

Collecte et analyse des logs, optimiser la sécurité de votre SI

-Référence: **PL-56**

-Durée: **2 Jours (14 Heures)**

Les objectifs de la formation

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

A qui s'adresse cette formation ?

POUR QUI :

- Administrateurs systèmes et réseaux.

PRÉREQUIS :

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

Programme

• Introduction

- Présentation et standards.
- Architectures.
- Autorité de certification.
- Kerberos.

• 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, 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).
 - 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.
 - Travaux pratiques Installation et configuration de Splunk.
 - 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.

- **Conclusions**

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

- **L'accès Internet des utilisateurs**

- Pourquoi un proxy ? Squid.
- Installation.
- Configuration.
- Authentification.
- Filtrage d'URL et de contenu.
- Contrôle des sites avec Squid Guard.
- Formats des logs.
- Travaux pratiques Mise en oeuvre : Squid, SquidGuard.



(+212) 5 22 27 99 01



(+212) 6 60 10 42 56



Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7ème étage N° 30
Casablanca 20340, Maroc