

CYBER FACTORY 4.0

1-15
APRILE
2026

IN EVIDENZA

CYBER 4.0- 3 E 4 GIUGNO 2026

Forum Cyber 4.0, a Roma il 3 e 4 Giugno 2026

Il Forum Cyber 4.0 2026, il 3 e 4 giugno, riunirà a Roma esperti, istituzioni e aziende leader nel settore della sicurezza informatica per due giornate di confronto, approfondimento e networking. L'edizione 2026 sarà articolata lungo due direttrici principali: da un lato, un focus sulle attività, le priorità e le progettualità sviluppate a livello nazionale; dall'altro, un approfondimento sulle prospettive di cooperazione internazionale, sia in ambito europeo che extra-UE.

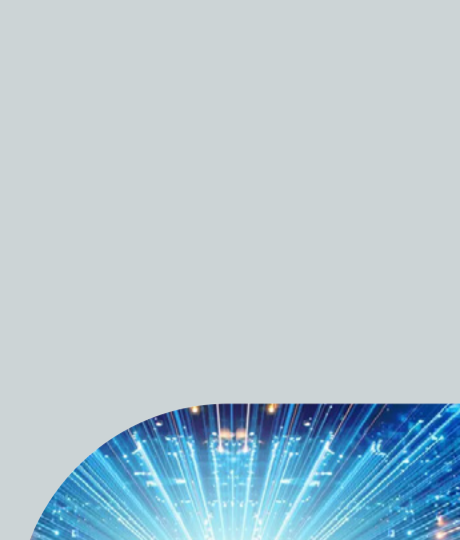


[LEGGI TUTTO](#)

CYBER 4.0- 17 APRILE 2026

Cyber capacity building: il programma Italia-Ghana entra nella fase operativa

Si è conclusa in Ghana la prima tappa operativa del programma di cooperazione in materia di cybersecurity tra il Ministero degli Affari Esteri e della Cooperazione Internazionale e la Cyber Security Authority del Ghana, implementato dal Centro di competenza Cyber 4.0. Nel corso delle sessioni di lavoro del workshop, che hanno coinvolto stakeholder provenienti da amministrazioni pubbliche, industria e mondo accademico, sono state individuate priorità condivise, principali gap di implementazione e proposte concrete per il rafforzamento della Strategia Nazionale di Cybersecurity del Ghana.



[LEGGI TUTTO](#)

Articoli Correlati:

- [TechAfrica News, Ghana Hosts Workshop to Advance National Cybersecurity Strategy, April 16, 2026.](#)
- [Tech Review Africa, Ghana collaborates with Italy on cybersecurity policy implementation, April 20, 2026.](#)
- [News Ghana, Ghana Records 3,500 Cyber Incidents in Three Months Amid Italy Partnership, April 20, 2026.](#)

CONSULTANCY.EU- APRIL 15, 2026

AI model Claude Mythos sends shockwaves through cybersecurity landscape

Anthropic's Claude Mythos AI model autonomously discovers zero-day vulnerabilities through recursive self-improvement, generating complex exploit chains that bypass current detection systems. This dual-use breakthrough accelerates vulnerability disclosure while raising concerns about sophisticated AI-driven attacks. Early tests exposed critical flaws in identity management systems and container platforms.



[LEGGI TUTTO](#)

Articoli Correlati:

- [Cloud Security Alliance, The "AI Vulnerability Storm": Building a "Mythos-ready" Security Program, April 12, 2026.](#)
- [Tech Review Africa, Ghana collaborates with Italy on cybersecurity policy implementation, April 20, 2026.](#)
- [Wired, Troppo potente per un rilascio pubblico: Anthropic limita Mythos a 40 aziende, 8 aprile 2026](#)
- [AISi, Our evaluation of Claude Mythos Preview's cyber capabilities, April 13, 2026](#)

CYBER 4.0

CYBER 4.0- 2 APRILE 2026

Cyber 4.0 entra nel Private Sector Advisory Group del D4D Hub

Cyber 4.0 è entrato nel Private Sector Advisory Group del D4D Hub, una piattaforma strategica promossa dall'Unione Europea e dai suoi Stati membri per rafforzare la cooperazione digitale a livello globale. L'adesione al PSAG consente a Cyber 4.0 di accedere a un ecosistema internazionale di scambio e collaborazione, all'interno del quale vengono condivise informazioni su opportunità progettuali, iniziative e strumenti operativi. I membri possono così contribuire all'orientamento delle progettualità e, al tempo stesso, partecipare a call e tender nell'ambito della trasformazione digitale.

[LEGGI TUTTO](#)

SBIRCIANOTIZIA - 15 APRILE 2026

Innovation Cybersecurity Summit 2026: IA, difesa e sovranità

Il Cybersecurity Summit 2026 si conferma hub strategico per il futuro della sicurezza digitale italiana. Istituzioni, imprese e mondo accademico si confrontano su resilienza, innovazione e sovranità tecnologica. Al centro, l'urgenza di rafforzare la difesa cibernetica come pilastro della sicurezza nazionale. Dal dialogo emergono proposte concrete e una visione condivisa per affrontare le nuove minacce. Un appuntamento chiave per capire dove sta andando davvero la cybersecurity in Italia.

[LEGGI TUTTO](#)

CYBER 4.0- 15 APRILE 2026

Cyber Crime Conference 2026: torna a Roma l'appuntamento dedicato al cybercrime

Anche quest'anno Cyber 4.0 contribuisce come partner scientifico alla Cyber Crime Conference, evento organizzato da ICT Security Magazine che si terrà il 6 e 7 maggio 2026 a Roma, presso l'Auditorium della Tecnica. Giunta alla quattordicesima edizione, la Cyber Crime Conference si conferma un appuntamento imprescindibile per chi opera nel settore della cybersecurity e per istituzioni, PMI e realtà locali interessate a comprendere e interpretare le dinamiche del crimine informatico. Tra le novità dell'edizione 2026, la possibilità di prenotare incontri non a one con i partner presenti in area espositiva.

[LEGGI TUTTO](#)

CYBER 4.0- 8 APRILE 2026

Biosat Marketplace - una piattaforma sicura di servizi per l'Osservazione della Terra

L'utilizzo dei dati di Earth Observation è oggi ampiamente riconosciuto come un fattore abilitante per il supporto alle decisioni in ambito pubblico, nonostante la complessità di accesso nei limiti ancora l'impiego sistematico nei processi operativi. Da questa esigenza nasce BIOSAT Marketplace, un progetto coordinato da IPTSAT e cofinanziato da Cyber 4.0, che ha portato allo sviluppo di una piattaforma digitale che consente di trasformare dati satellitari complessi in servizi di Earth Observation accessibili, certificati e pronti all'uso, a supporto delle attività operative di Pubbliche Amministrazioni e imprese.

[LEGGI TUTTO](#)

IN ITALIA

AGENZIA PER LA CYBERSICUREZZA NAZIONALE- 13 APRILE 2026

NIS: online le determinine sugli adempimenti per i nuovi soggetti e sulle modalità di accesso alla piattaforma ACN

L'Agenzia per la Cybersicurezza Nazionale ha pubblicato le nuove determinazioni operative per l'attuazione della direttiva NIS2, chiarendo obblighi e accesso alla piattaforma dedicata. Per i nuovi soggetti, si definiscono modalità precise di registrazione e gestione degli adempimenti.

[LEGGI TUTTO](#)

AGENZIA PER LA CYBERSICUREZZA NAZIONALE- APRILE 2026

Analisi dello stato della ricerca in cybersicurezza

Una fotografia aggiornata dello stato della ricerca in cybersicurezza in Italia, mettendo in luce punti di forza e margini di crescita. Basata sui dati VQR 2020-2024, l'analisi esplora temi emergenti, tecnologie chiave e il contributo della comunità scientifica. Al centro della pubblicazione, in particolare, il legame tra ricerca, innovazione e priorità strategiche nazionali.

[LEGGI TUTTO](#)

AGENDA DIGITALE EU- 13 APRILE 2026

L'anti allagamento di Venezia sotto cyber attacco: che ci insegna sulle nostre vulnerabilità Paese

Un presunto attacco cyber al sistema anti-allagamento di Piazza San Marco, a Venezia, accende i riflettori su una nuova frontiera del rischio: le infrastrutture fisiche colpite via digitale. Tra rivendicazioni, screenshot dei pannelli di controllo e minacce di accessi ancora attivi, il caso resta avvolto da incertezze ma solleva interrogativi concreti. Sul fondo, un cambio di paradigma: la guerra si combatte anche colpendo sistemi critici e servizi essenziali.

[LEGGI TUTTO](#)

CERT-AGID - 3 APRILE 2026

Rilasciati su Telegram oltre 500 MB di documenti d'identità italiani rubati

È stato rilasciato un archivio RAR contenente documenti di identità di cittadini italiani attraverso un canale Telegram attivo dal novembre 2025 che si firma con il nome "Anonymous Algeria". L'archivio, dalla dimensione di oltre 500 MB, contiene esattamente 500 file di guida corredati da immagini di **selfie identification**, ovvero fotografie dei titolari con il documento in mano accanto al volto. Questa tipologia di dato è particolarmente sensibile in quanto consente di superare i controlli KYC adottati da banche, piattaforme di trading, exchange di criptovalute e altri servizi online.

[LEGGI TUTTO](#)

HD BLOG- 10 APRILE 2026

Signal disinstallato da un iPhone, l'FBI trova il modo di recuperare i messaggi

Un caso giudiziario negli Stati Uniti rimette in discussione le certezze sulla messaggistica "sicura": anche i messaggi cancellati possono riemergere. L'FBI è riuscita a recuperarli da un iPhone sfruttando il database interno delle notifiche, senza violare la crittografia di Signal. Il punto critico non è l'app, ma il sistema operativo, che può conservare anteprime dei messaggi in mano accanto al volto. Questa tipologia di dato è particolarmente sensibile in quanto consente di superare i controlli KYC adottati da banche, piattaforme di trading, exchange di criptovalute e altri servizi online.

[LEGGI TUTTO](#)

NEWS INTERNAZIONALI

EUROPOL- APRIL 16, 2026

Europol-supported global operation targets over 75 000 users engaged in DDoS attacks

A major international operation supported by Europol has taken aim at the growing ecosystem of "DDoS-for-hire" services, now accessible even to non-experts. Authorities across 21 countries identified over 75,000 users and issued targeted warnings worldwide. The crackdown led to domain seizures, arrests and access to vast amounts of marketing data linked to illicit activity. Not just infrastructure, but end users are now in focus, marking a shift in enforcement strategy. A clear message: even those who outsource cyberattacks are firmly on law enforcement's radar.

[LEGGI TUTTO](#)

Articoli Correlati:

- [Interpol, 45,000 malicious IP addresses taken down in international cyber operation, March 13, 2026](#)

CERT-EU - APRIL 8, 2026

Threat Landscape Report 2025: A Year in Review

CERT-EU's Threat Landscape Report 2025 outlines an increasingly complex cyber ecosystem, where threats, actors, and techniques continue to multiply and overlap. The report highlights a growing number of malicious actors, with cyber espionage, supply chain compromise, and exposed internet-facing vulnerabilities remaining key attack vectors. Tactics are evolving rapidly, with wider use of AI, advanced social engineering, and identity-based intrusions. Overall, the report paints a picture of an environment where attacker agility still outpaces defensive capabilities.

[LEGGI TUTTO](#)

U.S. DEPARTMENT OF JUSTICE- APRIL 15, 2026

Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote Information Technology Worker Scheme that Generated \$5M in Revenue for the Democratic People's Republic of Korea

Two U.S. nationals have been sentenced for their role in a scheme that enabled North Korean IT workers to fraudulently obtain remote jobs at more than 100 American companies. The operation relied on stolen identities and "laptop farms" set up inside the U.S. to mask the real location of the workers. Through shell companies and coordinated infrastructure, the defendants helped route payments and sustain a system that generated millions in illicit revenue for the DPRK. The case highlights how remote hiring pipelines can be exploited as a vector for fraud and state-sponsored revenue generation.

[LEGGI TUTTO](#)

MIT TECHNOLOGY REVIEW- APRIL 15, 2026

Cyberscammers are bypassing banks' security with illicit tools sold on Telegram

Cybercriminals are increasingly exploiting Telegram as a marketplace for tools designed to bypass bank security systems, including identity verification and facial "liveness" checks. According to recent reporting, these services combine stolen biometric data with virtual camera software to convincingly impersonate real users during onboarding processes. What was once considered a high-security layer in digital banking is now being systematically undermined at scale through easily accessible kits and step-by-step fraud services.

[LEGGI TUTTO](#)

KREBS ON SECURITY- APRIL 7, 2026

Russia Hacked Routers to Steal Microsoft Office Tokens

Russia-linked hackers are exploiting vulnerabilities in older internet routers to intercept Microsoft Office authentication tokens at scale, affecting over 18,000 networks without using malware. The operation relies on DNS manipulation to enable stealthy adversary-in-the-middle access to cloud sessions. Security researchers link the campaign to GRU-affiliated group Forest Blizzard (APT28/Fancy Bear), targeting governments and critical organizations.

[LEGGI TUTTO](#)

Eventi

MIMIT, SSSCLT e Cyber 4.0, "Data power: governance, sicurezza e difesa della proprietà intellettuale", maggio 2026, webinar online.

Cybercrime Conference, 6-7 maggio 2026, Auditorium della Tecnica, Roma.

Regione Lazio & Lazio Innova, Safe Mobility Hack, 9-11 maggio 2026, Spazio Attivo Roma Tecnopolo, Roma.

Cyber 4.0, Forum Cyber 4.0 2026, 3-4 giugno 2026, Luiss Guido Carli, Aula Chiesa, Roma.

Nuove Pubblicazioni

ACN, Phishing: campagna a tema Klarna, Aprile 2026.

Council of Europe, The Steering Committee of Human Rights, "Human Rights and Artificial Intelligence", April 2026.

Federal Bureau of Investigation, Internet Crime Report.

EU CyberNet, Agentic AI systems Conducting Social Engineering Attacks, EU CyberNet Expert Series, No. 7, 2026.

Cyber FACTory 4.0 è una newsletter con cadenza bimensile. 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