Fattori umani e sicurezza informatica nel settore energetico

CSP001_C_E

PRESENTAZIONE DI:
DR. RICARDO G. LUGO, TALTECH DR. KITTY KIOSKLI, TRUSTILIO PROF. PARESH RATHOD, LAUREA

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

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

Ordine del giorno

Risultati di apprendimento
Aspetti psicologici della sicurezza informatica nel settore energetico Aspetti psicosociali

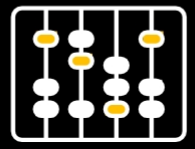
Tendenze future

Obiettivi: Chi-Cosa-Perché è necessario seguire questa formazione

CHI

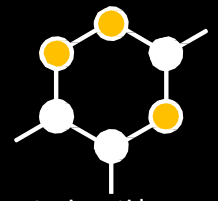
Aperto a tutti

COSA



Comprensione di base dei fattori umani per la sicurezza informatica nel settore energetico

PER



Fornire ai partecipanti le conoscenze e le competenze necessarie per comprendere come gli aspetti umani influenzano la sicurezza informatica nel settore energetico

Vantaggi per i partecipanti

- Livello del modulo formativo: Base
- Formazione professionale in materia di sicurezza informatica
- Basata sul quadro europeo delle competenze in materia di sicurezza informatica
- Approfondimenti all'avanguardia da parte di esperti del settore industriale e accademico
- Aiuta lo sviluppo delle competenze e l'avanzamento di carriera

Argomenti della formazione

- Introduzione agli aspetti umani dell'energia del settore energetico
- Fattori psicologici e sociali nella sicurezza informatica nel settore energetico
- Vulnerabilità umane nella sicurezza informatica nel settore energetico
- Cultura organizzativa, comunicazione e sicurezza informatica
- Comunicazione e collaborazione tra domini
- Processo decisionale a livello strategico, operativo e tattico
- Formazione, sensibilizzazione e comunicazione ms per il personale del settore energetico
- Tendenze future, sfide e ruolo di

Risultati di apprendimento

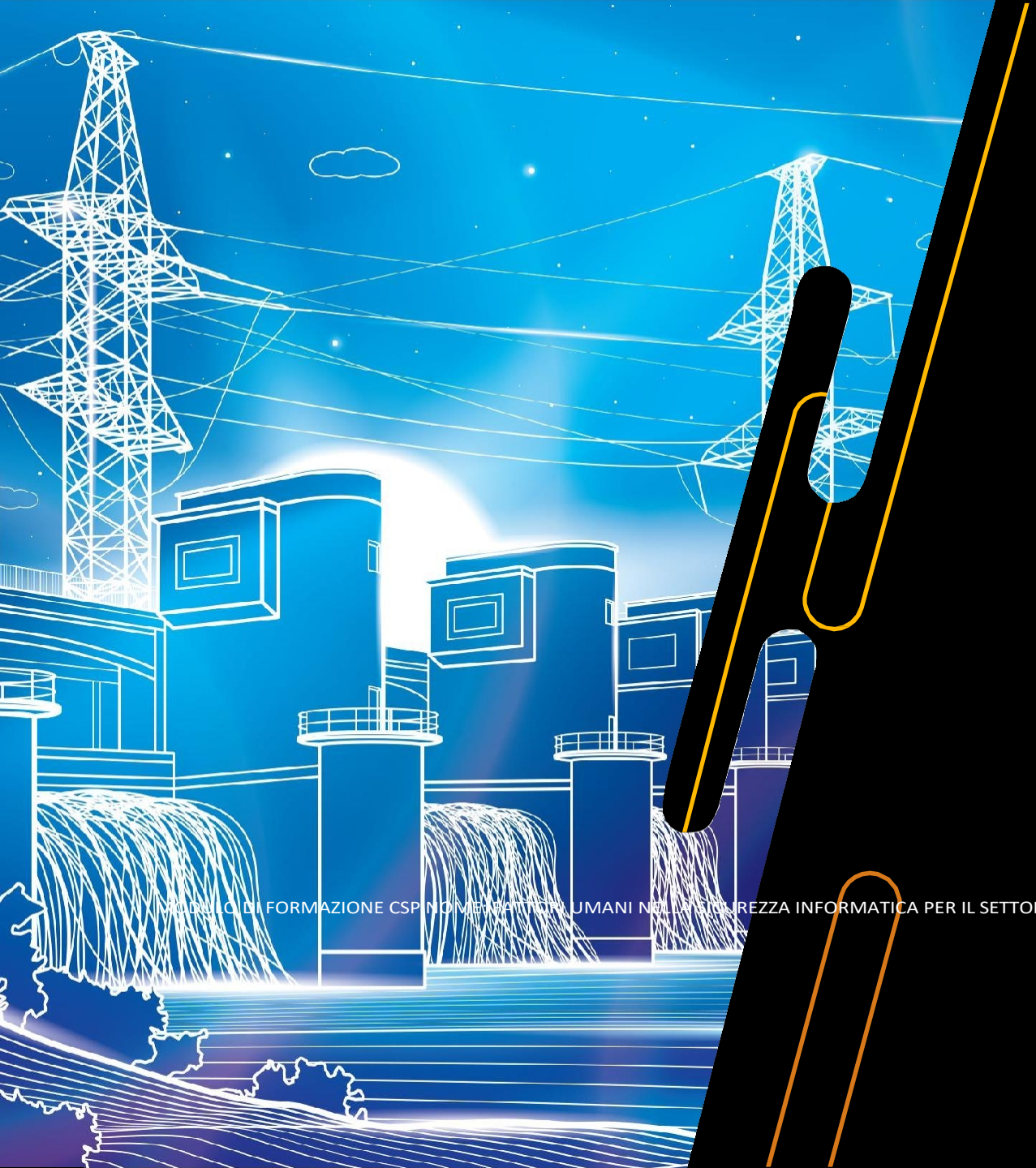
Conoscenze

- Acquisire una comprensione degli elementi psicologici, sociali e organizzativi che determinano le azioni di sicurezza informatica nel settore energetico.
- Comprendere il ruolo fondamentale della comunicazione e del lavoro di squadra nel rafforzamento della sicurezza informatica nel settore energetico in diversi ambiti.
- Riconoscere i profili e le strategie degli avversari che prendono di mira le operazioni del settore energetico.

Risultati di apprendimento

Competenze

- Comprendere le discussioni relative alla sicurezza informatica nel settore energetico a vari livelli decisionali.
- Essere in grado di promuovere un ambiente di comunicazione trasparente e di lavoro di squadra incentrato sulla sicurezza informatica nel settore energetico.
- Riflettere sul processo decisionale in materia di sicurezza informatica con la consapevolezza del ruolo svolto dai fattori umani nel settore energetico.
- Essere in grado di identificare le minacce e le vulnerabilità legate all'uomo nelle operazioni energetiche.



Importanza dei fattori umani:

Panoramica sulla sicurezza informatica nel settore energetico

- Importanza della sicurezza informatica nelle operazioni del settore energetico.
- Sfide uniche della sicurezza informatica nel settore energetico.
- Ruolo dei fattori umani nella sicurezza informatica nel settore energetico.
- Minacce identificate:
- Conversione IT/OT
- Bassa priorità e affidabilità
- 2023: oltre 250 violazioni da parte di terzi
- Esempi che verranno utilizzati:
  - Attacco alla rete elettrica ucraina nel 2015
  - Colonial Pipeline
  - Stuxnet

- Alzi la mano chi ha:
  - Cliccato su un link (da chiunque)
  - Una passphrase complessa (?)
  - Utilizzate la stessa password su siti/app diversi
  - Non avete cambiato la vostra password negli negli ultimi 30 giorni
  - Hai prestato il tuo telefono/pc a qualcun altro
  - Hai un login semplice per telefono/pc
  - Non hai aggiornato il PC/telefono negli ultimi 7 giorni

Importanza dei fattori umani:

Fattori umani nella sicurezza informatica

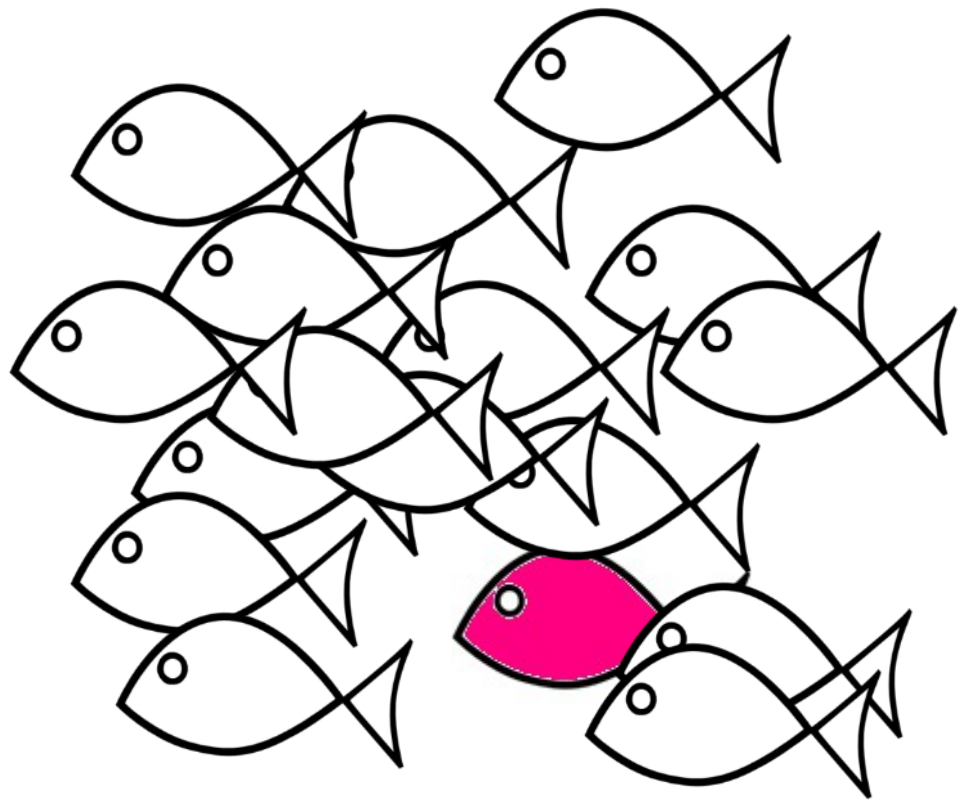
- Definizione e importanza dei fattori umani nella sicurezza informatica.
- Errori umani comuni che contribuiscono alle violazioni della sicurezza informatica

  .
- Strategie per mitigare i rischi legati all'errore umano.

Importanza dei fattori umani:

Implicazioni psicologiche

- Aspetti psicologici che influenzano i comportamenti relativi alla sicurezza informatica.
- L'effetto dei pregiudizi cognitivi sulle decisioni relative alla sicurezza.
- Attuazione dei principi psicologici per migliorare le misure di sicurezza informatica.



e cognitiva Dissonanza - Cognitiva

sulla privacy (PP)?

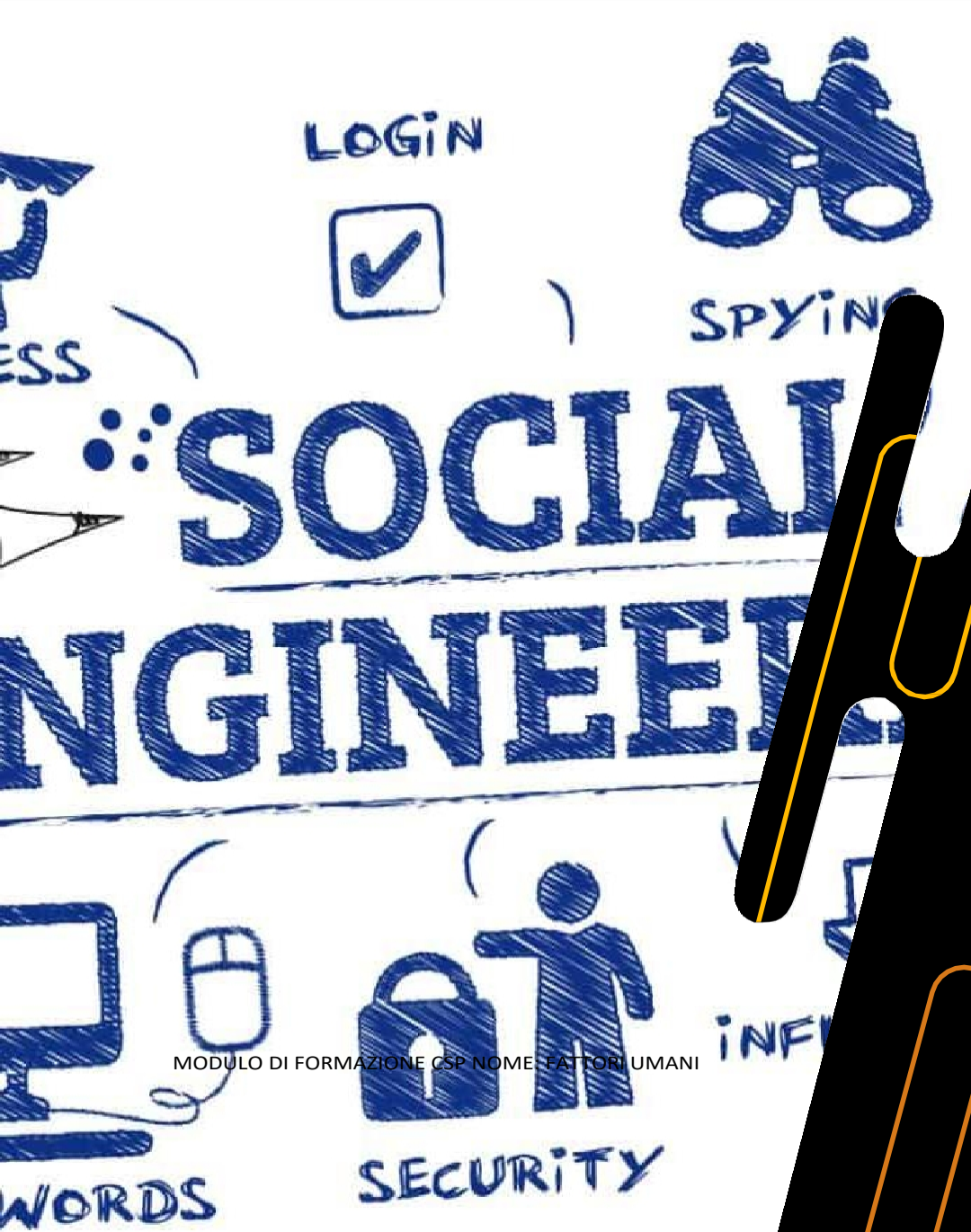
"3.1.1 NameDrop Data […] Any and all data generated and/or collected by NameDrop, by any means, may be shared with third parties. For example, NameDrop may be required to share data with government agencies, including the U.S. National Security Agency, and other security agencies in the United States and abroad. NameDrop may also choose to share data with third parties involved in the development of data products designed to assess eligibility. This could impact eligibility in the following areas: employment, financial service (bank loans, insurance, etc.), university entrance, international travel, the criminal justice system, etc. Under no circumstances will NameDrop be liable for any eventual decision made as a result of NameDrop data sharing."

2.3.1 Payment types (child assignment clause): In addition to any monetary payment that the user may make to NameDrop, by agreeing to these Terms of Service, and in exchange for service, all users of this site agree to immediately assign their first-born child to NameDrop, Inc. If the user does not yet have children, this agreement will be enforceable until the year 2050. All individuals assigned to NameDrop automatically become the property of NameDrop, Inc. No exceptions.

Importanza dei fattori umani:

Influenza sociale

- Impatto delle dinamiche sociali sulle pratiche di sicurezza informatica.
- Ruolo della cultura organizzativa nella definizione dei comportamenti relativi alla sicurezza informatica.
- Importanza della consapevolezza dell'ingegneria sociale.



Importanza dei fattori umani:

Ingegneria sociale

- Importanza della consapevolezza dell'ingegneria sociale.
- Ingegneria sociale
- Reciprocità; Impegno e coerenza, Prova sociale; Autorità; Simpatia; Scarsità

Importanza dei fattori umani:

Ingegneria sociale

- Ransomware
- Scarsità e reciprocità

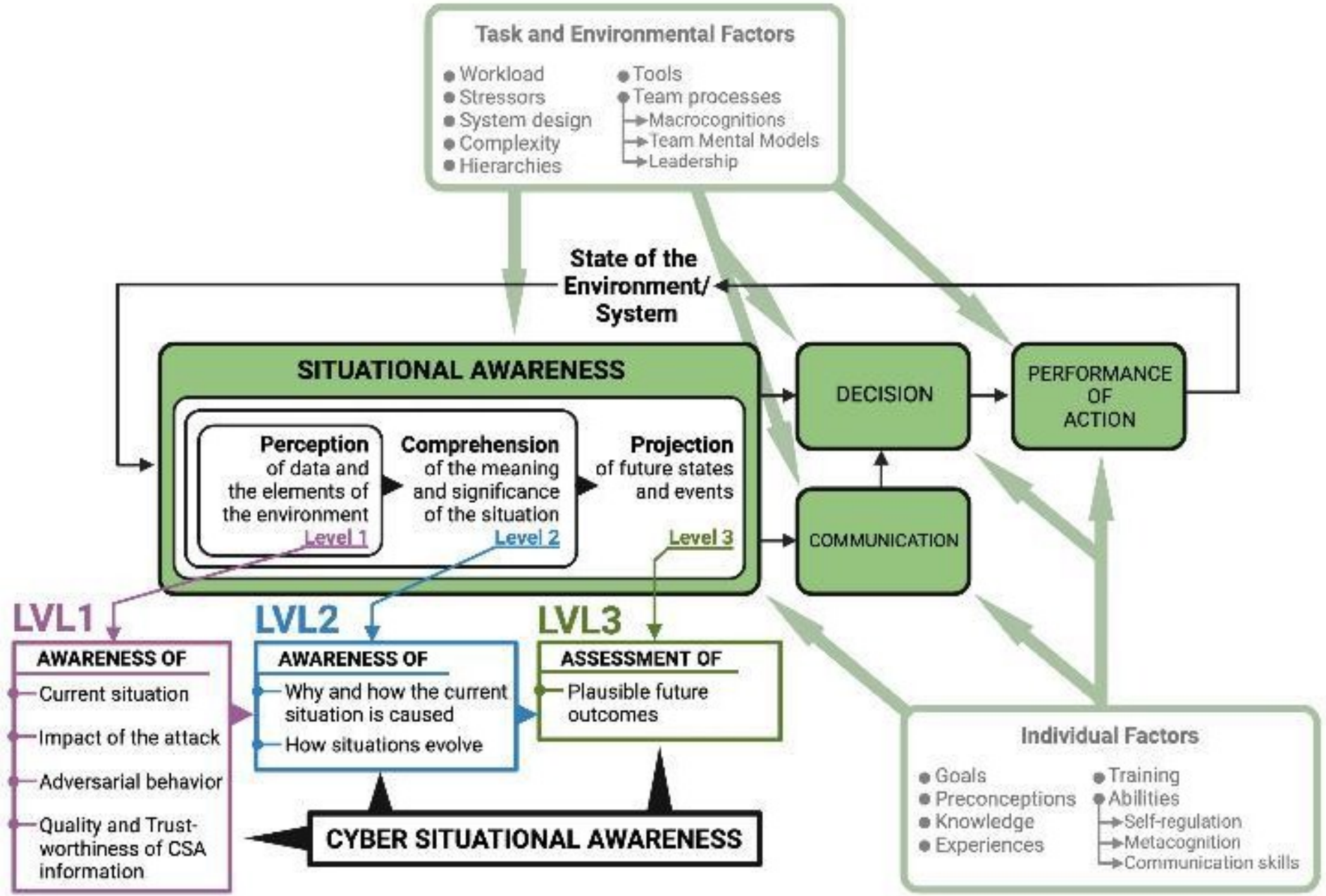
(molto) piccoli esempi

Fattori psicologici e sociali nella sicurezza informatica nel settore energetico

Comprendere la psicologia umana

- I pregiudizi cognitivi e il loro impatto sulla sicurezza informatica.
- Teorie psicologiche rilevanti per il comportamento in materia di sicurezza informatica.
- Progettare sistemi di sicurezza informatica tenendo conto della psicologia umana.
  - Consapevolezza situazionale (Endsley, 1998)
- Una riprogettazione dell'interfaccia che ha ridotto gli errori degli utenti sulla base di ricerche psicologiche.

Consapevolezza della situazione informatica (CSA) (Barford et al., 2009)



Fattori psicologici e sociali nella sicurezza informatica nel settore energetico

Dinamiche sociali e sicurezza informatica

- Influenza delle norme sociali e del comportamento dei pari sulle pratiche individuali di sicurezza informatica.
- Il ruolo della leadership nella promozione di una cultura attenta alla sicurezza.
  - Modelli di ruolo (Bandura, 1988)
- Fattori sociali nei programmi di formazione e sensibilizzazione sulla sicurezza informatica.

Fattori psicologici e sociali nella sicurezza informatica nel settore energetico

Migliorare la sicurezza attraverso la psicologia

- Strategie psicologiche per aumentare il rispetto dei protocolli di sicurezza.
- Tecniche di modifica comportamentale applicate alla sicurezza informatica.
- Il ruolo della motivazione e dei premi nel miglioramento dei comportamenti relativi alla sicurezza informatica .
- Esempio reale: un programma di ricompense che ha aumentato con successo la vigilanza sulla sicurezza informatica tra gli ingegneri.
- Futuro BCT e utilizzando l'intelligenza artificiale

Fattori psicologici e sociali nella sicurezza informatica nel settore energetico

Affrontare le minacce di ingegneria sociale

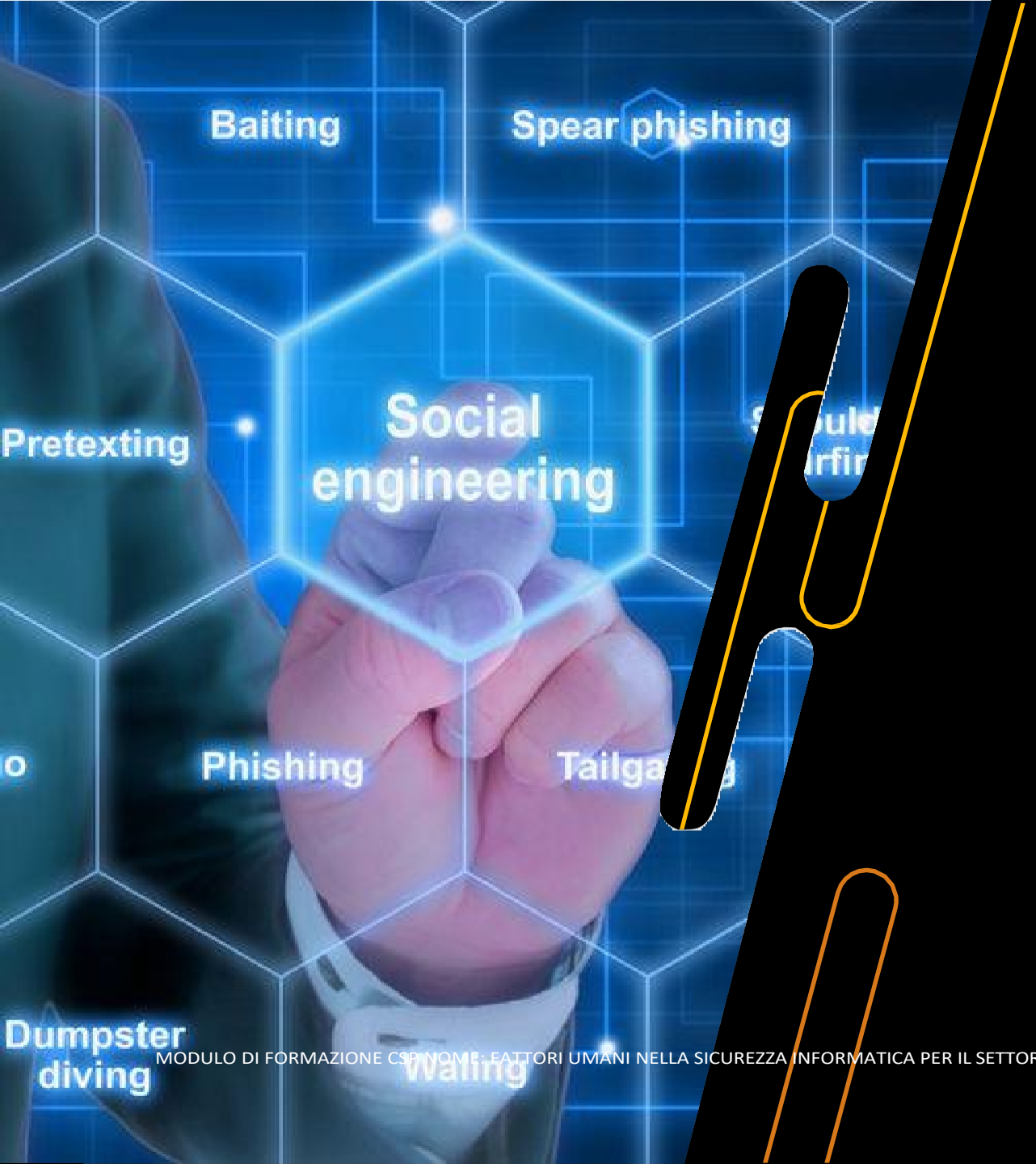
- Comprendere le tattiche di ingegneria sociale da una prospettiva psicologica.
- Formare il personale a riconoscere e rispondere agli agli attacchi di ingegneria sociale.
- Costruire una cultura basata su scetticismo, vigilanza e verifica.
- Esempio reale: la risposta di un'azienda a una campagna di spear-phishing rivolta ai dirigenti.

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

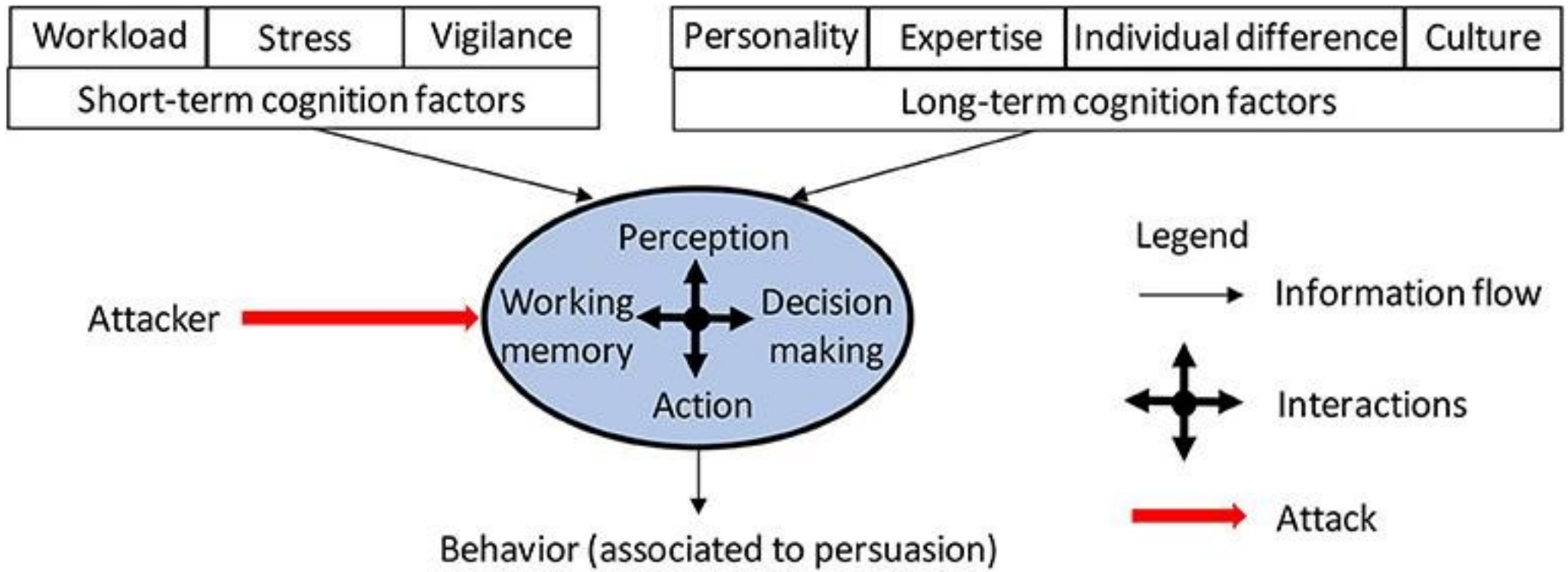


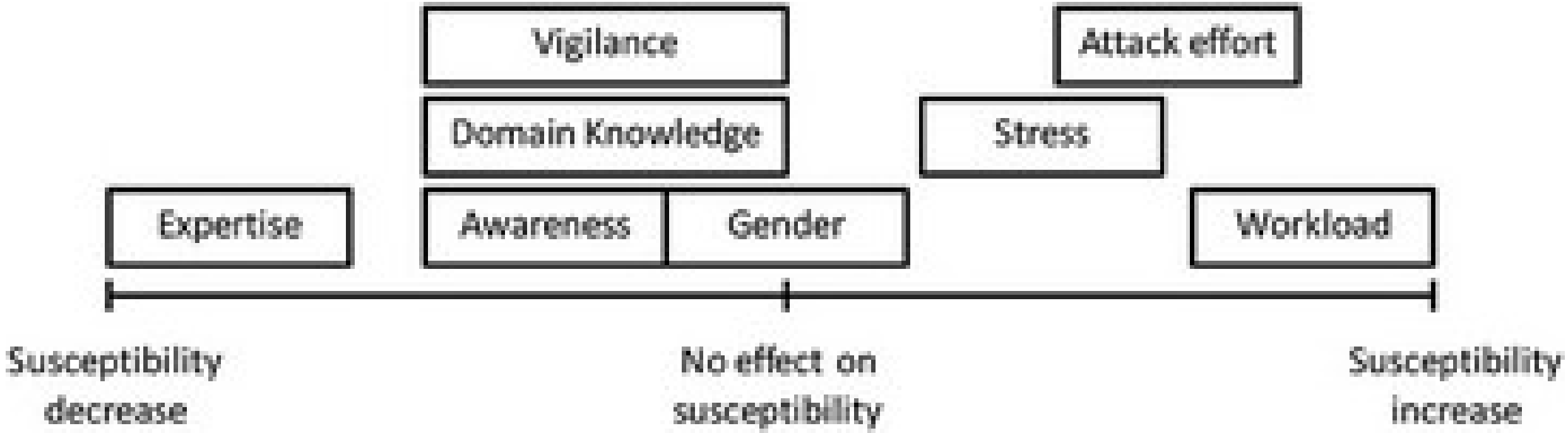
Vulnerabilità umane nella sicurezza informatica del settore energetico

Identificazione delle umane

- Vulnerabilità umane comuni nel contesto della sicurezza informatica nel settore energetico.
- Il ruolo dell'analisi del comportamento degli utenti nell'identificazione di comportamenti rischiosi
  .
- Strategie per mitigare le vulnerabilità umane.
- Esempio reale: incidente che ha coinvolto una vulnerabilità sfruttata a causa di pratiche inadeguate relative alle password.

Exploit cognitivi e vettori di attacco




Vigilance
Attack effort
Domain Knowledge
Stress
Expertise
Awareness
Gender
Workload
Susceptibility decrease
No effect on susceptibility
Susceptibility increase

9 Different Types of Phishing

Email phishing

Spear phishing

Whaling

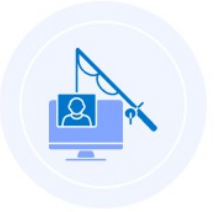
Smishing

Vishing

Crypto phishing

Watering hole attacks

Malvertisements



Angler phishing

10 Tips to Protect Yourself Against Phishing

Hover over links to preview the URL before clicking

Verify email addresses

Use reputable security software

Enable two-factor authentication (2FA)

Avoid pop-ups

Be cautious with personal info

Verify requests for money

Use strong passwords

Avoid using public networks

Report suspected scams

Techopedia

Techopedia

Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior

Abstract

There is interest in better und
ultimately impacted by their
perceived and how someone
framework for explaining this
victimization is essential to u
human despite increased relia
and in real time yet are still im
attitudes and behaviors that
students sampled from two pu
the Online Security Behavior
with an index of perceived vu
regression indicated subscale
competent enough to underst
resulting from a social desira
that knowledge is an essential
vulnerability may depend upo

Keywords: cybersecurity, pe

What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context

Lies De Kimpe [a], Michel Walrave [a], Pieter Verdegem [b] and Koen Ponnet [a,c]

[a]Department of Communication Studies, University of Antwerp Antwerp, Belgium; [b]Communication and Media Research Institute (CAMRI), University of Westminster, Northwick Park, UK.; [c]Department of Communication Studies, imec-mict-Ghent University Ghent, Belgium

ABSTRACT

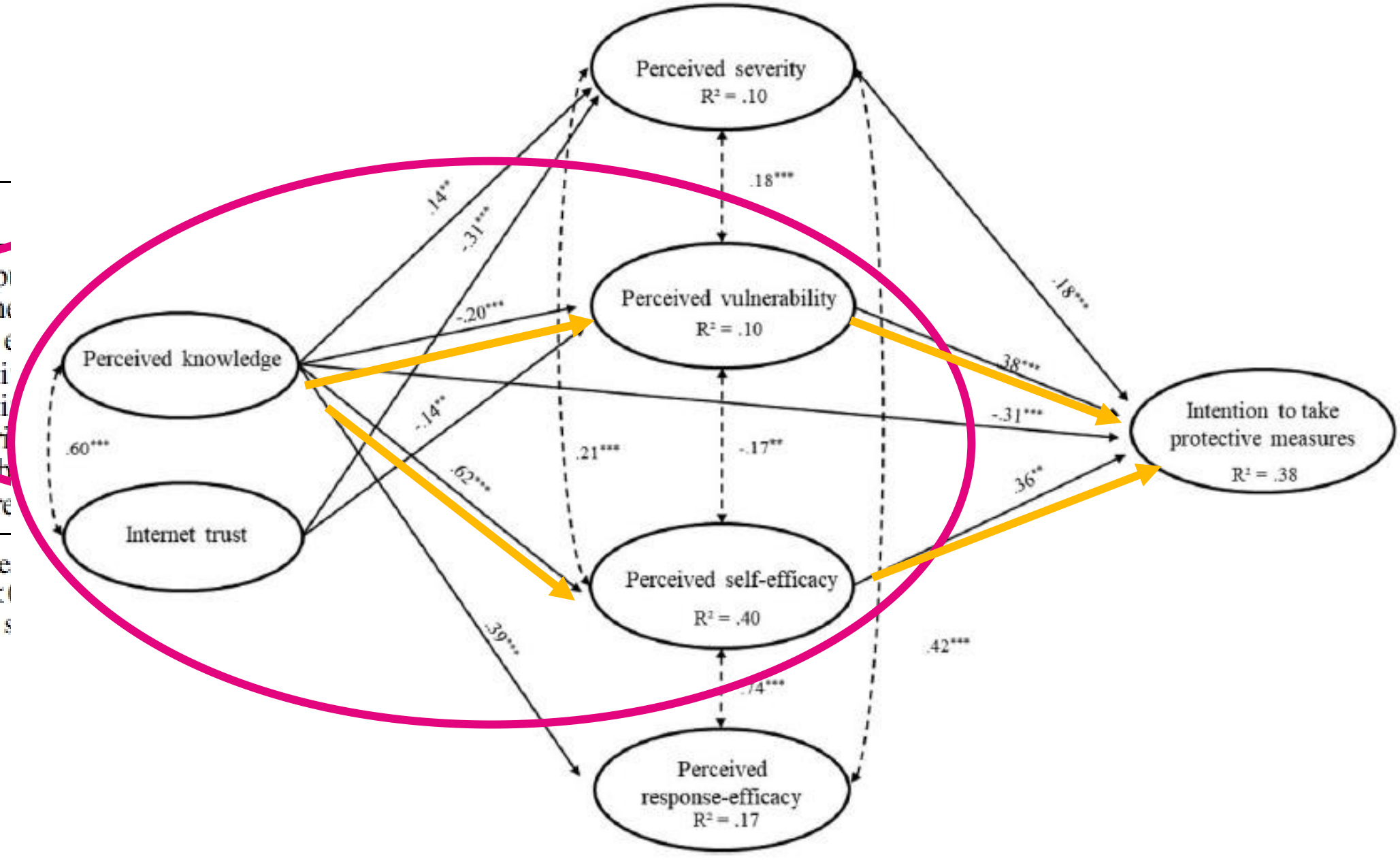
Individual internet users are commonly considered the weakest links in the cybersecurity chain. One reason for this is that they tend to be overoptimistic regarding their own online safety. To gain a better understanding of the cognitive processes involved in this assessment, the current study applies an extended version of the protection motivation theory. More specifically, this study includes perceived knowledge and internet trust to discover how these antecedents influence the threat and coping appraisal processes. Based on representative survey data collected from 967 respondents, we found that people who feel well-informed about online safety feel less vulnerable to cybercrime and are less inclined to take security measures. At the same time, feeling informed is associated with being more convinced of the severity of cybercrime. High levels of trust in the safety of the internet are linked to the feeling that one is less vulnerable to cybercrime and the perception that cybercrime is not a severe threat. Future interventions should remind internet users about their own perceived vulnerability and the risks that exist online while ensuring that internet users do not lose their trust in the internet and confidence in their own online knowledge.

ARTICLE HISTORY

Received 12 February 2019
Accepted 25 February 2021

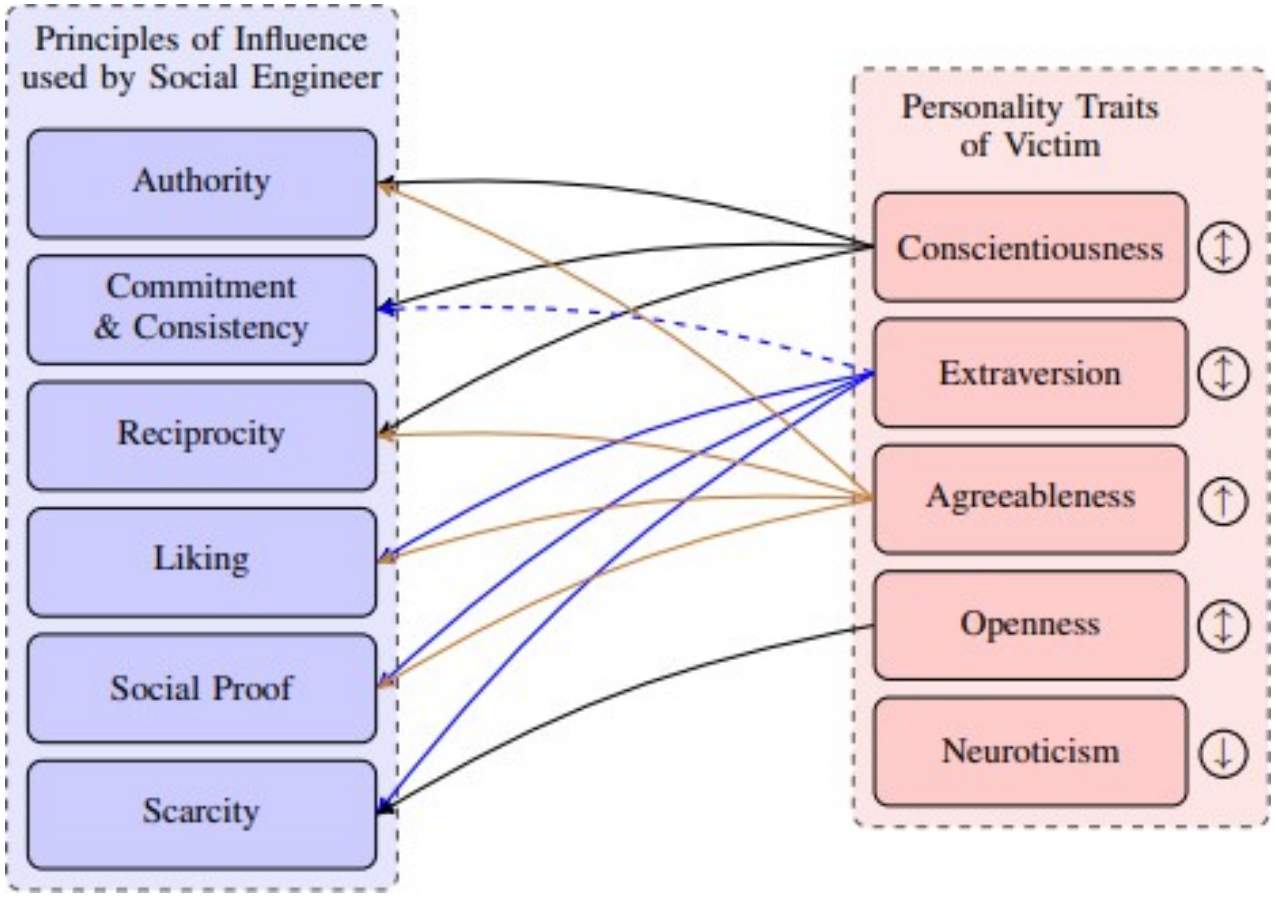
KEYWORDS

Protection motivation theory; cybercrime; optimism bias; perceived knowledge; internet trust


Perceived severity
R² = .10
Perceived vulnerability
R² = .10
Perceived knowledge
Internet trust
Perceived self-efficacy
R² = .40
Perceived response-efficacy
R² = .17
Intention to take protective measures
R² = .38
.14**
-.31***
.18***
-.18***
-.20***
.38***
-.31***
.60***
-.14**
.21***
-.17**
.62***
.36**
.39***
.42***
.74***

Modello di personalità dell'ingegneria sociale (SEPF)

- Attacco:
- C: regole
- E: Eccitazione
- A: Molti modi per...
- O: Scarsità - limitare libertà
- N: Protezione



Profili

Motivazioni:

1. **Guadagno finanziario**: molti aggressori sono motivati da incentivi finanziari
2. **Hacktivismo**: alcuni aggressori compiono attacchi informatici per promuovere un programma sociale o politico, spesso utilizzando mezzi digitali per esprimere la propria opinione.
3. **Curiosità**: gli aggressori spinti dalla curiosità, spesso definiti "script kiddies", esplorano le vulnerabilità per il gusto di farlo
4. **Spionaggio**: gli aggressori sponsorizzati dallo Stato o le spie informatiche mirano a raccogliere informazioni riservate, informazioni classificate o segreti commerciali.

Caratteristiche psicologiche:

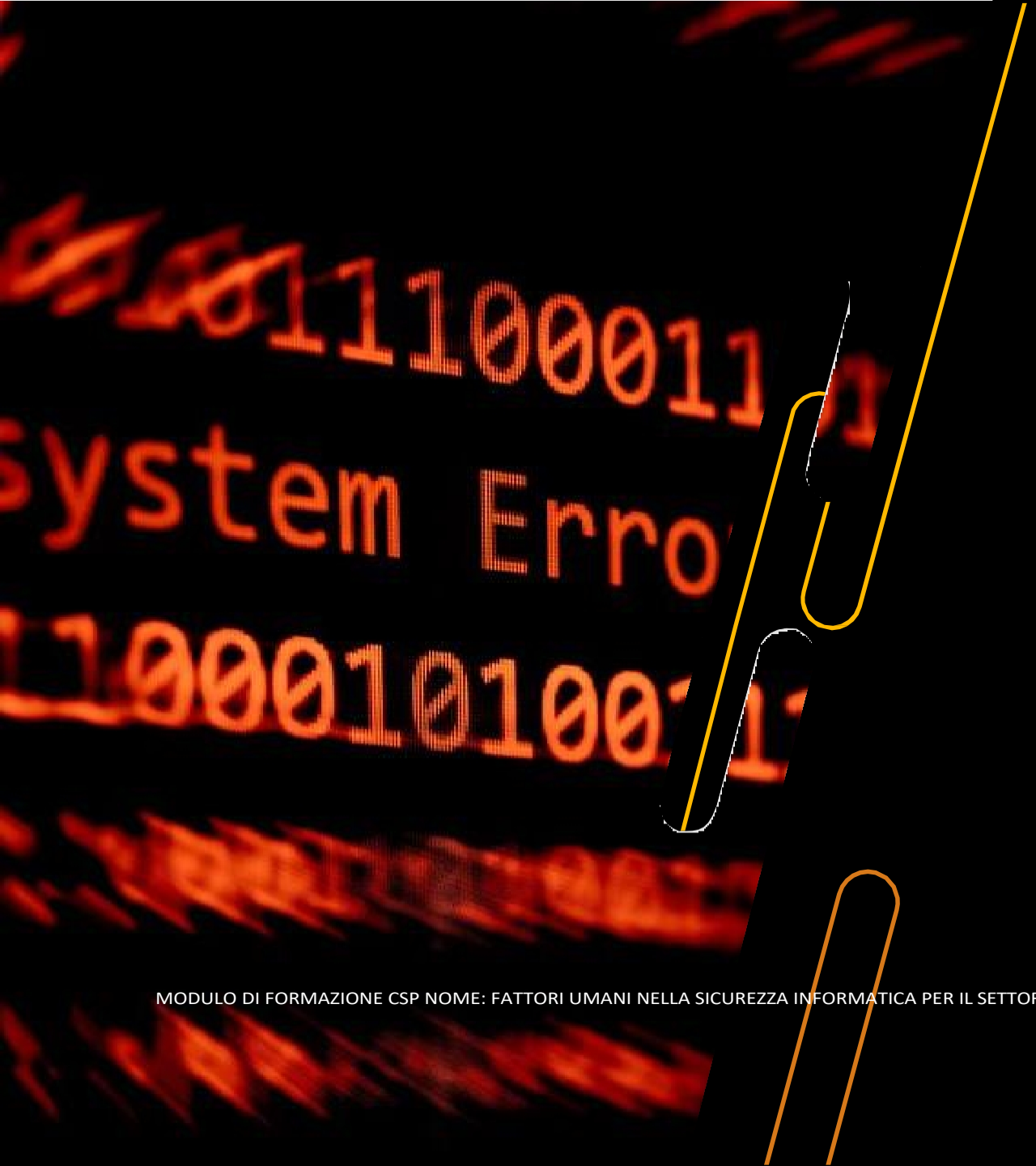
1. **Anonimato**
2. **Elevata intelligenza**
3. **Propensione al rischio**
4. **Mancanza di empatia**

Tecniche di attacco:

1. **Phishing**: gli aggressori utilizzano spesso tecniche di ingegneria sociale per indurre le persone a rivelare informazioni sensibili o a cliccare su link dannosi.
2. **Malware**: gli aggressori utilizzano vari tipi di software dannoso, come virus, worm e trojan, per compromettere i sistemi e rubare dati.
3. **Minacce persistenti avanzate (APT)**: gli aggressori sponsorizzati dallo Stato utilizzano le APT per infiltrarsi e mantenere un accesso discreto a lungo termine ai sistemi bersaglio.

Fattori psicologici:

1. il senso di potere e controllo derivante dal riuscire a violare i sistemi, che porta a un ciclo di dipendenza dal crimine informatico.
2. giustificano le loro azioni credendo di smascherare vulnerabilità o di lottare per una causa che ritengono giusta.



Vulnerabilità umane nella sicurezza informatica del settore energetico

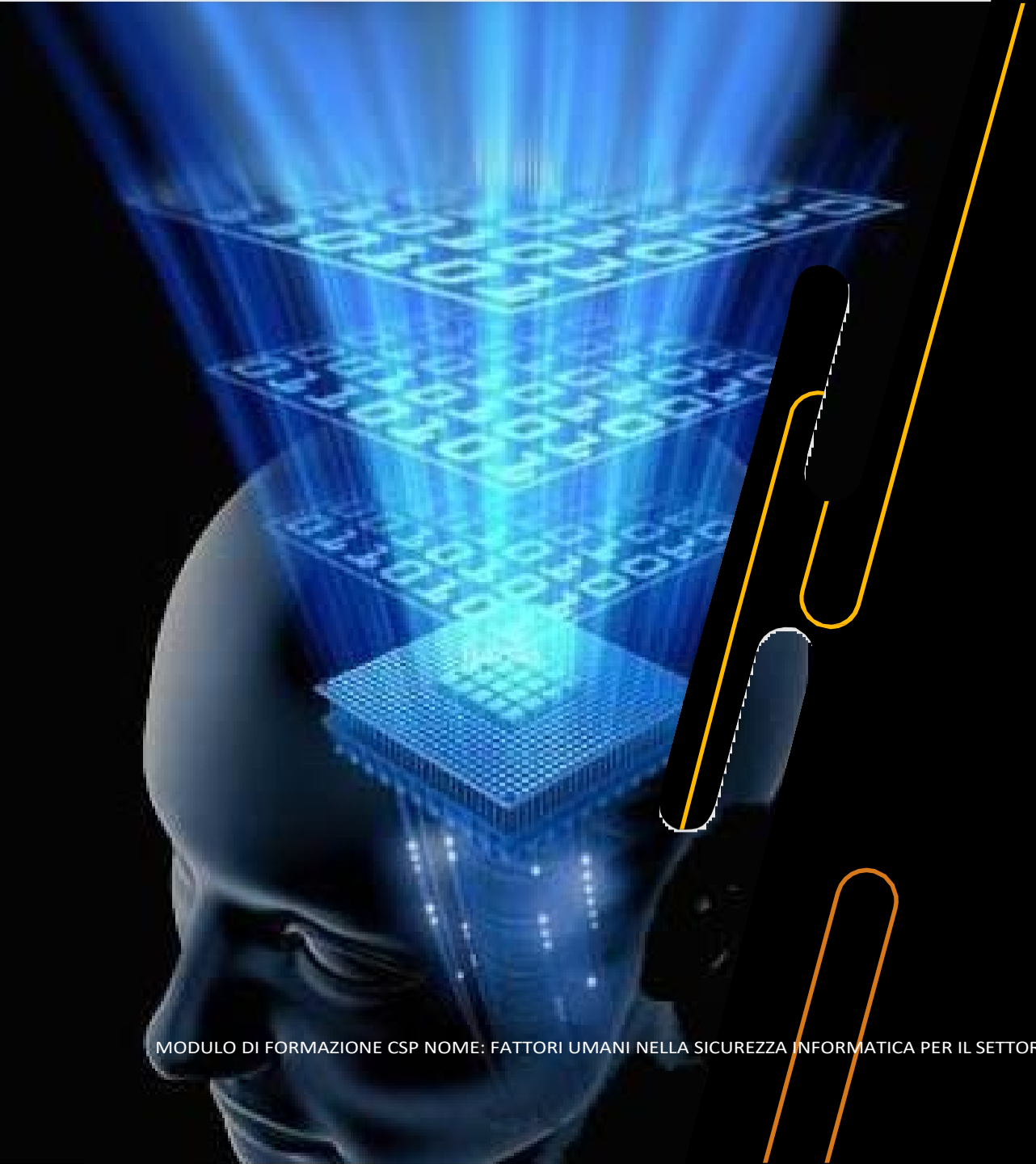
Impatto dell'errore umano

- Tipi di errori umani e loro conseguenze per la sicurezza informatica.
- Metodi per ridurre gli errori, quali semplificazione dei sistemi e dei processi.
- Importanza dei sistemi di segnalazione e gestione degli errori.
- ENISA

Vulnerabilità umane nella sicurezza informatica del settore energetico

Formazione per ridurre l'errore umano

- Ruolo dei programmi di formazione mirati nell'affrontare specifiche vulnerabilità umane.
- Simulazione
- Gamification
- Apprendimento basato su scenari
- Apprendimento continuo
- L'importanza della simulazione e delle esercitazioni nel rafforzare comportamenti corretti.
- Miglioramento continuo dei programmi di formazione sulla base del feedback sugli incidenti.

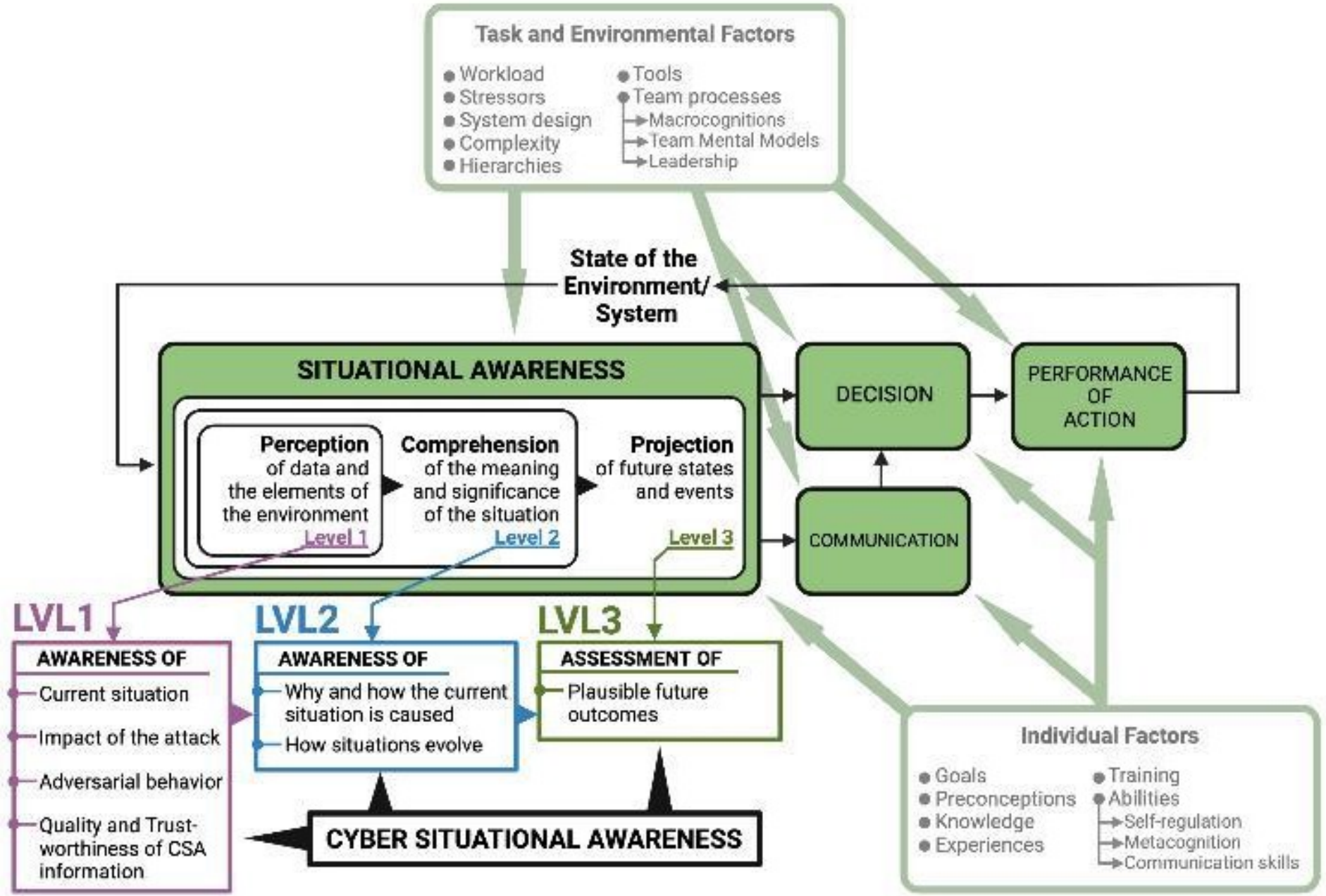


Vulnerabilità umane nella sicurezza informatica del settore energetico

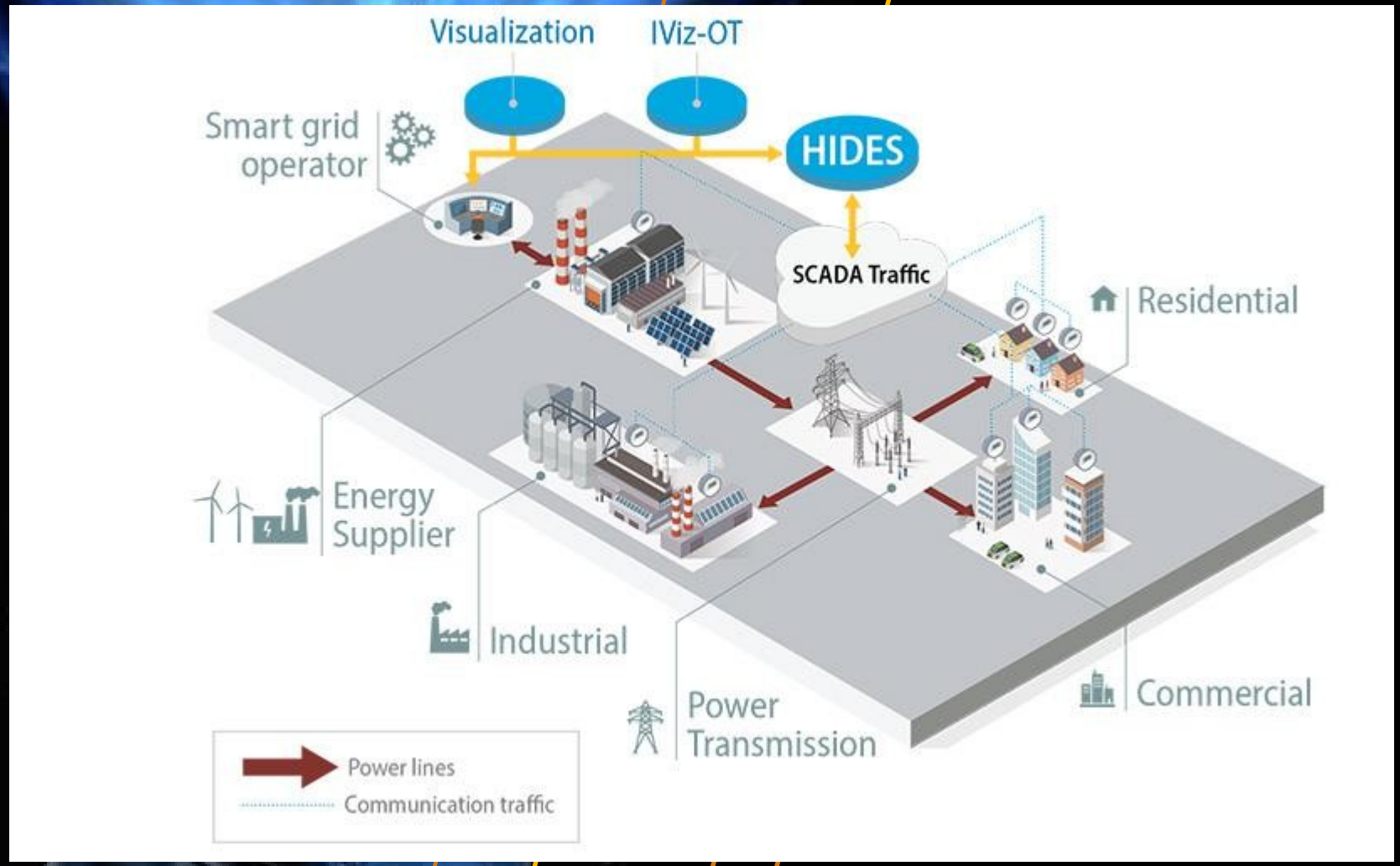
Miglioramento della consapevolezza situazionale dell'
Consapevolezza

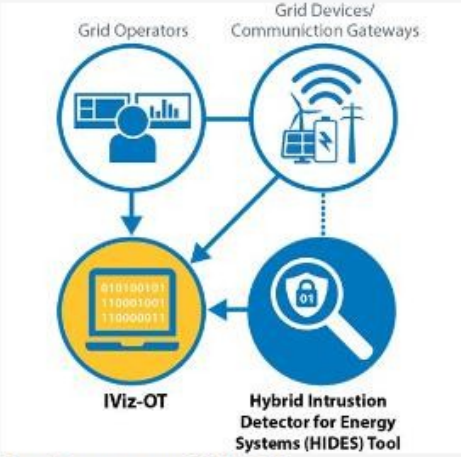
- Importanza della consapevolezza situazionale nella prevenzione degli errori umani.
- Percepire
- Percezione
- Comprensione
- Proiezione
- Strumenti e tecnologie a supporto della consapevolezza situazionale nella sicurezza informatica.
- Visualizzazioni adattate
- Integrazione della consapevolezza situazionale nelle operazioni quotidiane e nel processo decisionale.

Consapevolezza della situazione informatica (CSA) (Barford et al., 2009)



Migliorare la consapevolezza della situazione





Key Features of IViz-OT:

- Visualizes alerts to support situational awareness for grid operators
- Maps alerts to possible scenarios
- Customized application programming interface (API) and supports the integration of alert scenarios and databases
- Compatible with vendor devices.

Key Features of HIDES:

- Detects both IT- and SCADA-specific attacks
- Aggregates data to integrate cyber logs and grid information
- Visualizes grid on the dashboard to provide situational awareness.

Cultura organizzativa, comunicazione e sicurezza informatica

Ruolo della cultura organizzativa

- Definizione e impatto della cultura organizzativa sulla sicurezza informatica.
- Caratteristiche di una forte cultura della sicurezza informatica.
  - Valori (Lencioni, 2002)
  - Adesione e conformità
- Strategie per coltivare una cultura positiva della sicurezza informatica

.

  - Sicurezza psicologica sul posto di lavoro

Cultura organizzativa, comunicazione e sicurezza informatica

Comunicazione efficace in materia di sicurezza informatica

- Principi di comunicazione efficace nella sicurezza informatica.
- Superare gli ostacoli a una comunicazione efficace sulla sicurezza informatica.
- Ruolo della comunicazione trasparente nella risposta agli incidenti.
- Dopo un incidente di sicurezza informatica

Cultura organizzativa, comunicazione e sicurezza informatica

Leadership nella cultura della sicurezza informatica

- Sviluppare la leadership nella sicurezza informatica a tutti i livelli dell'organizzazione.
  - Verticalmente E orizzontalmente

Cultura organizzativa, comunicazione e sicurezza informatica

Promuovere la collaborazione e la fiducia

- Definizione di collaborazione e fiducia: *la collaborazione nel* settore energetico *comporta la condivisione di informazioni, risorse e best practice per migliorare le difese collettive in materia di sicurezza informatica. La fiducia è alla base di questi sforzi di collaborazione, garantendo che le informazioni condivise siano affidabili e che i partner agiscano in modo responsabile con i dati e le conoscenze condivisi*.

- Importanza della fiducia e della collaborazione negli sforzi di sicurezza informatica.
  - Condivisione delle informazioni
  - Esercitazioni congiunte sulla sicurezza informatica

- Tecniche per costruire la fiducia all'interno e tra i team.
  - Alleanze, partnership

- Approcci collaborativi alla risoluzione dei problemi di sicurezza informatica.

- Esempio reale: progetto di collaborazione interdipartimentale che ha rafforzato la posizione complessiva in materia di sicurezza informatica.

Comunicazione e collaborazione tra domini

Sicurezza informatica tra domini

Sfide

- Sfide e opportunità nella collaborazione tra domini in materia di sicurezza informatica.
- Importanza dell'interoperabilità e standard condivisi.
- ENISA, NIS 2
- Strategie per una comunicazione efficace tra i diversi settori

.

Comunicazione e collaborazione tra domini

Costruzione di reti collaborative

- Il ruolo delle reti professionali e delle alleanze nel miglioramento della sicurezza informatica.
- Vantaggi delle partnership pubblico-private nelle iniziative di sicurezza informatica.
  - ESCO
- Sfruttare le competenze in tutti i settori per soluzioni complete di sicurezza informatica.

Comunicazione e collaborazione tra i vari settori

Risposta collaborativa agli incidenti

- Principi di pianificazione collaborativa della risposta agli incidenti pianificazione.
  - Importanza di ruoli e canali di comunicazione chiari durante gli incidenti.
  - Vantaggi delle esercitazioni e delle simulazioni congiunte.
  - Processo decisionale sotto pressione
  - Aspetti culturali
  - Scudi bloccati e settore energetico

Comunicazione e collaborazione tra domini

Superare le barriere alla collaborazione

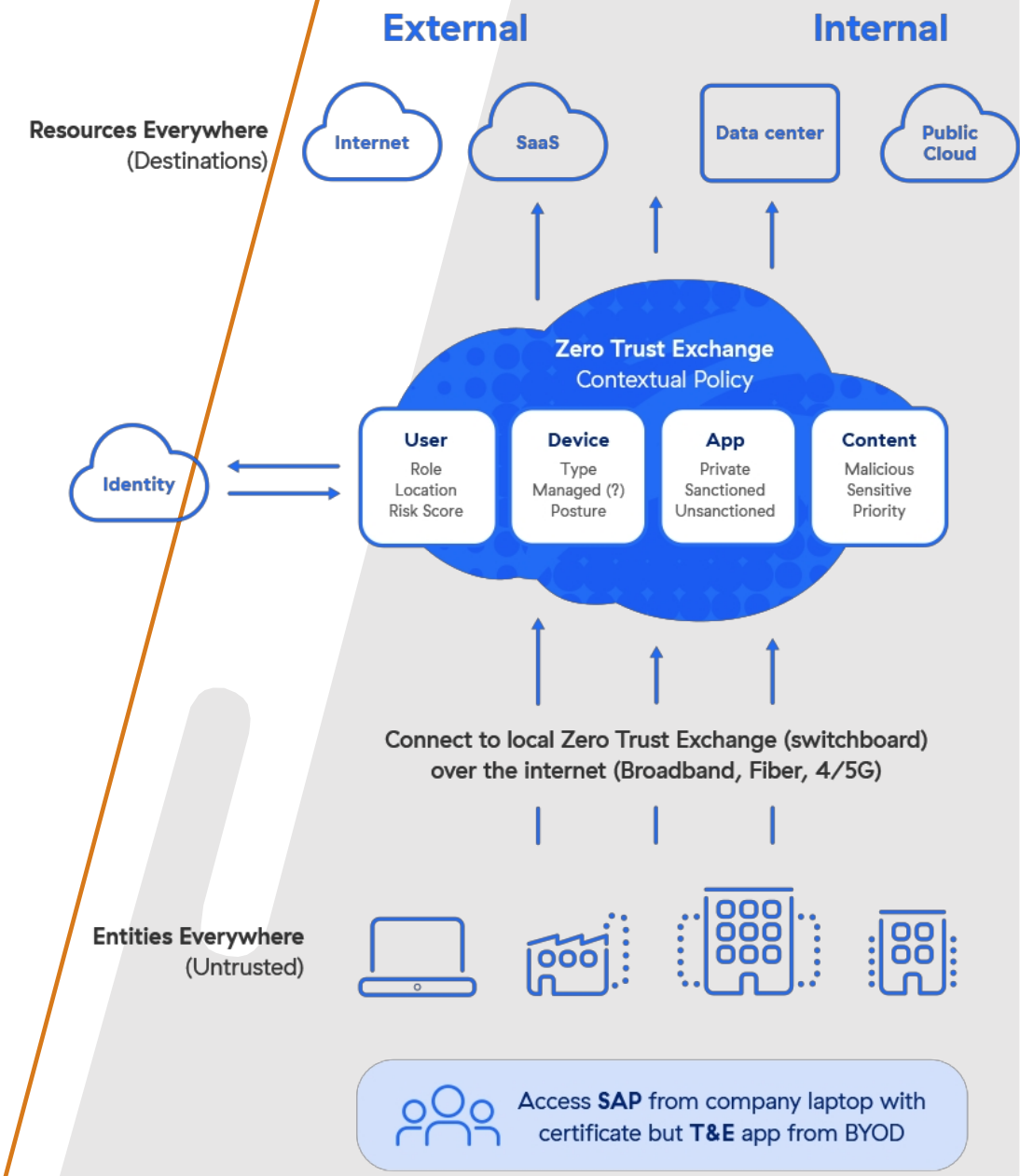
- Ostacoli comuni a una collaborazione efficace in materia di sicurezza informatica e come superarli.
- Il ruolo della fiducia e della trasparenza negli sforzi di collaborazione.
- Migliori pratiche per sostenere relazioni collaborative a lungo termine

  relazioni collaborative a lungo termine.

Processo decisionale a livello strategico, operativo e tattico

Processo decisionale strategico

- Panoramica del processo decisionale strategico nella sicurezza informatica del settore dell'energia .
- Pianificazione a lungo termine e sviluppo di politiche per solidi quadri di sicurezza informatica.
- Integrazione della sicurezza informatica nella strategia aziendale complessiva.
- Esempio reale: la decisione strategica di un'azienda del settore energetico di adottare un'architettura zero-trust.



Processo decisionale a livello strategico, operativo e tattico

Processo decisionale operativo

- Il ruolo delle decisioni operative nel mantenimento della sicurezza informatica quotidiana sicurezza informatica quotidiana.
- Risposte operative alle minacce e alle vulnerabilità identificate.
- Coordinamento tra i team di sicurezza informatica e altre unità operative.
- Esempio reale: una decisione operativa di isolare un sistema compromesso in un impianto, prevenendo una violazione più ampia.

Processo decisionale a livello strategico, operativo e tattico

Processo decisionale tattico

- Natura delle decisioni tattiche nella risposta alle minacce immediate alla sicurezza informatica.
- Strumenti e tecniche per un processo decisionale tattico efficace, compresi i team di risposta agli incidenti e l'intelligence sulle minacce in tempo reale.
- Importanza dell'agilità e della flessibilità nelle decisioni tattiche.
- Esempio reale: risposta tattica rapida a un attacco ransomware a un sistema di gestione.

Processo decisionale a livello strategico, operativo e tattico

Integrazione dei livelli decisionali

- Garantire la coerenza e l'allineamento tra i livelli decisionali strategico, operativo e tattico.
- Meccanismi di feedback e apprendimento tra i livelli decisionali.
- Ruolo della leadership nel colmare il divario tra i diversi livelli decisionali.
- Esempio reale: quadro decisionale integrato che ha consentito una risposta senza soluzione di continuità a un attacco cyber-fisico coordinato.

Programmi di formazione, sensibilizzazione e comunicazione per il personale del settore energetico

Importanza della formazione e della sensibilizzazione

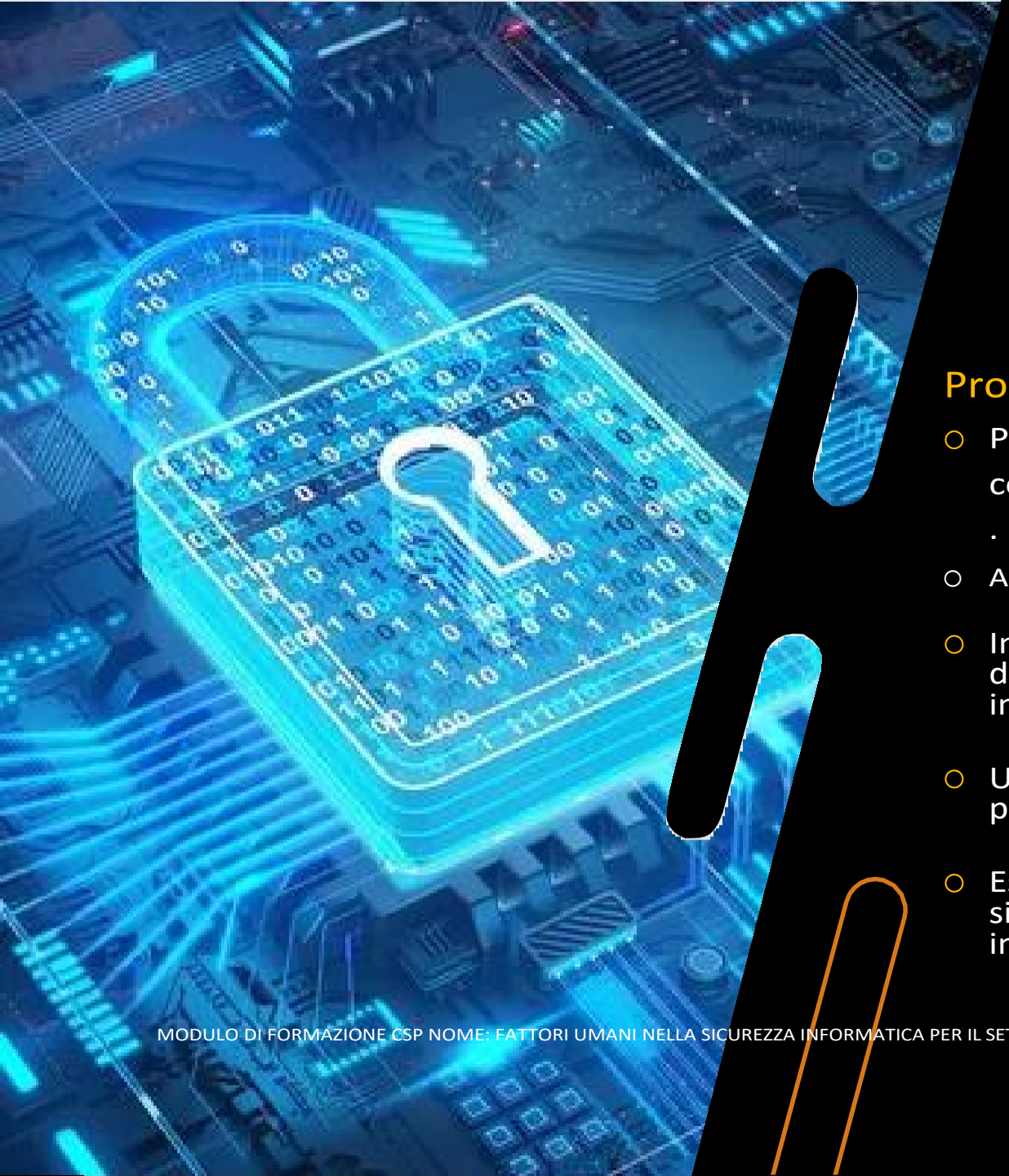
- Il ruolo fondamentale della formazione continua e della sensibilizzazione nella sicurezza informatica del settore energetico.
- Elementi di programmi di formazione efficaci sulla sicurezza informatica per il personale.
- L'impatto dei programmi di sensibilizzazione sulla riduzione degli errori umani e sul miglioramento della cultura della sicurezza.

, NIS 2

Programmi di formazione, sensibilizzazione e comunicazione per il personale del settore energetico

Miglioramento della comunicazione sull' ità per la sicurezza informatica

- Migliori pratiche per comunicare le politiche e gli incidenti relativi alla sicurezza informatica
  e degli incidenti relativi alla sicurezza informatica al personale del settore energetico.
- Il ruolo di una comunicazione chiara e coerente nel promuovere un approccio proattivo alla sicurezza informatica.
- Messaggi chiari
- Flusso di informazioni tempestivo
- Informazioni utili
- Strategie per superare le barriere comunicative in ambienti di energia diversificati e dinamici.
- Comunicazione multicanale
- fee d indietro



Programmi di formazione, sensibilizzazione e comunicazione per il personale del settore energetico

Progettare programmi di formazione efficaci

- Principi per la progettazione di programmi di formazione coinvolgenti e di grande impatto
  .
- Abitudini, autoefficacia, metacognizione
- Incorporare teorie e metodologie di apprendimento degli adulti nella formazione sulla sicurezza informatica.
- Uso di simulazioni ed esercitazioni per rafforzare l'apprendimento e la preparazione.
- Esempio reale: un'accademia dell' e del settore energetico utilizza simulazioni VR per formare i cadetti sui protocolli di sicurezza informatica.

Tendenze future, sfide e ruolo della comunicazione

Tendenze emergenti nella sicurezza informatica

- Panoramica delle tendenze emergenti nella sicurezza informatica, tra cui IA, apprendimento automatico e IoT.
- Le implicazioni di queste tendenze per le strategie di sicurezza informatica nel settore energetico.
- Prepararsi alle future sfide della sicurezza informatica attraverso l'innovazione e l'adattabilità.
- Esempio reale: adozione di sistemi di rilevamento delle minacce basati sull'intelligenza artificiale sulle navi intelligenti.

Tendenze future, sfide e ruolo della comunicazione

Affrontare le sfide future della sicurezza informatica

- Anticipare e mitigare i nuovi tipi di minacce informatiche nel settore energetico.
- L'importanza di stare al passo con i tempi attraverso la ricerca e la collaborazione con esperti di sicurezza informatica.
- Sfide poste dalla crescente complessità e connettività delle operazioni nel settore energetico.

Tendenze future, sfide e ruolo della comunicazione

Il ruolo in evoluzione della comunicazione

- Il ruolo fondamentale di una comunicazione efficace nell'affrontare le future sfide della sicurezza informatica.
- Migliorare la comunicazione intersettoriale e transfrontaliera per una risposta unificata alle minacce informatiche.
- Sfruttare le nuove tecnologie e piattaforme di comunicazione per una migliore condivisione delle informazioni sulle minacce.
- Esempio reale: Iviz-OT.

Tendenze future, sfide e ruolo della comunicazione

Prepararsi al futuro

- Pianificazione strategica e investimenti nelle capacità di sicurezza informatica per prepararsi alle sfide future.
- Il ruolo della leadership nella promozione di una cultura della sicurezza informatica lungimirante.
- Importanza della cooperazione globale e della condivisione delle informazioni nel rafforzamento della resilienza della sicurezza informatica nel settore energetico.
- Sistemi di automazione e controllo industriale (IACS)

Si prega di valutare

https://forms.gle/uTSmjnuBKU2o4Uiy9

Scegliere: **CSP002_S_E: Fattori umani e sicurezza informatica nel settore energetico**

Risorse: Libri e materiali di riferimento

1. "Quadro europeo delle competenze in materia di sicurezza informatica": Pubblicazione dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA)
2. Agenzia dell'Unione europea per la sicurezza informatica (ENISA). (2019). Linee guida sulla cultura della sicurezza informatica: aspetti comportamentali della sicurezza informatica. Tratto da https://www.enisa.europa.eu.
3. Hanzu-Pazara, R., Raicu, G. e Zăgan, R. (2019). L'impatto del comportamento umano sulla sicurezza informatica sicurezza informatica dei sistemi marittimi. Advanced Engineering Forum, 34, 267-274.
4. Wiederhold, B. (2014). Il ruolo della psicologia nel miglioramento della sicurezza informatica. Cyberpsicologia, comportamento e social networking, 17(3), 131-132.
5. Aşan, C. (2023). Il ruolo della consapevolezza situazionale informatica degli esseri umani negli attacchi informatici di ingegneria sociale nel settore marittimo. Rivista della Facoltà Marittima dell'Università di Mersin. Link
6. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S. e Michaloliakos, M. (2022). Le sfide della sicurezza informatica nel settore marittimo. Network, 2, 123-138.
7. Endsley, M. R. e Jones, D. G. (2024). Progettazione orientata alla consapevolezza della situazione: revisione e direzioni future. Rivista internazionale di interazione uomo-computer, 1-18.
8. Thackray, H., McAlaney, J., Dogan, H., Taylor, J., & Richardson, C. (2016). Psicologia sociale: uno strumento sottoutilizzato nella sicurezza informatica.
9. Knox, B. J., Lugo, R. G., & Sütterlin, S. (2019). La cognizione come fattore umano nella formazione militare sulla difesa informatica. IFAC-PapersOnLine, 52(19), 163-168.

Grazie

Per qualsiasi domanda, inviate un'e-mail all'indirizzo:
Ricardo.Lugo@taltech.ee