CISCO SPLUNK TEST DRIVE

Service Overview:

At Netnology, we specialize in Cisco Splunk implementation services to expedite the adoption of Cisco Splunk solutions. The Splunk SIEM & Observability Test Drive is designed to provide customers with a baseline understanding of Cisco Splunk's security and observability capabilities and its value proposition.

This 2–4-hour session will demonstrate the functionality of Splunk Enterprise using Cisco add-ons such as EventGen, Unix Add-on, and various monitoring capabilities. It will highlight the ease of configuration, manageability, and key security insights of this integrated solution.

This test drive is built and delivered by subject matter experts (SMEs) with extensive experience working with Cisco Splunk SIEM & O11y solutions.

Solution Overview:

Cisco Splunk is an industry leading **SIEM** and **Observability** platform that enhances security, infrastructure and application visibility, helps detect and predict issues quickly, and provides rapid responses at scale.

With Cisco Splunk, organizations can:

- Gain **comprehensive visibility** into their data.
- Enable **faster detection and investigation** of security incidents.
- Utilize **advanced analytics** to identify root causes.
- Improve infrastructure and application monitoring for real-time insights.

Service Benefits:

Netnology has a team of world-class engineers who specialize in Cisco Splunk Solution and are passionate about customer success. Netnology will partner with you to provide guidance on:

- Event Ingestion & Parsing (Cisco & Unix Add-ons)
- Infrastructure & Application Monitoring
- Real-time Security Event Analysis
- Data Analytics: Searches, Reporting, and Dashboards
- Leveraging SPL Commands for Effective Searching

Service Scope:

Up to 4-hour Test Drive engagement, Netnology will provide the following services:

- Solution Overview
- Solution Value Proposition
- Solution Use-case Demo
    - Cisco Splunk UI Overview
        - Landing Page
        - Apps
        - Settings
        - Preferences
        - User and Roles

  - Cisco Splunk SIEM (Security Information & Event Management)
    - Event Ingestion & Parsing
    - Cisco and Unix Add-ons
    - Real-Time Security Monitoring
    - Multiple Failed Login Attempts Scenario
    - Anomalous Traffic Detection
    - Charts, Dashboards, Reports
  - Cisco Splunk O11y (Observability)
    - Infrastructure Monitoring
    - Network & Server Health Monitoring
    - Application Performance Monitoring (APM)
    - Multi-Vendor Logging
    - Real-Time Monitoring
    - Service Availability & Performance Metrics
    - Incident Analysis & Response
    - Log Correlation & Root Cause Analysis
  - Search and Analysis (SPL)
    - SPL Commands
  - Visualization and Reporting
    - Charts
    - Graphics
    - Reports
  - Splunk Integrations
    - Cisco ThousandEyes + Splunk Integration
    - Cisco Nexus Dashboard + Splunk Integration
    - Cisco Catalyst + Splunk Integration
- Lessons Learned and Enhancements

Target Audience:

This service is designed for candidates with little or no Cisco Splunk experience or prior knowledge.

Service Deliverables:

No.	Deliverable	Service Details
1.	Solution Overview	• Environment Overview • Use-Case Overview
2.	Value-Prop	• Value Prop • Ease of Configuration • Ease of Manageability
3.	Use-Case Demo	• Cisco Splunk UI • Cisco Splunk SIEM • Cisco Splunk O11y • Log Aggregation • Real-Time Monitoring • Search and analysis (SPL) • Visualization and Reporting • Cisco Nexus Dashboard + Splunk Integration • Cisco ThousandEyes + Splunk Integration • Cisco Catalyst + Splunk Integration
4.	Wrap-up	• Lessons Learned • Q&A