Extracting insights from ES

The pre-configured notables in Splunk Enterprise Security represent many detections for use cases. You can also check the Use Case Library in Splunk Enterprise Security, accessed via the Configure menu, then Use Case Library. Many more can be found in the Splunk Enterprise Security Content updates, Security Essentials, and Splunk Lantern. Often the first place to start is to enable a few correlation searches and adjust them to fit the use case in your environment. Some common use cases that can be addressed with Splunk Enterprise Security are:

- Detecting Malware
- Identifying Suspicious Activity
- Privileged/ Non-Privileged User Monitoring
- Brute Force Activity (Local and Cloud)
- Advanced Threat Detection
- Traffic Over Time by Action
- Access Anomalies
- Communications with Known Bad Actor
- Cloud Provisioning Activity from Unusual Country
- Cloud Instance Created by Unusual User
- VPN Monitoring
- Suspicious AWS Activities
- Unusual Processes

Finally, using a framework like MITRE ATT&CK can help you find gaps in your coverage and areas you need to implement. Use MITRE ATT&CK to see how these use cases map to advisory Tactics, Techniques, and Procedures (TTP).

The Splunk Enterprise Security Content Update app is linked to the Splunk Security Research Team’s work and it is updated frequently with timely detections. It is a best practice to use this often.

Here are some common starting points for use cases organized by what is called security domains in Splunk Enterprise Security.

Access

- Brute force access behavior detected (local and cloud) (See the correlation search in Splunk Enterprise Security)
- Default account activity detected (See the correlation search in Splunk Enterprise Security)
- Concurrent login attempts detected (See the correlation search in Splunk Enterprise Security)
Endpoint

- Abnormally high number of endpoint changes by user (See the correlation search in Splunk Enterprise Security)
- Execution of a renamed psexec.exe to avoid detection (See the correlation search in Splunk Enterprise Security)
- Indicator of mimikatz activity using Microsoft Sysmon (Splunk Security Essentials)
- Basic malware outbreak (Splunk Security Essentials)
- Common ransomware extensions

Network

- Suspicious network connection (Splunk Security Essentials)
- Account compromised followed by exfiltration (Splunk Security Essentials)
- Excessive DNS queries (See the correlation search in Splunk Enterprise Security)
- Network traffic communications over Port 4444 (Metasploit Default) (Splunk Security Essentials)

Other resources on use cases development

- Risk-based alerting in Splunk Enterprise Security
  - Solution guide: Embark on your risk-based alerting journey with Splunk
  - .conf | Getting started with risk-based alerting and MITRE
  - .conf | Full speed ahead with risk-based alerting (RBA)
  - .conf | Streamlining analysis of security stories with risk-based alerting
- Webinar: 20 SIEM use cases in 40 minutes: Which ones have you mastered?
- Community: Example of how to detect basic malware outbreak
- Blog: Kaseya sera. What REvil shall encrypt, shall encrypt
- Blog: REvil ransomware threat research update and detections