Threat Intelligence and Threat Hunting

- **Application Security Monitoring**
  - Detecting Kubernetes scanning activity
  - Detecting software supply chain attacks
  - Improving Google Chrome security
  - Investigating Gsuite phishing attacks
  - Monitoring Kubernetes sensitive object access
  - Protecting a Salesforce cloud deployment

- **Cloud Security Monitoring**
  - Analyzing AWS service action errors
  - Detecting AWS cross-account activity
  - Detecting AWS network ACL activity
  - Detecting AWS security hub alerts
  - Detecting AWS suspicious provisioning activities
  - Detecting cloud federated credential abuse in AWS
  - Detecting cloud federated credential abuse in Microsoft Office and Azure Active Directory
  - Detecting Google Cloud Platform (GCP) cross-account activity
  - Detecting Office 365 attacks
  - Detecting privilege escalation in your AWS environment
  - Detecting ransomware activities within AWS environments
  - Detecting suspicious activities within cloud instances
  - Detecting suspicious new instances in your AWS Elastic Compute Cloud (EC2) environment
  - Monitoring AWS and AWS Elastic Compute Cloud (EC2) for suspicious login activities
  - Monitoring AWS Elastic Compute Cloud (EC2) for unusual modifications
  - Monitoring AWS for suspicious traffic
  - Monitoring AWS S3 for suspicious activities
  - Monitoring user activity spikes in AWS

- **Data Loss Monitoring**
  - 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.
Detecting data exfiltration activities
Detecting SNICat SNI data exfiltration
Finding large web uploads
Monitoring a network for DNS exfiltration
Monitoring use of Git repositories

**Endpoint Security Monitoring**

- Checking for files created on a system
- Detecting a ransomware attack
- Detecting BlackMatter ransomware
- Detecting Clop ransomware
- Detecting DarkSide ransomware
- Detecting domain trust discovery attempts
- Detecting FIN7 attacks
- Detecting IcedID attacks
- Detecting indicators of Remcos RAT malware
- Detecting malicious file obfuscation using certutil.exe
- Detecting Netsh attacks
- Detecting print spooler attacks
- Detecting recurring malware on a host
- Detecting techniques in the Orangeworm attack group
- Detecting the Baron Samedit sudo attack
- Detecting the disabling of security tools
- Detecting Trickbot attacks
- Detecting usage of popular Linux post-exploitation tools
- Detecting WhisperGate malware
- Detecting Windows Background Intelligent Transfer Service (BITS) abuse
- Detecting Windows file extension abuse
- Detecting XMRig CPU or GPU mining
- Detecting Zerologon attacks
- Finding interactive logins from service accounts
- Investigating unusual file system queries
- Monitoring command line interface actions
- Monitoring DNS queries
Fraud Analytics and Detection

- Detecting ATM fraud
- Detecting credit card fraud
- Detecting web fraud
- Detecting wire transfer fraud
- Monitoring consumer bank accounts for potential fraud

Insider Threat and Account Compromise

- Conducting an Azure new user census
- Detecting lateral movement with Active Directory data
- Detecting masquerading
- Detecting password spraying attacks within Active Directory environments
- Detecting unusual GCP service account usage
- Finding Windows audit log tampering
- Identifying new Windows local admin accounts
- Monitoring for signs of Windows privilege escalation attack
- Monitoring Kubernetes sensitive role activities
- Recognizing improper use of system administration tools

Network Security Monitoring

- Detecting host redirection attacks
- Detecting network and port scanning
- Detecting TOR traffic
- Detecting UDP service amplification abuse
- Monitoring employee network traffic
- Monitoring for network traffic volume outliers
- Terminating W3WP spawned processes

Web Activity Security Monitoring

- Deleting web shells automatically
- Detecting unencrypted web communications
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.