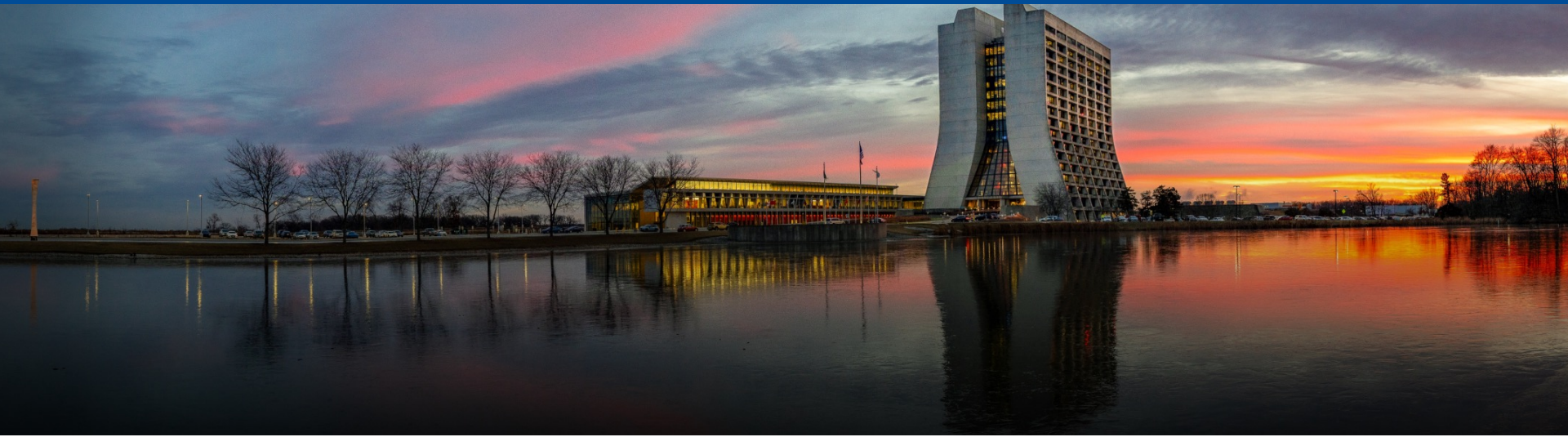


# WLCG SOC Hackathon: let's talk People and Process!

Jeny Teheran
Cybersecurity Team
Fermi National Accelerator Laboratory

# Overview

- The goal of your SOC
- People, Process, Tools, and Data
- SOC core functions
- SOC auxiliary functions
- The SOC processes
- The people you need
- Building and running your SOC

# The goal of your SOC

- What is a SOC?

  "A SOC is a combination of people, processes, and technology protecting the information systems of an organization through → proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects."

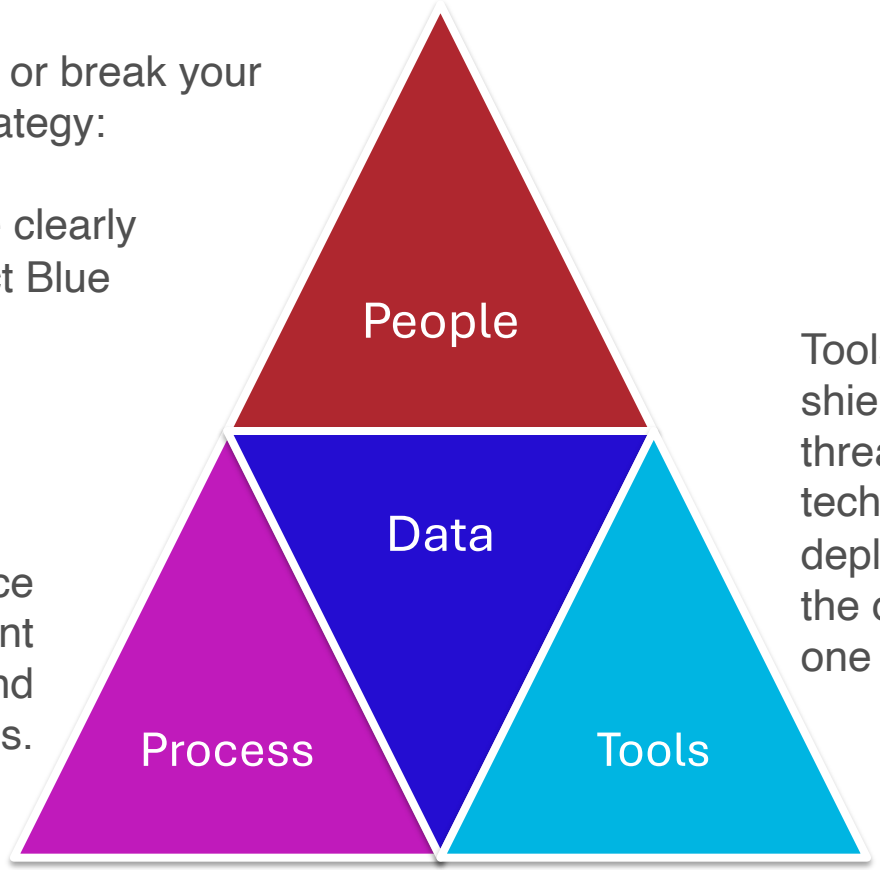
- Why do you need a SOC?
  - We have been facing an acceleration in the evolution of the adversary's tactics, techniques, and procedures (TTPs).
  - Protecting NRENs and all its assets require global collaboration and coordination for incident response.

*– Given enough time, an APT eventually gets through*

# People, Process, Tools and Data

People will make or break your cybersecurity strategy:

- Engage early
- Communicate clearly
- Think Red, act Blue



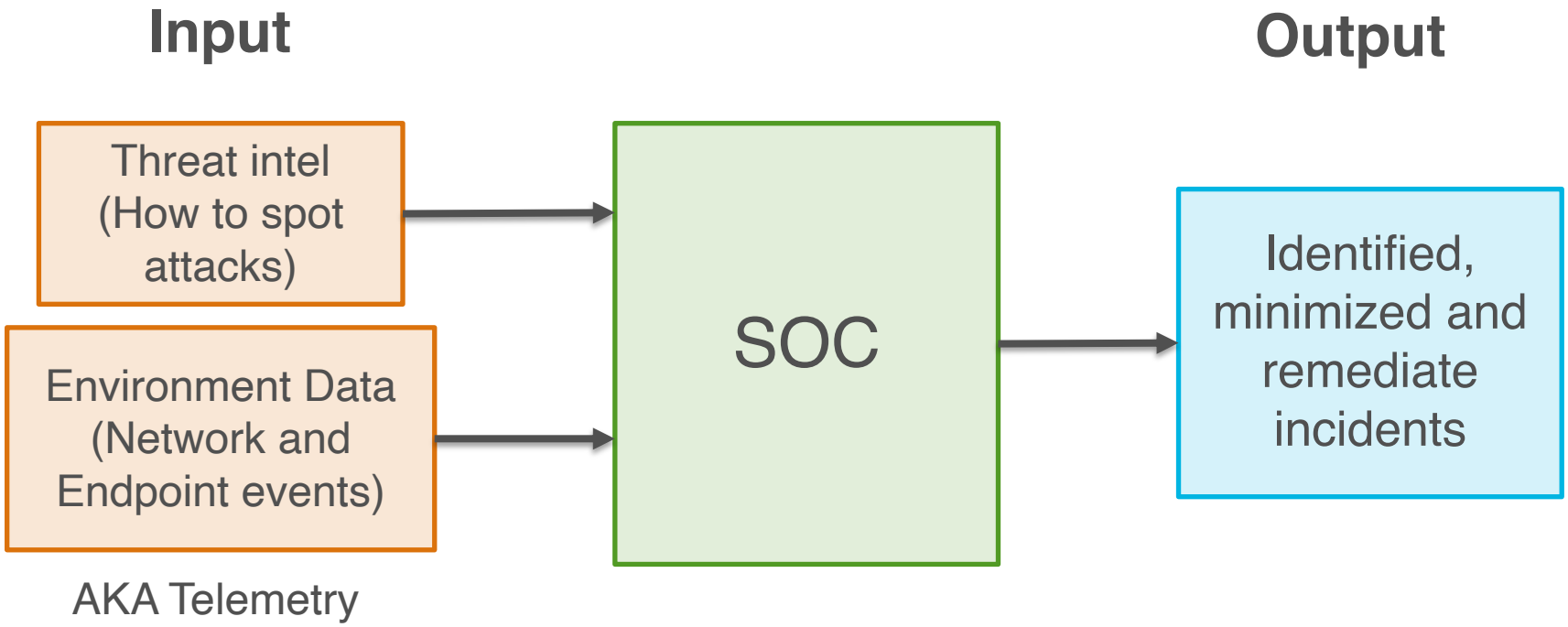

Having processes in place ensures a consistent approach to handling and preventing security incidents.

Tools are the protective shield against cyber threats. Tools and technology that are deployed correctly are the defense when no one else is watching.



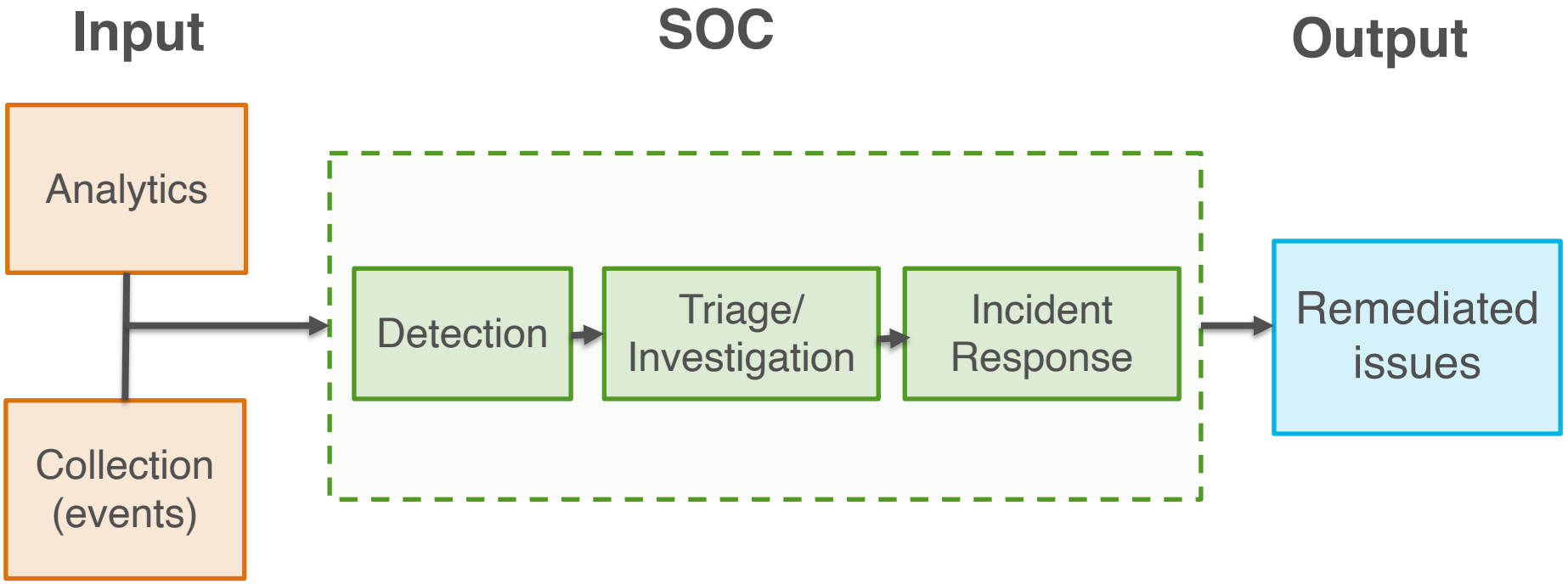
Fermilab

# What a SOC does?



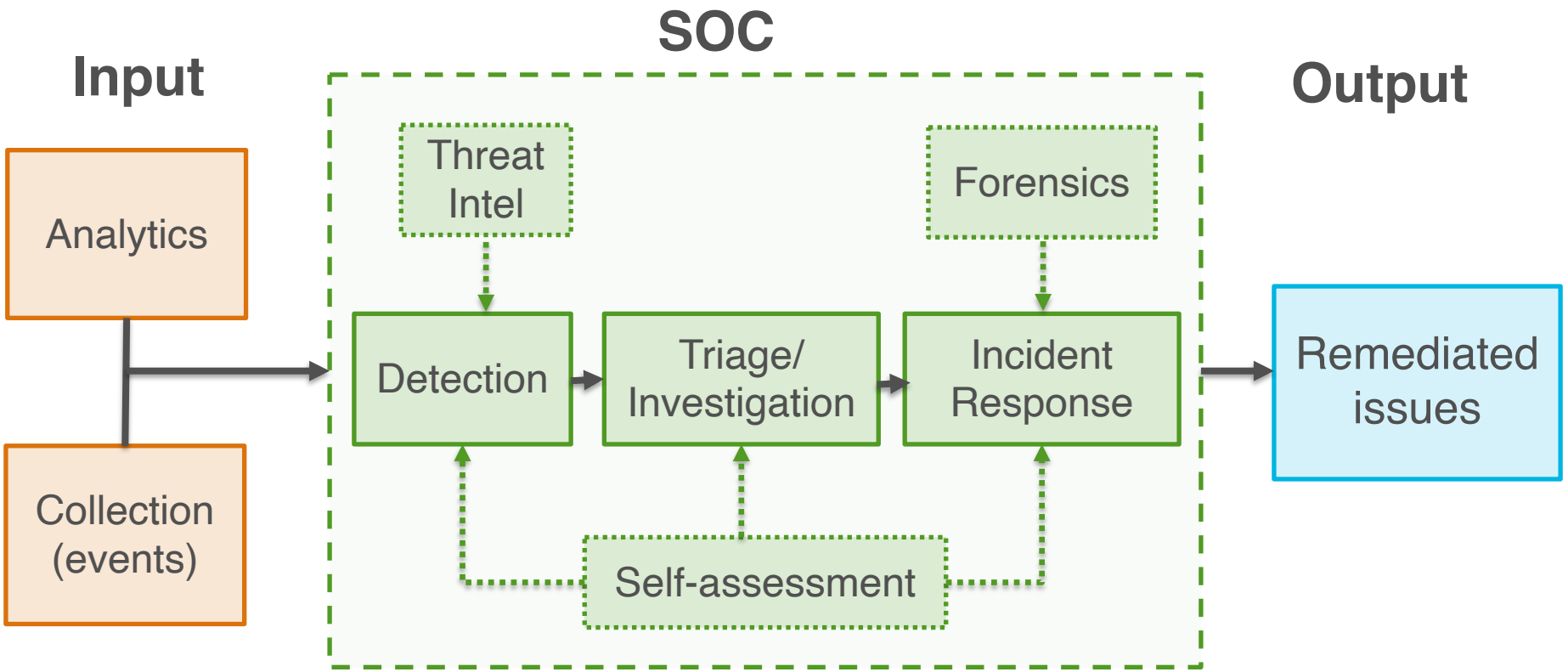

Original diagram from [SANS MGT551: Building and Leading SOCs]

# Core functions of the SOC




Original diagram from [SANS MGT551: Building and Leading SOCs]

# Core functions of the SOC and auxiliary functions



# The SOC processes

1. Preventing cybersecurity incidents through proactive measures including:
    a. Continuous analysis of threats
    b. Assessing vulnerabilities
    c. Deploying coordinated countermeasures
2. Responding to confirmed incidents by coordinating resources for remediation
3. Monitoring, detection, and analysis of potential intrusions

# The People component for your SOC

1. Know what you are protecting and why?
2. Select your SOC functions and services:

   ~~Build a SOC structure that matches your organization needs.~~

   Build a SOC structure that matches your resources and then, your organization needs.

   Select and collect the right data

   Leverage tools to support analysis

   Avoid alert-fatigue
3. Prioritize Incident Response (IR)
4. Communicate clearly, collaborate often, share generously

# Example: Cybersecurity Operations Team (CSO)

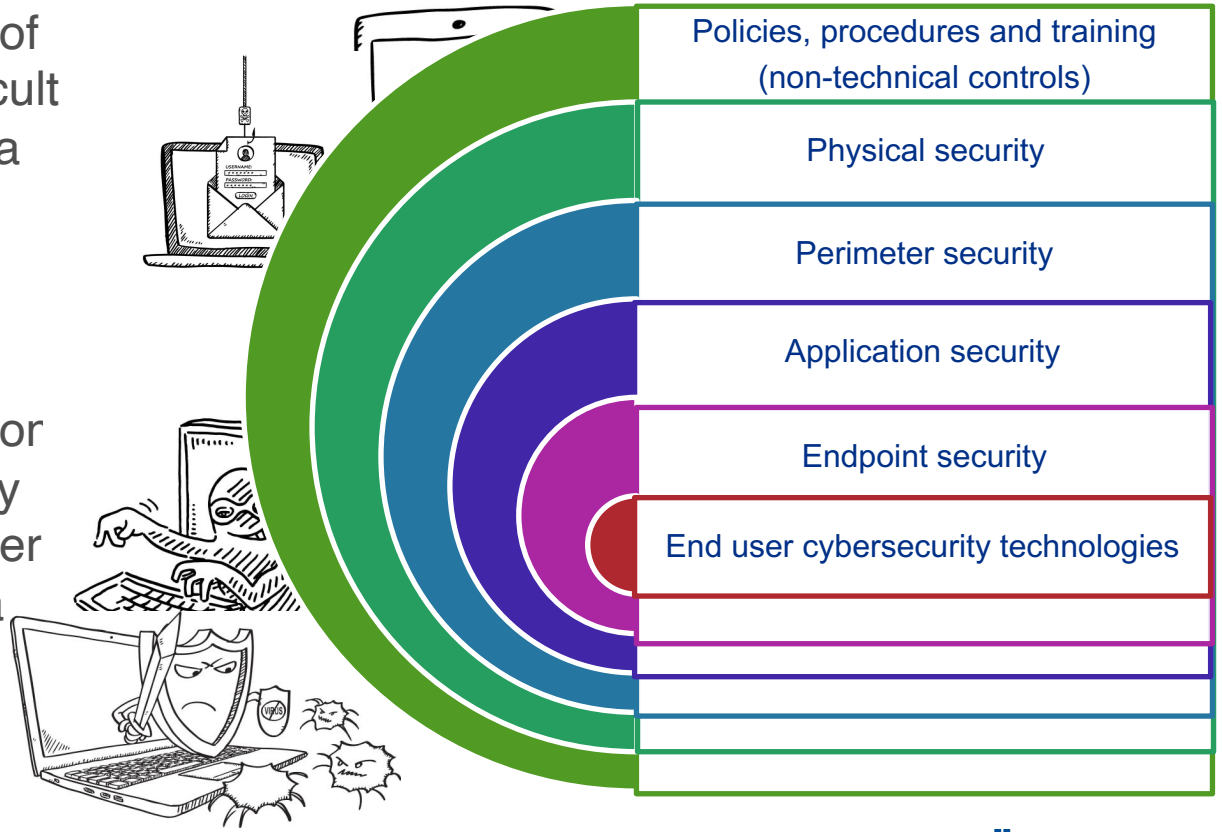
- A team of cybersecurity analysts and architects protecting Fermilab's information systems against cyber threats and attacks:
  - Ensuring a secure operating environment enforcing policy across the organization
  - Investigating reports and monitoring threats on the Internet
  - Responding to cyber security incidents
  - Analyzing risk and continuously improving defense mechanisms

- Main activities:
  - Operate cybersecurity systems and active defenses
  - Participate in on-call rotation for cybersecurity operations and incident response
  - Deploy new technologies and apply enhancements to existing mechanisms
  - Provide feedback to policy (CSP)

# Moving from defense-in-depth towards threat-informed defense

- Defense in depth is a way of trying to make it more difficult for someone to break into a system.

- 3-year goal: Evolve cybersecurity operations fror a defense-in-depth strategy deeply focused on perimeter security controls towards a threat-informed defense.






Fermilab

# Day-to-day cybersecurity operations

- Fermilab CSO performs Incident Response rotation with a weekly schedule for 8to5 coverage and ServiceDesk for off-hours:

  Primary (T1) --> Triage alerts and process requests

  Secondary (T2) → Investigation

  Tertiary (T3-Lead) → Coordinates daily briefing and allocate resources

- Knowledge Base contains Standard Operating Procedures (SOPs), escalation guidelines
- 15-min to 30-min daily rotation briefing guarantees Primary and Secondary are sharing the most important pieces of data for daily operations → ask for additional input, re-assess knowledge, and share jokes!

  This is crucial for an all-remote team!

# Fermilab IR rotation

- 3 Analysts on Primary rotation → 2 Junior analysts + 1 Senior analyst

  Primary every 3rd week

- 4 Analysts on Secondary rotation → 1 Junior analyst + 3 Senior analysts

  Secondary every 4th week

*A SOC's capacity to perform its entire mission is usually influenced more by its skill level, maturity, and automation that the number of analysts.*

*Growing a SOC team requires a consistent investment of time and resources but lead to long term success*

# References

- Course material from LDR551: Building and Leading Security Operations Centers
- 11 strategies of a world-class Cybersecurity Operations Center by MITRE corporation
- Podcast: Blueprint, build the best in cyber defense https://www.sans.org/podcasts/blueprint/
- Building a Security Operations Centre (SOC) NCSC UK
- NIST Cybersecurity Framework v2
- Detect Tactics, Techniques & Combat Threats