

Your Cyber INSURANCE



Plan de formation : Splunk Core Certified Advanced Power User

Jours	Module	Contenu
Jour 1	Module 1 : Recherches statistiques avancées Module 2 : Commande eval et manipulation des données Module 3 : Filtrage et modification des résultats	- Utilisation avancée de la commande stats - Analyse avec eventstats et streamstats - Fonctions d'agrégation (count, list, dc, avg, sum) - Utilisation de fieldsummary - Optimisation des résultats statistiques - Fonctions de conversion (tonumber, tostring) - Fonctions de texte et manipulation de chaînes - Conditions avec if, case, coalesce - Calculs dynamiques avec eval - Analyse logique et transformation des données - Utilisation de search et where - Gestion des valeurs nulles (fillnull) - Tri et formatage des résultats - Optimisation des résultats de recherche
Jour 2	Module 4 : Corrélation avancée des événements Module 5 : Field extraction et manipulation des données Module 6 : Knowledge Objects avancés	- Utilisation avancée des transactions - Regroupement d'événements par champs et temps - Différence entre transaction et stats - Analyse de comportements utilisateurs - Cas d'usage SOC et détection d'incidents - Extraction de champs avec regex - Extraction délimitée - Utilisation du Field Extractor (FX) - Création et gestion des champs avancés - Amélioration de la qualité des données - Field aliases et calculated fields - Tags et Event Types avancés - Macros (paramètres et variables) - Optimisation des objets de connaissance - Bonnes pratiques de structuration SPL

Your Cyber INSURANCE



Plan de formation : Splunk Core Certified Advanced Power User

Jours	Module	Contenu
Jour 3	Module 7 : Workflow Actions et automatisation	• Création de Workflow Actions (GET, POST, SEARCH) • Intégration avec outils externes (SIEM / SOC) • Automatisation des investigations • Navigation contextuelle des événements
	Module 8 : Data Models et CIM avancé	• Structure des Data Models • Accélération des Data Models • Utilisation du CIM (Common Information Model) • Normalisation des données multi-sources • Optimisation des performances Pivot
	Module 9 : Analyse avancée des données	• Subsearches et commandes imbriquées • Corrélation multi-sources • Optimisation des requêtes SPL complexes • Cas d'usage sécurité et monitoring