Cyberdefense

PLANNING FORMATIONS – S2 2024

MARDI, 3 SEPTEMBRE 2024 – DURÉE : 1/2 JOURNÉE (MATIN)

INCIDENT RESPONSE MANAGEMENT – FORMATEUR : FRÉDÉRIC BOURLA

Cette formation est idéale pour entreprendre le long périple de la réponse à incidents, laquelle ne se limite pas à l'acquisition d'outils et de techniques qu'il vous faudra utiliser dans le feu de l'action. La majeure partie du processus consiste en effet à se préparer en amont, et à établir des procédures sur lesquelles vous pourrez compter le moment venu. Cette formation d'une demi-journée est donc une introduction au concept de gestion des incidents, ainsi qu'aux bonnes pratiques, normes et standards sous-jacents. Elle vous permettra de poser les jalons de votre stratégie défensive sous l'angle de la préparation.

MERCREDI, 4 SEPTEMBRE 2024 – DURÉE : 1 JOURNÉE

ATTAQUE D'APPLICATIONS WEB PARTIE 1 – FORMATEUR : ALAIN MOWAT

Ce cours a pour but de préparer le participant à pouvoir non seulement tester la sécurité d'une application Web, mais également de corriger les failles les plus couramment rencontrées. La méthodologie d'analyse d'un site Web est développée en se concentrant tout d'abord sur l'identification des systèmes et des points d'entrées, puis sur l'exploitation de failles comme les injections SQL ou le Cross-Site Scripting. Il s'agit avant tout d'un cours pratique où les participants peuvent exploiter les failles discutées afin de bien comprendre leur fonctionnement et ainsi protéger au mieux leurs propres applications.

JEUDI, 5 SEPTEMBRE 2024 – DURÉE : 1 JOURNÉE

ATTAQUE D'APPLICATIONS WEB PARTIE 2 – FORMATEUR : ALAIN MOWAT

Ce cours est une suite logique du cours « HA1.01 – Attaque d'applications web – Niv. 1 ». Il reprend certains concepts en les poussant plus loin pour montrer que l'exploitation d'une faille permet souvent non seulement de compromettre une application, mais dans certains cas, toute l'infrastructure l'hébergeant. Le cours analyse autant des attaques côté serveur, tels que les XML eXternal Entites, les Local File Inclusion ou autres problèmes de chiffrement faible, que des attaques côté client visant à contourner la «Same Origin Policy» du navigateur.

MARDI, 10 SEPTEMBRE 2024 – DURÉE : 1 JOURNÉE

LOG MANAGEMENT – FORMATEUR : FRÉDÉRIC BOURLA

Cette formation d'une journée aborde les fondamentaux de la journalisation d'événements sur Windows et Linux, les différents types de logs, ainsi que la gestion et l'analyse desdits journaux. Elle complète idéalement la formation « INCIDENT RESPONSE MANAGEMENT » et vise à s'interroger sur ce qu'il faut logger et comment, dans le but de vous permettre d'améliorer vos capacités de réponse aux incidents de sécurité.

JEUDI, 19 SEPTEMBRE 2024 - DURÉE : 1/2 JOURNÉE (MATIN)

SENSIBILISATION DEVELOPPEURS (OWASP TOP 10) – FORMATEUR : ALAIN MOWAT

Découvrez le TOP10 des risques OWASP, les conseils et solutions pour les réduire, ainsi qu'une série d'exemples et conseils adaptés aux langages utilisés par vos équipes (PHP, Java, C, ...).

MARDI, 24 SEPTEMBRE 2024 – DURÉE : 1 JOURNÉE

INCIDENT RESPONSE & FORENSIC ANALYSIS (L1) – FORMATEUR : FRÉDÉRIC BOURLA

Cette formation intensive d'une journée vise à présenter les méthodes et outils d'investigation sur lesquels vous pourrez vous appuyer en cas d'incident de sécurité. Elle vous permettra de plonger dans le monde de la réponse à incidents et de l'analyse forensique, en abordant les différents scénarios d'acquisition de la RAM et des disques durs, puis en se focalisant sur le triage par le biais de l'analyse en directe, ainsi que sur l'investigation approfondie au travers de l'analyse hors ligne.

MARDI, 1 OCTOBRE 2024 – DURÉE : 1 JOURNÉE

INCIDENT RESPONSE & FORENSIC ANALYSIS (L2) – FORMATEUR : FRÉDÉRIC BOURLA

Cette formation intensive d'une journée permet d'approfondir le contenu de la FOR1.01 et d'introduire toutes les notions de base indispensables à la compréhension de la réponse à incident et de l'analyse forensique sur environnement Windows. Elle aborde les scénarios d'acquisition de disque avancés (comme le FDE et les SDD) et vous permettra de plonger dans le coeur du système de fichiers NTFS afin d'en exploiter les principales métadonnées. Vous apprendrez également à réaliser des acquisitions directes du système d'exploitation pour extraire de précieuses informations de ses nombreux artéfacts.

VENDREDI, 11 OCTOBRE 2024 – DURÉE : 1 JOURNÉE

INCIDENT RESPONSE & FORENSIC ANALYSIS (L3) – FORMATEUR : FRÉDÉRIC BOURLA

Cette formation intensive d'une journée permet de compléter les cours FOR1.01 et FOR1.02 en abordant les fondamentaux de l'analyse de malware sous Windows. Elle vise à vous apporter les méthodes et outils nécessaires à la réalisation d'analyses basiques, par le biais des approches statiques et dynamiques. Vous y apprendrez à évaluer rapidement le niveau de dangerosité des fichiers exécutables et autres documents Office.

MARDI, 5 NOVEMBRE 2024 – DURÉE : 1 JOURNÉE

ATTAQUE D'ENVIRONNEMENTS WINDOWS AVEC METASPLOIT – FORMATEUR : JULIEN OBERSON

Cette formation présente les caractéristiques du modèle de sécurité des systèmes Windows ainsi que les attaques les plus courantes contre les environnements d'entreprise. Des démonstrations et des exercices permettent aux participants de mieux comprendre le fonctionnement de ces attaque et – par extension – comment s'en protéger efficacement.

JEUDI, 7 NOVEMBRE 2024 – DURÉE : 1 JOURNÉE

SENSIBILISATION AU DARKNET – FORMATEUR : FRÉDÉRIC BOURLA

Cette formation d'une journée vous permettra d'appréhender les concepts du Darknet et plonger peu à peu dans les coins les plus sombres d'Internet. Elle vise à vous permettre d'améliorer vos capacités de monitoring et de sécurité proactive. Vous y apprendrez notamment à effectuer des recherches et à communiquer sur le réseau TOR, ainsi qu'à évaluer l'impact d'un leak d'une société tierce pour votre entreprise.

MARDI, 19 NOVEMBRE 2024 – DURÉE : 1 JOURNÉE

ATTAQUE D'APPLICATION MOBILE – FORMATEUR : FABRICE CARALINDA

Ce cours a pour but de partager des expériences et des connaissances dans les audits d'applications mobiles sous Android et iOS. Cette formation présente des processus et des techniques de vérification aidant un participant à préparer un environnement de test idéal pour évaluer la sécurité d'une application. Entre autres, elle présente plusieurs méthodologies pour des tests de sécurité passant de l'analyse locale à l'inspection du trafic réseau d'une application. Ce cours fournit également plusieurs exemples d'automatisation de tâches fastidieuses qui interviennent dans la majorité des audits de sécurité mobile (contournement root/jailbreak detection ou certificate pinning).

CONDITIONS ET PRIX

Formation « à la carte »

CHF 2'000 valable pour une journée de formation spécifique et pour un participant
(CHF 1'000 pour ½ journée).

« Pass formation »

CHF 8'000 valable pour une année calendaire dès la date d'inscription et incluant toutes les formations proposées, pour un participant. Le pass est transmissible et non-nominatif ; il est ainsi possible d'inscrire une personne différente par formation.

Payable à 30 jours dès inscription.

Les cours collectifs ne sont pas remboursables, même si le participant devait ne pas pouvoir être présent. En revanche, une autre personne peut le remplacer.

BackOffice@ch.orangecyberdefense.com
www.orangecyberdefense.com/ch/fr
+41 (0)21 802 64 01
Rue du Sablon 4
1110 Morges, Switzerland