CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

La cybersecurity e le PMI
Napoli, 28.06.2022

Strategie di protezione e sviluppo per una transizione digitale sicura

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

Cybersecurity e PMI – Il contesto EU

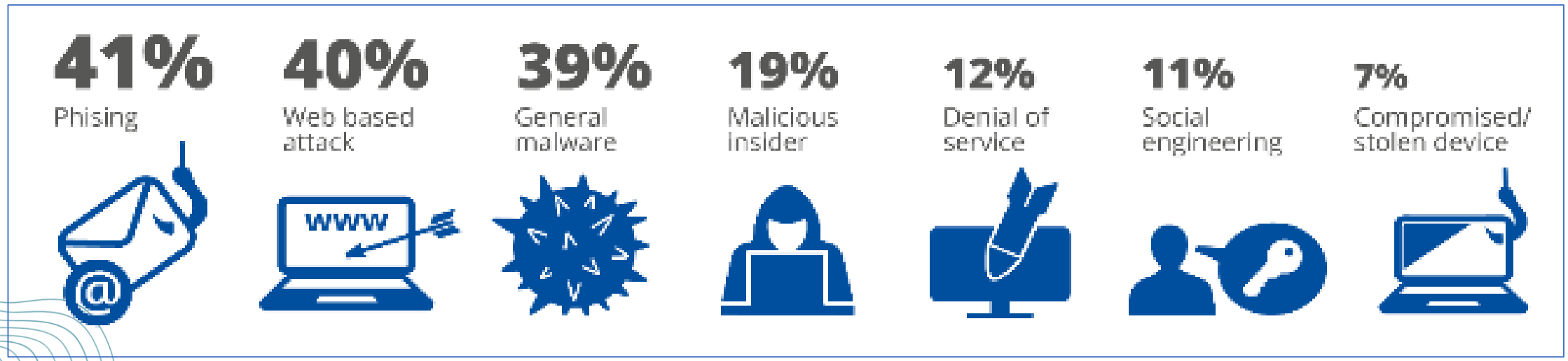
85%

Cybersecurity a key concern for businesses

84%

OF CYBERATTACKS

rely on social engineering



CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

L’uso delle tecnologie di protezione nelle PMI

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 – Chi siamo e cosa facciamo

- Avviato nel 2020, **Operativo dal 2021, HQ al Tecnopolo – Roma**
- **8 Organismi di ricerca, 1 Istituzione pubblica, 35 Partner privati, in espansione**
- **Servizi specialistici per PMI e PA**
- **Formazione e Orientamento**
- Finanziamento di **progetti di ricerca e innovazione** sui 4 domini di competenza: **CYBERSECURITY CORE, AEROSPACE, AUTOMOTIVE, HEALTHCARE**
- **Networking istituzionale e di business**

Network istituzionale e professionale

Collaborazioni NAZIONALI

- **MISE**
- **ACN**
- **Regione Lazio**
  - **Accademia Cybersicurezza Lazio**
- **Rete DIH**
- **Rete CC**
- **MoU Quantum Initiative**
- **Rete Nazionale ITS**
- **Lazio Innova**
  - Laboratorio di microinnovazione PMI e Start-up

Collaborazioni INTERNAZIONALI

- **ENISA**
- **ECSO**
- **Agenzia Catalana di Cybersecurity**
  - Cooperazione tecnica, promozione Innovazione, Best Practice, knowledge sharing
- **HorizonEurope**
  - HORIZON-CL3-2022-CS-01-01
- **CONCORDIA – Stakeholders' Group**
- **EU CyberNet** –Stakeholder Group
  - Capacity building, Rete di Esperti UE
- Altri Progetti UE

FOCUS PMI – I progetti in corso

Piano di assessment Cyber e IT

Cyber 4.0/ DIH

Vademecum PMI

Cyber 4.0/
Unindustria/ ENISA

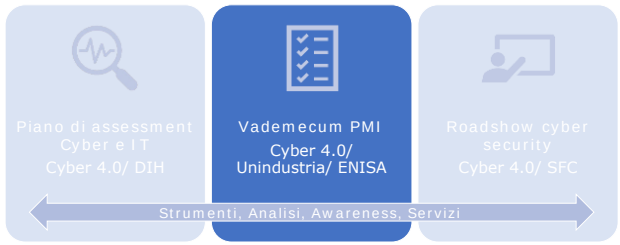
Roadshow cyber security

Cyber 4.0/ SFC

Strumenti, Analisi, Awareness, Servizi

VADEMECUM CYBERSECURITY per le PMI ITALIANE

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER



enisa

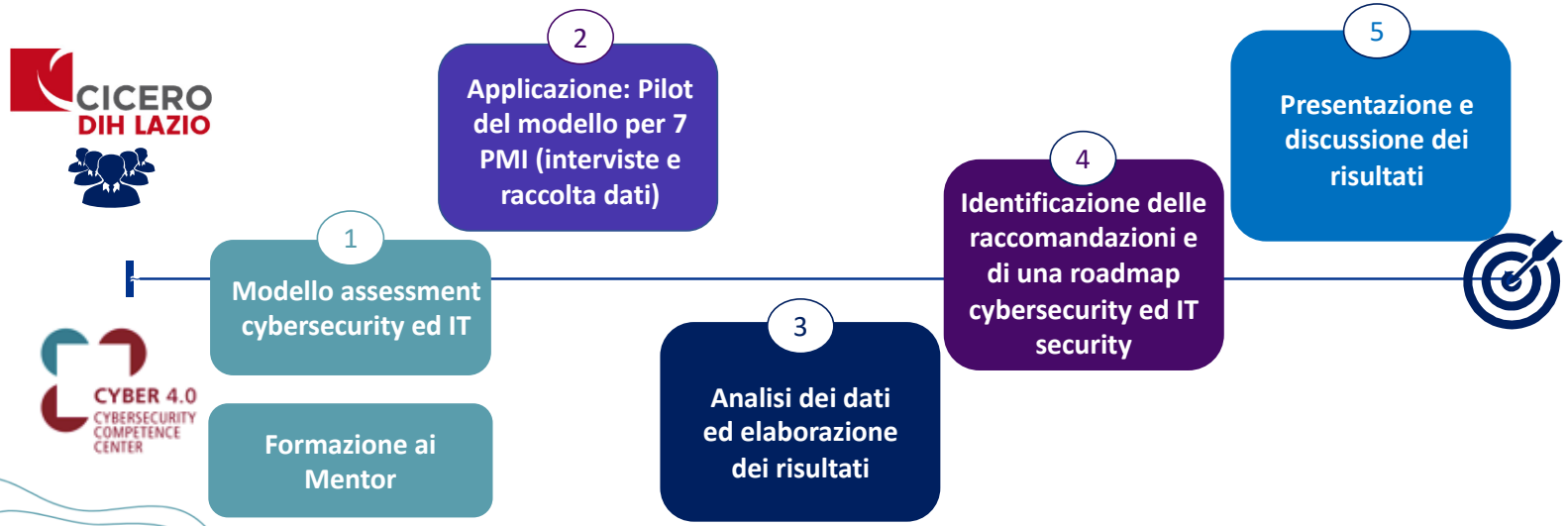
CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

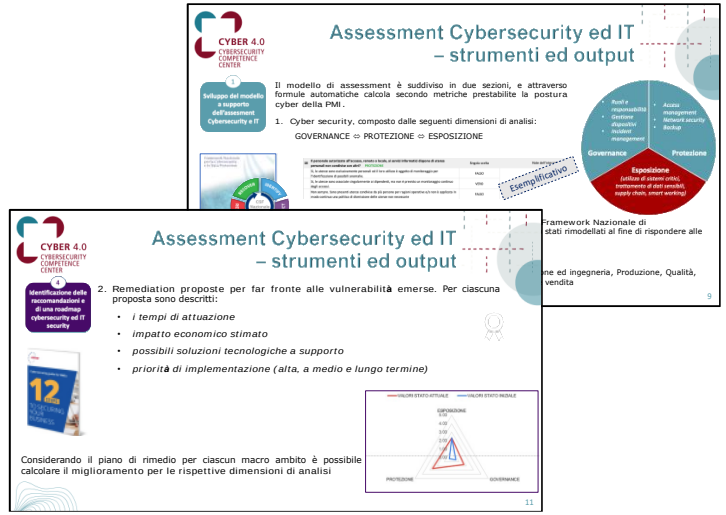
UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE DI ROMA • FROSINONE • RIETI • VITERBO

- Lancio a luglio 2022
- Realizzazione Area Demo
- **Forum Cyber 4.0**
  - **Roma, 19-20 Ottobre 2022**

Cyber/ IT Assessment

- Pilota con DIH Lazio per «Diagnosi Digitale» PMI del Lazio, supporto Regione Lazio
- Applicazione **Framework Nazionale di Cybersecurity e Protezione dei Dati Personali**
- **ESTENSIONE NAZIONALE** (pilota con DIH Lombardia)
- Coordinamento con rete dei PID delle Camere di Commercio





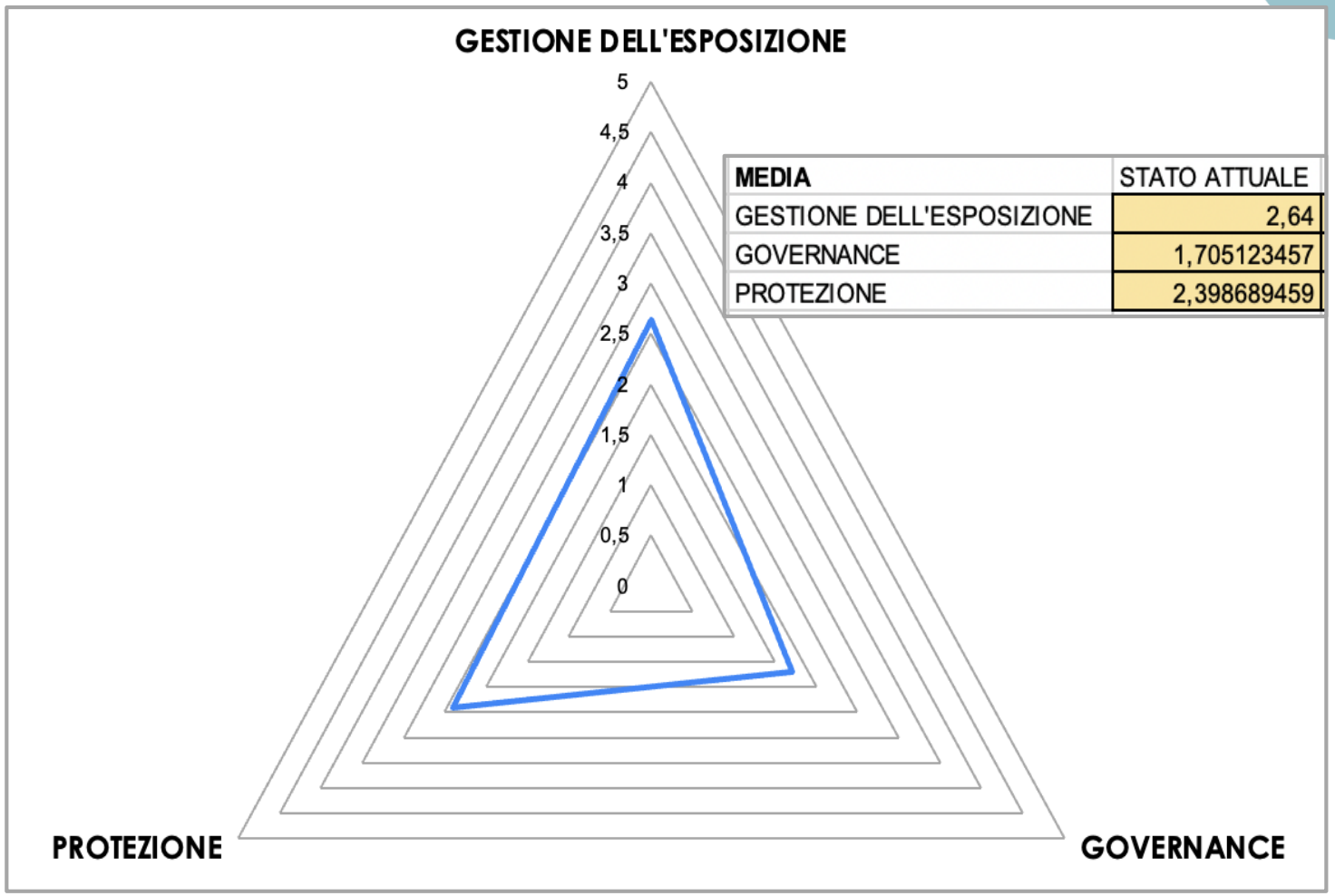
Risultati preliminari degli assessment effettuati su PMI della Regione Lazio

Gli assessment svolti finora permettono di monitorare, con un approccio statistico, i risultati degli AS-IS.

Il grafico mostra la **media** degli indici cyber per ambito di valutazione, derivanti dagli AS-IS.

È possibile notare come, in media, le PMI presentino un basso livello di **governance** e dei livelli medio-bassi di **protezione** e **gestione dell'esposizione.**

La tabella mostra la **media** di ciascuna dimensione di analisi in valore numerico.



MEDIA	STATO ATTUALE
GESTIONE DELL'ESPOSIZIONE	2,64
GOVERNANCE	1,705123457
PROTEZIONE	2,398689459

Le raccomandazioni di ENISA

Piani info/ formative per incrementare la Consapevolezza

Definizione di line guida specifiche per il contesto PMI

Valutare la definizione di standard specifici rivolti alle PMI

Promozione dell'uso di Framework di riferimento per la gestione del rischio cyber

Rendere accessibile la cybersecurity, risorse umane e economiche

Promuovere la creazione degli ISAC settoriali

La Strategia Nazionale di Cybersicurezza

Le sfide

- Assicurare una **transizione digitale cyber resiliente** della Pubblica Amministrazione (PA) e del tessuto produttivo
- **Anticipare l'evoluzione della minaccia cyber**
- Contrastare la **disinformazione online** nel più ampio contesto della cd. minaccia ibrida
- Gestione di **crisi cibernetiche**
- **Autonomia strategica nazionale ed europea nel settore del digitale**

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

La Strategia Nazionale di Cybersicurezza – Gli obiettivi

Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli obiettivi strategici sono suddivisi su

82 azioni

da implementare entro il 2026

Un Piano di Implementazione è definito con soggetti coinvolti e obiettivi temporali

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Servizi Cyber 4.0 per imprese
80+ servizi mappati su 8 categorie

Identificazione e gestione rischi cyber

Protezione dei Dati

Protezione dei Sistemi

Monitoraggio e rilevamento minacce cyber

Risposta e gestione degli incidenti

Certificazioni

Formazione

Consulenza

www.cyber40.it

Servizi Cyber 4.0 per imprese
Es. Cyber Risk

Identificazione e gestione rischi cyber

Protezione dei Dati

Protection dei Sistemi

Monitoraggio e rilevamento minacce cyber

Risposta e gestione degli incidenti

Certificazioni

Formazione

Consulenza

Cyber risk assessment and management

- Assessment e Gap Analysis su normative di settore, standard internazionali, framework e best practice. **Framework nazionale per la cyber security e la data protection**, GDPR, Direttiva NIS, Perimetro di sicurezza nazionale cibernetica, ISO 27001, ISO 22301, ISO 22318; COSO e ISO 31000
- Orchestrazione dati per Valutazione del rischio near-realtime
- Focus su ambienti industriali (ICS/ SCADA) e soluzioni IoT, Standard ISO/IEC 62443. Gestione del rischio e design di soluzioni di sicurezza
- Piattaforma di Cyber Risk Management in forma SaaS: mappatura degli asset e dei processi, identificazione dei rischi, supporto alla gestione del rischio e alla compliance normativa, audit.
- Valutazione del rischio cyber in forma SaaS: massimo danno probabile ed esposizione al rischio, secondo gli standard di riferimento ISO 31000 e ISO 27005

Risk monitoring

- Visual Analytics per il monitoraggio dei rischi cyber di una rete di calcolatori

Vulnerability assessment e Penetration Testing

- Vulnerability assessment e simulazione di attacco a più fasi per evidenziare capacità di difesa e livello di penetrazione raggiunto nei confronti delle vulnerabilità interne ed esterne al sistema e della sicurezza fisica
- Penetration testing con approccio grey box: analisi documentazione di prodotto e identificazione di una catena di attacco per ottenere il controllo del sistema testato o compromettere funzioni base per la safety o per il suo controllo remoto

Threat Intelligence

- Monitoraggio continuo del web open source e dark, identificazione minacce e analisi con tecnologie di intelligenza artificiale, machine learning, big data analytics e high performance computing.

Monitoraggio della supply chain

- Assessment, audit e valutazione dei fornitori – con scoring. Standard di riferimento: ISO 27001; NIST; OWASP; ISO 22301; NIS; GDPR; CS CCM.

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Ricerca e Innovazione
7 progetti finanziati – Bando 1

PILLAR	NOME PROPOSTA	Coordinatore	Partner	Collaborazione con Organismi di Ricerca
CORE	**ConTI** – Contextual Threat Inteligence	Haruspex	Leonardo	Cyber 4.0 Sapienza
CORE	**BRIE** – Blockchain register for Import Export	Moveax	Chainside	Cyber 4.0 Sapienza
CORE	**KEEPCALM** – Kernel Engines Enable (to) Prevent Cyber Attacks (with) Learning Machines	SOGEI	ISC	Cyber 4.0 Luiss
AUTO	**M-A-C-S** – Multibrand Automotive Cybersecurity Software	Tomware	NetGate Consorzio W3 Make	LazioConnect
HEALTH	**MAPS-EH** - Policy di sicurezza in campo eHealth	Aton	DeepBlue	Cyber 4.0 LazioConnect Uni Milano Bicocca
HEALTH	**ISHealth** - Improved Security e-Health	Sigma Consulting	IoT Maker	Sapienza
SPACE	**QCS-TB** - Quantum Communication and Synchronization Testbed	Thales Alenia Space Italia	Telespazio Micro Photon Devices	Cyber 4.0 Sapienza

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Ricerca e Innovazione
8 progetti finanziati – Bando 2

CORE	**CybersecH -** Cybersecurity hardening for AI solutions	3rd Place	[NO]	Uni Tuscia
CORE	**BINTRAWINE** - Blockchain, Tracking and Tracing solutions for Wine	Aton srl	BSD Design	Cyber 4.0 Sapienza
AUTO	**SHINE-ON** - Secured HIgh accuracy localizatioN Equipment for automotive applicatioNs	RadioLabs	Drivesec	Cyber 4.0 Uni Aquila
SPACE	**QKD SVS** - QKD System Volume Simulator	ThinkQuantum	Thales Alenia Space Italia Telespazio Officina Stellare Enginium	Cyber 4.0 Uni PD
HEALTH	**SI-PAC** - Sistema Informativo per la Sicurezza della Gestione dei Pacchetti Ambulatori Complessi	HMS IT	[NO]	Uni Tor Vergata
HEALTH	**PEHSA** - Pleyo E-Health: Secure APP	Dominio Project	[NO]	[NO]
HEALTH	**SEPLES** - SEcure PLatform of E-health Services	ECUBIT	Crypt Security	Uni Tor Vergata ISS
HEALTH	**CY-CAD** - Cyber-security framework for medical data dissemination	DeepBlue	Tlogos	Cyber 4.0 LazioConnect Uni Cattolica

Cyber 4.0 e Formazione 4.0 per PMI

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Formazione 4.0

Awareness

Programmi per **sviluppare e accrescere la cultura e la consapevolezza del contest e dei rischi in ambito cybersecurity**

- *Attiva*
- *Passiva*
- *Continua*

Seminari

Eventi, webinar e workshop realizzati da Cyber 4.0 in modalità uno a molti

Corsi

- *Formazione Base – Avanzata – Specialistica*
- *Sincrona / Asincrona*
- *A catalogo vs Customizzata*

ACADEMY

Percorsi di formazione ad alta specializzazione, tailor made per specifiche realtà aziendali, **sfruttando l'intera offerta formative CYBER 4.0 e la diversità di metodi e strumenti promossi dai Soci di Cyber 4.0**

Cyber 4.0 – I corsi di formazione disponibili per le PMI

- **Cybersecurity essentials**
  - Fondamenti di cybersecurity
  - Corsi avanzati per esperti cybersecurity
  - Cybersecurity e data control
  - Web Application Security
  - Social Media Security
  - Identità digitale
- **Cybersecurity Awareness**
  - Il fattore umano nella cybersecurity
  - Corso di awareness ad alto livello in ambito Cybersecurity
  - Programmi di awareness aziendale attiva in materia di cybersecurity
  - Programmi di awareness aziendale passiva in materia di cybersecurity
  - Programmi di self-awareness aziendale in materia di cybersecurity
- **Legislation**
  - Giurisprudenza, Cybersecurity and Information Security
  - NIS Directive e Cybersecurity ACT
  - Protezione dei dati: il regolamento2016/679 EU (GDPR)
- **Custom**
  - Training specializzato e customizzabile in cybersecurity e protezione dei dati nel contesto Industry 4.0
- **Industry 4.0 e cybersecurity**
  - Cybersecurity in IoT and Industry 4.0
  - IT e OT cybersecurity (ICS / SCADA)
  - Industry 4.0 e digital and green skills.
  - Soft Skills per Industry 4.0
- **Blockchain e criptovalute**
  - Fondamenti di crittografia
  - Introduzione alla blockchain
  - Blockchain - Corso avanzato
  - Blockchain - Governance decentralizzata e modelli di business
  - Smart contracts e applicazioni decentralizzate
  - Blockchain e IoT
  - AI e blockchain per l'automazione dei processi
  - Blockchain e applicazioni automotive
  - Blockchain - Casi d'uso (modulo interattivo)
  - Criptovalute - Introduzione
  - Criptovalute - Sicurezza e Applicazioni
- **Academy**
  - Strategie di formazione cybersecurity
  - Master in cybersecurity: Public policies, regulations and management
- **Data driven enterprise**
  - Data driven enterprise
  - Digital Discovery Lab
  - Digital Innovation & Governance - EMIT
  - Cloud security - Training livello base
  - Cloud computing e cybersecurity - Corso avanzato
- **Exercise**
  - Table top exercise - Gestione delle crisi cibernetiche
  - Sinulazione immersiva - Cyber crisis
  - Simulazione e sistemi cyber-fisici;
  - Cyber range
- **Open innovation**
  - Cybersecurity innovation - Laboratorio di microinnovazione e training

Ciclo di webinar con ACN – Impatto Strategia Nazionale di Cybersecurity

6 Luglio 2022	**Scrutinio tecnologico, certificazione e valutazione di sicurezza**
13 Luglio 2022	**Sanità digitale e impatti di cybersecurity**
20 Luglio 2022	**Information sharing pubblico-privato**
27 Luglio 2022*	**Formazione come leva strategica di cyber resilienza***

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

La cybersecurity e le PMI
Napoli, 28.06.2022

Grazie

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