GUIDEPOINT SECURITY
GOVERNMENT SOLUTIONS

DATA ANALYTICS OVERVIEW

# Our Experts Help With Your SIEM And SOAR, So You Can Focus On Your Security.

## Data Analytics Services Designed to Address Your Unique Needs

Our highly certified security practitioners can tailor your security analytics to fit your environment and meet your unique use cases and requirements. Spend less time on administration and management and more time reaping the value and benefits of using the platform.

## GuidePoint Security Data Analytics 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 organization's 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

### Security Orchestration & Automation Response (SOAR)

Implementing a SOAR program enables your organization's analysts and engineers to increase productivity and dedicate more time to proactive tasks such as threat hunting or alert tuning. Additionally, SOAR is one of the few cybersecurity investments that have a quantifiable cost savings. GuidePoint has helped many organizations onboard and operationalizes SOAR platforms. GuidePoint's SOAR offerings include:

- Assistance with SOAR platform selection, based on environmental considerations
- Identification of SOC processes that can be automated, and to what degree (SOAR Roadmap)
- Building Playbooks and integrating products into workflow actions

## Put an ELITE Team of Cybersecurity Practitioners on Your Side

GuidePoint's certified professionals have extensive knowledge in architecture, deployment, and integration in unique environments throughout the Commercial and Federal sectors. Partner with us to help manage your Splunk platform and obtain access to the services described below.

## Hundreds of Industry and Product Certifications

# GuidePoint Security Data Analytics Services continued:

## Architecture and Design for Implementation / Migration

GuidePoint Security can 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.

Our team is also well versed in rearchitecting environments that have become antiquated, designing and implementing architectures for migrations from alternate Security Information and Event Management (SIEM), or migrating from on-premise solutions to cloud infrastructures (whether that is in Splunk Cloud or AWS/Azure).

These architectures leverage the complete capability of the Splunk Platform and ensure that emerging technologies can be integrated to allow for continued future growth.

## Advanced Use Cases & Other Splunk Things

The Splunk platform supports a wide variety of data analytics use cases, and GuidePoint's Splunk professionals can 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
- Machine Learning
- Insider Threat
- Executive Dashboards
- Data refinement / tuning
- Log Enrichment
- Vulnerability Management
- Policy Monitoring

## Splunk as a Service (SaaS)

GuidePoint Security offers 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 Splunk professionals will maintain your Splunk environment and strive to ensure that your Splunk infrastructure operates at peak efficiency with maximum uptime. They will:

- Implement Splunk Best Practices and Optimize your Environment
- Implement requested custom use cases
- Conduct Splunk System Health Monitoring
- Perform Troubleshooting
- Onboard new data sources
- Perform software Upgrades

### Have security data analytics need not mentioned here?

Discuss your specific needs with a GuidePoint team member, and we'll help you with a solution that meets your unique challenges. GuidePoint can help you develop a robust machine data aggregation platform to give your team quicker response times, a flexible platform for machine data analysis, and real-time insight into your security posture.

## 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.

GUIDEPOINT SECURITY
GOVERNMENT SOLUTIONS

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132

GSA Schedule: GS-35F-508CA | DUNS: 005644870 | SINs 54151S, 54151 HACS