DAWAN

Plan de la formation

www.dawan.fr

# Formation Certified Stormshield Log Supervisor (NT-CSLS)

| | |
|---|---|
| **Durée :** | 2 jours (14 heures) |
| **Tarifs inter-entreprise :** | 2 363,00 CHF HT (standard)<br>1 890,40 CHF HT (remisé) |
| **Public :** | Responsables informatique, administrateurs réseaux, techniciens informatique |
| **Pré-requis :** | L'accès à cette formation est réservé aux personnes ayant réussi l'examen CSNA dans les 3 ans précédant la formation CSLS |
| **Objectifs :** | Configurer SLS, les utilisateurs et leurs privilèges - Configurer l'envoi sécurisé des journaux depuis les firewall SNS et agents SES vers la solution SLS - Effectuer des recherches ciblées - Générer des tableaux de bords personnalisés, contextuels - Paramétrer la génération automatique de rapports personnalisés - Automatiser l'identification et la remontée d'incidents - Analyser un incident de sécurité à partir des journaux - Automatiser les actions d'investigations d'un incident avec le SOAR |
| **Modalités pédagogiques, techniques et d'encadrement :** | • Formation synchrone en présentiel et distanciel.<br>• Méthodologie basée sur l'Active Learning : 75 % de pratique minimum.<br>• Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat.<br>• Un formateur expert. |

| | |
|---|---|
| **Modalités d’évaluation :** | • Définition des besoins et attentes des apprenants en amont de la formation.<br>• Auto-positionnement à l'entrée et la sortie de la formation.<br>• Suivi continu par les formateurs durant les ateliers pratiques.<br>• Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation. |
| **Sanction :** | Attestation de fin de formation mentionnant le résultat des acquis |
| **Référence :** | RéS102504-F |
| **Note de satisfaction des participants:** | Pas de données disponibles |
| **Contacts :** | commercial@dawan.fr - 09 72 37 73 73 |
| **Modalités d’accès :** | Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard. |
| **Délais d'accès :** | Variable selon le type de financement. |
| **Accessibilité :** | Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins |

## Installer, prendre en main et maintenir SLS

Paramétrer les différents types d’espace de stockage de logs
Gérer l’authentification des utilisateurs et de leurs privilèges
**Atelier : Créer et attribuer des rôles d’accès aux utilisateurs**

## Envoyer de manière sécurisée les journaux depuis les firewalls SNS et agents SES vers la solution SLS

**Atelier : Configurer un firewall SNS pour l’envoi sécurisé des logs**

## Réaliser des recherches avancées

Effectuer une recherche simple
Agréger des données
Utiliser des critères multiples pour affiner les résultats
Exploiter les labels pour catégoriser les résultats
Utiliser des macros pour automatiser certaines recherches

Manipuler des listes pour affiner les résultats
Enrichir les recherches avec des données externes
**Atelier : Associer des logs à des informations externes pour améliorer l'analyse**

## Définir le mode de présentation des résultats des recherches

**Atelier : Adapter la présentation des résultats pour faciliter leur analyse**

## Créer et utiliser des Search templates pour des recherches sur critères variables

**Atelier : Concevoir un Search template réutilisable pour automatiser les analyses**

## Prendre en main les tableaux de bord

Présenter et personnaliser les tableaux de bords pré-configurés
Créer de nouveaux tableaux de bord
**Atelier : Construire un tableau de bord personnalisé pour le suivi d'un indicateur clé**

## Générer et exploiter des rapports

Utiliser les rapports Stormshield pré-configurés
Créer de nouveaux rapports personnalisés
Planifier et envoyer des rapports de manière automatisée
**Atelier : Configurer l'envoi automatique d'un rapport périodique**

## Créer et gérer des règles d'alerte

Définir des règles d'alertes adaptées aux besoins
Suivre et traiter les alertes générées
**Atelier : Configurer une règle d'alerte pour détecter un événement critique**

## Découvrir et exploiter le SOAR

Comprendre les principes du SOAR
Intégrer SOAR avec d'autres outils de sécurité
Configurer des playbooks d'automatisation
Analyser les résultats des automatisations
**Atelier : Mettre en place un playbook pour automatiser une réponse à**

## incident