CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cyber 4.0

Centro di competenza nazionale ad alta specializzazione sulla cybersecurity

Filippo Silvestri – Chief BD Officer

Alessio Gerbaldi – Head of Research & Innovation

Cassino – 28/04/2026

1

Il Centro e il proprio ecosistema

I Centri di competenza

Selezionati nel 2018 dal MIMIT – Ministero delle Imprese e Made in Italy tramite bando pubblico, **i Centri di Competenza ad alta specializzazione sono partenariati pubblico-privati.**

Compiti istituzionali:

- attività di **orientamento e formazione** alle imprese su tematiche Industria 4.0
- **supporto nell'attuazione di progetti di innovazione, ricerca industriale e sviluppo sperimentale** finalizzati alla realizzazione di **nuovi prodotti, processi o servizi (o al loro miglioramento)** tramite tecnologie avanzate in ambito Industria 4.0

Cyber 4.0

- **Associazione no-profit, 8 Università, +40 imprese e fondazioni**
- **Soggetto Attuatore PNRR M4C2 – Inv.2.3 e per l'EDIH Seal of Excellence NEST (Network for EU Security & Trust)**
- **Partner in diversi progetti finanziati dall'Unione Europea** (sia Horizon Europe che Digital Europe)
- **Partner MAECI** per **cybersecurity e cybercrime capacity building internazionale**
- **Raccordo tra PMI ed istituzioni (locali, nazionali, comunitarie)** operanti nel settore della cybersecurity: networking, matchmaking, open innovation, startupping.
- Parte del **network internazionale** per il rafforzamento delle competenze cybersecurity: **EU CyberNet, ECSO, Global Cyber Alliance, ENISA, ECCC, LAC4**

Soci

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Università, enti pubblici e centri di ricerca

Università di Roma Tor Vergata · Roma Tre Università degli Studi · Università degli Studi dell'Aquila · Sapienza Università di Roma · Università degli Studi della Tuscia · LUISS · Università Campus Bio-Medico di Roma · Consiglio Nazionale delle Ricerche · INAIL Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro

Grandi imprese

Posteitaliane · AlmavivA · NETGROUP · DP · aizoon Technology Consulting · Gpi Cyberdefence. · eurosystem Business innovation beyond IT · LEONARDO · TIM · BV TECH · bip. · CY4GATE Elettronica Group · NEVERHACK · intelleraconsulting · HWG Sababa

PMI

Sistemi Formativi Confindustria · S&A Sistemi & Automazione · Data Informatica · Teleconsys · Radiogense · Gruppo infoteam · CYBERSA · Polo di Innovazione Automotive · iptsat · PRISMA improve your business · GRUPPOISC Information Sharing Company · Yalla security · ITHUM it's for human www.ithum.it · WHYSECURITY Cyber Security · LAND · DI.GI. Academy · mediavoice · HERMESBAY enhanced awareness · ANCHARIA cybersecurity · CYBEROO

Fondazioni, associazioni e altri enti

FORMIT · Clusit Associazione Italiana per la Sicurezza Informatica · Fondazione E. Amaldi · FPI Fondazione Piemonte Innova · Lazio Connect

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

2

Il supporto del Centro di Competenza a imprese e PA

PNRR – CdC - M4C2 – I2.3 (03/2023 – 04/2026)

Ministry of Enterprises and Made in Italy

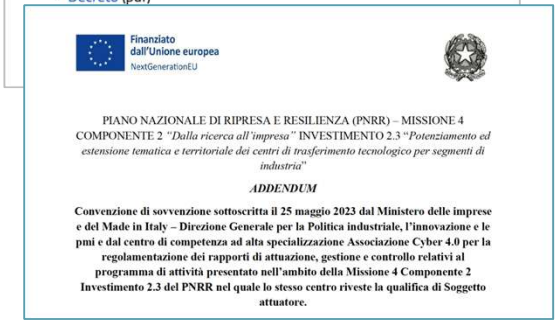
Funded by the European Union
NextGenerationEU

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Decreto ministeriale 10 marzo 2023 - Potenziamento ed estensione dei centri di trasferimento tecnologico

Il decreto ministeriale 10 marzo 2023 definisce le risorse, le procedure e i criteri e il finanziamento a valere sulle risorse messe a disposizione per l'investimento del PNRR "Potenziamento ed estensione tematica e territoriale dei centri di trasferimento tecnologico per segmenti di industria".

- Decreto (pdf)



Finanziato dall'Unione europea
NextGenerationEU

PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2 *"Dalla ricerca all'impresa"* INVESTIMENTO 2.3 *"Potenziamento ed estensione tematica e territoriale dei centri di trasferimento tecnologico per segmenti di industria"*

ADDENDUM

Convenzione di sovvenzione sottoscritta il 25 maggio 2023 dal Ministero delle imprese e del Made in Italy – Direzione Generale per la Politica industriale, l'innovazione e le pmi e dal centro di competenza ad alta specializzazione Associazione Cyber 4.0 per la regolamentazione dei rapporti di attuazione, gestione e controllo relativi al programma di attività presentato nell'ambito della Missione 4 Componente 2 Investimento 2.3 del PNRR nel quale lo stesso centro riveste la qualifica di Soggetto attuatore.

		Risorse	Valore progetti
LINEA A **PROGETTI INFRASTRUTTURALI**	Potenziamento infrastrutture del Centro per l'erogazione di servizi innovativi alle imprese	**3,5 Mln €**	**7 Mln €**
LINEA B1 BANDI DI INNOVAZIONE	Co-finanziamento progetti di ricerca industriale e sviluppo sperimentale ad alto livello di maturità	**4,7 Mln €**	**8 Mln €**
LINEA B2 SERVIZI INCENTIVATI	Servizi co-finanziati con sconto in fattura per la transizione digitale sicura	**10,2 Mln €**	**13 Mln €**
		18,4 Mln €	**28 Mln €**

PNRR – EDIH SoE NEST (03/2023 – 04/2026)

Ministry of Enterprises and Made in Italy

Funded by the European Union
NextGenerationEU

- Partner:
  - **Cyber 4.0** (Coord.)
  - **DIH Lazio**
  - **DIH Umbria**
  - **DIH Abruzzo**
  - **Innova**
- Finanziamento: **4.6 M€, di cui 2,3 M€ per Cyber 4.0**

nest
Network for European Security and Trust

European Commission
SEAL OF EXCELLENCE

		Risorse	Valore progetti
NEST	Servizi co-finanziati con sconto in fattura per la transizione digitale sicura – **PA incluse**	**4,6 Mln €**	**5,6 Mln €**

Servizi incentivati per imprese

988

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

443

Imprese servite
Imprese che hanno beneficiato concretamente dei servizi di supporto cyber erogati

11,5 M€

100%

Incentivi erogati
Utilizzo completo delle risorse disponibili per le imprese
Media aiuti: 80%

3.600+

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

902

Servizi erogati
Servizi contrattualizzati ed erogati, con piena tracciabilità

NEST - Pubbliche Amministrazioni

Ministero della Difesa, Comando per le Operazioni in Rete (COR): Sviluppo framework per la protezione delle infrastrutture spaziali e realizzazione di un teatro di esercitazione su cyber range

Marina Militare/ Centro Supporto e Sperimentazione Navale, Centro Eccellenza Underwater COE: Mappatura rischio infrastrutture, analisi quadro normativo, valutazione capacità operative di protezione, elaborazione scenari di minaccia

Ministero della Giustizia

Assesment tecnologico cyber, revisione, razionalizzazione e messa in sicurezza delle utenze e dei meccanismi di accesso all'ecosistema ICT del Ministero della Giustizia

AGID

Definizione del framework di controlli interni e compliance per adozione NIS 2 in AGID

CODAU
Convegno dei Direttori generali delle Amministrazioni Universitarie

CODAU: Formazione NIS2 Livelli Apicali, 26 Atenei pubblici, 975 discenti

1,1 M€

100%

Incentivi erogati

Utilizzo completo delle risorse disponibili per la PA

Formazione NIS2 CODAU

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

4

Progetti finanziati RI&SS

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CORE — **SATML-B** *Datrix*
Sicurezza degli algoritmi di **Artificial Intelligence e Machine Learning** contro adversarial attacks, data sanitization & anonymization

HEALTH — **WISEPACK** *Radio6ense*
Monitoraggio e protezione delle confezioni dei farmaci tramite **integrazione IoT e sistemi di Intelligenza Artificiali**

AUTO — **CyberGuardEV** *TME*
Dispositivo elettronico innovativo in grado di rilevare e di proteggere da attacchi side-channel le **stazioni di ricarica per veicoli elettrici**

SPACE — **Biosat Marketplace** *IPTSat*
Marketplace con servizi predefiniti per fruizione sicura di **dati provenienti dall'osservazione della Terra** (missioni ESA e costellazione IRIDE)

CORE — **ARGO** *Sistemi & Automazione*
Cyber Threat Intelligence (CTI) e supporto decisionale con Ricerca su Grafi per scoperta dati dispersi su fonti Open di tipo cyber

HEALTH — **Health-e-Data** *Moveax*
Gestione, scambio e utilizzo sicuro di **dati sanitari** – con particolare attenzione ai dati generati in **telemedicina e telemonitoraggio**

AUTO — **CYBORG** *Radiolabs*
Protezione passiva da attacchi cyber in ambiente intra-veicolare con autenticazione dati a rilevanza forense basata su **blockchain**

CORE — **ESII** *Sharelock*
Integrazione di un **Large Language Model** (LLM) locale, addestrato per investigazioni su alert di sicurezza, singole o multiple anomalie

HEALTH — **Here-HomeRehab** *Aenduo*
Riabilitazione respiratoria domiciliare attraverso dispositivo medico software (APP mobile + kit di attrezzi per gli esercizi di fisioterapia)

CORE — **BASE** *Keyless Technologies*
Metodo di **autenticazione e firma digitale** robusto e user-friendly utilizzando tecniche avanzate come ad es. zero-knowledge proof

HEALTH — **SafeBot4Twin** *RBF Morph*
Chatbot basato LLM per controllare Medical Digital Twin costruiti mediante dati clinici e garantire la sicurezza delle informazioni sensibili sottostanti necessarie

AUTO — **MACS 2.0** *Tomware*
Estende il primo progetto MACS, ampliando le funzionalità di **diagnostica sullo spettro radio** e vari altre funzionalità

SPACE — **ETERE** *Qascom*
Tecnologie avanzate per **monitoraggio di interferenze a radiofrequenza** con soluzione per l'analisi delle bande maggiormente utilizzate nei servizi satellitari

CORE — **Q-RoT** *Random Power*
Architettura di **Root-of-Trust** in grado di generare e custodire l'identità univoca dei dispositivi e generare e gestire chiavi crittografiche e di autenticazione

HEALTH — **ZOOMel** *Fondazione FORMIT*
Supporto alla **diagnostica del melanoma** con Deep Learning per l'analisi dell'immagine dermoscopica (DIA)

AUTO — **SENTINELLA** *NETCARING*
Sicurezza della persona in ambito automotive e per chi utilizza macchine operatrici. Il sistema impl strumenti di analisi del comportamento del conducente

SPACE — **HESI** *DIGIMAT*
Sistema software per eseguire operazioni mantenendo sempre i dati in forma cifrata progettato per la gestione e l'elaborazione di **immagini satellitari SAR**

CORE — **DCS** *Teleconsys*
Proteggere i dati aziendali da attacchi ransomware attraverso l'integrazione delle tecnologie **IOTA** (Internet of Things Application)

HEALTH — **SMARTCARE** *ESA System*
Piattaforma tecnologica avanzata per la telemedicina, focalizzata sull'**integrazione di dispositivi medici**, sulla facilità d'uso e la sicurezza dei dati

AUTO — **CYBERBOSS** *MAESTRALE IT*
Attraverso le identità biometrica multifattore, il sistema vuole rilevare e filtrare gli attacchi informatici verso gli IVI (**In Vehicle Infotainment**)

4,7 M€

100%

Incentivi erogati

SECURE - Strenghtening EU SMEs Cyber Resilience

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA

Adeguamento al Cyber Resilience Act PMI Europee

50% di finanziamento per valore progetti max € 60K

Consortium: **ACN** (IT) [coord], **NASK** (PL), **INCIBE** (ES), **CCB** (BE), **LHC** (LU), **DNSC** (RO), **EDIH AT** (AT), **Cyber 4.0**, IdeaRe

Budget progetto: 21,9 Mln €

Budget Cyber 4.0: 18,2 Mln € (inclusi i 16,5 di FSTP)

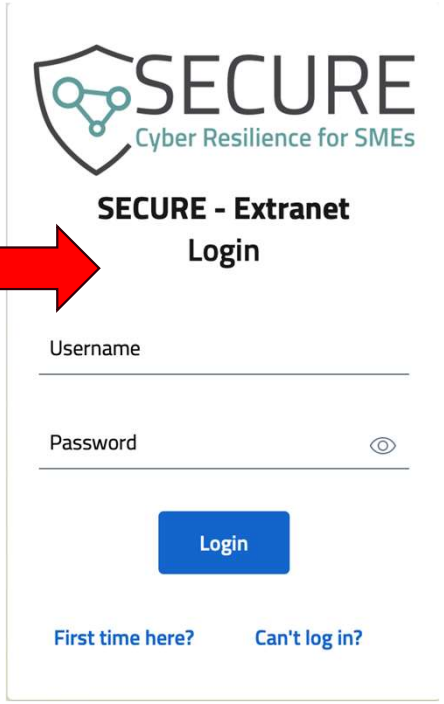
Prima call: chiusa il 29/03/2026 - € 5 Mln

Residuo prossime call: 11,5 M€

SECURE – Risultati Prima Call for Proposal

Item	#
Utenti registrati in Extranet	702
Proposals create	463
Proposals inviate in valutazione	**258**

https://secure4sme.eu



Country name	Number of companies
Italia	91
Germania	28
Spagna	27
Romania	16
Olanda	15
Belgio	14
Francia	10
Slovenia	6
Polonia	6
Portogallo	5
Finlandia	4
Lettonia	4
Grecia	3
Irlanda	3
Cipro	3
Slovacchia	3
Svezia	3
Croazia	2
Danimarca	2
Austria	2
Bulgaria	2
Lituania	2
Lussemburgo	1
Islanda	1
Estonia	1
Ungheria	1
Regno Unito	1
Repubblica ceca	1

EU Fundraising

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

European Commission

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations

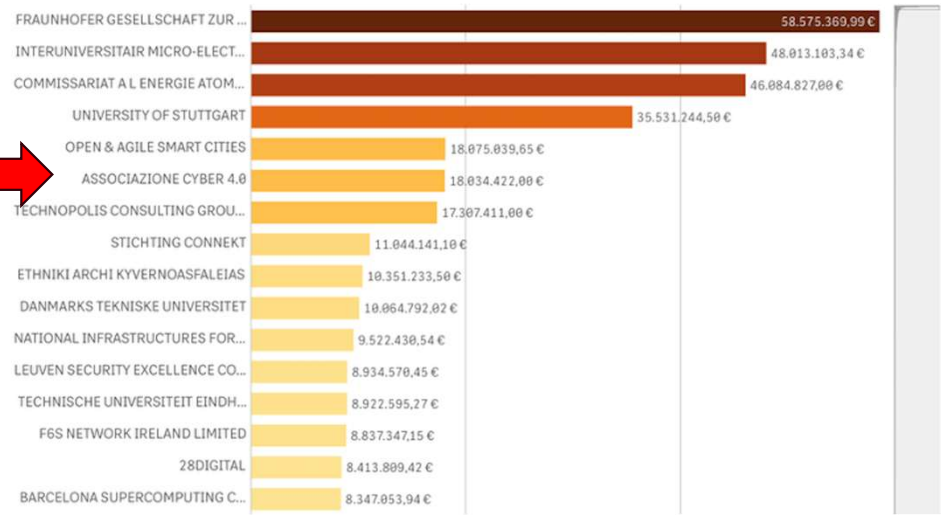
Home > Activities > The Digital Europe Programme > The DIGITAL Dashboard

The DIGITAL Dashboard

Total Cost	EU Contribution (EUR)	Signed Grants
4,16B 100,00% of total	2,34B 100,00% of total	707 100,00% of total

Participation	SME Participation
8.478 100,00% of total	1 950 23,00% of total

Top organisations



CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

3

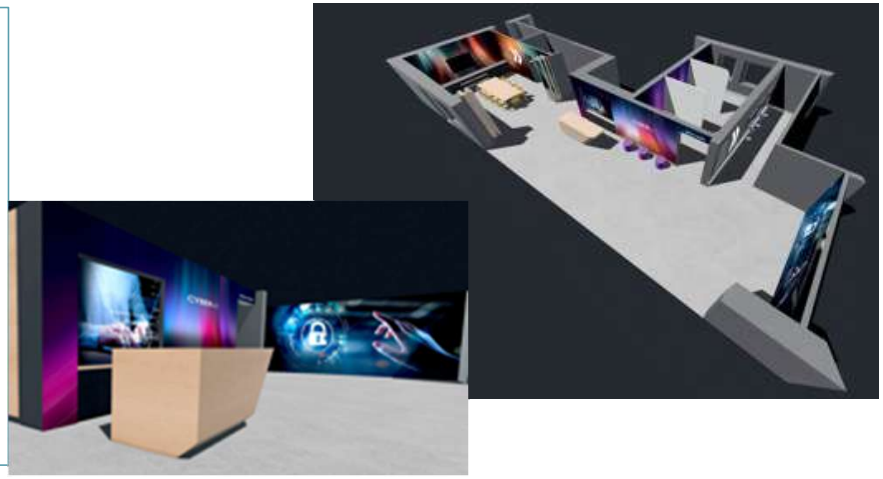
Laboratori e piattaforme Potenziamento Centro di Competenza

Orientamento tecnologico imprese e PA

T4 Demo Lab – Technology Transfer, Training and Testing

Parte del piano di supporto alle imprese, rende disponibile un ambiente in cui fare test di tecnologie innovative, formazione evoluta e awareness. Ospita inoltre alcune delle soluzioni sviluppate nei progetti di innovazione co-finanziati da Cyber 4.0

Demo in ambito:	**OT/ IoT Security**
Gestione del rishio cyber	**OSINT**
Awareness e Formazione	**Big Data Security**
Supply Chain Security	**Sicurezza delle applicazioni**
CERT & Security Operations	
Information Sharing	Progetti di ricerca e innovazione Cyber 4.0
Tecnologie di sicurezza	
Malware analysis	



L’ecosistema Cyber 4.0 integra infrastrutture di fisiche e servizi online per una resilienza cyber a 360 gradi

Cyber 4.0

Laboratori Fisici (Hardware e Software)

Formazione e ricerca nel campo della cybersecurity legata all’IoT

Cyber Safe AI Innovation: sviluppo di soluzioni di intelligenza artificiale affidabili, sicure e integrate nei processi organizzativi

[Healthcare & OT] [AI & Cyber Defence] [IoT & Mobility]

5 Poli universitari e 3 Soci

Servizi on-line (Cloud & Operations)

Soluzioni software applicate per il monitoraggio continuo, la protezione e la certificazione

[PMI Security] [Digital Trust] [Cloud & SOC]

5 Piattaforme online

Laboratori fisici per servizi di protezione, test-before-invest per settori industriali critici

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Healthcare & Critical OT

Tor Vergata | WHL – Wireless Healthcare Lab
Sviluppo di tecnologie abilitanti per la sicurezza elettromagnetica, informatica e fisica dei dispositivi medici

Infoteam | OT Cybersecurity Lab
Laboratorio integrato dedicato alla cybersecurity di apparati elettromedicali e reti idriche

AI & Defense Strategy

Luiss | XAI Lab (Cyber Safe AI Innovation)
Sviluppo di soluzioni AI affidabili, sicure ed integrate nei processi organizzativi

Sapienza | AI Sec Lab
Sviluppo di AI per il supporto avanzato alla difesa in ambito cyber security

CY4Gate | HDT - Hybrid Digital Twin Lab
Laboratorio finalizzato al training cyber immersivo (Cyber Range)

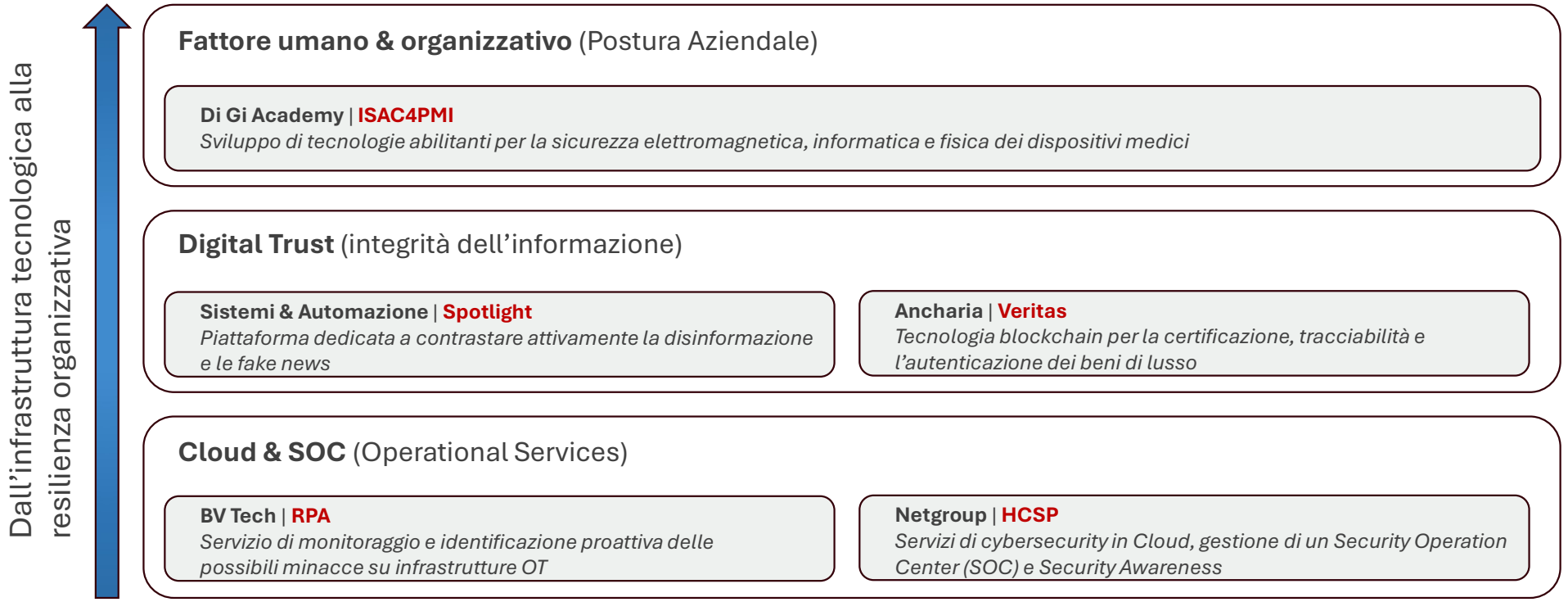
Mobility & IoT Ecosystem

UCBM (Campus BioMedico) | Cybershot Lab
Formazione e ricerca verticale nella cybersecurity legata agli ecosistemi IoT

UniCassino | VX2 – Veichle to X Cybersecurity Lab
Assessment specialistico di apparati e sistemi nell'ambito automotive

TIM | Bolla 5G
Infrastruttura per test-before-invest in ambito IoT

Erogazione di servizi per awareness, fiducia digitale e protezione infrastrutturale



4

Per restare in contatto…

Contatti Cyber 4.0

Website:

https://www.cyber40.it

Cyber FACTory 4.0 – La nostra newsletter

https://www.cyber40.it/newsletter/

LinkedIn:

https://www.linkedin.com/company/cyber40/

Youtube:

https://www.youtube.com/@CCCyber4.0

FORUM 2026
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

3-4 GIUGNO 2026

LUISS ROMA / Aula Chiesa

Con il Patrocinio di:

European Commission

ACN

per info: **forumcyber40@cyber40.it** **cyber40.it**

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

V2X
CYBERSECURITY
LAB

UNIVERSITÀ DEGLI STUDI DI CASSINO E DEL LAZIO MERIDIONALE
SOL PER NOCTEM
- 1979 -

V2X-Cybersecurity Lab

Prof. Domenico Capriglione

Responsabile scientifico V2X Cybersecurity Lab e EMC2 Lab

Funded by
the European Union
NextGenerationEU

V2X-Cybersecurity Lab: il contesto...

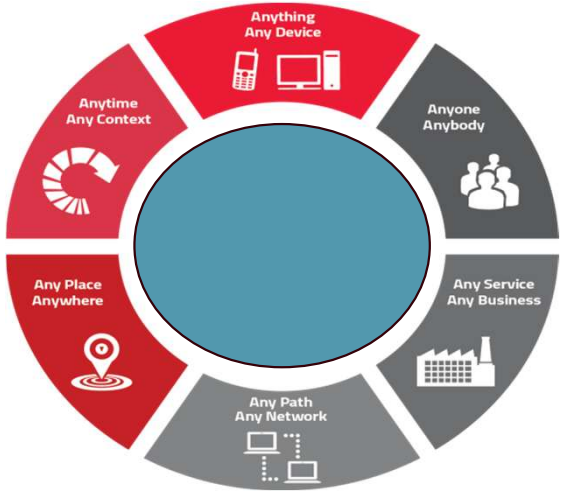
Automotive dei veicoli connessi e Internet of Vehicles (IoV)

ISO/SAE 21434
ROAD VEHICLES CYBERSECURITY ENGINEERING

UNECE R155
CYBERSECURITY MANAGEMENT SYSTEM (CSMS)

UNECE R156
SOFTWARE UPDATE MANAGEMENT SYSTEM (SUMS)

L'Internet of Things (IoT)



NIS 2

Cyber Resilience Act

CE

Automotive Vs Cybersecurity

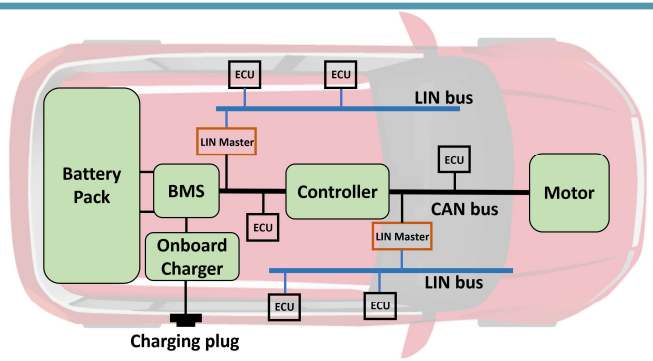
Il veicolo moderno come sistema cyber-fisico

- Tecnologie mobili per la connettività
- Sistemi Avanzati di Assistenza alla Guida (ADAS), infotainment evoluto, fleet management, aggiornamenti OTA
- Guida autonoma

Un attacco può avere impatti su **privacy**, **disponibilità del mezzo** e **funzioni di guida**

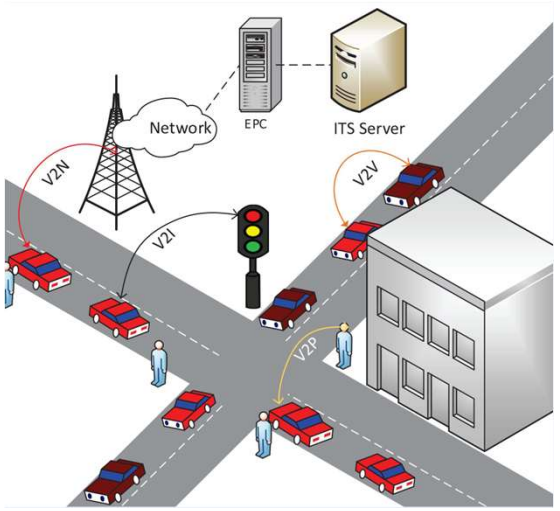
Automotive Vs Cybersecurity

Comunicazioni «interne» ed «esterne» (V2X)



Comunicazioni «interne»

- ❑ CAN
- ❑ LIN
- ❑ FlexRay/MOST
- ❑ Automotive Ethernet
- ❑ BT
- ❑ WiFi

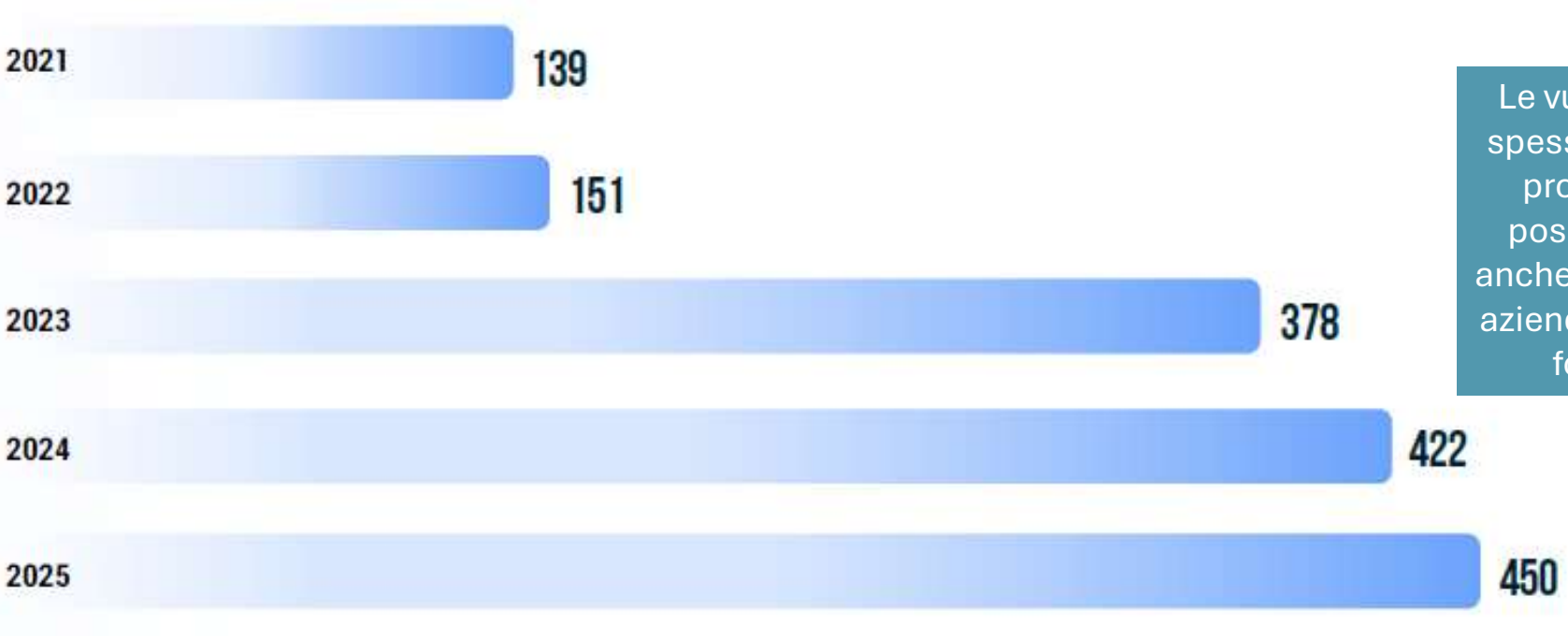


Comunicazioni V2X

- ❑ V2V (Vehicle-to-Vehicle)
- ❑ V2N (Vehicle to Network)
- ❑ V2I (Vehicle-to-Infrastructure)
- ❑ V2P (Vehicle-to-Pedestrian)
- ❑ V2G (Vehicle-to-Grid)

Automotive Vs Cybersecurity

Numero di vulnerabilità individuate (2021-2025)

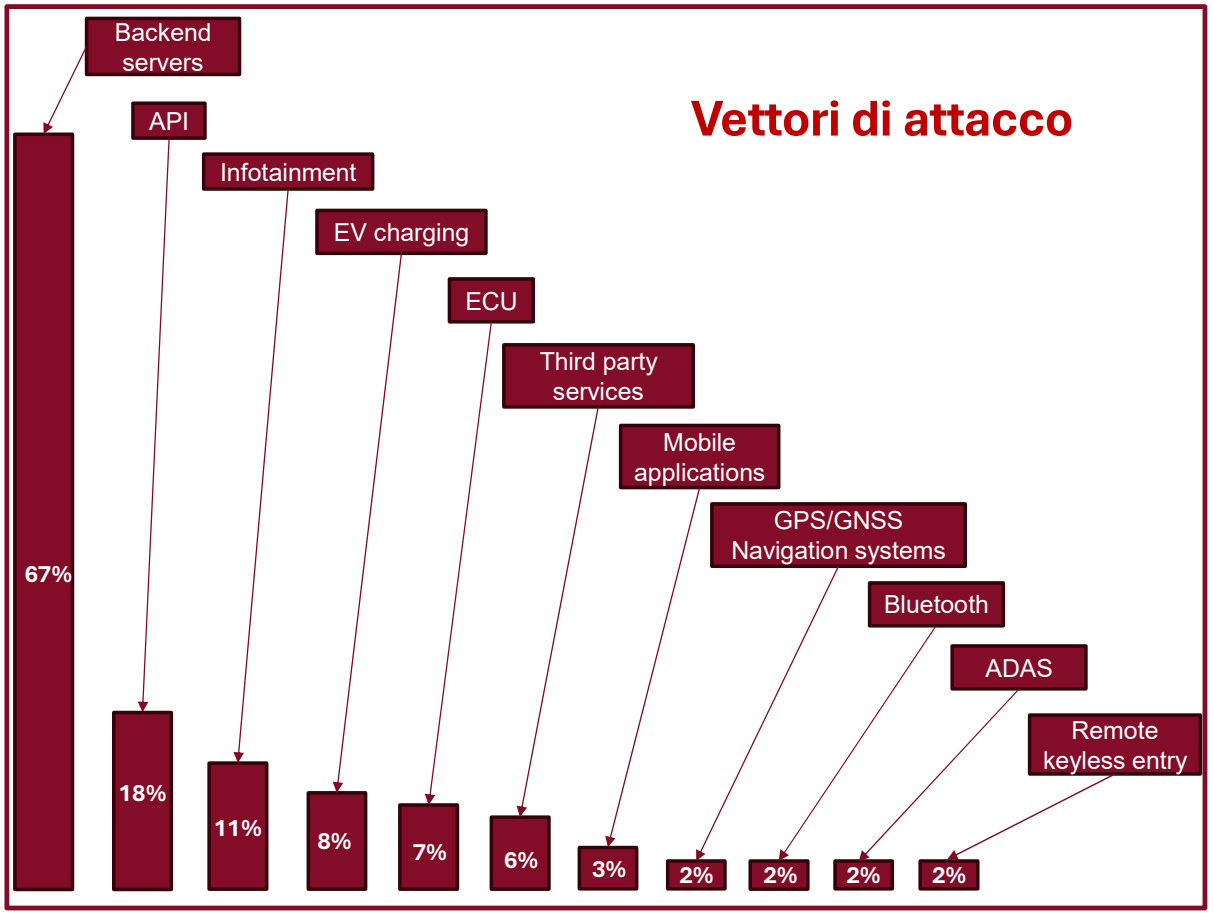


Le vulnerabilità sono spesso riscontrate nei prodotti OEM, ma possono comparire anche nei prodotti delle aziende della catena di fornitura OEM

https://upstream.auto/reports/global-automotive-cybersecurity-report-2025/
https://www.cve.org/

Automotive Vs Cybersecurity

- Le intrusioni mirano sempre più a piattaforme telematiche, servizi cloud e server applicativi
- Le Application Programming Interfaces (API) possono esporre al furto di dati personali sensibili, la manipolazione dei sistemi back-end o il controllo remoto malevolo dei veicoli
- Anche le infrastrutture di ricarica per veicoli elettrici si sono affermate come una superficie di attacco sempre più vulnerabile



https://upstream.auto/reports/global-automotive-cybersecurity-report-2025/

Automotive Vs Cybersecurity

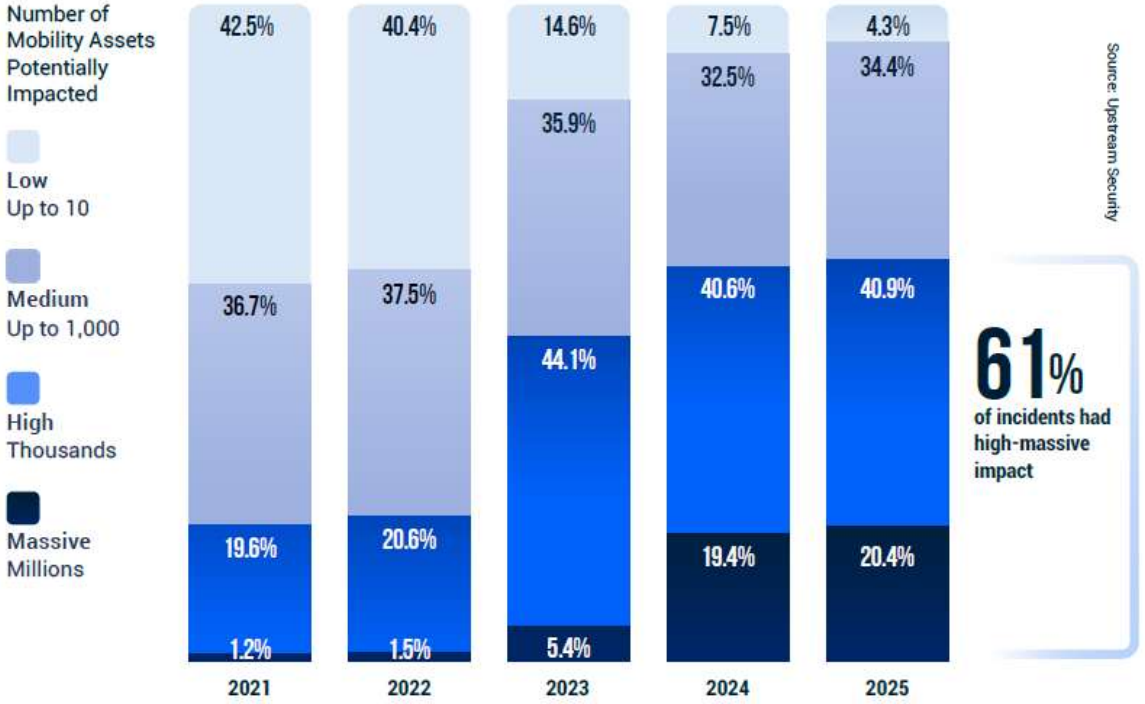
Un esempio recentissimo…

Intoxalock breathalyzer (2026)

- Compromissione dei sistemi back-end dell'azienda Intoxalock
- Impatto sul veicolo: I dispositivi breathanalyzer sono stati resi indisponibili e i conducenti non riuscivano ad avviare il mezzo

Automotive Vs Cybersecurity

Ripartizione degli incidenti resi pubblici in base alla potenziale portata



Strumenti di IA ampliano le superfici di attacco (già) abilitate dall'IA

https://upstream.auto/reports/global-automotive-cybersecurity-report-2025/

IoT Vs Cybersecurity

Esempi recenti...

MENU CERCA LA STAMPA IL QUOTIDIANO ABBONATI

IL CASO

Usa, robot hackerati: aspirapolvere intelligente insulta i proprietari. Ecco come proteggersi

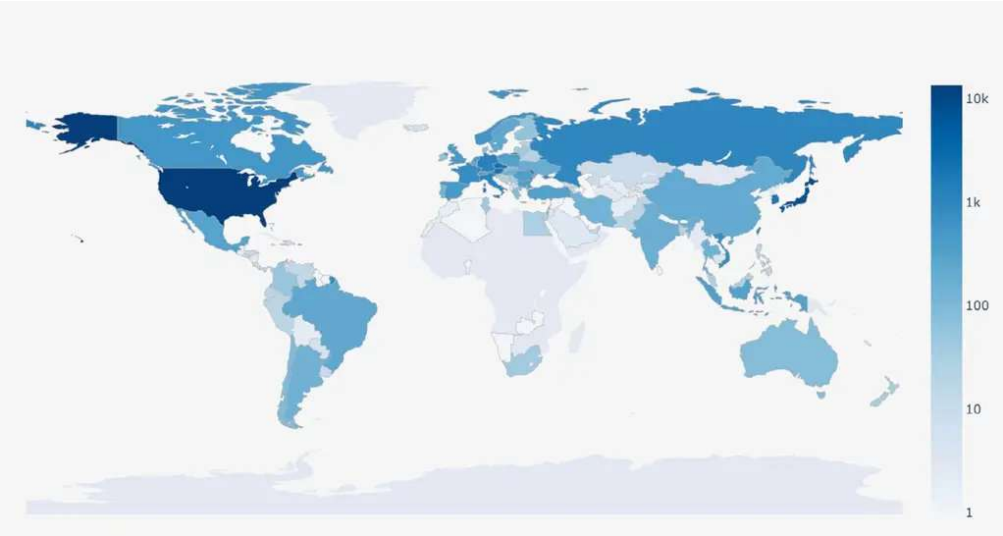
Essere insultati dai propri elettrodomestici è possibile. I robot sono vulnerabili, i dispositivi Ecovas sono pieni di falle, dai problemi con i Pin alle connessioni Bluetooth poco sicure

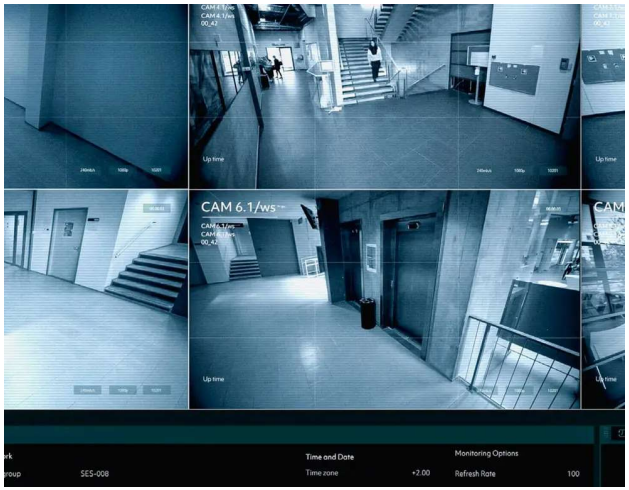
23 Gennaio 2025 | Aggiornato alle 11:46 | 2 minuti di lettura

https://www.lastampa.it/esteri/2025/01/23/news/usa_elettrodomestici_hackerati_insulti_proprietari-14957154/

IoT Vs Cybersecurity

Esempi recenti...





Nel mondo esistono almeno **40.000 videocamere di sicurezza e telecamere di videosorveglianza** accessibili liberamente da Internet, senza alcuna protezione, né password, né crittografia, né controlli di autenticazione

https://www.cybersecurity360.it/nuove-minacce/dalle-case-agli-uffici-come-40-000-videocamere-di-sicurezza-diventano-finestre-pubbliche/

V2X-Cybersecurity Lab: la strumentazione

Keysight SA8710A Automotive Cybersecurity Test Platform

- Piattaforma di test modulare per valutare la robustezza di ECU (Electronic Control Unit), TCU (Telematics Control Unit), sottosistemi e veicolo completo rispetto ad attacchi informatici
- Audits disponibili: **Wi-Fi, Bluetooth Classic, Bluetooth Low Energy, CAN, Automotive Ethernet, Ethernet, IPV4, IPV6, ADB, WEB,** Cellular 2G\3G\4G\5G
- Automatizzazione dei test, assessment, fuzzing, scansione delle vulnerabilità e reporting
- **Test CVE (Common Vulnerability and Exposure)**
- **Possibilità di customizzazione e di creazione di nuovi test**

V2X-Cybersecurity Lab: la strumentazione

Keysight SA8710A Automotive Cybersecurity Test Platform

≈ 400 test disponibili

Categoria	Audit Correlati
Device Security	Hardware, Firmware, Boot, Patching
Access Management	Auth, IAM, Password, Access Control
Data Security	Privacy, Crypto, Secure Comm
Infrastructure	Cloud, API, Network, Server
Ops & Governance	Vulnerability, Incident, Logging

V2X-Cybersecurity Lab: la strumentazione

Keysight SA8710A Automotive Cybersecurity Test Platform

Bluetooth Low Energy - Intrusive - Invalid Sequence

Module: Wi-Fi and Bluetooth LE Audits
Version: 20260131001450

Assessment Summary

Rules Evaluation

Fail

Is Vulnerable: Target Is Secure - Fail

Custom Parameters

Target: 76:24:99:76:2F:F2
NRF Interface: /dev/ttyACM0
Script Timeout: 90
Crash Timeout: 6

Description

This audit targets the Invalid Sequence Memory Corruption vulnerability (CVE-2020-10061). This vulnerability allows an attacker within radio range to cause memory corruption by incorrectly starting a BLE connection with the target. During a connection, the central and the peripheral read and write to the flow control/acknowledgement bits (NESN and SN) on the Link Layer header to acknowledge each other. However, if the central starts a connection by sending an Anchor Point packet with NESN and SN bits set to 1, the peripheral does not accept such bits as valid and performs invalid operation on its internal packet buffer. If the central proceeds with the connection by sending further packets, the peripheral retry-buffer gets full, which leads to a memory corruption (dangling pointer) and eventual crash of the peripheral.

MITRE Mapping

CVE: CVE-2020-10061
MITRE attack techniques/tactics: T1642

V2X-Cybersecurity Lab: la strumentazione

Keysight SA8710A Automotive Cybersecurity Test Platform

Bluetooth Low Energy - Compliance - KNOB Tester BLE

Module: Wi-Fi and Bluetooth LE Audits
Version: 20260131001450

Assessment Summary

Rules Evaluation

Fail

Is Vulnerable: Target Is Secure - Fail

This audit targets the KNOB (Key Negotiation of Bluetooth) vulnerability, disclosed in 2019 by researchers from the University of Oxford and the Singapore University of Technology and Design. The vulnerability affects the encryption key negotiation process in Bluetooth, allowing an attacker to downgrade the entropy of the negotiated key to just 1 byte. This significantly weakens the encryption, making it feasible to brute-force the key and compromise the confidentiality of the communication. The audit simulates this downgrade scenario to determine whether the device accepts low-entropy keys during pairing. Because the key negotiation is handled internally by the Bluetooth stack and remains invisible to end users, the attack is stealthy and difficult to detect. Devices vulnerable to this behavior may unknowingly establish encrypted connections with minimal security, exposing sensitive data to interception.

MITRE Mapping

CVE: CVE-2019-9506
MITRE attack techniques/tactics: T1120

Findings

Message

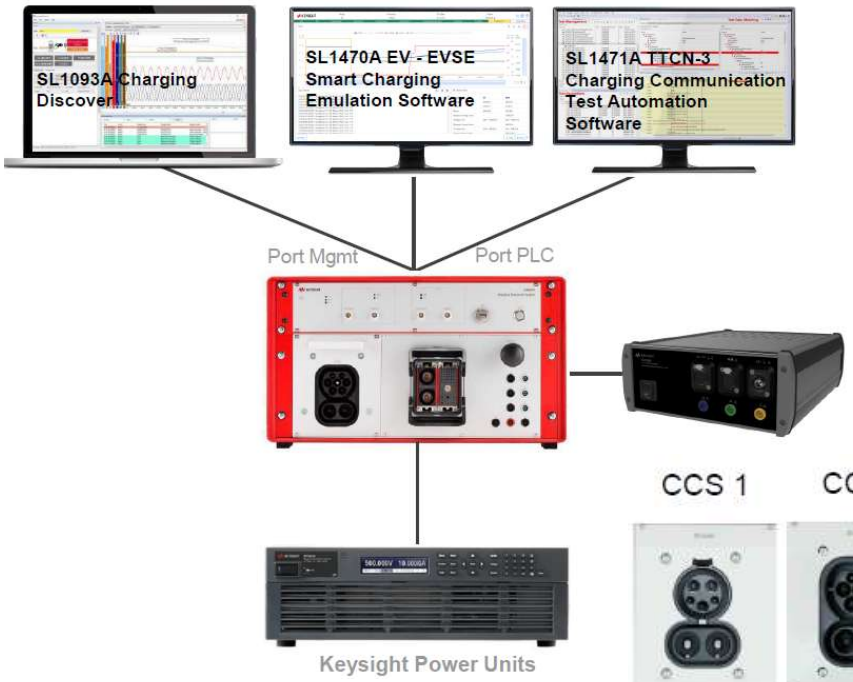
BLE compliance completed

Scan Result

Non-compliance detected on DUT

V2X-Cybersec Lab: sinergia con il CNMS (Centro Nazionale per la Mobilità Sostenibile)

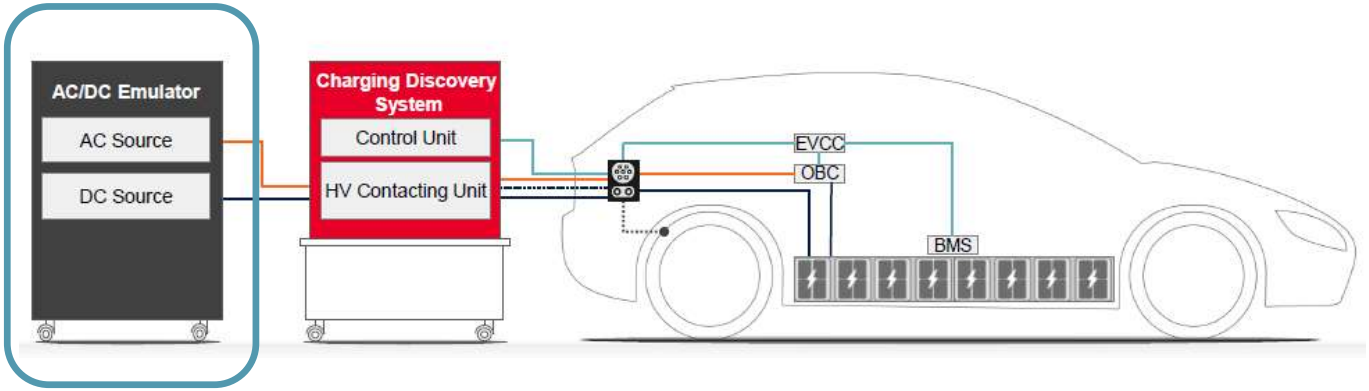
Keysight SL1040A Scienlab Charging Discovery System



- Analisi di compatibilità, sicurezza e funzionamento nei processi di ricarica dei veicoli elettrici:
  a. **Emulatore di veicolo (EV Test)**
  b. **Emulatore di colonnina (EVSE Test)**
  c. **Analisi di interoperabilità (Man-in-The-Middle)**

V2X-Cybersec Lab: sinergia con il CNMS (Centro Nazionale per la Mobilità Sostenibile)

Keysight SL1040A Scienlab Charging Discovery System

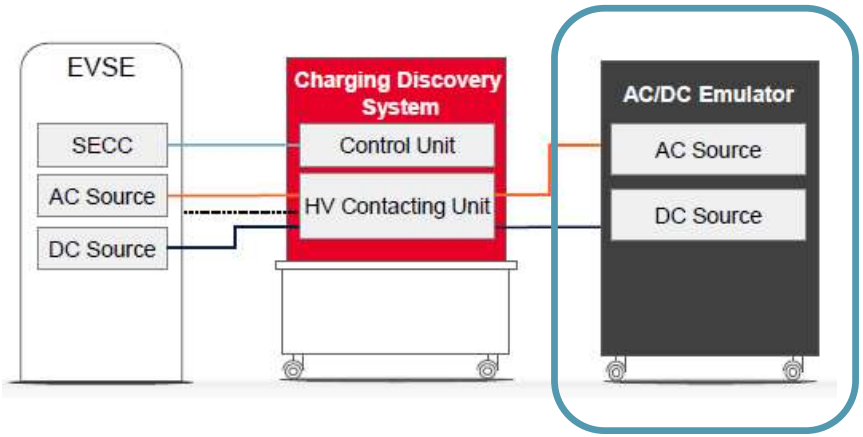


EV test

- Verifica del sistema EVCC o OBC (con o senza trasferimento di energia)
- Verifica di tutti i componenti relativi alla ricarica, inclusa la rete (BMS + batteria)
- Test funzionale dell'interfaccia di ricarica di un veicolo (completo)
- Test di conformità e interoperabilità

V2X-Cybersec Lab: sinergia con il CNMS (Centro Nazionale per la Mobilità Sostenibile)

Keysight SL1040A Scienlab Charging Discovery System

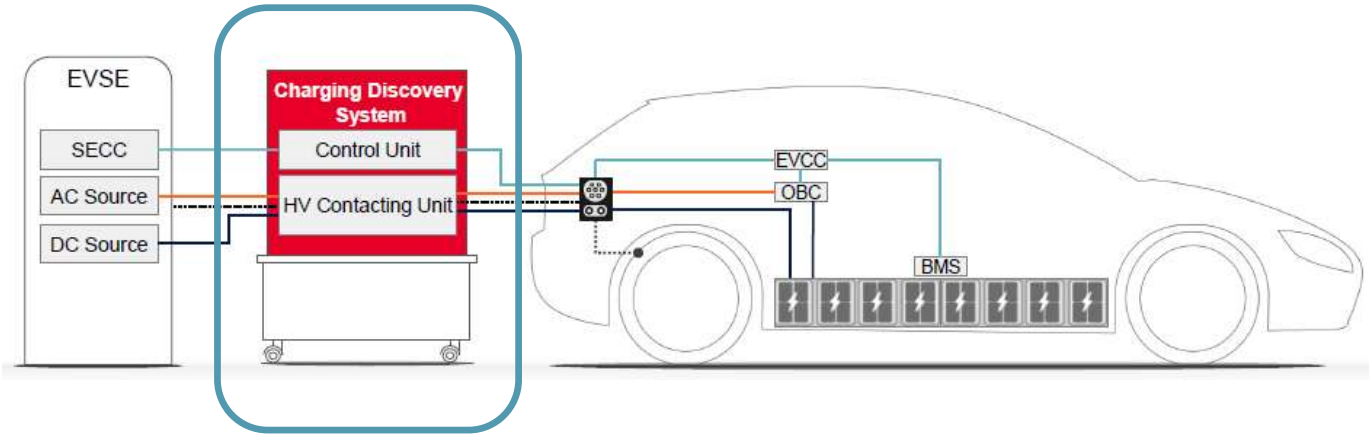


EVSE Test

- Verifica del Supply Equipment Communication Controller (SECC).
- Verifica di tutti i componenti relativi alla ricarica come rete (SECC + convertitore AC/DC).
- Test funzionale dell'interfaccia di ricarica di una stazione di ricarica (completa).
- Test di conformità e interoperabilità.

V2X-Cybersec Lab: sinergia con il CNMS (Centro Nazionale per la Mobilità Sostenibile)

Keysight SL1040A Scienlab Charging Discovery System



Man-in-the-Middle test

- Analisi delle interruzioni di ricarica
- Analisi di specifiche problematiche di interoperabilità
- *Cybersecurity test*

V2X-Cybersecurity Lab: sintesi dei servizi

AMBITI	DESCRIZIONE
TESTING	Scansione delle vulnerabilità su varie interfacce di comunicazione, allestimento di scenari sperimentali ad-hoc
GOVERNANCE & COMPLIANCE	NIS2, CRA, UNECE
FORMAZIONE	Awareness, specialistica, preparazione audit
R&D & INNOVAZIONE	Progettazione e sviluppo di IDS, AI per cybersecurity, Tecniche di crittografia, bandi di ricerca e innovazione

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Grazie!