FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Con il patrocinio di:

Sotto l'alto patrocinio del Parlamento europeo

Ministero delle Imprese e del Made in Italy

Finanziato dall'Unione europea NextGenerationEU

Cyber 4.0

Competenze, Capacità, Collaborazione, Concretezza

Matteo Lucchetti

Direttore Operativo, Cyber 4.0

Matteo.Lucchetti@cyber40.it

Hosted by:

ROMA TRE UNIVERSITÀ DEGLI STUDI

Cyber 4.0

Centro di Competenza Nazionale sulla Cybersecurity

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

- Partenariato pubblico-privato, 50+ soci, promosso e co-finanziato dal MIMIT
- Centro di Trasferimento Tecnologico nazionale e soggetto attuatore PNRR

- Infrastrutture, piattaforme e strumenti per le imprese – T4 Lab
- Innovazione, ricerca industriale, sviluppo sperimentale
- Servizi incentivati per transizione digitale sicura
- Formazione, awareness e capacity building
- Rete di collaborazioni nazionali e internazionali

Cyber 4.0 – Centro di Trasferimento Tecnologico PNRR

Next Gen EU

Kick-off 10 marzo 2023/ deadline 30 aprile 2026

Totale incentivi erogati attraverso a fine PNRR: 19,7 Mln EUR

LINEA A **PROGETTI INFRASTRUTTURALI**	Progetti per il miglioramento/ rafforzamento/ adeguamento delle infrastrutture proprie del Centro per l'erogazione di servizi innovativi alle imprese	**3,5 Mln EUR**
LINEA B1 **BANDI DI INNOVAZIONE**	Bandi di trasferimento tecnologico, per cofinanziamento iniziative di innovazione ad alto livello di maturità e supporto alla messa in produzione di prototipi avanzati	**5,1 Mln EUR**
LINEA B2 **SERVIZI INCENTIVATI**	Servizi di supporto alla transizione digitale sicura di imprese, incentivi nella forma di sconti in fattura a intensità variabile sulla base della dimensione aziendale	**4 + 5,1 Mln EUR**
SoE NEST **SERVIZI INCENTIVATI**	Servizi di supporto alla transizione digitale sicura di PMI e PA, incentivi nella forma di sconti in fattura a intensità variabile sulla base della dimensione aziendale	**2 Mln EUR**

Centro di Trasferimento Tecnologico PNRR

Infrastrutture – 3,5 M

Servizi evoluti per imprese, focus PMI

- Piattaforma servizi cloud per PMI/ SOC as a service – NETGROUP
- Piattaforma per rilevazione e contrasto fonti di disinformazione – S&A

Rete di laboratori per test e valutazioni di sicurezza

- Cyber SHOT Lab/ OT security test lab, focus healthcare – UCBM
- Rete privata 5G per sperimentazioni e test tecnologici presso T4 Demo Lab – TIM

Formazione avanzata e simulazioni immersive

- Cyber Range con digital twin di sistemi cyber-fisici – CY4GATE

Stato di avanzamento – 54%

Proposte in fase di finalizzazione

BV Tech, DiGi Academy, Università di Cassino e del Lazio Meridionale, Almaviva, Luiss, HWG Sababa, Sapienza Università di Roma, Università Tor Vergata, Università Roma Tre, Ancharia

Centro di Trasferimento Tecnologico PNRR

Progetti di innovazione – 5,1 M

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Bando 1/ 2023 – 2,4 Mln EUR, 9 progetti

CORE — **SATML-B** *Datrix*
Sicurezza degli algoritmi di **Artificial Intelligence e Machine Learning** contro adversarial attacks, data sanitization & anonymization

HEALTH — **WISEPACK** *Radio6ense*
Monitoraggio e protezione delle confezioni dei farmaci tramite **integrazione IoT e sistemi di Intelligenza Artificiali**

AUTO — **CyberGuardEV** *TME*
Dispositivo elettronico innovativo in grado di rilevare e di proteggere da attacchi side-channel le **stazioni di ricarica per veicoli elettrici**

SPACE — **Biosat Marketplace** *IPTSat*
Marketplace con servizi predefiniti per fruizione sicura di **dati provenienti dall'osservazione della Terra** (missioni ESA e costellazione IRIDE)

CORE — **ARGO** *Sistemi & Automazione*
Cyber Threat Intelligence (CTI) e supporto decisionale con Ricerca su Grafi per scoperta dati dispersi su fonti Open di tipo cyber

HEALTH — **Health-e-Data** *Moveax*
Gestione, scambio e utilizzo sicuro di **dati sanitari** – con particolare attenzione ai dati generati in **telemedicina e telemonitoraggio**

AUTO — **CYBORG** *Radiolabs*
Protezione passiva da attacchi cyber in ambiente intra-veicolare con autenticazione dati a rilevanza forense basata su **blockchain**

CORE — **ESII** *Sharelock*
Integrazione di un **Large Language Model** (LLM) locale, addestrato per investigazioni su alert di sicurezza, singole o multiple anomalie

HEALTH — **Here-HomeRehab** *Aenduo*
Riabilitazione respiratoria domiciliare attraverso dispositivo medico software (APP mobile + kit di attrezzi per gli esercizi di fisioterapia)

Bando 1/ 2024 – 2,7 Mln EUR, 11 progetti

CORE — **BASE** *Keyless Technologies*
Metodo di **autenticazione e firma digitale** robusto e user-friendly utilizzando tecniche avanzate come ad es. zero-knowledge proof

HEALTH — **SafeBot4Twin** *RBF Morph*
Chatbot basato LLM per controllare Medical Digital Twin costruiti mediante dati clinici e garantire la sicurezza delle informazioni sensibili sottostanti necessarie

AUTO — **MACS 2.0** *Tomware*
Estende il primo progetto MACS, ampliando le funzionalità di **diagnostica sullo spettro radio** e vari altre funzionalità

SPACE — **ETERE** *Qascom*
Tecnologie avanzate per **monitoraggio di interferenze a radiofrequenza** con soluzione per l'analisi delle bande maggiormente utilizzate nei servizi satellitari

CORE — **Q-RoT** *Random Power*
Architettura di **Root-of-Trust** in grado di generare e custodire l'identità univoca dei dispositivi e generare e gestire chiavi crittografiche e di autenticazione

HEALTH — **ZOOMel** *Fondazione FORMIT*
Supporto alla **diagnostica del melanoma** con Deep Learning per l'analisi dell'immagine dermoscopica (DIA)

AUTO — **SENTINELLA** *NETCARING*
Sicurezza della persona in ambito automotive e per chi utilizza macchine operatrici. Il sistema impl strumenti di analisi del comportamento del conducente

SPACE — **HESI** *DIGIMAT*
Sistema software per eseguire operazioni mantenendo sempre i dati in forma cifrata progettato per la gestione e l'elaborazione di **immagini satellitari SAR**

CORE — **DCS** *Teleconsys*
Proteggere i dati aziendali da attacchi ransomware attraverso l'integrazione delle tecnologie **IOTA** (Internet of Things Application)

HEALTH — **SMARTCARE** *ESA System*
Piattaforma tecnologica avanzata per la telemedicina, focalizzata sull'**integrazione di dispositivi medici**, sulla facilità d'uso e la sicurezza dei dati

AUTO — **CYBERBOSS** *MAESTRALE IT*
Attraverso le identità biometrica multifattore, il sistema vuole rilevare e filtrare gli attacchi informatici verso gli IVI (**In Vehicle Infotainment**)

Stato di avanzamento – 100%

Centro di Trasferimento Tecnologico PNRR

Servizi (9,1 M) e Polo NEST (2 M)

Disponibilità iniziale:

4 M EUR (B2) + 2 M EUR (NEST)

Rifinanziamento 2025:

+ 5,1 M EUR (B2)

- Sconto in fattura direttamente applicato all'azienda servita
- Controlli di ammissibilità a carico del Centro di Competenza
- Erogazione servizi a carico di soci individuati da Cyber 4.0

Servizi e incentivi per dimensione	P	M	G
Audit tecnico, Valutazione maturità	90%	80%	40%
Prova prima dell'investimento	90%	75%	30%
Formazione (fino a 24h)	90%	75%	50%
Formazione (oltre le 24h)	70%	60%	40%
Consulenza accesso ai finanziamenti	70%	60%	50%
Cons. innovazione di processo e di prodotto	75%	70%	50%
Consulenza protezione proprietà intellettuale	70%	60%	50%
Progettazione intervento di innovazione	50%	40%	30%

Stato di avanzamento – 61%

4,3 M EUR

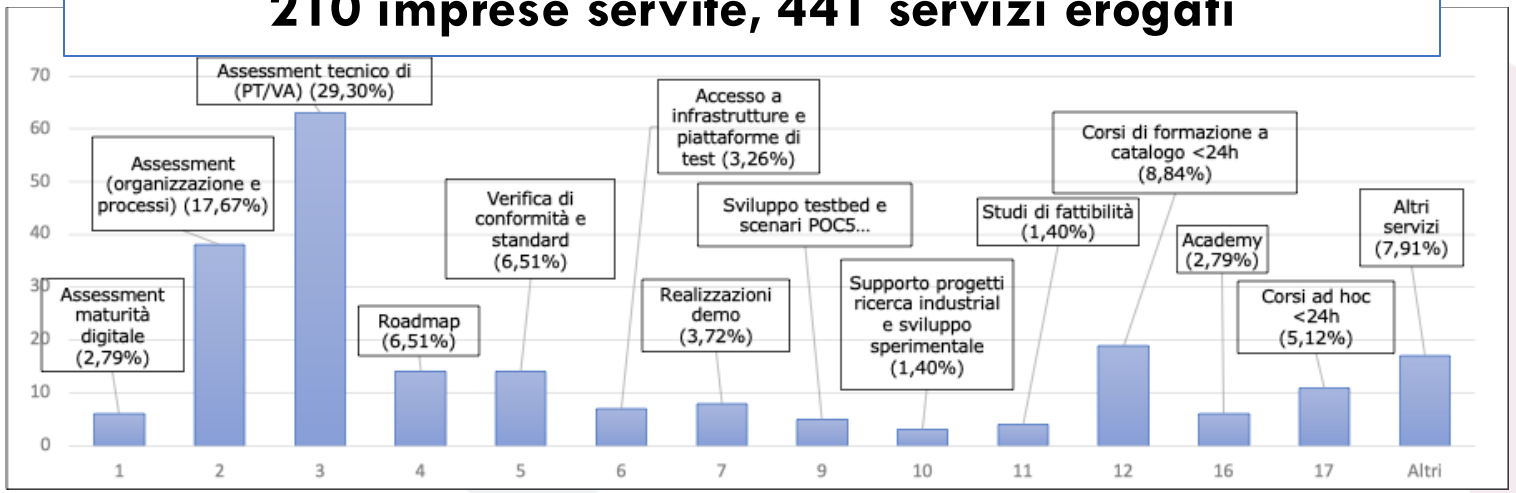
Incentivi ancora disponibili

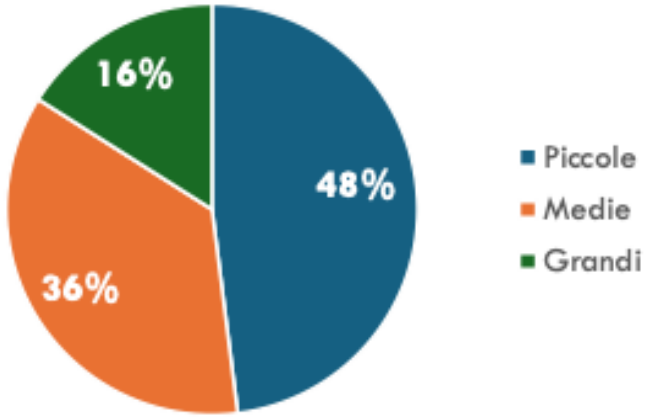
Capacità

I servizi di Cyber 4.0, un primo bilancio

- Servizi maggiormente richiesti: audit tecnico, assessment organizzativo, formazione, awareness aziendale, consulenza progetti di innovazione
  - **Interventi puntuali ancora predominanti rispetto a interventi strutturali**
- Consapevolezza in crescita e spinta dell'evoluzione del quadro normativo in materia di cybersecurity
  - **Adeguamenti NIS 2, GDPR, DORA**
- Entità media dell'aiuto pari al 75%
  - **Le imprese che maggiormente beneficiano degli incentivi sono imprese piccole e medie**

210 imprese servite, 441 servizi erogati





Preallocazioni su nuove commesse da finalizzare pari ad ulteriori 1,8 M EUR

Capacità

Confindustria e Camere di Commercio per MPMI

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

SISTEMA CONFINDUSTRIA

Cybersecurity Assessment PMI

Realizzazione di un assessment cyber per PMI a livello nazionale e sviluppo di una piattaforma di raccolta dati

DIH Digital Innovation Hub

L'analisi prevede:

- l'individuazione dello specifico **Fattore di Rischio** di cyber-esposizione dell'azienda;
- l'analisi dell'effettivo **Livello di cyber-esposizione,** con la valorizzazione del Digital Cyber Score in una scala da 1 a 5;
- la definizione e restituzione all'azienda di una roadmap con le **possibili remediation,** Quick Win e Next Steps.

SISTEMA CAMERE DI COMMERCIO

PID - Cybercheck

Realizzazione di un assessment cyber per il Punti di Impresa Digitale delle Camere di Commercio

punto impresa digitale

Test di autovalutazione rapido e disponibile online per guidare l'impresa, attraverso alcune domande mirate, verso **una primissima valutazione del livello di rischio di un attacco informatico.** Il test non dà indicazione circa i presidi da mettere in atto per proteggere l'impresa da attacchi cyber, ma permette di individuare gli eventuali rischi a cui l'azienda può andare incontro

Competenze

Webinar MIMIT Cyber 4.0

Ministero delle Imprese e del Made in Italy

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Ciclo di webinar co-organizzato da Cyber 4.0, rivolto a lavoratori pubblici e privati, per aggiornamento professionale sul tema della sicurezza informatica.

Il ciclo di webinar si inserisce all'interno degli obiettivi del MIMIT nel contesto della Strategia di Cybersicurezza Nazionale.

2024

- **Automotive** e cybersecurity: vulnerabilità, sistemi di protezione e quadro normative
- **Cybersecurity e AI** – Il Quadro regolamentare in materia di AI – Italia, EU e mondo a confront
- **Cybersecurity e AI** – Applicazioni dell'AI – Aspetti di sicurezza dei dati e degli algoritmi
- **Cybersecurity e AI** – AI e cybercrime – Minacce reali e potenziamento delle difese
- Il **Cyber Resilience Act**: impatti e implementazione nell'industria italiana
- La **Direttiva NIS 2** – Il recepimento in Italia, requisiti e tempistiche
- La cybersecurity nel settore sanità: qual è lo stato di salute cyber?

Media di 350 partecipanti a incontro

2025

12/03/25 – I **cavi sottomarini** e la rilevanza strategica delle infrastrutture critiche di connettività

10/04/25 – La sfida dei **data center**: Standard, Normative, Investimenti e Nuove Tecnologie

13/05/25 – Cybersecurity e **comunicazioni satellitari**: rischi e opportunità

24/06/25 – Quantum & Post-Quantum revolution: stato dell'arte e previsioni in ambito cyber

16/10/25 – Un anno dall'adozione della **NIS 2**: risultati, impatto e prospettive evolutive

19/11/25 – **Intelligenza Artificiale**, LLM e rischio cibernetico tra Modelli, Brevetti, Applicazioni, Chip e Robotica

Media di 500 partecipanti a incontro

Competenze

Formazione per la PA

Ministero delle Imprese e del Made in Italy

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

- **Formazione per i livelli apicali**, nel quadro della Strategia Nazionale di Cybersecurity del Ministero delle Imprese e del Made in Italy
  - Nuova edizione 2025 – Focus su Ai e tecnologie emergenti, TTX, Case Study

- **Formazione mirata** per dirigenti di prima e seconda fascia, contesto normativo, responsabilità e sanzioni, gestione del rischio cyber

- **Formazione specialistica** per team tecnici: risposta agli incidenti, gestione dei sistemi di sicurezza delle informazioni, framework e controlli

- **Awareness generalizzata** su temi di cybersecurity per i dipendenti, gamification, cyber hygiene, escape room

Capacità

Le Case delle Tecnologie Emergenti

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Ministero delle Imprese e del Made in Italy

CAGLIARI DIGITAL LAB

Valore totale progetto: € 12.550.000

Durata: 30 mesi – **Decorrenza:** 02/02/2023

- **Laboratorio Tecnologie Quantistiche - Quantum Communication**
- Realizzazione di una **Escape Room di cybersecurity sul tema tecnologie emergenti** fruibile dal pubblico
- **Monitoraggio e sensing** - Assesment di security (VA/PT) sulla piattaforma Xplore (piattaforma di gestione sensori smart in campo)
- **Seminari e workshop** - Organizzazione di corsi sui rischi di natura cyber derivanti dall'uso delle tecnologie emergenti e produzione di 10 videopillole sulle tecnologie emergenti

PESARO CTE SQUARE

Valore totale progetto: € 10.977.000

Durata: 30 mesi – **Decorrenza:** 02/02/2023

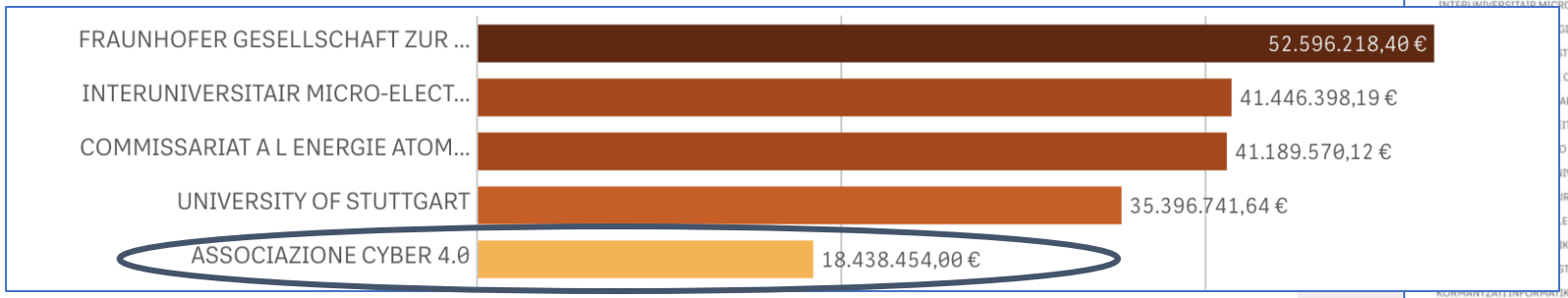
- **Proof of Attendance** - Gestione degli eventi con certificazione blockchain della presenza

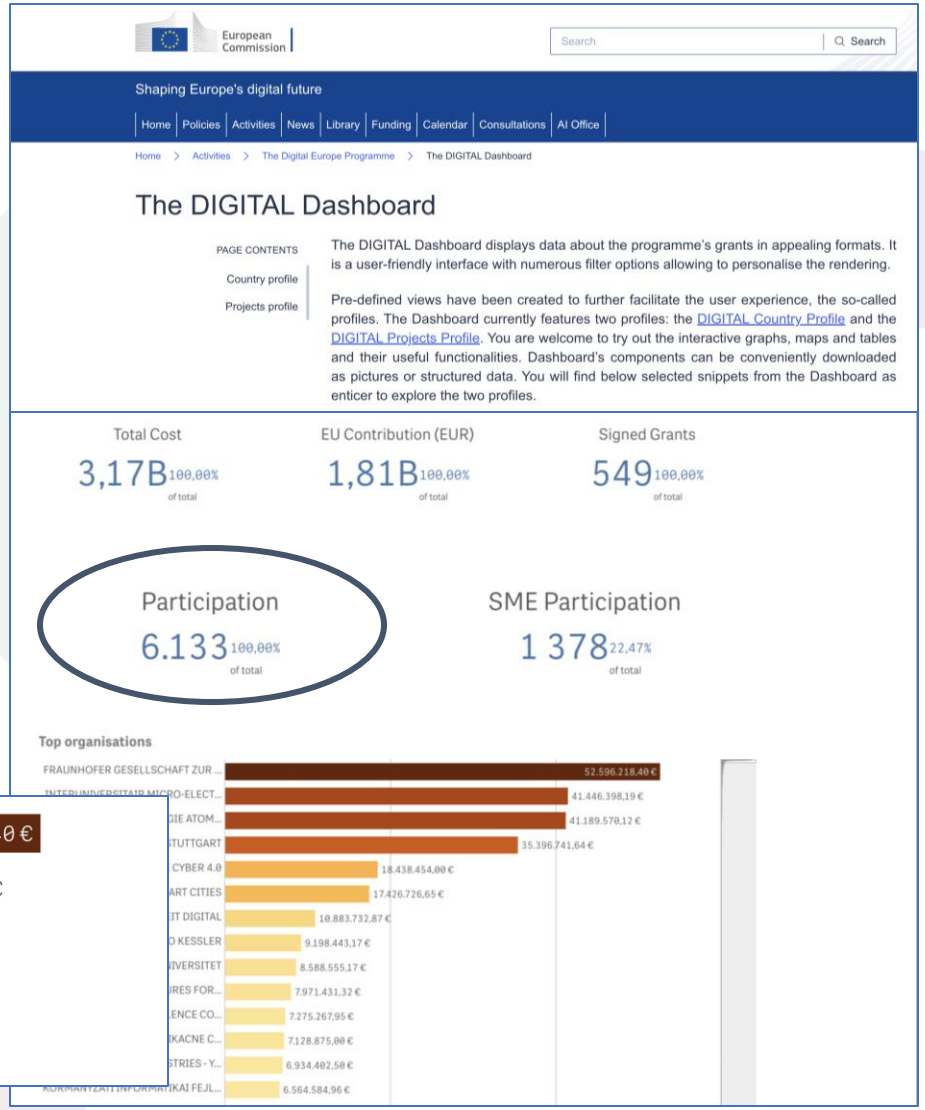
Capacities and cooperation

EU cyber capacity building

SECURE
Cyber Resilience for SMEs

- SECURE Project – 21 Mln EUR, 2025-2027
- Supporting SMEs to comply with the Cyber Resilience Act
- FSTP and Knowledge portal
- 14 partners, 7 Member States
- Coordination ACN (National Cybersecurity Agency)
- Cyber 4.0 is technical reference partner – **18 Mln EUR funding**





Collaborazioni

Il network internazionale

- **Membri dell'ecosistema nazionale di cyber capacity building (MAECI)**
- **Partner del GFCE (Global Forum for Cyber Expertise)**
- **Ad-Hoc Working Group on the European Cybersecurity Skills Framework di ENISA**
- **Membri dello Stakeholder Group di EU CyberNet**
- **Contributing Member del Latin America and Caribbean Cyber Competence Center (LAC4)**
- **AI Hub for Sustainable Development/ Piano Mattei**
- Contributors dello EU AI Office per la definizione di uno European AI Code of Practice
- Esperti a supporto dell'iniziativa EU-LAC Digital Alliance
- Membri di European Cyber Security Organization (ECSO)
- Membri di Global Cyber Alliance

Capacities

International cyber capacity building

Revision of the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP)

- To establish a practical, harmonised standard of practices, systems and expertise to address cyber security vulnerabilities in the Region, to which each Caribbean country could aspire in the short and medium terms
- To build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of Cybercrime and possible linkages to other forms of criminal activity

Public Awareness, Education and Advocacy;
Policy, Institutional and Regulatory Frameworks;
Capability Development and Capacity Building;
Enhancing and Harmonising Technical Standards and Infrastructure;
Incident Management;
Regional and International Cooperation.

Strong focus on fostering PPP throughout the region and internationally

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

IMPACS – Implementation Agency for Crime and Security

Global Gateway

EU-LAC DIGITAL ALLIANCE POLICY DIALOGUES

EL PACCTO 2.0 EU-LAC Partnership on justice and security

Competeze e capacità

Cyber 4.0 per gli studenti

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CyberX Mind4Future 2024

452 iscritti, 60 finalisti, 10 vincitori, 10 tirocini attivati

Iniziativa di Leonardo, con Cyber 4.0

Coimvolte le 8 Università del Centro

Competenze e capacità

Cyber 4.0 per gli studenti

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

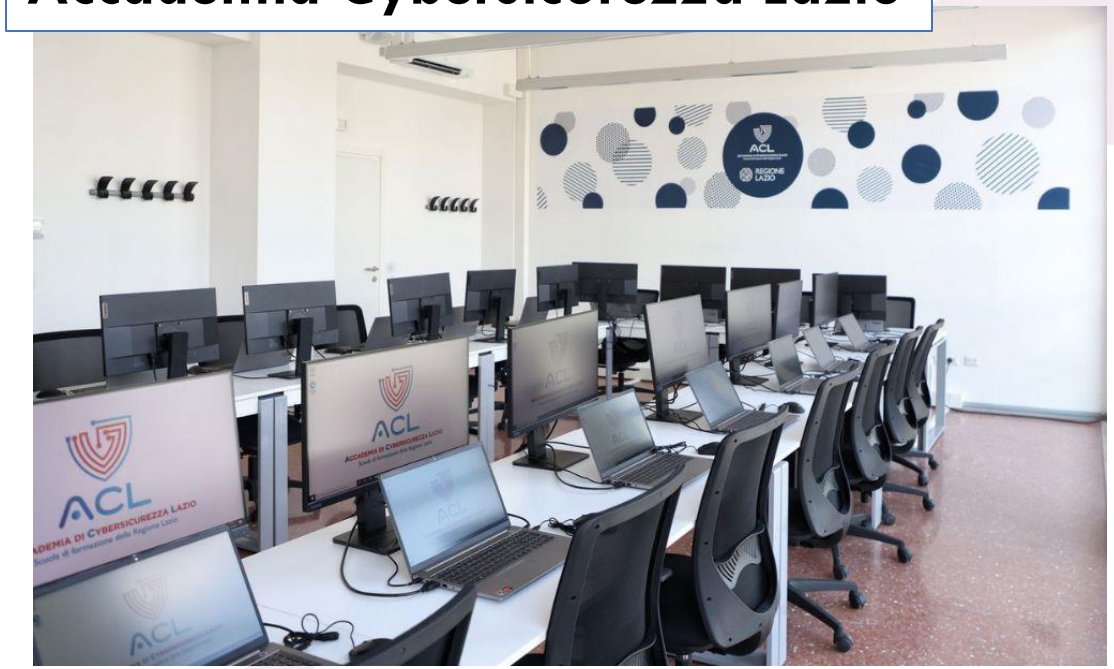
CyberX Mind4Future 2024

452 iscritti, 60 finalisti, 10 vincitori, 10 tirocini attivati

Iniziativa di Leonardo, con Cyber 4.0

Coimvolte le 8 Università del Centro

Accademia Cybersicurezza Lazio



Corsi Cybersecurity Technician, Cybersecurity Expert

Iniziativa di Regione Lazio con ACN, supporto Cyber 4.0

20 stage attivati presso imprese, anche in Cyber 4.0

Competenze e capacità

Cyber 4.0 per gli studenti

+5500
STUDENTI

+500
INSEGNANTI

+90
ISTITUTI CANDIDATI

40
ISTITUTI SELEZIONATI

+70
SESSIONI FORMATIVE

Call to action

Cyber 4.0 è punto d'incontro di

competenze di cyber sicurezza, capacità di innovazione,

reti di collaborazione e risultati concreti

Call to action

Cyber 4.0 è punto d'incontro di

competenze di cyber sicurezza, capacità di innovazione,

reti di collaborazione e risultati concreti

Unitevi ai nostri progetti

Call to action

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Cyber 4.0 è punto d'incontro di

competenze di cyber sicurezza, capacità di innovazione,

reti di collaborazione e risultati concreti

Unitevi ai nostri progetti

Portate le vostre idee

Call to action

Cyber 4.0 è punto d'incontro di

competenze di cyber sicurezza, capacità di innovazione,

reti di collaborazione e risultati concreti

Unitevi ai nostri progetti

Portate le vostre idee

Fate crescere la rete con noi

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Con il patrocinio di:

Sotto l'alto patrocinio del Parlamento europeo

Ministero delle Imprese e del Made in Italy

Finanziato dall'Unione europea NextGenerationEU

Grazie a tutti

Matteo Lucchetti

Direttore Operativo, Cyber 4.0

Matteo.Lucchetti@cyber40.it

Hosted by:

ROMA TRE UNIVERSITÀ DEGLI STUDI