

CISCO SPLUNK MENTORED POV PLUS

Service Overview:

At Netnology, we specialize in Cisco Splunk implementation services to expedite the adoption of Cisco Splunk Solution. As part of this Mentored PoV Plus service offer, our subject matter experts (SMEs) partner with your team to ensure a smooth deployment of Cisco Splunk solution in the lab environment and provide knowledge transfer to equip your staff with the necessary skills to configure and manage the Cisco Splunk solution.

Solution Overview:

Cisco Splunk is a SIEM and Network Analysis tool and is an industry-leading security and observability platform. It helps you shine a light across all your digital systems, so you can spot and fix problems early, pivot quickly when the moment demands, and make the breakthroughs that drive progress. You can connect all the data intelligently, predict issues, and rapidly respond at scale.

Cisco Splunk Solution will help you provide better insights into security intelligence, business operation, identify root causes, prioritize what is business critical, and deliver optimal responses that minimize disruptions with automated workflows. With Cisco Splunk Solution you will get comprehensive visibility of your data, faster detection and investigation of incidents, guidance to root causes, and understanding of the impact these are having on your businesses.

Cisco Splunk provides industry-leading SIEM and Observability features, enabling customers to:

- Gain real-time visibility across infrastructure and applications
- Accelerate detection and investigation of incidents
- Ingest and parse event data from Cisco, Unix, and other sources
- Use powerful dashboards, alerts, and analytics

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:

- Step-by-step guidance from an SME on Cisco Splunk solution deployment in a lab environment
- Configuration and documentation assistance of Cisco Splunk solution
- Knowledge transfer to ensure customer is ready to configure and manage the environment

Service Scope:

As part of the 3-day engagement, Netnology will help with the following:

- Splunk Overview: Architecture, Use Cases, UI walkthrough
- Installation (Linux & Windows) and admin basics
- Event Ingestion:
 - Cisco Add-on
 - Unix Add-on
 - EventGen for demo data

- Search & Reporting (SPL Commands)
 - Field extraction, lookups, macros, event types
- Dashboards & Visualization
 - Real-time monitoring dashboards
 - Charts, Reports, KPI views
- Alerting & Incident Detection
 - Multiple Failed Login Attempts
 - Anomalous Traffic Detection
- Use Case-Based Walkthroughs:
 - Security & Observability scenarios
- Splunk Admin Settings

Add-on ⁽¹⁾

- Cisco Integrations
 - Splunk and ThousandEyes Integration
 - Splunk and Nexus Dashboard Integration
 - Splunk and Cisco Catalyst Integration

Target Audience:

This service is designed for Network Architects, Network Engineers, Application Operators, Developers, Infrastructure Engineers, and Administrators configuring, deploying, and managing Cisco Splunk.

Prerequisites:

Customers need to ensure that all equipment and devices are racked and stacked, cabled, and powered-up prior to the kick-off. Customers also need to acquire the necessary software licenses for the deployment of Cisco Splunk Enterprise or SaaS solutions.

Service Deliverables:

No	Deliverable	Service Details
1.	Project Kickoff	<ul style="list-style-type: none"> • Project Overview • Solution Overview
2.	Solution Deployment	<ul style="list-style-type: none"> • Installation <ul style="list-style-type: none"> ○ Linux ○ Windows • Administration <ul style="list-style-type: none"> ○ Creating Users and Roles ○ Preferences of the User ○ Management User Interface ○ Settings ○ Apps • Event Ingestion <ul style="list-style-type: none"> ○ Cisco Add-on ○ Unix Add-on • Search and Reporting <ul style="list-style-type: none"> ○ SPL Commands • Alerting • Dashboards Overview and Creation <ul style="list-style-type: none"> ○ Graphics ○ Charts • Reports
3.	Lessons Learned	<ul style="list-style-type: none"> • Understand how to gain value by analyzing and troubleshooting business critical data to identify the root cause
4.	Knowledge Transfer	<ul style="list-style-type: none"> • Explain to the customer how to configure and manage the Cisco Splunk Solution in a lab environment
5.	Q&A	<ul style="list-style-type: none"> • Q&A

(1) **Note:** Add-on service is not included in the Cisco Splunk Mentored PoV Plus scope. Additional charges will apply for add-on services.