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

Cours Pratique de 3 jours - 21h
Réf : LCA - Prix 2024 : 2 390CHF 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

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

LE PROGRAMME

dernière mise à jour : 07/2022

1) 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.

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

- Panorama des solutions et des produits.
- Etude 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...).

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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LES DATES

CLASSE À DISTANCE
2024 : 22 mai, 10 juin, 11 sept.,
13 nov.