AJC FORMATION

CYCLE

120 jours – 840 heures

PRODUCT SECURITY

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 PRODUCT SECURITY

Programme

OBJECTIFS

- Se familiariser avec les attaques pour mieux les contourner
- S'initier aux méthodes et process de l'audit / Pentest
- Appréhender la norme et la règlementation
- Connaître les différentes typologies d'attaques
- Rechercher et exploiter des vulnérabilités
- Savoir coder de façon sécurisée dans différents langages et savoir durcir un système
- 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

- Consultant Audit et Pentest, Consultant Protection des données, Consultant en Sécurité de l'Information, Vulnerability Manager ...

LIEU

- Présentiel et/ou Distanciel

CERTIFICATION / ATTESTATION

- Attestation de formation
- Certification Comp TIA Security +

Programme - Contenu pédagogique

COMPORTEMENTAL	RÔLE ET COMPORTEMENT DU CONSULTANT OBJECTIF « QUALITÉ » DE LA MISSION	2 jours
	TRAVAIL EN ÉQUIPE	1 jour
INTÉGRATION	LES FONDAMENTAUX DE LA SÉCURITÉ DEFENSIVE	2 jours
COMPRENDRE LES ATTAQUES POUR MIEUX LES CONTOURNER	EXEMPLES D'ARCHITECTURES DU SI	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 DÉFENSIFS DE DÉTECTION DES ATTAQUES ET COMPROMISSIONS	2 jours
	VULNERABILITY SCORING & RISK SCORING (CVSS, CVE …..)	2 jours
PROJET	PROJET CONTOURNER LES ATTAQUES	2 jours
LE PENTEST / L'AUDIT : METHODE ET PROCESS	QU'EST CE QU'UN PENTEST / AUDIT	1 jour
	LES DIFFÉRENTS TYPES DE PENTEST (RED TEAM, BLACK BOX ….)	1 jour
	LES MÉTHODOLOGIES (OWASP, OSSTIM, CWE ….)	2 jours
	LES OUTILS DEFENSIFS DE DÉTECTION DES VULNÉRABILITÉS	2 jours
	LES METHODES DE PENTEST (PTEST, ETC)	1 jour
	LA RÈGLEMENTATION ET ASPECTS JURIDIQUES	1 jour
	LES NORMES	3 jours
PROJET	PROJET PENTEST	2 jours
LANGAGES ET SECURITE DU CODE	JAVA / J2EE	8 jours
	SECURE JAVA ET WEB	2 jours
	C / C++	8 jours
	SECURE C / C++	2 jours
	PYTHON / PERL	7 jours

Programme - Contenu pédagogique

LANGAGES ET SECURITE DU CODE	SECURITE IOT	3 jours
	ADMINISTRATION ET SECURITE WINDOWS (AD)	3 jours
	ADMINISTRATION ET SECURITE LINUX	4 jours
	SECURITE DES SYSTEMES EMBARQUES	3 jours
PROJET	PROJET LANGAGES ET SECURITE	3 jours
DEFINITION DE LA STRATEGIE SURFACE D'ATTAQUE	IDENTIFIER LES POINTS D'ENTRÉE	2 jours
	LES ÉQUIPEMENTS DE SÉCURITÉ FW IPS IDS PROXY	3 jours
	CHIFFREMENT	4 jours
	LES ACCÈS AU CLOUD	2 jours
	LES INTERCONNEXIONS	2 jours
PROJET	PROJET STRATÉGIE SURFACE D'ATTAQUE	3 jours
CYCLE DE DÉVELOPPEMENT SÉCURISÉ DES APPLICATIONS	INTÉGRATION DE LA SÉCURITÉ DANS LES PROJETS DE DÉVELOPPEMENT	4 jours
DURCISSEMENT DES SYSTÈMES D'EXPLOITATION	ARCHITECTURE DES SYSTÈMES D'EXPLOITATION	3 jours
	DURCISSEMENT DU POSTE DE TRAVAIL	3 jours
	DURCISSEMENT DES SYSTÈMES D'EXPLOITATION WINDOWS	3 jours
	DURCISSEMENT DES SYSTÈMES D'EXPLOITATION LINUX	4 jours
	SÉCURITÉ DES SYSTÈMES INDUSTRIELS	3 jours
PROJET	PROJET CYCLE DEVELOPPEMENT SECURISE ET DURCISSEMENT	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 – PRODUCT SECURITY	4 jours

PROGRAMMES DÉTAILLÉS

COMPORTEMENTAL

AJC FORMATION

PRODUCT SECURITY

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

AJC FORMATION

PRODUCT SECURITY

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

INTEGRATION

AJC FORMATION

PRODUCT SECURITY

FONDAMENTAUX DE LA CYBERSECURITE 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
- 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
- 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
- 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 CONTOURNER

AJC FORMATION

PRODUCT SECURITY

EXEMPLES D'ARCHITECTURES DU SI

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

PRODUCT SECURITY

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

PRODUCT SECURITY

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

PRODUCT SECURITY

LES DIFFERENTES 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)

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
- Imaginer les attaques possibles en fonction de la cible
- Détecter les attaques visibles et dormantes
- Prévenir plutôt que guérir

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

LES OUTILS DEFENSIFS DE DETECTION DES ATTAQUES ET COMPROMISSIONS

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
- 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)

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
- Etudier des sondes de détection d'intrusion IPS / IDS
- Devenir efficace dans la veille technologique
- 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

PRODUCT SECURITY

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 de la criticité d'une vulnerabilité 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

PROGRAMME DETAILLE

PROJET

PRODUCT SECURITY

PROJET CONTOURNER LES 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 de Contournement des attaques

PROGRAMME DETAILLE

LE PENTEST/ L'AUDIT : METHODE ET PROCESS

PRODUCT SECURITY

QU'EST-CE QU'UN AUDIT / PENTEST

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Objectifs et types de PenTest

- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test
- Le cycle du PenTest
- Différents types d'attaquants
- Types d'audits
  - Boîte Noire
  - Boîte Blanche
  - Boîte Grise
- Avantages du PenTest
- Limites du PenTest
- Cas particuliers
  - Dénis de service
  - Ingénierie sociale

Prise d'information

- Objectifs
- Prise d'information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)
- Prise d'information active (traceroute, social engineering, etc.)
- Bases de vulnérabilités et d'exploits

OBJECTIFS

- Bien délimiter un audit
- Connaître les méthodes existantes , les règles, les engagements d'un audit, et ses limitations
- Connaître les méthodologies reconnues
- Mettre en place une situation d'audit à l'aide d'outils spécifiques

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

LES DIFFÉRENTS TYPES DE PENTEST (RED TEAM, BLACK BOX ….)

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Le pentest BlackBox

- Simulation d'une attaque en se mettant dans la peau d'un hacker,
- Conditions d'un piratage réel.
- Définition avec fiabilité des seuils critiques de la sécurité d'une entreprise.
- Exploration du système d'information à partir de peu ou pas d'éléments
- Définir des scénarios en cas de tentative d'intrusion par une entité extérieure à l'entreprise.
- Audits sur une courte période.

Le pentest WhiteBox

- Travaille en étroite collaboration avec la DSI de son client.
- Accèder à l'ensemble des informations relatives à la configuration du SI.
- pentest WhiteBox / audit informatique officiel,
- Approfondir la détection des vulnérabilités en accédant à toutes les strates du SI.

Le pentest Greybox

- Méthodologie intermédiaire,
- Avantages du BlackBox et du WhiteBox.
- pentester en s'aidant d'un nombre restreint d'informations.
- Approche du test du stagiaire
- Elévation des droits
- Stratégie de pentesting optimale,
- Simuler plusieurs types d'attaques, (greybox + redteam)
- Élaboration le scénario d'une attaque émanant d'un membre de l'entreprise ou d'un ancien salarié, voire même d'un prestataire externe, en fonction des droits qui lui sont alloués.

OBJECTIFS

- Lister les vulnérabilités d'un système ou d'une organisation
- Démontrer la capacité d'un hacker à pirater le système de l'intérieur (test du visiteur, du stagiaire ....)
- Tester l'efficacité des outils de détection d'intrusion mis en place si tel est le cas, ainsi que la réactivité des experts techniques lors d'une attaque

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

LES MÉTHODOLOGIES (OWASP, OSSTIM, CWE ….)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

OSSTMM (Open Source Security Testing Methodology Manual)

OWASP (Open Web Application Security Project)

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

CIS pour les audits de configuration

CWE/OWASP pour les audits de code

Démarche qualité basée sur le RGS de l'ANSSI (qualification PASSI)

OBJECTIFS

- Comprendre les méthodologies de pentesting OWASP et OSSTMM pour les tests d'intrusion CIS pour les audits de configuration CWE/OWASP,pour les audits de code
- Appréhender une démarche qualité basée sur le RGS de l'ANSSI (qualification PASSI)

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

LES OUTILS DEFENSIFS DE DETECTION DES VULNERABILITES

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Attaques à distance

- Introduction à Metasploit Framework
- Scanner de vulnérabilités
- Attaques d'un poste client
- Attaque d'un serveur
- Introduction aux vulnérabilités Web

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

Techniques de scan

- Différents types de scans
- Personnalisation des flags
- Packet-trace
- Utilisation des NSE Scripts

Détection de filtrage

- Messages d'erreur / Traceroute
- Sorties nmap
- Firewalking avec le NSE Firewalk

Plan d'infrastructure

- Problématiques / Erreurs à ne pas faire
- Eléments de défense

Forger les paquets

- Commandes de base
- Lire des paquets à partir d'un pcap
- Créer et envoyer des paquets

Sniffer les paquets

- Exporter au format pcap
- Exporter au format PDF
- Filtrage des paquets avec le filtre - filter
- Modifier des paquets via scapy
- Les outils de fuzzing de scapy
- Création d'outils utilisant scapy
- Détournement de communications

Système

- Metasploit
- Attaques d'un service à distance
- Attaque d'un client et bypass d'antivirus
- Attaque visant Internet Explorer, Firefox
- Attaque visant la suite Microsoft Office
- Génération de binaire Meterpreter
- Bypass AV (killav.rb, chiffrement, padding etc.)

Utilisation du Meterpreter

- Utilisation du cmd/Escalade de privilège
- MultiCMD, attaque 5 sessions et plus
- Manipulation du filesystem
- Sniffing / Pivoting / Port Forwarding

Attaque d'un réseau Microsoft

- Architecture / PassTheHash
- Vol de token (impersonate token)

Rootkit

OBJECTIFS

- Comprendre et mener les attaques sur un SI
- Définir l'impact et la portée d'une vulnérabilité
- Réaliser un test de pénétration
- Corriger les vulnérabilités
- Sécuriser un réseau

PROGRAMME DETAILLE

PRODUCT SECURITY

LES METHODES DE PENTEST (PTEST, ETC)

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Définition du contexte

Prise d'empreinte

Liste des menaces

Analyse des vulnérabilités

Lancement des attaques

Nettoyage des traces

Élaboration du rapport

OBJECTIFS

- Se familiariser avec les méthodologies en vigueur actuellement dans le cadre de Pentest

PROGRAMME DETAILLE

PRODUCT SECURITY

LA RÈGLEMENTATION ET ASPECTS JURIDIQUES

1 jour,
7 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Règles et engagements

Portée technique de l'audit

- Responsabilité de l'auditeur
- Contraintes fréquentes
- Législation : articles de loi
- Précautions usuelles

Méthodologie

- Utilité de la méthodologie
- Méthodes d'audit
- Méthodologies reconnues

Aspect règlementaire

- Responsabilité de l'auditeur
- Contraintes fréquentes
- Législation : articles de loi
- Précautions
- Points importants du mandat

Exemples de méthodologies et d'outils

- Préparation de l'audit
  Déroulement
  Cas particuliers
  – Habilitations
  – Dénis de service
  – Ingénierie sociale
- Déroulement de l'audit
  Reconnaissance
  Analyse des vulnérabilités
  Exploitation
  Gain et maintien d'accès
  Comptes rendus et fin des tests

OBJECTIFS

- Se familiariser aux règles et engagements
- Comprendre la portée technique de l'audit
- Intégrer la responsabilité de l'auditeur
- Connaitre les contraintes fréquentes
- S'initier à la législation : articles de loi
- Comprendre les précautions usuelles

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

LES NORMES

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Les normes ISO/CEI

Les nomes pour les SMSI

ISO/CEI 27001

ISO/CEI 27002

ISO/CEI 27034

ISO/CEI 31000

Les normes sur la cybersécurité industrielle

IEC 62443

- Les bases communes pour la cybersécurité industrielle
- General 62443-1
- Policies & procedures 62443-2
- System 62443-3
- Component 62443-4

Les guides ANSSI

Les guides ENISA (rail, car)

Les framweork NIST, SANS

OBJECTIFS

- Appréhender les normes en vigueur dans le cadre de la cybersécurité des systèmes d'information et industriels

PROGRAMME DETAILLE

PROJET

PRODUCT SECURITY

PROJET PENTEST

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 de Pentest

PROGRAMME DETAILLE

LANGAGES ET SECURITE DU CODE

AJC FORMATION

PRODUCT SECURITY

JAVA / J2EE

8 jours,
56 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

JAVA

Applications Java

- Compilation et exécution
- Kit de développement Java
- La compilation Just In Time et la technologie Hot Spot
- Déploiement des applications

Eléments de base du langage

- types primitifs, structures de contrôle, tableaux, …

Java, un langage de classes

- Déclaration d'une classe
- Visibilité d'une classe et de ses membres. Bloc d'initialisation statique
- Constructeurs
- Spécialisation des classes. Classes abstraites, classes d'interface
- Les méthodes à arguments variables
- Les types énumérés
- Les imports statiques
- Transtypage des objets. Autoboxing des types primitifs
- Les types génériques
- Les classes internes

Les collections

Les entrées / sorties

Les exceptions

Connexion JDBC

SERVLET / JSP

L'API Servlet

Présentation

- Principales classes de l'architecture Servlet (ServletContext, ServletRequest, ServletResponse, …)
- Le cycle de vie d'une servlet et la gestion des servlets par le conteneur.
- Méthodes doGet et doPost

Les JSP

Présentation des JSP

- Forme des JSP
- Les étapes d'une requête JSP

Composants d'une JSP

- Directives
- Scripts JSP (déclarations, expressions et scriplets)
- Les objets implicites et leur portée
- Traitement des erreurs JSP

Les bibliothèques de balises

- Les taglibs et leur descripteur XML
- Balises personnalisées
- Balises d'actions prédéfinies
- Utilisation des JavaBeans dans les JSP

CLASSES JPA HIBERNATE

Introduction

- Notion de mapping Objet/Relationnel
- Historique d'hibernate
- Hibernate et les spécifications JPA
- Concurrents : EclipseLink, iBatis
- Versions d'hibernate

OBJECTIFS

- Connaître l'architecture de Java SE
- Connaître les fonctions essentielles de Java SE
- Comprendre les principes de la programmation orientée objet
- Utiliser les données d'une BDD en Java
- Comprendre et savoir utiliser les composants Web de l'architecture JEE (Servlet, JSP)
- Acquérir les notions de persistance
- Utiliser les frameworks J2EE (Spring, …)

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

JAVA / J2EE (Suite)

8 jours,
56 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Persistance avec JPA

- Spécification JPA 2.0
- Fournisseur de persistence
- EntityManagerFactory
- EntityManager
- persistence.xml
- Persistence unit
- @ManyToOne, @ManyToMany
- Eager, Lazy
- Implications Jee
- Fetching

Persistance avec Hibernate

- Processus de développement
- Top-down, Bottom-up, Meet in the meedle
- Connexion à la base de données
- Configuration d'Hibernate et Session Factory
- Création, ajout et suppression d'objets
- Session Hibernate
- HibernateUtils

Mapping objet relationnel

Utilisation de Spring MVC / BOOT/ REST ...

OBJECTIFS

- Connaître l'architecture de Java SE
- Connaître les fonctions essentielles de Java SE
- Comprendre les principes de la programmation orientée objet
- Utiliser les données d'une BDD en Java
- Comprendre et savoir utiliser les composants Web de l'architecture JEE (Servlet, JSP)
- Acquérir les notions de persistance
- Utiliser les frameworks J2EE (Spring, …)

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

SECURE JAVA ET WEB

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction aux concepts liés à la sécurité

- Identification et méthodes d'authentification.
- Autorisations et permissions.
- Confidentialité, non-répudiation, cryptage, clés publiques/privées, autorités de certification.
- Pare-feu et DMZ, rupture de protocole.
- Les types d'attaques.
- Le modèle de sécurité de la JVM

Chargement et vérification des classes

- Rôle du compilateur Java
- Rôle des classloader
- Les différentes zones mémoires de la JVM et
- leur gestion par le garbage collector
- Hiérarchie des différents classloader
- Vérification du byte-code
- Chargement dynamique ce classe
- Implémenter un class loader

Cross-site scripting et sécurité

- Le principe du XSS (injection de contenu)
- Liens avec les programmes Java Déclinaisons (Stored XSS, Reflected XSS, DOM-based XSS)
- Nouvelles "possibilités" avec le HTML 5
- Gestionnaire de sécurité et permissions
  - Opérations contrôlables
  - Activation du gestionnaire de sécurité
  - Domaine de protection, provenance du code et permissions
  - Parcours de l'API
  - Fichier .policy
  - Les classes Permission
  - Implémentation d'une classe Permission

JAAS, Authentification et Autorisations

- Présentation de JAAS
- LoginContext / LoginModule, Configuration et empilement des login modules
- LoginModule communément disponibles
- Implémentation d'un login module spécifique, les CallbackHandler Autorisations, Objet Subject et Principals,
- Configuration des permissions
- Signatures numériques et chiffrement

Signatures numériques et chiffrement

- Empreinte de messsage, SHA1 et MD5 Signature numérique, clé publiques et clés privées
- L'outil keytool et les keystore
- L'outil jarsigner
- Les autorités de certification
- Déploiement de code signé dans un intranet ou sur internet
- Permissions basées sur des keystore
- Chiffrement de données, les algorithmes AES et RSA

SSL et Java

- Fonctions de Java Secure Socket Extension (JSSE). Comparaison avec Java GSS-API
- Authentification via certificats X.509. TLS et SSL.

OBJECTIFS

- Connaitre les concepts liés à la sécurité
- Savoir charger et vérifier des classes
- Connaitre le cross-site scripting et la sécurité liée
- Maitriser le gestionnaire de sécurité et permissions
- Maitriser SSL et Java

PROGRAMME DETAILLE

PRODUCT SECURITY

SECURE JAVA ET WEB (Suite)

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

- Encryption à base de clés publiques, Java Cryptography Extension (JCE).
- Utilisation de SSL avec HTTP.
- La sécurité d'une application JEE
- Authentification au niveau des conteneurs Web et EJB.
- Rôles applicatifs, permissions et descripteurs de déploiement XML.
- Contrôles dynamiques via les API Servlets et EJB.
- La sécurité dans les API : JDBC/JPA, JNDI, JTA, JMS, JCA.

La sécurité des services web SOAP

- Sécurité au niveau HTTP.
- Sécurité au niveau SOAP & WSDL avec WS-Security (WSS4J, XWSS...) & WS-Policy.
- Les handlers SOAP WS-Security exploitant JAAS.

La sécurité des services web REST

- Utilisation de SSL avec JAX-RS.
- Les apports de

oAuth (authentification sur Internet).
oAuth 1.0 et 2.0.

OBJECTIFS

- Connaitre les concepts liés à la sécurité
- Savoir charger et vérifier des classes
- Connaitre le cross-site scripting et la sécurité liée
- Maitriser le gestionnaire de sécurité et permissions
- Maitriser SSL et Java

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

C / C++

8 jours,
56 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

LE LANGAGE C

Présentation du langage C

- Historique, utilisation, organisation des fichiers, éditeur, compilation, environnement de développement, domaines d'utilisation, la norme ANSI

Le Langage C

- Caractères autorisés, la fonction main, blocs et instructions, commentaires, initiation préprocesseur, types de données élémentaires

Les variables

- Déclaration, déclarations globales et locales, initialisation des variables
- Sorties formatées d'un programme
- Entrées/sorties formatées.
- Formatage numérique, formatage caractère, entrées formatées

Les opérateurs

- Opérateurs arithmétiques.
- Mécanismes d'évaluation des expressions.
- Post et pré-incrémentation de décrémentation.
- Précédence et associativité des opérateurs.

Expressions logiques

- Instruction d'affectation
- Mécanismes de fonctionnement des expressions logiques.

Opérateurs de comparaison

- if, switch, while, do, for, break, continue

Opérateurs de type

- Cast, sizeof, malloc, delete

Opérateurs travaillant au niveau du bit

- ET, OU, OU exclusif, complément à 1.Décalages.

Tableaux, pointeurs et chaînes de caractères

- Définition. Tableau à une dimension. Initialisation. Tableau multi-dimensionnel. Chaînes de caractères - Copie de chaînes de caractères. Opération sur les chaînes de caractères.

Les fonctions

- Présentation, définition, déclaration, paramètres de fonction, retour d'une fonction, appel, passage de l'adresse d'une fonction

Compléments sur les directives de compilation

LE LANGAGE C++

Les classes

- Déclaration dans le fichier cpp
- Méthodes
- Paramètres par défaut
- Masquage
- Surcharge

Les constructeurs

- Exemples d'utilisation
- Types de constructeurs
- Constructeur par copie
- Constructeurs par transtypage
- Usage du mot clé explicit
- Constructeurs à arguments multiples
- Liste d'initialisations
- Le destructeur

OBJECTIFS

- Acquérir les bases du langage C, le langage utilisé pour sa rapidité
- Aborder les éléments du langage et les spécificités du compilateur gnc c
- Appréhender les concepts objets (Classe, Encapsulation, polymorphisme, héritage) qui ne sont pas présents en langage C.
- Tester des Bibliothèques et API

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

C / C++ (Suite 1)

8 jours,
56 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Qualifieurs

- Constance
- Variables statiques
- Méthodes statiques
- Autres types de classe de stockage
- Constance
- Fonctions amis
- Classes amies

Surcharge des opérateurs

- Liste des opérateurs qui peuvent être surchargés
- Surcharge d'un opérateur par une fonction membre
- Surcharge d'un opérateur par une fonction non membre
- Surcharge de l'opérateur d'affectation `operator=`
- Opérateur de conversion vers un autre type
- Symétrie

Les exceptions

- Exemple d'exception
- Remarques
- Attraper une exception
- La classe exception et sa dérivée stdexcept
- Réponses
- Laisser échapper une exception
- Déclaration de fonction avec exception non traitées
- Faire/défaire

Espaces de nommage

- Présentation
- Déclaration
- Définition
- Utilisation
- Exemples connus
- Exclusion de méthodes d'un namespace
- Espace de nommage anonyme

Préprocesseur

- Les directives
- Directives include et define simple
- Instructions conditionnelles
- ifndef define ifdef
- identificateur
- Les macros
- Macros prédéfinies

Dérivation - Héritage

- Classe fille
- Déclaration de la classe fille
- Encapsulation
- Particularité amusante
- Héritage multiple
- Portée d'héritage
- Redéfinition vs surcharge
- Problématiques des classes dérivées

Polymorphisme

- Méthodes virtuelles
- Contrainte sur les fonctions virtuelles
- Fonctions virtuelles pures et classes abstraites

OBJECTIFS

- Acquérir les bases du langage C, le langage utilisé pour sa rapidité
- Aborder les éléments du langage et les spécificités du compilateur gnc c
- Appréhender les concepts objets (Classe, Encapsulation, polymorphisme, héritage) qui ne sont pas présents en langage C.
- Tester des Bibliothèques et API

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

C / C++ (Suite 2)

8 jours,
56 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Pointeurs

- Rappels
- Définition d'un pointeur
- Difficultés de notation
- Pointeurs et allocation mémoire
- Désallocation
- Organisation de la mémoire
- Pointeurs et classes
- Le pointeur *this*
- Arithmétique sur les pointeurs
- Cas d'utilisation des pointeurs : pas

RTTI

- Définition
- Exemple pratique
- Règles à respecter
- TypeId
- Utilisation

Templates

- Présentation
- Patrons de fonction
- Utilisation
- Remarques
- Piège sur les pointeurs
- Patron de fonction à l'intérieur d'une classe
- Instanciation implicite et explicite
- Spécialisation

Patrons de classe

- Exemple
- Fonctions exportées
- Template sur les opérateurs
- Foncteurs
- A quoi servent les foncteurs ?
- Cas d'utilisation
- Performance

OBJECTIFS

- Acquérir les bases du langage C, le langage utilisé pour sa rapidité
- Aborder les éléments du langage et les spécificités du compilateur gnc c
- Appréhender les concepts objets (Classe, Encapsulation, polymorphisme, héritage) qui ne sont pas présents en langage C.
- Tester des Bibliothèques et API

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

SECURE C / C++

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Découvrir le Secure Coding

- Connaître les risques liés au développement
- Repérer les traces laissées par les développeurs : mémoire, journaux…
- Identifier les attaques
- Connaître les différents acteurs : CERT, PCI, CWE, OWASP…
- Apprendre le codage sécurisé d'une application

Classification des risques CERT

- Les domaines : integer, string, floating point, array…
- Analyser la sévérité, priorité, etc.
- Les guidelines

Le langage C++

- Modèle mémoire
- Compilation
- Comprendre les appels de fonction : structure de la pile
- Legacy code en langage C

Coder de manière à sécuriser le code

- Exemples de code
- Les chaînes de caractères
- Les pointeurs
- Gestion de la mémoire
- Les entiers
- Les sorties formatées
- Les fichiers

Les bonnes pratiques

- Apprendre les bonnes pratiques de codage :
  macro et inline
- Gestion de la mémoire : new, free, gestion des erreurs
- Structure des classes
- Passer à C++14 et C++17 : généralités (nullptr, enum, deleted fonctions) , utilisation des smart pointers, nouveaux mots clés
- Connaître les standards de sécurité
- Vérifier son code

OBJECTIFS

- Connaître le fonctionnement de la pile
- Repérer les erreurs dans le code
- Connaître le rôle des acteurs et la classification des risques : CERT, CWE, OWASP
- Appliquer les bonnes pratiques

PROGRAMME DETAILLE

PRODUCT SECURITY

PYTHON / PERL

7 jours,
49 heures

PRESENTIEL
et/ou
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.
- Les packages
- Map, reduce et filter

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.
- Notion de modèle de conception (design pattern).

Programmation Objet en Python

Utilisation StdLib

- Les arguments passés sur la ligne de commande.
- L'utilisation du moteur d'expressions régulières Python avec le module "re", les caractères spéciaux, les cardinalités.
- La manipulation du système de fichiers.
- Présentation de quelques modules importants de la bibliothèque standard : module "sys", "os", "os.path".
- Empaquetage et installation d'une bibliothèque Python.
- Les accès aux bases de données relationnelles, le fonctionnement de la DB API.
- Utilisation de contenus XML

Introduction au langage Perl

OBJECTIFS

- S'initier aux méthodes et réflexes de la programmation orientée objet et leur apporter la maîtrise opérationnelle du langage Python
- Apprendre à scripter en Perl

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

SECURE IOT

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction à l'IoT (Internet of Things ou Internet des Objets) et au paysage de la sécurité

- L'IoT aujourd'hui
- Statistiques hardware vs software
- Anecdotes, APT (Advanced Persistent Threats) et vulnérabilités connues
- Attaques, menaces et risques
- Etudes des différentes attaques qui ont touché l'IoT
- L'impact sur les organisations
- Comment les attaques auraient pu être prévenues ?
- "Secure by design" pour l'IoT
- Vecteurs d'attaques : l'Internet des problèmes
- "Threat Modeling"

Introduction

- Sécurité matérielle
- Rappels d'électronique analogique et numérique
- Equipement de l'analyste
- Présentation du lab (mise en place de l'environnement de travail)
- Rétro-ingénierie du schéma électronique
  - Identification des composants
  - Interconnexions et rôle...

Ports de communication série et debugger

- Protocole de communication UART (Universal Asynchronous Receiver Transmitter)
- Interfaçage avec ordinateur
- Extraction des micrologiciels
- Interfaces de débogage et de programmation
  - JTAG
  - SWD
  - CC
  - NAND Glitching
- Exploitation des "bootloaders"
- Exploitation de mécanismes de mise à jour
- "Chip-off" et "dump"

Rétro-ingénierie de micrologiciels

- Système d'exploitation
- Interruptions matérielles
- Extraction de systèmes de fichiers
- Désassemblage et analyse
- Recherche de vulnérabilités
- Analyse de configuration
- Mots de passe faibles et par défaut
- Fonctionnalités cachées
- Vulnérabilités :

  Système

  Web

  Réseau

Backdooring

- Mécanismes d'installation de porte dérobée
- Compilation de portes dérobées pour architectures embarquées
  - ARM
  - MIPS
- Persistance de la porte dérobée

OBJECTIFS

- Interfacer et communiquer avec un objet connecté
- Déterminer la surface d'attaque d'un objet connecté
- Comprendre les cybermenaces liées à l'IoT
- Extraire les firmwares IoT
- Analyser un firmware
- Identifier des vulnérabilités dans un firmware et les exploiter
- Analyser les protocoles de communication IoT

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

SECURE IOT (Suite)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Communications sans-fil

- Introduction à la radio logicielle
  - RTL SDR
  - HackRF One...
- Utilisation simple de la radio logicielle
  - Capture et rejeu de communications
  - Brouillage
- Protocoles propriétaires
  - Analyse d'un protocole propriétaire
  - Attaque d'un équipement
- Interception de communications SPI
- Bluetooth Low Energy

Les frameworks pour sécuriser l'IoT

- Sécurité du code
- Sécurité des infrastructures
- Chiffrement des canaux de communication
- Patch management
- Mettre un cycle de développement sécurisé

OBJECTIFS

- Interfacer et communiquer avec un objet connecté
- Déterminer la surface d'attaque d'un objet connecté
- Comprendre les cybermenaces liées à l'IoT
- Extraire les firmwares IoT
- Analyser un firmware
- Identifier des vulnérabilités dans un firmware et les exploiter
- Analyser les protocoles de communication IoT

PROGRAMME DETAILLE

PRODUCT SECURITY

ADMINISTRATION ET SECURITE WINDOWS (AD)

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Un annuaire Active Directory, pourquoi ?

Les classes, identifiants et attributs

Les différents types de groupe

Contrôleur de domaine et domaine

Les cinq rôles FSMO

Domaine, arbre et Forêt

Le catalogue global

Les relations d'approbations

Les protocoles LDAP, DNS et Kerberos

OBJECTIFS

- Comprendre les mécanismes des annuaires de type Active Directory

PROGRAMME DETAILLE

PRODUCT SECURITY

ADMINISTRATION ET SECURITE LINUX

4 jours,
28 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

Notions de sécurité

OBJECTIFS

- Acquérir les compétences essentielles en matière d'administration Linux, en se concentrant sur les tâches d'administration de base.
- Apprendre à sécuriser un serveur Linux

PROGRAMME DETAILLE

AJC FORMATION

PRODUCT SECURITY

SECURITE DES SYSTEMES EMBARQUES

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Généralités
- Les conséquences
- Vocabulaire

IoT / IIoT

- Principes
- Secteurs d'utilisation
- Exemples

La cybersécurité et les risques dans l'embarqué

- Risques produits
- Risques connectivité
- Risques production

Les normes

- IEC 62443
- ISO 27000
- La cybersécurité dans les autres normes
  - IEC 61508
  - ISO 26262
  - IEC 62304...

La gestion de projets embarqués et la SSI

- Identification des risques liés aux équipes de développement
- Informations aux équipes de développement
- Protection des sources
- Cycle de vie du produit (maintenance corrective / évolutive)

La sécurisation des systèmes embarqués

- Méthodes de développement
- Architecture de sécurité système
- Fonctions de sécurité embarquées

La sécurisation de la production de systèmes embarqués

- Identification des risques
- Informations aux équipes de production
- Protection des binaires

La protection des systèmes embarqués existants

- Identification des risques
- Solutions de protection

Sécurité des communications sans fil : NNFC, RFID, BlueTooth, Zigbee

OBJECTIFS

- Comprendre les enjeux liés aux systèmes embarqués
- Appréhender les diverses solutions, techniques et classes d'outils permettant d'évaluer les risques que ce soit au niveau du codage, de l'architecture système ou de la communication du dispositif
- Améliorer la cybersécurité d'un système embarqué
- Aborder sereinement la conception de nouveaux produits et services connectés
- Adapter les moyens de protection à votre contexte
- Vous positionner dans une démarche "Secure by Design"

PROGRAMME DETAILLE

PROJET

PRODUCT SECURITY

PROJET LANGAGES ET SECURITE

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 Langages et sécurité

PROGRAMME DETAILLE

DEFINITION DE LA STRATEGIE SURFACE D'ATTAQUE

AJC FORMATION

PRODUCT SECURITY

IDENTIFIER LES POINTS D'ENTRÉE

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Etude de la cible

- L'identification des risques pour l'entreprise d'un point de vue « business ».
- Traduction des risques business en risque IT
- Traduction des risques IT en risques cybersécurité

Exposition (internet, ports, etc.....)

Définition de la surface d'attaque et de la méthodologie

Les outils de prise d'information

- 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

- Arriver à définir une surface d'attaque, la collecte d'informations
- Découvrir l'exposition d'une cible, les bons outils pour les bonnes cibles

PROGRAMME DETAILLE

PRODUCT SECURITY

LES ÉQUIPEMENTS DE SÉCURITÉ FW IPS IDS PROXY

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

La sécurité des accès, Firewalls, Sécurité, 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

- 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

PRODUCT SECURITY

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

PRODUCT SECURITY

LES ACCÈS AU CLOUD

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...).

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.

OBJECTIFS

- Identifier les vulnérabilités les plus courantes des applications Web / cloud
- 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

PRODUCT SECURITY

LES INTERCONNEXIONS

2 jours,
14 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Filtrage, translation d'adresses et la DMZ

- Rappels réseau
- Mise en place d'un pare-feu
- Le filtrage simple
- Le suivi des connexions
- La translation d'adresses et de ports
- La journalisation
- Pare-feu et DMZ
- Étude des flux et des risques
- Cloisonnement des services
- Redirection et équilibrage de charge
- Mise en place des services communs publics (DNS, mail, FTP, WEB, etc.)
  LAB3 - Pare-feu applicatif et proxy
- Analyse d'un proxy protocolaire (objectifs et limites)
- Fonction proxy et reverse proxy
- Exploitation dans le cadre de l'analyse de protocoles, du contrôle d'accès et du filtrage

Les VPN

- Mise en place d'un tunnel simple d'élongation de réseau
- Architecture VPN d'opérateurs
- Sécurisation des élongations par VPN cryptologiques de type Host2Lan et Lan2LAN

OBJECTIFS

- Comprendre et mettre en œuvre les principes de sécurisation d'un Réseau Local d'Entreprise
- Comprendre les architectures de sécurité, identifier et cloisonner les flux réseau
- Exploiter une architecture VPN dans le cadre du télétravail et de l'interconnexion de sites, architectures VPN en entreprise, VPN opérateurs.

PROGRAMME DETAILLE

PROJET

PRODUCT SECURITY

PROJET STRATEGIE SURFACE D'ATTAQUE

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 Stratégie surfaces d'attaque

PROGRAMME DETAILLE

CYCLE DE DEVELOPPEMENT SECUSRISE DES APPLICATIONS

PRODUCT SECURITY

INTEGRATION DE LA SECURITE DANS LES PROJETS DE DEVELOPPEMENT

4 jours,
28 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Design

Implémentation et test unitaire

Intégration des tests

Business testing

Audit de sécurité externe

Fixer les problématiques

Fin de sprint

OpenSAMM

Méthodologie et norme actuelle (SDLC)

Introduction (Statistiques, ...)

Les étapes du SSDLC :

Définition du besoin

Architecture

Développement (SAST, DAST, analyse des dépendances)

Tests (Top 10 OWASP)

Les phases de releases, maintenance (prod, preprod, automatisation)

Les outils d'évaluation du niveau de maturite (openSAMM, ASVS, ...)

SDL – CLPsS,BSIMM

Modélisation des menaces STRIDE, PASTA

SARA, TARA, HARA

Analyse de risque (NIST Framework, Heaven, EBIOS, etc)

OBJECTIFS

- Apprendre à conduire un projet de développement en intégrant la sécurité
- Maitriser la sécurité des cycles de développement des applications

PROGRAMME DETAILLE

DURCISSEMENT DES SYSTEMES D'EXPLOITATION

PRODUCT SECURITY

ARCHITECTURE DES SYSTEMES D'EXPLOITATION

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Les différents systèmes d'exploitation et leurs spécificités

Les systèmes monolithiques

Les systèmes en couches

Les noyaux

La gestion de la mémoire

La gestion des processus

Gestionnaire de périphériques (entrées / sorties)

Gestion des fichiers

Gestion des applications

OBJECTIFS

- Comprendre les mécanismes de fonctionnement des systèmes d'exploitation

PROGRAMME DETAILLE

PRODUCT SECURITY

DURCISSEMENT DU POSTE DE TRAVAIL

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Les constituants d'un poste de travail

Sécurisation du BIOS UEFI

Sécurité des sessions

Antivirus

Pare feu

Limitation des applications exécutées

Limitation des périphériques

Mises à jour du système d'exploitation

Mises à jour des applications

Trace d'intrusion en cas de compromission

OBJECTIFS

- Savoir renforcer la sécurité des postes de travail

PROGRAMME DETAILLE

PRODUCT SECURITY

DURCISSEMENT DES SYSTEMES D'EXPLOITATION WINDOWS

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Gestion des utilisateurs (les SID)

Gestion des groupes

Les profils

Gestion des périphériques et des entrées / sorties (USB, etc....)

Les partages

Gestion de l'exécution des applications (AppLocker)

Le protocole NetBIOS

Gestion du pare feu

OBJECTIFS

- Comprendre et paramétrer les systèmes d'exploitation Linux dans un environnement exposé

PROGRAMME DETAILLE

PRODUCT SECURITY

DURCISSEMENT DES SYSTEMES D'EXPLOITATION LINUX

4 jours,
28 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Gestion des utilisateurs (PAM, NSS)

Gestion des droits sur les fichiers (Umask, SUID, GUID, etc)

Configuration des services (syslog)

Cloisonnement (chroot, sudo)

OBJECTIFS

- Comprendre et paramétrer les systèmes d'exploitation Linux dans un environnement exposé

PROGRAMME DETAILLE

PRODUCT SECURITY

SECURITE DES SYSTEMES INDUSTRIELS

3 jours,
21 heures

PRESENTIEL
et/ou
DISTANCIEL

PROGRAMME DU MODULE

Architecture réseau des systèmes industriels

Architecture des systèmes SCADA

Failles des protocoles inter-automates (ModBUS, Profibus, etc.)

Surveillance des programmes des automates (temps de cycle, variables, etc.)

Sécurité des IHM

OBJECTIFS

- Comprendre et appréhender les problématiques de sécurité sur les systèmes industriels

PROGRAMME DETAILLE

PROJET

PRODUCT SECURITY

PROJET CYCLE DEVELOPPEMENT SECURISE ET DURCISSEMENT

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 cycle de développement sécurisé et durcissement

PROGRAMME DETAILLE

COMPORTEMENTAL

AJC FORMATION

PRODUCT SECURITY

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

PRODUCT SECURITY

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

PRODUCT SECURITY

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

PRODUCT SECURITY

PROJET FINAL & SOUTENANCE PRODUCT SECURITY

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 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