

Your Cyber INSURANCE



Plan de formation : Splunk Core Certified User

Jours	Module	Contenu
Jour 1	Module 1 : Introduction à Splunk	• Présentation de la plateforme Splunk. • Architecture et composants Splunk. • Cas d'usage : IT Operations, Observability et Cybersécurité. • Navigation dans l'interface Splunk Web. • Gestion des applications Splunk. • Configuration des préférences utilisateur.
	Module 2 : Recherche de base (Basic Searching)	• Exécution des recherches simples. • Sélection des plages de temps. • Compréhension des résultats de recherche. • Affinage des recherches. • Utilisation de la Timeline. • Gestion des événements. • Gestion des Search Jobs. • Sauvegarde des résultats de recherche.
	Module 3 : Utilisation des champs (Fields)	• Comprendre les champs dans Splunk. • Recherche basée sur les champs. • Utilisation du panneau des champs. • Filtrage et regroupement des données. • Exploitation des métadonnées.
	Module 4 : Fondamentaux du Search Processing Language (SPL)	• Introduction au langage SPL. • Structure d'une requête Splunk. • Utilisation des pipelines. • Recherche dans des index spécifiques. • Commandes essentielles : • Bonnes pratiques de recherche.
Jour 2	Module 5 : Commandes statistiques de base	• Commande stats. • Commande top. • Commande rare. • Agrégation des données. • Analyse statistique simple. • Création de tableaux de résultats.

Your Cyber INSURANCE



Plan de formation : Splunk Core Certified User

Jours	Module	Contenu
	Module 6 : Création de rapports et tableaux de bord	• Création de rapports. • Modification des rapports. • Rapports tabulaires. • Création de graphiques et visualisations. • Création de dashboards. • Ajout de rapports à un dashboard. • Personnalisation des tableaux de bord.
Jour 3	Module 7 : Création et utilisation des Lookups	• Concepts des Lookups. • Création de fichiers de correspondance. • Création des Lookup Definitions. • Configuration des Lookups automatiques. • Enrichissement des données avec des Lookups. • Cas pratiques d'intégration de données externes.
	Module 8 : Rapports planifiés et alertes	• Planification des rapports. • Configuration des Scheduled Reports. • Création d'alertes. • Définition des seuils et conditions. • Gestion des notifications. • Consultation des alertes déclenchées.