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

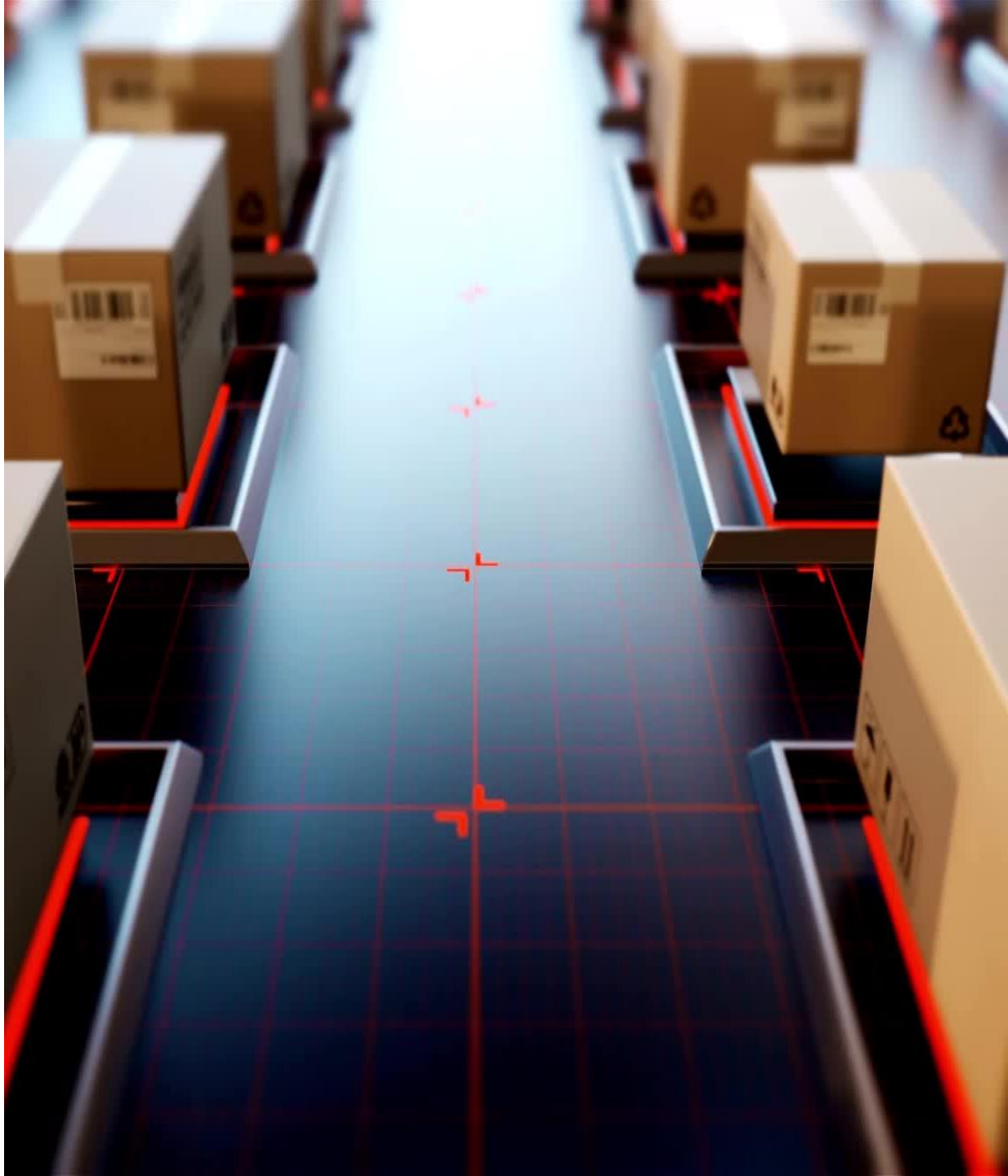
If funding available purchase new elastic nodes, older elastic nodes becoming cold storage.

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

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

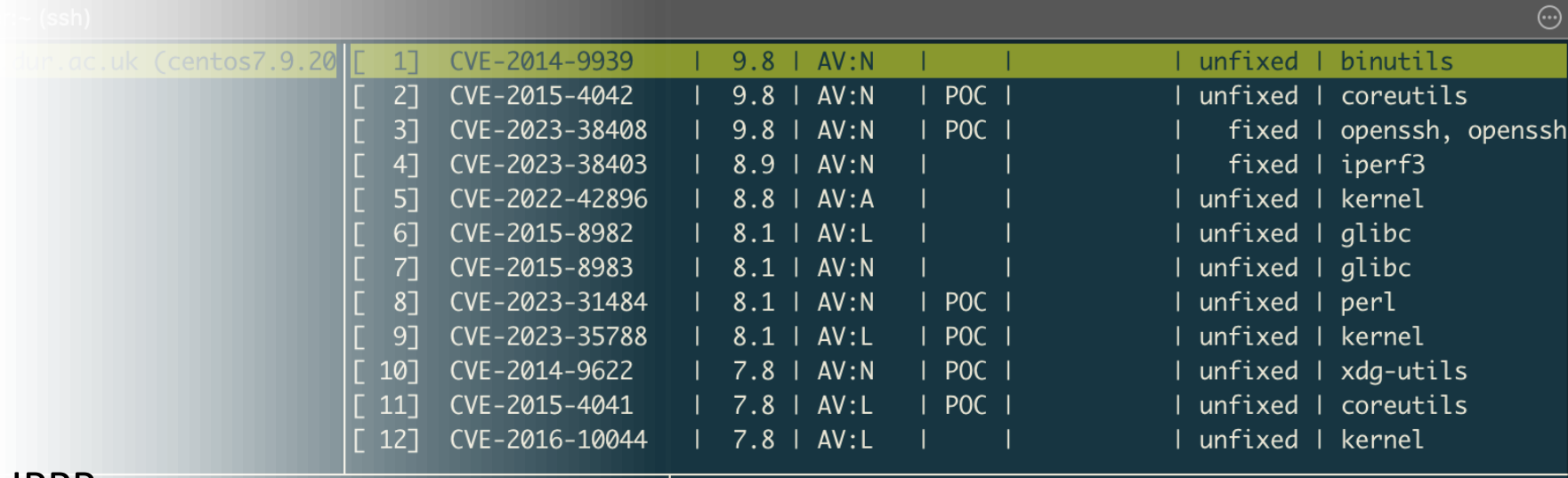
Basic Webui (Vupsrepo) or email notifications/reports

Linux support

https://vuls.io

Local Setup

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



Vuls – To work on

Get service owners on side

Meaningful Report – Too complex, details include CVE with zero patch availability/very low risk/highly complex

Windows alternative for standalone device that provides visibility

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

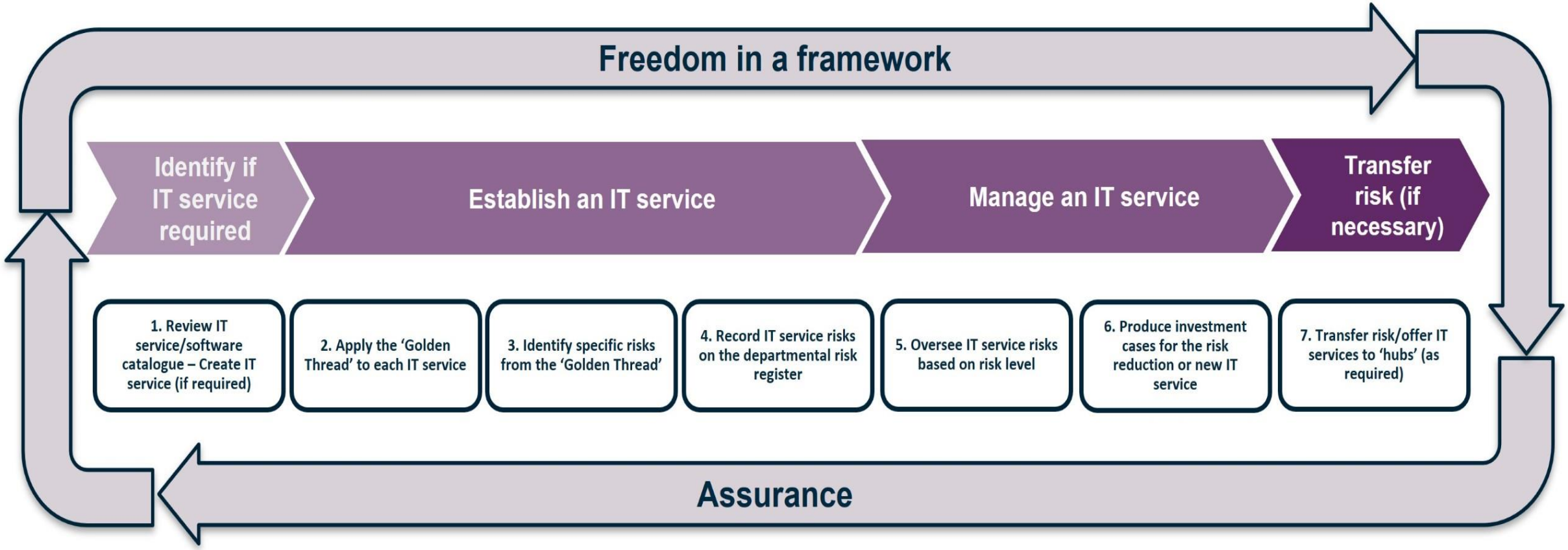
Boxes to tick

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?