Student Security Operations Center: Tools, Workflows, and Real-World Response

Aiden West, Emanuel Reynoso, Ibrahima Balde, Nehemia Araia

CYSE 368

4/23/2026

Introduction - Tools and Workflow

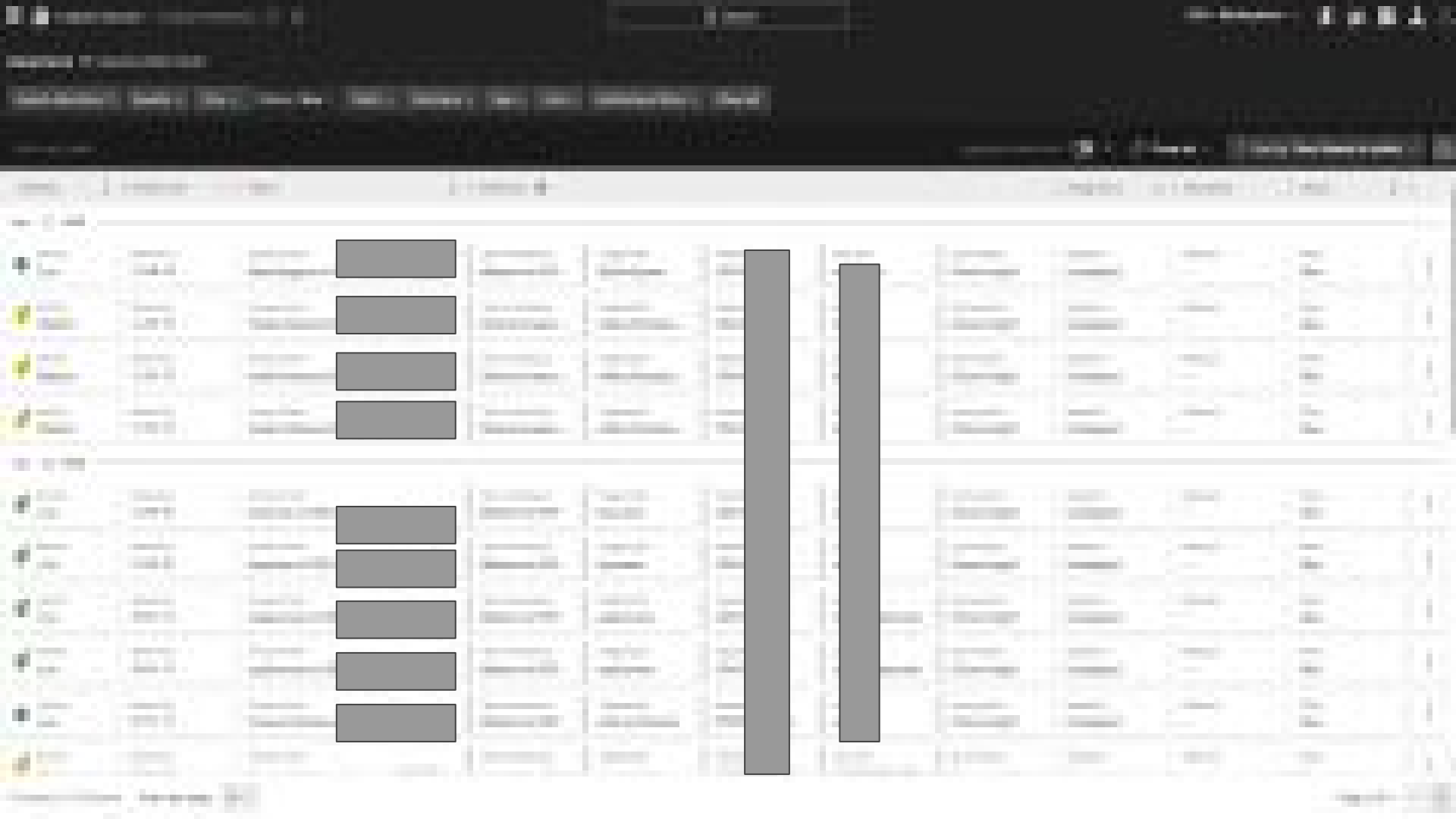
Crowdstrike

What is CrowdStrike?

- Cloud based cybersecurity platform
- Gives SOC analysts visibility into threats
- Uses AI analytics to detect known attack patterns

What is EDR?

- Technology that monitors endpoints (laptops, phones, cameras, etc)
- Detects suspicious or malicious activity in real time
- Allows SOC Analysts to investigate and respond to threats immediately



PagerDuty

Phishing and Incident Response

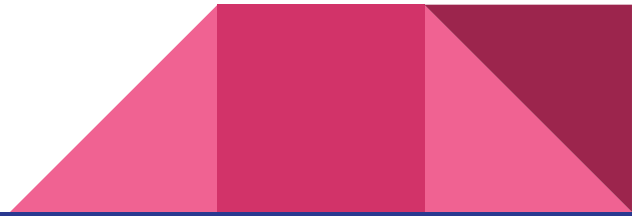
- Coordinating Alerts
- Documenting Incidents
- MTTA & MTTR Analytics

1: Email reported -> Alert generated

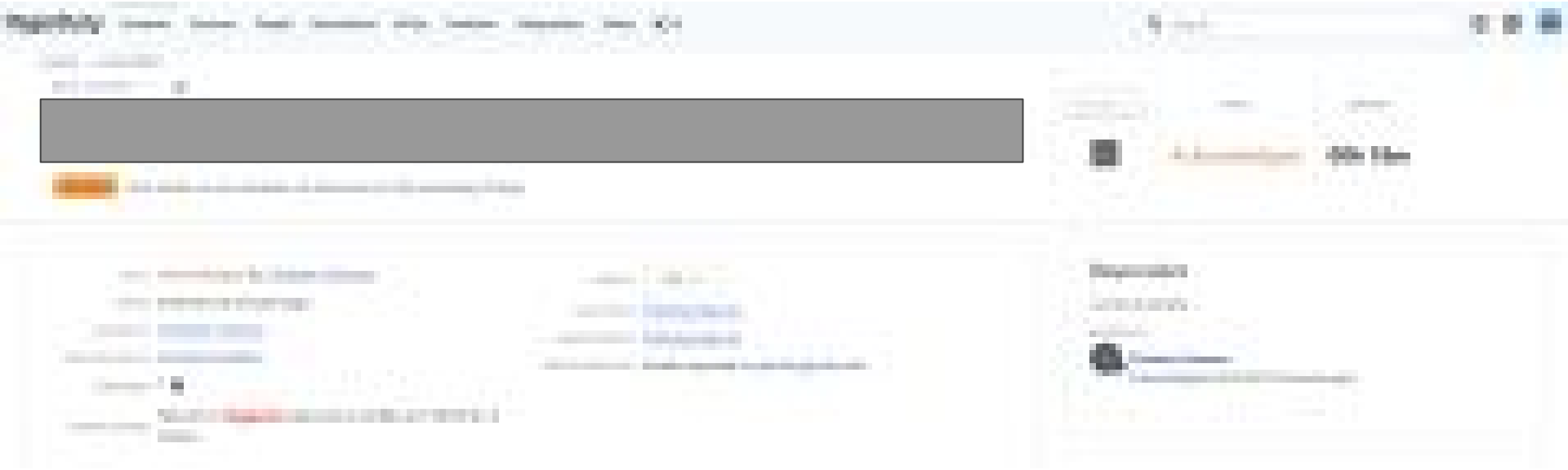
2: Review email

3: Check for similar reports

4: Document and conclude



PD Interface



CSU Account Alert: Immediate Action Required

[redacted]

[illegible]

⚠️ Your Account May Be Affected – Check Eligibility Now

[redacted]

Hi there,

We noticed you may be eligible for exclusive student discounts through our partner network. Some offers are time-sensitive and may expire soon.

To see what you qualify for and access your available offers, click below:

👉 Check Your Eligibility & Unlock Discounts

Popular offers include discounts on:

- Tech & laptops
- Clothing & shoes
- Food delivery services
- Streaming platforms

You're receiving this email because you signed up for student offers through a verified partner.

If you no longer wish to receive these emails, you can unsubscribe at any time below.

Best,
The Student Deals Team
Unsubscribe

[illegible]

[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

[illegible]

IBM Qradar

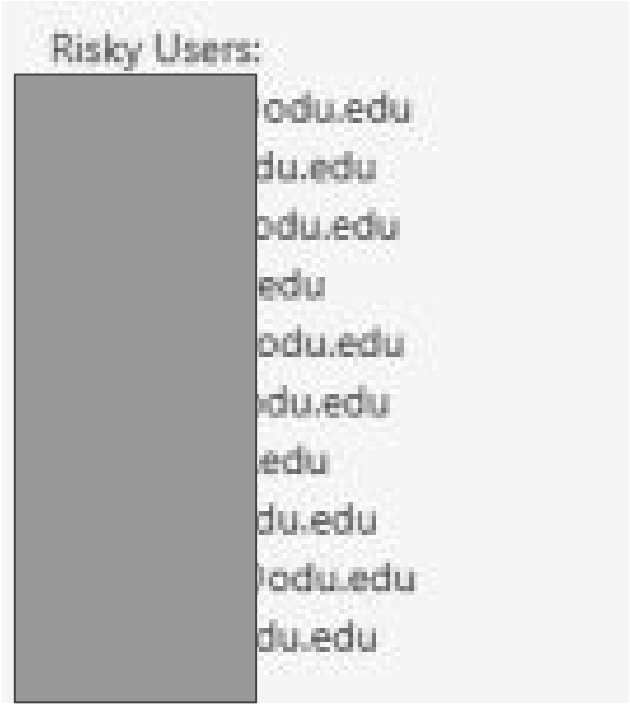
Why is it important?

- Halts malicious activity
- Prevents data breaches
- Enforces security

User Investigation Protocol

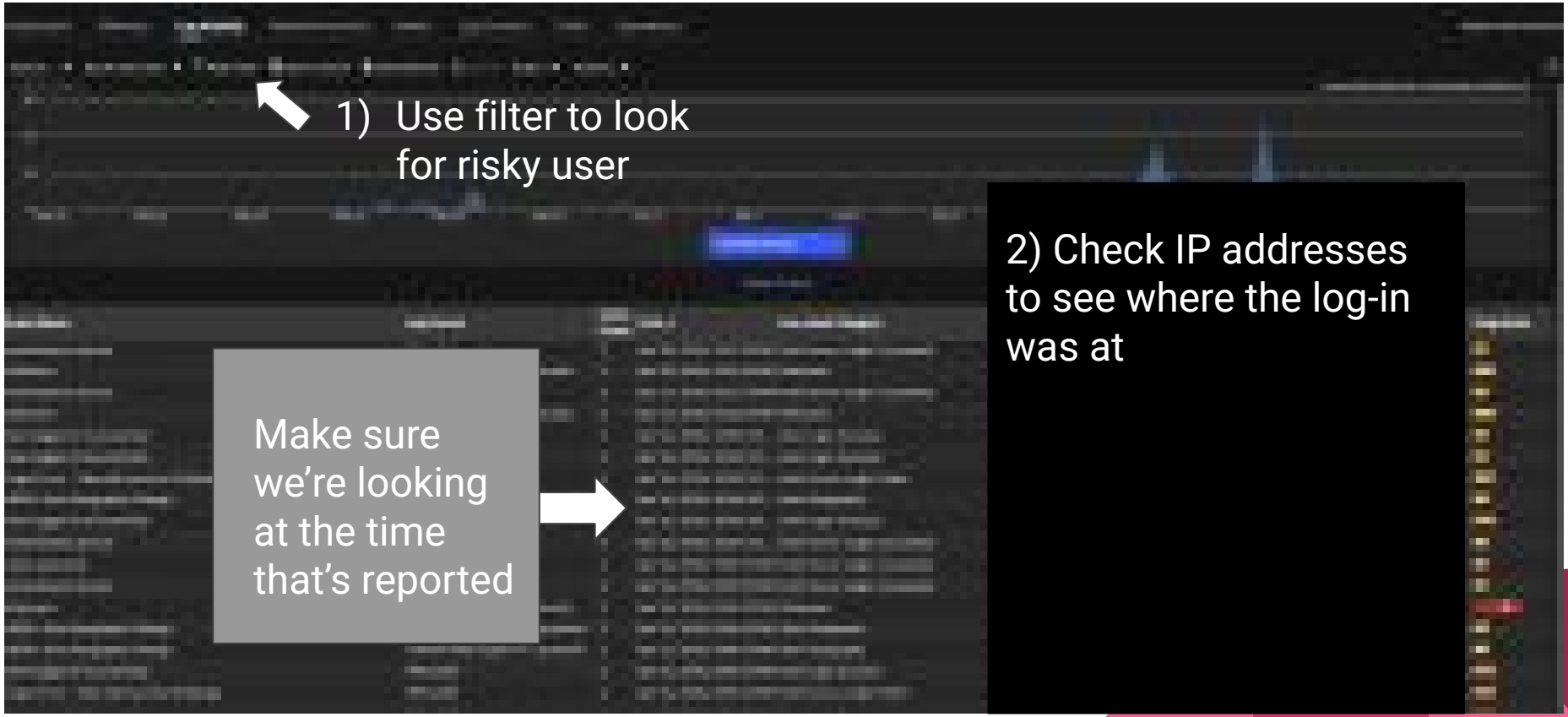
- List of Risky Users (Time, Day, and Username)
    - QRadar Log Analysis
- Analyse for false positives and compromised accounts

Example Scenario Pt.1

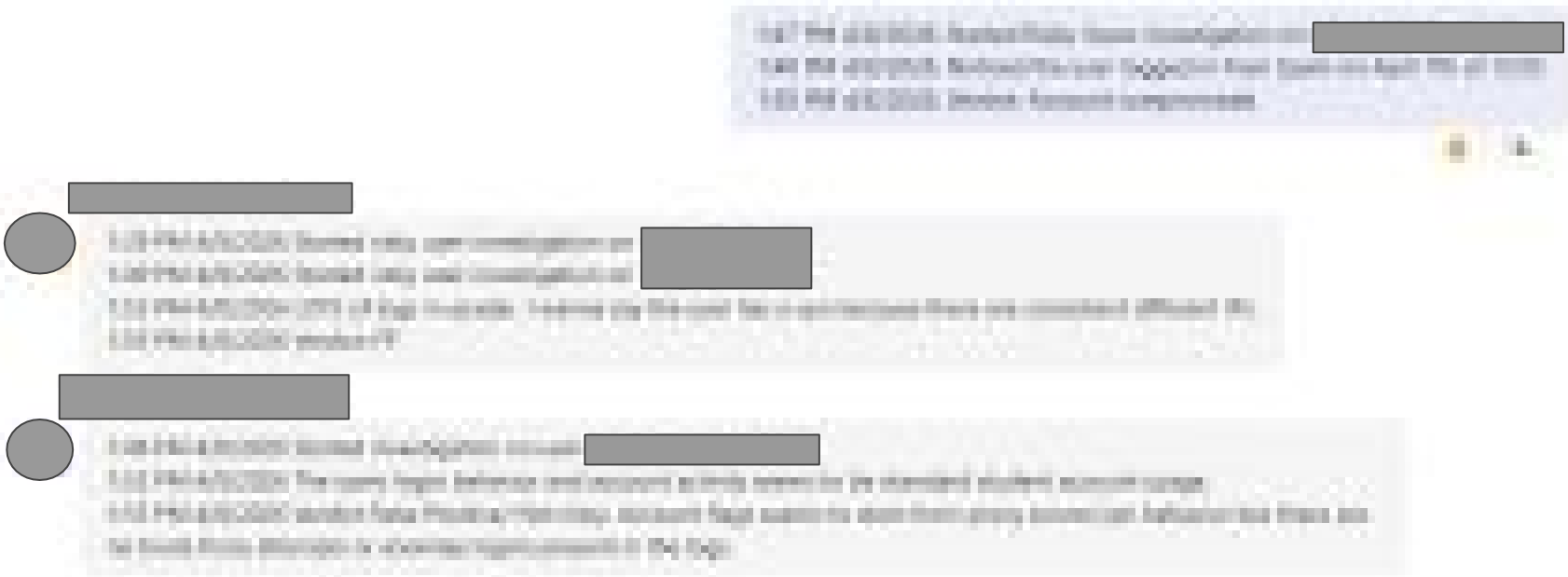


- List of Risky Users
- Go through each one in-depth
- Possibly reset password

Example Scenario Pt. 2



Example Scenario Pt. 3



Real SOC Workflow

Alert Triggered

- **PagerDuty** - Phishing email reports
- **QRadar** - Risky user flags
- **CrowdStrike** - Endpoint detection

Review

- **PagerDuty & QRadar** - Note key indicators
- **CrowdStrike** - Prioritize by severity

Investigate

- **PagerDuty** - Sender domain, URLs, Attachments, etc.
- **QRadar** - Geo location, login attempts, etc.
- **CrowdStrike** - Trace full process tree

Verdict

- **True positive** - Real threat
- **False positive** - Normal activity flagged by mistake

Wrap up

- Document findings
- Resolve and close ticket
- Notify team

Concluding Remarks

Thank you!

Any Questions?

Stay Connected with us on LinkedIn!

Nehemia Araia, Aiden West, Emanuel Reynoso, Ibrahima Balde