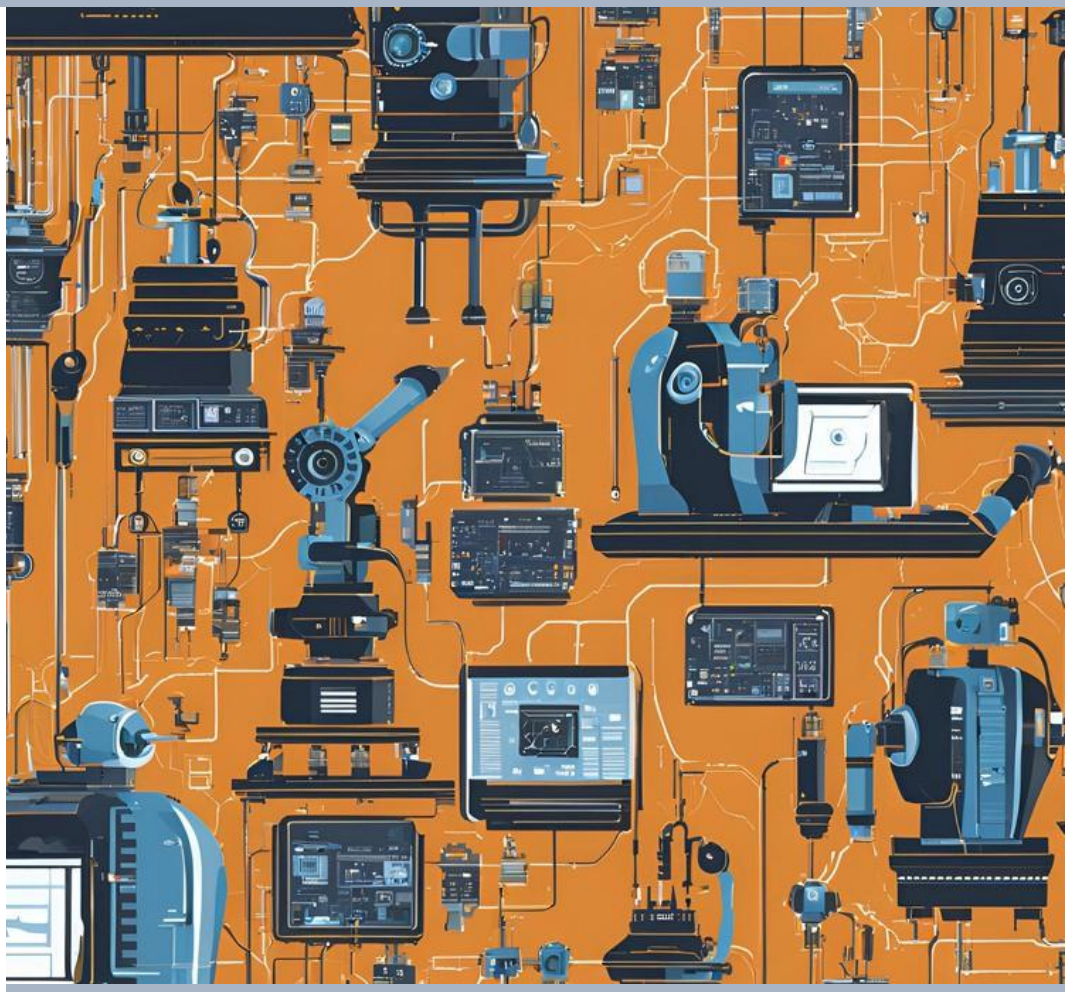
Co-funded by the European Union

CYBERSECURITY NEGLI AMBIENTI OT

SKILL GAPS E FABBISOGNI FORMATIVI

Riferimento progetto: 2023-1-NL01-KA220-VET-000153812



A cura di:

da Vinci college

maristak Durango Ikastetxea

HETEL

ÉCOLE ENTI CONFINDUSTRIALI LOMBARDI PER L'EDUCATION

BCS Koolitus

Roskilde Tekniske Skole

www.cyber-in.eu

Cyber-In

QUESTO PROGETTO È STATO FINANZIATO CON IL SOSTEGNO DELLA COMMISSIONE EUROPEA. LA PRESENTE PUBBLICAZIONE RISPECCHIA ESCLUSIVAMENTE LE OPINIONI DELL'AUTORE E LA COMMISSIONE NON PUÒ' ESSERE RITENUTA RESPONSABILE PER L'USO CHE POTREBBE ESSERE FATTO DELLE INFORMAZIONI IN ESSA CONTENUTE.

Indice

Introduzione

La sicurezza informatica è una delle principali sfide che le aziende devono affrontare nel contesto dell'"Internet delle cose industriali" (IoT), in cui una serie di dispositivi intelligenti associati a macchine, computer e persone sono collegati in rete e comunicano tra loro.

In questo scenario industriale connesso, il personale deve essere consapevole delle tematiche relative alla sicurezza informatica al fine di prevenire o ridurre al minimo il verificarsi di incidenti di sicurezza informatica e violazioni dei dati aziendali, rendendo così le aziende resilienti agli attacchi informatici.

Sebbene vi sia un crescente interesse nella letteratura per i diversi elementi chiave che caratterizzano la gestione della sicurezza informatica nei contesti industriali dell'IoT, è stata prestata scarsa attenzione ai vari aspetti della consapevolezza in materia di sicurezza informatica negli stessi contesti industriali.

Inoltre, la sicurezza informatica non è un argomento nuovo nelle nostre scuole, né nella serie di progetti Erasmus+ realizzati fino ad oggi. Nella piattaforma Erasmus+ sono presenti 100 progetti KA2 relativi all'argomento. Tuttavia, se si prendono in considerazione le applicazioni della sicurezza informatica all'industria (e in particolare al paradigma dell'Industria 4.0), i risultati si riducono significativamente.

Mentre le aziende industriali si orientano verso la produzione intelligente e la digitalizzazione di macchinari, dati, processi e postazioni di lavoro con l'applicazione di tecnologie facilitanti come l'IoT, il cloud computing o i big data, con l'obiettivo di ottenere maggiore efficienza nella loro risposta a mercati in continua evoluzione, le vulnerabilità in termini di sicurezza informatica aumentano in modo esponenziale.

L'obiettivo finale di questo documento è determinare quindi quali sono le lacune dei professionisti IT e OT che lavorano in settori con un alto livello di automazione in termini di sicurezza informatica, in modo che le scuole professionali possano colmare tali lacune quando offrono formazione agli studenti nei programmi IT e OT.

A tal fine, abbiamo condotto interviste e focus group nei paesi partner (Paesi Bassi, Spagna, Danimarca, Estonia e Italia) per comprendere più a fondo le sfide reali degli impianti industriali interconnessi in termini di sicurezza informatica e protezione dei dati.

Il primo passo è stato quello di comprendere le sfide, i punti deboli e le esigenze dell'industria interconnessa in termini di sicurezza informatica, al fine di definire e descrivere in modo più dettagliato il profilo di un operatore OT con competenze di sicurezza informatica richieste dalle industrie interconnesse e di un tecnico IT industriale con le competenze necessarie per fare da ponte con il mondo OT.

Successivamente abbiamo combinato il feedback ricevuto dalle aziende con un'analisi degli attuali programmi di studio che stiamo già insegnando nelle nostre scuole professionali, identificando le lacune relative alla sicurezza informatica. Il risultato è stata una definizione delle competenze in materia di sicurezza informatica per i professionisti IT e OT che può essere utilizzata come base per sviluppare materiali di formazione volti a colmare tali lacune; tali materiali possono essere utilizzati da insegnanti/formatori per l'autoapprendimento, nonché essere integrati negli attuali programmi di studio dei nostri corsi di formazione professionale o utilizzati dalle aziende per la formazione interna del proprio personale IT e OT.

Nelle sezioni seguenti presentiamo le nostre conclusioni ed i risultati della nostra ricerca e analisi.

Risultati delle indagini presso le aziende

Ciascun partner ha condotto focus group e/o interviste con le aziende in ogni contesto locale (Italia, Danimarca, Spagna, Paesi Bassi ed Estonia).

La combinazione di attori IT e OT e formatori/docenti ci ha permesso di raccogliere informazioni ponendo domande mirate al fine di comprendere quali sono le sfide di sicurezza informatica affrontate dai settori interconnessi.

Numero di aziende che hanno fornito un feedback

34 aziende

Numero di settori coinvolti

11 settori

L'obiettivo dei focus group e delle interviste è stato quello di individuare le principali lacune rilevate dal punto di vista tecnico e delle competenze trasversali e di trarre conclusioni sulla necessità di un nuovo profilo OT/IT con l'aggiornamento e la riqualificazione dei lavoratori e degli studenti attuali:

- Comprendere cosa sanno già le aziende OT dei settori definiti in materia di sicurezza informatica (concetti principali, contesto aziendale…)
- Definire il grado di consapevolezza dei rischi (punti deboli specifici del settore, fattore umano, esistenza di protocolli e normative...)
- Esplorare le regole note in materia di sicurezza informatica (standard e normative applicate al settore specifico)
- Esplorare gli incidenti affrontati da altre aziende (casi di studio, simulazioni...)
- Comprendere quali sono le conoscenze delle aziende di sicurezza informatica IT e/o dei professionisti IT sui rischi affrontati dalle aziende OT
- Individuare le lacune e le esigenze in termini di conoscenze, competenze e consapevolezza tra studenti e lavoratori in entrambi i settori.

Per motivi di privacy, non condividiamo i nomi delle aziende intervistate, ma riportiamo i settori da cui provengono e il ruolo dell'intervistato/partecipante nel focus group.

COUNTRY	PARTNER	COMPANY AREA	ROLE OF THE INTERVIEWED
DK	Roskilde Tekniske Skole	Production for aviation	Infrastructure Supervisor
DK	Roskilde Tekniske Skole	water supply	Team Leader
DK	Roskilde Tekniske Skole	production of medicin	SVP Education Proffessional
DK	Roskilde Tekniske Skole	water supply	
DK	Roskilde Tekniske Skole	water supply	Operations Manager
ITA	ECOLE SCARL	Cybersecurity and consultancy	Lead Reliability & Planning
ITA	ECOLE SCARL	Electrical engineering	Strategic Planner & Automation Specialist
ITA	ECOLE SCARL	Chemicals and energy company	APC & Cybersecurity Specialist
ITA	ECOLE SCARL	Pharmaceutical chemical	CYBER SECURITY MANAGER
ITA	ECOLE SCARL	ENGINEERING, PROCUREMENT & CONSTRUCTIO	ICT Budget & Reporting Analyst
ITA	ECOLE SCARL		Account Specialist, Senior Security Engineer
EST	BCS Koolitus	Telecommunication equipment production	Cybersecurity engeneer
EST	BCS Koolitus	IT security solutions	Head of Department, IT specialist (2 people)
EST	BCS Koolitus	IT security solutions	IT specialist
EST	BCS Koolitus	Telecommunication, production	Sysadmin
EST	BCS Koolitus	Governmental Institution	Helpdesk Operations Manager
EST	BCS Koolitus	Gambling software development	IT specialist
EST	BCS Koolitus	VET College	IT specialist, teacher of IT
EST	BCS Koolitus	Wood production	IT specialists (2 people)
EST	BCS Koolitus	Food production	IT specialist
EST	BCS Koolitus	VET	IT specialist, teacher of IT
EST	BCS Koolitus	VET	Teacher of Cybersecurity, cybersecurity expert
EST	BCS Koolitus	VET	Teacher of Cybersecurity, cybersecurity expert
ES	Maristak / HETEL	IT security solutions	CEO
ES	Maristak / HETEL	Cybersecurity association	Managing Director
ES	Maristak / HETEL	Transport - Automotive	IT Manager
ES	Maristak / HETEL	Energy - Solar	Cybersecurity manager
ES	Maristak / HETEL	Energy - Wind	Cybersecurity manager
ES	Maristak / HETEL	Energy - Chemical	IT manager
ES	Maristak / HETEL	Energy - Electric equipment	Cybersecurity manager
ES	Maristak / HETEL	Transport - Aviation	Cybersecurity manager
ES	Maristak / HETEL	Transport - Machine tool	HR manager
NL	Da Vinci College	Robotics (welding)	Device manager
NL	Da Vinci College	Industrial Analytics en Machine Learing	Junior consultant smart technologies
NL	Da Vinci College	IT solutions	CEO
NL	Da Vinci College	Fiber optics/network solution	Manager
NL	Da Vinci College	Security	Support specialist

Abbiamo posto 10 domande alle aziende, suddivise in 3 aree tematiche:

- **Area 1**. Comprendere cosa sanno già le aziende OT in materia di sicurezza informatica.
- **Area 2.** Comprendere quali sono le conoscenze delle aziende di sicurezza informatica IT sui rischi affrontati dalle aziende OT
- **Area 3**. Individuare le lacune e le esigenze in termini di conoscenze, competenze e consapevolezza tra gli studenti e i lavoratori di entrambi i settori.

I risultati ottenuti nei paesi del progetto (Italia, Estonia, Spagna, Danimarca e Paesi Bassi) hanno fornito una panoramica dettagliata delle sfide e delle opportunità nel panorama della sicurezza informatica. Di seguito sono disponibili i risultati ottenuti, raggruppati per aree tematiche e domande poste durante i focus group/le interviste.

Area tematica 1: Consapevolezza della sicurezza informatica e rischi nelle aziende OT

Domande chiave poste durante i focus group/ interviste su questo tema:

1 Quali sono i benefici o i vantaggi competitivi della sicurezza informatica nel vostro settore?

2 Che tipo di incidenti o minacce alla sicurezza informatica avete subito e come li avete gestiti? Quali lezioni avete tratto dagli incidenti di sicurezza informatica subiti da voi o da altre aziende?

3 Qual è il livello di formazione e consapevolezza in materia di sicurezza informatica dei vostri dipendenti e collaboratori? Quali azioni di formazione o informazione svolgete a questo proposito?

Vantaggi

Le aziende dei paesi coinvolti riconoscono che la sicurezza informatica offre numerosi vantaggi, tra cui una maggiore fiducia dei clienti, la protezione delle informazioni sensibili e la garanzia della continuità operativa. Tuttavia, esistono differenze significative nelle motivazioni specifiche e nei benefici percepiti tra i diversi settori e paesi.

Analisi specifica per paese

Italia: le aziende italiane, in particolare nel settore farmaceutico, hanno registrato un aumento significativo della consapevolezza in materia di sicurezza informatica negli ultimi anni. Molte grandi aziende hanno implementato funzioni di sicurezza informatica centralizzate e programmi di formazione obbligatori per tutti i dipendenti, compresi i fornitori. Questo approccio ha migliorato la protezione delle informazioni sensibili e ha creato un ambiente di lavoro più sicuro e regolamentato, rafforzando la competitività di queste aziende.

Spagna: in Spagna, la sicurezza informatica è diventata una componente essenziale delle strategie aziendali, specialmente in settori regolamentati come l'energia e la produzione operativa (OT). La conformità alle normative, come la direttiva NIS2, è vista come un vantaggio competitivo che rafforza la posizione delle aziende sul mercato. La sicurezza informatica rafforza inoltre la fiducia dei clienti e riduce i rischi finanziari associati alle violazioni dei dati e agli attacchi informatici.

Estonia: Le aziende estoni riconoscono che un sistema di sicurezza informatica ben configurato aumenta la fiducia dei clienti e protegge le informazioni sensibili. La riduzione del rischio di attacchi e il miglioramento dell'efficienza operativa rappresentano vantaggi significativi. Inoltre, la fiducia dei dipendenti nei confronti dei datori di lavoro è aumentata grazie a solide misure di sicurezza informatica.

Paesi Bassi: Nei Paesi Bassi, la sicurezza informatica è considerata un elemento chiave per mantenere la competitività, in particolare nei settori marittimo e offshore. Le aziende che adottano standard di sicurezza avanzati, come NIS2, possono garantire un ambiente sicuro per i propri clienti, migliorando la loro posizione di mercato e prevenendo interruzioni operative.

Area tematica 1: Consapevolezza e rischi della sicurezza informatica nelle aziende OT

Gestione degli incidenti e lezioni apprese

Le aziende hanno segnalato esperienze comuni relative ad attacchi di phishing, ransomware e problemi legati a sistemi obsoleti. Le risposte agli incidenti includono miglioramenti tecnici, politiche più rigorose e formazione avanzata. La risposta rapida agli incidenti, la formazione dei dipendenti e il miglioramento continuo delle politiche di sicurezza sono essenziali per mitigare i danni e prevenire attacchi futuri.

Analisi specifica per paese

Italia: le aziende italiane hanno affrontato vari incidenti, tra cui attacchi di phishing e problemi con firewall obsoleti. In un caso, una grande azienda farmaceutica ha ha scoperto delle vulnerabilità attraverso sistemi di monitoraggio del dark web. Le risposte agli incidenti hanno sottolineato l'importanza di un approccio zero-trust e della conferma di ogni transazione tramite autenticazione. Una gestione rapida degli incidenti e una documentazione accurata delle operazioni dei fornitori sono state identificate come elementi chiave per migliorare la sicurezza.

Spagna: gli incidenti di sicurezza informatica sono una realtà in tutti i settori, compresi quello governativo, le aziende private, l'energia, la produzione, il settore bancario e quello assicurativo. Nella sicurezza informatica IT, gli incidenti comuni includono vishing, spam, ransomware e phishing, mentre nell'OT gli incidenti possono interessare i sistemi di controllo industriale e i dispositivi connessi, con minacce quali attacchi denial-of-service, manipolazione dei dati, malware specifico per l'OT, accesso non autorizzato ai sistemi SCADA e fughe di informazioni sensibili. Le aziende hanno compreso l'importanza dell'autenticazione a più fattori, della formazione continua e della prontezza a rispondere agli attacchi. L'adozione di misure preventive e il miglioramento delle politiche di sicurezza sono stati cruciali per una gestione efficace degli incidenti.

Estonia: Le aziende estoni hanno sottolineato la crescente sofisticazione degli attacchi di phishing e l'importanza della formazione degli utenti per prevenire gli incidenti. Gli attacchi alla catena di approvvigionamento e il ransomware sono stati particolarmente problematici. Le risposte efficaci agli incidenti hanno incluso miglioramenti tecnici, politiche più rigorose e un'attenzione particolare alla formazione dei dipendenti.

Paesi Bassi: Le aziende nei Paesi Bassi hanno dovuto affrontare attacchi DDoS e problemi legati a software obsoleti. La formazione continua e gli aggiornamenti dei sistemi sono stati identificati come fattori cruciali per prevenire gli incidenti. La preparazione e la formazione continua sono state considerate essenziali per mantenere un solido livello di sicurezza e rispondere efficacemente agli attacchi.

Danimarca: In Danimarca, gli attacchi simulati e i brownout sono pratiche comuni per preparare le aziende a situazioni reali. La gestione dei rischi e la preparazione agli scenari peggiori sono considerate fondamentali per mitigare i danni e garantire la continuità operativa.

Area tematica 1: Consapevolezza e rischi della sicurezza informatica nelle aziende OT

Formazione e sensibilizzazione

Formazione regolare, simulazioni di phishing e programmi di sensibilizzazione sono ampiamente implementati. Tuttavia, esistono differenze significative nel livello di strutturazione e nella natura obbligatoria dei programmi di formazione tra i diversi paesi.

Analisi specifica per paese

Italia: La consapevolezza è aumentata negli ultimi 5-6 anni. Le industrie non gestiscono quotidianamente la sicurezza informatica e il networking, poiché queste sono solo le ultime due competenze che hanno sviluppato. La consapevolezza in materia di sicurezza informatica è aumentata grazie a cicli di formazione online obbligatori per tutti i dipendenti e i fornitori in settori quali quello farmaceutico e chimico. Le aziende conducono simulazioni continue e richiedono ai dipendenti di completare almeno sei ore di formazione prima di accedere ai sistemi aziendali. Questo approccio garantisce che tutti i dipendenti mantengano un alto livello di consapevolezza e competenza in materia di sicurezza informatica. La sicurezza informatica è oggi una questione che riguarda tutti i dipendenti che operano nell'ambiente aziendale.

Spagna: C'è un deficit significativo nella formazione completa, con un'attenzione particolare alla sensibilizzazione e all'integrazione delle misure di sicurezza nella cultura quotidiana dell'azienda. La formazione è spesso limitata a corsi online e cambi di password, ma sono in corso iniziative per migliorare la consapevolezza e la preparazione dei dipendenti attraverso programmi più strutturati.

Estonia: La consapevolezza in materia di sicurezza informatica varia tra le aziende estoni. Alcune aziende implementano programmi di formazione obbligatori e test di phishing regolari, mentre altre necessitano di miglioramenti nella comunicazione delle politiche di sicurezza. La formazione continua e la collaborazione tra i reparti IT e gli altri reparti sono fondamentali per affrontare efficacemente le sfide della sicurezza informatica.

Paesi Bassi: La formazione annuale mirata e i programmi di apprendimento continuo sono la norma. Le aziende sottolineano l'importanza di un aggiornamento continuo sulle nuove minacce e tecnologie, fornendo ai dipendenti le competenze necessarie per proteggere efficacemente le infrastrutture aziendali.

Danimarca: E' comune la formazione pratica basata su scenari, con misure di sicurezza concrete e aggiornamenti regolari forniti da CERT specifici per settore. Questa formazione prepara efficacemente i dipendenti a gestire incidenti reali e a mantenere una solida posizione di sicurezza.

Area tematica 2: Pratiche di sicurezza informatica in ambito IT e OT

Specificità dell'IT e dell'OT e implicazioni per la sicurezza informatica

I sistemi OT sono spesso più datati, meno connessi a Internet e presentano requisiti operativi unici rispetto ai sistemi IT, che si concentrano maggiormente sulla sicurezza dei dati. Entrambi gli ambienti richiedono misure di sicurezza informatica su misura, con particolare attenzione alle operazioni in tempo reale e alla compatibilità con i sistemi legacy.

Analisi specifica per paese

Italia: i sistemi OT richiedono investimenti significativi in aggiornamenti di sicurezza e una stretta collaborazione con i reparti IT. La segregazione della rete e la gestione sicura dei fornitori sono fondamentali per proteggere i sistemi da accessi non autorizzati e vulnerabilità.

Spagna: la mancanza di standardizzazione nei sistemi OT rappresenta una sfida significativa. La sicurezza informatica deve essere personalizzata per soddisfare le esigenze specifiche di ciascun sistema, con particolare attenzione alla conformità normativa e alla gestione dei rischi.

Estonia: le aziende estoni utilizzano spesso sistemi legacy e reti isolate, che richiedono la segmentazione della rete e dispositivi ridondanti per mantenere la sicurezza. La connettività Internet limitata riduce i vettori di attacco, ma rende anche più difficile l'aggiornamento e l'applicazione di patch ai sistemi.

Danimarca: in Danimarca, le reti isolate e crittografate sono comuni per proteggere le infrastrutture critiche. Misure di sicurezza pratiche, come l'uso di tunnel crittografati e la segmentazione della rete, sono essenziali per proteggere i sistemi OT da accessi non autorizzati.

Paesi Bassi: la velocità e l'affidabilità dei sistemi sono prioritarie. Le aziende devono aggiornare continuamente le tecnologie e formare i dipendenti per mantenere un elevato livello di sicurezza. La segmentazione della rete e i controlli di accesso rigorosi sono pratiche comuni.

Area tematica 2: Pratiche di sicurezza informatica in ambito IT e OT

Limiti e soluzioni

I principali vincoli includono limitazioni finanziarie, attrezzature obsolete e accesso limitato a Internet. Le soluzioni comuni includono la segmentazione della rete, controlli rigorosi degli accessi e aggiornamenti regolari. La collaborazione tra i reparti IT e OT è fondamentale per superare queste sfide.

Analisi specifica per paese

Italia: i vincoli finanziari e normativi rappresentano sfide significative per le aziende italiane. La responsabilità dei fornitori e lo sviluppo congiunto di soluzioni di sicurezza sono strategie utilizzate per migliorare la protezione dei sistemi OT. La sincronizzazione con il reparto IT e una buona gestione interna sono fondamentali per mantenere un elevato livello di sicurezza.

Spagna: l'obsolescenza dei sistemi OT e la mancanza di controlli rigorosi rappresentano sfide comuni. La conformità normativa e un approccio basato sul rischio sono essenziali per proteggere gli ambienti OT. Le aziende devono implementare soluzioni su misura per gestire efficacemente la sicurezza dei sistemi legacy.

Estonia: le aziende estoni devono affrontare sfide legate alle apparecchiature obsolete e all'accesso limitato a Internet. Per migliorare la sicurezza si raccomandano una formazione specializzata e controlli di accesso rigorosi. La segmentazione della rete e l'isolamento dei sistemi legacy sono pratiche comuni per proteggere i dispositivi dagli attacchi esterni.

Danimarca: le sfide includono i sistemi obsoleti e la comunicazione sicura tra i dispositivi OT. La preparazione e la sicurezza a più livelli sono considerate fondamentali per mitigare i danni e garantire la continuità operativa. Le aziende devono implementare misure di sicurezza pratiche e aggiornamenti regolari per proteggere le infrastrutture critiche.

Paesi Bassi: i vincoli finanziari e la mancanza di competenze specifiche in materia di OT rappresentano sfide significative. La formazione continua e la conformità normativa sono essenziali per migliorare la sicurezza. Le aziende devono trovare il giusto equilibrio tra sicurezza e operatività per mantenere un alto livello di protezione.

Area tematica 2: Pratiche di sicurezza informatica in ambito IT e OT

Criteri, priorità e impatto sulla gestione della sicurezza informatica

È fondamentale garantire continuità, qualità ed efficienza attraverso procedure standardizzate, backup regolari e monitoraggio in tempo reale. Trovare un equilibrio tra esigenze operative e requisiti di sicurezza è fondamentale per una gestione efficace della sicurezza informatica.

Analisi specifica per paese

Italia: L'adozione di sistemi senza password e la connettività sicura dei dipendenti sono priorità. Le politiche "no shaming" migliorano la cultura della sicurezza informatica e incoraggiano i dipendenti a segnalare gli incidenti senza timore di ripercussioni.

Spagna: la classificazione per criticità e l'analisi dell'impatto sono essenziali per identificare i componenti critici e implementare misure di sicurezza adeguate. La segmentazione della rete e l'implementazione di sistemi di monitoraggio avanzati sono pratiche comuni per proteggere le infrastrutture OT.

Estonia: le aziende estoni adottano backup regolari, formazione degli utenti e conformità agli standard internazionali per mantenere un solido livello di sicurezza. La segmentazione della rete e l'isolamento dei sistemi legacy sono essenziali per proteggere i dispositivi dagli attacchi esterni.

Danimarca: la sicurezza multilivello e i piani di emergenza sono considerati fondamentali per garantire la continuità operativa e la sicurezza delle infrastrutture critiche. Le aziende implementano misure di sicurezza pratiche e aggiornamenti regolari per proteggere i sistemi OT da accessi non autorizzati.

Paesi Bassi: una chiara struttura organizzativa e una risposta in tempo reale sono essenziali per garantire la sicurezza e la continuità operativa. La flessibilità nella gestione della sicurezza è fondamentale per affrontare le nuove minacce e mantenere un alto livello di protezione.

Area tematica 3: Lacune di conoscenza e fabbisogno di competenze

Profili professionali e competenze ricercate

Le aziende apprezzano una combinazione di competenze tecniche, capacità di risoluzione dei problemi e una comprensione sistemica della sicurezza informatica. Anche il lavoro di squadra e le capacità di comunicazione sono fondamentali. Ciò evidenzia la necessità di professionisti a tutto tondo, in grado di adattarsi alle sfide in continua evoluzione della sicurezza informatica.

Analisi specifica per paese

Italia: È importante comprendere i rischi aziendali e avere una visione sistemica. Le competenze tecniche nell'automazione e nell'IT sono fondamentali. La collaborazione interfunzionale e il pensiero critico sono apprezzati. Le aziende cercano professionisti in grado di comprendere i rischi in modo olistico e di comunicare efficacemente con i vari stakeholder.

Spagna: le aziende spagnole richiedono una combinazione di competenze trasversali quali comunicazione, lavoro di squadra, risoluzione dei problemi e flessibilità, nonché competenze tecniche quali SCADA, firewall industriali e segmentazione di rete, sempre accompagnate da una comprensione olistica dell'organizzazione e del core business.

Estonia: la capacità di lavorare in modo trasversale tra i reparti e le competenze tecniche per garantire la protezione dei sistemi legacy e la segmentazione della rete sono al centro delle competenze richieste dalle aziende estoni. Gli specialisti nella gestione delle reti industriali e gli amministratori sono profili altamente ricercati.

Danimarca: sono comuni le competenze pratiche nella gestione delle infrastrutture critiche, la formazione interna e gli approcci basati su scenari. La sicurezza multilivello e la preparazione sono fondamentali. Le aziende cercano profili con esperienza pratica nella gestione della sicurezza dei sistemi OT.

Paesi Bassi: sono fondamentali competenze tecniche nel campo delle TIC e della sicurezza informatica, la conoscenza degli standard internazionali e ottime capacità comunicative. L'apprendimento continuo e la capacità di adattamento sono essenziali. Le aziende cercano professionisti con competenze nella sicurezza del cloud e nell'intelligenza artificiale.

Area tematica 3: Lacune di conoscenza e fabbisogno di competenze

Competenze tecniche specifiche in materia di sicurezza informatica

La conoscenza di SIEM, EDR, sicurezza di rete e conformità agli standard internazionali è ampiamente riconosciuta. Il pensiero critico e le capacità di risoluzione dei problemi sono molto apprezzati. L'apprendimento continuo e il tenersi aggiornati sulle ultime tendenze e tecnologie in materia di sicurezza sono essenziali per i professionisti della sicurezza informatica.

Analisi specifica per paese

Italia: Le competenze tecniche richieste includono la gestione degli eventi di sicurezza (SIEM), il rilevamento e la risposta agli endpoint (EDR) e la sicurezza di rete. Il pensiero critico e la valutazione dei rischi sono fondamentali. Le aziende cercano anche competenze nella gestione delle identità e degli accessi (IAM) e nell'analisi dei log di sicurezza.

Spagna: le competenze richieste includono l'analisi delle vulnerabilità, la gestione degli incidenti e la conoscenza dei sistemi OT. Si pone l'accento sulla formazione continua e sulle misure proattive. Le aziende ricercano inoltre competenze in materia di crittografia, sicurezza cloud e monitoraggio della rete.

Estonia: le competenze tecniche includono la familiarità con SIEM, EDR e sicurezza di rete. L'apprendimento continuo e l'adattabilità sono essenziali per affrontare le nuove minacce. Le aziende cercano anche competenze nella gestione delle identità, nella configurazione dei firewall e nell'analisi delle vulnerabilità.

Danimarca: sono apprezzate le competenze pratiche nella gestione delle infrastrutture critiche, nella segmentazione della rete e nelle misure di sicurezza concrete. La preparazione e la sicurezza a più livelli sono fondamentali. Le aziende cercano anche competenze nella gestione dei log di sicurezza e nella risposta agli incidenti.

Paesi Bassi: le competenze richieste includono la sicurezza di rete, il cloud computing e l'intelligenza artificiale. La conformità alle normative e l'apprendimento continuo sono essenziali per mantenere un alto livello di sicurezza. Le aziende cercano anche competenze nell'analisi dei dati di sicurezza, nella gestione delle identità e nella protezione delle informazioni sensibili.

Area tematica 3: Lacune di conoscenza e fabbisogno di competenze

Standard e certificazioni

Certificazioni come CISSP, ISO 27001 e altri standard di settore sono ampiamente riconosciute e raccomandate. L'esperienza pratica e l'apprendimento continuo sono altrettanto importanti. Le certificazioni forniscono un punto di riferimento per le competenze e le conoscenze, ma l'esperienza pratica e l'apprendimento continuo sono essenziali per mantenere un'elevata competenza in materia di sicurezza informatica.

Analisi specifica per paese

Italia: le certificazioni raccomandate includono CISSP, ISO 27001 e programmi di formazione interna. L'accento è posto sull'apprendimento continuo e sull'adattabilità. Le aziende ricercano anche certificazioni nella sicurezza dei sistemi industriali e nella gestione delle identità.

Spagna: le certificazioni comprendono CISSP, CISM, CEH e ISO 27001. Viene sottolineata l'importanza della conformità a nuove normative come la NIS2. Le aziende ricercano anche certificazioni nella gestione degli incidenti e nella sicurezza del cloud.

Estonia: le certificazioni richieste includono CISSP, GSEC, ISO 27001 e standard locali come E-ITS. La formazione continua e i test di phishing sono pratiche comuni. Le aziende cercano anche certificazioni nella gestione delle identità e nella risposta agli incidenti.

Danimarca: sono apprezzate le certificazioni pratiche come CompTIA Security+, insieme alla formazione interna. La formazione basata su scenari è fondamentale. Le aziende cercano anche certificazioni nella gestione delle identità e nella sicurezza delle infrastrutture critiche.

Paesi Bassi: le certificazioni richieste sono ISO 27001, NIS2 e altri standard di settore. Si pone l'accento sull'esperienza pratica e sull'adattabilità. Le aziende ricercano anche certificazioni in sicurezza cloud e gestione degli incidenti.

Area tematica 3: Lacune di conoscenza e fabbisogno di competenze

Aree emergenti nella sicurezza informatica

La sicurezza del cloud, la sicurezza basata sull'intelligenza artificiale e la sicurezza dell'IoT sono identificate come aree di crescente domanda. La rapida evoluzione della tecnologia richiede ai professionisti della sicurezza informatica di aggiornare continuamente le proprie competenze e di adattarsi alle nuove sfide.

Analisi specifica per paese

Italia: L'attenzione è rivolta al pensiero sistemico, alla sicurezza nel cloud e alla sicurezza basata sull'intelligenza artificiale. La collaborazione in team e la formazione continua sono fondamentali per affrontare le nuove minacce. Le aziende ricercano competenze nell'analisi dei dati di sicurezza e nella gestione delle identità.

Spagna: la regolamentazione dell'IA e la sicurezza dell'IoT sono aree di competenza emergenti. L'integrazione dell'IA e la gestione dei dati nel cloud sono considerate cruciali per la sicurezza. Le aziende cercano competenze nella crittografia e nella protezione delle informazioni sensibili.

Estonia: il duplice ruolo dell'IA nella sicurezza informatica, la sicurezza del cloud e la conformità normativa sono aree di crescente domanda. La formazione continua e l'adattabilità sono essenziali per affrontare le nuove minacce. Le aziende cercano competenze nell'analisi dei dati di sicurezza e nella gestione delle identità.

Danimarca: la sicurezza basata sull'IA e la sicurezza dell'IoT sono aree di crescente domanda. La sicurezza a più livelli e la preparazione sono fondamentali per mitigare i rischi. Le aziende cercano competenze nella gestione delle identità e nella protezione delle informazioni sensibili.

Paesi Bassi: la sicurezza del cloud, la sicurezza basata sull'IA e la sicurezza dell'IoT sono identificate come aree emergenti. La conformità alle normative e l'apprendimento continuo sono essenziali per mantenere un alto livello di sicurezza. Le aziende cercano competenze nell'analisi dei dati di sicurezza e nella gestione delle identità.

Sintesi dei risultati

Area tematica 1: Consapevolezza della sicurezza informatica e rischi nelle aziende OT

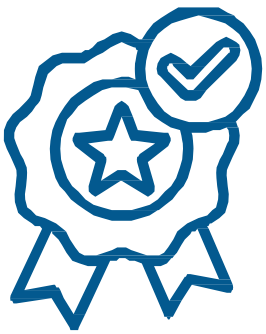
Risultati chiave. Per migliorare la sicurezza informatica è necessario: aumentare la consapevolezza, aggiornare la formazione, garantire una risposta rapida agli incidenti e rivedere e migliorare continuamente le politiche di sicurezza.

LA CONSAPEVOLEZZA, LA FORMAZIONE E LE POLITICHE DI SICUREZZA SONO ESSENZIALI

Vantaggi derivanti da migliore sicurezza informatica: maggiore fiducia dei clienti, protezione delle informazioni sensibili, continuità operativa, aumento della competitività, conformità normativa ed efficienza operativa.

Sfide: carenze di competenze,scarsa consapevolezza, gestione dei sistemi legacy mantenendo la sicurezza operativa in tempo reale.

Buone pratiche: segmentazione della rete, controlli di accesso rigorosi e aggiornamenti regolari del sistema, collaborazione tra i reparti OT e IT.



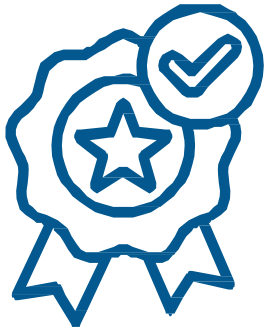
Sintesi dei risultati

Area tematica 2: Pratiche di sicurezza informatica in IT e OT

Risultati chiave: Misure di sicurezza informaticaper OT, garantire continuità, qualità ed efficienza e il monitoraggio in tempo reale sono fondamentali.

LA SICUREZZA INFORMATICA SU MISURA E LA SEGMENTAZIONE DELLA RETE SONO FONDAMENTALI NEGLI AMBIENTI OT

Sfide: limitazioni finanziarie, apparecchiature obsolete, mancanza di standardizzazione e accesso limitato



Buone pratiche: segmentazione della rete, gestione sicura dei fornitori, misure di sicurezza multilivello, formazione pratica basata su scenari e aggiornamenti continui dei sistemi.

Raccomandazioni: investire in formazione specializzata e fornire agli specialisti IT gli strumenti necessari per affrontare le sfide specifiche dell'OT. Promuovere la collaborazione tra i reparti IT e OT e garantire un approccio olistico alla sicurezza

Sintesi dei risultati

Area tematica 3: Lacune di conoscenza e fabbisogno di competenze

Risultati chiave: è fondamentale una combinazione di competenze tecniche, capacità di risoluzione dei problemi e una comprensione sistemica della sicurezza informatica.

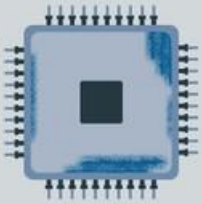
Fabbisogno di competenze: Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) e sicurezza di rete. Le aziende hanno inoltre apprezzato le competenze nell'analisi delle vulnerabilità, nella gestione degli incidenti e nella conformità agli standard internazionali. Sono state particolarmente apprezzate l'esperienza pratica nella gestione di infrastrutture critiche e la familiarità con i sistemi IT e OT.

L'APPRENDIMENTO CONTINUO E UN APPROCCIO OLISTICO SONO ESSENZIALI

Certificazioni: certificazioni quali Certified Information Systems Security Professional (CISSP), ISO 27001 e altri standard di settore sono state ampiamente riconosciute e raccomandate. Queste certificazioni forniscono un punto di riferimento per le competenze e le conoscenze richieste nei ruoli di sicurezza informatica.

Aree emergenti di competenza: Sicurezza, sicurezza basata sull'intelligenza artificiale e sicurezza IoT.

Cybersecurity weak points in companies



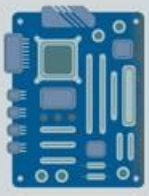
- Outdated firewalls
- Vulnerable identification systems
- Integration issues
- Lack or weak security policies
- Deficit in a comprehensive approach to cybersecurity risks
- Lack of standardization in OT systems
- Financial constraints
- Lack of specific OT expertise

Recommendations to improve cybersercurity in OT environments

- Continuous training of workers
- System updates
- Regular phishing tests / penetration tests
- Effective communication of security policy in the company
- Network segmentation and encryption
- Secure supplier management
- Regular backups
- Just in time monitoring
- Identification of critical components
- Comply with international standards
- Count with emergency plans
- Scenario based training

Skills demand for IT profiles

- Cybersecurity elements in an industrial plant
- Application of cybersecurity activities in operations and maintenance, according to the company´s security policy.
- Detection of anomalies in industrial control systems using monitoring tools and analysis procedures.



Skills demand for OT profiles

- Cloud security and AI
- Security Event Management (SIEM) and Endpoint Detection and Response (EDR)
- Network monitoring
- Security log management

Skills demand for both IT and OT profiles

- Understanding business risks and have a systematic vision
- Effective communication across profiles and departments regarding cybersecurity issues (policy, vulnerability detection, incidents...)
- International standards and regulations applied to the sector (with different proficiency levels of knowledge for IT and OT professionals). For example, CISSP, ISO 27001, NIS2.
- Understanding of the most frequent critical cybersecurity risks and their consequences/impact on the company (in terms of safety at work, money loses, environmental impact...)
- Critical thinking, problem solving, team collaboration, and continuous learning

Revisione degli attuali programmi di studio IT e OT della formazione professionale

I focus group e le interviste condotti dai partner ci hanno permesso di comprendere quali sono i punti deboli in materia di sicurezza informatica negli ambienti industriali automatizzati. Il feedback ricevuto includeva anche alcuni elementi chiave per migliorare la sicurezza informatica e quali sono le competenze necessarie nei profili IT e OT per attuarli. Analizzando gli attuali programmi di formazione professionale che vengono attualmente insegnati nei diversi paesi partner (Paesi Bassi, Spagna, Danimarca, Italia ed Estonia), siamo stati in grado di identificare lacune concrete in relazione alle competenze di sicurezza informatica richieste dalle aziende.

Poiché esistono diversi programmi di formazione professionale relativi all'IT e all'OT, sebbene con denominazioni diverse nei paesi partner, abbiamo concentrato la nostra analisi su 2 profili:

- Per l'IT, il profilo è quello di un Tecnico in Gestione e Amministrazione di Reti, ovvero il professionista che progetta e implementa l'infrastruttura di rete in un'organizzazione, sceglie i componenti hardware e software appropriati, configura i dispositivi e i protocolli di rete e coordina l'installazione delle apparecchiature e dei cavi di rete, risolve eventuali problemi che si presentano e documenta la configurazione e la topologia della rete.

- Per l'OT, il profilo è quello di un tecnico in automazione e robotica industriale, ovvero il professionista che lavora in aziende legate ai sistemi industriali automatici, nei settori della progettazione, dell'assemblaggio e della manutenzione dei sistemi di automazione industriale.

Di seguito, quando si fa riferimento ai profili IT/OT, ci si riferirà in particolare a questo tipo di tecnici.
Per il profilo IT, abbiamo analizzato le certificazioni descritte nella tabella sottostante. Dopo aver esaminato i contenuti e i risultati di apprendimento già coperti dagli attuali programmi di studio nei paesi del progetto, abbiamo identificato le lacune relative alla sicurezza informatica in ambienti industriali interconnessi, sulla base dei risultati emersi dalle aziende.

Paese	Titolo tradotto del programma di formazione	Durata del programma e numero di ore	Livello EQF	Breve descrizione dei settori professionali di attivita'
Paesi Bassi	Ingegnere di sistemi ICT	3 anni accademici (2500 ore)	4	Un ingegnere di sistemi ICT a livello MBO, Il percorso 4 (BOL) è specializzato nella progettazione, implementazione, gestione e manutenzione delle infrastrutture IT all'interno delle organizzazioni. Assicura il corretto funzionamento di reti, server e sistemi operativi, supportando i vari aspetti delle esigenze tecnologiche di un'organizzazione.
Spagna	Tecnico superiore in gestione di reti informatiche	2 anni accademici (2000 ore)	5	Il titolare di questo diploma avrà acquisito le competenze generali relative a: configurazione, amministrazione e manutenzione dei sistemi informatici, garantendo la funzionalità del sistema, l'integrità delle risorse e dei servizi, con la qualità richiesta e nel rispetto della legislazione vigente.

Estonia	Tecnologie dell'informazione e della comunicazione (TIC) – Livello 4	2 anni (se si proviene dalla scuola secondaria)	5	Uno specialista in sistemi informatici sviluppa e gestisce l'infrastruttura IT di un'organizzazione, fornendo soluzioni tecniche moderne per sistemi completi
Italia	Tecnico superiore per infrastrutture IT, rete, cloud e virtualizzazione - Specialista di rete e cloud ITS	2 anni (2000 ore)	5	Questo professionista è in grado di gestire, comprendere e progettare sistemi di sicurezza per le infrastrutture, integrando le norme di conformità in materia di protezione dei dati con le diverse esigenze aziendali

La certificazione di ingegnere di sistemi ICT nei **Paesi Bassi** è strutturata in 5 aree di competenza.

Confrontando i risultati di apprendimento già previsti dall'attuale curriculum con le richieste delle aziende industriali in termini di sicurezza informatica, di seguito sono riportate le lacune di competenze rilevate in ciascuna di queste aree.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Supporta utenti/richiedenti/clienti	Possiede una conoscenza di base della struttura degli ambienti OT.Comprende l'importanza dell'integrazione tra IT e OT, comprese le differenze fondamentali e le potenziali sfide in materia di sicurezza tra gli ambienti IT e OT. È in grado di comunicare con i professionisti OT e di fungere da tramite tra le esigenze dell'OT e dell'IT.
Installa e gestisce l'infrastruttura	Possiede conoscenze relative a protocolli e reti specifici dell'OT, come ad esempio Modbus. Possiede conoscenze e comprende la struttura e i componenti dei sistemi OT, quali i sistemi SCADA, i PLC (controllori logici programmabili) e i DCS (sistemi di controllo distribuito). Comprende la segmentazione di rete per gli ambienti OT e conosce i principi di progettazione di rete che isolano i sistemi OT dalle reti IT per ridurre al minimo i rischi.
Gestisce le applicazioni	Ha conoscenze di gestione delle patch per i sistemi OT e comprende le sfide specifiche dell'aggiornamento dei dispositivi OT, tenendo conto di fattori quali i tempi di inattività del sistema e la compatibilità. Ha conoscenze delle applicazioni utilizzate per i sistemi OT.
Sviluppa sistemi informative digitali (gestione database)	Possiede conoscenze relative agli script di base utilizzati nell'ambiente OT e alle relative vulnerabilità. Possiede conoscenze relative alle diverse piattaforme di dati per la protezione dei (big) data.
Controlli di sicurezza	Ha conoscenza delle potenziali vulnerabilità associate ai sistemi OT come SCADA. È in grado di eseguire valutazioni dei rischi specifiche per gli ambienti OT al fine di individuare le vulnerabilità di base nei sistemi OT. Possiede conoscenze relative alle potenziali vulnerabilità associate all'hardware OT, come i PLC. Conosce le varie normative e leggi relative alla sicurezza informatica OT, come NIS2 e ISO 27001.

In **Spagna, il piano di studi del corso di Tecnico Superiore in Gestione dei Sistemi di Reti Informatiche** è strutturato in moduli. Per ciascuno dei moduli tecnici, abbiamo individuato le lacune relative alla sicurezza informatica industriale

.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Implementazione dei sistemi operativi	Conosce il funzionamento di un sistema SCADA in un impianto di produzione.
Pianificazione e gestione delle reti	Progetta e configura la segmentazione di rete in un impianto di produzione, garantendo l'implementazione di misure di sicurezza informatica per proteggere le infrastrutture critiche e limitare l'accesso ai sistemi sensibili. Conosce i protocolli industriali come Modbus e OPC-UA
Fondamenti hardware	Implementa politiche di sicurezza fisiche (autenticazione, telecamere) e logiche (antivirus, anti-malware) per proteggere i dispositivi OT critici, garantendo l'integrità e la disponibilità dei sistemi industriali. Conosce cos'è un PLC, le sue caratteristiche e le funzioni generali
Gestione di database	Progetta ed esegue query SQL sicure, implementando tecniche di sanificazione degli input per prevenire attacchi di SQL injection.
Linguaggi di marcatura e sistemi di gestione delle informazioni	Implementa misure di convalida dei dati per prevenire iniezioni di codice nei documenti XML, la crittografia dei dati nello scambio di informazioni sensibili e configura le autorizzazioni di controllo degli accessi per prevenire attacchi Cross-Site Scripting (XSS) nelle interfacce HTML
Gestione dei sistemi operativi	Implementa Active Directory per controllare l'accesso ai sistemi industriali, applica le politiche di sicurezza ed esegue attività di auditing e monitoraggio per proteggere dalle minacce alla sicurezza. Configura servizi cloud, quali Infrastructure as a Service (IaaS) e Platform as a Service (PaaS), per migliorare l'efficienza, la sicurezza e la scalabilità dei sistemi industriali.
Servizi di rete e Internet	Implementa reti wireless industriali applicando gli standard del settore. Gestisce servizi di rete critici in ambienti industriali, quali server SCADA, sistemi di controllo distribuito (DCS) e reti di sensori industriali. Implementa sistemi di rilevamento delle intrusioni (IDS) e la segmentazione della rete per proteggere i sistemi critici da accessi non autorizzati.
Implementazione di applicazioni web	Configura le applicazioni web utilizzate in ambienti industriali, assicurando che siano implementate misure di sicurezza appropriate quali l'autenticazione, la crittografia dei dati e la protezione contro vulnerabilità comuni quali attacchi SQL injection e Cross-Site Scripting (XSS).

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Amministrazione dei sistemi di gestione di database	Attua misure di sicurezza informatica con sistemi MES, controllando l'accesso ai dati, monitorando costantemente e garantendo la disponibilità dei database distribuiti
Sicurezza e alta disponibilita'	Configura firewall specifici per proteggere le reti industriali da accessi non autorizzati e attacchi informatici. Conosce e applica le normative (NIS2) e gli standard (IEC 62443, NIST SP 800-82, ISO 27001) di sicurezza informatica specifici per gli ambienti industriali. Sviluppa, implementa e gestisce politiche di sicurezza in ambienti OT. Conosce le tecniche per identificare, conservare, analizzare e presentare le prove in caso di incidenti di sicurezza, utilizzando strumenti di analisi forense (Autopsy) per eseguire indagini forensi nei sistemi industriali. Implementa soluzioni di virtualizzazione per migliorare la sicurezza e la gestione dei sistemi industriali, consentendo una risposta rapida agli incidenti. Configura sistemi ad alta disponibilità per garantire la continuità operativa dei sistemi industriali critici, riducendo al minimo i tempi di inattività in caso di attacchi.
Competenze trasversali relative alla sicurezza informatica in ambienti industriali interconnessi	Comprende le operazioni aziendali e i rischi critici, avendo una visione sistemica/olistica delle diverse aree/dipartimenti e delle interazioni tra di essi. Comprende i rischi critici di sicurezza informatica più frequenti e le loro conseguenze/impatto sull'azienda (in termini di sicurezza sul lavoro, perdite economiche, impatto ambientale...) Comunica in modo efficace con i vari profili e reparti dell'organizzazione in merito alle questioni relative alla sicurezza informatica (politiche, individuazione delle vulnerabilità, incidenti...) Collabora con i profili OT dell'organizzazione per implementare attività di sicurezza informatica nell'ambito del funzionamento e della manutenzione dell'impianto industriale. Prende decisioni in situazioni critiche. Pianifica le attività. Segnala gli incidenti.

I corsi di studi estoni in Tecnologie dell'informazione e della comunicazione offrono diverse opzioni di specializzazione basate su materie opzionali. Il piano di studi è strutturato in crediti ECVET e garantisce un'ampia modularizzazione. Tuttavia, anche i percorsi specializzati in sicurezza informatica presentano delle lacune per quanto riguarda la sicurezza informatica industriale. Sono proprio queste le lacune che abbiamo individuato, concentrandoci su 7 aree di competenza:

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Gestione della sicurezza delle informazioni	Comprensione di framework quali il NIST Cybersecurity Framework, la norma ISO 27001 e i CIS Controls. Creazione e gestione della documentazione secondo standard quali E-ITS e ISO 27002.
Gestione della continuità operativa	È fondamentale comprendere e affrontare i rischi di sicurezza specifici del cloud. Comprendere le normative sulla protezione dei dati (ad es. GDPR, CCPA) e attuare misure volte a proteggere i dati sensibili.
Erogazione dei servizi	Identificare, valutare e mitigare le vulnerabilità nei sistemi e nelle applicazioni. Sviluppare e implementare piani di risposta agli incidenti per gestire efficacemente le violazioni della sicurezza. Sviluppare e fornire formazione sulla consapevolezza della sicurezza ai dipendenti per migliorare la loro comprensione delle minacce alla sicurezza e delle migliori pratiche. Comprendere la sicurezza modelli (IaaS,PaaS,SaaS) e l'implementazione di misure per proteggere i dati e le applicazioni nel cloud. Configurazione di firewall, sistemi di rilevamento delle intrusioni e altri controlli di sicurezza di rete per proteggere da accessi non autorizzati.
Protezione delle soluzioni IT	Comprensione dei diritti e delle autorizzazioni degli utenti all'interno dei sistemi di sicurezza. Familiarità con tecnologie specifiche, come MS Security. Conoscenza delle leggi e delle norme pertinenti (ad es. E-ITS, ISO). Capacità di configurare e comprendere le politiche di sicurezza. Conoscenza delle regole dei firewall, dell'analisi dei log e della gestione. Competenza nell'uso di vari strumenti di sicurezza informatica, tra cui IDS, firewall e sistemi SIEM. Comprensione e implementazione delle best practice di sicurezza delle applicazioni per proteggere le applicazioni dalle vulnerabilità.
Competenze trasversali	Capacità analitiche e di risoluzione dei problemi: capacità di analizzare incidenti di sicurezza complessi e sviluppare soluzioni efficaci. Capacità comunicative: ottime capacità comunicative per collaborare con team, parti interessate e soggetti esterni. Conoscenza dell'hacking etico: una profonda comprensione delle tecniche di hacking etico per identificare le vulnerabilità e migliorare il livello di sicurezza. Formazione continua: impegno a tenersi aggiornati sulle ultime tendenze, minacce e best practice in materia di sicurezza informatica.

I programmi di studio della formazione professionale in Italia sono definiti dalle regioni e possono presentare differenze, talvolta anche notevoli, tra loro. Inoltre, i programmi possono variare anche da istituto a istituto, specialmente nelle professioni legate alla tecnologia e alla digitalizzazione. Nel caso **dell'Italia**, abbiamo scelto di analizzare il programma di studio per il **Tecnico Superiore in Infrastrutture IT, Reti, Cloud e Virtualizzazione – Specialista in Reti e Cloud ITS,** in quanto il più affine agli altri analizzati dai partner.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Installazione di hardware e software	Formazione su metodi specifici per garantire la sicurezza durante l'installazione di hardware e software, in particolare in ambienti misti IT/OT. Garantire la compatibilità mantenendo la sicurezza delle informazioni. Identificazione e mitigazione delle vulnerabilità che potrebbero insorgere durante l'integrazione dei sistemi. Affrontare i rischi derivanti dall'integrazione di nuove tecnologie con i sistemi legacy, in particolare quelli vulnerabili a minacce comuni come il phishing o i componenti obsoleti. Migliorare la consapevolezza e la risposta ai vettori di attacco comuni durante l'installazione e la configurazione dei componenti.
Architettura dei computer	Identificare e risolvere potenziali vulnerabilità nella progettazione hardware/software. Implementare funzionalità di sicurezza che si adattino sia ai cambiamenti aziendali che a quelli tecnologici. Garantire la sicurezza delle nuove modifiche architetturali per mitigare il rischio di minacce informatiche. Enfatizzare i principi di progettazione sicura per architetture scalabili e interoperabili. Rafforzare la comprensione sistemica delle esigenze di sicurezza informatica, garantendo che la scalabilità e l'interoperabilità siano allineate a solidi framework di sicurezza. Incorporare una formazione pratica sull'identificazione e la valutazione delle vulnerabilità durante la progettazione dell'architettura. Migliorare la formazione sulla conformità normativa e applicare gli standard di sicurezza informatica durante la fase di progettazione dell'architettura.
Amministrazione dei sistemi IT	Comprendere le pratiche sicure per l'installazione e l'aggiornamento del software. Implementare procedure sicure per la configurazione degli aggiornamenti di sistema. Sensibilizzazione sui rischi legati all'utilizzo di software obsoleto e alla mancata installazione degli aggiornamenti. Enfasi sulle pratiche sicure di aggiornamento del software, compresa la gestione delle patch che risolve le vulnerabilità sia nei sistemi IT che OT. Formazione pratica su come gestire i sistemi OT obsoleti e le relative sfide di sicurezza informatica, come il mantenimento della sicurezza durante l'aggiornamento delle vecchie tecnologie. Colmare le lacune nelle competenze relative a strumenti di sicurezza specifici, come i sistemi di rilevamento e risposta sugli endpoint (EDR) e di gestione delle informazioni e degli eventi di sicurezza (SIEM).

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Manutenzione del sistema	Applicazione di metodi sicuri durante le riparazioni del sistema per prevenire le vulnerabilità. Riconoscimento delle minacce alla sicurezza informatica durante l'esecuzione delle attività di manutenzione. Rispondere agli incidenti legati alle vulnerabilità delle prestazioni del sistema; gestire gli incidenti in modo globale, garantendo al contempo un elevato livello di soddisfazione dei clienti. Gestione sicura delle attività di riparazione, in particolare per quanto riguarda i sistemi legacy. Garantire la sicurezza informatica durante le attività di riparazione fisica e allinearle alle procedure definite per impedire accessi non autorizzati.
Operazioni IT	Tecniche avanzate di rilevamento e mitigazione delle minacce alla sicurezza informatica. Piani di ripristino di emergenza con misure di sicurezza informatica. Risposte in tempo reale alle minacce, garantendo la continuità operativa. Backup sicuri, compresa la gestione dei rischi di sicurezza durante l'archiviazione e il recupero dei dati. Affrontare le sfide nel garantire continuità, qualità ed efficienza nei sistemi OT, mantenendo gli standard di sicurezza informatica.
Automazione	Pratiche di scripting sicure per garantire che l'automazione della gestione non introduca vulnerabilità. Comprensione delle potenziali vulnerabilità negli strumenti e nelle procedure di automazione. Sicurezza informatica relativa agli strumenti di automazione, comprese le vulnerabilità inerenti ai sistemi OT più vecchi o legacy Automazione dei controlli di sicurezza informatica per la conformità e l'integrità del sistema. Collaborazione con i reparti OT per affrontare in modo completo la sicurezza informatica nell'automazione.
Cloud computing	Applicazione misure di sicurezza informatica per proteggere ambienti virtuali. Garantire la privacy dei dati negli ambienti cloud. Sicurezza delle reti decentralizzate, in particolare per gli ambienti OT con requisiti operativi specifici. Sicurezza basata sull'intelligenza artificiale e sicurezza IoT. Comprensione delle misure di sicurezza multilivello, in particolare quelle volte a gestire in modo sicuro i servizi cloud di terze parti
Definizione e gestione degli indicatori chiave di prestazione (KPI)	KPI incentrati sulla sicurezza per valutare e migliorare il livello di sicurezza informatica degli ambienti IT e OT Analisi dei dati per identificare le lacune di sicurezza informatica nelle prestazioni del sistema. Incorporazione di KPI basati sul rischio che tengano conto dei sistemi legacy e delle loro potenziali vulnerabilità. Garantire che i KPI riflettano le minacce alla sicurezza informatica in continua evoluzione, come gli attacchi ransomware e di phishing, e che siano utilizzati per promuovere miglioramenti proattivi della sicurezza. Interpretazione dei dati dei KPI per migliorare il processo decisionale relativo alle misure e alle priorità di sicurezza informatica e le priorità.

Abbiamo svolto lo stesso esercizio analitico con i programmi di formazione professionale relativi a figure professionali adatte a lavorare in ambienti industriali con un elevato livello di digitalizzazione. In questo caso, abbiamo identificato 2 profili principali: meccatronica e automazione industriale. Ciascun partner ha analizzato il programma relativo a uno di essi per identificare le lacune relative alla sicurezza informatica

Paese	Titolo tradotto del programma di formazione	Durata del programma e numero di ore	EQF livello	Breve descrizione dei settori professionali di attivita'
Paesi Bassi	Tecnico meccatronico	3 anni accademici (2500 ore)	4	Un "Technicus Mechatronica" di livello MBO 4 (percorso BOL) è specializzato nella progettazione, costruzione, collaudo e manutenzione di sistemi meccatronici che combinano tecnologie meccaniche, elettriche e informatiche. Il suo lavoro abbraccia diversi settori, tra cui la produzione, l'automazione, la robotica e i macchinari ad alta tecnologia
Spagna	Tecnico superiore in automazione industriale e robotica	2 anni accademici (2000 ore)	5	Il titolare di questo diploma avrà acquisito le competenze generali relative a: sviluppo e gestione di progetti di assemblaggio e manutenzione di impianti automatici di misurazione, regolazione e controllo dei processi nei sistemi industriali, nonché supervisione, assemblaggio, manutenzione e implementazione di tali sistemi, nel rispetto dei criteri di qualità, sicurezza, tutela dell'ambiente e progettazione.
Estonia	Automatico	2 anni (se si proviene dalla scuola secondaria)	5	L'obiettivo del corso di studi è l'acquisizione di competenze che consentano di operare come operatore specializzato in aziende specializzate nell'automazione della produzione o nell'automazione degli edifici.
Italia	ITS Digital Solution 4.0 Specialista nella transizione digitale	2 anni (2000 ore)	5	Gli specialisti IDT sono professionisti IT che sviluppano soluzioni integrate su misura per guidare le aziende verso la digitalizzazione, creando ambienti cyber-fisici che ottimizzano la gestione dei dati

Nel programma di studi offerto nei **Paesi Bassi per il "Technicus Mechatronica MBO 4"** sono presenti 3 aree di competenza principali. Sebbene il programma di studi fornisca una buona combinazione di conoscenze e competenze IT e OT, abbiamo comunque rilevato grandi lacune relative alla sicurezza informatica.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Produzione di prodotti meccatronici	Possiede conoscenze di base sull'IoT (Internet delle cose) e comprende come l'IoT sia integrato nei sistemi meccatronici per il monitoraggio, il controllo e la raccolta dati a distanza Possiede una conoscenza di base dell'IT in ambito industriale e comprende gli aspetti IT rilevanti coinvolti. Possiede la consapevolezza necessaria per garantire la sicurezza degli sviluppi Possiede conoscenze per garantire la sicurezza dell'infrastruttura delle macchine e dell'apprendimento automatico
Installazione e modifica di prodotti e/o sistemi meccatronici	Possiede conoscenze di base sulla sicurezza informatica per gli ambienti industriali. Conosce i rischi di sicurezza informatica comuni di base negli ambienti industriali. Conoscenze di base sulle reti e sulla connettività, comprensione dei fondamenti della risoluzione dei problemi relativi alle connessioni di rete. Capacità di valutare i rischi legati all'uso/installazione degli strumenti Consapevolezza delle possibili minacce all'interno dei programmi o degli strumenti da utilizzare.
Guida e gestione del processo lavorativo	È in grado di utilizzare strumenti di monitoraggio e diagnostica remota che consentono la diagnostica, il monitoraggio e la manutenzione a distanza di apparecchiature meccatroniche. È in grado di comunicare con gli specialisti IT per lavorare in modo orientato alla risoluzione dei problemi. Possiede conoscenze in materia di protezione dei dati Possiede conoscenze o comprende le minacce alla sicurezza informatica, quali phishing, malware o tattiche di ingegneria sociale.

In **Spagna abbiamo analizzato il profilo del Tecnico Superiore in Automazione Industriale e Robotica**, che è quello più richiesto dalle aziende nel nostro contesto per integrare competenze informatiche relative alla sicurezza informatica. Il governo spagnolo ha persino istituito un corso di specializzazione sulla sicurezza informatica negli ambienti OT, accessibile a chi è già in possesso del certificato di Tecnico Superiore in Automazione Industriale e Robotica (maggiori informazioni nel supplemento Europass:

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Sistemi elettrici, pneumatici e idraulici	È consapevole della necessità di modificare le password predefinite per dispositivi quali relè o controllori pneumatici al fine di proteggere l'accesso alle apparecchiature.
Sistemi sequenziali programmabili	Implementa controlli di accesso tramite password sui sistemi di controllo sequenziale per garantire che solo il personale autorizzato possa modificare la logica di controllo.
Sistemi di misurazione e controllo	Monitora e registra le letture dei sensori in modo da poter identificare comportamenti anomali o manomissioni dei dati al fine di rilevare potenziali problemi di sicurezza.
Sistemi di alimentazione	Conosce l'importanza di modificare le credenziali predefinite dei dispositivi connessi in rete, quali inverter o sistemi UPS, una pratica semplice ma cruciale per impedire accessi non autorizzati
Documentazione tecnica	Include una cronologia delle modifiche nella documentazione tecnica, che registra chi ha modificato ogni sezione e quando, contribuendo così a prevenire e individuare eventuali alterazioni non autorizzate.
Informatica industriale	Installa e configura antivirus e firewall sui sistemi informatici che controllano la produzione, come misura semplice per proteggere i sistemi dal malware.
Sistemi programmabili avanzati	Blocca l'accesso remoto ai PLC quando non è necessario, come misura di base per proteggersi da accessi non autorizzati.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Robotica industriale	Imposta elenchi di accesso sui robot industriali per definire quali utenti possono modificare i programmi o controllare il robot, riducendo il rischio di manipolazioni indesiderate.
Comunicazione industriale	Conosce le principali vulnerabilità legate al cloud computing (configurazioni errate, minacce interne, perdita e fuga di dati, interfacce e API non sicure) e i metodi utilizzati dagli hacker per sfruttarle (phishing, bug software, attacchi DoS, ingegneria sociale, ransomware e malware). Conosce i metodi e gli strumenti per proteggere le vulnerabilità relative al cloud computing, in linea con la politica di sicurezza dell'organizzazione. Conosce il piano di risposta agli incidenti, parte della soluzione SIEM implementata dall'organizzazione. Interpreta e rileva le anomalie sulla base dei dati forniti dai sistemi MES (Manufacturing Execution Systems) e dai sistemi HMI. Configura la crittografia di base nella trasmissione dei dati, ad esempio utilizzando VPN o protocolli sicuri per proteggere le comunicazioni tra i dispositivi industriali.
Integrazione dell'automazione industriale	Tiene conto dei rischi esistenti nella pianificazione e nell'installazione di un sistema automatizzato, identificando quando è necessario un sistema EDR e quale scegliere. Conosce gli standard e le normative internazionali applicati al settore (ad esempio, CISSP, ISO 27001, NIS2) e, in particolare, lo standard ISA/IEC 62443, particolarmente rilevante per l'automazione industriale. Applica la gestione dei registri di sicurezza durante la progettazione e l'installazione di un sistema automatizzato. Conosce i sistemi di controllo industriale (ICS, come ad esempio SCADA) e sa quali sono i diversi componenti di una rete OT e come sono interconnessi. Segmentazione della rete: creare diagrammi che isolino le reti di automazione critiche dal resto delle reti aziendali.
Competenze trasversali relative alla sicurezza informatica in ambienti industriali interconnessi	Comprende i rischi aziendali e ha una visione sistemica/olistica delle diverse aree/dipartimenti e delle interazioni tra di essi. Elevata consapevolezza dei rischi informatici che interessano i sistemi OT, conoscenza di siti come shodan.io e della sua sezione dedicata agli ICS o MITREATT&CKforICS1 per valutare il numero di minacce a cui questi sistemi sono esposti. Comunica in modo efficace tra profili e reparti in merito a questioni di sicurezza informatica (politiche, rilevamento delle vulnerabilità, incidenti…) Consapevolezza: identificazione delle minacce comuni negli ambienti industriali. Risoluzione dei problemi: individuazione e correzione delle falle di sicurezza. Gestione dei rischi: valutazione dei rischi: identificazione delle potenziali vulnerabilità. Comunicazione efficace: spiegare le migliori pratiche di sicurezza di base a un pubblico non tecnico (come gli operatori). Responsabilità ed etica professionale: analisi delle violazioni della sicurezza che possono influire su individui e aziende. Autonomia e apprendimento continuo: tenersi aggiornati sulle ultime tendenze nella cyber sicurezza industriale.

Dopo aver esaminato diversi profili in **Estonia**, abbiamo selezionato il curriculum per "Automaticista", che è molto simile nei contenuti a quello spagnolo, sebbene strutturato in modo diverso, con una combinazione di studi generali e studi tecnici. Per l'analisi, ci siamo concentrati solo sulla parte tecnica. Le lacune relative alla sicurezza informatica industriale sono molto simili a quelle rilevate nel curriculum spagnolo.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Funzionamento di apparecchiature e sistemi di automazione	Architetture ICS: acquisire familiarità con le architetture ICS più comuni, inclusi i sistemi SCADA (Supervisory Control and Data Acquisition), i sistemi di controllo distribuito (DCS) e i controllori logici programmabili (PLC). Protocolli di comunicazione industriale: comprendere protocolli come Modbus, Profibus, Ethernet/IP e OPC UA, nonché le loro implicazioni in termini di sicurezza. Dispositivi OT: essere consapevoli delle vulnerabilità specifiche dei dispositivi OT, quali sensori, attuatori e controllori.
Installazione di apparecchiature e sistemi di automazione	Segmentazione della rete: implementare la segmentazione della rete per isolare le reti OT dalle reti IT aziendali e ridurre la superficie di attacco. Configurazione del firewall: configurare i firewall per limitare l'accesso alle reti e ai dispositivi OT. Gestione delle patch: aggiornare regolarmente i dispositivi OT e il software con patch di sicurezza. Controllo degli accessi: implementare rigorosi controlli degli accessi per limitare l'accesso ai sistemi e ai dispositivi OT. Monitoraggio della sicurezza: utilizzare strumenti di monitoraggio della sicurezza per rilevare e rispondere ad attività anomale sulle reti OT.
Conoscenze di base di automazione	Spionaggio industriale: comprendere i rischi di accesso non autorizzato ai sistemi OT finalizzato al furto di proprietà intellettuale o all'interruzione delle operazioni. Sabotaggio: prestare attenzione alle minacce provenienti da soggetti malintenzionati che mirano a danneggiare o interrompere le infrastrutture critiche. Attacchi alla catena di approvvigionamento: comprendere i rischi legati alla compromissione di componenti hardware o software.
Fondamenti di ingegneria elettrica ed elettronica	Conoscere l'importanza di modificare le credenziali predefinite dei dispositivi connessi alla rete, come inverter o sistemi UPS, una pratica semplice ma cruciale per prevenire accessi non autorizzati. Controllo e aggiornamento delle password.
Competenze trasversali	Aggiornamento professionale sull'hacking dei sistemi di controllo industriale: resta informato sulle ultime tecniche utilizzate dagli hacker per attaccare gli ICS. Intelligenza artificiale e apprendimento automatico per migliorare la sicurezza OT, ad esempio per il rilevamento delle anomalie e la manutenzione predittiva.

Il curriculum analizzato nel caso **dell'Italia** è senza dubbio quello che offre il programma più "ibrido" tra conoscenze e competenze IT e OT tra quelli esaminati dal partenariato ai livelli 4-5 dell'EQF nei nostri rispettivi paesi. Sebbene offra una buona combinazione, abbiamo comunque individuato diverse lacune in termini di sicurezza informatica.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Implementazione dell'impresa digitale	Integrità dei dati, riservatezza e rilevamento delle minacce. Standard e protocolli di sicurezza nei sistemi IT. Formazione pratica basata su scenari e simulazioni per migliorare la risposta agli incidenti.
Codifica e test	Pratiche di codifica sicura per prevenire le vulnerabilità. Modellazione delle minacce come parte dello sviluppo del software. Analisi delle vulnerabilità, sistemi SIEM ed EDR per migliorare la sicurezza della codifica Metodologie di debug sicure per identificare e mitigare i rischi di sicurezza.
Progettazione e sviluppo di applicazioni	Comunicazione sicura tra dispositivi di automazione industriale. Vulnerabilità specifiche dei sistemi di controllo in tempo reale. Mitigazione dei rischi nelle reti di automazione.
Progettazione e implementazione di soluzioni IoT	Architetture di rete sicure per l'integrazione IT OT. Tecniche di segmentazione per ridurre i rischi di sicurezza. Sistemi legacy e sicurezza operativa in tempo reale. Mitigazione delle minacce specifiche per l'OT e risposta agli incidenti
Tecnologia di monitoraggio	Impatto della sicurezza informatica sull'integrazione delle nuove tecnologie. Identificazione delle vulnerabilità introdotte dalle tecnologie emergenti. Convalida della sicurezza prima dell'implementazione delle nuove tendenze. La sicurezza del cloud, la sicurezza basata sull'intelligenza artificiale e la sicurezza dell'IoT come settori emergenti in cui cresce la domanda.
Processo decisionale strategico	Incorporare le considerazioni relative alla sicurezza informatica nella pianificazione strategica delle TIC. Concentrarsi sulle misure di protezione dei dati per i processi orientati al cliente. Allineare le strategie TIC agli standard di sicurezza informatica del settore e alla conformità. Sviluppo di framework di sicurezza informatica che rafforzino la fiducia dei clienti e il vantaggio competitivo.
Gestione dei dati	Protezione dei dati durante la raccolta, l'analisi e l'archiviazione. Gestione dei dati in un cloud sicuro e sicurezza basata sull'IA. Tecniche di crittografia per l'integrità dei dati.

Aree di competenza	Lacune relative alla sicurezza informatica negli ambienti industriali interconnessi
Gestione dei clienti	Valutazione dei rischi di sicurezza informatica nell'ambito della consulenza ai clienti. Gestione sicura dei fornitori e standard di sicurezza informatica. Soluzioni tecnologiche resilienti e sicure. Analisi delle esigenze di sicurezza del cliente per una consulenza su misura sulle alternative tecnologiche. Gestione degli incidenti.
Trasformazione digitale	Gestione dei rischi di sicurezza informatica durante le iniziative di trasformazione digitale. Procedure standardizzate di backup e monitoraggio in tempo reale per la continuità del progetto. Comunicazione sicura e integrità del sistema durante le modifiche. Protezione delle risorse digitali durante tutto il ciclo di vita della trasformazione.
Gestione dei progetti	Gestione dei rischi di sicurezza informatica nella pianificazione del progetto. Gestione sicura delle tappe fondamentali del progetto che comportano la convergenza IT-OT. Comunicazione e coordinamento sicuri all'interno di team interfunzionali. Conformità normativa e approccio basato sul rischio per la gestione della sicurezza informatica. KPI di sicurezza informatica quali la frequenza degli incidenti e le vulnerabilità del sistema. Rendicontazione delle misure di sicurezza informatica. Valutazione delle prestazioni secondo gli standard di sicurezza informatica.

Risultati chiave

I programmi di formazione professionale sia IT che OT analizzati sono simili in tutti i paesi del progetto, a conferma del feedback ricevuto dalle aziende durante i focus group, indipendentemente dal settore in cui operano.

Ai livelli EQF analizzati, abbiamo osservato che i programmi di formazione professionale in Estonia e in Italia offrono una gamma più ampia di specializzazioni e un mix di contenuti IT e OT, ma trascurano ancora competenze specifiche di sicurezza informatica in contesti industriali.

Prossimi passi

Dopo aver analizzato i diversi programmi di formazione professionale relativi all'IT (gestione delle reti) e all'OT (automazione industriale e digitalizzazione), abbiamo classificato le lacune in tre gruppi di competenze necessarie ai lavoratori IT e OT per operare in ambienti industriali cybersicuri:

COMPETENZE TECNICHE

Competenze necessarie per svolgere il proprio lavoro quotidiano, comprese le competenze tecniche in materia di sicurezza informatica in base al proprio profilo e al proprio ruolo nell'organizzazione.

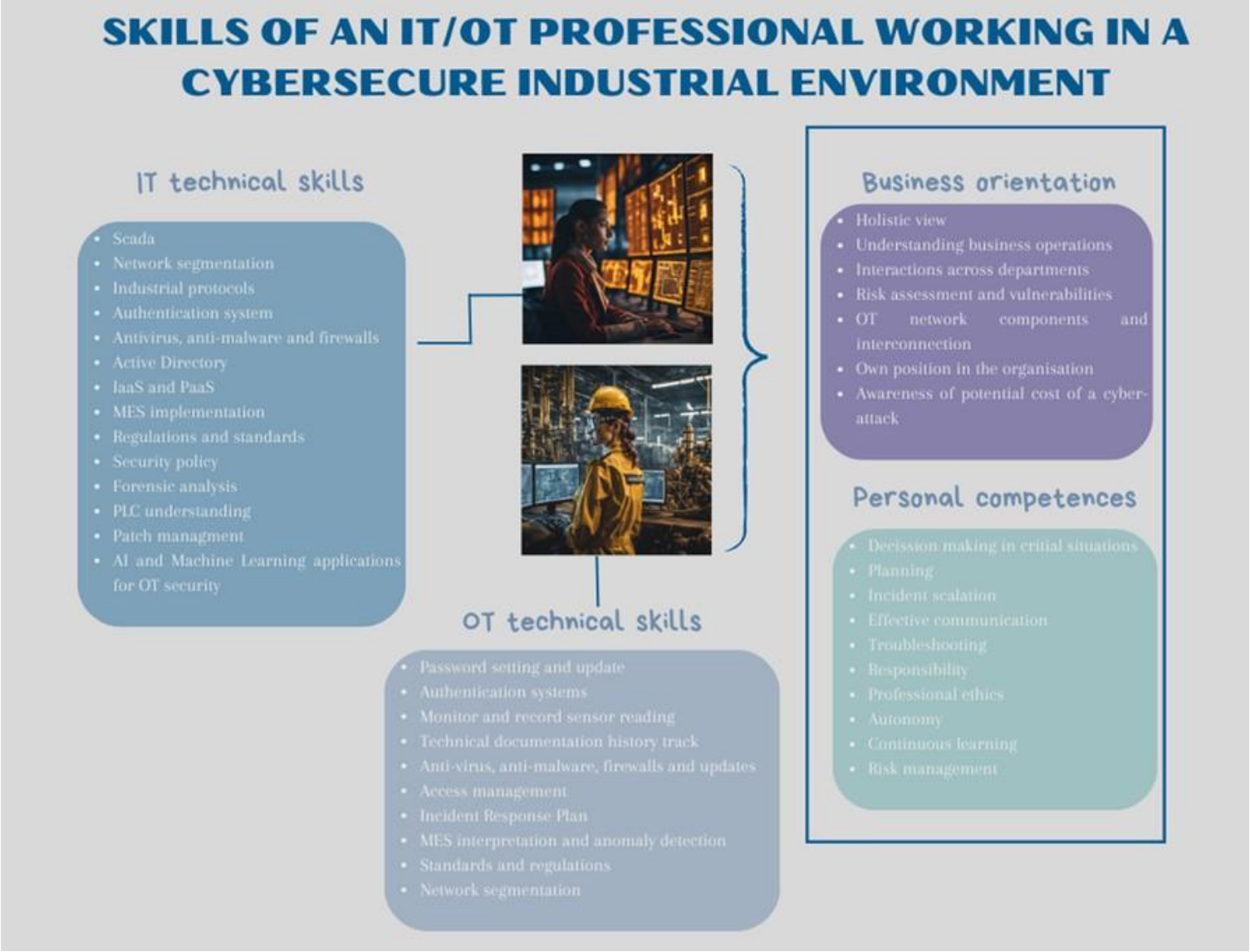
ORIENTAMENTO AL BUSINESS

La capacità di comprendere l'azienda nel suo complesso e di sapersi posizionare all'interno della struttura aziendale. Comprende anche la capacità di valutare i potenziali rischi di un attacco informatico per l'azienda, nonché l'impatto che potrebbe avere sulla sicurezza delle persone, sulla capacità produttiva o sui dati sensibili.

COMPETENZE PERSONALI

Competenze necessarie per interagire con i colleghi e tra reparti aziendali, riflettere e pensare in modo critico, risolvere problemi, analizzare situazioni da prospettive diverse, lavorare in modo autonomo ma anche come parte di un team agendo in modo collaborativo.

Abbiamo raggruppato le competenze individuate come lacune in ciascun curriculum secondo la classificazione menzionata. Le competenze tecniche sono specifiche per ciascun profilo (IT/OT), mentre quelle che rientrano nelle categorie “orientamento aziendale” e “competenze personali” per quanto riguarda la sicurezza informatica, sono le stesse per entrambi.



Mentre nei diversi paesi esistono opzioni per proseguire gli studi e specializzarsi in sicurezza informatica industriale rivolte sia ai profili OT che IT della formazione professionale, l’approccio di Cyber-In è quello di intendere le competenze di sicurezza informatica come trasversali a qualsiasi figura professionale e, in particolare, la sicurezza informatica industriale come trasversale ai professionisti IT e OT, specialmente a quelli maggiormente coinvolti nei processi industriali automatizzati, come richiesto dalle aziende.

Al fine di garantire ambienti industriali sicuri con un elevato livello di automazione (intendendo la sicurezza da tutti i possibili punti di vista), la sicurezza informatica deve essere integrata nel curriculum dei professionisti IT e OT.

Inoltre, le richieste del settore puntano verso un profilo ibrido/interdisciplinare IT/OT, specializzato in sicurezza informatica industriale. Mentre l'integrazione dei risultati di apprendimento relativi alla sicurezza informatica negli attuali profili IT e OT offerti nei diversi paesi migliorerà la preparazione di questi professionisti, la nostra raccomandazione, sulla base dei risultati delle nostre ricerche, è quella di offrire un programma di formazione professionale interdisciplinare in sicurezza informatica industriale come specializzazione per entrambi i tipi di professionisti.

Abbiamo definito un programma di studi di questo tipo allineato ai quadri EQF ed ECVET, utilizzando una struttura modulare che può essere suddivisa in microcredenziali per facilitare l'acquisizione e l'accreditamento delle competenze necessarie

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Struttura del programma ed integrazione nei programmi di IFP esistenti

Questo **programma di studi interdisciplinare** integra le competenze in materia di sicurezza informatica delle tecnologie dell'informazione (IT) e delle tecnologie operative (OT) in un programma di specializzazione rivolto a laureati/lavoratori di questi settori. Affronta le lacune di competenze individuate nel report Cyber-In sulle esigenze delle aziende e promuove pratiche di sicurezza collaborative in ambienti OT, garantendo che i laureati/lavoratori in questo campo siano in grado di progettare, implementare e mantenere sistemi industriali sicuri.

Il programma è in linea con i profili ESCO quali "**Tecnico della sicurezza informatica**" e "Tecnico dell'automazione industriale", coprendo le competenze comuni a questi due profili. È stato strutturato secondo i principi ECTS, dove 1 credito equivale a circa 25 ore di apprendimento.

Il numero totale di ore del programma di studi è di circa **250 ore, equivalenti a 10 crediti ECTS**. Secondo il Quadro europeo delle qualifiche e considerando che questo programma di specializzazione si rivolge principalmente a laureati di programmi di istruzione e formazione professionale (IFP) in ambito IT/OT con un livello EQF 4-5, il programma di specializzazione è stato concepito come un livello EQF 5.

Sebbene lo sviluppo del curriculum interdisciplinare completo proposto dal progetto Cyber-In sia incoraggiato, l'obiettivo di Cyber-In non è quello di sviluppare un programma di specializzazione da completare come aggiunta agli attuali diplomi IT e OT, ma di INTEGRARE alcuni dei risultati di apprendimento (conoscenze, abilità e competenze) definiti nel curriculum e identificati dalle aziende intervistate dai partner del progetto come trasversali ed essenziali per un professionista nell'amministrazione e gestione di reti IT e per gli operatori in ambienti industriali automatizzati e interconnessi.

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Abbiamo quindi progettato un corso più breve che affronta i suddetti risultati di apprendimento e che può essere più facilmente integrato nei programmi attuali perché:

- Ha una durata più breve ed è suddiviso in moduli e capitoli brevi, facilitando la sua integrazione nei contenuti già insegnati nei programmi di informatica e di formazione professionale.

- Ha un impatto particolare sugli aspetti attitudinali e influenza il fattore umano e la concezione della sicurezza informatica come parte della cultura aziendale.

- Si concentra su concetti chiave, definizioni e strumenti relativi alla sicurezza informatica industriale. Non approfondisce gli aspetti tecnici, ma copre comunque gli elementi essenziali e lascia spazio per concentrarsi su aspetti particolari della sicurezza informatica industriale a seconda dello scopo del corso o degli obiettivi di apprendimento fissati dall'insegnante/formatore o dal lavoratore nel caso di dipendenti o neolaureati.

Il **MOOC Cyber-**In consente ai partecipanti di comprendere i concetti e gli elementi principali relativi alla sicurezza informatica industriale. Permette loro di utilizzare e interpretare gli strumenti di monitoraggio, analizzare i potenziali rischi e le vulnerabilità e adottare un approccio proattivo per ridurre al minimo i rischi di violazione. Il Mooc fornisce inoltre ai partecipanti le conoscenze relative alle più recenti normative in materia di sicurezza informatica negli ambienti industriali e al modo in cui queste influiscono sulle aziende e sul loro ruolo di professionisti.

Il MOOC è aperto, senza necessità di registrazione, a qualsiasi utente interessato a migliorare tali competenze. L'accesso è disponibile tramite il sito web del progetto: **www.cyber-in.eu**, nella sezione "**risorse didattiche".**

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Programma ed integrazione nei programmi di istruzione e formazione professionale esistenti

Titolo del modulo	ECVET/ECTS Credits	Durata
Modulo 1. Introduzione alla sicurezza informatica negli ambienti OT	0,4	**10 ore**
Modulo 2. Segmentazione e protocolli industriali	1,6	**40 ore**
Modulo 3. Sistemi di rilevamento delle intrusioni (IDS) per la gestione della continuità operativa	1,2	**30 ore**
Modulo 4. Standard e normative sulla sicurezza informatica OT	0,8	**20 ore**
Modulo 5. Sistemi di gestione centralizzata della sicurezza e applicazioni di IA	1,2	**30 ore**
Modulo 6. Gestione della continuità operativa e fornitura dei servizi	0,8	**20 ore**
Modulo 7. Progetto: Protezione di una fabbrica intelligente	4	**100 ore**

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Descrizioni dei moduli

Modulo 1 — Introduzione alla sicurezza informatica negli ambienti OT

Durata: 10 ore | 0,4 crediti ECTS

Obiettivo: Comprendere i fondamenti della sicurezza informatica, la convergenza IT-OT e il panorama delle minacce industriali.

Contenuti:

- Principi e definizioni della sicurezza informatica: triade CIA, difesa in profondità, rischio vs. resilienza.
- Differenze tra le priorità IT e OT.
- Casi di studio: Stuxnet, BlackEnergy, Industroyer

Risultati di apprendimento:

- Conoscenze: spiegare i principi OT, il controllo dei processi e la relazione tra CIA e sicurezza.
- Competenze: Identificare i componenti del sistema OT e mapparli all'interno dell'architettura di un impianto.
- Competenze: Riconoscere le conseguenze cyber-fisiche delle violazioni della sicurezza.

Metodi di valutazione: Discussione di gruppo, valutazione pratica, test.

Micro-credenziale 1: Cyber-In Modulo 1. Introduzione alla sicurezza informatica negli ambienti OT

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Descrizioni dei moduli

Modulo 2 — Segmentazione e protocolli industriali

Durata: 40 ore | 1,6 crediti ECTS

Obiettivo: Identificare e classificare i componenti e le architetture industriali utilizzando il Modello Purdue.

Contenuti:

- Componenti OT: PLC, RTU, SCADA, sensori, HMI.
- Mappatura del sistema, inventario delle risorse e interdipendenze.
- Gerarchia di controllo industriale e mappatura del flusso di dati.

Risultati di apprendimento:

- Conoscenze: Descrivere il modello Purdue, le zone di rete, i condotti e i flussi di dati.
- Abilità: Applicare la segmentazione e identificare i protocolli non sicuri.
- Competenze: Progettare e documentare un piano di segmentazione della rete OT.

Metodi di valutazione: Discussione di gruppo, valutazione pratica, test.

Micro-credenziale 2: **Modulo 2 di Cyber-In. Segmentazione e protocolli industriali**

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Descrizioni dei moduli

Modulo 3 — Reti industriali e sicurezza dei protocolli

Durata: 30 ore | 1,2 crediti ECTS

Obiettivo: garantire la sicurezza dei protocolli industriali e dei canali di comunicazione.

Contenuti:

- Sicurezza di Modbus, OPC-UA, PROFINET, DNP3 e MQTT.
- Strumenti di analisi di rete e ispezione dei pacchetti.
- Progettazione e implementazione di canali sicuri (TLS, VPN).

Risultati di apprendimento:

- Conoscenze: firewall di nuova generazione
- Abilità: configurare sensori IDS/IPS, interpretare gli avvisi, valutare le anomalie.
- Competenze: Correlare i dati di monitoraggio con le esigenze di sicurezza operativa e proporre azioni correttive.

Metodi di valutazione: discussione di gruppo, valutazione pratica, prova

Micro-credenziale 3: Cyber-In Modulo 3. Sistemi di rilevamento delle intrusioni e sicurezza nei firewall

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Descrizione dei moduli

Modulo 4 — Standard e normative sulla sicurezza informatica OT

Durata: 20 ore | 0,8 crediti ECTS

Obiettivo: apprendere i principali standard e normative in materia di sicurezza informatica OT

Contenuti:

- Legge UE sulla resilienza informatica
- IEC 62443
- Valutazione della sicurezza informatica e tipi di test

Risultati di apprendimento:

- Conoscenze: Differenza tra direttiva, norma e regolamento
- Abilità: Pentesting e rilevamento delle vulnerabilità
- Competenze: Conformità a norme e regolamenti

Metodi di valutazione: discussione di gruppo, valutazione pratica, prova

Micro-credenziale 4. Modulo 4 di Cyber-In. Standard e normative sulla sicurezza informatica OT

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Descrizioni dei moduli

Modulo 5 — Sistemi di gestione centralizzata della sicurezza e applicazioni di IA

Durata: 30 ore | 1,2 crediti ECVET/ECTS

Obiettivo: applicare gli standard pertinenti e condurre valutazioni dei rischi per la sicurezza informatica industriale.

Contenuti:

- Gestione centralizzata della sicurezza
- Applicazioni di IA
- Governance e politiche

Risultati di apprendimento:

- Conoscenze: comprensione del CMS
- Abilità: identificare i ruoli, le politiche e le procedure essenziali per la governance della sicurezza
- Competenze: applicare il CMS e utilizzare applicazioni di IA per il rilevamento delle minacce e risposte

Metodi di valutazione: Discussione di gruppo, valutazione pratica, test.

Micro-credenziale 5. Modulo Cyber-In Sistemi di gestione centralizzata della sicurezza e rilevamento delle minacce in tempo reale negli ambienti IT aziendali

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Descrizioni dei moduli

Modulo 6 — Gestione della continuità operativa ed erogazione dei servizi

Durata: 20 ore | 0,8 crediti ECTS

Obiettivo: integrare l'ingegneria della sicurezza e la sicurezza informatica nelle infrastrutture critiche.

Contenuti:

- Concetto e sfide della gestione della continuità operativa
- Best practices
- Erogazione dei servizi
- ITIL

Risultati di apprendimento:

- Conoscenze: Comprendere i concetti di BCM, erogazione dei servizi e Zero Trust
- Abilità: Come garantire la gestione della continuità operativa e l'erogazione dei servizi
- Competenze: applicare strategie di ripristino e progettare piani di risposta agli incidenti

Metodi di valutazione: Discussione di gruppo, valutazione pratica, test.

Micro-credenziale 6 — Modulo Cyber-In: Gestione della continuità operativa e fornitura dei servizi

Un programma di studi interdisciplinare di istruzione e formazione professionale (IFP) in materia di sicurezza informatica industriale

Descrizioni dei moduli

Modulo 7 — Progetto. Protezione di una fabbrica intelligente

Durata: 100 ore | 4 crediti ECTS

Obiettivo: applicare tutte le competenze acquisite nei moduli precedenti in uno scenario simulato di fabbrica intelligente.

Contenuti:

- Progettazione e implementazione in team di una rete industriale sicura.
- Test di sicurezza, mitigazione dei rischi e gestione degli incidenti.
- Presentazione del progetto.

Risultati di apprendimento:

- Conoscenze: integrare la progettazione OT, la gestione dei rischi e i concetti relativi a standard e normative.
- Abilità: Sviluppare e presentare un piano di sicurezza informatica industriale.
- Competenze: giustificare le decisioni prese in materia di progettazione e sicurezza.

Metodi di valutazione: Discussione di gruppo, valutazione pratica, test.

Micro-credenziale 7. Attività didattica basata su sfide

Conclusioni

La sicurezza informatica OT aumenta la fiducia dei clienti e garantisce la continuità operativa

Le aziende dei paesi coinvolti riconoscono che la sicurezza informatica offre numerosi vantaggi, tra cui una maggiore fiducia dei clienti, la protezione delle informazioni sensibili e la garanzia della continuità operativa. I benefici derivanti dalla protezione dell'ambiente OT si scontrano con la sfida di trovare professionisti IT con conoscenze specifiche delle reti OT, nonché professionisti OT con un livello adeguato di consapevolezza dei rischi di sicurezza informatica e sufficiente autonomia e competenze tecniche per svolgere un ruolo nell'architettura complessiva di sicurezza informatica dell'azienda.

Aumentare la consapevolezza e la formazione è quindi fondamentale per migliorare la sicurezza informatica in ambienti industriali con un alto livello di automazione. Le aziende che danno priorità alla formazione continua, alla collaborazione tra i reparti IT e OT e all'implementazione delle migliori pratiche sono meglio attrezzate per proteggere le loro infrastrutture critiche e mantenere la continuità operativa.

La sensibilizzazione e la formazione in materia di competenze tecniche e personali sono fondamentali

È fortemente richiesta una combinazione di competenze personali, abilità tecniche e un approccio olistico all'azienda, inclusa la capacità di collaborazione tra i reparti IT e OT per garantire un approccio efficace alla sicurezza.
La realtà, tuttavia, nelle scuole professionali al momento è che i programmi di studio IT e OT non rispondono a queste esigenze. C'è una generale mancanza di attenzione alla sicurezza informatica nei programmi di formazione professionale IT quando si fa riferimento agli ambienti industriali, e questa mancanza di attenzione alla sicurezza informatica è assoluta nei programmi OT. Potremmo affermare che il problema principale per i professionisti IT è la mancanza di conoscenze e competenze relative a una rete OT, mentre la carenza nei professionisti OT inizia dalla mancanza di consapevolezza. Questa realtà è comune a tutti i paesi partner, pertanto le lacune rilevate in entrambi i tipi di professionisti per quanto riguarda le competenze in materia di sicurezza informatica sono quasi le stesse.
Partendo da questa realtà, non c'è altra opzione che iniziare a costruire consapevolezza e conoscenza integrando la sicurezza informatica nei programmi di studio IT e OT come competenza trasversale, a partire dagli insegnanti e dai formatori per arrivare poi agli studenti.

Ringraziamenti

Desideriamo ringraziare le aziende coinvolte nel progetto Cyber-In, in particolare quelle che hanno partecipato ai focus group nazionali, per la loro disponibilità, entusiasmo e impegno nel migliorare la formazione professionale continua. Il loro contributo è stato essenziale non solo per sviluppare questo rapporto e per implementare le fasi future del progetto, ma anche per aggiornare le conoscenze, le abilità e le competenze di tutto il personale del progetto, degli insegnanti e degli studenti coinvolti.

Un riconoscimento speciale va alle 5 entità che hanno esaminato, valutato e convalidato il curriculum modulare proposto da Cyber-In. Un grande GRAZIE va a Secure Network SRL (IT), Cybasque (ES), Rapla County Vocational College (Estonia), NTO Automation (DK) e OIXIO (Estonia).

Contattaci

Telefono

+ 31 088-6572657

E-mail

rbezemer@davinci.nl

Sito

www.cyber-in.eu

Indirizzo

Leerparkpromenade 100
3312 KW Dordrecht