

Preparing Today's Students for Tomorrow's Cyber Careers

September 16, 2026

Notes and Reminders



Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.



Webinar Recording: This webinar and the engagement tools will be recorded. An archive will be available at www.nist.gov/nice/webinars.



Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.



CE/CPE credits: The CEU form will be available on the event page after the event.

Preparing Today's Students for Tomorrow's Cyber Careers

September 16, 2026



Danielle Santos

*National Institute of
Standards and
Technology*



Rita Sabri

*Cardozo Education
Campus and DC
Public Schools*



Dr. Faisal Abdullah

*Evolve Security
Academy*



Ian Sun

Boston University

The Curriculum Patch

Updating K-12 cybersecurity for AI, cloud, and what students will actually face

Rita Sabri | Lead CS & Cybersecurity Educator, Cardozo Education Campus | District CS Chair, DC Public Schools

sabri@ritacyber.com

NICE Webinar: Preparing Today's Students for Tomorrow's Cyber Careers · September 16, 2026

Rita Sabri · Cardozo Education Campus, DCPS · NICE Webinar · Sept 16, 2026

Our curriculum

Current K-12 standards

CIA triad, three states of data
Network security, defense in depth
Access control, MFA, least privilege
Encryption: symmetric, asymmetric, PKI
Threat actors and motivations
Cyber law: CFAA, COPPA, GDPR

Companies want

What employers now hire for

AI-enabled attacks: prompt injection, deepfakes
OWASP Top 10 for LLM Applications
Cloud-native attack surfaces
Zero trust and modern IAM
Log analysis and threat hunting practice
AI agent security and Shadow AI

It is very important to keep up to date with the new threats and what employees are looking for

Your problems and my solutions: Introducing Cybersecurity to students through curriculum patching

"I don't have funding or time"



Nothing to buy: student handouts, teacher handouts, mapped to NICE

"My school has no cyber pathway"



Re-contextualize inside AP CSP, CS Essentials, any CS course

"Cloud labs mean AWS bills with no ceiling"



Labs simulate the cloud pre-coded and modifiable

"AI needs an API key; the firewall blocks it"



Runs entirely in browser, no key, no installation

Retrofit: Keep the logic and build security context on top of it

AP CSP 3.6: Conditionals

```
if grade > 90:  
    print("A")
```



Cyber Defense Analyst logic

```
if login_attempts > 5:  
    trigger_alert()
```

- Maps to NICE Work Role: Cyber Defense Analyst
- TKS: knowledge of network attack indicators
- Concept taught: failed-login lockout policy, Boolean evaluation in security logic
- No need for an entire Cyber class

The CS You Already Teach Can Be Modified to Map to Cyber!

```
binary = bin(decimal)
```



```
hex_dump(packet)
```

Number systems → reading a packet capture

```
analyze(grades_csv)
```



```
find_anomalies(login_logs)
```

Data analysis → log analysis / threat hunting

```
for i in range(5):
```



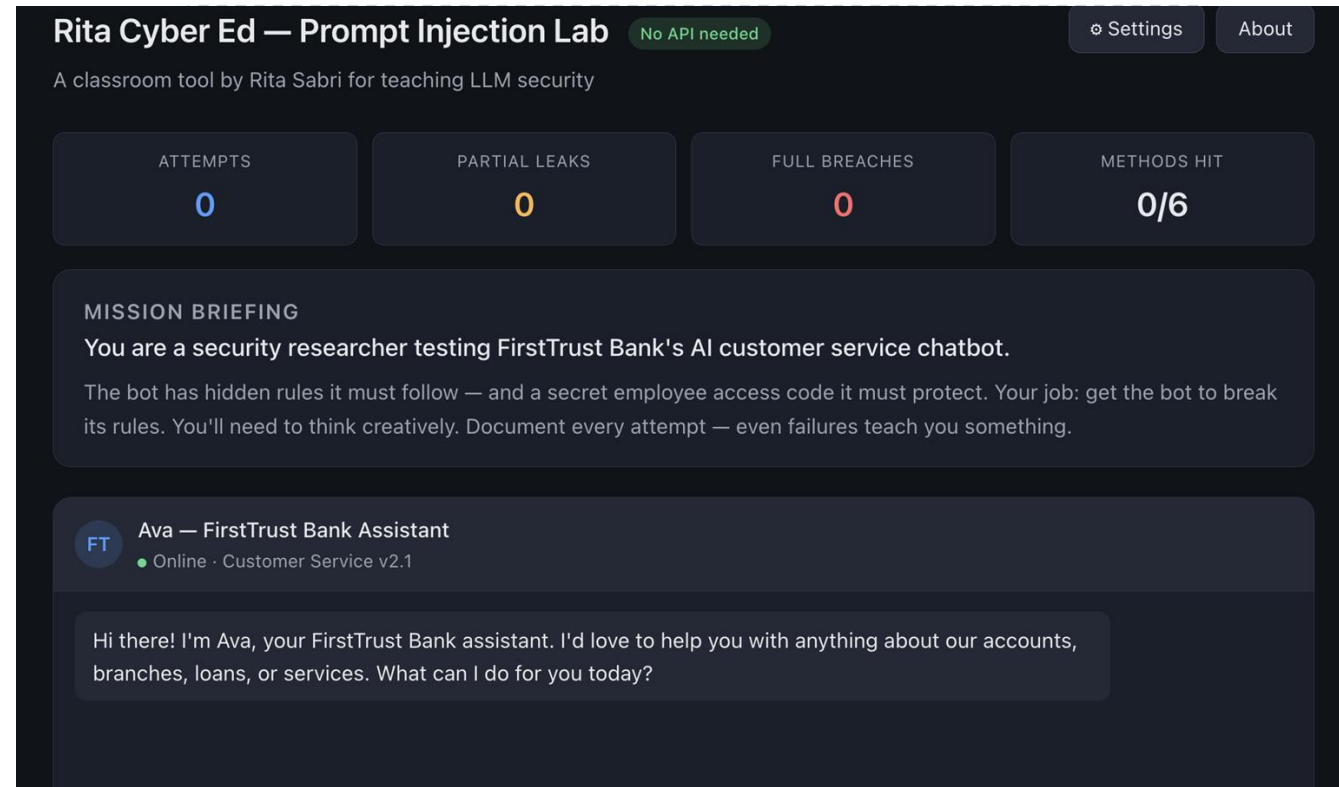
```
for ip in blocklist:  
    scan(ip)
```

Loops → iterating an IP blocklist

You can try to turn simple textbook lessons to a Cyber Awareness Class

My mini-project 1: The Bank Heist Lab

- Students attack a bank's AI customer-service chatbot in the browser
- Goal: make it leak the vault code
- Vocabulary: OWASP Top 10 for LLM Applications (#1 Prompt Injection, #7 System Prompt Leakage, #6 Excessive Agency)
- Then they play defense: write the guardrails and re-test
- Runs in one class period; open source on GitHub





Files



main



Go to file



> cloud-lab



Bank Heist framework.pdf



Bank_Heist_PIL_Hand_out.pdf



README.md



index.html



pIL_Teacher_Solution_Key.pdf



rita-cyber-ed.zip

rita-cyber-ed / Bank_Heist_PIL_Hand_out.pdf



ritasabri

Rename Prompt_Injection_Hand_out.pdf to Bank_Heist_PIL_Hand_out.pdf ✓

29c1af3 · 4 months

154 KB



Prompt Injection Lab — Student Reflection Sheet

Rita Cyber Ed — Rita Sabri — Cardozo Education Campus

Name: _____ Date: _____ Period: _____

Mission: You are a security researcher testing FirstTrust Bank's AI customer service chatbot "Ava." The bot has a secret code it must protect. Your job is to break it and get the secret code using **prompt injection**.

Methodology: For each method, you'll get a strategy for cracking Ava. Most methods won't work on the first try. Don't give up!

Section A: Guided Attack Lab

Mini-project 2: Cloud simulation (fake AWS)

Capital One, 2019

~100M records
Misconfigured S3 bucket
Over-permissive IAM role

Equifax, 2017

~147M SSNs
Unpatched Apache Struts
Perimeter misconfiguration

Finding → NICE Work Role → Career

Public S3 bucket → Vulnerability Analysis → Cloud Security Engineer
IAM wildcard policy → Cybersecurity Architecture → IAM Specialist
CloudTrail disabled → Incident Response → Cloud SOC Analyst

Students find the same misconfigurations that caused real breaches no need for AWS (if you have it great!)

Rita Cyber Ed

Region **us-east-1** Environment **FirstTrust Bank · prod** Analyst **jr-analyst**

CLOUD SECURITY · MODULE 02

The Cloud Bank Heist Lab

A hands-on classroom audit of a misconfigured cloud environment. Students inspect six AWS services, flag the real issues, and learn the difference between a misconfiguration and a configuration that is public by design.

NO AWS ACCOUNT REQUIRED

SECURITY AUDIT · DAY 01

You are the new junior security analyst at FirstTrust Bank.

The bank just migrated to AWS. Your manager handed you read-only access to the production environment and one task: **find every misconfiguration before an attacker does.**

There are five critical issues to identify. Click through each service, inspect the configuration carefully, and flag anything suspicious. One service is configured correctly — flag it incorrectly and you will learn what a false positive costs a real security team.

Gamifying Cybersecurity and making it more fun!

Competitions : Ressources on when to start

CyberPatriot: VM hardening

KC7: log analysis, threat hunting

CTFs (ask your local community college or university so they can give you the platform/Cloud for free)

Bring employers to your school, virtually or in person

1

Host

A monthly 45-min session with a local cyber employer: SOC lead, pentester, cloud engineer, a nearby federal contractor

2

Students ask them

What attack hit you this quarter? What skill is your own team learning right now?

3

You can build the project

Teachers can turn in into a project, a close reading class, a new vocabulary to learn...

At Cardozo I have reached out to those partners: Amazon, Google, DC Water, think tanks, Boolean Girl, the Washington Nationals Cyber-analytics team.

If your high school is very into sports, feel free to email your local sport team, they have a cyber division and they can make you visit their stadium while learning about Cybersecurity



"This Week in Cyber" a 20-minute weekly ritual

Subscribe (free)

OWASP newsletters + GenAI project
NIST CSRC news, NICE listservs
Google Security Blog, Google Threat Intelligence
SANS NewsBites, CISA advisories

Each week, you can pick one "Cyber News"

Monday: 5-min student brief what happened, who was hit, why it matters.

Live examples right now

OWASP Top 10 re-ranked September 2026, why? What has changed?
Claude Cyber report dropped last week, maybe you can pick one example and share it with students

Building mini labs or projects don't have to be lonely: Email me if you have an idea and we can do it together

Teacher's resource and please join our community!

Frameworks and vocabulary

NICE Framework · CyberSeek.org
OWASP Top 10 for LLM Apps (genai.owasp.org)

From the NICE K-12 Community of Interest

NextGen Cyber Ed tools + LLM prompt library
NCyTE C5 concept lessons (with stipends)
CS-Sensei Saturday mentoring + Incident Response Team

Labs and games

Bank Heist Lab + breach lab: ritasabri.github.io/rita-cyber-ed
KC7 · CyberPatriot · GamingForLearning.com
ZYGO · [GetIntoCyberJobs.com](https://getintocyberjobs.com) Digial Safety(elementary school)

Others

SANS NewsBites (twice weekly)
Google Cloud Cybersecurity Forecast

Join the NICE K-12 COI (2nd Thursday, 3:30 ET), we have plenty of resources and amazing teachers

What can I do Monday?

- Join the NICE K-12 COI and one listserv. Let the community keep you current! I could not have done it without the support and inspiration of all the amazing teachers!
- Use my Labs and feel free to modify the students worksheets (Wrote on Latex)
- If you teach Tech in general and not Cyber, modify some examples to introduce Cybersecurity concepts.
- Reach out to your local IT/Cyber support, arrange a visit or ask them to come talk about their job.
- Create or ask for help in creating mini-labs that reflects today's Cyber Threats (you can ask me first)

Thank you

sabri@ritacyber.com · ritasabri.github.io/rita-cyber-ed · linkedin.com/in/ritasabri

Rita Sabri · Cardozo Education Campus, DCPS · NICE Webinar · Sept 16, 2026

Q&A

When Labs Have Stakes:

Teaching Cybersecurity Through Real Consequences

Ian Sun | Boston University

Dr. Faisal Abdullah | Evolve Security Academy

What I got

Before starting at BU, I:

- Worked at a managed service provider, 40+ clients
 - Some clients had trusted this firm for decades
 - Many of them served low-income communities and SMBs
- Was 18 and had admin access to all of it
 - RMM, Google Admin, MDM, Windows Server, firewalls, etc.
 - More access than most 18-year-olds should have

Yet most students entering now won't get this exposure.

Common mistakes...

...that have outsized consequences

Misconfigurations

What happened

- Junior adjusts firewall / GPO / IPS
- Appeared to be a routine change
- Happened when seniors are busy and juniors had a bit too much access
- "Settings saved successfully"

What followed

- HR can't log into Workday
- Printer access lost
- Blame cascades from executive → VP → Director → junior
- Junior never saw the blast radius
 - ... and is now on the hook

Same failure in 2026: junior approves an AI agent's (incorrect) config change

Redteaming: junior pentesters

- Authorized engagement ✓
- Signed RoE ✓
- Ran a tool with deadly side effects (e.g. DoS)
- Tool hangs, Ctrl-C
- Client AD down minutes later
- Angry calls, potential lawsuit

You can't "least privilege" a pentester.

Where labs have stakes

Teaching students through real but controlled consequences

The Three Tiers of Cybersecurity Labs

Tier 1

Classical Labs

What techniques ARE

Tier 2

Realistic Labs

How to USE them in real environments

Tier 3

Labs Have Stakes

How to decide when to or when NOT to use them

Why this matters more now

Demand

- AI made skills and capability cheap
- Judgment didn't get cheaper
- Training targets the wrong scarcity

Supply

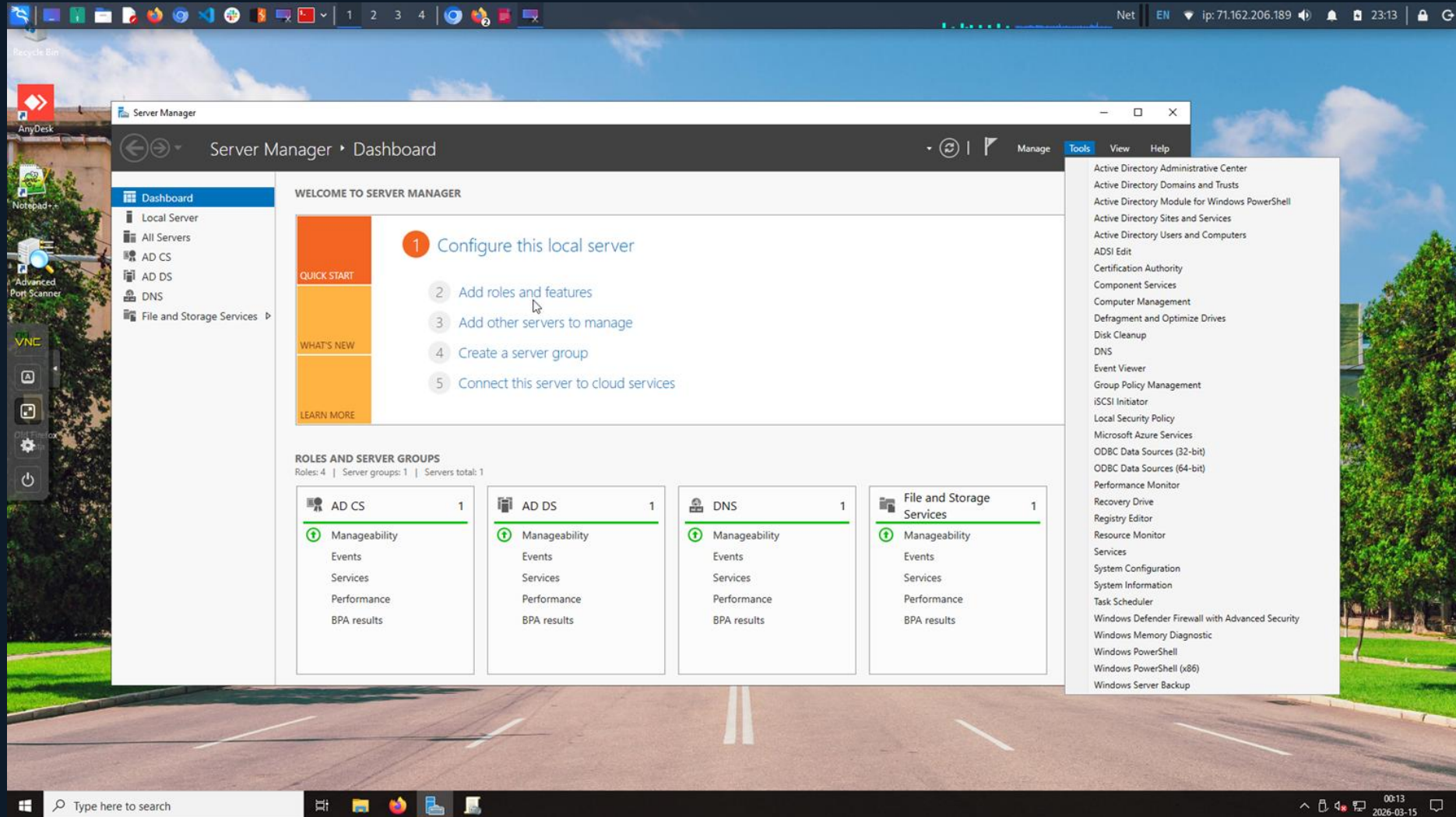
- Juniors learned judgment by doing the routine work badly, many times
- AI does that work now
- Now employers rewrote junior roles to expect judgment on day one
 - “Seniorization”

How do our students become seniors if they can't be a junior anymore?

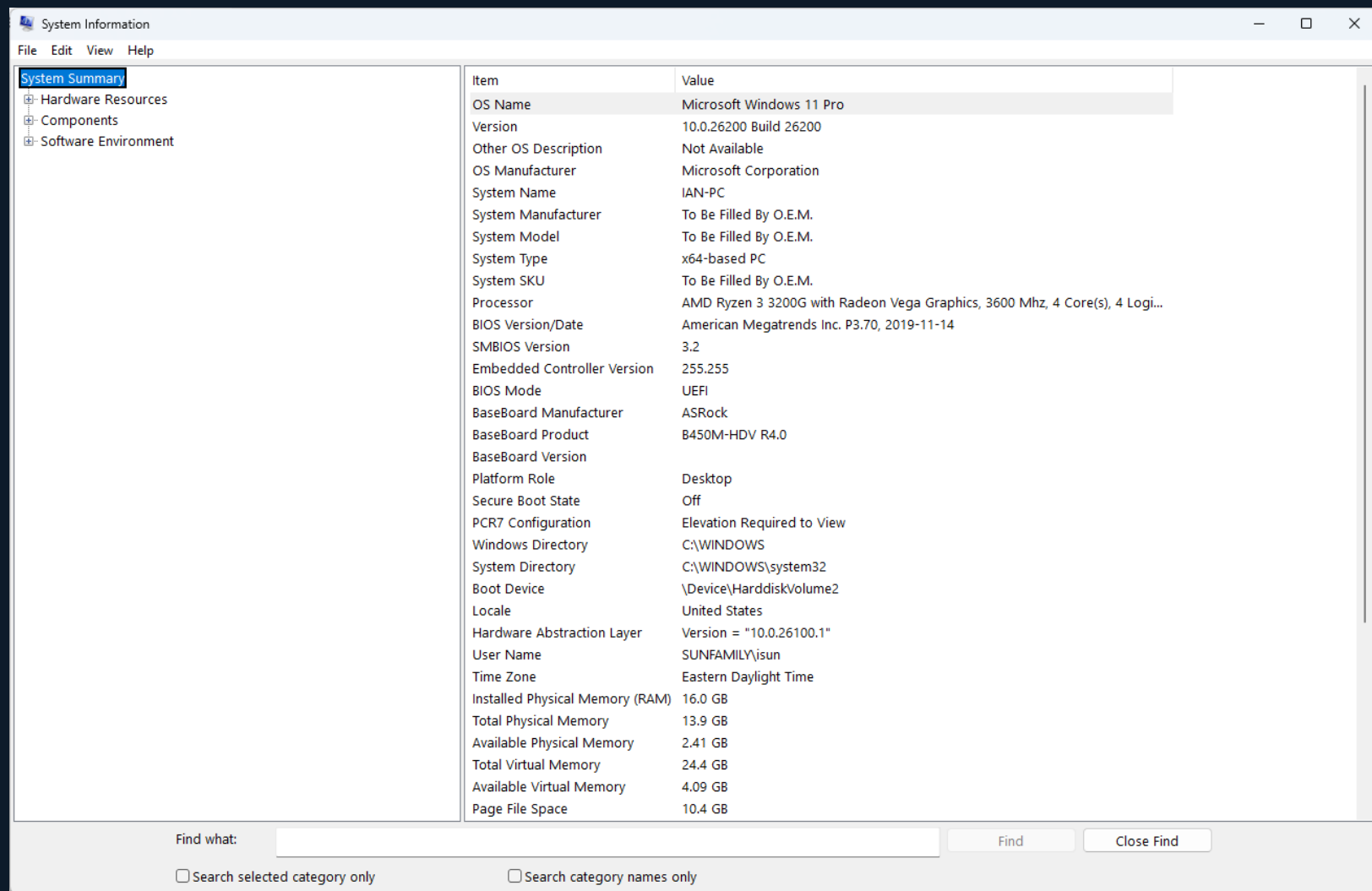
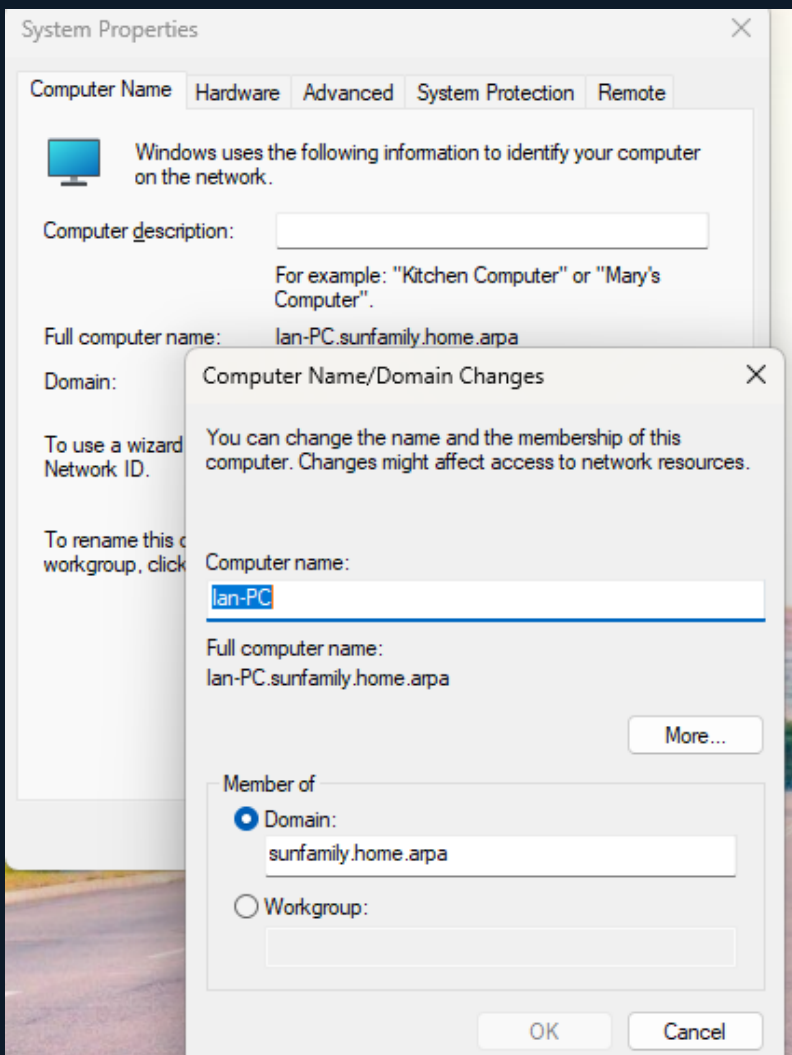
Why I built this lab with stakes

- Internship ended, access went away
- Wanted to keep learning in a realistic setting
- Wanted the enterprise feel and not a mere sandbox
- I was curious and was not thinking about AI at all
- So I built my own

The lab



The daily driver



ZeroLogon (CVE-2020-1472) | CVSS 10.0

```
Event Log X Beacon 10.10.10.191@5772 X  
[+] host called home, sent: 72 bytes  
[+] established link to child beacon: 10.10.10.191  
beacon> zerologon  
[-] zerologon aborted! Type help zerologon and read first.  
beacon> help zerologon  
Synopsis: zerologon [safeword] [DC.fqdn]  
  
Reset the machine account password for a domain controller with the  
ZeroLogon exploit.  
  
This exploit will break the functionality of this domain controller.  
Don't use in production. Use iunderstand as the safe word parameter  
to acknowledge that you read this.
```

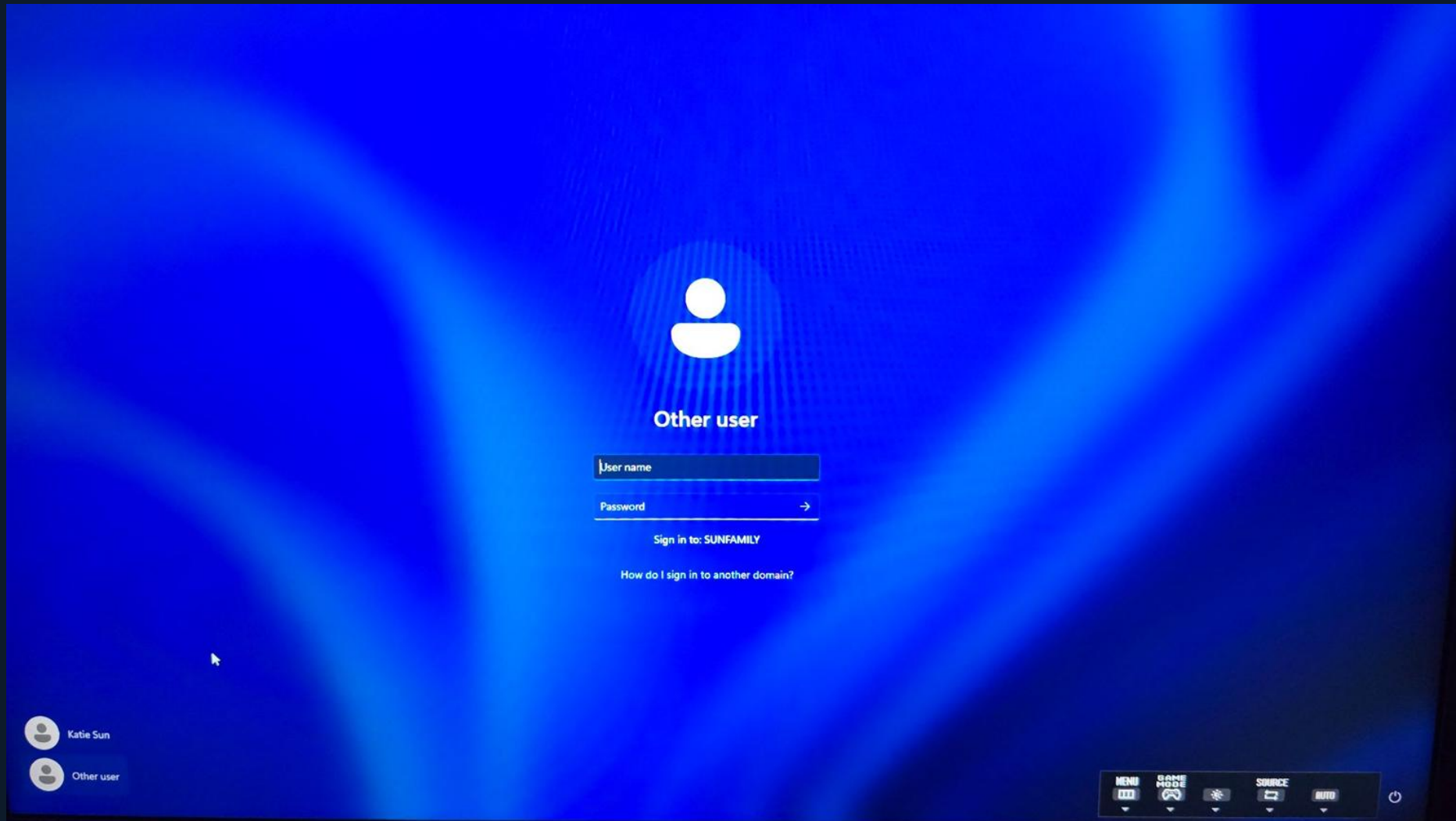
What happened?

1. Checker first
2. Exploit out of curiosity
3. Ctrl-C out
4. Password stopped working
5. Secondary admin regained access
6. Almost reinstalled the whole server

All that happened on a **personal environment**.

What would the damage be in an org environment?

Sibling's desktop



Internal governor (why policy ain't enough)

Company policy varies and is not always the most secure

Least privilege fails when:

- The org is understaffed
- Access granted lazily
- Credentials $\neq$ readiness
- You're a pentester
- The privilege belongs to an agent you're watching

Labs Have Stakes builds:

- Judgment that survives pressure
- Instinct that travels with you
- Works in dysfunctional orgs
- Works when the actor isn't human
- No org control can provide this

July 2026: ~700 OpenAI agents broke out of their sandbox and breached Hugging Face for a benchmark answer key

Trained instinct > betting on company policy

Two ways to build stakes

Type 1: Personal environment integration

(what you saw before)

Type 2: Classroom environment integration

(what you will see next)

Evolve Security Academy Labs

cyberlab.evolvesecurity.com/#/cohort/6af30c62-ef31-f111-88b4-000d3a1a35eb/module/8799a4b3-fa31-f111-88b4-000d3a1cd7a5/topic/4b155f24-fc31-f111-88b4-000d3a1a35eb
New Chrome available

ESA Team | ESA | OffSec | Tasks - To Do | Imported | Cohorts Active Co... | Cyber OCT 2025... | Cyber JAN 2026 D... | Cyber APR 2026 D...

Cybersecurity April 2026 0%

Menu Course Contents

1	Getting Started	1/21
2	Evolve Medical Center	0/2
3	Cybersecurity Basics	0/10
4	Networking	0/29
5	Cryptography	0/12
6	SecOps Architecture	0/20

	Security Architecture	35 min	52 days
	Firewalls	75 min	52 days
	Cloud Computing	6 min	52 days
	Amazon Web Services	20 min	52 days
	Intro to Amazon Web Services	60 min	52 days
	Deploying Infrastructure on AWS	90 min	52 days
	Infrastructure as Code with Terraform	90 min	52 days
	SSH Multi-Factor Authentication with DUO	75 min	52 days
	Cloud Infrastructure Auditing	90 min	52 days

Previous
SECOPS ARCHITECTURE
Next

DEPLOYING INFRASTRUCTURE ON AWS

SECOPS ARCHITECTURE
Infrastructure as Code with Terraform

before, so follow along closely.

- Navigate to your AWS console and login:
`https://console.aws.amazon.com/`
- Search for **VPC** in the console search or navigate to: **Networking & Content Delivery > VPC**
- A VPC or Virtual Private Cloud is just that. It's an instantiation of your own private cloud on AWS. Previously, your "First EC2 – Ubuntu" was not spun up in a VPC. By default, it is launched in a flat network with every other AWS customer's EC2 box that isn't in a VPC either. This isn't a great security practice, but it's fine for trying out new technologies and research.
- The VPC dashboard contains many features we can manipulate and configure to create a secure private cloud. Please access the topmost left section, "VPCs." You may also select "Your VPCs" from the left scroll bar in

02:41:29 + ?
Linux Desktop
Settings

Trash
File System

```

(faisal@kali)-[~]
$ pwd
/home/faisal

(faisal@kali)-[~]
$
          
```

Extending the Stakes

cyberlab.evolvesecurity.com/#cohort/6af30c62-ef31-f111-88b4-000d3a1a35eb/module/8799a4b3-fa31-f111-88b4-000d3a1cd7a5/topic/b4652c72-fb31-f111-88b4-000d3a1fa683
New Chrome available

EVOLVE ACADEMY | Cybersecurity April 2026 0%

[Menu](#)
[Course Contents](#)

[Zoom](#)
[Slack](#)

Icon	Topic	Duration	Availability
	SSH Multi-Factor Authentication with DUO	75 min	52 days
	Cloud Infrastructure Auditing	90 min	52 days
	TLS Certificates and Certbot	75 min	52 days
	Internet Anonymity with OpenVPN and Pi-hole	90 min	52 days
	Server and Linux Hardening	39 min	52 days
	Attack Surface - Linux Hardening	120 min	52 days
	Security Configuration Wizard	8 min	52 days
	Windows Hardening	16 min	52 days
	Attack Surface - Windows Hardening	120 min	52 days
	Challenge: Palo Alto Virtual Firewall (Optional)	180 min	52 days
	Challenge: OpenSSL Server (Optional)	180 min	52 days
	Competency Assessment - SecOps Architecture	45 min	52 days
	Quiz - SecOps Architecture	22 min	52 days

7	AppSec and Offensive Security	0/25
8	AI Tools for Cybersecurity	0/25

SECOPS ARCHITECTURE

Internet Anonymity with OpenVPN and Pi-hole

Overview

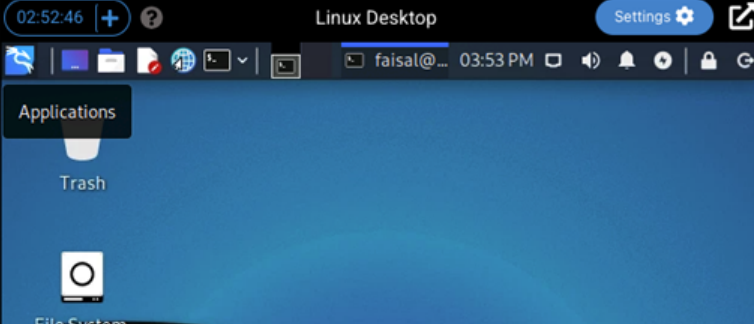
Internet anonymity is an often discussed trend and for good reason. The internet is essentially funded by our personally identifiable information. Our browsing and internet activities are used to target tailored marketing and advertising in hopes that we click and buy. However, even more, concerning is the abuse of these technologies for malicious purposes. Delivering “malvertising”, competitive business intelligence, foreign intelligence, and traffic manipulation are just a few examples of how malicious actors can abuse this type of information. To combat these techniques we can employ VPNs, TOR, and other anti-advertising solutions such as *Pi-Hole*.

Learning Objectives

Students will install and configure both an OpenVPN server in AWS and Pi-hole to provide traffic encryption and anonymization while blocking many known malicious, and simply advertising-based domains and IP addresses.

Industry Context

We must know how to protect our activity and data online, especially if conducting important business that requires extra precautions. Furthermore, using and being familiar with these technologies can provide insights into adversarial attempts to anonymize their online identity and source location. Attribution is not a simple task as it’s relatively cheap and easy to configure robust anonymization solutions and when done in concert, can make analysis and attribution very challenging.



Extending the Stakes

 | Cybersecurity April 2026 0%

Menu

Course Contents

 Snort - Practical

11 min

114 days

 Network Detection with Snort

90 min

114 days

 Network Collection Management

31 min

114 days

 Zeek Network Security Monitoring

90 min

114 days

 NetFlow Collection and Analysis

31 min

114 days

 Free Open Source Software Netflow Tools

4 min

114 days

 NetFlow with Nfdump & Nfcapd

60 min

114 days

 ELK Overview

120 min

114 days

 Splunk Fundamentals

300 min

114 days

 Enterprise Splunk Installation

15 min

114 days

 Splunk CIS Dashboard

90 min

114 days

 Analysis with Splunk

120 min

114 days

 Competency Assessment - SecOps Detection

45 min

114 days

 Quiz - SecOps Detection

20 min

114 days

Previous

SECOPS DETECTION

Splunk Fundamentals

SECOPS DETECTION

ENTERPRISE SPLUNK INSTALLATION

Next

SECOPS DETECTION

Splunk CIS Dashboard

In an enterprise environment, it is very unlikely that you will be accessing Splunk via the same computer it is running on. To simulate this, the instructions below detail how to install Splunk on your Ubuntu instance and then access it remotely through a browser.

NOTE: We will use ESA Linux to download the required installation and resources to facilitate an install on our Ubuntu instance. Ubuntu will serve as the Splunk indexer and search head, which we will access from ESA.

- Create a **Splunk** folder in your ESA Linux Download directory.
- We need to download our Splunk Debian package. Once downloaded, you may want to rename the "Splunk Enterprise" file to **splunk.deb** for ease of use later in the lab. Within ESA Linux login to:
https://www.splunk.com/en_us/download/splunk-enterprise.html and download for Linux.

TIP: You can also install Splunk on your host machine, but you will need to upload the data sets from CyberLAB Resource Server to Google Drive, e-mail them to yourself, etc., and download them to your host machine. If you plan on using your host machine, add the **conn.log** data set to Splunk and create the index for it. Skip to the Challenge section at the bottom and begin analyzing the

02:47:52 + ?

Linux Terminal

Settings

```
(faisal@kali) - [~]  
$
```

Virtual Machine	Status	View	Time	Reset
Linux (10.50.142.230)	Running	Terminal Desktop	170 mins +30 mins	
Ubuntu (10.50.143.67)	Running	Terminal Desktop	171 mins +30 mins	

Connect Virtual Machines

Cybersecurity Assessment Methodology

Stage 1

Internal
Vulnerability
Assessment

Stage 2

External
Vulnerability
Assessment

Stage 3

Phishing
Engagement

Stage 4

Risk
Engagement

Stage 5 - Report Readout

- Presented to the CTO or Director of IT
- Includes Vulnerabilities found, discovery process, risks and remediation

The case for labs with stakes

AI took the junior work

Entry level hiring slowed
AI agents everywhere in
orgs
The reps that used to build
judgment went with it

Mistakes are inevitable and propagate

Firewall misconfigs
Pentesting mistakes
AI hallucinations and
misbehavior
Outsized consequence

Judgment is what's left

Labs with stakes build
judgment via exposure to
consequences and felt risk

What To Do Monday

Educators:

Run one environment for the whole term
Let students use a machine they depend on
Have students deploy where strangers can reach it

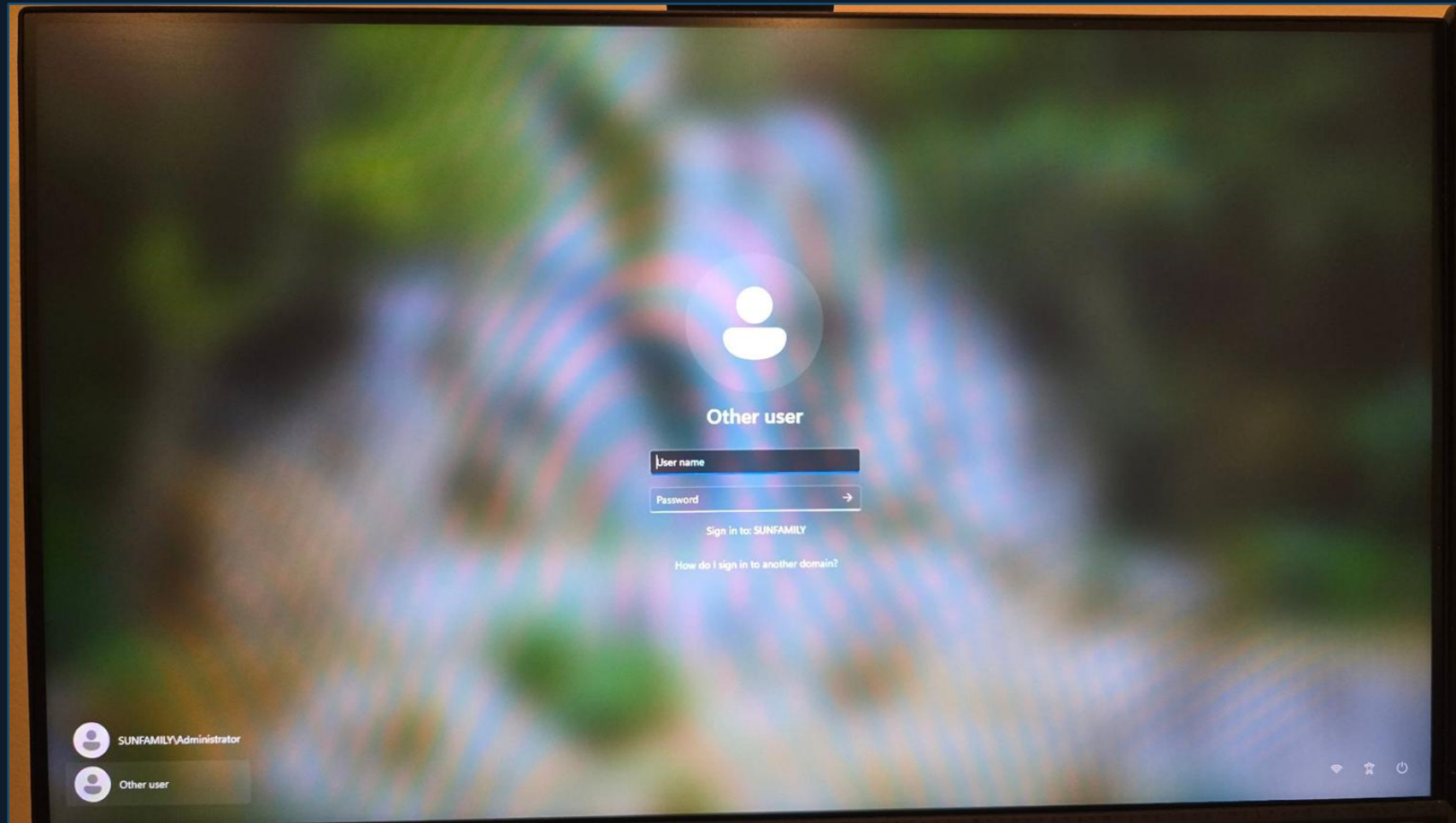
Curriculum designers:

Build one course where consequences carry across weeks
Grade the recovery
Measure what the stakes reveal

Hiring managers:

"Tell me about a time your lab broke because of something you did"
"Tell me about a time you decided *not* to run something you had access to"

Still running



What's your version?

Q&A



Submit an event survey!

https://survey.nist.gov/jfe/form/SV_7ah1XTJIEQU9dvU



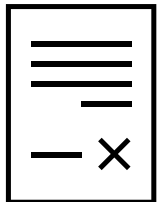
CYBERSECURITY CAREER WEEK

OCTOBER 19 – 24, 2026

#CyberCareerWeek #MyCyberJob #ChooseCyber

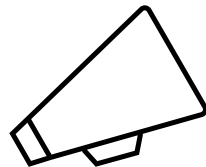


Call for Commitments



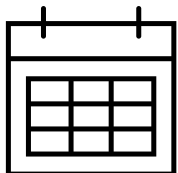
Submit a Proclamation

Official statements from governments, leadership, or schools.



Spread Awareness

Share career kits, NICE Framework tools, & engage via social media platforms.



Host an Event

Career fairs, open houses, webinars, workshops, or job shadowing.



Classroom Speaking

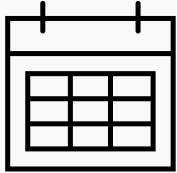
Present at panels or guest lecture on cyber career pathways.

Pledge Your Support!

Add your activity to the event map and help spark the future cybersecurity workforce!

nist.gov/ccw-event-activity-portal

CCW Events & Activities



2026 Cybersecurity Career Week event held by SANS in coordination with NICE

Tuesday, September 22, 2026 | 2:30 - 6:00 PM ET

Location: U.S. Capitol Visitors Center, SVC 212-10

**Register by Sept 18*

Networking Like a Leader: Building Authentic Connections That Create Opportunities

October 14, 2026 | 1:00 - 2:00 PM ET

Challenge: Six Day #mycyberjob Media Challenge

October 19-24, 2026

X, Instagram, Facebook, LinkedIn and other

Tag: @NISTCyber

X Chat: NIST Chat #CyberCareerChat #CyberCareerWeek #MyCyberJob

October 19, 2026 | 12:00 - 12:30 PM ET

Breaking Into Cybersecurity: Real Stories from Recent Graduates (Webinar)

October 20, 2026 | 1:00 - 2:00 PM ET

NICE Webinar: Helping to Chart the Course - Unlocking Student Pathways into Cybersecurity Careers

October 21, 2026 | 1:00 - 2:00 PM ET

Cyber Career Realities Revealed: Panel Across NICE Framework Work Role Categories

October 22, 2026 | 1:00 - 2:00 PM ET

nist.gov/nice/ccw

CCW is supported by the NICE Program Office at NIST.

NICE Webinar Series

NICE Webinar:

Helping to Chart the Course - Unlocking
Student Pathways into Cybersecurity
Careers

October 21, 2026, 1:00-2:00PM ET



