

Your Cyber INSURANCE



Plan de formation : Splunk Core Certified Power User

Jours	Module	Contenu
Jour 1	Module 1 : Introduction à la certification Splunk Core Certified Power User Module 2 : Utilisation du Splunk Common Information Model (CIM)	• Présentation du parcours de certification Splunk. • Compréhension des objectifs de l'examen SPLK-1002. • Révision des concepts fondamentaux de Splunk. • Bonnes pratiques pour préparer la certification. • Introduction au Common Information Model. • Normalisation des données provenant de différentes sources. • Utilisation des Data Models basés sur le CIM. • Exploitation du CIM pour les cas d'usage de sécurité et de conformité. • Amélioration de la corrélation des événements.
Jour 2	Module 3 : Optimisation des champs, Tags et Event Types Module 4 : Création de recherches SPL avancées Module 5 : Corrélation des événements avec Transactions	• Création et gestion des champs personnalisés. • Utilisation des Field Aliases. • Création et gestion des Tags. • Configuration des Event Types. • Optimisation de la recherche et de la classification des données. • Bonnes pratiques de gestion des Knowledge Objects. • Utilisation avancée du Search Processing Language (SPL). • Sous-recherches (Subsearches). • Fonctions statistiques avancées. • Recherches conditionnelles et dynamiques. • Création de rapports analytiques. • Optimisation des performances des recherches. • Comprendre le concept de transaction. • Regroupement d'événements liés. • Analyse des activités utilisateur. • Corrélation d'événements multi-sources. • Détection de comportements suspects. • Cas pratiques de cybersécurité et d'investigation.

Your Cyber INSURANCE



Plan de formation : Splunk Core Certified Power User

Jours	Module	Contenu
Jour 3	Module 6 : Création et utilisation des Workflow Actions Module 7 : Création de Data Models et optimisation de Pivot	• Présentation des Workflow Actions. • Création d'actions personnalisées. • Intégration avec des outils tiers. • Automatisation des tâches d'investigation. • Navigation contextuelle entre les données. • Amélioration de l'efficacité opérationnelle. • Conception de Data Models. • Gestion des ensembles de données structurées. • Utilisation de Pivot sans programmation SPL. • Création de rapports interactifs. • Optimisation des performances des Data Models. • Exploitation des tableaux de bord analytiques.