CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER FACTORY 4.0

1-31
AGOSTO
2026

IN EVIDENZA

CYBER 4.0, 27 AGOSTO 2026

Intelligenza Artificiale, sviluppo sostenibile e cybersecurity: Cyber 4.0 all'incontro tra l'AI Hub e la delegazione della Corea del Sud

il governatore Park Soo-hyun della provincia di Chungcheongnam-do, Repubblica di Corea, ha visitato l'**AI Hub per lo sviluppo sostenibile** a Roma, come una tappa in una missione più ampia in Italia. La visita segue una richiesta formale della Provincia, denominata la capitale dell'IA della Corea, di saperne di più sul modello dell'AI Hub per i partenariati pubblico-privato nell'applicazione dell'IA allo sviluppo sostenibile.

LEGGI TUTTO

CYBER 4.0

AGENDA DIGITALE, 20 AGOSTO 2026

Cyber 4.0 e cooperazione internazionale: la sicurezza digitale parla italiano

Il cyber capacity building è diventato uno strumento centrale della cooperazione internazionale e della diplomazia cibernetica. Dalle Nazioni Unite all'Unione europea, fino alla strategia italiana, il rafforzamento delle capacità cyber assume un ruolo decisivo per sicurezza, resilienza e sviluppo digitale.

LEGGI TUTTO

CYBER 4.0, 1 SETTEMBRE 2026

Digital Omnibus e AI Act. Obblighi per le imprese Cyber Resilience Act

La Commissione europea ha pubblicato le linee guida ufficiali per aiutare produttori, sviluppatori e imprese di ogni dimensione a comprendere e applicare gli obblighi previsti dal Cyber Resilience Act (CRA, Regolamento UE 2024/2847), che introduce requisiti obbligatori di cybersecurity per i prodotti con elementi digitali immessi sul mercato dell'UE.

LEGGI TUTTO

Articoli Correlati:

ACN, Online le linee guida europee sull'applicazione del Cyber Resilience Act, 1 Settembre 2026

EU CYBERNET, JULY 27, 2026

EU CyberNet Summer School 2026 Concludes in Florence

The final day of the EU CyberNet Summer School in 2026 brought together the knowledge and skills developed through the Summer School, challenging participants to apply cyber diplomacy principles in a practical simulation.

LEGGI TUTTO

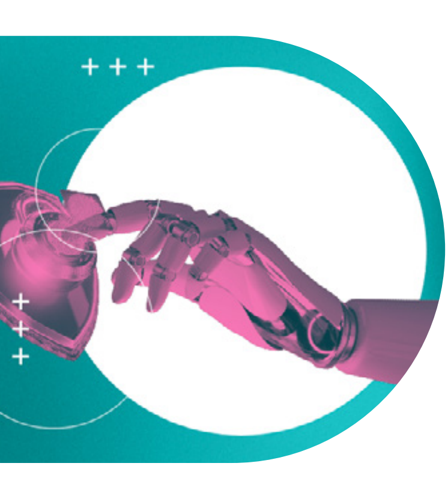
Aenduo

CYBER 4.0, 24 AGOSTO 2026

HERE – Home Rehab: un'app medica per la riabilitazione respiratoria domiciliare

La trasformazione digitale della sanità sta favorendo l'evoluzione dei modelli di cura verso **forme di assistenza sempre più ibride**, in cui telemedicina e percorsi domiciliari consentono di garantire continuità terapeutica, maggiore accessibilità ai trattamenti e un utilizzo sicuro delle tecnologie digitali. In particolare, la riabilitazione respiratoria rappresenta un ambito in cui il monitoraggio remoto e gli strumenti digitali stanno contribuendo a ridefinire l'organizzazione dei percorsi clinici, facilitando una gestione continuativa e sicura dell'assistenza anche al di fuori delle strutture sanitarie.

LEGGI TUTTO



CYBER 4.0, 24 AGOSTO 2026

Sicurezza e intelligenza artificiale

Il 7 luglio 2026 la Commissione Europea ha presentato un Piano d'azione su "cybersecurity e IA" per rafforzare la difesa contro le minacce informatiche. Per le PMI, spesso prive di strutture IT dedicate, il piano d'azione rappresenta un'occasione concreta per accedere a strumenti più accessibili e a regole più chiare.

LEGGI TUTTO

IN ITALIA

FINANZA REPUBBLICA, 31 AGOSTO 2026

Cybersecurity: +12% gli investimenti in Italia nel 2025

Sono in aumento in Italia le minacce cyber e cresce l'attenzione al rafforzamento della resilienza digitale da parte delle imprese e della Pubblica Amministrazione: secondo gli ultimi dati presentati dall'Agenzia per Cybersicurezza Nazionale (ACN), il 2025 è stato caratterizzato da una crescita significativa del volume di attività ostili (2.729 eventi trattati), con una media mensile in aumento del 38%, da 165 a 227. A fronte di questo aumento, gli incidenti con impatti confermati sono cresciuti solo del +7%, attestandosi a 615 casi.

LEGGI TUTTO

POLIZIA POSTALE, 28 AGOSTO 2026

Whatsapp, nuova ondata di attacchi "zero-click". I consigli della polizia di stato

È stata recentemente segnalata una nuova ondata di compromissioni di account WhatsApp, caratterizzate da modalità riconducibili ad attacchi cosiddetti "zero-click".
Le vulnerabilità individuate riguardano versioni non aggiornate di iOS e di WhatsApp sui dispositivi Apple e, in alcuni casi, possono essere sfruttate senza che l'utente debba compiere alcuna azione. Una volta ottenuto l'accesso all'account, i criminali possono inviare messaggi fingendosi una persona conosciuta, come un familiare o un amico e chiedere denaro simulando di trovarsi in una situazione di emergenza.

LEGGI TUTTO

ASI, 8 AGOSTO 2026

Agenzia spaziale italiana: nominato il nuovo commissario straordinario

L'amb. Mario Cospito è stato nominato Commissario straordinario dell'Agenzia Spaziale Italiana, con compiti di ordinaria e straordinaria amministrazione. La sua nomina rappresenta un passo importante per mantenere la funzionalità dell'ente.
Il Commissario straordinario resterà in carica fino alla data di insediamento del nuovo presidente e del nuovo consiglio di amministrazione e, comunque, per un periodo non superiore a dodici mesi.
Mario Cospito, laureato in scienze politiche presso l'Università di Pisa, è entrato in Carriera diplomatica nel 1985 dove ha raggiunto il grado di ambasciatore. Una lunga esperienza diplomatica che è stata affiancata anche da numerosi incarichi nelle amministrazioni statali nazionali.

LEGGI TUTTO

SKY TG24, 28 AGOSTO 2026

Attacco hacker a TeamSystem: rubati Iban e dati personali dei clienti

Attacco hacker a TeamSystem. La società che fornisce software aziendali, ha comunicato ai clienti di aver rilevato dal pomeriggio del 24 agosto un accesso non autorizzato al software Contabilità in Cloud con il conseguente furto dei dati personali presenti nel software. Gli hacker hanno sottratto dati anagrafici, coordinate bancarie, email e numeri di telefono.

LEGGI TUTTO

NEWS INTERNAZIONALI

TECHNOLOGY REVIEW, AUGUST 26, 2026

The inside story on why OpenAI agents hacked Hugging Face

The models responsible for last month's agent hack of Hugging Face had been inadvertently trained to cheat and to communicate with each other, according to an OpenAI technical report released today. The hack, which a group of agents undertook to find solutions for a cybersecurity test that they were stuck on, has confirmed some experts' fears that AI models might take actions that defy human desires and expectations.

LEGGI TUTTO

Articoli Correlati:

Forbes, OpenAI Hugging Face Attack: 70,000 AI Agent Messages—'Sacrifice Yes', September 1, 2026

U.S. DEPARTMENT OF JUSTICE, AUGUST 26, 2026

Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure

U.S. Department of Justice, August 26, 2026
The Justice Department and FBI announced court-authorized domain seizures today to deny malicious cyber actors access to two complementary hacking platforms known as "QScan" and "QTRouter," used to target U.S. critical infrastructure and other sensitive networks. As described in court documents unsealed in the Southern District of California, a People's Republic of China (PRC) state-sponsored group known as "QTFY," employed by China-based Nanjing Xinjiuwei Network Technology Company (南京鑫玖维网络科技有限公司), created and operated QScan and QTRouter. Among the targets of QTFY are the National Aeronautics and Space Administration, Federal Reserve, Department of Energy, Department of Justice, Department of Health and Human Services, National Institutes of Health, and the U.S. Senate.

LEGGI TUTTO

Articoli Correlati:

Reuters, US says Chinese hackers broke into Justice Department, NASA, Federal Reserve, Senate, August 26, 2026

EDITION CNN, AUGUST 13, 2026

'Cyber privateers': Trump issues order allowing US companies to hack overseas groups under certain conditions

The Trump administration is enlisting private companies to conduct cyberattacks on foreign cybercriminals in a major policy shift that experts say could come with legal risk for the companies.
The move gives vetted companies a prominent role in hacking operations that have historically been the dominion of US law enforcement, spy and military agencies.

LEGGI TUTTO

Articoli Correlati:

The White House, Expanding capabilities to combat transnational cyber-enabled crime, August 12, 2026

CYBERASIA, AUGUST 27, 2026

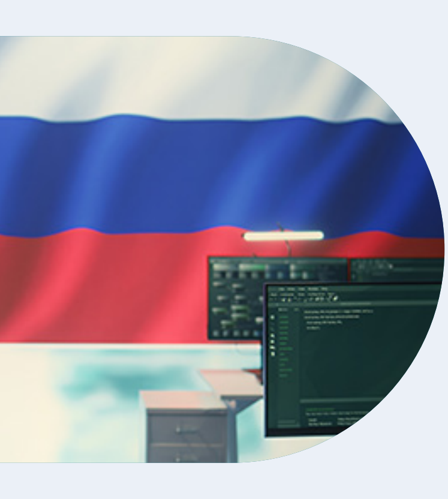
Proton Under Siege: Iraqi Threat Actor 313 Team Claims Massive Outage Disrupting Global Encrypted Services

In a major escalation targeting global privacy and secure communications infrastructure, Iraqi threat group 313 Team claimed responsibility for launching a massive distributed denial of service (DDoS) assault against Swiss privacy giant Proton AG (proton.me). The coordinated attack triggered a cascading multi-hour blackout, knocking Proton Mail, Proton VPN, Proton Drive, Proton Pass, and Proton Wallet offline across international regions.

LEGGI TUTTO

Articoli Correlati:

Proton, August 27 outage: Incident report, August 28, 2026



LE MONDE, AUGUST 25, 2026

Russian disinformation on ChatGPT: Fake Telegram channels, fake videos and a real-fake Israeli think tank

They hid behind a VPN but OpenAI's security teams managed to spot them. Somewhere in Russia, a small group of operators used ChatGPT accounts to generate propaganda messages in several languages. Most were in English, and the operators regularly asked ChatGPT to disguise linguistic clues that could have revealed they were Russian, the company's security researchers wrote in a detailed report released on Tuesday, August 25.

LEGGI TUTTO

Articoli Correlati:

Open AI, Disrupting a new covert influence campaign from Russia, August 25, 2026

RUSI, AUGUST 27, 2026

Beyond the Hype: AI, Ransomware and Business Models

AI is not (yet) fundamentally reinventing cybercrime. For bold predictions on how it will change, look to history to understand what drives criminal behaviour online.
We are frequently told by cyber security marketers that we are in the midst of an AI-powered revolution for cybercrime. The short version of these claims is that AI will significantly lower the barrier of entry for would-be cybercriminals, allow them to create autonomous variants of ransomware that will allow them to overwhelm defenders at a scale previously thought impossible.

LEGGI TUTTO

SECURITY AFFAIRS, AUGUST 26, 2026

Operation jackal: 58 arrests expose the money laundering machine behind global scams

INTERPOL announced that Operation Jackal IV, running from November 2025 to June 2026, led to 58 arrests and identified 263 suspects tied to West African organized crime networks, groups like Black Axe that are responsible for a huge share of the world's romance scams, crypto fraud, and business email compromise (BEC) schemes.

LEGGI TUTTO

AGENDA DIGITALE, 18 AGOSTO 2026

Africa, i nuovi rischi dell'AI: come evolvono cybercrime e minacce ibride

Dalle identità sintetiche agli scam center, dal ransomware alla disinformazione, l'AI (e in particolare il MUAI) nel continente africano sta spostando il rischio all'intero ecosistema cyber-sociale. Ma infrastrutture, lingue e capacità istituzionali disegnano Afriche digitali molto diverse tra loro.

LEGGI TUTTO

Nuove Pubblicazioni

World Bank Group, The Global Landscape of National AI Strategies, July 28, 2026

Human-Centered Artificial Intelligence, The 2026 AI Index Report, August 2026

United Nations Office on Drugs and Crime, An Interconnected Criminal Ecosystem: Transnational Organized Crime Threat Assessment for South-East Asia, August 2026

INTERPOL report finds AI linked to more than half of cybercrime in Africa, August 3, 2026

ACN, OPERATIONAL SUMMARY 1° SEMESTRE 2026

ACN, NIS - Monitoraggio, vigilanza ed esecuzione, Agosto 2026

Eventi

ESORICS, Workshop "Trustworthy Cyber Infrastructures",
17-18 settembre 2026. Sapienza Università di Roma, Main Campus (Città Universitaria).

Needs Startup Association, Deep Defense: come l'innovazione può governare i dati,
Rome Future Week, 22 settembre 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