Formation Détection d'intrusion et SOC

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Ce cours très pratique présente les techniques d'attaque les plus évoluées à ce jour et montre comment les détecter. A partir d'attaques réalisées sur des cibles identifiées (serveurs Web, clients, réseaux, firewall, bases de données...), vous apprendrez à déclencher la riposte la plus adaptée. Vous apprendrez également le concept de SOC ainsi que l'ensemble des outils nécessaires en tant qu'analyste SOC.

Référence	TRU
Durée	4 jours (28h)
Tarif	2 920 €HT
Repas	repas inclus

Objectifs

| Identifier les techniques d'analyse et de détection
| Déployer différents outils de détection d'intrusion
| Mettre en oeuvre les solutions de prévention et de détection d'intrusions
| Identifier les concepts et l'environnement d'un SOC
| utiliser les outils d'analyse

Public

| Techniciens et administrateurs systèmes et réseaux.

Prérequis

| Bonnes connaissances en réseaux et sécurité.
| Connaître le guide d'hygiène sécurité de l'ANSSI.
| Avoir suivi le parcours introductif à la cybersécurité.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 3 au 6 juin 2025
du 9 au 12 septembre 2025
du 16 au 19 décembre 2025

PARIS

du 20 au 23 mai 2025
du 2 au 5 septembre 2025
du 9 au 12 décembre 2025

VOIR TOUTES LES DATES

Programme de la formation

Bien comprendre les protocoles réseaux
| D'autres aspects des protocoles IP, TCP et UDP.
| Zoom sur ARP et ICMP.
| Le routage forcé de paquets IP (source routing).
| La fragmentation IP et les règles de réassemblage.
| De l'utilité d'un filtrage sérieux.
| Sécuriser ses serveurs : un impératif.
| Les parades par technologies : du routeur filtrant au firewall stateful inspection ; du proxy au reverse proxy.
| Panorama rapide des solutions et des produits.
| Travaux pratiques : Visualisation et analyse d'un trafic classique. Utilisation de différents sniffers.

Les attaques sur TCP/IP
| Comment les pirates informatique mettent en oeuvre le "Spoofing" IP.
| Réaliser des attaques par déni de service.
| La technique de la prédiction des numéros de séquence TCP.
| Vol de session TCP : Hijacking (Hunt, Juggernaut).
| Comprendre comment les pirates arrivent à réaliser des attaques sur SNMP.
| Attaque par TCP Spoofing (Mitnick) : démystification.
| Travaux pratiques : Injection de paquets fabriqués sur le réseau. Utilisation au choix des participants d'outils graphiques, de Perl, de C ou de scripts dédiés.

Intelligence Gathering
| Chercher les traces : interrogation des bases Whois, les serveurs DNS, les moteurs de recherche.
| Apprendre les techniques pour mettre en place l'identification des serveurs.
| Comprendre le contexte : analyser les résultats, déterminer les règles de filtrage, cas spécifiques.
| Travaux pratiques : Recherche par techniques non intrusives d'informations sur une cible potentielle (au choix des participants). Utilisation d'outils de scans de réseaux.

Détecter les trojans et les backdoors
| Etat de l'art des backdoors sous Windows et Unix. Qu'est ce un backdoor ?
| Comment mettre en place des backdoors et des trojans.
| Le téléchargement de scripts sur les clients, exploitation de bugs des navigateurs.
| Les "Covert Channels" : application client-serveur utilisant ICMP.
| Exemple de communication avec les Agents de Déni de Service distribués.
| Travaux pratiques : Analyse de Loki, client-serveur utilisant ICMP. Accéder à des informations privées avec son navigateur.

Attaques et exploitation des failles
| Prise de contrôle d'un serveur : recherche et exploitation de vulnérabilités.
| Exemples de mise en place de "backdoors" et suppression des traces.
| Comment contourner un firewall (netcat et rebonds) ?
| Les techniques pour effectuer la recherche du déni de service.
| Qu'est ce que le déni de service distribué (DDoS)? Comment les pirates s'organisent pour effectuer une telle attaque ?
| Les attaques par débordement (buffer overflow).
| Exploitation de failles dans le code source. Techniques similaires : "Format String", "Heap Overflow".
| Quelles sont les vulnérabilités dans les applications Web ? Comment les détecter et se protéger ?
| Comment les personnes malveillantes arrivent à voler les informations dans une base de données.
| Qu'est ce que sont les RootKits.
| Travaux pratiques : Exploitation du bug utilisé par le ver "Code Red". Obtention d'un shell root par différents types de buffer overflow. Test d'un déni de service (Jolt2, Ssping). Utilisation de netcat pour contourner un firewall. Utilisation des techniques de "SQL Injection" pour casser une authentification Web.

Le SOC (Security Operation Center)
| Qu'est-ce qu'un SOC ?
| A quoi sert-il ? Pourquoi de plus en plus d'entreprises l'utilisent ?
| Les fonctions du SOC : Logging, Monitoring, Reporting audit et sécurité, analyses post incidents.
| Les bénéfices d'un SOC.
| Les solutions pour un SOC.
| Le SIM (Security Information Management).
| Le SIEM (Security Information and Event Management).
| Le SEM (Security Event Management).
| Exemple d'une stratégie de monitoring.

Le métier de l'analyste SOC
| En quoi consiste le métier de l'analyste SOC ?
| Quelles sont ses compétences ?
| Monitorer et trier les alertes et les événements.
| Savoir prioriser les alertes.

Comment gérer un incident ?
| Les signes d'une intrusion réussie dans un SI.
| Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
| Comment réagir face à une intrusion réussie ?
| Quels serveurs sont concernés ?
| Savoir retrouver le point d'entrée et le combler.
| La boîte à outils Unix/Windows pour la recherche de preuves.
| Nettoyage et remise en production de serveurs compromis.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.