Elementi essenziali e gestione della sicurezza informatica per il settore energetico

CSP001_C_E

PRESENTAZIONE DI:
Paresh Rathod, Pasi Kämppi, Cristina Alcaraz,
Stylianos Karagiannis, Ricardo Lugo,
Kitty Kioskli, Paulinus Ofem e Louise Praestiin

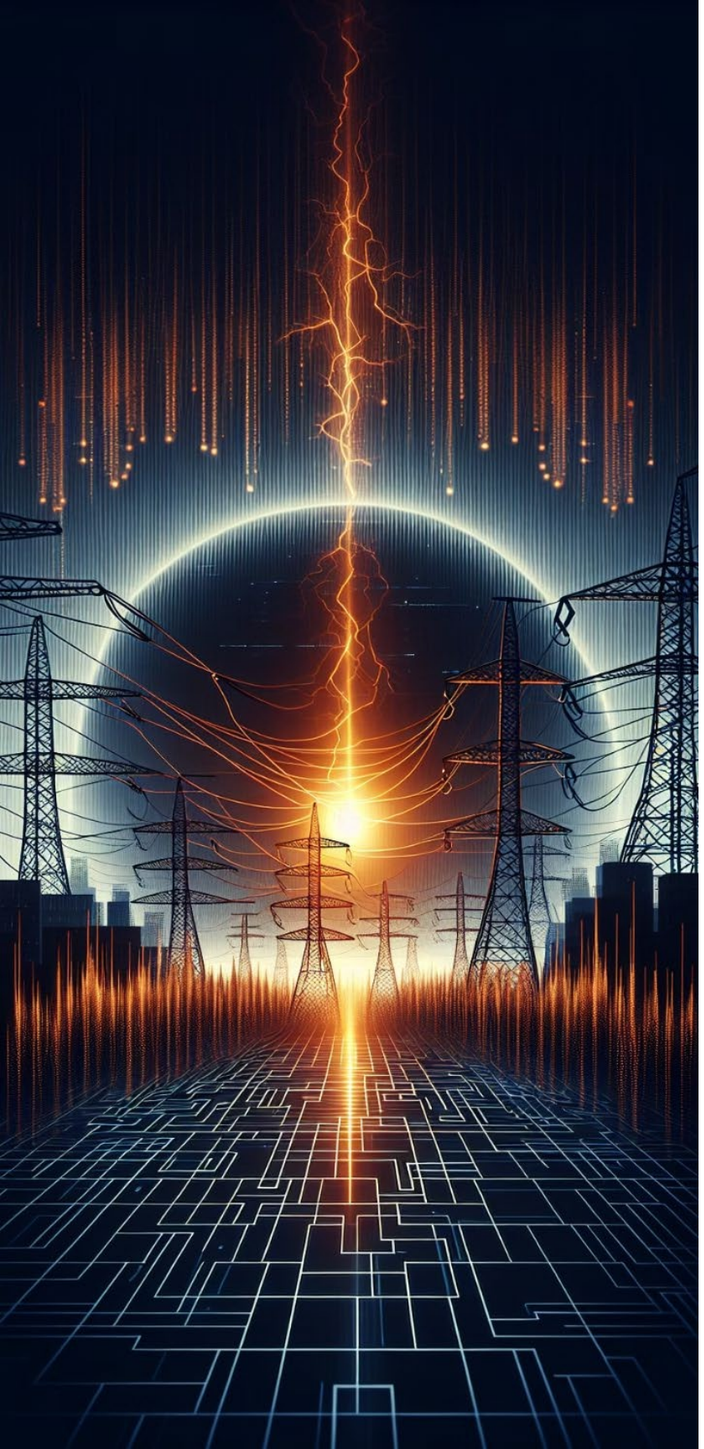
CyberSecPro

Ringraziamenti

- Finanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità concedente possono essere ritenute responsabili per essi.
- Accordo di progetto n. 101083594

Funded by the European Union

CyberSecPro

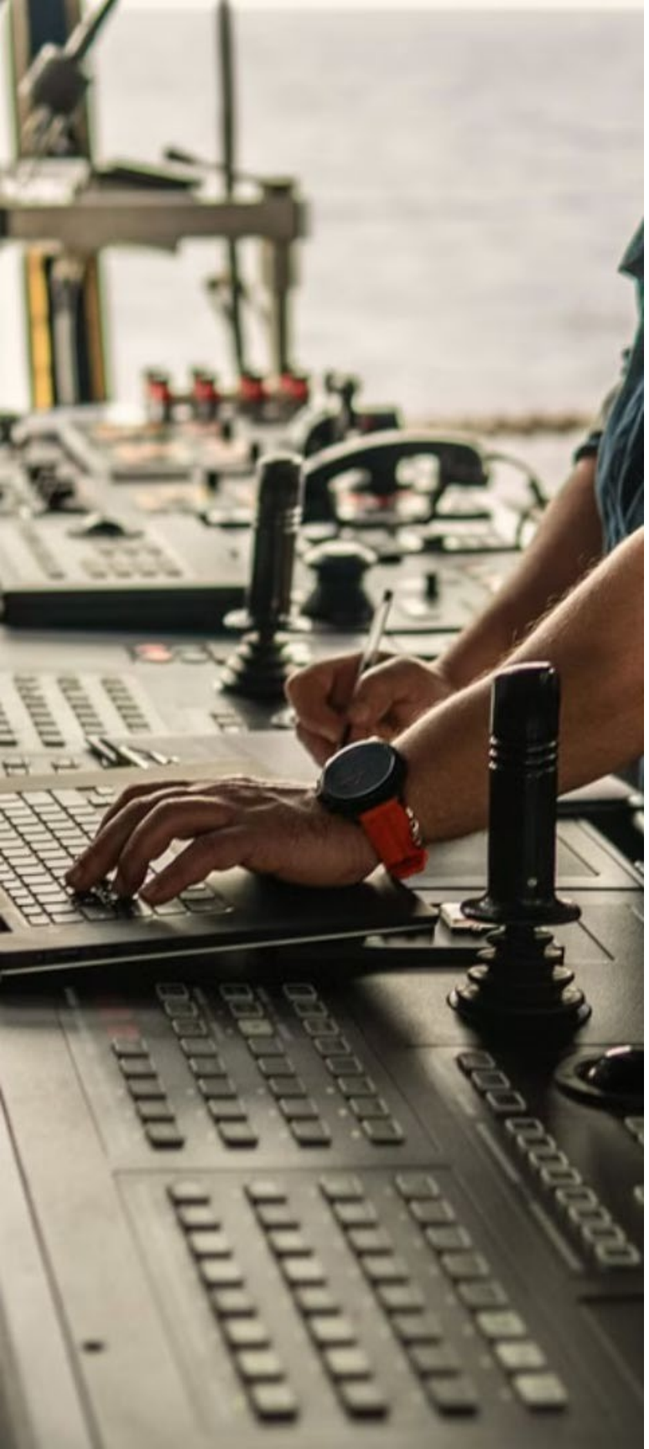


CyberSecPro Modulo di formazione professionale 1:

Elementi essenziali e gestione della sicurezza informatica per il settore energetico

Benvenuti al modulo di formazione completo di CyberSecPro che fornisce ai professionisti del settore energetico le conoscenze e le competenze essenziali per difendersi dalle minacce informatiche in continua evoluzione. Progettato specificamente per il settore energetico, questo programma affronta le sfide uniche che devono affrontare i fornitori di energia, fornendovi gli strumenti necessari per salvaguardare le infrastrutture e le operazioni critiche. Preparatevi a intraprendere un viaggio nel complesso mondo della sicurezza informatica, imparando dai formatori, dagli esperti del settore e acquisendo una profonda comprensione del panorama informatico che prende di mira le infrastrutture energetiche. Preparatevi a intraprendere un viaggio nel complesso mondo della sicurezza informatica, imparando da formatori ed esperti del settore e acquisendo una profonda comprensione del panorama informatico che prende di mira le infrastrutture energetiche.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin



Comprendere l'importanza della sicurezza informatica nel settore energetico

1

Conoscenze essenziali

I partecipanti acquisiranno le conoscenze essenziali per identificare, prevenire e rispondere alle minacce informatiche, garantendo la sicurezza e la protezione delle infrastrutture energetiche.

2

Apprendimento accessibile

Il programma è stato concepito per essere accessibile a chiunque abbia una conoscenza di base dei computer e delle reti.

3

Panoramica completa

Al termine di questo modulo, gli studenti avranno una panoramica completa del ruolo della sicurezza informatica nel settore energetico.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Incontra i tuoi formatori

Paresh Rathod

Specializzato in formazione sulla sicurezza informatica e responsabile tematico RDI presso Laurea, Finlandia.
Apporta un bagaglio di conoscenze nel campo della tecnologia e della formazione.

Pasi Kämppi

Specializzato in formazione sulla sicurezza informatica e coordinatore dei corsi di laurea presso Laurea, Finlandia.
Porta un bagaglio di conoscenze nel campo delle infrastrutture di rete e della formazione

Cristina Alcaraz

Specializzata in sicurezza informatica, attualmente ricercatrice post-dottorato Marie Curie e professore associato, lavora nel gruppo di ricerca del Laboratorio di sicurezza informatica, delle reti e delle informazioni (NICS) dell'Università di Malaga (UMA).

Stylianos Karagiannis

Esperto tecnico in PDM, Portogallo, che contribuisce con approfondimenti pratici.
Possiede una solida formazione accademica e competenze pratiche in cyber range e scenari di sicurezza attacco-difesa.

Incontra i tuoi formatori

Ricardo Gregorio Lugo

Specializzato in aspetti umani della formazione sulla sicurezza informatica, ricercatore post-dottorato e senior presso TalTech, Accademia marittima estone.

Kitty Kioskli

Specializzata in aspetti umani della formazione sulla sicurezza informatica, è amministratore delegato e cofondatrice di trustilio BV, Paesi Bassi. Ha conseguito un dottorato in psicologia della salute presso il King's College di Londra.

Paulinus Ofem

Specializzato in sicurezza informatica e attualmente anche project manager nel progetto MONELO dell'UE sull'intelligenza artificiale presso Laurea, Finlandia.

Louise Præstiin

Game designer presso SGI, Danimarca, contribuisce con approfondimenti pratici sull'uso dei giochi in scenari di sicurezza informatica.

Formatori CyberSecPro

Chi dovrebbe partecipare?

1 Studenti dell'istruzione superiore

Studenti dell'istruzione superiore (livello EQF 6, 7 o superiore) e futuri talenti che aspirano a una carriera nel settore tecnologico e/o in settori critici come la sicurezza informatica

2 Personale ICT

I dipendenti delle aziende energetiche e delle autorità competenti comprenderanno come gestire i rischi informatici.

3 Professionisti della sicurezza energetica

I responsabili della sicurezza dei porti e dei terminal approfondiranno le loro conoscenze sulle minacce informatiche.

4 Neofiti della sicurezza informatica nel settore energetico

Gli aspiranti professionisti acquisiranno una comprensione di base della sicurezza informatica nel settore energetico.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Proposte di valore

Vantaggi per i partecipanti

- Livello del modulo formativo: Base / Avanzato
- Formazione professionale sulla sicurezza informatica
- Sviluppo di competenze pratiche e operative
- Basato sul quadro europeo delle competenze in materia di sicurezza informatica
- Approfondimenti all'avanguardia da parte di esperti del settore industriale e accademico
- Certificato di completamento
- Aiuta lo sviluppo delle competenze e l'avanzamento di carriera

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofemile Louise Praestiin

Panoramica del programma di formazione

1. **Argomento 1**
   Condotta etica e professionalità nel campo della sicurezza informatica
2. **Argomento 2**
   Conoscenze di base sulla sicurezza informatica e corpus di conoscenze
3. **Argomento 3**
   Minacce e vulnerabilità (anche specifiche del settore energetico)
4. **Argomento 4**
   Considerazioni sul fattore umano nella sicurezza informatica
5. **Argomento 5**
   Progettazione e implementazione di architetture sicure

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Panoramica del programma di formazione

6 **Argomento 6**
Selezione e implementazione dei controlli di sicurezza

7 **Argomento 7**
Sicurezza dei dati e privacy by design (SDPbd) per il settore energetico

8 **Argomento 8**
Governance della sicurezza informatica per le organizzazioni energetiche

9 **Argomento 9**
Conformità e normative in materia di sicurezza informatica nel settore energetico

10 **Argomento 10**
Competenze trasferibili e apprendimento continuo nella professione della sicurezza informatica

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

CyberSecPro

Risultati attesi

Concetti fondamentali

Descrivere i concetti fondamentali della sicurezza informatica e la loro importanza nel settore energetico.

Minacce comuni

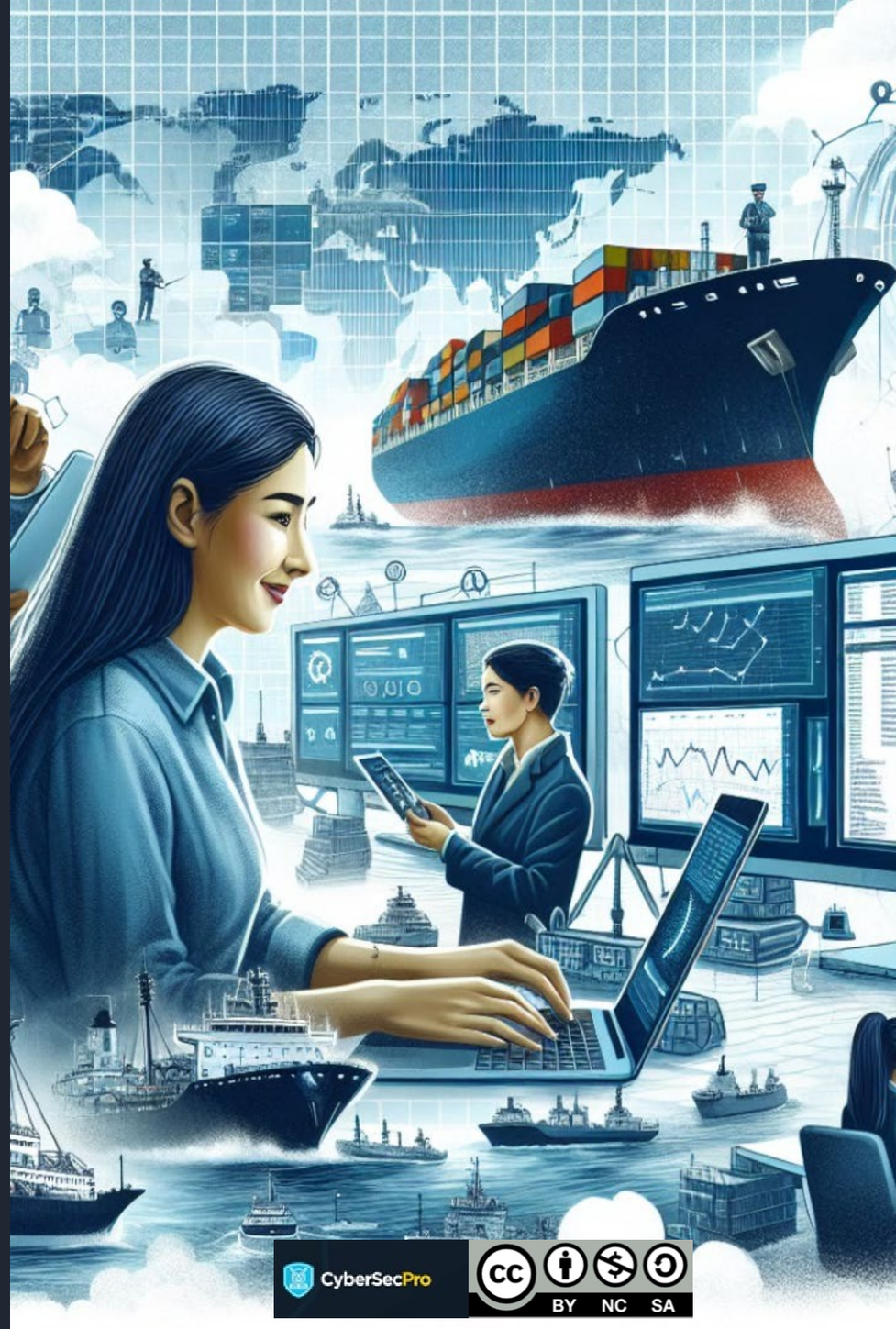
Identificare le minacce informatiche comuni, le vulnerabilità e i rischi specifici del settore energetico

Impatto degli attacchi informatici

Spiegare l'impatto degli attacchi informatici sulla sicurezza energetica.

Migliori pratiche

Applicare le migliori pratiche di sicurezza informatica per proteggere i sistemi e le reti energetiche.



Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Condotta etica e professionalità

Etica e integrità

Sviluppare una solida base etica, promuovendo la fiducia, la responsabilità e un comportamento responsabile nel campo della sicurezza informatica.

Condotta professionale

Mantenere i più elevati standard di condotta professionale, dimostrando rispetto, obiettività e dedizione alla salvaguardia dei sistemi energetici critici.

Riservatezza e privacy

Dare priorità alla protezione delle informazioni sensibili, garantendo la riservatezza e preservando la privacy delle persone e delle organizzazioni.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Fondamenti di sicurezza informatica

1

Definizione di sicurezza informatica

Esplora l'essenza della sicurezza informatica, la sua importanza nel settore energetico e il ruolo cruciale che svolge nella protezione delle infrastrutture e delle operazioni critiche.

2

Panorama delle minacce

Ottieni informazioni dettagliate sul panorama delle minacce in continua evoluzione, comprese le minacce specifiche del settore, le vulnerabilità che prendono di mira i sistemi SCADA, le reti intelligenti e altre risorse energetiche critiche.

3

Gestione dei rischi

Padroneggia i principi della gestione dei rischi legati alla sicurezza informatica, che ti consentiranno di identificare, valutare e mitigare efficacemente i rischi nel settore energetico.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Architettura e controlli sicuri

Sicurezza della rete

Approfondisci i principi della segmentazione di rete, della configurazione dei firewall e del controllo degli accessi, imparando a progettare e implementare architetture di rete sicure per i sistemi energetici.

Sicurezza dei dati e degli accessi

Scopri l'importanza della sicurezza delle password, dell'autenticazione a più fattori (MFA), della crittografia dei dati e della gestione delle patch, garantendo la protezione delle informazioni e dei sistemi sensibili.

Controlli di sicurezza

Imparate a implementare e gestire i controlli di sicurezza essenziali per i sistemi energetici, inclusi i sistemi di rilevamento e prevenzione delle intrusioni, i software antivirus e altre misure di protezione.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Risposta agli incidenti e continuità operativa

1

Preparazione

Sviluppare piani e procedure completi di risposta agli incidenti su misura per il settore energetico, garantendo la prontezza ad affrontare potenziali incidenti informatici.

2

Rilevamento e analisi

Migliorare la capacità di rilevare e analizzare le minacce informatiche, sfruttando strumenti e tecniche di monitoraggio avanzati per identificare tempestivamente potenziali incidenti.

3

Contenimento ed eliminazione

Implementare strategie efficaci di contenimento ed eradicazione per ridurre al minimo l'impatto degli incidenti informatici e ripristinare in modo efficiente il normale funzionamento.

4

Recupero e resilienza

Stabilire misure solide di ripristino e resilienza, garantendo la continuità operativa e riducendo al minimo i tempi di inattività in caso di attacco informatico riuscito.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Conformità e normative

1 Standard di settore

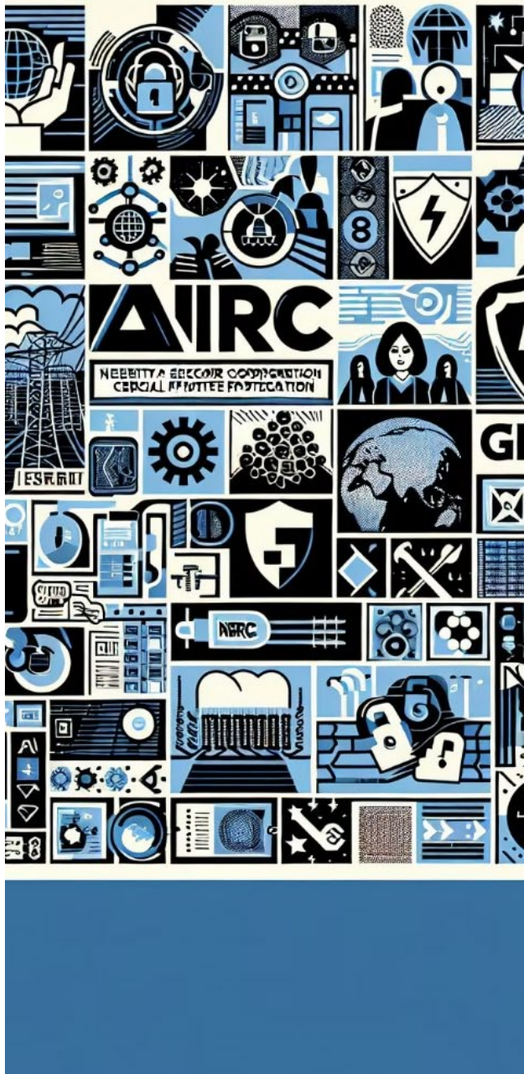
Acquisisci informazioni approfondite sugli standard specifici del settore e sulle best practice, come gli standard NERC Critical Infrastructure Protection (CIP), garantendo la conformità e il rispetto dei requisiti normativi.

2 Privacy e protezione dei dati

Comprendere l'importanza delle normative sulla privacy e sulla protezione dei dati, compreso il Regolamento generale sulla protezione dei dati (GDPR) e le leggi specifiche del settore, garantendo la gestione sicura delle informazioni sensibili.

3 Audit e rendicontazione

Imparate processi efficaci di audit e reporting che vi consentiranno di dimostrare la conformità, identificare le aree di miglioramento e comunicare efficacemente le misure di sicurezza informatica agli stakeholder.



Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Il fattore umano nella sicurezza informatica

Sensibilizzazione e formazione

Riconoscere il ruolo fondamentale della consapevolezza e della formazione delle persone nella sicurezza informatica, fornendo ai dipendenti le conoscenze e le competenze necessarie per identificare e mitigare i rischi, promuovendo una cultura della sicurezza all'interno dell'organizzazione.

Ingegneria sociale

Esplora le tecniche utilizzate negli attacchi di ingegneria sociale, come il phishing, il pretexting e il baiting, e sviluppa contromisure per proteggerti da queste minacce.

Minacce interne

Comprendere i rischi rappresentati dalle minacce interne, intenzionali o non intenzionali, e implementare strategie per rilevare, prevenire e rispondere efficacemente a tali incidenti.

Gestione degli accessi

Apprendere le best practice per la gestione degli accessi, compresi i principi del privilegio minimo, della separazione dei compiti e della gestione del ciclo di vita degli utenti, al fine di mitigare i rischi associati ai fattori umani.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Governance della sicurezza informatica

Aspetto	Descrizione
Politiche e procedure	Sviluppare e implementare politiche e procedure complete di sicurezza informatica adattate al settore energetico, fornendo un quadro di riferimento per una gestione efficace della sicurezza.
Gestione dei rischi	Stabilire un solido processo di gestione dei rischi, identificando, valutando e mitigando i rischi di sicurezza informatica per le infrastrutture e le operazioni energetiche critiche.
Ruoli e responsabilità	Definire ruoli e responsabilità chiari per la sicurezza informatica all'interno dell'organizzazione, garantendo la responsabilità e un coordinamento efficace delle attività di sicurezza.
Miglioramento continuo	Promuovere una cultura del miglioramento continuo, rivedendo e aggiornando regolarmente le misure di sicurezza informatica per stare al passo con le minacce in continua evoluzione e le migliori pratiche del settore del settore.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Sicurezza dei dati e privacy by design

Classificazione dei dati

Implementare un sistema completo di classificazione dei dati, garantendo la corretta gestione e protezione delle informazioni sensibili in base alla loro criticità e sensibilità.

Crittografia e gestione delle chiavi

Esplorare le tecniche di crittografia e le pratiche di gestione delle chiavi, salvaguardando i dati inattivi, in transito e in uso, garantendo al contempo l'accesso e l'archiviazione sicuri delle chiavi di crittografia.

Privacy fin dalla progettazione

Incorporare i principi di privacy e le misure di protezione dei dati nella progettazione e nell'implementazione dei sistemi energetici, garantendo la conformità alle normative e salvaguardando la privacy individuale.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioski, Paulinus Ofem e Louise Praestiin

Formazione continua e sviluppo professionale sviluppo

1

2

3

4

Informazioni sulle minacce

Rimanete informati sulle ultime minacce alla sicurezza informatica, sulle vulnerabilità e sui vettori di attacco specifici del settore energetico sfruttando le fonti di intelligence sulle minacce e i rapporti di settore.

Collaborazione nel settore

Impegnarsi nella collaborazione industriale e nella condivisione delle conoscenze, partecipando a conferenze, workshop e comunità professionali per scambiare le migliori pratiche e le lezioni apprese.

Certificazioni e formazione

Perseguire certificazioni pertinenti e opportunità di formazione continua per migliorare le proprie competenze, rimanere aggiornati sulle tecnologie e le tendenze emergenti e mantenere un vantaggio competitivo nel campo della sicurezza informatica.

Ricerca e innovazione

Contribuisci agli sforzi di ricerca e innovazione, esplorando nuove tecnologie, metodologie e soluzioni per affrontare le sfide in continua evoluzione della sicurezza informatica che il settore energetico deve affrontare.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Casi di studio reali

1

Attacco Stuxnet

Analizza il famigerato attacco Stuxnet, un sofisticato malware che prende di mira i sistemi di controllo industriale, e le sue implicazioni per il settore energetico, traendo preziosi insegnamenti per la risposta agli incidenti e la preparazione.

2

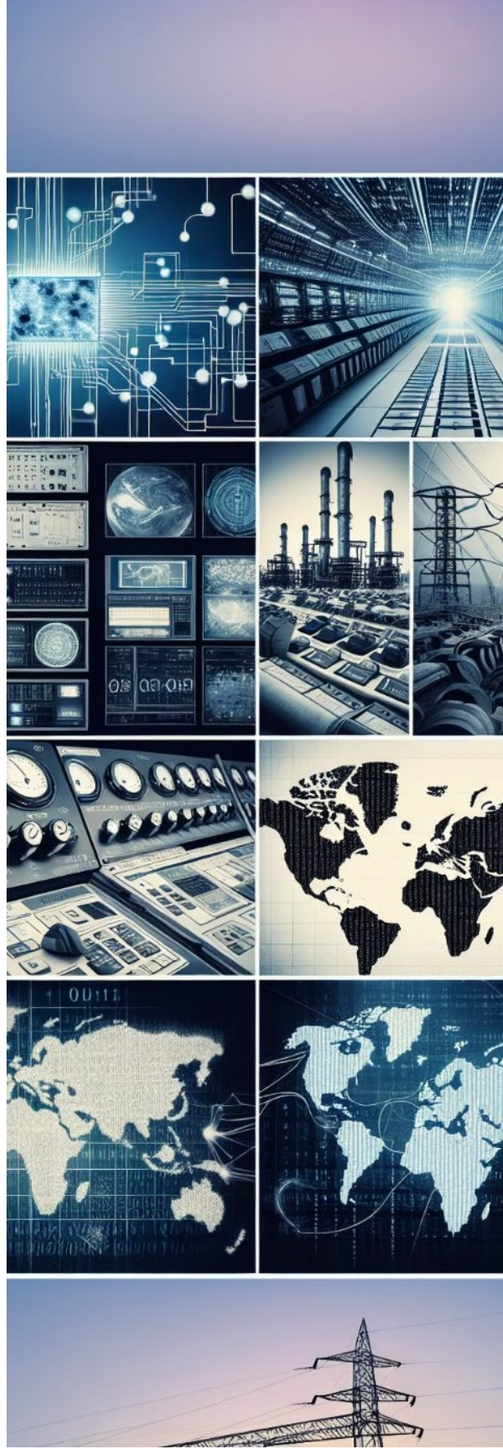
Attacco ransomware alla Colonial Pipeline

Esplora il clamoroso attacco ransomware alla Colonial Pipeline Company, che ha interrotto la fornitura di carburante in tutti gli Stati Uniti, ed esamina le misure adottate per mitigare l'impatto e migliorare le misure di sicurezza informatica.

3

Attacco informatico alla rete elettrica ucraina

Indaga sugli attacchi informatici che hanno preso di mira la rete elettrica ucraina, causando interruzioni di corrente su vasta scala, e studia le tecniche impiegate dagli aggressori e le successive misure difensive messe in atto.



Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Attività pratiche e simulazioni

Esercitazioni pratiche

Partecipa ad attività pratiche e scenari incentrati sulla sicurezza della rete, dove imparerai le basi su come implementare architetture di rete sicure, configurare firewall e mettere in pratica misure di controllo degli accessi.

Apprendimento basato sul gioco

Partecipa a un apprendimento realistico basato sul gioco, in cui applicherai le tue conoscenze e competenze nel rilevare, analizzare e rispondere a simulazioni di attacchi informatici alle infrastrutture energetiche.

Scenari

Apprendimento basato su vari scenari durante l'intero modulo di formazione CSP da parte di istruttori e materiali forniti. Ciò offre approfondimenti su situazioni di lavoro reali.

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

Corrispondenza con il profilo CISO dell'ECSF

Modulo CSP-1 Argomento	Compiti CISO ECSF	Competenze CISO ECSF	Conoscenze CISO ECSF
Argomento-1: Condotta etica e professionalità	Definire, implementare, comunicare e mantenere obiettivi, requisiti, strategie e politiche di sicurezza informatica in linea con la strategia aziendale per supportare gli obiettivi organizzativi	Valutare e migliorare la posizione di un'organizzazione in materia di sicurezza informatica	Politiche di sicurezza informatica
Argomento 2: Conoscenze di base sulla sicurezza informatica	Sviluppare, promuovere e guidare l'attuazione di una strategia di sicurezza informatica	Analizzare e implementare politiche, certificazioni, standard, metodologie e framework di sicurezza informatica	Standard, metodologie e framework di sicurezza informatica
Argomento 2: Corpus di conoscenze sulla sicurezza informatica	Monitorare i progressi nella sicurezza informatica	Analizzare e rispettare le leggi, i regolamenti e le normative in materia di sicurezza informatica	Leggi, regolamenti e normative relativi alla sicurezza informatica
Argomento 3: Minacce e vulnerabilità	Identificare e risolvere i problemi relativi alla sicurezza informatica	Analizzare e implementare raccomandazioni e best practice in materia di sicurezza informatica	Raccomandazioni e best practice in materia di sicurezza informatica
Argomento 4: Considerazioni sul fattore umano	Sviluppare relazioni con le autorità e le comunità competenti in materia di sicurezza informatica	Identificare e migliorare la posizione di un'organizzazione in materia di sicurezza informatica	Requisiti etici per l'organizzazione della sicurezza informatica
Argomento 5: Progettazione e implementazione di un'architettura sicura	Rivedere, pianificare e allocare risorse adeguate per la sicurezza informatica	Gestire le risorse di sicurezza informatica	Procedure di sicurezza informatica

Corrispondenza con il profilo CISO dell'ECSF

Modulo CSP-1 Argomento	Compiti del CISO dell'ECSF	Competenze CISO ECSF	Conoscenze del CISO ECSF
Argomento-6: Selezione e implementazione dei controlli di sicurezza	Rivedere e migliorare i documenti di sicurezza, i rapporti, gli SLA e garantire il raggiungimento degli obiettivi di sicurezza	Progettare, applicare, monitorare e rivedere il Sistema di gestione della sicurezza delle informazioni (ISMS) direttamente o guidandone l'esternalizzazione	Politiche di sicurezza informatica
Argomento 7: Sicurezza dei dati e privacy by design	Stabilire un piano di sicurezza informatica	Implementare le raccomandazioni e le migliori pratiche in materia di sicurezza informatica	Raccomandazioni e best practice in materia di sicurezza informatica
Argomento 8: Governance della sicurezza delle informazioni (ISG) e gestione dei rischi per la sicurezza delle informazioni (ISRM)	Negoziare il budget per la sicurezza informatica con l'alta dirigenza	Gestire le risorse per la sicurezza informatica	Standard, metodologie e quadri di riferimento per la gestione dei rischi
Argomento 9: Audit di sicurezza e conformità	Comunicare, coordinare e cooperare con gli stakeholder interni ed esterni	Anticipare i cambiamenti necessari alla strategia di sicurezza delle informazioni dell'organizzazione e formulare nuovi piani	Standard, procedure e linee guida per l'auditing della sicurezza informatica
Argomento 9: Conformità legale ed etica	Anticipare le minacce alla sicurezza informatica, le esigenze e le sfide future	Garantire che l'alta dirigenza approvi i rischi di sicurezza informatica dell'organizzazione	Requisiti etici dell'organizzazione della sicurezza informatica
Argomento 9: Standard e quadri di riferimento per la gestione della sicurezza	Motivare e incoraggiare le persone		

Riferimenti

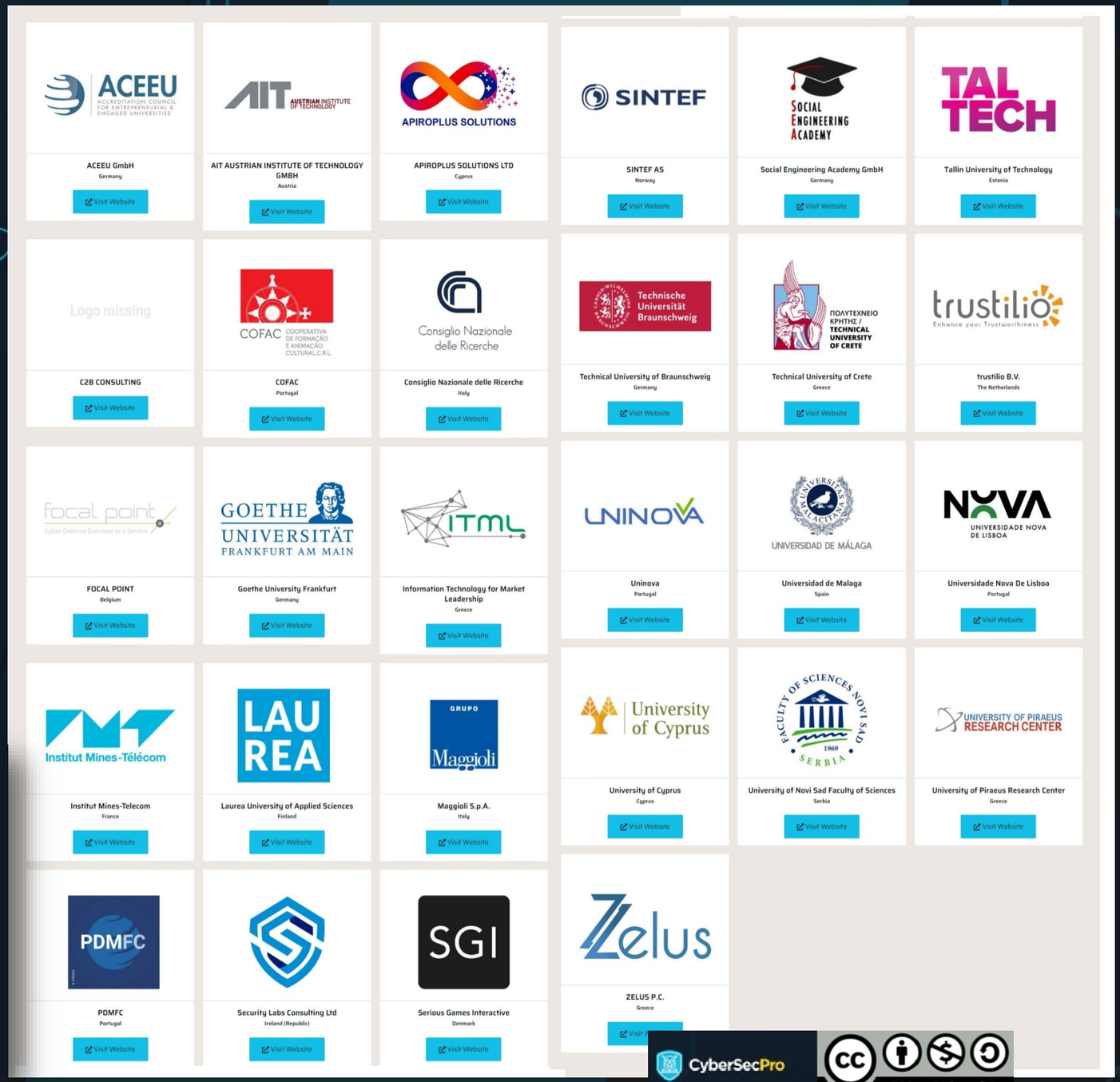
1. Agenzia dell'Unione europea per la sicurezza informatica. (2022). ECSF, Quadro europeo delle competenze in materia di sicurezza informatica. Ufficio delle pubblicazioni. https://doi.org/10.2824/859537
2. R. Schoon e S. Kleinaltepohl, Cybersecurity nel settore elettrico: gestione delle infrastrutture critiche (SpringerLink, 2018).
3. J. R. Vacca, Industrial Cybersecurity for Engineers (Elsevier, 2015).
4. ECSO, “Energy Networks and Smart Grids”, Cyber Security for the Energy Sector, WG3, Sectoral Demand, novembre 2018 URL: https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf
5. ENISA, "Panorama delle minacce alle reti intelligenti e guida alle buone pratiche", dicembre 2013 URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
6. Altri riferimenti elencati in ciascun argomento del modulo CSP

Trasparenza: Fonti

1. Contenuto del video teaser: Il contenuto di questo video teaser si basa sui risultati del Work Package 3 del progetto CyberSecPro, con preziosi contributi dei partner CyberSecPro.
2. Competenza linguistica: il deliverable D3.1 è stato sottoposto a un rigoroso controllo linguistico. Ciò ha comportato l'utilizzo dell'intelligenza artificiale di Grammarly e la revisione meticolosa da parte di madrelingua inglesi.
3. Contenuti multimediali: tutte le immagini, i video e gli audio utilizzati sono stati ricavati da Pictory, Getty Images e altri database multimediali open stock.
4. Collaborazione dei partner: Ringraziamo i nostri partner CyberSecPro per il loro contributo, comprese le foto dei formatori presenti nel programma.
5. Materiali didattici: i materiali didattici per questo modulo CyberSecPro sono stati forniti da un formatore accreditato e il merito va agli autori.
6. Crediti creativi: video teaser creato utilizzando queste risorse dal professionista europeo della sicurezza informatica Paresh Rathod.
7. I materiali della formazione sono stati creati utilizzando letteratura accademica e di ricerca e Open Education Material (OEM), con il dovuto riconoscimento agli autori.
8. Alcuni dei materiali hanno utilizzato strumenti basati sull'intelligenza artificiale, tra cui simulatori vocali (con il dovuto riconoscimento agli autori), per offrire ai partecipanti la migliore esperienza di apprendimento possibile.

Entra in contatto con CyberSecPro: Come registrarsi e altre informazioni pratiche

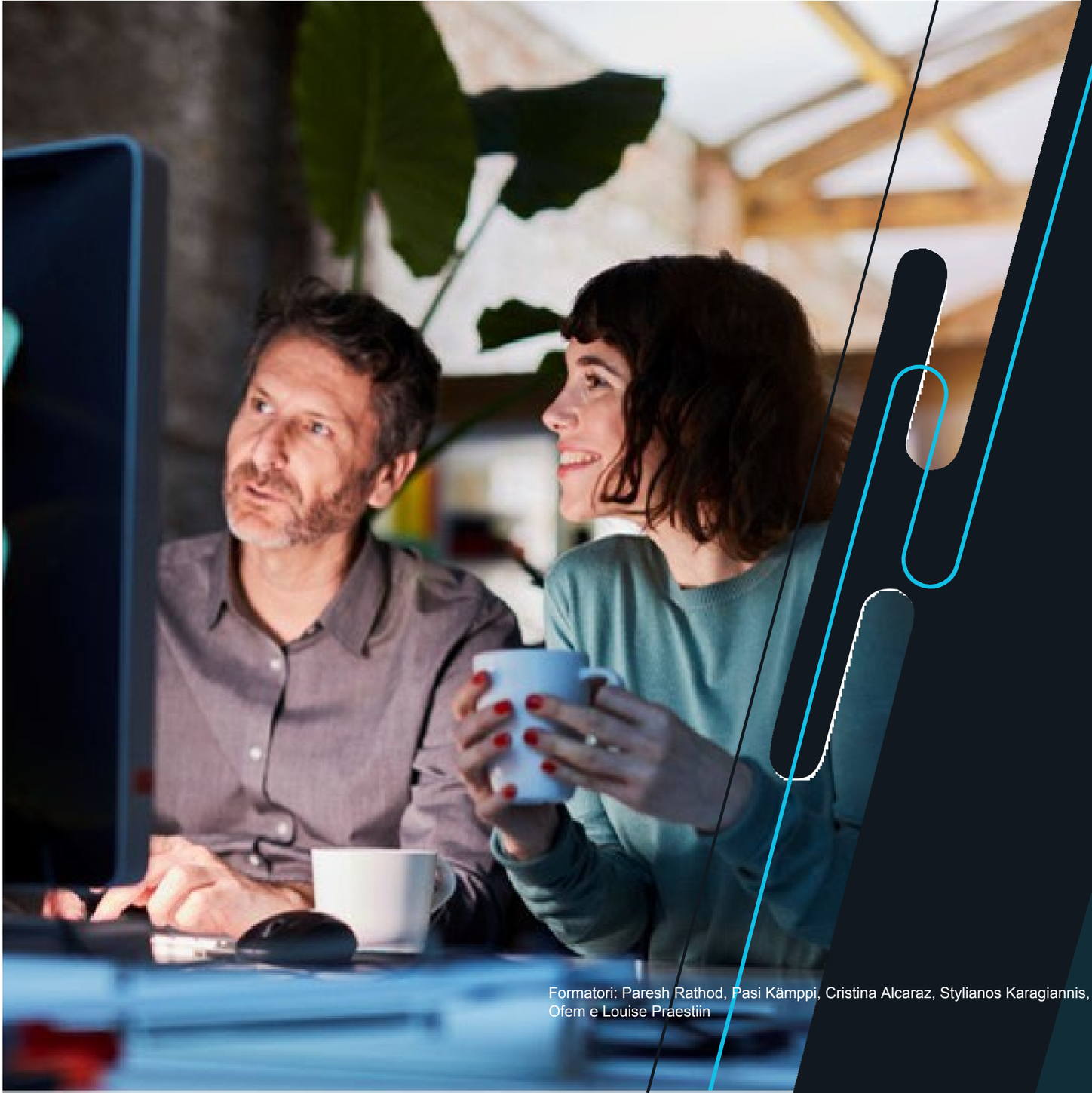
1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/



Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594



Grazie

Si prega di inviare tutte le domande ai formatori (e/o):
paresh.rathod@laurea.fi

Formatori: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem e Louise Praestiin

CyberSecPro