CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Aspetti di cybersecurity nel settore automotive e il ruolo dell'innovazione

Matteo Lucchetti

Direttore Operativo, Cyber 4.0

www.cyber40.it

Matteo.Lucchetti@cyber40.it

Veicoli connessi e vulnerabilità

- **Connettività** del veicolo
  - Aggiornamenti Over-The-Air per qualità, sicurezza e usabilità di applicazioni e servizi a bordo
- API per applicazioni di bordo e connettività verso Internet → **Vulnerabilità** sempre più numerose e più facili da sfruttare
  - Vulnerabilità rilevate (CVE) triplicate 2023 vs. 2022, e raddoppiate 2021 vs. 2020
- **Incremento consistente dei cyber attacchi** rivolti al veicolo, in numero, impatto e livello di sofisticazione

Connected Car 2023, mercato in crescita: in Italia l'auto connessa vale 2,5 miliardi

Home > AutomotiveUp > Connected Car

Il mercato della Connected Car & Mobility ha raggiunto un valore di 2,5 miliardi di euro, +16% rispetto al 2021, tra auto connessa (1,4) sistemi ADAS (740 milioni) e smart mobility (340 milioni). Quasi un italiano su due ha un'auto connessa. I dati dell'Osservatorio del Polimi nel report 2023

Pubblicato il 26 Mag 2023

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

I produttori
(Original Equipment Manufacturers)

- OEM restano obiettivo di attacchi cyber che si rilevano anche in tutti gli altri settori produttivi
  - Attacchi verso dati, sistemi e informazioni
    - Furto di dati, proprietà intellettuale
    - Ransomware
    - Leva sul fattore umano
  - Compromissione nativa del firmware dei componenti di bordo
  - Attacchi alla **supply chain**

Major trucking software provider confirms ransomware incident

One of the biggest providers of software for the trucking industry acknowledged a ransomware attack on Friday after reports emerged of issues that customers had with its products.

An executive of the company, New Jersey-based ORBCOMM, confirmed the attack to Recorded Future News but would not say which ransomware group was behind the incident or whether a ransom would be paid.

"On September 6, 2023, ORBCOMM experienced a ransomware attack that is temporarily impacting our FleetManager platform and BT product line, which is used by some of our customers to track and monitor their transportation assets," said Vice President Michelle Ferris. The incident was first reported by BleepingComputer.

ORBCOMM provides dozens of trucking companies with electronic logging device (ELD) systems, which are mandated by the U.S. Department of Transportation to track how long drivers spend behind the wheel. The department granted an extension to all carriers using ELD models from ORBCOMM, allowing drivers to use paper logs while the system is down.

TSMC confirms supplier data breach following ransom demand by Russian-speaking cybercriminal group

By Sean Lyngaas, CNN

2 minute read · Published 11:41 AM EDT, Fri June 30, 2023

Le stazioni di ricarica dei Veicoli Elettrici – Rischi cyber

- Le stazioni di ricarica sono connesse a Internet
  - Connessione alla rete di distribuzione dell'energia
  - Sistemi di pagamento
- La trasmissione dei dati tra Veicolo e Stazione di ricarica introduce rischi cyber (**hacking, malware, data leak**, etc.) che possono portare in linea teorica **fino a black-out della rete energetica** nazionale (o internazionale)
- Gran parte delle stazioni di ricarica, fisicamente, sono liberamente accessibili a tutti

Electric car charger to be removed over cybersecurity fears that hackers could target the National Grid

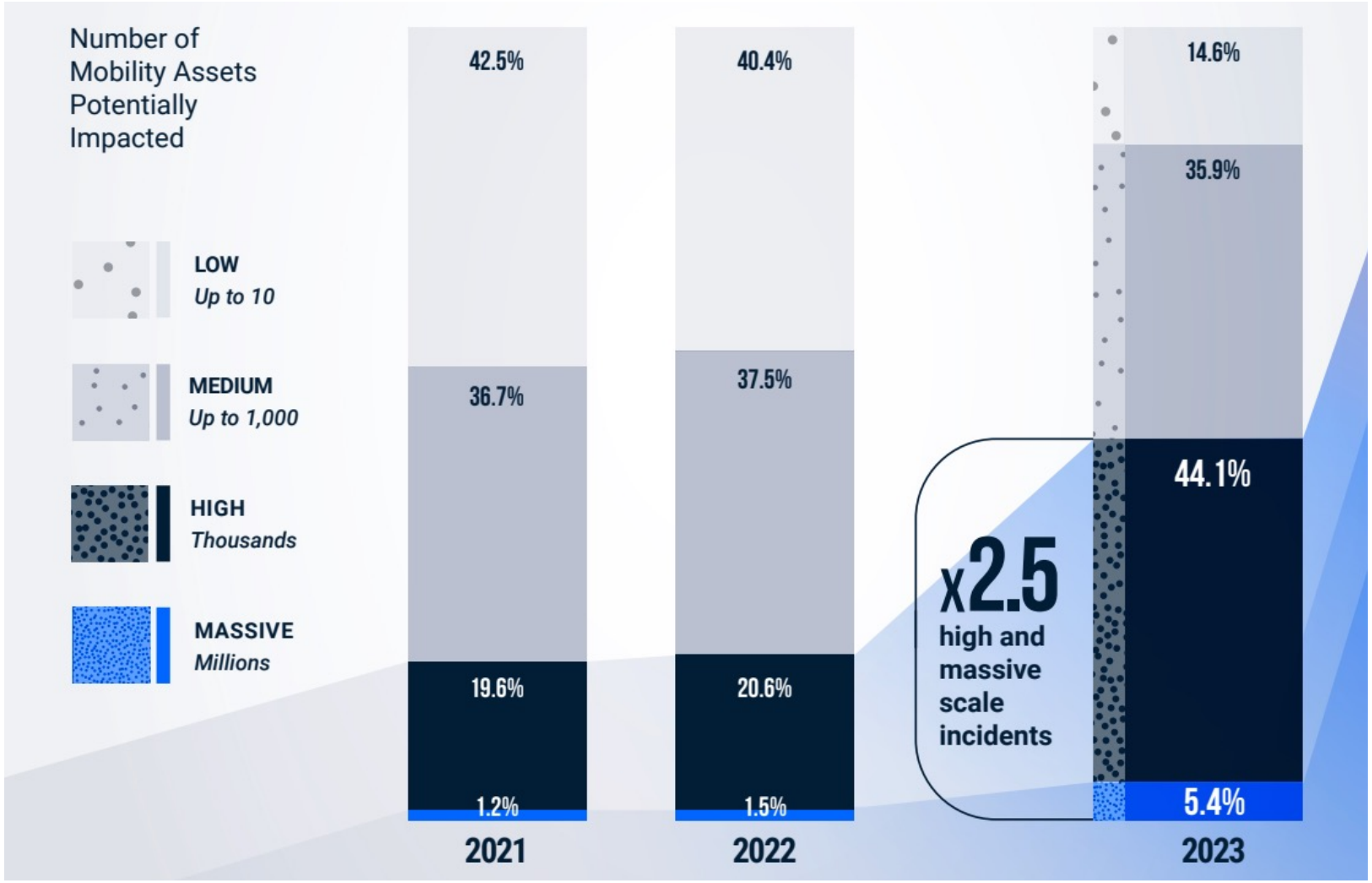
WATCH: Prime Minister comments on electric vehicles at PMQs GB NEWS

By Hemma Visavadia

Published: 22/02/2024 - 10:44 | Updated: 22/02/2024 - 11:10

Comment

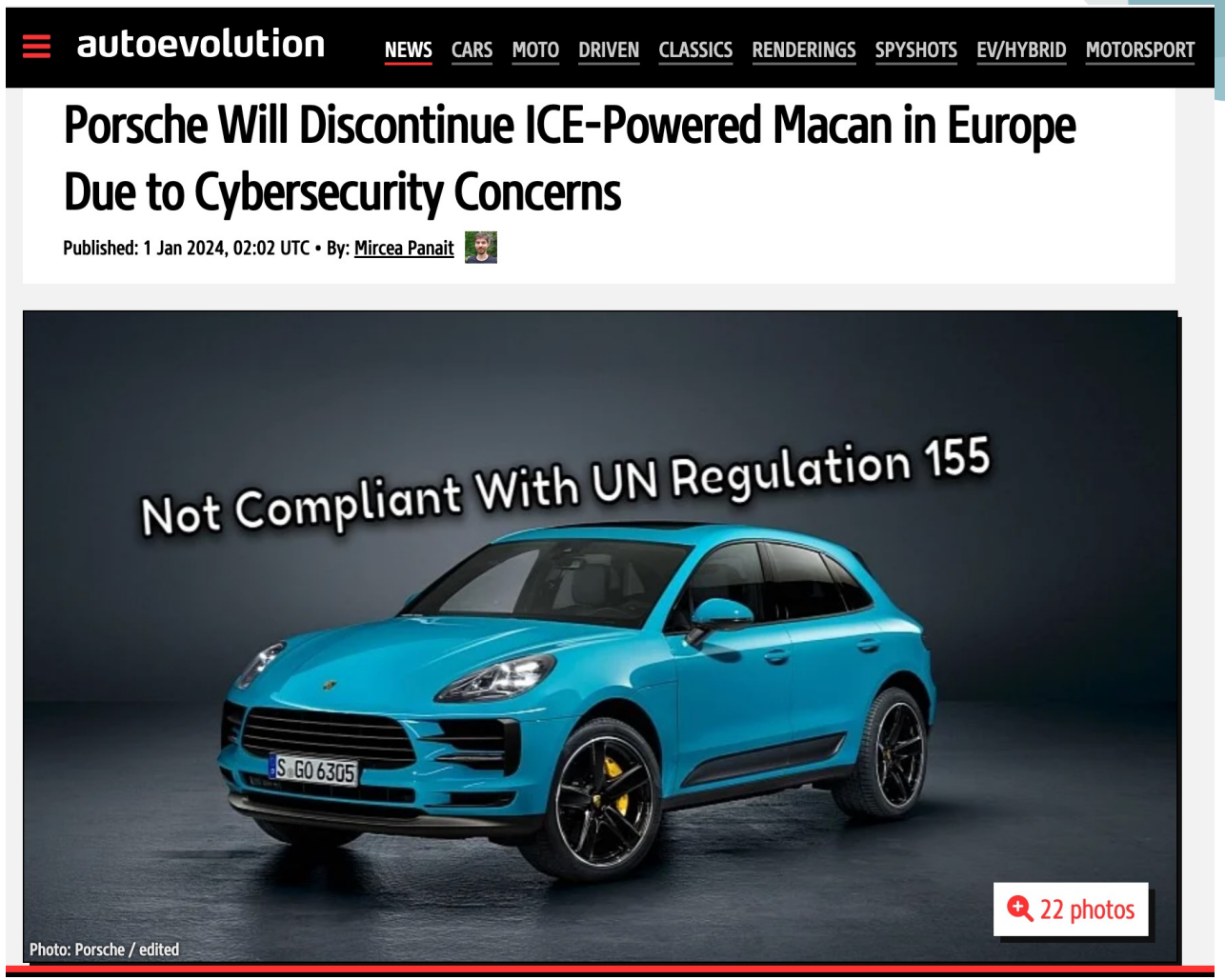
Numero di incidenti cyber noti nel settore automotive 2021-2023



Upstream, GLOBAL AUTOMOTIVE CYBERSECURITY REPORT, 2024

Cyber security compliance nel settore automotive

- EU Cyber Resilience Act
- EU NIS 2 Directive
- UNECE WP.29 per requisiti minimi per la sicurezza informatica
  - **UN Regulation 155 – Cybersecurity and Cybersecurity Management System** → Certificato di compliance
- Norme ISO/SAE 21434 e ISO 24089
  - Requisiti organizzativi, procedurali e tecnici per la sicurezza informatica e gli aggiornamenti software lungo il ciclo di vita del veicolo



CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cosa fare?

- Awareness e formazione
- Rafforzamento delle capacità tecniche e procedurali
- Innovazione

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Cyber 4.0

Centro di competenza nazionale sulla cybersecurity

Centro di competenza nazionale ad alta specializzazione sulla cybersecurity, promosso e co-finanziato dal MIMIT, nato nel piano Industria 4.0 e oggi soggetto attuatore PNRR

15+ Milioni di Euro per (co)finanziare la transizione digitale sicura (2023-2025)

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

- **Attività istituzionali**
- **Servizi di mercato**
- **Progetti finanziati**
- **Networking**

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Bandi Cyber 4.0 ricerca e innovazione

Programma 2023-2026

Bando in uscita ad Aprile 2024

- **2,5 Mln**
- **Durata 12-18 mesi**
- TRL di uscita >= 7
- 400k di massimo co-finanziabile per progetto
- **Intensità contributo variabile** per attività e dimensione

	Micro e piccole	Medie imprese	Grandi imprese
Ricerca Industriale	Fino a 80%	Fino a 60%	Fino a 50%
Sviluppo Sperimentale	Fino a 45%	Fino a 35%	Fino a 25%

Core Cybersecurity

- Artificial Intelligence
- Blockchain
- Cryptography and applications

Automotive

- **Vehicle security**
- **Software and charging station security**
- **Security of people**

Healthcare

- Protection of medical data
- Secure technologies for telemedicine
- Anti-counterfeiting in the pharmaceutical sector

Space

- Protection of critical resources
- Secure satellite protocols
- Secure use of satellite data

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

I filoni di ricerca finanziati

- **Sicurezza del veicolo**
  - Progettazione e sviluppo di tecnologie volte a preservare la **protezione dei veicoli, dei loro occupanti e del traffico circostante**, incluse architetture di sicurezza, sistemi di guida autonoma, sensori, attuatori, comunicazioni di bordo, raccolta e analisi di dati finalizzati alla identificazione di possibili minacce, anche attraverso l'utilizzo della tecnologia blockchain
- **Sicurezza del software e delle stazioni di ricarica**
  - Progettazione e sviluppo di tecnologie volte ad assicurare la **sicurezza dei sistemi software installati sui veicoli e delle piattaforme di ricarica**, inclusa la certificazione degli aggiornamenti software, l'accuratezza, integrità e resilienza del posizionamento dei veicoli, e la protezione delle stazioni di ricarica dagli attacchi di tipo side channel, anche attraverso l'utilizzo della tecnologia blockchain
- **Sicurezza della persona**
  - Analisi del **comportamento del conducente** tramite lo studio di modelli di attenzione e segnali fisiologici (Elettroencefalografia-EEG, ElettrocardiogrammaECG, etc.), sviluppo di tecniche e algoritmi per la rivelazione di sonnolenza e affaticamento del conducente

Costruzione capacità – Il supporto alle imprese per transizione digitale sicura

Categorie di servizi	Intensità massima di aiuto		
	Micro Piccole	Medie	Grandi
Audit tecnico, valutazione maturità tecnologica – **Assessment**	100%	80%	30%
Prova prima dell'investimento – **Demo Lab e Test-before-invest**	100%	90%	40%
Formazione (<=24h)	100%	80%	60%
Formazione (>24h)	70%	60%	50%
Consulenza su proprietà intellettuale	70%	60%	50%
Consulenza su **accesso ai finanziamenti**	70%	60%	50%
Consulenza su **innovazione tecnologica di processo e di prodotto, sensibilizzazione e networking**	80%	70%	50%
Progettazione dell'intervento di innovazione	50%	40%	30%

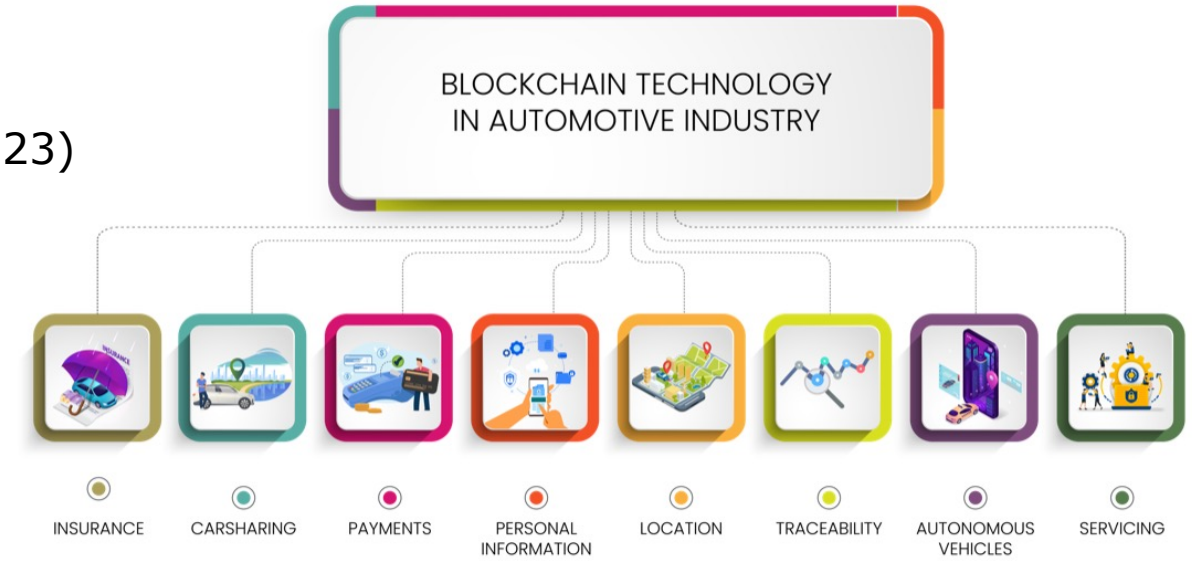
Formazione specialistica imprese

Es. Blockchain e Automotive

Blockchain & Automotive

Sapienza, LUISS, AizoOn

- Fundamentals of cryptography (2022)
- Blockchain intro, basic module (2022)
- Blockchain and automotive applications (2023)
- Smart contracts and decentralized applications (2023)
- Blockchain advanced, tech module (2023)
- Blockchain & IOT (2023)
- Blockchain & security (2023)
- AI & Blockchain (2023)
- Interactive module – Use cases (2023)



Forum Cyber 4.0 – Prossima edizione 3-4 Giugno 2024, Roma

Appuntamento annuale di riferimento per la comunità dell'innovazione e delle competenze in materia di cybersecurity e momento di interlocuzione del Centro con le proprie controparti istituzionali – nazionali e internazionali – e i propri partner del settore privato e del mondo della ricerca

Alcuni numeri dell'edizione 2023

- **497 iscritti**
- **341 partecipanti singoli nei 2 gg.**
- **30+ sessioni**
- **60+ relatori**
- **100+ organizzazioni partecipanti**

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Grazie per l'attenzione

Matteo Lucchetti

Direttore Operativo, Cyber 4.0

www.cyber40.it

Matteo.Lucchetti@cyber40.it

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Back-up

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

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Era il 2015

ANDY GREENBERG SECURITY JUL 21, 2015 6:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

The Jeep's strange behavior wasn't entirely unexpected. I'd come to St. Louis to be Miller and Valasek's digital crash-test dummy, a willing subject on whom they could test the car-hacking research they'd been doing over the past year. The result of their work was a hacking technique---what the security industry calls a zero-day exploit---that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.