



Splunk security and operations visibility for public sector

A practical path to cyber resilience, operational insights & modernization

Public sector organizations are under pressure to protect essential services, modernize hybrid environments, and demonstrate operational accountability, often across complex, distributed systems.

GDT helps agencies like yours leverage Splunk to connect security, infrastructure, application, and cloud data to increase visibility, respond faster, and make more informed decisions. The result is a practical path to stronger cyber resilience, improved operational insight, and confident modernization.

Benefits

- More complete visibility across siloed environments
- Faster prioritization of security and operational events
- Better alignment between security, IT operations, and mission teams
- A clearer path from assessment to implementation and ongoing operations
- Greater value from existing Splunk investments

Why GDT

GDT combines public-sector modernization experience with capabilities across cybersecurity, hybrid infrastructure, cloud, and managed services. Our teams help translate Splunk data into operating practices that are aligned to mission priorities, not just technology deployments.

GDT is recognized by Splunk for Premier Partner certification in Cloud Migration: Co-Delivery and has documented experience leveraging Splunk Enterprise Security for analytics, monitoring, and compliance reporting.



What GDT can help you achieve with Splunk

- Security visibility across users, endpoints, networks, applications, and cloud environments
- Threat detection, investigation, threat hunting, risk-based alerting, and incident management
- Compliance-oriented monitoring and reporting across mission-critical systems
- IT operations visibility, infrastructure health, and application performance
- Automated response workflows using integrations such as Splunk SOAR
- Platform optimization ahead of renewal, expansion, or cloud migration

The GDT approach



Assess

We review your architecture, data ingestion, search performance, security workflows, and platform utilization to establish a clear picture of your Splunk environment today.



Improve

We design and implement a right-sized approach to visibility, detection, compliance-oriented reporting, and response automation.



Operate

We extend the value of your investment through advisory support, dashboard development, optimization, managed services, and ongoing improvement.

Start with a Splunk optimization assessment

This structured, weeklong technical engagement gives your team a clear, data-informed view of your Splunk environment. The assessment may include:

- Architecture and environment review to identify issues and potential inefficiencies
- Search audit to understand scheduled and ad hoc search performance
- Data ingestion review, including Common Information Model compliance and data model evaluation
- Performance and resource utilization assessment
- Report with findings and actionable recommendations delivered to your team

You'll receive a practical report with findings and actionable recommendations your team can use to prioritize next steps.



Reach out to discuss your Splunk priorities.