



Formation Sécurité des systèmes industriels

Durée : 7 heures
organisations option solutions logicielles et applications métiers (SIO SLAM)

Certification : BTS services informatiques aux

Prix : 1650

Référence : 2102106

Catégorie	Gestion de production, industrie
Sous-catégorie	Industrie 4.0
Pour qui ?	Toutes les personnes souhaitant apprendre les fondamentaux de la sécurité des SI.
Prérequis	Avoir suivi la formation "La sécurité dans le cyberspace".
Objectifs pédagogiques	<p>Appréhender les composants d'un système SCADA</p> <p>Analyser les risques d'une architecture SCADA</p> <p>Comprendre les menaces et les vulnérabilités de ces systèmes</p> <p>Identifier les mesures de protection</p>
Contenu de la formation	<p>Introduction aux systèmes de supervision et de contrôle industriel (SCADA)</p> <p>Panorama de la cybersécurité industrielle. Pourquoi un pirate informatique cible de plus en plus les systèmes SCADA ?</p> <p>Les menaces susceptibles d'affecter les systèmes industriels et les infrastructures informatiques de l'industrie.</p> <p>Quels sont les référentiels sur la sécurité des systèmes d'information industriels ?</p>

	<p>Qu'est-ce que l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ? Quel est son rôle ?</p> <p>Secteurs d'activité cible, typologie, population cible dans l'industrie française.</p> <p>Les types d'architectures de système SCADA.</p> <p>Composants et architectures réseaux des systèmes SCADA</p> <p>Les composants hardware et software : quelles sont les architectures et les fonctionnalités dans un système SCADA ?</p> <p>Que sont les automates programmables industriels (PLC) ? Les terminaux distants (RTU).</p> <p>Quels sont les différents flux de communication dans les systèmes SCADA ? Sont-ils sécurisés par défaut ?</p> <p>Les protocoles de communication temps réel, PLC (contrôleurs logiques programmables).</p> <p>Introduction à la sécurité des systèmes SCADA</p> <p>La problématique de sécurité dans les systèmes SCADA. Les méthodes de classification.</p> <p>Les menaces et vulnérabilités, les intrusions connues, les attaques APT (menaces persistantes avancées).</p> <p>Les cyberattaques ciblées sur les systèmes et infrastructures informatiques industriels.</p> <p>Les scénarios d'attaques réelles sur les systèmes SCADA : STUXNET, FLAME.</p> <p>L'analyse des attaques : construction de l'arbre d'attaque de STUXNET.</p> <p>Les techniques d'authentification et les méthodes de chiffrement. Leurs apports, leur mise en place.</p> <p>Protéger l'ensemble de la chaîne industrielle et les postes opérationnels.</p> <p>Bien sécuriser les accès et les postes à distance et garantir la disponibilité du réseau.</p>
<p>Suite de parcours possible</p>	
<p>Éligible au CPF</p>	

FINANCEMENTS

OPCO
OPCA
FAF
Pôle Emploi
La Région



CONTACTS



IFFP - Tour Belvédère SPACES
1 Cours Valmy 92 800 Puteaux



01 80 88 44 55



administration@iffp.pro