

## SECURITY DATA PIPELINE SERVICES

# Take ownership of your data from start to finish.

Your security data should be just that—yours. Gathering high-quality data that you control is critical to running an agile, flexible security program.

GuidePoint Security has extensive experience architecting, deploying, and operationalizing data pipeline applications at some of the world's largest organizations. Our expert teams will work with you to build a security data pipeline of vendor-agnostic, high-fidelity data that you can bring to any tool.

The large amount of data created by today's cybersecurity prevention and monitoring tools can leave many teams shorthanded as they try to sift through it all for actionable insights. Taking control of that data leads to better visibility and faster responses, but to do that, you need to decouple the data from individual platforms and vendors.

Our Security Data Pipeline experts will work with you to reap the benefits of a vendor-agnostic data flow architecture. We can help you develop a scalable, flexible, yet simple data pipeline platform that:

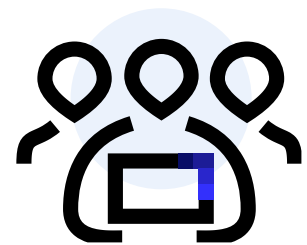
- ✓ Acts as an abstraction layer before your log analytics tools, enabling you to fully control your security data flow
- ✓ Improves data fidelity by enriching important data while reducing the noisy events
- ✓ Reduces investigation & response time by only ingesting quality data to surface actionable insights

### Data Pipeline Use Cases

**SIEM Migrations:** Avoid vendor lock-in and take control of your data. A Data Pipeline tool allows you to easily migrate between SIEMs and format your data (i.e. CIM, CEF, JSON, etc.).

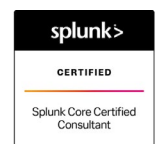
**Data Lake:** Facilitate the storage, access, and retrieval of data at a fraction of the cost for a longer retention time.. Search your data lake or replay the data to your SIEM when you need it.

**Support IT Ops and Security:** To address the challenges of growing data volumes, proprietary data tools and distributed systems, you can create a one-stop data platform for your teams to regain control.



## Put a Highly-Trained **ELITE** Team on Your Side

More than 50% of our workforce consists of tenured cybersecurity engineers, architects and consultants.



North of Bengal, Bengal

# GuidePoint Security Data Pipeline Services

Our Security Data Pipeline services are designed to meet your organization at its current maturity level, whether you need to build from the ground up or mature your existing processes.



**Architecture** - Whether you're designing a new security data pipeline solution or updating an existing one, we can help.

- ✓ Review the current log flow from source to destination to outline infrastructure needs, cluster management, and data optimization and encryption requirements.
- ✓ Tailor infrastructure requirements to your environment, landing at the intersection of resiliency, maintainability, and cost optimization.
- ✓ Thorough logical and physical topologies are provided to easily visualize log flow and end-state environment architecture.



**Deployment** - Our professionals will set the foundation for success by optimizing the deployment of your infrastructure based on your process and requirements.

- ✓ Determine the most effective configurations and architecture for your organization.
- ✓ Thoroughly configure the platform to meet your unique needs.
- ✓ Logically compartmentalize the application based on your environment.



**Operationalization** - From log reduction, redaction, and in-flight enrichment to routing data to multiple destinations, our team has done it all.

- ✓ Validate that injecting the Security Data Pipeline application does not alter events received by destination systems.
- ✓ Configure the pipeline to manipulate the data to meet your engagement objectives. This may include, but is not limited to, log reduction, enrichment, or selective dual-routing of logs to cheap storage and your SIEM, depending on which events should be analyzed.
- ✓ Configure re-ingestion to retrieve a subset of events into your SIEM (e.g., only ingest low-value/high-volume logs if/when needed).

## 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.