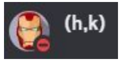
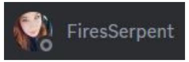
Fireside Fridays

Intro to secure architecture
Week 3

Thanks to our sponsors!

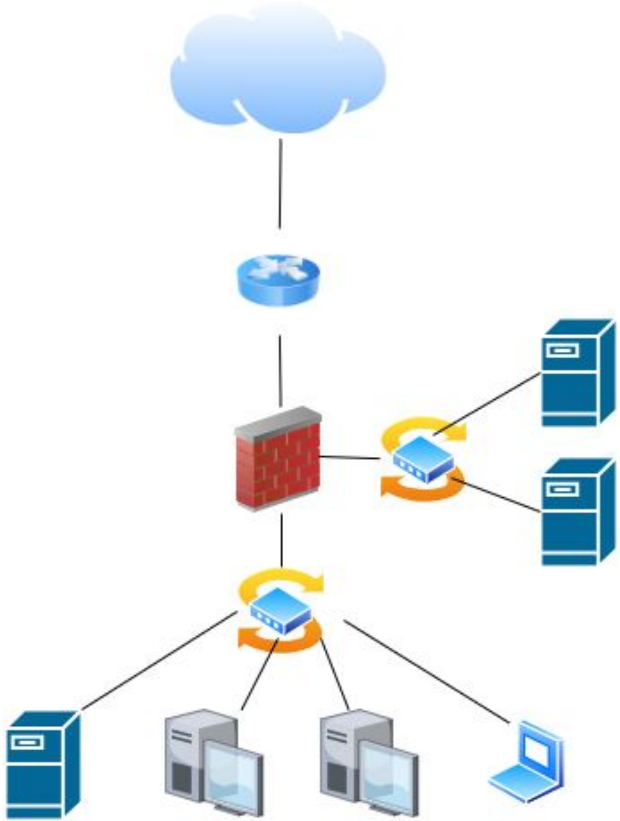
Special Thanks to…

- Hermon  (h,k)
- Emily  FiresSerpent
- Both gave up many late nights to help with QA and development of this content
- Very much appreciate their efforts!
- Please give them a warm "thanks" the next time you see them online

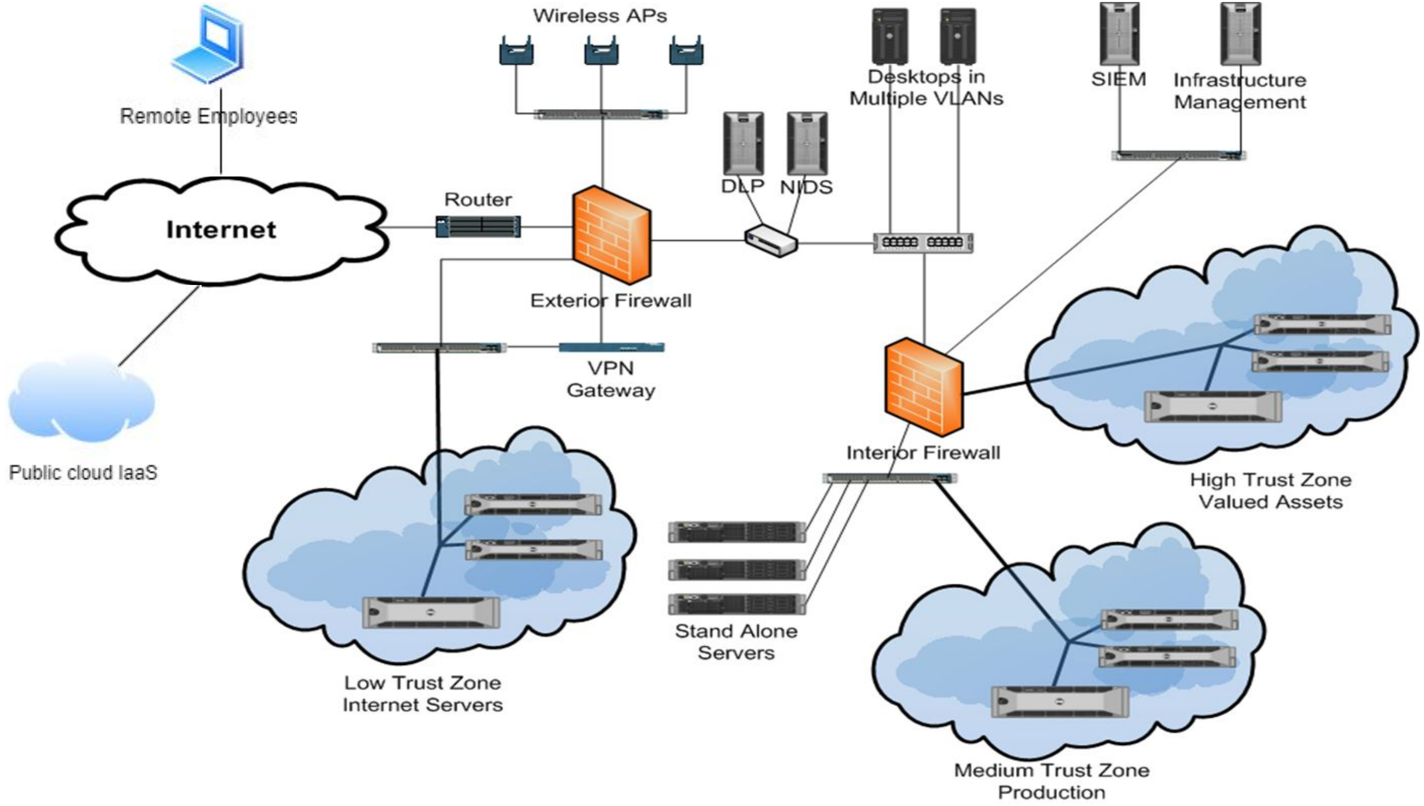
Lab requirements for this section

- No labs
- This section will be all lecture

This used to be easy…



Today things are far more complex…


Remote Employees
Wireless APs
Desktops in Multiple VLANs
SIEM
Infrastructure Management
DLP
NIDS
Internet
Router
Exterior Firewall
VPN Gateway
Public cloud IaaS
Interior Firewall
High Trust Zone Valued Assets
Low Trust Zone Internet Servers
Stand Alone Servers
Medium Trust Zone Production

Where do we start?

- The great pyramids were built one stone at a time…
- What connectivity is required to support the organization?
- What are the assets involved?
- What is the business value of each of the assets?
- What are the risks to those assets?
- How should these risks be managed?
- ***How will security be maintained?***
- A systematic approach is worth the investment

What is a systematic approach?

- Most security is grown ad-hoc
  - Throw tools at it as Gartner recommends
  - Or Reddit, or Quora, or Discord, or your buddies…
  - Solving short term pain, not necessarily long term problems
- Systematic approach starts with the last slide
  - Understand the requirements
  - Segregate assets into security zones
  - Don't forget about long term maintenance

"Trust" zones are dead

- Long live security zones
- If it has a CPU, it's potentially hostile, both outside and inside the perimeter
- Segregation of resources by zone
    - Permits management in groups
    - Simplifies policy and implementation
- Zones can/should also be segregated by asset value

Security zone example

- What can be said about on-prem users?
  - They need access to internal servers
  - They will access the Internet at large
  - Potential source of malware
  - Should not need to access each other's systems
- Collect users together and apply group policy
  - Block/monitor cross traffic
  - Monitor for command and control traffic
  - Apply behaviour analytics and verify deviations

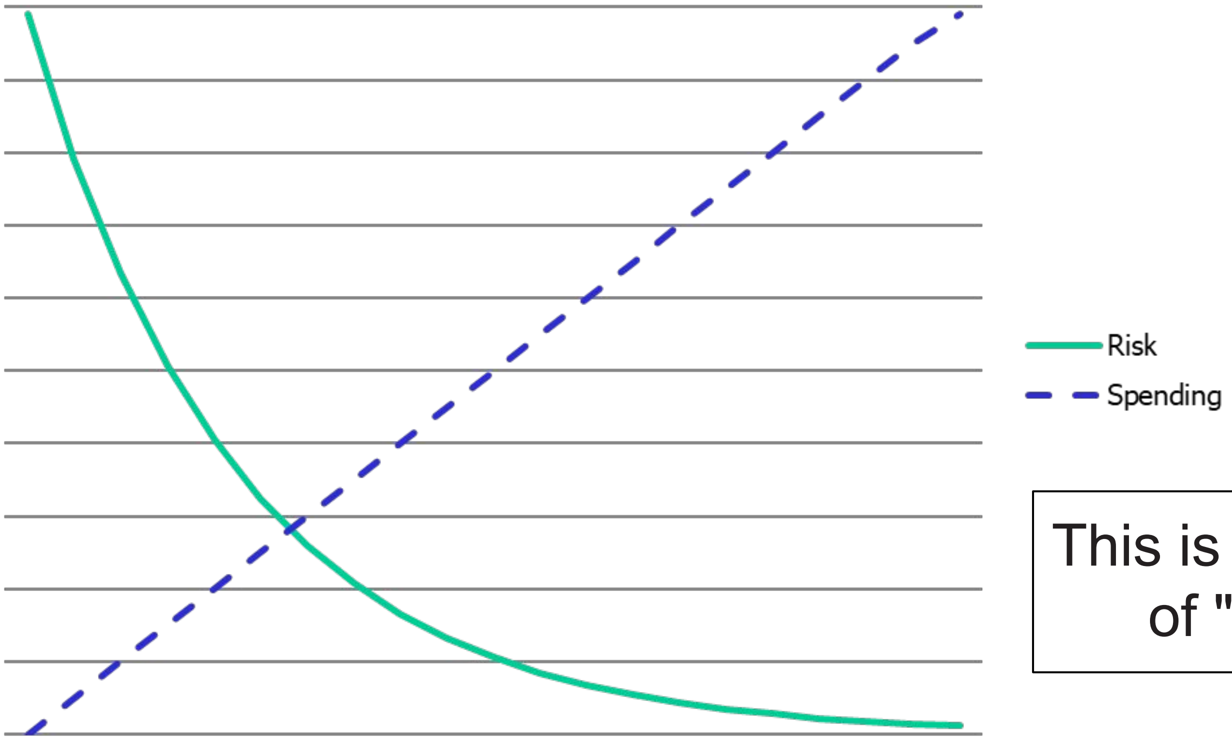
Security zones

- On-prem servers, internal or VPN access only
- On-prem users
- Internet accessible resources
- Public cloud resources
- Remote users
- The Internet at large

The importance of a test environment

- Changes need to be tested
- Misconfigured security can easily break things
- You don't want to learn in production
- A test environment is a requirement
    - Isolated portion of the org's network
    - Home lab
- Coding best practices apply equally to security

Diminishing return $$$ Vs risk mitigation



This is also true of "time"

Can we ever achieve absolute security?

- If the data center is a mile underground
- With self contained nuclear power
- All wrapped in a Faraday cage
- With no physical access
- Flamethrowers to prevent electromatic snooping
- Then maybe, possibly…
- Anything less requires the acceptance of risk

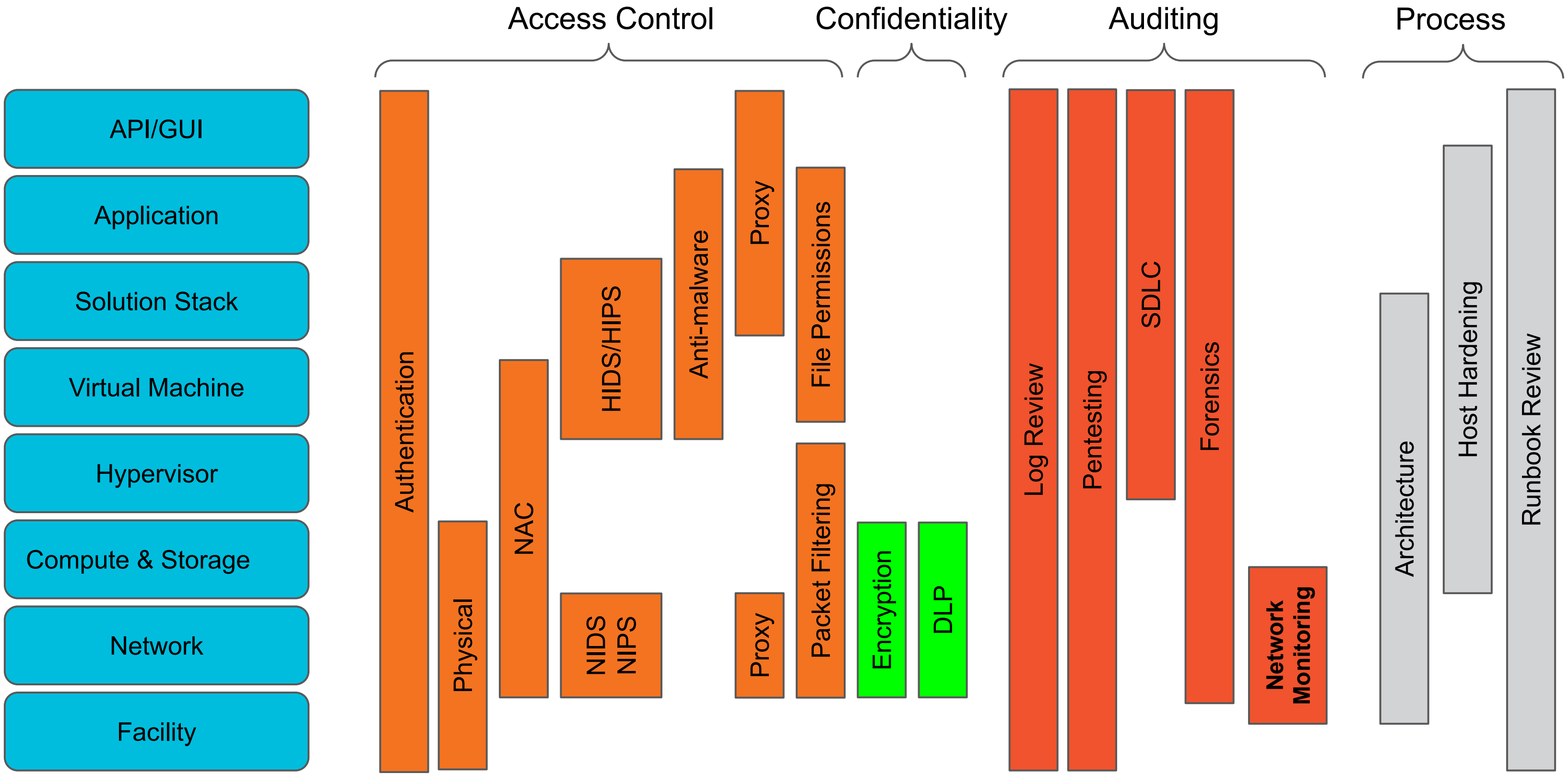
Handling threats

- How much risk do you really need to mitigate?
- Does it make more sense to:
  - Minimal spend on risk neutralization
  - Invest in detection and recovery
- Example (small numbers which are easy to process):
  - Asset value is $1 per day
  - $50 annual to mitigate a risk to near zero
  - $5 annual to implement early detection

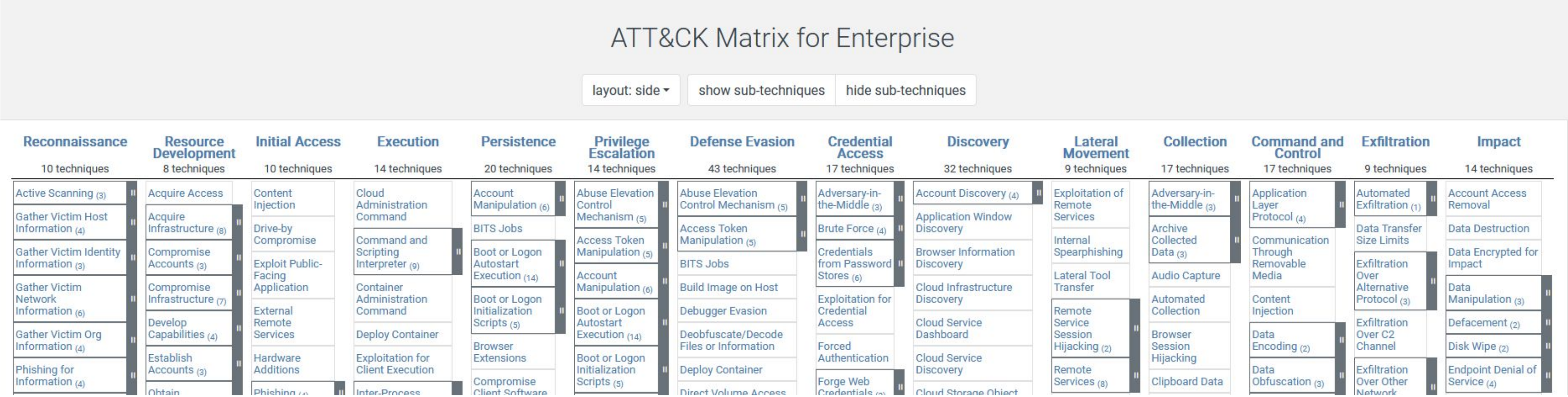
Security frameworks

- Can provide a holistic approach to security
    - PCI, HIPAA, FedRAMP
    - ISO 27001, SOC II
- Identify different elements where risk can be mitigated
    - Network
    - Authentication and access control
    - Vulnerability management
- Protection in layers
- Never invest solely in one security vertical
- More on this topic later

Work towards a layered defense



Another layered perspective



ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process	Compromise Client Software		Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery		Clipboard Data			Disk Wipe (2)
	Obtain					Deploy Container		Cloud Storage Object					Endpoint Denial of Service (4)
						Direct Volume Access							

https://attack.mitre.org/

Common initial threat vectors

- Phishing
- Known exploits not addressed
- 0-Day exploits
- Supply chain attacks
- Credential stuffing
- Malicious employee
- Improperly trained employee

Common threat objectives

- Ransomware
- Advanced Persistent Threat (APT)
  - For the purposes or theft
  - For the purposes of leveraging control
- Cryptomining
- Activism

# of studies ID "insider" as > threat

- Arguably the greatest number of security issues are generated within the org itself
- Misconfiguration or poor implementation due to:
  - Insufficient training
  - Deficient processes, documentation or audit controls
- Malicious insider
  - "Culture" can go a long way towards curing this
  - Take time to properly vet new hires

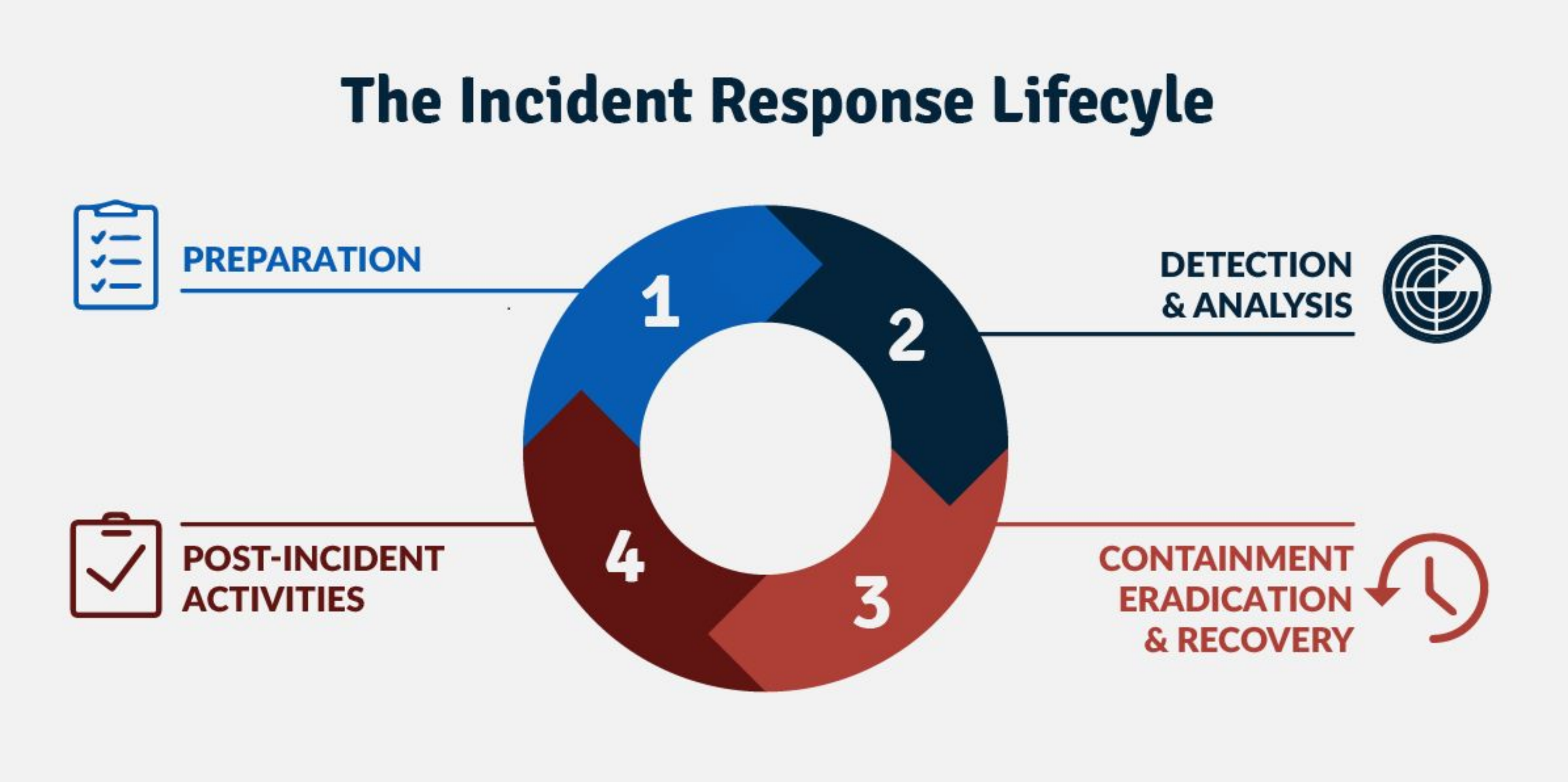
Incident handling/response, what is it?

- "Incident" = Event that can negatively impact an organization
    - Building fire
    - Attacker encrypts data making it inaccessible
    - Leaking of customer data
- "Incident Management" = Resolve and mitigate the impact of an identified incident
- Generic term but we'll focus on cyber

Blameless postmortem

- Examination of an event or process with the benefit of hindsight
- "Blameless" focuses on process, not people
    - "Bill screwed up" is an easy out
    - But is this an accurate root cause analysis?
    - Could "Sally" potentially do the same?
- How can we improve the process while accepting that people are fallible?
- Can be leveraged for incident handling or any other process

NIST incident response life cycle



The Incident Response Lifecyle

Goal on incident response cycle

- Continuous improvement
- Don't just ass-u-me your processes work, test them
- Both testing and real incidents should be leveraged to improve security posture
- 3rd parties can help generate unexpected vectors
- You should test this more frequently than you think

Wrap up

- Thank you for attending!
- Certs & video usually go out in 24 hours
- If you have any lingering questions, the Discord channel will remain active
  - Also a good chance to socialize with others in the class
  - Have other tips and tricks? Please share with others!
  - Posting screenshots can be helpful :-)