

Your Cyber INSURANCE



Plan de formation : Splunk Enterprise Certified Architect

Jours	Module	Contenu
Jour 1	Module 1 : Fondamentaux de l'architecture Splunk Enterprise	• Présentation de l'architecture Splunk Enterprise • Concepts de conception et d'architecture • Analyse des besoins métier et techniques • Dimensionnement de l'infrastructure • Bonnes pratiques d'architecture Splunk
	Module 2 : Conception d'une architecture Splunk distribuée	• Architecture distribuée Splunk • Rôle des Search Heads, Indexers et Forwarders • Déploiements multisites et multi-datacenters • Répartition de charge (Load Balancing) • Architecture haute disponibilité (HA)
	Module 3 : Clustering avancé des Indexers	• Architecture Indexer Cluster • Configuration du Cluster Manager • Facteurs de réplication et de recherche • Clustering multisite • Maintenance et dépannage des clusters
Jour 2	Module 4 : Clustering des Search Heads	• Architecture Search Head Cluster • Élection du Captain • Gestion du Deployer • Synchronisation des configurations • Haute disponibilité et continuité de service
	Module 5 : Architecture de collecte et d'ingestion des données	• Stratégies de déploiement des Universal Forwarders • Architecture des Heavy Forwarders • Routage et filtrage des données • Gestion centralisée des collecteurs • Optimisation des flux d'ingestion
	Module 6 : Deployment Server et gestion des configurations	• Architecture du Deployment Server • Création des Server Classes • Déploiement des applications et configurations • Gestion du changement et automatisation • Administration des environnements à grande échelle

Your Cyber INSURANCE



Plan de formation : Splunk Enterprise Certified Architect

Jours	Module	Contenu
Jour 3	Module 7 : Optimisation des performances et montée en charge	• Optimisation des performances de recherche • Optimisation de l'indexation • Gestion des ressources système • Planification du stockage • Stratégies de scalabilité
	Module 8 : Architecture de sécurité et gouvernance	• Sécurisation de l'environnement Splunk • Gestion des rôles et permissions • Intégration LDAP, Active Directory et SAML • Chiffrement et gestion des certificats • Conformité et gouvernance des données
	Module 9 : Reprise après sinistre et continuité d'activité	• Planification de la reprise après sinistre (Disaster Recovery) • Sauvegarde et restauration • Architecture multisite résiliente • Définition des objectifs RPO et RTO • Bonnes pratiques de continuité d'activité
Jour 4	Module 10 : Supervision et dépannage des environnements complexes	• Utilisation de la Monitoring Console • Surveillance de l'état de santé de la plateforme • Diagnostic des clusters Splunk • Analyse des performances et résolution des incidents • Bonnes pratiques opérationnelles
	Module 11 : Intégration SIEM et Security Operations Center (SOC)	• Architecture Splunk pour les SOC • Intégration avec les solutions de cybersécurité • Collecte des journaux de sécurité • Infrastructure de détection des menaces • Analyse et corrélation des événements de sécurité
	Module 12 : Préparation à la certification Splunk Enterprise Certified Architect	• Révision des objectifs de certification • Études de cas d'architecture avancée • Ateliers pratiques et scénarios réels • Questions types d'examen • Évaluation finale et préparation à la certification