Connection
we solve IT

Splunk Enterprise Security (ES) Implementation Services

Connection's Splunk Enterprise Security Services suite is a sequence of implementation services, each building upon the last, to strengthen and mature your Splunk security posture. Leveraging the advanced architectural and security capabilities of our Splunk subject matter experts, this service delivers resilient security architecture and workflows to increase security detection coverage, increase alert fidelity, lower MTTR, and automate detection responses. The foundation of these service offerings is Splunk's Enterprise Security (ES) module, a comprehensive platform designed to enhance threat detection, investigation, and response (TDIR) capabilities. It integrates advanced features like SIEM, SOAR, UEBA, and AI-driven workflows to streamline security operations and improve SOC efficiency.

Features and Functionality of a Full Splunk Enterprise Security (ES) Deployment

Our experienced Splunk engineers deliver a streamlined, yet comprehensive, Splunk architecture that identifies, alerts to, and mitigates security threats. Using Splunk Enterprise Security as the foundation, the MITRE framework is leveraged to maximize security visibility, and then paired with Splunk SOAR and Splunk AI to respond to potential threats. Some of the most fundamental features and benefits of a full Enterprise Security deployment are:

- **Splunk Enterprise Security**: Connection normalizes all security to be CIM-compliant, allowing for Enterprise Security's powerful data models to be of full use.
- **Assets and Identities**: Connection aggregates all of your organization's assets and identities from multiple sources to be used for advanced data enrichment within Enterprise Security.
- **Risk Based Alerting**: Using a proprietary algorithm, Connection calculates the fidelity and priority of threats on a user-by-user and asset-by-asset basis, reducing alert fatigue and decreasing time to investigate / respond.
- **Splunk SOAR**: Connection builds upon the higher fidelity alerting by creating custom automation (SOAR playbooks) to respond to threats, lowering threat sprawl and allowing analysts more time to focus on investigation.
- **Splunk AI**: Connection utilizes proprietary artificial intelligence packages to better identify, understand, and validate inbound threats.

Splunk Enterprise Security Implementation Services Outcomes:

A full implementation of Splunk ES provides the following features and functionality:

- Fully deployed Splunk Enterprise Security with integrated SOAR
- SOC-integrated security workflows
- Automated threat detection and response
- Enriched investigative tooling for SOC analysts
- Continuous detection updates to keep up with ever-changing threat landscape
- Documentation of architecture, security coverage, and workflows

splunk> a CISCO company

What is the Splunk Enterprise Security Implementation Service?

The Splunk Enterprise Security Implementation Services offering is a customizable suite of security implementation services intended for all Splunk customers at all stages of security maturity. The foundation of this service is Splunk's Enterprise Security Module. 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
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 Enterprise Security Implementation Services Sequence:

A comprehensive implementation of Splunk Enterprise Security (ES) may follow the sequence of services outlined below:

- **Splunk Enterprise Security Implementation**: Architect, install, and configure Splunk Enterprise Security as the foundation of the Splunk security posture. All data will be normalized for data model use, and assets and identities will be aggregated for data enrichment.
- **Splunk Use Case Development Workshop**: A complete mapping of the organization's threat vectors is performed in alignment with the MITRE framework in order to define which security detections are required.
- **Splunk Risk Based Alerting Implementation**: All detections outlined previously are written, tested, and scheduled for active security coverage. Our algorithm will be used to integrate data enrichment and further maximize alert fidelity.
- **Splunk AI Enablement**: Additional AI-enabled security detections are written, tested, and scheduled to achieve increased coverage and fidelity.
- **Splunk SOAR Implementation**: Architect, install, and configure Splunk SOAR to become the executive arm of the organization's security posture, acting upon the alerts generated by Splunk Enterprise Security.
- **Splunk SOAR Playbook Implementation**: Construction of custom automations (playbooks) that respond to threats generated by Splunk Enterprise Security.

Related Splunk Services Offerings and Add-On Service Modules:

- **Splunk Data Ingestion**: As the implementation and configuration of Splunk Security Services evolves, additional data feeds are often necessary to increase visibility and protect against specific threat vectors. This service add-on accelerates the onboarding of multiple data sources and feeds into Splunk Enterprise Security.
- **Splunk Health Check**: A comprehensive review of your Splunk environment from the operating system up. This one-week health check and assessment deep dives into the Splunk architecture, data onboarding configurations, search / indexing practices, overall security posture, user behavior, and more.
- **License Reduction and Optimization Service**: This service begins with a full review of all cost drivers within your Splunk environment, providing expert recommendations on cost reduction—then delivers with a hands-on implementation of cost-optimization measures—averaging a 20% savings!

CISCO Partner

Unlock the Full Value of Splunk with Connection

Expert-led Services to Maximize Your Splunk Investment

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

1.800.998.0067 ■ www.connection.com/services