individuato dalla Fondazione. Al termine dell'unità formativa,in occasione di un pitch finale, ogni team presenterà i risultati del progetto all'azienda committente, ai tutor della Fondazione e al Mentor d'aula. Inoltre, con riferimento al settore professionale d'appartenenza, verranno affrontati i valori di base della parità di trattamento e della lotta alla discriminazione nella vita sociale e nel mercato del lavoro. In questa unità formativa saranno sviluppate le conoscenze essenziali "Modalità di gestione delle risorse ambientali ed energetiche" per la durata di due ore, "Nuovi modelli di consumo e di mobilità a basso impatto ambientale" per la durata di due ore e "Problematiche sociali e sanitarie" per la durata di un'ora relative all'Obiettivo "Contribuire allo sviluppo sostenibile e alla difesa dell'ambiente".
Comunicazione efficace		
Tecniche di negoziazione e persuasione		
Gestione e risoluzione dei conflitti		
Leadership e Gestione del Team		
Creatività e Innovazione		
Metodi per il pensiero creativo		
Strategie per la promozione dell'innovazione nel team		
Tecniche di problem solving		
Presentazione finale		
Costruzione e presentazione della relazione di fine progetto		
Learning by Project - Tech		
Principi di elaborazione testi		
Elementi teorici e pratici di formattazione e struttura per l'elaborazione di Report di carattere tecnico-scientifico		
Elementi di foglio elettronico		
Elementi teorici e pratici di formattazione e struttura per l'elaborazione di fogli elettroni da utilizzare in contesti di project management al fine di elaborare piani di azione progettuali per garantire cronoprogrammi in coerenza fra l'organizzazione interna del contesto lavorativo e i requirements/desiderata della committenza		
Elementi di presentazione multimediale		
Elementi teorici e pratici di formattazione e struttura per l'elaborazione di presentazioni multimediali da utilizzare in contesti di project management al fine di elaborare pitch finali di progetto efficaci termini di comunicazione e presentazione degli output finali di progetto in coerenza ai requirements di alto livello, deliverables e risultati attesi		
Progettazione e Pianificazione del Progetto	**24**	La presente Unità formativa offre un'importante occasione in cui valorizzare la connessione tra il sapere acquisito in contesti applicativi e il sapere teorico-astratto, riuscendo di fatto a coniugare conoscenze tecniche con abilità e capacità personali, sociali e/o metodologiche, in situazioni di lavoro o di studio e nello sviluppo professionale e/o personale. Assegnato un prodotto/servizio IT da un'azienda committente, la caratteristica principale è la creazione di business unit all'interno delle quali ogni studente sperimenta la collaborazione di figure professionali dello stesso profilo in un team complementare in termini di competenze e abilità da mettere in campo. Nell'u.f. in oggetto, le soft skill - affrontate con ore dedicate da un docente esperto - ricoprono un ruolo centrale, a fianco delle competenze tecniche, oggetto della presente unità formativa. Il docente esperto per la parte tecnica ricopre la figura di Mentor d'aula, occupandosi sia dell'aspetto di progettazione e pianificazione del progetto (assegnando ruoli e responsabilità nel team, definendo tempi e obiettivi ai gruppi di lavoro, organizzando SAL), sia del supporto degli studenti dal punto di vista tecnico (scelta delle tecnologie e degli strumenti da applicare, codifica e sviluppo del software ove necessario, testing e verifica della qualità della soluzione adottata), in un percorso di crescita e accompagnamento dello studente dall'inizio del progetto fino al pitch conclusivo. Inoltre, con riferimento al settore professionale d'appartenenza, verranno affrontati i valori di base della parità di trattamento e della lotta alla discriminazione nella vita sociale e nel mercato del lavoro. In questa unità formativa verranno inoltre affrontate le conoscenze essenziali "Principi elaborazione testi", "Elementi di foglio elettronico", "Elementi di presentazione multimediale" relative all'Obiettivo "Tecnologie informatiche"
Selezione del progetto		
Definizione degli obiettivi e pianificazione		
Assegnazione dei ruoli e responsabilità nel team		
Monitoraggio e aggiornamento del piano di progetto		
Sviluppo e Implementazione Tecnica		
Analisi dei requisiti e specifiche tecniche		
Scelta delle tecnologie e degli strumenti		
Codifica e sviluppo del software ove necessario		
Testing e qualità della soluzione adottata		
Documentazione tecnica e reportistica		
Presentazione finale		
Costruzione e presentazione della relazione di fine progetto		
PROFESSIONALE		
Stage	**630**	/
Esame Finale		
Esame Finale	**10**	/
Ore Totali percorso	**1.800**	