FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

mPMI e cybersecurity

Claudio Telmon
Board of Directors, CLUSIT

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

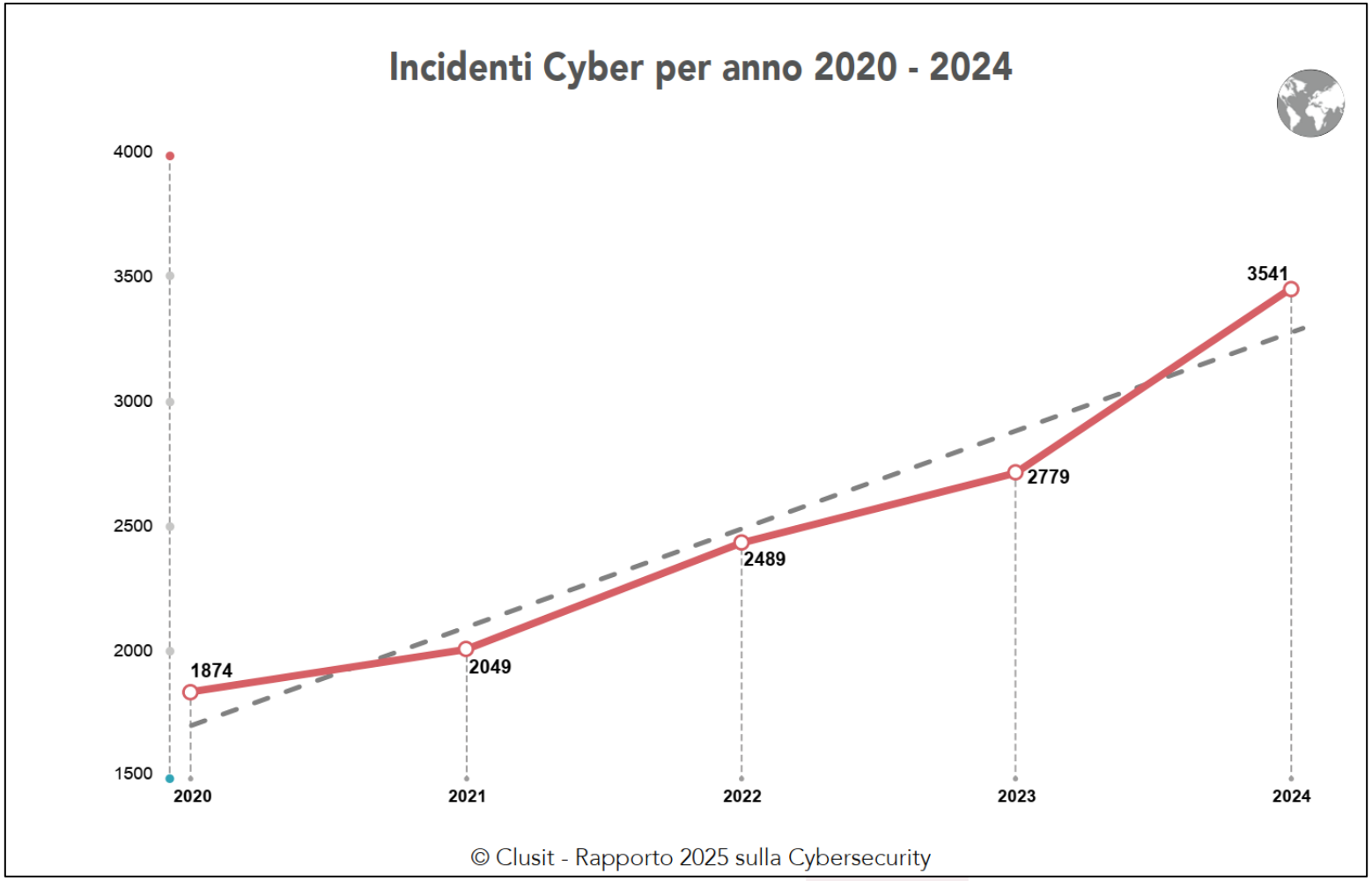
Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Incidenti: andamento mondiale 2020 - 2024



Il contesto geopolitico

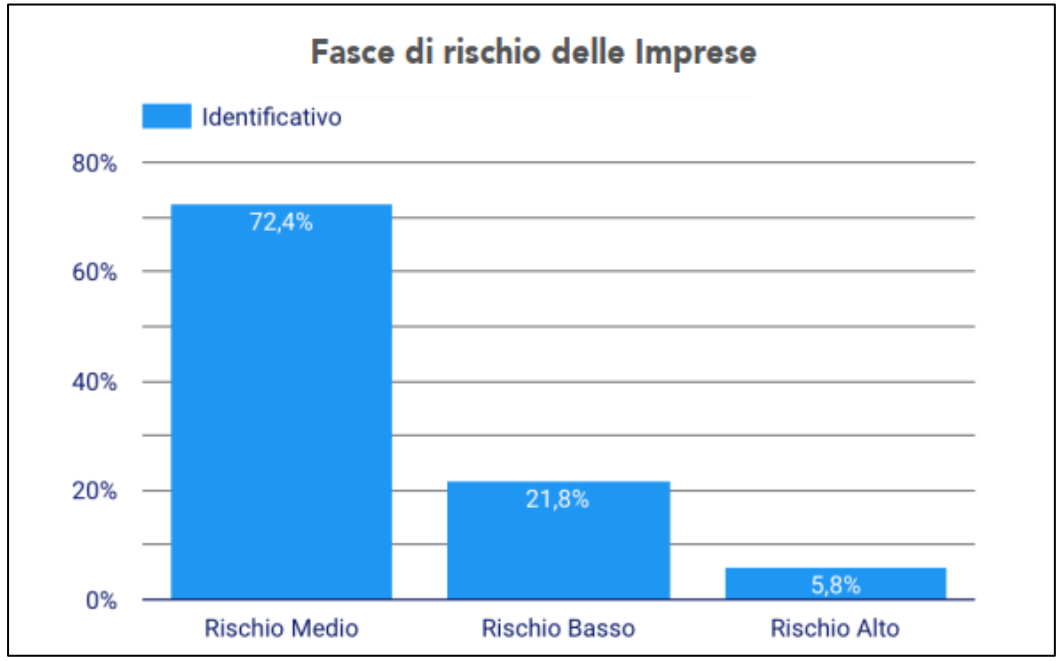
euro news. Latest Europe World EU Policy Business Travel Next Culture Green Health Eu

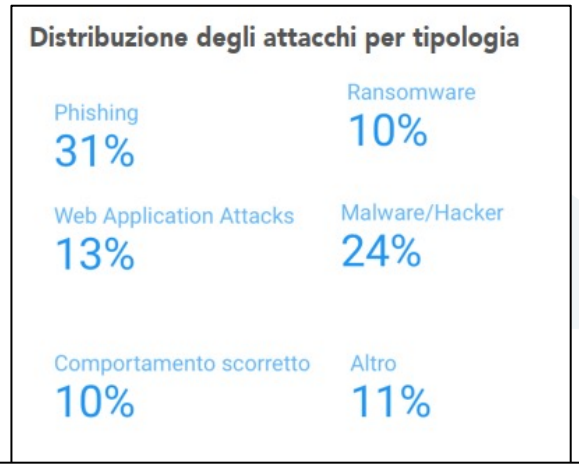
Europe > Europe News

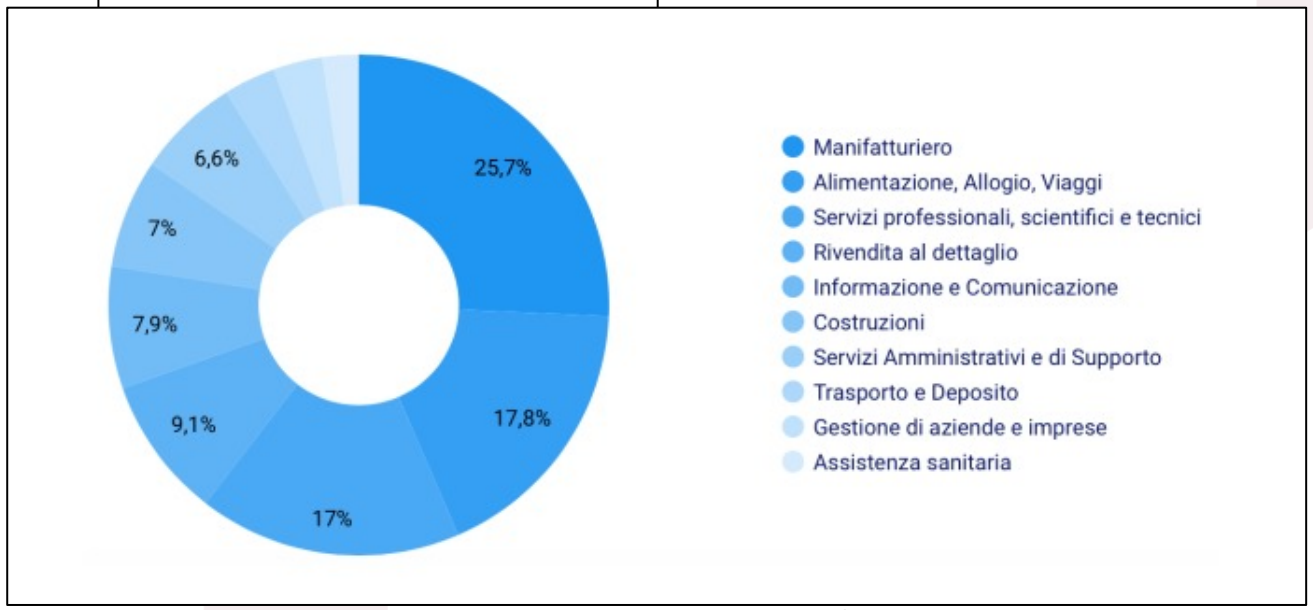
EU 'ready to impose costs' on China over cyberattack against Czechia, warns Kallas

Copyright European Union, 2025.

mPMI: rischi e incidenti





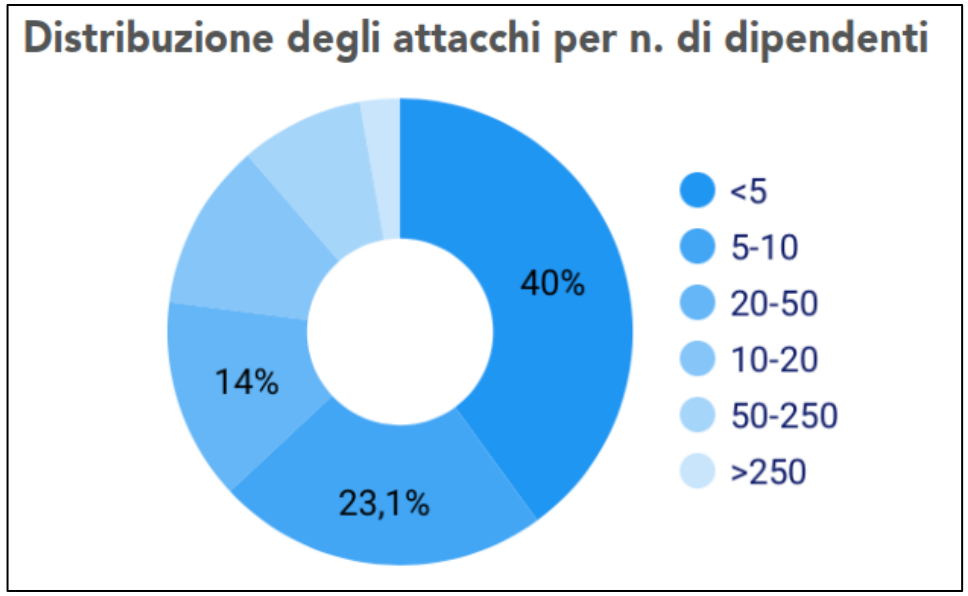


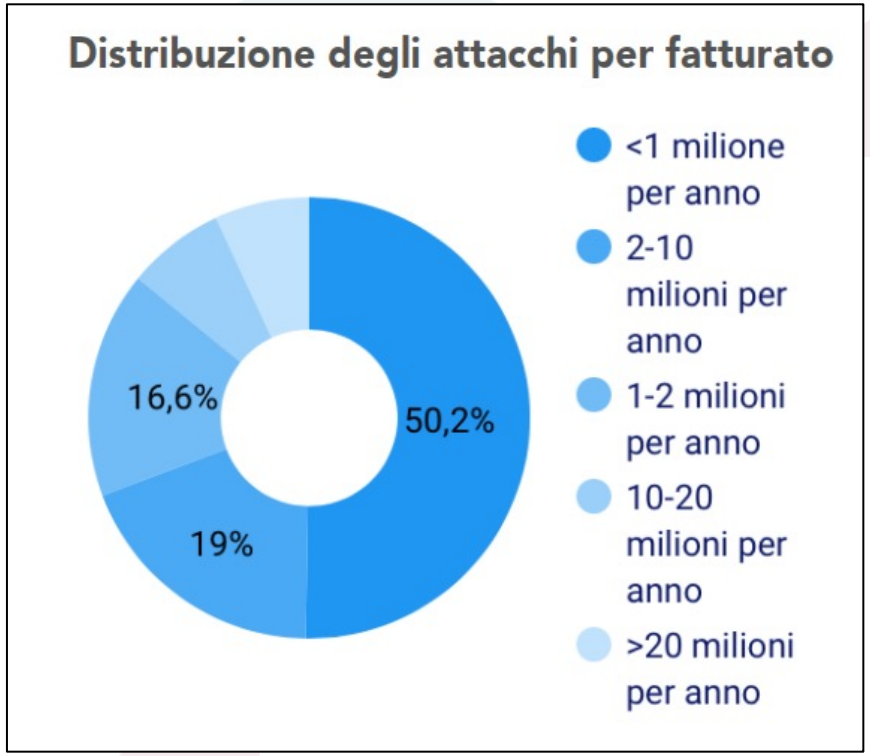
Settori maggiormente colpiti

Fonte: Rapporto Clusit 2025

Contributo dallo studio 2022 – 2023 DINTEC
da un modello IIT - CNR e START 4 0

mPMI: rischi e incidenti





Fonte: Rapporto Clusit 2025

Contributo dallo studio 2022 – 2023 DINTEC
da un modello IIT - CNR e START 4 0

FORUM 2025 CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

La rete dei *Digital Innovation Hub* di Confindustria lavora di squadra: il modello di *cyberassessment*

Ing. Mariella Ferraro
Responsabile innovazione del Campania DIH- Rete Confindustria scarl
ferraro@campaniadih.it

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea NextGenerationEU

Hosted by: ROMA TRE UNIVERSITÀ DEGLI STUDI

- La rete dei DIH di Confindustria, chi siamo
- L’evoluzione della rete a supporto delle imprese
- Il modello di *cybersecurity assessment*
- Risultati raggiunti
- Evoluzione, prossimi obiettivi e nuove sfide

La rete nazionale dei DIH

CONFINDUSTRIA

Il *network* dei *Digital Innovation Hub* di Confindustria - **costituito da Confindustria** in attuazione del Piano Nazionale Industria 4.0 e operativo **dal 2017** - rappresenta la **porta di accesso delle imprese** al mondo della digitalizzazione, accompagnando **imprese** e **filiere** nella valutazione della maturità digitale e orientandole verso l'ecosistema dell'innovazione.

Il Campania DIH è un nodo della rete del Sistema.

Cybersecurity Assessment

Gruppo di Lavoro e Obiettivi

INIZIATIVA DI:

Sistemi Formativi Confindustria

Rete dei *Digital Innovation Hub*

REALIZZATO DAL GDL:

Competence Center Cyber 4.0

Digital Innovation Hub Liguria

Fondazione Piemonte innova

Competence Center Start 4.0

Nell'ambito dell'elaborazione del "Piano di sviluppo dei DIH" è stato costituito un **Gruppo di Lavoro** dedicato allo sviluppo del **modello di *Assessment*** per la valutazione del livello di *cybersecurity* delle PMI.

Il Gruppo di Lavoro ha messo a fattor comune le rispettive competenze e collaborato per **unificare differenti approcci** alla valutazione della maturità *cyber*.

Dopo oltre un anno di lavoro è stato possibile realizzare **un modello nazionale unico** di *cybersecurity maturity assessment* dedicato alla fascia delle **micro, piccole e medie imprese**.

FONDAZIONE PIEMONTE INNOVA

Luca Mancino
Innovation Manager

Nicola D'Angelo
Cybersecurity Specialist

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

DIH Digital Innovation Hub

Mariella Ferraro

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Alessandro Calabrese
Responsabile Advisory e Formazione

Matteo Lucchetti
Direttore Operativo

START4.0

Georgia Cesarone
Head of Innovation and Training

Cybersecurity Assessment

il modello di *assessment*

STRUMENTO

Cyber4.0, **DIH Liguria, Fondazione Piemonte Innova (FPI)** e **Start4**, su mandato del network dei **DIH** di Confindustria e di **Sistemi Formativi Confindustria (SFC)**, hanno sviluppato uno strumento unico e di riconosciuta validità, configurandolo eventualmente come Prassi di Riferimento UNI.

OBIETTIVO

Il ***cybersecurity assessment*** nasce per aiutare il *management* aziendale a comprendere l'importanza della protezione dai rischi cyber e promuovere la Data Protection. Ha quindi l'obiettivo di **aumentare la consapevolezza delle aziende sul tema della cybersecurity e fornire una fotografia del livello di maturità cyber basata su standard di riferimento nazionali e internazionali**.

RIFERIMENTI

Il ***cybersecurity assessment*** segue i riferimenti del ***Framework* nazionale per la *Cybersecurity e Data Protection* (FNCS)**, che discende dal **framework NIST**, National Institute of Standards and Technology americano, e dello *standard* internazionale **ISO/IEC 27001**.

Cybersecurity Assessment

processo

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

INDIVIDUAZIONE PROFILO DI RISCHIO

Lo strumento individua il profilo di rischio dell'impresa andando a individuare un livello di maturità *target* da raggiungere

IL *cyber assessment* si adatta allo specifico contesto

MISURAZIONE DEL LIVELLO CYBER

Lo strumento misura il livello *cybersecurity* che raggiunge l'impresa e indica se il livello di maturità minimo è superato o meno

IL *cyber assessment* fornisce la postura di sicurezza dell'organizzazione analizzandola

- a livello generale -
- per category -
- per function -

SUGGERIMENTI PRATICI: *QUICK WIN* e *NEXT STEPS*

Lo strumento fornisce suggerimenti per orientare una *gap analysis* e definire azioni per superare il livello di maturità *target* e implementare una *roadmap* di *remediation*

IL *cyber assessment* restituisce *quick win* e *next steps*

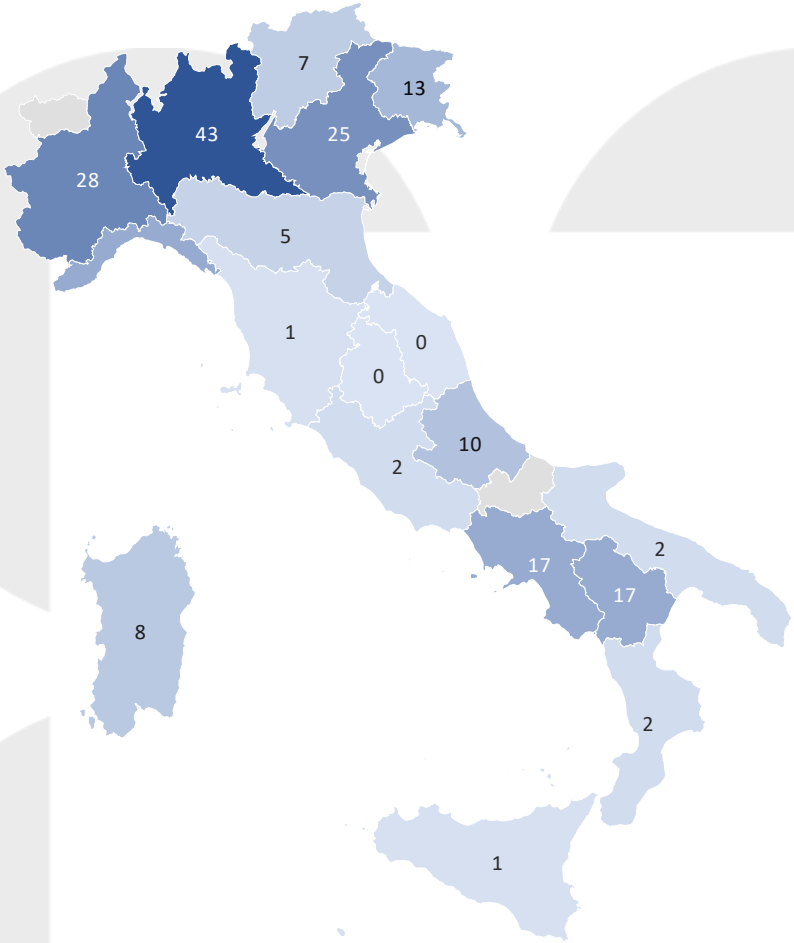
Cybersecurity Assessment:
un lavoro di squadra a supporto delle PMI

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

RISULTATI RAGGIUNTI

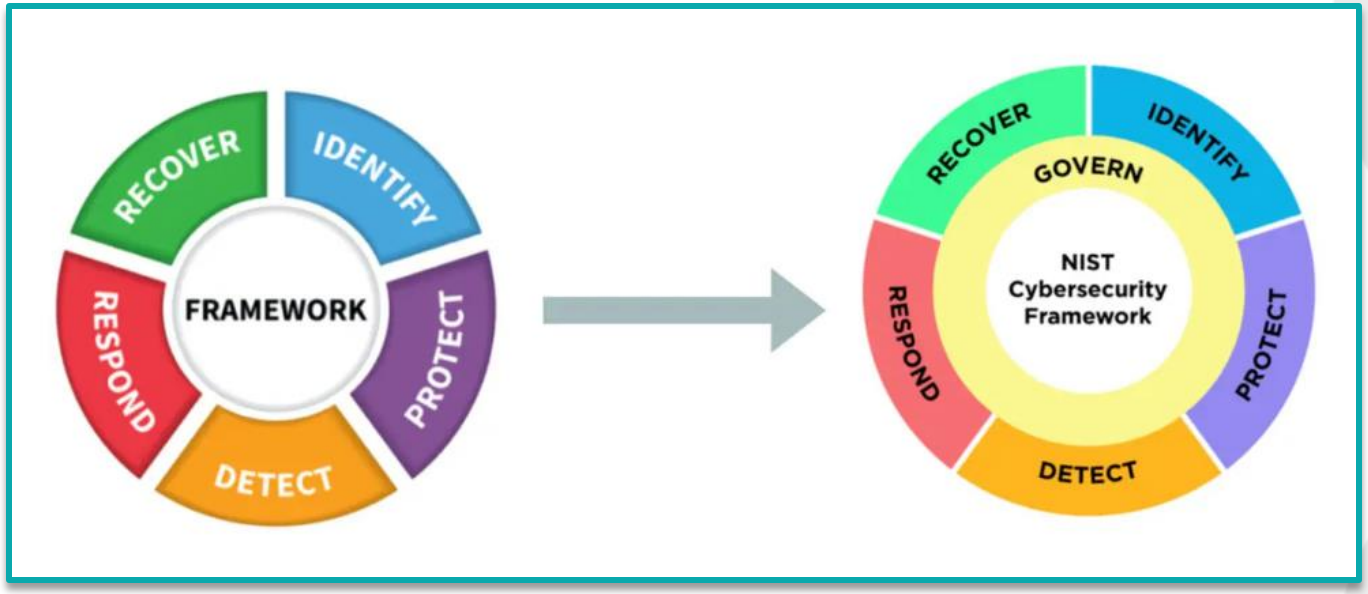
Ad oggi grazie alla collaborazione attiva tra la rete dei DIH, centri di competenza e Fondazione Piemonte Innova sono stati erogati **oltre 200 *cyberassessment*** ed il numero è destinato ad aumentare vertiginosamente, soprattutto a seguito dell'evoluzione del panorama legislativo.



Cybersecurity Assessment: what next

Evoluzione, prossimi obiettivi e nuove sfide

A seguito della pubblicazione del nuovo *Framework* nazionale per la *Cybersecurity e Data Protection* (2025) ed a seguito della Determinazione di ACN del 14/04/25, che, all'art. 2, definisce le misure di base per l'adempimento agli obblighi del decreto NIS, **il gruppo di lavoro ha accolto la sfida di aggiornare lo strumento già progettato.**
Inoltre, sarà a breve *online* la piattaforma con lo strumento aggiornato. Non essendo uno strumento di self assessment, si procederà ad un aggiornamento dei *manager* deputati all'erogazione dell'*assessment*.



FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Cybersecurity di filiera

Antonio Truglio
Direttore Digital Innovation Hub Lazio

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI

FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Humans for Cybersecurity – Il fattore umano per guidare la Cybersecurity e l'AI applicata alla cybersecurity nel mondo delle PMI – la piattaforma HCSP

Mario Gaetano Di Dio
Direttore Generale, NETGROUP SpA
gdidio@netgroup.it

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:
ROMA TRE
UNIVERSITÀ DEGLI STUDI

Sensibilizzazione delle PMI alla cybersicurezza

Il recepimento della Direttiva NIS2

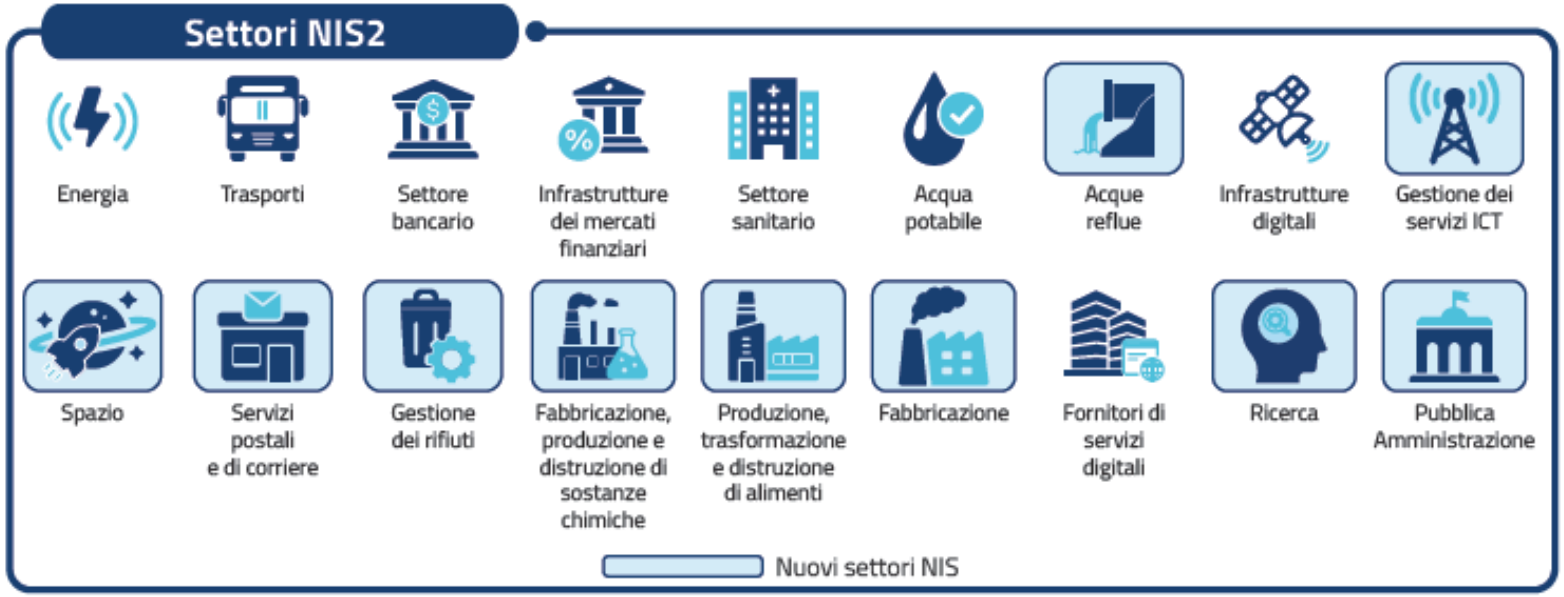
FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Il livello di Cybersecurity nelle PMI Italiane è generalmente basso, ed il problema è estremamente serio sia per la fragilità rispetto ad attacchi informatici, oramai all'ordine del giorno, sia per la conformità normativa.

Direttiva NIS2 – non un vincolo, ma una grande opportunità.

Misure di s **o e di rete**



Regime sanzionatorio definito dalla Direttiva NIS2: arriva a punire le violazioni più gravi fino a

un massimo del 2% del fatturato

La protezione delle infrastrutture invisibili

Il digitale è un patrimonio da proteggere

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Proteggere le infrastrutture invisibili significa attuare misure per garantire la sicurezza di reti, sistemi e dati che oggi sono fondamentali per il funzionamento di un comparto industriale.

Molto spesso non vediamo, o sottovalutiamo l'importanza di tali componenti, che svolgono un ruolo cruciale nel funzionamento di un processo produttivo.

Siamo abituati a rendere sicuro e resiliente il visibile, con sistemi di allarmistica, controllo fisico degli accessi, barriere di vario genere, videosorveglianza, sistemi di backup dell'energia elettrica, ma quasi mai prestiamo la stessa attenzione per i nostri sistemi informativi e le nostre infrastrutture IT.

Eppure sappiamo che viviamo in un mondo totalmente interconnesso:

il fermo di un sistema informativo produce quasi sempre il fermo del processo produttivo

Supporto preventivo e reattivo alle PMI

HCSP – la risposta di Netgroup e Cyber 4.0 per la cybersicurezza delle PMI

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Per indirizzare questa esigenza, è stata sviluppata un'idea progettuale per la realizzazione di una **piattaforma di servizi evoluti a supporto delle PMI** (di seguito anche **HCSP-PMI**), che è diventata velocemente realizzabile grazie al supporto di CYBER 4.0, mediante i finanziamenti previsti nell'ambito della:

LINEA A – Potenziamento dell'infrastruttura del Centro per erogazione servizi

Il coinvestimento di Netgroup in tale ambito ha consentito di massimizzare gli investimenti pubblici che ricadono proprio nella Linea A.

SECURITY OPERATION CENTER

Team di professionisti per la sicurezza Enterprise IT e Industrial OT, a supporto del monitoraggio continuo

SECURITY VULNERABILITY ASSESSMENT

Vulnerability Scanning, Vulnerability Assessment, Penetration Test e Servizi per la Sicurezza

DIGITAL RISK MONITORING

Monitoraggio continuo delle darknet per l'early warning di data-breach

CYBER THREAT INTELLIGENCE

Monitoraggio delle attività online dei gruppi criminali, basato su algoritmi di machine learning e AI

FORMAZIONE, SECURITY AWARENESS E CONSULENZA

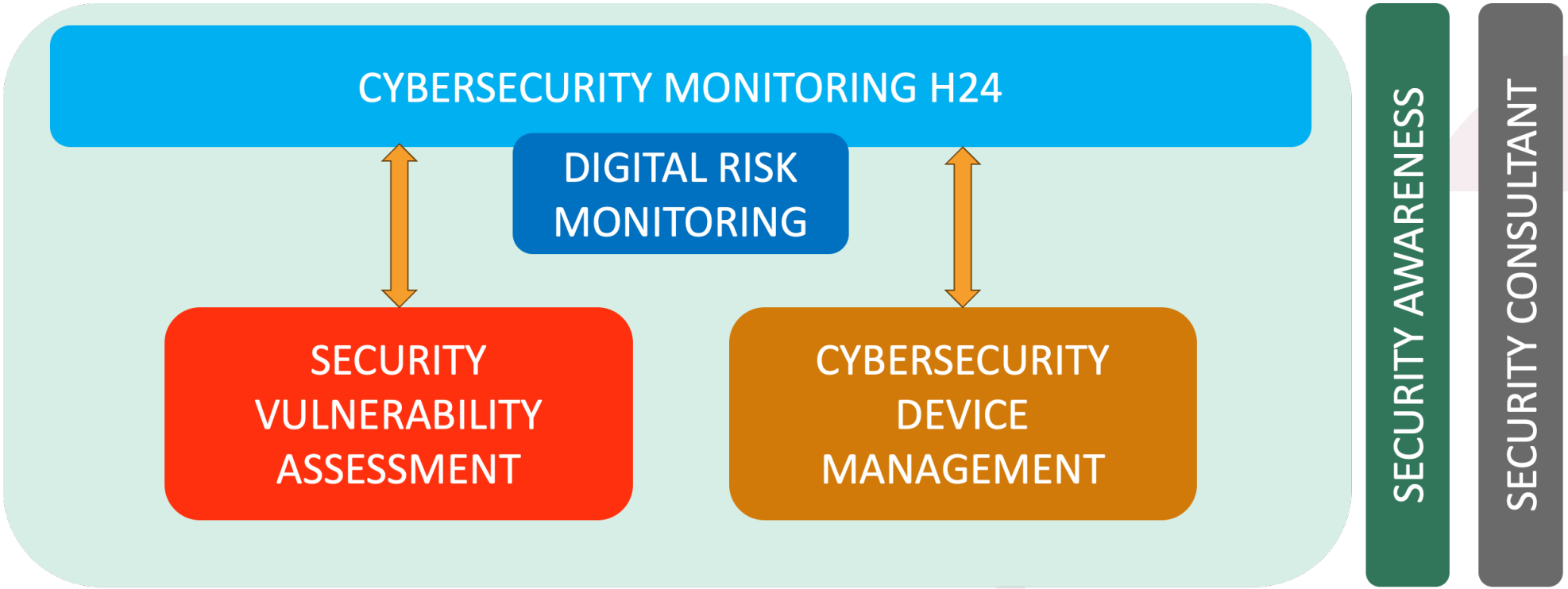
Formazione specialistica e consulenza personalizzata sui temi della Cybersecurity e della Governance IT

CONDUZIONE APPARATI DI SICUREZZA

Gestione ordinaria e supporto agli interventi di manutenzione straordinaria

La piattaforma HCSP

Caratteristiche e Business Model



Business Model: Il modello di business ipotizzato di HCSP-PMI prevedrà una fee annuale di adesione per le PMI, per la sola copertura costi, che consentirà di accedere a un primo livello di servizi di sicurezza erogabili attraverso la piattaforma, e l'accesso ad un numero di servizi ulteriori di tipologia più evoluta a pagamento.

FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Cybersecurity Info-Sharing, Un ISAC per le PMI

Stefano Bordi
Executive VP, Di.Gi. Academy

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI