Advanced Security Monitoring Tools

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.

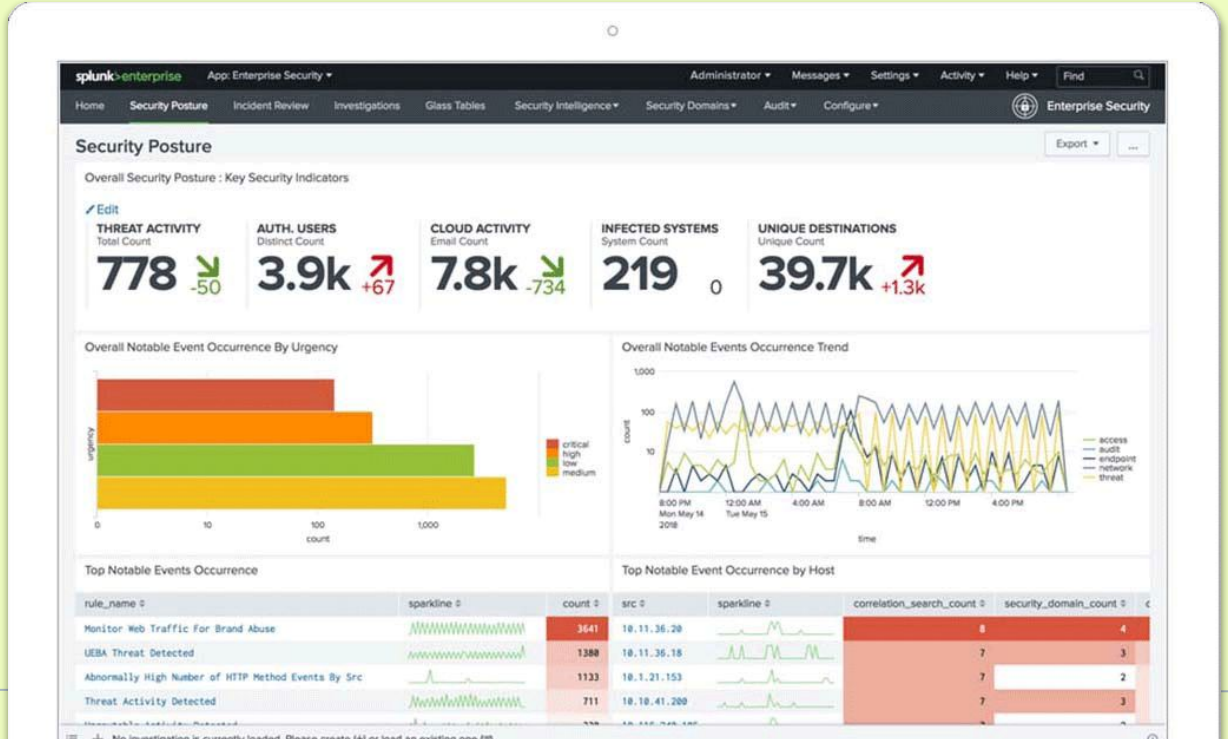
Understand how knowledge of SIEM software and Splunk is valued in the information security job market.

Continue learning about Splunk with free training courses

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.



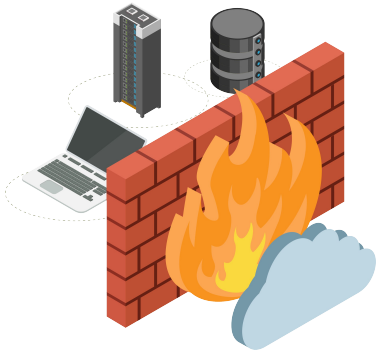
(splunk.com)

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

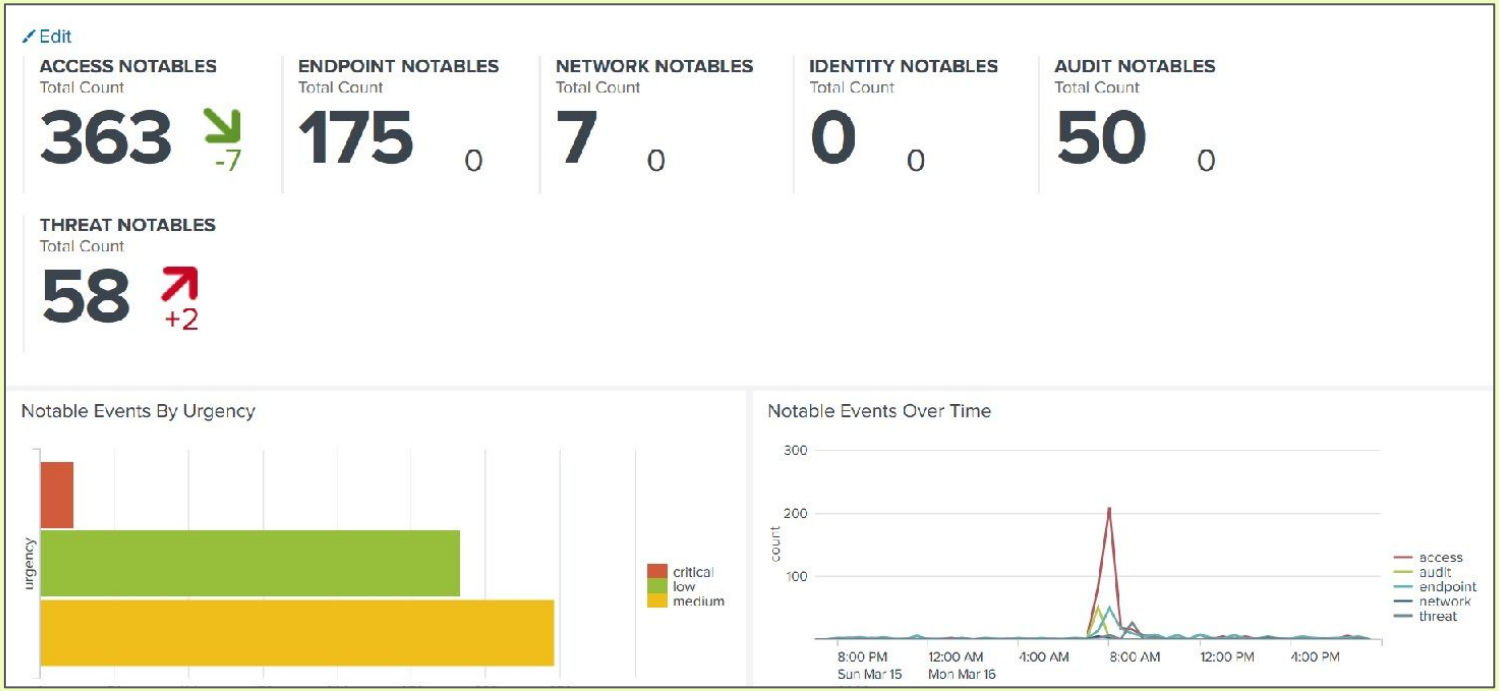
Splunk ES

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.

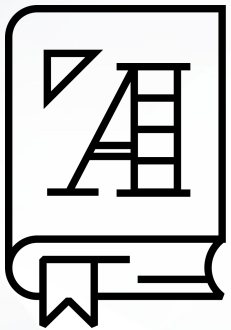
Advanced Security Monitoring

Advanced security monitoring solutions provide additional benefits such as machine learning, artificial intelligence, automation, and response.
The most popular advancements in the information security industry are:

UBA = **U**ser **B**ehavior **A**nalytics

UEBA = **U**ser *and* **E**ntity **B**ehavior **A**nalytics

SOAR = **S**ecurity **O**rchestration, **A**utomation, *and* **R**esponse



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

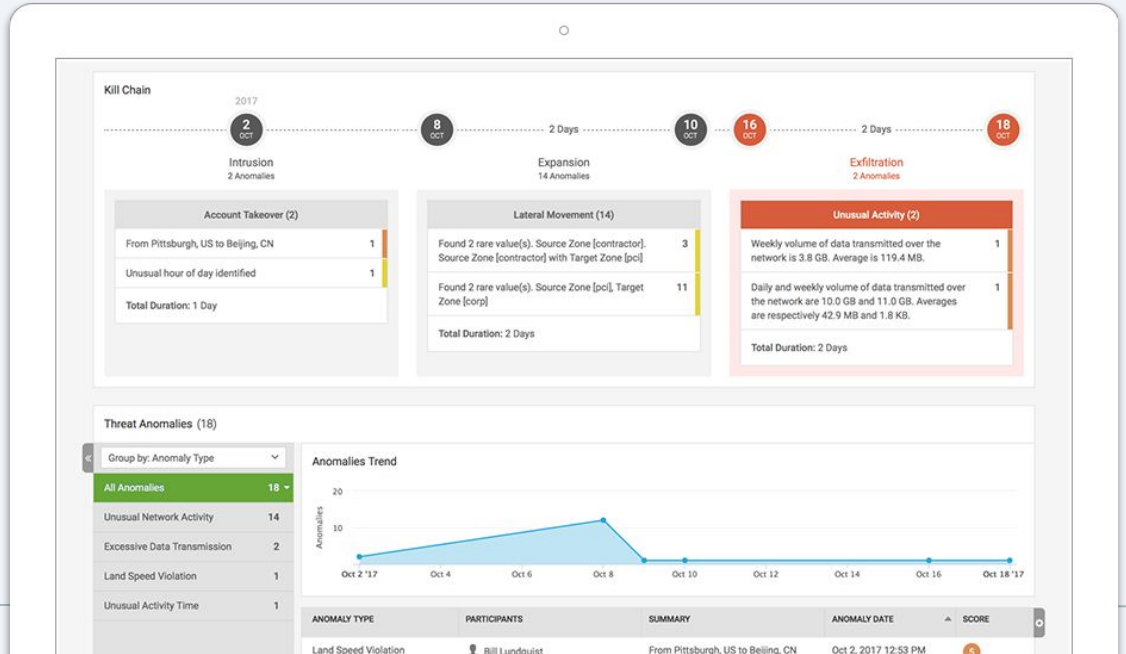
User Behavior Analytics (UBA)

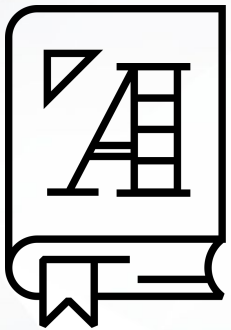
UBA gathers information about typical user behaviors and creates baselines.

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.

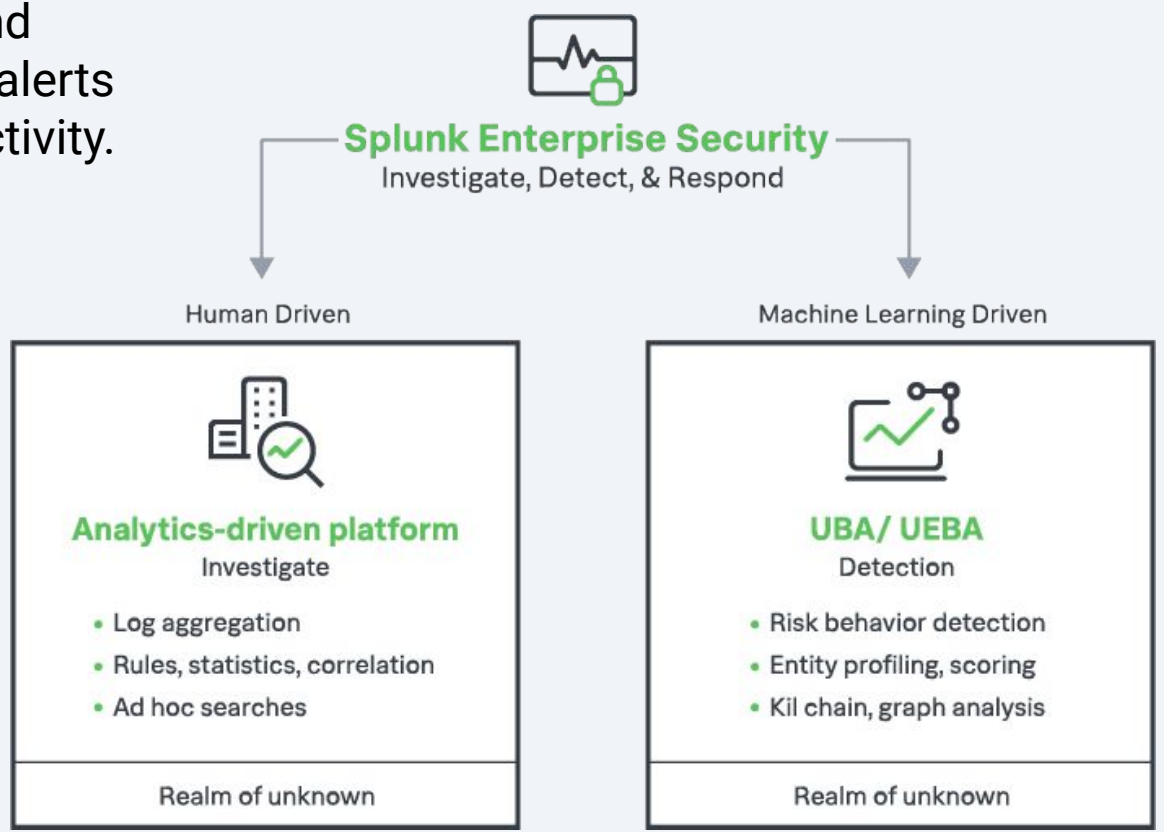




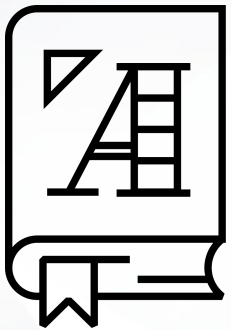
UEBA is a security monitoring tool similar to UBA, except it extends monitoring to other “entities,” such as routers, servers, and IoT devices.

User and Entity Behavior Analytics (UEBA)

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



(splunk.com)



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.

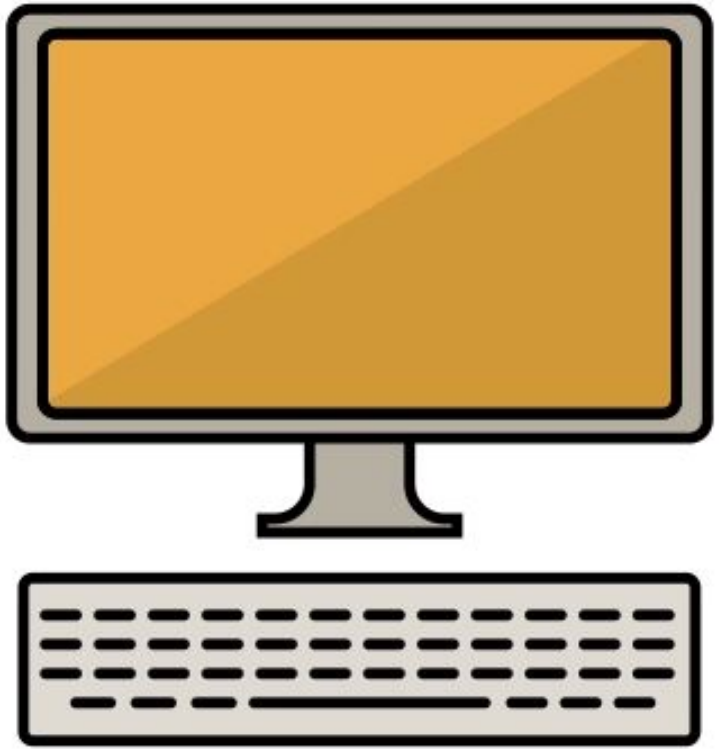
Examples of **responding to security incidents** include:

- 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.

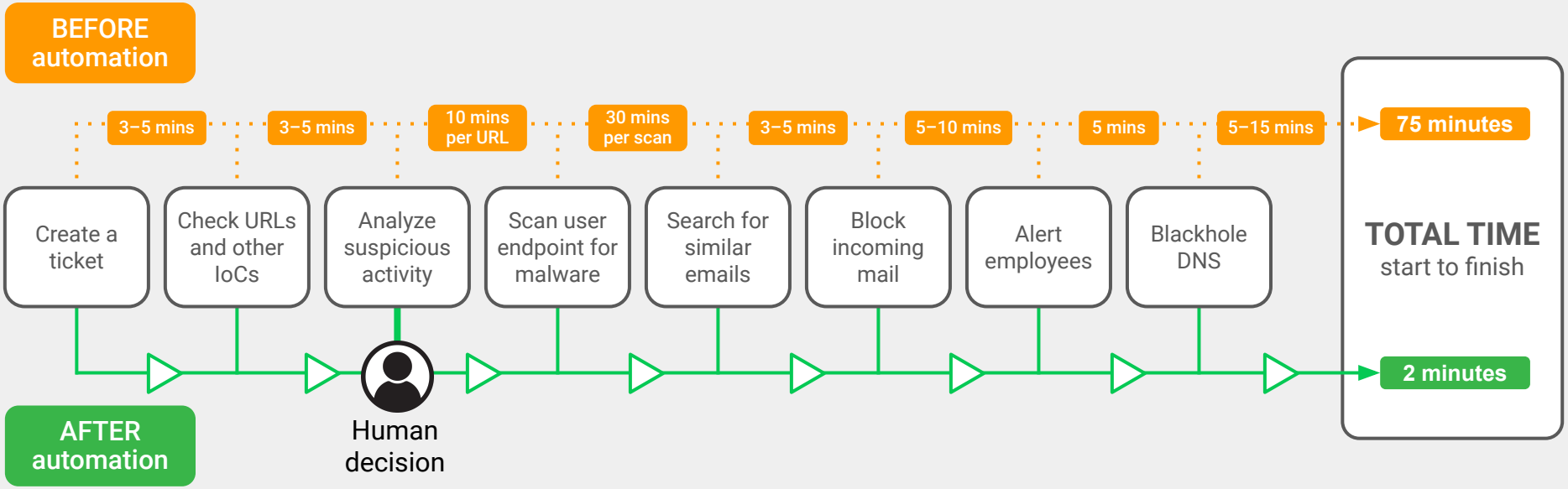
For example, an organization can design a playbook to automate responses to phishing incidents.

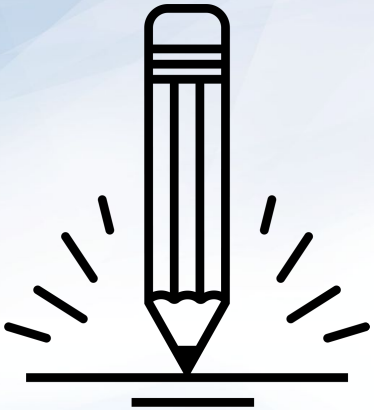


(Source)

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.

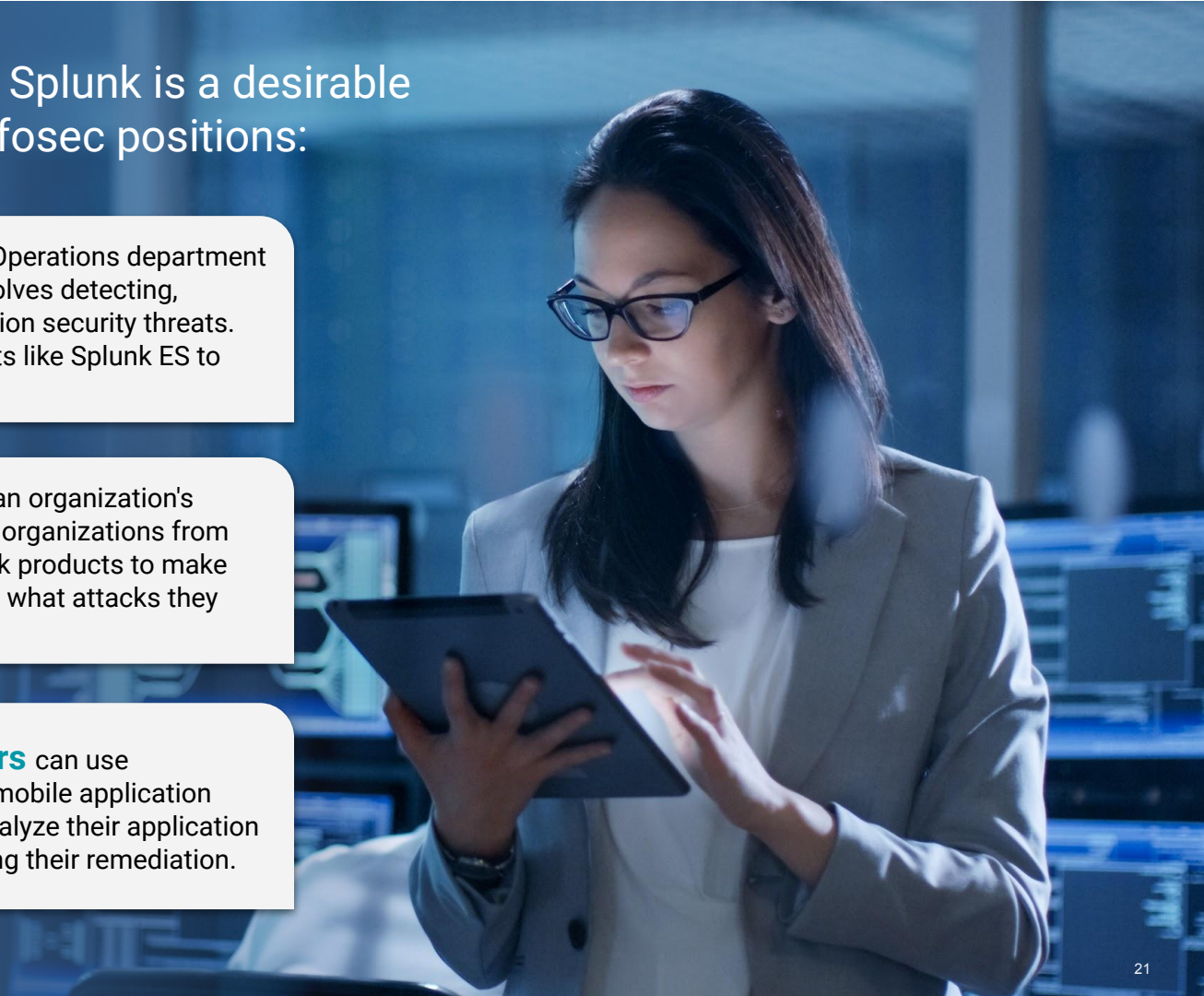
Now, we'll explore careers and certifications related to the Splunk knowledge and tools learned over the past five days.

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

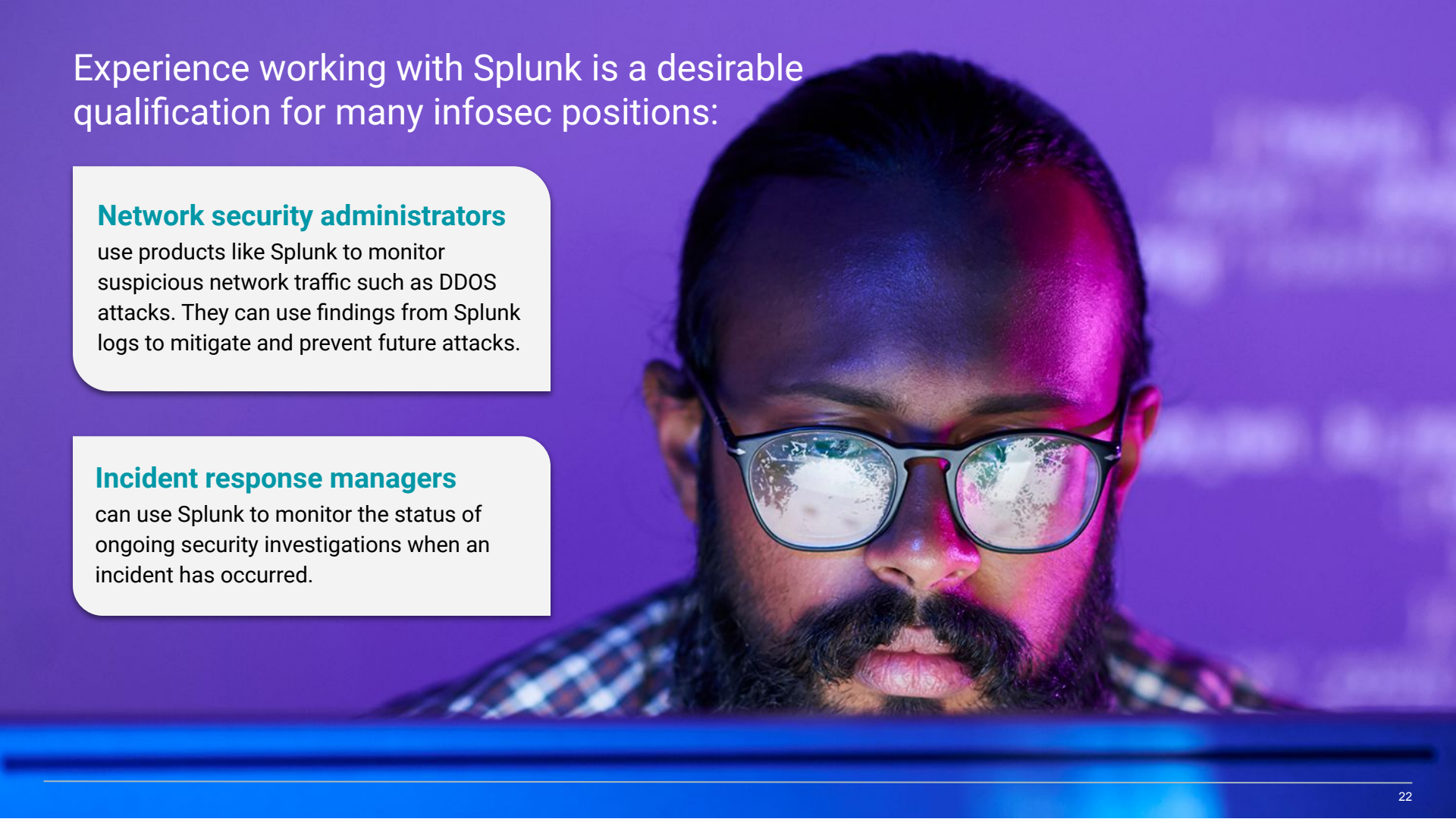
SOC analysts work in a Security Operations department with security engineers. This role involves detecting, containing, and remediating information security threats. Most SOC analysts use SIEM products like Splunk ES to monitor their environment.

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

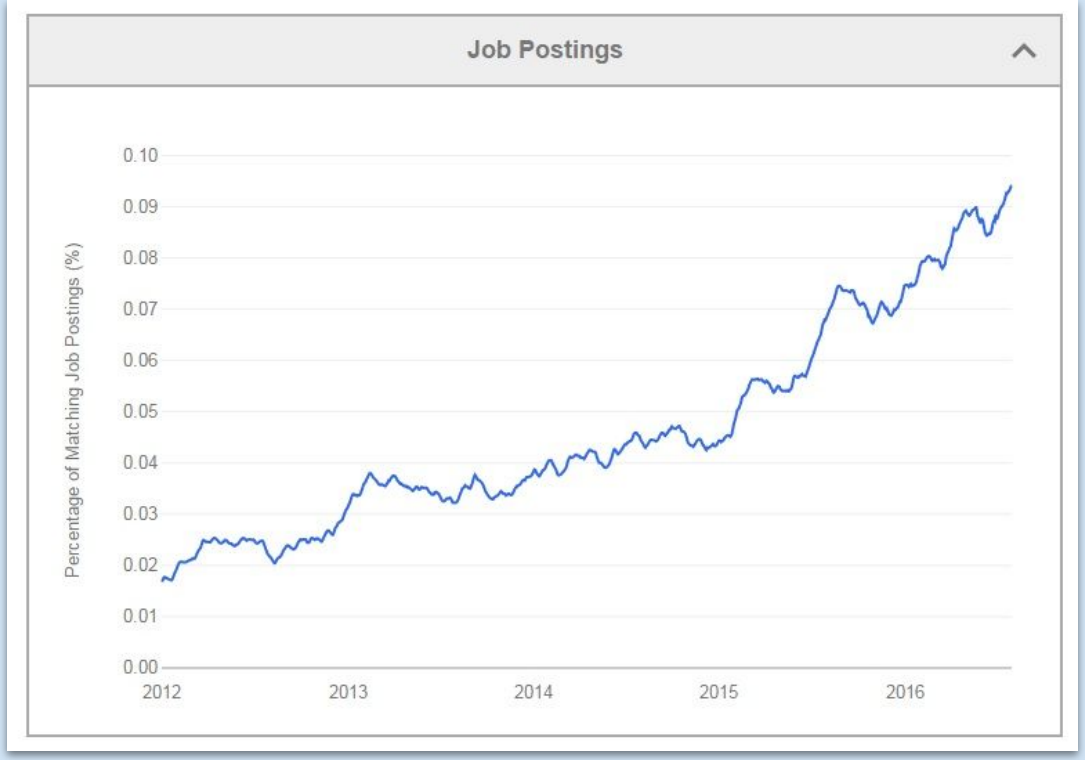
use products like Splunk to monitor suspicious network traffic such as DDOS attacks. They can use findings from Splunk logs to mitigate and prevent future attacks.

Incident response managers

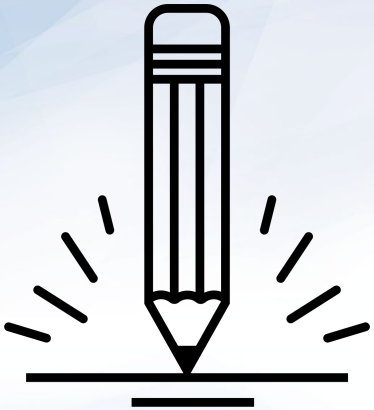
can use Splunk to monitor the status of ongoing security investigations when an incident has occurred.

Splunk in InfoSec Careers

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



(Source: Indeed)



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)

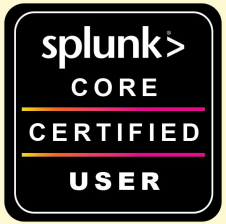
Similar to other domains in cybersecurity, Splunk skills are validated through certifications.

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.

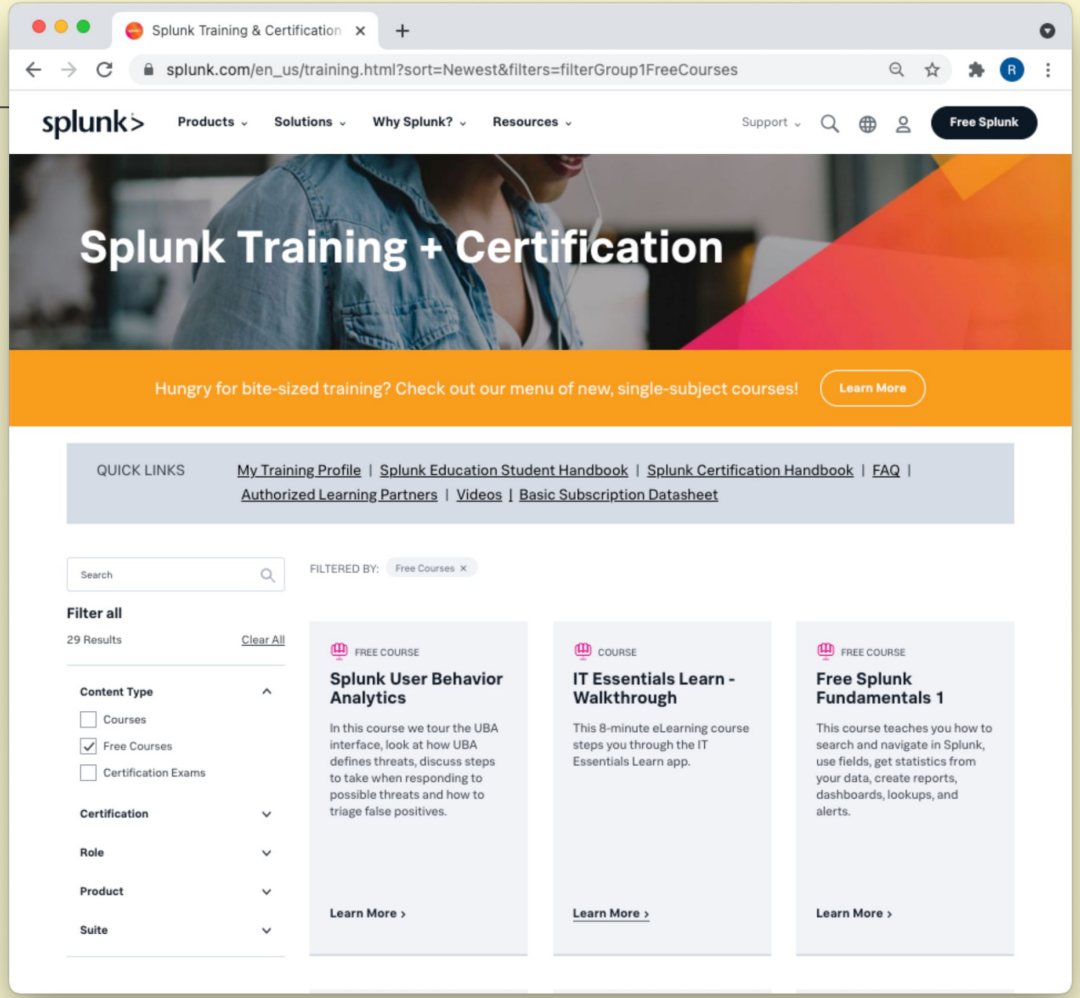
Splunk Enterprise Security Certified Admin

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

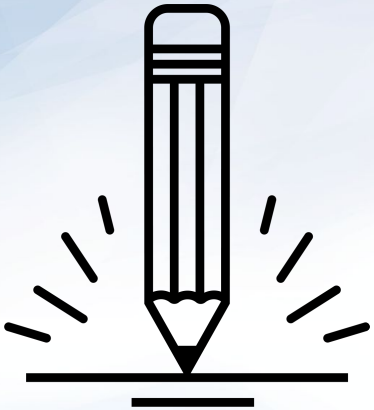
Splunk Certifications

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

Fortunately, Splunk offers the many single-subject courses for free.



(splunk.com)



Activity: Splunk Certifications

In this activity, you will register for a Splunk account and begin Splunk single-subject courses.

Suggested Time:
50 Minutes

Time’s Up! Let’s Review.

Splunk Certification

If you are interested in continuing your education towards a Splunk Core Certified User certification, you can access additional learning courses on your own time.

Afterward, you can take the Splunk Core Certified User exam to earn a Splunk Certificate!

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


The End