Présentiel/distanciel

TOP FORMATION

Cybersécurité des systèmes industriels

Objectifs pédagogiques

- Identifier et décrire les applications et spécificités des systèmes industriels
- Décrire les architectures de référence ISA-IEC 62443 et ANSSI
- Définir le processus analyse des risques et mettre en place une gestion de risques
- Identifier les vulnérabilités sur les différentes couches d'une architecture industrielle
- Décrire les principes et les applications de défense en profondeur

Prérequis

- Utiliser et réinvestir des connaissance générale en informatique et en sécurité des systèmes d'information
- Expliquer le protocole TCP/IP et mettre en oeuvre des notions sur les architectures de sécurité
- Mettre en oeuvre des notions sur les protocoles réseaux filaires et sans fil
- Aucune connaissance préalable sur les systèmes industriels n'est indispensable.

Public concerné

- Cette formation s'adresse aux responsables sécurité, sureté, cybersécurité, sécurité industrielle, aux différents responsables souhaitant étendre leurs compétences aux systèmes industriels et aux consultants et auditeurs en sécurité.
- Le public visé peut se répartir en deux profils :
- Le profil « automaticien » : personne ayant un bagage technique dans le domaine de l'automatisme et des systèmes industriels ;
- Le profil « informaticien » : personne ayant un bagage technique dans le domaine informatique et tout particulièrement la sécurité des systèmes d'information (SSI).

Programme détaillé

Introduction aux domaines industriels, architectures et applications associées (7 heures)

- IoT, objets connectés, smart city, industrie 4.0, ...
- Composants d'un système industriel (PLC, capteurs, actionneurs, RTU, IED, ...)
- Les serveurs et applications (SCADA, MES, BMS, EMS, PCS, Historian, ...)
- Les protocoles industriels (Modbus, DNP3, PI, EtherNet/IP, OPC UA, ...)
- Les 4 niveaux du modèle CIM (Computer Integrated Manufacturing)
- Le modèle ISA99

Présentation et démonstration des vecteurs d'attaques (10 heures)

- Protocoles liés aux réseaux sans-fil (Wifi, Bluetooth, 802.15.4, Zigbee, ...)
- Protocoles industriels (Modbus, OPC, CIP, ...)
- Applications industrielles (MES, SCADA, Développement, ...)
- Interconnexions avec des réseaux de sensibilité différentes (gestion, Internet, partenaires, intégrateurs, ...)
- Exposition d'IHM sur Internet
- Média amovible USB/DVD
- Equipements de terrain (API/PLC, sondes, capteurs, ...)

Mesures de sécurité (11 heures)

- Solutions techniques de filtrage, de cloisonnement et de détection d'intrusion
  - Firewall industriel
  - Diode et passerelle unidirectionnelle industrielle
  - Chiffrement IPSEC/SSL
  - Sondes de détection d'intrusion
  - Analyse passive de trafic
  - Honeypot
- Solutions techniques de durcissement système
  - Automates de nouvelle génération certifiés CSPN (Siemens S7_1500 et Schneider M580)
  - Commutateurs Ethernet (bureautique et industriel)
  - Systèmes d'exploitation Windows et Linux
  - Applications
  - Automates programmables
- Guides ANSSI et référentiels de sécurité pour le domaine industriel (LPM, NIST, ISA/IEC, NERC, ISO 27000 ...)

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes, le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

Patrice ROY Certifié CISSP (Certified Information Systems Security Professional) et GICSP (Global Industrial Cyber Security Professional). Il possède une expérience de plus de 10 ans dans la sécurisation des architectures chez différents opérateurs de service Internet.
Après 6 ans chez Thales Communications & Security où il a travaillé dans une cellule d'expertise Sécurité au sein du Pôle Network & Endpoint Security, il a contribué à des projets de R&D liés à la sécurisation des protocoles de routage, ainsi qu'à la réalisation de tests d'intrusion et différents types d'audits chez les OIVs (opérateurs d'importance vitale) et au sein de programmes de Défense.
Actuellement, Patrice est leader technique en tant qu'Analyste N3 chez IBM Security au sein du SOC France X-Force. Il est également spécialisé dans la cybersécurité des Systèmes Industriels, et dispense à ce titre la formation associée ENI. Depuis mars 2017, il est Officier de cyber-réserve opérationnelle spécialité cyberdéfense ; il a ainsi participé au cyberexercice LockShield » organisé par l'OTAN en 2017 et 2018, et au « DefNet »

ENI Service

référence
T130-079

28h

Cybersécurité des systèmes industriels

Mise à jour
20 mars 2026

2690 € HT

Présentiel/distanciel

TOP FORMATION

Accessibilité de la formation

ENI Service s'engage en faveur de l'accessibilité pour les personnes en situation de handicap (PSH). Toutes nos formations sont ainsi accessibles aux PSH. Pour en savoir plus, nous vous invitons à consulter la page "Accueil des personnes en situation de handicap" de notre site internet.