Programme

Événements associés

CF CYBERSECURITY FOR INDUSTRY

ID &KYC FORUM

TRUST &SAFETY FORUM

W3S WEB3 SECURITY SUMMIT

INCYBER INVESTOR DAY

JOURNÉE OSINT

FORUM INCYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

CFI

CYBERSECURITY
FOR INDUSTRY

FORUM INCYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Cybersecurity For Industry, est l'événement associé du Forum InCyber dédié aux problématiques de cybersécurité du monde industriel. Unique en Europe, il est un carrefour d'échanges et de découverte des solutions de cybersécurité pour l'industrie, ainsi que des solutions industrielles sécurisées.

Tables rondes

Mise en place de la cybersécurité dans les réseaux OT et les systèmes industriels : retours du terrain

Les technologies opérationnelles (TO) et les systèmes de contrôle industriel (SCI) jouent un rôle fondamental pour les infrastructures critiques, dans des domaines tels que l'énergie, les transports et l'approvisionnement en eau. Cependant, ces systèmes font face à des menaces croissantes de la part d'acteurs malveillants. Il est crucial de comprendre comment ces attaquants exploitent les vulnérabilités spécifiques de ces systèmes et d'évaluer les conséquences potentielles d'une intrusion réussie. Le renforcement de la résilience des systèmes TO/SCI est de la plus haute importance pour assurer la continuité des services essentiels dans notre société moderne. Un retour du terrain pour appréhender concrètement ces enjeux cruciaux.

Comment assurer la protection des systèmes autonomes ?

L'avènement des systèmes autonomes, tels que les véhicules autonomes, les drones et les robots industriels, promet d'améliorer l'efficacité, la précision et la sécurité dans divers domaines. Cependant, cette autonomie croissante engendre un défi majeur en matière de cybersécurité, en particulier dans les Technologies Opérationnelles (OT). La question centrale est de concilier l'autonomie des systèmes avec leur cybersécurité. Comment concevoir des systèmes autonomes capables de prendre des décisions complexes tout en résistant aux attaques sophistiquées ? Comment protéger les infrastructures critiques basées sur des systèmes OT autonomes ?

Tables rondes

Sécuriser l'ensemble de la chaîne logistique dans le cadre de l'usine connectée

La sécurisation de l'ensemble de la chaîne logistique au sein d'une usine connectée est une préoccupation majeure dans l'ère de l'industrie 4.0. Dans ce contexte, l'objectif principal est de garantir la continuité des opérations tout en protégeant les données et les processus industriels sensibles. Les usines connectées intègrent des technologies avancées telles que l'Internet des objets (IoT), l'automatisation, la robotique, et les systèmes de gestion informatisée. Cela permet une efficacité accrue, une meilleure gestion des stocks et une traçabilité améliorée, mais cela expose également l'ensemble de la chaîne logistique à de nouveaux risques de sécurité. Quels sont les risques potentiels dans l'usine connectée, et comment peuvent-ils être évalués pour mettre en place des mesures de sécurité adéquates ? Comment garantir la cybersécurité des systèmes de contrôle industriel (SCI) tout en maintenant la disponibilité et la performance des équipements dans une usine connectée ?

Micro-segmentation : Clé de la résilience OT ?

La micro-segmentation dans l'environnement industriel représente un enjeu majeur à l'ère de la numérisation et de l'automatisation croissante. Cette approche consiste à diviser les réseaux informatiques en segments, isolant ainsi les différentes parties de l'infrastructure industrielle les unes des autres, renforçant de fait la sécurité des systèmes industriels. En isolant chaque composant ou appareil, elle limite la propagation des menaces potentielles au sein du réseau. Chaque segment peut être configuré avec des règles spécifiques, autorisant ou interdisant la communication avec d'autres segments. En conséquence, elle offre une réponse proactive aux menaces cybernétiques, préservant l'intégrité et la performance des entreprises industrielles. Comment peut-elle aider les entreprises à renforcer leur sécurité dans un contexte industriel ? Quelles sont les meilleures pratiques pour maintenir une micro-segmentation efficace à long terme dans un environnement industriel en constante évolution ?

FORUM IN CYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Contact

partenariats

partenariat@forum-incyber.com

programme

programme@forum-incyber.com