FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Formazione e awareness

La prima linea di difesa per la mitigazione del rischio cyber

FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Interviene:

Paolo Atzeni

Direttore per lo Sviluppo di Capacità e Competenze, Agenzia di Cybersicurezza Nazionale (ACN)

Competenze in Cybersicurezza: quadro di riferimento per i percorsi formativi

Motivazione

- Carenza e divario di competenze in cybersicurezza e più in generale in tutta l'area ICT (per non parlare dell'intelligenza artificiale …)
  - Comunicazione della Commissione Europea sulla "Cybersecurity Skills Academy"

    https://ec.europa.eu/newsroom/dae/redirection/document/95048
  - Rapporto ENISA "Addressing the EU cybersecurity skills shortage and gap through higher education"

    https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport
  - Rapporti DESI 2022 e Digital Decade 2023 (pochi specialisti, pochi laureati):

    https://ec.europa.eu/newsroom/dae/redirection/document/88751

    https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo di figure ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi
- Che cosa possiamo e dobbiamo fare?
  - Tante cose!

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo di figure ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi

Iniziative a supporto, per l'approccio a lungo termine

- Dobbiamo avvicinare i giovani alla cybersicurezza e più in generale alle discipline informatiche
- Possibili azioni:
  - promozione dell'insegnamento dell'informatica nella scuola, per tutti e il più presto possibile, fin dalle primarie
  - potenziamento delle competizioni in cybersicurezza
  - formazione e coinvolgimento degli insegnanti (importante a supporto delle due azioni precedenti)

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo di figure ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo di figure ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi

Non abbiamo bisogno solo di specialisti

- La cybersicurezza (come l'informatica in generale) è pervasiva:
- La tecnologia è solo in parte una "scatola nera" (altrimenti rischiamo le frasi assurde come "lo dice il computer" oppure "lo decide l'algoritmo")
  - Gli informatici debbono avere la consapevolezza dell'importanza dei domini applicativi
  - Gli specialisti dei vari domini (o almeno parte di loro), se vogliono utilizzare una tecnologia ricca e flessibile, debbono conoscere almeno qualcosa dei suoi principi
- Servono approcci multidisciplinari:
  - Informatici e specialisti dei domini applicativi si debbono poter parlare
  - I corsi di laurea e laurea magistrale debbono essere aperti
  - Sono utili i master che prevedono contaminazione fra le discipline

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo di figure ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo di figure ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi

ITS, un approccio mirato e più veloce

- Sistema ITS:
  - formazione terziaria non universitaria, di durata più breve (due anni, di solito)
  - in collaborazione con le aziende (con ottime prospettive di inserimento)
  - ispirato almeno in parte alle esperienze di altri paesi
    - ad esempio Germania, con le Fachhochshulen che risalgono ad almeno cinquanta anni fa
  - In Italia numeri per ora piccoli, ma con ottime possibilità di crescita

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi

Approccio a lungo termine

- Se abbiamo pochi laureati ICT e pochi specialisti ICT (DESI e Digital Decade), dobbiamo aumentarne il numero
  - lauree, lauree magistrali, dottorati in cybersicurezza o almeno informatica e ingegneria informatica
- Ma questo
  - non funziona: i laureati sono pochi perché gli studenti non sono abbastanza e dobbiamo attrarli
  - non basta: non abbiamo bisogno solo di specialisti e non solo ad altissimo livello
  - non funziona subito: dobbiamo aspettare che completino i percorsi

Formazione nel mondo del lavoro

- Azienda e amministrazioni hanno spesso necessità di personale con competenze specifiche e hanno difficoltà a reperirlo sul mercato oppure dispongono di personale valido con competenze non allineate a quelle che si desiderano.
- Tante situazioni ed esigenze diverse, tante sfaccettature, legate alle esigenze ad esempio, schematizzando
  - formazione verso gli aspetti tecnici della cybersicurezza di
    - laureati (anche magistrali), in discipline informatiche, senza competenze di cybersicurezza
    - laureati in discipline tecnico scientifiche non informatiche (fisica, matematica, settori dell'ingegneria diversi dall'informatica)
  - approfondimenti specifici, su tematiche emergenti, per specialisti già in possesso di competenze mirate in cybersicurezza
  - formazione verso gli aspetti organizzativi o giuridici della cybersicurezza di laureati in discipline giuridiche o economiche.
  - formazione di base cybersicurezza per funzionari o dirigenti del settore informatico o di settori applicativi diversi dall'informatica

Formazione nel mondo del lavoro, come procedere

- Iniziative articolate
  - percorsi brevi o percorsi lunghi
  - percorsi personalizzabili e adattabili
  - obiettivi formativi definiti sulla base dei profili di riferimento e delle conoscenze e competenze possedute
    - può essere utile il riferimento a "body of knowledge" (CyBOK, ACM/IEEE, JRC Taxonomy) e a ruoli professionali (NICE del NIST, USA, e ECSF di ENISA, Europa)
  - certificazioni e corsi di preparazione ad esse possono essere utili
  - i master possono avere un ruolo

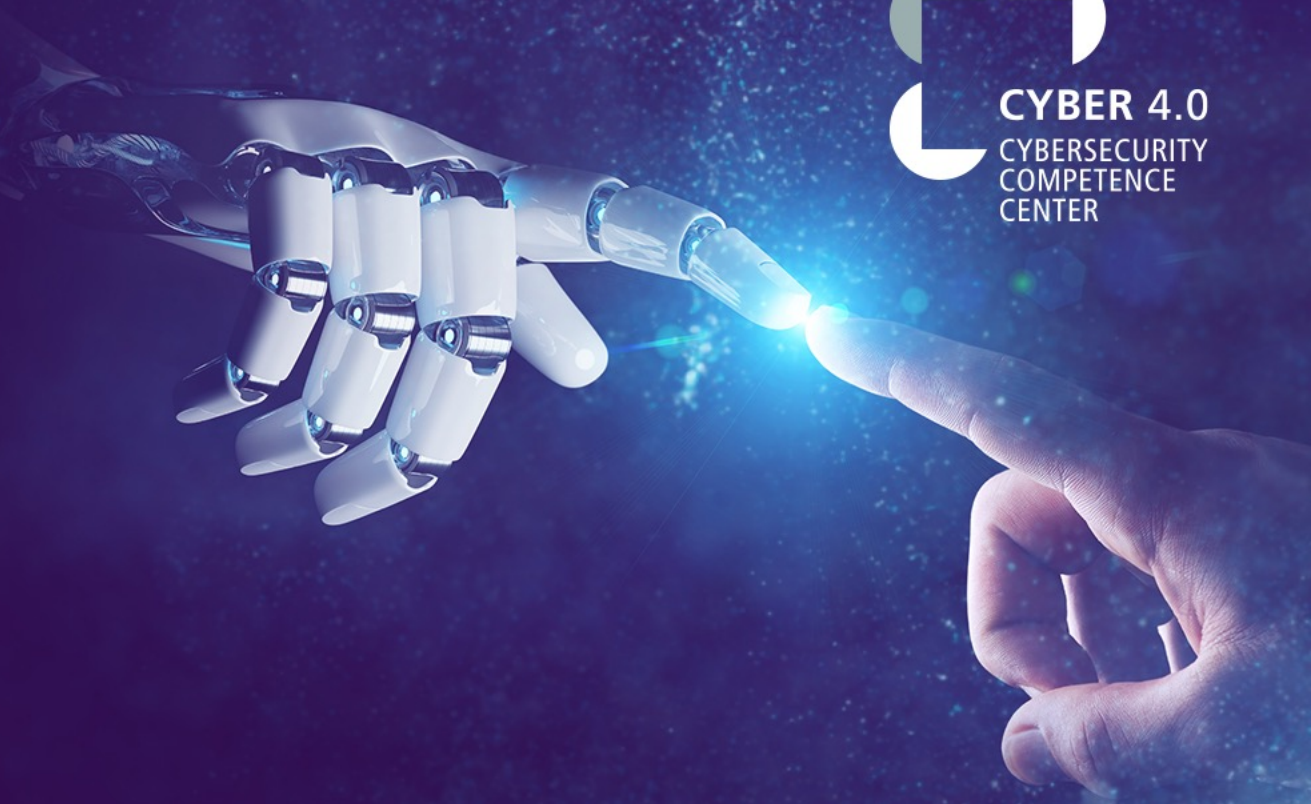
Conclusioni

- Il problema è complesso e articolato
- Richiede la collaborazione di tutti i soggetti e la creazione di un ecosistema:
  - aziende
  - sistema scolastico e universitario
  - enti di formazione pubblici e provati
  - realtà associative e consortili
  - istituzioni

FORUM 2024
CYBER 4.0

The Dome LUISS Roma
3-4 Giugno 2024

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER



Paolo Atzeni

p.atzeni@acn.gov.it

Grazie per l’attenzione

FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Modera:

Alessandro Calabrese

Head of Advisory and Training, Cyber 4.0

Formazione, Awareness & Training: le iniziative di Cyber 4.0

Awareness & Training

Le iniziative di Cyber 4.0

FORUM 2024 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Attività incentivate e di mercato: imprese

- **LINEA B2**
  Servizi Finanziati con Focus PMI
- **LINEA A**
  Potenziamento strumenti formazione
- **SERVIZI DI MERCATO**
  L'offerta Cyber 4.0 con focus Big Enterprise

Attività Istituzionali e iniziative PA

- **WEBINAR MIMIT**
  Ciclo di webinar rivolto a lavoratori pubblici e privati
- **SEMINARI PER PA**
  Ciclo di seminari rivolti ai ruoli apicali delle PA
- **FONDO EDIH NEST PA**
  1 MLN dedicato a servizi incentivati PA

Iniziative per scuole e ITS

- **A SCUOLA CONNESSI**
  Iniziativa rivolta a scuole medie e superiori (Reg. Lazio)
- **LET'S CYBER GAME!**
  Contest MIMIT rivolto agli ITS: videogiochi a tema cyber
- **FORMAZIONE ITS**
  Attività di formazione per ITS

Attività incentivate e di mercato per le imprese

L'offerta di Cyber 4.0 e le modalità di erogazione del servizio

FORUM 2024 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Cyber 4.0, in collaborazione con i propri soci fornitori, ha consolidato una proposta di Cyber Awareness & Training a 360 gradi.

Skills Assessment
- Phishing Campaigns
- Skills Assessment
- Evaluation Tools

…

Self Awareness
- News Feed /Bulletin
- E-Learning & Video Pills
- Quiz, Test & Minigame

…

Active Training
- Exercise (TT, live, VR)
- Cyber Range
- Hacking Challenges

…

Passive Training
- Workshop & Webinar
- Passive Simulation
- Eventi

…

Courses

A CATALOGO

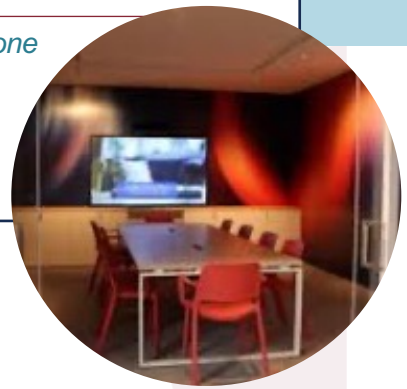
Linee di Azione in ambito Formazione

LINEA B2 - *Servizi Incentivati: PNRR e EDIH NEST - Focus PMI*

I servizi di formazione rappresentano il 37% delle richieste su 7 tipologie di macro-servizi

LINEA A - *Potenziamento delle infrastrutture del Centro*

In fase di pianificazione progetti cofinanziati per implementare tool e piattaforme di awareness



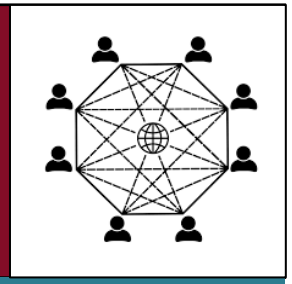
SERVIZI DI MERCATO - *Offerte custom - Focus Big Enterprise*

Il Centro è in grado di proporsi come fornitore unico per servizi di formazione personalizzati

Attività istituzionali e iniziative per le PA

Alcune attività 2024

WEBINAR MIMIT/CYBER 4.0



Un ciclo di seminari in modalità webinar, rivolto a lavoratori pubblici e privati, dedicato all'aggiornamento professionale sul tema della sicurezza informatica, Organizzato dal MIMIT in collaborazione con Cyber 4.0.

CONCLUSI

11 Aprile 279 partecipanti
- *Automotive e cybersecurity*

14 Maggio 401 partecipanti
- *Cybersecurity e AI 1*

27 Maggio 405 partecipanti
- *Cybersecurity e AI 2*

PROGRAMMATI

Giugno
- *Cybersecurity e AI 3*

Settembre
- *Il Cyber Resilience Act*

Ottobre
- *La Direttiva NIS 2*

Novembre
- *La cybersecurity nel settore sanità*

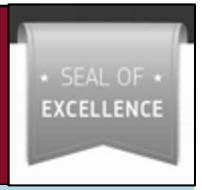
SEMINARI PER ALTA DIREZIONE PA

Il MIMIT ha lanciato, in collaborazione con Cyber 4.0, un format di seminari in ambito cybersecurity rivolti ai livelli apicali delle Pubbliche Amministrazioni.

ALCUNE DELLE PA COINVOLTE

MIMIT
CNVVF
RGS
MASE (TBC)

FONDO EDIH NEST PER PA



Cyber 4.0 ha stanziato 1 Mln di euro per incentivi da rivolgere alle Pubbliche Amministrazioni in ambito di servizi di innovazione, grazie al fondo EDIH NEST.

IN CORSO PROPOSTE DI COLLABORAZIONE PER ATTIVITA' FINANZIATE E NON, RIVOLTE ALLE PA

Iniziative per Scuole e ITS

Alcune attività 2024

FORUM 2024 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

DOMANI POMERIGGIO AL SIDE EVENT “COMPETENZE CYBER PER IL FUTURO”!

Cyber 4.0 in collaborazione Regione Lazio, Accademia di Cybersicurezza Lazio e USR Lazio ha avviato un’iniziativa di formazione in ambito cybersecurity presso gli istituti superiori della Regione Lazio coinvolgendo **più di 30 istituti e più di 2000 studenti**.

“LET’S CYBER GAME” è un contest nazionale promosso dal MIMIT, con il supporto di Cyber 4.0 e di Invitalia. Il concorso ha coinvolto gli studenti di **22 ITS Academy** italiani appartenenti all’Area Tecnologie della informazione e della comunicazione per **ideare, sviluppare, testare e prototipare un videogioco sulla cybersecurity** anche per il contrasto al cybercrime. Domani avremo il piacere di ospitare i 3 vincitori del concorso, premiati in occasione del Forum PA.

Affiliazioni EU in ambito Formazione e Competenze

Ad-Hoc WG on the European Cybersecurity Skills Framework

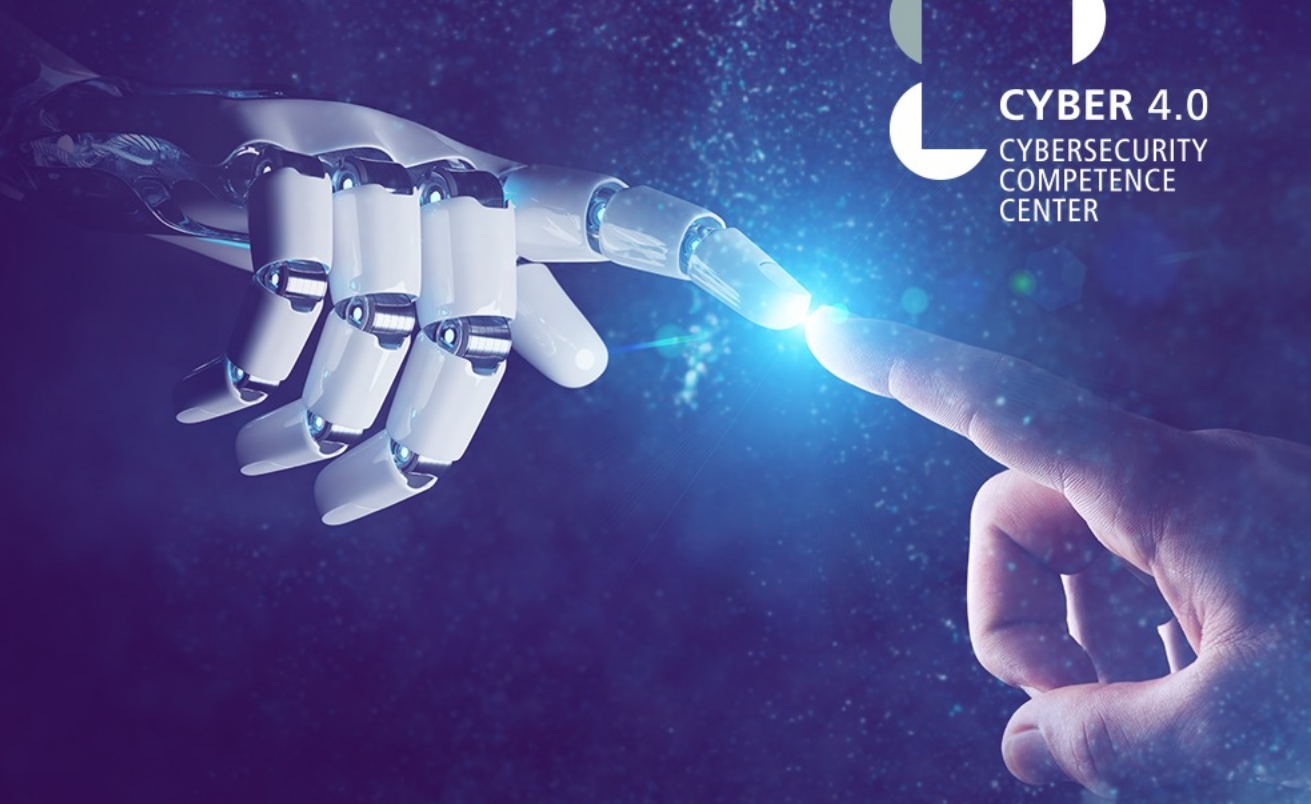
Cyber 4.0 partecipa come «Permanent Observer» all' ***Ad-Hoc Working Group on the European Cybersecurity Skills Framework (ECSF).***
L'obiettivo del Gruppo di Lavoro consiste nel supportare ENISA nella gestione, implementazione e evoluzione dell'ECSF.

L'ECSF è uno strumento pratico per supportare l'identificazione e l'articolazione dei compiti, delle competenze, delle abilità e delle conoscenze associate ai ruoli dei professionisti della cybersecurity in Europa. È il punto di riferimento dell'UE per definire e valutare le competenze rilevanti, come definito nell'Accademia delle Competenze in materia di Cybersecurity, recentemente annunciata dalla Commissione Europea.

FORUM 2024
CYBER 4.0

The Dome LUISS Roma
3-4 Giugno 2024

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER



Alessandro Calabrese

alessandro.calabrese@cyber40.it

Grazie per l’attenzione

FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Interviene:

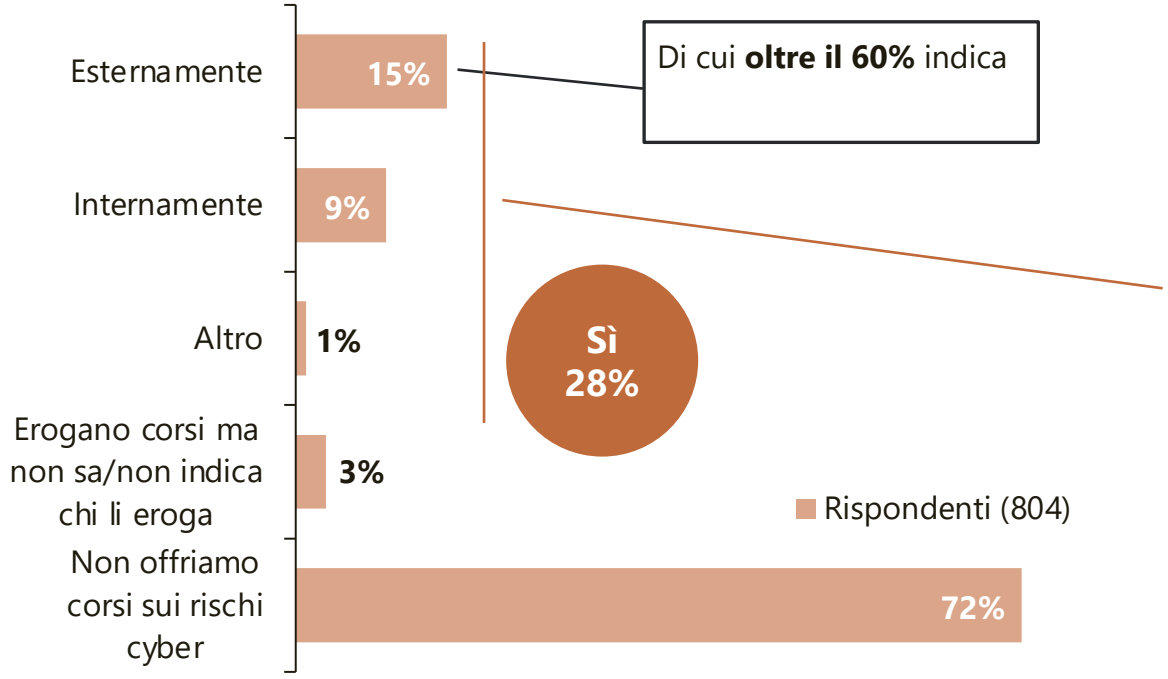
Alessandro Curioni

Presidente, Di.Gi. Academy

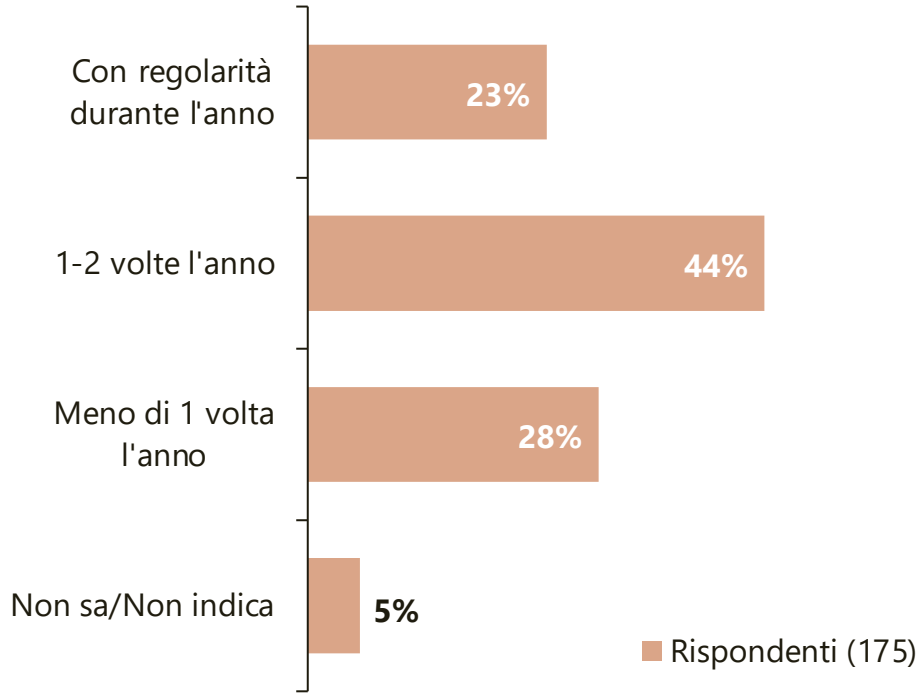
Formazione progressiva per le PMI

Formazione poca, poca

E l'azienda mettete a disposizione dei dipendenti **corsi/webinar sui rischi cyber** e sulle precauzioni da adottare?



E con **quale frequenza** vengono erogati i corsi di formazione e aggiornamento sulla cybersecurity ai dipendenti?



Problemi di base

- Spesso noiosa
- Molte delle informazioni sono incomprese

Percepita come:
un obbligo non utile
un esigenza dell'azienda e non personale

Approccio progressivo

Interventi brevi per un tempo lungo
Con qualità crescente nel tempo

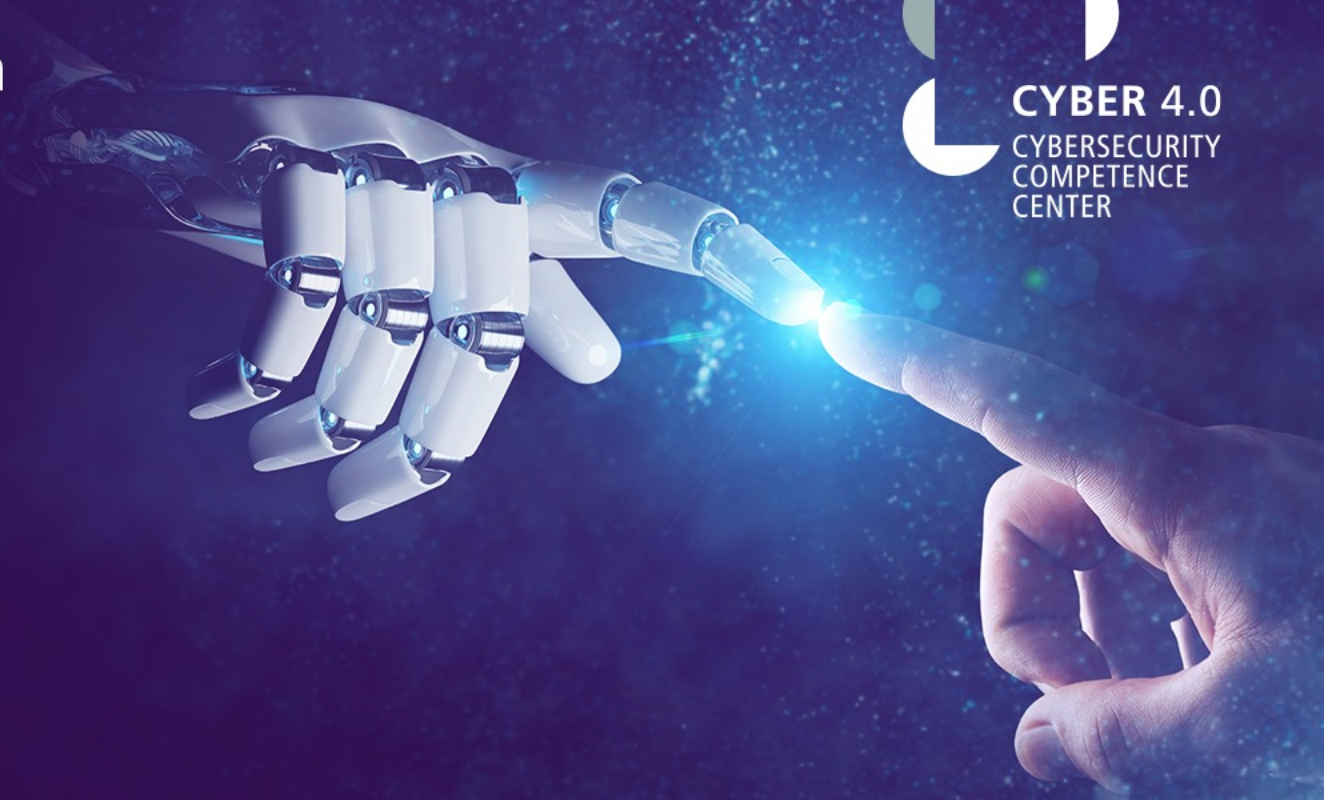
Siamo solo all’inizio

DI.GI. Academy

FORUM 2024
CYBER 4.0

The Dome LUISS Roma
3-4 Giugno 2024

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER



Alessandro Curioni

alessandro.curioni@digiacademy.it

Grazie per l’attenzione

FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

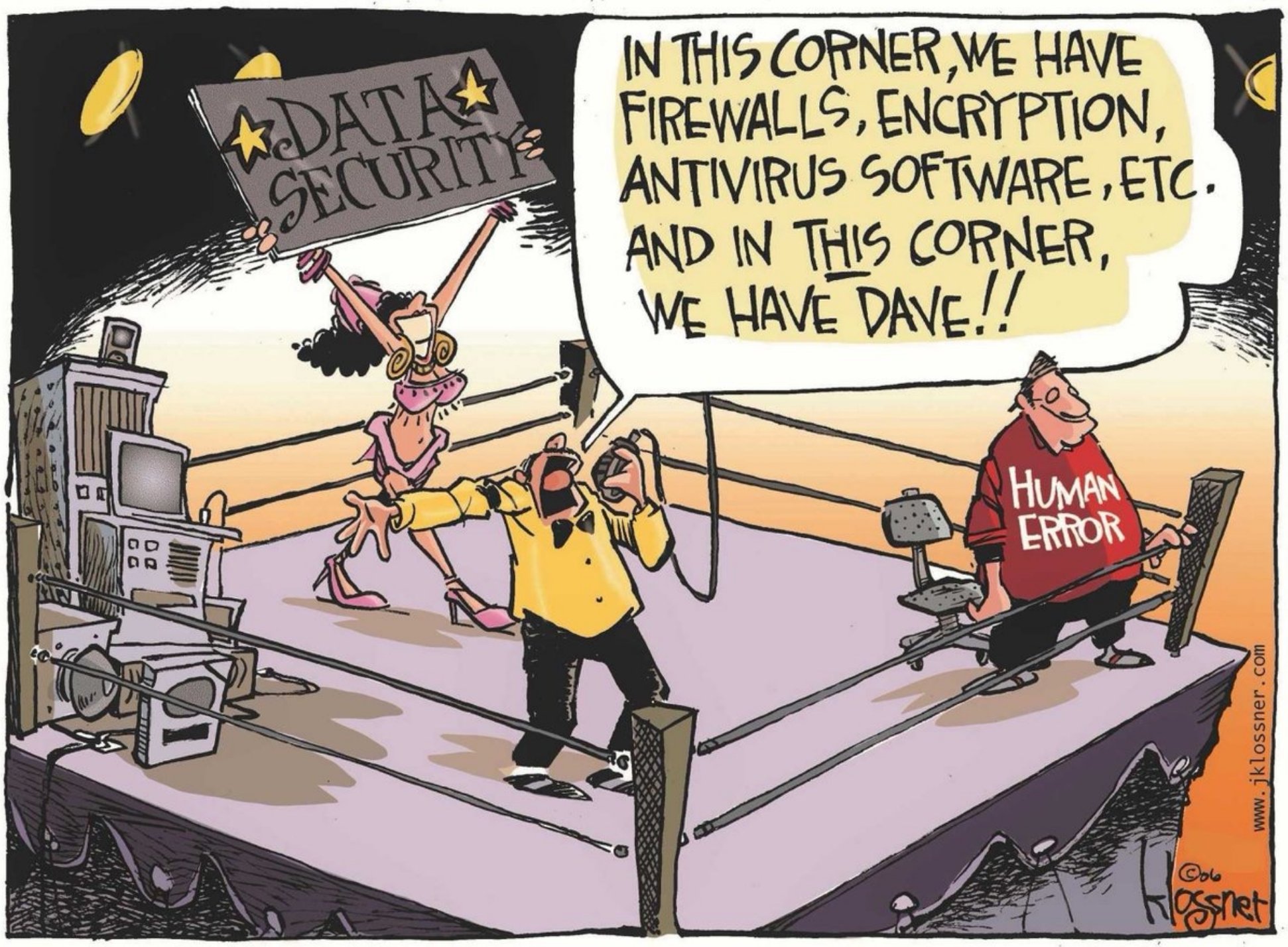
LUISS

Interviene:

Antonio Capobianco

Chief Executive Officer, Fata Informatica

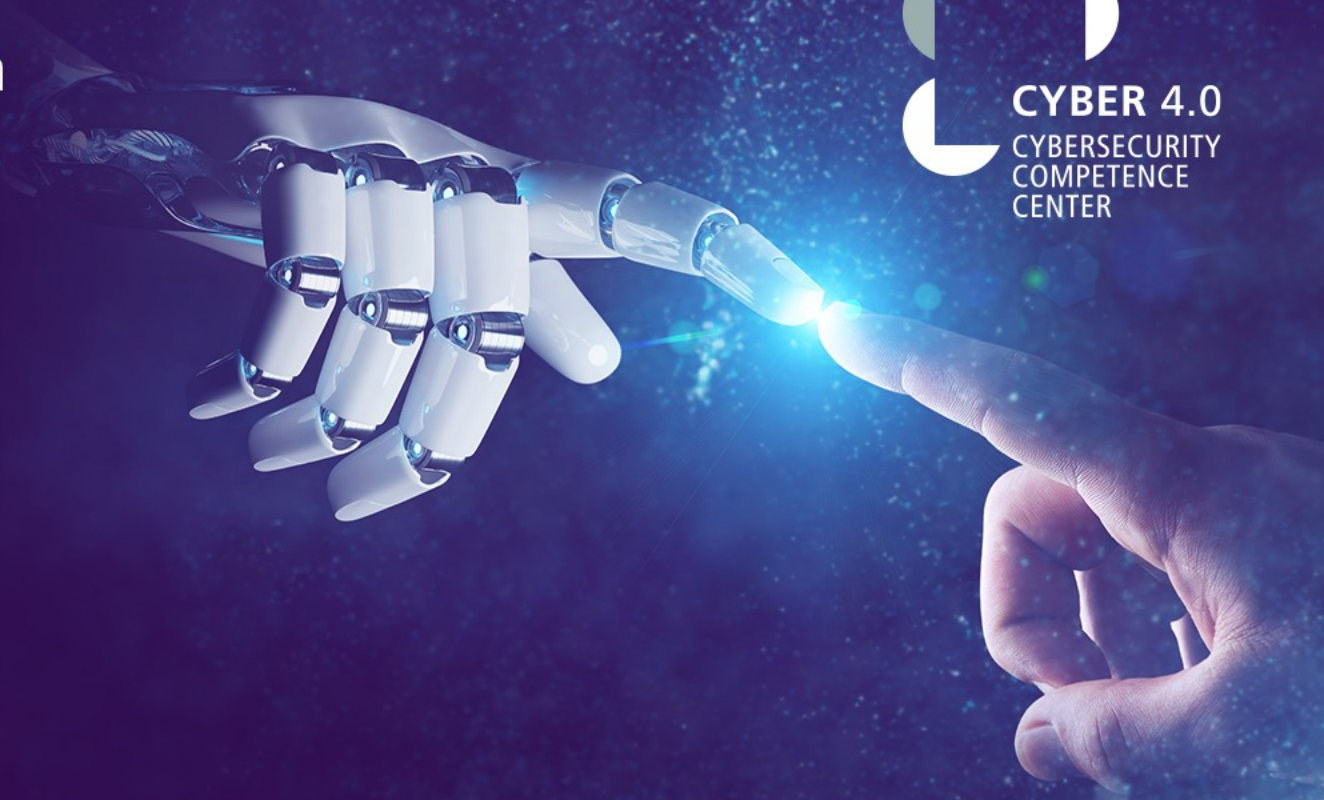
Approcci innovativi alla formazione aziendale


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06
Klossner

FORUM 2024
CYBER 4.0

The Dome LUISS Roma
3-4 Giugno 2024

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER



Antonio Capobianco

a.capobianco@fatainformatica.com

Grazie per l’attenzione

FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Interviene:

Alessio Aceti

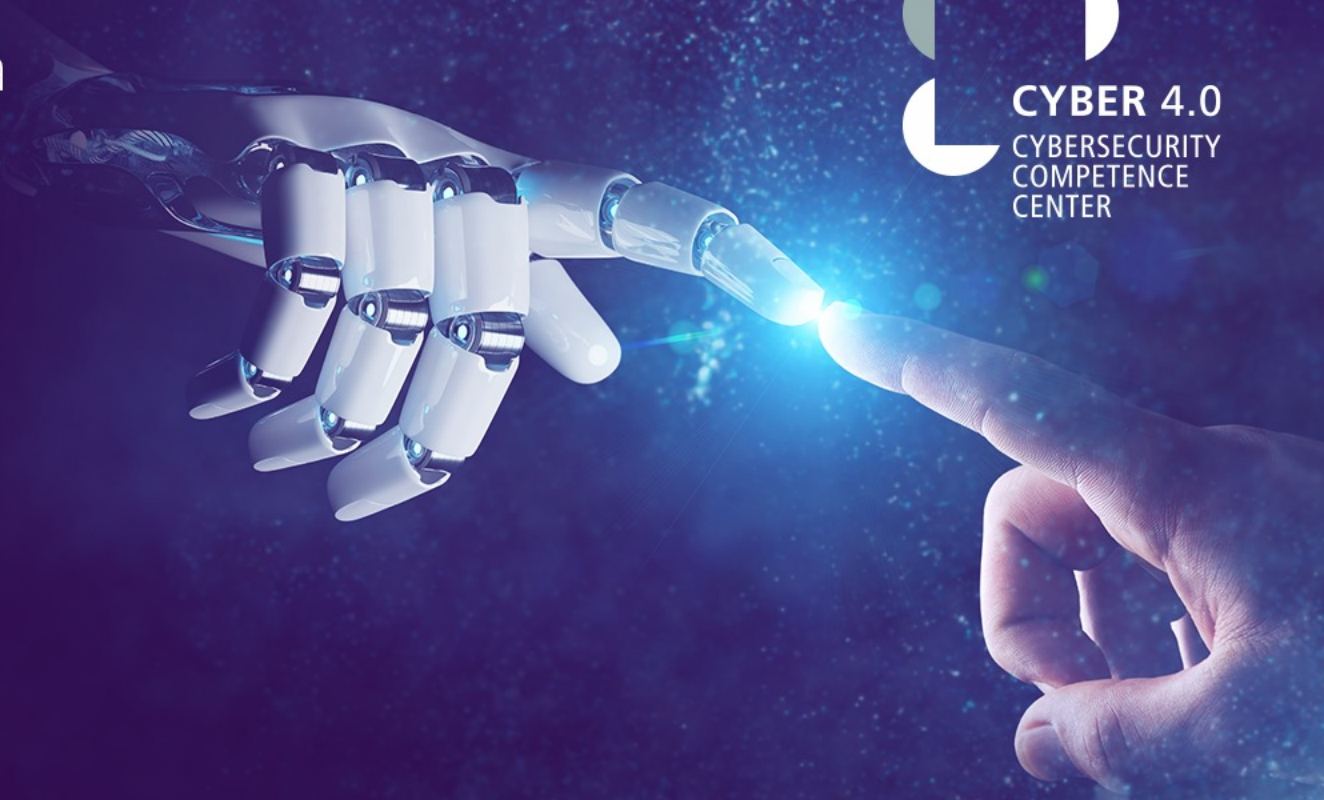
Chief Executive Officer, Hwg Sababa

Approcci innovativi alla formazione aziendale

FORUM 2024
CYBER 4.0

The Dome LUISS Roma
3-4 Giugno 2024

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER



Alessio Aceti

alessio.aceti@hwgsababa.com

Grazie per l’attenzione

FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Interviene:

Thomas Mascioli Colavecchi

Ciso, Polo Strategico Nazionale

Shared responsibilities

Polo Strategico Nazionale per una responsabilità condivisa della sicurezza

Chi siamo

Polo Strategico Nazionale

a seguito dell'aggiudicazione di gara e firma della Convenzione con il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri, si impegna a erogare a ciascuna amministrazione aderente servizi cloud che possano beneficiare delle più alte garanzie di affidabilità e resilienza.

È una società di scopo dedicata al progetto e caratterizzata da specifici elementi di **autonomia e sovranità**, al fine di garantire e **assicurare riservatezza e disponibilità di dati e** servizi della Pubblica Amministrazione, inclusi quelli «Strategici» la cui compromissione può avere un impatto sulla sicurezza nazionale..

La solidità tecnica e finanziaria dell'iniziativa è garantita dalle **expertise dei soci**:

TIM, primo operatore di tlc italiano, che grazie a tecnologie e **servizi innovativi nel Cloud, nell'IoT e nella cybersecurity** guida la transizione digitale in Italia;

Leonardo, azienda globale ad alta tecnologia nell'Aerospazio, Difesa, Sicurezza e principale azienda industriale italiana, **leader nel campo della sicurezza** e resilienza delle infrastrutture digitali;

Cassa Depositi e Prestiti Equity, in qualità di socio finanziario e **investitore istituzionale** a sostegno dello sviluppo in settori chiave per il Paese;

Sogei, partner primario della PA centrale nei processi di digital transformation e gestione delle infrastrutture tecnologiche strategiche per il Paese, fornisce **servizi di business culture enablement e formazione** favorendo la crescita e le competenze della PA.

38

Polo Strategico Nazionale si inserisce in un **piano complessivo di trasformazione digitale della PA**, realizzato e gestito dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri e dall'Agenzia per la Cybersicurezza Nazionale.

Vision

Abilitare l'**innovazione** e la **trasformazione digitale** italiana attraverso la **gestione sicura dei dati** e dei servizi della Pubblica Amministrazione

Valori

Mission

Creare un'infrastruttura in cloud tecnologicamente innovativa, per garantire la **sicurezza e la sostenibilità economica e ambientale,** nella gestione di dati e applicazioni della PA italiana

Strategia Cloud Italia e principio Cloud First

STRATEGIA CLOUD ITALIA

1. **Classificazione di dati e servizi**
2. **Qualificazione dei servizi cloud**
3. **Istituzione del Polo Strategico Nazionale**

POLICY “CLOUD FIRST“

Tecnologie e infrastrutture Cloud

40

Avanzamento Polo Strategico Nazionale

- **77** Grandi Amministrazioni Centrali (tra cui Interno, Lavoro, AgID, Presidenza del Consiglio dei Ministri)
- **105** Prefetture
- Oltre **130** Aziende Sanitarie Locali e Aziende Ospedaliere
- Oltre **80** PAL tra le quali più di 50 Comuni e 5 Città metropolitane

286

Contratti sottoscritti con le PA

312

PA aderenti agli avvisi PNRR*

41

Tecnologia per la sicurezza della PA

Il cardine di Polo Strategico Nazionale è un'infrastruttura in linea con i più elevati standard tecnologici, con logiche integrate di funzionamento per garantire affidabilità, resilienza e disaster recovery.

- 4 data center in doppia region, Lombardia e Lazio
- Connettività intra-region 100 GB
- Sicurezza fisica dei data center
- Security Operation Center (SOC) per la cyber security
- Computer Emergency Response Team (CERT)

42

Sicurezza certificata e qualificata

Qualifiche ACN

(Decreto direttoriale n. 29 del 02/01/2023, requisiti di cui all'allegato 1 della determina n. 307 del 18 gennaio 2022)

- QI4 alla infrastruttura "'Infrastruttura Cloud PSN"
- QC4 al servizio IaaS "IaaS Private PSN"
- QC4 al servizio IaaS "'IaaS Shared PSN"
- QC4 al servizio IaaS \'CaaS PSN"
- QC4 al servizio PaaS "'DRaaS PSN"
- QC4 al servizio PaaS "BaaS PSN"
- QC4 al servizio PaaS "AI PSN"
- QC4 al servizio PaaS "BigData PSN"
- QC4 al servizio PaaS "PaaS IAM PSN"
- QC4 al servizio PaaS "DBaaS PSN"

La sicurezza dell'infrastruttura e dei servizi PSN è comprovata da numerose certificazioni e risponde ai massimi standard di sicurezza

- ISO/IEC 27001 Sistema di gestione della Sicurezza delle Informazioni
- ISO/IEC 22301 Business Continuity Management System
- ISO/IEC 9001 Quality Management System
- ISO/IEC 20000-1 Service Management
- CSA Star Cloud Security Alliance – Star – Level2

- ISO/IEC 27017 Sistema di gestione della Sicurezza delle Informazioni per i servizi nel Cloud
- ISO/IEC 27018 Sistema di gestione della Sicurezza delle Informazioni per i dati personali nei Servizi Cloud
- ISO/IEC 27035-1 e ISO/IEC 27035-2 Gestione degli incidenti di Sicurezza
- ISO/IEC 27701 Specifica delle Informazioni sulla Privacy
- ISO/IEC 29100 Privacy framework
- ISO 14001 Sistema di gestione ambientale
- ISO 14064:2018 Gestione, rendicontazione e verifica di dati ed informazioni riferiti ai GHG ISO 45001:2018 Sistema di gestione per la salute e sicurezza sul lavoro (SSL)
- ISO 37001:2016 Anti corruzione
- ISO 50001 Sistema di gestione dell'energia (SGE)
- ANSI/TIA-942 Rating 3/4 - Leed Gold Standard per affidabilità Datacenter
- ISO/IEC TS 22237 Data center facilities and infrastructures

43

Polo Strategico Nazionale

CYBERSECURITY

Shared responsibilities: Polo Strategico Nazionale per una responsabilità condivisa della sicurezza

Shared Security Responsability Model come strumento di awareness

Lo Shared Security Responsibility Model (SSRM) è lo strumento previsto all’interno della Cloud Control Matrix – dominio «Supply Chain Management, Trasparency and Accountability», attraverso il quale Cloud Service Provider e Cloud Service Customer definiscono e regolano in che modo la responsabilità e l’accountability per la sicurezza dei dati e delle risorse venga suddivisa nell’ambito di uno specifico servizio Cloud.

Al fine di **consentire la trasparenza** e **rafforzare la sensibilizzazione alla sicurezza** da parte dei propri clienti, ognuno dei servizi Cloud venduti alle P.A. deve disporre di una **matrice di responsabilità** all’interno della quale vengono identificate le **accountability per l’applicazione dei singoli controlli di sicurezza**, indicando:

RESPONSABILITÀ DEL PROVIDER

In che misura il PSN è accountable dell’applicazione di ogni controllo, **nonché eventuali terze parti (soci gestori) responsabili** della concreta applicazione nelle attività operative.

RESPONSABILITA’ DEL CLIENTE

In che misura la Pubblica Amministrazione è accountable dell’applicazione di ogni controllo, nonché **linee guida per la corretta applicazione** dei controlli di propria competenza.

Il provider è responsabile della sicurezza «del» Cloud,

il cliente è responsabile della sicurezza «nel» Cloud.

45

Cosa contengono le Matrici di Responsabilità Condivisa della Sicurezza?

Le Matrici di Responsabilità Condivisa della Sicurezza vengono strutturate sulla base del framework di controlli specifico per servizi cloud, definito nella **Cloud Control Matrix**, all’interno della quale sono previsti **197 controlli di sicurezza** suddivisi in **17 domini** di diversa natura:

GOVERNANCE

- GRC,
- Audit,
- HR Security,
- Supply Chain,
- Data Security & Privacy

DI PROCESSO

- IAM,
- Change Management,
- Vulnerability Management,
- Endpoint Management,
- Business Continuity,
- Log collecting
- Incident Management

TECNOLOGICI

- Crittografia,
- Data Center Security,
- Virtualization Securiy,
- Portabilità ed Interoperabilità

Ognuno dei domini è composto da una serie di **controlli**, per ognuno dei quali viene indicato:

Applicazione	Indica se lo specifico controllo è applicato o non applicato.
Responsabilità	Identifica se la responsabilità è solo di PSN (CSP-owned), se è della PA (CSC-owned), se è condiviso fra PSN e PA (Shared CSP and CSC) o se è affidato ad una terza parte (3rd-party outsourced)
Implementazione PSN	Identifica la quota di responsabilità in capo a PSN, indicando eventualmente le modalità di implementazione.
Linee Guida PA	Indica la quota di responsabilità in capo alla Pubblica Amministrazione, con l’inserimento di specifiche linee guida di implementazione contenenti delle best practices finalizzate a fornire guidance alla PA nell’applicazione della componente di controllo di sicurezza di propria competenza.

46

I contributi alla sensibilizzazione sulla sicurezza verso la PA

Ognuno dei servizi Cloud venduti alle P.A. dispone di una matrice di responsabilità all’interno della quale vengono identificati puntualmente gli ambiti di competenza sia di PSN che della P.A. Cliente, utilizzando i seguenti strumenti di comunicazione:

Scheda di Servizio

Documento riassuntivo in formula Executive summary:

- Descrizione della **metodologia** utilizzata;
- Descrizione High-Level delle **responsabilità per ogni area di sicurezza**;
- **Riepilogo finale** delle aree di responsabilità di PSN e della Pubblica Amministrazione Cliente.

Questionario (CAIQ) di Servizio*

Documento di dettaglio destinato alle linee tecniche:

- Descrizione **controllo per controllo**;
- Descrizione delle **attività svolte da PSN** in quanto provider;
- Descrizione delle **attività attese da parte della PA** cliente;
- **Linee guida orientative** fornite alla PA per la realizzazione delle componenti di propria competenza.

La documentazione prodotta in ambito è oggetto di condivisione sia con le **Pubbliche Amministrazioni Clienti**, sia nel **Registro Pubblico CSA**.

PSN ha pubblicato le Schede di Servizio all’interno del proprio sito istituzionale.

47 * CAIQ: Consensus Assessment Initative Questionnaire, ossia un questionario di controlli di Cloud Security che ne analizza, per singolo controllo, le modalità di implementazione.

Un esempio di linea guida: estratto dalla Scheda per IaaS

Audit & Assurance

Il dominio Audit e Assurance (A&A) è progettato per supportare il CSP e il CSC nella definizione e attuazione di un **processo di gestione dell’audit** finalizzato a: la pianificazione dell'audit, l'analisi dei rischi, la valutazione dei controlli di sicurezza, la conclusione, la correzione, la generazione dei report e le revisioni di report precedenti e delle relative evidenze a sostegno.

Responsabilità Pubblica Amministrazione (CSC)

E’ responsabilità del cliente svolgere attività di **audit ed assurance sulla base delle proprie esigenze di compliance ed ai controlli di propria necessità, sugli ambienti virtuali costruiti sull’infrastruttura fornita dal PSN**.

La PA dovrà dunque elaborare le proprie politiche e procedure formali per la determinazione dello scope di analisi, degli standard rispetto ai quali svolgere le verifiche, stabilire le proprie metodologie di audit e di verifica, sulla base della propria valutazione dei rischi e delle proprie esigenze di compliance.

Responsabilità PSN (CSP)

PSN, quale organo responsabile del coordinamento e corretto funzionamento dei servizi, si occupa di svolgere attività di **audit e assurance sulle componenti di propria competenza del servizio**, assicurandone la conformità ai principali standard di settore (ISO/IEC 27001, ISO 9001, ISO/IEC 20000-1, ISO 22301 e Cloud Control Matrix).

L’attività si concentra sulla **componente infrastrutturale**, la quale tiene conto degli ambenti fisici, del network e dell’hardware utilizzati, sino alla **configurazione iniziale degli strumenti di virtualizzazione**.

SERVICE LAYERS

- DATA
- APPLICATION
- RUNTIMES
- MIDDLEWARE
- OS (Operating System)
- HYPERVISOR
- HARDWARE
- NETWORK
- PHYSICAL

Legenda Responsabilità

= P.A.

= PSN

= Non Applicabile

Una rubrica per diffondere cultura e consapevolezza

La **rubrica social** Shared Responsibilities nasce dalla sinergia tra l’Area **Information Security**, l’Area **Comunicazione** e il team social e digital di Polo Strategico Nazionale, allo scopo di diffondere la cultura sulla cybersicurezza e di sottolineare l’importanza della condivisione delle responsabilità tra Polo Strategico Nazionale, in qualità di cloud service provider, e Pubblica Amministrazione. Due le fasi:

- una **fase introduttiva** con i post sui principi del modello di responsabilità condivisa tra PSN e PA (target: generalista e PA interessate)
- una **fase di approfondimento** in cui l’utente è invitato a scoprire nel dettaglio gli aspetti più tecnici delle matrici presenti nelle schede di servizio (target: B2B, esperti di settore e PA interessate).

Una chiara identità grafica rende **i contenuti immediatamente riconoscibili**: la scelta del **logo dei due lucchetti,** che completa lo stile distintivo della campagna, serve a ribadire Il concetto che solo attraverso la condivisione di responsabilità tra PSN e PA si possono raggiungere i migliori livelli di securizzazione per l’infrastruttura, i dati e gli applicativi. I contenuti prodotti dialogano con la **sezione ad hoc del sito internet** che reca materiali di approfondimento e schede di servizio.

49

I primi contenuti

3 post

1 newsletter dedicata

10.936 visualizzazioni totali*

419 interazioni*

(tra commenti, diffusioni, reazioni e clic)

L’attuale piano editoriale prevede una serie di contenuti legati al modello SSRM e alla certificazione CSA Star 2 Gold

- **le matrici di responsabilità**: 5 contenuti su come si declina la Shared Responsibility in base ai servizi cloud offerti da Polo Strategico Nazionale
- **il glossario**: le parole di uso comune
- **le FAQ**: le risposte alla domande più frequenti in ottica di supporto alla Pubblica Amministrazione per implementare la sicurezza all’interno del cloud

* dati cumulativi sui profili X e Linkedin dalla data di pubblicazione dei post fino al 28 maggio

50

FORUM 2024
CYBER 4.0

The Dome LUISS Roma
3-4 Giugno 2024

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Thomas Mascioli Colavecchi

thomas.mascioli@polostrategiconazionale.it

Grazie per l’attenzione