CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

1-31 AGOSTO 2025

IN EVIDENZA

AGENZIA PER LA CYBERSICUREZZA NAZIONALE, 11 AGOSTO 2025

Cybersicurezza: ACN diffonde guide pratiche per supportare le PMI nella protezione dai rischi informatici

Pacchetto di schede operative per imprenditori e uffici IT: backup, MFA, gestione password, phishing, aggiornamenti e piani di risposta. Materiali "plug & play" pensati per chi ha poco tempo ma deve alzare in fretta il livello di sicurezza. Un punto di riferimento unico per la compliance minima e la cultura interna.

LEGGI TUTTO

INTERPOL, 22 AGOSTO 2025

African authorities dismantle massive cybercrime and fraud networks, recover millions

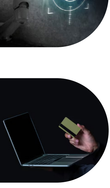
Operazione congiunta in più Paesi africani: smantellate reti di frodi e cybercrime, recuperati milioni di dollari e sequestrata infrastruttura criminale. L'azione conferma il focus transnazionale del fenomeno e l'impatto su supply chain e pagamenti globali.

LEGGI TUTTO

CYBER 4.0

LA REPUBBLICA, 28 AGOSTO 2025

I giovani talenti che portano le imprese nel futuro.



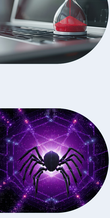
L'Università Campus Bio-Medico di Roma ha lanciato il Cybersecurity Seminars Program, un'iniziativa formativa realizzata con il supporto di Google.org e pensata per formare i giovani nelle discipline STEM. Le attività pratiche si svolgeranno presso il Cyber Shot Lab, il laboratorio congiunto tra UBCM e Cyber 4.0, il Centro di Competenza Nazionale per la Cybersecurity.

LEGGI TUTTO

IN ITALIA

IL SOLE 24 ORE, 20 AGOSTO 2025

Cybercrime: in 4 anni +45,5% di reati informatici contro le imprese



Allarme Confartigianato: tra 2019 e 2023 i reati digitali contro le aziende crescono del 45,5% (contro il +10% degli altri illeciti). Toscana, Veneto e Marche le più colpite. Il dato segnala urgenza di investimenti in difesa, formazione e assicurazioni cyber nelle PMI.

LEGGI TUTTO

ACN, 20 AGOSTO 2025

Videosorveglianza e dispositivi IoT: rischi e consigli utili

Linee guida pratiche per mettere in sicurezza telecamere IP e altri device connessi: cambio credenziali default, segmentazione di rete, aggiornamenti e cifratura. Focus su errori ricorrenti che aprono la porta a intrusioni e data leak.

LEGGI TUTTO

AGID,AGENZIA PER L'ITALIA DIGITALE, 13 AGOSTO 2025

Documenti di identità trafugati da strutture alberghiere: attenzione alle truffe

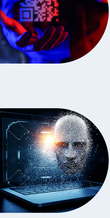
Avviso su esfiltrazioni di dati d'identità trattenuti dagli hotel: rischio furti di identità e frodi online. Sono vivamente raccomandate verifiche agli esercizi, notifiche di data breach e segnalazioni degli utenti in caso di uso indebito, per poter reagire in modo adeguato alle violazioni.

LEGGI TUTTO

NEWS INTERNAZIONALI

INFOSECURITY MAGAZINE, AUGUST 11, 2025

Eight Countries Face EU Action Over NIS2 Deadline Failings



Eight EU states in the crosshairs for NIS2 delays: possible infringement proceedings. Impacts: uncertainty for cross-border businesses and risk of fragmentation in controls. To be followed for compliance and European supply chains.

LEGGI TUTTO

BLEEPINGCOMPUTER, AUGUST 27, 2025

Scattered Spider hacker sentenced to 10 years in US

First heavy sentence related to the "Scattered Spider" group: 10 years for extortion, intrusions, and SIM-swapping campaigns. A strong signal to affiliates and a warning for defense programs against social engineering and initial access brokers.

LEGGI TUTTO

ABNORMAL SECURITY, AUGUST 14, 2025

Compromised Police and Government Email Accounts Abused in Social Engineering

Criminals exploit compromised institutional mailboxes to target supply chains and executives: zero-day-free payloads, high credibility, and high response rates. Recommendations: aggressive DMARC, "impossible travel" detection, and out-of-band verification processes.

LEGGI TUTTO

UNITED NATIONS, AUGUST 26, 2025

UN General Assembly agrees to develop proposals for new AI governance mechanisms.

Significant political step: the Assembly is tasked with defining global mechanisms for AI governance. Moving toward coordination on security, transparency, and rights protection, with implications for standards and the responsibility of private actors.

LEGGI TUTTO

ENISA, AUGUST 26, 2025

ENISA to operate the EU Cybersecurity Reserve of Incident Response Services for the next 4 years

ENISA has been entrusted with the management of the European "reserve" of IR services (budget €36M): a task force that can be activated for serious incidents to support states and critical operators, reducing response times and engagement costs.

LEGGI TUTTO

CYBER SECURITY NEWS, AUGUST 21, 2025

Hackers weaponize QR codes embedded in images

New vector: QRs embedded in digital images spread via email/social media lead to phishing pages and payloads. Users are caught off guard because the QR is not "visible" as an attachment. Filters on images and continuous training are suggested.

LEGGI TUTTO

DARK READING, AUGUST 24, 2025

"PromptLock": AI-powered ransomware hides payloads in artistic text prompts

Researchers report a RaaS model that camouflages malicious code in artistic prompts to bypass controls: AI becomes a means of obfuscation. Defensive focus on content analysis and exfiltration control.

LEGGI TUTTO

Nuove Pubblicazioni

Agenzia per la Cybersicurezza Nazionale, Rilevata campagna di sfruttamento vulnerabilità note, 2025

Agenzia per la Cybersicurezza Nazionale, Rilevato sfruttamento in rete della CVE-2025-8088 relativa a WinRAR, 2025

OSCE, The State of Digital Transformation, Cybersecurity, and Emerging Technology in the OSCE Region, 2025

European Commission, Annual Report NISD Security Incidents 2024, 2025

EL PACCTO 2.0, Artificial Intelligence and organised crime, 2025

Governance AI Governance Observatory, Global Index for AI Safety Readiness, 2025

Global Forum on Cyber Expertise (GFCE), Internet Infrastructure Initiative (Triple-I) Handbook, uploaded version, 2025

RagaBot blog, Your Go-To List for AI Red Teaming and ML Security Resources

Cyber FACTory 4.0 è una newsletter con cadenza bisettimanale.
Le notizie sono selezionate per attinenza alle attuali aree di interesse di Cyber 4.0 e non rappresentano posizioni ufficiali del Centro di Competenza.
Ricevi questo contenuto in quanto hai preso parte alle attività del Centro.
Per ulteriori informazioni, contributi, iscrizioni o rimozioni da questa lista di distribuzione, contattare: comunicazione@cyber40.it

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER