ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation Fondamentaux de SAP Enterprise Threat Detection

SAP Enterprise Threat Detection Fundamentals

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

Objectifs

| Identifier ce qu'est SAP Enterprise Threat Detection et son fonctionnement
| Avoir une compréhension de base des composants techniques, des connexions système et des options de configuration
| Obtenir une vue détaillée des différentes données de journal provenant en particulier des systèmes SAP ERP
| Ingérer des données de journal non pré-apprises/non-SAP dans ETD
| Identifier le modèle de données sémantique d'ETD, c'est-à-dire les événements de journal sémantique et les attributs sémantiques
| Identifier le traitement des alertes dans ETD
| Identifier l'analyse de la sécurité dans ETD et Threat Hunting

Référence	SECETD
Durée	3 jours (21h)
Tarif	2 460 €HT

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Public

| Analyste/spécialiste/expert en sécurité SAP
| Analyste/spécialiste/expert en sécurité informatique
| Membre de l'équipe interne de réponse à la sécurité
| Responsable de la sécurité et de la conformité
| Administrateur du système
| Architecte système
| Consultant en technologie

Prérequis

| Aucun

Programme de la formation

Introduction
Technical Overview - Solution Architecture
Technical Overview - Log Sources
Semantic Data Model
Technical Overview - System Landscape, Sizing and High Availability
Readiness Checks and Troubleshooting/Monitoring (Hana Cockpit-Tools/Smart Data Streaming)
Pattern Creation Introduction
Technical Overview - High Availability, Log-Loss Prevention, Pattern Replay
Integration Scenarios - 3rd Party to ETD
Integration Scenarios - ETD to 3rd Party
Onboarding Lifecycle Overview
Alert Processing
Business Process Threat Patterns
Pseudonymization of User Data
Monitoring Dashboard
Compliance (Retention period, ETD logs, Who did what in ETD?)
Good Practices on Onboarding Lifecycle

Read Access Logging and UI logging as Special Log Sources
Pattern Building Best Practices
Custom Extensions
Possible role-play with exchanging roles, one group of participants acting as attackers, the other group acting as defenders.

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.

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.