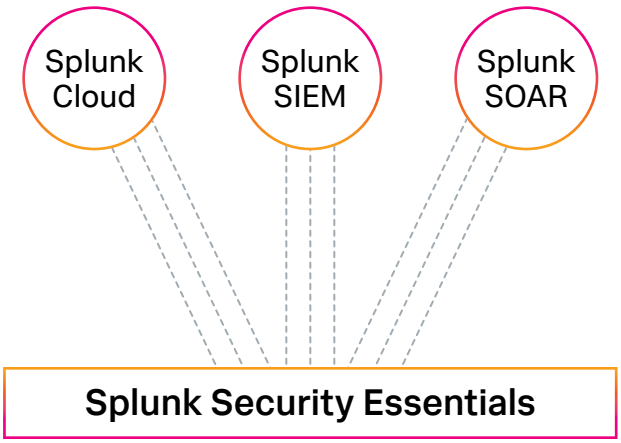
Splunk Security Essentials

Put your data to work and better secure your organization

- **Bolster** your Splunk environment with an extensive Security Content Library and deploy 600+ security detections and analytic stories.
- **Improve** your security posture by mapping security data to MITRE ATT&CK® and Cyber Kill Chain® frameworks.
- **Utilize** the Security Data Journey to strengthen your security strategy with security and data recommendations.

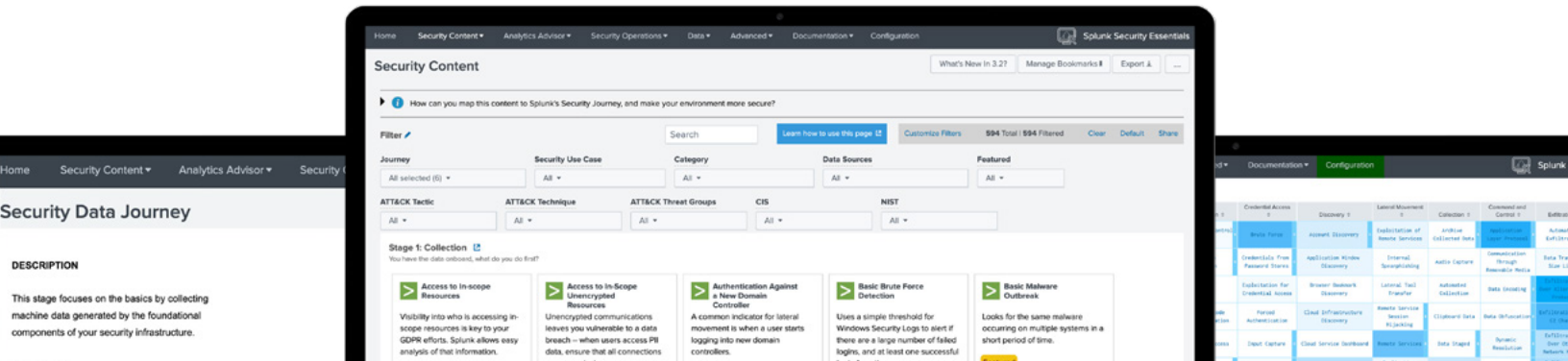


It's become widely accepted that security should be integrated into all aspects of the business. Your security team, however, may discover that different parts of the organization are at different stages of the security journey. If you're struggling to know where to start, Splunk Security Essentials (SSE) provides you with security detections and data onboarding recommendations to guide you through your security maturity journey.

Splunk Security Essentials shows you how the data you're already collecting and analyzing can be used to enrich security detections and perform better incident reviews. SSE tracks data and saved searches in your environment to provide prescriptive recommendations to help you continually strengthen your security strategy.

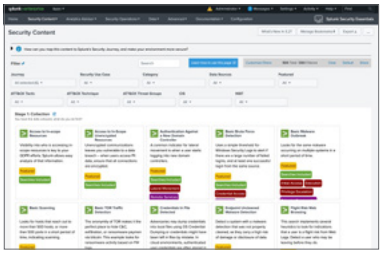
Take advantage of over 600 pre-built security detections and analytic stories in SSE's Security Content Library to enhance searches in your Splunk environment. You can start using basic security monitoring and detections in Splunk Cloud and graduate to more advanced security detections in Splunk SIEM and playbooks in Splunk SOAR. The Analytics Advisor dashboards map your security data and detections to known tactics and techniques in MITRE ATT&CK® and the phases in Cyber Kill Chain.® You can leverage different visualizations to improve your security posture and further operationalize the industry frameworks.

By starting to centralize analysis and visibility across your multi-layered security environment, you'll create a strong security strategy to protect your business. From day one with Splunk Security Essentials, your analysts will be able to use data combined with analytics to improve security monitoring, fraud and threat detections, incident investigation and forensics, and incident response.

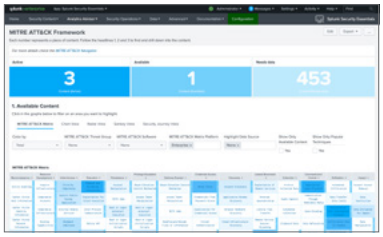


Security Content Library

Browse, bookmark and deploy over 600 security detections and analytic stories from the Security Content Library with just a few clicks. You can find the right security content by narrowing down your search by security use case, cybersecurity frameworks, threat and data source categories and other filters. Begin running basic security detections in Splunk Cloud and more advanced security detections and playbooks in Splunk SIEM and SOAR. Leverage the library to stay ahead of emerging and existing threats with security content that pulls the latest detections and stories published by the Splunk Threat Research Team.



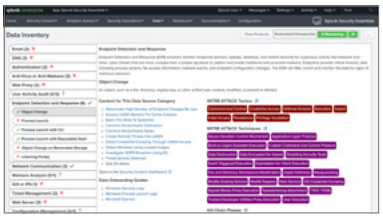
Cybersecurity Frameworks



Get control of your security posture with automatic mapping of data and detections to cybersecurity frameworks like MITRE ATT&CK® and Cyber Kill Chain.® The Analytics Advisor dashboards are designed with visualizations and a custom heat map so you can measure your business's security posture against the frameworks. Drill down on MITRE tactics, techniques, and the threat groups that target your environment and know what detections are tied to different phases of the Kill Chain. Easily identify gaps and quickly implement security content from the Security Content Library to strengthen your defenses.

Data and Content Introspection

Gain visibility by inspecting and analyzing data and security content already in your environment. Data Introspection detects over 150 common source types and categorizes them by security products. This gives you a better understanding of your Splunk environment and standardizes data to be Common Information Model (CIM) compliant. Content Introspection runs a quick scan of your saved searches to map them to the pre-built content from the library. This enriches your existing security content by attaching tags and metadata such as threat and data source categories, MITRE ATT&CK notes and more.



Security Data Journey

Develop a maturity roadmap with security and data recommendations to secure your business. Track the progress of your security program with the Security Data Journey and understand milestones and challenges at each stage of the journey. Implement best practices and security detections with the data you're already collecting to improve your security posture and use the data onboarding guides to collect and analyze additional host, network, and account activity. Prioritize the ingestion of new data sources to improve coverage and reduce risks.

Take a look under the hood with a Splunk Security Essentials Online Demo experience now.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

21-17555-SPLK-Splunk Security Essentials-105-PB