Date de publication : 24/07/2025

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

Cours pratique - 3j - 21h00 - Réf. LCA
Prix : 2470 € H.T.

4,3 / 5

Clé en main

Formation éligible au financement Mobilités

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, le participant sera en mesure de :

- 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

Public concerné

Administrateurs système et réseau.

Prérequis

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

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Méthodes et moyens pédagogiques

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

PARTICIPANTS

Administrateurs système et réseau.

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.

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.

Programme de la formation

1 La collecte des informations

- L'hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
- Le Security Information and Event 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.

2 Optimiser la sécurité du SI : outils, bonnes pratiques, pièges à éviter

- Panorama des solutions et des produits.
- Étude de Syslog.
- Le programme SEC.
- Le logiciel Splunk.
- La législation française.

Travaux pratiques

Installation et configuration de Syslog, de SEC, de Splunk, ELK ou autre. Exemple d'analyse et de corrélation des données.

3 La détection d'intrusion, principales problématiques

- Bien comprendre les protocoles réseaux (TCP, UDP, ARP, ICMP, routeurs, firewall, proxy...).
- Les attaques sur TCP/IP (spoofing, déni de service, vol de session, attaque SNMP...).
- Intelligence gathering, recherche de traces, scans de réseaux.
- Détecter trojans, backdoors, exploitation de bugs navigateurs, covert channels, agents de déni de service distribués...
- Attaques et exploitation des failles (prise de contrôle, DDoS, buffer overflow, rootkits...).

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.

Découvrez-les sur notre page Comment financer sa formation ou contactez votre conseiller formation.

Financement par les OPCO

- Adhérents Mobilités, découvrez les avantages négociés par votre OPCO en cliquant ici

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation 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 participant 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.

Horaires

Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.
Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts.
Pour les formations de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 16h le dernier jour.

Dates et lieux

CLASSE À DISTANCE
2026 : 11 mars, 1 juin, 9 sep., 5 oct., 16 nov.

PARIS LA DÉFENSE
2026 : 1 juin, 9 sep., 5 oct., 16 nov.

LYON
2026 : 1 juin, 9 sep., 16 nov.

NANTES
2026 : 1 juin, 9 sep., 16 nov.