

Administering Splunk Enterprise Security

2 jours (13,5 heures)

Perfectionnement

Classe à distance

à partir de

1 500 € HT par personne (TVA en vigueur)

Contenu mis à jour le 25/09/2026. Document téléchargé le 01/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Administrer, personnaliser et optimiser Splunk Enterprise Security (ES) pour l'adapter aux besoins métiers et SOC.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Analystes SOC et ingénieurs SOC.

Prérequis

Avoir suivi la formation SPLUNK-USES "Using Splunk Enterprise Security". Il est également recommandé d'avoir suivi les formations "Intro to Splunk", "Using Fields", "Visualizations", "Search Under the Hood", "Intro to Knowledge Objects", "Creating Knowledge Objects", "Creating Field Extractions", "Enriching Data with Lookups", "Data Models", "Introduction to Dashboards", "Splunk Enterprise System Administration", "Splunk Enterprise Data Administration", "Splunk Cloud Administration" ou d'avoir les connaissances équivalentes.

Programme

1 Pendant votre formation

Administering Splunk Enterprise Security

Introduction à Enterprise Security

- Expliquer le rôle d'un SIEM
- Présenter Splunk Enterprise Security (ES)
- Décrire les détections et les findings
- Configurer les rôles et les permissions dans ES
- Présenter la navigation dans ES

Personnalisation de la file d'attente analyste et des findings

- Présenter la file d'attente analyste
- Créer et utiliser des vues de file d'attente analyste
- Personnaliser la file d'attente analyste
- Modifier l'urgence
- Créer de nouveaux statuts
- Ajouter des champs aux attributs de finding
- Créer des findings ad hoc
- Supprimer des findings

Gestion des investigations

- Présenter le fonctionnement d'une investigation
- Utiliser et créer des plans de réponse
- Ajouter des événements Splunk à une investigation
- Utiliser les playbooks et les actions

Gestion des assets et des identités

- Examiner l'interface de gestion des assets et des identités
- Décrire les collections KV Store des assets et des identités
- Configurer et ajouter des lookups d'assets et d'identités à l'interface
- Configurer les paramètres et les champs pour les lookups d'assets et d'identités
- Expliquer le processus de fusion des assets et des identités
- Décrire le processus de récupération des données LDAP pour la recherche d'un asset ou d'une identité

Normalisation des données

- Comprendre comment ES utilise les modèles de données accélérés
- Vérifier que les données sont correctement configurées pour une utilisation dans ES

- Valider les configurations de normalisation
- Installer des add-ons supplémentaires
- Ingérer des données personnalisées dans ES
- Créer un add-on pour un sourcetype personnalisé
- Décrire le dépannage des add-ons

Ingénierie de détection

- Présenter la création de détections basées sur les événements
- Examiner l'éditeur de détections
- Présenter la création de détections basées sur les findings

Alertes basées sur les risques

- Présenter les alertes basées sur les risques (RBA)
- Expliquer les scores de risque et comment ils peuvent être modifiés par les détections ou manuellement
- Examiner le tableau de bord d'analyse des risques
- Comprendre les détections basées sur les findings
- Décrire les annotations
- Consulter les informations de risque dans les findings de la file d'attente analyste

Gestion du renseignement sur les menaces

- Comprendre et configurer le renseignement sur les menaces
- Utiliser l'interface de renseignement sur les menaces pour configurer les listes de menaces
- Configurer de nouvelles listes de menaces

Configuration post-déploiement

- Présenter les exigences générales d'installation d'ES
- Expliquer les différents add-ons et leur emplacement d'installation
- Détailler les prérequis d'installation d'ES
- Décrire l'application Splunk_TA_ForIndexers et son emplacement d'installation
- Définir les options de configuration générales
- Configurer les informations de domaine local et cloud
- Travailler avec le KV Store d'Incident Review
- Personnaliser la navigation
- Configurer les recherches d'indicateurs clés

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

[Accessibilité aux personnes en situation de handicap](#)

Sessions

À distance

Du 18 novembre 2026 au 19 novembre 2026