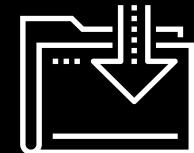




# Advanced Security Monitoring Tools

Cybersecurity  
SIEM 2 Day 2



# Class Objectives

---

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



Differentiate between various advanced security monitoring solutions, such as SOARs, UBAs, and UEBAs, and determine which is most appropriate for a specific security situation.



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



Continue learning about Splunk with free Splunk training courses.

# Advanced Security Monitoring Tools

# Introduction to Advanced Security Monitoring Tools

---

Today, we'll learn about other information security products used by security organizations.

We'll introduce Splunk's SIEM product, Enterprise Security, and explore several other security products available in the marketplace.

We will introduce and work towards the Splunk Fundamentals certification.



**First**

**Next**

**After the break**

**Finally**

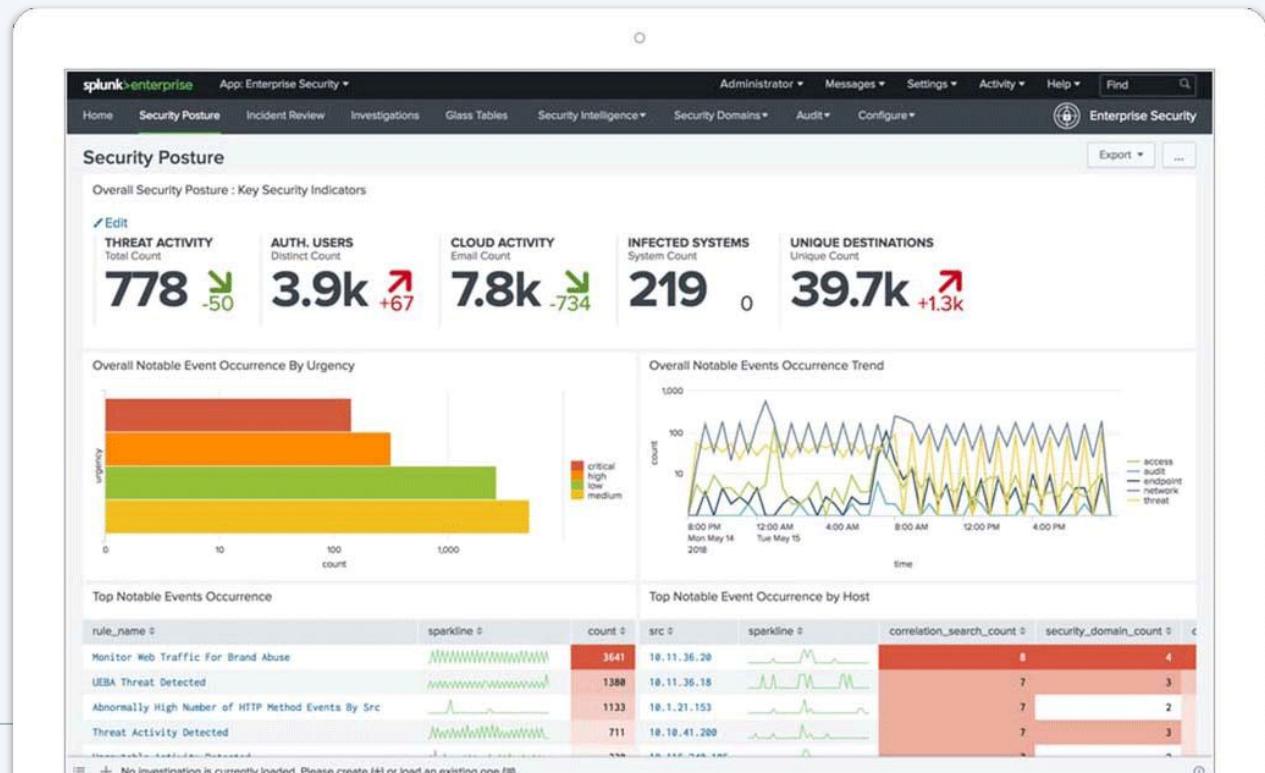
We'll focus on security careers relevant to the knowledge and tools learned in the last five classes.

We'll introduce the final project, the bootCon presentation.

# Splunk Enterprise Security

In the past five classes, we 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.

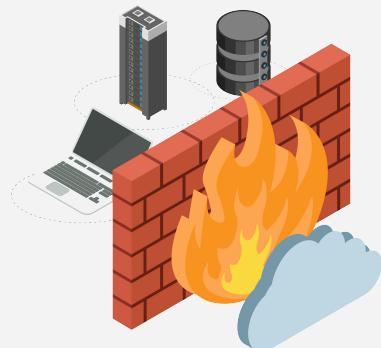


# Splunk ES

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** is one of the most popular add-on products for security professionals, as it has pre-built dashboards, reports, and built-in features.



# Splunk ES

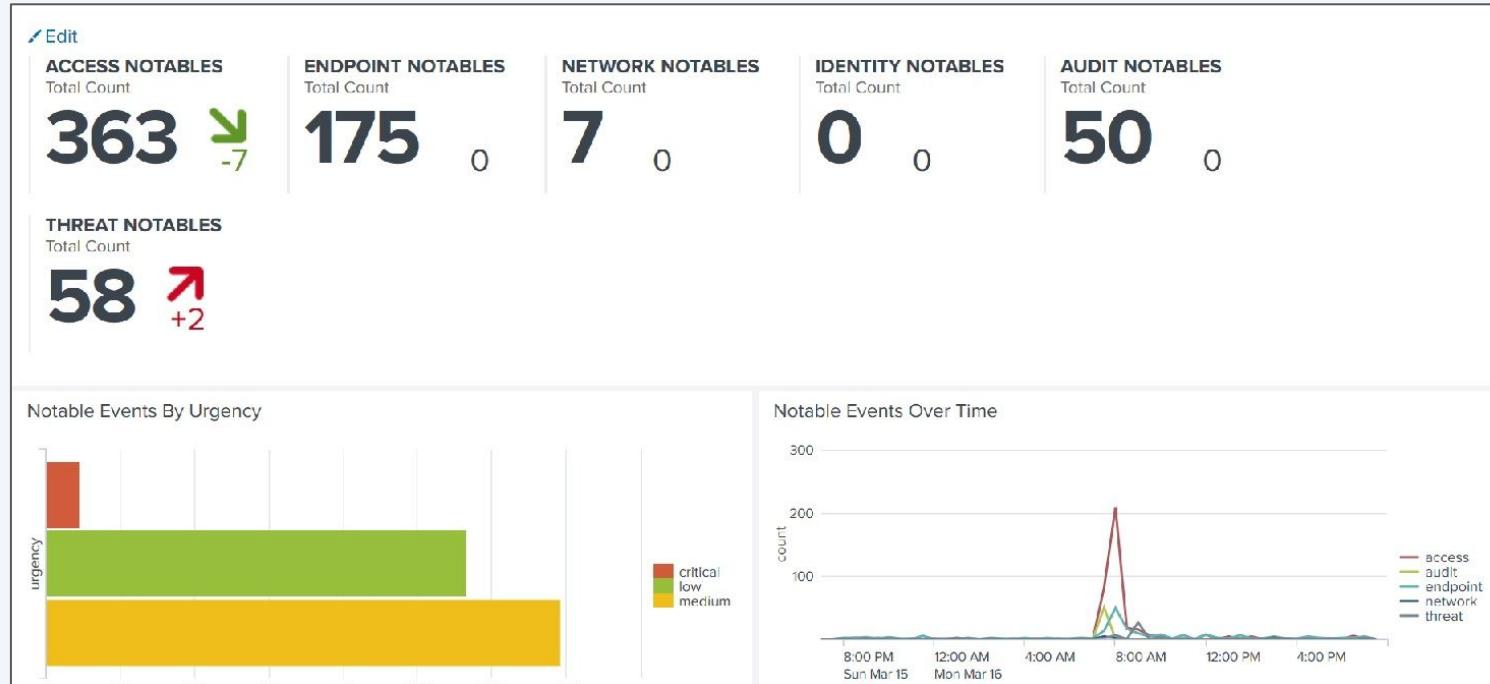
---

Splunk ES features allow you to:

-  Identify, prioritize, and investigate security events
-  Gain insights into security events
-  Monitor the status of a security environment
-  Audit security events
-  Navigate these tasks with a pre-built, easy-to-use interface

# Splunk ES

## 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 include:

<b>UBA</b>	<b>User behavior analytics</b>	A security monitoring tool that uses machine learning, artificial intelligence, and data processing to detect abnormalities in user activity
<b>UEBA</b>	<b>User and entity behavior analytics</b>	A security monitoring tool similar to UBA, except it extends its monitoring to other “entities”
<b>SOAR</b>	<b>Security orchestration, automation, and response</b>	Comparable to a SIEM, it automates security processes and responds to security incidents

# UBA

UBA gathers information about typical user behaviors and creates baselines.

The screenshot shows the Splunk User Behavior Analytics (UBA) interface. At the top, there's a navigation bar with links for Explore, Analytics, Manage, System, Scope, and admin. Below the navigation is a summary section with counts for Threats, Anomalies, Users, Devices, and Apps. On the right side of this summary are three green buttons: Threats Review, Users Review, and Analytics Dashboard. The main content area is divided into four sections: Latest Threats, Threats Timeline (Last 7 Days), Latest Anomalies, and Anomalies Timeline (Last 7 Days). Each section contains a table or chart with threat or anomaly details and a timeline of events over the last 7 days.

**Latest Threats**

Threat Type	Date	Count
Data Exfiltration by Suspicious User or Device	May 29	4
Data Exfiltration by Suspicious User or Device	May 28	4
Malware	May 28	6
Malware	May 28	8
Data Exfiltration by Suspicious User or Device	May 28	4
Malware	May 28	8

Showing top 20 of 23 threats [View Details](#)

**Threats Timeline (Last 7 Days)**

Threat Types: Malware, Compromised Account, Data Exfiltration after Account Takeover, Exfiltration, Privilege Escalation... Powershell Activity, Data Exfiltration by Compromised Account, Data Exfiltration by...icious Data Transfer

**Latest Anomalies**

Anomaly Type	Date	Count
USB storage attached an unusually high number of times	May 29	2
USB storage attached an unusually high number of times	May 29	2
Blacklisted IP Address	May 29	7
Suspicious Network Connection	May 28	8

**Anomalies Timeline (Last 7 Days)**

Anomaly Types: Unusual Printer Usage, Blacklisted IP Address, Blacklisted Domain, Excessive Data Transmission

# UBA

---

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 can then create alerts for when a user's activity deviates from this typical behavior.



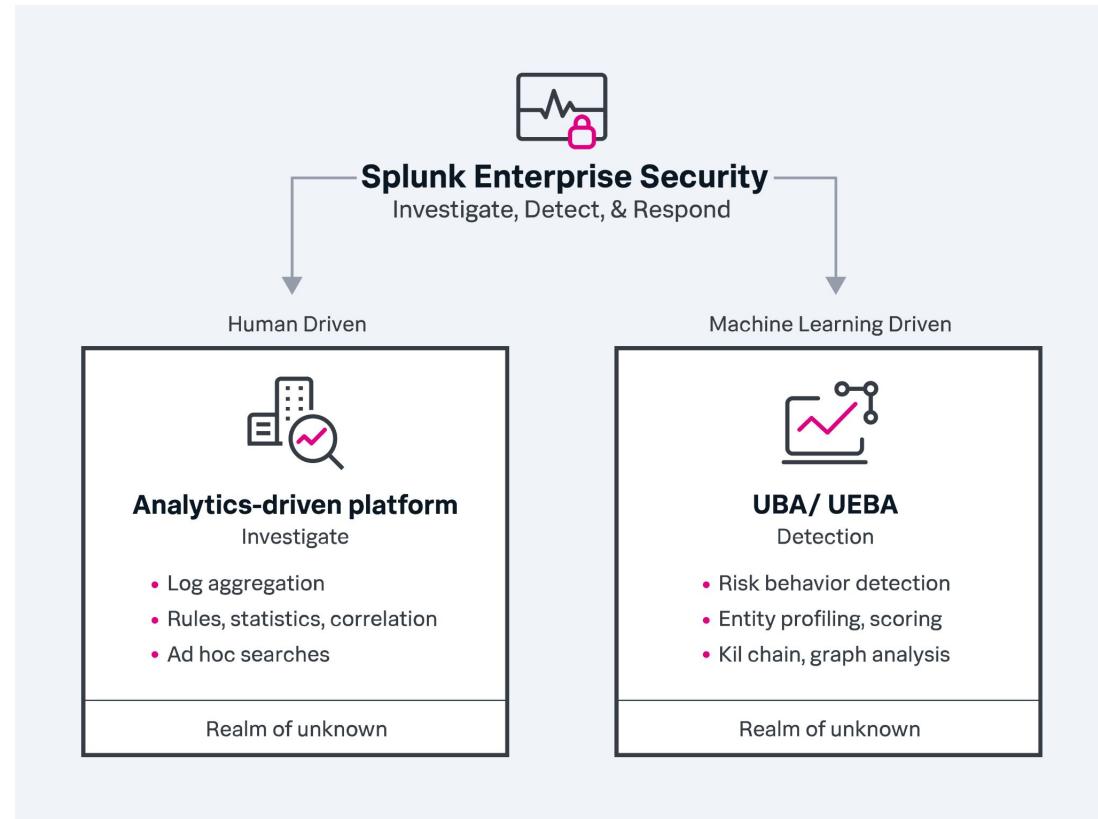
If a user usually only logs in to a server between 9am and 5pm Monday through Friday, UBA would create an alert if the user logged in at 2am on a Saturday.

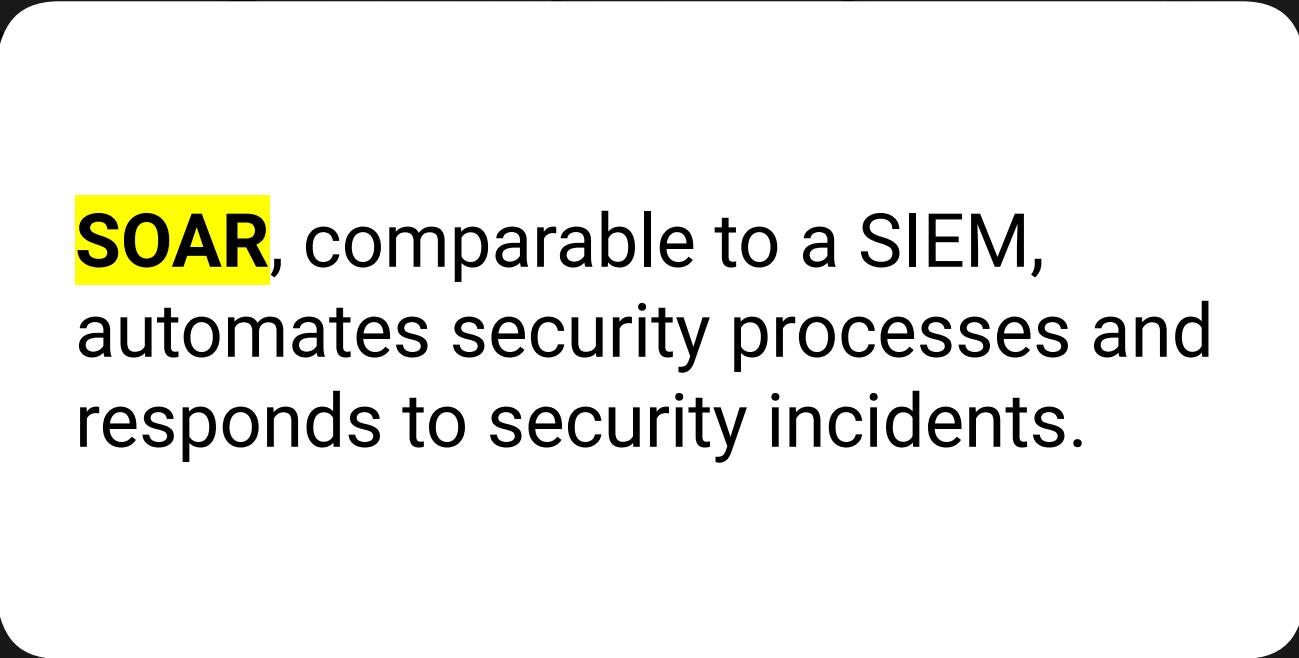
**UEBA** is a security monitoring tool similar to UBA, except it extends its monitoring to other “entities.”

*Entities can include routers, servers, and IoT devices.*

# UEBA

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





**SOAR**, comparable to a SIEM,  
automates security processes and  
responds to security incidents.

# SOAR

---

Examples of:

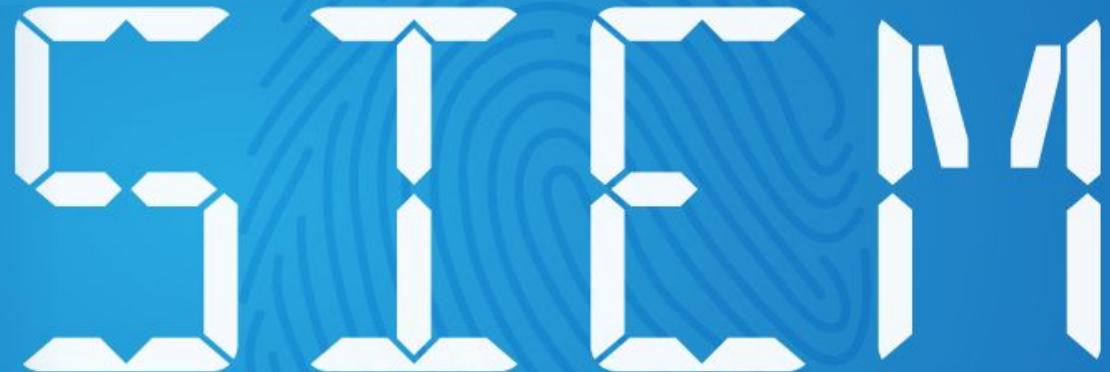
Automating security processes

- Creating logging
- Assigning priorities to security incidents

Responding to security

- Launching security investigations
- Mitigating threats

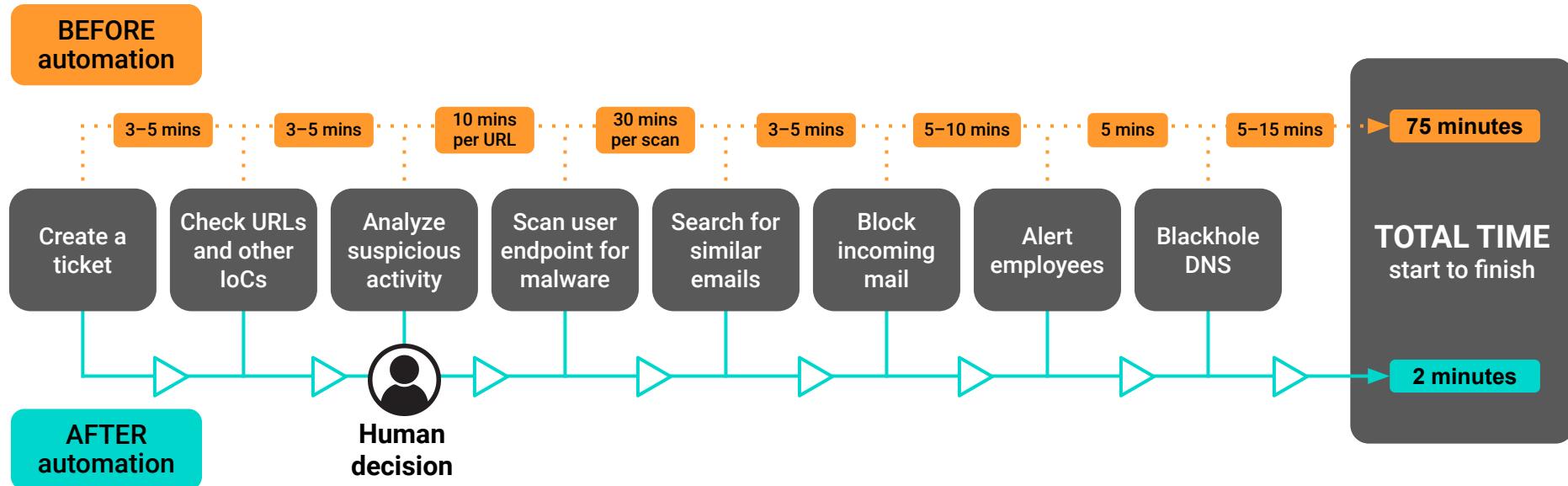
Similar to a SIEM, SOAR gathers machine data from multiple entities and analyzes the data for security events.



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

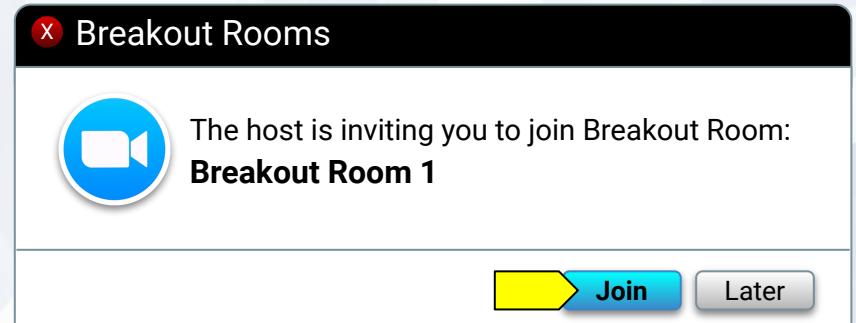
# SOAR

This diagram illustrates how using SOAR playbooks can decrease incident response time. Playbooks are uniquely designed and configured by each organization.



# 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.

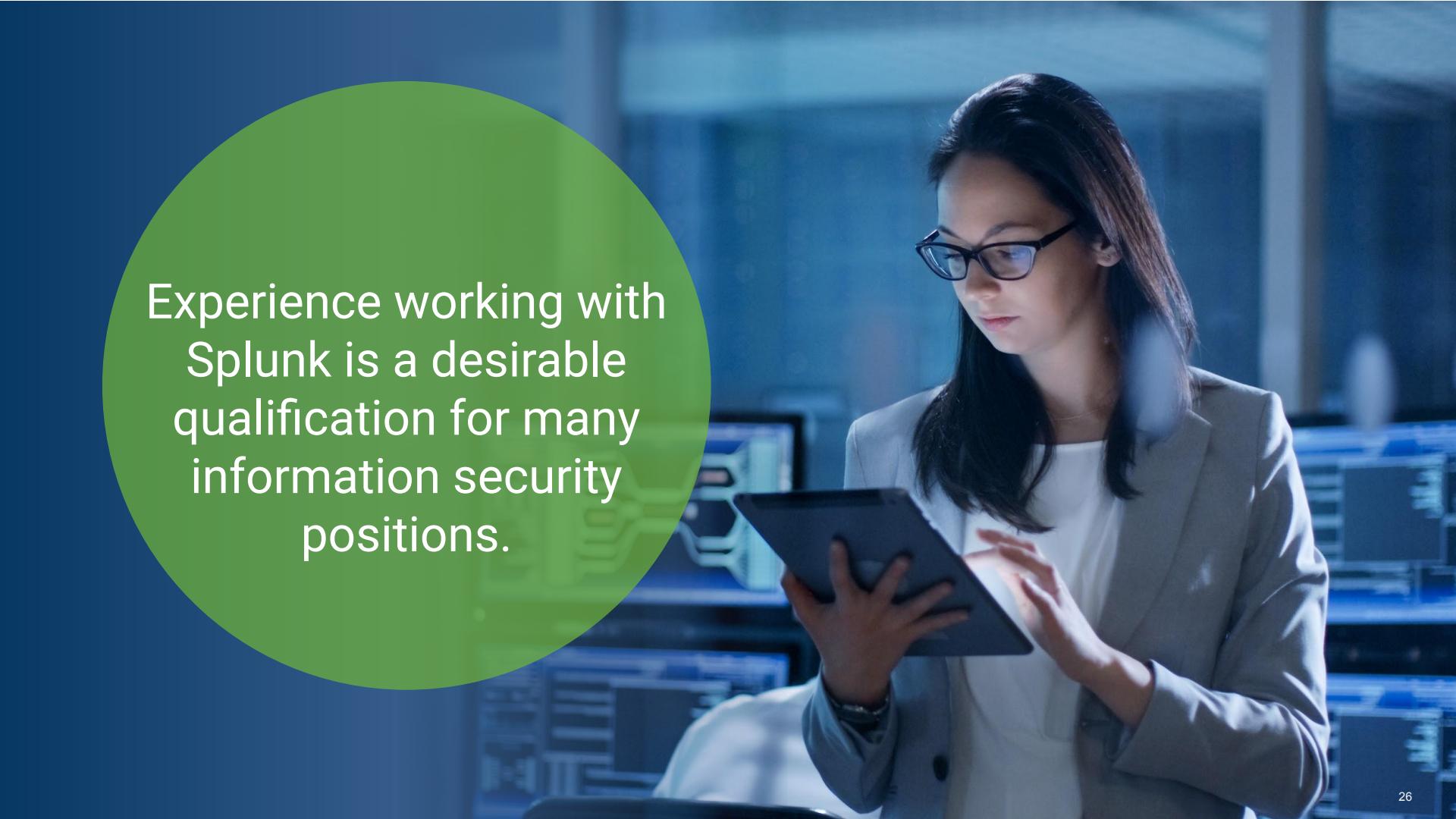
# Questions?



# Splunk Careers

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



A professional woman with long dark hair and glasses, wearing a light-colored blazer over a white top, is focused on a tablet device she is holding with both hands. She is positioned in a dark room that appears to be a control room or server room, with multiple computer monitors in the background displaying various data and graphs. A large green circular graphic overlaps the left side of the slide, containing the text.

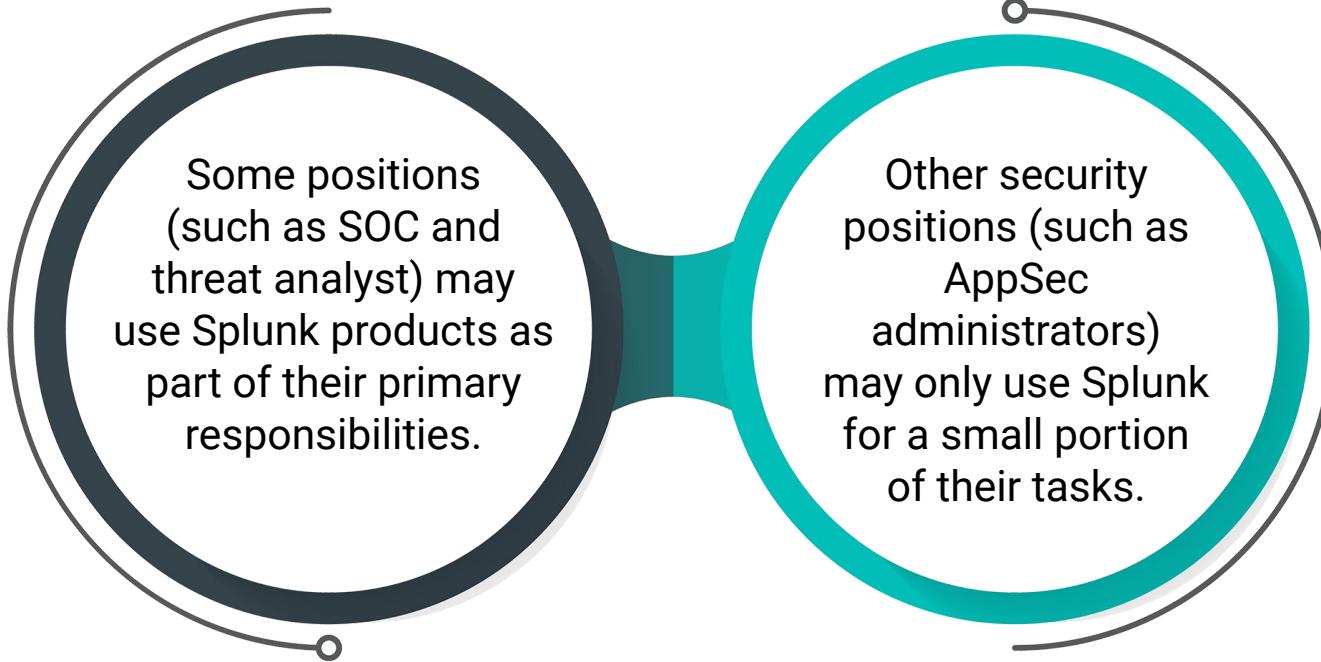
Experience working with Splunk is a desirable qualification for many information security positions.

# Splunk Careers: InfoSec Positions

<b>SOC analysts</b>	Work in a security operations department alongside security engineers. Their positions involve detecting, containing, and potentially remediating information security threats. Most SOC analysts use SIEM products, such as Splunk ES, to monitor their environment.
<b>Cyber threat analysts</b>	Analyze an organization's networks and applications to protect organizations from cybercriminals. Cyber threat analysts often use Splunk products to make predictions about cybercriminals and what attacks they may conduct.
<b>Application security engineers</b>	Use Splunk to fix web and mobile application vulnerabilities. AppSec engineers use Splunk to analyze their application logs to assist with creating and testing their remediation.
<b>Network security administrators</b>	Use products like Splunk to monitor suspicious network traffic, such as DDOS attacks. They can use the findings from Splunk logs to mitigate and prevent future attacks.
<b>Incident response managers</b>	Use Splunk to monitor the status of ongoing security investigations when an incident has occurred.

# Splunk Careers: InfoSec Positions

---

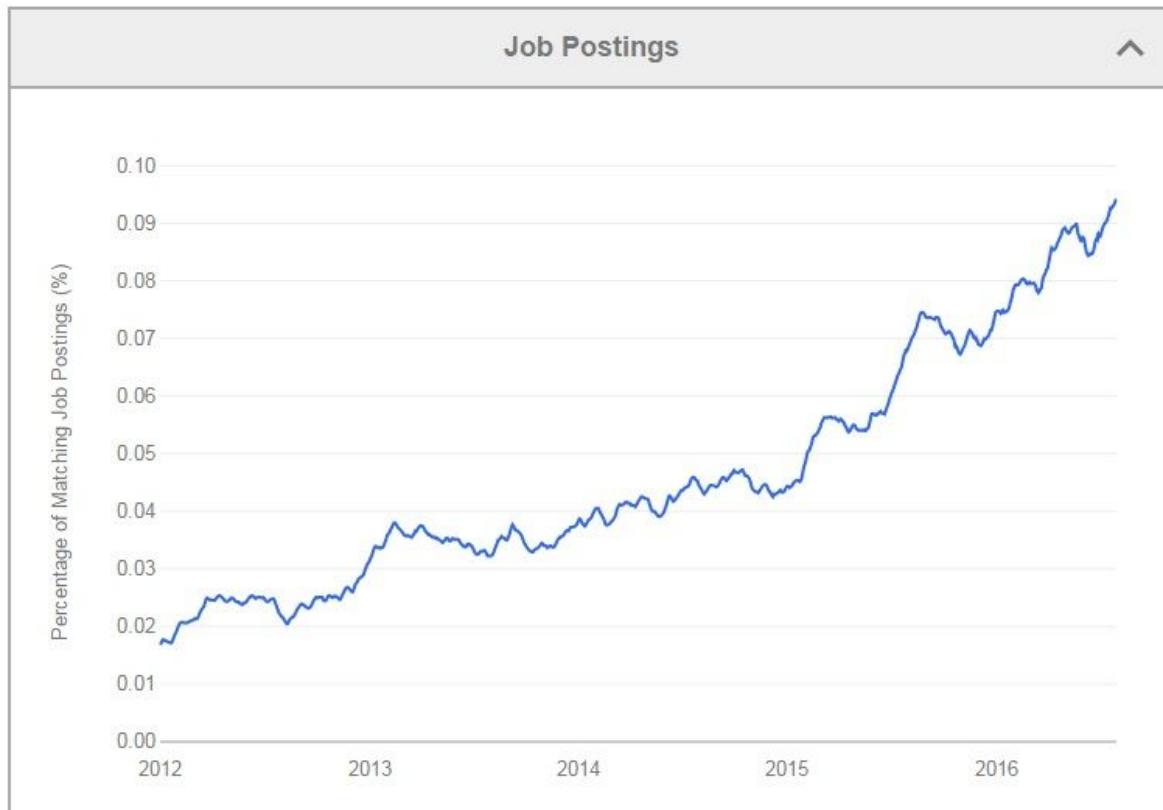


Either way, understanding how to use Splunk is a valuable skill for InfoSec professionals.

# Splunk in InfoSec Careers

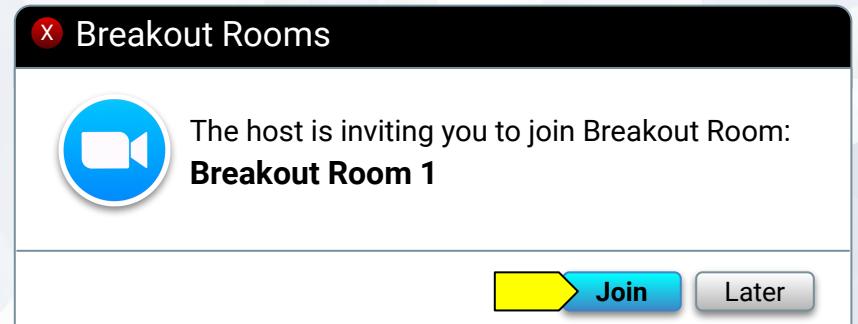
Splunk is already a required skill in many roles, and the industry demand is increasing every year.

This chart shows the rising percentage of job postings for Splunk roles.



# 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.

# Questions?





Countdown timer

15:00

(with alarm)

Break



# SIEM Certifications



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, receive a promotion, and attain 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 ES

## Splunk Enterprise Certified Architect

Focused on a Splunk administrator's role supporting advanced troubleshooting, configurations, and deployments in Splunk ES

## Splunk Enterprise Security Certified Admin

Focused on a Splunk administrator's role to support installation, advanced troubleshooting, configurations, and deployments in Splunk ES

# Splunk Certifications

Like for many certifications in the InfoSec field, training for Splunk certifications is expensive.

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

The screenshot shows a web browser displaying the Splunk Training & Certification page at [splunk.com/en\\_us/training.html?sort>Newest&filters=filterGroup1FreeCourses](https://splunk.com/en_us/training.html?sort>Newest&filters=filterGroup1FreeCourses). The page features a large banner with the text "Splunk Training + Certification". Below the banner, a yellow bar encourages users to check out new, single-subject courses. A search bar and a "Learn More" button are also visible. The main content area includes a "QUICK LINKS" section with links to My Training Profile, Splunk Education Student Handbook, Splunk Certification Handbook, FAQ, Authorized Learning Partners, Videos, and Basic Subscription Datasheet. On the left, a sidebar titled "Filter all" allows users to refine their search by Content Type (Courses, Free Courses, Certification Exams), Certification, Role, Product, and Suite. Three course cards are displayed: "Splunk User Behavior Analytics" (Free Course), "IT Essentials Learn - Walkthrough" (Course), and "Free Splunk Fundamentals 1" (Free Course). Each card provides a brief description and a "Learn More" link.



# Activity: Splunk Certifications

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

Suggested Time:

---

60 Minutes

# Activity: Splunk Certifications

---

Resources for taking the Core Certified User certification exam:



**Splunk:** [Core Certified User certification](#)



**Splunk:** [Journey to getting certified \(video\)](#)



**Splunk:** [Exam registration tutorial](#)



**Pearson VUE:** [Exam registration](#)

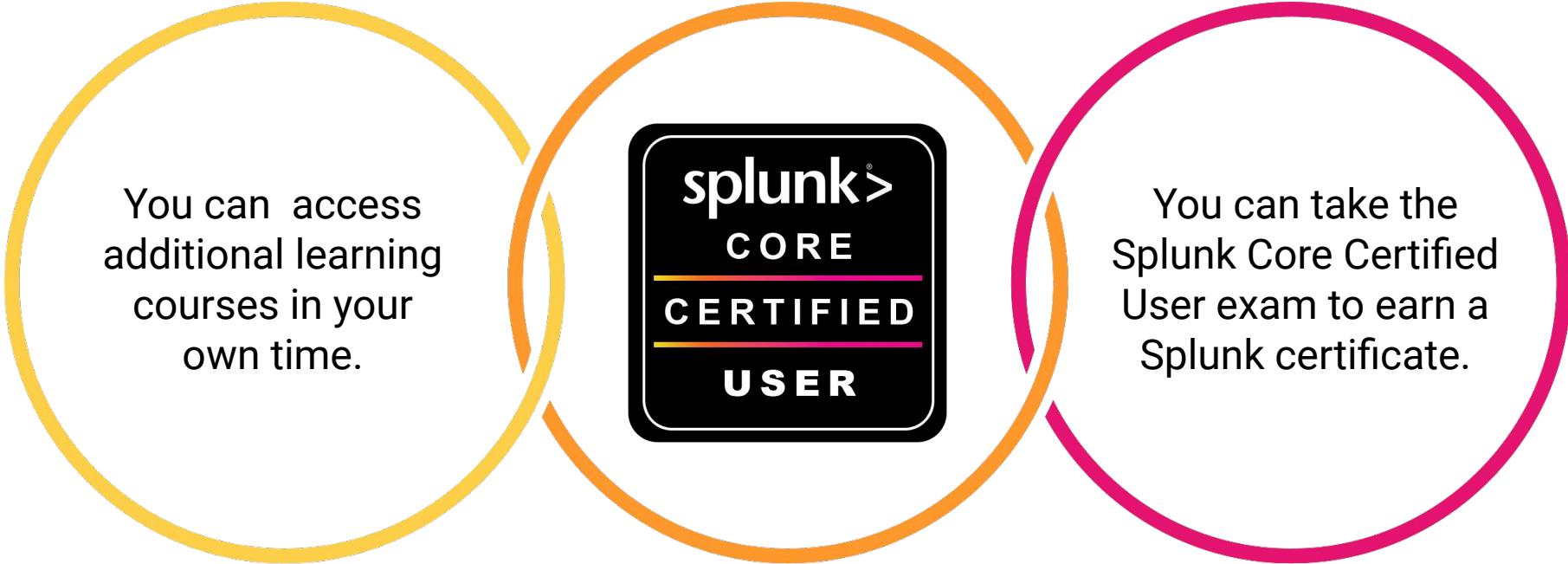


**Splunk:** [Certification study guide](#)

# Splunk Certifications

---

If you are interested in continuing your education towards a **Splunk Core Certified User** certification:



You can access additional learning courses in your own time.



You can take the Splunk Core Certified User exam to earn a Splunk certificate.

# Questions?



# Next Week

---

Next week, we will move on to the Forensics module

# Project Weeks

---

You will complete two more projects in this course:

01

Defensive Security Project

- This project will occur at the end of the Defensive Security module and incorporate everything you learn in this module.
- We'll cover the details next week.

02

Final Project: BootCon

- This project will occur in the last week of class.
- We'll get an overview now so that you can begin brainstorming and preparing.

# Cybersecurity Research Presentations

---

Cybersecurity professionals commonly present the following to their peers:



Security research they're conducting



Newly discovered security vulnerabilities of products, devices, software, or hardware



Demonstrations of the “hacks” that will exploit these vulnerabilities



Mitigations to protect against these vulnerabilities



- These presentations often occur at security conferences, trade shows, and other industry events.
- Cybersecurity professionals commonly attend these events to remain up to date with new technological developments and techniques.

# BootCon Presentations

---

Similarly, you will have an opportunity to showcase your skills during bootCon.



On the last day of class, we will hold a cyber class conference called bootCon.



Each student will have an opportunity to showcase the skills they learned during the bootcamp with a presentation.



If students elect to present as a group, every group member must participate in the presentation.



Most cyber professionals present at conferences when they've found a new vulnerability. However, for bootCon presentations, it is acceptable and recommended that you recreate a finding that has already been discovered.



A bootCon presentation  
is **NOT** a research paper.

While research will be required, all presentations must be tangible and demonstrable.

**A demonstration can either be:**

- Conducted in person
- A prerecorded video that accompanies the presentation  
*(if a live demonstration isn't practical)*



# BootCon Presentations

---

Each bootCon presentation should fall into one of the following three categories:

01

02

03

## Category

Exploiting a vulnerability of an IOT device

Developing code or a program that can complete a cybersecurity task

Demonstrating how a cybersecurity tool that was not covered in class can accomplish a specific goal

## Example

Hacking your personal Blu-Ray player

Developing a Python script that can automate an Nmap scan

Using SET to design a social engineering campaign

# BootCon Rules and Requirements

# BootCon Rules and Requirements

---

You must submit a project summary to your instructor for approval.  
The summary should be submitted with a Slack message by **Week 22**.

**Your project summary should include:**

-  Topic and title of your presentation
-  End goal or vulnerability being exploited
-  List of devices and/or technologies that will be used to accomplish the goal
-  Summary of how the devices and technologies will be used to accomplish the goal

# BootCon Rules and Requirements

---



Under no circumstances may any aspect of your bootCon presentation be unethical or illegal.

You must:



Perform all hacks and tests in simulated environments



Complete any network connections in your home and/or controlled environment



Only perform IoT hacks on devices that you own

# BootCon Rules and Requirements

Presentations must have a goal whose achievement you can demonstrate.

For example:

## Goal:

Cracking WEP wireless traffic  
from your home router



## Demonstration:

How you captured and cracked  
your wireless traffic



You can either conduct your demonstration live or record it  
and present it while you walk through what took place.

# BootCon Rules and Requirements

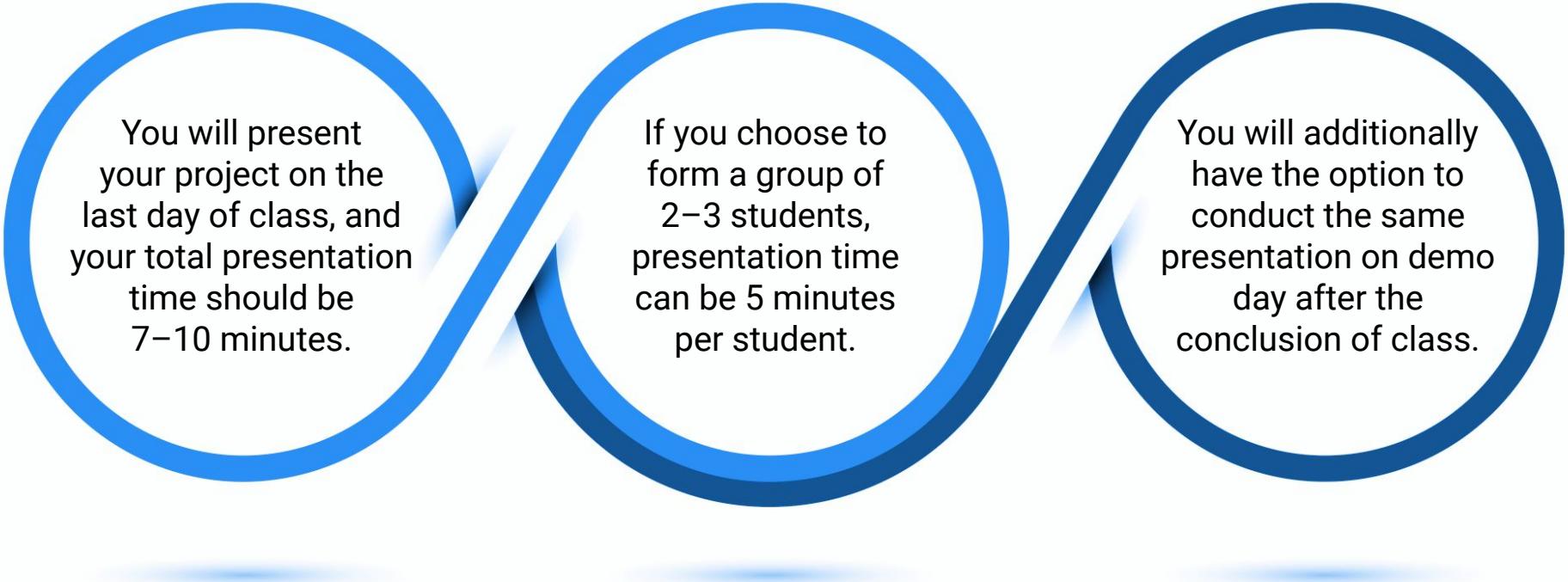
---

You must submit your presentation in the form of a Google Slides deck that, at a minimum, includes the following:

Cover slide	Presentation title and team member(s) presenting
Technical background	<ul style="list-style-type: none"><li>• Explanation of why you selected the topic you are presenting</li><li>• Networking, cryptographic, or security concepts applied</li><li>• Research steps taken</li></ul>
Demonstration preview	Preview of the steps that you'll take in the upcoming demonstration
Demonstration	A live or recorded demonstration is conducted here
Demonstration summary	Summary of the demonstration that you just conducted and any impact that it may have
Mitigation	Recommendations for mitigating against the attack that you just conducted. If your presentation isn't about an attack, this is not required.

# BootCon Rules and Requirements

---



You will present your project on the last day of class, and your total presentation time should be 7–10 minutes.

If you choose to form a group of 2–3 students, presentation time can be 5 minutes per student.

You will additionally have the option to conduct the same presentation on demo day after the conclusion of class.

# BootCon Presentations

---

If you need ideas for your presentation, refer to the [bootCon presentation guide](#), which contains:



Sample presentations



List of Kali Linux tools



List of IoT hacks



Videos of hacks presented at security conferences



**Remember:** Your project proposals are due in Week 22!

*The  
End*