VALSCH Consulting

Expertise Technique & Développement

Formations en Sécurité Informatique

Catalogue de Formations **Edition 2021/202**

VALSCH Consulting
Expertise Technique & Développement

FORMATION CYBERSÉCURITÉ ORGANISATIONNELLE

FORMATIONS	Durée
Formation ISO 27001 - Lead Auditor	5 Jours
Formation ISO 27005 - Risk Manager	3 jours
PECB / IEC 27001 FOUNDATION	2 jours
PECB / IEC 27001 LEAD IMPLEMENTER	5 jours
Formation CISA, Préparation Certified Information Systems Auditor	5 Jours

VALSCH Consulting
Expertise Technique & Développement

FORMATION CYBERSÉCURITÉ TECHNIQUE

Formations	Durée
Certified Ethical Hacker CEH	5 Jours
Formation Tests d'intrusion - Mise en situation d'audit	3 Jours
Fondamentaux de la Cybersécurité	5 Jours
PECB / IEC 27032 LIGNES DIRECTRICES POUR LA CYBER SÉCURITÉ	5 Jours
ADMIN & SECURISATION UNIX / LINUX	3 jours
PECB / IEC 27035 GESTION DES INCIDENTS SCADA	5 Jours
Sécurisation de l'environnement système Windows et infrastructures Virtuelles	3 Jours

Formation ISO 27001 - Lead Auditor

Objectifs

- Apprendre à auditer sur la norme ISO 27001 et les guides associés
- Devenir auditeur ou responsable d'équipe d'audit pour les systèmes de management de la sécurité de l'information (SMSI)
- Disposer de la vision auditeur vis-à-vis de la norme ISO 27001,
- Intégrer le modèle PDCA lors des activités d'audits,
- Auditer les différentes catégories de mesures de sécurité (Annexe A de l'ISO27001 / ISO27002) et conduire un audit de SMSI et ses entretiens en maîtrisant les notions de non-conformités majeures ou mineures.

Durée

5 jours soit 35 heures.

Public visé

les membres des équipes de contrôle interne, des équipes sécurité ou des équipes d'audit, les qualiticiens, et ceux devant être audités et devant comprendre l'état d'esprit de l'auditeur.

VALSCH Consulting
Expertise Technique & Développement

Programme

Jour 1 :

Introduction au système de management de la sécurité de l'information (SMIS) et à l'ISO 27001

Jour 2 :

Principes d'audit : préparation et initiation d'un audit

Impact des tendances et de la technologie en audit, Audit basé sur les preuves
Audit basé sur les risques, Initiation du processus d'audit

Jour 3 :

Activités d'audit sur site Communication pendant l'audit
Procédures d'audit
Création de plans d'échantillonnage d'audit

Jour 4 :

Clôture de l'audit, Évaluation des plans d'action par l'auditeur

Gestion d'un programme d'audit interne

Jour 5 :

Examen de certification

VALSCH Consulting
Expertise Technique & Développement

Formation ISO 27005 - Risk Manager

Objectifs

Ce séminaire, basé en partie sur la norme ISO/CEI 27005:2018, permet aux participants d'acquérir les bases théoriques et pratiques de la gestion des risques liés à la sécurité de l'information. Elle prépare efficacement les candidats à la certification ISO 27005 Risk Manager à partir d'études de cas

Durée : 3 Jours

Public visé

1- Responsables de la sécurité d'information,

2- Membres d'une équipe de sécurité de l'information,

3- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation,

VALSCH Consulting
Expertise Technique & Développement

Programme

Introduction

- Terminologie ISO 27000.
- Définitions de la Menace. Vulnérabilité. Risques.
- Les exigences Disponibilité Intégrité et Confidentialité : la prise en compte de la traçabilité/preuve.
- Rappel des contraintes réglementaires et normatives (RGPD, LPM/NIS, PCI DSS...).
- Le rôle du RSSI versus le Risk Manager.
- La norme 31000, de l'intérêt de la norme "chapeau" en référentiel universel.

Le concept "risque"

- Identification et classification des risques.
- Risques opérationnels, physiques et logiques.
- Les conséquences du risque (financier, juridique, humain...).
- La gestion du risque (prévention, protection, évitement de risque, transfert).
- Assurabilité d'un risque, calcul financier du transfert à l'assurance.

Le management de risques selon l'ISO

- L'appréciation initiale en phase Plan de la section 6 : Planification.
- La norme 27005:2018 : Information Security Risk Management.
- La mise en œuvre d'un processus PDCA de management des risques.
- Le partage des risques avec des tiers (cloud, assurance, …); Le domaine 15 de ISO 27002.
- La méthode de la norme 27001:2013 et son processus « Gestion des Risques ».

Les méthodes d'analyse de risques

- Approche par conformité vs approche par scénarios de risques.
- La prise en compte des menaces intentionnelles sophistiquées de type APT.
- Les objectifs de EBIOS RM (Identifier le socle de sécurité, Être en conformité, Identifier et analyser, etc).

Conclusion et choix d'une méthode

- La convergence vers l'ISO, la nécessaire mise à jour.
- Etre ou ne pas être "ISO spirit" : les contraintes du modèle PDCA.
- Une méthode globale ou une méthode par projet.
- Le vrai coût d'une analyse de risques.
- Comment choisir la meilleure méthode ?
- Les bases de connaissances (menaces, risques...).

FORMATION CISA, PRÉPARATION CERTIFIED INFORMATION SYSTEMS AUDITO

Objectifs

La formation s'articule autour des thèmes du CISA : la pratique de l'audit SI; la gouvernance des SI; l'acquisition et l'implantation des SI; l'exploitation et la gestion des SI; l'audit de l'informatique et des opérations, l'audit des infrastructures et des réseaux, la sécurité des actifs informationnels

Duréé : 5 Jours

Public

- Consultants en organisation, consultants en systèmes d'information, consultants en sécurité. Auditeurs
- Informaticiens
- Responsables informatiques
- Chefs de projets, urbanistes, managers

VALSCH Consulting
Expertise Technique & Développement

Programme

Le processus d'audit des SI : méthodologie d'audit, normes, référentiels, la réalisation de l'audit, les techniques d'auto- évaluation.

La gouvernance et la gestion des SI : Pratique de stratégie et de gouvernance SI, politiques et procédures, pratique de la gestion des SI, organisation et comitologie, gestion de la continuité des opérations.

L'acquisition, la conception et l'implantation des SI : la gestion de projet, l'audit des études et du développement, les pratiques de maintenance, contrôle applicatifs.

L'exploitation, l'entretien et le soutien des SI : l'audit de la fonction information et des opérations, l'audit des infrastructures et des réseaux.

La protection des actifs informationnels : audit de sécurité, gestion des accès, sécurité des réseaux, audit de management de la sécurité, sécurité physique, sécurité organisationnelle.

Le stage se termine lors de la dernière journée par un exposé de pratiques pour se préparer et passer

l'examen (QCM de 4 heures).

Cet exposé est suivi d'un un examen blanc (2 heures) de 100 questions suivi d'une revue des réponses des

stagiaires.

CISA Certified Information Systems Auditor
An ISACA Certification

Formation Certification ISO 27001 Lead Implementer

FORMATION CYBERSÉCURITÉ TECHNIQUE Formation **Certification ISO 27001 Lead Implementer**

Formation Certification ISO 27001 Lead Implementer

Objectifs

La formation ISO 27001 Lead Implementer est conçue pour vous permettre d'acquérir les connaissances et compétences nécessaires pour accompagner votre organisation dans la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI).

Vous maîtriserez les bonnes pratiques relatives à l'établissement, l'implémentation, la gestion et le suivi du SMSI conformément aux dispositions de la norme ISO/IEC 27001:2013.

Sécurisez les informations sensibles, améliorez l'efficacité et in fine la performance globale de votre organisation grâce à ce stage intensif de 5 jours.

A l'issue de notre formation, les participants passeront la certification ISO 27001 Lead Implementer. L'examen s'effectuera durant la dernière journée de formation, sous la supervision d'un formateur accrédité. Le coût de l'examen est inclus dans le prix de la formation.

Durée

5 jours,

VALSCH Consulting
Expertise Technique & Développement

Formation **Certification ISO 27001 Foundation**

FORMATION CYBERSÉCURITÉ TECHNIQUE PECB / IEC 27001 FOUNDATION

VALSCH Consulting
Expertise Technique & Développement

Formation PECB / IEC 27001 FOUNDATION

Objectifs

La formation ISO 27001 Foundation couvre les concepts essentiels de la gestion de la sécurité de l'information. Vous y apprendrez toutes les bonnes pratiques liées à la mise en œuvre et à la gestion d'un Système de management de la sécurité de l'information (SMSI) selon la norme ISO/IEC 27001.

Les mesures de sécurité définies dans la norme ISO 27002 sont également passées en revue, ainsi que la corrélation entre les différentes normes et cadres règlementaires. A l'issue de notre formation, les participants passeront la certification ISO/IEC 27001 Foundation.

L'examen s'effectuera durant la deuxième journée de formation, sous la supervision d'un formateur accrédité.

Durée

2 jours,

FORMATION CYBERSÉCURITÉ TECHNIQUE PECB / IEC 27001 FOUNDATION

VALSCH Consulting
Expertise Technique & Développement

FORMATION : CERTIFIED ETHICAL HACKER CEH V11

FORMATION CYBERSÉCURITÉ TECHNIQUE Formation Certified Ethical Hacker

FORMATION : CERTIFIED ETHICAL HACKER CEH V11

Objectif de formation

- Comprendre les méthodes et modes opératoires employés par les pirates lors d'une attaque informatique
- Identifier et utiliser les outils permettant de tester les protections d'un système d'information d'entreprise
- Evaluer et analyser les points de faiblesses et vulnérabilités latentes d'un système informatique
- Défendre plus efficacement une infrastructure d'entreprise ou d'un composant informatique
- Gagner une expérience notable dans le domaine de la sécurité informatique et du Ethical Hacking
- Se préparer à l'examen de certification CEH v11

Objectifs pédagogique

- Compréhension approfondie des phases de piratage éthique, des différents vecteurs d'attaque et des contre-mesures préventives.
- Compréhension des faiblesses et des vulnérabilités des systèmes afin de renforcer les contrôles de sécurité et de minimiser le risque d'incident ayant pour origine une menace d'ordre logique
- Maitrise de la démarche basée sur les Cinq Phases de l'Ethical Hacking : Reconnaissance, Obtention d'accès, Enumération, Maintien de l'Accès et Disparition des traces
- Apprendre à développer & élaborer un plan de réponse aux cyber-incidents

FORMATION : CERTIFIED ETHICAL HACKER CEH V11

Jours	Contenus/ Concepts clés à aborder	Méthodes, Moyens Pédagogiques et Equipements	Durée (Heure)	
			Théorie	Pratique
J1	Module 1 : Introduction au Ethical Hacking Module 2 : Footprinting et Reconnaissance Module 3 : Scanning de réseaux Module 4 : Enumération	Plateforme de cours, Exercices pratiques Challenges	4	4
J2	Module 6 : Analyse des vulnérabilités Module 7 : System Hacking Module 8 : Analyse de Malwares Chevaux de Troie, Backdoors, Virus, Vers, etc. Module 9 : Sniffing		4	4
J3	Module 10 : Ingénierie sociale Module 11 : Denial-of-service Module 12 : Session Hijacking Module 13 : Evasions d'IDS, Firewalls & Honeypots		4	4
J4	Module 14 : Web Server Hacking Module 15 : Web Application Hacking Module 16 : Injection SQL Module 17 : Hacking de réseaux sans fil		4	4
J5	Module 18 : Hacking des plateformes Mobiles Module 19 : IoT et OT Hacking Module 20 : Cloud Computing Module 21 : Cryptographie		4	4
		Total	20	20

FORMATION : CERTIFIED ETHICAL HACKER CEH V11

Méthodologie et Outils d'évaluation

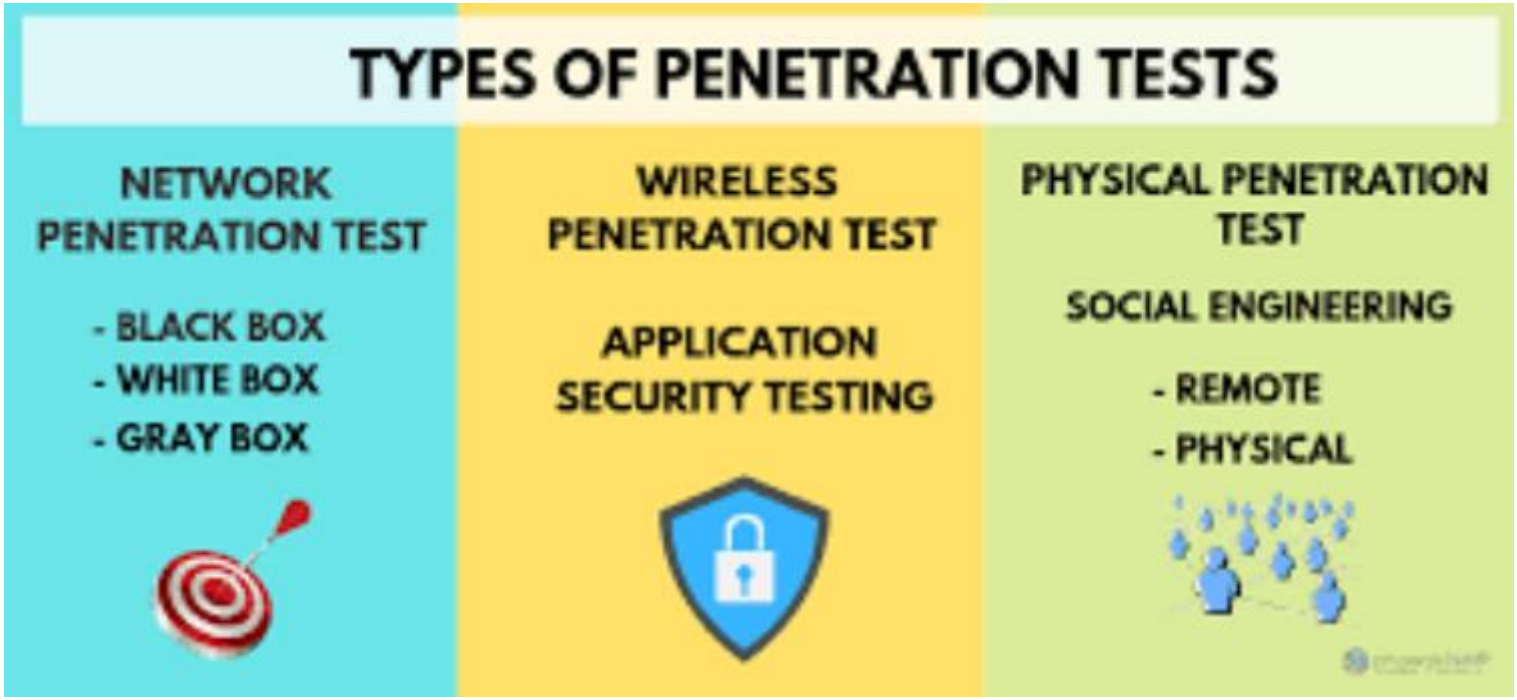
- Modalité d'évaluation de la formation : formative et Sommative
- Validation :
  - ✓ Fiche d'évaluation post-formation
  - ✓ Examen de certification
- Gérer les problèmes de ressources
- Attestation de participation remise à la fin de la formation

Population Cible

Analyste de la sécurité de l'information /Administrateur Sécurité de l'information, Responsable/spécialiste de la sécurité de l'information Ingénieur/Manager de la sécurité des systèmes d'information, Professionnels de la sécurité de l'information /Officers, Sécurité de l'information / Auditeurs informatiques, Analyste des risques, menaces et vulnérabilités, Administrateurs système, Administrateurs et ingénieurs réseau

VALSCH Consulting
Expertise Technique & Développement

FORMATION TESTS D'INTRUSION - MISE EN SITUATION D'AUDIT



FORMATION CYBERSÉCURITÉ TECHNIQUE Formation Tests d'intrusion

Programme : Formation Tests d'intrusion

Jour 1

Techniques d'attaques expertes réseau & système

Contenu & Objectifs

- Introduction aux enjeux, menaces et impacts
- Connaitre les approches des Tests de Sécurité (Pentesting) + Références Normatives
- Comprendre l'Approche HAIM (Hacking Attack Intrusion Methodology)
- Se préparer à la réalisation des tests d'intrusion Réseau (dresser le plan des tests intrusifs réseau) / Ateliers Techniques
- Se préparer à la réalisation des tests d'intrusion Système (dresser le plan des tests intrusifs réseau Système) / Ateliers Techniques

Jour 2

Techniques d'attaques expertes applicatifs & données

Contenu & Objectifs

- Présentation de la démarche des tests d'intrusion externe + Scénarios des tests de pénétration externe depuis Internet
- Présentation des risques de cybersécurité liés aux cybermenaces : failles des applications mobiles, messagerie externe, vitrines WEB
- Démonstrations des tests de pénétration – SGBD Oracle / SQL SERVER / MySQL / SyBase
- Démonstrations des tests de pénétration Applications Mobile
- Démonstration des tests de pénétration des plateformes WEB
- Démonstrations des techniques « Phishing » / campagne de Phishing

Programme : Formation Tests d'intrusion

Jour 3

Protection contre les attaques avancées

Contenu & Objectifs

- Assistance au déploiement des mesures de sécurisation des environnements systèmes & réseau *(solutions de type anti-malwares, chiffrement à la volée / cryptage total et/ou partiel des disques, solutions de type PAM, SIEM , Firewalls nouvelles générations et sécurisation des liaisons VPN par MFA)*
- Comprendre les architectures de sécurité et les mesures de protection avancée *(présentation des études de cas sur des architectures de sécurité réseau complexes)*

Examen & Evaluation des compétences (*)

Type

- Formation en intra

Personnel ciblé

- Informaticiens (RSSI, administrateurs sécurité, réseau, système, Base de données, applicatifs)

Documents à fournir

- Support du cours : Oui / format papier

Autres formes support

Format électronique (séquence vidéo du cours) + présentation des techniques de sécurisation SI sur CDROM et/ou DVD + attestation de formation + Cartables, pauses café, déjeuner

VALSCH Consulting
Expertise Technique & Développement

FORMATION ISO/CEI 27035 LEAD INCIDENT MANAGER

FORMATION CYBERSÉCURITÉ TECHNIQUE Formation ISO/CEI 27035 LEAD INCIDENT MANAGER

VALSCH Consulting
Expertise Technique & Développement

Formation ISO/CEI 27035 Lead Incident Manager

Objectifs

- Maîtriser les concepts, les approches, les méthodes, les outils et les techniques qui permettent une gestion efficace des incidents de sécurité de l'information selon l'ISO/CEI 27035
- Connaître la corrélation entre la norme ISO/CEI 27035 et les autres normes et cadres réglementaires
- Acquérir l'expertise nécessaire pour accompagner une organisation durant la mise en œuvre, la gestion et la tenue à jour d'un plan d'intervention en cas d'incident de la sécurité de l'information
- Acquérir les compétences pour conseiller de manière efficace les organismes en matière de meilleures pratiques de gestion de sécurité de l'information
- Comprendre l'importance d'adopter des procédures et des politiques bien structurées pour les processus de gestion des incidents
- Développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux incidents

Durée

5 jours soit 35 heures.

FORMATION CYBERSÉCURITÉ TECHNIQUE Formation ISO/CEI 27035 LEAD INCIDENT MANAGER

VALSCH Consulting
Expertise Technique & Développement

FORMATION SÉCURISER UN SYSTÈME LINUX/UNIX

FORMATION CYBERSÉCURITÉ TECHNIQUE SÉCURISER UN SYSTÈME LINUX/UNIX

VALSCH Consulting
Expertise Technique & Développement

Formation Sécuriser un système Linux/Unix

Objectifs

Objectifs pédagogiques

- À l'issue de la formation, le participant sera en mesure de :Mesurer le niveau de sécurité de votre système Linux/Unix
- Connaître les solutions de sécurisation du système
- Mettre en place la sécurité d'une application Linux/Unix
- Établir la sécurisation au niveau réseau

Travaux pratiques

Les nombreux exercices seront effectués sur un réseau de serveurs Unix et Linux.

Durée

3 jours,

VALSCH Consulting
Expertise Technique & Développement

FORMATION CYBERSÉCURITÉ, ISO 27032, CERTIFICATION

ISO/IEC 27032
Lead Cybersecurity Manager

FORMATION CYBERSÉCURITÉ TECHNIQUE **Formation Cybersécurité, ISO 27032, certification**

Formation Cybersécurité, ISO 27032, certification

Objectifs

- À l'issue de la formation, le participant sera en mesure de :Connaître les composants et les opérations d'un programme de cybersécurité en conformité avec la norme ISO 27032
- Expliquer l'objectif, le contenu et la corrélation entre l'ISO 27032 et d'autres normes et référentiels
- Maîtriser les concepts, méthodes, normes et techniques pour gérer un programme de cybersécurité
- Piloter un programme de cybersécurité tel que spécifié dans la norme ISO 27032

Durée

5 jours,

FORMATION CYBERSÉCURITÉ TECHNIQUE Formation Cybersécurité, ISO 27032, certification

VALSCH Consulting
Expertise Technique & Développement

Programme de formation

Fondamentaux de la cybersécurité pour les services gouvernementaux et services financiers

Fondamentaux de la cybersécurité pour les services gouvernementaux et services financiers

FORMATION CYBERSÉCURITÉ

VALSCH Consulting
Expertise Technique & Développement

Programme de la formation :

Objectif de formation

L'objectif du séminaire est de permettre aux participants d'acquérir l'expertise et les compétences indispensables à la mise en œuvre, au pilotage et à la pérennisation d'un programme de cybersécurité, en conformité avec la norme ISO/IEC 27032.

ce séminaire permettra de :

- **Comprendre les lignes directrices relatives à la mise en œuvre d'un programme de cybersécurité conforme à la norme ISO 27032 ;**
- **Acquérir l'expertise nécessaire pour assister une organisation dans le management des risques liés à la cybersécurité ;**
- **Acquérir une compréhension globale des mécanismes d'attaques ciblant les plateformes applicatives de la finance numérique ;**
- **Acquérir les connaissances nécessaires pour la sécurisation des applications mobiles ;**
- **Acquérir l'expertise nécessaire au management des incidents de cybersécurité.**

Fondamentaux de la cybersécurité pour les services gouvernementaux et services financiers

FORMATION CYBERSÉCURITÉ

Informations générales sur la formation

Modalités de formation : Répartition équilibrée entre formation théorique et ateliers pratiques (50/50)

- **Lieu du séminaire :** Abidjan
- **Formation dispensée en français**

Un manuel en français contenant plus de 200 pages d'informations et d'exemples

- pratiques sera fourni aux participants. Ce manuel intégrera une **feuille de route**
- **individualisée pour chaque participant** résultant du diagnostic réalisé lors des
- ateliers
pratiques.

Un certificat de participation sera également délivré à l'issue de la formation

Programme détaillé

- **Jour 1 : Introduction : Cybersécurité et notions connexes**

- Présentation des normes ISO 27000, ainsi que du cadre normatif, légal et réglementaire
- Principes fondamentaux de la Cybersécurité
- Politique de Cybersécurité (PCS)
- Approche et méthodologie de mise en œuvre d'un programme de Cybersécurité
- Exemple pratique : Feuille de route (plan d'action) cybersécurité d'un établissement financier
- Savoir rédiger une politique de cybersécurité (PCS)
- Analyser les écarts rapport aux meilleurs pratiques en matière de cybersécurité

- **Jour 2 : Management des risques en matière de cybersécurité**

- Objectifs de la gestion des risques en matière de cybersécurité
- Cadres normatif et méthodologique de management des risques
- Sélection de l'approche et de la méthode d'évaluation des risques
- Gestion des risques : Identification, analyse et traitement du risque *(d'après les dispositions de la norme ISO 27005)*
- Mécanismes d'attaques (cyberattaques) internes, externes et combinées
- Attaques ciblant les applications mobiles
- Attaques ciblant les fournisseurs de services applicatifs au niveau du Cyberspace
- Attaques ciblant les infrastructures des fournisseurs d'accès Internet & opérateurs télécom

Jour 3: Mesures de contrôle de cybersécurité

- Mesures de contrôle applicatives
- Mesures de protection desserveurs
- Mesures de contrôle de l'utilisateur final
- Mesures de contrôl d'accès
- Mesure de partage et coordination de information
- Cyberculture (programme de formation de sensibilisation)

Jour 4 : Sécurité des applications *(focus applications WEB, applications Mobile)*

- Sécurité applicative et norme ISO 27034
- Présentation de l'OWASP 2017 : TOP 10 des risques les plus critiques pour une application WEB Mise en place d'une politique de sécurité applicative
- Bonnes pratiques et mesures de sécurité pour les applications mobile et les applications WEB

Jour 5 : Continuité d'activité & management des incidents de cybersécurité

- Objectifs de la continuité d'activité
- Orientations pour la mise en œuvre d'une stratégie de continuité d'activité Objectifs du management des incidents de cybersécurité
- Intervention et récupération en cas d'incident de cybersécurité
- Tests de cybersécurité, mesure de la performance & amélioration continue

Formation Technique

Programme de la formation spécifique :

Sécurisation de l'environnement système Windows et infrastructures Virtuelles

FORMATION CYBERSÉCURITÉ

SÉCURISATION DE L'ENVIRONNEMENT SYSTÈME ET INFRA VIRTUELLE

Objectifs

- Disposer des connaissances techniques nécessaires pour la mise en œuvre des mesures de sécurité système Windows
- Disposer des connaissances techniques nécessaires pour la mise en œuvre des mesures de sécurité de l'Infrastructure virtuelle (Vmware, Hyper-V)
- Connaitre les solutions et techniques avancées de sécurité Système Windows
- Connaitre

Méthodologie

- Animation d'un atelier technique pour le déploiement des mesures (appui technique, transfert de compétences, formation sur les outils d'audit système et les solutions de sécurité système) :

  - ✓ Présentation des bonnes pratiques de sécurisation des environnements système serveurs Windows & système des postes de travail (NIST/DISA, CisBenchmark)
  - ✓ Présentation des bonnes pratiques de sécurisation des infrastructures virtuelles (Vmware et Hyper-V)
  - ✓ Assistance au déploiement des mesures de sécurisation des environnements systèmes (solutions de type anti-malwares, chiffrement à la volée / cryptage total et/ou partiel des disques, PAM, SIEM)
  - ✓ Assistance à l'installation et à l'utilisation des outils d'audit technique des environnements système + contrôle d'intégrité système (solution open source OSSEC)

Durée calendaire :
- Atelier technique : 3 jours

Livrables

- Fiche de suivi des failles & mise en œuvre des recommandations (fiche type de gestion des vulnérabilités techniques – volet système)
- Politique de filtrage et contrôle d'accès système (règles d'administration système, gestion des accès privilégiés aux systèmes serveurs)
- Spécifications techniques des solutions de sécurisation des systèmes d'exploitation
- Plan de formation des administrateurs système