Security Use Case Guidance

What can you accomplish with Splunk?

Here are some of the most popular security use cases implemented by Splunk customers:

- Monitoring a network for DNS exfiltration
- Detecting lateral movement with Active Directory data
- Monitoring for network traffic volume outliers
- Monitoring employee network traffic
- Reconstructing a website defacement

Not what you’re looking for? There’s plenty more! Browse the categories below to find use case content that supports your business needs.

- Compliance and Data Privacy
  - No image available
  - Geographically-Specific Compliance
  - Industry-Specific Compliance

- Operational Foundations
  - No image available
  - Configuration Management
  - Policy Enforcement
  - Threat Intelligence
  - Vulnerability Management

- Security Investigations
  - No image available
  - Incident Investigation and Forensics
  - Incident Response and Reporting

- Threat Intelligence and Threat Hunting
  - No image available

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
- Application Security Monitoring
- Cloud Security Monitoring
- Data Loss Monitoring
- Endpoint Security Monitoring
- Fraud Analytics and Detection
- Insider Threat and Account Compromise
- Network Security Monitoring
- Web Activity Security Monitoring