Programme

Associated Events

CF
CYBERSECURITY FOR INDUSTRY

ID &KYC
FORUM

TRUST &SAFETY
FORUM

W3S
WEB3 SECURITY SUMMIT

INCYBER INVESTOR DAY

OSINT DAY

INCYBER FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

CF

CYBERSECURITY
FOR INDUSTRY

IN CYBER
FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Cybersecurity For Industry is the event associated with the InCyber Forum, dedicated to cybersecurity issues in the industrial world. The only one of its kind in Europe, it provides a forum for the exchange and discovery of cybersecurity solutions for industry, as well as secure industrial solutions.

Implementing Cybersecurity in OT and Industrial Systems: Insights from the Field

Operational Technologies (OT) and Industrial Control Systems (ICS) play a crucial role in critical infrastructures such as energy, transportation, and water supply. However, these systems are increasingly facing threats from malicious actors.
Understanding how attackers exploit specific vulnerabilities in these systems and assessing the potential consequences of a successful intrusion is essential. Strengthening the resilience of OT/ICS systems is of the utmost importance toensure the continuity of essential services in our modern society. This session provides practical insights from the field to address these critical challenges.

Ensuring the Security of Autonomous Systems

The rise of autonomous systems, including autonomous vehicles, drones, and industrial robots, promises to enhance efficiency, precision, and safety in various domains. However, this growing autonomy poses a significant cybersecurity challenge, especially in Operational Technologies (OT). The central question is how to reconcile system autonomy with cybersecurity. How can autonomous systems be designed to make complex decisions while resisting sophisticated attacks? What measures can be taken to protect critical infrastructure based on autonomous OT systems?

Securing the Entire Supply Chain in the Connected Factory

Securing the entire supply chain within a connected factory is a major concern in the era of Industry 4.0. The primary goal is to ensure operational continuity while safeguarding sensitive data and industrial processes. Connected factories integrate advanced technologies such as the Internet of Things (IoT), automation, robotics, and computerized management systems. While this enhances efficiency, inventory management, and traceability, it also exposes the entire supply chain to new security risks. What are the potential risks in the connected factory, and how can they be assessed to implement appropriate security measures? How can cybersecurity for Industrial Control Systems (ICS) be ensured while maintaining the availability and performance of equipment in a connected factory?

Micro-Segmentation: Key to OT Resilience?

Micro-segmentation in the industrial environment is a significant challenge in the era of increasing digitization and automation. This approach involves dividing computer networks into segments, thereby isolating different parts of the industrial infrastructure and reinforcing the security of industrial systems. By isolating each component or device, it limits the spread of potential threats within the network. Each segment can be configured with specific rules, allowing or disallowing communication with other segments. As a result, it offers a proactive response to cyber threats, preserving the integrity and performance of industrial enterprises. How can micro-segmentation help companies enhance their security in an industrial context? What are the best practices for maintaining effective micro-segmentation in the long term in an industrially evolving environment?

IN CYBER FORUM

EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Contacts

partnerships

partenariat@forum-incyber.com

programme

programme@forum-incyber.com