CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SISTEMI FORMATIVI CONFINDUSTRIA

LUISS

ROADSHOW CYBER 4.0

PROSSIME TAPPE

16 Marzo - Potenza

21 Marzo - Cosenza

6 Aprile - Milano

13 Aprile - Ancona

10 Maggio - Firenze

18 Maggio - Torino

15 Giugno - Parma

22 Giugno - Udine

4 Luglio - Trento

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Roadshow Cyber 4.0

Cybersecurity per le PMI della Regione Basilicata

Contesto strategico e opportunità di sviluppo

Confindustria Basilicata

16.03.23

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Apertura dei lavori e saluti istituzionali

- **Francesco SOMMA**, *Presidente Confindustria Basilicata e DIH Basilicata*
- **Leonardo QUERZONI**, *Presidente Cyber 4.0 (in videocollegamento)*

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Cybersecurity nel contesto delle PMI

Obblighi, minacce e rischi: le priorità di azione e le iniziative in corso

- **Martina CASTIGLIONI,** *Responsabile formazione ed orientamento, Cyber 4.0*

Cyber 4.0

Centro di competenza nazionale sulla cybersecurity

Centro di competenza nazionale ad alta specializzazione sulla cybersecurity, promosso e finanziato dal MISE nel piano Industria 4.0

- Avviato nel 2020, **Operativo da Aprile 2021, HQ al Tecnopolo Tiburtino – Roma**
- **8 Organismi di ricerca, 1 Istituzione pubblica, 35 Partner privati**
- **Target delle attività – PMI e PA**
- **Mandato istituzionale**
  - Linea A: offrire a PMI e PA servizi di orientamento e formazione – 4,0 M€
  - Linea B: finanziare progetti R&I, in ambito dei servizi core di cybersecurity, trasversali a tutti i settori, sia in specifici contesti verticali: Healthcare, Automotive e Aerospace – 2,2 M€
- Possibilità di erogare **servizi commerciali**
- **Partecipazione a iniziative finanziate**

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cyber 4.0
Compagine associativa

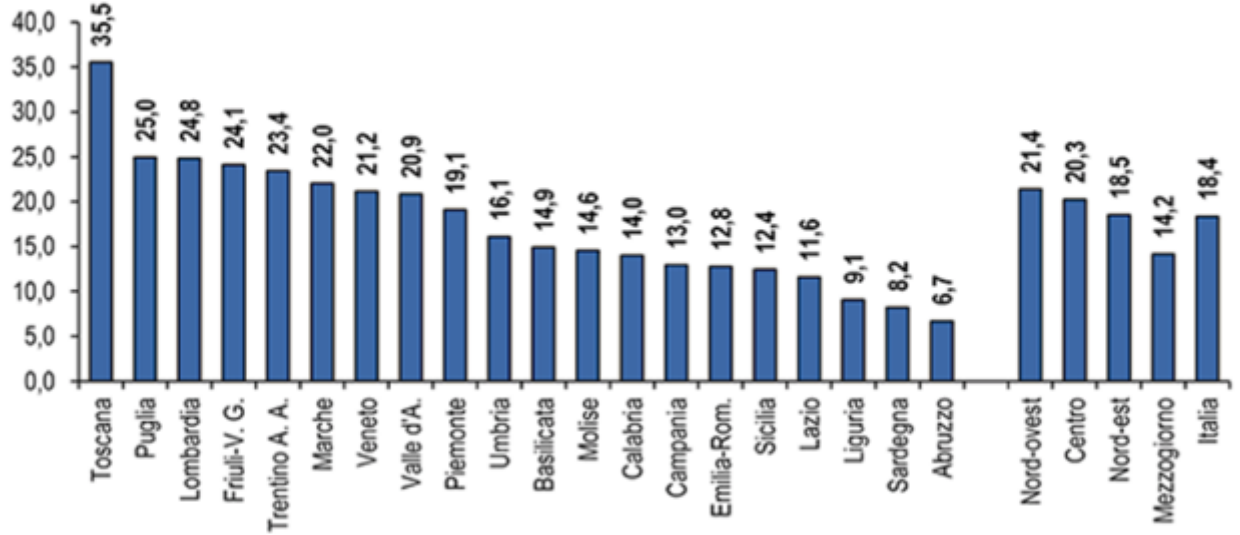
Minacce cyber: un rischio reale?

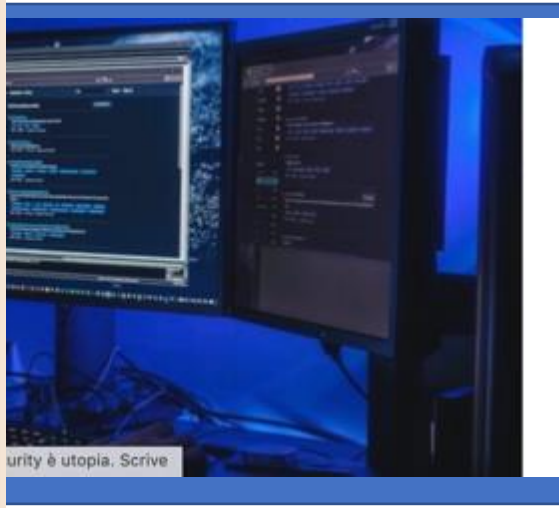
CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

L'Italia è
ransom

Piccole imprese e attacchi informatici: colpite 4 su 10. Le contromisure

Dinamica delitti, truffe e frodi informatiche per regione
Var.% 2020-2021 – Elaborazione Ufficio Studi Confartigianato su dati Istat





CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Rompiamo il ghiaccio

slido.com

#1302107

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

La transizione digitale offre più opportunità o rischi per una PMI?

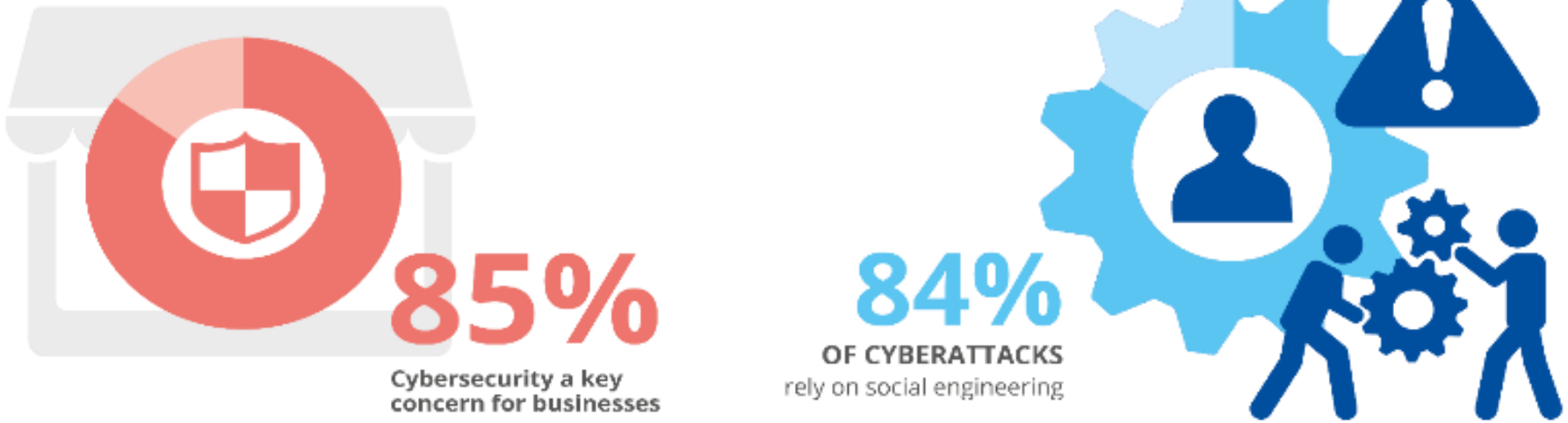
CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Quali rischi la preoccupano maggiormente?

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Quali sono le principali sfide che una PMI deve affrontare in ambito cyber?

La survey ENISA sullo stato delle PMI in Europa



il POST

ITALIA | GIOVEDÌ 12 MAGGIO 2022

In Italia si sa sempre pochissimo degli attacchi informatici

Le istituzioni decidono spesso di non comunicare nulla o di negare, con il rischio che le conseguenze vengano ingigantite o sminuite

Gli investimenti delle PMI in Italia

Contesto di riferimento:

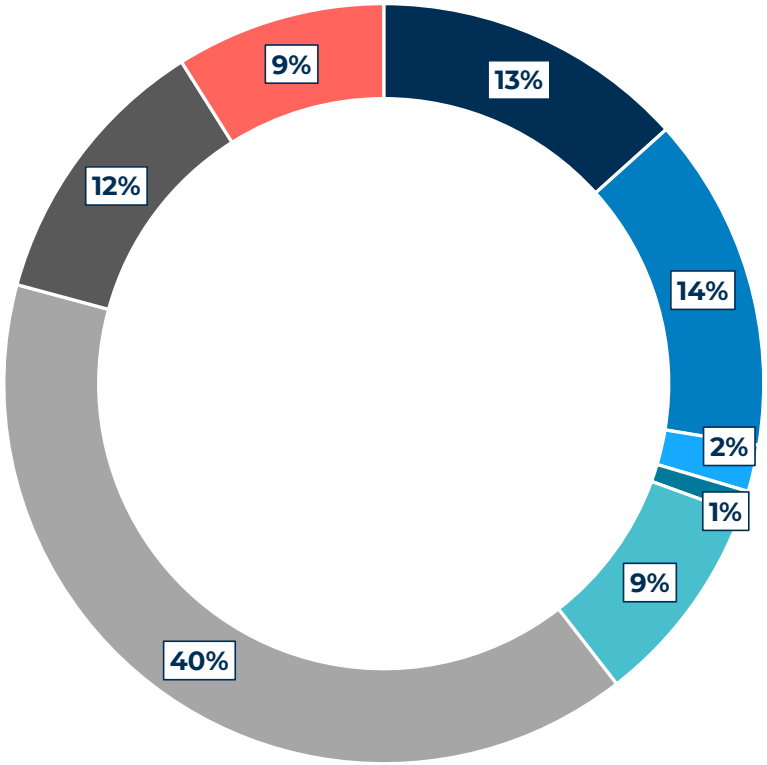
- 4.4 Mln di imprese in Italia:
  - 95.05% → **Micro**
  - **4.86% → Piccole Medie Imprese**
  - 0.09% → **Grandi Imprese**

Secondo un sondaggio condotto da SWG per Confesercenti:

- **26% delle Piccole Medie Imprese è stata colpita da un attacco informatico durante il 2022**
- **il 52% delle PMI tra i 10 e i 50 dipendenti prevede di destinare risorse a questo fine nell'anno in corso,**
- **con una spesa media di 4.800 euro per impresa per un totale di oltre 470milioni.**

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

Le responsabilità della sicurezza informatica nelle PMI



- Esiste una figura interna responsabile della sicurezza delle informazioni
- È nella funzione Sistemi Informativi
- È nella funzione Risorse Umane
- È nella funzione Legal and Compliance
- Altre funzioni
- Consulenti esterni
- Imprenditore/ Direttore Generale
- NESSUNO

Fonte: Survey 2021 PMI – Campione: 503 piccole e medie imprese

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Le misure di protezione e prevenzione attualmente in uso

LESS THAN

30%

OF THE PARTICIPANTS

MORE THAN

70%

OF THE PARTICIPANTS

Consapevolezza e formazione nelle PMI italiane

q4 In che misura ritiene che i Suoi dipendenti siano informati in merito ai rischi della criminalità informatica? (%)

Italia
(Grafico esterno)

UE27	Italia
15	17
41	42
22	25
10	7
12	8

Molto informato/a
Abbastanza informato/a
Non molto informato/a
Per niente informato/a
Non sa

q5 Negli ultimi 12 mesi, la Sua azienda ha organizzato per i propri dipendenti corsi di formazione o eventi di sensibilizzazione in merito ai rischi della criminalità informatica? (%)

Italia
(Grafico esterno)

UE27	Italia
19	15
79	85
3	0

Sì
No
Non sa

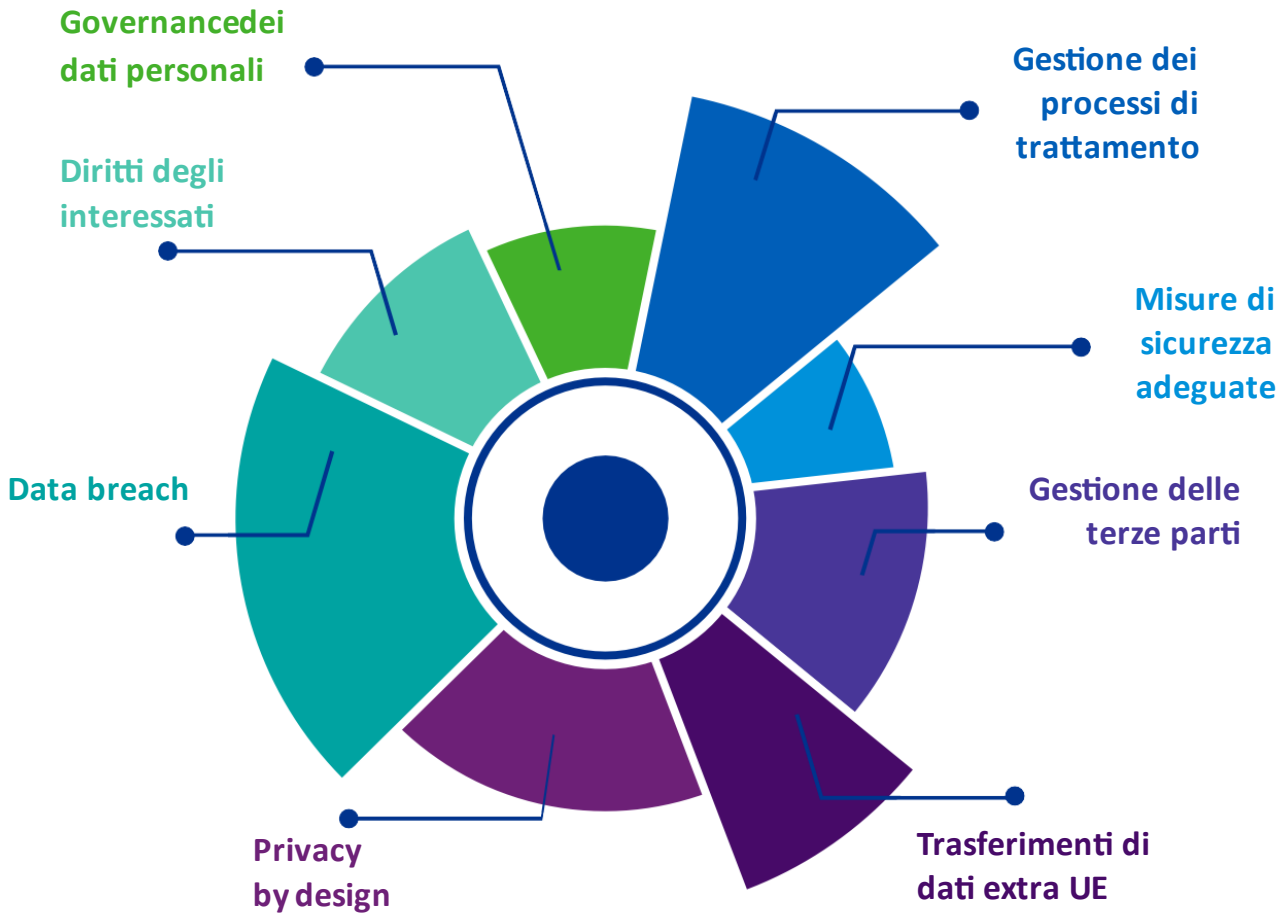
Obblighi normativi applicabili alle PMI

GDPR
La protezione dei dati personali

La mancata conformità può esporre la società a rischi **reputazionali, economici, operativi.**

Le sanzioni amministrative pecuniarie introdotte dal GDPR:

- **10 milioni di euro o 2% del fatturato** mondiale annuo per le imprese
- **20 milioni di euro o 4% del fatturato** per le imprese (nei casi più gravi)



Obblighi normativi applicabili alle PMI

NIS e PSNC

- La Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione (Direttiva NISUE 2016/1148) mira a raggiungere un livello comune elevato in materia di sicurezza delle reti e dei sistemi di informazione in tutta l'UE, applicabile alle aziende che forniscono un servizio essenziale per il mantenimento di attività sociale e/o economiche fondamentali sono conosciute come OES.

- **PSNC: framework normativo nazionale in ambito cybersecurity, indirettamente comporta obblighi per le PMI**

OBBLIGHI indiretti sulla filiera di fornitura delle infrastrutture critiche

.. Verso la NIS 2.0

- **Si applica direttamente anche alle medie imprese**

- **Obblighi di analisi e gestione del rischio, applicazione di specifiche misure tecniche ed organizzative, obbligo di notifica (ref. Tassonomia degli incidenti informatici)**

- **Le sanzioni amministrative pecuniarie introdotte ammontano fino a:**
  - ✓ **10 milioni di euro, o 2% del fatturato oppure**
  - ✓ **fino a 7 milioni di euro, o 1,4% del fatturato**

Sintesi: le sfide da affrontare

- Consapevolezza del personale
- Budget insufficiente, Mancanza di personale specializzato, Scarso supporto da parte del top management
- Strumenti di protezione e prevenzione
- Mancanza di linee guida specifiche per le PMI in ambito cybersecurity
- Sistemi IT non gestiti direttamente – Gestione fornitori
- Gestione degli incidenti

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Quali iniziative in corso?

Piano di assessment Cyber e IT

Cyber 4.0/ DIH

Vademecum PMI

Cyber 4.0/ Unindustria/ ENISA

Roadshow cyber security

Cyber 4.0/ SFC

Area Demo

Cyber 4.0/ Research Partners

Strumenti, Analisi, Awareness, Servizi, Test-before-invest

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Costruzione di una rete Quantum Key Distribution per la sicurezza dei dati

- **Giampiero PEPE**, *Responsabile scientifico CTE Matera*
- **Angelo GIULIANA**, *Direttore Generale Meditech*

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Opportunità di formazione ed orientamento in materia di cybersecurity

Il Cybersecurity Assesment per le PMI: conoscere i propri punti deboli per difendersi

- **Martina CASTIGLIONI,** *Responsabile formazione ed orientamento, Cyber 4.0*

Opportunità di formazione ed orientamento - le iniziative in corso

Piano di assessment Cyber e IT

Cyber 4.0/ DIH

Vademecum PMI

Cyber 4.0/ Unindustria/ ENISA

Roadshow cyber security

Cyber 4.0/ SFC

Area Demo

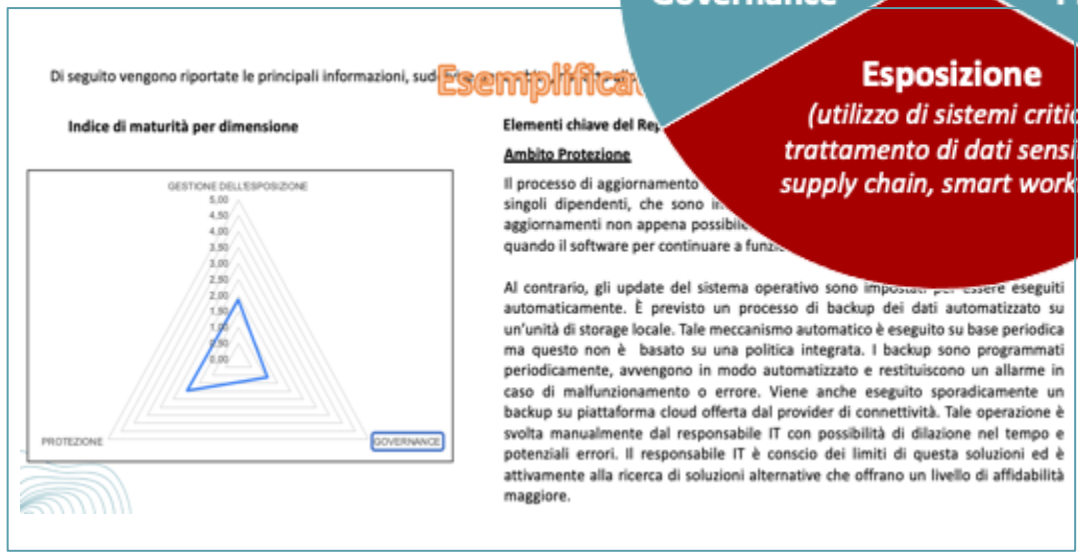
Cyber 4.0/ Research Partners

Strumenti, Analisi, Awareness, Servizi, Test-before-invest

Cybersecurity assessment per le PMI

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Il *Test Cybersecurity e Infrastrutture IT - OT fornisce una valutazione del* ***livello di sicurezza cibernetica delle infrastrutture e soluzioni IT presenti in azienda.***



Tutti i risultati sono poi elaborati in maniera personalizzata, sulla base di quanto raccolto dagli specialisti del DIH e con il supporto specialistico di Cyber 4.0; all'interno di uno specifico report sono illustrate le evidenze specifiche e le possibili linee di intervento.

Cybersecurity assessment per le PMI

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Remediation proposte per far fronte alle vulnerabilità emerse. Per ciascuna proposta sono descritti:

- ***i tempi di attuazione***
- ***impatto economico stimato***
- ***possibili soluzioni tecnologiche a supporto***
- ***priorità di implementazione (alta, a medio e lungo termine)***

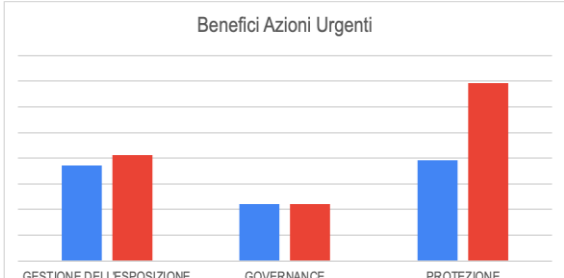
La priorità di implementazione è stata stabilita in accordo con le indicazioni di ENISA presenti nel documento «Cybersecurity for SMES».

Summary remediation Cyber azioni PRIORITARIE

CICERO DIH LAZIO

VALUTAZIONE BENEFICI

Come si vede dal grafico, i primi miglioramenti prodotti dalle remediation **prioritarie** si riflettono in un aumento significativamente la **protezione** (quasi del doppio), lasciando invariata la **governance**. Il livello di **gestione dell'esposizione** aumenta leggermente.



VALUTAZIONE IMPATTO

L'impatto relativo allo sviluppo delle remediation **PRIORITARIE** è stimato rispetto ai seguenti range:

1. **Effort risorse umane intere**: dalle 2 alle 4 giornate
2. **Costi servizi professionali**: tra i 1.000 e i 1.200 euro
3. **Costi HW-SW**: nessun costo

Costi Servizi Professionali

Gestione Esposizione	Protezione	Governance	Infrastruttura
0	1.000/1.200€	0	0

Costi HW-SW

Gestione Esposizione	Protezione	Governance	Infrastruttu
0	0	0	0

Esemplificativo

Cybersecurity assessment per le PMI

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Lo stato delle pratiche di cybersecurity dell'impresa viene valutata su una scala a 5 livelli

	GESTIONE DELL'ESPOSIZIONE	GOVERNANCE	PROTEZIONE
5	Esposizione al rischio gestita in maniera integrata attraverso le diverse funzioni aziendali; ottima maturità digitale/preparazione al cambiamento.	Aspetti di governance sistematicamente controllati, sviluppati e gestiti in maniera integrata attraverso le diverse funzioni aziendali; ottima maturità digitale/preparazione al cambiamento.	Procedure e tecnologie a protezione degli asset sistematicamente sviluppate e gestite in maniera integrata attraverso le diverse funzioni aziendali; ottima maturità digitale/preparazione al cambiamento.
4	Esposizione al rischio gestita in maniera integrata attraverso le diverse funzioni aziendali; buona maturità digitale/preparazione al cambiamento.	Aspetti di governance generalmente controllati, sviluppati e gestiti in maniera generalmente integrata attraverso le diverse funzioni aziendali; buona maturità digitale/preparazione al cambiamento.	Procedure e tecnologie a protezione degli asset generalmente sviluppate e gestite in maniera generalmente integrata attraverso le diverse funzioni aziendali; buona maturità digitale/preparazione al cambiamento.
3	Esposizione al rischio gestita in maniera parzialmente integrata attraverso le diverse funzioni aziendali; discreta maturità digitale/preparazione al cambiamento.	Aspetti di governance discretamente controllati, e gestiti in maniera parzialmente integrata attraverso le diverse funzioni aziendali; discreta maturità digitale/preparazione al cambiamento.	Procedure e tecnologie a protezione degli asset discretamente controllate e gestite in maniera parzialmente integrata attraverso le diverse funzioni aziendali; discreta maturità digitale/preparazione al cambiamento.
2	Esposizione al rischio gestita esclusivamente a partire dall'esperienza dell'imprenditore, amministratore delegato o manager di area; limitata maturità digitale/preparazione al cambiamento.	Aspetti di governance parzialmente controllati e gestiti esclusivamente a partire dall'esperienza dell'imprenditore, amministratore delegato o manager di area; limitata maturità digitale/preparazione al cambiamento.	Procedure e tecnologie a protezione degli asset gestite esclusivamente a partire dall'esperienza dell'imprenditore, amministratore delegato o manager di area; limitata maturità digitale/preparazione al cambiamento.
1	Fattori di esposizione al rischio poco controllati, gestiti *ad hoc* e solo reattivamente; scarsa maturità digitale/preparazione al cambiamento.	Aspetti di governance poco controllati, gestiti *ad hoc* e solo reattivamente; scarsa maturità digitale/preparazione al cambiamento.	Procedure e tecnologie a protezione degli asset poco controllate, con sistemi poco avanzati, gestiti *ad hoc* e solo reattivamente; scarsa maturità digitale/preparazione al cambiamento.

Fonte = Università della Sapienza di Roma

Cybersecurity assessment per le PMI

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Sezione Questionario Infrastrutture IT – OT

Esempio compilato dal Mentor (questionario base)

Quali soluzioni software sono adottate in azienda?

	Soluzioni				Dipendenza dei processi		
	1	2	3	4	Totale	Parziale	Nulla
Progettazione ed Ingegneria	CAD	CAM	VC/PDM	EXCEL	FALSO	FALSO	FALSO
Produzione	MES	APS	ERP	Altro (specificare)	FALSO	FALSO	FALSO
Qualità	DMS	AMS	IMS	Altro (specificare)	FALSO	FALSO	FALSO
Manutenzione	CMMS	EAM		Altro (specificare)	FALSO	FALSO	FALSO
Logistica	WMS	TMS		INVOICEX per magazzino e DDT	FALSO	VERO	FALSO
Supply Chain	MRP	EDI		Altro (specificare)	FALSO	FALSO	FALSO
Risorse Umane	Amministrazione	Gestione personale	WFM	Altro (specificare)	FALSO	FALSO	FALSO
Marketing, Customer Care e Vendita	CRM	Chatbot	E Commerce	su sit vendi			

Sono presenti stampanti condivise in rete oppure individuali? **INFRASTRUTTURA IT**
Utilizziamo solo stampanti condivise in rete con un sistema di autorizzazioni e monitoraggio delle stampe.
Utilizziamo sia stampanti condivise in rete che stampanti individuali.
Utilizziamo stampanti individuali assegnate agli uffici.

L'azienda utilizza applicazioni e servizi sul cloud? **INFRASTRUTTURA IT**
Si, tutte le applicazioni utilizzate sono su cloud (es. webmail, servizi di cloud data store come Dropbox, etc.)
Sì, utilizziamo applicazioni basate su cloud, insieme ad applicazioni installate sulla nostra infrastruttura IT locale.
No, utilizziamo solo applicazioni installate sui server della nostra infrastruttura IT locale.
No, utilizziamo solo applicazioni installate sui personal computer desktop presenti in azienda.

Il censimento degli asset per processo permette di:

1) ***Acquisire consapevolezza da parte della PMI in merito agli strumenti utilizzati, per ciascun processo;***
2) *Concretizzare gli output dei risultati cybersecurity, inserendo riferimenti* ***in merito ad asset e processi supportati;***
3) ***Customizzare l'identificazione delle raccomandazioni*** *che compongono la roadmap cybersecurity consigliata;*
4) ***Formalizzare*** *, tramite l'aiuto del Mentor ed in maniera efficace,* ***un primo censimento del perimetro tecnologico della PMI,*** *e dunque della superficie a rischio informatico.*

Cybersecurity assessment per le PMI

Project Stream Misure di Remediation Cybersecurity

In base alla priorità, è stato determinato un ordine di attivazione delle remediation

Esemplificativo

Azioni Prioritarie

1. Politica di gestione delle password
2. Adozione antivirus e antimalware

Le misure prioritarie rappresentano un set di misure minime da applicare al fine di incrementare il livello di sicurezza cyber dell'Organizzazione (che rientrano tra i 12 steps del framework ENISA «Cybersecurity guide for SMEs).

Ulteriori Azioni suggerite

1. Identificazione dati personali
2. Censimento hardware e software
3. Verifica dispositivi in uso
4. Protezione dispositivi
5. Piano gestione degli incidenti
6. Nomina responsabili IT
7. Attività di formazione cyber
8. Nomina responsabile comunicazione

Le ulteriori azioni suggerite definiscono una serie di azioni da programmare per il consolidamento e il potenziamento degli aspetti di sicurezza cyber in ottica di prevenzione dei rischi alla sicurezza delle informazioni.

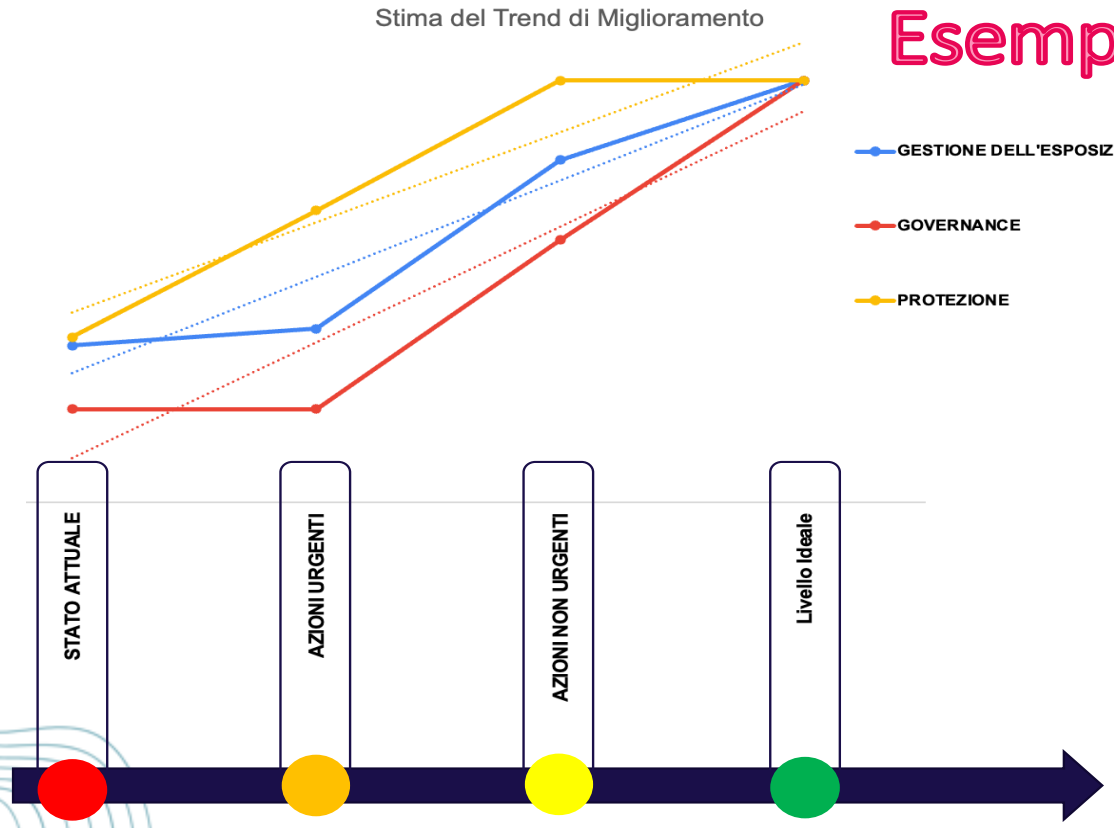
Cybersecurity assessment per le PMI

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CICERO DIH LAZIO

Risultati Attesi - Cybersecurity

Nel presente grafico viene illustrata una stima di miglioramento per quanto riguarda gli ambiti di Esposizione, Governance e Protezione.
N.B. La presente stima costituisce una simulazione indicativa dei miglioramenti apportati grazie all'applicazione delle remediation.



Esemplificativo

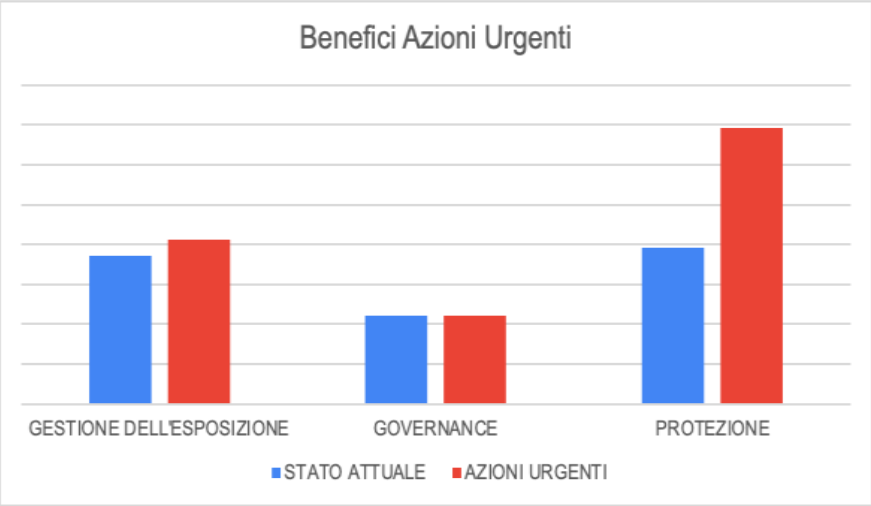
Come si vede dal grafico, partendo dallo stato attuale dopo l'implementazione delle azioni urgenti, il livello di protezione aumenta significativamente. Allo stesso tempo, si può notare un leggero incremento nel livello di gestione dell'esposizione. Con l'applicazione delle azioni non urgenti, si nota come la protezione continui a crescere proporzionalmente allo stadio precedente. In questo caso, si verificano aumenti significativi sia nei livelli di gestione dell'esposizione che in quelli di governance.

Cybersecurity assessment per le PMI

Summary remediation Cyber azioni PRIORITARIE

VALUTAZIONE BENEFICI

Come si vede dal grafico, i primi miglioramenti prodotti dalle remediation **prioritarie** si riflettono in un aumento significativamente la **protezione** (quasi del doppio), lasciando invariata la **governance**. Il livello di **gestione dell'esposizione** aumenta leggermente.



VALUTAZIONE IMPATTO

L'impatto relativo allo sviluppo delle remediation **PRIORITARIE** è stimato rispetto ai seguenti range:

1. **Effort risorse umane intere**: dalle 2 alle 4 giornate
2. **Costi servizi professionali**: tra i 1.000 e i 1.200 euro
3. **Costi HW-SW**: nessun costo

Costi Servizi Professionali

Gestione Esposizione	Protezione	Governance	Infrastruttura
0	1.000/1.200€	0	0

Costi HW-SW

Gestione Esposizione	Protezione	Governance	Infrastruttura
0	0	0	0

Esemplificativo

Le iniziative in corso

Piano di assessment Cyber e IT

Cyber 4.0/ DIH

Vademecum PMI

Cyber 4.0/ Unindustria/ ENISA

Roadshow cyber security

Cyber 4.0/ SFC

Area Demo

Cyber 4.0/ Research Partners

Strumenti, Analisi, Awareness, Servizi, Test-before-invest

Vademecum - Le buone pratiche per le PMI

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

1 SVILUPPARE UNA SOLIDA CULTURA DELLA CIBERSICUREZZA

2 FORNIRE UNA FORMAZIONE APPROPRIATA

3 GARANTIRE UN'EFFICACE GESTIONE DEI TERZI

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

enisa

AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA

4 SVILUPPARE UN PIANO DI RISPOSTA AGLI INCIDENTI

5 RENDERE SICURO L'ACCESSO AI SISTEMI

11 RENDERE SICURI I SITI ONLINE

12 CERCARE E CONDIVIDERE LE INFORMAZIONI

Overview – 4. Sviluppare un piano di risposta agli incidenti

Elaborare un piano formale di risposta agli incidenti che contenga orientamenti, ruoli e responsabilità chiari e documentati per garantire che tutti gli incidenti a livello della sicurezza siano affrontati in modo tempestivo, professionale e appropriato. Per rispondere prontamente alle minacce per la sicurezza, studiare gli strumenti che potrebbero monitorare e creare allerta in caso di attività sospette o di violazioni della sicurezza.

Parole chiave (data breach, incidente ad impatto rilevante,…)

- **Come costruire un modello di gestione degli incidenti**? Descrizione delle fasi e delle attività e controlli organizzativi, tecnici.

- Modalità di segnalazione e notifica degli incidenti informatici

- Normativa nazionale e comunitaria (NIS, D.Lgs 65/2018, PSNC)
- Riferimento ai portali e modalità di notifica degli incidenti (Garante Privacy, CSIRT)
- Framework Nazionale Cybersecurity e data protection
- ISO 27035 – Information Security Incident Management System

Box di approfondimento

Le iniziative in corso

Piano di assessment Cyber e IT

Cyber 4.0/ DIH

Vademecum PMI

Cyber 4.0/ Unindustria/ ENISA

Roadshow cyber security

Cyber 4.0/ SFC

Area Demo

Cyber 4.0/ Research Partners

Strumenti, Analisi, Awareness, Servizi, Test-before-invest

Le iniziative in corso

Piano di assessment Cyber e IT

Cyber 4.0/ DIH

Vademecum PMI

Cyber 4.0/ Unindustria/ ENISA

Roadshow cyber security

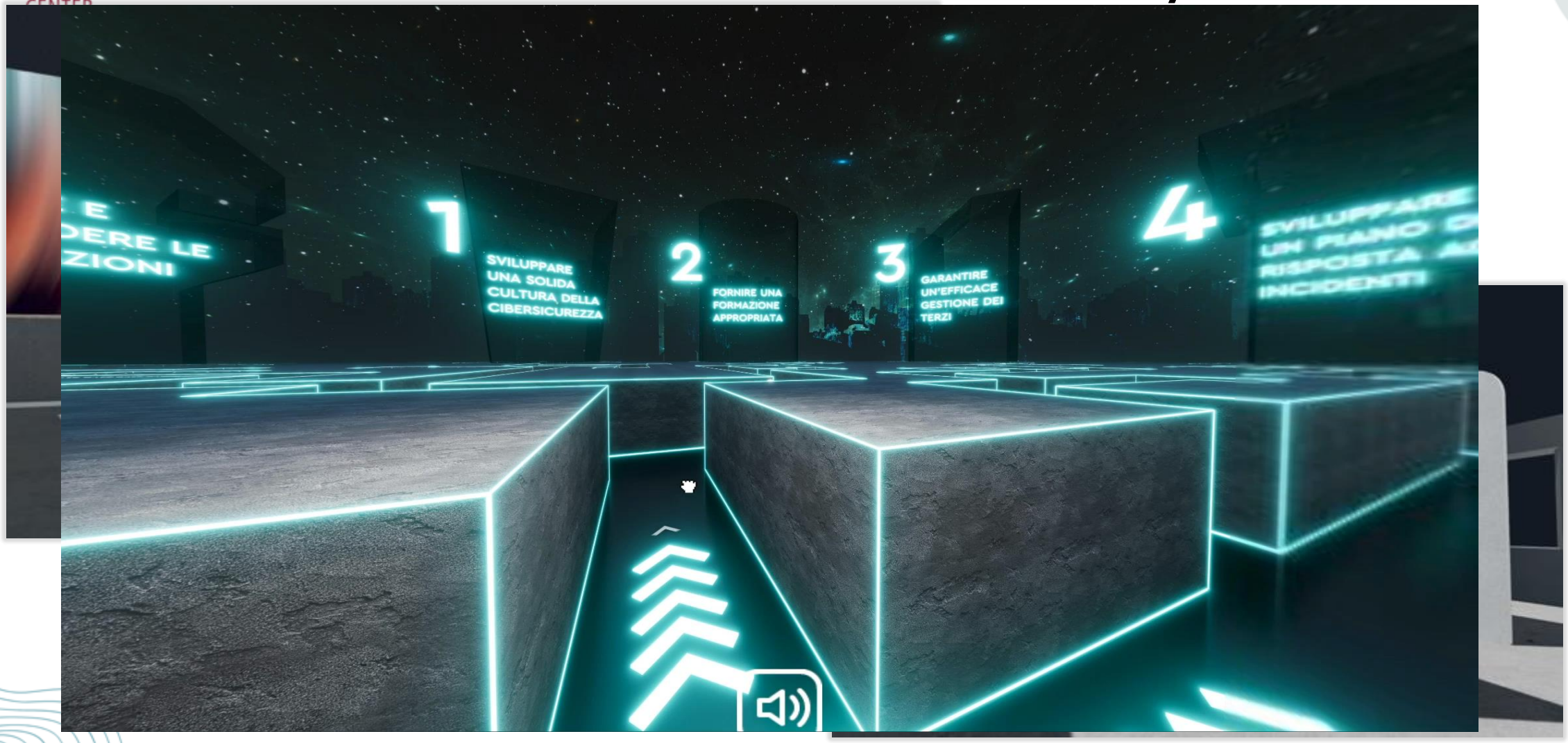
Cyber 4.0/ SFC

Area Demo

Cyber 4.0/ Research Partners

Strumenti, Analisi, Awareness, Servizi, Test-before-invest

Area demo Cyber 4.0 – Test before invest – Cyber Atlas



Catalogo dei servizi a supporto delle PMI

Servizi a catalogo che il Centro eroga 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

L’offerta Cyber 4.0 per informare e formare le PMI

Formazione a catalogo

Formazione customizzata

Istituzione

Impresa

Singolo cittadino

PMI (cofinanziamento)

L’offerta Cyber 4.0 per informare e formare le PMI

IL CATALOGO FORMATIVO

- 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

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Iniziative di formazione ed orientamento per la regione Basilicata

- **Silvia Masciulli, HR Manager Italy,** *Innovery (in videocollegamento)*

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

PRIMA PARTE

Gestione del rischio cyber, un paradigma culturale da adottare: dalla simulazione di un attacco cyber alle attività di rimedio

- **Daniele Riccardo INCERTI**, *Consulente Cybersecurity Sistemi Formativi Confindustria*
- **Vincenzo VITIELLO**, *Consulente Cybersecurity Sistemi Formativi Confindustria*

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SECONDA PARTE

Simulazione di attacchi cyber e modalità di difesa

- **Daniele Riccardo**, *Consulente Cybersecurity Sistemi Formativi Confindustria*
- **Vincenzo VITIELLO**, *Consulente Cybersecurity Sistemi Formativi Confindustria*

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Per rimanere aggiornati sulle attività di Cyber 4.0

Profilo LinkedIn

CYBER 4.0 - Cybersecurity Competence Center

Sito web

www.cyber40.it

Newsletter bisettimanale

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Chiusura lavori

Grazie per l’attenzione

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SISTEMI FORMATIVI CONFINDUSTRIA

LUISS

ROADSHOW CYBER 4.0

PROSSIME TAPPE

16 Marzo - Potenza

21 Marzo - Cosenza

6 Aprile - Milano

13 Aprile - Ancona

10 Maggio - Firenze

18 Maggio - Torino

15 Giugno - Parma

22 Giugno - Udine

4 Luglio - Trento