

Sessions garanties disponibles

Formation Splunk

Réf. SF33531

Maîtrisez Splunk et transformez vos données en informations exploitables par toute votre organisation !

4 j Durée	3 200 € HT Inter / participant	9 000 € HT Intra (≤12 pers.)	1 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Découvrir le fonctionnement et les capacités de Splunk
- ✓ Apprendre le langage SPL pour requêter les données efficacement
- ✓ Enrichir les données opérationnelles à partir de sources externes
- ✓ Créer des tableaux de bord dynamiques pour l'aide à la décision et la synthèse d'informations
- ✓ Créer des requêtes matures pour la détection d'attaque

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Auditeurs, Business analysts, Responsables de la sécurité des systèmes d'information (RSSI)

Prérequis Connaissances informatiques générales (qu'est-ce qu'une adresse IP, une authentification, etc.) Compréhension des enjeux généraux en sécurité informatique (qu'est-ce qu'une attaque par bruteforce, une exfiltration de données, etc.)

Programme détaillé

Introduction à la formation Splunk

Produits de la marque Splunk
Fonctions de Splunk Enterprise
Architecture
Flux de données

Ajouter des données

Processus d'indexation
Téléversement à travers l'interface graphique
Organisation de la donnée dans les indexes
Envoi à travers un Universal Forwarder
Envoi à travers un collecteur syslog
Supervision de modifications dans des fichiers
Envoi par API
Extraction de champs
Normalisation des champs

Requêter

Accès aux données indexées
Filtre temporel
Paramètres des tâches de recherche
Exploration des résultats
Modes de recherche
Différences entre les événements et les statistiques
Commandes

- Search
- Fieldsummary
- Where
- fields
- rename
- rex
- eval
- Fonctions d'évaluation
- dedup
- sort
- head
- tail
- fillnull
- table
- Calculs statistiques
- Commande stats
- Fonctions d'agrégations
- Agrégats multiples
- Combinaison des fonctions d'agrégation et des fonctions d'évaluation
- Manipulation des JSON
- Enrichissement de données
- Types de lookups
- Manipulation des lookups
- Recoupement des données
- Utilisation des lookups pour faire une chasse de marqueurs
- Jointures
- Macros de recherche
- Sous-recherches

Configurer

- Fichiers de configuration
- Précédence des configurations
- Périmètres et gestion des droits
- Objets de connaissance
- Partage d'objets
- Installation d'une application

Tableaux de bord

- Utilisation des tableaux de bord Studio
- Forces et limitations du moteur
- Sélecteurs et filtres
- Commande timechart
- Requêtes chaînées
- Utilisation des tokens
- Interactivité des tableaux de bord

Requêtes avancées

- Commandes bin et transaction
- Requêtes pour l'investigation numérique
- Requêtes pour la détection
- Détection par seuil
- Création d'alertes pour un SOC

Conclusion

Ressources pertinentes pour l'apprentissage continu

Prochaines sessions

DATE	LIEU	STATUT
03/11/2026	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière DevOps, Automation & SRE : 4,9/5 — 121 avis

Pierre B. — Même formateur que lors de ma dernière formation, celui-ci est toujours autant accessible, pédagogue et compétent. Je recommande !

Tian G. — Intense, pas facile à digérer dans son intégralité.

Votre formateur

Herve S. — Formateur Observabilité & Monitoring

Herve intervient sur des formations portant sur l'observabilité et le monitoring. Parmi les formations qui lui sont confiées figurent notamment « Splunk » et « ElasticSearch ». La conception de...

Ils nous font confiance

Cette année notre filière Observabilité & Monitoring a accompagné plus de 32 entreprises dont :

CAPGEMINI TECHNOLOGY SERVICES GROUPAMA SUPPORTS & SERVICES ORANGE BUSINESS SERVICES SA ANSYS FRANCE SAS APSIDE TOP ASNR ASTEK FRANCE COEXYA CS GROUP FRANCE DASSAULT SYSTEMES AMERICAS CORP +22 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com