AJC FORMATION

CYCLE

120 jours – 840 heures

IT CYBERSECURITY ENGINEER

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 IT CYBERSECURITY ENGINEER

Programme

OBJECTIFS

- Maîtriser les fondamentaux de la cyber sécurité défensive
- Se familiariser avec les attaques pour mieux les contrer
- Comprendre les vulnérabilités et leur exploitation
- Protéger son architecture. Détecter des menaces
- Déployer, paramétrer et utiliser les solutions défensives
- Investiguer, analyser les niveaux d'alerte et corrélation d'événements
- Réaliser une veille technologique pour adapter son infrastructure aux nouvelles menaces
- Acquérir le savoir être du consultant

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, Projet fil Rouge
- 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

Informations concernant les classes virtuelles

- Pour les formations en classe virtuelle, avec @JC CLASSROOM, vous profiterez des mêmes possibilités et interactions avec votre formateur que lors d'une formation présentielle : votre formation se déroulera en connexion continue 7h/7.
- Vous pourrez échanger directement avec le formateur et l'équipe pédagogique à travers notre système de visioconférence, mais aussi grâce aux forums et chats présents dans @JC CLASSROOM.
- Votre formateur sera à même de vérifier l'avancement de votre travail et de vous évaluer à l'aide d'exercices et de cas pratiques. Cela lui permettra de vous apporter un suivi pédagogique et des conseils personnalisés pendant toute la durée de la formation.
- Notre équipe technique vous enverra les modalités de connexion (accès, identifiants, dates, heures et numéro de la hotline) par mail dès votre inscription.
- Si vous rencontrez un problème de connexion, vous pourrez joindre à tout moment (avant ou même pendant la formation) notre hotline assistance technique au 01 82 83 72 41 ou par mail (hotline@ajc-formation.fr)

PRE-REQUIS

- Des notions systèmes seraient un plus

PARTICIPANTS

- Scientifique ou toute personne en reconversion métier

POSTES VISES

- Analyste Sécurité, Consultant sécurité - SOC/SIEM, Incident Response Specialist, Ingénieur Cyberdéfense Reverse-engineering …

LIEU

- Présentiel et/ou Distanciel

CERTIFICATION / ATTESTATION

- Attestation de formation
- Certification Splunk Core Certified Power User

Programme - Contenu pédagogique

COMPORTEMENTAL	RÔLE ET COMPORTEMENT DU CONSULTANT OBJECTIF « QUALITÉ » DE LA MISSION	2 jours
	TRAVAIL EN ÉQUIPE	1 jour
FONDAMENTAUX	FONDAMENTAUX RESEAUX	2 jours
	WINDOWS ACTIVE DIRECTORY	4 jours
	WINDOWS SERVICES RESEAUX	3 jours
	POWERSHELL	2 jours
PROJET	PROJET WINDOWS	1 jour
FONDAMENTAUX	LIGNE DE COMMANDES SHELL	3 jours
	ADMINISTRATION LINUX	5 jours
PROJET	PROJET LINUX	2 jours
INTÉGRATION	LES FONDAMENTAUX DE LA SÉCURITÉ DÉFENSIVE	2 jours
COMPRENDRE LES ATTAQUES POUR MIEUX LES CONTRER	EXEMPLES D'ARCHITECTURES	2 jours
	DÉFINITION D'UNE VULNÉRABILITÉ	2 jours
	LES DIFFÉRENTS ACCÈS À RISQUES (EXTERNE, WEB, INTERNES, MOBILES …….)	2 jours
	LES DIFFÉRENTES TYPOLOGIES D'ATTAQUES	2 jours
	LES OUTILS OFFENSIFS DE DÉTECTION DES VULNÉRABILITÉS	2 jours
	EXPLOITATION D'UNE VULNÉRABILITÉ	2 jours
	LES OUTILS DÉFENSIFS DE DÉTECTION DES ATTAQUES ET COMPROMISSIONS	2 jours
	VULNERABILITY SCORING & RISK SCORING (CVSS, CVE …..)	2 jours
PROJET	PROJET ATTAQUES	2 jours

Programme - Contenu pédagogique

SECURISATION DE L'ARCHITECTURE ET DES APPLICATIONS	SÉCURISATION SYSTÈME (LINUX, WINDOWS, AD ….)	3 jours
	SÉCURISATION RÉSEAU (FIREWALL, IPS, IDS…..)	3 jours
	CHIFFREMENT	4 jours
	DEVOPS ET OUTILS	4 jours
	DÉVELOPPEMENT SÉCURISÉ (DEVSECOPS)	2 jours
	SÉCURITÉ VPN, SANS-FIL ET MOBILITÉ	2 jours
	SENSIBILISATION À LA SÉCURITÉ DES APPAREILS ANDROID ET IOS	2 jours
	LES PROTOCOLES (SSH, SSL……)	2 jours
	SECURITE CLOUD	3 jours
PROJET	PROJET SÉCURISATION	4 jours
SURVEILLANCE ET MANAGEMENT DE LA SECURITE : LE SOC/SIEM	QU'EST CE QU'UN SOC/SIEM	2 jours
	MISE EN PLACE D'UN SOC / SIEM	2 jours
	LES DIFFÉRENTS SOC ET SIEM	1 jour
	SPLUNK	4 jours
	LES POINTS DE CONTRÔLE ET NIVEAUX D'ALERTE	2 jours
	DÉTECTION DES MENACES (CORRÉLATION D'ÉVÈNEMENTS)	3 jours
	INVESTIGATION SUR LES INCIDENTS (ANALYSE DES LOGS…..)	3 jours
	SUIVI ET SUPPORT À LA REMÉDIATION	2 jours
	MISE EN PLACE DE MESURES CORRECTIVES (PATCH MANAGEMENT …)	2 jours
PROJET	PROJET SURVEILLANCE	3 jours

Programme - Contenu pédagogique

LES NOUVELLES MENACES APT	VEILLE TECHNOLOGIQUE SUR LES NOUVELLES MENACES	2 jours
	MISE EN PLACE DES MESURES PRÉDICTIVES	2 jours
	NORMES DE SÉCURITÉ ET GESTION DES RISQUES	3 jours
	LA PRODUCTION DES INDICATEURS	2 jours
COMPORTEMENTAL	PRÉSENTER SES NOUVELLES COMPÉTENCES	1 jour
	CONDUITE DE RÉUNION	1 jour
	GESTION DU TEMPS ET DES PRIORITÉS	1 jour
PROJET	PROJET FINAL & SOUTENANCE – IT CYBERSECURITY ENGINEER	10 jours

PROGRAMMES DÉTAILLÉS

COMPORTEMENTAL

AJC FORMATION

IT CYBERSECURITY ENGINEER

ROLE ET COMPORTEMENT DU CONSULTANT

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Pourquoi s'intéresser aux comportements en tant que consultant ?

- Qu'est-ce qu'un comportement ? Qu'est-ce qu'un rôle ?
- En quoi les comportements peuvent faire la différence ?
- Pourquoi choisit-on d'adopter un comportement ? Le processus d'apprentissage d'un « savoir-être »

Adopter la meilleure stratégie de coopération pour mieux travailler en équipe

- Comment agir pour développer des relations positives et durables ?
- La théorie CRP

Savoir communiquer et éviter les malentendus

- Pourquoi la communication passe-t-elle mal : les filtres, le cadre de référence ?
- Savoir utiliser l'écoute active : questionnement ouvert et reformulation
- Savoir convaincre : comment influencer positivement les échanges

Comment faire évoluer ses comportements

- Qu'est-ce qui conditionne nos comportements ?
- Sur quel levier agir pour ajouter des « cordes à son arc »

Comprendre sa personnalité et mieux cerner celle des autres

- Savoir se situer et comprendre en quoi notre personnalité se traduit à travers nos comportements
- Situer les autres et comprendre leur mode de fonctionnement pour mieux coopérer

Développer son intelligence émotionnelle pour modifier ses comportements

- Qu'est-ce que l'intelligence émotionnelle ?
- En quoi notre QE est-il déterminant par rapport à nos comportements
- Apprendre à gérer son stress pour éviter les comportements inadaptés
  - Le stress : de quoi parle-t-on ?
  - Comment prévenir le stress et le gérer ?

Appréhender le rôle des croyances et de l'éducation dans nos comportements

- Qu'est-ce qu'une croyance ?
- Pourquoi conditionnent-elles nos comportements ?

L'assertivité et l'empathie pour mieux travailler en équipe

- Qu'est-ce que l'assertivité ? Qu'est-ce que l'empathie ?
- La notion de respects des besoins et de gagnant-gagnant
- Savoir recadrer un comportement qui ne nous convient pas et renouer avec des relations positives

Savoir rédiger des documents de synthèse et réaliser des présentations harmonieuses

OBJECTIFS

- Savoir communiquer à l'oral et à l'écrit à destination de l' interne et l'externe
- Adapter et maîtriser les différents types de communication pour accroître son efficacité personnelle

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

LE TRAVAIL EN EQUIPE

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Le travail en équipe

- Définition
- La dynamique de groupe
- La structuration de l'équipe de travail
- La taille de l'équipe
- Les facteurs d'influence
- Les comportements
- Les styles de leadership
- Les points clés de réussite du travail en équipe.

La dynamique de groupe

- Les facteurs de cohésion et de dissociation
- La vie affective du groupe et son évolution dans le temps

La structuration de l'équipe

- Sa mission
- Ses objectifs
- Les ressources et les moyens
- L'information et le suivi d'activité

Les facteurs d'influence

- Les facteurs de démoralisation
- Les facteurs de cohésion

Les comportements

- Individuels et de groupe

Les points clés de réussite du travail en équipe

- Savoir écouter et s'exprimer
- Savoir accepter le consensus
- Savoir négocier
- Respecter les autres
- Savoir mettre en œuvre une méthode de travail qui vise à atteindre les objectifs fixés

OBJECTIFS

- Comprendre la dynamique d'une équipe
- Susciter la participation et l'engagement
- Utiliser les techniques et les outils appropriés pour agir en équipe
- S'organiser au sein d'une équipe
- Communiquer efficacement quel que soit son rôle

PROGRAMME DETAILLE

FONDAMENTAUX

AJC FORMATION

IT CYBERSECURITY ENGINEER

FONDAMENTAUX RESEAUX

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Maintenance de la qualité de service
- Classification des réseaux: LAN, WAN
- Paquet
- Circuit
- Câblé
- Sans fil
- Standardisation des communications de données

Couche OSI/ISO

Développement de réseaux avec les liaisons de données

Information d'encodage

- Bits, octets et paquets
- Avantages de l'encodage numérique

Amélioration de l'efficacité avec le contrôle d'erreurs

- Acheminement de paquets dans les trames
- Détection et correction des erreurs
- Utilisation d'ACK et correction d'erreur par retransmission

Déploiement de médias physiques

Identification des types de médias

- Sélection des types de câbles de cuivre (Cat. 5e ou plus)
- Avantages par rapport à la fibre optique

Utilisation de liaisons sans fil

- Utilisation des bandes et fréquences radio
- Gestion des interférences et bruits

Miser sur Ethernet

Etude des standards IEEE 802

- Transfert avec des adresses MAC
- 1 Mo/s à 100 Go/s
- Comparaison entre LAN commuté et partagé

Étude détaillée d'Ethernet

- Étude de la commutation Ethernet
- Ajout de QoS à Ethernet
- Commutation de couche 2 et de couche 3

Exploiter le Wi-Fi pour permettre la mobilité

Communication via les ondes radio

- Types de réseaux Wi-Fi: a, b, g et n
- Miser sur le mode infrastructure et la mobilité

Intégration du Wi-Fi

- Vérification de la transmission
- Augmenter le débit et la portée avec 802.11n
- Fournir une QoS pour la voix et le multimédia

Déploiement des points d'accès

- Transfert du trafic via les points d'accès
- Points d'accès bi-bande
- Utilisation de SSID (Service Set Identifiers)

OBJECTIFS

- Appliquer les concepts, la terminologie et les solutions réseaux
- Mettre en œuvre des réseaux grâce aux liaisons de données et aux médias physiques
- Déployer des réseaux locaux (LAN) Ethernet et Wi-Fi
- Construire des réseaux et intranets fiables reposant sur les concepts TCP/IP
- Évaluer les technologies réseaux de pointe

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

FONDAMENTAUX RESEAUX (Suite)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Créer des sous-réseaux avec TCP/IP et des routeurs

TCP/IP: Une suite de protocoles

- Utiliser TCP pour les données, UDP pour la voix et la vidéo
- Maximisation des applications et équipements TCP/IP
- Optimisation du trafic VoIP et de données

Diagrammes de données et adressage IP

- Augmentation de l'efficacité avec des schémas d'adressage
- Interprétation des masques sous-réseaux et préfixes réseaux

Mode opératoire des routeurs

- Relais du trafic avec les tables de routage
- Découverte de chemins avec les protocoles de routage
- Migration des routeurs pour la QoS

Mise en œuvre de la sécurité

VPN (réseau privé virtuel)

- Authentification des utilisateurs
- Tunnels chiffrés VPN
- Vérifier l'intégrité et la source des informations

Évaluation des risques et contre-mesures

- Analyse des menaces et besoins en sécurité
- Chiffrement des données
- Tunnels L2 et L3
- Utilisation de certificats et signatures numériques

Sécurité LAN

- Sécurité Wi-Fi: WPA, WPA2, 802.11i, AES
- Isolation des groupes de travail avec les VLAN

Création de réseaux d'entreprise

Utilisation des liaisons Télécoms

- Flux de données en circuits commutés
- Lignes louées E1 et T1

Communication intersites

- Choix des options xDSL
- LAN Extension Services (LES) et Metro-Ethernet

Sélection de services réseau évolutifs

- MPLS (Multi Protocol Label Switching)
- Frame Relay
- Services ISP améliorés et Informatique et services en nuage

OBJECTIFS

- Appliquer les concepts, la terminologie et les solutions réseaux
- Mettre en œuvre des réseaux grâce aux liaisons de données et aux médias physiques
- Déployer des réseaux locaux (LAN) Ethernet et Wi-Fi
- Construire des réseaux et intranets fiables reposant sur les concepts TCP/IP
- Évaluer les technologies réseaux de pointe

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

WINDOWS ACTIVE DIRECTORY

4 jours,
28 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

L'architecture de l'Active Directory

- Les rôles et services d'Active Directory.
- Les nouveautés des services de domaine AD 2016.
- Les services de l'AD et l'orientation Cloud.

L'installation de l'Active Directory

- Le déploiement de l'annuaire.
- Le système DNS et l'Active Directory.
- Les zones DNS intégrées et sécurisées.
- Les enregistrements DNS liés à l'AD.

Le déploiement de contrôleur de domaine

- Le déploiement à distance et en PowerShell.
- Le clonage de contrôleur de domaine.
- L'implémentation de domaine enfant.
- Le déploiement de DC en lecture seule (RODC).

La gestion des objets

- Les interfaces de gestion.
- La gestion des objets en PowerShell.
- Les comptes de services administrés.
- La gestion des accès privilégiés (PAM).
- Les silos et stratégies d'authentifications.

Les stratégies de groupe

- Le principe de fonctionnement.
- Le magasin central. Le filtrage WMI.
- Les héritages, blocages et filtrages.

Le contrôle d'accès dynamique

- Vue d'ensemble du contrôle d'accès dynamique.
- Principes des revendications.
- Principes des règles, stratégies d'accès centralisés.
- Le gestionnaire de ressources FSRM, les autorisations.

Les sites, services et les relations d'approbations

- Les rôles d'un site AD.
- La gestion des sites, des réplications.
- Les relations d'approbations : vue d'ensemble et configuration.

La maintenance et le dépannage des services

- Sauvegarde et restauration des services.
- Procédures de maintenance d'une base AD.
- Dépannage des réplications.
- La gestion des rôles FSMO.

OBJECTIFS

- Installer et paramétrer un Active Directory sous Windows Server 2016
- Déployer des contrôleurs de domaine
- Réaliser des tâches d'administration courantes via les interfaces et PowerShell
- Déployer des GPO pour administrer les stations de travail et les serveurs
- Déployer le contrôle d'accès dynamique pour affiner les permissions aux ressources
- Sauvegarder et restaurer un Active Directory

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

WINDOWS SERVICES RESEAUX

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Implémenter les services IP v4

- Planification de l'adressage
- Gestion et dépannage de la connectivité IP

Mettre en œuvre le DHCP

- Gestion et dépannage du DHCP

Implémenter la résolution de noms DNS

Implémenter le service DNS

- Configuration des zones DNS
- Configurer l'intégration DNS avec AD DS
- Configurer les paramètres DNS avancés

Implémentation d'IP v6

- Présentation des spécificités de l'adressage IPv6
- Implémentation de la coexistence IPv4 et IPv6
- Gestion de la transition vers IPv6

Implémentation de l'accès distant

Implémentation d'un VPN

Implémentation d'un proxy

Mise en œuvre de la sécurité réseau

Implémentation et gestion réseau dans Hyper-V

OBJECTIFS

- Apprendre à configurer certaines des principales fonctionnalités tels que l'adressage IP, DNS et DHCP
- Savoir mettre en œuvre les technologies d'accès à distance tel que VPN
- Apprendre à mettre en place un Proxy et de la Sécurité

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

POWERSHELL

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction aux technologies de scripts Microsoft

- Composants principaux d'un script.
- Technologies actuelles.
- Interopérabilité des scripts.
- Scripts interprétés et scripts compilés.
- Outils complémentaires.

Les technologies objets

- Introduction à l'objet.
- Manipulation et exploration d'objets.
- Les différentes connexions.
- Classes, bibliothèques et autres objets.
- Composants Windows Script.

Mise en œuvre des objets de connexions

- Les composants ADSI.
- Principale manipulation des objets et des attributs.
- Active Directory.
- Les Composants WinNT.
- L'accès aux fichiers et bases de données.

Mise en œuvre des objets WSH

- Les moteurs d'exécution de l'environnement d'objets.
- Les objets WSH.
- Le contrôle d'applications et les ajouts d'évènements.

Mise en œuvre de Microsoft Windows Powershell

- Capacités de base de PowerShell.
- Installation et configuration de PowerShell.

Utilitaires en ligne de commandes et outils en mode graphique.

- Applets de commande.
- Interopérabilité WMI /PowerShell.
- Administration des tâches communes.
- Gestion des fichiers Texte et XML.
- Gestion des erreurs et gestion de l'aide.
- Conversion de scripts VBS en scripts PowerShell.

Gestion de la sécurité des scripts Powershell

- Introduction au modèle de sécurité.
- Sécuriser l'environnement Powershell.
- Signature des scripts et certificats.
- Précautions d'écriture de scripts : authentification.
- Scripting, sécurité et chiffrement.

Utilisation de Windows Powershell pour des tâches d'administration

- Gestion des processus locaux et des services.
- Collecte d'informations sur des ordinateurs.
- Utilisation et inventaire des installations logicielles.
- Tâches de gestion de réseau.
- Manipulation des fichiers et dossiers.
- Manipulation des clefs et des entrées de registre.

OBJECTIFS

- Savoir utiliser PowerShell en mode interactif
- Connaître les commandes de base de PowerShell pour un usage quotidien
- Comprendre comment exécuter une séquence de commandes au moyen d'un script simple
- Être à même d'utiliser les fonctionnalités de traitement en arrière-plan et d'administration à distance fournies par PowerShell
- Savoir automatiser l'administration de systèmes avec PowerShell

PROGRAMME DETAILLE

PROJET

IT CYBERSECURITY ENGINEER

PROJET WINDOWS

1 jour,

7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Déroulement du module

- Les stagiaires travaillent en toute autonomie, en binôme. Ils sont libres d'effectuer les choix adaptés, de développer les parties dont ils jugent avoir le plus besoin et d'apporter leurs propres solutions aux problèmes posés.
- Le formateur encadre les stagiaires par sa présence et répond aux questions. Il intervient pour épauler un binôme en difficulté ou pour faire le point à l'ensemble du groupe sur des notions non acquises. Il peut être amené à approfondir ou compléter certaines connaissances.

OBJECTIFS

- Mettre en application les acquis de la formation sur un projet Windows

PROGRAMME DETAILLE

FONDAMENTAUX

AJC FORMATION

IT CYBERSECURITY ENGINEER

LIGNE DE COMMANDES SHELL

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction à ligne de Commandes

- Présentation des shells
- Premières commandes
- Les différents Shell
- Comparaison de sh, bash, ksh et dash

Aide

- L'aide locale
- À savoir
- Freenode
- Usage IRC

Commandes de base

- Accéder au contenu des fichiers
- Commandes de compression, d'impression et de gestion du temps
- Gestion administration
- Commandes composites pipes et redirections

Variables

- Présentation
- Variables utilisateur
- Prompt
- Substitutions

Commandes internes

- Set
- cd, pushd, popd, umask, type, enable
- Historique et Alias
- Commande sur les processus : kill, jobs, wait, ulimit

Utilitaires

- Commandes cut, tr, uniq, sort, wc, find, grep
- Commandes de transformation : iconv, od, nl, basename, diff
- Commande utilitaires : xargs, tee, cmp, comm, paste, sed
- Expressions régulières

Introduction au Shell

- Rôle d'un Shell
- Présentation des différents shell sous Unix/Linux
- Types et syntaxes

Aide

- Les man
- Help
- IRC freenode

Paramétrage de l'environnement

- Options du Shell
- Variables et fichiers d'environnement
- Historique des commandes

Utilisation du Shell en mode interactif

- Énumérer les commandes essentiels par thème
- Substitution de nom de fichiers
- Protection des caractères spéciaux
- Redirections et Tubes de communication
- Regroupement des commandes

Base de la programmation

- Structure d'un script
- Commentaires
- Exécution d'un script
- Débogage d'un script et Code de retour

Variables et constantes

- Variables et Constantes
- Tableaux
- E/S de données
- Commandes de substitution
- Pushd et popd

OBJECTIFS

- Maitriser les commandes de base, l'utilisation poussée du bash, les grands utilitaires Unix dont les expressions régulières, sed et awk.
- Acquérir les compétences pour écrire des scripts en Shell et exploiter les possibilités des filtres Unix/Linux

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

LIGNE DE COMMANDES SHELL (Suite)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Structure de contrôle

- Instructions conditionnelles
- Choix multiples
- Boucles et Sauts inconditionnels

Alias et fonctions

- Alias
- Sous-programme sous forme de script
- Sous-programme sous forme de fonction

Arithmétiques

- Syntaxe
- Commande expr

Expressions régulières

- Meta-caractères des expressions régulières
- Utilisation des expressions régulières avec Grep

Chaine de caractères

- Manipulation de chaînes de caractères
- Expressions de variables
- Commandes basename et dirname

Filtre Sed

- Principe de fonctionnement
- Commandes de sed
- Utilisation des expressions régulières
- Présentation des sous-expressions

Processeur de texte AWK

- Principes de fonctionnement
- Structure d'un programme awk
- Critères
- Variables et les expressions
- Tableaux
- Instructions et Fonctions prédéfinies

OBJECTIFS

- Maitriser les commandes de base, l'utilisation poussée du bash, les grands utilitaires Unix dont les expressions régulières, sed et awk.
- Acquérir les compétences pour écrire des scripts en Shell et exploiter les possibilités des filtres Unix/Linux

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

ADMINISTRATION LINUX

5 jours,
35 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Gestion du stockage physique

Installation et configuration des composants logiciels et des services

Établissement de connexions réseau et d'accès par le pare-feu

Surveillance et gestion des processus

Gestion et sécurisation des fichiers

Gestion des utilisateurs et des groupes

Accès aux systèmes de fichiers Linux

Vérification des fichiers journaux et de l'historique

Sécurité

OBJECTIFS

- Acquérir les compétences essentielles en matière d'administration Linux, en se concentrant sur les tâches d'administration de base

PROGRAMME DETAILLE

PROJET

AJC FORMATION

IT CYBERSECURITY ENGINEER

PROJET LINUX

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Déroulement du module

- Les stagiaires travaillent en toute autonomie, en binôme. Ils sont libres d'effectuer les choix adaptés, de développer les parties dont ils jugent avoir le plus besoin et d'apporter leurs propres solutions aux problèmes posés.
- Le formateur encadre les stagiaires par sa présence et répond aux questions. Il intervient pour épauler un binôme en difficulté ou pour faire le point à l'ensemble du groupe sur des notions non acquises. Il peut être amené à approfondir ou compléter certaines connaissances.

OBJECTIFS

- Mettre en application les acquis de la formation sur un projet Linux

PROGRAMME DETAILLE

INTEGRATION

AJC FORMATION

IT CYBERSECURITY ENGINEER

LES FONDAMENTAUX DE LA SECURITE DEFENSIVE

2 jours,
14 heures

PRESENTIEL
et/ou
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
- labellisation de sécurité
- introduction à la crypto

Introduction aux systèmes

- définitions et concepts clés
- les composants d'un système industriel
- les langages de programmation
- Les protocoles et bus de terrain
- les architectures
- panorama des normes et standards
- Introduction à la sûreté de fonctionnement

La cybersécurité pour les systèmes

- les enjeux
- état 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
- Identifier les particularités de ce domaine
- Acquérir les fondamentaux de la cybersécurité des systèmes
- Travailler efficacement avec des experts en sécurité numérique et des experts de systèmes

PROGRAMME DETAILLE

COMPRENDRE LES ATTAQUES POUR MIEUX LES CONTRER

AJC FORMATION

IT CYBERSECURITY ENGINEER

EXEMPLES D'ARCHITECTURES

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Historique du marché, positionnement des acteurs.
- L'architecture technique aujourd'hui, rôles, enjeux.
- Qu'est-ce que l'urbanisation ? La cartographie de l'existant. Définir le SI cible.
- Qui sont les acteurs ? Quelle durée ? Quels sont les livrables ?
- Plan de convergence : virage culturel pour l'entreprise et la DSI.

Architectures Web : les fondamentaux

- Les technologies Web.
- TCP/IP, HTTP/HTTPS, HTML5, CSS3, JavaScript.
- Les fondamentaux. Les architectures : du serveur centralisé aux architectures n-tiers.
- Le client, les serveurs d'applications, le mode connecté et déconnecté.
- Les notions de contexte, transaction, middleware, composants, objets.
- Présentation de l'architecture .NET.et Java J2EE VS Open source.

Architectures orientées service (SOA)

- Qu'est-ce qu'un service ? Orchestration de services. Aspects transactionnels.
- Le couplage lâche et ses quatre dimensions.
- Sécurité, supervision et maintenance.
- Exemples d'applications.
- Les ESB (Enterprise Service Bus)
- Les Web Services. Concept et standards associés (SOAP, WSDL, WS-*).

Enterprise Content Management et Portail

- Le Web 2.0 et les nouvelles IHM. Définition, impact sur les applications.
- Les technologies Web 2.0 avec HTML5 et leurs retombées sur les applications Web.
- Les applications mobiles natives.
- Les enjeux de la gestion de contenu.
- Les offres : Sharepoint, Alfresco...
- Apports de la personnalisation.
- Gestion de la connaissance (Knowledge Management).
- Portail d'intégration : rassembler les sources de données et les diffuser à travers une interface unifiée.
- Problématiques techniques. Architecture technique.
- Le projet moteur de recherche.
- Les outils du marché : IBM WebSphere Portal, Oracle, MS SharePoint Server, Liferay.

OBJECTIFS

- Découvrir les différentes types d'architectures SI
- Comprendre les enjeux des évolutions majeures des architectures SI
- Evaluer le positionnement des principaux acteurs du marché
- Comprendre les fondamentaux de l'urbanisation SI
- Définir une stratégie d'évolution de l'architecture technique du SI

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

DEFINITION D'UNE VULNERABILITE

2 jours,
14 heures

PRESENTIEL
et/ou
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.

OBJECTIFS

- Comprendre les risques et les menaces qui peuvent atteindre le SI
- 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

AJC FORMATION

IT CYBERSECURITY ENGINEER

LES DIFFÉRENTS ACCÈS À RISQUES (EXTERNE, WEB, INTERNES, MOBILES ...)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Les vulnérabilités des applications Web

- Pourquoi les applications Web sont-elles plus exposées ?
- Les risques majeurs des applications Web selon l'OWASP (Top Ten 2017).
- Les attaques "Cross Site Scripting" ou XSS - Pourquoi sont-elles en pleine expansion ? Comment les éviter ?
- Les attaques en injection (Commandes injection, SQL Injection, LDAP injection...).
- Les attaques sur les sessions (cookie poisonning, session hijacking...).
- Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode...).
- Attaques sur les configurations standard (Default Password, Directory Transversal...).

Sécuriser un réseau WiFi

- Les algorithmes de chiffrement symétrique et asymétrique.
- Les fonctions de hachage.
- L'authentification et les certificats. Serveur Radius.
- Les problématiques de sécurité d'un réseau WiFi.
- Les protocoles WEP, TKIP, WPA et WPA2. Les normes.
- L'authentification 802.1x. EAP...

Sécurité des mobiles

- Présentation des risques selon l'OWASP (GoatDroid, IOS Project).
- Stockage de données métier, sessions, authentification (mémoire, SD, FS, keychain, etc.).
- Comprendre le Root Android, Jailbreaking.
- Protocoles d'échanges serveur.
- Impact des injections SQL et XSS dans les applications in-App, SMS.
- Solutions de Authentification, autorisation, émergence biométrie.
- Solutions de cryptographie (données, filesystem), backup restauration du terminal.
- Antivirus, antiphishing.

OBJECTIFS

- Identifier les vulnérabilités les plus courantes des applications Web
- Sécuriser un réseau WiFi
- Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS
- Identifier les services de sécurité des systèmes d'exploitation mobiles

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

LES DIFFÉRENTES TYPOLOGIES D'ATTAQUES

2 jours,
14 heures

PRESENTIEL
et/ou
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)

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

IT CYBERSECURITY ENGINEER

LES OUTILS OFFENSIFS DE DETECTION DES VULNERABILITES

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Rappel TCP/IP / Réseau Matériel
- Protos / OSI - Adressage IP
- Vocabulaire
- BDD de Vulnérabilités et Exploits
- Informations générales

Prise d'information

- Informations publiques
- Moteur de recherche
- Prise d'information active

Scan et prise d'empreinte

- Enumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation

Prise d'empreinte des services

- Attaques réseau
- Idle Host Scanning
- Sniffing réseau
- Spoofing réseau
- Hijacking
- Attaques des protocoles sécurisés
- Dénis de service

Attaques système

- Scanner de vulnérabilités
- Exploitation d'un service vulnérable distant
- Elévation de privilèges
- Espionnage du système
- Attaques via un malware
  - Génération d'un malware avec Metasploit
  - Encodage de payloads
- Méthode de détection

Attaques Web

- Cartographie du site et identification des fuites d'information
- Failles PHP (include, fopen, Upload,etc.)
- Injections SQL
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Bonnes pratiques

Attaques applicatives

- Escape shell
- Buffer overflow sous Linux
  - L'architecture Intel x86
  - Les registres
  - La pile et son fonctionnement
  - Présentation des méthodes d'attaques standards
  - Ecrasement de variables
  - Contrôler EIP
  - Exécuter un shellcode
  - Prendre le contrôle du système en tant qu'utilisateur root

OBJECTIFS

- Comprendre et savoir mener les attaques sur un SI
- Définir l'impact et la portée d'une vulnérabilité
- Réaliser un test de pénétration
- Trouver les vulnérabilités
- Contourner les sécurités

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

EXPLOITATION D'UNE VULNERABILITE

2 jours,
14 heures

PRESENTIEL
et/ou
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
- Connaître 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

AJC FORMATION

IT CYBERSECURITY ENGINEER

LES OUTILS DEFENSIFS DE DETECTION DES ATTAQUES ET COMPROMISSIONS

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Rôle de la détection d'intrusion

- Terminologie
- Faux positifs, détection, prévention, etc.

Architecture et types d'IDS / IPS

- Présentation de l'IDS
- Déploiement et configuration de base
- Langage d'écriture de règles
- Journalisation via Syslog

Présentation du HIDS et architecture

- Déploiement et configuration de base
- Syntaxe d'écriture de règles

Limites des IDS / IPS

- Intégration avec les autres composants du SI

Défis modernes posés à la supervision classique

- Objectifs d'un SIEM
- Architecture et fonctionnalités
- Syslog et centralisation des journaux
- Synchronisation du temps (NTP)
- Présentation d'ELK
- Configuration avancée de Logstash
- Configuration d'agents Logstash
- Ecriture de Groks avancés
- Environnement hétérogène : Linux, Windows

Visualisation des résultats dans Kibana

OBJECTIFS

- Comprendre la détection d'intrusion ; étude des sondes de détection d'intrusion IPS / IDS
- Comprendre les limites des outils de sécurité classiques
- Découvrir les principes technologiques derrière l'acronyme SIEM
- Comprendre le fonctionnement d'une solution SIEM et la gestion des évènements

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

VULNERABILITY SCORING & RISK SCORING (CVSS, CVE…)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Evaluation de la criticité d'une vulnérabilité

- CVE (Common Vulnerability Enumeration)
- CME (Common Malware Enumeration)
- CVSS (Common Vulnerability Scoring System)
- Construire une chaine de caractères (un vecteur) présentant les caractéristiques de cette vulnérabilité,
- Critères utilisés pour ce calcul

Caractéristiques générales

- Critères de « Base »
- Critères « Temporel »
- Critères « Environnemental »

Evolution des critères du groupe de base

- "Access Vector" (AV) ou "Attack vector".
  - mesure de « l'éloignement » de l'attaquant par rapport au composant vulnérable,
  - plus l'attaquant peut exploiter la vulnérabilité en étant éloigné, plus la vulnérabilité est critique.
  - Physical(P).
  - distinguer les attaques locales nécessitant un accès au système local de celles nécessitant un accès physique.

Attack Complexity & User Interaction

- Le critère "Access Complexity" Les valeurs possibles de ce critère sont None (N) ou Required (R).

Authentification

- Le critère "Authentication" (A) ou "Privilèges Required" (PR).
- Les valeurs possibles de ce critère sont None (N), Low (L), High (H).

Scope

- Le cas d'une vulnérabilité d'un système virtualisé, invité, qui a un impact sur le système hôte.
- Le cas d'une vulnérabilité d'un logiciel s'exécutant dans un environnement restreint dont l'impact est en dehors de cet environnement.
- Le cas d'un Cross-site scripting permettant d'utiliser un système vulnérable comme rebond pour attaquer un autre système.

Impacts

- Les critères relatifs à l'impact des vulnérabilités, "Confidentiality Impact" (C), "Integrity Impact" (I) et "Availability Impact" (A).
- Les valeurs possibles de ces trois critères, None (N), Partial (P), Complete (C) ou None (N), Low (L), High (H).
- Estimer le degré de gravité d'une attaque plutôt que le "pourcentage" impacté du système.

Evolution des critères du groupe de temporel

- "Exploitability" ou "Exploit code maturity" afin de mieux représenter ce que ce critère mesure.
- L'influence de ce groupe de critères sur le calcul du score temporel

Evaluation du risque lié à plusieurs vulnérabilités

- CVSS est conçu pour évaluer des vulnérabilités indépendamment les unes des autres.
- Un score ou un vecteur CVSS est associé à une vulnérabilité unique
- Evaluer le risque lié à une attaque enchainant l'exploitation de plusieurs vulnérabilités.

Conclusion sur les apports de CVSS v3.0

OBJECTIFS

- Evaluer la criticité d'une vulnérabilité CVE (Common Vulnerability Enumeration) CME (Common Malware Enumeration) CVSS (Common Vulnerability Scoring System)
- Construire une chaine de caractères (un vecteur) présentant les caractéristiques de cette vulnérabilité, les critères utilisés pour ce calcul

PROGRAMME DETAILLE

PROJET

IT CYBERSECURITY ENGINEER

PROJET ATTAQUES

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Déroulement du module

- Les stagiaires travaillent en toute autonomie, en binôme. Ils sont libres d'effectuer les choix adaptés, de développer les parties dont ils jugent avoir le plus besoin et d'apporter leurs propres solutions aux problèmes posés.
- Le formateur encadre les stagiaires par sa présence et répond aux questions. Il intervient pour épauler un binôme en difficulté ou pour faire le point à l'ensemble du groupe sur des notions non acquises. Il peut être amené à approfondir ou compléter certaines connaissances.

OBJECTIFS

- Mettre en application les acquis de la formation sur un projet d'Attaques

PROGRAMME DETAILLE

SECURISATION DE L'ARCHITECTURE ET DES APPLICATIONS

AJC FORMATION

IT CYBERSECURITY ENGINEER

SECURISATION SYSTÈME (LINUX, WINDOWS, AD…)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

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 fichier

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

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

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 de 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

AJC FORMATION

IT CYBERSECURITY ENGINEER

SECURISATION RESEAUX (FIREWALL, WAF, IPS, IDS…)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

La sécurité des accès, 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 exemples d'architectures

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

La sécurité des échanges

OBJECTIFS

- Sécuriser les réseaux d'entreprise
- Déployer des configurations robustes et appliquer les bonnes pratiques
- Protéger efficacement les utilisateurs
- Défendre les points d'entrée extérieurs
- Configurer correctement les équipements de protection

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

CHIFFREMENT

4 jours,
28 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Les différents types de chiffrement

Symétrique (TES, AES ...)

Asymétrique (RSA, Courbes elliptiques)

Notions de signatures

La gestion des certificats

Chiffrement mémoire RAM

Chiffrement des bases de données

Chiffrement des disques

Mise en place d'une infrastructure PKI

OBJECTIFS

- Comprendre les différents principes de chiffrement et leurs applications

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

DEVOPS ET OUTILS

4 jours,
28 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction Devops

Automatisation avec Ansible

Orchestration avec Kubernetes

Panorama des autres outils

OBJECTIFS

- Connaitre la méthode Devops
- Savoir automatiser et orchestrer des tâches

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

DEVELOPPEMENT SECURISE (DEVSECOPS)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Culture et management

- Termes et concepts clés
- Modèle d'incitation
- La résilience
- La culture organisationnelle
- Générativité
- Erickson, Westrum et LaLoux
- Exercice : Influencer la culture

Considérations stratégiques

- Termes et concepts clés
- Quel volume de sécurité est considéré comme suffisant?
- Modélisation de la menace
- Le contexte est tout
- Gestion des risques dans un monde à grande vitesse
- Exercice: Mesurer le succès

Considérations générales sur la sécurité

- Eviter le piège de la case à cocher
  Hygiène de sécurité élémentaire
- Considérations architecturales
- Identité fédérée
- Gestion des journaux

IAM : Gestion des identités et des accès

- Termes et concepts clés
- Concepts de base d'IAM
- Directives de mise en œuvre
- Opportunités d'automatisation
- Comment se faire mal avec IAM
- Exercice: surmonter les défis de l'IAM

Sécurité des applications

- Tests de sécurité des applications (AST)
- Techniques d'essai
- Prioriser les techniques de test
- Intégration de la gestion des problèmes
- Modélisation de la menace
- Automatiser

Sécurité opérationnelle

- Termes et concepts clés
- Pratiques d'hygiène de sécurité de base
- Rôle de la gestion des opérations
- L'environnement des opérations
- Exercice: Ajout de sécurité à votre pipeline CI / CD

DevSecOps

OBJECTIFS

- Se familiariser aux objets, avantages, concepts et vocabulaire de DevSecOps
- Connaitre les différences entre les pratiques de sécurité de DevOps et les autres approches de sécurité
- S'initier aux stratégies de sécurité axées sur les entreprises
- Comprendre et appliquer les sciences de la sécurité et des données
- Comprendre l'utilisation et les avantages des équipes rouges et bleues
- Apprendre à intégrer de la sécurité dans les flux de travaux de livraison continue
- Comprendre comment les rôles de DevSecOps s'intègrent à la culture et à l'organisation de DevOps

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

SECURITE VPN, SANS FIL ET MOBILITE

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Les vulnérabilités des applications Web / cloud

- §Pourquoi les applications Web / cloud sont-elles plus exposées ?
- §Les risques majeurs des applications Web : cloud selon l'OWASP (Top Ten2017).
- §Les attaques "Cross Site Scripting" ou XSS -Pourquoi sont-elles en pleine expansion ? Comment les éviter ?
- §Les attaques en injection (Commandes injection, SQL Injection, LDAP injection...).
- §Les attaques sur les sessions (cookie poisonning, session hijacking...).
- §Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode...).
- §Attaques sur les configurations standard (Default Password, Directory Transversal...).

Sécuriser un réseau WiFi

- Les algorithmes de chiffrement symétrique et asymétrique.
- Les fonctions de hachage.
- L'authentification et les certificats. Serveur Radius.
- Les problématiques de sécurité d'un réseau WiFi.
- Les protocoles WEP, TKIP, WPA et WPA2. Les normes.
- L'authentification 802.1x. EAP...

Sécurité des mobiles

- Présentation des risques selon l'OWASP (GoatDroid, IOS Project).
- Stockage de données métier, sessions, authentification (mémoire, SD, FS, keychain, etc.).
- Comprendre le Root Android, Jailbreaking.
- Protocoles d'échanges serveur.
- Impact des injections SQL et XSS dans les applications in-App, SMS.
- Solutions de Authentification, autorisation, émergence biométrie.
- Solutions de cryptographie (données, filesystem), backup restauration du terminal.
- Antivirus, antiphishing.

OBJECTIFS

- Former et sensibiliser des équipes techniques aux problématiques de sécurité liées aux réseaux sans-fil, dans le contexte actuel de forte mobilité des outils technologiques

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

SENSIBILISATION À LA SÉCURITÉ DES APPAREILS ANDROID ET IOS

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction au système Android / IOS

- Modèle de sécurité d'Android / IOS
- Permissions
- Anatomie d'une application
- Manifeste d'application
- Activités et Intents
- Utilisation de Content Providers
- Stockage de fichiers sur carte SD

Présentation des outils d'analyse

- Le SDK Android
- ADB (Android Debug Bridge)
- JADX
- Drozer

Préparation à l'analyse

- Installation du SDK
- Déploiement d'une autorité de certification sur Burp Suite

Prise d'information

- Découverte de l'activité principale
- Récupération d'informations concernant l'API utilisée
- Récupération d'informations depuis les fichiers de logs

Attaque de l'API

- Cross-Site Scripting
- Injection de code SQL
  Isolation de comptes utilisateur
- Chiffrement des communications
- Gestion des sessions

Reverse Engineering

- Analyse statique via JADX
- Récupération des points d'entrée de l'API
- Analyse des algorithmes de chiffrement utilisés
- Emplacement de stockage des données (local, carte SD)
- Type de données stockées
- Mots de passe présents dans le code source
- Utilisation d'intents en broadcast

OBJECTIFS

- Maîtriser les fonctionnalités avancées du système Android
- Organiser une procédure d'audit de sécurité de type test de pénétration sur une application mobile Android
- Se mettre en situation réelle d'audit

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

LES PROTOCOLES (SSH, SSSL…)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Installation et configuration d'OpenSSH

- Installer OpenSSH sur Linux
- Changement de port : configurer le pare-feu !
- Les principaux clients SSH sous Windows et Linux
- Les logs de connexion
- Utilisation de Fail2Ban ?
- Sécuriser SSH avec TCP Wrapper et le fichier /etc/hosts.allow
- Chroot SSH
- OpenSSH sur Windows ?

L'authentification par clé

- Générer un jeu de clés avec PuTTY et ssh-keygen
- La commande ssh-copy-id
- Configurer les accès au serveur avec les clés publiques
- Désactiver l'authentification par mot de passe
- Utilisation de la clé privée

La copie de fichier

- Les protocoles SCP et SFTP
- Principaux clients
- Rsync via SSH
- SSHFS

Les tunnels SSH

- Configuration d'un tunnel
- Le X11 Forwarding
- Utilisation de Xming sur Windows

OBJECTIFS

- Apprendre à installer, configurer et utiliser SSH

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

SECURITE CLOUD

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Rappel des éléments matériels et logiciels de l'architecture Cloud selon les organismes de standardisation NIST (National Institute of Standards and Technology)
- Complexité du contexte de l'utilisation en tout lieu avec tout type de terminaux de connexion

Déceler les points de vulnérabilité du Cloud

- Solutions et architectures du Cloud proposées par des grands acteurs du secteur (OS Cloud, virtualisation, stockage, Datacenter, réseaux...)
- Points de vulnérabilité du terminal d'accès au Datacenter du Cloud
- Problèmes de sécurité spécifique aux Clouds ouverts et interconnectés
- Quatre niveaux de sécurité (technologique, organisationnel, contractuel et de conception d'architectures techniques)

S'appuyer sur les solutions techniques de sécurité du Cloud, proposées par les constructeurs et opérateurs Cloud

- Synthèse des approches, matériels et logiciels de sécurité adoptés par des fournisseurs de Cloud
- Solutions de sécurité offertes par les opérateurs de Cloud public
- Internalisation des dispositifs privés dans le Datacenter du Cloud
- Cloud intermédiaire de sécurité (SecaaS : Security as a Service)
- Avantages et inconvénients de chaque solution

Sécuriser le Cloud par l'organisation des processus et le contrat de SLA

- Classification des applications éligibles pour le Cloud
- Évaluation des risques et mise en place de leur gestion
- Plan de reprise d'activité
- Choix entre les Clouds souverains et ouverts
- Définir les critères de SLA de sécurité
- Responsabilité de l'entreprise : terminaux d'accès et réseaux locaux et distants
- Responsabilités partagées des parties prenantes (entreprise cliente et son fournisseur des services du Cloud) en cas de problèmes liés à la sécurité

Sécuriser le Cloud par la conception des architectures

- Isolement et étanchéité des solutions impliquées (Virtualisation, Stockage, orchestration, API, connecteurs...) et des applications
- Association des moyens de protection, en fonction du niveau de sécurité nécessaire des éléments du Cloud
- Cloud hybride
- Cryptage de la transmission au niveau des réseaux locaux du Datacenter
- Firewall local au sein du Cloud
- Sécuriser les accès locaux et distants au Cloud en tout lieu pour des terminaux mobiles : VPN SSL, VPN IPSec et IEEE802.11i
- Dispositifs out-band de sécurité et de Firewall d'identité pour les accès mobiles en local
- Impact des solutions incohérentes de sécurité et métriques de qualité indispensable
- Ingénierie du trafic IP et des flux de données pour le bon fonctionnement des applications

OBJECTIFS

- Comprendre comment s'appuyer sur des référentiels de normes et de standards pour sécuriser le Cloud
- Connaître les moyens génériques de la sécurité du Cloud
- Être en mesure de s'inspirer des solutions et des démarches des opérateurs de Cloud pour sécuriser son approche
- Comprendre comment éviter la mise en place d'une sécurité coûteuse et laborieuse pouvant dégrader la performance du réseau global

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

SECURITE CLOUD (Suite)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Sécuriser l'utilisation des périphériques personnels des employés pour accéder au Cloud (BYOD : Bring Your Own Device)

- Choix des solutions sécurisées d'accueil des terminaux (VDI, TS-WEB, RDP, PCoIP…)
- Sélection des périphériques : tablettes, Smartphone, OS, navigateurs…. et leurs contraintes
- Étude des vulnérabilités pour fixer les règles d'utilisation d'accès au Cloud
- Affectation des droits selon des critères techniques et organisationnels

OBJECTIFS

- Comprendre comment s'appuyer sur des référentiels de normes et de standards pour sécuriser le Cloud
- Connaître les moyens génériques de la sécurité du Cloud
- Être en mesure de s'inspirer des solutions et des démarches des opérateurs de Cloud pour sécuriser son approche
- Comprendre comment éviter la mise en place d'une sécurité coûteuse et laborieuse pouvant dégrader la performance du réseau global

PROGRAMME DETAILLE

PROJET

IT CYBERSECURITY ENGINEER

PROJET SECURISATION

4 jours,
28 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Déroulement du module

- Les stagiaires travaillent en toute autonomie, en binôme. Ils sont libres d'effectuer les choix adaptés, de développer les parties dont ils jugent avoir le plus besoin et d'apporter leurs propres solutions aux problèmes posés.
- Le formateur encadre les stagiaires par sa présence et répond aux questions. Il intervient pour épauler un binôme en difficulté ou pour faire le point à l'ensemble du groupe sur des notions non acquises. Il peut être amené à approfondir ou compléter certaines connaissances.

OBJECTIFS

- Mettre en application les acquis de la formation sur un projet de Sécurisation

PROGRAMME DETAILLE

SURVEILLANCE ET MANAGEMENT DE LA SECURITE : SOC/SIEM

IT CYBERSECURITY ENGINEER

QU'EST CE QU'UN SOC/SIEM

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Rôle de la détection d'intrusion

Les différents types de SOC / SIEM

Terminologie

- Faux positifs, détection, prévention, etc.

Architecture et types d'IDS

Présentation de l'IDS Suricata

Déploiement et configuration de base

Langage d'écriture de règles

Journalisation via Syslog

Présentation du HIDS OSSEC et architecture

Déploiement et configuration de base

Syntaxe d'écriture de règles

Limites des IDS

Intégration avec les autres composants du SI

Défis modernes posés à la supervision classique

- Objectifs d'un SIEM
- Architecture et fonctionnalités
- Syslog et centralisation des journaux
- Synchronisation du temps (NTP)
- Présentation d'ELK
- Configuration avancée de Logstash

Visualisation des résultats dans Kibana

OBJECTIFS

- Comprendre les techniques d'analyse et de détection d'intrusion
- Savoir mettre en œuvre les solutions de prévention dans un SOC
- Apprendre le métier d'analyste SOC

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

MISE EN PLACE D'UN SOC/SIEM

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Rôle de la détection d'intrusion

Les différents types de SOC / SIEM

Terminologie

- Faux positifs, détection, prévention, etc.

Architecture et types d'IDS

Présentation de l'IDS Suricata

Déploiement et configuration de base

Langage d'écriture de règles

Journalisation via Syslog

Présentation du HIDS OSSEC et architecture

Déploiement et configuration de base

Syntaxe d'écriture de règles

Limites des IDS

Intégration avec les autres composants du SI

Défis modernes posés à la supervision classique

- Objectifs d'un SIEM
- Architecture et fonctionnalités
- Syslog et centralisation des journaux
- Synchronisation du temps (NTP)
- Présentation d'ELK
- Configuration avancée de Logstash

Visualisation des résultats dans Kibana

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

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

LES DIFFÉRENTS SOC ET SIEM

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Rôle de la détection d'intrusion

Les différents types de SOC / SIEM

Terminologie

- Faux positifs, détection, prévention, etc.

Architecture et types d'IDS

Présentation de l'IDS Suricata

Déploiement et configuration de base

Langage d'écriture de règles

Journalisation via Syslog

Présentation du HIDS OSSEC et architecture

Déploiement et configuration de base

Syntaxe d'écriture de règles

Limites des IDS

Intégration avec les autres composants du SI

Défis modernes posés à la supervision classique

- Objectifs d'un SIEM
- Architecture et fonctionnalités
- Syslog et centralisation des journaux
- Synchronisation du temps (NTP)
- Présentation d'ELK
- Configuration avancée de Logstash

Visualisation des résultats dans Kibana

OBJECTIFS

- Se familiariser au fonctionnement d'un SIEM, aux différents SIEM (Splunk, Qradar) et à leur mise en oeuvre
- Connaitre les limites d'utilisation et défis modernes posés à la supervision classique
- S'initier aux objectifs d'un SIEM

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

SPLUNK

4 jours,
28 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction Splunk

Exploration de la recherche de données, sauvegarde des recherches (Reports)

Les tableaux de bord ou l'art de faire ressortir les données avec Splunk

Les modèles de données, la notion de pivot

Recherche approfondie, enrichissement de données avec Splunk

Devenir proactif avec les alertes

OBJECTIFS

- Utiliser Splunk pour collecter, analyser et générer des rapports sur les données
- Créer des tableaux de bord afin de donner du relief aux données significatives
- Construire une application d'intelligence opérationnelle avec des fonctionnalités étendues
- Enrichir les données opérationnelles à l'aide de recherches et de flux
- Modéliser et synthétiser les données et effectuer des recherches basées sur le pivot
- Créer des alertes en temps réel, scriptées et d'autres alertes intelligentes
- Résumer les données avec des tendances à long terme, des rapports et analyses

IT CYBERSECURITY ENGINEER

LES POINTS DE CONTRÔLE ET NIVEAUX D'ALERTE

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Détection d'intrusion et SOC / SIEM

- Bien comprendre les protocoles réseaux.
- Intelligence Gathering.
- Détecter les trojans et les backdoors. Attaques et exploitation des failles.
- Le SOC et le SIEM
- Le métier de l'analyste .
- Comment gérer un incident ?

Les attaques sur TCP/IP

- Le "Spoofing" IP.
- Attaques par déni de service.
- Prédiction des numéros de séquence TCP.
- Vol de session TCP : hijacking (Hunt, Juggernaut).
- Attaques sur SNMP.
- Attaque par TCP Spoofing (Mitnick) : démystification.

Les points de contrôle

Niveau de gravité

Facilités des messages Prévention et détection d'intrusion

Les méthodes de détection

La détection par analyse scénaristique

L'analyse comportementale Analyse et corrélation (SIEM)

Principe de fonctionnement Capacité d'un SIEM

Collecte

Normalisation

Agrégation

Corrélation

OBJECTIFS

- Identifier le rôle de la détection d'intrusion
- Se familiariser avec la terminologie : faux positifs, détection, prévention, etc.

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

DÉTECTION DES MENACES (CORRÉLATION D'ÉVÈNEMENTS)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Détection d'intrusion et SOC / SIEM

- Bien comprendre les protocoles réseaux.
- Intelligence Gathering.
- Détecter les trojans et les backdoors. Attaques et exploitation des failles.
- Le SOC et le SIEM
- Le métier de l'analyste .
- Comment gérer un incident ?

Les attaques sur TCP/IP

- Le "Spoofing" IP.
- Attaques par déni de service.
- Prédiction des numéros de séquence TCP.
- Vol de session TCP : hijacking (Hunt, Juggernaut).
- Attaques sur SNMP.
- Attaque par TCP Spoofing (Mitnick) : démystification.

Les points de contrôle

Niveau de gravité

Facilités des messages Prévention et détection d'intrusion

Les méthodes de détection

La détection par analyse scénaristique

L'analyse comportementale Analyse et corrélation (SIEM)

Principe de fonctionnement Capacité d'un SIEM

Collecte

Normalisation

Agrégation

Corrélation

OBJECTIFS

- Réagir à un incident de sécurité Principe d'un NSM Bonnes pratiques

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

INVESTIGATION SUR LES INCIDENTS (ANALYSE DES LOGS…..)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Collecte et analyse des logs, optimiser la sécurité de votre SI

- Introduction à la collecte et à l'analyse des logs.
- La collecte des informations.
- Syslog.
- Le programme SEC.
- Le logiciel Splunk.

Introduction à la gestion des logs

- La sécurité des systèmes d'information.
- Les problématiques de la supervision et des logs.
- Les différentes possibilités de normalisation.
- Les solutions du marché.

La collecte des informations

- L'hétérogénéité des sources.
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, BDD, etc.).
- La collecte passive en mode écoute et la collecte active.

Analyse forensic

- L'analyse forensic d'un système.
- La cybercriminalité moderne.
- La preuve numérique.

Détection et réaction face à une attaque connue / inconnue

Réaction et contre-mesure

Les mesures correctives et les nouvelles APT

Politique de patch management

OBJECTIFS

- Prendre les bonnes décisions suite à l'analyse des remontées d'informations et à leur corrélation

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

SUIVI ET SUPPORT À LA REMÉDIATION

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Collecte et analyse des logs, optimiser la sécurité de votre SI

- Introduction à la collecte et à l'analyse des logs.
- La collecte des informations.
- Syslog.
- Le programme SEC.
- Le logiciel Splunk.

Introduction à la gestion des logs

- La sécurité des systèmes d'information.
- Les problématiques de la supervision et des logs.
- Les différentes possibilités de normalisation.
- Les solutions du marché.

La collecte des informations

- L'hétérogénéité des sources.
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, BDD, etc.).
- La collecte passive en mode écoute et la collecte active.

Analyse forensic

- L'analyse forensic d'un système.
- La cybercriminalité moderne.
- La preuve numérique.

Détection et réaction face à une attaque connue / inconnue

Réaction et contre-mesure.

Les mesures correctives et les nouvelles APT

Politique de patch management

OBJECTIFS

- Apprendre à suivre la correction des bugs trouvés en fonction des attaques et des menaces

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

MISE EN PLACE DE MESURES CORRECTIVES (PATCH MANAGEMENT …)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Collecte et analyse des logs, optimiser la sécurité de votre SI

- Introduction à la collecte et à l'analyse des logs.
- La collecte des informations.
- Syslog.
- Le programme SEC.
- Le logiciel Splunk.

Introduction à la gestion des logs

- La sécurité des systèmes d'information.
- Les problématiques de la supervision et des logs.
- Les différentes possibilités de normalisation.
- Les solutions du marché.

La collecte des informations

- L'hétérogénéité des sources.
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, BDD, etc.).
- La collecte passive en mode écoute et la collecte active.

Analyse forensic

- L'analyse forensic d'un système.
- La cybercriminalité moderne.
- La preuve numérique.

Détection et réaction face à une attaque connue / inconnue

Réaction et contre-mesure.

Les mesures correctives et les nouvelles APT

Politique de patch management

OBJECTIFS

- Savoir faire évoluer le SIEM en fonction des attaques et des menaces

PROGRAMME DETAILLE

PROJET

IT CYBERSECURITY ENGINEER

PROJET SURVEILLANCE

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Déroulement du module

- Les stagiaires travaillent en toute autonomie, en binôme. Ils sont libres d'effectuer les choix adaptés, de développer les parties dont ils jugent avoir le plus besoin et d'apporter leurs propres solutions aux problèmes posés.
- Le formateur encadre les stagiaires par sa présence et répond aux questions. Il intervient pour épauler un binôme en difficulté ou pour faire le point à l'ensemble du groupe sur des notions non acquises. Il peut être amené à approfondir ou compléter certaines connaissances.

OBJECTIFS

- Mettre en application les acquis de la formation sur un projet de Surveillance

PROGRAMME DETAILLE

LES NOUVELLES MENACES APT

IT CYBERSECURITY ENGINEER

VEILLE TECHNOLOGIQUE SUR LES NOUVELLES MENACES

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Veille Technologique

Définition d'une vulnérabilité

Définition de l'exploitation

Types de mesures correctives

Base de données CVE et score CVSS , CPE, CWE

Sources d'information (listes de diffusion Twitter, Reddit, etc.)

Flux RSS (Tiny Tiny RSS)

Automatisation (Google Alerts, Zapier, Netvibes)

Organisation d'une équipe de veille (CERT, CSIRT, ENISA)

OBJECTIFS

- Apprendre à identifier les nouvelles menaces avant d'en être victime

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

MISE EN PLACE DES MESURES PRÉDICTIVES

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Collecte et analyse des logs, optimiser la sécurité de votre SI

Modèles MITRE @ATTACK , TTP

La collecte des informations

- L'hétérogénéité des sources.
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, BDD, etc.).
- La collecte passive en mode écoute et la collecte active.

Analyse forensic

- L'analyse forensic d'un système.
- La cybercriminalité moderne.
- La preuve numérique.

Détection et réaction face à une attaque connue / inconnue

Réaction et contre-mesure

Les mesures correctives et les nouvelles APT

Politique de patch management

OBJECTIFS

- Savoir alimenter un SIEM en fonction des nouvelles menaces

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

NORMES DE SECURITE ET GESTION DES RISQUES

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

27001

- Présentation de la norme
- Périmètre
- Exemples d'application

27002

- Présentation de la norme
- Périmètre
- Exemples d'application

62443

- Présentation de la norme
- Périmètre
- Exemples d'application

27034

- Présentation de la norme
- Périmètre
- Exemples d'application

OBJECTIFS

- Identifier les normes par rapport aux problématiques des sujets traités : systèmes industriels, systèmes d'information, protection des données

PROGRAMME DETAILLE

IT CYBERSECURITY ENGINEER

LA PRODUCTION DES INDICATEURS

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Mettre en œuvre un reporting

- Identification de KPIs
- Monitoring de l'activité
- Analyse des données pour mettre en place des actions préventives et correctives

OBJECTIFS

- Savoir matérialiser au travers d'indicateurs le niveau de défense
- TOP20 SANS Controls

PROGRAMME DETAILLE

COMPORTEMENTAL

AJC FORMATION

IT CYBERSECURITY ENGINEER

PRESENTER SES NOUVELLES COMPETENCES

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Les bases de la communication

- Ecoute active
- Le questionnement
- Reformulation et feedback

La communication verbale et non verbale

- Importance de la communication non verbale
- Savoir se présenter à l'oral
- Postures – Attitudes – Discours

Les profils comportementaux

- Les 4 profils
- Auto évaluation
- Développer son adaptabilité relationnelle

Développer son Capital Talents

- Définition d'un talent
- Talent vs points forts
- 5 stratégies pour gérer ses points faibles

OBJECTIFS

- Se présenter en entretien tout en mettant en valeur ses nouvelles compétences en les considérant acquises

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

CONDUITE DE REUNION

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Faire le point sur ses pratiques actuelles

- Faire le bilan des réunions existantes : points forts, points faibles
- Augmenter la pertinence dans la sélection des participants
- Lutter contre les réunions stériles et réduire le temps passé en réunion (sans perdre en efficacité)

Organiser une réunion et en définir l'objectif

- La préparation et l'organisation matérielle
- Le cadrage de la réunion :objectif, durée et règles du jeu
- Les conditions nécessaires à l'implication des participants

Structurer ses réunions pour les rendre productives

- Utiliser les techniques adaptées à chaque réunion : réunion de service, réunion d'information ascendante et descendante, réunion de négociation, réunion de résolution de problèmes avec consensus ou avec concertation
- Formaliser pendant et après la réunion : conclure, valider et formaliser les points clés de la réunion, rédiger un compte-rendu (pertinence des informations et rapidité de diffusion)

Exercer les fonctions clés de l'animateur pour faire fonctionner efficacement le groupe de travail

- Développer ses capacités d'écoute
- Répartir les rôles pour être plus efficace
- Faciliter les échanges et la production d'idées
- Connaître et repérer les phénomènes de groupe pour mieux les utiliser
- Favoriser la créativité en utilisant des techniques appropriées
- Gérer les participants difficiles

Gérer les comportements des participants

- Réaliser votre « casting »
- Fixer le rôle des participants
- Reconnaître les comportements types des participants pour mieux comprendre leurs réactions
- Réguler les échanges et distribuer la parole
- Gérer les désaccords
- Aboutir à un plan d'action partagé

OBJECTIFS

- Savoir organiser une réunion productive : l'avant et l'après
- Gérer les comportements des participants
- Acquérir des techniques d'animation pour rendre les réunions participatives

PROGRAMME DETAILLE

AJC FORMATION

IT CYBERSECURITY ENGINEER

GESTION DU TEMPS ET DES PRIORITES

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Le temps : un allié de la croissance professionnelle

Connaître les différentes manières de structurer son temps

- Types de personnalités et structuration du temps
- Bilan de ses pratiques actuelles et de l'influence de son environnement
- Prise de conscience individuelle, premier diagnostic et niveaux de motivation de chacun

Savoir faire des choix

- Clarifier sa mission et les tâches qui en découlent
- Fixer et fractionner des objectifs
- Hiérarchiser ses priorités
- Savoir filtrer, sélectionner les véritables urgences

Maîtriser son temps sans subir

- Déterminer et agir sur les "voleurs de temps"
- Mieux renoncer pour mieux choisir

Gérer son temps avec les autres

Savoir dire "non"

- Gérer les interruptions
- Savoir déléguer

Utiliser ses forces positives

- Mieux connaître son capital énergie, ses rythmes de travail
- Contacter ses ressources positives, s'en servir comme multiplicateur d'énergie
- Savoir se concentrer, se motiver, s'arrêter, se relaxer

Intégrer le stress

- Rôle du stress, personnalités sensibles
- Se servir du "bon" stress, se protéger du "mauvais" stress
- Gestion des situations de stress les plus fréquentes ou cas particuliers

Qu'acceptez-vous de changer ?

- Déterminer les points réalistes de son contrat de changement
- Visualiser les résultats, modéliser ceux qui savent gérer leur temps

OBJECTIFS

- Acquérir des outils et des méthodes de gestion du temps afin de mettre en place des comportements nouveaux
- Prendre conscience de son comportement
- Reprendre le contrôle de son temps

PROGRAMME DETAILLE

PROJET

IT CYBERSECURITY ENGINEER

PROJET FINAL & SOUTENANCE IT CYBERSECURITE ENGINEER

10 jours,
70 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Déroulement du module

- Les stagiaires travaillent en toute autonomie, en binôme. Ils sont libres d'effectuer les choix adaptés, de développer les parties dont ils jugent avoir le plus besoin et d'apporter leurs propres solutions aux problèmes posés.
- Le formateur encadre les stagiaires par sa présence et répond aux questions. Il intervient pour épauler un binôme en difficulté ou pour faire le point à l'ensemble du groupe sur des notions non acquises. Il peut être amené à approfondir ou compléter certaines connaissances.

OBJECTIFS

- Mettre en application les acquis de la formation en complétant les mini projets réalisés dans tout le cursus

PROGRAMME DETAILLE

NOUS CONTACTER

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

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