EDITION 2023

CATALOGUE DES FORMATIONS

forSSIc

SOMMAIRE

À PROPOS DES FORMATIONS

LA PÉDAGOGIE APPLIQUÉE

L'ensemble de nos formations sont axées sur la mise en pratique d'ateliers, de travaux dirigés et d'études de cas concrêts et d'actualités.

La Répartition Théorique / Pratique est de l'ordre de 30% / 70%.

LES SOLUTIONS DE FINANCEMENT

Pour trouver la meilleure solution de financement adaptée à votre situation : contactez votre conseiller formation.

- Il vous aidera à choisir parmi les solutions suivantes :
- Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
- Le dispositif FNE-Formation.
- L'OPCO (opérateurs de compétences) de votre entreprise.
- Pôle Emploi sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

LES HORAIRES

En présentiel, les cours ont lieu de 9h à 12h30 et de 14h à 17h30. Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts. En classe à distance, la formation démarre à partir de 9h. Pour les stages pratiques de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 15h30 le dernier jour.

AF-ESS - LES ESSENTIELS DE LA CYBERSÉCURITÉ

DESCRIPTION

Le monde est aujourd'hui digital. Tout est connecté et un écosystème numérique évolue avec notre vie. Cet écosystème hyperconnecté, complexe n'est pas sans danger. Pour pouvoir l'aborder sereinement, dans sa vie personnelle comme dans sa vie scolaire ou professionnelle, il est primordial d'avoir une hygiène numérique adaptée et comprise. Cette formation permet de valider l'essentiel des savoirs permettant d'obtenir les bons réflexes pour une meilleure hygiène numérique.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Connaitre les différents acteurs de la cybersécurité en France
- Savoir mettre en œuvre les bonnes pratiques de sécurité
- Connaitre les définitions et les typologies de menaces
- Connaitre les risques pesant sur ma société et savoir les appréhender
- Comprendre l'importance de la charte informatique

PUBLIC CONCERNÉ

- Tout public

PRÉREQUIS

- Aucun

TARIF : 950 € HT

PROGRAMME DE LA FORMATION

1 - LA CYBERSÉCURITÉ C'EST QUOI ? :

- Les VIP de la cybersécurité
- Les acteurs
- Suis-je un acteur ?
- Gendarme ou voleur ?
- Vocabulaire

TRAVAUX DIRIGÉS

Quizz

2 - LES DANGERS VENUS D'INTERNET :

- Que trouve-t-on sur moi sur internet ?
- Mot de passe : passoire ou forteresse ?
- Phishing, spear-phishing, ma boite mail est-elle un espace sûr ?
- La navigation web, un espace de liberté à sécuriser
- Rouages et mécanique d'une cyberattaque
- Matériels et protocoles associés

TRAVAUX DIRIGÉS

Crack de mot de passe faible, mail piégé, exemple site vulnérable, OSINT

3 - LA SÉCURITÉ EN ENTREPRISE :

- Mon entreprise est-elle vulnérable ?
- La charte informatique : le contrat de sécurité
- Une hygiène de sécurité
- Chiffrer ? Vous avez dit chiffrer ?
- Un VPN pour quoi faire ?

TRAVAUX DIRIGÉS

Shodan, quizz guide hygiène, démonstration protocole en clair vs chiffrés

4 - LA SÉCURITÉ CHEZ SOI :

- Télétravail : chez moi je ne risque rien ?
- Mon poste de travail, une mine d'or d'informations
- Et mon mobile ?
- Où sont mes données ?
- Qui accède à mes données ?
- Comment devenir un maitre des bonnes pratiques de sécurité ?

TRAVAUX DIRIGÉS

Quizz

AF-CDPO – CERTIFICATION DATA PROTECTION OFFICER

DESCRIPTION

Depuis 2018 la RGPD est entré en vigueur afin de pouvoir mieux protéger les données personnelles. Cette règlementation change en profondeur les actions et responsabilités entre les responsables de traitement, les sous traitants et définit des principes et des droits pour chaque personne concernée. Toute entreprise se doit de se mettre en conformité vis-à-vis du RGPD. Un des moyens d'y arriver est de mettre en place un DPO qui devient aujourd'hui le garant du respect de la conformité lié à la protection de la vie privée. Cette certification permet l'acquisition et la validation des savoirs utilent pour occuper un poste de DPO.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les concepts de base et les composants de la protection des données
- Comprendre le rôle et les missions du Délégué à la Protection des Données (DPO)
- Comprendre le contenu et l'importance de la réglementation générale de la protection des données
- Comprendre les concepts, les approches, les méthodes et les techniques pour la protection efficace des données
- Comprendre comment réaliser une AIPD (Analyse d'impact à la protection des données)

PRÉREQUIS

- Connaissances du fonctionnement managérial et organisationnel d'une organisation et connaissances de base en sécurité de l'information
- Connaissances juridiques

PUBLIC CONCERNÉ

- DSI - RSSI, Risk manager - Chefs de projet sécurité, Auditeurs sécurité – Consultants sécurité, Auditeurs – DPO, Juristes

TARIF : 3 200 € HT

PROGRAMME DE LA FORMATION 1/2

1 - FONDAMENTAUX DES LOIS ET RÈGLEMENTS SUR LA PROTECTION DES DONNÉES :

- Champ d'application
- Définitions
- LIL
- RGPD
- Autres lois sur la Protection de la vie privée

TRAVAUX DIRIGÉS

Quizz

2 - LES GRANDS PRINCIPES DU RGPD :

- Licéité du traitement
- Loyauté et transparence
- Limitation des finalités
- Minimisation des données
- Exactitude des données
- Conservation limitée des données
- Intégrité, confidentialité des données

TRAVAUX DIRIGÉS

Quizz et étude de cas

3 - LA VALIDITÉ DU TRAITEMENT :

- Bases juridiques d'un traitement
- Consentements
- Catégories particulières
- Données relatives aux condamnations pénales et aux infractions

TRAVAUX DIRIGÉS

Quizz et étude de cas

4 - LES TRANSFERTS DE DONNÉES PERSONNELLES :

- Décision d'adéquation
- Garanties appropriées
- Règles d'entreprise contraignantes
- Dérogations
- Autorisation de l'autorité de contrôle
- Suspension temporaire
- Clauses contractuelles

TRAVAUX DIRIGÉS

Quizz et étude de cas

5 - LES DROITS DES PERSONNES CONCERNÉES :

- Transparence et information
- Accès, rectification et effacement (droit à l'oubli)
- Opposition
- Décisions individuelles automatisées
- Portabilité
- Limitation du traitement
- Limitation des droits

TRAVAUX DIRIGÉS

Quizz et étude de cas

PROGRAMME DE LA FORMATION 2/2

6 - ACTEURS ET AUTORITÉS DE CONTRÔLE :

- Responsable du traitement
- Sous-traitant du traitement
- DPO
- Les autorités de contrôle
- Le CEPD
- Responsabilités de chacun

7 - ANALYSE D'IMPACT SUR LA VIE PRIVÉE :

- L'appréciation des risques sur la vie privée
- L'évaluation des risques sur la vie privée
- Le traitement du risque sur la vie privée
- Le suivi et la communication des risques

TRAVAUX DIRIGÉS

Analyse des risques sur la vie privée, étude de cas

8 - MESURES À METTRE EN ŒUVRE :

- Anonymisation, pseudonymisation et chiffrement des données personnelles
- Mesures techniques
- Mesures organisationnelles
- Mesures juridiques, doctrines et jurisprudence
- Code de conduite et certification

9 - PRÉPARATION EXAMEN

AF-MSEC - LES FONDAMENTAUX DU MANAGEMENT DE LA SÉCURITÉ

DESCRIPTION

Aujourd'hui de par l'évolution de la réglementation et de la gouvernance des entreprises, la notion de maîtrise des risques est mise en avant.
Cette formation vous permettra d'appréhender les éléments fondamentaux pour mettre en œuvre un cadre et gérer un processus de management des risques. Elle donnera au RSSI ou au Risk-manager les clés pour élaborer un plan d'action et piloter sa mise en œuvre.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Maîtriser les définitions et notions essentielles de la Sécurité du SI (DICP , PDCA, SMSI...)
- Accompagner les RSSI dans leurs premiers projets de sécurité
- Comprendre les enjeux de la fonction RSSI dans une organisation

PUBLIC CONCERNÉ

- RSSI - DSI, Consultants SSI

PRÉREQUIS

- Connaissances de base en sécurité de l'information

TARIF : 900 € HT

PROGRAMME DE LA FORMATION

1 - ETAT DES LIEUX DE LA SÉCURITÉ :

- Les dernières menaces cybercriminelles
- Quelques événements marquants
- Quelques statistiques

2 - NOTIONS FONDAMENTALES DU SMSI :

- Définitions
- Les 4 critères DICP
- La logique PDCA
- L'approche par les risques
- Le soutien du management

3 - LES NORMES ISO 27000 :

- Panorama des normes ISO 27000
- La norme ISO 27001
- La norme ISO 27002
- La norme ISO 27005
- La norme ISO 27701
- Autres normes

4 - METTRE EN PLACE UNE FILIÈRE SSI :

- Rôle et missions du RSSI
- Politique de Sécurité et charte sécurité
- Déploiement des instances SSI
- Distribution des rôles de la filière SSI

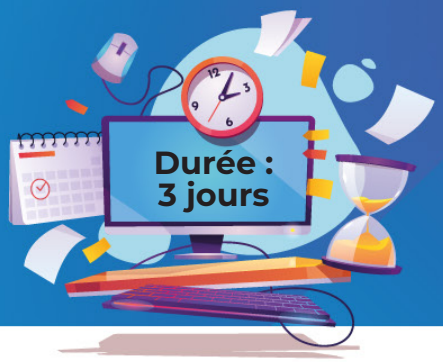
5 - PILOTER LA SSI :

- Tableaux de Bord SSI
- Audits et contrôles
- Sensibilisation des collaborateurs

6 - LES PREMIERS PROJETS SSI :

- Analyse de risques
- Contractualisation avec les tiers externes
- Gestion des habilitations
- Gestion des incidents

AF-DPO - LES ESSENTIELS DU RGPD



DESCRIPTION

Entré en vigueur le 25 mai 2018, le RGPD/GDPR (Règlement Général sur la Protection des Données) encadre le traitement des données personnelles au sein de l'Union Européenne. Pour répondre aux besoins des secteurs privés et publics le rôle du DPO devient primordial. Nous vous proposons une formation afin d'être capable de reconnaître toute donnée personnelle au sein de votre entreprise/organisation, tout en identifiant les impacts du RGPD sur votre quotidien, les obligations qui vous incombent... mais aussi les opportunités offertes !

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les principaux points clés du RGPD et leurs implications opérationnelles
- Appréhender les chantiers à mettre en place pour la mise en conformité
- Comprendre le rôle et les missions du Délégué à la Protection des Données (DPO)
- Comprendre le contenu et l'importance de la réglementation générale de la protection des données

PUBLIC CONCERNÉ

- Futur DPO -DPO Débutants, DSI – Direction, Juristes cyber - RSSI, Chefs de projet - Auditeurs

PRÉREQUIS

- Aucun – Connaitre le RGPD dans ses grandes lignes peut être un plus

TARIF : 2 300 € HT

PROGRAMME DE LA FORMATION

1 - INTRODUCTION :

- Fondamentaux juridiques
- Historique et avenir du règlement européen
- Enjeux de la protection des données personnelles

2 - QUELS SONT LES ENJEUX FONDAMENTAUX DU RGPD ?

- Champ d'application du règlement
- Principes fondamentaux
- Notions essentielles et acteurs
- Responsabilités (responsabilité du DPO, du sous-traitant, responsabilité conjointe, etc)
- Les risques de non-conformité

3 - COMMENT ASSURER LA CONFORMITÉ DE SON ORGANISME ?

- Piloter la protection des données personnelles avec un DPO
- Gérer les risques avec l'analyse d'impact (PIA : Privacy Impact Assessment)
- Cartographier avec le registre des activités de traitements
- Veiller aux données particulières (données sensibles, judiciaires, protection des mineurs, etc)
- Assurer la sécurité des données
- Gérer les droits des personnes concernées
- Veiller aux transferts de données en dehors de l'UE
- Se préparer à un contrôle
- Coopérer avec les autorités

4 - QUELS SONT LES OUTILS PERMETTANT D'ASSURER LA CONFORMITÉ ?

- Certification et codes de conduite
- Méthodologies de conformité
- Veille
- Références

AF-RSSI - LES ESSENTIELS DU RSSI

DESCRIPTION

La formation les essentiels du RSSI apporte au nouveau responsable sécurité des SI ou au nouveau manager d'un RSSI un panorama complet de ses fonctions et des attentes des organisations sur son rôle. Les connaissances indispensables à la prise de fonction du RSSI et un retour d'expérience sur les chantiers et la démarche à mettre en œuvre dans le rôle sont détaillés par des consultants expérimentés et d'anciens RSSI.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Connaître les bases pour la mise en place d'une bonne gouvernance de la sécurité des systèmes d'information
- Acquérir les connaissances techniques de base indispensables à la fonction de RSSI
- Comprendre pourquoi et comment mettre en œuvre un SMSI en s'appuyant sur la norme ISO 27001
- Connaitre l'état du marché de la sécurité informatique
- Obtenir un panorama des méthodes d'appréciation des risques
- Comprendre les enjeux de la SSI au sein des organisations
- Echanger sur les stratégies de prise de fonction et des retours d'expériences de RSSI

PUBLIC CONCERNÉ

- Nouveaux ou futurs RSSI, RSSI expérimentés, Ingenieurs en SSI, DSI - Auditeurs

PRÉREQUIS

- Expérience au sein d'une direction informatique en tant qu'informaticien ou bonne connaissance générale des systèmes d'information
- Notions de base en sécurité de l'information

TARIF : 3 300 € HT

PROGRAMME DE LA FORMATION 1/2

1 - INTRODUCTION :

- Accueil
- Présentation de la fonction de RSSI avec mise en perspective par rapport à tous les aspects de son environnement
- Production, direction, métiers, conformité, juridique, etc.

2 - ASPECTS ORGANISATIONNELS DE LA SÉCURITÉ :

- Panorama des référentiels du marché
- Politique de sécurité
- Rédaction
- Politiques globales, sectorielles, géographiques
- Conformité
- Gouvernance de la sécurité
- Indicateur sécurité
- Gestions des incidents
- Aspects techniques de la sécurité
- Sécurité du système d'exploitation
- Sécurité des applications (sessions, injections, SQL, XSS)
- Sécurité réseau (routeurs, firewalls)
- Sécurité du poste de travail

3 - L'ISO 27001 :

- Bases sur les SMSI
- Panorama des normes ISO 27000
- L'ISO 27001 et l'ISO 27002

4 - PRÉPARATION À L'AUDIT :

- Formation et communication
- Audit à blanc
- Document à préparer
- Considérations pratiques
- Réception des auditeurs (SoX, Cour des comptes, Commission bancaire...)

5 - GESTION DES RISQUES :

- L'ISO 27005
- Identification des risques
- Analyse des risques
- Evaluation des risques
- Traitements des risques
- Acceptation des risques
- Méthodologies d'appréciation des risques :
  - EBIOS -RM
  - MEHARI
  - NIST SP 800-30

6 - ASPECTS JURIDIQUES DE LA SSI :

- Informatique et libertés
- Communications électroniques
- Conservation des traces
- Contrôle des salariés
- Atteintes aux STAD
- Charte informatique
- Administrateurs

PROGRAMME DE LA FORMATION 2/2

7 - ACTEURS DU MARCHÉ DE LA SÉCURITÉ :

- Gestion des relations avec les partenaires
- Infogérance
- Prestataire en sécurité

8 - STRATÉGIES DE PRISE DE FONCTION DU RSSI :

- Rôle du RSSI
- Relations avec les métiers, la DSI, la DG, les opérationnels
- Retour d'expérience
- Questions / Réponses avec les stagiaires

AF-RSXN - RÉSEAUX INFORMATIQUES POUR NON-INITIÉS

DESCRIPTION

Cette formation vous permettra de comprendre le vocabulaire, les concepts, les technologies et les usages des réseaux. Elle vous permettra également d'apprendre les bases des réseaux informatiques et à configurer des postes de travail avec des équipements réseaux.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Connaître les différents équipements réseaux
- Appréhender les principaux services et protocoles : tcp/ip, udp, arp, http, https

Connaître les différents types de réseaux : LAN, MAN, WAN, et sans fil

Installer un réseau physique : hôtes, câbles, commutateurs, routeurs

PUBLIC CONCERNÉ

- Techniciens, toute personne souhaitant une approche très pratique et fonctionnelle des réseaux informatiques

PRÉREQUIS

- Aucun

TARIF : 1 500 € HT

PROGRAMME DE LA FORMATION

1 - INTRODUCTION :

- Le réseau fédérateur des briques du SI
- Les différents éléments et leur rôle
- Les utilisateurs et leurs besoins

2 - TYPOLOGIE DES RÉSEAUX :

- Le LAN, le MAN et le WAN
- Le modèle client/serveur

3 - LES ALTERNATIVES DE RACCORDEMENT :

- La paire torsadée
- La fibre optique
- La technologie sans fil

4 - LES RÉSEAUX LOCAUX (LAN) :

- La carte réseau. L'adressage MAC
- Le fonctionnement d'Ethernet, le CSMA/CD
- Les débits possibles
- Les réseaux locaux sans fil (802.11x)

EXERCICE PRATIQUE

Mise en place d'un réseau local avec des commutateurs et des stations de travail

5 - LE PROTOCOLE TCP/IP :

- La notion de protocole. Principes de TCP/IP
- L'architecture et la normalisation. La communication
- L'adressage IP. Le broadcast et le multicast
- Présentation de TCP et UDP.

Notion de numéro de port

EXERCICE PRATIQUE

Configurer l'adresse IP et le masque de sous-réseau sur une station de travail. Partager des données

6 - LA SÉCURITÉ CHEZ SOI :

- Mon poste de travail, une mine d'or d'informations

7 - LES RÉSEAUX WAN :

- Pourquoi et quand utiliser un WAN ?
- La nouvelle infrastructure MAN Ethernet
- Présentation de la technologie xDSL (ADSL/SDSL)

8 - LE PROTOCOLE TCP/IP :

- Pourquoi et quand utiliser un routeur ?
- Présentation des mécanismes de routage
- Notion sur les protocoles de routage RIP et OSPF
- La translation d'adresses et de ports (NAT/PAT)

EXERCICE PRATIQUE

Simuler un réseau WAN. Configurer la passerelle par défaut sur une station de travail

9 - LES SERVICES APPLICATIFS :

- Le DNS, rôle et intérêt . Notion de domaine
- Présentation de DHCP. Exemple d'utilisation
- La messagerie Internet, http et FTP. La VoIP
- De la Voix à la téléphonie

EXERCICE PRATIQUE

Configurer les stations de travail en DHCP. Transférer un fichier avec FTP. Configurer un serveur DNS

AF-SECN1 – SÉCURITÉ RÉSEAUX NIVEAU 1

DESCRIPTION

Cette formation permet d'acquérir des savoirs fondamentaux pour pouvoir intégrer une sécurisation des réseaux d'entreprises. Elle vous permettra d'identifier les enjeux de la sécurité des systèmes d'information. A l'issue de ce stage vous serez en mesure de pouvoir proposer des solutions afin de faire transiter des données sur un réseau d'entreprise en toute sécurité. Vous saurez installer et paramétrer un pare-feu approprié, installer et configurer un proxy, mettre en place un filtrage et utiliser différents outils permettant de détecter une intrusion.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les menaces qui pèsent sur les réseaux
- Maîtriser le rôle des équipements de sécurité
- Mettre en œuvre un réseau sécurisé

PUBLIC CONCERNÉ

- Techniciens et administrateurs systèmes et réseaux, Architectes sécurité – Intégrateurs sécurité et réseau, Ingénieurs sécurité – Responsables sécurité, Chefs de projet sécurité

PRÉREQUIS

- Connaissance du fonctionnement des réseaux informatiques

TARIF : 2 500 € HT

PROGRAMME DE LA FORMATION 1/2

1 - INTRODUCTION SSI :

- Le numérique en entreprise
- La convergence des réseaux
- Etat des menaces sur les réseaux en 2021
- Les typologies des attaquants
- Les outils d'attaques
- Les typologies d'attaques
- Les CVE & CVSS
- Les attaques APT
- Thu Unified Kill Chain
- Les piliers de la sécurité
- Les principes généraux de la sécurité
- La sécurité dans le cyber-espace
- Les acteurs de la cybersécurité
- La sécurité offensive

2 - LES BASES DE LA CRYPTOGRAPHIE :

- Vocabulaire
- Objectifs
- Chiffrement de César & chiffrement de Vigenère
- Principe de Kerckhoffs
- Le chiffrement symétrique
- Le chiffrement asymétrique
- Les recommandations de sécurité
- Fonction de hash

3 - VIRTUAL PRIVATE NETWORK & ACCÈS SÉCURISÉ :

- Définition
- Les implémentations VPN
- Les protocoles VPN
- IPSEC
- TLS
- Autres protocoles sécurisés : SSH

TRAVAUX PRATIQUES

Mise en place du VPN IPSec & mise en place de SSH

4 - IAM :

- Gestion des identités et des accès
- IAAA
- Les méthodes d'authentification
- Cycle de vie des accès
- Stratégie de gestion des identités
- SLDAP
- Les modèles de contrôle des accès
- Les implémentations
- Focus sur Kerberos

TRAVAUX PRATIQUES

Mise en place de Kerberos

PROGRAMME DE LA FORMATION 2/2

5 - PARE-FEU :

- Définition
- Place du pare-feu dans le modèle OSI
- Règles de pare-feu
- Pare-feu Stateless & Statefull
- Politique de filtrage
- Les limites des pare-feux traditionnels
- Les pare-feux de nouvelles générations
- Méthodologie de la mise en place d'une politique de filtrage
- Bonnes pratiques d'ordre général

TRAVAUX PRATIQUES

Etude d'une cartographie et mise en place d'une politique de filtrage

6 - PROXY :

- Définition
- Pourquoi un serveur mandataire ?
- Le filtrage URL
- Les types de proxy
- Les implémentations de proxy

TRAVAUX PRATIQUES

Mise en place d'un proxy et de règles de filtrage

7 - LES ARCHITECTURES DE PASSERELLE D'INTERCONNEXION :

- Le concept
- La passerelle d'interconnexion selon les niveaux de sécurité
- L'amélioration continue

8 - SÉCURITÉ DES ÉQUIPEMENTS RÉSEAUX :

- Administration
- Cloisonnement des réseaux
- Sécurisation des ports
- Mécanismes liés à la disponibilité
- Synchronisation horaire et horodatage
- Journalisation

TRAVAUX PRATIQUES

Durcissement de commutateurs et routeurs, mécanismes liés à la disponibilité

AF-HAC1 – ETHICAL HACKING - NIVEAU 1

DESCRIPTION

Cette formation vous permettra d'apprendre les techniques pour mesurer le niveau de sécurité de votre système d'information. Vous apprendrez à appliquer des mesures et des règles pour lutter contre le hacking et identifier le mécanisme des principales attaques.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre la méthodologie du hacker
- Apprendre le vocabulaire lié au Hacking
- Mettre en pratique le cycle de l'attaquant
- Rédiger un rapport de pentest

PUBLIC CONCERNÉ

- Techniciens et administrateurs systèmes et réseaux, architectes sécurité – Intégrateurs sécurité, personnes étudiant la cybersécurité, responsables sécurité – Auditeurs sécurité

PRÉREQUIS

- Connaissances en réseaux et systèmes Windows et Linux
- CISR1

TARIF : 3 000 € HT

PROGRAMME DE LA FORMATION 1/2

1 - PRINCIPE DU HACKING :

- Définition
- Typologie des attaquants
- Vocabulaire

2 - MÉTHODOLOGIE DU HACKING :

- PTES
- OWASP
- OSSTMM
- Red Team / Blue Team
- Kill Chain unified

3 - PRÉPARATION AUDIT + RAPPORT

- Contrat
- Contexte et périmètre
- Lois
- La trousse à outil d'un pentesteur
- Mise en place dans le cloud
- Comment s'organiser un rapport

4 - VECTEURS D'ATTAQUE :

- Virus / ver / cheval de Troie
- Blackdoor
- Logiciel espion / Keylogger
- Exploit
- Rootkit
- Ransomware
- Pourriel / Hameçonnage / Canular informatique
- Spearphishing
- Botnet
- Scanner de réseaux et de failles

5 - OSINT :

- Présentation OSINT
- Méthodologie OSINT
- Exemple : Google dorks/recherche d'emails/recherche de sous-domaine

6 - RECONNAISSANCE ACTIVE :

- Principe
- Méthodologie
- Pratique : Nmap, métasploit, scapy

7 - VULNÉRABILITÉS :

- MITRE ATT&CK
- Scanner de vulnérabilités
- Social ingénierie
- CVE

8 - TYPOLOGIE DES ATTAQUES :

- Exploitation réseau (MITM)
- Social ingénierie/Pishing/deepfake
- Server side (Exploit CVE, Cracking + Bruteforce)

9 - HACKING WEB & APPLICATION WEB :

- Principe
- Méthodologie
- Typologie d'attaque : Client side, Back side

10 - FRONT SIDE :

- Top10 OWASP
- Exploitation de failles

PROGRAMME DE LA FORMATION 2/2

11 - ATTAQUE AVANCÉE :

- Création de Payload
- Customiser ses exploits
- Mise en œuvre du Pivoting
- Exploitation Browser

12 - POST-EXPLOITATION :

- Mise en œuvre de technique d'exfiltration
- C&C
- Les élévations de privilège
- Effectuer une énumération locale
- Effacer ses traces

13 - RAPPORT :

- Exemple de rapport
- Etude d'un rapport
- Communication et résultats

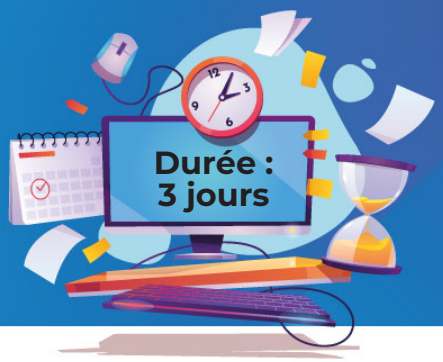
14 - MISE EN SITUATION :

- Pentest d'un lab
- Rédaction du rapport

15 - FOCUS SUR DES TECHNIQUES SPÉCIFIQUES

- Hack Wifi
- Hack Cloud
- Hack IoT
- Hack Mobile

AF-DEV1 – SÉCURITÉ DU DÉVELOPPEMENT DE NIVEAU 1



DESCRIPTION

La forte digitalisation de notre société voit une profonde évolution du WEB et de l'Industrie. Tout est connecté et controlé via une application web, mobile ou non. Cette formation permet d'acquérir les compétences nécessaires pour aborder le développement sécurisé.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Identifier les vulnérabilités les plus courantes des applications Web
- Comprendre le déroulement d'une attaque
- Tester la sécurité de ses applications Web
- Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS
- Mettre en place des mesures de sécurisation simples pour les applications Web

PUBLIC CONCERNÉ

- Administrateurs réseaux, systèmes Webmasters, auditeurs sécurité, chefs de projet développement sécurité

PRÉREQUIS

- Connaissances de base en systèmes, réseaux et d'internet
- Maitriser les fondamentaux de la programmation
- Connaissances d'un langague de programmation

TARIF : 1 850 € HT

PROGRAMME DE LA FORMATION 1/2

1 - INTRODUCTION :

- Présentation des normes et efforts de standardisation
- Importance de la sécurité du développement
- Rgpd et sécurité du développement
- Security by design
- Security by default
- Les acteurs

EXERCICE PRATIQUE

Quizz

2 - MÉTHODOLOGIES :

- Principes SecDevOps
- Architectures associées
- DREAD et STRIDE
- SSDLC
- BSSIM
- OWASP
- Analyse de risques

TRAVAUX DIRIGÉS

Réalisation d'une analyse de risques

3 - COMPRÉHENSION DES VULNÉRABILITÉS ET EXPLOITATIONS ASSOCIÉES :

- Typologie des menaces le top 10 OWASP
- Failles applicatives
- Attaques côté client
- Gestion de session et authentification
- Failles de configuration
- Attaques de type DDOS
- Attaque Buffer-Overflow, XXE

TRAVAUX DIRIGÉS

Etude top 10 owasp

4 - SÉCURISER SON ARCHITECTURE

- Firewalls n-tier, outils
- Filtres des requêtes HTTP Rappel algorithmique
- Autorités de certification
- Chiffrement de données
- Protocoles

TRAVAUX PRATIQUES

Sécurisation d'un serveur, certificat, waf, authentification

5 - SÉCURISER SON CODE :

- Protections basiques
- Usurpation d'identité
- Se protéger des attaques client
- Se protéger contre CSRF
- Sécurité d'accès au SGBD
- Protections contre les attaques de force brute, liste de contrôle d'accès
- Cheat cheat

TRAVAUX PRATIQUES

Protection d'un code vulnérable

PROGRAMME DE LA FORMATION 2/2

6 - AUDITS ET TESTS DE SÉCURITÉ :

- Les types d'audits
- Tester la robustesse
- Apprendre à connaitre son architecture
- Organiser une veille technologique
- Tests statique vs dynamique

TRAVAUX DIRIGÉS

Réalisation d'une analyse de risques

7 - VUE SUR LA SÉCURITÉ DES APPLICATIONS MOBILES :

- Composants et contexte
- Taxonomie des risques
- Les principales menaces et attaques
- Principes de sécurisation

TRAVAUX PRATIQUES

Attaque sur application Android

AF-FON1 – ANALYSTE FORENSIQUE - NIVEAU 1

DESCRIPTION

Les cyber attaques font parties du lot quotidien du monde de l'entreprise et du numérique. Il devient alors vital de pouvoir investiguer sur le cyber crime et retrouver tous les éléments utiles pour réagir et être recevable devant la loi.
Cette formation vous permettra de comprendre le forensique, de savoir investiguer avec méthodologie pour collecter, analyser et préserver les preuves et ainsi améliorer la sécurité de votre SI.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre le forensique et ses enjeux.
- Savoir mener une investigation forensique avec méthodologie.
- Prendre en main les outils de l'analyse forensique.
- Pratiquer les différents aspects de l'analyse forensique.

PUBLIC CONCERNÉ

- Administrateurs système et réseau, ingénieurs système et réseau, développeurs ayant des bases, responsables Sécurité, responsables Gestion des incidents, analystes Incident de sécurité.

PRÉREQUIS

- Connaissances des bases des réseaux
- Connaissances des bases systèmes Linux et Windows
- Connaissances des bases de la SSI
- Quelques connaissances en développement peuvent être un plus

TARIF : 2 500 € HT

PROGRAMME DE LA FORMATION 1/2

1 - INTRODUCTION DE LA SSI :

- Le numérique en entreprise
- Les risques qui pèsent sur les entreprises

2 - DIGITAL FORENSIQUE :

- Le Forensique & le « Digital Forensics »
- Comment est apparu le Digital Forensic
- Les enjeux du forensique pour une entreprise aujourd'hui
- Mener une investigation forensique : La méthodologie

3 - L'ANALYSE FORENSIQUE RÉSEAU :

- Les cas d'utilisation de la forensique en réseau
- Les types de sources de données
- Les équipements sur lesquels collecter les sources de données
- Les protocoles réseau à surveiller
- Les traces laissées par une attaque sur le réseau (exemple d'une attaque)
- Boîte à outils de criminalistique réseau

TRAVAUX PRATIQUES

Prise en main de WIRESHARK et étude de PCAP

4 - L'ANALYSE FORENSIQUE DES JOURNAUX :

- L'utilité de l'analyse des journaux
- Les types de journaux
- L'importance de l'horodatage
- L'analyse des journaux traditionnels
- Les outils de l'analyse des journaux traditionnels
- L'analyse des journaux moderne : Les SIEM
- Les éditeurs de SIEM
- La méthodologie de l'analyse des journaux

TRAVAUX PRATIQUES

Prise en main de Kibana et analyse forensique des journaux dans la pratique

5 - L'ANALYSE FORENSIQUE MÉMOIRE :

- Qu'est-ce que l'analyse mémoire ?
- Pourquoi faire une analyse mémoire ?
- Faire un dump mémoire : Les outils
- La méthodologie de l'analyse mémoire

TRAVAUX PRATIQUES

Prise en main de volatility et analyse de dump de systèmes infectés

PROGRAMME DE LA FORMATION 2/2

6 - L'ANALYSE DE DISQUE DUR :

- Qu'est-ce que l'analyse de disque dur ?
- Pourquoi faire une analyse du disque dur ?
- Faire une copie du disque dur : Les outils
- Les systèmes des fichiers
- La méthodologie de l'analyse de disque dur

TRAVAUX PRATIQUES

Prise en main d'Autopsy et analyse de disque dur Windows et Linux

7 - L'ANALYSE DE FICHIER :

- Qu'est-ce que l'analyse de fichiers ?
- Pourquoi faire une analyse de fichiers ?
- Les types de fichiers
- Anatomie d'un des types de fichiers
- La méthodologie de l'analyse de fichier
- Les outils

TRAVAUX PRATIQUES

Analyse de fichiers malveillants

AF-FORX – ANALYSTE FORENSIQUE RÉSEAUX

DESCRIPTION

Aujourd'hui, l'informatique est devenu centré sur le réseau. Les cyber attaques font parties du lot quotidien et il devient nécessaire de pouvoir investiguer sur le cyber crime. Cette formation vous permettra de pratiquer les défférents outils de l'analyse forensique.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre le forensique et ses enjeux.
- Savoir mener une investigation forensique avec méthodologie.
- Prendre en main les outils de l'analyse forensique.
- Pratiquer les différents aspects de l'analyse forensique.

PUBLIC CONCERNÉ

- Administrateurs système et réseau, ingénieurs système et réseau, développeurs ayant des bases, responsables Sécurité, responsables Gestion des incidents, analystes Incident de sécurité.

PRÉREQUIS

- Connaissances des bases des réseaux
- Connaissances des bases systèmes Linux et Windows
- Connaissances des bases de la SSI
- Quelques connaissances en développement peuvent être un plus

TARIF : 2 500 € HT

PROGRAMME DE LA FORMATION

1 - INTRODUCTION AU FORENSIQUE RÉSEAU :

- Relation avec les autres domaines de la forensique.
- Les différents types de preuves
- Relation avec les NIDS/IPS
- Collecte de preuves
- Outils

TRAVAUX PRATIQUES

Analyse attaques avec wirershark, Règles NIDS/IPS, Collecte de preuves

2 - JOURNALISATION ET SURVEILLANCE :

- Principes
- Conditions préalables pour l'analyse
- Analyse de la chronologie
- Agrégation et corrélation des sources
- Collecte et stockage du trafic
- Principes juridiques

TRAVAUX PRATIQUES

Collecte et analyse de logs, réalisation de timelines de preuves

3 - DÉTECTION :

- Distinguer le trafic malveillant
- Détecter les intrusions
- Threat intellingence

TRAVAUX PRATIQUES

Mise en situation d'intrusions, détection et mise en place de modèles

4 - ANALYSE / INTERPRÉTATION DES DONNÉES :

- Méthodologie
- Vue d'ensemble
- Chaine de contrôle
- Rapports
- Leçons apprises
- Amélioration continue

TRAVAUX PRATIQUES

Analyser un environnement compromis. Rapport, analyse

AF-DET1 - DÉTECTION D'INTRUSION & SOC

DESCRIPTION

Cette formation vous permettra d'identifier et de comprendre les techniques d'analyse et de détection. Ce cours présente les techniques d'attaque les plus évoluées. Vous pourrez acquérir les connaissances pour déployer différents outils de détection d'intrusion et mettre en œuvre les solutions de prévention. Vous apprendrez également les concepts et l'environnement d'un SOC.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Identifier et comprendre les techniques d'analyse et de détection
- Acquérir les connaissances pour déployer différents outils de détection d'intrusion
- Mettre en œuvre les solutions de prévention et de détection d'intrusions
- Comprendre les concepts et l'environnement d'un SOC
- Savoir utiliser les outils d'analyse

PUBLIC CONCERNÉ

- Ingénieurs/Administrateurs systèmes et réseaux, Responsables de la sécurité, Analyste SOC/ Forensique, toute personne qui respecte les prérequis.

PRÉREQUIS

- Bonnes connaissances des réseaux et des systèmes (Windows & Linux)
- Bonnes connaissances en sécurité informatique

TARIF : 2 500 € HT

PROGRAMME DE LA FORMATION 1/2

1 - SYSTÈME DE JOURNALISATION :

- Prérequis à la mise en place d'un système de journalisation
- Architecture et conception d'un système de journalisation
- Introduction à la détection des incidents de sécurité

2 - INTRUSION DETECTION/PREVENTION SYSTEM :

- Définition et terminologie
- Les objectifs d'un IDS/IPS
- Le fonctionnement d'un IDS/IPS
- Le NIDS/NIPS dans une architecture réseau
- Les différentes solutions IDS/IPS
- Les règles NIDS/NIPS

3 - SECURITY INFORMATION AND EVENT MANAGEMENT :

- Définition et terminologie
- Les objectifs d'un SIEM
- Le fonctionnement d'un SIEM
- Les règles SIEM (Alerte, Sigma, ...)
- Le SIEM dans une architecture réseau
- Les différentes solutions SIEM
- Etude d'une solution SIEM

4 - ENDPOINT DETECTION AND RESPONSE :

- Définition et terminologie
- Les objectifs d'un EDR
- Le fonctionnement d'un EDR
- Les règles EDR (Alerte, Yara, ...)
- Les différentes solutions EDR
- Etude d'une solution EDR

5 - HONEYPOT :

- Définition et terminologie
- Les objectifs d'un Honeypot
- Le fonctionnement d'un Honeypot
- Les différentes solutions Honeypot
- Etude d'une solution Honeypot

6 - ANALYSE RÉSEAU : WIRESHARK :

- Les objectifs de Wireshark
- Le fonctionnement de Wireshark
- Personnalisation des menus
- Analyse de flux malveillants

7 - SECURITY OPERATIONS CENTER :

- Introduction SOC
- Objectifs d'un SOC
- Services et fonctions d'un SOC
- Structure d'un SOC

PROGRAMME DE LA FORMATION 2/2

8 - MISE EN PLACE D'UN SOC :

- Définir son projet SOC
- Architecture du SOC
- Les outils du SOC
- Sélectionner et collecter les bonnes données
- Les SLA, indicateurs et reporting
- Etape BUILD
- Etape RUN

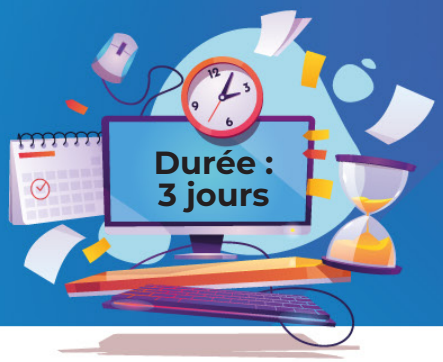
9 - LA RÉPONSE À INCIDENT :

- Qu'est-ce que le traitement des incidents ?
- Préparation
- Détection et analyse
- Confinement, éradication et récupération
- Activité Post-Incident

10 - INTRODUCTION CYBER THREAT INTELLIGENCE :

- Définition et terminologie
- Les objectifs de la CTI
- L'importance de la CTI dans un SOC

AF-JUSE - JUNIPER, SÉCURITÉ RÉSEAUX



DESCRIPTION

Au travers de cette formation vous apprendrez à mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux avec l'aide de routeurs pare-feu Juniper. Vous serez en mesure de concevoir une architecture de sécurité en apprenant le rôle des équipements de sécurité dans la protection de l'entreprise.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Mettre en œuvre des politiques de sécurité Juniper
- Mettre en œuvre la translation d'adresse IP avec Juniper
- Déploiement d'un tunnel IPSEC site à site avec Juniper
- Comprendre les fonctionnalités de Screen

PUBLIC CONCERNÉ

- Administrateurs système et réseau, Techniciens système et réseau.

PRÉREQUIS

- Bonnes connaissances en réseaux et systèmes

TARIF : 2 000 € HT

PROGRAMME DE LA FORMATION

1 - CYBERSÉCURITÉ :

- Définitions et terminologies
- Les piliers de la cybersécurité
- Les menaces

2 - PARE-FEU & POLITIQUE DE FILTRAGE :

- Définitions et terminologies
- Méthodologie politique de filtrage
- Politique de sécurité Juniper
- Critères d'action

3 - NETWORK ADDRESS TRANSLATION :

- NAT/PAT
- Les typologies NAT dans Juniper
- Architecture JunOS
- Les priorités

4 - SCREEN :

- Définitions et terminologies
- Attaque par déni de service
- Paquets suspects ou anormaux
- Reconnaissance réseau
- Les profils Screen

5 - VPN IPSEC :

- Définitions et terminologies
- Fonctionnement du protocole IPSEC
- La mise en place dans Juniper

AF-CHEP - CHECKPOINT R81, SÉCURITÉ RÉSEAUX

DESCRIPTION

Cette formation vous permettra d'acquérir toutes les connaissances pour démarrer, configurer et gérer les opérations quotidiennes de Check Point. Notamment comment mettre en place et gérer une politique de sécurité unifiée ainsi que des politiques de sécurité partagées.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Installer et configurer CheckPoint R81
- Mettre en œuvre une politique de sécurité
- Mettre en œuvre l'examen et le filtrage des logs
- Déployer un tunnel VPN IPSEC avec Checkpoint

PUBLIC CONCERNÉ

- Administrateurs système et réseau, Ingénieurs système et réseau, Techniciens, Responsable Sécurité.

PRÉREQUIS

- Connaissances des bases des réseaux.
- Connaissances des bases systèmes Linux et Windows.
- Bonnes connaissances de TCP/IP.

TARIF : 2 500 € HT

PROGRAMME DE LA FORMATION

1 - INTRODUCTION À LA TECHNOLOGIE CHECK POINT :

- 1 – Concept d'un pare-feu
- 2 – Contrôle du trafic réseau
- 3 – Introduction au système d'exploitation Gaia
- 4 – Check Point Security Management
- 5 – Communication réseau
- 6 – SmartConsole
- 7 – Application SmarConsole
- 8 – Plateformes de déploiement
- 9 – Considération sur le déploiement

2 - GESTION DE LA POLITIQUE DE SÉCURITÉ :

- 1 – Introduction
- 2 – Package Policy
- 3 – Installation Package Policy
- 4 – inspection HTTPS
- 5 – Translation d'adresse
- 6 – Administration
- 7 – Gestion des passerelles distante
- 8 – Sauvegarde

3 - POLICY LAYERS :

- 1 – Concept Policy Layers
- 2 – Contrôle d'accès PL
- 3 – Prévention des menaces PL

4 - SOLUTIONS ET LICENCES CHECK POINT :

- 1 – Architecture Software Blades
- 2 – Vue d'ensemble des licences
- 3 – Smart Update
- 4 – Gestion des licences

5 - VISIBILITÉ DU TRAFIC :

- 1 – Analyse des logs
- 2 – Surveillance du trafic et des connexions

6 - VPN :

- 1 – Introduction VPN
- 2 – Déploiement VPN
- 3 – Communauté VPN
- 4 – Contrôle d'accès connexion VPN
- 5 – Gestion et surveillance des tunnels

7 - GESTION DES ACCÈS UTILISATEURS :

- 1 – Vue d'ensemble des composants de la gestion des utilisateurs
- 2 – Identity Awareness
- 3 – Gestion des utilisateurs
- 4 – Authentification des utilisateurs
- 5 – Gestion des accès utilisateurs

AF-SPLU - COLLECTE ET ANALYSE DE LOG SPLUNK

DESCRIPTION

Splunk, numéro un sur son marché, propose aux administrateurs systèmes et réseaux un panel d'outils et des fonctionnalités aussi variées que performantes. Cette formation vous permettra de comprendre les concepts Splunk, d'écrire des requêtes de recherche, appliquer les différentes techniques de visualisation, comprendre comment utiliser Splunk pour analyser et surveiller les systèmes, savoir configurer les alertes et les rapports.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Être capable de comprendre les concepts Splunk Utilisateur et Splunk Administrateur
- Apprendre à installer Splunk
- Pouvoir écrire des requêtes de recherche simple dans les données
- Savoir appliquer les différentes techniques de visualisation de données en utilisant les graphes et tableaux de bord
- Être en mesure d'implémenter Splunk pour analyser et surveiller les systèmes
- Comprendre comment écrire des requêtes avancées de recherche dans les données
- Savoir configurer les alertes et les rapports

PUBLIC CONCERNÉ

- Administrateurs système et réseaux

PRÉREQUIS

- Connaissance de base des réseaux et des systèmes

TARIF : 1 400 € HT

PROGRAMME DE LA FORMATION 1/2

1 - INTRODUCTION À SPLUNK :

- Qu'est-ce que Splunk ?
- Qu'est-ce qu'une donnée ?
- Comment fonctionne Splunk ?
- Comment déployer Splunk ?
- A quoi servent les applications Splunk ?
- Quelles solutions pour améliorer Splunk ?

2 - COMPOSANTS SPLUNK :

- Les Forwarders
- L'indexeur
- Les Search Heads
- Les modèles de déploiements

3 - OBTENIR DES DONNÉES :

- Processus temporel de l'index de Splunk
- Types des saisies de données et métadonnées par défaut
- Ajouter une entrée avec Splunk Web
- Définir le type de source, paramétrage et résumé

4 - LES RECHERCHES BASIQUES :

- Assistant de recherche
- Affichage des résultats de la recherche
- Les plages de temps : sélectionner, abréviation, gérer la chronologie
- Contrôle et enregistrement des panneaux de recherche. Affichage de l'historique

5 - UTILISER DES CHAMPS DE RECHERCHE :

- Que sont les champs ? Découverte, spécificité et description, utilisation
- La fenêtre FIelds
- Distinction entre != et NOT
- Les différents modes de recherche

6 - LES MEILLEURS PRATIQUES :

- Bonne pratique de recherche
- Travailler avec des index

7 - LE LANGAGE DE RECHERCHE SPLUNK :

- Syntaxe de la langue de recherche
- Pipeline de recherche, la rendre plus lisible
- Création d'un tableau et ses champs
- Utilisation des commandes Fields, Dedup, Sort

8 - LES COMMANDES DE TRANSFORMATION :

- Commande Top (unique et multiple)
- Commande Rare
- Commande Stats : Opérations statistiques
- Mise en forme des tableaux stats

PROGRAMME DE LA FORMATION 2/2

9 - CRÉATIONS DE RAPPORTS ET DE TABLEAUX DE BORD :

- Que sont les rapports ? Les nommer intelligiblement, création à partir d'une recherche
- Exécuter des rapports, les modifier
- Création de tableaux et des visualisations
- Modifier la visualisation
- Ajouter un rapport à un tableau de bord, le modifier, l'exporter, le définir par défaut

10 - LES PIVOTS ET LA PRÉPARATION DE LA DONNÉE :

- Ouvrir un pivot, sélectionner la plage horaire, diviser les lignes, l'ajouter au tableau de bord
- Organiser les résultats, les visualiser

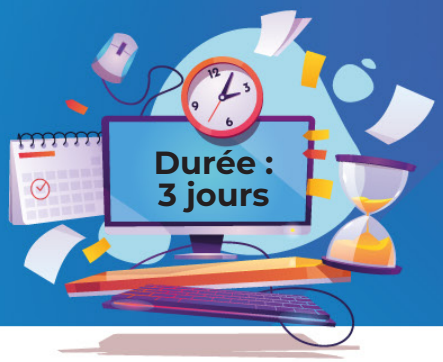
11 - CRÉATION ET UTILISATION DE LOOKUPS :

- Qu'est-ce que lookup ? Exemple de fichier
- Créer lookup, ajout d'un nouveau fichier dans la table de lookup
- Utilisation de lookup automatique
- Commande inputlookup et lookup
- Création d'une définition de lookup
- Options avancées, lookup basés sur le temps

12 - CRÉATION DE RAPPORTS ET ALERTE PROGRAMMÉE :

- Création d'un rapport programmé, planifié, programme
- Gestion des rapports : modifier les autorisations, les intégrer
- Création d'une alerte, définir les autorisations
- Alerte en temps réel ou planifiée
- Définir les conditions des déclencheurs

AF-KUBO - KUBERNETES, MISE EN OEUVRE



DESCRIPTION

Cette formation vous permettra de comprendre le positionnement de Kubernetes et la notion d'orchestration. Vous apprendrez à déployer un cluster Kubernetes et comment définir les bonnes pratiques pour travailler avec Kubernetes.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre le positionnement de Kubernetes et la notion d'orchestration
- Installer Kubernetes et ses différents composants
- Utiliser les fichiers descriptifs YAML
- Définir les bonnes pratiques pour travailler avec Kubernetes

PUBLIC CONCERNÉ

- Développeurs, Architectes, Ingénieurs de production, Administrateurs

PRÉREQUIS

- Administration système Linux
- Connaissances générales en conteneurisation (Docker ou CoreOS)

TARIF : 2 100 € HT

PROGRAMME DE LA FORMATION 1/2

1 - DU MONOLITHE AUX MICRO-ONDES :

- Inconvénient d'application monolithe
- Le micro-service moderne
- Comment fonctionne Splunk ?
- Refactoring : défi et implication

2 - CONTENEUR & ORCHESTRATEUR :

- Qu'est-ce qu'un conteneur ?
- Qu'est-ce que l'orchestration de conteneur ? Exemples et outils de déploiement

TRAVAUX PRATIQUES

Utilisation basique de Docker

3 - KUBERNETES :

- Origine de Kubernetes / K8S
- Fonctionnalités principales
- Pourquoi utiliser Kubernetes ?
- Utilisateurs sur le marché

4 - ARCHITECTURE KUBERNETES :

- Le control plane
- Le compute machines
- Les autres composants essentiels

5 - INSTALLATION DE KUBERNETES :

- Principaux types d'installation
- Infrastructure pour l'installation
- Installation en localhost, on-premise, cloud
- Outils et ressource pour l'installation
- Installation sous Windows

6 - MINIKUBE :

- Installation de Minikube, conditions nécessaires

TRAVAUX PRATIQUES

Mise en pratique de Minikube

7 - ACCÉDER À KUBERNETES :

- Présentation des Méthodes d'accès à Kubernetes
- Le client kubectl
- L'interface Web UI
- Serveurs APIs

TRAVAUX PRATIQUES

Mise en œuvre de Kubectl et GUI

8 - LES MODULES DE BASE :

- Modèle d'objet Kubernetes
- Pods, Labels, ReplicationControllers
- Deployement, namespaces

TRAVAUX PRATIQUES

Déploiement des modules

PROGRAMME DE LA FORMATION 2/2

9 - AUTHENTIFICATION, AUTORISATION, CONTRÔLE D'ADMISSION :

- Les étapes du contrôle d'accès
- Authentification (utilisateurs et compte de service), les modules impliqués
- Modèle d'autorisation
- Politique de contrôle d'admission

TRAVAUX PRATIQUES

Authentification et Autorisation

10 - SERVICES :

- Connection des utilisateurs ou applications à des pods
- Exemple d'objet de service
- Le Kube-Proxy
- Service Discovery
- Service Type : ClusterIP & NodePort, Load-Balancer, ExternalIP, ExternalName

TRAVAUX PRATIQUES

Déploiement d'application Stand-Alone

11 - VOLUMES MANAGEMENT :

- Qu'est-ce qu'un volume ? Son objectif ?
- Type de volume
- PersistantVolumes et
- PersistantVolumeClaims
- Container Storage Interface (CSI)

TRAVAUX PRATIQUES

Volume hostPath, ConfigtMaps & Secrets

12 - INGRESS :

- Qu'est-ce qu'Ingress ? Exemple de définition dans le code et de définition des règles
- Ingress Controller : contrôles d'entrée, proxy...

TRAVAUX PRATIQUES

Ingress

13 - NOTIONS AVANCÉES :

- Les annotations, Quota & Limits Management
- Autoscaling
- Jobs et CronJobs
- DaemonSets
- StatefulsSets
- Custom Resources
- Kubernetes Federation
- Security Contexts & Pods Security Policies
- Politiques réseau
- Surveillance et journalisation
- Helm
- Service Mesh

TRAVAUX PRATIQUES

Déploiement d'un cluster

14 - COMMUNAUTÉ :

- Popularité, réunions hebdomadaires et groupes de rencontres
- Stack Channels and Mailing Lists
- Evènements CNCF

AF-CCESS – LES ESSENTIELS DU CLOUD COMPUTING

DESCRIPTION

Dans tous les secteurs d'activité, le Cloud fait l'objet de toutes les attentions mais de nombreuses questions se posent encore. Découvrez dans ce séminaire tout ce que vous devez savoir sur cette technologie.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Découvrir ce qu'est le Cloud Computing
- Comprendre comment mener un projet de Cloud Computing
- Identifier les impacts structurels et ceux liés à la sécurité de la DSI
- Évaluer les apports du Cloud pour l'entreprise
- Identifier les principales offres Cloud du marché
- Intégrer les enjeux managériaux, organisationnels et techniques dans la DS
- Connaître les possibilités des solutions de cloud, ainsi que les contraintes de mise en œuvre
- Connaître les différents types de Cloud
- Identifier les technologies concernées par le Cloud
- Anticiper les impacts directs et indirects du Cloud sur l'entreprise et son système d'informations

PUBLIC CONCERNÉ

- Architecte SI, Chef de projet, Responsables DSI

PRÉREQUIS

- Connaissance de base en sécurité de l'information
- QCM de 15 questions à réaliser en amont de la formation

TARIF : 1 600 € HT

PROGRAMME DE LA FORMATION 1/2

1 - DÉFINITION OPÉRATIONNELLE DU CLOUD COMPUTING

- Concept et définition opérationnelle
- Cinq apports essentiels qui font le succès du Cloud
- Quatre technologies fondamentales des plateformes Cloud, définies par le NIST
- Classification générique des Clouds : IaaS, PaaS, SaaS, PBaaS, XXaaS
- Déploiement du Cloud : public, privé, hybride, virtuel, communautaire
- Définitions opérationnelles des Cloud selon leurs usages : moteurs d'application (SaaS), d'externalisation d'infrastructures (IaaS), de développement d'applications (PaaS), d'infogérance, de « managed services »

2 - TECHNOLOGIES DE RÉFÉRENCE DES PLATES-FORMES DE CLOUD

- Architecture technique du Cloud : Microservices/Apps et API
- Deux composants essentiels du Cloud : Openstack et Cloud Foundry
- Technologies de l'OpenStack : 6 composants principaux et le socle de l'écosystème
- Technologies du Cloud Foundry et ses composants logiciels pour le développement et le déploiement des applications (IaC, Devops, Docker ...)
- Conception d'une plateforme générique de Cloud à partir des composants techniques de l'écosystème
- Architecture opérationnelle de bout en bout d'un Cloud

3 - NIVEAU DE PERFORMANCE D'UNE PLATE-FORME CLOUD IAAS

- Infrastructure virtuelle pour déployer le système informatique des entreprises
- Architecture de stockage et de traitement distribués pour déployer le Big Data
- Solutions complètes pour déployer l'Internet des Objets (télémétrie, IoT, M2M...)
- Architecture pour le déploiement de la Blockchain
- Dispositifs pour exploiter l'Intelligence artificielle et la Machine Learning
- Métrique de management : qualité d'usage, respect des standards, risques...

4 - NIVEAU DE SÉCURITÉ D'UNE PLATEFORME CLOUD IAAS

- Sécurité conventionnelle recommandée par le CSA (Cloud Sécurité Alliance) : Firewall, NGFW, IDS/IPS...
- Sécurité opérationnelle et architecturale du Cloud
- Solutions techniques de sécurité de base pour protéger les données, éviter l'escalade de privilège dans le cadre de la virtualisation, d'intégrité des applications...
- Solutions faisant appel aux Software Defined Security, Self Healing, IA et Machine Learning, informatique quantiquecloud

PROGRAMME DE LA FORMATION 2/2

5 - PLATEFORMES MAJEURES CLOUD PUBLIC DU MARCHÉ

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- IBM
- Particularité et différence de chaque plateforme
- Positionnement concurrentiel

6 - MIGRATION DES APPLICATIONS DANS LE CLOUD PUBLIC

- Adoption d'une stratégie Cloud public
- Questions à se poser avant le déploiement pour valider la démarche, les risques, la sécurité et la confidentialité
- Facteurs clés de succès
- Causes d'échec et risques
- Détermination du SLA (Service-level agreement) et PLA (Privacy-level agreement)
- Référentiels et normes sur lesquels s'appuyer pour la migration
- Exemple de cas de migration

7 - IMPACTS ET GRANDES TENDANCES

- Cloud, la partie virtuelle des solutions et équipements informatiques de l'entreprise
- Impacts sur les compétences des équipes informatiques et sur l'organisation de la DSI
- Opportunités pour bâtir des activités nouvelles
- Fusion naturelle du Cloud public (SI d'entreprise) et le Cloud public ?

8 - CLOUD PRIVÉ VERSUS CLOUD HYBRIDE

- La définition du Cloud Computing privé.
- Différences avec Data Center et Compute Grid.
- Bases et principales technologies de virtualisation.
- Les outils Open Source. Les technologies propriétaires. Les grandes familles de Clouds privés.
- Quels défis pour la réalisation d'un vrai Cloud privé ? Infrastructures IT convergentes.
- Pourquoi le Cloud privé ne prend-il vraiment tout son sens qu'en mode hybride ?
- Quels défis pour mettre en place une solution hybride ?
- Quelles solutions aujourd'hui pour des Clouds hybrides ? Cloud ou VDC ?
- Les solutions techniques pour le Cloud.
- Les bases de données pour le Cloud. Utilisation.
- Émergence des bases de données NoSQL et RDBMS. Fondements des bases de données RDBMS et NoSQL.
- Possibilités et limites des SGBDR.
- Principales bases de données NoSQL utilisées pour le Cloud (MongoDB Cassandra, CouchDB, Hadoop).
- Les plateformes du marché IaaS (Amazon EC2 et S3). Les plateformes du marché PaaS (Amazon SQS, SimpleDB...).
- RunMyProcess.com, Cordys, Facebook, Twitter...

AF-CYB1 - CYBERCRIMINALITÉ : FAIRE FACE À LA MENACE

DESCRIPTION

La cybercriminalité est une menace touchant toutes les sociétés, organisations ou administrations. Les cybercriminels agissent de n'importe où pour vous attaquer. Ce cours permet de détecter, de se préparer, d'anticiper et de gérer les cybercrises.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Connaître les dangers et identifier les sources de menaces
- Comprendre les risques et les enjeux de sécurité
- Détecter les intrusions et réagir face aux malveillances
- Savoir organiser une riposte efficace, utile et graduée
- Planifier son plan de crise face à la cyberguerre

PUBLIC CONCERNÉ

- RSSI, Fonction SSI, Direction générale, DSI, Juristes

PRÉREQUIS

- Connaissance de base en sécurité de l'information
- QCM de 15 questions à réaliser en amont de la formation

TARIF : 1 200 € HT

PROGRAMME DE LA FORMATION 1/2

1 - CYBERCRIMINALITÉ DANS L'ACTUALITÉ

- Données sensibles : cyber vols, espionnage.
- Nouvelle guerre froide Est/Ouest, USA/Chine.
- Dénis de services d'envergure mondiale.
- Hackers organisés, rôle des agences de renseignements.
- Actualité : malwares, bots/botnets, ransomwares.
- APT (Advanced Persistant treat), infractions aux CB, skimming

2 - DÉTECTER LES INTRUSIONS

- Gestion des traces, preuves, enregistrements.
- Détecter une activité anormale, signaler un incident.
- Analyse et corrélation d'évènements de sécurité (SIEM).
- Pertinence du SOC (Security Operation Center).
- Automatiser la gestion des incidents.
- Tests d'intrusion, mesure d'anticipation incontournable.
- Recourir à une société spécialisée de détection des incidents

3 - ORGANISATION DE LA RIPOSTE

- Recherche et collecte de preuves.
- Déclarer un incident, préparer sa communication de crise.
- Rôle des CERTs.
- Cellule de crise : organiser, gestion de la crise.
- Gestion des vulnérabilités et patch management.

4 - ORDRE ÉTATIQUE FACE À LA CYBERCRIMINALITÉ

- Cyber délits (France, Europe) : quel dispositif répressif ?
- Rôle de l'ANSSI (France) et de l'ENISA (Europe).
- Gestion de la preuve : recevabilité, collecte sur Internet.
- Directive européenne Network and Information Security (2018).
- Règlement Européen « cyber security Act » (2019).
- Loi de Programmation Militaire (2016).
- Rôle des états et de l'Europe : lois, directives et règlements.

PROGRAMME DE LA FORMATION 2/2

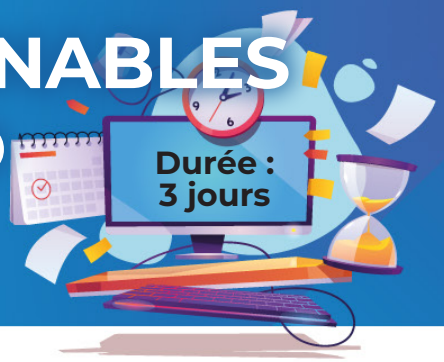
5 - LES BONNES PRATIQUES TYPES OIV / OSE

- Gouvernance de la cybersécurité : rôles, responsabilités, implication des métiers dans la gestion des risques.
- Défense en profondeur : politique de contrôle d'accès, gestion des comptes à privilège.
- Gestion des incidents de cybersécurité : politique de détection, réaction.

6 - MIGRATION DES APPLICATIONS DANS LE CLOUD PUBLIC

- Politique de gestion des vulnérabilités, traitement (correctif).
- Périmètres sensibles : gestion des mises à jour.
- Déclaration des attaques subies.
- Prestataires certifiés obligatoires (PDIS, PRIS).
- Audit de sécurité par l'ANSSI, recours aux auditeurs certifiés (PASSI, LPM).

AF-CCSE – LES INCONTOURNABLES DE LA SÉCURITÉ DU CLOUD COMPUTING



DESCRIPTION

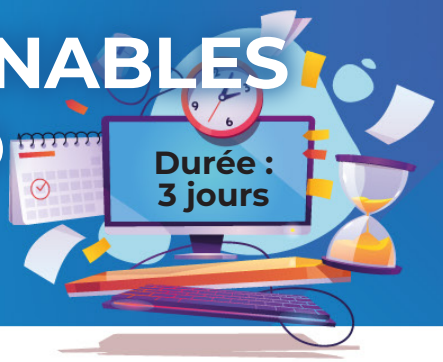
La sécurité du cloud est l'ensemble des stratégies et pratiques de protection des données et des applications hébergées dans le cloud. Comme la cybersécurité, la sécurité du cloud est un domaine très vaste et il n'est jamais possible d'empêcher toutes sortes d'attaques. Cependant, une stratégie de sécurité du cloud bien conçue réduit considérablement le risque de cyberattaques. Cette formation permet d'expliquer comment évaluer les risques et quelles solutions mettre en place.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Evaluer les principales menaces, vulnérabilités et risques dans le cloud.
- Acquérir les principales clés issues du guide sécurité et de la CCM de la cloud security alliance
- Comprendre les risques identifiés par l'ENISA
- Evaluer la maturité et le niveau de sécurité des fournisseurs cloud
- Découvrir les principes fondamentaux de la sécurité dans le cloud
- Avoir une vision globale des apects de conformité (juridique, niveaux de service, audit, standards...)
- Comprendre la sécurité d'une architecture de Cloud Computing
- Comprendre les risques induits par ces services en termes de sécurité de l'information
- Obtenir une vision globale des offres de Cloud Computing
- Savoir répondre à un incident de sécurité
- Comprendre comment s'appuyer sur des référentiels de normes et de standards pour sécuriser le Cloud
- Connaitre les moyens génériques de la sécurité du Cloud
- Etre 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

AF-CCSE – LES INCONTOURNABLES DE LA SÉCURITÉ DU CLOUD COMPUTING



PUBLIC CONCERNÉ

- Architectes SI, Chefs de projet sécurité – Consultants Cyber, Responsables DSI – RSSI

PRÉREQUIS

- Connaissance de base en sécurité de l'information
- QCM de 15 questions à réaliser en amont de la formation

TARIF : 2 600 € HT

PROGRAMME DE LA FORMATION 1/2

1 - INTRODUCTION AU CLOUD :

- Chiffres clés du Cloud
- Actualité du Cloud
- Informatique traditionnelle et Cloud Computing
- Définition du Cloud selon le NIST
- Les 5 caractéristiques essentielles
- Les 3 modèles de service (SaaS, PaaS, IaaS)
- Les 4 modèles de déploiement (Cloud public, privé, hybride et communautaire)
- Les grandes étapes d'une migration réussie d'un point de vue sécurité dans le cloud
- Les offres SecaaS

2 - LA SÉCURITÉ DES ENVIRONNEMENTS VIRTUALISÉS DANS LE CLOUD :

- Les risques liés à la virtualisation des serveurs (VM Escape, VM Hopping, VM Theft et VM Sprawl)
- La problématique de la protection anti-malware dans une infrastructure virtualisée
- Les risques liés aux vulnérabilités, aux API et aux logiciels (Openstack, Docker, VmWare...)

3 - LA SÉCURITÉ DES RÉSEAUX DANS LE CLOUD :

- Software Definied Network : Principes et enjeux
- L'approche SASE
- Les accès sécurisés via Ipsec, VPN, https et SSH
- Les solutions spécifiques d'accès au Cloud (Intercloud, Aws Direct connect...)

4 - LA SÉCURITÉ DES DONNÉES DANS LE CLOUD :

- Les données dans le cloud : cycle de vie, classification, anonymisation, pseudonymisation, tokenisation
- Le CASB (Cloud Access Security Broker), principes et solutions
- L'approche BYOK (Bring Your Own Key) et les solutions HSM dans le cloud
- Les ILM (Information Lifecycle Management)

5 - LE CSA (CLOUD SECURITY ALLIANCE) : RÔLE ET RÉFÉRENTIELS

- Les 14 domaines du security guidance for critical areas of focus in cloud computing
- Les menaces dans le cloud selon l'ENISA
- La cloud controls matrix (CCM) et le consensus assessments initiative questionnaire (CAIQ)
- Le framework de certification OCF et l'annuaire STAR (Security Trust & Assurance Registry)
- La certification CCSK (Certificate of Cloud Security Knowledge)

PROGRAMME DE LA FORMATION 2/2

6 - LES RISQUES CLOUD SELON L'ENISA :

- Evaluation et gestion des risques du cloud par la norme ISO 27005
- Les spécificités de la gestion des risques dans le cloud
- Les 35 principaux risques identifiés par l'ENISA

7 - LE CONTRAT CLOUD :

- Les accords de service (SLA) : pénalités versus indemnités
- Les clauses de sécurité à insérer dans un contrat de cloud (confidentialité, effacement des données...)
- Clauses de réversibilité amont & aval

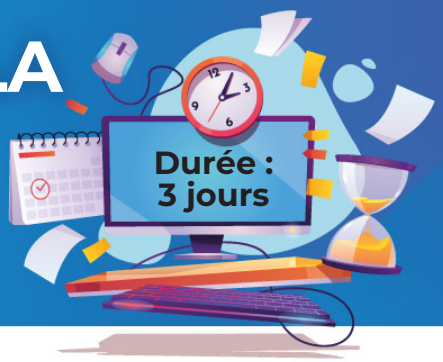
8 - LE CONTRÔLE DU CLOUD :

- Les audits de sécurité
- Cloud et test d'intrusion : périmètre d'action
- Panorama des certifications / qualifications (SecNumCloud, SSAE18, HDS...)
- La certification de sécurité européenne issue du Cybersecurity Act
- Intérêts et limites de la certification ISO 27001 pour les services cloud
- Les normes ISO 27017 et ISO 27018
- La gestion des incidents dans le cloud : rôle et responsabilité des acteurs

9 - ASPECTS JURIDIQUES :

- Quelles sont les responsabilités juridiques du fournisseur ? Quid des sous-traitants du fournisseur ?
- La nationalité du fournisseur et la localisation des Datacenters
- Le cadre juridique des données à caractère personnel (Directive 95/46 CE, GDPR, CCT, BCR...)
- Après l'annulation du « Privacy Shield », comment migrer ses données vers les USA ?
- Le Cloud Act menace-t-il des données dans le Cloud à l'extérieur des USA ?
- Les hébergeurs de données de santé (agrément ASIP, obligations de sécurité, localisation des données, etc)

AF-CYB2 – LES BASES DE LA SÉCURITÉ DES SYSTEMES D'INFORMATIONS



DESCRIPTION

« Les essentiels de la sécurité » est une certification fournissant les principes et actions à mettre en œuvre au candidat certifié afin qu'il puisse intégrer cette notion de sécurité au sein du système d'information d'une organisation donnée avec l'aide du responsable de la sécurité des systèmes d'information et d'en maitriser les outils nécessaires.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Connaître l'étendue des risques qui pèsent sur les informations de l'entreprise
- Comprendre l'évolution des analyses de risque pour faire face aux nouvelles menaces
- Identifier les risques associés à l'émergence de nouvelles technologies
- Savoir mettre en œuvre une gouvernance efficace
- Comprendre l'intérêt de disposer d'une surveillance et d'une gestion des incidents de dernière génération
- Connaitre l'évolution de la cybercriminalité et de ses enjeux
- Maîtriser la sécurité du Cloud, des applications, des postes clients
- Comprendre les principes de la cryptographie
- Gérer les processus de supervision de la sécurité SI

PUBLIC CONCERNÉ

- DSI - RSSI, Architectes – Developpeurs, Chefs de projets, Administrateurs système & réseau

PRÉREQUIS

- Connaissance de base en sécurité de l'information

TARIF : 2 500 € HT

PROGRAMME DE LA FORMATION 1/2

1 - ETAT DE L'ART ET ÉVOLUTION DE LA CYBERSÉCURITÉ :

- Cybersécurité : nouveaux acteurs et nouvelles portées
- Sécurité et juridique
- CNIL, ANSSI
- ENISA
- Les normes, certifications et labels sécurité

2 - EVOLUTION DES ANALYSES DE RISQUES :

- Comprendre les analyses de risques
- Les cartographies
- Modélisation de la menace
- Risque IT vs Risque liée aux personnes concernées
- Rapport d'analyse de risques
- Les mesures de sécurité et le ROSI

3 - LA GOUVERNANCE DE LA SÉCURITÉ :

- Les indicateurs de sécurité performants
- Les indicateurs de sécurité efficaces
- Le TBSSi
- Matrice des compétences cyber
- RSSI évolution des fonctions
- DPO rôles et missions

4 - EVOLUTIONS TECHNOLOGIQUES :

- Etat des menaces et attaques contemporaines
- Dissection d'une APT
- Les nouvelles architectures sécurisées
- Automatisation et sécurité
- L'IA et la sécurité
- Sécurité des systèmes embarquées et IoT
- Sécurité dans le développement
- La sécurité en environnement Cloud
- Mobilité et sécurité

5 - SURVEILLANCE ET GESTION DES INCIDENTS :

- Gestion et automatisation de la cartographie
- Sécurité offensive
- Supervision de la sécurité Gestion des incidents, SIEM, SOC CSIRT
- La cyber résilience
- Les CERT et gestion d'un programme de cyber sécurité

6 - GESTION ET SUPERVISION ACTIVE DE LA SÉCURITÉ :

- Les audits de sécurité (scope et référentiels : ISO 27001, RGPD...)
- Les tests d'intrusion (black box, gray box et white box)
- Les plateformes de « bug Bounty »
- Comment répondre efficacement aux attaques ?
- Mettre en place une solution de SIEM
- Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?
- Les technologies du SOC 2.0 (CASB, UEBA, Deceptive Security, EDR, SOAR, machine learning...)
- Les labels ANSSI (PASSI, PDIS & PRIS) pour l'externalisation
- Les procédures de réponse à incident (ISO 27035 et NIST SP 800-61 R2)

PROGRAMME DE LA FORMATION 2/2

7 - FONDAMENTAUX DE LA CRYPTOGRAPHIE :

- Les techniques cryptographiques
- Les algorithmes à clé publique et symétriques
- Les fonctions de hachage simple, avec sel et avec clé (HMAC)
- Les architectures à clés publiques (PKI)
- Certification CC et qualification ANSSI des produits cryptographiques

AF-EBRM- EBIOS RISK MANAGER

DESCRIPTION

EBIOS-RM est devenue la méthode de référence en France pour évaluer les risques dans le secteur public et privé. Cette formation vous permettra d'acquérir les compétences nécessaires pour mener à bien l'évaluation des risques de bout en bout, depuis l'étude des besoins jusqu'à la formalisation des objectifs de sécurité. De plus, cette formation vous préparera à la certification EBIOS Risk Manager.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les concepts de bases liés à la gestion des risques.
- Savoir cerner le contexte d'une organisation souhaitant mettre en œuvre une analyse des risques.
- Savoir mener des ateliers liés d'analyse de risque.
- Avoir une connaissance précise des typologies de menaces et des vulnérabilités associés
- Connaitre les principaux concepts de gouvernance et ses principaux enjeux et implication en matière de sécurité de l'information.
- Savoir réaliser le suivi des risques

PUBLIC CONCERNÉ

- RSSI, Risk Manager, DSI, Chef de projet sécurité

PRÉREQUIS

- Connaissance du fonctionnement managériale d'une organisation
- Connaissance de base en analyse de risque

TARIF : 1 600 € HT

PROGRAMME DE LA FORMATION

1 - FONDAMENTAUX DU MANAGEMENT DU RISQUE

- Le risque
- Actifs, Menaces et Vulnérabilités
- La gravité et vraisemblance du risque
- Evaluation du risque
- ISO 31000
- ISO 27005

2 - CADRAGE ET SOCLE DE SÉCURITÉ

- Usages d'EBIOS RM
- Valeur métier
- Biens supports
- Evénement redouté
- Echelle de gravité
- Socle de sécurité

3 - SOURCES DE RISQUE

- Panorama des attaques récentes
- Sources de risques
- Objectifs visés
- Pertinence d'une source de risque

4 - SCÉNARIOS STRATÉGIQUES

- Parties prenantes
- Niveau de menace
- Cartographie de l'écosystème
- Scénarios stratégiques

5 - SCÉNARIOS OPÉRATIONNELS

- Vraisemblance
- Méthode Expresse
- Méthode Standard
- Méthode Avancée
- Scénario Opérationnel
- Mode Opératoire
- Action Elémentaire

6 - TRAITEMENT DU RISQUE

- Stratégie de traitement du risque
- Evaluation des risques
- PACS
- Synthèse des risques résiduels
- Cadre du suivi des risques

AF-IM27- IMPLÉMENTER UN PROJET ISO 27001

DESCRIPTION

La sécurité des systèmes d'information est une préoccupation majeure de toutes les Directions des Systèmes d'Information, quel que soit le secteur d'activité de l'entreprise. Cette formation vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation dans la mise en place, la mise en œuvre, la gestion et la mise à jour d'un SMSI conforme à la norme ISO/IEC 27001:2022. En outre, cette formation vous préparera à la certification ISO 27001 Lead Implementer.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les composants d'un système de management de la sécurité de l'information (SMSI) conforme à ISO 27001
- Expliquer le contenu et la corrélation entre ISO 27001 et 27002 ainsi qu'avec d'autres normes et cadres réglementaires
- Adapter les exigences de la norme ISO 27001 au contexte spécifique d'un organisme
- Interpréter les exigences d'ISO 27001 dans le cadre de l'audit d'un SMSI
- Savoir mener une analyse de risque
- Savoir mener un projet ISO 27001 et le maintenir

PUBLIC CONCERNÉ

- RSSI, Correspondant sécurité, Technicien réseau et système...

PRÉREQUIS

- Connaissances de base en sécurité informatique.

TARIF : 3 000 € HT

PROGRAMME DE LA FORMATION 1/3

1 - INTRODUCTION, PRINCIPES FONDAMENTAUX DE LA SÉCURITÉ DE L'INFORMATION

- Les bases de la cybersécurité
- Le rôle du Lead SMSI
- Les outils du Lead SMSI
- Les normes ISO
- Comment lire une norme ISO
- Définition du SMSI
- Structure des normes et le PDCA
- Les exigences de l'ISO 27001
- Le contenu de l'annexe A de l'ISO 27001
- Les livrables attendus

Exercice pratique en groupe :
Les stagiaires devront reprendre la norme et en extirper les exigences en indiquant les livrables et les responsables associés pour chaque exigence.

2 - PRÉPARATION ET PLANIFICATION DU PROJET SMSI

- Le lancement du projet SMSI
- Compréhension de l'organisme
  - Rédaction du plan projet
  - Enjeux interne et externes
  - Présentation d'outils
  - Cartographie de l'existant
  - Cartographie des flux
  - Revue des processus
  - Analyse des écarts
  - Définition du domaine d'application
- Matrice des compétences
  - RSSI
  - DPO
  - Responsable du traitement des données personnelles
  - Sous-traitant du traitement des données personnelles
  - Répartition des rôles
- Leadership et management
  - Présentation du projet à la Direction
  - Avantages juridique, économiques et internes du SMSI
  - Budgétisation
- Politique de sécurité de l'information et politique de protection des données
  - Introduction
  - Domaine d'application
  - Objectifs
  - Principes
  - Rôles et responsabilités
  - Principaux éléments attendus
  - Politiques connexes
  - Diffusion de la politique
- L'analyse de risque
  - La méthodologie d'appréciation du risque
  - L'identification des risques
  - L'appréciation du risque
  - L'évaluation du risque
  - Le traitement du risque
  - Le risque résiduel et acceptation du risque
  - Plan de traitement des risques
- Déclaration d'applicabilité

PROGRAMME DE LA FORMATION 2/3

3 - MISE EN PLACE DU SMSI

- La mise en place d'un processus de gestion documentaire
  - La création de modèle
  - Le contenu type d'un document
  - La classification
  - La gestion des enregistrements
  - Le cycle de vie documentaire
- Plan de formation et de sensibilisation
  - Définition de la compétence, de la formation et de la sensibilisation
  - Conception et planification de la sensibilisation
  - Support de sensibilisation
  - Programme de formation
  - La matrice de compétence
  - Résultats des campagnes de sensibilisation et de formation
- Plan de communication
  - Les principes de communication
  - Les objectifs de communication
  - L'identification des parties intéressés
  - Les supports de communication
  - Les activités de communications
- Gestion des incidents
  - La politique de gestion des incidents
  - Les processus de remontée des incidents
  - Les CERT
  - Les mesures de réponses à incidents
  - L'analyse forensique
  - Sauvegarde et stockage des incidents de sécurité
  - Revue et interprétation des incidents de sécurité
- Autres mesures à mettre en œuvre
  - La gestion des actifs
  - La gestion des identités et des accès
  - La gestion du chiffrement
  - La protection des réseaux
  - Les relations avec les fournisseurs
  - La sécurité du développement
  - La continuité d'activité
  - Le choix des indicateurs

4 - SURVEILLANCE, REVUE ET AMÉLIORATION CONTINUE DU SMSI

- Le suivi et la mesure des performances
  - L'ISO 27004
  - Indicateur de performance
  - Indicateur d'efficacité
  - Interprétation du tableau de bord
- L'audit interne
  - Audit interne (1ère partie) /externe (2nde et tierce partie)
  - Les objectifs de l'audit interne
  - Nomination d'un responsable d'audit
  - Déroulé d'un audit interne (pont avec la 19011)
  - Relevé de non-conformités (majeure et mineure)
  - Suivi des non-conformités

PROGRAMME DE LA FORMATION 3/3

- Revue de direction
  - Périodicité de la revue de direction
  - Exemple d'ordre du jour
  - Plan d'action pour le traitement des non-conformités
  - Opportunités d'amélioration continue
  - Rapport de revue de direction
- Le traitement des non-conformités
- L'amélioration continue

AF-IM701- IMPLÉMENTER UN PROJET ISO 27701

DESCRIPTION

Avec la collecte croissante de données personnelles et leur traitement, les organisations sont confrontées à des préoccupations de confidentialité liées aux données à caractères personnelles. Cette formation vous fournira l'expertise nécessaire pour aider une organisation à établir, mettre en œuvre, entretenir et améliorer continuellement un système de management de la protection de la vie privée basé sur la norme ISO/IEC 27701. En outre, cette formation vous préparera à la certification ISO 27701 Lead Implementer.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Décrire l'objectif et les avantages d'un système de management de la vie privée
- Savoir mettre en œuvre un système de management basé sur la norme ISO 27701.
- Savoir mener une analyse d'impact sur la protection des données
- Connaitre les principaux concepts de gouvernance et ses principaux enjeux et implication en matière de sécurité de l'information.
- Utiliser la norme ISO 27701 comme cadre pour l'amélioration continue.
- Obtenir la note de passage requise à l'issue de l'examen.

PUBLIC CONCERNÉ

- Ce stage pratique s'adresse à : DPO, RSSI, Correspondant sécurité, Technicien réseau et système...

PRÉREQUIS

- Connaissance du fonctionnement managériale et organisationnelle d'une organisation
- Connaissance de base en sécurité de l'information notamment dans les sujets juridiques.

TARIF : 3 000 € HT

PROGRAMME DE LA FORMATION 1/3

1 - INTRODUCTION, PRINCIPES FONDAMENTAUX DE LA SÉCURITÉ DE L'INFORMATION

- Les bases de la cybersécurité
- Le rôle du Lead SMVP
- Les outils du Lead SMVP
- Les normes ISO
- Comment lire une norme ISO
- Définition du SMVP
- Structure des normes et le PDCA
- Les exigences de l'ISO 27701
- Le contenu des annexes A et B de l'ISO 27701
- Les livrables attendus

Exercice pratique en groupe :
Les stagiaires devront reprendre la norme et en extirper les exigences en indiquant les livrables et les responsables associés pour chaque exigence.

2 - PRÉPARATION ET PLANIFICATION DU PROJET SMVP

- Le lancement du projet SMVP
- Compréhension de l'organisme
  - Rédaction du plan projet
  - Enjeux interne et externes
  - Présentation d'outils
  - Cartographie de l'existant
  - Cartographie des flux
  - Revue des processus
  - Analyse des écarts
  - Définition du domaine d'application
- Matrice des compétences
  - RSSI
  - DPO
  - Responsable du traitement des données personnelles
  - Sous-traitant du traitement des données personnelles
  - Répartition des rôles
- Leadership et management
  - Business Case
  - Présentation du projet à la Direction
  - Avantages juridique, économiques et internes du SMvp
  - Budgétisation
- Politique de sécurité de l'information et politique de protection des données
  - Introduction
  - Domaine d'application
  - Objectifs
  - Principes
  - Rôles et responsabilités
  - Principaux éléments attendus
  - Politiques connexes
  - Diffusion de la politique
- L'analyse de risque
  - La méthodologie d'appréciation du risque
  - L'identification des risques
  - L'appréciation du risque
  - L'évaluation du risque
  - Le traitement du risque
  - Le risque résiduel et acceptation du risque
  - Plan de traitement des risques
- Déclaration d'applicabilité

PROGRAMME DE LA FORMATION 2/3

3 - MISE EN PLACE DU SMVP

- La mise en place d'un processus de gestion documentaire
  - La création de modèle
  - Le contenu type d'un document
  - La classification
  - La gestion des enregistrements
  - Le cycle de vie documentaire
- Plan de formation et de sensibilisation
  - Définition de la compétence, de la formation et de la sensibilisation
  - Conception et planification de la sensibilisation
  - Support de sensibilisation
  - Programme de formation
  - La matrice de compétence
  - Résultats des campagnes de sensibilisation et de formation
- Plan de communication
  - Les principes de communication
  - Les objectifs de communication
  - L'identification des parties intéressés
  - Les supports de communication
  - Les activités de communications
- Gestion des incidents et des violations de données personnelles
  - La politique de gestion des incidents
  - Les processus de remontée des incidents
  - Les CERT
  - Les mesures de réponses à incidents
  - L'analyse forensique
  - Sauvegarde et stockage des incidents de sécurité
  - Revue et interprétation des incidents de sécurité
- Autres mesures à mettre en œuvre
  - La gestion des actifs
  - La gestion des identités et des accès
  - La gestion du chiffrement
  - La protection des réseaux
  - Les relations avec les fournisseurs
  - La sécurité du développement
  - La continuité d'activité
  - Le choix des indicateurs

4 - SURVEILLANCE, REVUE ET AMÉLIORATION CONTINUE DU SMVP

- Le suivi et la mesure des performances
  - L'ISO 27004
  - Indicateur de performance
  - Indicateur d'efficacité
  - Interprétation du tableau de bord
- L'audit interne
  - Audit interne (1ère partie) /externe (2nde et tierce partie)
  - Les objectifs de l'audit interne
  - Nomination d'un responsable d'audit
  - Déroulé d'un audit interne (pont avec la 19011)
  - Relevé de non-conformités (majeure et mineure)
  - Suivi des non-conformités

PROGRAMME DE LA FORMATION 3/3

- Revue de direction
  - Périodicité de la revue de direction
  - Exemple d'ordre du jour
  - Plan d'action pour le traitement des non-conformités
  - Opportunités d'amélioration continue
  - Rapport de revue de direction
- Le traitement des non-conformités
- L'amélioration continue

AF-05RM- L'ANALYSE DE RISQUE SELON LA NORME ISO 27005 :2018

DESCRIPTION

Avec la prolifération des échanges sur Internet, la sécurité de l'information est devenue un enjeu majeur. Pour éviter les fraudes en ligne, le vol d'identité ou la détérioration des sites Web, il est primordial de gérer et d'évaluer les risques conformément à la norme internationale ISO/CEI 27005.
Cette formation prépare à la certification de ISO/IEC 27005 Risk Manager.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les concepts de bases liés à la gestion des risques.
- Savoir cerner le contexte d'une organisation souhaitant mettre en œuvre une analyse des risques.
- Savoir mener des ateliers liés d'analyse de risque.
- Avoir une connaissance précise des typologies de menaces et des vulnérabilités associés
- Connaitre les principaux concepts de gouvernance et ses principaux enjeux et implication en matière de sécurité de l'information.
- Utiliser la norme ISO 27005 comme cadre pour la mise en œuvre et le suivi de la gestion des risques.

PUBLIC CONCERNÉ

- RSSI, Risk Manager, DSI, Chef de projet sécurité

PRÉREQUIS

- Connaissance du fonctionnement managériale d'une organisation
- Connaissance de base en analyse de risque

TARIF : 1 600 € HT

PROGRAMME DE LA FORMATION

1 - LE RÔLE ET LES COMPÉTENCES DU RISK MANAGER

- Qualité de communiquant
- Animer une réunion
- Préparer un ordre du jour
- Suivre et conclure
- La gestion de projet
- Connaissance des règlementations
- Les normes
- Comprendre les risques
- Cartographie
- Stratégie d'entreprise
- Outils de veille
- Les méthodologies

2 - L'APPRÉCIATION DES RISQUES

- Le processus de management des risques
- Appréhender le contexte
- Comprendre les cartographies, et la stratégie
- Trouver les actifs primordiaux et actifs supports critiques associés
- Les composantes : menaces, actifs, vulnérabilités
- Les échelles, conception, et compréhension
- Evaluer le risque

3 - LE TRAITEMENT DES RISQUES

- Les options de traitements
- Exercices sur les options de traitement
- Les mesures de sécurité
- Les risques résiduels
- Propriétaires des risques
- Le PTR, et gestion de projet associée
- Les indicateurs et tableau de bord

4 - COMMUNICATION, SUIVI ET AMÉLIORATION CONTINUE

- La communication et le risque
- Stratégie de communication
- Conduite du changement
- Suivi, surveillance et revue du risque
- Amélioration continue

AF-AU27- L'AUDIT ISO 27001

DESCRIPTION

La mise en place de normes vise à garantir la sécurité, la fiabilité et la qualité des produits et services offerts par les entreprises. Cette formation permet aux participants d'acquérir les compétences nécessaires pour réaliser des audits internes et externes des systèmes de management de la sécurité de l'information en appliquant les principes, les procédures et les techniques d'audit reconnus conformément à la norme ISO 19011 et au processus de certification de l'ISO/IEC 17021-1. Elle prépare également à la certification ISO 27001 Lead Auditor.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les tenants et les aboutissants de la mise en œuvre un système de management basé sur la norme ISO/IEC 27001.
- Savoir planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO/IEC 19011
- Comprendre le rôle et les attentes autour de la fonction d'auditeur.
- Savoir interpréter et auditer les exigences de la norme ISO/IEC 27001
- Obtenir la note de passage requise à l'issue de l'évaluation de l'atelier.

PUBLIC CONCERNÉ

- Auditeurs, Auditeurs sécurité, RSSI, Risk Manager, Chef de projet sécurité

PRÉREQUIS

- Connaissance du fonctionnement managériale et organisationnelle d'une organisation
- Connaissance de base des audits et connaissance en sécurité de l'information.

TARIF : 3 000 € HT

PROGRAMME DE LA FORMATION 1/4

JOUR 1

- Introduction :
  - Brainstorming sur les connaissances générales des stagiaires
  - Les principes fondamentaux de la sécurité de l'information et de la protection des données :
    - Les normes ISO
    - Historique des ISO 27k
    - Le CID
    - Le risque en sécurité de l'information
    - Vulnérabilité et menace

Quizz sur les différentes notions évoqués

- Le métier d'auditeur
  - Le processus de sélection de l'auditeur
  - L'expérience requise
  - Les compétences attendues
  - Le responsable d'audit
- Les organismes d'accréditation
- Structure de la norme ISO 27001 :
  - Définition du SMSI
  - Structure des normes et le PDCA
  - Les exigences de l'ISO 27001
  - Le contenu de l'annexe A de l'ISO 27001
  - Les livrables attendus

Exercice pratique en groupe :

Les stagiaires devront reprendre la norme et en extirper les exigences en indiquant les livrables et les responsables associés pour chaque exigence.

JOUR 2

- L'ISO 19011
- Les concepts de base de l'audit
  - Les types d'audit
  - Objectifs et critères d'audit
  - Principes d'audit
    - Déontologie
    - Restitution impartiale
    - Conscience professionnelle
    - Confidentialité
    - Indépendance
    - Approche fondée sur la preuve
    - Approche fondée sur les risques
  - Cartographie de l'existant
  - Cartographie des flux
  - Revue des processus
  - Analyse des écarts
  - Définition du domaine d'application

Exercice et mise en situation :

Dans un premier temps, les apprenants devront par groupe indiquer comment mettre en œuvre de manière concrète certains points d'audit. Dans un second temps le formateur donnera des situations d'audit et les apprenants devront indiquer comment ils réagiraient en fonction des principes d'audit.

PROGRAMME DE LA FORMATION 2/4

- La réalisation d'un audit en se basant sur les preuves
  - Matérielle
  - Mathématique
  - Confirmative
  - Technique
  - Analytique
  - Documentaire
  - Verbale

Cas pratique :

En se basant sur des preuves fournies dans le cadre d'un cas pratique, les apprenants devront indiquer de quel type de preuve il s'agit mais également si cette preuve répond à des exigences de la norme ISO 27001 (les exigences en question seront communiquées).

- La réalisation d'un audit en se basant sur les risques
  - Risque inhérent
  - Risque de contrôle
  - Risque de détection
- Initialisation de l'audit
  - L'offre d'audit
  - L'équipe d'audit
  - Les compétences attendues de l'équipe d'audit
  - Faisabilité de l'audit
  - Objectif de l'audit
  - Périmètre
  - Référentiel sur lequel est basé l'audit (critères)
  - Le contrat

Cas pratique :

En se basant sur un cas pratique, les apprenants devront préparer réaliser une offre d'audit qui servira de base pour le contrat entre l'auditeur et l'entreprise du cas pratique.

JOUR 3

- Audit d'étape 1
  - Rappel des objectifs de l'audit d'étape 1
  - Préparation des activités sur site
  - Observation du site physique
  - Entretien avec le personnel de l'audité
  - Revue des documents du SMSI
  - Rapport d'audit d'étape 1

Cas pratique :

En vous basant sur les documents fournis dans le cas pratique, vous réaliserez un audit d'étape 1 et vous indiquerez si l'organisation est apte à passer l'audit d'étape 2.

- Préparation de l'audit d'étape 2
  - Réalisation du plan d'audit
  - Rappel des objectifs de l'audit
  - Périmètre d'audit
  - Attribution des tâches à l'équipe d'audit
  - Planification des entretiens

PROGRAMME DE LA FORMATION 3/4

Cas pratique :
En se basant sur le plan d'audit associé au cas pratique, corrigez les erreurs contenues dans ce dernier.

- Audit d'étape 2
  - Conduite de la réunion d'ouverture
  - Collecte d'information
  - Comportement lors de l'audit
  - Gestion des conflits
  - Communication avec la direction
  - Procédure d'audit
    - Entretien
    - Revue de l'information documentée
    - Observation
    - Analyse
    - Échantillonnage
    - Vérification technique
    - Corroboration
    - Évaluation
- L'ISO 27007
- L'ISO 27008

Cas pratique :
En se basant sur un cas pratique et en reprenant l'ISO 27007 et l'ISO 27008, les apprenants devront indiquer quelles seront les différentes preuves à apporter sur plusieurs points de la norme ISO 27001.

JOUR 4

- Constatation d'audit
  - Non-Conformité Mineure
  - Non-Conformité Majeure
  - Observations
  - Points d'amélioration
  - Conformité

Cas pratique :
En se basant sur des preuves d'audit provenant d'un cas pratique, les apprenants devront indiquer et justifier leur constatation d'audit.

- Réunion de clôture
  - Présentation des résultats
  - Recommandation d'audit
  - Question et réponses
  - Suite de l'audit

Cas pratique :
Les apprenants devront préparer et effectuer une réunion de clôture avec la direction du cas pratique. Ils devront évoquer les constatations et conclusions d'audit, les non-conformités détectées, les accords sur les actions correctives proposées...

- Rédaction du rapport d'audit
  - Présentation de la société
  - Constats d'audit
  - Recommandation
  - Notes d'audit

PROGRAMME DE LA FORMATION 4/4

Cas pratique :
En se basant sur quelques non-conformités fournies dans l'étude de cas, les apprenants devront créer des rapports de non-conformités.

- Audit de suivi
  - Préparation des actions correctives
  - Réalisation des actions correctives
  - Revue par l'auditeur

Cas pratique :
En se basant sur quelques plans d'actions fournis dans l'étude de cas, les apprenants devront indiquer s'ils valident ou non les plans d'actions. Les apprenants devront également préciser quel est pour eux le meilleur plan d'action à mettre en œuvre selon eux pour corriger les non-conformités.

- Le cycle d'audit et les audits ultérieurs
  - Audit de suivi
  - Audit de surveillance
  - Audit de re certification
  - Cycle d'audit

AF-AU701- L'AUDIT ISO 27701

DESCRIPTION

La norme ISO 27701 définit les exigences liées à la mise en place d'un système de management de la vie privée (SMVP). Cette formation permet aux participants d'acquérir les compétences nécessaires pour réaliser des audits internes et externes des systèmes de management de la vie privée en appliquant les principes, les procédures et les techniques d'audit reconnus conformément à la norme ISO 19011 et au processus de certification de l'ISO/IEC 17021-1. Elle prépare également à la certification ISO 27701 Lead Auditor.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les tenants et les aboutissants de la mise en œuvre un système de management basé sur la norme ISO/IEC 27701.
- Savoir planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO/IEC 19011
- Comprendre le rôle et les attentes autour de la fonction d'auditeur.
- Savoir interpréter et auditer les exigences de la norme ISO/IEC 27701
- Obtenir la note de passage requise à l'issue de l'évaluation de l'atelier.

PUBLIC CONCERNÉ

- Auditeurs, Auditeurs sécurité, RSSI, Risk Manager, Chef de projet sécurité

PRÉREQUIS

- Connaissance du fonctionnement managériale et organisationnelle d'une organisation
- Connaissance de base des audits et connaissance en sécurité de l'information.

TARIF : 3 000 € HT

PROGRAMME DE LA FORMATION 1/4

JOUR 1

- Introduction :
  - Brainstorming sur les connaissances générales des stagiaires
  - Les principes fondamentaux de la sécurité de l'information et de la protection des données :
    - Les normes ISO
    - Historique des ISO 27k
    - Le CID
    - Le risque en sécurité de l'information
    - Vulnérabilité et menace

Quizz sur les différentes notions évoqués

- Le métier d'auditeur
  - Le processus de sélection de l'auditeur
  - L'expérience requise
  - Les compétences attendues
  - Le responsable d'audit
- Les organismes d'accréditation
- Structure de la norme ISO 27701 :
  - Définition du SMVP
  - Structure des normes et le PDCA
  - Les exigences de l'ISO 27701
  - Le contenu de l'annexe A et B de l'ISO 27701 :2019
  - Les livrables attendus

Exercice pratique en groupe :

Les stagiaires devront reprendre la norme et en extirper les exigences en indiquant les livrables et les responsables associés pour chaque exigence.

JOUR 2

- L'ISO 19011
- Les concepts de base de l'audit
  - Les types d'audit
  - Objectifs et critères d'audit
  - Principes d'audit
    - Déontologie
    - Restitution impartiale
    - Conscience professionnelle
    - Confidentialité
    - Indépendance
    - Approche fondée sur la preuve
    - Approche fondée sur les risques
  - Cartographie de l'existant
  - Cartographie des flux
  - Revue des processus
  - Analyse des écarts
  - Définition du domaine d'application

Exercice et mise en situation :

Dans un premier temps, les apprenants devront par groupe indiquer comment mettre en œuvre de manière concrète certains points d'audit. Dans un second temps le formateur donnera des situations d'audit et les apprenants devront indiquer comment ils réagiraient en fonction des principes d'audit.

PROGRAMME DE LA FORMATION 2/4

- La réalisation d'un audit en se basant sur les preuves
  - Matérielle
  - Mathématique
  - Confirmative
  - Technique
  - Analytique
  - Documentaire
  - Verbale

Cas pratique :

En se basant sur des preuves fournies dans le cadre d'un cas pratique, les apprenants devront indiquer de quel type de preuve il s'agit mais également si cette preuve répond à des exigences de la norme ISO 27701 (les exigences en question seront communiquées).

- La réalisation d'un audit en se basant sur les risques
  - Risque inhérent
  - Risque de contrôle
  - Risque de détection
- Initialisation de l'audit
  - L'offre d'audit
  - L'équipe d'audit
  - Les compétences attendues de l'équipe d'audit
  - Faisabilité de l'audit
  - Objectif de l'audit
  - Périmètre
  - Référentiel sur lequel est basé l'audit (critères)
  - Le contrat

Cas pratique :

En se basant sur un cas pratique, les apprenants devront préparer réaliser une offre d'audit qui servira de base pour le contrat entre l'auditeur et l'entreprise du cas pratique.

JOUR 3

- Audit d'étape 1
  - Rappel des objectifs de l'audit d'étape 1
  - Préparation des activités sur site
  - Observation du site physique
  - Entretien avec le personnel de l'audité
  - Revue des documents du SMVP
  - Rapport d'audit d'étape 1

Cas pratique :

En vous basant sur les documents fournis dans le cas pratique, vous réaliserez un audit d'étape 1 et vous indiquerez si l'organisation est apte à passer l'audit d'étape 2.

- Préparation de l'audit d'étape 2
  - Réalisation du plan d'audit
  - Rappel des objectifs de l'audit
  - Périmètre d'audit
  - Attribution des tâches à l'équipe d'audit
  - Planification des entretiens

PROGRAMME DE LA FORMATION 3/4

Cas pratique :
En se basant sur le plan d'audit associé au cas pratique, corrigez les erreurs contenues dans ce dernier.

- Audit d'étape 2
  - Conduite de la réunion d'ouverture
  - Collecte d'information
  - Comportement lors de l'audit
  - Gestion des conflits
  - Communication avec la direction
  - Procédure d'audit
    - Entretien
    - Revue de l'information documentée
    - Observation
    - Analyse
    - Échantillonnage
    - Vérification technique
    - Corroboration
    - Évaluation
- L'ISO 27007
- L'ISO 27008

Cas pratique :
En se basant sur un cas pratique et en reprenant l'ISO 27007 et l'ISO 27008, les apprenants devront indiquer quelles seront les différentes preuves à apporter sur plusieurs points de la norme ISO 27701.

JOUR 4

- Constatation d'audit
  - Non-Conformité Mineure
  - Non-Conformité Majeure
  - Observations
  - Points d'amélioration
  - Conformité

Cas pratique :
En se basant sur des preuves d'audit provenant d'un cas pratique, les apprenants devront indiquer et justifier leur constatation d'audit.

- Réunion de clôture
  - Présentation des résultats
  - Recommandation d'audit
  - Question et réponses
  - Suite de l'audit

Cas pratique :
Les apprenants devront préparer et effectuer une réunion de clôture avec la direction du cas pratique. Ils devront évoquer les constatations et conclusions d'audit, les non-conformités détectées, les accords sur les actions correctives proposées...

- Rédaction du rapport d'audit
  - Présentation de la société
  - Constats d'audit
  - Recommandation
  - Notes d'audit

PROGRAMME DE LA FORMATION 4/4

Cas pratique :
En se basant sur quelques non-conformités fournies dans l'étude de cas, les apprenants devront créer des rapports de non-conformités.

- Audit de suivi
  - Préparation des actions correctives
  - Réalisation des actions correctives
  - Revue par l'auditeur

Cas pratique :
En se basant sur quelques plans d'actions fournis dans l'étude de cas, les apprenants devront indiquer s'ils valident ou non les plans d'actions. Les apprenants devront également préciser quel est pour eux le meilleur plan d'action à mettre en œuvre selon eux pour corriger les non-conformités.

- Le cycle d'audit et les audits ultérieurs
  - Audit de suivi
  - Audit de surveillance
  - Audit de re certification
  - Cycle d'audit

forSSIc

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE

LA CERTIFICATION QUALITÉ A ÉTÉ DÉLIVRÉE AU TITRE DE LA CATÉGORIE : ACTIONS DE FORMATION.

SAS - N° SIREN : 811 182 450 - RCS de Chartres - Siège Social : 1 Chemin des Mésanges - Fermaincourt - 28500 MONTREUIL
Code APE : 6202A - N° TVA intracommunautaire : FR13811182450
N° téléphone : 06 15 87 08 72 - Adresse e-mail : contact@forssic.fr - Site internet : www.aforssic.fr