

Optimize Your Logging Architecture

Maximizing Splunk ROI & Controlling Data Growth

In today's world, security and operational data is growing exponentially, leaving customers questioning the value of their investments and frequently facing compromising trade-offs between budget constraints and having complete visibility.

At Discovered Intelligence, we deliver a solution that eliminates this compromise by identifying opportunities to simplify logging architectures, maximize Splunk performance, lower the costs of search and data storage, identify gaps in data management, and a remediation plan that actually reduces costs while solving the problems your business faces.

| SOLUTION OVERVIEW

1. Logging Architecture Review

Comprehensive end-to-end review of the existing logging architecture with a focus on:

- Complexity of Design
- Resiliency of Design
- Technology Footprint
- Data Storage and Tiering

3. Splunk Assessment

Maximize computing capacity and search performance with Splunk by assessing:

- Search Performance
- Index Design and Performance
- Best Practice Configurations
- Monitoring and Alerting

2. Data Pipeline Assessment

Detailed audit of all aspects of the data pipeline infrastructure, including:

- Architecture design
- Data Source Integrations
- Pipeline Design and Performance
- Monitoring and Alerting

4. Data Management & Governance

Assessment of operational processes to improve localized data governance:

- Data Onboarding Processes
- Data Cataloging
- Use Case Library
- Knowledge/Support Library

| THE CHALLENGES WE ADDRESS

Through our comprehensive set of assessments, we identify and plan the remediation of consistent friction points:

- **Fragmented & Complex Topologies:** A lack of a formal data pipeline leading to multiple tools and unneeded complexity, architectural blind spots, and prolonged Mean Time to Identification (MTTI) during outages.
- **Inefficient Resource Utilization:** Misconfigured Splunk deployments, poorly written Splunk searches and dashboards, and misconfigured pipelines that quietly waste compute and license volume.
- **Data Waste:** High-volume, redundant, or unparsed logs sent directly to premium storage platforms without strategic reduction and/or data tiering.
- **Lack of Standardized Process:** Fragmented control and a lack of standardized processes contribute to the risk of prolonged outages and silent operational failures.

DEMONSTRATED OUTCOMES

The following matrix details realistic outcomes and savings calculated across prior assessments from the identification of optimization and remediation opportunities:

Optimization	Technical Methodology	Value
Data Ingestion	Identification of unused data, transforming high-volume events to reduce waste, targeted rules suppressing noisy events and tiering data based on functional requirements.	~ 30% Data Reduction Eliminate unneeded waste and reduce data footprint.
Splunk Optimization	Identifying indexing performance opportunities, identifying search and dashboard inefficiencies to improve search performance, best practice implementation for configurations and monitoring.	~ 25% Compute & Storage Savings Freed capacity for future growth and performance.
Pipeline Optimization	Improving pipeline performance, standardizing configurations and improving monitoring and alerting against silent failures.	~ 20% Faster Data Processing Improved data processing.
Hardware Savings	Simplifying logging architecture, centralizing data management and decommissioning redundant on-premise and cloud servers.	~ 35% Less Hardware Elimination of wasted overhead.
Operational Processes	Standardizing data onboarding and management practices, centralizing support information and defining clear roles and service ownership.	~ 50% Faster Onboarding Improved employee efficiency and lowered MTI / MTTR.

ABOUT US

Discovered Intelligence is a boutique consultancy specializing in helping enterprises operationalize their most critical asset: data. We believe that deep technical expertise should be the default, not the exception. With deep roots in security and observability, we align client requirements with high-level technical expertise to deliver scalable, high-performance solutions that maximize ROI.

15+ Years

Splunk experience and expertise across global, multi-terabyte and petabyte architectures.

5+ Years

Pipeline implementation and adoption experience for multi-terabyte architectures and 1M+ dollar cost savings.

500+ Projects

Proven experience from 13 years in business with over 500 successful customer projects.