A day in the life of an incident responder 

Disclaimer

The views and opinions expressed in this presentation are solely those of the author and do not necessarily reflect the official policy or position of my employer.

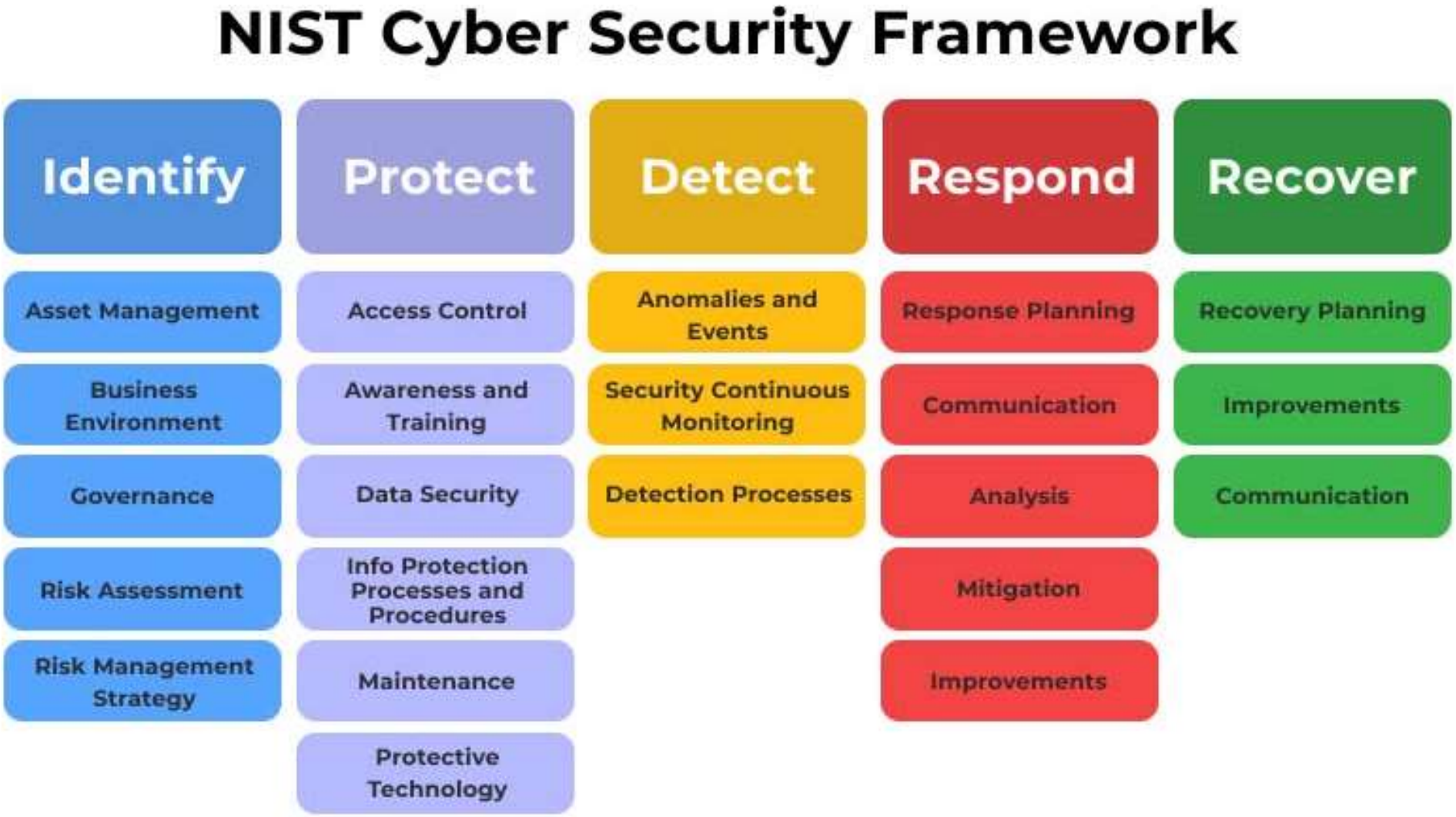
Any content provided in this presentation, including case studies and examples, is of the author’s opinion and is not intended to malign any organization, company, individual, or entity.

Intro

- ✓what's like to do IR
- ✓how your forensic skills might help you in IR
- ✓"Forensic-O-Meter"
- ✓ask anytime

Summary 

- Disclaimer
- Intro.
- What is IR
- Typical day
- Case Work.
- Ad-hoc/ Non Case Work
- Pros vs Cons .
- Outro

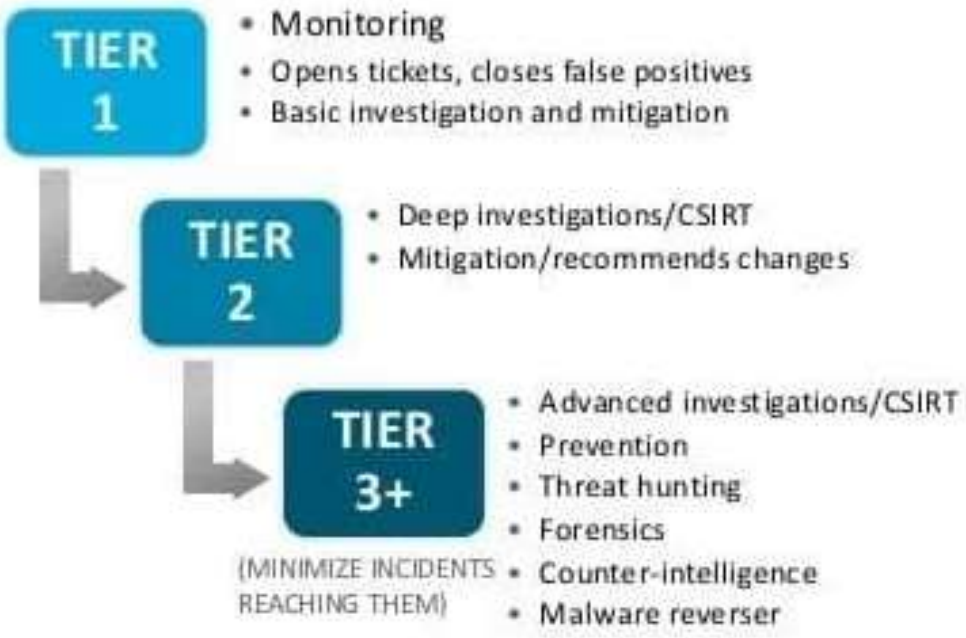

NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communication
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communication

What is IR?

What is IR?

SOC? SIEM? 24/7? IR?

L3 position



Event ➡ Security Event ➡ Incident

IR Commander; IR Eng.; Mas-Com; Inc-Com;

SIEM showcase

What is IR?

Typical day 

- Comms (email, messaging) 😳
  - update on cases/ ad-hoc jobs
  - new cases/ ad-hoc jobs
  - news
- Case management (SIEM, case-mgmt, paging) 😊
  - update on running cases
  - new cases
- News (twitter, feedly, talkback) 😊
  - Why news? more on hunting
- To Do 😳
- Acquire access/ PAM 😳
  - depends on case/ ad-hoc jobs acquire access
- Work on cases 🤩
- Ad-hoc/ non case work 😊

Case work🤩

- Non-IR/ SOC case
  - technical advice for L1, L2, ISO🤩 (win, lin, log analysis)
- IR
  - IR Workflow: Preparation ➡️ Detection & Analysis 🤩 ➡️ Containment 😊, Eradication 😊, Recovery 😊➡️ Lesson learned

Non Case Work: Improvements

- Detection Eng.
  - New application/ log 😊 (log analysis)
  - Improvement of current use cases 😊 (win, lin, cloud, log analysis)
- Knowledge Base
  - Update KB, create new articles 😳😊 (win, lin, cloud, log analysis, DF knowledge)
- Process Improvement

Non Case Work: Hunting 😊

CTI/ other sources ➡ hypothesis ➡ hunts

Non Case Work: Personal Projects

- L3 projects
  - collection script (https://aldosimon.com/improving-sentinel-live-response-collection)
  - IR capability Matrix (WIP)

Pros vs cons

Pros	Cons
Fun stuff	On calls
New tech	Stress
Meet people	
Learn new stuff	

Outro

Credits:

- https://www.letsdefend.io/blog/soc-analyst-levels-description-requirements-career
- https://pei.com/siem-soc-security-benefits/
- https://www.bitlyft.com/resources/introduction-cyber-threat-hunting
- https://www.reddit.com/r/AskNetsec/comments/se8667/anyone_have_a_good_list_of_people_to_follow_on/
- https://www.cyentia.com/the-death-of-infosec-twitter/
- https://www.wallarm.com/what/nist-cybersecurity-framework-csf

Contact: me@aldosimon.com

Questions? 🧐