Date de publication : 05/12/2024

Formation : Using Splunk Enterprise Security (USES)

Cours officiel SP-USES, préparation à l'examen

Formation pratique - 2j - 14h00 - Réf. US1
Prix : 2020 € H.T.

Avec cette formation, vous apprendrez à utiliser Splunk pour collecter, analyser et générer des rapports sur les données, à Enrichir les données opérationnelles à l'aide de recherches et de flux, à créer des alertes en temps réel, à réaliser du scripting sur Splunk, à intégrer des graphiques avancés, à utiliser l'API de Splunk, à mettre en place les bons réflexes d'exploitation de Splunk, à améliorer l'exploitation de données avec Splunk, à reconnaître les obligations légales en matière de conservation des données, à définir la démarche d'une analyse de log, et bien plus encore.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Identifie les concepts, fonctionnalités et capacités ES
- Surveiller la sécurité et enquête sur les incidents
- Utiliser les avertissements basés sur le risque d'analyse d'alerte.
- Présenter les actifs et les identités
- Créer et utiliser les enquêtes et investigation Workbench
- Détecter les types de menaces connues
- Surveiller les nouveaux types de menace
- Utiliser des outils d'analyse et des tableaux de bord
- Analyser le comportement des utilisateurs pour détecter les menaces internes
- Utiliser des outils de renseignement pour analyser les menaces
- Utiliser le protocole d'intelligence

Public concerné

Professionnel de la sécurité réseau.

Prérequis

Avoir une bonne compréhension et des connaissances fondamentales sur Splunk.

PARTICIPANTS

Professionnel de la sécurité réseau.

PRÉREQUIS

Avoir une bonne compréhension et des connaissances fondamentales sur Splunk.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi 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 trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
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.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

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 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.

Programme de la formation

1 Faire ses premiers pas avec ES

- Décrire les fonctionnalités et capacités de Splunk Enterprise Security (ES).
- Expliquer comment ES aide les professionnels de la sécurité à prévenir détecter et répondre aux menaces.
- Décrire les recherches de corrélation, les modèles de données et les événements notables.
- Décrire les rôles des utilisateurs dans ES.
- Connecter-vous à Splunk Web et accédez à Splunk for Enterprise Security.

2 Surveiller la sécurité et enquêter sur les incidents.

- Utilisez le tableau de bord Security Posture pour surveiller l'état de l'ES.
- Utilisez le tableau de bord d'examen des incidents pour enquêter sur les événements notable.
- S'approprier un incident et le faire progresser dans le flux de travail d'enquête.
- Créer des événements marquants.
- Supprimer les événements notables.

3 Supprimer les événements notables.

- Donner un aperçu des alertes basées sur les risques.
- Afficher les risques notables et les informations sur les risques sur le tableau de bord d'examen des incidents.
- Expliquer les scores de risque et comment modifier le score de risque d'un objet.
- Consulter le tableau de bord d'analyse des risques.
- Décrire les annotations.
- Décrire le processus de récupération des données LDAP pour une recherche d'actif ou d'identité.

4 Identifier les actifs et identités

- Donner un aperçu du cadre ES Assets and Identities.
- Afficher des exemples où des données d'actifs ou d'identité sont manquantes dans les tableaux de bord ES.
- Afficher des exemples où des données d'actifs ou d'identité sont manquantes dans les évènements notables.
- Voir l'interface de gestion des actifs et des identités.
- Afficher le contenu d'une table de recherche d'actif ou d'identité.

5 Mener des enquêtes

- Utiliser les enquêtes pour gérer l'activité de réponse aux incidents.
- Utiliser l'atelier d'investigation pour gérer visualiser et coordonner les enquêtes sur les incidents.
- Ajoutez divers éléments aux enquêtes notes, historique des actions collaborateurs évènements actifs identités.
- Utiliser des calendriers, des listes et des résumés d'enquête pour documenter et examiner les efforts.
- Utiliser des calendriers listes des résumés d'enquête pour examiner les efforts d'analyse d'atténuation des violations.

6 Analyser les tableaux de bord du domaine de sécurité

- Décrire les domaines de sécurité ES.
- Utiliser les tableaux de bord du domaine de sécurité pour résoudre diverses menaces de sécurité.
- Découvrez comment lancer les tableaux de bord du domaine de sécurité à partir de l'examen des incidents.
- Découvrez comment lancer les tableaux de bord du menu Action d'un événement notable.

7 Utiliser l'intelligence utilisateur

- Comprendre et utiliser l'analyse de l'activité des utilisateurs.
- Utiliser des enquêteurs pour analyser les événements liés à un actif ou à une identité.
- Utiliser les anomalies d'accès pour détecter les modèles d'accès suspects.

8 Utiliser l'intelligence Web

- Utilisez les tableaux de bord de web intelligence pour analyser votre environnement réseau.
- Filtrer et mettre en évidence les événements.

9 Analyser les renseignements sur les menaces

- Donner un aperçu du cadre Threat Intelligence.
- Donner un aperçu et de la façon dont les informations sur les menaces sont configurées dans ES.
- User du tableau de bord Activité des menaces pour voir quelles sources de menaces interagissent avec l'environnement.
- Utiliser le tableau de bord Threat Artifacts pour examiner l'état des informations sur les menaces.

10 Utiliser le renseignement protocolaire

- Expliquer comment les données réseau sont entrées dans les événements Splunk.
- Décrire les événements du flux.
- Donner un aperçu des tableaux de bord Protocol Intelligence.
- Analyser la manière dont ils peuvent être utilisés pour analyser les données du réseau.

Options

Certification : 230 € HT

Cette formation prépare à la certification "Splunk Certified Cybersecurity Defense Analyst (SCCDA)".
Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.