GUIDEPOINT® SECURITY

SPLUNK PROFESSIONAL SERVICES

When it Comes to Cybersecurity, One Size Does NOT Fit All

Each customer environment is different. Your needs, gaps, skillsets and risks are also unique. We work with you to understand your business and challenges, and evaluate your cybersecurity posture and ecosystem to provide tailored recommendations that deliver your desired security outcomes.

GuidePoint's Splunk certified professionals have extensive knowledge in architecture, deployment, and integration in unique enviornments throughout the Commercial and Federal sectors. Partnering with us to help manage your Splunk platform will provide your organization with:

- ⊘ Greater visibility into information security and operational events
- ⊘ Reduced incident remediation time
- ⊘ Improved information security posture
- ⊘ Vastly improved information security and operational metrics

GuidePoint Security Splunk Services include:

Health Check

GuidePoint's Splunk professionals thoroughly examine your existing Splunk environment to determine whether it is configured optimally for your organization's security and business needs. Through extensive examination and investigation, GPS certified engineers will determine the most accurate and efficient configurations and architecture for your organizations requirements and unique environment; and provide a full-scope remediation plan to ensure maximum performance. The Splunk professional will assess your Splunk infrastructure and data flows for:

- Splunk and Industry Recommended Practices
- Scaling and Performance recommendations
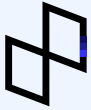- Misconfigurations
- Provide a remediation plan

Put an ELITE Team of Cybersecurity Practitioners on Your Side

Our highly-certified, operational cybersecurity experts have lived and breathed your job.

- More than **70%** of ourworkforce consists of tenured cybersecurity engineers, architects and consultants

- Many have managed security within the DoD and U.S. intelligence agencies and **Fortune 500 companies**

Leverage Our Splunk Expertise:

splunk> CORE CERTIFIED USER

splunk> CORE CERTIFIED POWER USER

splunk> ENTERPRISE CERTIFIED ADMIN

splunk> ACCREDITED ES IMPLEMENTATION

splunk> ENTERPRISE CERTIFIED ARCHITECT

splunk> CORE CERTIFIED CONSULTANT

splunk>partner+ PREMIER ACCREDITED PROFESSIONAL SERVICES PROVIDER

Architecture / Implementation

As a scalable solution, a Splunk environment will continuously evolve as its value-added impact and potential become apparent to the organization. GuidePoint Security has the capability to design and implement a Splunk architecture of any magnitude that will continue to develop and mature as the organization advances, increasing the data analytics capability in lockstep with the organizations' growing presence in the global marketplace.

GuidePoint Security is also well versed in rearchitecting environments which have become antiquated in order to not only leverage the complete capability of the Splunk Platform, but to also ensure that emerging technologies can be integrated to allow for continued future growth.

- Core
- Enterprise Security
- ITSI
- Phantom

Splunk as a Service

GuidePoint Security offers a managed Splunk service to allow your organization to spend less time managing and operating Splunk, and to spend more time reaping the value and benefits of using Splunk. GuidePoint's Splunk professionals will strive to ensure that your Splunk infrastructure operates at peak efficiency with maximum uptime.

- Let us maintain your Splunk environment
- Implement Splunk Best Practices and Optimize your Environment
- Software Upgrades
- Splunk System Health Monitoring
- Troubleshooting
- Onboarding new data sources

Advanced Use Cases & Other Splunk Items

The Splunk platform supports extensive variety of data analytics use cases, and GuidePoint's Splunk professionals are able to advise and deliver on them. Identifying the best-fit use cases for your organization is critical to providing and maintaining the most precise and efficient security information regarding your environment.

- Security Use Case Development
- Data Refinement/Tuning
- Insider Threat
- Executive Dashboards
- Security Orchestration, Automation and Response (eg. Phantom)
  - Build Playbooks
  - Help with decrease SOC response time
  - Integrating products into one workflow action

- SIEM Replacement
- Machine Learning
- Vulnerability Management
- Policy Monitoring

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.