

Using Splunk Enterprise Security

2,5 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 03/10/2026.

Objectifs

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

- Identifier les concepts, fonctionnalités et capacités de Splunk Enterprise Security
- Surveiller la sécurité et investiguer des incidents
- Utiliser les alertes basées sur les risques et analyser les scores de risque
- Gérer les assets et les identités
- Créer des investigations à l'aide de l'Investigation Workbench
- Détecter les types de menaces connus
- Surveiller l'apparition de nouvelles menaces
- Exploiter les outils analytiques et les tableaux de bord
- Analyser le comportement des utilisateurs afin d'identifier les menaces internes
- Utiliser les outils de renseignement sur les menaces
- Mettre en pratique le renseignement sur les protocoles.

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

À qui s'adresse cette formation ?

Analystes SOC, équipes sécurité, RSSI, Blue Team ou toute personne utilisant Splunk Enterprise Security au quotidien.

Prérequis

Il est recommandé d'avoir suivi les formations "Intro to Splunk", "Using Fields", "Visualizations", "Search Under the Hood", "Intro to Knowledge Objects", "Introduction to Dashboards" ou d'avoir les connaissances équivalentes.

Programme

1 Pendant votre formation

Using Splunk Enterprise Security

Prise en main d'ES

- Décrire les fonctionnalités et capacités de Splunk Enterprise Security (ES)
- Expliquer comment ES aide les praticiens 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
- Se connecter à Splunk Web et accéder à Splunk Enterprise Security

Surveillance de la sécurité et investigation d'incidents

- Utiliser le tableau de bord Security Posture pour surveiller l'état d'ES
- Utiliser le tableau de bord Incident Review pour investiguer les événements notables
- Prendre en charge un incident et le faire progresser dans le workflow d'investigation
- Créer des événements notables
- Supprimer des événements notables

Alertes basées sur les risques

- Présenter les alertes basées sur les risques
- Consulter les Risk Notables et les informations de risque dans le tableau de bord Incident Review
- Expliquer les scores de risque et comment modifier le score de risque d'un objet
- Examiner le tableau de bord Risk Analysis
- Décrire les annotations
- Décrire le processus de récupération des données LDAP pour la recherche d'un asset ou d'une identité

Assets et identités

- Présenter le framework Assets and Identities d'ES
- Montrer des exemples où les données d'asset ou d'identité sont manquantes dans les tableaux de bord ou les événements notables d'ES
- Consulter l'interface de gestion des assets et identités

- Afficher le contenu d'une table de correspondance d'assets ou d'identités

Investigations

- Utiliser les investigations pour gérer les activités de réponse aux incidents
- Utiliser l'Investigation Workbench pour gérer, visualiser et coordonner les investigations d'incidents
- Ajouter différents éléments aux investigations (notes, historique des actions, collaborateurs, événements, assets, identités, fichiers et URL)
- Utiliser les chronologies, listes et résumés d'investigation pour documenter et examiner les analyses de brèches et les efforts de remédiation

Tableaux de bord des domaines de sécurité

- Décrire les domaines de sécurité d'ES
- Utiliser les tableaux de bord des domaines de sécurité pour diagnostiquer diverses menaces
- Apprendre à lancer les tableaux de bord des domaines de sécurité depuis Incident Review et depuis le menu Action d'un événement notable

Renseignement utilisateur

- Comprendre et utiliser l'analyse de l'activité des utilisateurs
- Utiliser les investigateurs pour analyser les événements liés à un asset ou une identité
- Utiliser les anomalies d'accès pour détecter des schémas d'accès suspects

Renseignement Web

- Utiliser les tableaux de bord de renseignement Web pour analyser votre environnement réseau
- Filtrer et mettre en évidence des événements

Renseignement sur les menaces

- Présenter le framework de renseignement sur les menaces et sa configuration dans ES
- Utiliser le tableau de bord Threat Activity pour identifier les sources de menaces interagissant avec votre environnement
- Utiliser le tableau de bord Threat Artifacts pour examiner l'état des informations de renseignement sur les menaces dans votre environnement

Renseignement sur les protocoles

- Expliquer comment les données réseau sont intégrées dans les événements Splunk
- Décrire les événements de flux
- Présenter les tableaux de bord Protocol Intelligence et leur utilisation pour analyser les données réseau

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 16 novembre 2026 au 18 novembre 2026