

WiCyS 2023

#role-join WiCyS
#signin wicys



ROCHESTER INSTITUTE OF TECHNOLOGY
STUDENT CHAPTER

Schedule!

Weekly Meetings

*Wednesdays at 7:00 PM in GCI
Security Lab
Golisano Hall 2740*



Official WiCyS Website



RIT WiCyS Website

WiCyS@RIT 2022-2023
Spring Semester Schedule
Meetings at 7:00pm in GCI Security Lab
Golisano Hall 2740

25 January	Semester Goals
1 February	Intro to Red Team
8 February	Maximize your College Experience
15 February	Kubing Around
22 February	SOC Talk
1 March	Preparing for Interviews
8 March	Midterm Madness
15 March	No Meeting - WiCyS Conference
22 March	Homelabbing with Ashley
29 March	Making the Most of Your Co-op
5 April	Intro to Pentesting
12 April	The Art of Fiddling
19 April	Eboard Elections
26 April	Spring Final Fun



ROCHESTER INSTITUTE OF TECHNOLOGY
STUDENT CHAPTER

Follow our Socials!



@WiCySRIT



@WiCySRIT

Announcements

- **It's snowing outside**





What is a sock?





What is a **soek** SOC?



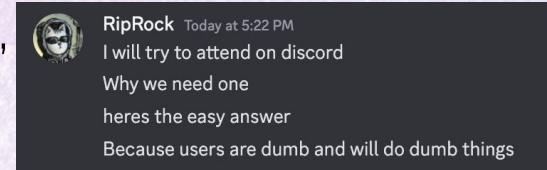
What is a SOC?

- SOC -> Security Operations Center
- Centralized team that is responsible for managing and monitoring the organization's security posture
 - Triage alerts (escalate/remediate)



We have firewalls and EDRs. Why is a SOC important?

- Need humans to be like "uh-oh" or "it's fine"
- Humans overall have better judgement than computers
- "Because users are dumb and will do dumb things"



What is a SOC?

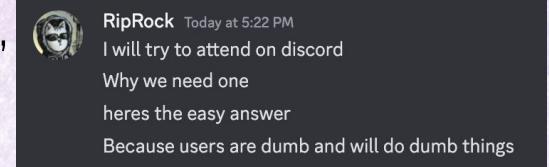
- SOC -> Security Operations Center
- Centralized team that is responsible for managing and monitoring the organization's security posture
 - Triage alerts (escalate/remediate)



MakeAGIF.com

We have firewalls and EDRs. Why is a SOC important?

- Need humans to be like "uh-oh" or "it's fine"
- Humans overall have better judgement than computers (except Kenny)
- "Because users are dumb and will do dumb things"

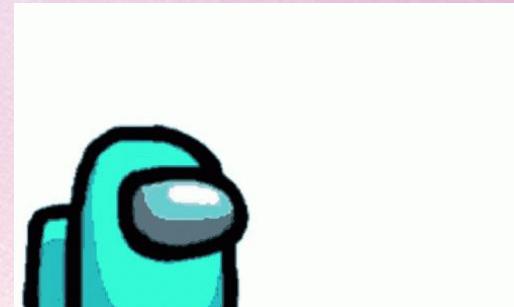
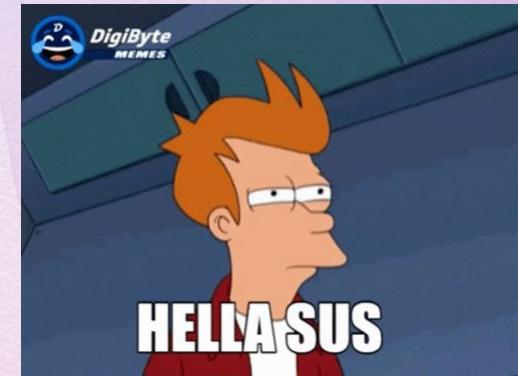
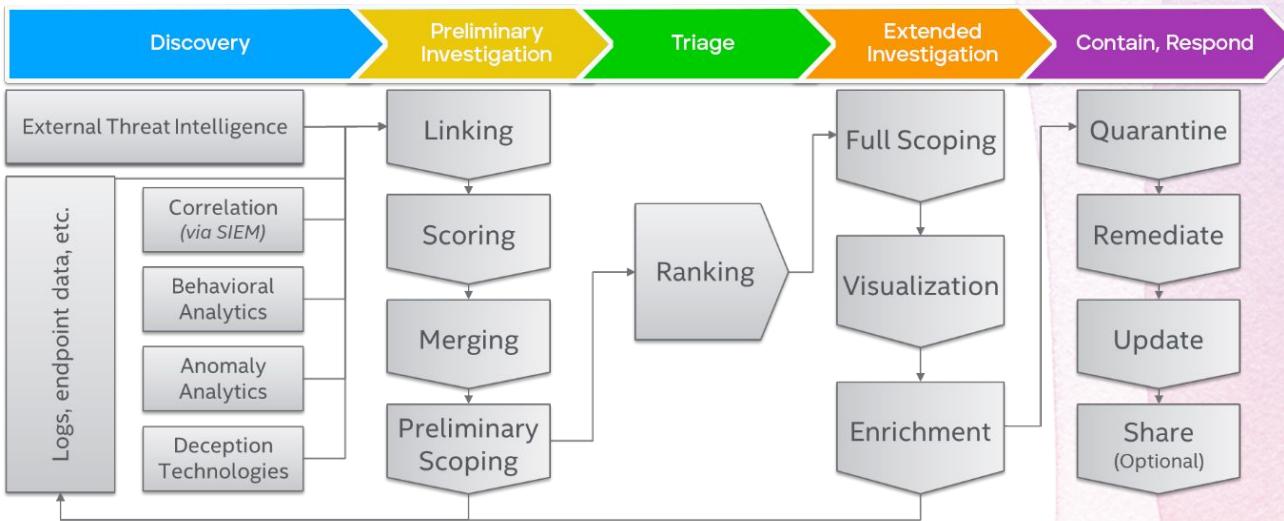




What's the purpose of a SOC?

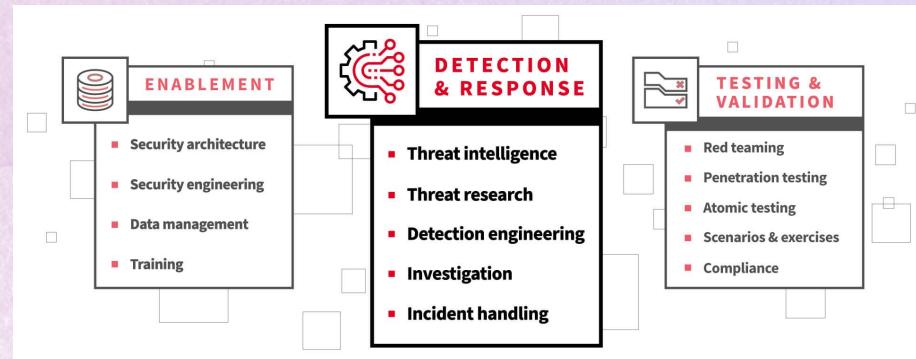
Purposes

- Provide 24x7x365 coverage for our clients (or as much as they pay for)
- Escalate/remediate suspicious activity
- Close out benign activity
- Perform ad-hoc tasks



What people/roles are involved in a SOC?

- Managers
- Client Leads
- Security Analysts/Defenders
- Security Engineers
- Threat Hunters
- Incident Response
- Threat Intelligence
- Infrastructure management



How does a SOC even work?

Logs... logs... logs...

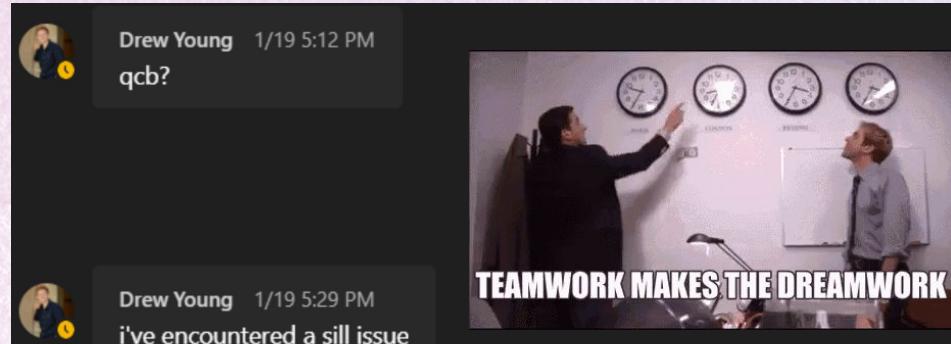


Logs... logs... logs...

- It's a process...
 - EDR -> Logs -> SIEM -> Alerts
 - Alerts -> Triage
 - Escalation
 - Closure

Things that help us!

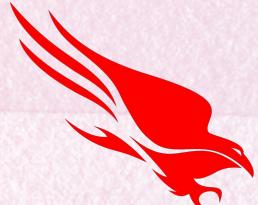
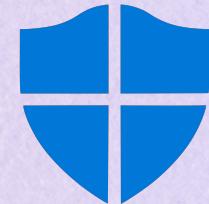
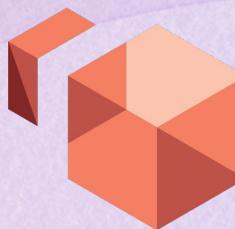
- SOAR
 - Security Orchestration Automation & Response
 - Make our jobs easier!
- OSINT Tools
- Collaboration



1/19 5:12 PM
yuh huh

What tools are used in a SOC?

Oh so many tools...



CROWDSTRIKE



CYLANCE¹⁸

**What are some of the
best practices in a
SOC?**

- SOCs should always be looking to improve
- Threat Hunting
 - Proactive → find hidden threats in the environment
 - Can be based on recent IOCs/client choice/SOC choice
- Tuning
 - Can weed out False Positives >> saves time
 - Better threat detection
- Threat Intelligence (@SRA_ThreatWatch) 
 - Collects and analyzes current threat data
 - Distributes among SOC



Story Time!

- Client reached out to me and asked SRA to hop on a call with them since a bunch of their accounts were being logged into from a weird country, we got on the call, got a bunch of information then investigated for a couple hours, determined it seemed like pen testing activity and turns out it was our own team... nice