Connection
we solve IT

Splunk Observability Implementation Services

What is the Splunk Observability Implementation Service?

The Splunk Observability Implementation Services offering is a customizable suite of observability implementation services intended for all Splunk customers, at all stages of observability maturity. The foundation of this service is Splunk's Observability Cloud offering. This suite of services can be adapted to fit the immediate needs and future roadmap of any organization.

Connection partners with Keos to deliver industry-leading professional services for Splunk adoption and optimization. Keos is Splunk's largest professional services provider in the U.S., holding the highest certifications across the entire Splunk portfolio, with 10 years of experience delivering Splunk services. Offerings encompass the entire lifecycle spectrum—from design and architecture to full platform implementation and expansion services—with performance optimization and environment remediation ensuring operational, data, and licensing efficiency.

Why Connection?

Connection offers products, technical expertise, services, and solutions to help your business adapt to the ever-changing technology landscape. Connection designs and deploys infrastructure solutions tailored to each customer's unique business needs, enabling them to optimize spend while enhancing agility.

Connection's Splunk Observability Services is a package of implementation services designed to strengthen and mature your Splunk observability posture. Leveraging the advanced architectural and ITOps capabilities of our Splunk subject matter experts, this service delivers resilient architecture and workflows to enhance observability coverage, increase application performance, lower mean time to response (MTTR), and improve user experience. The foundation of these service offerings is Splunk Observability Cloud, a comprehensive, full-stack observability platform designed to provide unified visibility and real-time troubleshooting across any environment. It integrates metrics, logs, and traces into a single platform, enabling organizations to monitor, analyze, and resolve issues faster while improving system performance and reliability.

Features and Functionality of a Full Observability Deployment

Our experienced Splunk engineers deliver a streamlined yet comprehensive Splunk architecture that identifies, alerts upon, and aids in remediating infrastructure and application issues. Splunk ITSI and Splunk O11y Cloud are used as the foundation to maximize visibility and enable customers to quickly identify and remediate problems. Some of the most fundamental features and benefits are:

- **Splunk ITSI**: Connection normalizes all data to be CIM compliant, allowing for ITSI's powerful tools to be of full use.
- **Splunk ITSI Service Tree and KPIs**: Connection aggregates all of your organization's assets for tracking within the Service Analyzer and builds KPIs to monitor and alert upon infrastructure and application performance.
- **Splunk O11y APM**: Application logging is ingested into O11y Cloud for performance monitoring, through dashboard visualization, real time alerting, and detailed troubleshooting investigations.
- **Splunk O11y RUM**: Similar to APM, Connection builds tooling for real user monitoring that enables developers to identify issues early and then dive deep into trace logging to find solutions.
- **Splunk O11y SUM**: Connection builds the infrastructure allowing developers to simulate user activity on applications, creating confidence in applications before being deployed into production.

Splunk Observability Implementation Services Outcomes:

Splunk O11y Cloud

- Fully implemented O11y APM, RUM, and SUM
- Custom dashboarding to visualize applications and assets
- Alerting for app performance and optimal user experience

Splunk ITSI

- Fully implemented ITSI Service Analyzer
- Creation of KPIs with dynamic thresholding
- AI integration for precise alerting
- Service-specific visibility and monitoring

Connection
we solve IT

Splunk gives organizations visibility into the health, security, and performance of IT systems by turning raw machine data into actionable intelligence.

Splunk is a data analytics platform designed to help IT operations and security teams leverage the massive volumes of machine-generated data produced by modern systems—servers, applications, networks, cloud services, and security tools. Splunk centralizes this data and makes it searchable and actionable in near-real-time. Splunk elevates an organization's data into operational and security intelligence that helps reduce downtime, improve resilience, and manage cyber risk.

Organizations utilize Splunk in four primary operational domains:

1. **IT Operations and Reliability**: Quickly diagnose outages, performance slowdowns, and system failures by correlating logs and metrics across the entire environment, reducing downtime and improving service availability.
2. **Cybersecurity (SIEM/SOAR/XDR)**: Detect and investigate threats by analyzing activity from firewalls, endpoints, identity systems, and cloud platforms. Splunk can generate alerts, support incident response, and help meet regulatory requirements.
3. **Observability and Application Performance**: Monitor how applications and infrastructure behave in production, especially in complex cloud and microservices environments.
4. **Compliance and Reporting**: Retain logs and generate audit reports showing access, changes, and security events.

Our Splunk Services combine Cisco Gold Partner expertise with Keos's elite engineering to deliver end-to-end value. **Splunk + Keos = Actionable Data**.

Splunk Observability Implementation Services Sequence:

A comprehensive implementation of Splunk Observability may follow the sequence of services outlined below:

- **Splunk O11y Implementation**: Architect, install, and configure OpenTelemetry (OTel) collector agents for the ingestion of logs, traces, and metrics. All data will be normalized and utilized within O11y's three primary tools: Application Performance Management, Real User Monitoring, and Synthetic User Monitoring. Dashboarding will be created for holistic visualization, and scheduled alerting built to identify problems as early as possible.
- **Splunk ITSI Implementation**: Architect, install, and configure Splunk ITSI as the foundation of the Splunk observability posture. All data will be normalized, and assets will be onboarded for data enrichment. The Service Analyzer tree will be assembled with relevant KPIs and dynamic thresholding to provide clear monitoring of customer infrastructure and services. Then, scheduled correlation searches and notable event aggregation policies will be built to provide insightful alerting and contextual information for investigation and remediation.

Related Splunk Services Offerings and Add-on Service Modules:

- **Splunk Data Ingestion**: As the implementation and configuration of Splunk Observability evolves, additional data feeds are often necessary to increase visibility and cover specific use cases. This service add-on accelerates the onboarding of multiple data sources and feeds into Splunk ITSI or Splunk O11y Cloud.
- **Splunk General Consulting – Staff Augmentation**: During the delivery of Splunk Observability Services, more KPIs, alerting, and service onboarding may be necessary to increase visibility and monitoring. This add-on service provides additional resources to complete the desired ITSI or O11y deployment tasks.

cisco Partner

Unlock the Full Value of Splunk with Connection

Expert-led Services to Maximize Your Splunk Investment

To learn more about our Splunk Observability Implementation Services, contact your Connection Account Team today!

1.800.998.0067 ■ www.connection.com/services