

Your Cyber INSURANCE



Plan de formation : Splunk Enterprise Certified Admin

Jours	Module	Contenu
Jour 1	Module 1: Introduction to Splunk Enterprise Administration Module 2: Splunk Enterprise Installation and Configuration Module 3: Data Inputs and Data Management	• Overview of Splunk Enterprise architecture • Splunk components and deployment models • Administrator roles and responsibilities • Splunk licensing concepts • Installation and deployment planning • Installing Splunk Enterprise • Initial configuration and setup • Managing configuration files • Splunk startup and shutdown procedures • System requirements and best practices • Configuring data inputs • File and directory monitoring • Network and scripted inputs • Data onboarding and validation • Managing indexes and storage
Jour 2	Module 4: Forwarders and Data Collection Module 5: User, Role, and Authentication Management Module 6: Search Head and Indexer Administration	• Universal Forwarder deployment • Heavy Forwarder configuration • Forwarder management and monitoring • Data routing and filtering • Troubleshooting forwarding issues • Creating and managing users • Role-Based Access Control (RBAC) • Authentication methods (LDAP, SAML, Active Directory) • User permissions and capabilities • Security best practices • Search Head management • Indexer configuration • Distributed search architecture • Search Head clustering concepts • Indexer clustering fundamentals

Your Cyber INSURANCE



Plan de formation : Splunk Enterprise Certified Admin

Jours	Module	Contenu
Jour 3	Module 7: Splunk Knowledge Objects Administration	• Managing fields and field extractions • Tags and event types • Lookups and lookup tables • Macros and workflow actions • Data models and knowledge management
	Module 8: Monitoring, Maintenance, and Troubleshooting	• Monitoring Splunk health and performance • Using Monitoring Console • Troubleshooting indexing and search issues • Managing resource utilization • Backup and recovery strategies
	Module 9: Security and Compliance	• Securing Splunk deployments • Data protection and access controls • Audit logging and compliance requirements • Security monitoring best practices • Governance and risk management
Jour 4	Module 10: Splunk Enterprise Deployment Best Practices	• Capacity planning • Scaling Splunk environments • High availability concepts • Performance optimization • Enterprise deployment recommendations
	Module 11: Certification Exam Preparation	• Review of certification objectives • Hands-on administration labs • Practice exam questions • Exam-taking strategies • Final assessment