Teaching with Cybersecurity Playable Case Studies

Derek Hansen[1], Elizabeth Bosignore[2], Justin Giboney[1], Kira Gedris[3], Aatish Neupane[1], Andy Fellows[2], Skylar Hoffman[2], Trevor McClellan[1], Angelina Lopez[1]

1. Brigham Young University, 2. University of Maryland, 3. University of Virginia

Playable Case Study – Online Platform Components

(1) Time-Released Narrative: *The city of Bronze Falls is under attack by r0binh00d, a hacker group who has been attacking cities across the nation. Junior Associates in the Bronze Falls Professional Development Program will take on 1 of 4 professional roles and collaboratively perform a risk assessment, respond to a live cyber attack and identify who was behind the attack.*

Day 1	Day 2	Day 3	Day 4	Day 5
☑☑☑☑	☑☑☑	☑☑☑☑	☑☑☑☑	☑☑☑

(2) Immersive, Transmedia Interface

(3) Embedded Activities & Assessments

Individual Daily Tasks

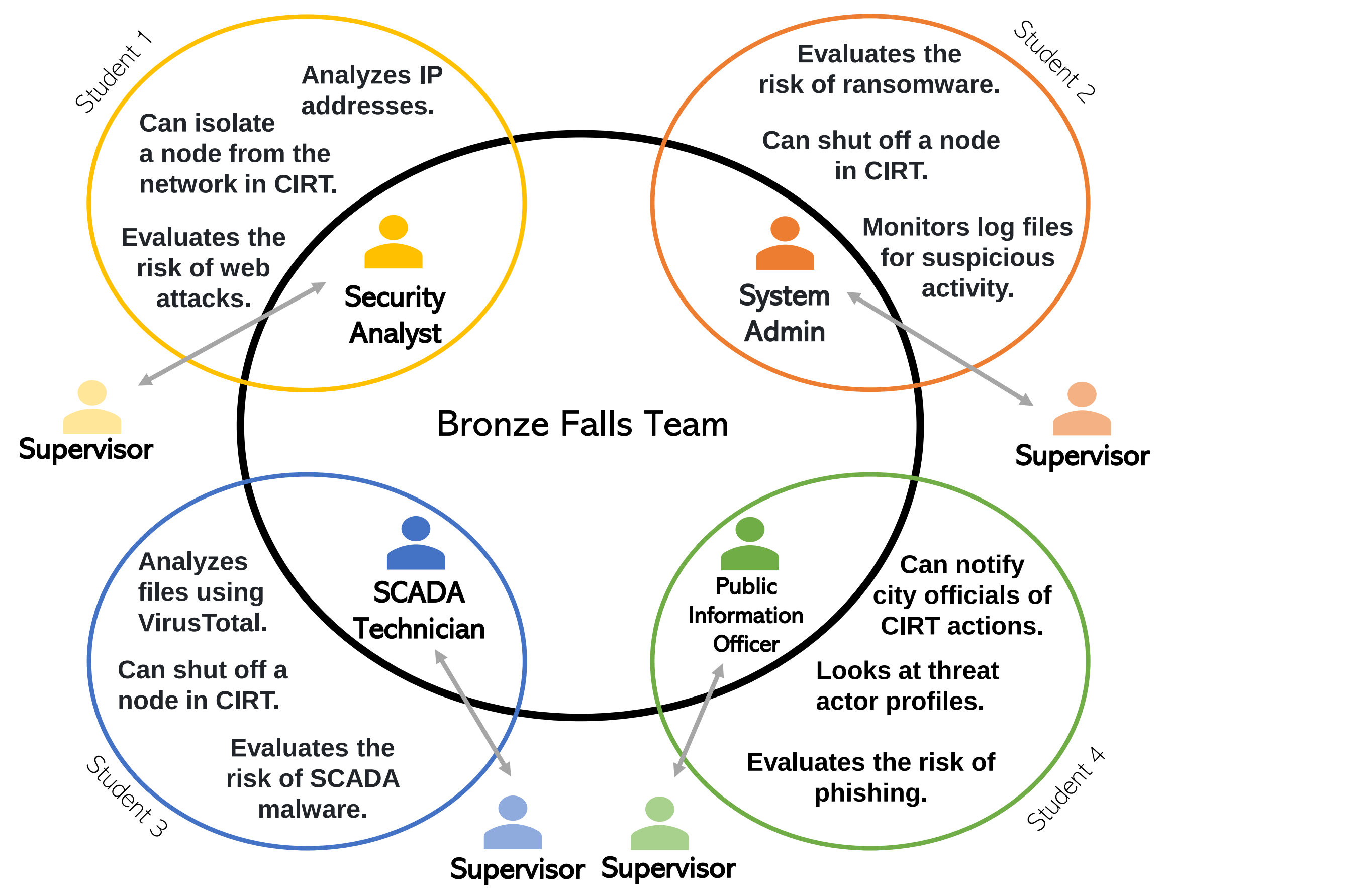
Group Daily Tasks

Game Mechanics

Formative Assessments

Final Report

(4) Role-Based Interactions


Student 1
Analyzes IP addresses.
Can isolate a node from the network in CIRT.
Evaluates the risk of web attacks.
Security Analyst
Supervisor
Student 2
Evaluates the risk of ransomware.
Can shut off a node in CIRT.
Monitors log files for suspicious activity.
System Admin
Supervisor
Bronze Falls Team
Student 3
Analyzes files using VirusTotal.
Can shut off a node in CIRT.
Evaluates the risk of SCADA malware.
SCADA Technician
Supervisor
Student 4
Can notify city officials of CIRT actions.
Looks at threat actor profiles.
Evaluates the risk of phishing.
Public Information Officer
Supervisor

In-Class Component

(5) Case Study Discussions

Class reflections, activities & discussions about the case

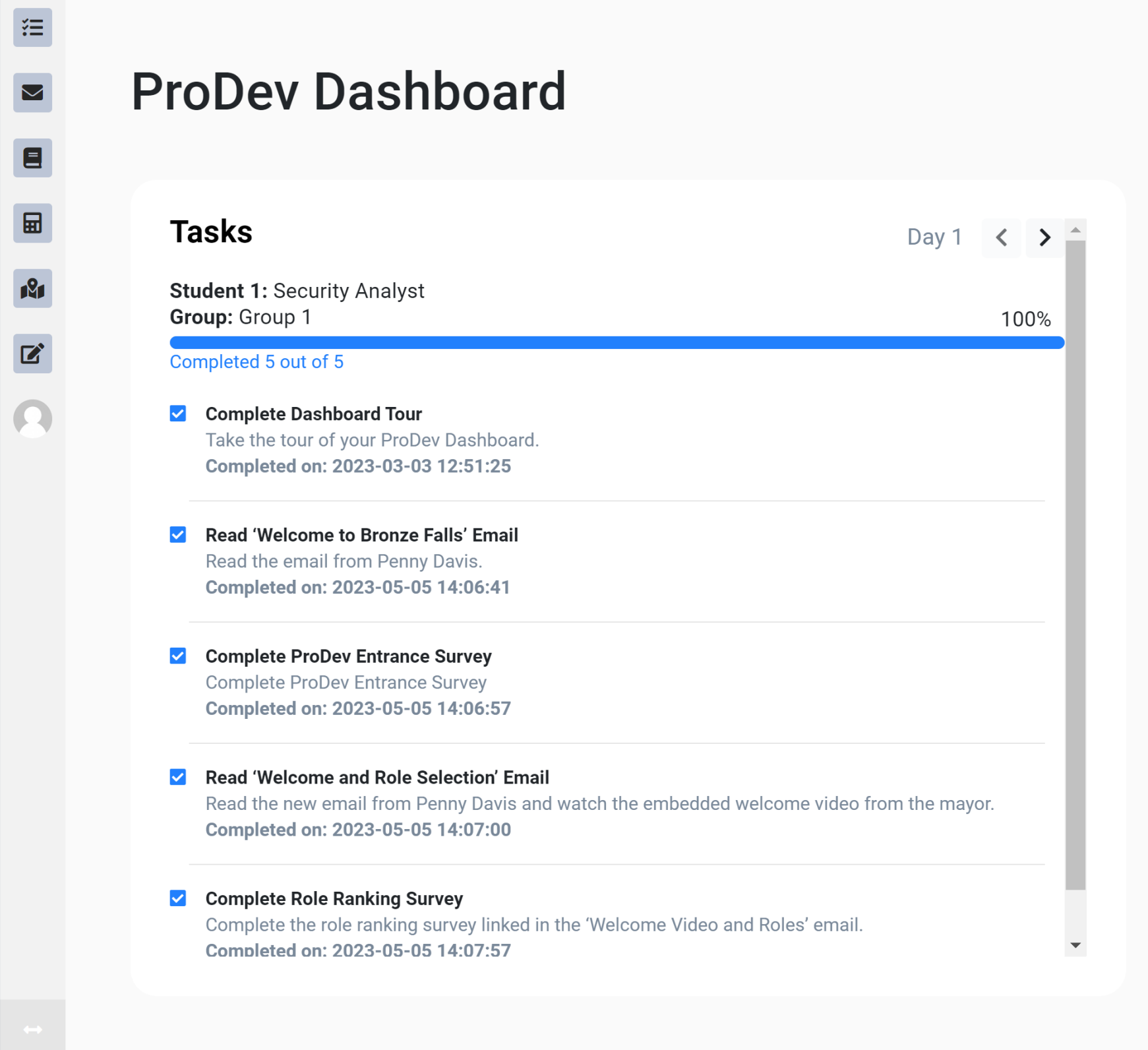
(6) Expansive Framing

Connect learning to people, places topics, & times outside the case

(7) Out-of-game Assessment

Complete self & peer assessments of student performance & outcomes

Day 1



ProDev Dashboard

Tasks

Day 1

Student 1: Security Analyst
Group: Group 1

100%

Completed 5 out of 5

☑ **Complete Dashboard Tour**
Take the tour of your ProDev Dashboard.
Completed on: 2023-03-03 12:51:25

☑ **Read 'Welcome to Bronze Falls' Email**
Read the email from Penny Davis.
Completed on: 2023-05-05 14:06:41

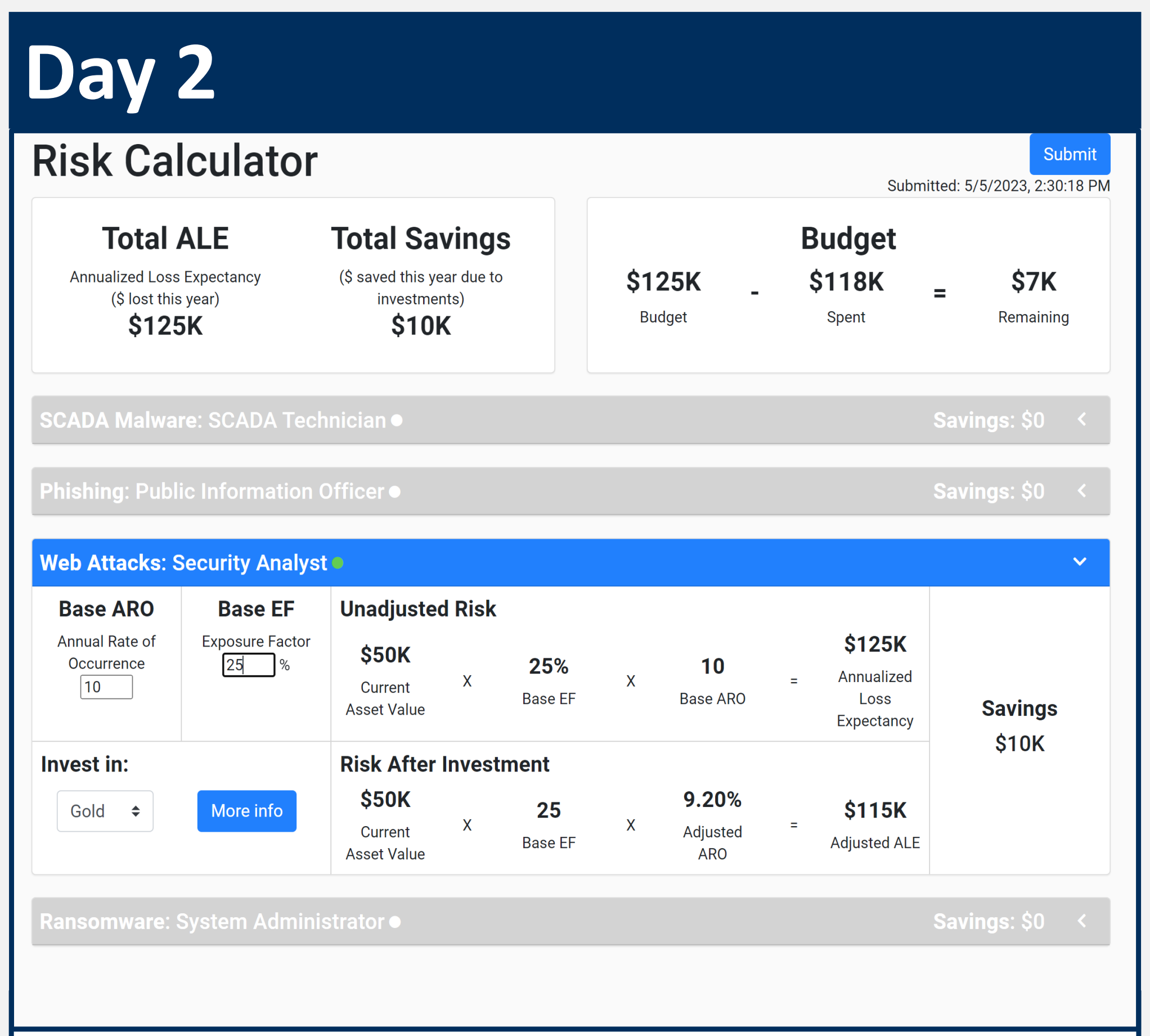
☑ **Complete ProDev Entrance Survey**
Complete ProDev Entrance Survey
Completed on: 2023-05-05 14:06:57

☑ **Read 'Welcome and Role Selection' Email**
Read the new email from Penny Davis and watch the embedded welcome video from the mayor.
Completed on: 2023-05-05 14:07:00

☑ **Complete Role Ranking Survey**
Complete the role ranking survey linked in the 'Welcome Video and Roles' email.
Completed on: 2023-05-05 14:07:57

Students familiarize themselves with the dashboard and PCS system. Actions include reading and writing emails, communicating with virtual team members via chat, and completing a role ranking survey to determine which role best fits the student.

Day 2



Risk Calculator

Submit

Submitted: 5/5/2023, 2:30:18 PM

Total ALE
Annualized Loss Expectancy ($ lost this year)
$125K

Total Savings
($ saved this year due to investments)
$10K

Budget

$125K	-	$118K	=	$7K
Budget		Spent		Remaining

SCADA Malware: SCADA Technician ● — Savings: $0

Phishing: Public Information Officer ● — Savings: $0

Web Attacks: Security Analyst ●

Base ARO
Annual Rate of Occurrence
10

Base EF
Exposure Factor
25 %

Unadjusted Risk

$50K	X	25%	X	10	=	$125K
Current Asset Value		Base EF		Base ARO		Annualized Loss Expectancy

Invest in: Gold — More info

Risk After Investment

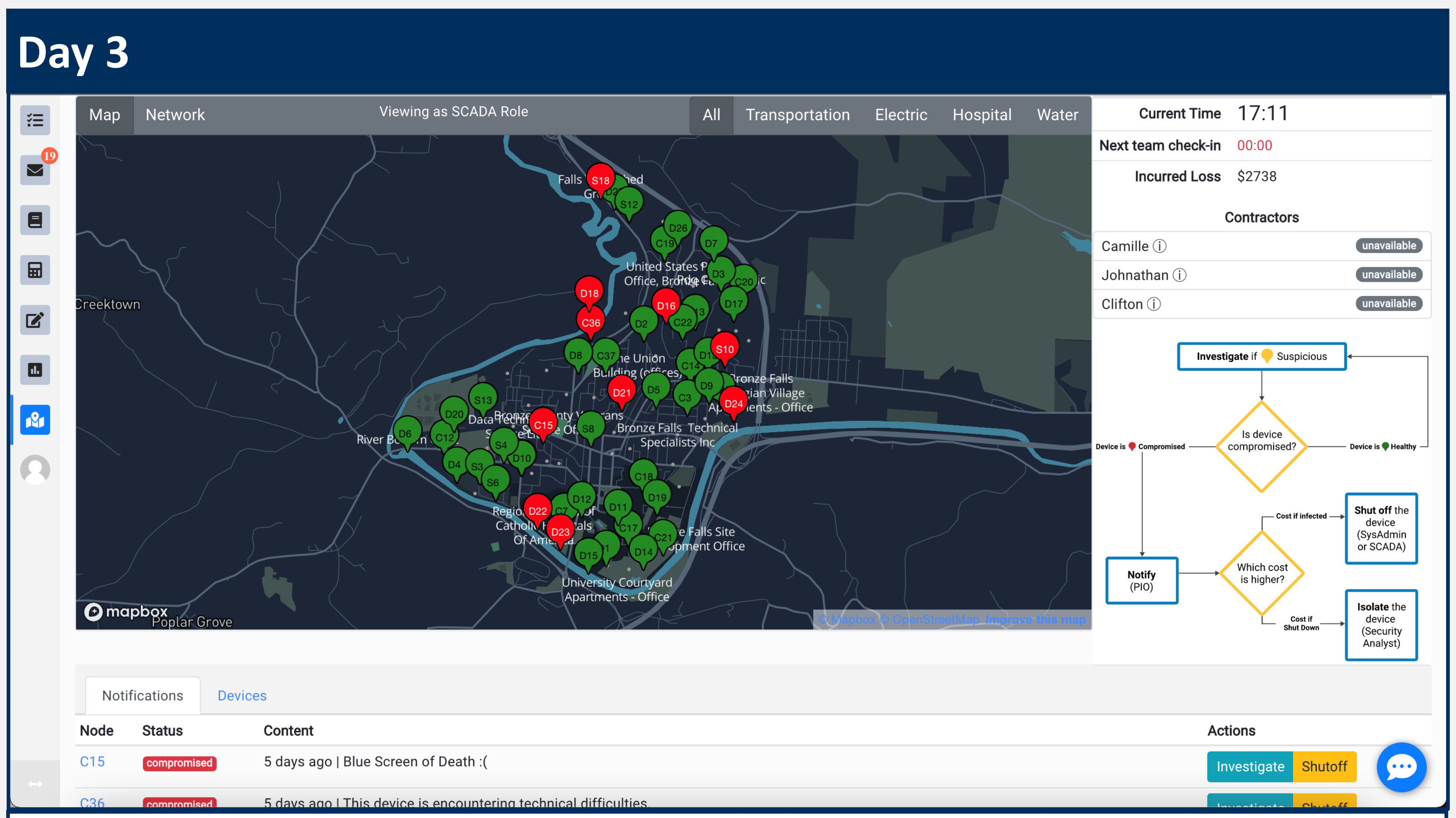
$50K	X	25	X	9.20%	=	$115K
Current Asset Value		Base EF		Adjusted ARO		Adjusted ALE

Savings
$10K

Ransomware: System Administrator ● — Savings: $0

Students perform a risk assessment based on data from the city and a nationwide Cyber City Breach Report. They use a risk calculator to determine what security controls they should invest in to reduce economic loss. They must negotiate with team members given their limited budget.

Day 3



Current Time	17:11
Next team check-in	00:00
Incurred Loss	$2738

Contractors

Camille ⓘ	unavailable
Johnathan ⓘ	unavailable
Clifton ⓘ	unavailable

Notifications — Devices

Node	Status	Content	Actions
C15	compromised	5 days ago | Blue Screen of Death :(	Investigate Shutoff
C36	compromised	5 days ago | This device is encountering technical difficulties	Investigate Shutoff

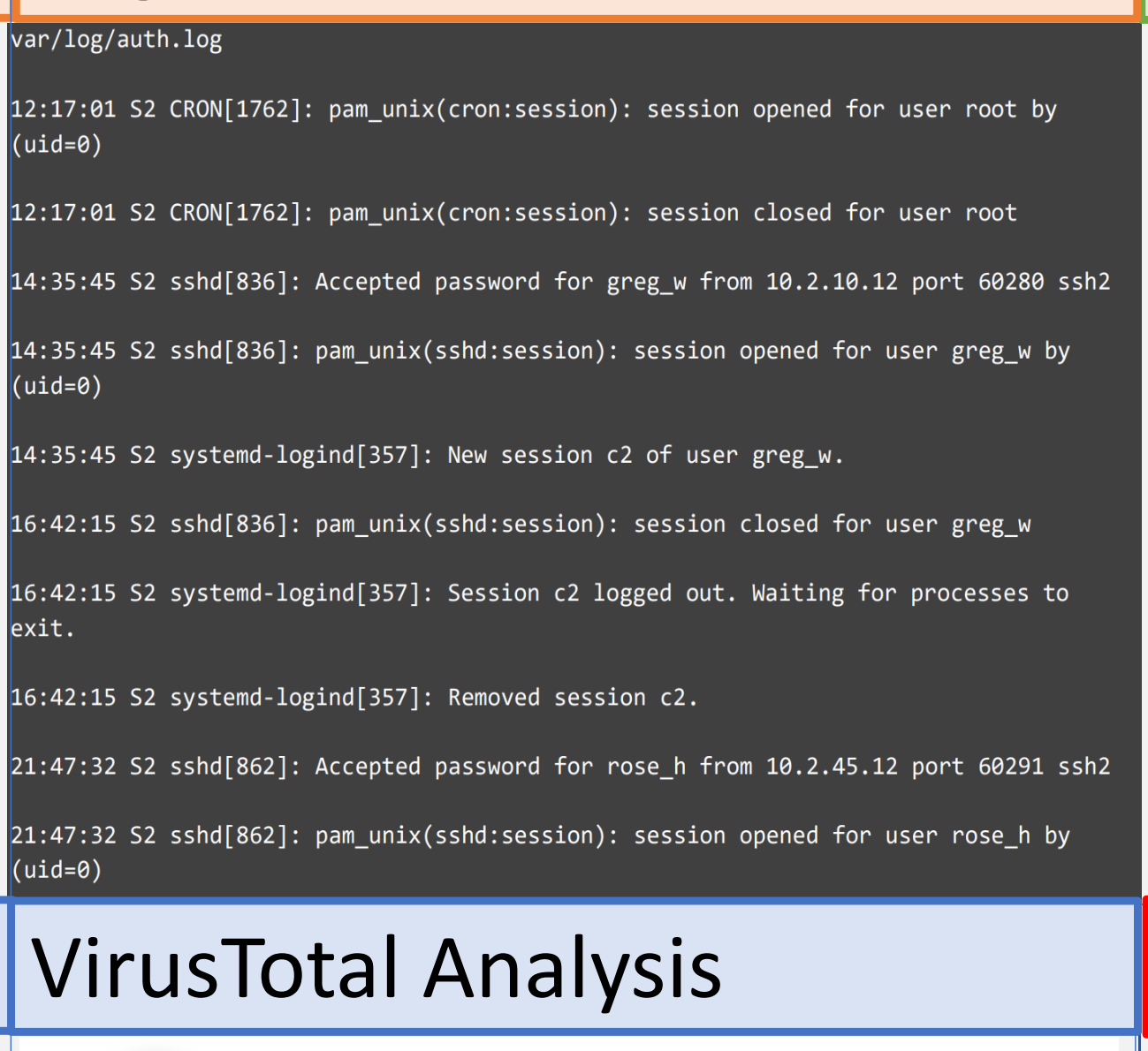
Students respond to a live attack on the city's infrastructure by using the Cyber Incident Response Tool (CIRT). Students must investigate potentially compromised computers and SCADA devices, isolate or shut down devices, and notify the city of updates. Students must collaborate to protect the city's infrastructure in real-time, since each student role views different information and completes unique actions.

Day 4

System Admin

"…
We've been combing through some of the computer and server log files on our system and we believe we've found the server from which the attacks spread. Sometimes an attacker will get in before the attack to scout out the network. Take a look at this log file from a week prior to the attack and see if the attackers were already accessing our systems.
…"

Log File

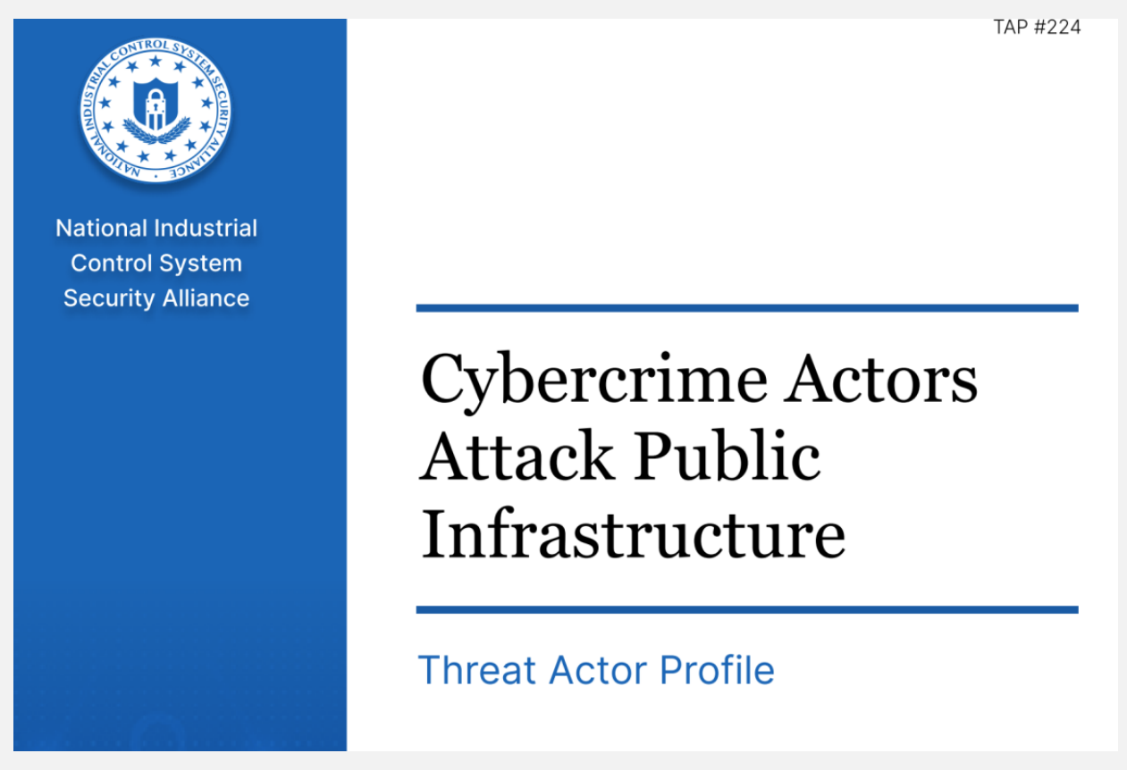


```
var/log/auth.log

12:17:01 S2 CRON[1762]: pam_unix(cron:session): session opened for user root by
(uid=0)

12:17:01 S2 CRON[1762]: pam_unix(cron:session): session closed for user root

14:35:45 S2 sshd[836]: Accepted password for greg_w from 10.2.10.12 port 60280 ssh2

14:35:45 S2 sshd[836]: pam_unix(sshd:session): session opened for user greg_w by
(uid=0)

14:35:45 S2 systemd-logind[357]: New session c2 of user greg_w.

16:42:15 S2 sshd[836]: pam_unix(sshd:session): session closed for user greg_w

16:42:15 S2 systemd-logind[357]: Session c2 logged out. Waiting for processes to
exit.

16:42:15 S2 systemd-logind[357]: Removed session c2.

21:47:32 S2 sshd[862]: Accepted password for rose_h from 10.2.45.12 port 60291 ssh2

21:47:32 S2 sshd[862]: pam_unix(sshd:session): session opened for user rose_h by
(uid=0)
```

Public Information Officer

"…
I found what appear to be good leads! I'm attaching two TAPs for you to read through that seem to have some tactical similarities to what we experienced when R0b1nh00d attacked. I've uploaded them to the document repository as well, in case you want to share them with your team.
TAP #224
TAP #312
…"

TAP Report



TAP #224

National Industrial Control System Security Alliance

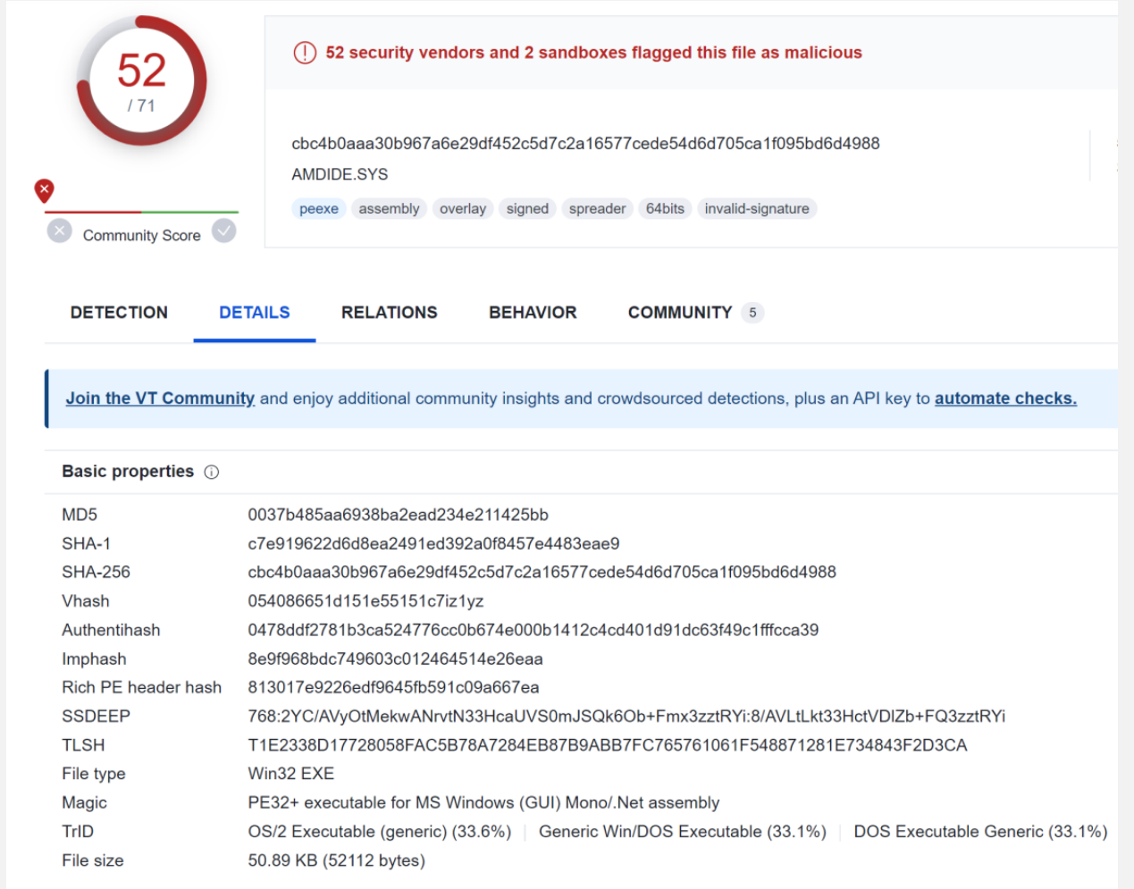
Cybercrime Actors Attack Public Infrastructure

Threat Actor Profile

SCADA Technician

"…
Once you find a match for the file hash, VirusTotal will show information that different anti-virus and malware detection applications have reported about the file. I highly recommend checking out the Community tab where users that submitted the file hashes talk about what the file is, where it may have come from, or what systems it can infect. If you're lucky, sometimes they include links to websites with more details. Share the malware file results that you find with your team and integrate the evidence into the attribution template that the CISO sent you.
…"

VirusTotal Analysis



52 / 71

Community Score

ⓘ 52 security vendors and 2 sandboxes flagged this file as malicious

cbc4b0aaa30b967a6e29df452c5d7c2a16577cede54d6d705ca1f095bd6d4988
AMDIDE.SYS

peexe · assembly · overlay · signed · spreader · 64bits · invalid-signature

DETECTION · DETAILS · RELATIONS · BEHAVIOR · COMMUNITY 5

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

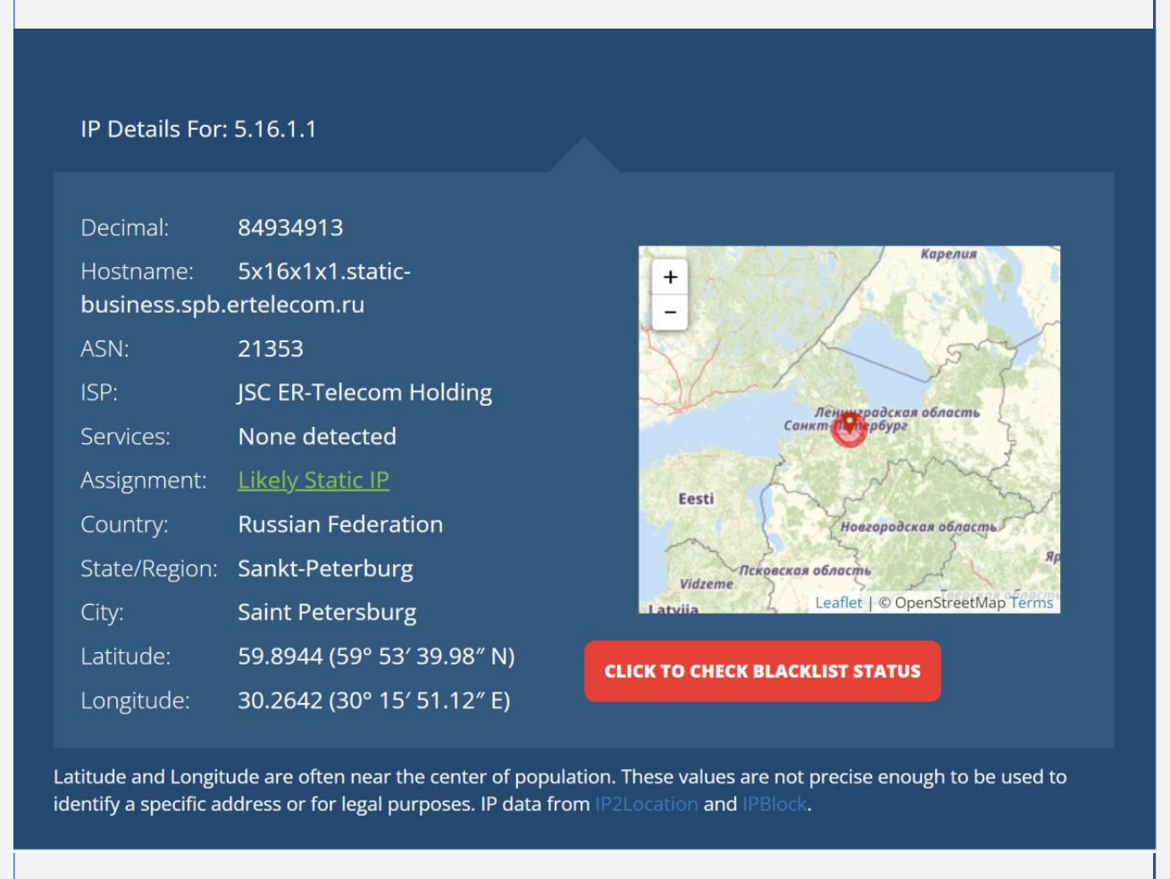
Basic properties ⓘ

MD5	0037b485aa6938ba2ead234e211425bb
SHA-1	c7e919622d6d8ea2491ed392a0f8457e4483eae9
SHA-256	cbc4b0aaa30b967a6e29df452c5d7c2a16577cede54d6d705ca1f095bd6d4988
Vhash	054086651d151e55151c7iz1yz
Authentihash	0478ddf2781b3ca524776cc0b674e000b1412c4cd401d91dc63f49c1fffcca39
Imphash	8e9f968bdc749603c012464514e26eaa
Rich PE header hash	813017e9226edf9645fb591c09a667ea
SSDEEP	768:2YC/AVyOtMekwANrvtN33HcaUVS0mJSQk6Ob+Fmx3zztRYi:8/AVLtLkt33HctVDlZb+FQ3zztRYi
TLSH	T1E2338D17728058FAC5B78A7284EB87B9ABB7FC765761061F548871281E734843F2D3CA
File type	Win32 EXE
Magic	PE32+ executable for MS Windows (GUI) Mono/.Net assembly
TrID	OS/2 Executable (generic) (33.6%) | Generic Win/DOS Executable (33.1%) | DOS Executable Generic (33.1%)
File size	50.89 KB (52112 bytes)

Security Analyst

"…
First -- It looks like several of the compromised devices have been trying to access source devices within different IP address ranges. Use https://whatismyipaddress.com/ip-lookup and see if you can uncover the locations these IP ranges are associated with. Your findings may give us a better idea what countries R0b1nh00d already has a foothold in.
…"

IP Address Info



IP Details For: 5.16.1.1

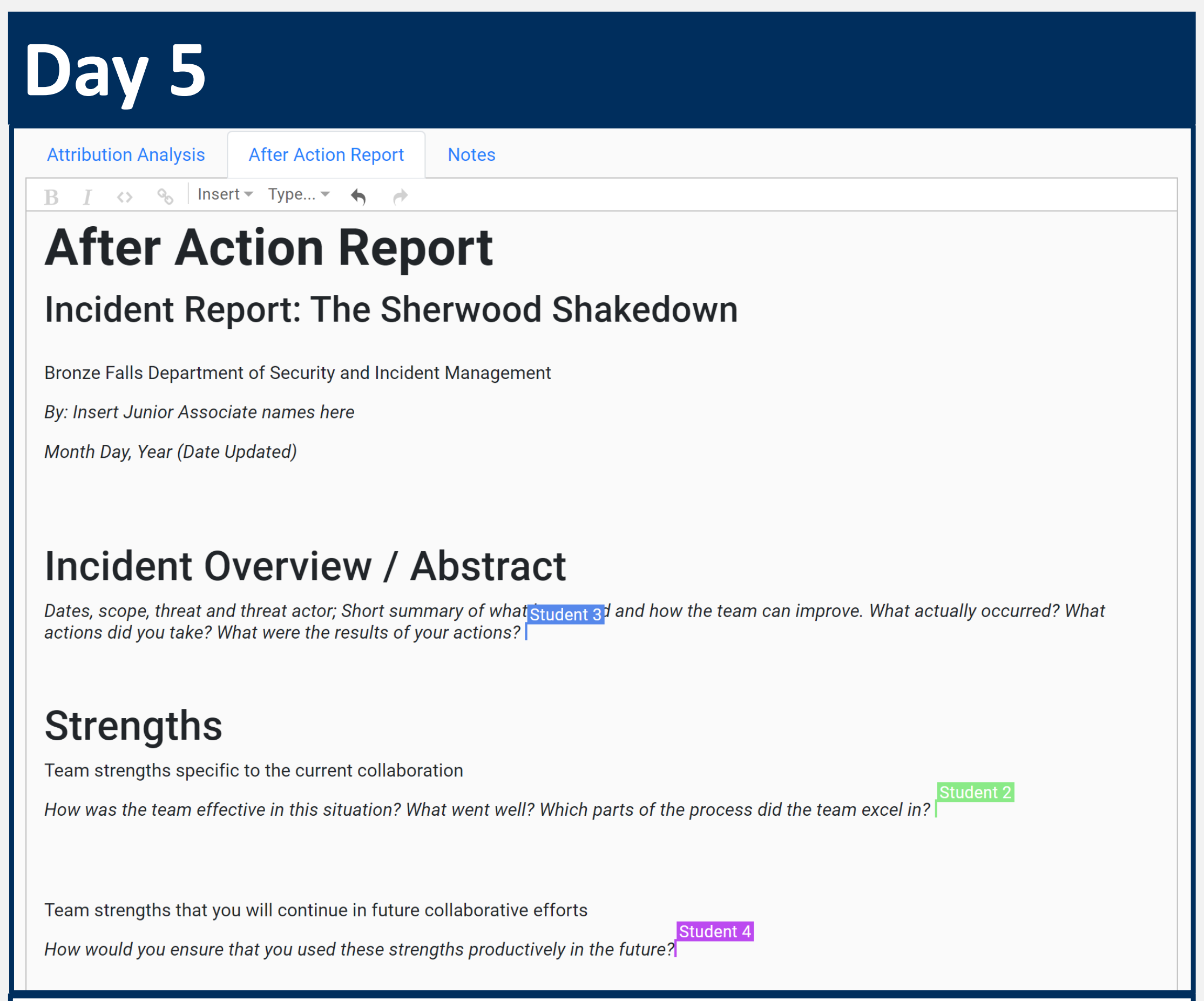
Decimal:	84934913
Hostname:	5x16x1x1.static-business.spb.ertelecom.ru
ASN:	21353
ISP:	JSC ER-Telecom Holding
Services:	None detected
Assignment:	Likely Static IP
Country:	Russian Federation
State/Region:	Sankt-Peterburg
City:	Saint Petersburg
Latitude:	59.8944 (59° 53′ 39.98″ N)
Longitude:	30.2642 (30° 15′ 51.12″ E)

CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address or for legal purposes. IP data from IP2Location and IPBlock.

Students analyze unique information tied to their role and write an Attribution report detailing the most likely Advanced Persistent Threat (APT) behind the attack. They also provide evidence about an insider threat.

Day 5



Attribution Analysis · After Action Report · Notes

B I Insert Type...

After Action Report

Incident Report: The Sherwood Shakedown

Bronze Falls Department of Security and Incident Management

By: Insert Junior Associate names here

Month Day, Year (Date Updated)

Incident Overview / Abstract

Dates, scope, threat and threat actor; Short summary of what Student 3 d and how the team can improve. What actually occurred? What actions did you take? What were the results of your actions?

Strengths

Team strengths specific to the current collaboration

How was the team effective in this situation? What went well? Which parts of the process did the team excel in? Student 2

Team strengths that you will continue in future collaborative efforts

How would you ensure that you used these strengths productively in the future? Student 4

Students use the collaborative editor to draft an after-action report for city leaders. They reflect on teamwork, collaboration, and lessons learned from the incident.

Research funded by National Science Foundation (NSF) Awards #1915563 and #1915620.

CAE IN CYBERSECURITY COMMUNITY