

SCADA : Sécurité des infrastructures informatiques industrielles (certification comprise)

Référence : SCADA

Durée : 5 jours

Certification : Lead SCADA Security Manager

CONNAISSANCES PREALABLES

- Une compréhension fondamentale de la sécurité des SCADA.

PROFIL DES STAGIAIRES

- Développeurs SCADA. • Ingénieurs et utilisateurs de SCADA. • Professionnels de la sécurité. • Professionnels des TI. • Professionnels des TI des SCADA. • Responsables des TI et du risque.

OBJECTIFS

- Comprendre et expliquer l'objet et les risques que l'on associe à un SCADA, un système numérique de contrôle-commande ou des automates programmables industriels. • Comprendre les risques qui menacent de tels environnements et les approches qui conviennent pour gérer de tels risques. • Acquérir les savoir-faire nécessaires pour soutenir un programme de sécurité proactive pour les SCADA lequel comprend des politiques ainsi qu'une gestion des vulnérabilités. • Définir et concevoir une architecture réseau dont la défense est incorporée aux mesures de contrôle de la sécurité avancées visant les SCADA. • Expliquer la relation entre les mesures de contrôle de la direction, opérationnelles et techniques dans un programme de sécurité SCADA. • Améliorer la capacité à concevoir des systèmes SCADA résilients offrant une disponibilité élevée. • Apprendre à gérer un programme offrant des activités efficaces de mise à l'essai de la sécurité.

CERTIFICATION PREPAREE

Certified Lead SCADA Security Manager

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Automates PLC / Télétransmetteurs RTU / Automates de sécurité SIS

- Objectifs et structure du cours
- Principes et notions fondamentaux des SCADA et de la sécurité SCADA
- État de l'art de la sécurité SCADA
- Les architectures SCADA
- Services couramment présents
- Vulnérabilités rencontrées

- Protocoles courants
- Déni de service / robustesse des automates

IHM (Interfaces Homme-Machine) / Système d'exploitation Windows

- Vulnérabilités rencontrées
- Top 10 OWASP
- Windows dans les environnements SCADA
- Vulnérabilités courantes

Les vulnérabilités des protocoles

- S7
- Modbus
- ICCP/TASE

Les systèmes SCADA distants

- VPN
- Boitiers de télétransmission
- Sans fil (Wi-Fi, liaisons radio)
- Problèmes des automates et IHM exposés sur Internet (exemples avec shodan)
- Conclusion de la formation

Examen final

- L'examen couvre les domaines de compétences suivants :
- Domaine 1 : Notions et principes fondamentaux des SCADA et de la sécurité SCADA
- Domaine 2 : Organisation dans les milieux industriels
- Domaine 3 : L'architecture SCADA
- Domaine 4 : Les vulnérabilités du WEB
- Domaine 5 : Les protocoles vulnérables