



# Pheno Security Management

Soc Hackathon 2023

Paul Clark

# Currently:

Zeek

MISP

Elastic

- Filebeat for log movement
- Auditbeat

Kibana

Shared-F2B

Vuls

HIDS

DITO

- Trial
- HUB

# ZEEK

Worked wonderfully.... Until we went 40gb

Currently up but we experience high percentage of packet loss.

Planning to redesign with new hardware including:

- Bluefield 1 Test – Free time may arrive
- Optical Taps
- Spread the load using older Lenovo nodes (High CPU/Memory, 8 to a chassis).

# MISP

- RPM Build on C7 – Looking to migrate/containerize
- Variety of Threat sources
  - TOR
  - Shared-F2B
  - CIRCL
- Still not yet linked to STFC/CERN instance due to poor communication on our part
- Currently in Maintenance mode due to Zeek refresh
- Integrate with Hiveproject

# ELASTIC - Current

- 3x Elastic nodes
- 1x Master, 2x Data
- Large amounts of data, mixed use between security/Grid which isn't great.
- Kibana for sweet sweet visuals
- Filebeat for log movement
- Auditbeat for Endpoints
  - Not a HID but will show individual user commands/filter against certain commands.

# Elastic - Future

---

Rebuild/Redesign

---

Opensearch looking attractive

---

If funding available purchase new elastic nodes, older elastic nodes becoming cold storage.

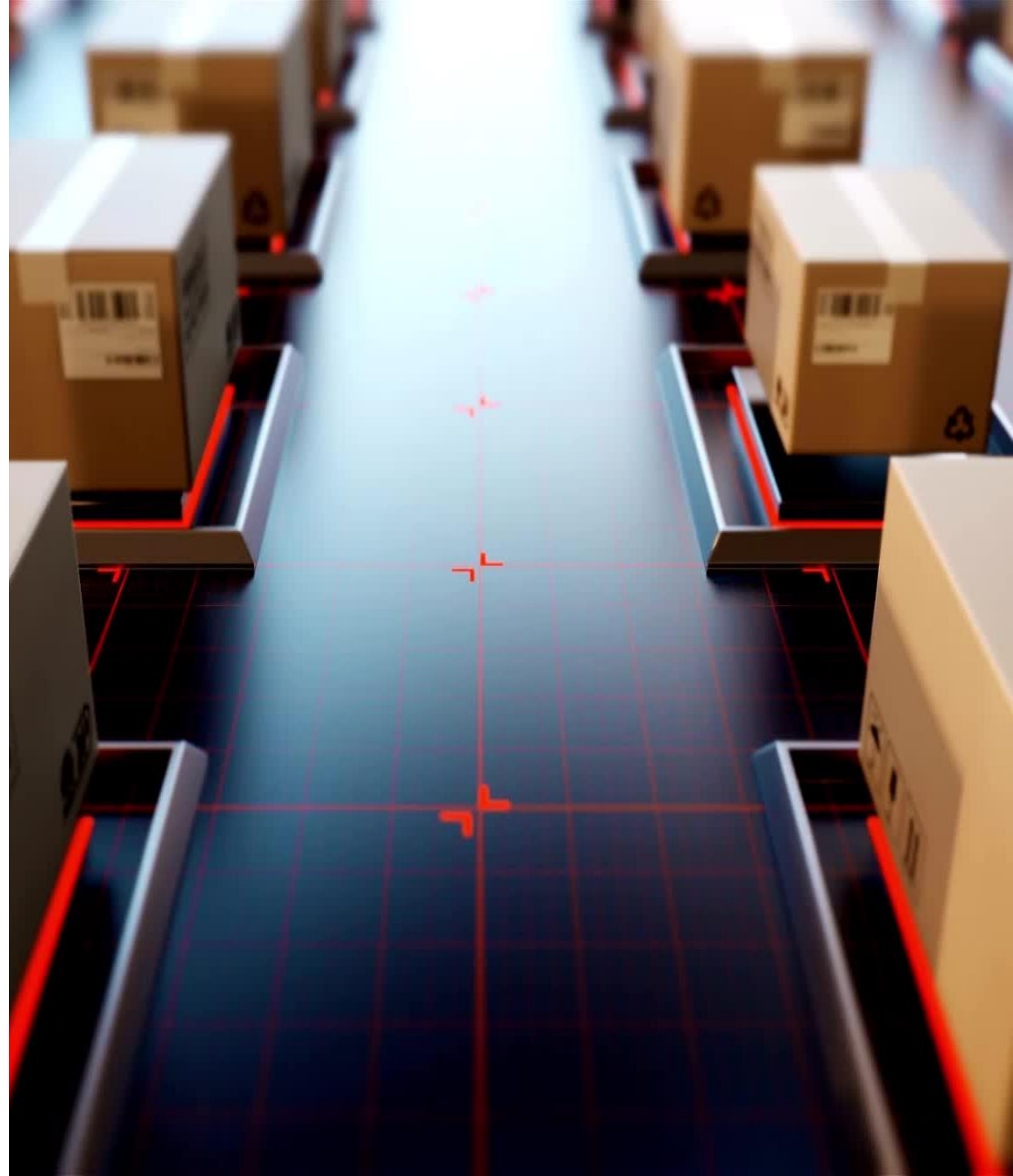
---

Need to test opensearch for close feature match such as log movement



# Shard-F2B

- Persistent operation
  - Grid
  - IPPP
  - Wider Physics Planned
- No Further core feature updates planned



# Vuls

- Features of Note
- Scanning attributes from a number of sources
- Fast non Privilege scan or Root Scan
- Offline Scans
- Push results to server, no requirement for server to login

Basic Webui (Vupsrepo) or email notifications/reports

Linux support

<https://vuls.io>



# Local Setup

- Central Vuls server within IPPP
- Clients push to server
- Sources
  - NVD
  - ExploitDB
  - OVAL – Redhat Daily feed

```

[ 1] CVE-2014-9939 | 9.8 | AV:N | | | unfixed | binutils
[ 2] CVE-2015-4042 | 9.8 | AV:N | POC | | unfixed | coreutils
[ 3] CVE-2023-38408 | 9.8 | AV:N | POC | | fixed | openssh, openssh
[ 4] CVE-2023-38403 | 8.9 | AV:N | | | fixed | iperf3
[ 5] CVE-2022-42896 | 8.8 | AV:A | | | unfixed | kernel
[ 6] CVE-2015-8982 | 8.1 | AV:L | | | unfixed | glibc
[ 7] CVE-2015-8983 | 8.1 | AV:N | | | unfixed | glibc
[ 8] CVE-2023-31484 | 8.1 | AV:N | POC | | unfixed | perl
[ 9] CVE-2023-35788 | 8.1 | AV:L | POC | | unfixed | kernel
[10] CVE-2014-9622 | 7.8 | AV:N | POC | | unfixed | xdg-utils
[11] CVE-2015-4041 | 7.8 | AV:L | POC | | unfixed | coreutils
[12] CVE-2016-10044 | 7.8 | AV:L | | | unfixed | kernel
    
```

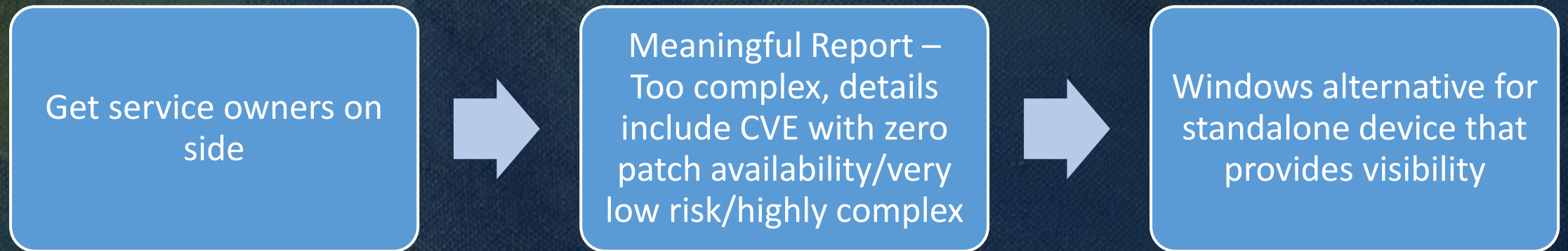
```

Affected Packages, Processes
=====
* binutils-2.27-44.base.el7_9.1 -> Affected

Cyber Threat Intelligence
=====
MITRE ATT&CK:

CAPEC:
* CAPEC-100: Overflow Buffers
* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-123: Buffer Manipulation
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-42: MIME Conversion
* CAPEC-44: Overflow Binary Resource File
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities
    
```

# Vuls – To work on



# Host Based Intrusion Detection (HIDS)

Current implementation a mix between:

- Auditbeat
- Legacy OSSEC

Moving Forward:

- Auditbeat will retire with elastic
- Ossec vs Wazuh – Faceoff testing

# End Goals - Buzz buzz buzz words

Anticipate

Identify

Protect

Detect

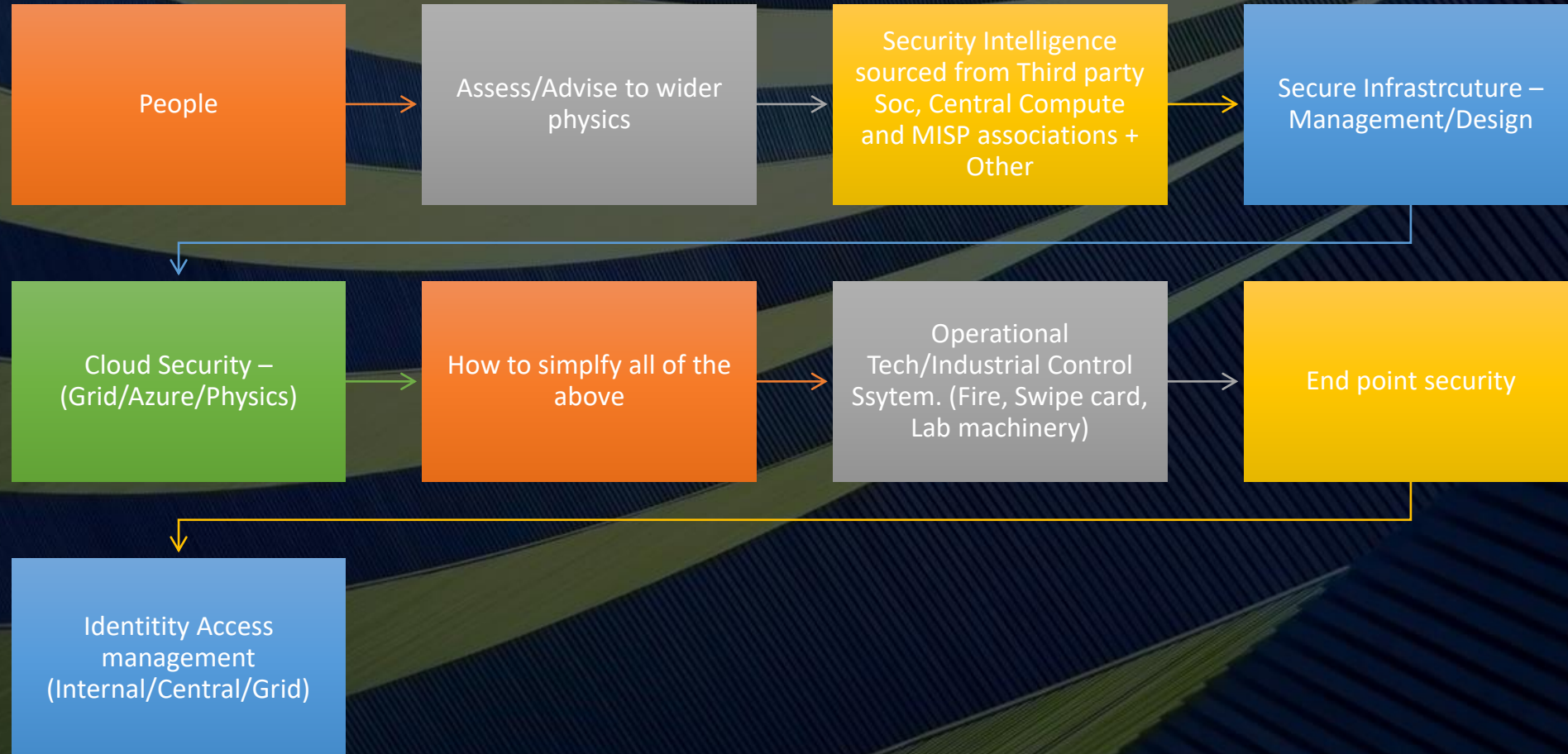
Alerts/Anomaly Detection

Respond

- Containment
- Remediation



# Boxes to tick





# DITO – Freedom at what cost

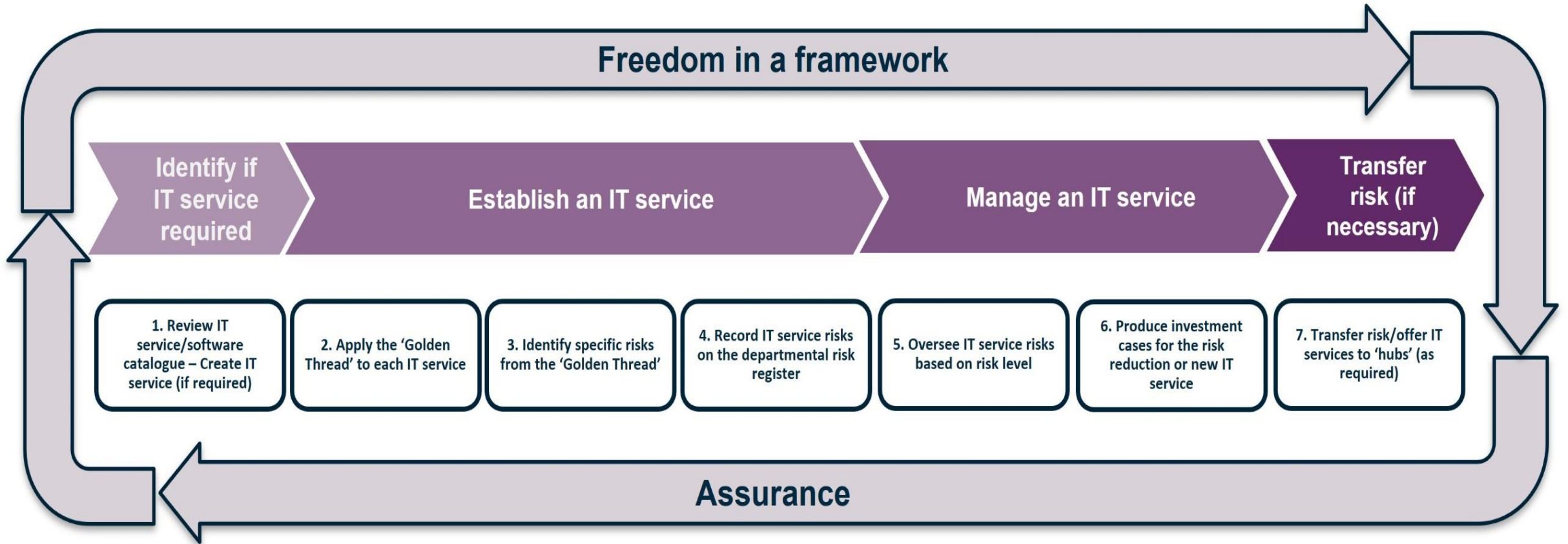
- Core framework integration using the term “Golden Thread”
- DITO (Durham IT Operations) Governance group
  - Academics
  - Corporate
  - IT

Provides oversight to departmental IT decision making that goes against standard corporate policy.
- NIST framework heavily condensed to make it more manageable to end users.
- Roughly 100 Rules





# DITO – Framework



# Local to Core Communication

---

- Communication External to DITO
- Access to Third Party SOC – Helped Tender
  - Some sort of view planned for DITO members however expect this to take a long time and be heavily restricted in terms of view
- Reporting of known CVEs  
Working with security teams for testing purposes:  
Example:
  - Papercut
  - Zenbleed
  - etc



Questions?

