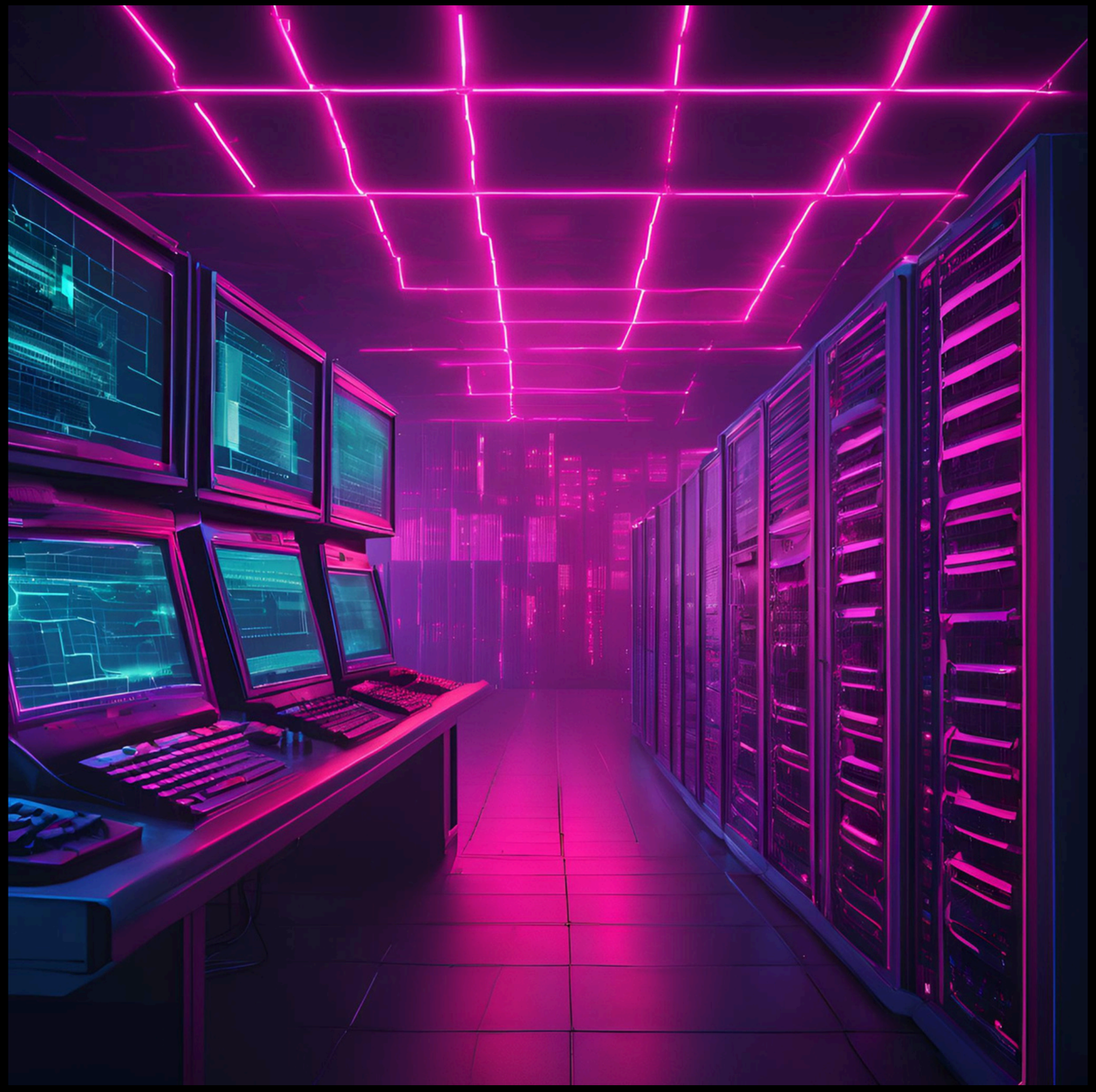
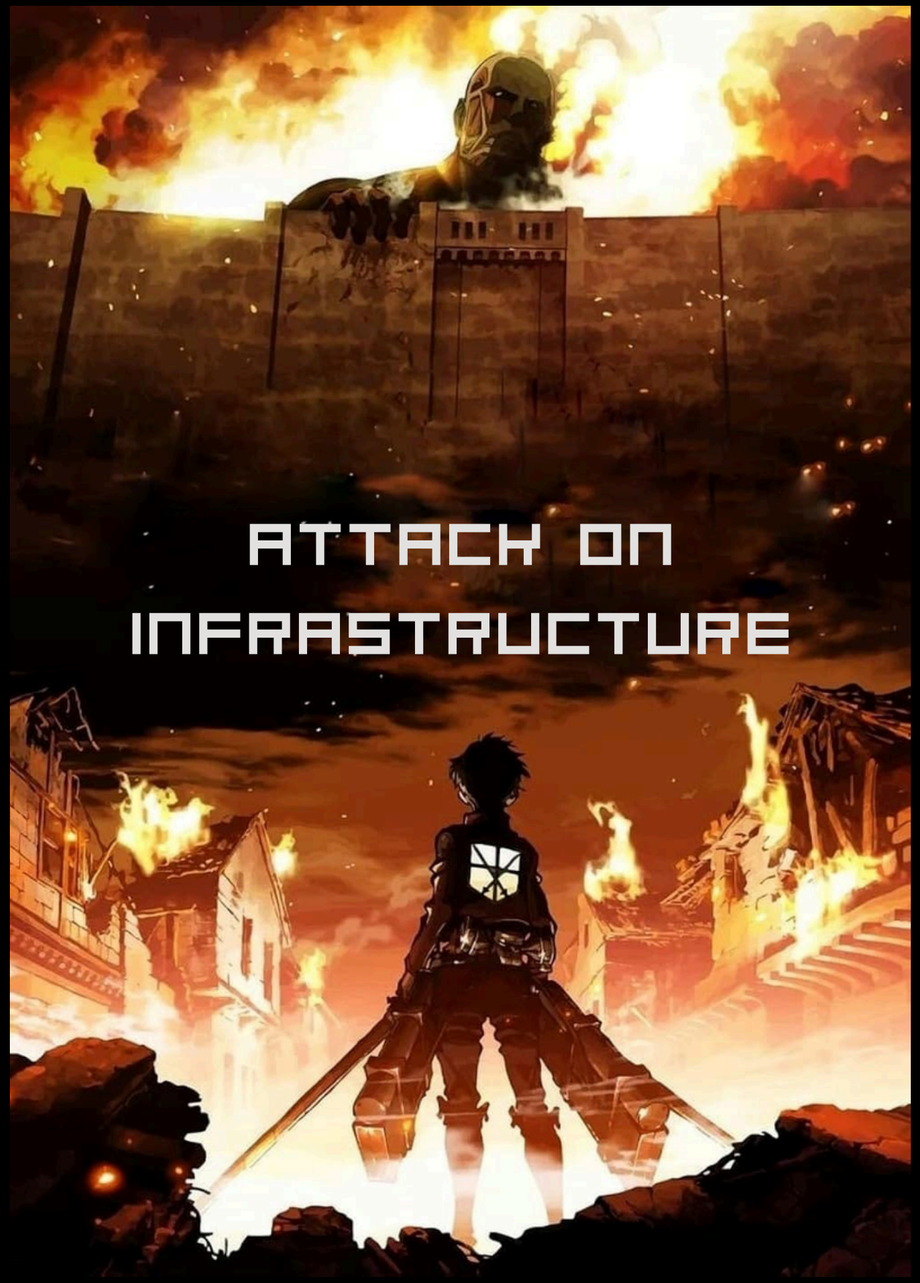


cyber673

INFRASTRUCTURE CYBER ATTACKS WITH TABLE TOP EXERCISE

28/05/2025



cyber673

ATTACK ON INFRASTRUCTURE WITH TABLE TOP EXERCISE

28/05/2025

cyber673


STAY SHARP
MUTHA PUAKA
PUNJABY DAWAT
madq pizza
KAERU THRIFT STORE
SAPPORO
Carlsberg
DENMARK
BLANC
DRAUGHT BEER
CARLSBERG/SAPPORO PINT
KRONENBOURG BLANC 1664 PINT
SAPPORO BLACK

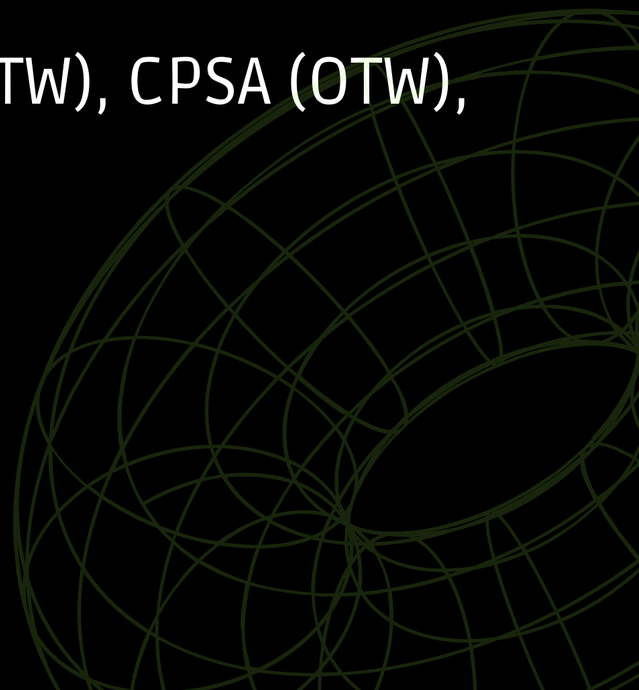
cyber673

WHOAMI

Red Team Engineer in Telecommunication Sector

CTF Enthusiast

CompTIA Security+, ITIL, SAL1, CC (OTW), CPSA (OTW), CISSP (OTW)



CRITICAL INFRASTRUCTURE TARGETS

cyber673

Energy Sector
Power grids, nuclear plants, oil & gas

Water Systems
Treatment plants, dams, distribution

Transportation
Railways, airports, traffic control

Healthcare
Hospitals, medical devices, records

Financial Systems
Banks, payment networks, markets

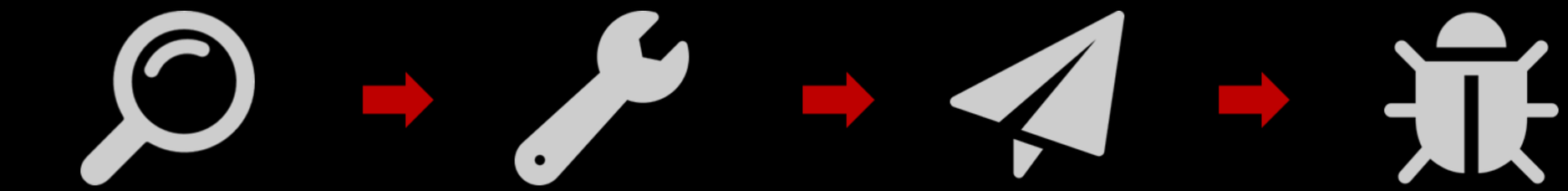
Telecommunications
Internet, mobile, satellite networks

Government
Defense systems, public services

Industrial Control
Manufacturing, SCADA, ICS

CYBER KILL CHAIN & ATTACK METHODS

cyber673



1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on objective

cyber673

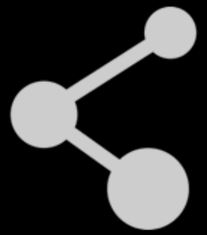
ATTACKER'S TTPs
Tactics, Techniques & Procedures

Initial Access
Techniques used to gain entry into infrastructure networks

Phishing, Stolen Credentials, Public Facing Applications, Supply Chain Compromises, Hardware Additions

Persistence
Methods to maintain access despite system restarts

Backdoor Implants, Boot/Logon Autostarts, Account Manipulation, External Remote Services, Valid Accounts



Lateral Movement
Techniques to move through and explore the network

Remote Services Exploitation, Internal Spearphishing, Pass-The-Hash/Ticket, Taint Shared Content, Lateral Tool Transfer

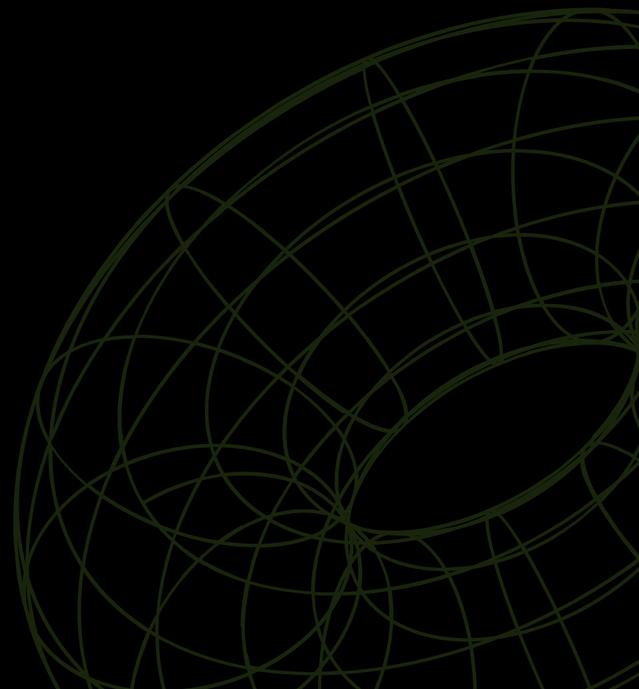
Impact & Execution
Final objectives and malicious actions executed against targets

Service Interruption, Data Manipulation, Safety System Tampering, Firmware Corruption, Resource Hijacking

cyber673

AGENDA

- Security Policy Framework
- Identify
- Protect
- Detect
- Respond
- Recover



cyber673

WHOAMI

Founder of Nitro Security (cybersecurity training for non-technicals).

Degree in Geography

Non-technical perspective of cybersecurity

CRTP, PWPA, PNPT, PJPT, eJPT, CySA+, Pentest+

scan here for free networking fundamentals

NITRO
NITRO
NITRO
NITRO
SECURITY

SECURITY CONTROLS

cyber673

APT

ADMINISTRATIVE

PHYSICAL

TECHNICAL

ADMINISTRATIVE

cyber673

Frameworks; ISO27001, NIST 800-53, COBIT, PCI-DSS

Policies

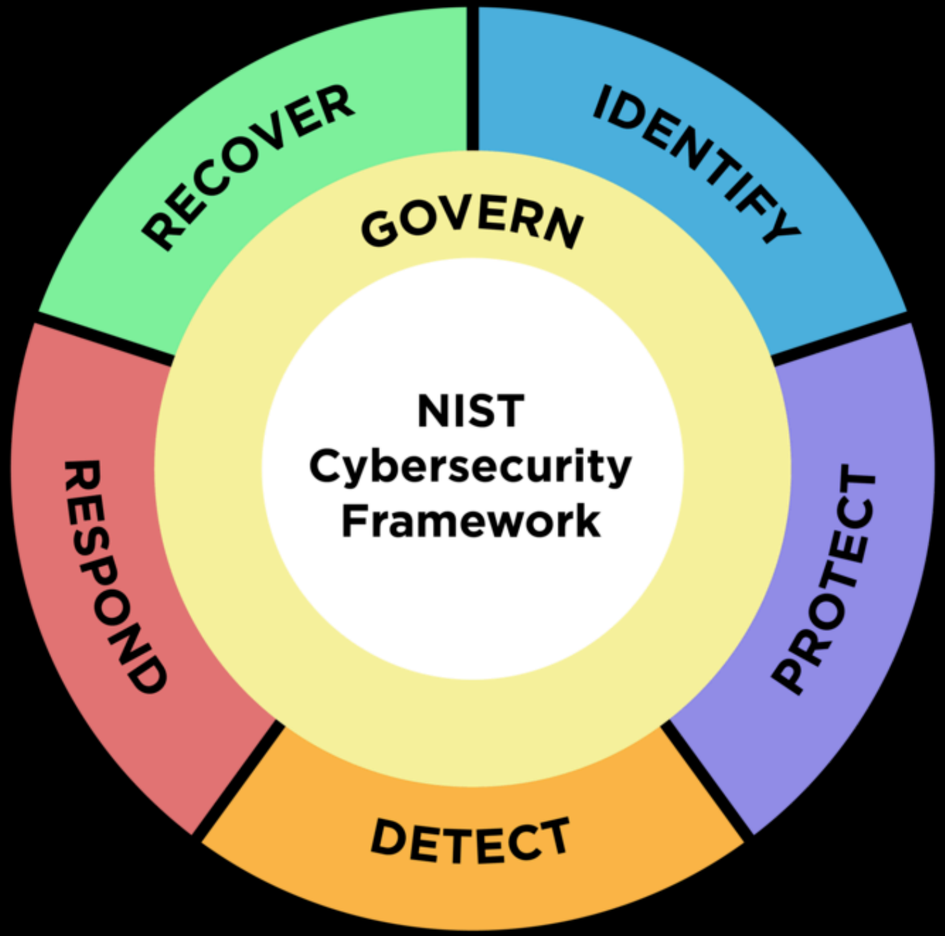
Standards

Procedures

Guidelines

NIST (National Intitute of Standards & Technology)

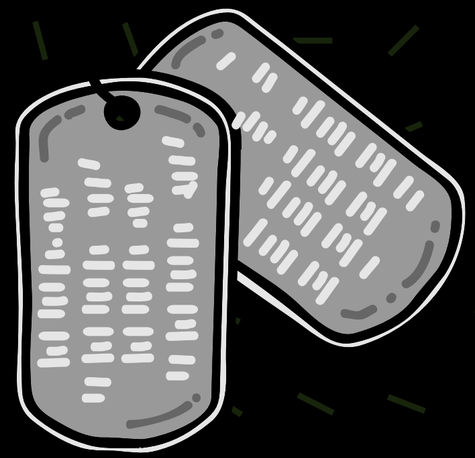
cyber673



https://www.nist.gov/cyberframework

identify - “what do I have?” cyber673

- Asset tagging, following a naming convention
  - Example:
    - Laptops: cyber673/LP/001, cyber673/LP/002
    - Servers: cyber673/SRV/001, cyber673/SRV/002
  -
- Inventory:
  - Name, IP Address, OS, Brand, State, Priority, Assigned to who?, etc



When there is a breach, your organization can easily identify & investigate (what, where, when, why, how).

protect – “am I prepared?”

cyber673

- From your inventory, which of those assets:
  - Have software vulnerabilities?
  - Hardware warranty?
  - Maintenance support?
  - Propert patching schedule?

- Access control
  - Privileged access, role-based, discretionary, mandatory

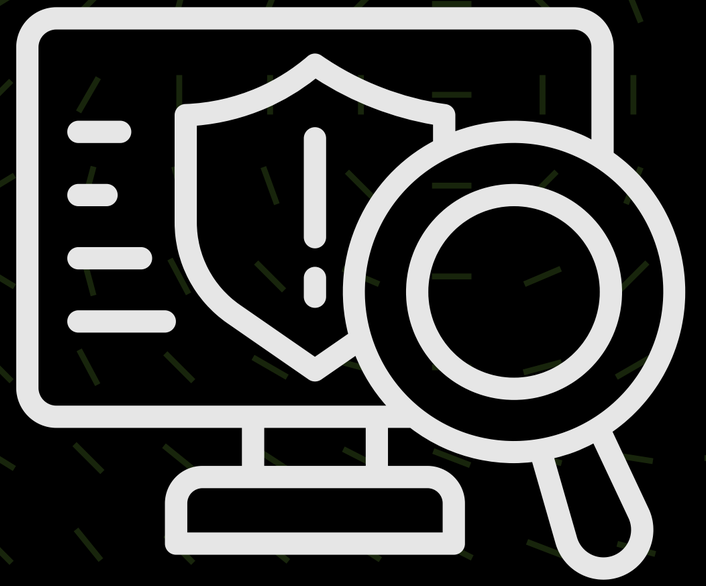
Attackers will always look for vulnerabilities such as zero day.
If access control is not in place, anybody can have access.

detect - “can i see?”

cyber673

- Monitoring tools to detect to the following:
  - Abnormal network traffic
  - Malware installation
  - New vulnerabilities
  - Alert/notify IT Security Team

- Log Analysis:
  - Name, IP Address, OS, Brand, State, Priority, Assigned to who?, Source, destination



When an attack occurs, how are you notified? Attackers can counter this by using different ports, anti-virus evasion techniques

respond - “stop the bleeding!” cyber673

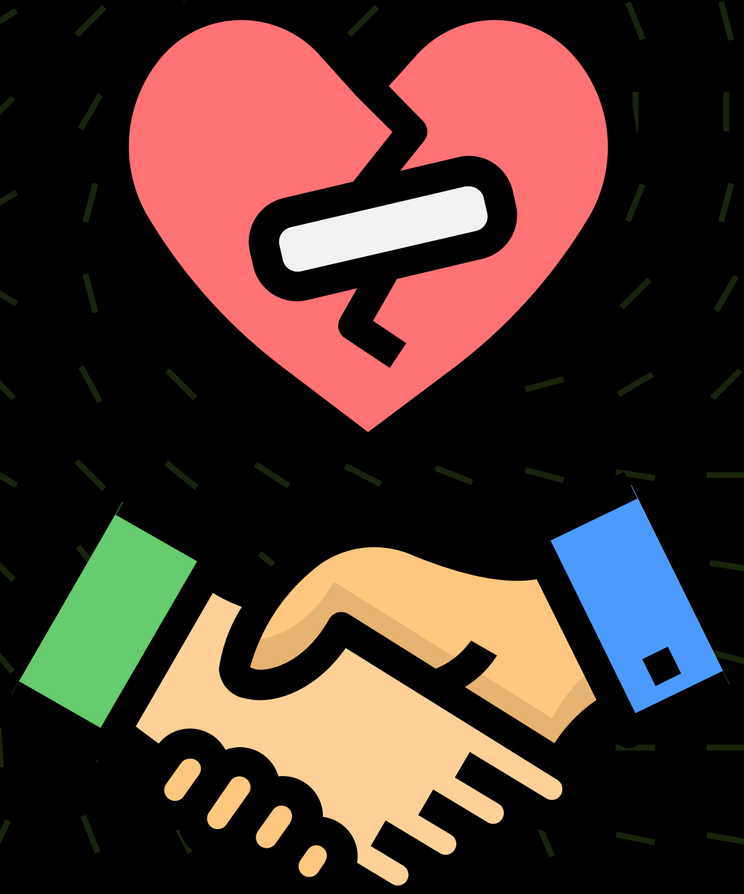
- Incident response, table top exercises, scenario & role-based incident response exercises
- Segmentation, isolating the malware, malware analysis
- Incident communications & reporting

Similar to fire-drill exercises, are people in your organization prepared what to do?

recover – “healing”

cyber673

- Lessons learned
- Recovering files from backups
- Zero Trust Policy



When will it happen again?

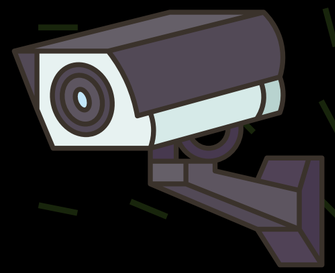
NIST at home

cyber673

Identify

Prepare

Detect



Respond

Recover

cyber673

cyber673

cyber673

WHOAMI

- Rabbani
- Cyber security enthusiast
- MSc in Cyber Security
- 2.5 + years experience in cyber security
- Maybe just here for pizza but also Im on a diet

Incident Response

cyber673

What counts as an security Incident?

- An event
- Has impact
- Org need to respond and potentially recover

What is Incident response?

- A process for detecting, analyzing, and responding to security incidents
- To mitigate the impact
- To recover from incident

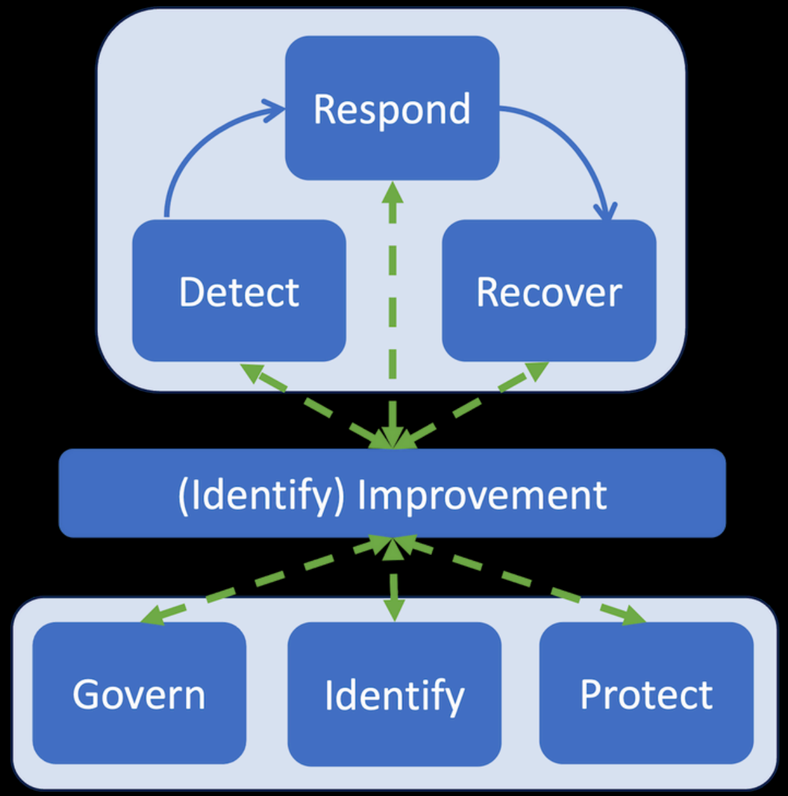
NIST - Incident Response

cyber673

Incident Response ->

Lessons Learned ->

Preparation ->



Detect

cyber673

- Monitoring and analysis activities to find and characterize potentially harmful events.

- Example:
  - Set up monitoring system to check malicious emails coming into your org.
  - Detecting a phishing email from a fake amazon sender.
  - Detecting malicious URLs in the email body content.
  - Detecting malicious PDF files in the email attachment.

Respond

cyber673

- Actions taken after a detected cybersecurity incident.
- Example:
  - Inform email recipient not to open anything (URLs and attachment).
  - Find out why the URLs and attachments were marked as malicious.
  - Block malicious URLs and attachments.
  - Scan user computer (just in case).
  - User reported did not click malicious URL or open pdf, but LIED. Now monitoring system is picking up some activities.
  - We have to isolate the device to contain threat and remove account access.
  - Find and remove threat (malware or unauthorised user account).

NIST - Incident Response - Recover

cyber673

- Assets and operations affected by a cybersecurity incident are restored.
- Example:
  - Restore system from backup or install a new system.
  - Make configuration stronger.
  - Patch vulnerabilities.
  - Reset password then grant access back to user.

cyber673

THANK YOU!

GET YOUR FREE CYBER673 STICKERS!

HTTPS://CYBER673.COM