CYBER FACTORY 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

16-31
LUGLIO
2025

IN EVIDENZA

CYBER 4.0, 29 LUGLIO 2025

Cyber 4.0 cerca nuove risorse

Il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity è alla ricerca di **due profili** da inserire all'interno del proprio team. Entrare a far parte di Cyber 4.0 significa lavorare in un ambiente dinamico e stimolante, con opportunità di crescita e formazione continua, ma anche contribuire ad accompagnare policy maker, imprese e PA in un percorso di crescita verso una digitalizzazione sicura.

LEGGI TUTTO

CYBER 4.0

CYBER 4.0, 24 LUGLIO 2025

Spazio e cybersecurity: nuove sfide e competenze nell'era della legge spazio

Mercoledì 23 luglio, Cyber 4.0 in collaborazione con Fondazione E. Amaldi, ha organizzato un webinar dedicato alla cybersicurezza nel settore spaziale, con un focus sulle nuove sfide e competenze richieste a PMI e startup per affrontare e prevenire i rischi digitali in un contesto sempre più complesso e interconnesso.
Gli speaker Paolo Spagnoletti, Alberto Tuozzi, Lorenzo Scatena, Matteo Lucchetti e Valerio Roscani hanno condiviso analisi, esperienze e spunti di valore per affrontare in modo concreto un tema oggi cruciale per il comparto spazio.

LEGGI TUTTO

CYBER 4.0, 23 LUGLIO 2025

Cyber 4.0 riceve l'Ambasciatore del Lussemburgo in Italia

Cyber 4.0 ha avuto l'onore di ospitare l'Ambasciatore del Granducato di Lussemburgo in Italia, Christophe Schiltz, insieme al suo Consigliere Dominique Chevolet.
Durante l'incontro abbiamo avuto l'opportunità di presentare le attività e le iniziative del Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, esplorando possibili sinergie e collaborazioni tra l'Italia e il Lussemburgo in ambito di innovazione digitale e sicurezza informatica.

LEGGI TUTTO

IN ITALIA

CYBERSECURITY ITALIA, 22 LUGLIO 2025

Cybersecurity, Alfredo Mantovano ottiene la delega per la resilienza delle infrastrutture critiche

Mantovano, già titolare delle deleghe per la sicurezza nazionale e Segretario del Consiglio dei ministri, avrà il compito di coordinare le misure di prevenzione e risposta agli attacchi fisici e cyber contro reti e servizi vitali, aggiornando periodicamente la Presidenza sullo stato delle attività.

LEGGI TUTTO

CYBERSECURITY 360, 1 AGOSTO 2025

La nuova determinazione ACN del 31 luglio 2025: cosa cambia davvero per i soggetti NIS

Il 31 luglio 2025, nel giorno di chiusura della finestra per l'aggiornamento annuale, l'ACN ha pubblicato una nuova determinazione che sostituisce quella con cui i soggetti NIS si sono appena confrontati per la loro conformità. Ma non è una contraddizione: è un messaggio per dire che da oggi si fa sul serio

LEGGI TUTTO

MINISTRO PER LA PUBBLICA AMMINISTRAZIONE, PRESIDENZA DEL CONSIGLIO, 22 LUGLIO 2025

Sicurezza digitale nella PA: pubblicato il vademecum dell'Agenzia per la Cybersicurezza Nazionale

L'Agenzia per la Cybersicurezza Nazionale ha pubblicato un vademecum operativo rivolto alla pubblica amministrazione. Il documento raccoglie buone pratiche, raccomandazioni tecniche e linee guida per migliorare la protezione delle reti e dei dati. L'iniziativa mira a colmare le lacune nella cultura della sicurezza digitale del settore pubblico. Il vademecum è destinato a dirigenti, responsabili tecnici e personale operativo.

LEGGI TUTTO

RED HOT CYBER, 26 LUGLIO 2025

DDoS ancora contro l'Italia: NoName057(16) colpisce altri 6 obiettivi

Il collettivo filorusso NoName057(16) ha condotto una nuova serie di attacchi DDoS contro sei obiettivi italiani, tra cui enti pubblici e soggetti del comparto energetico. Gli attacchi, parte di una campagna ostile in corso da mesi, hanno causato disservizi temporanei e acceso i riflettori sulla vulnerabilità delle infrastrutture. Le autorità italiane hanno attivato procedure di contenimento e monitoraggio.

LEGGI TUTTO

Articoli Correlati:

Cybersecurity Italia, NoName, in Italia la Polizia Postale identifica 5 criminal hacker. Disattivati 600 server in diversi Paesi, 17 Luglio 2025

CYBERSECURITY ITALIA, 29 LUGLIO 2025

Attacco ransomware contro ACEA: la rivendicazione di World Leaks

Il gruppo World Leaks ha rivendicato un attacco ransomware contro ACEA, una delle principali utility italiane. I criminali avrebbero sottratto e cifrato dati sensibili, mettendo a rischio la continuità operativa. L'episodio ha suscitato forte attenzione per le implicazioni sulla sicurezza delle infrastrutture critiche. ACEA ha avviato verifiche e contromisure tecniche per limitare i danni e ripristinare i servizi.

LEGGI TUTTO

GARANTE PRIVACY, 30 LUGLIO 2025

Referti medici e IA, allarme del Garante privacy sui rischi di un uso scorretto

È sempre più diffusa la prassi di caricare analisi cliniche, radiografie e altri referti medici sulle piattaforme di intelligenza artificiale generativa chiedendo interpretazioni e diagnosi. Si tratta di un fenomeno allarmante sia per il rischio di perdita di controllo su dati sanitari di straordinaria importanza per le persone, sia per il rischio che soluzioni di intelligenza artificiale non specificamente progettate allo scopo di fornire le indicazioni richieste e non rese disponibili al pubblico come dispositivi medici a valle dei necessari test e controlli previsti dalla disciplina di settore forniscano indicazioni errate.

LEGGI TUTTO

NEWS INTERNAZIONALI

EUROPOL, JULY 23, 2025

Key figure behind major Russian-speaking cybercrime forum targeted in Ukraine

Ukrainian authorities, with support from Europol, targeted a key figure behind a major Russian-speaking cybercrime forum. The operation led to the seizure of digital evidence and the dismantling of infrastructure used for illegal activities. This marks a significant strike against transnational cybercrime networks. Investigators emphasize the role of cross-border cooperation in tackling cyber threats.

LEGGI TUTTO

ENISA, JULY 22, 2025

Joint statement on SharePoint vulnerabilities: assessment and advice

A joint statement from ENISA and European cybersecurity agencies warns about actively exploited SharePoint vulnerabilities. The document outlines the technical characteristics of the flaws and offers guidance for remediation. Organizations using affected versions are urged to apply updates immediately. The advisory also provides recovery strategies for compromised systems.

LEGGI TUTTO

EUROPEAN COMMISSION, JULY 28, 2025

Commission preliminarily finds Temu in breach of the Digital Services Act in relation to illegal products on its platform

Today, the Commission preliminarily found Temu in breach of the obligation under the Digital Services Act (DSA) to properly assess the risks of illegal products being disseminated on its marketplace. Evidence showed that there is a high risk for consumers in the EU to encounter illegal products on the platform. Specifically, the analysis of a mystery shopping exercise conducted by the Commission found that consumers shopping on Temu are very likely to find non-compliant products among the offer, such as baby toys and small electronics.

LEGGI TUTTO

REUTERS, JULY 28, 2025

Pro-Ukrainian hackers claim massive cyberattack on Russia's Aeroflot

Russian airline Aeroflot (AFLT.MM), opens new tab was forced to cancel more than 50 round-trip flights on Monday, disrupting travel across the world's biggest country, as two pro-Ukraine hacking groups claimed to have inflicted a crippling cyberattack.
The Kremlin said the situation was worrying, and lawmakers described it as a wake-up call for Russia. Prosecutors confirmed the disruption at the national flag carrier was caused by a hack and opened a criminal investigation.

LEGGI TUTTO

REUTERS, JULY 30, 2025

Google to sign EU's AI code of practice despite concerns

Google will sign the European Union's code of practice which aims to help companies comply with the bloc's landmark artificial intelligence rules, its global affairs president said in a blog post on Wednesday, though he voiced some concerns.
The voluntary code of practice, drawn up by 13 independent experts, aims to provide legal certainty to signatories on how to meet requirements under the Artificial Intelligence Act (AI Act), such as issuing summaries of the content used to train their general-purpose AI models and complying with EU copyright law.

LEGGI TUTTO

Articoli Correlati:

Cyberdaily.au, Meta rejects EU's AI Code of Practice, refuses to sign, July 21, 2025
Using LLMs as a reverse engineering sidekic Talos, July 31, 2025

Nuove Pubblicazioni

ACN, Vademecum Buone pratiche di cybersecurity di base per i dipendenti delle PP. AA., Luglio 2025

Banca D'Italia, Ricerca, innovazione e trasferimento tecnologico in Italia, Luglio 2025

Arxiv, Balancing Confidentiality and Transparency for Blockchain-based Process-Aware Information Systems, July 2025

ENISA, Telecom Security Incidents 2024, July 15 2025

Check Point, Ransomware in Q2 2025: AI Joins the Crew, Cartels Rise, and Payment Rates Collapse, July 31, 2025

DTI Domaintools, From Laptops to Laundromats: How DPRK IT Workers Infiltrated the Global Remote Economy, July 31, 2025

MIT, Mapping AI Risk Mitigations, July 28, 2025

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