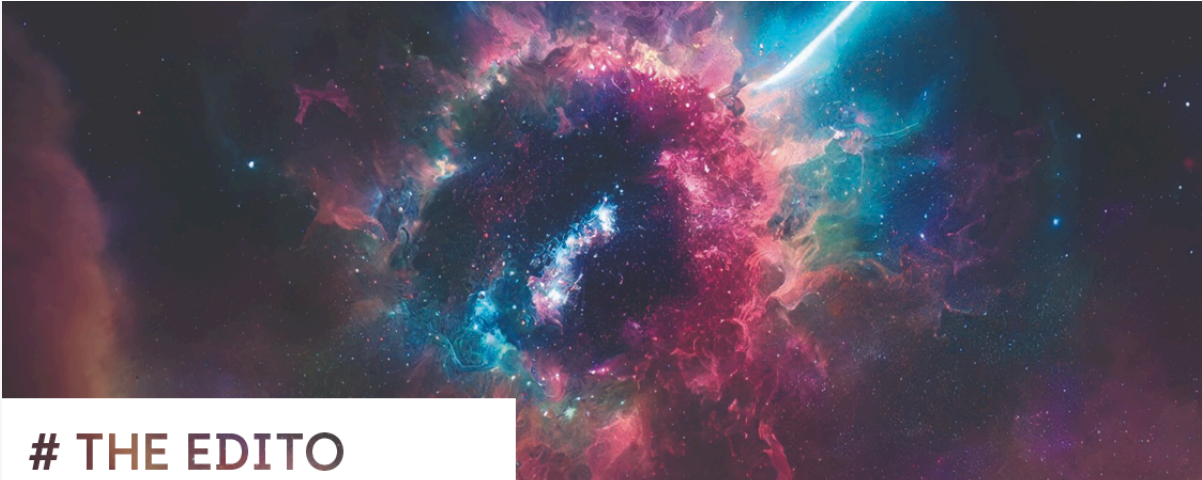**IN CYBER NEWS**
THE MEDIA HUB
OF DIGITAL TRUST

February 2025

inCyber News Newsletter

THE EDITO

In just a few days, DeepSeek, the new Chinese generative artificial intelligence, has caused a seismic shift in this cutting-edge field. Developed at a fraction of the cost compared to its American counterparts and delivering performance that rivals—or even surpasses—that of OpenAI or Google DeepMind, this free, energy-efficient, and fully open-source chatbot is a wake-up call for the AI world.

Read the edito

VIDEO of the MONTH

Cybersecurity: the challenge of scaling up

CYBER INFO

Zero-trust architecture: comprehensive guide based on nist guidelines

👉 **Thomas Joos**

The zero-trust architecture (ZTA) is a modern security paradigm designed to replace traditional perimeter-based security models. It assumes that no device, user, or network is inherently trustworthy. Instead, trust is explicitly established through continuous verification and context-based decisions. Deloitte describes zero trust as a paradigm shift in cybersecurity, replacing traditional static security concepts. The motto "never trust, always verify" underscores the necessity of dynamically, risk-based, and context-sensitive verification for all data access.

Read the article

Challenge or Opportunity: Should Chinese Tech Be Concerned About Donald Trump's Return?

👉 **Emmanuel Langlois**

ZTE, Huawei, TikTok, DeepSeek, and now RedNote... Chinese technologies are flooding screens and networks worldwide, including in the United States. Since his return, Donald Trump has had nothing but harsh words for this so-called Chinese "invasion," threatening China with severe measures such as increased tariffs or an outright ban on TikTok in the U.S. However, behind the scenes, the new White House occupant is primarily focusing on deals negotiated with Chinese authorities, fully aware that the United States cannot do without Beijing in this sector—just as China cannot do without the U.S.

Read the article

Social Networks: The End of Fact-Checking Disrupts Moderation Policies

👉 **Xavier Biseul**

Following X's lead, Meta has decided to discontinue the use of human fact-checkers, instead relying on AI and user self-regulation to moderate content on Facebook and Instagram. Is this a return to basics or a step backward? Opinions are divided.

Read the article

Local Authorities in Disarray Against Cyber Risks

👉 **Alain Clapaud**

Occasionally collateral victims of large-scale phishing campaigns, sometimes targets of deliberate attacks, local authorities are paying a high price for the relatively low cyber maturity, especially among smaller entities. Despite evident efforts, limited budgets and human resources hinder progress in the sector.

Read the article

FOLLOW US!
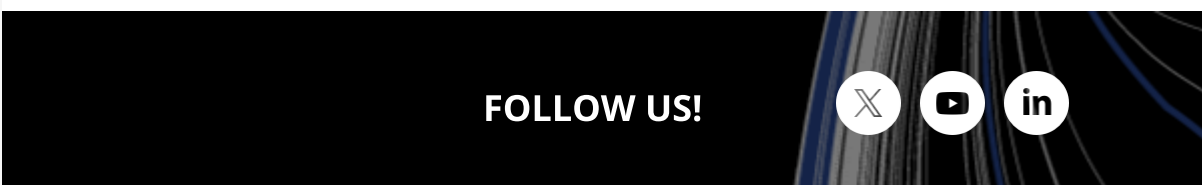
SAVE THE DATE

PDJ - ID governance as the cornerstone of application security (FR)

March, 05th 2025

Businesses are increasingly relying on applications. Their functions and uses have become strategic. They facilitate collaboration, automate repetitive tasks, and enhance productivity. The advent of cloud technology has been—and continues to be—a revolution for the industry.

However, there is an element of risk: the information shared within these software applications, their proper functioning, and dependencies are frequent targets of attacks. These attacks vary in their intentions and forms. The consequences are dire for organizations, their clients, and employees.

The focus will be on practical field insights:

- How to anticipate and mitigate the risks of compromise while adhering to essential regulatory frameworks (ISO 27001, SOC 2, GDPR)?
- What are the best practices in identity governance?
- What technologies can secure access?
- What tools are available to adapt to the ever-growing use of cloud applications?

Register for the webinar!

Contact : media@forum-incyber.com