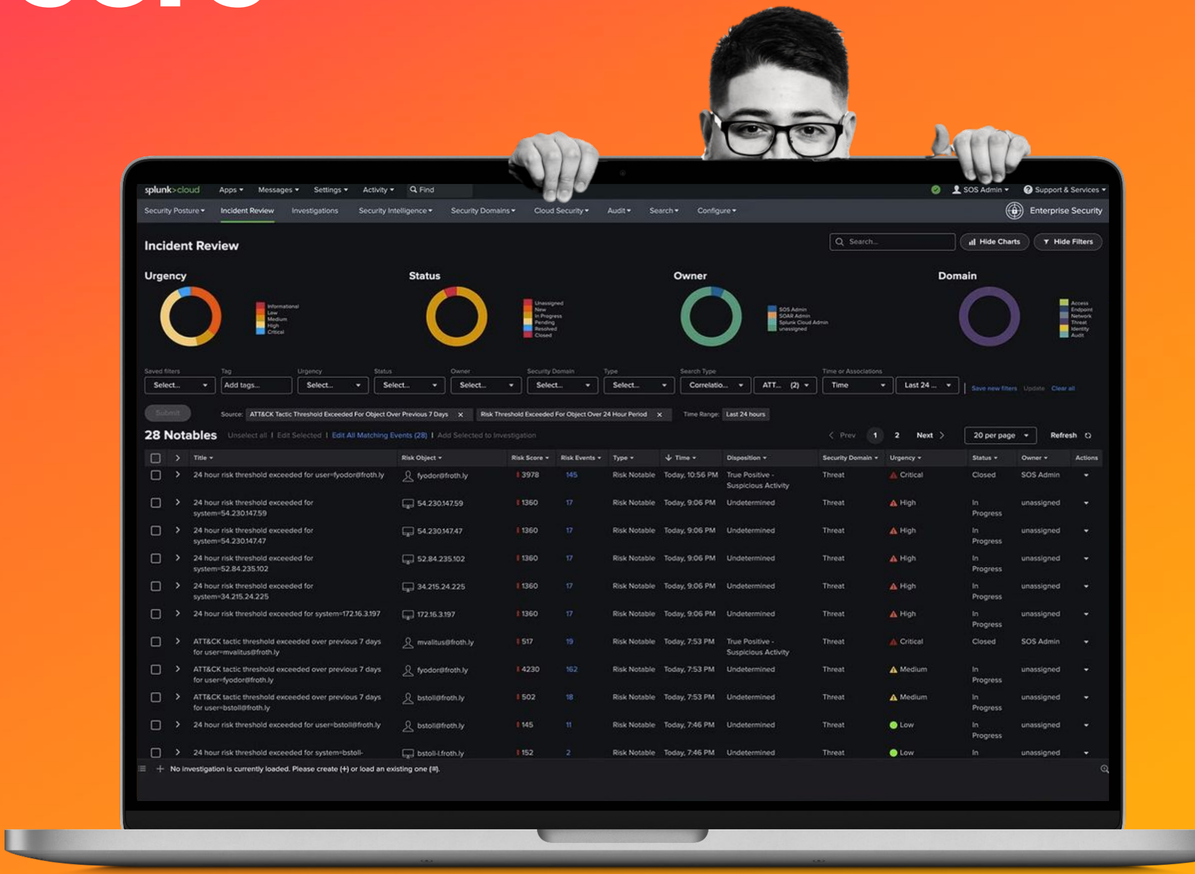
Onboarding Toolkit for Splunk Security Users

A 3 phase guide to Splunk Success



Incident Review

Saved filters: Select... | Tag: Add tags... | Urgency: Select... | Status: Select... | Owner: Select... | Security Domain: Select... | Type: Select... | Search Type: Correlatio... ATT... (2) | Time or Associations: Time, Last 24 ...

Source: ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days ✕ Risk Threshold Exceeded For Object Over 24 Hour Period ✕ Time Range: Last 24 hours

28 Notables Unselect all | Edit Selected | Edit All Matching Events (28) | Add Selected to Investigation

□		Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
□	>	24 hour risk threshold exceeded for user=fyodor@froth.ly	fyodor@froth.ly	3978	145	Risk Notable	Today, 10:56 PM	True Positive - Suspicious Activity	Threat	Critical	Closed	SOS Admin	▾
□	>	24 hour risk threshold exceeded for system=54.230.147.59	54.230.147.59	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
□	>	24 hour risk threshold exceeded for system=54.230.147.47	54.230.147.47	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
□	>	24 hour risk threshold exceeded for system=52.84.235.102	52.84.235.102	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
□	>	24 hour risk threshold exceeded for system=34.215.24.225	34.215.24.225	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
□	>	24 hour risk threshold exceeded for system=172.16.3.197	172.16.3.197	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
□	>	ATT&CK tactic threshold exceeded over previous 7 days for user=mvalitus@froth.ly	mvalitus@froth.ly	517	19	Risk Notable	Today, 7:53 PM	True Positive - Suspicious Activity	Threat	Critical	Closed	SOS Admin	▾
□	>	ATT&CK tactic threshold exceeded over previous 7 days for user=fyodor@froth.ly	fyodor@froth.ly	4230	162	Risk Notable	Today, 7:53 PM	Undetermined	Threat	Medium	In Progress	unassigned	▾
□	>	ATT&CK tactic threshold exceeded over previous 7 days for user=bstoll@froth.ly	bstoll@froth.ly	502	18	Risk Notable	Today, 7:53 PM	Undetermined	Threat	Medium	In Progress	unassigned	▾
□	>	24 hour risk threshold exceeded for user=bstoll@froth.ly	bstoll@froth.ly	145	11	Risk Notable	Today, 7:46 PM	Undetermined	Threat	Low	In Progress	unassigned	▾
□	>	24 hour risk threshold exceeded for system=bstoll-	bstoll-l.froth.ly	152	2	Risk Notable	Today, 7:46 PM	Undetermined	Threat	Low	In	unassigned	▾

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Onboarding Part 1: Setting the Foundation

Sign up for free EDU courses

- Begin your Splunk training with our FREE EDU Starter Path for Security
- Learn (Splunk) and earn (swag)! Read about the Splunk learning rewards program

Join the Splunk Community

- Sign-up here!
- Join the #security slack channel for real time troubleshooting
- Head to Splunk Answers for crowd-sourced guidance

Identify the security use case

- Explore use cases tied to your business goals via Use Case Explorer
- Access more Enterprise-Security use cases via Use Case Library and the free Splunk Security Essentials app.

Get your basic settings ready

- Explore product tours to learn about key features.
  - ○ Enterprise-Security
    - ■ Mission Control
  - ○ SOAR
  - ○ User Behavior Analytics
  - ○ Splunk Attack Analyzer
- Check out the step-by-step guide for Getting Started with Splunk Security!
  - ○ Enterprise Security: Getting data ready
  - ○ SOAR: Setup and Configure

Onboarding Part 2: Getting Value from Splunk

Set up high-value features

- Enterprise Security
  - Investigating and monitoring suspicious events using ES dashboards
  - Activate Mission Control to streamline your SOC process
  - Enable Risk-based Alerting to prioritize alerting and shorten response time
- SOAR
  - Get started with Apps. See what's available.
  - Use playbooks to automate security actions at machine speed
  - Use a no-code/low code visual playbook editor
- User Behavior Analytics (UBA)
  - Get Started
  - Assess Security Posture
  - Security Analyst Workflow

Check out Security Content

- Get security research and alerts for high-profile security incidents from SURGe
- Make the most of out-of-the-box security content developed by the Splunk Threat Research Team:
  - View the full repository of detections, use cases, and playbooks
  - Read the team's blogs to learn how to use this content to respond to the latest threats

Onboarding Part 3: How do I keep learning?

Sign up for key communications

- Sign up for “Product News and Announcements” to stay current on key product updates.
- Attend “Tech Talks” - highly technical, practitioner-focused webinars
  - Sign-up here to receive notifications of new “Tech Talks”
  - Enjoy our library of On-Demand Security “Tech Talks”

Get real time guidance

- Security Workshops (virtual, in-person, or on-demand!)
- Community Office Hours - live, hands-on help in a small group format

Prescriptive Adoption Motions

- Follow these prescriptive adoption motions as you continue to mature on your path to digital resilience with Splunk:
  - For Enterprise Security:
    - Data sources and normalization
    - Security monitoring with correlation and content
  - For SOAR:
    - Incident Management
    - Automation and Orchestration

More advanced training

- If you’re looking to take the next step in your Splunk training, check out our more advance EDU Course
- Watch past .conf sessions to get more inspiration from our Security experts and guest speakers