Développez vos talents
Certifiez vos compétences

Sécurité défensive

Cybersécurité des systèmes industriels (SCADA)

3 jours (21h00) | ★★★★★ 5/5 | SEC-SCA | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Sécurité défensive

À l'issue de ce stage vous serez capable de :

- Connaître le métier et les problématiques
- Dialoguer avec les automaticiens
- Connaître et comprendre les normes et standards propres au monde industriel
- Auditer un système SCADA
- Développer une politique de cybersécurité.

Niveau requis

Avoir de bonnes connaissances générales en informatique et en sécurité des systèmes d'information.

Public concerné

Auditeurs, responsables de sécurité, automaticiens, architectes et administrateurs réseaux et systèmes ICS / SCADA (Industrial Control Systems / Supervisory Control And Data Acquisition).

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Introduction : enjeux d'une infrastructure industrielle

- Les enjeux d'un système d'information
- Spécificités et contraintes opérationnelles
- Prise de conscience de l'importance de la sécurité des SI industriels au sein de l'Etat et des entreprises : les différents aspects
- Evolution des infrastructures industrielles

Risques et menaces

- Retour d'expérience sur les incidents majeurs connus
- Exemples d'attaques réelles, déroulements et impacts (Stuxnet)
- Les facteurs de risques
- Les grands risques et familles de vulnérabilités
- Les menaces APT (Advanced Persistent Threat)
- Les postures de sécurité moderne des systèmes ICS

Tour d'horizon des ICS

- Familles fonctionnelles d'ICS
- Types d'équipements et exemples
- Architectures ICS par secteur
- Contraintes
- Protocoles industriels
- Impact des attaques sur les ICS / SCADA
- Analyse du risque dans les systèmes ICS / SCADA

Vulnérabilités intrinsèques des ICS

- Vulnérabilité réseau
- Vulnérabilité applicative
- Analyse avancée de la sécurité des PLC (Programmable Logic Controller)
- Retours sur expérience :
  - Le malware Stuxnet et Duqu
  - Le malware Triton
  - Attaques sur les ICS

Exemples de travaux pratiques (à titre indicatif)

- *TP offensif*
  - *Découvrir le protocole Modbus*
  - *Maîtriser les attaques sur le protocole Modbus*
  - *Découvrir les attaques sur S7comm*
  - *Découvrir les protocoles BACnet et EtherNet/IP*
  - *Maîtriser le "fuzzing" protocolaire des protocoles ICS / SCADA avec Aegis*
  - *Découvrir les surfaces d'attaque sur les PLC*
  - *Découvrir des attaques complémentaires sur les PLC*
  - *Maîtriser l'analyse de firmware sur les PLC*

Evaluer la sécurité de ses installations

- Diagnostic préalable
- Tests à prévoir pour des installations locales et/ou distribuées
- Outillage nécessaire pour l'audit
- Failles les plus couramment rencontrées
- Les plans d'actions types à appliquer et les outils requis

Exemples de travaux pratiques (à titre indicatif)

- *TP offensif*
  - *Mettre en place un threat modelling pour attaquer les architectures réseaux ICS / SCADA*
  - *Introduire metasploit pour le test d'intrusion des systèmes ICS / SCADA*
  - *Maîtriser l'exploitation de vulnérabilités dans les environnements ICS / SCADA*
  - *Découvrir le pivoting dans les environnements ICS / SCADA*
- *TP défensif*
  - *Analyse de trames / Forensic*
  - *Réalisation de règles Snort*
  - *Configuration d'un honeypot*
  - *Conception d'une architecture sécurisée*

Accès distants

- RTC
- VPN
- Boîtiers de télétransmission
- Sans-fil (Wi-Fi, liaisons radio)
- Problèmes des automates et IHM exposés sur Internet

Postures défensives de protection des ICS

- Définir une politique de sécurité
- Mener une évaluation des risques
- Sécurisation technique
  - Chiffrement
  - Durcissement
  - Equipements dédiés...
- Sécurisation fonctionnelle
- Références
- Réagir à un incident
- Facteurs-clés de succès et bonnes pratiques
- Intégration avec la sûreté industrielle
- Stratégie de sécurisation des réseaux industriels
- Focus sur le "patch management"
- Sécurité organisationnelle du réseau industriel

Architecture SCADA

- Détermination des zones et conduites
- Points sensibles
- Sécurisation d'architecture

Détermination des niveaux de classification ANSSI

- Analyse basée sur le guide ANSSI relatif aux réseaux industriels

Normes

- Les normes de sécurité des SI de gestion (type ISO 2700x)
- Panorama des normes et guides de sécurité industrielle
- Zoom sur l'IEC 62443
- Guide ANSSI
  - Maîtriser la SSI pour les systèmes industriels
  - Méthode de classification et mesures

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)