CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

LA NEWSLETTER SULLA CYBERSICUREZZA

1-15 SETTEMBRE 2023

CYBER 4.0

CYBER 4.0 - **29 AGOSTO 2023**

Consulta le FaQ aggiornate sul Bando 1/2023!

[Leggi tutto]

IN EVIDENZA

CORRIERE COMUNICAZIONI - **4 SETTEMBRE 2023**

Cybersecurity, Mantovano: "In arrivo 220 milioni per rafforzare le difese"

L'annuncio del sottosegretario alla Presidenza del Consiglio: "Sicurezza informatica priorità di governo". E sul fronte competenze: "L'Agenzia per la cybersicurezza a lavoro per ingaggiare alte professionalità"

LEGGI TUTTO

NEWS NAZIONALI

Firmato il protocollo d'intesa per l'infrastruttura di supercalcolo Cineca

È stato firmato oggi il protocollo d'intesa tra ACN e il consorzio Cineca, nell'ambito dell'evento inaugurativo dell'ampliamento della sede di CINECA a Napoli con la realizzazione di un data center ad alta efficienza energetica. L'accordo prevede una procedura ad evidenza pubblica - di cui Cineca sarà stazione appaltante - per l'acquisizione del sistema High Performance Computing (HPC) dell'Agenzia da collocare presso il nuovo centro di Napoli. Il sistema sarà dedicato, come previsto dal PNRR, al monitoraggio della minaccia cyber centrale, l'HyperSOC, anche attraverso l'utilizzo di strumenti di intelligenza artificiale e machine learning.

ACN - **11 SETTEMBRE 2023**

LEGGI TUTTO

Sventato attacco informatico alla Regione Campania. Il Governatore De Luca: "Ci siamo difesi bene"

"Questo fine settimana il sistema informatico della Regione Campania ha subito un attacco informatico che abbiamo governato, essendoci preparati per tempo". Lo ha detto il governatore della Campania **Vincenzo De Luca** nel corso del suo intervento alla cerimonia inaugurale del congresso nazionale della Società italiana di Fisica, ospitato quest'anno nella sede di Fisciano dell'Università di Salerno.

CYBERSECURITY ITALIA - **11 SETTEMBRE 2023**

LEGGI TUTTO

Un attacco informatico paralizza i siti di Roma Capitale gestiti da Zetema progetto cultura

Una situazione di emergenza si è verificata questa mattina quando i siti web di **Roma Capitale** gestiti da **Zetema Progetto Cultura** sono stati oggetto di un attacco informatico che li ha resi completamente inaccessibili. L'evento ha scatenato una reazione immediata da parte dell'azienda, che ha iniziato a indagare sulla portata e la natura dell'attacco.

RED HOT CYBER - **11 SETTEMBRE 2023**

LEGGI TUTTO

Sintesi riepilogativa delle campagne malevole nella settimana 02 – 08 Settembre 2023

In questa settimana, il CERT-AgID ha riscontrato ed analizzato, nello scenario italiano di suo riferimento, un totale di **39 campagne malevole**, di cui 31 con obiettivi italiani e 8 generiche che hanno comunque interessato l'Italia, mettendo a disposizione dei suoi enti accreditati i relativi **228 indicatori di compromissione (IOC) individuati**.

CERT - AGID - **8 SETTEMBRE 2023**

LEGGI TUTTO

NIST: standardizzazione degli algoritmi di crittografia in grado di resistere agli attacchi dei computer quantistici

Il National Institute of Standards and Technology (NIST), l'anno scorso aveva selezionato quattro algoritmi progettati per resistere agli attacchi dei computer quantistici. Ora ha avviato il processo di standardizzazione di questi algoritmi, il passo finale prima di rendere disponibili questi strumenti matematici in modo che le organizzazioni di tutto il mondo possano integrarli nella loro infrastruttura di crittografia.

CYBERSECURITY TRENDS - **4 SETTEMBRE 2023**

LEGGI TUTTO

Articoli correlati

NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers, August 24, 2023
https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

NEWS INTERNAZIONALI

FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com

The FBI is issuing this release to warn the public regarding the theft of approximately $41 million in virtual currency from Stake.com, an online casino and betting platform. The FBI has confirmed that this theft took place on or about September 4, 2023, and attributes it to the Lazarus Group (also known as APT38) which is comprised of DPRK cyber actors.

FBI - **SEPTEMBER 6, 2023**

READ MORE

Is the energy sector prepared for cyber breaches?

An instant and endless supply of electricity is taken for granted in many parts of the world. The flick of a switch powers the work and family lives of billions of people.
But the energy systems that underpin entire economies are facing "an unprecedented threat" from cyberattacks, according to the International Energy Agency (IEA).

WORLD ECONOMIC FORUM - **SEPTEMBER 5, 2023**

READ MORE

Thinking about the security of AI systems

One of the most widely reported weaknesses in the security of the current generation of LLMs is their vulnerability to 'prompt injection', which is when a user creates an input designed to make the model behave in an unintended way. This could mean causing it to generate offensive content, reveal confidential information, or trigger unintended consequences in a system that accepts unchecked input from the LLM.

NCSC UK - **AUGUST 30, 2023**

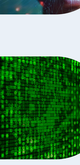
READ MORE

The Rise of Deepfakes: From Virtual Reality to Misinformation

In an era where the veracity of visual and audio evidence has historically been taken for granted, the rise of deepfakes presents a critical challenge. Here, we explore the impact of seemingly undetectable deepfakes on society, investigations, and disputes, examining how the prevailing trust in what people see or hear can be – and increasingly is – exploited.

ALIX PARTNERS - **SEPTEMBER 12, 2023**

READ MORE



Russian infosec boss gets nine years for $100M insider-trading caper using stolen data

Vladislav Klyushin, the Russian owner of security penetration testing firm M-13, was jailed for nine years in the US on Thursday for his involvement in a cyber-crime operation that stoke top corporations' confidential financial information to make $93 million through insider trading.

THE REGISTER - **SEPTEMBER 8, 2023**

READ MORE

Nuove pubblicazioni

- CSIRT Nazionale, La Settimana Cibernetica del 10 settembre 2023, 11 Settembre 2023
- Europol, Cyber-attacks: the apex of crime-as-a-service (IOCTA 2023), September 13, 2023
- NCSC UK, Ransomware, Extortion and the Cyber Crime Ecosystem, September 11, 2023
- ICJ, Joint Cybersecurity Advisory, Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475, September 7, 2023
- CISA, CISA Releases Capacity Enhancement Guide to Strengthen Agency Resilience to DDoS Attack, September 6, 2023
- Enisa, Dive into the Deep Sea. A View of the Subsea Cable Ecosystem, August 31, 2023
- Council of Europe – Parliamentary Assembly, Pegasus and similar spyware and secret state surveillance, September 8, 2023

Prossimi eventi

Roadshow Cyber 4.0, Cybersecurity per le Imprese della Regione Puglia, Contesto Strategico e Opportunità di Sviluppo, Martedì 26 Settembre ore 9.30, Bari, Confindustria Bari-BAT, Via Amendola 172/5

Cybersecurity in, for and from space, Giovedì 28 Settembre ore 9:00, Roma, Agenzia Spaziale Italiana, Via del Politecnico

Roadshow Cyber 4.0, Cybersecurity per le Imprese della Regione Sardegna, Contesto Strategico e Opportunità di Sviluppo, Confindustria Cagliari, Martedì 3 Ottobre 2023

Cybersecurity in azienda, L'importanza della prevenzione e del monitoraggio, 12 Ottobre 2023 ore 17.00, Confindustria Como, Via Raimondi 1, Como

SECURE TALKS Cybersecurity Forum, 13 ottobre 2023, Villa Malfitano, Palermo

VUOI DARCI IL TUO FEEDBACK SULLA NEWSLETTER?

COMPILA IL FORM

Cyber FACTory 4.0 è una newsletter con cadenza bisettimanale.
Le notizie sono selezionate per ottenere 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@cyber4.it**

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

© Cyber 4.0 - All Rights Reserved