Formation Lutte informatique défensive

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

SOC, CERT et CTI, autant d'acronymes au coeur de la Lutte Informatique Défensive (LID). La LID constitue l'ensemble coordonné d'actions qui consistent à détecter, analyser, prévenir des cyberattaques, et à y réagir le cas échéant.
En quatre jours, cette formation couvre une vue d'ensemble des processus et moyens exploités par les équipes de CTI ,de SOC et de CERT pour assurer les fonctions de détection, de confinement et d'assainissement des menaces informatiques.
L'équilibre entre les aspects théoriques et pratiques de la formation assure au stagiaire l'acquisition de compétences durables qu'il saura aisément actionner pour mettre en place la posture de défense optimale de son organisation face aux cyber-menaces actuelles.

Référence	LID14
Durée	4 jours (28h)
Tarif	à partir de 3 400 €HT

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| Identifier l'utilité de la CTI, des SOC et des CERT/CSIRT
| Connaître les outils et technologies utilisés
| Savoir comment analyser et détecter une menace
| Donner une vision complète des moyens de défense face aux menaces

Public

| RSSI, DSI
| consultants en sécurité
| ingénieurs, techniciens
| administrateurs systèmes & réseaux
| développeurs

Prérequis

| Connaissances de base en système, réseau et développement.
| Connaissance de l'environnement Linux conseillée.

Programme de la formation

Introduction
CTI
| Définition
| Les règles
| Analyser une intrusion
| Partager

SOC
| Contexte et besoin
| Terminologie
| Législation et cadre réglementaire
| Les grandes étapes de la détections d'incidents
| Établir une stratégie de détection d'intrusion
| Capture et analyse de l'activité pour la détection d'intrusion
| NIDS: Network Intrusion Detection System
| HIDS: Host Intrusion Detection System
| Phase de collecte et d'analyse des évènements
| Exemples de SIEM

CERT
| Comprendre la menace
| La réponse à incidents
| Organisation du SOC/CERT
| L'analyse forensique
| L'analyse de malware
| Productions d'indicateurs de compromission et de règles de détection
| Outillage pour l'investigation

La LID passe à l'échelle
| Intelligence et Operations
| IACD
| Machine Learning Non-supervisé pour l'anomaly détection
| Machine Learning supervisé

Conclusions sur l'automatisation de la LID

Informations pratiques

Il est demandé aux stagiaires de se munir d'un ordinateur portable portable :

| Ubuntu ou Debian à jour
| RAM: minimum 6Go, conseillé 8Go
| Equipé de Virtual Box (logiciel gratuit)

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.

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.