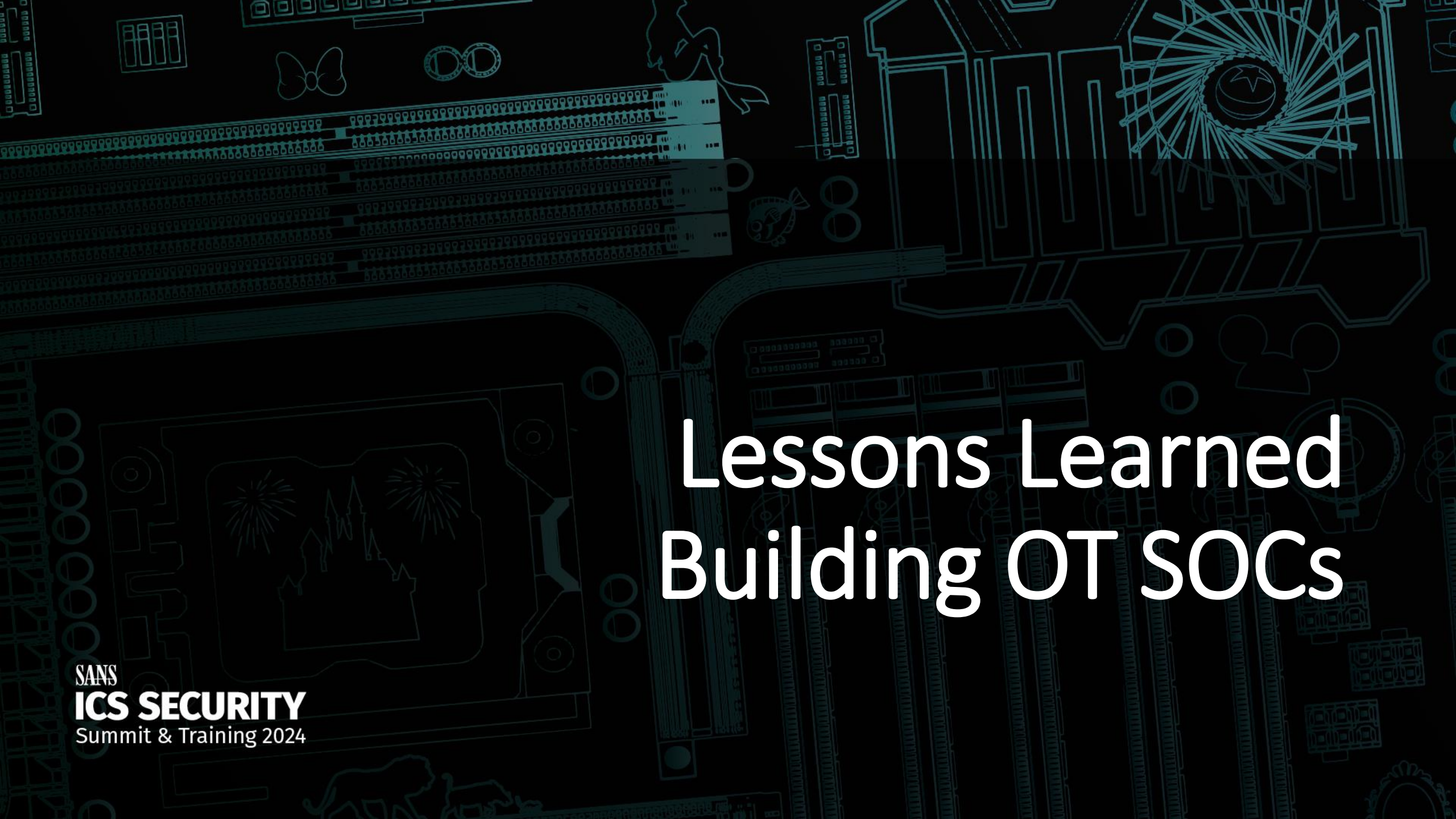

SANS
ICS SECURITY
Summit & Training 2024
Summit: June 17 - 18 | Training: June 19 - 24
Join us at Disney's Contemporary Resort
Orlando, FL or Live Online
sans.org/ICS-Summit
ICS



Lessons Learned Building OT SOCs

SANS
ICS SECURITY
Summit & Training 2024

/whois @beLarge

- Chief Evangelist & Principal OT Cyber Security Architect at Secolve
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for 15+ years
- Chartered Engineer (CPEng) and Registered Professional Engineer of Queensland (RPEQ)
- Convenor of CIGRE WG 2.51 *Implementation of SOCs in Electric Power Industry as part of Situational Awareness System*
- Bachelor Engineering (Telecomms) QUT and Master Business (Applied Finance) QUT

SABSA FOUNDATION LEVEL SCF

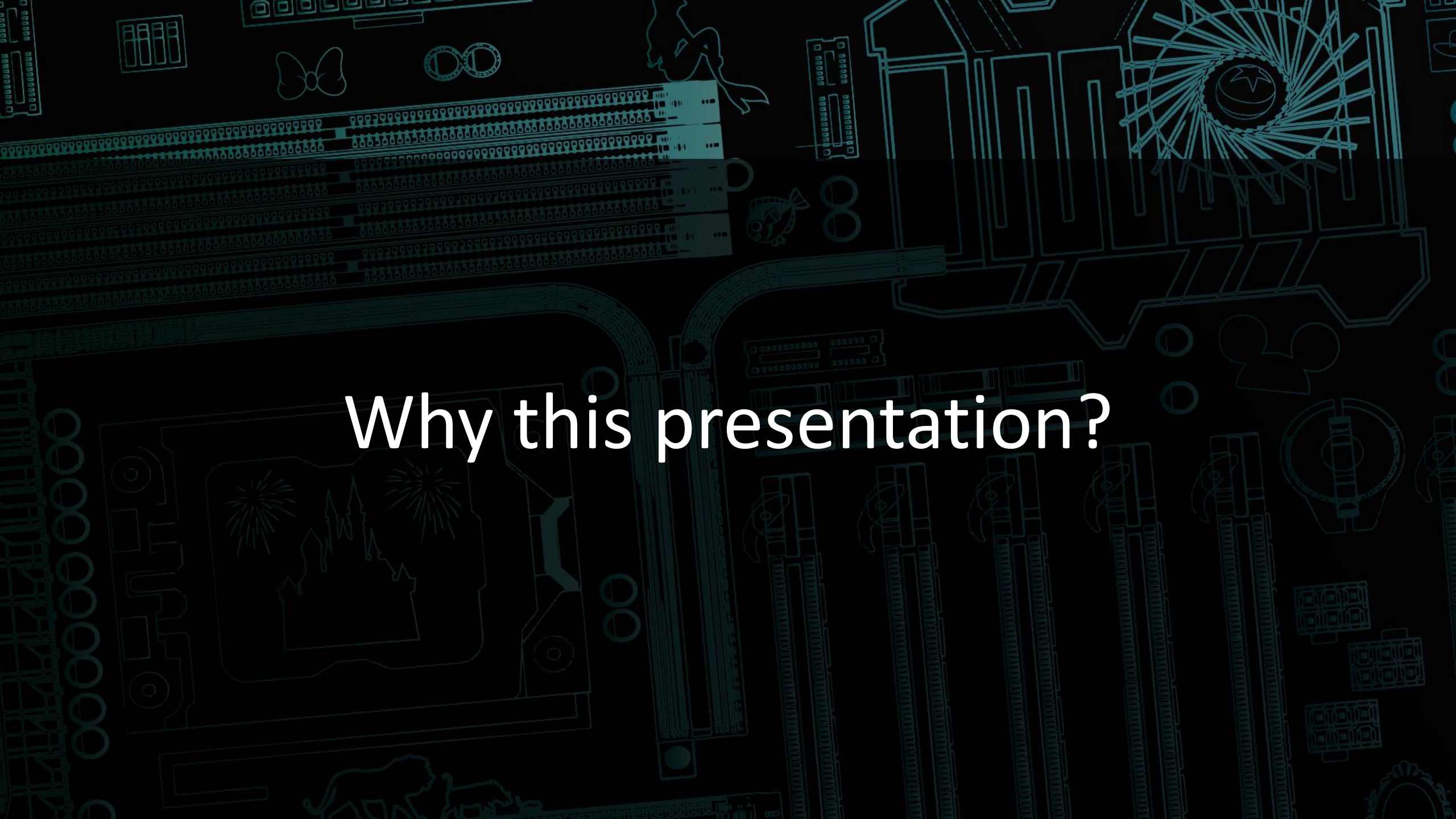
GIAC INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

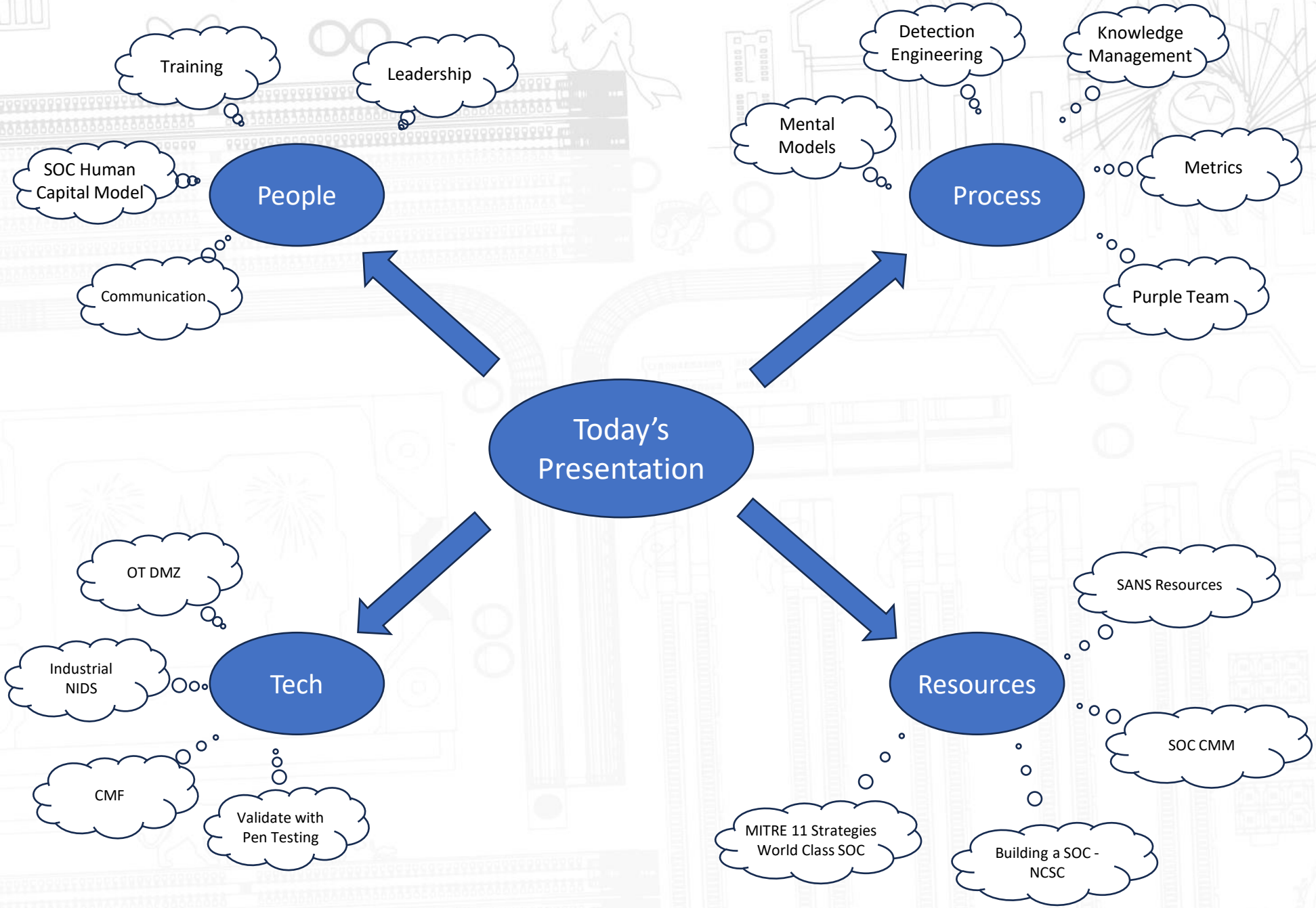
GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

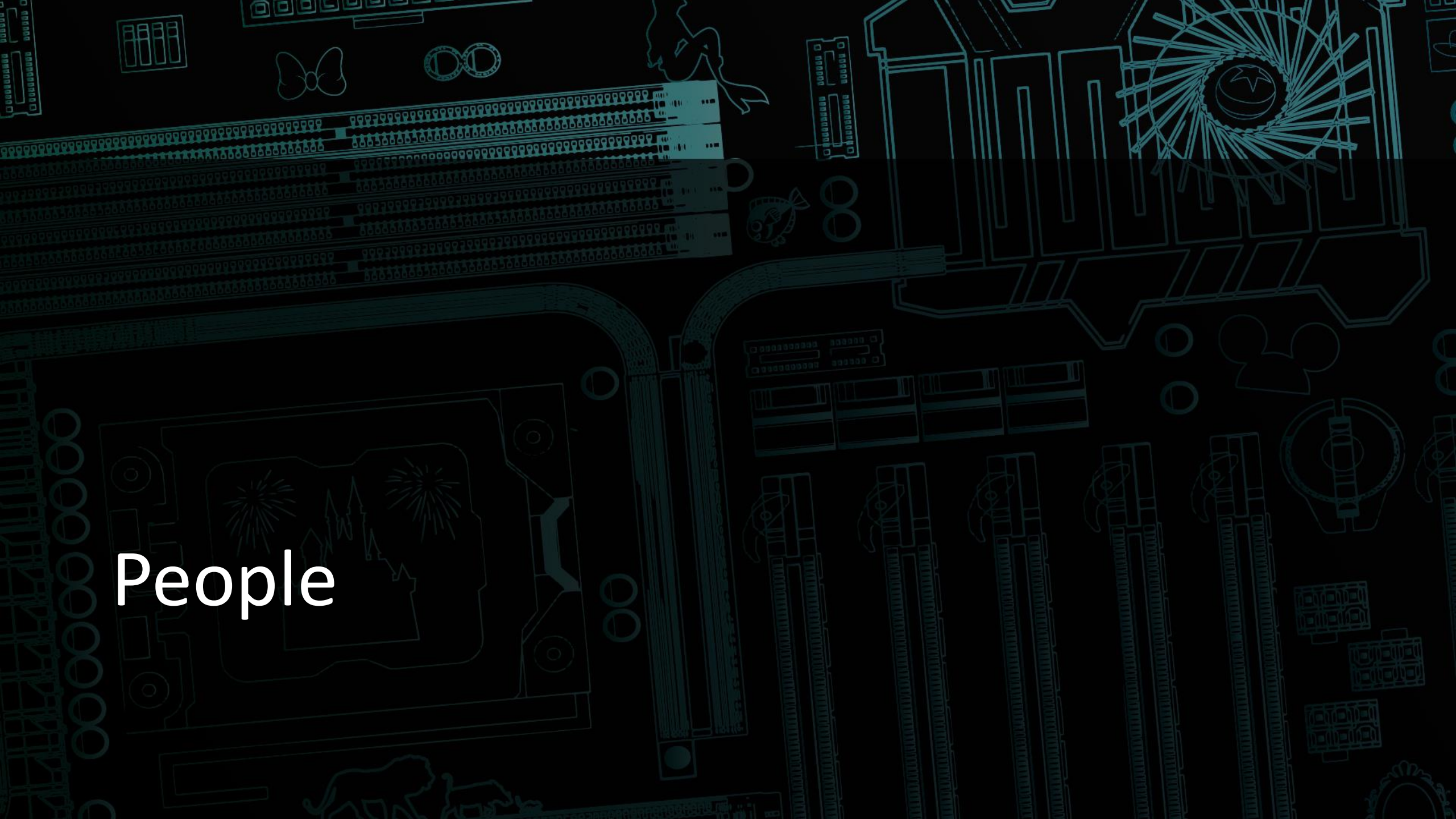
GIAC SECURITY OPERATIONS MANAGER GSOM

ISA/IEC 62443 CYBERSECURITY EXPERT ISA

alc Cyber Security Foundation+Practitioner CERTIFIED


Why this presentation?

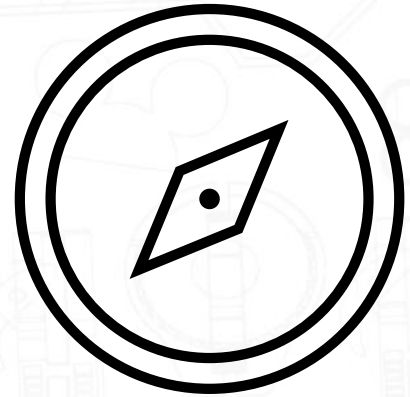

Today's Presentation
People
Training
Leadership
SOC Human Capital Model
Communication
Process
Detection Engineering
Knowledge Management
Mental Models
Metrics
Purple Team
Tech
OT DMZ
Industrial NIDS
CMF
Validate with Pen Testing
Resources
SANS Resources
SOC CMM
MITRE 11 Strategies World Class SOC
Building a SOC - NCSC



People

Leading the team

- As the leader, you need to balance being the technical lead and the team lead – your job is to guide and support the team!
- You need to flex your management style to each team member
- Manage the team's workload - I like Kanban Boards
- You need to manage Up and Out through the Organisation
- Invest the time in developing a SOC charter

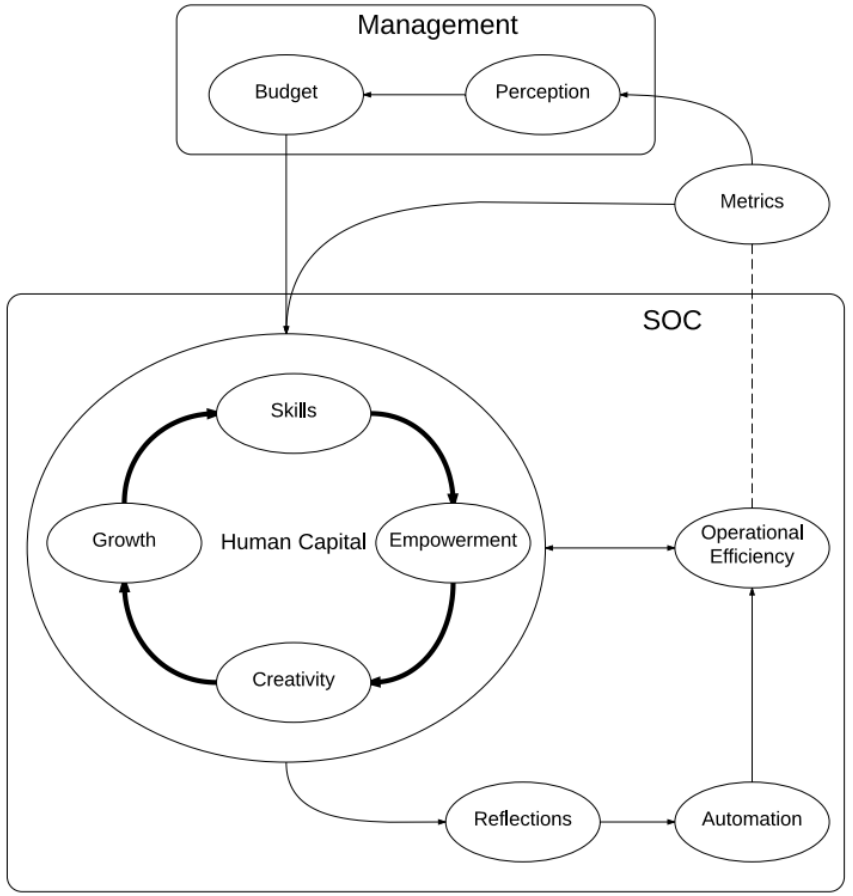


Training and Development

- Training Budgets are scarce resources
- You need to balance skill needs of the team and the interests of the individual
- Use 1 on 1s to guide training plans – understand the individual goals and learning preferences of your team
- Use Teach backs!
- Start with free community resources – paid training saves time
- Try to find opportunities to train as a team, cyber security operations is a team sport!

Using the SOC Human Capital Model

- A research project conducted by actually working in SOCs
- Gives insights that by focusing on Growth a cycle of developing skills, empowerment and creativity will improve SOC capabilities
- This improvement will encourage investment by the organisation

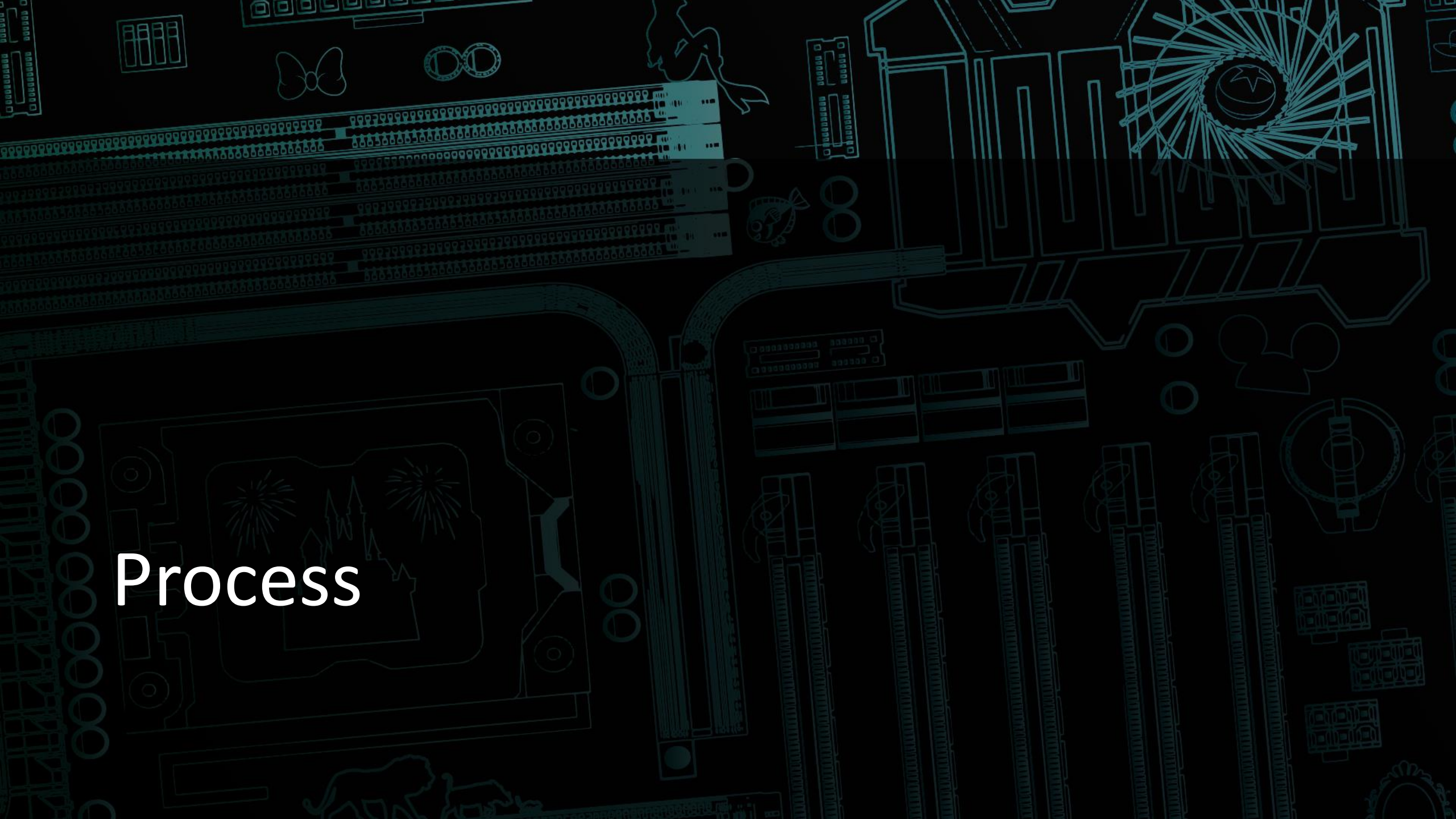


Ref - https://www.usenix.org/system/files/conference/soups2015/soups15-paper-sundaramurthy.pdf

Communication

- Vital to invest in the communication training for the team – both written and verbal
- Spend time developing the teams understanding of everyone's communication preferences
- Effective Information Security Writing is an excellent training course from Applied Network Defense

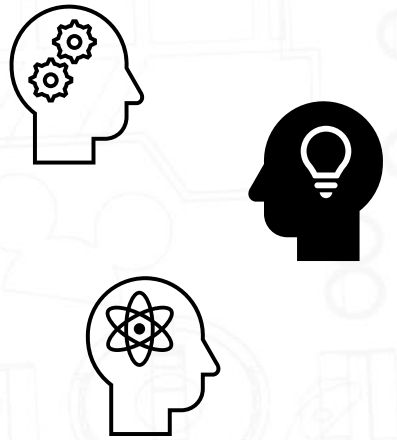
https://chrissanders.org/training/writing/



Process

Mental Models – How to use them

- How do you orient in the environment? How do you onboard new analysts?
- Can you rotate analysts between teams (IT SOC, Site Engineering, Security Architecture) to develop a shared understanding of the enterprise environment
- SOC Ride Along Days
- Chris Sanders publications are a must read - https://chrissanders.org/publications/

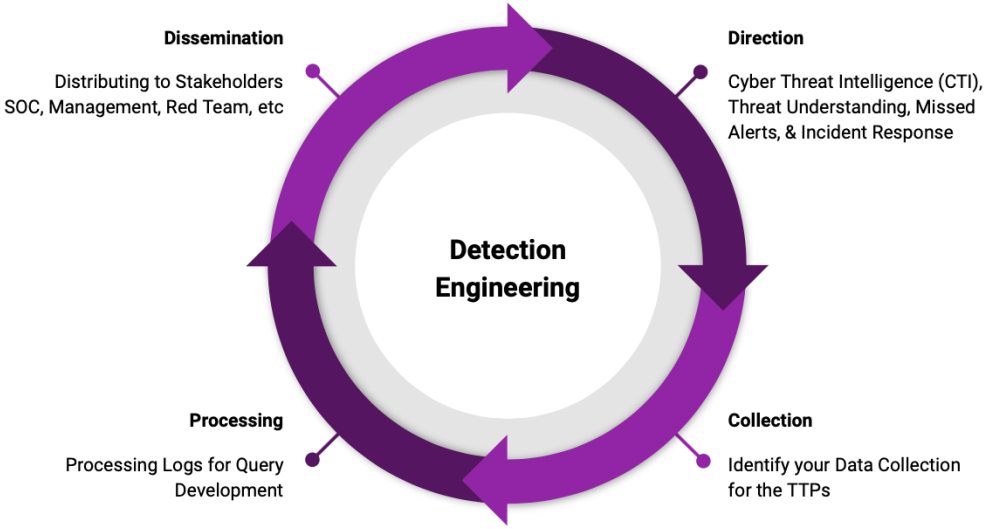


Knowledge Base

- Your ICS is different and your team will have a wealth of critical knowledge
- How do you capture knowledge for new team members?
- Identify SMEs in your team, ask them to do lunch and learns about environments and use that to organically build out your KB
- Do you have a controlled document framework? What lives in the KB vs Controlled Docs
- Where does the KB live, can you get to it if you are isolated, how is it secured?

Detection Engineering

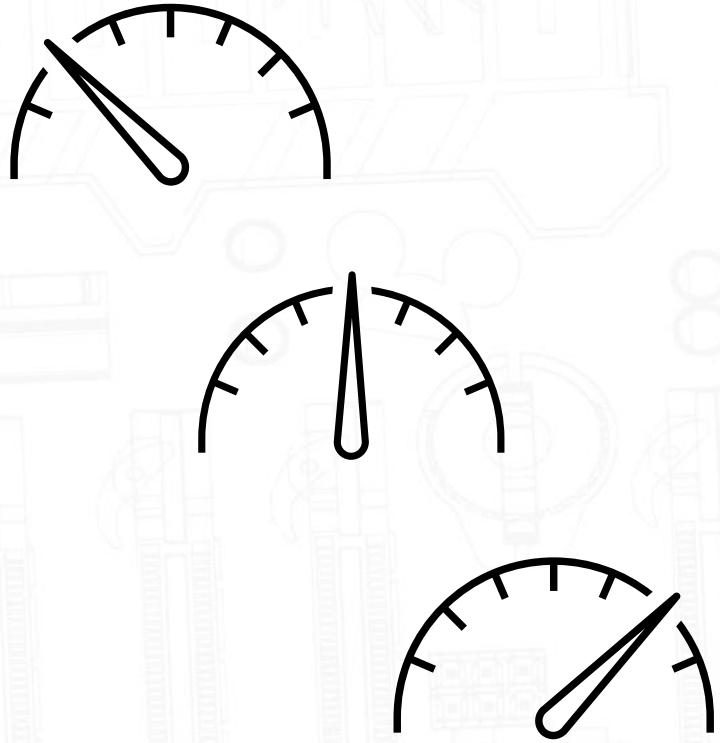
- Enables the alignment of Use Cases to other Security Activities (e.g. Risk Assessments, Cyber Threat Intelligence, Project Work)
- How to make Use Cases that Analysts can Action
  - Next Steps & Playbook Guidance
  - Types of Rules – High Confidence, Investigative, Anomaly
  - Note the Life cycle of the rule- Experimental, Functional, Stable, Retired
- Define a Request for Detection Process



Ref- https://www.sans.org/blog/purple-teaming-threat-informed-detection-engineering/

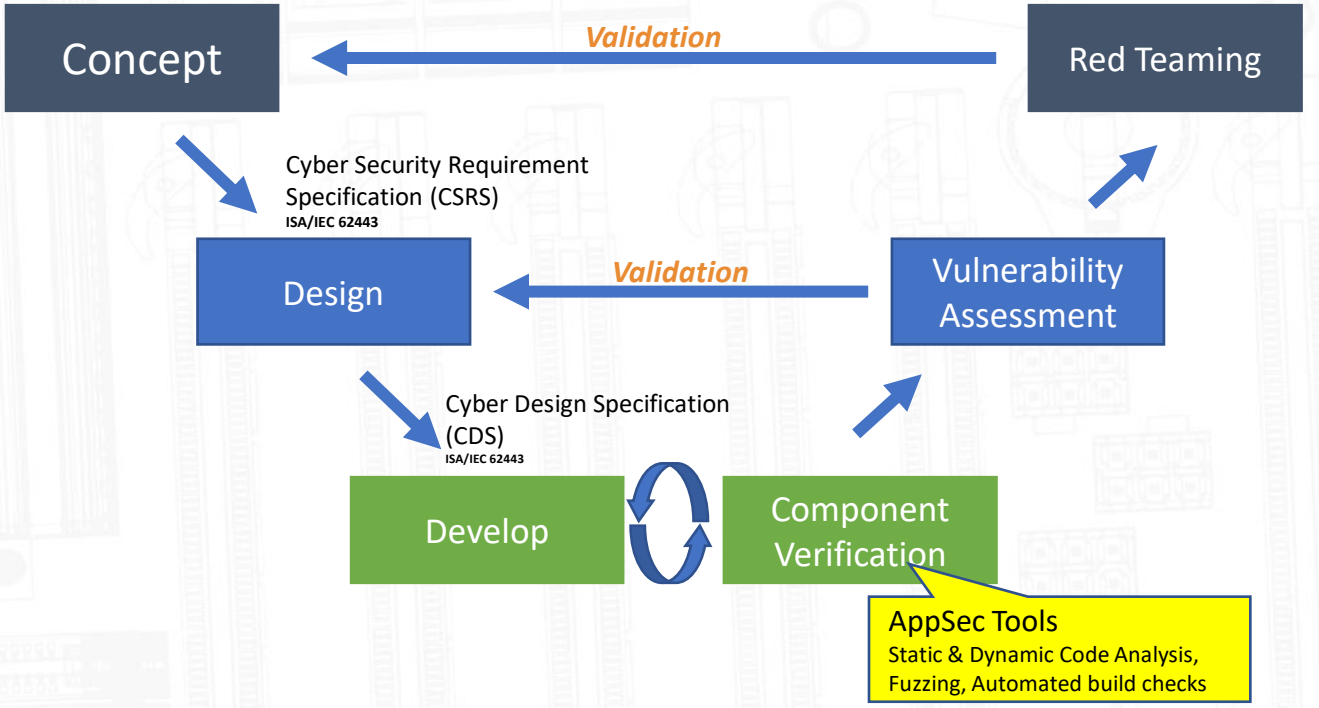
Metrics & Reporting

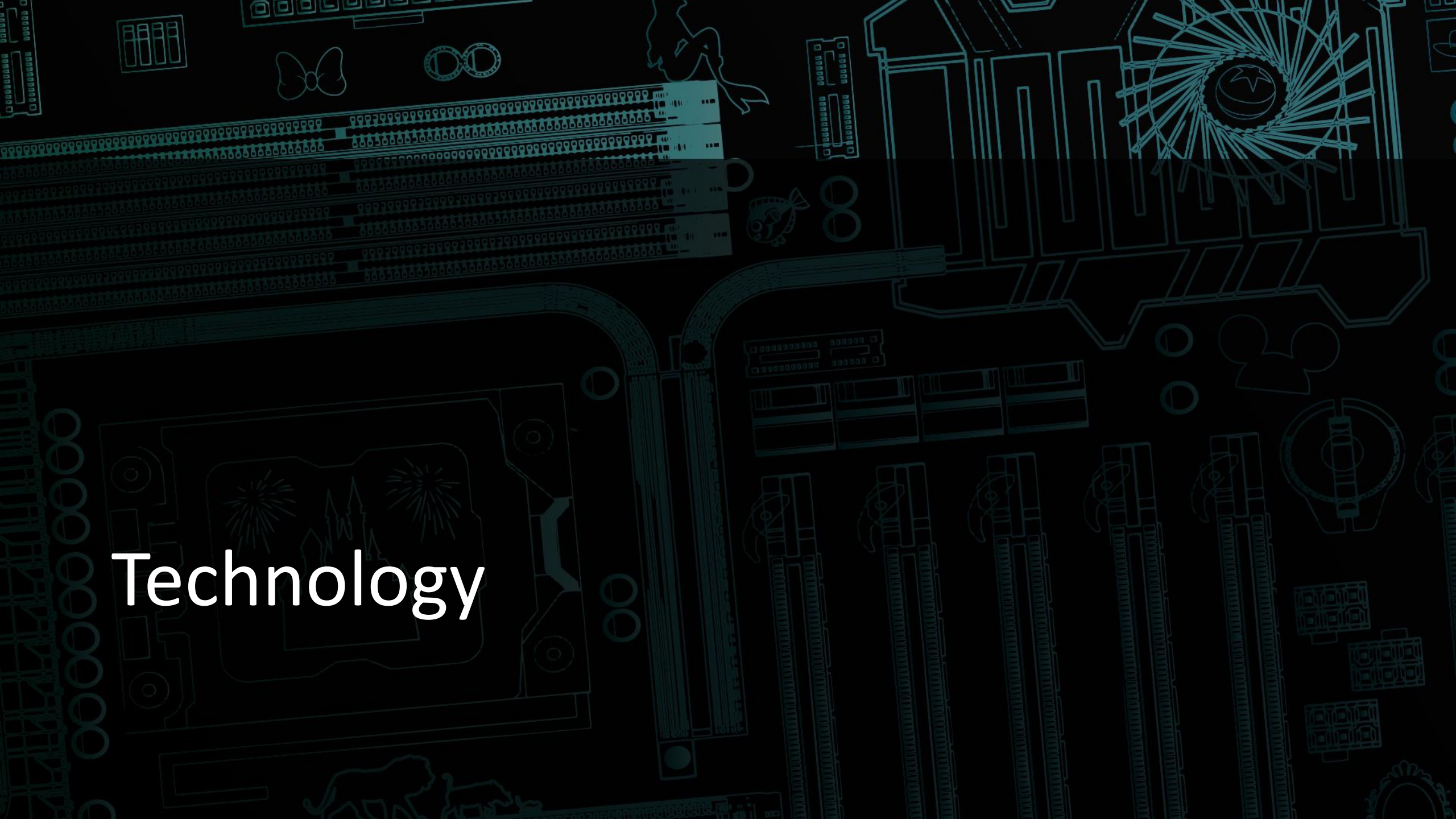
- You want a mix of leading and lagging metrics
- Less is more – try not to exceed 6 key metrics and link them to your SOC Functions
- Combine Operational Metrics and Improvement Metrics (OKRs)
- Blueprint Season 4, Strategy 10 Blueprint Episode & Episode 11 SOC Metrics: Measuring Success and Preventing burnout are awesome reference



Purple Team for Validating the Capability

- SOCs are more than just security controls – they are complex capabilities of People, Process and Tech
- Cyber Vee Model

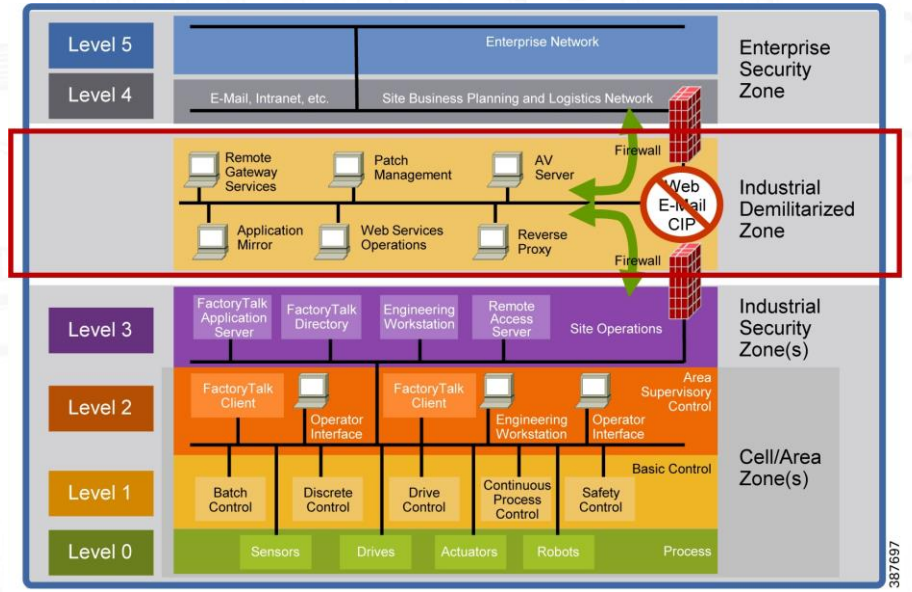




Technology

Stuck? Start at the OT DMZ

- The OT DMZ (or iDMZ) contains a lot of familiar IT systems and technology
- It is the easiest place to start collecting logs
- 90% of OT Incidents* start at the IT/OT DMZ so it is a defensible place to start
- A good way to build trust with your OT Stakeholders



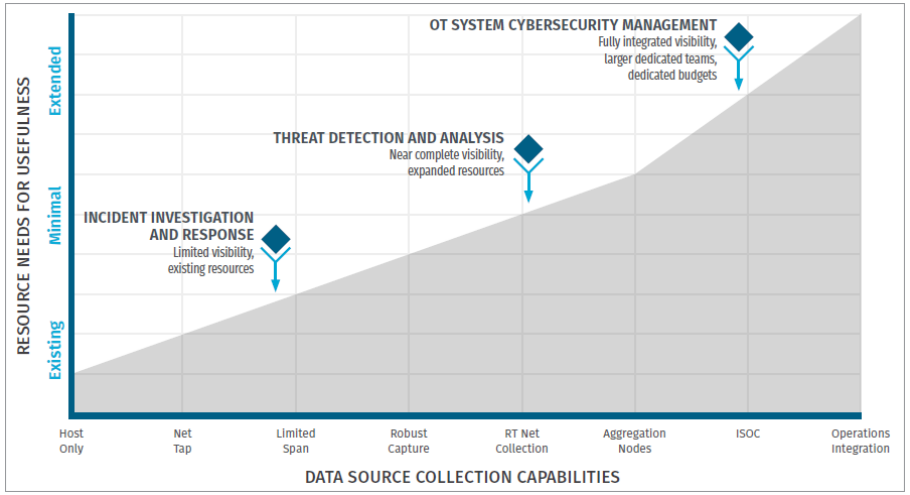
Ref- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_2_CVD/CPwE_IDMZ_2_Chap1.html

Industrial NIDS - SANS Cyber Security ICS Critical Control #3

- Make sure you understand your key network chokepoints
- Use your scenarios from Control #1 and understand your threat actor TTPs to ensure you have the right visibility
- If budget constrained –
  - Determine Chokepoints
  - Use Open Source NSM Tools to prove value

ICS NETWORK VISIBILITY MONITORING

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control



Ref https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Use a Collection Management Framework to determine logging requirements

- A collection management framework is a defensible method to determine logging requirements, retention and measure coverage
- Is used by other security operations processes e.g. Threat Hunting and Detection Engineering

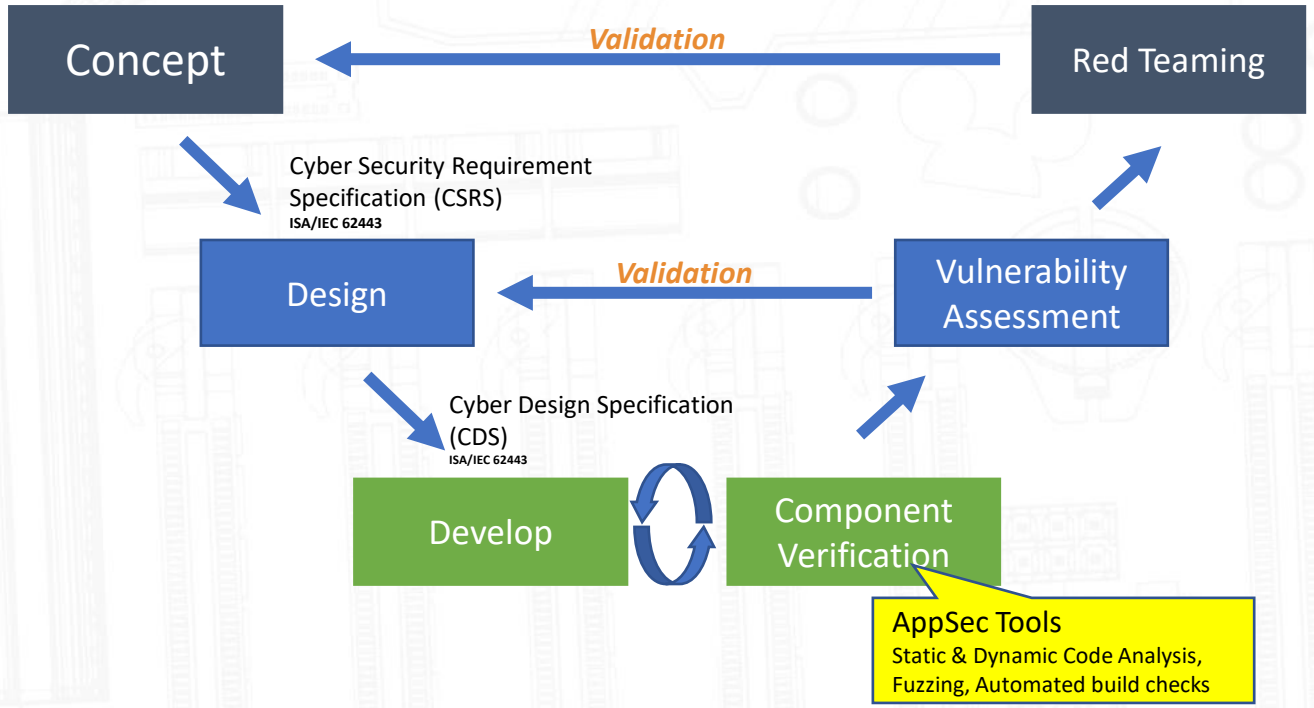
	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

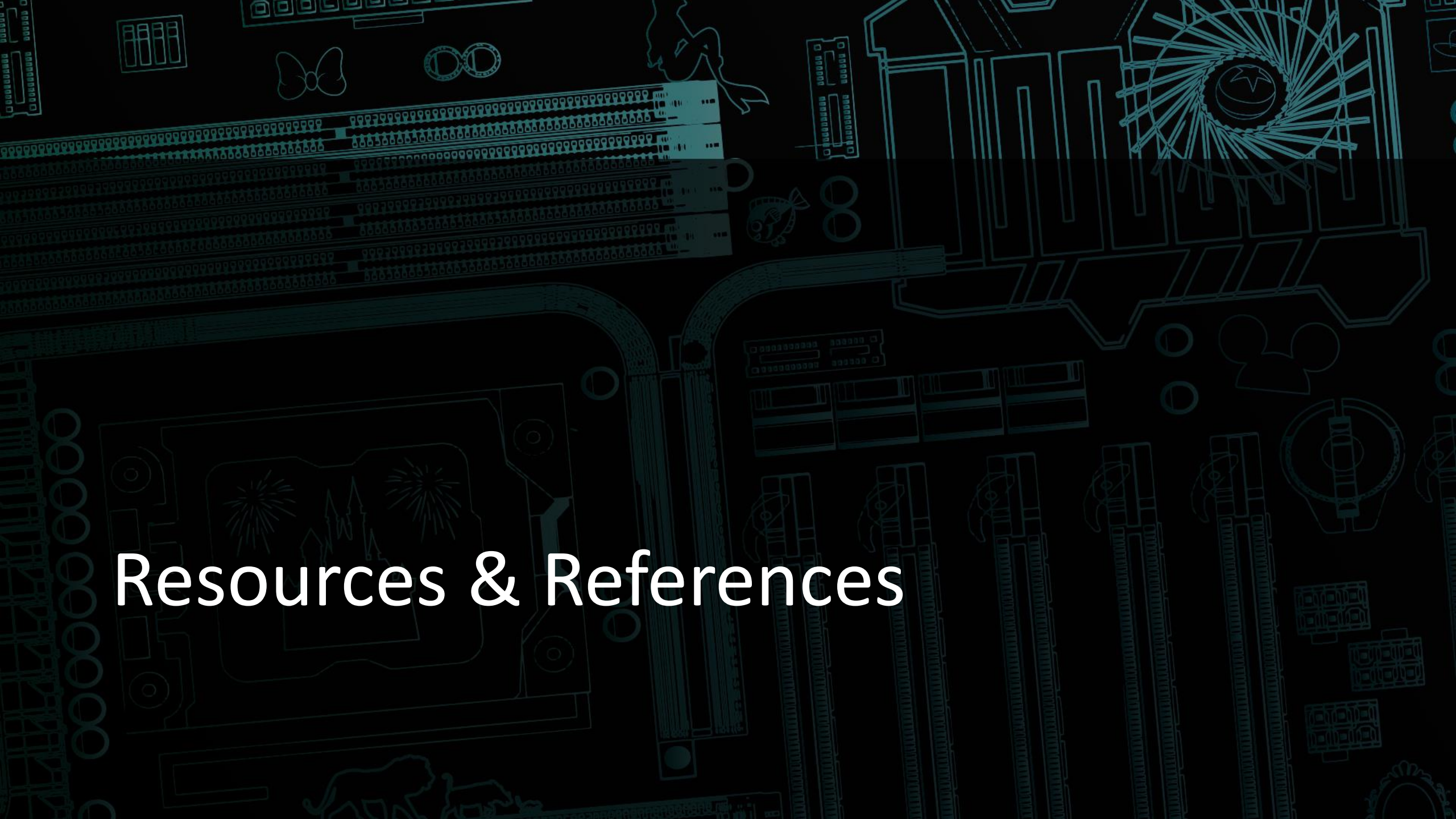
Figure 2: Sample CMF of a Hypothetical Electric Company

Ref - https://www.dragos.com/resources/webinar/using-a-collection-management-framework-for-ics-security-operations-and-incident-response/

Validate Technology with Penetration Testing

- The best way to validate use cases by testing it
- Creates rich data for Detection Engineering activities
- Build analyst confidence

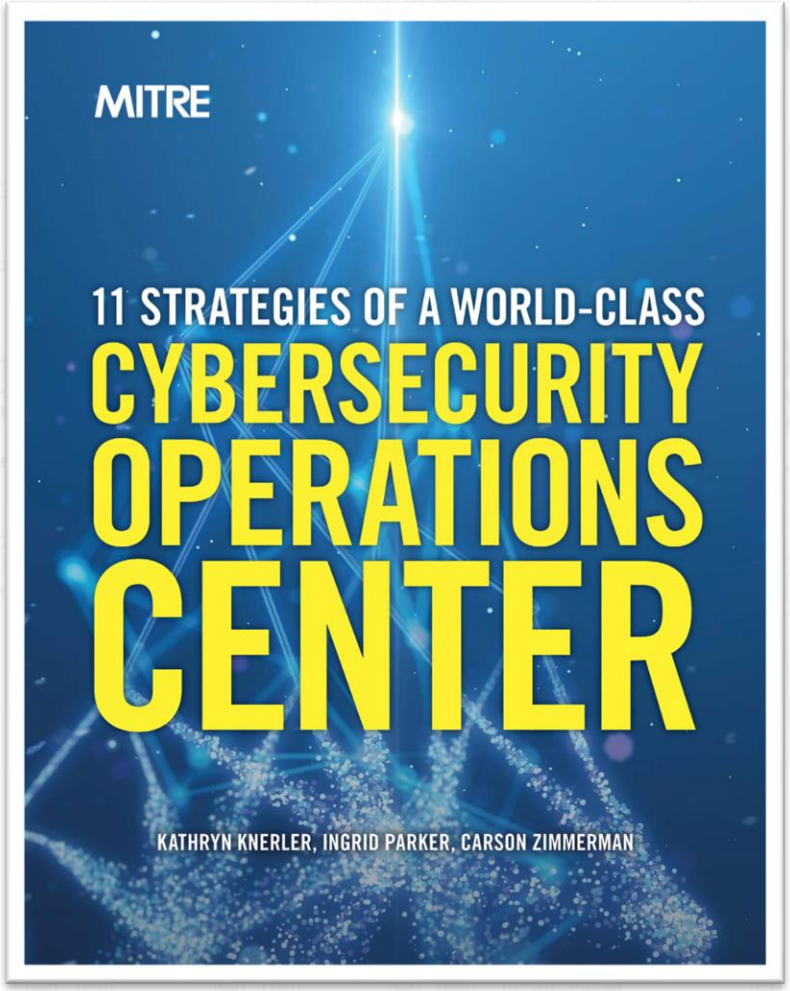




Resources & References

MITRE 11 Strategies for a World Class SOC

1. Know what you are protecting and why
2. Give the SOC Authority to do its job
3. Build a SOC structure to match your organizational needs
4. Hire and grow quality staff
5. Prioritise Incident Response
6. Illuminate adversaries with CTI
7. Select and collect the right data
8. Leverage tools to support analyst workflow
9. Communicate clearly, collaborate often, share generously
10. Measure performance to improve performance
11. Turn up the Volume by expanding SOC functionality



Ref - https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

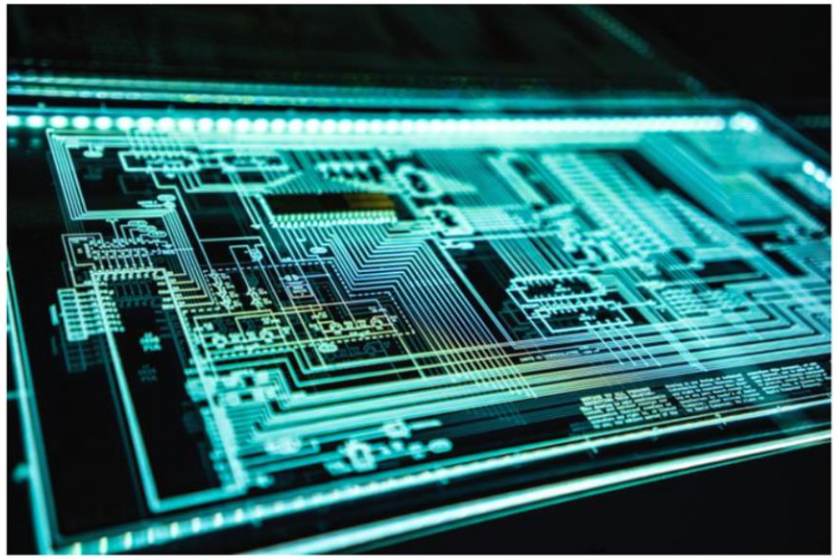
Building a Security Operations Centre - NCSC

GUIDANCE

Building a Security Operations Centre (SOC)

Guidance to help organisations design a SOC and security monitoring capability proportionate to the threat they face, their resources and assets.

Pages



Why have a Security Operations Centre?

Security Operations Centres (SOCs) can vary widely in scope, but most are responsible for detecting *and* responding to cyber attacks.

PUBLISHED
23 May 2022

REVIEWED
23 May 2022

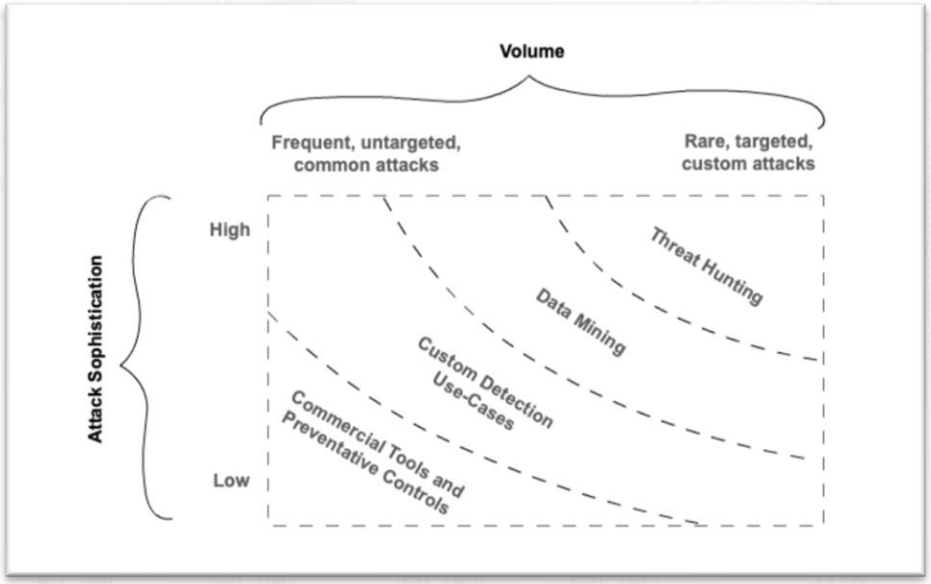
VERSION
1.0

WRITTEN FOR

"Must-have" logs

Before delving into the process of systematically identifying log sources, there are some quick wins for monitoring.

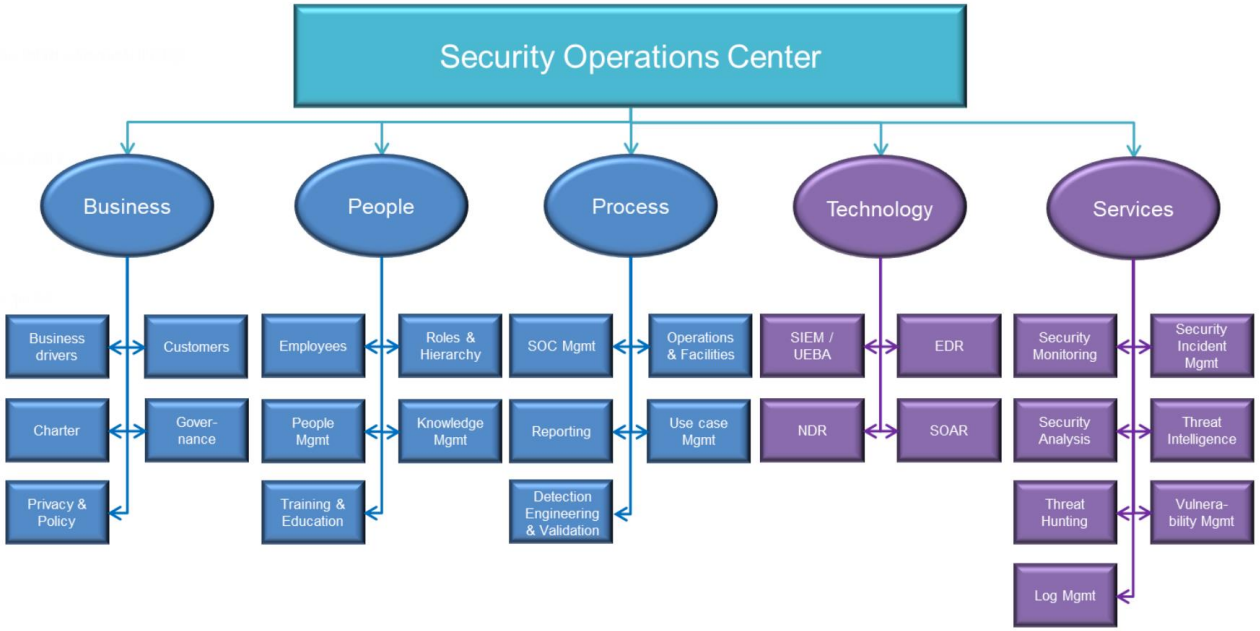
- **Authentication** - These logs will allow the SOC to identify where and when users logged onto a system - or attempted to logon to a system. These logs provide big red flags when adversaries attempt to gain unauthorised access to systems.
- **Security Controls** - This can include anti-malware software, security controls such as firewalls, access control list changes and anything that performs a security function within the organisation. Similarly to above, the logs provided by these controls are must haves as they will provide a first indication of something going wrong.
- **DNS** - These logs can be invaluable in identifying malicious behaviour within an organisation. An example could be "EUD123 has requested www[.]n0t-m4lw4re[.]com" - which may provide the first indications of a compromised device, allowing the SOC to intervene.

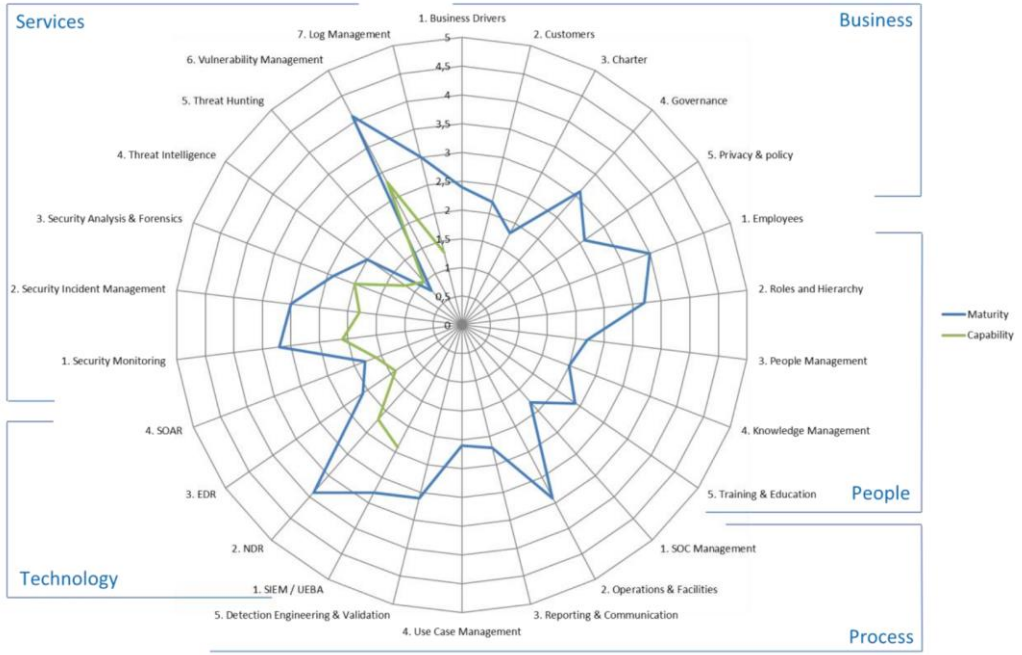


Ref - https://www.ncsc.gov.uk/collection/building-a-security-operations-centre

SOC-CMM

- Open source Project by Rob van Os
- Includes an Excel Assessment Toolkit

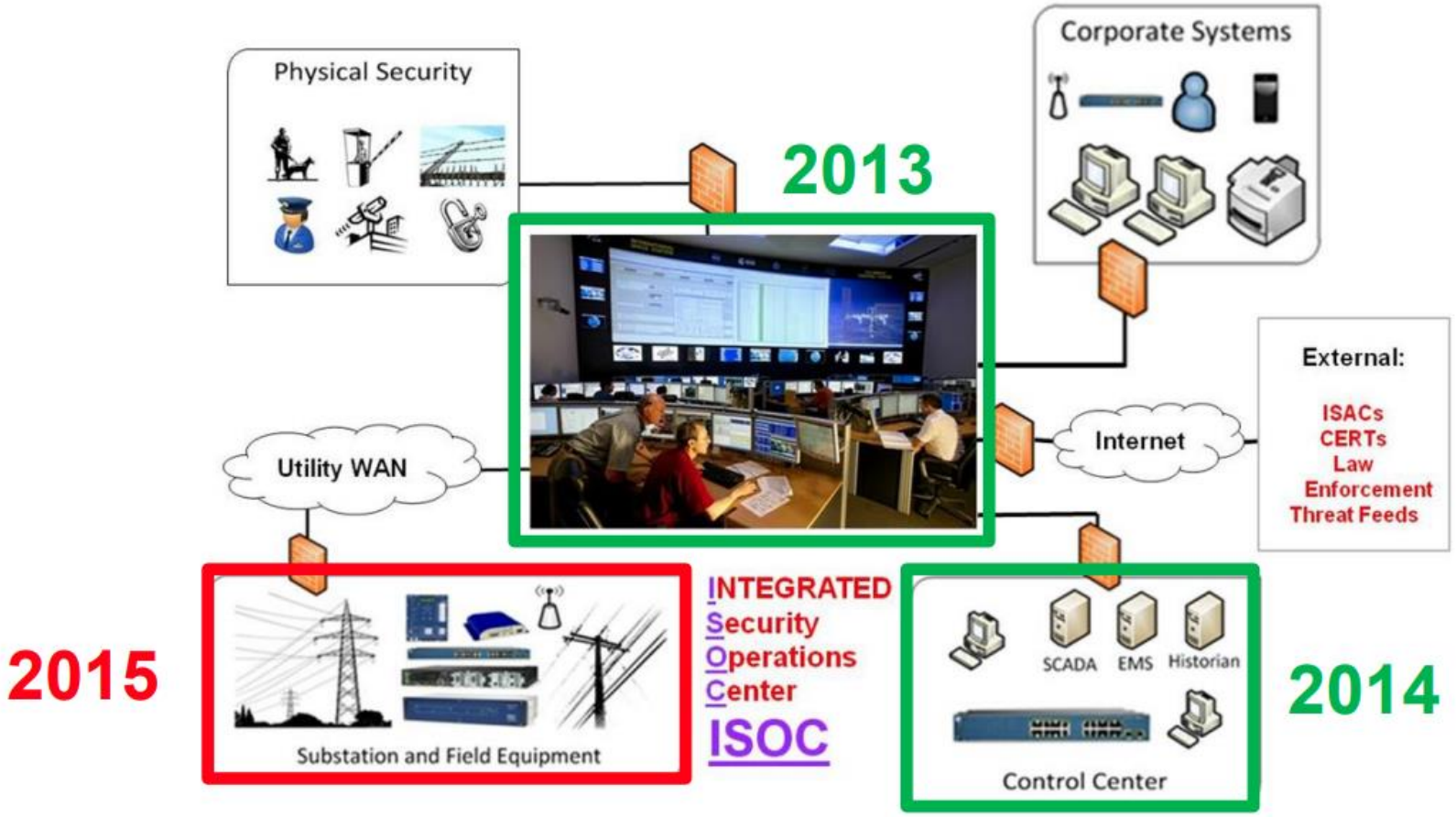




Ref - https://www.soc-cmm.com/downloads/soc-cmm%20whitepaper.pdf

EPRI Integrated SOC (iSOC)

- A great reference model if you an EPRI Member
- Combines:
  - Physical
  - Corporate
  - Control Centre
  - Field Networks



Ref - https://smartgrid.epri.com/doc/ICCS_Summit/C4.1_King_EPRI%20European%20Summit%20-%20Threat%20Management%20Presentation%20-%20Ralph%20King%20-%20FINAL.pdf

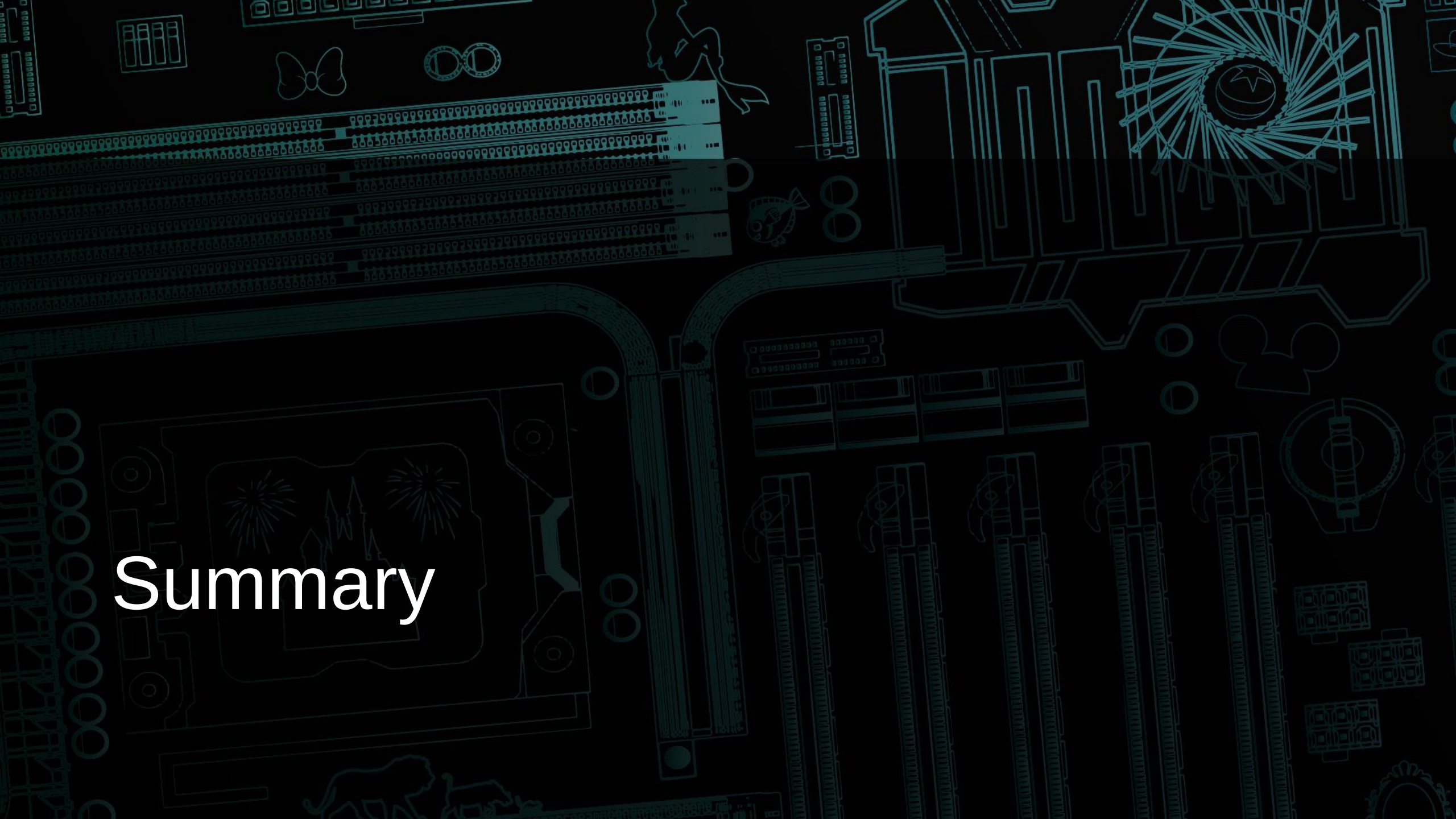
SANS Resources

LDR551 (GSOM)

1. SOC Design and Operational Planning
2. SOC Telemetry and Analysis
3. Attack Detection, Hunting and Triage
4. Incident Response
5. Metrics, Automation and Continuous Improvement

https://www.sans.org/cyber-security-courses/building-leading-security-operations-centers/

https://www.sans.org/podcasts/blueprint/



Summary

Summary

People

- **Be** an enabling leader
- **Guide** training in your team – don't dictate
- **Use** the SOC Human Capital Model
- **Focus** on developing team communication

Process

- **Develop** Mental Models
- **Use** Detection Engineering
- **Enable** Knowledge Management
- **Empower** with Metrics
- **Validate your capabilities** with Purple Teams

Tech

- **Start** with the OT DMZ
- **Deploy** Industrial NIDS
- **Develop** a CMF
- **Validate technology** with Penetration Testing

Thank you! Questions?


https://linkedin.com/in/blargeau


https://github.com/beLarge


@beLarge

SANS
ICS SECURITY
Summit & Training 2024