AJC FORMATION

CYCLE

20 jours – 140 heures

CYBERSECURITE DEFENSIVE

Filière

AJC FORMATION – 6 rue Rougemont 75009 - 01 81 51 64 85 –formonsnous@ajc-formation.fr
S.A.R.L. au capital de 10 000 € - SIRET : 50096702100030
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)

www.ajc-formation.fr
www.ajc-classroom.fr

PROGRAMME DE LA FILIERE

AJC FORMATION – 6 rue Rougemont 75009 - 01 81 51 64 85 –formonsnous@ajc-formation.fr
S.A.R.L. au capital de 10 000 € - SIRET : 50096702100030
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)

www.ajc-formation.fr
www.ajc-classroom.fr

FILIERE CYBER DEFENSIVE

Programme

OBJECTIFS

- Maîtriser les fondamentaux de la cybersécurité défensive en environnement industriel
- Se familiariser aux attaques pour mieux les contrer et identifier les vulnérabilités pour les exploiter
- Etre capable de protéger son architecture et ses applications et s'initier au système de sécurité SCADA
- Savoir paramétrer et utiliser un SOC/SIEM pour surveiller et manager les niveaux d'alerte, menaces, incidents et mettre en place des mesures correctives

METHODES ET MOYENS PEDAGOGIQUES

Méthodes pédagogiques. Pour l'ensemble des stagiaires, le cours intégrera les suivantes :

- Alternance d'exercices, cas pratiques, QCM et de notions théoriques
- Evaluations

Moyens pédagogiques

- AJC met à la disposition de chaque stagiaire un accès à notre plateforme à distance ainsi qu'éventuellement les logiciels utiles dans le cadre de chaque module
- Les supports de cours seront remis via notre la plate-forme de téléchargement Quest et/ou AJC Classroom

PRE-REQUIS

- Une formation ou une première expérience en système et réseaux serait un plus

PARTICIPANTS

- Toute personne cherchant à acquérir toutes les compétences nécessaires pour devenir un spécialiste SOC / SIEM

LIEU

Distanciel

CERTIFICATION / ATTESTATION

Attestation de formation

Programme - Contenu pédagogique

INTEGRATION	LES FONDAMENTAUX DE LA CYBERSECURITE EN ENVIRONNEMENT INDUSTRIEL	1 jour
COMPRENDRE LES ATTAQUES POUR MIEUX LES CONTRER	LES DIFFERENTES TYPOLOGIES D'ATTAQUES	1 jour
	SCRIPTING (PYTHON, SHELL)	2 jours
	DECOUVERTE ET EXPLOITATION D'UNE VULNERABILITE	1 jour
SECURISATION DE L' ARCHITECTURE ET DES APPLICATIONS	SECURISATION SYSTÈME (LINUX, WINDOWS, AD...)	1 jour
	SECURISATION RESEAU (FIREWALL, WAF, IPS, IDS...)	1 jour
	SCADA, LES ARCHITECTURES ET LEUR VULNERABILITE	3 jours
SURVEILLANCE ET MANAGEMENT DE LA SECURITE	MISE EN PLACE D'UN SOC/SIEM	10 jours

PROGRAMMES DÉTAILLÉS

INTEGRATION

CYBER DEFENSIVE

FONDAMENTAUX DE LA CYBERSECURITE EN ENVIRONNEMENT INDUSTRIEL

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Définitions et concepts clés
- Les enjeux
- Attaques classiques et exemples d'incidents
- Les bonnes pratiques
- Les produits de sécurité
- Les normes et standards
- La labellisation de sécurité
- Introduction à la crypto
- Introduction aux systèmes industriels
- Définitions et concepts clés
- Les composants d'un système industriel
- Les langages de programmation
- Les protocoles et bus de terrain
- Les architectures
- Le panorama des normes et standards
- Introduction à la sûreté de fonctionnement

La cybersécurité pour les systèmes industriels

- Les enjeux
- Etat des lieux, contraintes, mythes et légendes
- Les incidents, les attaquants, les motivations
- Les vulnérabilités et vecteurs d'attaques régulièrement rencontrés
- Les bonnes pratiques et les recommandations (organisationnelles et techniques)
- La gouvernance de la cybersécurité des systèmes industriels
- La réglementation (notamment LPM et NIS)

OBJECTIFS

- Comprendre les enjeux de la cybersécurité des systèmes industriels
- Identifier les particularités de ce domaine
- Acquérir les fondamentaux de la cybersécurité des systèmes industriels

PROGRAMME DETAILLE

COMPRENDRE LES ATTAQUESPOUR MIEUX LES CONTRER

AJC FORMATION

CYBER DEFENSIVE

LES DIFFERENTES TYPOLOGIES D'ATTAQUES

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

Les différentes attaques

- Attaque informatique par déni de service distribué (DDoS)
- Chevaux de Troie(Trojan)
- Logiciels espions (Spyware)
- Détournement de domaine
- Man in the middle
- Hameçonnage (*Phishing*)
- Virus
- Logiciel malveillant (Malware)
- Piratage
- Cryptovirus et Cryptolocker
- Vers informatiques (Computer Worm)
- Vol d'appareils portatifs ou mobiles (Theft)

Vulnérabilités Réseaux

- Différents types de scan
- Firewalking
- Analyse des transmissions chiffrées
- Sniffing réseau
- Spoofing réseau
- Détournement de sessions TCP

Vulnérabilités WEB

- Cross Site Scripting (XSS)
- Injection de code
- Inclusion de fichier
- Accès à une référence interne
- Cross Site Request Forgery (CSRF)
- Divulgation d'information
- Vol de session
- Sécurité du stockage
- Sécurité des échanges
- Restriction d'URL

Dans le détail

- Les méthodes d'attaque et de propagation
- Les cibles
- Les conséquences immédiates et à venir
- La détection
- Les actions préventives et curatives

OBJECTIFS

- Identifier les différentes attaques
- En fonction de la cible imaginer les attaques possibles

Détecter les attaques visibles et dormantes

- Prévenir plutôt que guérir

PROGRAMME DETAILLE

AJC FORMATION

CYBER DEFENSIVE

SCRIPTING (PYTHON, SHELL)

2 jours,
14 heures

DISTANCIEL

PROGRAMME DU MODULE

Syntaxe du langage Python

- Les Identifiants et les références. Les Conventions de codage et les règles de nommage.
- Les blocs, les commentaires.
- Les types de données disponibles.
- Les variables, l'affichage formaté, la portée locale et globale.
- La manipulation des types numériques, la manipulation de chaînes de caractères.
- La manipulation des tableaux dynamiques (liste), des tableaux statiques (tuple) et des dictionnaires.
- L'utilisation des fichiers.
- La structure conditionnelle if / elif / else.
- Les opérateurs logiques et les opérateurs de comparaison.
- Les boucles d'itérations while et for. Interruption d'itérations break / continue.
- La fonction range.
- L'écriture et la documentation de fonctions.
- Les Lambda expression.
- Les générateurs.
- La structuration du code en modules.

Approche Orientée Objet

- Les principes du paradigme Objet.
- La définition d'un objet (état, comportement, identité).
- La notion de classe, d'attributs et de méthodes.
- L'encapsulation des données.
- La communication entre les objets.
- L'héritage, transmission des caractéristiques d'une classe.
- La notion de polymorphisme.
- Association entre classes.
- Les interfaces.
- Présentation d'UML.
- Les diagrammes de classes, de séquences, d'activités, ...
- Notion de modèle de conception (design pattern).

Programmation Objet en Python

- Les particularités du modèle objet de Python.
- L'écriture de classes et leur instanciation.
- Les constructeurs et les destructeurs.
- La protection d'accès des attributs et des méthodes.
- La nécessité du paramètre self.
- L'héritage simple, l'héritage multiple, le polymorphisme.
- Les notions de visibilités.
- Les méthodes spéciales.
- L'introspection.
- L'implémentation des interfaces.
- Les bonnes pratiques et les modèles de conception courants.
- L'utilisation du mécanisme d'exception pour la gestion des erreurs.

OBJECTIFS

- Initier les participants aux méthodes et réflexes de la programmation orientée objet et leur apporter la maîtrise opérationnelle du langage Python.

PROGRAMME DETAILLE

AJC FORMATION

CYBER DEFENSIVE

DECOUVERTE ET EXPLOITATION D'UNE VULNERABILITE

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

Les menaces et les risques

- Qu'est-ce la sécurité informatique ?
- Comment une négligence peut-elle créer une catastrophe ?
- Les responsabilités de chacun.
- L'architecture d'un SI et leurs vulnérabilités potentielles.
- Les réseaux d'entreprise (locaux, distantes, Internet).
- Les réseaux sans fil et mobilité. Les applications à risques : Web, messagerie...
- La base de données et système de fichiers. Menaces et risques.
- La sociologie des pirates.

La sécurité du poste de travail

- La confidentialité, la signature et l'intégrité. Les contraintes liées au chiffrement.
- Les différents éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Les différentes menaces sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ?
- Les ports USB. Le rôle du firewall client.

Le processus d'authentification

- Les contrôles d'accès : l'authentification et l'autorisation.
- L'importance de l'authentification.
- Le mot de passe traditionnel.
- L'authentification par certificats et par token.
- La connexion à distance via Internet.
- Qu'est-ce qu'un VPN ?
- Pourquoi utiliser une authentification renforcée.

Prise d'information

- Sources ouvertes
- Active

Scanning

- Scan de ports
- Scan de vulnérabilités

Les outils d'attaque

- Outils réseau
- Outils d'analyse système
- Outils d'analyse web
- Frameworks d'exploitation
- Outils de maintien d'accès

OBJECTIFS

- Comprendre les risques et les menaces qui peuvent atteindre le SI et les conséquences possibles d'une attaque informatique
- Identifier les mesures de protection de l'information
- Apprendre les actions nécessaires à la sécurisation de son poste de travail

PROGRAMME DETAILLE

SECURISATION DE L'ARCHITECTURE ET DES APPLICATIONS

AJC FORMATION

CYBER DEFENSIVE

SECURISATION SYSTÈME (LINUX, WINDOWS, AD)

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

SYSTÈME LINUX

Mise en place des premières sécurisations

- Secure Boot
- Signatures MOK / EFI
- Grub
- Attaques DMA

Gestion des droits et des accès

- Le système d'authentification PAM
- SUDO
- Kernel capabilities
- SELinux / AppArmor

Sauvegardes

- Gestion des sauvegardes
- Sauvegardes complètes
- Sauvegardes bases de données

Système de fichiers

- Permissions
- ACL / Quotas
- Chiffrement
- ZFS/BTRFS
- Effacement sécurisé

ACTIVE DIRECTOY

Sécurisation des services de domaine Active Directory

- Sécuriser les contrôleurs de domaine
- Mettre en œuvre les stratégies de mots de passe et de verrouillage des comptes
- Audit des authentifications

SYSTÈME WINDOWS

Protection du BIOS/UEFI

Protection du système

- Mises à jour
- Journaux d'événements Windows
- La suite d'outils Sysinternals
- La base SAM et le stockage mots de passe
- Les méthodes d'authentification Windows
- Chiffrement du disque avec Bitlocker

Administration du Powershell

Protection des utilisateurs

- Gestion des droits
- SmartScreen
- Applocker
- Device Guard
- UAC

Déploiement d'un domaine sécurisé

- Stratégie de groupe essentielle
- Déploiement de la solution LAPS
- La technologie ATA
- Déploiement de certificat
- Tester la configuration de son infrastructure (BTA, BloodHound, etc.)
- Segmentation en silos

Protection de la mémoire sous Windows

- DEP, ASLR, Stack canary, SEHOP

Protection des services

- Déployer une autorité de certification
- Infrastructure à clé publique
- Durcissement des services (LDAP, SMB, SQL, Bureau à distance, DNS, IIS...)

OBJECTIFS

- Savoir exploiter les vulnérabilités applicatives sur des systèmes récents, en contournant les protections usuelles
- Être capable d'exploiter une vulnérabilité applicative sur les systèmes Linux et Windows
- Comprendre les failles pour sécuriser le SI et le poste de travail

PROGRAMME DETAILLE

CYBER DEFENSIVE

SECURISATION (FIREWALL, WAF, AD)

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

La sécurité des accès, Firewall, Firewall, Waf, Proxy, Nac

- L'accès des stations aux réseaux d'entreprise,802.1X, NAC
- Les différents types de firewalls
- Les règles de filtrage
- Les règles de la translation d'adresse (NAT)
- La mise en œuvre d'une zone démilitarisée (DMZ)
- La détection et surveillance avec les iDS
- L'intégration d'un firewall dans le réseau d'entreprise
- La gestion et l'analyse des fichiers log

La sécurité des systèmes d'exploitation

- Le Hardening de Windows
- Le Hardening d'Unix/Linux
- Le Hardening des nomades : IOS / Android

La sécurité des applications avec exemple d'architectures

- Les serveurs et clients Web
- La messagerie électronique
- La VoIP IPbx et téléphones

La sécurité des échanges, la cryptographie

- Le cryptage et les fonctions de base
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les algorithmes de hashing
- Les méthodes d'authentification (pap,chap,Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Les protocoles SSL IPSEC S/MIME
- Les VPN réseau privé virtuel site à site et nomade

OBJECTIFS

- Savoir exploiter les vulnérabilités applicatives sur des systèmes récents, en contournant les protections usuelles
- Être capable d'exploiter une vulnérabilité applicative sur les systèmes Linux et Windows
- Comprendre les failles pour sécuriser le SI et le poste de travail

PROGRAMME DETAILLE

AJC FORMATION

CYBER DEFENSIVE

SCADA, LES ARCHITECTURES ET LEURS VULNERABILITES

3 jours,
21 heures

DISTANCIEL

PROGRAMME DU MODULE

L'environnement SCADA

- La problématique de sécurité dans les systèmes SCADA.
- La cybersécurité des systèmes industriels, les méthodes de classification.
- Les composants des Systèmes de Contrôle Industriel (ICS)/SCADA.
- IHM (Interfaces Homme/Machine/Automate).
- Réseau : les automates via les navigateurs Web, Telnet, SSH, accès filaire TCP...)/sans-fil (WiFi, liaisons radio).
- Automate : contrôleur logique programmable (programmable Logic Controller, PLC).
- Les principaux protocoles utilisés par les architectures ICS/SCADA : DNP3, ModBus, IEC 60870, BACnet, LonWorks et EPICS.
- Appareils finaux

Vulnérabilités des architectures SCADA

- La recherche de vulnérabilités.
- Les mécanismes d'authentification, la gestion des accès distants.
- Les liaisons d'un système SCADA avec son environnement (connectivité) : réseau, capteur, automate et périphérique.
- Identifier et utiliser les applications et programmes hébergés sur un système SCADA.
- La méthodologie des tests d'intrusion.
- Les outils : framework de test d'intrusion, injecteur de code dans les automates, analyseurs de réseau, débogueurs.
- Les attaques physiques.
- Les intrusions connues, les attaques APT (menaces persistantes avancées).
- Les scénarios d'attaques réelles sur les systèmes SCADA : STUXNET, FLAME.
- Les vulnérabilités liées aux IHM.
- Les automates et IHM exposés sur Internet.
- Les failles des systèmes d'exploitation gérant les systèmes SCADA (serveurs et postes de travail).

OBJECTIFS

- Définir l'impact et la portée d'une vulnérabilité
- Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
- Mesurer le niveau de sécurité d'une architecture SCADA
- Réaliser un test de pénétration
- Identifier les mesures de protection

PROGRAMME DETAILLE

SURVEILLANCE ET MANAGEMENT DE LA SECURITE : LE SOC/SIEM

AJC FORMATION

CYBER DEFENSIVE

MISE EN PLACE D'UN SOC/SIEM

10 jours,
70 heures

DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Rôle de la détection d'intrusion
- Terminologie : faux-positifs, détection, prévention, etc.
- Architecture et types d'IDS
- Déploiement et configuration de base
- Langage d'écriture de règles
- Journalisation
- Les incidents de sécurité
- La gestion des risques
- Réagir à un incident de sécurité
- Principe d'un NSM
- Bonnes pratiques

Le SIEM

- Présentation
- Fonctionnement d'un SIEM
- Les différents SIEM (Splunk, Qradar...)
- Mise en œuvre
- Limites d'utilisation
- Défis modernes posés à la supervision classique
- Objectifs d'un SIEM
- Architecture et fonctionnalités
- Syslog et centralisation des journaux
- Synchronisation du temps (NTP)
- Configuration avancée

Les IDS

- Avantages des IDS
- Attaques et contournement d'un IDS
- Précautions à prendre
- Limites des IDS
- Intégration avec les autres composants du SI

Les agents IDS ET HIDS

- Panorama des agents
- Implémenter un agent sur Windows
- Implémenter un agent sur Linux
- Présentation
- Implémenter un IDS
- Paramétrage de base
- Configuration avancée

Travaux Pratiques

- Mise en place d'une architecture IDS virtualisée : firewall, cible, attaquant Jeu d'attaques et création de règles de détection (scans, bruteforce, exploitation de vulnérabilité)
- HIDS et architecture
- Déploiement et configuration de base Syntaxe d'écriture de règles
- Ecriture de règles
- Configuration d'agents
- Ecritures avancés
- Environnement hétérogène : Linux, Windows

OBJECTIFS

- Traiter des incidents et leur management
- Aborder les problématiques liées à la détection d'intrusion ainsi que leurs limites
- Mettre en place le SIEM avec implémentation de sondes et d'agents HIDS dans un réseau existant
- Mettre en place des points de contrôles et niveaux d'alerte
- Prendre les bonnes décisions suite à l'analyse des remontées d'informations et à leur corrélation.

AJC FORMATION

NOUS CONTACTER

AJC FORMATION
01 81 51 64 85
formonsnous@ajc-formation.fr
6 rue ROUGEMEONT
75009 PARIS

www.ajc-formation.fr
www.ajc-classroom.fr