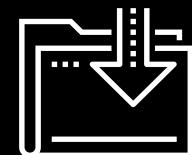




Splunk Enterprise Security

Cybersecurity
SIEM Day 5



Class Objectives

By the end of class, you will be able to:



Differentiate between advanced security monitoring solutions, such as SOARs, UBAs, and UEBAs.



Understand how knowledge of SIEM software and Splunk is valued in the information security job market.

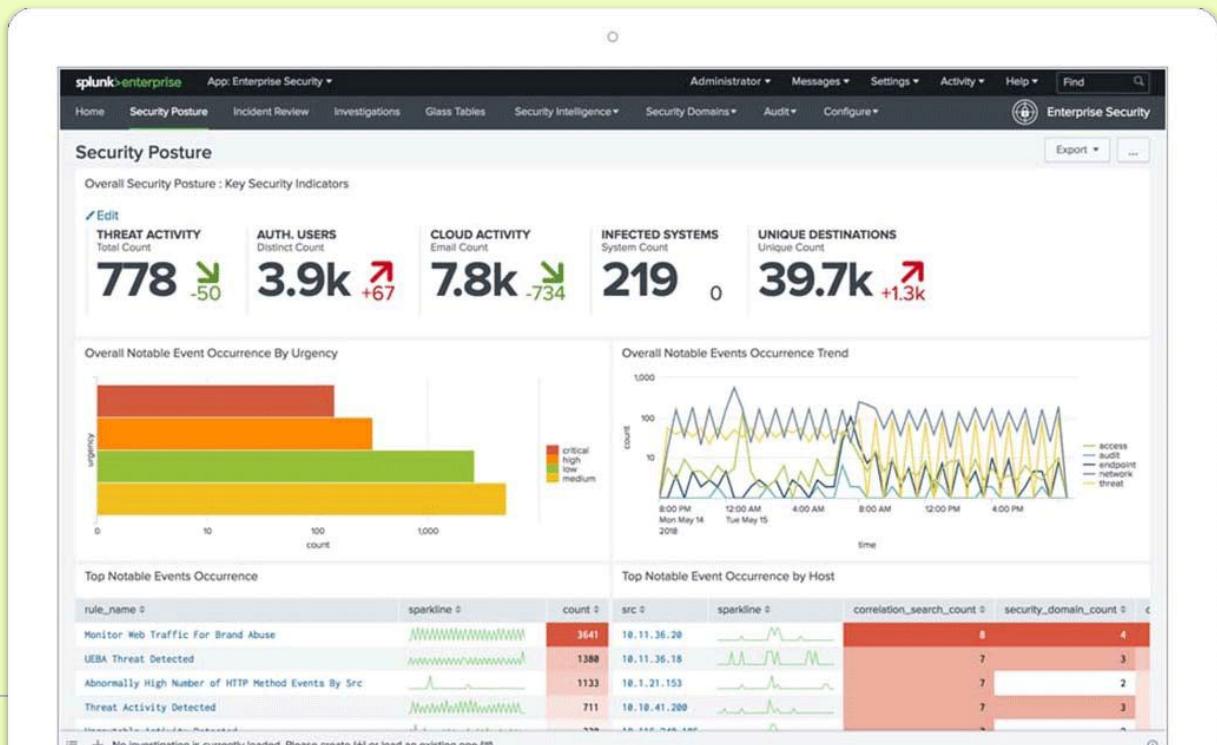


Work toward a Splunk certification using the Splunk Fundamentals eLearning program.

Splunk Enterprise Security

Throughout the past two units, we have covered many of Splunk's capabilities and add-on applications.

The Splunk SIEM product, **Splunk Enterprise Security (ES)**, is one of the most popular add-on products for security professionals.

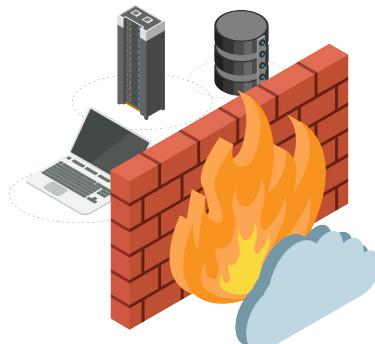


Splunk ES

Splunk ES is a SIEM product that provides security professionals insights from machine-generated data generated by such sources as:

01

Network devices
like routers and firewalls



02

Endpoint devices
like antivirus solutions



03

Vulnerability management systems
like Nessus



Splunk ES

Splunk ES features allow you to:



Identify, prioritize, and investigate security events.



Gain insights into security events.



Monitor the status of your security environment.



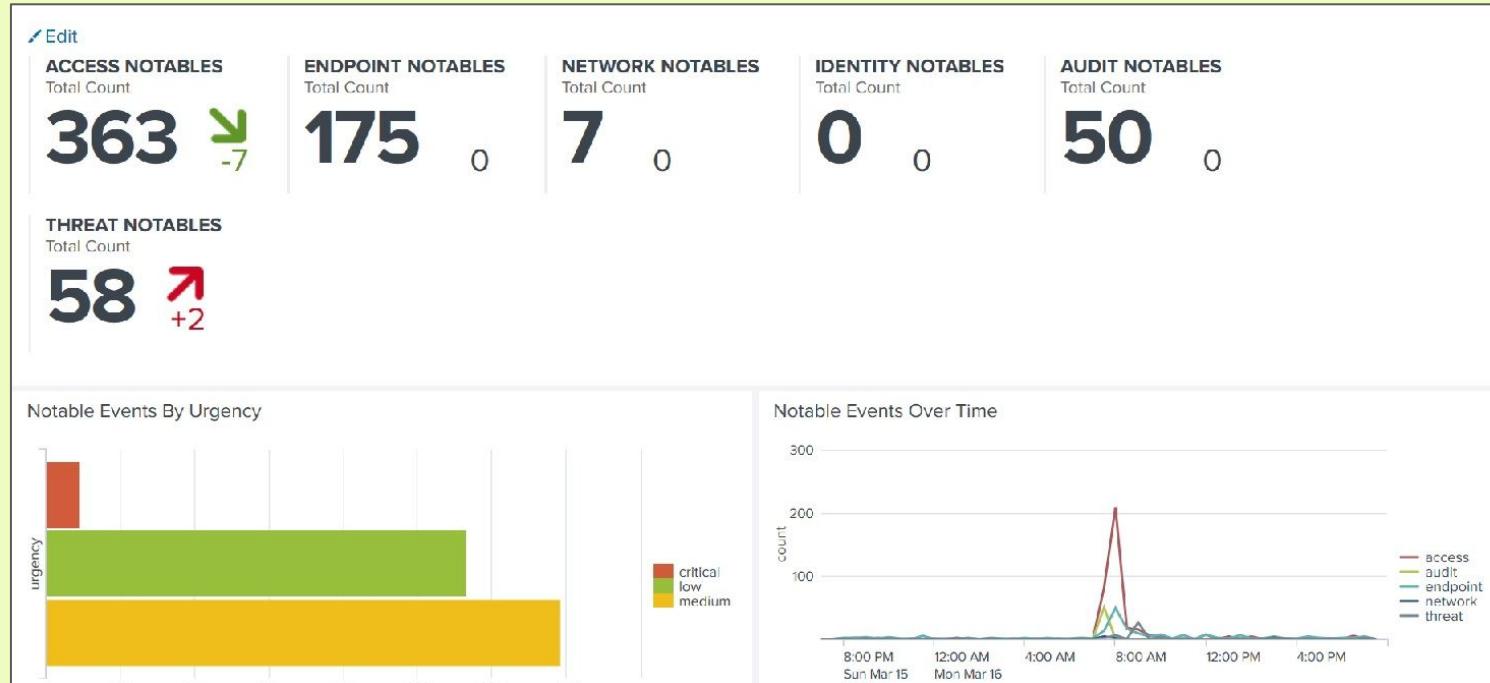
Audit your security events.



Navigate these tasks with a pre-built, easy-to-use interface.

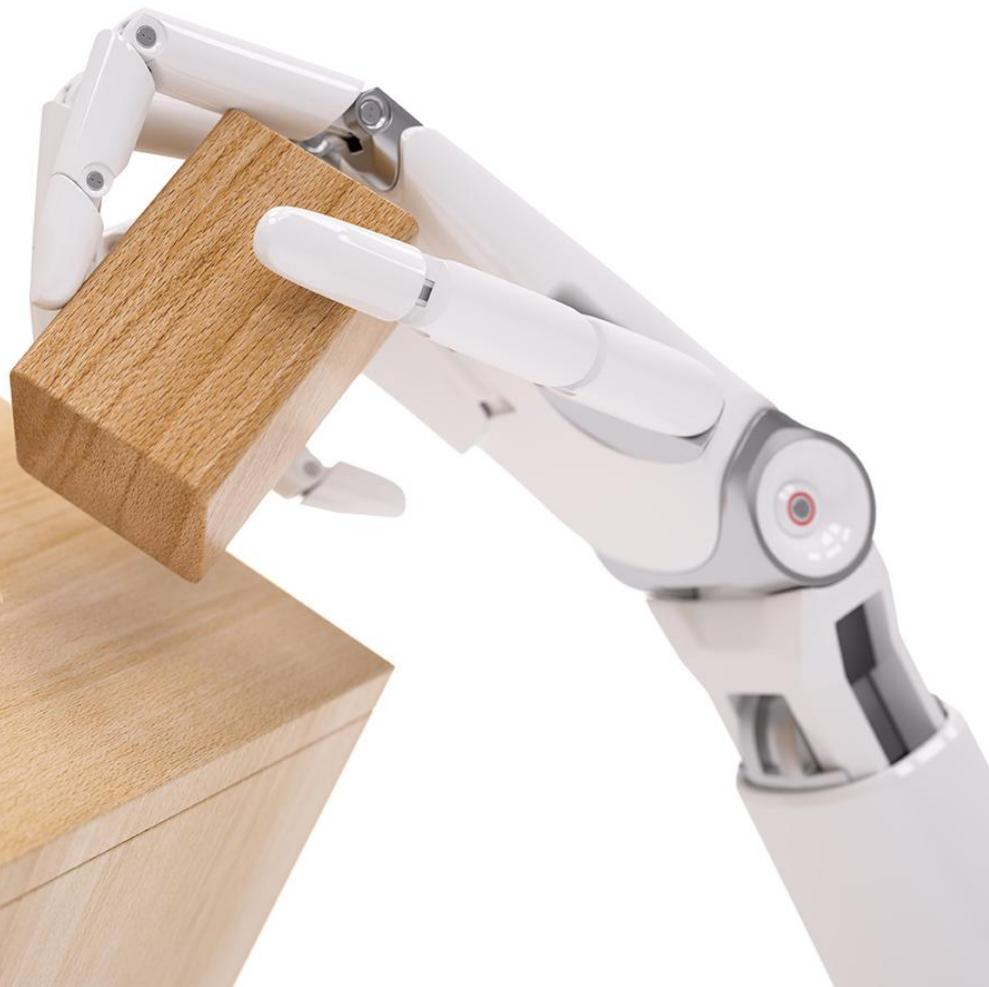
Splunk ES

Here's an example of a basic Splunk ES dashboard.



Advanced security monitoring solutions

provide additional benefits such as machine learning, artificial intelligence, automation, and response.



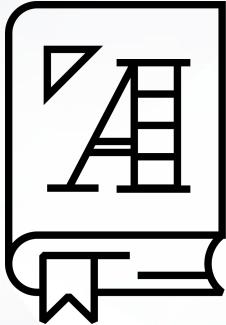
Advanced Security Monitoring

The most popular advancements in the information security industry are machine learning, artificial intelligence, automation, and response.

UBA = User Behavior Analytics

UEBA = User *and* Entity Behavior Analytics

SOAR = Security Orchestration,
 Automation, *and* Response



UBA is a security monitoring tool that uses machine learning, artificial intelligence, and data processing to detect abnormalities in user activity.

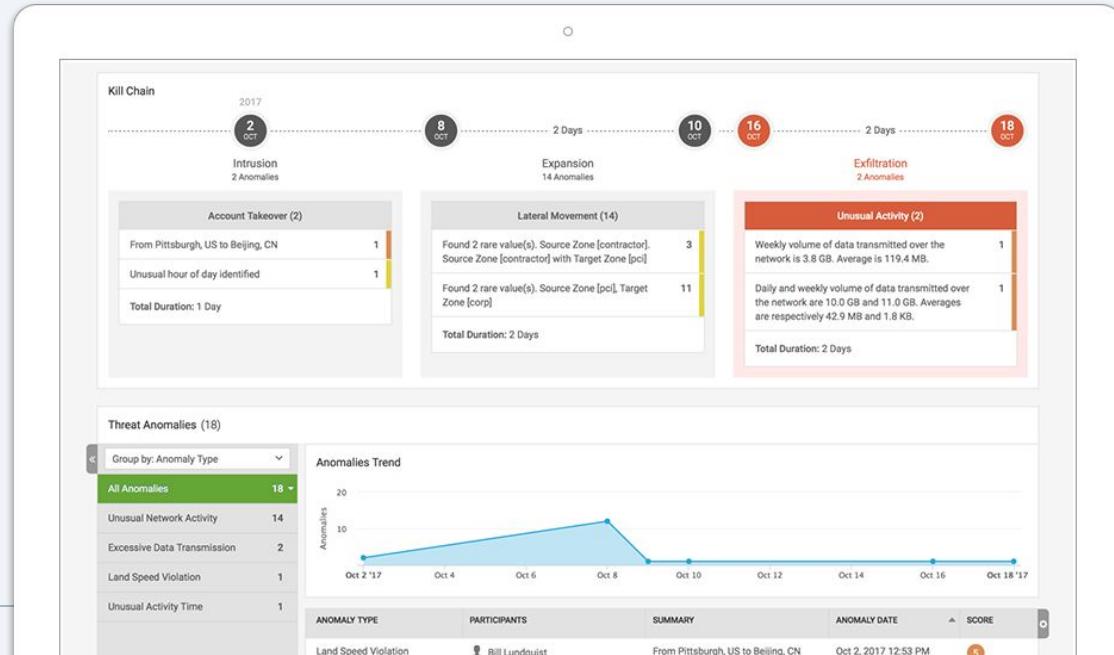
User Behavior Analytics (UBA)

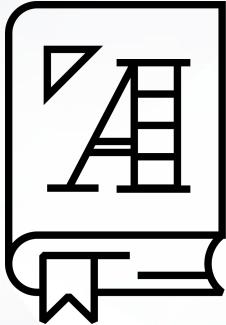
UBA gathers information about typical user behaviors and creates baselines.

For example

UBA can gather information on the servers and systems that a user accesses as well as when and how frequently they do so.

- UBA then creates alerts when a user's activity deviates from their typical behavior.
- If they usually only log onto a server between 9 a.m. and 5 p.m., Monday through Friday, UBA would create an alert if the user logged in on at 2 a.m. on a Saturday.

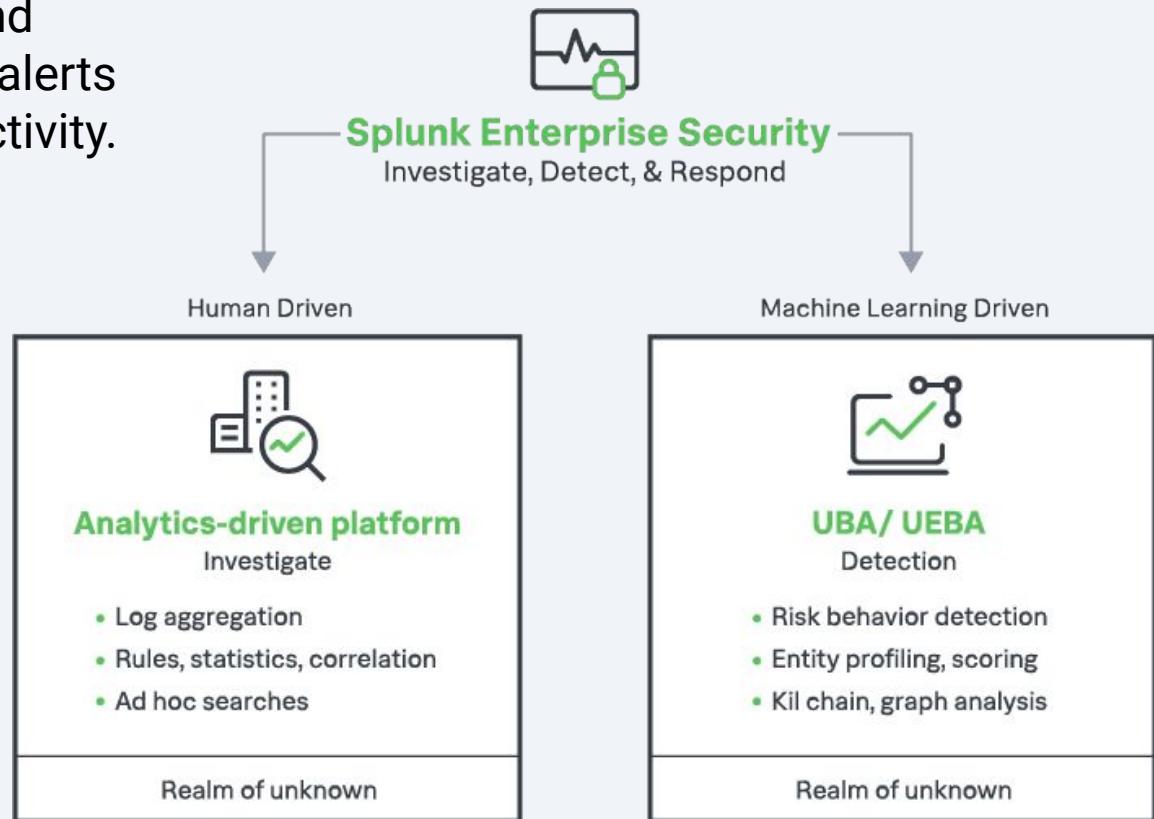


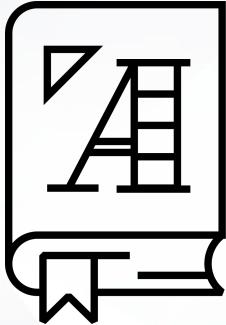


UEBA is a security monitoring tool similar to UBA, except it extends monitoring to other “entities,” such as routers, servers, and IoT devices.

User and Entity Behavior Analytics (UEBA)

UEBA looks at typical user and entity behaviors and creates alerts when they display unusual activity.





SOAR is like a SIEM that automates security processes and responds to security incidents.

Security Orchestration, Automation, and Response (SOAR)

Examples of **automating security processes** include:



Creating logs.



Assigning priorities to security incidents.

Examples of **responding to security incidents** include:



Launching security investigations.



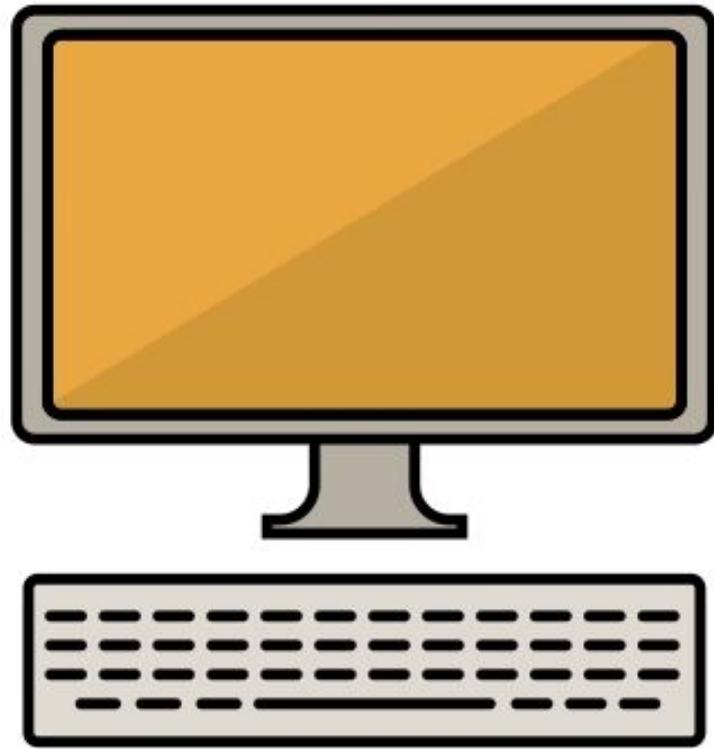
Threat mitigation.



Similar to a SIEM, SOAR gathers machine data from multiple entities and analyzes the data for security events.

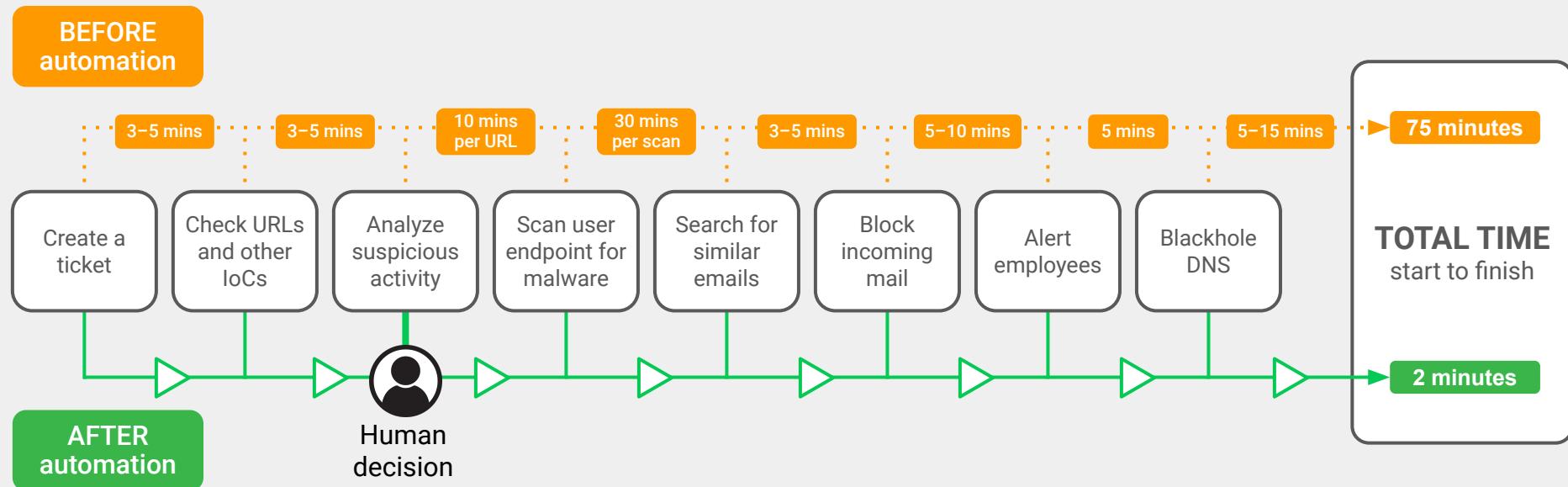
SOAR uses playbooks that detail the processes and response actions for specific event.

For example, an organization can design a playbook to automate responses to phishing incidents.



SOAR

This diagram illustrates how using SOAR playbooks can decrease incident response time.





Activity: Advanced Security Monitoring Tools

In this activity, you will research SOAR, UBA, and UEBA vendors to find a best fit for your organization.

Suggested Time:
15 Minutes





Time's Up! Let's Review.



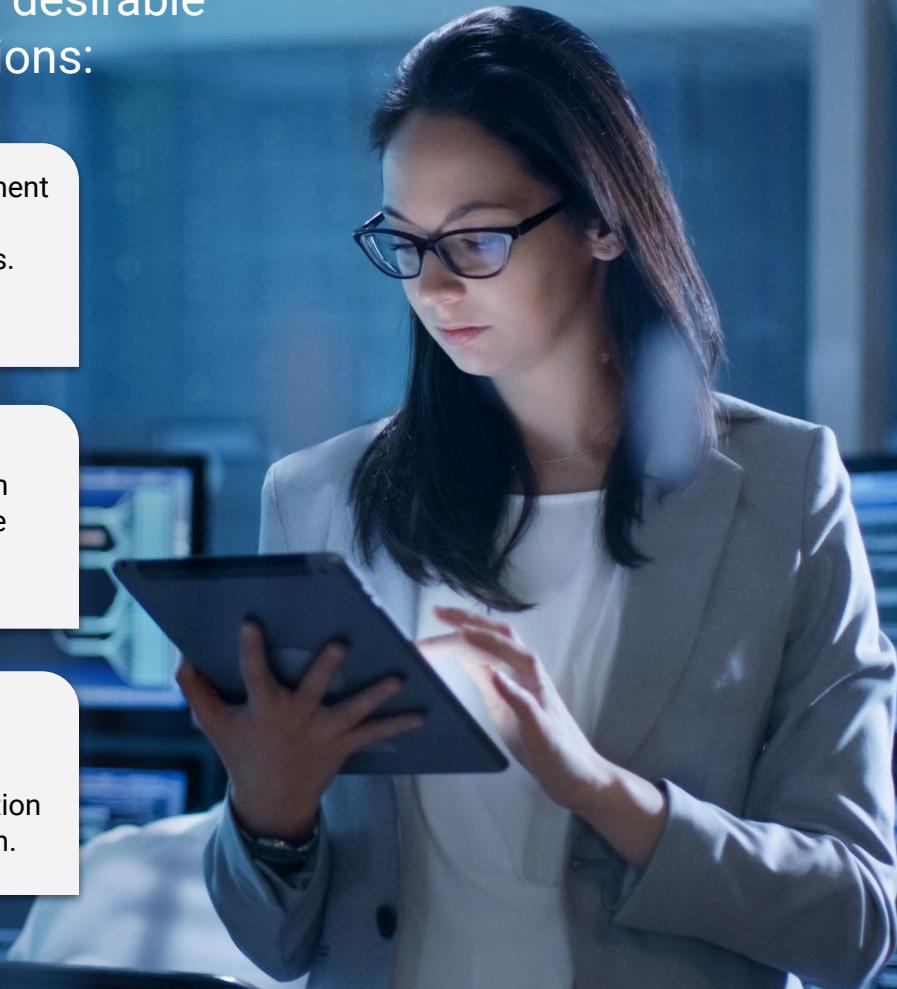
Now, we'll explore careers
and certifications related to the
Splunk knowledge and tools
learned over the past five days.

Experience working with Splunk is a desirable qualification for many infosec positions:

SOC analysts work in a Security Operations department with security engineers. This role involves detecting, containing, and remediating information security threats. Most SOC analysts use SIEM products like Splunk ES to monitor their environment.

Cyber threat analysts analyze an organization's networks and applications to protect organizations from cybercriminals. They often use Splunk products to make predictions about cybercriminals and what attacks they may conduct.

Application security engineers can use Splunk to assist with fixing web and mobile application vulnerabilities. They use Splunk to analyze their application logs to assist with creating and testing their remediation.



Experience working with Splunk is a desirable qualification for many infosec positions:

Network security administrators

use products like Splunk to monitor suspicious network traffic such as DDOS attacks. They can use findings from Splunk logs to mitigate and prevent future attacks.

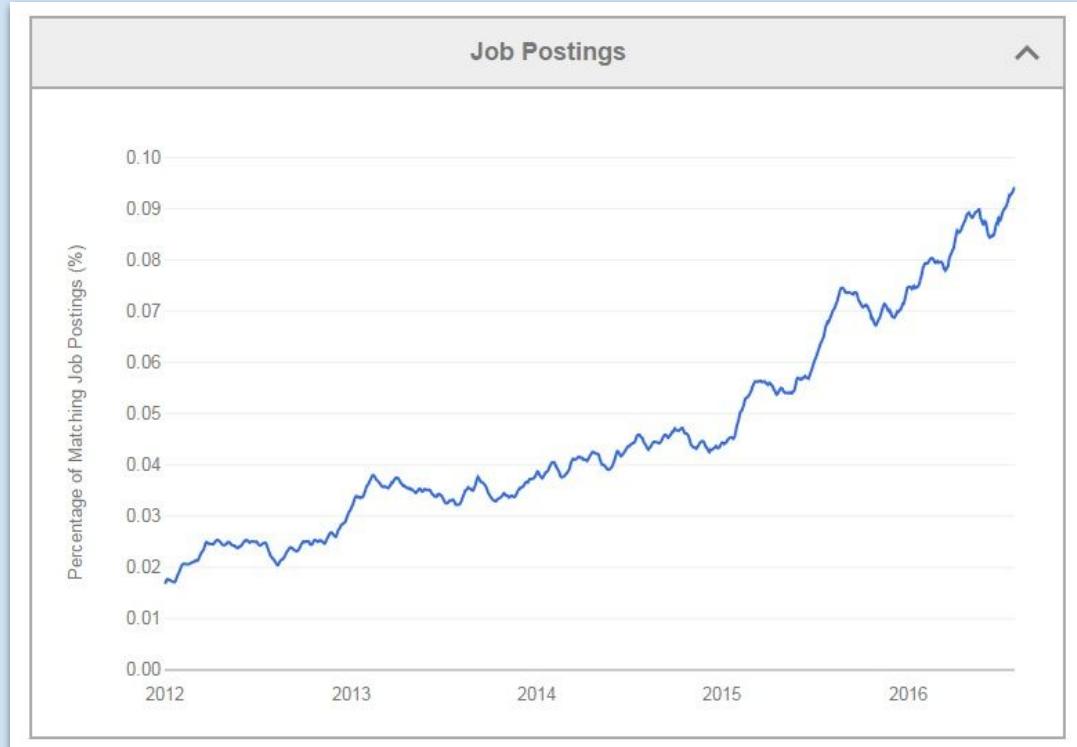
Incident response managers

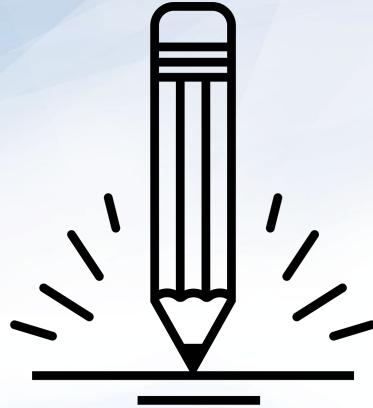
can use Splunk to monitor the status of ongoing security investigations when an incident has occurred.



Splunk in InfoSec Careers

Splunk is already a required skill in many roles, and the industry demand is increasing every year.





Activity: Splunk Careers

In this activity, you will search several job sites for Splunk-related careers and answer questions about each position.

Suggested Time:
15 Minutes





Time's Up! Let's Review.



Countdown timer

15:00

(with alarm)

Break





Similar to other domains in cybersecurity, Splunk skills are validated through certifications.

Splunk Certifications

Having a certification can help a cyber professional acquire a new position or receive a promotion, and can provide networking opportunities with professionals who have similar certifications.



Splunk Certifications

Splunk offers many certifications, for a variety of skill levels.



Splunk Core Certified User

Entry-level certification that demonstrates a user's basic ability to use the Splunk software.



Splunk Core Certified Power User

Demonstrates a user's foundational skills with Splunk's core software, plus more complex skills, such as creating calculated fields and data models.



Splunk Core Certified Advanced Power User

Demonstrates a user's capability to design reports, complicated searches, and dashboards.

Splunk Certifications

Splunk offers many certifications, for a variety of skill levels.



Splunk Enterprise Certified Admin

Focused on an individual's ability to support daily administrative tasks using Splunk Enterprise software.

Splunk Enterprise Certified Architect

Focused on a Splunk administrator's role supporting advanced troubleshooting, configurations, and deployments within Splunk Enterprise.

Splunk Enterprise Security Certified Admin

Focused on a Splunk administrator's role to support installation, advanced troubleshooting, configurations and deployments within Splunk Enterprise Security.

Splunk Certifications

Like many certifications in the infosec field, Splunk certifications are expensive.

Fortunately, Splunk offers the first certification class, **Splunk Fundamentals 1**, for free.

The screenshot shows a web browser displaying the Splunk website at splunk.com/en_us/training/free-courses/splunk-fundamentals-1.html. The page has a pink-to-orange gradient header with the text "SPLUNK TRAINING + CERTIFICATION" and "Splunk Fundamentals 1". Below the header, there's a sidebar with sections for "Training + Certification" and "Free Courses". The "Free Courses" section lists "Overview", "**Free Splunk Fundamentals 1**" (which is highlighted in pink), "Splunk Infrastructure Overview", "Splunk User Behavior Analytics", and "SignalFx Fundamentals Series (eLearning)". A "Download Course Description" button is located at the bottom of the sidebar. The main content area to the right describes the course and includes a "Download Course Description" button.

SPLUNK TRAINING + CERTIFICATION

Splunk Fundamentals 1

Training + Certification

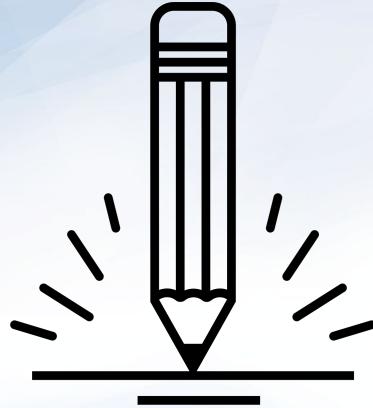
Free Courses

- Overview
- Free Splunk Fundamentals 1**
- Splunk Infrastructure Overview
- Splunk User Behavior Analytics
- SignalFx Fundamentals Series (eLearning)

Course Description

This course teaches you how to search and navigate in Splunk, use fields, get statistics from your data, create reports, dashboards, lookups, and alerts. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts. It will also introduce you to Splunk's datasets features and Pivot interface.

[Download Course Description](#)



Activity: Splunk Certifications

In this activity, you will register for a Splunk account and begin the first three modules of the Splunk Fundamentals 1 certification.

Suggested Time:
50 Minutes





Time's Up! Let's Review.

Splunk Certification

You are encouraged to complete the remaining modules on your own time.

Afterward, you can take the Splunk Fundamentals certification exam to earn a Splunk Certificate!



Next class, we will finish the SIEM unit with an activity incorporating everything we've learned about SIEM.

MASTER of the SOC

*The
End*