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

Cours Pratique de 2 jours - 14h
Réf : LOG - Prix 2025 : 1 700 HT

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.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaitre les obligations légales en matière de conservation des données

Connaitre la démarche d'une analyse de log

Installer et configurer Syslog

Appréhender la corrélation et l'analyse avec SEC

TRAVAUX PRATIQUES

De nombreux exercices et études de cas seront proposés tout au long de cette formation.

LE PROGRAMME

dernière mise à jour : 05/2024

1) 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.

2) 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.

3) 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.

4) Le programme SEC

- Présentation de SEC (Simple Event Correlator).
- Le fichier de configuration et les règles.
- Comment détecter des motifs intéressants ?

PARTICIPANTS

Administrateurs systèmes et réseaux.

PRÉREQUIS

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

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

- La corrélation et l'analyse avec SEC.

Travaux pratiques : Installation et configuration de SEC. Exemple d'analyse et de corrélation des données.

5) 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.

6) 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.

7) Conclusion

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

LES DATES

CLASSE À DISTANCE	PARIS
2025 : 23 juin, 08 sept., 13 nov.	2025 : 01 sept., 06 nov.