Formation Collecte et analyse des logs, un SIEM pour optimiser la sécurité de votre SI

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

Cette formation vous permettra d'acquérir une vision d'ensemble des problématiques de la supervision, des obligations légales concernées en matière de conservation des données et de maîtriser rapidement les compétences nécessaires pour mettre en place une solution logicielle adaptée à votre besoin.

Référence	LOGS
Durée	2 jours (14h)
Tarif	1 590 €HT
Repas	repas inclus

Objectifs

| Identifier les obligations légales en matière de conservation des données
| Identifier la démarche d'une analyse de log
| Installer et configurer Syslog
| Appréhender la corrélation et l'analyse avec SEC

Public

| Administrateurs systèmes et réseaux.

Prérequis

| Bonnes connaissances des réseaux, des systèmes et de la sécurité des SI.

Programme de la formation

Introduction
| La sécurité des Systèmes d'Information.
| Les problématiques de la supervision et des logs.
| Les possibilités de normalisation.
| Quels sont les avantages d'une supervision centralisée ?
| Les solutions du marché.

La collecte des informations
| L'hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
| Le Security Event Information Management (SIEM). Les événements collectés du SI.
| Les journaux système des équipements (firewalls, routeurs, serveurs, bases de données, etc.).
| La collecte passive en mode écoute et la collecte active.
| Travaux pratiques : Démarche d'une analyse de log. La géolocalisation d'une adresse. La corrélation de logs d'origines différentes, visualiser, trier et chercher les règles.

Syslog
| Le protocole Syslog.
| La partie client et la partie serveur.
| Centraliser les journaux d'événements avec Syslog.
| Syslog est-il suffisant ? Avantages et inconvénients.
| Travaux pratiques : Installation et configuration de Syslog. Exemple d'analyse et de corrélation des données.

Le programme SEC
| Présentation de SEC (Simple Event Correlator).

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 30 au 31 mai 2024
du 3 au 4 octobre 2024
du 19 au 20 décembre 2024

PARIS
du 23 au 24 mai 2024
du 26 au 27 septembre 2024
du 12 au 13 décembre 2024

LYON
du 30 au 31 mai 2024
du 3 au 4 octobre 2024
du 19 au 20 décembre 2024

VOIR TOUTES LES DATES

| Le fichier de configuration et les règles.
| Comment détecter des motifs intéressants ?
| La corrélation et l'analyse avec SEC.
| Travaux pratiques : Installation et configuration de SEC. Exemple d'analyse et de corrélation des données.

Le logiciel Splunk
| L'architecture et le framework MapReduce. Comment collecter et indexer les données ?
| Exploiter les données machine. L'authentification des transactions.
| L'intégration aux annuaires LDAP et aux serveurs Active Directory.
| Les autres logiciels du marché : Syslog, SEC (Simple Event Correlator), ELK (suite Elastic), Graylog, OSSIM, etc
| Travaux pratiques : Installation et configuration d'un logiciel (Splunk, ELK ou autre). Exemple d'analyse et de corrélation des données.

La législation française
| La durée de conservation des logs. Le cadre d'utilisation et législation. La CNIL. Le droit du travail.
| La charte informatique, son contenu et le processus de validation.
| Comment mettre en place une charte informatique ?
| Sa contribution dans la chaîne de la sécurité.
| Travaux pratiques : Exemple de mise en place d'une charte informatique.

Conclusion
| Les bonnes pratiques. Les pièges à éviter. Choisir les bons outils. Le futur pour ces applications.

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.