CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER FACTORY 4.0

1-15
SETTEMBRE
2026

IN EVIDENZA

AGENDA DIGITALE, 16 SETTEMBRE 2026

Laboratori Cyber 4.0, la rete nazionale per l'innovazione sicura

Cyber 4.0 mette a disposizione una rete di laboratori, piattaforme e ambienti di simulazione per aiutare imprese e PMI a sperimentare tecnologie, valutare i rischi informatici, formare il personale e rafforzare la resilienza digitale attraverso servizi specialistici e trasferimento tecnologico.

LEGGI TUTTO

CYBER 4.0

IL MATTINO, 14 SETTEMBRE 2026

Necessaria una governance consapevole e strategica per gestire la transizione

Intelligenza artificiale e comunicazione. La 42esima edizione del Premio Sele d'Oro Mezzogiorno di Oliveto Citra, in provincia di Salerno, si è conclusa con un dibattito focalizzato su questo binomio quanto mai centrale e delicato. [...]La progressiva automazione e la parziale sostituzione dell'uomo sollevano, come evidenziato da Paolo Spagnoletti, un'improrogabile questione di responsabilità.

LEGGI TUTTO

CYBER 4.0, 8 SETTEMBRE 2026

Cyber Capacity Building e cooperazione internazionale: le prospettive per l'Italia nel nuovo approfondimento su Agenda Digitale

Quali prospettive si aprono per l'Italia e per il suo ecosistema nel **rafforzamento delle capacità cyber a livello internazionale?**
A questa domanda risponde l'approfondimento firmato da **Pietro Trebisonda**, International Cyber Capacity Building Manager di Cyber 4.0, pubblicato su **Agenda Digitale**. L'articolo analizza esperienze, modelli di cooperazione e direttrici di sviluppo del Cyber Capacity Building (CCB), evidenziando come la sicurezza digitale sia diventata una componente essenziale della diplomazia cibernetica e della politica estera.

LEGGI TUTTO

CYBER 4.0, 7 SETTEMBRE 2026

ECCC, nuove opportunità europee per la cybersecurity: 96 milioni per innovazione e resilienza

L'**European Cybersecurity Competence Centre (ECCC)** ha aperto una nuova call nell'ambito del **Digital Europe Programme**, mettendo a disposizione fino a **96 milioni di euro** per rafforzare tecnologie, capacità e preparazione dell'Europa in materia di cybersecurity.
Dall'intelligenza artificiale alla resilienza delle PMI, dalla preparazione agli incidenti alla protezione delle infrastrutture critiche, l'iniziativa interviene su alcuni degli ambiti oggi prioritari per lo sviluppo della cybersecurity europea.

LEGGI TUTTO

IN ITALIA

ACN, 11 SETTEMBRE 2026

Online il Vademecum per i soggetti NIS

È disponibile il Vademecum NIS con le indicazioni di carattere generale sui principali adempimenti le relative scadenze e alcuni focus su temi specifici.
La prima scadenza, nel prossimo ottobre, riguarda il termine per l'attuazione delle misure di sicurezza di base per i soggetti inseriti nell'elenco NIS nel 2025.
La prossima scadenza riguarda la registrazione per il 2027. Come ogni anno, dal 1 ° gennaio al 28 febbraio tutti i soggetti NIS sono tenuti a fare o aggiornare la registrazione online attraverso l'accesso al portale dei servizi di ACN.
I focus riguardano anche l'aggiornamento delle informazioni e la categorizzazione di attività e i servizi.

LEGGI TUTTO

ACN, 3 SETTEMBRE 2026

Transizione alla crittografia post-quantistica: call to action del Gruppo di lavoro G7 sulla cybersicurezza

Nell'ambito del Gruppo di lavoro G7 sulla cybersicurezza, l'Agenzia Nazionale per la Cybersicurezza (ACN) ha contribuito alla pubblicazione del documento congiunto sulla migrazione verso la crittografia post-quantistica (PQC) "Preparing for the Post-Quantum Era: A Call to Action: apre un link esterno".
Proposto dall'Agenzia francese per la cybersicurezza (ANSSI) e negoziato dalle agenzie cyber dei paesi G7 e dall'UE durante il primo semestre 2026 il documento raccomanda uno **sforzo coordinato tra governi ed attori privati per favorire la transizione alla PQC e mettere così in sicurezza i loro sistemi ICT.**

LEGGI TUTTO

CORCOM, 16 SETTEMBRE 2026

Sovranità, le regole non bastano. Von der Leyen: "AI e connettività al centro della politica industriale"

Nel discorso sullo Stato dell'Unione, la presidente della Commissione Ue indica capacità di calcolo, sicurezza dei modelli e uso dei dati nei settori produttivi come priorità. Il piano comprende anche chip, reti energetiche, cyber e Spazio.

LEGGI TUTTO

AGENDA DIGITALE, 7 SETTEMBRE 2026

Il CRA sposta la cybersecurity dentro i prodotti: gli effetti su NIS2 e DORA

Il Cyber Resilience Act porta la sicurezza dentro i prodotti digitali e offre alle organizzazioni nuove evidenze per gestire fornitori, vulnerabilità e componenti software. Ecco come sfruttare le sinergie con NIS2 e DORA senza confondere integrazione normativa e conformità automatica.

LEGGI TUTTO

DIRITTO BANCARIO, 14 SETTEMBRE 2026

Cybersecurity e IA: le richieste delle Autorità per rafforzare la governance

BCE, Banca d'Italia e **IVASS**, in considerazione della qualificazione del rischio informatico come grave da parte del CERS – in ragione del diffondersi di sistemi di intelligenza artificiale sempre più avanzati – hanno recentemente chiesto a banche, intermediari e imprese di assicurazione di valutare l'impatto delle più avanzate tecnologie di IA sulla **cybersecurity**, e, in particolare, di **rafforzare la governance ed i presidi di controllo di ciascun ente.**

LEGGI TUTTO

GEOPOP, 15 SETTEMBRE 2026

Quali sono le reali preoccupazioni nei confronti dell'AI: intervista a Corrado Giustozzi

Il cybersecurity expert Corrado Giustozzi analizza i nuovi allarmi sull'AI avanzata e sugli agenti autonomi. Tra rischi esistenziali, concorrenza globale e la necessità di regole simili all'AI Act europeo, l'esperto discute le reali minacce di queste tecnologie.

LEGGI TUTTO

STARTUP BUSINESS, 15 SETTEMBRE 2026

Exein, round da 270 milioni di dollari e valutazione a 1,7 miliardi

Exein, deeptech italiana della cybersecurity per la physical AI, rende noto di avere chiuso un round di finanziamento da 270 milioni di dollari, con una valutazione di 1,7 miliardi di dollari che ne sancisce l'ingresso nel club degli unicorni tech. Il finanziamento accelererà l'espansione di Exein negli Stati Uniti e nell'area Asia-Pacifico e il suo posizionamento nella sicurezza della physical AI: la protezione delle macchine intelligenti che utilizzano l'IA per percepire, prendere decisioni e agire nel mondo fisico, dai robot ai droni, fino ai veicoli a guida autonoma.

LEGGI TUTTO

NEWS INTERNAZIONALI

ENISA, SEPTEMBER 11, 2026

The CRA Single Reporting Platform is launched

The Agency has developed, operates and maintains the online tool to enable manufacturers and open-source software stewards to meet their new Cyber Resilience Act (CRA) reporting obligations for actively exploited vulnerabilities and severe incidents. Designed to support effective vulnerability management across the EU, the SRP allows users to report once and communicate the relevant information to all appropriate authorities.

LEGGI TUTTO

EU CYBER DIRECT, SEPTEMBER 10, 2026

From National Initiatives to Regional Impact: Engaging the Private Sector under the Tallinn Mechanism Framework

In May 2026, the Tallinn Mechanism Project Office (TMPO), together with the European Cyber Security Organisation (ECSO), the European External Action Service (EEAS), GIZ, the German Federal Foreign Office, and the European Commission, organised the first in-person event for the private sector under the Tallinn Mechanism framework. Held in Brussels, the event brought together more than 70 representatives of the Ukrainian and European cybersecurity community, international organisations, donors, and Ukrainian government institutions.

LEGGI TUTTO

EUROPOL, SEPTEMBER 2, 2026

Global public-private operation disrupts Sality botnet active for two decades

An international operation supported by Europol has disrupted the Sality peer-to-peer (P2P) botnet, a long-running criminal infrastructure used to distribute malicious payloads to thousands of infected computers worldwide.

LEGGI TUTTO

ECONOMY MAGAZINE, 16 SETTEMBRE 2026

Microsoft, nuova stretta sull'IA: arriva il codice di condotta

Microsoft rafforza il presidio sulla sicurezza dell'intelligenza artificiale e istituisce un **codice di condotta per i propri modelli**. Al centro dell'iniziativa c'è un principio preciso: l'IA deve restare uno strumento al servizio delle persone, senza sostituirne il controllo.

LEGGI TUTTO

RUTERS, SEPTEMBER 10, 2026

Anthropic disrupts bioweapons research efforts, Russian hacking, Chinese Claude misuse

Anthropic broke up attempts to use its Claude models to develop biological weapons and carry out a suspected Russia-linked cyber espionage campaign against Ukraine, the AI heavyweight said in a report published on Thursday.
It also accused Chinese competitors of hacking attempts aimed at extracting Claude's capabilities in its latest Threat Intelligence report, which documented malicious use of its technology over the past eight months.

LEGGI TUTTO

REUTERS, SEPTEMBER 16, 2026

OpenAI's rogue agents probed Hugging Face for weaknesses two months before major hack

Rogue AI agents from OpenAI hijacked Hugging Face user accounts and probed the site itself for vulnerabilities as early as May, nearly two months before the July breach of the open-source repository drew global attention, according to researchers who reviewed the activity.
The newly uncovered malicious activity showed that the rogue agents' efforts to find a way into Hugging Face began earlier than publicly known.

LEGGI TUTTO

NATIONAL CYBER SECURITY CENTER, SEPTEMBER 15, 2026

Iranian cyber targeting of dissidents, activists and journalists

Advisory on CHOSEN BRICK malware, including technical analysis and advice to help individuals and organisations protect themselves.

LEGGI TUTTO

Nuove Pubblicazioni

Antropic, Detecting and countering misuse of AI: September 2026

Groupe De Travail Cybersecuritè, Transition post-quantique, l'ANSSI et ses partenaires du G7 publient un appel à action, 3 septembre 2026

Federal Bureau of Investigation, Cyber Strategy, September 2026

Europol, Horizon scanning on emerging privacy enhancement technologies, September 8, 2026

CISA, China-Based Artificial Intelligence Companies Conducting Industrial-Scale Distillation Campaigns Against U.S. AI Companies, September 8, 2026

Eventi

Needs Startup Association e Zest, "Origin | The Startup Hub", 22 settembre 2026.
Rome Future Week 2026, Zest HUB, Via Marsala, 29 H- Roma

MIMIT, SSSCLT e Cyber 4.0, "Cognitive warfare: disinformazione, social engineer e minacce cyber", 29 settembre 2026, webinar online.

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