IN CYBER FORUM EUROPE

PRESS RELEASE

The InCyber Europe 2025 Forum will focus on the issue: "Zero trust, trust for all?"

There is no trust without cybersecurity, and cybersecurity is sometimes based on the absence of a priori trust. In an increasingly hyperconnected, distributed, and transactional world, which demands collective and collaborative cybersecurity, “Zero Trust” is emerging as a response to the growing challenges of cybersecurity.

Trust and security have always had an ambivalent relationship. Although there is no precise definition of the concept of digital trust, it is generally accepted that cybersecurity is one of the key conditions for trust. Yet, although it is necessary, it is not sufficient to ensure trust, whether it be the trust of individuals "in" digital technologies, or the relationship of trust that two individuals or two machines can establish "via" digital technologies. Other essential trust criteria include reliability, privacy protection, algorithmic transparency, accessibility, and interoperability. Therefore the two concepts do not completely overlap. In fact, they differ quite widely in their characteristics: whereas security is built using measures, procedures, and policies, and evaluated using objective criteria, trust is first and foremost a belief or hope in the identity, reliability, integrity, or capacity of an individual or a system. Finally, trust - or rather its excess - can be opposed to security when it is granted implicitly and a priori, i.e. without proof or regular verification.

This is precisely what the "Zero Trust" model is all about: in a transactional world, where exchanges take place mainly online, making trust objective by relying on tangible evidence to guarantee that a given individual, organization, system, or network is what it claims to be, and is worthy of the trust it claims to deserve. In order to access resources, applications, or data, individuals or systems must identify themselves and be authenticated. This is the end of fortresses. Remote working, extended organizations, hyperconnectivity, the public cloud, IoT, the endless extension of our attack surface

FORUM INCYBER
contact@forum-incyber.com
europe.forum-incyber com

and their corollary, and the multiplication of IT threats, have all taken their toll on the implicit trust that once prevailed. Now comes the era of "never trust, always control".

Technologies for identity management, access control, detection and reaction, micro-segmentation, etc. promise multi-layered, granular security, focused on the network endpoints. Invisibility and decoy technologies are also making headway. Trust is no longer implicit. Rather, it is explicit and constantly monitored. "Zero Trust", or even distrust, has become the prerequisite for (re)establishing trust. Some criticize the marketing buzz surrounding this concept, while others point the finger at the illusion of security that these approaches provide, the technical complexity involved, the lack of interoperability of solutions, the difficulty of the user experience, and their limited social acceptance.

"There's a "Zero Trust" paradox because it's all about creating trust through prior mistrust. But this is undoubtedly the price we have to pay for a safer digital world," points out General (2S) Marc Watin-Augouard, founder of the InCyber Forum. What is valid in the digital space is also true in the real world: in an uncertain environment, relationships between individuals, organizations, or states are increasingly established and based on explicit trust, founded on compliance criteria, verifications, due diligence, etc.".

"The "Zero Trust" model undoubtedly contains an element of utopianism. But it's a virtuous utopia, once you confront it with real-life situations. It would be a mistake to think that this transformation is purely technical", explains Guillaume Tissier, Managing Director of the InCyber Europe Forum.

The 16th InCyber Forum, held from March 26 to 28, 2024, attracted 17,500 participants (+10%). Its next editions will take place in Montreal on October 29 and 30, 2024, in Lille (April 1 to 1, 2025), and in San Antonio (Texas) on June 17 and 18, 2025.

FORUM INCYBER
contact@forum-incyber.com
europe.forum-incyber com

PRESS RELEASE

ABOUT THE FORUM INCYBER

Today, the InCyber Forum is Europe's leading digital security and trust event. The event combines a forum, a trade show, and a summit attended by numerous French and foreign institutions and companies, bringing together the entire digital security and digital trust ecosystem: end customers, service and solution providers, government agencies, local authorities, research organizations, and associations.

Press contacts:

DGM Conseil

Théodore Michel - Consultant theodore.michel@dgm-conseil.fr

Clémence Naizet - Consulting Director clemence.naizet@dgm-conseil.fr