Threat Intelligence appliquée aux environnements OTICS MITRE ATT&CK for ICS

Lien : https://innov-systems.com/formation/threat-intelligence-appliquee-aux-environnements-otics-mitre-attck-for-ics

DURÉE
5 jours (35h)

RÉFÉRENCE
SI120

CATÉGORIE
Cyber Threat Intelligence (CTI)

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les spécificités de la cybersécurité OT/ICS
- Utiliser le framework MITRE ATT&CK for ICS pour modéliser les menaces
- Collecter et analyser des données de Threat Intelligence industrielle
- Détecter les attaques ciblant les systèmes SCADA et PLC
- Intégrer la Threat Intelligence dans un SOC industriel
- Améliorer la détection des incidents en environnement OT
- Développer des modèles de menace pour infrastructures critiques
- Renforcer la résilience des systèmes industriels
- Mettre en place des stratégies de défense adaptées aux environnements OT
- Corréler les événements IT et OT pour une meilleure visibilité
- Optimiser les capacités de réponse aux incidents industriels
- Étudier des cas concrets d’attaques sur infrastructures OT

POUR QUI ?

- Ingénieurs cybersécurité OT/ICS
- Analystes SOC industriels
- Architectes sécurité industrielle
- Ingénieurs systèmes SCADA/PLC
- Responsables cybersécurité industrielle (CISO OT)
- Consultants en cybersécurité industrielle
- Ingénieurs réseau industriel
- Threat intelligence analysts
- Responsables infrastructure critique
- Intégrateurs systèmes industriels
- Experts en sécurité des infrastructures énergétiques, transport et manufacturing
- Toute personne impliquée dans la sécurité des environnements OT et industriels critiques

Innov Systems

Programme détaillé

1 / Introduction à la Threat Intelligence en environnements OT/ICS

- Différences entre IT, OT et ICS
- Enjeux de cybersécurité industrielle critique
- Rôle de la Threat Intelligence dans la défense OT

2 / Panorama des systèmes OT/ICS

- SCADA, DCS et PLC : architecture et fonctionnement
- Supervision industrielle et systèmes critiques
- Surface d’attaque des environnements industriels

3 / MITRE ATT&CK for ICS

- Structure du framework MITRE ATT&CK ICS
- Tactiques, techniques et procédures (TTPs)
- Cartographie des menaces industrielles

4 / Sources de Threat Intelligence industrielles

- Feeds de menaces (CERT, ISACs, vendors industriels)
- Logs industriels et télémétrie OT
- Open Source Intelligence (OSINT) appliquée à l’OT

5 / Collecte et analyse des données de menace

- Agrégation des événements de sécurité OT
- Corrélation des incidents industriels
- Détection des comportements suspects

Innov Systems

6 / Détection des attaques ciblant l’OT/ICS

- Attaques sur protocoles industriels (Modbus, OPC UA, DNP3)
- Malware industriel et sabotage
- Détection des intrusions en environnement SCADA

7 / Intégration avec les SOC et SIEM

- Corrélation IT/OT des événements de sécurité
- Intégration avec SIEM et SOAR
- Cas d’usage de réponse automatisée

8 / Modélisation des menaces et scénarios d’attaque

- Construction de threat models industriels
- Simulation d’attaques sur infrastructures critiques
- Analyse des risques opérationnels

9 / Stratégies de défense et mitigation

- Segmentation réseau IT/OT
- Zero Trust appliqué aux environnements industriels
- Plans de réponse aux incidents OT

10 / Cas pratiques et retour d’expérience industriel

- Analyse d’incidents réels OT/ICS
- Utilisation de MITRE ATT&CK ICS en environnement SOC
- Bonnes pratiques de cybersécurité industrielle

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés