ESD

CATALOGUE

2018

L'ESD BAC+5

Titre de niveau: (RCNP) reconnu par le ministère du travail et apparu au journal officiel code NSF 326 par arrêter du 16/12/2016. Celui pest disponible en alternance mais aussi sur des formats pour les personnes désirant faire une spécialité en cybersécurité ou bien monter en compétences sur des domaines précis de la sécurité de l'information. L'objectif du diplôme est d'avoir une vision transverse et d'aborder des modules techniques, fonctionnels ou bien managériales dans le domaine.
5 blocs de compétences sont à valider tout au long de la formation avec à travers des travaux sur la gouvernance incluant la gestion des risques, SMSI, PCA/PRA, la réponse à incident, etc. Des modules techniques sont également abordés avec le passage de la certification CEH, du Forensic, Ethical hacking avancé, Appsec et de la mise en place d'infrastructure sécurisée.

Python pour test d'intrusion

Fabrication d'outils pour test d'intrusion avec Python et PS (Scapy, BeautifulSoup, API .net)

Sécurité offensive

Utilisation des techniques offensives avancées et ses outils (Empire, Mimikatz, PTH, Golden ticket, MITM, etc)

ISO 27005/EBIOS

Formation à la gestion des risques suivant la norme ISO 27005 et la méthode de l'ANSSI "EBIOS"

CEH

Formation et préparation à la certification CEH afin de maîtriser les bases de la sécurité offensive

ISO 27001/SMSI

Formation et passage de la certification ISO 27001 Lead Implementer pour la mise en place d'un SMSI

Forensic

Forensic Windows et Linux pour la recherche d'évidence, artefact et analyse de charge (TSK, Rekall, Regripper, dd, GDB, etc)

Cybersécurité et juridique

Sensibilisation aux règlements et lois liées à la SSI (RGPD, CNIL, LPM, Informatique et liberté, article 323)

Sécurité défensive

Protéger les infrastructures avec l'intégration de services (durcissement Windows, Linux, SIEM, PKI, Firewall, IDS, etc)

Veille SSI

Évaluation sur l'approfondissement et la présentation d'un sujet lié à la cybersécurité

PRA/PCA Gestion de crise

Mise en action d'un Plan de reprise et de continuité d'activité

Mener un test d'intrusion

Étude des méthodologies pour la gestion d'un test d'intrusion avec PTES et OWASP testing guide

Appsec/DevSecOps

Étude du TOP OWASP pour l'appréhension technique. Durcisemment d'une application et ajout demodèle SDL, BSIMM

FORENSIQUE WINDOWS

Description:

le premier module a pour but, de faire un panorama des différentes branches et parties prenantes du Forensic (Forensic légal, Réponse à incident, outils, etc.) Une fois cela fait, la collecte de données sur disque, RAM, fichier d'hibernation est étudié avec ses différentes propriétés. Le deuxième module concerne l'approfondissement des systèmes d'exploitation Windows (NTFS, API .net, etc.). La suite est la création d'une timeline et d'y trouver des évidences à l'aide d'artefacts tels que des clés de registre, Shellbag, Prefetch, évènements Windows, etc. Le troisième module consiste à observer les mouvements d'exfiltration, de pivoting et de persistance. Pour finir, une analyse statique et dynamique des charges malveillantes est mis en pratique.

avoir les compétences systèmes pour réponse à incident et une investigation légale sur le OS Microsoft

étudiant, administrateur système, développeur

avec des bases en réseau TCP/IP, Windows et programmation

3 jours

FORENSIQUE RESEAUX

Description:

Le cours commence avec un récapitulatif des différentes souches du Forensic et a quel moment utiliser le forensic réseau. L'ensemble des modules étant technique, l'outil Wireshark est utilisé avec une introduction aux différents items du logiciel. La suite commence par l'investigation des techniques de reconnaissances (Nmap like) et d'homme du milieu (MITM) sur une infrastructure. Le deuxième module consiste à mettre en pratiqu l'analyse des tentatives de craquage de mots de passe ainsi que les attaques sur les communications emails. Le troisième et dernier module permet la recherche et remonté de botnet avec les différentes analyses pour la remontée des C&C.

avoir les compétences systèmes pour réponse à incident et une investigation légale sur le OS Microsoft

étudiant, administrateur système, développeur

avec des bases en réseau TCP/IP, Windows et programmation

3 jours

FORENSIQUE LAMP

Description:

ce cours a pour objectif de monter en compétence sûr de la réponse à incident sur un système Linux apache Mysql PHP. Le premier module introduit les concepts de base d'une application WEB et des différents éléments techniques à prendre en compte pour commencer une investigation. L'introduction aux vulnérabilités dites classiques est effectuée avec la mise en pratique de la détection, collecte et analyse de traces. Les différents artefacts sont mis en évidence dans des cas pratiques pour que le stagiaire puisse reproduire la théorie vue au préalable.

avoir les compétences systèmes pour réponse à incident et une investigation légale sur un système Linux, Apache, MySql, PHP

étudiant, administrateur système, développeur

avec des bases en réseau TCP/IP, Linux et programmation

2 jours

SÉCURITÉ WEB

Description:

aujourd'hui, 75 % des attaques informatiques tirent profit des vulnérabilités applicatives. La sécurisation des applications web est donc primordiale. Durant le cours, le premier module consiste à approfondir les attaques les plus connues sur une application WEB, souvent regroupés par le TOP 10 OWASP (SQLI, XSS, CSRF, IDOR, SSRF, etc.) Ceci étant fait, le deuxième module met en pratique le durcissement de code, de l'infrastructure, des serveurs, avec l'insertion de service SAST, DAST, monté de charge en intégration continue. Les règles telles que CSP, X-Frame-option, HTTOnly, Secure flag, sont ajoutées dans les travaux pratiques. Le troisième module, consiste à l'approbation des bonnes pratiques à la gestion de projets et la gouvernance application par l'étude du SDL (Security Development Lifecycle). Celui-ci utilise les techniques des bugs bar, threat modeling, vérification de l'alignement des exigences de sécurité de l'organisation. Pour terminer, une introduction aux exigences ISO 27001 et 27034 est planchée pour une mise au point sur la gouvernance de la sécurité applicative.

insérer de la sécurité applicative sur l'ensemble d'un système d'information

étudiants, chef de projet, administrateur système, développeur

avoir des connaissances en gestion de projet et développement

5 jours

PYTHON POUR TEST D'INTRUSION

fabriquer des outils avec Python pour un test d'intrusion

5 jours

étudiant, administrateur système, développeur,pentester

avec des bases en réseau TCP/IP et programmation

Description:

ce cours est orienté vers l'utilisation du langage Python et Powershell pour la fabrication d'outils pour le métier de Pentester. Les bibliothèques telles que Scapy, Beautiful Soup, API .net sont étudiées. Le cours commence par la création d'une connexion socket pas à pas afin de créer un reverse shell transparent pour un antivirus.La suite du cours consiste à utiliser ce même socket avec un flux chiffré, l'utilisation du protocole HTTPS et le bypass d'IDS.Le prochain module est orienté sur l'utilisation du framework Scapy avec la construction d'un reverse proxy pour l'exfiltration de données, sniff de packet, manipulation de .pca et technique d'ARP poisoning.
Pour terminer, la construction d'un module pour le logiciel Burp suite et l'ajout d'une charge Powershell indétectable est étudié.

SÉCURITÉ OFFENSIVE

Comprendre les attaques SI, les modéliser, préparer un plan d'action pour les contrer

5 jours

étudiant, administrateur système, consultant en sécurité de l'information

Connaissance de Linux, compréhension des architectures SI actuelles, administration des environ nements Windows / Linux

Description:

Ce cours permet d'avoir une vue d'ensemble sur les attaques modernes pesant sur la sécurité de l'information. La double vision (Attaquant/Défense) permet de comprendre les choix effectués par attaquants, afin de prévoir l'implémentation des mesures de sécurité les plus efficaces possible. De la prise de contrôle de l'organisation aux différentes phases de rebonds interne qu'un attaquant pourrait être tenté d'utiliser, l'ensemble de ces phases seront analysés. Durant la formation, la mise en oeuvre de scénarios réels sera déployé afin d'être plonger au plus près des problématiques (attaquant/défense).

SÉCURITÉ DES ARCHITECTURES

Description:

Ce cours permet d'avoir une vue d'ensemble sur les mécanismes de défense permettant aux organisations de créer une protection efficace et efficiente. La mise en oeuvre d'infrastructure reproduisant les conditions réelles d'une organisation seront mises en oeuvre et confronter aux différentes attaques modernes. L'approche par l'attaque est mise en avant afin d'implémenter et configurer au plus juste les systèmes de défense SI.

Établir un plan de défense adaptés aux menaces actuelles

étudiant, administrateur système, consultant en sécurité de l'information

Connaissance de Linux, compréhension des architectures SI actuelles, administration des environnements Windows / Linux

5 jours

PCA / PRA

Description:

Ce cours permet d'avoir l'ensemble les éléments pour la compréhension et l'implémentation d'un système de management de la continuité d'activité. Il permet de créer un alignement fort avec les besoins en continuité des processus des organisations et s'intègre parfaitement dans une démarche de gestion par le risque. Ce cours permettra d'avoir une vision claire sur les choix liés à la continuité d'activité ainsi que leurs efficiences en fonctions des besoins identifiés par l'organisation. Les différents T.P permettront progressivement d'obtenir l'ensemble des éléments nécessaire à la construction d'un plan de continuité efficient aux différents risques et impacts que l'organisation pourrait rencontrer.

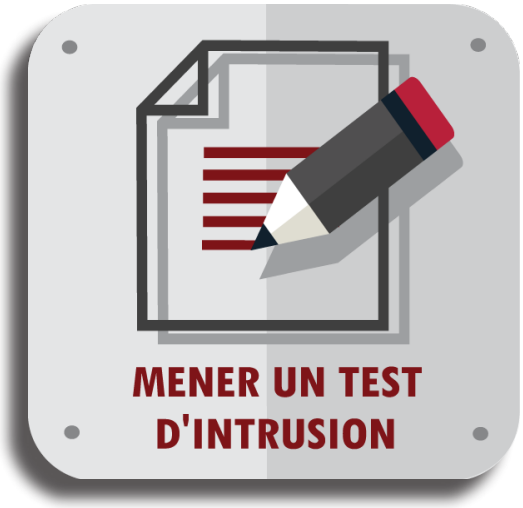
Compréhension des architectures SI actuelles, gestion d'un système d'information (processus, documentation etc..)

étudiant, administrateur système, consultant en sécurité de l'information, responsable des risques, directeur des systèmes d'information

Comprendre et savoir implémenter un plan de continuité/reprise d'activité

5 jours

MENER UN TEST D'INTRUSION



Description:

un test d'intrusion bien mené nécessite une méthode rigoureuse afin de rédiger un rapport de test qui ne se contente pas d'énumérer les vulnérabilités détectées chez le client. À ce titre, l'accent a été mis sur la définition des règles de pré engagement, la réglementation et sur la rédaction du rapport afin qu'il soit en clair et en adéquation avec les craintes et les motivations du client. La méthode PTES et OWASP testing guide pour le WEB est étudiée avec de matérialiser une méthode technique et fonctionnelle à un test d'intrusion. La fin de l'exercice a consisté en une présentation du rapport de test d'intrusion au client. Des études de cas et des labs servent de support à la pédagogie. Ce cours est donc dédié à des chefs de projet en sécurité, RSSI, voir des Pentester désirant monter en compétences sur du fonctionnel.

des bases en gestion de projet et ethical hacking

chef de projet, RSSI, risk manager, pentester

savoir gérer les différentes phases d'un test d'intrusion

5 jours

Certification ISO 27005 et EBIOS

Description:

la formation « ISO/CEI 27005 Risk Manager » vous permettra de développer les compétences pour maîtriser les processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/CEI 27005 comme cadre de référence. Au cours de cette formation, nous présenterons également d'autres méthodes d'appréciation des risques telle que EBIOS et la méthodologie harmonisée d'EMR. Cette formation s'inscrit parfaitement dans le processus de mise en œuvre du cadre SMSI selon la norme ISO/CEI 27001. Après avoir compris l'ensemble des concepts relatifs à la gestion des risques de la sécurité d'information conforme à la norme ISO/CEI 27005, vous pouvez vous présenter à l'examen et postuler au titre de « ISO/CEI 27005 Risk Manager ». En étant titulaire d'une certification « PECB Certified ISO/CEI 27005 Risk Manager », vous démontrez que vous disposez des connaissances et des compétences nécessaires pour réaliser une appréciation optimale des risques de la sécurité de l'information et pour gérer les risques de la sécurité de l'information dans les délais.

des connaissances en gestion de projet

étudiant

appréhender la gestion des risques et savoir mener une analyse. Passage de certification et badge

5 jours

Certification ISO 27001 Lead implementor

Description:

ISO/IEC 27001 Lead Implementer vous permet de développer l'expertise nécessaire pour aider une organisation à établir, mettre en œuvre, gérer et maintenir un Système de Gestion de la Sécurité de l'Information (SMSI). Durant cette formation, vous gagnerez aussi une compréhension approfondie des meilleures pratiques des systèmes de gestion de la sécurité de l'information pour sécuriser les informations sensibles de l'organisation et améliorer la performance globale et l'efficacité. Après avoir maîtrisé tous les concepts nécessaires des systèmes de gestion de la sécurité de l'information, vous pouvez vous présenter à l'examen et demander un certificat d'accréditation «PECB Certified ISO/IEC 27001 Lead Implementer». En étant titulaire d'un certificat PECB Lead Implementer, vous serez en mesure de démontrer que vous avez les connaissances pratiques et les capacités professionnelles nécessaires pour implémenter ISO/IEC 27001 dans une organisation.

des connaissances en gestion de projet

étudiant

appréhender la mise en place d'un SMSI avec l'utilisation des normes ISO/IEC 27001/2 et passage de certification ou badge

5 jours

Certification ISO 27034 sécurité des applications

Description:

La formation ISO/IEC 27034 Lead Implementer vous permet de développer l'expertise nécessaire pour soutenir une organisation dans l'établissement, la mise en œuvre et la gestion de la sécurité applicative (AS).
Pendant cette formation, vous apprendrez les meilleures pratiques des techniques de sécurité des applications et être en mesure d'identifier et d'éviter les vulnérabilités courantes des applications. Après avoir maîtrisé tous les concepts nécessaires des techniques de sécurité applicative, vous pouvez vous présenter à l'examen et postuler pour une certification «PECB Certified ISO/IEC 27034 Lead Implementer». En étant titulaire d'un certificat PECB Lead Implementer, vous serez en mesure de démontrer que vous possédez les connaissances pratiques et les capacités professionnelles nécessaires pour implémenter des techniques de sécurité applicative dans une organisation.

des connaissances en gestion de projet et SSI

étudiant

comprendre la norme ISO/IEC 27034 afin d'intégrer la sécurité applicative sur l'ensemble d'un SI et particulièrement l'imbrication au SMSI

2 ou 5 jours