



CYBER 4.0 – Competenze per l'innovazione

MATTEO LUCCHETTI

DIRETTORE OPERATIVO CYBER 4.0



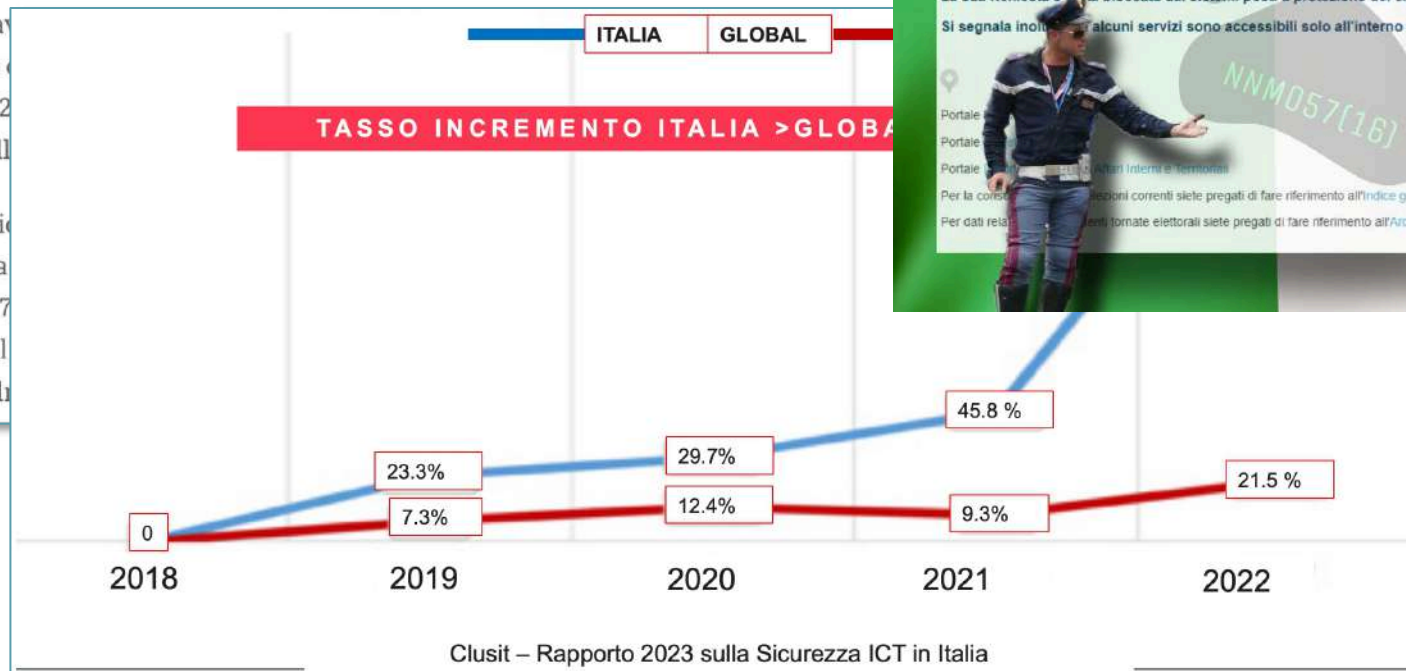
Lo scenario di cybersecurity – Minacce

Clusit: Italia nel mirino degli hacker; +169% gli attacchi nel 2022 rispetto al 2021. A livello mondiale la crescita è del 21%

DI REDAZIONE PUBBLICATO IL 7 MARZO 2023 NESSUN COMMENTO

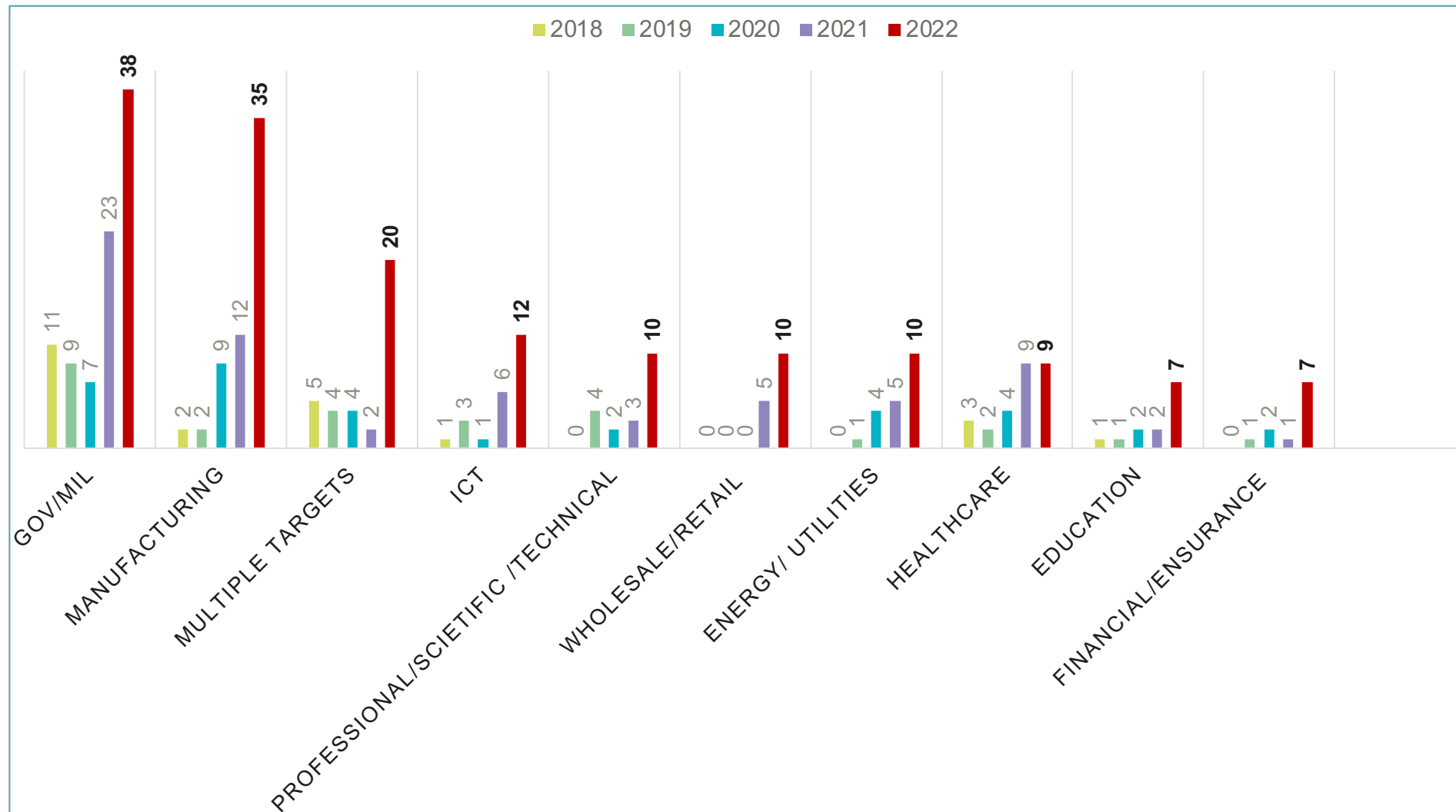
MILANO. Con 2.489 incidenti gravi l'anno peggiore da sempre per la...

Nel contesto delle crescenti tensioni combattuto ai confini dell'Europa...



Cybersecurity threat landscape

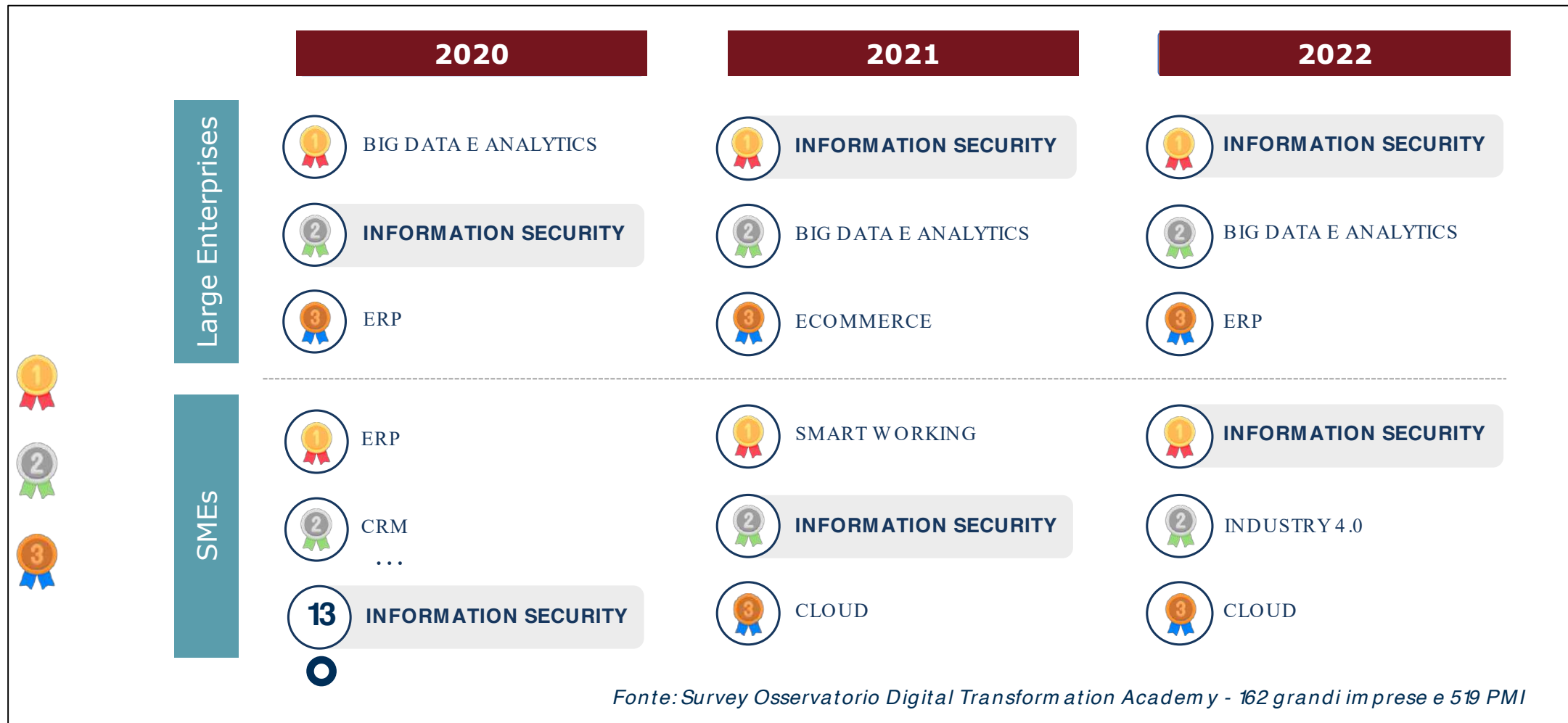
I settori più colpiti



I principali trend in corso

- **Contesto geopolitico** e aumento azioni collegate
- **Espansione della superficie di attacco**
 - Es. IoT/ OT, Firmware
- Maturità raggiunta da **nuovi paradigmi tecnologici**
 - Es. AI generativa a supporto di attacchi cyber
- **Contesto normativo** in forte evoluzione
 - UE – NIS 2, CRA, ...
 - Nazionale – Implementazione del PSNC, CVCN
 - Autonomia tecnologica
- **Supply chain**
 - Focus su rischio fornitori
 - Nuovo Codice Appalti
- **PMI e transizione digitale**
- **Crisi delle competenze cyber**
 - Coordinamento UE – es. Cybersecurity Skills Academy
 - Coordinamento nazionale – es. ITS, Accademie, Corsi universitari, PhD

Priorità di investimento per interventi di trasformazione digitale



Contesto nazionale e cybersecurity

- 4.4 Mln Imprese in Italia
 - 95.05% micro (<10 dipendenti)
 - 4.86% PMI (10-50 dipendenti) – 206.000 → 41% del fatturato totale, 33% impiegati totali
 - 0.09% grandi imprese (>50 impiegati)
- Dati recenti di una ricerca condotta su un campione significativo (10.000+)*:
 - 97% delle PMI ha adottato uno o più sistemi digitali, gestiti internamente
 - [e.g. email (90%), sito web (73%), BPM (61%), WiFi per esterni (35%), ecommerce (28%)]
 - **26% delle PMI italiane ha subito cyber attacchi nel 2022**
 - **52% of delle PMI ha allocato risorse nel 2023 per la protezione di dati e sistemi informativi, per una spesa media di 4.800 EUR, per un totale complessivo di più di 470Mln EUR** – Solo il 50% di loro ha già identificato anche il fornitore

* <https://www.cybersecitalia.it/le-pmi-italiane-pronte-ad-investire-470-milioni-di-euro-sulla-sicurezza-informatica-nel-2023-i-dati-di-confesercenti/23204/>

Contesto PMI Misura in uso

LESS THAN
30%
OF THE PARTICIPANTS

-  Removable media management
-  ISMS
-  Security Officer
-  Incident response structure
-  Business continuity and Disaster recovery plan
-  Cyber/Information

MORE THAN
70%
OF THE PARTICIPANTS

-  Backup
-  Antivirus
-  Firewall
-  Systematic updating of software





Cyber 4.0

Centro di competenza nazionale sulla cybersecurity

Centro di competenza nazionale ad alta specializzazione sulla cybersecurity, promosso e finanziato dal MIMIT, inizialmente nel piano Industria 4.0 e ora soggetto attuatore PNRR

- Avviato nel 2020, **Operativo da Aprile 2021**, HQ al **Tecnopolo Tiburtino – Roma**
- **8 Organismi di ricerca, 1 Istituzione pubblica, 35 Partner privati**
- **Supporto a imprese e PA**
- Possibilità di erogare **servizi commerciali**
- **Partecipazione a iniziative finanziate**
- **13+ Milioni di Euro per (co)finanziare la transizione digitale sicura (2023-2025)**



Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Compagine associativa





Cyber 4.0 come soggetto attuatore PNRR

Supporto all'innovazione

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Azioni co-finanziabili con intensità di aiuto correlata alla dimensione aziendale

- Audit tecnico, valutazione maturità tecnologica – **Assessment**
- Prova prima dell'investimento – **Test-before-invest**
- **Formazione**
- Consulenza su proprietà intellettuale
- Consulenza su **accesso ai finanziamenti**
- Consulenza su **innovazione tecnologica di processo e di prodotto, sensibilizzazione e networking**
- **Progettazione dell'intervento di innovazione**

Co-finanziamento

- Micro – 70-100%
- Piccole – 70-100%
- Medie – 60-90%
- Grandi – 40-50%

Attività istituzionali Formazione

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

- **Corsi co-finanziati per PMI e PA**
- **Supporto nell'elaborazione strategie di formazione**
- **Webinar gratuiti, eventi informativi, workshop**
- **Attività di formazione extra accademica**
 - **CyberX Mind4Future**
 - **ITS**
- **Supporto a enti e istituzioni**
 - **Accademia Cybersicurezza Lazio** (start-up della scuola, definizione programmi, piani formativi, profili docenti e loro selezione e formazione, produzione materiali, controllo qualità, piano awareness nelle scuole)



CYBERX - MIND4FUTURE

Il nuovo programma di formazione evoluta ed
mi della cyber security



Attività istituzionali

Formazione Studenti/ Imprese

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking



Totale iscritti
449

- 218** Sapienza Università di Roma
- 62** Roma Tre
- 59** Università degli studi dell'Aquila
- 42** Università degli Studi di Roma Tor Vergata
- 24** Luiss Guido Carli
- 23** Università Campus Bio medico di Roma
- 19** Università degli Studi di Cassino e del Lazio Meridionale
- 2** Università degli Studi della Tuscia

Attività istituzionali Orientamento PMI

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Orientamento PMI

Vademecum PMI

- **12 azioni** per un business sicuro
- Basato su 12 Step ENISA



Postura cyber security PMI

- Basato su **Framework Nazionale Cybersecurity e Data Protection**
- **Analisi** aree di intervento prioritario, remediation roadmap, impatto economico e benefici
- **Estensione nazionale** – DIH, PID, Case Tecnologie Emergenti

Roadshow Cyber 4.0

- Coinvolgimento DIH e altre realtà attive in regione (Polizia Postale, CTE, etc.)
- Sessioni di info/formazione e incontri con esperti, case studies e buone pratiche, quick Cyber Checkup
- Aggregazione di comunità locali per **information sharing**



Attività istituzionali

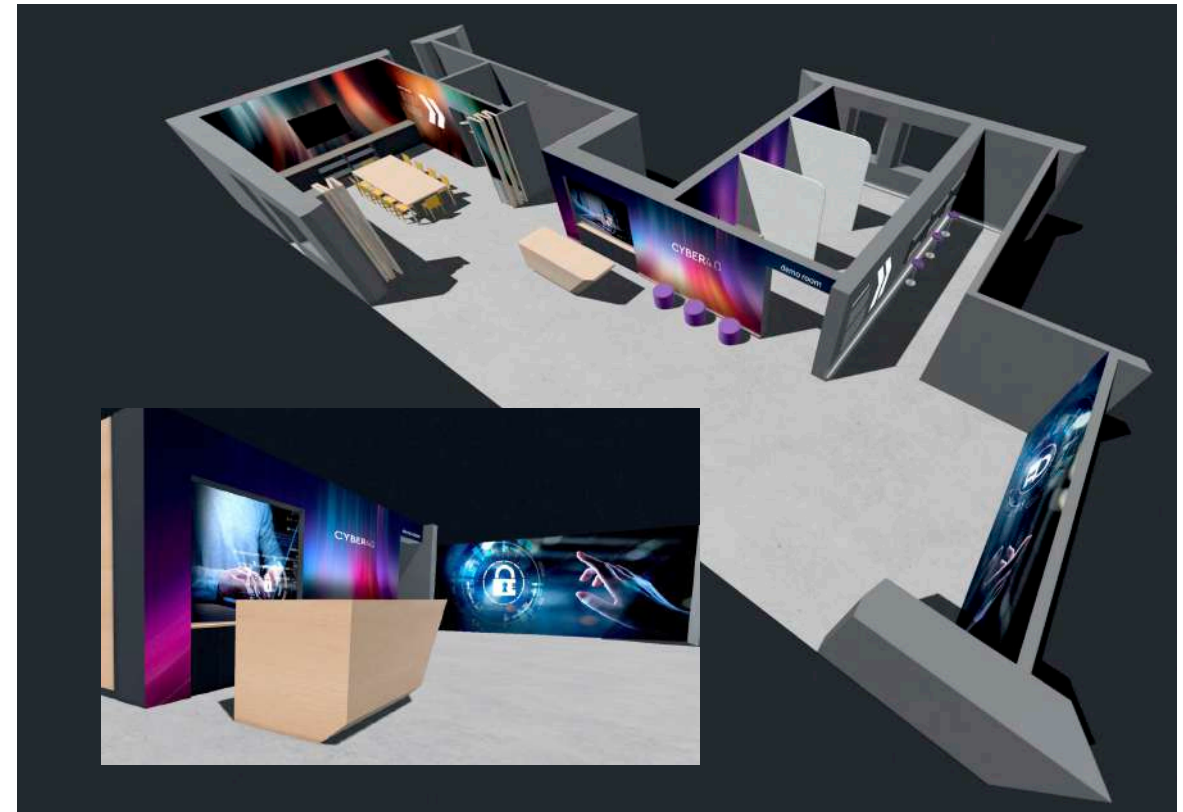
Servizi di mercato

Progetti finanziati

Networking

Demo Lab e Test Before Invest – T4

- 1 SVILUPPARE UNA SOLIDA CULTURA DELLA CIBERSICUREZZA 
- 2 FORNIRE UNA FORMAZIONE APPROPRIATA 
- 3 GARANTIRE UN'EFFICACE GESTIONE DEI TERZI 
- 4 SVILUPPARE UN PIANO DI RISPOSTA AGLI INCIDENTI 
- 5 RENDERE SICURO L'ACCESSO AI SISTEMI 
- 6 RENDERE SICURI I DISPOSITIVI 
- 7 RENDERE SICURA LA PROPRIA RETE 
- 8 MIGLIORARE LA SICUREZZA FISICA 
- 9 RENDERE SICURI I BACKUP 
- 10 LAVORARE CON IL CLOUD 
- 11 RENDERE SICURI I SITI ONLINE 
- 12 CERCARE E CONDIVIDERE LE INFORMAZIONI 



Attività istituzionali

Orientamento imprese e PA

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Strategic Advisory Istituzionale

- Position paper, benchmark, analisi, osservatori dedicati per advisory strategico alle istituzioni di riferimento
- Sviluppare azioni volte a rafforzare la collaborazione con Agenzia di Cybersicurezza Nazionale e MIMIT, anche alla luce della Strategia Nazionale di Cybersecurity

- **Analisi di mercato OT Security**
- **Strategia Industria Cyber Nazionale**
- **Osservatorio standard e normative cyber** (Ita e UE)
- **Osservatorio Cyber Security Framework e settori specifici** (es. sanità, finance, etc.)
- **Rischio terze parti**
- **Studio di fattibilità ISAC PMI**
- **Analisi nazionale della percezione del rischio di cybersecurity**
- **Supporto e partecipazione al policy making nazionale e EU**
- **Approfondimenti su tematiche verticali**
 - IoT
 - Metaverso
 - SCADA/ ICS

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Progetti di innovazione finanziati dal Centro

- Alto TRL, breve-media durata
- **Cofinanziamento 2.2 M€**, budget totale progetti ca. 7 M€
- **15 progetti finanziati** (2021-2023), 29 aziende coinvolte – 80% PMI innovative e start-up
- **Nuovi bandi per 5+ M€ (2023-2025)**

CORE CYBER SECURITY

- **ConTI** – Contextual Threat Intelligence
- **BRIE** – Blockchain register for Import Export
- **KEEPCALM** – Kernel Engines Enable (to) Prevent Cyber Attacks (with) Learning Machines
- **CybersecH** - Cybersecurity hardening for A.I. solutions
- **BINTRAWINE** - Blockchain, Tracking and Tracing solutions for Wine

AUTOMOTIVE

- **M-A-C-S** – Multibrand Automotive Cybersecurity Software
- **SHINE-ON** - Secured High accuracy localizatiON Equipment for automotive applicatiONs

HEALTHCARE

- **MAPS-EH** - Policy di sicurezza in campo eHealth
- **ISHealth** - Improved Security e-Health
- **SI-PAC** - Sistema Informativo per la Sicurezza della Gestione dei Pacchetti Ambulatori Complessi
- **PEHSA** - Pleyo E-Health: Secure APP
- **SEPLES** - SEcure PLatform of E-health Services
- **CY-CAD** - Cyber-security framework for medical data dissemination

AEROSPACE

- **QCS-TB** - Quantum Communication and Synchronization Testbed
- **QKD SVS** - QKD System Volume Simulator

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Servizi che il Centro può erogare attraverso i propri soci

Identificazione e gestione dei rischi

- Cyber risk assessment and management
- Risk monitoring
- Vulnerability assessment e Penetration Testing
- Threat Intelligence
- Monitoraggio della supply chain

Protezione dei Dati

- Data Protection Office as as service
- Data protection assessment
- Privacy governance
- Data protection impact assessment

Protezione dei Sistemi

- Identity and access management, Identity governance and administration
- Network security
- End Point security
- Defence in depth
- Patch management

Consulenza

- Consulenza tecnica, organizzativa, strategica in merito a: ICS, SCADA, IoT, CLOUD
- Ricerca on demand, in collaborazione con il mondo accademico
- Innovation Ecosystem

Monitoraggio e rilevamento minacce cyber

- Cyber threat intelligence e cyber threat modelling, SIEM, Threat detection, Proactive monitoring
- Sistemi di early warning e rilevamento attacchi
- Ransomware readiness

Risposta e gestione degli incidenti

- Orientamento e consulenza in merito a: SOC, CSIRT / CERT as a services
- Supporto alla definizione di un modello (tecnico ed organizzativo) per la gestione degli incidenti informatici
- Supporto alla gestione operativa di incidenti cyber

Certificazione

- Supporto per l'ottenimento di certificazioni in ambito information security e cybersecurity
- Laboratorio di Valutazione di Sicurezza accreditato dall'organismo di certificazione OCSI

Formazione

- A catalogo
- Custom
- Piani di awareness

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Formazione a catalogo che il Centro eroga direttamente o attraverso i soci

Fondamenti di cybersecurity

Normativa e governance cybersecurity

Tecnologie e tecniche di cybersecurity

Cloud security

IoT security

Blockchain

AI

Impresa digitale

Esercitazioni immersive

Formazione professionale

Alta formazione

Tecniche di formazione

Blockchain & Automotive

Sapienza, LUISS, AizoOn



- Fundamentals of cryptography (2022)
- Blockchain intro, basic module (2022)
- Blockchain and automotive applications
- Smart contracts and decentralized applications
- Blockchain advanced, tech module
- Blockchain & IOT
- Blockchain & security
- AI & Blockchain
- Interactive module – Use cases

International capacity building

Cyber 4.0



OCWAR-C



unded by the
European
Union



European Digital Innovation Hub

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

Digital Europe – EDIH NEST

The Network for European Security and Trust is a one-stop shop for **cybersecurity solutions and capacity building initiatives**, targeting **SMEs and Public Administration of Central Italy**.

- Partners: **Cyber 4.0** (Coordinator), **DIH Lazio, DIH Umbria, DIH Abruzzo, Innova**
- Budget: **4.7 M€**
- Duration: **36 months** (2023-2025)
- Endorsements and collaborations: **National Cybersecurity Agency, Regione Lazio, Enterprise Europe Network, Italian Banking Association**

Cybersecurity tools and services

Facilities for test-before-invest

Capacity building initiatives

Assistance for access to finance and funding

Innovation ecosystems

EU regulatory framework, policies and strategies



Case delle Tecnologie Emergenti

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

MIMIT – Case delle Tecnologie Emergenti

CAGLIARI DIGITAL LAB

Valore totale progetto: € 12.550.000 – **Durata:** 24 mesi –
Decorrenza: 02/02/2023

Allestimento:

- **piattaforma di quantum computing** per sperimentazione di soluzioni per le smart cities;
- **infrastruttura 5G indoor**
- **infrastruttura 5G outdoor e mobile edge computing;**
- **piattaforma in cloud con nodi adatti allo sviluppo di applicazioni di Intelligenza Artificiale e Deep Learning;**
- **piattaforma di open APIs** per l'integrazione dei servizio.

Attività Cyber 4.0: soluzioni di cybersecurity per tutti i sistemi e applicativi sviluppati, animazione, gestione comunicazione/divulgazione

PESARO CTE SQUARE

Valore totale progetto: € 10.977.000 – **Durata:** 24 mesi –
Decorrenza: 02/02/2023

Allestimento:

- **Laboratorio Attivo** per ricerca, sviluppo, e sperimentazione in ambiente reale, trasferimento tecnologico di tecnologie innovative in ambiente urbano
- **Innovation Accelerator:** Startup building, Hackathon, Open Call, incubazione e accelerazione.
- **ICT Skill Transfer:** Coinvolgimento attivo end user

Attività Cyber 4.0: soluzioni di cybersecurity per tutti i sistemi e applicativi sviluppati, animazione, gestione comunicazione/divulgazione

La rete di collaborazioni istituzionali

Attività istituzionali

Servizi di mercato

Progetti finanziati

Networking

- **MIMIT**

- Network dei **Competence Center**
- Network delle **CTE**

- **ACN**

- **Regione Lazio**

- **Accordi e partnership a livello nazionale**

- Partnership con **rete dei DIH di Confindustria**
- Collaborazione con **rete dei PID delle Camere di Commercio**
- Europe Enterprise Network
- Protocollo d'Intesa con **Società Italiana di Intelligence (SOCINT)**
- MoU **Quantum for Space**
- Protocollo d'Intesa con **Fondazione Amaldi**

- **Networking internazionale**

- **EDIH** Network
- **Ad Hoc Working Group su European Cybersecurity Skills Framework di ENISA**
- Membri di **ECSO, European Cybersecurity Organization**
- Protocollo di intesa con **Agenzia Catalana di Cybersecurity**
- Membri di **Global Cyber Alliance**
- Membri dello Stakeholder Group di **EU CyberNet**
- Advisory Board **GFCE, Global Forum for Cyber Expertise**



4C per le sfide di cybersecurity

Competenze

Capacità

Cooperazione

Concretezza



F O R U M
CYBER 4.0

GRAZIE

MATTEO LUCCHETTI
DIRETTORE OPERATIVO CYBER 4.0