

# CYBERFACTORY 4.0

16-31  
MARZO  
2024

## IN EVIDENZA

**CYBER 4.0, 28 MARZO 2024**

### Save the Date- Forum Cyber 4.0 - 3 e 4 giugno

Il Forum sarà l'occasione per mettere a confronto istituzioni nazionali e comunitarie di riferimento e fare il punto su cybersecurity e transizione digitale in Italia, innovazione tecnologica e competenze, ricerca industriale e prospettive di sviluppo delle imprese cyber, a livello nazionale e internazionale.

[LEGGI TUTTO](#)

FORUM 2024  
CYBER 4.0

**LA REPUBBLICA, 28 MARZO 2024**

### Cyber 4.0, il Centro di competenza nazionale per la sicurezza informatica coinvolge oltre 800 imprese

Quasi un quarto delle aziende italiane ha subito attacchi informatici nel 2022. Un dato che assume ancora più rilevanza se consideriamo quanto il nostro Paese sia particolarmente colpito da questo tipo di problema. Nel 2023, l'Italia è stata vittima dell'11% degli attacchi gravi a livello globale, con un incremento del 65% rispetto all'anno precedente. E sono soprattutto le realtà manifatturiere a rappresentare un bersaglio.

[LEGGI TUTTO](#)



## CYBER 4.0

**AUTOMAZIONE NEWS, 22 MARZO 2024**

### Competence Center al centro dello sviluppo delle imprese

Per la prima volta riuniti a MECSPE tutti gli otto Competence Center, i centri di trasferimento tecnologico, consulenza e formazione co-finanziati dal Mimit che, presente in fiera, ha incontrato aziende e imprenditori sul Piano Transizione 5.0 e sui vantaggi dei progetti e dei servizi dei centri di competenza.

[LEGGI TUTTO](#)

**ANSA, 27 MARZO 2024**

### È on line il sito di Cagliari Digital Lab

E' on line il sito di Cagliari Digital Lab, il progetto, finanziato dal ministero delle Imprese e del Made in Italy che ha come obiettivo aumentare in maniera sostenibile la competitività del territorio con l'applicazione e la diffusione delle tecnologie emergenti, sviluppando progetti di ricerca e trasferendo le tecnologie nei settori strategici che caratterizzano il tessuto economico della città.

[LEGGI TUTTO](#)

## IN ITALIA

**ACN, 18 MARZO 2024**

### ACN e ENISA insieme a Roma per il Programma di Apprendimento e Formazione LETRA

Assidua partecipazione per il programma di apprendimento e formazione, frutto della collaborazione tra l'Agenzia Italiana per la Cybersicurezza Nazionale (ACN) e l'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA). Il programma, tenutosi a Roma e svolto nell'ambito dell'Anno Europeo delle Competenze e dell'iniziativa Cybersecurity Skills Academy, ha visto la partecipazione di 60 dipendenti pubblici provenienti da diverse amministrazioni nazionali ed europee, desiderosi di migliorare le loro conoscenze e competenze in diversi ambiti della cybersicurezza.

[LEGGI TUTTO](#)

**GARANTE PRIVACY, 25 MARZO 2024**

### Intelligenza artificiale: il Garante privacy scrive a Parlamento e Governo. Necessario individuare Autorità di vigilanza indipendenti e imparziali

Intelligenza artificiale: il Garante privacy scrive a Parlamento e Governo Necessario individuare Autorità di vigilanza indipendenti e imparziali. Il Garante per la protezione dei dati personali possiede i requisiti di competenza e indipendenza necessari per attuare il Regolamento europeo sull'intelligenza artificiale coerentemente con l'obiettivo di un livello elevato di tutela dei diritti fondamentali.

[LEGGI TUTTO](#)

**CYBERSECURITY 360, 28 MARZO 2024**

### World Backup Day 2024: i consigli degli esperti per una maggiore resilienza operativa

Il 31 marzo è il World Backup Day 2024, la Giornata Internazionale del Backup che ci ricorda l'importanza di salvaguardare i dati in azienda. La data non è frutto della casualità, ma precede il primo aprile, giorno dei pesci d'aprile (in inglese April Fools), dove solo i pazzi non hanno consapevolezza della priorità di mettere in sicurezza i dati, sempre a rischio perdita, in seguito ad incidenti o cyber attacchi.

[LEGGI TUTTO](#)

**INNOVATION POST, 24 MARZO 2024**

### Verso l'Industria 5.0: tecnologia, sostenibilità e umano-centrismo per vincere la sfida delle twin transitions

Per vincere le sfide delle "transizioni gemelle" digitale e green l'innovazione tecnologica è fondamentale al pari del driver della sostenibilità e della centralità umana. Esperti del settore accademico e industriale a confronto sul ruolo della formazione, della governance aziendale e delle tecnologie come l'AI nel supportare un modello di business resiliente e sostenibile, in linea con il paradigma dell'Industria 5.0, evidenziando come queste trasformazioni richiedano un approccio olistico e interdisciplinare.

[LEGGI TUTTO](#)

**MILANO FINANZA, 23 MARZO 2024**

### Ibm, apre a Roma la scuola di Cybersec

La lotta agli attacchi informatici passa per la capitale. Dopo Washington e Bangalore infatti Ibm, il colosso americano dell'informatica, ha scelto Roma per il suo nuovo hub dedicato alla protezione informatica. Situato nel centro di Roma, a due passi da Piazza di Spagna, il nuovo centro a regime sarà in grado di formare circa 2200 persone all'anno grazie anche alle collaborazioni con il laboratorio Ibm Research di Zurigo e degli esperti di Sistemi Informativi, società del gruppo Ibm, che ha investito sulle competenze digitali a Rieti in collaborazione con la Regione Lazio.

[LEGGI TUTTO](#)

## NEWS INTERNAZIONALI

**PROOFPOINT, MARCH 18, 2024**

### FBI's IC3 Report: Losses from Cybercrime Surpass \$12.5 Billion—a New Record

The 2023 Internet Crime Report from the FBI's Internet Crime Complaint Center (IC3) is out. And for defenders, it's a troubling read. The FBI saw only a minor uptick in reported cybercrime complaints last year from the American public. On the surface, this seems like positive news. There were only 79,474 more complaints filed than in 2022. However, that total is much more significant when you consider the potential losses from cybercrime. Losses surpassed \$12.5 billion last year, a 22% increase from 2022 and a new record high.

[LEGGI TUTTO](#)

**AP NEWS, MARCH 22, 2024**

### The UN adopts a resolution backing efforts to ensure artificial intelligence is safe

The General Assembly approved the first United Nations resolution on artificial intelligence Thursday, giving global support to an international effort to ensure the powerful new technology benefits all nations, respects human rights and is "safe, secure and trustworthy."

The resolution, sponsored by the United States and co-sponsored by 123 countries, including China, was adopted by consensus with a bang of the gavel and without a vote, meaning it has the support of all 193 U.N. member nations.

[LEGGI TUTTO](#)

**VENTURE BEAT, MARCH 21, 2024**

### Why adversarial AI is the cyber threat no one sees coming

Security leaders' intentions aren't matching up with their actions to secure AI and MLOps according to a recent report. An overwhelming majority of IT leaders, 97%, say that securing AI and safeguarding systems is essential, yet only 61% are confident they'll get the funding they will need. Despite the majority of IT leaders interviewed, 77%, saying they had experienced some form of AI-related breach (not specifically to models), only 30% have deployed a manual defense for adversarial attacks in their existing AI development, including MLOps pipelines.

[LEGGI TUTTO](#)

**RESECURITY, MARCH 16, 2024**

### The Aviation And Aerospace Sectors Face Skyrocketing Cyber Threats

The aerospace sector has become a rising target for cyberattacks due to its reliance on vastly interconnected digital infrastructures, global supply chains, and the torrential volume of sensitive data it handles. More recently, this attack trend has been amplified by the rapidly growing integration of Industrial Internet of Things (IIoT) technologies, rising geopolitical tensions, and the U.S. governments' decision to designate aerospace and aviation as critical infrastructure.

[LEGGI TUTTO](#)

**THE NEW YORK TIMES, MARCH 25, 2024**

### U.K. Accuses China of Cyberattacks Targeting Voter Data and Lawmakers

The British government on Monday accused China of cyberattacks that compromised the voting records of tens of millions of people, a sharp rebuke that underlined the hardening of Britain's stance toward China since its leaders heralded a "golden era" in British-Chinese relations nearly a decade ago.

[LEGGI TUTTO](#)

**INTERNATIONAL MONETARY FUND, MARCH 15, 2024**

### IMF Investigates Cyber-Security Incident

Washington, DC: The International Monetary Fund (IMF) recently experienced a cyber incident, which was detected on February 16, 2024. A subsequent investigation, with the assistance of independent cybersecurity experts, determined the nature of the breach, and remediation actions were taken.

[LEGGI TUTTO](#)

**SECURITY AFFAIRS, MARCH 19, 2024**

### New acidpour wiper targets Linux x86 devices. is it a Russia's weapon?

A new variant of a data wiper AcidRain, tracked as AcidPour, is specifically designed for targeting Linux x86 devices has been detected in the wild. Researchers at SentinelLabs first discovered the wiper AcidRain in March 2022. The malware that hit routers and modems and was suspected to be linked to the Viasat KA-SAT attack that occurred on February 24th, 2022.

[LEGGI TUTTO](#)

## Nuove Pubblicazioni

Enisa, Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats, March 27, 2024

NRD Cybersecurity, Collective Cybersecurity Evaluation, vol 2, March 2024

Csirt, La settimana Cibernetica del 24 marzo 2024

Securelist, Threat landscape for industrial automation systems, H2 2023, March 19, 2024

Proofpoint, The 2024 Data Loss Landscape Report Explores Carelessness and Other Common Causes of Data Loss, March 19, 2024

## Prossimi Eventi

Mimit, Strategia Nazionale di Cybersicurezza 2022-2026 – Ciclo di Seminari Online  
Automotive e Cybersecurity: vulnerabilità, sistemi di protezione e quadro normativo, 11 Aprile 2024 ore 9:30  
Per partecipare richiedere il link a: [scuolasuperiore.tlc@mise.gov.it](mailto:scuolasuperiore.tlc@mise.gov.it)

ICT Security Magazine, Cyber Crime Conference, Roma Auditorium della Tecnica, 17 e 18 Aprile 2024

Forum Cyber 4.0, 3-4 Giugno 2024, The Dome Luiss, Roma

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 rimosioni da questa lista di distribuzione, contattare: [comunicazione@cyber40.it](mailto:comunicazione@cyber40.it)