

DATA ANALYTICS SERVICES

# Helping You Turn Raw Data Into Security Focused Conclusions

## Bridge the gap between technology and security operations

GuidePoint Security has extensive experience architecting, deploying, and operationalizing security-focused data analytics programs at some of the world's largest organizations.

Unlock the power of security analytics to gain greater visibility into information security events, reduce the time to remediate incidents and improve your overall security posture.

We can help you develop a robust, data aggregation platform that:

- Enables your team to have quicker response times
- Provides machine-learning data analysis
- Drives real-time insight into your security posture



### Architect

- Review, analyze, compare + vet current and emerging technology
- Design for continuous development and maturity
- Build for any magnitude and around your requirements



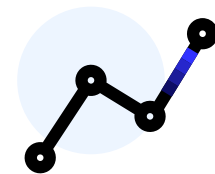
### Deploy

- Provide you with assistance from start to finish
- Well versed and experienced engineers
- On-Premise or Cloud deployments



### Operationalize

- Best fit use cases for your needs and requirements
- Dashboards, enrichment and tuning to make your data work for you
- Integrate emerging technologies for continued growth



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

Our team of practitioners has extensive experience architecting, deploying and operationalizing security-focused data analytics programs at some of the world's largest organizations.

### Highly Certified



# GuidePoint Security Solutions and Services include:



## Security Orchestration, Automation, and 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. Our team can help with your SOAR program by:

- Assisting with platform selection based on your environment
- Identifying SOC processes that can be automated and to what degree (SOAR Roadmap)
- Building playbooks and integrating products into workflow actions



## Architecture & Design Services

We have the capability to design and implement a data analysis architecture of any magnitude that continues to develop and mature as your organization advances. Our engineers are also well versed in rearchitecting environments that have become antiquated, designing and implementing architectures for migrations from alternate SIEMs and migrating from on-premise solutions to cloud infrastructures.



## Advanced Security Analytics Services

Our practitioners can advise you and deliver upon the extensive variety of data analytics use cases depending on the platform that is being used. 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. We can help you with:

- Security use case development
- Executive dashboards
- Vulnerability management
- Machine learning analytics
- Data refinement or tuning
- Policy monitoring
- Insider threat identification
- Log enrichment



## Security Analytics as a Service

Our Security Analytics as a Service is a managed service offering that allows your organization to spend less time managing and operating Splunk, and more time making informed security and risk-based decisions. Our team can maintain your environment and ensure that your infrastructure operates at peak efficiency with maximum uptime.

- Implement best practices and optimize your environment
- Conduct system health monitoring
- Onboard new data sources
- Perform software upgrades
- Perform troubleshooting
- Implement requested custom use cases



## Security Analytics Health Check

Our professionals thoroughly examine your existing data analytics environment to determine if it is configured optimally for your organization's security and business needs. Through extensive examination and investigation, our engineers will:

- Determine the most effective configurations and architecture for your organization's requirements and unique environment.
- Provide a full-scope remediation plan to ensure maximum performance.

## 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.