Hewlett Packard
Enterprise

Pragmatic Security Audits
Fortifying HPC Environments at a Consumable Pace

Dennis Walker, HPE
Alden Stradling, LANL
Monica Dessouky, HPE

May 4th, 2025

Agenda

Level-set: Why security matters, what's in an audit

Structured Scanning

Security Scanning Tools

Threat Modeling

Simplifying Analysis

DevSecOps Automation

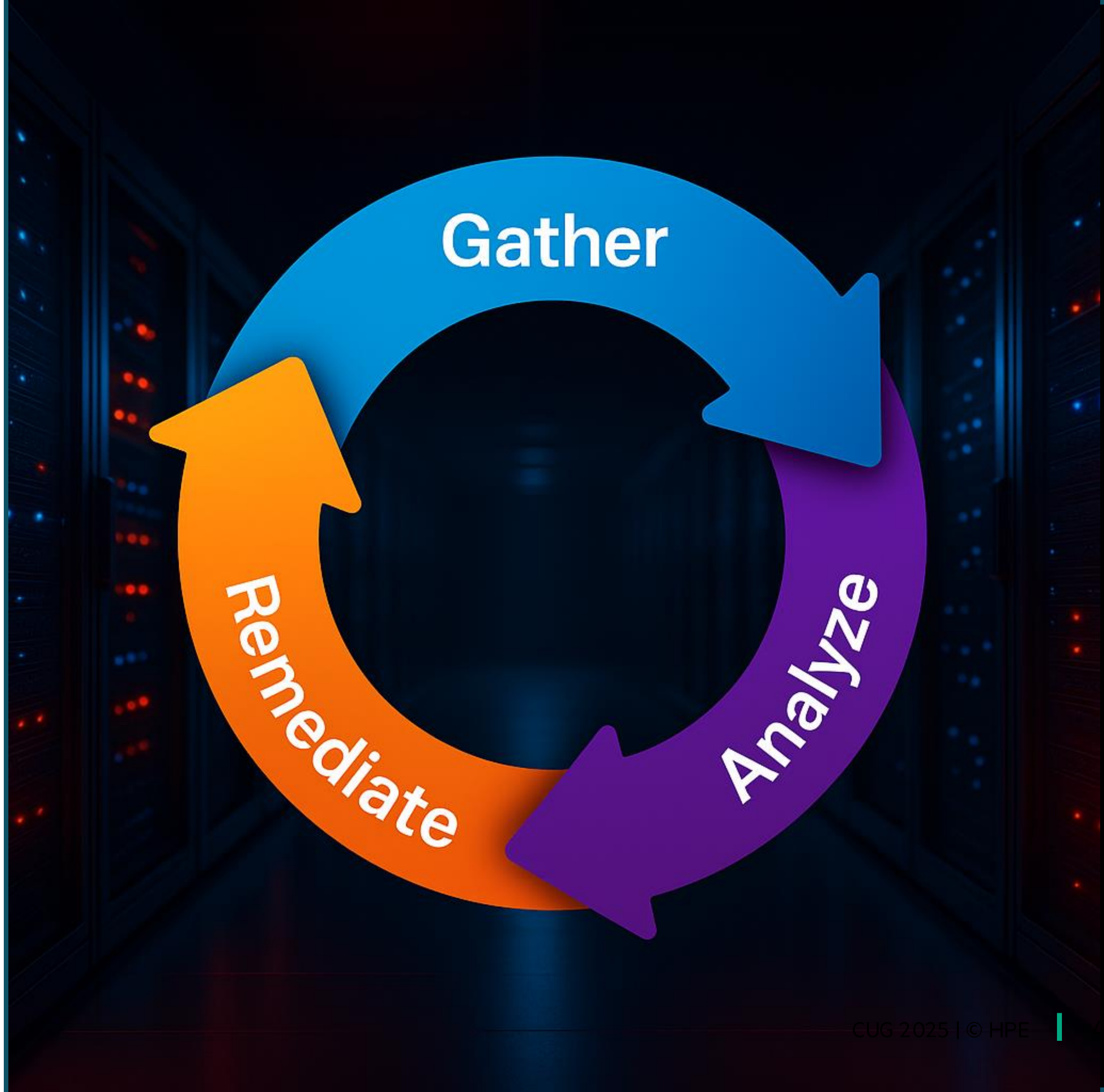
Why Security Matters?

- Breaches incur lengthy recovery downtime
- HPC Data is often the most sensitive
- Result must be true

Security Audit Overview

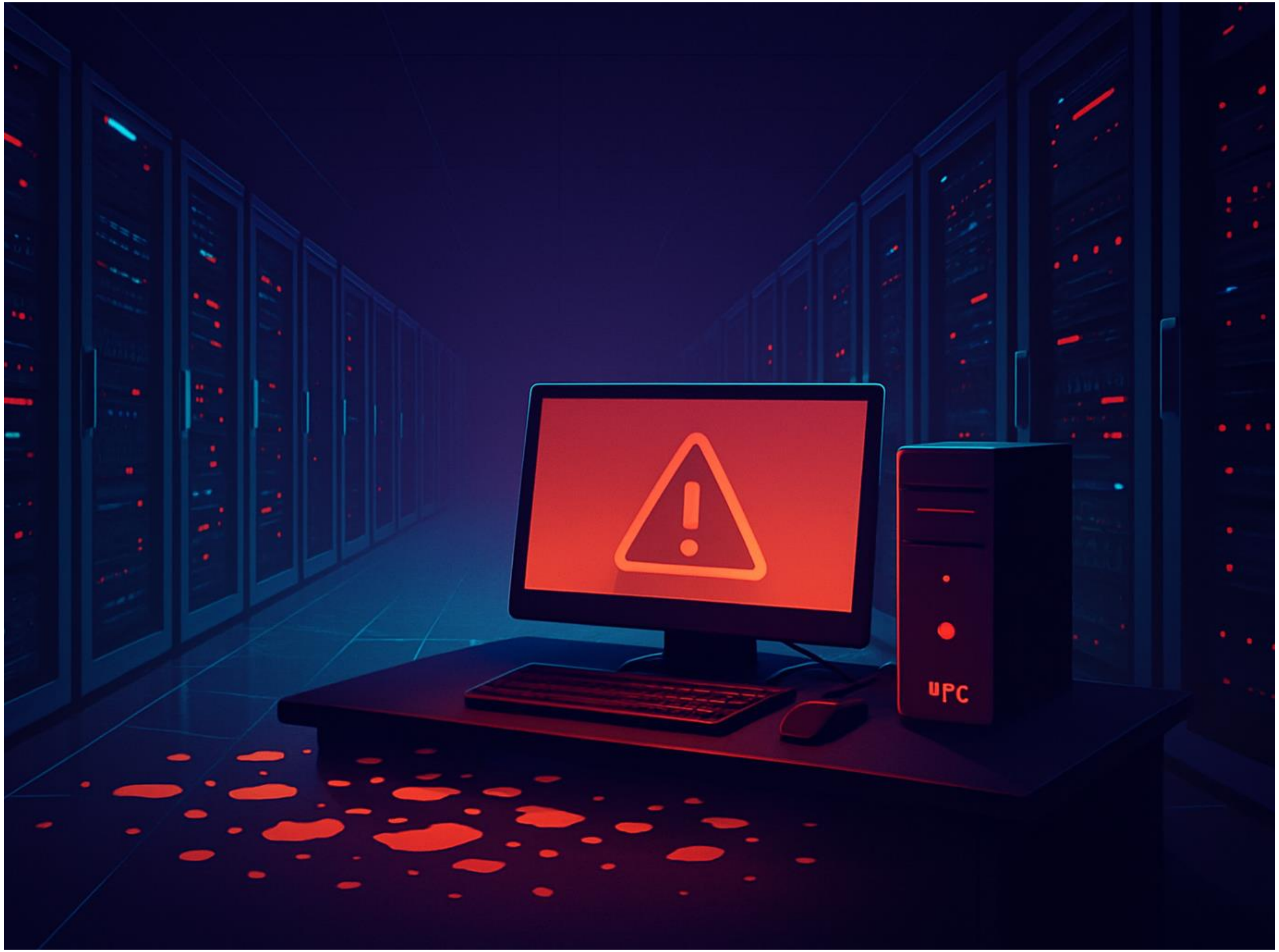
Includes

- Structure reconnaissance
- Scan the environment. Gather the data
- Prioritize remediation plan by the risk model
- Maintain visibility through automation



Structure Scanning

- Enumerate node types
- Identify example nodes of each type
- Instrument scanning w/ CI pipelines
- Normalize and aggregate results



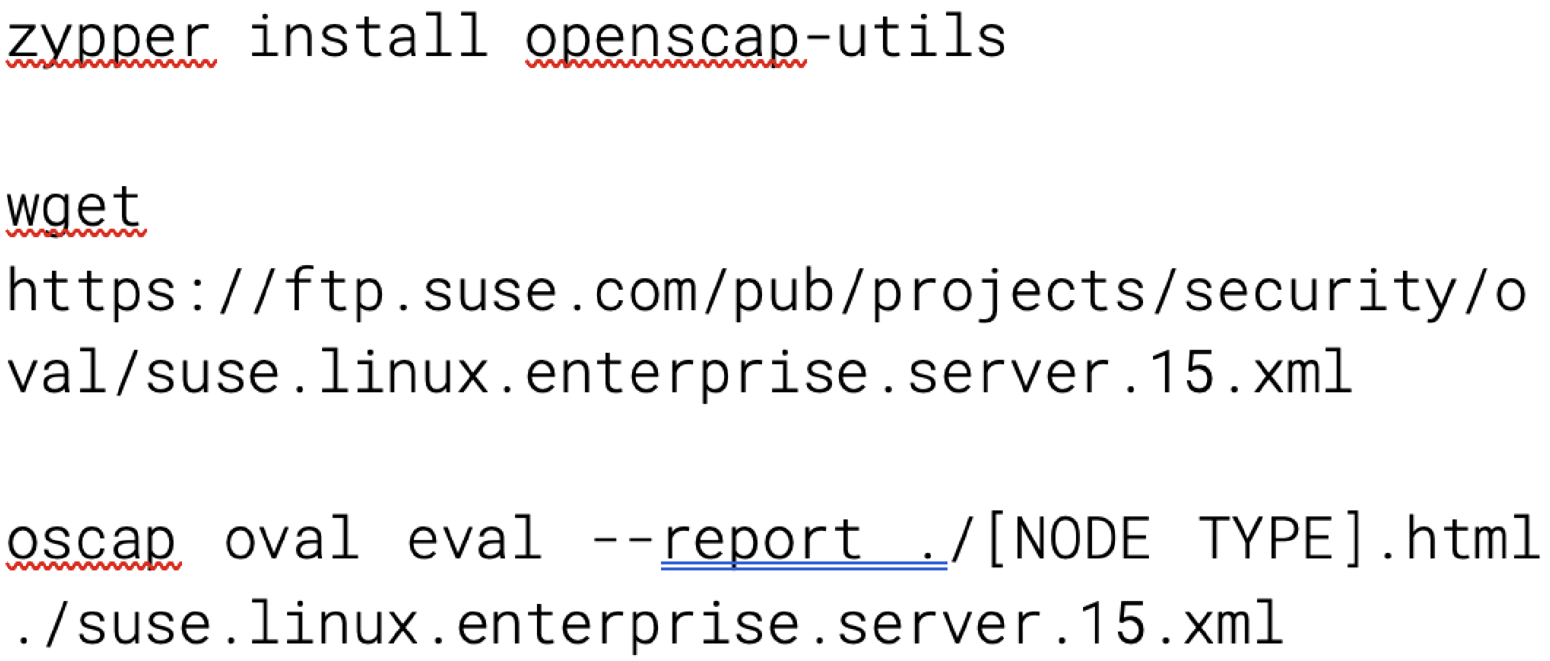
Gather Data

- OpenSCAP + OVALs = Common Vulnerabilities and Exposures (CVEs) Scan
- NMAP = Network Vulnerability Scan
- CIS-cat Pro + STIGs = Security Benchmarks

OpenSCAP

- Major distros include package
- OVAL definitions provided separately
- Remediations available via internet cross-reference

SuSE example (right)



```
zypper install openscap-utils

wget
https://ftp.suse.com/pub/projects/security/o
val/suse.linux.enterprise.server.15.xml

oscap oval eval --report ./[NODE TYPE].html
./suse.linux.enterprise.server.15.xml
```

NMAP

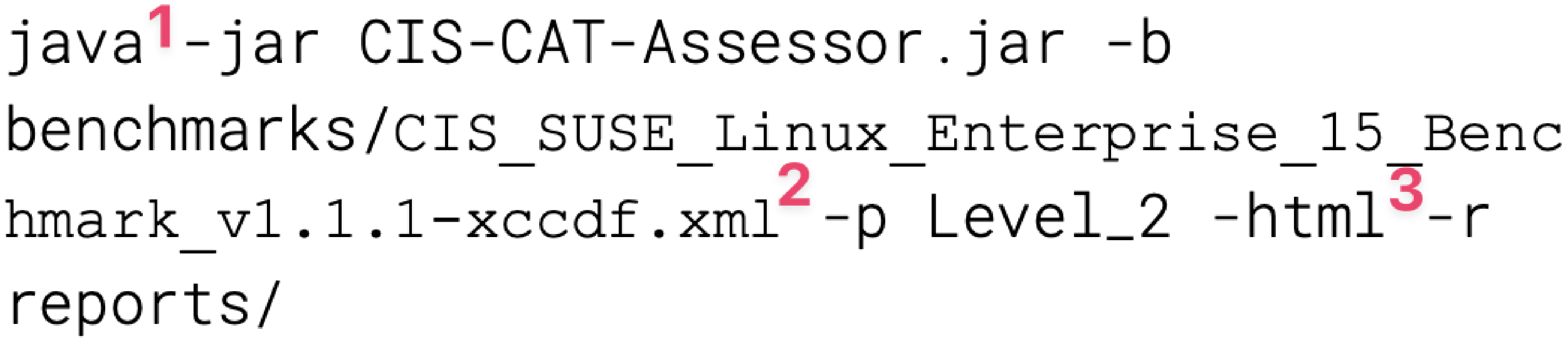
- Fingerprint OS or services
- Detect firewalll rules
- Identify vulnerabilities

```
# Show OS, service type, and vulnerabilities
nmap -A 10.92.100.0/16 -oX output.xml

# Detect firewall rules
nmap -sA 10.94.100.0/16 -oX
firewall_rules.xml
```

CIS-cat Pro

- Requires NIST account
- Requires Java (1)
- STIG file available for download (2)
- Exports to HTML (3)



```
java -jar CIS-CAT-Assessor.jar -b
benchmarks/CIS_SUSE_Linux_Enterprise_15_Benc
hmark_v1.1.1-xccdf.xml -p Level_2 -html -r
reports/
```

Model Risk / Threat

Example Threat Model:
Exploitability + Impact + Exposure

- Exploitability: AuthN, Complexity, Available Exploits
- Impact: CVSS Score (if CVE), Tool-provided score
- Exposure: User Adjacency

Aggregate & Normalize Data

- Parsers available for each tool
- Apply threat score to each finding
- Stackrank findings
- Create actionable backlog based on capacity

Automate for Continuous Visibility of Security Posture

- CI pipelines executes on change
- OpenSCAP provides CVE
- CIS-cat provides security benchmark data and automates remediation
- NMAP provides port scans and known vulnerabilities
- Python for data normalization and threat modeling
- Source code available on request

Recap

- Vulnerability scanning tools are free and widely available
- Visibility of security posture can be maintained continuously
- Modeling threat helps translate the data into an actionable plan

Thank you