FORUM 2026
CYBER 4.0

3-4 GIUGNO 2026
Luiss | Aula 200

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

03 Giugno 2026

Oltre gli incentivi: l'impatto del PNRR nell'implementazione di Cyber 4.0

Matteo Lucchetti, Direttore Operativo Cyber 4.0

Matteo.Lucchetti@cyber40.it

Con il Patrocinio di:

European Commission

Ministero delle Imprese e del Made in Italy

Ministero degli Affari Esteri e della Cooperazione Internazionale

ACN Agenzia per la Cybersicurezza Nazionale

Funded by the European Union NextGenerationEU

Hosted by: LUISS Università di Roma

Servizi incentivati per imprese

988

Applicants

Aziende e organizzazioni che hanno presentato domanda ai programmi Linea B2 e NEST

450+

Imprese servite

Imprese che hanno beneficiato concretamente dei servizi di supporto cyber erogati

3.600+

Servizi richiesti

Totale delle richieste di servizio pervenute attraverso i portali PIC e PIEN

900+

Servizi erogati

Servizi contrattualizzati ed erogati, con piena tracciabilità

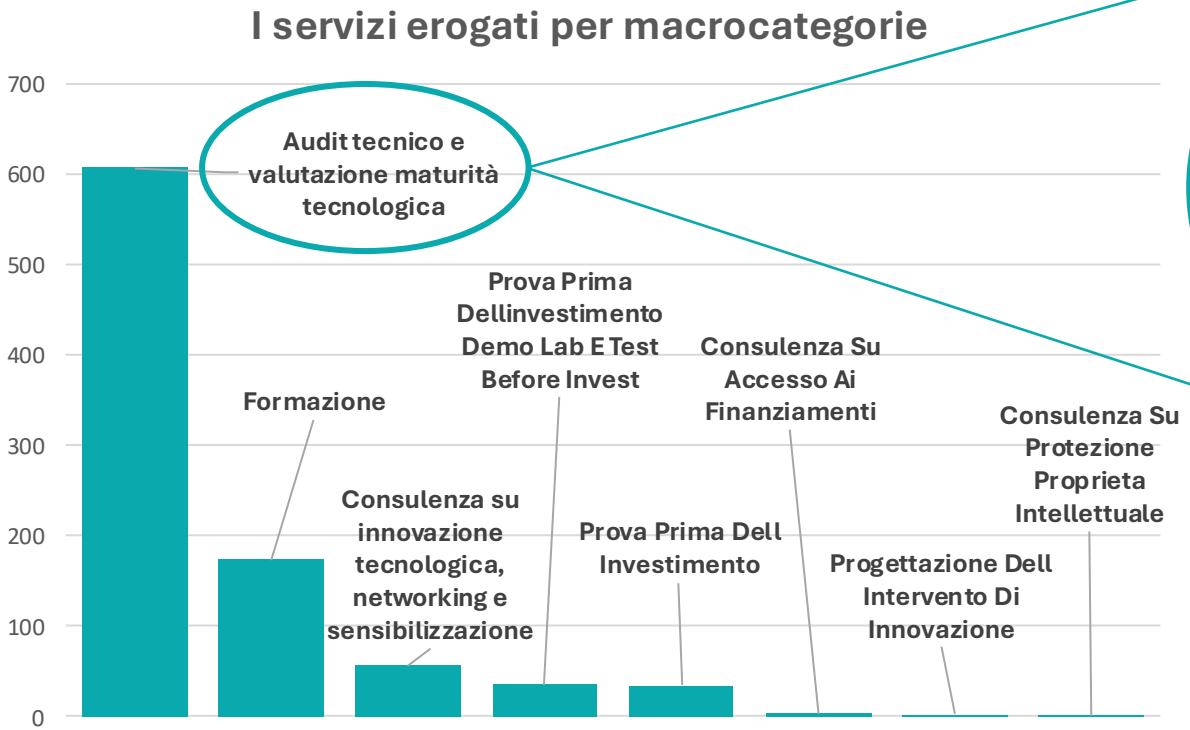
11.5 M€

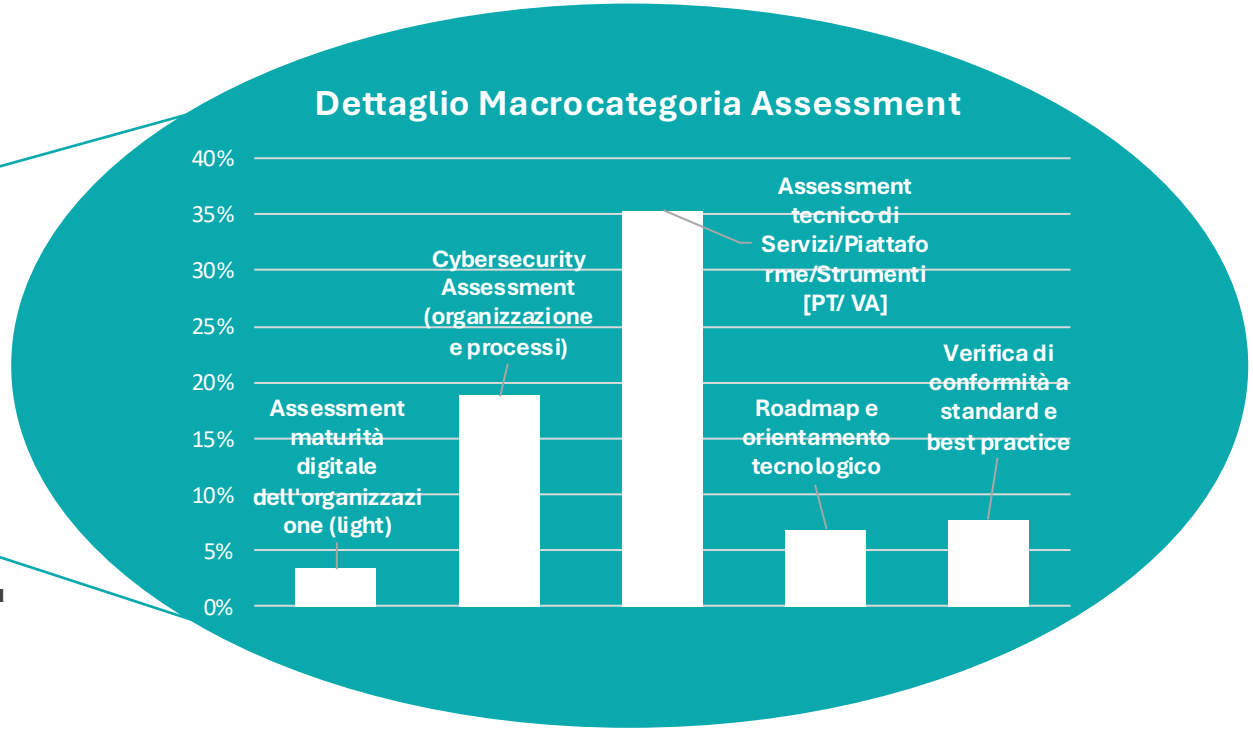
100%

Incentivi erogati verso le imprese beneficiarie

14.6 M€ valore totale servizi erogati

Servizi incentivati per imprese
Bilancio operativo





56% Piccole

34% Medie

10% Grandi

La situazione riscontrata nelle PMI
Vulnerabilità tecniche e organizzative

FORUM 2026 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

>57% MISCONFIGURAZIONI

Servizi esposti su Internet senza necessità, credenziali di default attive, protocolli insicuri

>51% AGGIORNAMENTI MANCANTI

Sistemi operativi, server web e applicazioni non aggiornati. Presenza di CVE pubbliche note da anni, sfruttabili tramite attacchi automatizzati

>27% GESTIONE ACCESSI INADEGUATA

Assenza cronica di MFA, privilegi amministrativi non giustificati e credenziali condivise

La vulnerabilità tecnica è solo il sintomo evidente

L'assenza strutturale di governance e processi trasforma rischi altrimenti gestibili in esposizioni croniche

- **Assenza di Incident Response Plan**
- **Mancanza di policy e formazione**
- **Scarsi controlli sulla supply chain**
- **Budget estremamente sottodimensionato**

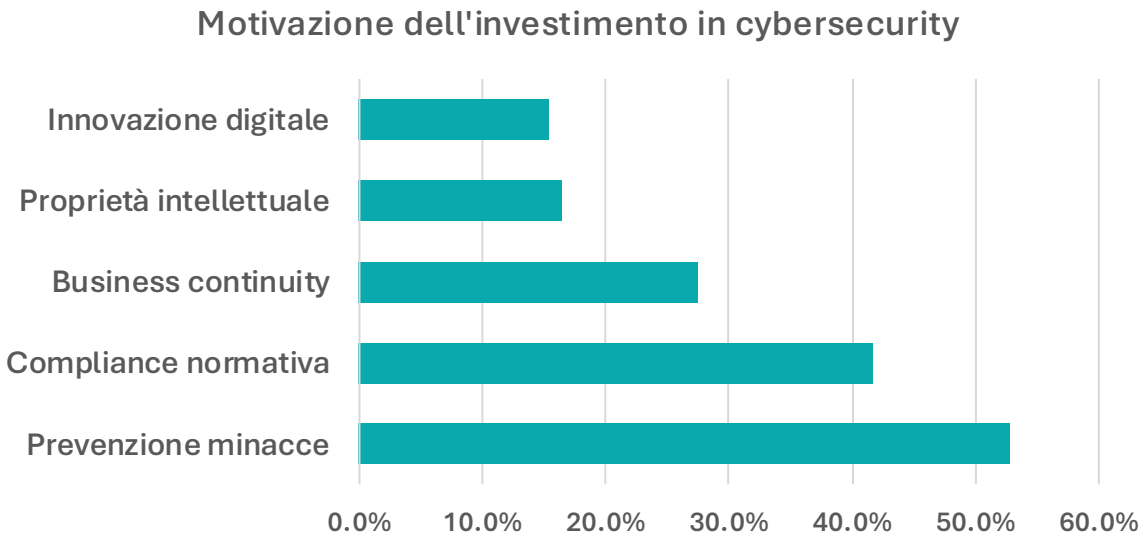
L’effetto leva del PNRR

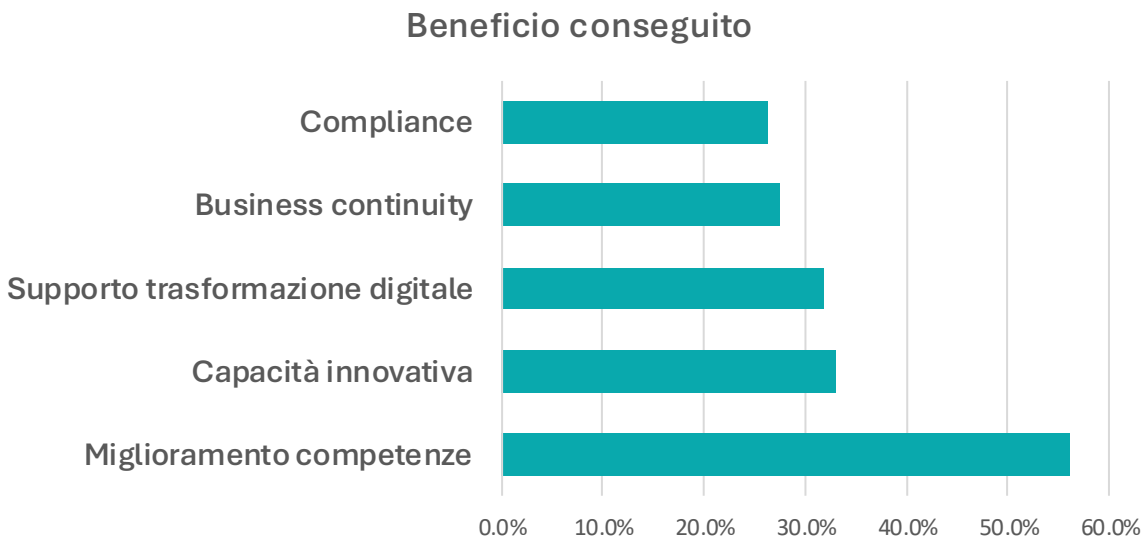
Le PMI italiane:

- **risultano sotto-investite;**
- **soffrono carenza di competenze;**
- **hanno difficoltà di accesso a capability avanzate;**
- **non dispongono di SOC;**
- **non hanno monitoring continuo;**
- **non possiedono capacità OT evolute.**

- Budget annuo in cybersecurity per una PMI oscilla tra 5 e 20k
- **Gli interventi di Cyber 4.0 avrebbero rappresentato dal 50% al 200% del budget cyber annuale ordinario di una PMI**

La crescita di consapevolezza delle PMI





- Le imprese identificano come principali criticità: competenze, ecosistema, accesso a expertise, capacità progettuale.
- Il principale impatto percepito non è economico immediato, mao rganizzativo, tecnologico;, culturale;, strategico.

- Cyber 4.0 ha quindi operato contemporaneamente come: abilitatore finanziario, trasferitore di competenze, orchestratore di ecosistema e trusted advisor.
- Cyber 4.0 ha generato capability, maturità, competenze, resilienza.

Gli asset generati dal PNRR – Laboratori e piattaforme

- **T4 DemoLab**
  Rete privata 5G per technology test
- **5 Laboratori OT Security**
  Automotive
  Healthcare
  IoT security
  Trasporti
  OT Security
- **2 Laboratori AI**
  Cyber Safe AI
  AI Sec Lab LLM
- **4 piattaforme servizi imprese**
  SOC-a-a-S,
  ISAC4PMI,
  Spotlight – Disinformazione,
  Blockchain lusso
- **1 Cyber Range**

Laboratori e piattaforme
L’approccio strategico

Da erogatore di servizi a Infrastruttura di cyber resilienza nazionale distribuita

Ecosistema cyber full-stack per PMI

- Prevention → Detection → Intelligence → Experimentation → Compliance → Resilience

AI come elemento trasformativo

Competenze OT molto rare, ma molto richieste, messe a sistema

Capability che il mercato non avrebbe sviluppato autonomamente

- Investimenti elevati,
- ROI di lungo periodo
- Valore sistemico

Trasferimento tecnologico e innovazione

FORUM 2026 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

4.7M

Co-finanaiamento allocato e rendicontato

20

Progetti

- **Core**
- **Space**
- **Automotive**
- **Healthcare**

NOTIZIE

Progetto ESII – AI a supporto dei team SOC nell'investigazione degli incidenti

12 Marzo 2026

NOTIZIE

CyberGuardEV: sicurezza avanzata per le infrastrutture di ricarica dei veicoli elettrici

NOTIZIE

Progetto WISE PACK – Protezione dei prodotti farmaceutici tramite sensori wireless integrati nel packaging

NOTIZIE

ARGO – Ottimizzare l'analisi cyber per decisioni più rapide e precise

BIOSAT MARKETPLACE

NOTIZIE

Biosat Marketplace - u piattaforma sicura di servizi per l'Osservazio della Terra

NOTIZIE | NOTIZIE

Progetto CYBORG – Sistemi di comunicazione sicura a bordo veicolo basati su blockchain

...

Le azioni PNRR di Cyber 4.0

FORUM 2026 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Modello integrato di:

Conoscenza profonda di ecosistema, bisogni e opportunità

Servizi scalabili di resilienza cyber

Trasferimento tecnologico altrimenti molto difficoltoso

Industrial policy che funziona – Efficiente ed efficace

Capability building, oltre l'erogazione di incentivi

Readiness normativa, fondamentale per affrontate le sfide correnti

FORUM 2026
CYBER 4.0

3-4 GIUGNO 2026
Luiss | Aula 200

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

03 Giugno 2026

GRAZIE!

Matteo Lucchetti, Direttore Operativo Cyber 4.0
Matteo.Lucchetti@cyber40.it

Con il Patrocinio di:

European Commission
Ministero delle Imprese e del Made in Italy
Ministero degli Affari Esteri e della Cooperazione Internazionale
ACN
Funded by the European Union NextGenerationEU

Hosted by: LUISS Università di Roma