ENISA

ECSF

QUADRO EUROPEO DELLE COMPETENZE IN MATERIA DI CYBERSICUREZZA
SETTEMBRE 2022

INFORMAZIONI SU ENISA

L'Agenzia dell'Unione europea per la cybersicurezza (ENISA) nasce con l'obiettivo del conseguimento di un elevato livello comune di cybersicurezza in tutta Europa. Istituita nel 2004 e rafforzata attraverso il Cybersecurity Act, l'Agenzia dell'Unione europea per la cybersicurezza contribuisce alla politica informatica dell'UE, rafforza l'affidabilità dei prodotti, dei servizi e dei processi ICT con sistemi di certificazione della cybersicurezza, coopera con gli Stati membri e con gli organismi dell'UE e aiuta l'Europa a prepararsi alle sfide informatiche di domani. Attraverso la condivisione delle conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con le principali parti interessate per rafforzare la fiducia nell'economia connessa, rafforzare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sul suo lavoro sono disponibili sul sito istituzionale dell'Agenzia all'indirizzo www.enisa.europa.eu.

CONTATTI
Per contattare l'editore si prega di utilizzare l'indirizzo email: euskills@enisa.europa.eu.

RICONOSCIMENTI
Questo lavoro è il risultato dell'opinione di esperti e dell'accordo del gruppo specificamente dedicato al quadro delle competenze, composto da: Agata Bekier, Vladlena BENSON, Jutta BREYER, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku Korkiakoski, Csaba Krasznay, Haralambos Mouratidis, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta Polemi*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN e Jan Hajny.Questo quadro è il risultato dell'opinione di esperti e dell'accordo del gruppo di lavoro ad hoc sul quadro delle competenze composto da Agata Bekier, Vladlena BENSON, Jutta BREYER,*

Fabio DI FRANCO e Athanasios GRAMMATOPOULOS hanno guidato questa attività per ENISA.

Relatore del gruppo di lavoro ad hoc sul quadro europeo delle competenze in materia di cybersicurezza

NOTA LEGALE

La presente pubblicazione rappresenta le opinioni e le interpretazioni dell'ENISA, salvo diversa indicazione. Non approva un obbligo normativo dell'ENISA o degli organismi dell'ENISA ai sensi del Regolamento UE 2019/881.

L'ENISA ha il diritto di modificare, aggiornare o rimuovere la pubblicazione o qualsiasi suo contenuto. La pubblicazione è destinata esclusivamente a scopo informativo e deve essere accessibile gratuitamente. Tutti i riferimenti ad essa o al suo uso (nel suo insieme o in parte) devono contenere l'ENISA come fonte.

Fonti di terze parti sono citate a seconda dei casi. L'ENISA non è responsabile per il contenuto delle fonti esterne, compresi i siti web esterni di cui alla presente pubblicazione.

Né l'ENISA né chiunque agisca per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute nella presente pubblicazione.

* *
* ENISA
*

AVVISO SUL COPYRIGHT

ISBN: 978-9204-584-5 — DOI: 10.2824/85953

1. PROFILI

1.1 RESPONSABILE DELLA SICUREZZA DELLE INFORMAZIONI (CISO)

Titolo del profilo	Responsabile della sicurezza delle informazioni (CISO)
Titolo/i alternativo/i	Responsabile della sicurezza informatica (ISO) Responsabile della sicurezza delle informazioni Head of Information Security Officer IT/ICT Security Officer
Sintesi	Gestisce la strategia di sicurezza informatica di un'organizzazione e la sua implementazione per garantire che i sistemi, i servizi e le risorse digitali siano adeguatamente sicuri e protetti.
Missione	Definisce, mantiene e comunica la visione, la strategia, le politiche e le procedure in materia di sicurezza informatica. Gestisce l'attuazione della politica di sicurezza informatica in tutta l'organizzazione. Assicura lo scambio di informazioni con le autorità esterne e gli organismi professionali.
Prodotto/i da fornire	• Strategia per la cybersicurezza • Politica in materia di cybersicurezza
Compito/i principale/i	• Definire, implementare, comunicare e mantenere obiettivi, requisiti, strategie, politiche di sicurezza informatica in linea con la strategia aziendale a supporto degli obiettivi organizzativi • Preparare e presentare la visione, le strategie e le politiche in materia di sicurezza informatica per l'approvazione da parte dell'alta dirigenza dell'organizzazione e garantirne l'esecuzione • Supervisionare l'applicazione e il miglioramento del sistema di gestione della sicurezza delle informazioni (ISMS) • Educare l'alta dirigenza sui rischi di sicurezza informatica, le minacce e il loro impatto sull'organizzazione • Assicurarsi che l'alta dirigenza approvi i rischi per la sicurezza informatica dell'organizzazione • Sviluppare piani di cybersicurezza • Sviluppare relazioni con le autorità e le comunità legate alla cybersicurezza • Segnalare incidenti di sicurezza informatica, rischi, risultati all'alta dirigenza • Monitorare i progressi nella sicurezza informatica • Risorse sicure per attuare la strategia in materia di cybersicurezza • Negoziare il bilancio per la cybersicurezza con l'alta dirigenza • Garantire la resilienza dell'organizzazione agli incidenti informatici • Gestire lo sviluppo continuo di capacità all'interno dell'organizzazione
Abilità chiave	• Valutare e migliorare la posizione di sicurezza informatica di un'organizzazione • Analizzare e implementare politiche, certificazioni, standard, metodologie e framework in materia di cybersicurezza • Analizzare e rispettare le leggi, i regolamenti e le normative in materia di sicurezza informatica • Attuare le raccomandazioni e le migliori pratiche in materia di cybersicurezza • Gestire le risorse per la sicurezza informatica • Sviluppare, sostenere e guidare l'esecuzione di una strategia di sicurezza informatica • Influenzare la cultura della sicurezza informatica di un'organizzazione • Progettare, applicare, monitorare e rivedere il sistema di gestione della sicurezza delle informazioni (ISMS) direttamente o dirigendo l'outsourcing • Rivedere e migliorare i documenti di sicurezza, i rapporti, gli SLA e garantire gli obiettivi di sicurezza • Identificare e risolvere i problemi connessi alla cybersicurezza • Stabilire un piano di sicurezza informatica • Comunicare, coordinare e cooperare con le parti interessate interne ed esterne • Anticipare le modifiche necessarie alla strategia di sicurezza delle informazioni

	• Definire e applicare modelli di maturità per la gestione della sicurezza informatica • Anticipare le minacce, le esigenze e le sfide future in materia di cybersicurezza • Motivare e incoraggiare le persone	
Conoscenze chiave	• Politiche in materia di cybersicurezza • Norme, metodologie e quadri di cybersicurezza • Raccomandazioni e migliori pratiche in materia di cybersicurezza • Leggi, regolamenti e legislazioni in materia di cybersicurezza • Certificazioni legate alla cybersicurezza • Requisiti etici dell'organizzazione della cybersicurezza • Modelli di maturità della cybersicurezza • Procedure di cybersicurezza • Gestione delle risorse • Pratiche di gestione • Norme, metodologie e quadri di gestione del rischio	
e-Competences (dall'e-CF)	A.7. Monitoraggio delle tendenze tecnologiche D.1. Sviluppo della strategia di sicurezza dell'informazione E.3. Gestione del rischio E.8. Gestione della sicurezza delle informazioni E.9. Is-Governance	Livello 4 Livello 5 Livello 4 Livello 4 Livello 5

1.2 SOCCORRITORE DI INCIDENTI INFORMATICI

Titolo del profilo	Risponditore di incidenti informatici
Titolo/i alternativo/i	Gestore di incidenti informatici Esperto di crisi informatica Ingegnere di risposta agli incidenti Analista del Security Operations Center (SOC) Cyber Fighter/Difensore Analisi delle operazioni di sicurezza (SOC Analyst) Responsabile SIEM per la sicurezza informatica
Sintesi	Monitorare lo stato della sicurezza informatica dell'organizzazione, gestire gli incidenti durante gli attacchi informatici e assicurare il proseguimento delle operazioni dei sistemi ICT.
Missione	Monitora e valuta lo stato della cybersicurezza dei sistemi. Analizza, valuta e attenua l'impatto degli incidenti di cybersicurezza. Identifica le cause profonde degli incidenti informatici e gli attori malintenzionati. Secondo il piano di risposta agli incidenti dell'organizzazione, ripristina le funzionalità dei sistemi e dei processi a uno stato operativo, raccogliendo prove e documentando le azioni intraprese.
Prodotto/i da fornire	• Piano di risposta agli incidenti • Report sugli incidenti informatici
Compito/i principale/i	• Contribuire allo sviluppo, alla manutenzione e alla valutazione del piano di risposta agli incidenti • Sviluppare, attuare e valutare le procedure relative alla gestione degli incidenti • Identificare, analizzare, mitigare e comunicare gli incidenti di sicurezza informatica • Valutare e gestire le vulnerabilità tecniche • Misurare il rilevamento degli incidenti di cybersicurezza e l'efficacia della risposta • Valutare la resilienza dei controlli e delle azioni di mitigazione della cybersicurezza intraprese dopo un incidente in materia di cybersicurezza o violazione dei dati • Adottare e sviluppare tecniche di test di gestione degli incidenti • Stabilire procedure per l'analisi dei risultati degli incidenti e la segnalazione della gestione degli incidenti • Documentare l'analisi dei risultati degli incidenti e le azioni di gestione degli incidenti • Collaborare con i centri operativi sicuri (SOC) e i gruppi di risposta agli incidenti di sicurezza informatica (CSIRT) • Cooperare con il personale chiave per la segnalazione di incidenti di sicurezza conformemente al quadro giuridico applicabile
Abilità chiave	• Praticare tutti gli aspetti tecnici, funzionali e operativi della gestione e della risposta degli incidenti di cybersicurezza • Raccogliere, analizzare e correlare le informazioni sulle minacce informatiche provenienti da più fonti • Lavorare su sistemi operativi, server, cloud e infrastrutture pertinenti • Lavori sotto pressione • Comunicare, presentare e riferire alle parti interessate • Gestire e analizzare i file di registro
Conoscenze chiave	• Incidente movimentazione norme, metodologie e quadri di riferimento • Incidente movimentazione raccomandazioni e migliori pratiche • Incidente movimentazione strumenti • Incidente movimentazione procedure di comunicazione • Sicurezza dei sistemi operativi • Sicurezza delle reti informatiche • Minacce informatiche • Procedure di attacco alla cybersicurezza • Vulnerabilità dei sistemi informatici • Certificazioni legate alla cybersicurezza • Leggi, regolamenti e legislazioni in materia di cybersicurezza • Funzionamento dei centri operativi sicuri (SOC) • Funzionamento dei team di risposta agli incidenti di sicurezza informatica (CSIRTs)
e-Competences (dall'e-CF)	A.7. Monitoraggio delle tendenze tecnologiche Livello 3 B.2. Integrazione dei componenti Livello 2

	B.3. Test B.5. Produzione di documentazione C.4. Gestione dei problemi	Livello 3 Livello 3 Livello 4

1.3 CYBER LEGAL, POLICY & COMPLIANCE OFFICER

Titolo del profilo	Cyber Legal, Policy & Compliance Officer
Titolo/i alternativo/i	Responsabile della protezione dei dati (RPD) Responsabile della protezione della privacy Consulente di diritto cibernetico Consulente legale informatico Responsabile della governance dell'informazione Responsabile della conformità dei dati Funzionario legale per la sicurezza informatica Responsabile della conformità IT/ICT Consulente per la conformità al rischio di governance (GRC)
Sintesi	Gestisce la conformità con gli standard relativi alla sicurezza informatica, i quadri giuridici e normativi sulla base della strategia e dei requisiti legali dell'organizzazione.
Missione	Supervisiona e assicura la conformità con i quadri legali, normativi e normativi relativi alla sicurezza informatica e ai dati in linea con la strategia e i requisiti legali dell'organizzazione. Contribuisce alle azioni relative alla protezione dei dati dell'organizzazione. Fornisce consulenza legale nello sviluppo dei processi di governance della sicurezza informatica dell'organizzazione e raccomanda strategie/soluzioni di risanamento per garantire la conformità.
Prodotto/i da fornire	• Manuale di conformità • Relazione sulla conformità
Compito/i principale/i	• Garantire il rispetto e fornire consulenza legale e orientamenti in materia di privacy dei dati e standard, leggi e regolamenti in materia di protezione dei dati • Individuare e documentare le lacune in materia di conformità • Condurre valutazioni d'impatto sulla privacy e sviluppare, mantenere, comunicare e formare le politiche sulla privacy, le procedure • Applicare e sostenere il programma di protezione e privacy dei dati dell'organizzazione • Garantire che i titolari dei dati, i titolari del trattamento, i responsabili del trattamento, i soggetti, i partner interni o esterni e le entità siano informati in merito ai loro diritti, obblighi e responsabilità in materia di protezione dei dati • Fungere da punto di contatto chiave per gestire domande e reclami relativi al trattamento dei dati • Assistenza nella progettazione, implementazione, auditing e test di conformità al fine di garantire la conformità alla cybersicurezza e alla privacy • Monitorare gli audit e le attività di formazione in materia di protezione dei dati • Cooperare e condividere informazioni con le autorità e i gruppi professionali • Contribuire allo sviluppo della strategia, delle politiche e delle procedure in materia di cybersicurezza dell'organizzazione • Sviluppare e proporre una formazione di sensibilizzazione del personale per raggiungere la conformità e promuovere una cultura della protezione dei dati all'interno dell'organizzazione
Abilità chiave	• Comprensione completa della strategia aziendale, dei modelli e dei prodotti e capacità di prendere in considerazione i requisiti legali, normativi e standard • Eseguire pratiche di vita lavorativa delle questioni relative alla protezione dei dati e alla privacy coinvolte nell'attuazione dei processi organizzativi, della finanza e della strategia aziendale • Guidare lo sviluppo di politiche e procedure adeguate in materia di cybersicurezza e privacy che integrino le esigenze aziendali e i requisiti giuridici; assicurarne ulteriormente l'accettazione, la comprensione e l'attuazione e comunicarla tra le parti interessate • Condurre, monitorare e rivedere le valutazioni d'impatto sulla privacy utilizzando standard, quadri, metodologie e strumenti riconosciuti • Spiegare e comunicare gli argomenti relativi alla protezione dei dati e alla privacy alle parti interessate e agli utenti • Comprendere, praticare e rispettare i requisiti e gli standard etici • Comprendere le implicazioni delle modifiche del quadro giuridico alla strategia e alle politiche in materia di sicurezza informatica e protezione dei dati dell'organizzazione • Collaborare con altri membri del team e colleghi
Conoscenze chiave	• Leggi, regolamenti e normative in materia di sicurezza informatica

	• Norme, metodologie e quadri di cybersicurezza • Politiche in materia di cybersicurezza • Requisiti legali, normativi e legislativi in materia di conformità, raccomandazioni e migliori pratiche • Norme, metodologie e quadri di valutazione dell'impatto sulla vita privata	
e-Competences (dall'e-CF)	A.1. Sistemi informativi e strategia aziendale Allineamento D.1. Sviluppo della strategia di sicurezza dell'informazione E.8. Gestione della sicurezza delle informazioni E.9. Is-Governance	Livello 4 Livello 4 Livello 3 Livello 4

1.4 SPECIALISTA DI CYBER THREAT INTELLIGENCE

Titolo del profilo	Cyber Threat Intelligence Specialista
Titolo/i alternativo/i	Cyber Intelligence Analyst Cyber Threat Modeller
Sintesi	Raccogliere, elaborare, analizzare dati e informazioni per produrre report di intelligence attuabili e diffonderli agli stakeholder target.
Missione	Gestisce il ciclo di vita dell'intelligence sulle minacce informatiche, compresa la raccolta, l'analisi e la produzione di informazioni sulle minacce informatiche e la diffusione alle parti interessate della sicurezza e alla comunità CTI, a livello tattico, operativo e strategico. Identifica e monitora le tattiche, le tecniche e le procedure (TTP) utilizzate dagli attori delle minacce informatiche e le loro tendenze, monitora le attività degli attori delle minacce e osserva come gli eventi non informatici possono influenzare le azioni informatiche.
Prodotto/i da fornire	• Manuale di Cyber Threat Intelligence • Rapporto sulle minacce informatiche
Compito/i principale/i	• Sviluppare, implementare e gestire la strategia di cyber threat intelligence dell'organizzazione • Sviluppare piani e procedure per gestire l'intelligence sulle minacce • Tradurre i requisiti aziendali in requisiti di intelligence • Implementare la raccolta di informazioni sulle minacce, l'analisi e la produzione di intelligence attuabile e la diffusione agli stakeholder della sicurezza • Identificare e valutare gli attori delle minacce informatiche che prendono di mira l'organizzazione • Identificare, monitorare e valutare le tattiche, le tecniche e le procedure (TTP) utilizzate dagli attori delle minacce informatiche analizzando dati, informazioni e intelligence open-source e proprietari • Produrre report fruibili basati su dati di intelligence sulle minacce • Elaborare e consigliare piani di mitigazione a livello tattico, operativo e strategico • Coordinarsi con le parti interessate per condividere e consumare informazioni sulle minacce informatiche pertinenti • Sfruttare i dati di intelligence per supportare e assistere nella modellazione delle minacce, raccomandazioni per la mitigazione dei rischi e la caccia alle minacce informatiche • Articolare e comunicare l'intelligenza apertamente e pubblicamente a tutti i livelli • Trasmettere l'adeguata gravità della sicurezza spiegando l'esposizione al rischio e le sue conseguenze alle parti interessate non tecniche
Abilità chiave	• Collaborare con altri membri del team e colleghi • Raccogliere, analizzare e correlare le informazioni sulle minacce informatiche provenienti da più fonti • Identificare gli attori delle minacce TTP e campagne • Automatizzare le procedure di gestione dell'intelligence sulle minacce • Condurre analisi tecniche e reportistica • Identificare eventi non informatici con implicazioni sulle attività informatiche • Modelli di minacce, attori e TTP • Comunicare, coordinare e cooperare con le parti interessate interne ed esterne • Comunicare, presentare e riferire alle parti interessate • Utilizzare e applicare piattaforme e strumenti CTI
Conoscenze chiave	• Sicurezza dei sistemi operativi • Sicurezza delle reti informatiche • Controlli e soluzioni di sicurezza informatica • Programmazione informatica • Cyber Threat Intelligence (CTI) che condividono standard, metodologie e framework • Procedure di divulgazione responsabile delle informazioni • Conoscenze cross-domain e border-main relative alla cybersicurezza • Minacce informatiche • Attori delle minacce informatiche • Procedure di attacco alla cybersicurezza • Minacce informatiche avanzate e persistenti (APT) • Tattiche, tecniche e procedure (TTP) • Certificazioni legate alla cybersicurezza

e-Competences (dall'e-CF)	B.5. Produzione di documentazione D.7. Scienza dei dati e analisi D.10. Gestione delle informazioni e della conoscenza E.4. Gestione delle relazioni E.8. Gestione della sicurezza delle informazioni	Livello 3 Livello 4 Livello 4 Livello 3 Livello 4

1.5 ARCHITETTO DELLA SICUREZZA INFORMATICA

Titolo del profilo	Architetto della sicurezza informatica
Titolo/i alternativo/i	Progettista di soluzioni di sicurezza informatica Progettista di sicurezza informatica Architetto di sicurezza dei dati
Sintesi	Progetta e progetta soluzioni di security-by-design (infrastrutture, sistemi, risorse, software, hardware e servizi) e controlli di sicurezza informatica.
Missione	Progetta soluzioni basate su principi di security-by-design e privacy-by-design. Crea e migliora continuamente modelli architettonici e sviluppa adeguate documentazioni e specifiche architettoniche. Coordinare lo sviluppo, l'integrazione e la manutenzione sicuri delle componenti della cybersicurezza in linea con gli standard e altri requisiti correlati.
Prodotto/i da fornire	• Diagramma dell'architettura della sicurezza informatica • Relazione sui requisiti di cybersicurezza
Compito/i principale/i	• Progettare e proporre un'architettura sicura per implementare la strategia dell'organizzazione • Sviluppare l'architettura di sicurezza informatica dell'organizzazione per soddisfare i requisiti di sicurezza e privacy • Produrre documentazione architettonica e specifiche • Presentare alle parti interessate un'architettura di sicurezza di alto livello • Creare un ambiente sicuro durante il ciclo di vita di sistemi, servizi e prodotti • Coordinare lo sviluppo, l'integrazione e la manutenzione delle componenti della cybersicurezza garantendo le specifiche di cybersicurezza • Analizzare e valutare la sicurezza informatica dell'architettura dell'organizzazione • Garantire la sicurezza delle architetture della soluzione attraverso revisioni e certificazioni di sicurezza • Collaborare con altri team e colleghi • Valutare l'impatto delle soluzioni di cybersecurity sulla progettazione e le prestazioni dell'architettura dell'organizzazione • Adattare l'architettura dell'organizzazione alle minacce emergenti • Valutare l'architettura implementata per mantenere un adeguato livello di sicurezza
Abilità chiave	• Condurre analisi dei requisiti di sicurezza degli utenti e delle aziende • Disegnare specifiche architettoniche e funzionali per la sicurezza informatica • Decomporre e analizzare i sistemi per sviluppare requisiti di sicurezza e privacy e identificare soluzioni efficaci • Progettare sistemi e architetture basate su sicurezza e privacy fin dalla progettazione e dai principi di sicurezza informatica predefiniti • Guida e comunica con gli implementatori e il personale IT/OT • Comunicare, presentare e riferire alle parti interessate • Proporre architetture di cybersicurezza basate sulle esigenze e sul bilancio delle parti interessate • Selezionare specifiche, procedure e controlli appropriati • Costruire resilienza contro i punti di fallimento in tutta l'architettura • Coordinare l'integrazione delle soluzioni di sicurezza
Conoscenze chiave	• Certificazioni legate alla cybersicurezza • Raccomandazioni e migliori pratiche in materia di cybersicurezza • Norme, metodologie e quadri di cybersicurezza • Analisi dei requisiti connessi alla cybersicurezza • Ciclo di vita sicuro dello sviluppo • Modelli di riferimento dell'architettura di sicurezza • Tecnologie connesse alla cybersicurezza • Controlli e soluzioni di sicurezza informatica • Rischi per la cybersicurezza • Minacce informatiche • Tendenze in materia di cybersicurezza • Requisiti legali, normativi e legislativi in materia di conformità, raccomandazioni e migliori pratiche • Procedure di cybersicurezza legacy • Tecnologie per migliorare la privacy (PET)

	• Privacy-by-design standard, metodologie e framework	
e-Competences (dall'e-CF)	A.5. Progettazione dell'architettura A.6. Progettazione dell'applicazione 8.1. Sviluppo delle applicazioni 8.3. Test 8.6. Ingegneria dei sistemi ICT	Livello 5 Livello 3 Livello 3 Livello 3 Livello 4

1.6 REVISORE DELLA CYBERSICUREZZA

Titolo del profilo	Revisore della cybersicurezza	
Titolo/i alternativo/i	Revisore della sicurezza delle informazioni (IT o Legal Auditor) Governance Risk Compliance (GRC) Auditor Cybersecurity Audit Manager Procedure e processi di sicurezza informatica Auditor Information Security Risk and Compliance Auditor Analista della valutazione della protezione dei dati	
Sintesi	Eseguire audit di sicurezza informatica sull'ecosistema dell'organizzazione. Garantire la conformità con le informazioni legali, regolamentari, politiche, i requisiti di sicurezza, gli standard di settore e le migliori pratiche.	
Missione	Conduce revisioni indipendenti per valutare l'efficacia dei processi e dei controlli e la conformità generale con le politiche dei quadri giuridici e normativi dell'organizzazione. Valuta, testa e verifica i prodotti relativi alla sicurezza informatica (sistemi, hardware, software e servizi), funzioni e politiche che garantiscono la conformità alle linee guida, agli standard e alle normative.	
Prodotto/i da fornire	• Piano di audit della cybersicurezza • Relazione di audit sulla cybersicurezza	
Compito/i principale/i	• Sviluppare la politica di audit, le procedure, gli standard e le linee guida dell'organizzazione • Stabilire le metodologie e le pratiche utilizzate per l'audit dei sistemi • Stabilire l'ambiente target e gestire le attività di auditing • Definire l'ambito di applicazione dell'audit, gli obiettivi e i criteri da sottoporre a revisione contabile • Elaborare un piano di audit che descriva i quadri, le norme, la metodologia, le procedure e le prove di audit • Rivedere l'obiettivo di valutazione, gli obiettivi e i requisiti di sicurezza in base al profilo di rischio • Verifica della conformità con le leggi e i regolamenti applicabili in materia di cybersicurezza • Verifica della conformità alle norme applicabili in materia di cybersicurezza • Eseguire il piano di audit e raccogliere prove e misurazioni • Mantenere e proteggere l'integrità dei registri di audit • Elaborare e comunicare relazioni di valutazione della conformità, affidabilità, audit,	
Abilità chiave	• Organizzare e lavorare in modo sistematico e deterministico sulla base di prove • Seguire e mettere in pratica quadri, standard e metodologie di audit • Applicare strumenti e tecniche di auditing • Analizzare i processi aziendali, valutare e rivedere la sicurezza software o hardware, nonché i controlli tecnici e organizzativi • Decomporre e analizzare i sistemi per individuare le debolezze e i controlli inefficaci • Comunicare, spiegare e adattare i requisiti legali e normativi e le esigenze aziendali • Raccogliere, valutare, mantenere e proteggere le informazioni di auditing • Audit con integrità, imparzialità e indipendenza	
Conoscenze chiave	• Controlli e soluzioni di sicurezza informatica • Requisiti legali, normativi e legislativi in materia di conformità, raccomandazioni e migliori pratiche • Monitorare, testare e valutare l'efficacia dei controlli di cybersicurezza • Norme, metodologie e quadri di valutazione della conformità • Norme, metodologie e quadri di revisione contabile • Norme, metodologie e quadri di cybersicurezza • Certificazione relativa all'audit • Certificazioni legate alla cybersicurezza	
e-Competences (dall'e-CF)	B.3. Test B.5. Produzione di documentazione E.3. Gestione del rischio E.6 Gestione della qualità delle TIC	Livello 4 Livello 3 Livello 4 Livello 4
	E.8. Gestione della sicurezza delle informazioni	Livello 4

1.7 EDUCATORE DELLA SICUREZZA INFORMATICA

Titolo del profilo	Educatore della sicurezza informatica	
Titolo/i alternativo/i	Specialista di sensibilizzazione alla sicurezza informatica Allenatore della sicurezza informatica Facoltà di Cybersecurity (Professore, Docente)	
Sintesi	Migliora le conoscenze, le abilità e le competenze in materia di sicurezza informatica degli esseri umani.	
Missione	Progetta, sviluppa e conduce programmi di sensibilizzazione, formazione e istruzione in materia di cybersicurezza e protezione dei dati. Utilizza metodi, tecniche e strumenti di insegnamento e formazione adeguati per comunicare e migliorare la cultura, le capacità, le conoscenze e le competenze delle risorse umane in materia di cybersicurezza. Promuove l'importanza della sicurezza informatica e la consolida nell'organizzazione.	
Prodotto/i da fornire	• Programma di sensibilizzazione alla sicurezza informatica • Materiale di formazione sulla cybersicurezza	
Compito/i principale/i	• Sviluppare, aggiornare e fornire programmi di cybersicurezza e protezione dei dati e materiale didattico per la formazione e la sensibilizzazione sulla base di contenuti, metodi, strumenti, necessità di tirocinanti • Organizzare, progettare e realizzare attività di sensibilizzazione in materia di cybersicurezza e protezione dei dati, seminari, corsi, formazione pratica • Monitorare, valutare e segnalare l'efficacia della formazione • Valutare e segnalare le prestazioni del tirocinante • Trovare nuovi approcci per l'istruzione, la formazione e la sensibilizzazione • Progettare, sviluppare e fornire simulazioni di sicurezza informatica, laboratori virtuali o ambienti di cyber range • Fornire orientamenti sui programmi di certificazione della sicurezza informatica per gli individui • Mantenere e migliorare continuamente le competenze; incoraggiare e potenziare il miglioramento continuo delle capacità e delle capacità in materia di cybersicurezza	
Abilità chiave	• Individuare le esigenze in materia di sensibilizzazione, formazione e istruzione in materia di cybersicurezza • Progettare, sviluppare e fornire programmi di apprendimento per soddisfare le esigenze in materia di cybersicurezza • Sviluppare esercitazioni di sicurezza informatica, comprese simulazioni utilizzando ambienti di cyber range • Fornire formazione per le certificazioni professionali in materia di cybersicurezza e protezione dei dati • Utilizzare le risorse formative esistenti in materia di cybersicurezza • Sviluppare programmi di valutazione per le attività di sensibilizzazione, formazione e istruzione	
Conoscenze chiave	• Standard, metodologie e quadri pedagogici • Sensibilizzazione alla cybersicurezza, sviluppo di programmi di istruzione e formazione • Certificazioni legate alla cybersicurezza • Norme, metodologie e quadri di istruzione e formazione in materia di cybersicurezza • Leggi, regolamenti e legislazioni in materia di cybersicurezza • Raccomandazioni e migliori pratiche in materia di cybersicurezza • Norme, metodologie e quadri di cybersicurezza • Controlli e soluzioni di sicurezza informatica	
e-Competences (dall'e-CF)	D.3. Disposizioni in materia di istruzione e formazione D.9. Sviluppo del personale E.8. Gestione della sicurezza delle informazioni	Livello 3 Livello 3 Livello 3

1.8 ESECUTORE DELLA CYBERSICUREZZA

Titolo del profilo	Implementazione della sicurezza informatica	
Titolo/i alternativo/i	Implementazione della sicurezza delle informazioni Esperto di soluzioni di sicurezza informatica Sviluppatore di sicurezza informatica Ingegnere della sicurezza informatica Sviluppo, sicurezza e operazioni (DevSecOps) Ingegnere	
Sintesi	Sviluppare, implementare e gestire soluzioni di sicurezza informatica (sistemi, risorse, software, controlli e servizi) su infrastrutture e prodotti.	
Missione	Fornisce lo sviluppo tecnico, l'integrazione, il test, l'implementazione, il funzionamento, la manutenzione, il monitoraggio e il supporto delle soluzioni di sicurezza informatica. Garantisce l'aderenza alle specifiche e ai requisiti di conformità, assicura prestazioni solide e risolve i problemi tecnici richiesti nelle soluzioni relative alla sicurezza informatica dell'organizzazione (sistemi, risorse, software, controlli e servizi), infrastrutture e prodotti.	
Prodotto/i da fornire	• Soluzioni per la sicurezza informatica	
Compito/i principale/i	• Sviluppare, implementare, mantenere, aggiornare, testare i prodotti di sicurezza informatica • Fornire supporto relativo alla sicurezza informatica a utenti e clienti • Integrare le soluzioni di sicurezza informatica e assicurarne il buon funzionamento • Configurare in modo sicuro sistemi, servizi e prodotti • Mantenere e aggiornare la sicurezza di sistemi, servizi e prodotti • Attuare procedure e controlli in materia di cybersicurezza • Monitorare e assicurare le prestazioni dei controlli di cybersicurezza attuati • Documento e relazione sulla sicurezza di sistemi, servizi e prodotti • Lavorare a stretto contatto con il personale IT/OT sulle azioni connesse alla cybersicurezza • Implementare, applicare e gestire le patch ai prodotti per affrontare le vulnerabilità	
Abilità chiave	• Comunicare, presentare e riferire alle parti interessate • Integrare soluzioni di sicurezza informatica nell'infrastruttura dell'organizzazione • Configurare le soluzioni in base ai criteri di sicurezza dell'organizzazione • Valutare la sicurezza e le prestazioni delle soluzioni • Sviluppare codici, script e programmi • Identificare e risolvere i problemi connessi alla cybersicurezza • Collaborare con altri membri del team e colleghi	
Conoscenze chiave	• Ciclo di vita sicuro dello sviluppo • Programmazione informatica • Sicurezza dei sistemi operativi • Sicurezza delle reti informatiche • Controlli e soluzioni di sicurezza informatica • Pratiche di sicurezza offensive e difensive • Raccomandazioni di codifica sicure e migliori pratiche • Raccomandazioni e migliori pratiche in materia di cybersicurezza • Norme, metodologie e quadri di prova • Procedure di prova • Tecnologie connesse alla cybersicurezza	
e-Competences (dall'e-CF)	A.5. Progettazione dell'architettura A.6. Progettazione dell'applicazione 8.1. Sviluppo delle applicazioni 8.3. Test 8.6. Ingegneria dei sistemi ICT	Livello 3 Livello 3 Livello 3 Livello 3 Livello 4

1.9 RICERCATORE IN MATERIA DI CYBERSICUREZZA

Titolo del profilo	Ricercatore sulla sicurezza informatica	
Titolo/i alternativo/i	Ingegnere di ricerca sulla sicurezza informatica Chief Research Officer (CRO) in materia di sicurezza informatica Senior Research Officer in cybersecurity Responsabile Ricerca e Sviluppo (R & S) in materia di sicurezza informatica Personale scientifico nella sicurezza informatica Responsabile della ricerca e dell'innovazione/Esperto in materia di sicurezza informatica Ricercatore in cybersecurity	
Sintesi	Ricercare il settore della cybersicurezza e incorporare i risultati nelle soluzioni di cybersicurezza.	
Missione	Conduce ricerche fondamentali/di base e applicate e facilita l'innovazione nel settore della cybersicurezza attraverso la cooperazione con altre parti interessate. Analizza le tendenze e i risultati scientifici in materia di sicurezza informatica.	
Prodotto/i da fornire	• Pubblicazione in Cybersecurity	
Compito/i principale/i	• Analizzare e valutare le tecnologie, le soluzioni, gli sviluppi e i processi di sicurezza informatica • Condurre attività di ricerca, innovazione e sviluppo su temi connessi alla cybersicurezza• Manifestare e generare idee di ricerca e innovazione • Portare avanti l'attuale stato dell'arte in materia di cybersicurezza • Assistere nello sviluppo di soluzioni innovative legate alla cybersicurezza • Condurre esperimenti e sviluppare una prova di concetto, piloti e prototipi per soluzioni di sicurezza informatica • Selezionare e applicare quadri, metodi, standard, strumenti e protocolli, tra cui un edificio e testare una prova di concetto per sostenere i progetti • Contribuisce a idee, servizi e soluzioni di business all'avanguardia in materia di sicurezza informatica • Assistere nello sviluppo di capacità connesse alla cybersicurezza, compresa la consapevolezza, la formazione teorica, la formazione pratica, i test, il tutoraggio, la supervisione e la condivisione • Identificare i risultati intersettoriali in materia di cybersicurezza e applicarli in un contesto diverso o proporre approcci e soluzioni innovativi • Guidare o partecipare ai processi e ai progetti di innovazione, compresa la gestione dei progetti e il budgeting • Pubblicare e presentare lavori scientifici e risultati di ricerca e sviluppo	
Abilità chiave	• Generare nuove idee e trasferire la teoria in pratica • Decomporre e analizzare i sistemi per individuare le debolezze e i controlli inefficaci • Decomporre e analizzare i sistemi per sviluppare requisiti di sicurezza e privacy e identificare soluzioni efficaci • Monitorare i nuovi progressi nelle tecnologie legate alla cybersicurezza • Comunicare, presentare e riferire alle parti interessate • Identificare e risolvere i problemi connessi alla cybersicurezza • Collaborare con altri membri del team e colleghi	
Conoscenze chiave	• Ricerca, sviluppo e innovazione in materia di cybersicurezza (RDI) • Norme, metodologie e quadri di cybersicurezza • Requisiti giuridici, normativi e legislativi relativi al rilascio o all'utilizzo di tecnologie connesse alla cybersicurezza • Aspetto multidisciplinare della sicurezza informatica • Procedure di divulgazione responsabile delle informazioni	
e-Competences (dall'e-CF)	A.7. Monitoraggio delle tendenze tecnologiche A.9. Innovare D.7. Scienza dei dati e analisi C.4. Gestione dei problemi D.10. Gestione delle informazioni e della conoscenza	Livello 5 Livello 5 Livello 4 Livello 3 Livello 3

1.10 GESTORE DEL RISCHIO DI CYBERSICUREZZA

Titolo del profilo	Responsabile dei rischi per la sicurezza informatica	
Titolo/i alternativo/i	Analista di sicurezza informatica Analista del rischio di sicurezza informatica Consulente di sicurezza informatica Valutazione del rischio di sicurezza informatica Analista di impatto della cybersicurezza Responsabile del rischio informatico	
Sintesi	Gestire i rischi legati alla sicurezza informatica dell'organizzazione in linea con la strategia dell'organizzazione. Sviluppare, mantenere e comunicare i processi e i report di gestione del rischio.	
Missione	Gestisce continuamente (identifica, analizza, valuta, stima, mitiga) i rischi connessi alla sicurezza informatica delle infrastrutture, dei sistemi e dei servizi ICT attraverso la pianificazione, l'applicazione, la segnalazione e la comunicazione dell'analisi, della valutazione e del trattamento dei rischi. Stabilisce una strategia di gestione del rischio per l'organizzazione e garantisce che i rischi rimangano a un livello accettabile per l'organizzazione selezionando azioni e controlli di mitigazione.	
Prodotto/i da fornire	• Relazione sulla valutazione dei rischi per la cybersicurezza • Piano d'azione per la correzione dei rischi di cybersicurezza	
Compito/i principale/i	• Sviluppare la strategia di gestione del rischio di sicurezza informatica di un'organizzazione • Gestire un inventario delle risorse dell'organizzazione • Identificare e valutare le minacce e le vulnerabilità connesse alla cybersicurezza dei sistemi TIC • Identificazione del panorama delle minacce, compresi i profili degli aggressori e la stima del potenziale degli attacchi • Valutare i rischi di cybersicurezza e proporre opzioni di trattamento dei rischi più appropriate, compresi i controlli di sicurezza e l'attenuazione e l'elusione dei rischi che meglio affrontano la strategia dell'organizzazione • Monitorare l'efficacia dei controlli di cybersicurezza e dei livelli di rischio • Garantire che tutti i rischi per la sicurezza informatica rimangano a un livello accettabile per le risorse dell'organizzazione	
Abilità chiave	• Implementare quadri, metodologie e linee guida per la gestione del rischio di cybersicurezza e garantire la conformità con i regolamenti e gli standard • Analizzare e consolidare le pratiche di gestione della qualità e del rischio dell'organizzazione • Consentire ai proprietari di asset aziendali, ai dirigenti e ad altre parti interessate di prendere decisioni informate sul rischio per gestire e mitigare i rischi • Creare un ambiente consapevole dei rischi per la cybersicurezza • Comunicare, presentare e riferire alle parti interessate • Proporre e gestire le opzioni di condivisione dei rischi	
Conoscenze chiave	• Norme, metodologie e quadri di gestione del rischio • Strumenti di gestione del rischio • Raccomandazioni sulla gestione dei rischi e migliori pratiche • Minacce informatiche • Vulnerabilità dei sistemi informatici • Controlli e soluzioni di sicurezza informatica • Rischi per la cybersicurezza • Monitorare, testare e valutare l'efficacia dei controlli di cybersicurezza • Certificazioni legate alla cybersicurezza • Tecnologie connesse alla cybersicurezza	
e-Competences (dall'e-CF)	E.3. Gestione del rischio E.5. Miglioramento del processo E.7. Gestione del cambiamento aziendale E.9. Is-Governance	Livello 4 Livello 3 Livello 4 Livello 4

1.11 INVESTIGATORE FORENSE DIGITALE

Titolo del profilo	Digital Forensics Investigator	
Titolo/i alternativo/i	Digital Forensics Analyst Cybersecurity & Forensic Specialist Computer Forensics Consultant	
Sintesi	Assicurarsi che l'indagine sui criminali informatici riveli tutte le prove digitali per dimostrare l'attività dannosa.	
Missione	Collega artefatti a persone fisiche, cattura, recupera, identifica e conserva i dati, comprese manifestazioni, input, output e processi dei sistemi digitali oggetto di indagine. Fornisce analisi, ricostruzione e interpretazione delle evidenze digitali sulla base di un parere qualitativo. Presenta una visione qualitativa imparziale senza interpretare i risultati ottenuti.	
Prodotto/i da fornire	• Risultati dell'analisi forense digitale • Prove elettroniche	
Compito/i principale/i	• Sviluppare la politica, i piani e le procedure di indagine forense digitale • Identificare, recuperare, estrarre, documentare e analizzare le prove digitali • Conservare e proteggere le prove digitali e metterle a disposizione delle parti interessate autorizzate • Ispezionare gli ambienti per verificare le prove di azioni non autorizzate e illecite • Documento, relazione e presentazione sistematica e deterministica dei risultati e dei risultati dell'analisi forense digitale • Selezionare e personalizzare le tecniche di test, analisi e reportistica forense	
Abilità chiave	• Lavorare in modo etico e indipendente; non influenzati e distorti da attori interni o esterni • Raccogliere informazioni preservandone l'integrità • Identificare, analizzare e correlare gli eventi di sicurezza informatica • Spiegare e presentare prove digitali in modo semplice, diretto e facile da capire • Elaborare e comunicare relazioni d'indagine dettagliate e motivate	
Conoscenze chiave	• Raccomandazioni e best practice forensi digitali • Standard, metodologie e framework forensi digitali • Procedure di analisi forense digitale • Procedure di prova • Procedure, norme, metodologie e quadri di indagine penale • Leggi, regolamenti e legislazioni in materia di cybersicurezza • Strumenti di analisi malware • Minacce informatiche • Vulnerabilità dei sistemi informatici • Procedure di attacco alla cybersicurezza • Sicurezza dei sistemi operativi • Sicurezza delle reti informatiche • Certificazioni legate alla cybersicurezza	
e-Competences (dall'e-CF)	A.7. Monitoraggio delle tendenze tecnologiche B.3. Test B.5. Produzione di documentazione E.3. Gestione del rischio	Livello 3 Livello 4 Livello 3 Livello 3

1.12 TESTER DI PENETRAZIONE

Titolo del profilo	Tester di penetrazione	
Titolo/i alternativo/i	Pentester Hacker etico Analista di vulnerabilità Tester di sicurezza informatica Esperto di sicurezza informatica offensivo Esperto di cybersicurezza difensiva Red Team Expert Red Teamer	
Sintesi	Valutare l'efficacia dei controlli di sicurezza, rivelare e utilizzare le vulnerabilità della sicurezza informatica, valutarne la criticità se sfruttata dagli attori delle minacce.	
Missione	Pianifica, progetta, implementa ed esegue attività di test di penetrazione e scenari di attacco per valutare l'efficacia delle misure di sicurezza implementate o pianificate. Identifica vulnerabilità o guasti nei controlli tecnici e organizzativi che incidono sulla riservatezza, l'integrità e la disponibilità dei prodotti TIC (ad esempio sistemi, hardware, software e servizi).	
Prodotto/i da fornire	• Relazione sui risultati della valutazione delle vulnerabilità • Rapporto sui test di penetrazione	
Compito/i principale/i	• Identificare, analizzare e valutare le vulnerabilità tecniche e organizzative della cybersicurezza • Identificare i vettori di attacco, scoprire e dimostrare lo sfruttamento delle vulnerabilità tecniche di sicurezza informatica • Conformità ai sistemi di prova e alle operazioni con gli standard normativi • Selezionare e sviluppare tecniche appropriate di test di penetrazione • Organizzare piani di prova e procedure per i test di penetrazione • Stabilire procedure per l'analisi e la comunicazione dei risultati dei test di penetrazione • Documentare e riferire i risultati dei test di penetrazione alle parti interessate • Implementa strumenti di test di penetrazione e programmi di test	
Abilità chiave	• Sviluppare codici, script e programmi • Eseguire ingegneria sociale • Identificare e sfruttare le vulnerabilità • Condurre hacking etico • Pensa in modo creativo e fuori dagli schemi • Identificare e risolvere i problemi connessi alla cybersicurezza • Comunicare, presentare e riferire alle parti interessate • Utilizzare efficacemente gli strumenti di test di penetrazione • Condurre analisi tecniche e reportistica • Decomporre e analizzare i sistemi per individuare le debolezze e i controlli inefficaci • I codici di revisione valutano la loro sicurezza	
Conoscenze chiave	• Procedure di attacco alla cybersicurezza • Apparecchiature di tecnologia dell'informazione (IT) e di tecnologia operativa (OT) • Procedure di sicurezza offensive e difensive • Sicurezza dei sistemi operativi • Sicurezza delle reti informatiche • Penetrazione test procedure • Penetrazione test norme, metodologie e quadri • Penetrazione test strumenti • Programmazione informatica • Vulnerabilità dei sistemi informatici • Raccomandazioni e migliori pratiche in materia di cybersicurezza • Certificazioni legate alla cybersicurezza	
e-Competences (dall'e-CF)	8.2. Integrazione dei componenti 8.3. Test 8.4. Implementazione della soluzione 8.5. Produzione di documentazione	Livello 4 Livello 4 Livello 2 Livello 3

E.3. Gestione del rischio	Livello 4

2. LIBRERIA DEI DELIVERABLE

L'elenco dei deliverable fornisce alcuni esempi indicativi e pratici dei risultati/delle realizzazioni di ciascun profilo di ruolo. Gli elementi da fornire elencati sono offerti come esempi in quanto l'elenco non è esaustivo e quindi non copre tutti gli aspetti di ciascun profilo.

Titolo del profilo	Da fornire	Descrizione
Responsabile della sicurezza delle informazioni (CISO)	Strategia per la cybersicurezza	La strategia per la sicurezza informatica è un piano di azioni progettato per migliorare la sicurezza e la resilienza delle infrastrutture e dei servizi di un'organizzazione.
Responsabile della sicurezza delle informazioni (CISO)	Politica in materia di cybersicurezza	Una politica che elenca le regole per garantire la sicurezza informatica dell'organizzazione.
Risponditore di incidenti informatici	Piano di risposta agli incidenti	Una serie di procedure documentate che descrivono le misure da adottare in ogni fase di una risposta agli incidenti (preparazione, rilevazione e analisi, contenimento, eradicazione e recupero, attività post-incidente).
Risponditore di incidenti informatici	Report sugli incidenti informatici	Una relazione che fornisce dettagli su uno o più incidenti informatici.
Cyber Legal, Policy & Compliance Officer	Manuale di conformità	Un manuale che fornisce una comprensione approfondita degli obblighi di conformità normativa di un'organizzazione. Può includere politiche o procedure interne per garantire il rispetto di leggi, regolamenti e/o standard.
Cyber Legal, Policy & Compliance Officer	Relazione sulla conformità	Un rapporto che presenta lo stato attuale della posizione di conformità di un'organizzazione.
Cyber Threat Intelligence Specialista	Cyber Threat Intelligence Manuale (o Manuale)	Un manuale che presenta strumenti e/o metodologie per la raccolta e/o condivisione di informazioni sulle minacce informatiche.
Cyber Threat Intelligence Specialista	Rapporto sulle minacce informatiche	Un rapporto che identifica le principali minacce, le principali tendenze osservate per quanto riguarda le minacce, gli attori delle minacce e/o le tecniche di attacco. La relazione può includere anche misure di mitigazione pertinenti.
Architetto della sicurezza informatica	Diagramma dell'architettura della sicurezza informatica	Rappresentazione visiva dell'architettura di sistema di sicurezza informatica di un'organizzazione utilizzata per proteggere le risorse dagli attacchi informatici.
Architetto della sicurezza informatica	Sicurezza informatica Relazione sui requisiti	Una relazione che elenca una serie di requisiti necessari per garantire la cybersicurezza di un sistema.
Revisore della cybersicurezza	Piano di audit della cybersicurezza	Un piano che presenta la strategia globale e le procedure che un revisore seguirà per condurre un audit sulla cybersicurezza.
Revisore della cybersicurezza	Relazione di audit sulla cybersicurezza	Una relazione che fornisce una comprensione approfondita del livello di sicurezza di un sistema, valutandone i punti di forza e le debolezze in materia di cybersicurezza. Può anche fornire azioni di risanamento per migliorare la cybersicurezza complessiva del sistema.
Educatore della sicurezza informatica	Programma di sensibilizzazione alla sicurezza informatica	Un programma di attività di sensibilizzazione sulle questioni legate alla sicurezza informatica (ad es. lezioni sugli attacchi

		e minacce) aiutare le organizzazioni a prevenire e mitigare i rischi connessi alla sicurezza informatica.
Educatore della sicurezza informatica	Materiale di formazione sulla cybersicurezza	Materiale che spiega i concetti, le metodologie e gli strumenti relativi alla cybersicurezza per la formazione o il miglioramento delle competenze degli individui. Potrebbe includere manuali per insegnanti, strumenti per studenti e/o immagini virtuali per supportare le sessioni di formazione.
Implementazione della sicurezza informatica	Soluzioni per la sicurezza informatica	Le soluzioni per la sicurezza informatica potrebbero includere strumenti e servizi che mirano a proteggere le organizzazioni dagli attacchi informatici.
Ricercatore sulla sicurezza informatica	Pubblicazione in Cybersecurity	Pubblicazione accademica che rilascia risultati e risultati della ricerca nel contesto della sicurezza informatica. Lo scopo della pubblicazione potrebbe essere quello di far progredire la tecnologia e/o sviluppare nuove soluzioni innovative.
Responsabile dei rischi per la sicurezza informatica	Relazione sulla valutazione dei rischi per la cybersicurezza	Una relazione che elenca i risultati dell'identificazione, dell'analisi e della valutazione dei rischi di cybersicurezza di un sistema. Potrebbe anche includere controlli per attenuare o ridurre i rischi individuati a un livello accettabile.
Responsabile dei rischi per la sicurezza informatica	Rischio per la cybersicurezza Piano d'azione per la bonifica	Un piano d'azione che elenca le attività connesse all'attuazione di misure di mitigazione volte a ridurre i rischi di cybersicurezza.
Digital Forensics Investigator	Risultati dell'analisi forense digitale	Risultati dell'analisi dei dati digitali che rivelano potenziali prove di incidenti dolosi e identificano i possibili attori delle minacce.
Digital Forensics Investigator	Prove elettroniche	Prove potenziali derivate da dati contenuti o prodotti da qualsiasi dispositivo, il cui funzionamento dipende da un programma software o da dati memorizzati o trasmessi su un sistema o una rete informatica. (ad es. raccolta accurata dei tronchi)
Tester di penetrazione	Relazione sui risultati della valutazione delle vulnerabilità	Un report che elenca e valuta la criticità delle vulnerabilità scoperte in un sistema durante una scansione (solitamente automatica) delle vulnerabilità. La relazione potrebbe anche suggerire azioni di risanamento di base.
Tester di penetrazione	Rapporto sui test di penetrazione	Un rapporto che fornisce un'analisi dettagliata e completa delle vulnerabilità di un sistema identificate durante un test di sicurezza. La relazione potrebbe anche includere azioni di risanamento suggerite.

TP-09-22-510-EN-N

INFORMAZIONI SU ENISA

L'Agenzia dell'Unione europea per la cybersicurezza, l'ENISA, è l'agenzia dell'Unione europea dedicata al conseguimento di un elevato livello comune di cybersicurezza in tutta Europa. Istituita nel 2004 e rafforzata dall'atto dell'UE sulla cybersicurezza, l'Agenzia dell'Unione europea per la cybersicurezza contribuisce alla politica informatica dell'UE, rafforza l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cybersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi alle sfide informatiche di domani. Attraverso la condivisione delle conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con le sue principali parti interessate per rafforzare la fiducia nell'economia connessa, rafforzare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sul suo lavoro sono disponibili qui: www.enisa.europa.eu.

ENISA
Agenzia dell'Unione europea per la cybersicurezza

Ufficio di Atene
Agamemnonos 14, Chalandri 15231, Attiki, Grecia

Ufficio di Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grecia

enisa.europa.eu — nma

ISBN: 978-92-9204-584-5
DOI: 10.2824/859537