From Overwhelmed to In Control

How to move to Proactive Vulnerability Reduction

Ivan Ortiz

Solution Engineer

November 2025

Table of Contents

1. The Evolving Risk & Compliance Landscape
2. The Shift to Autonomous Workflows
3. Data-Driven Decisions for Risk Reduction
4. Operational Impact: Unlock Resources & Reduce Costs

Who am I?

Ivan Ortiz – Solution Engineer @ Tanium

- Solution Engineer, focused on DFIR
- Previously, Security Operations in banking and digital payments.
- Education:
  - B.Sci., Information Technology, UNAM
  - MS, Cybersecurity, La Salle.

1

The Evolving Risk & Compliance Landscape

The Evolving Risk & Compliance Landscape

Threat Actors

Attacker 'dwell time' has been reduced to a median of 2 days (Sophos Active Adversary Report, 2025)

As many as 81% of attacks were 'malware-free' (CrowdStrike Global Threat Report, 2025)

Vulnerabilities

2024: 40,009

(38% increase since 2023)

2025: 28,992 *(so far)*

Known-Exploited Vulnerabilities:

2024: 881

2025: 574 (so far) (VulnCheck)

Artificial Intelligence

New attacks such as CVE-202-54136 are accelerating.

AI has lowered the barrier for threat actors in a variety of campaigns

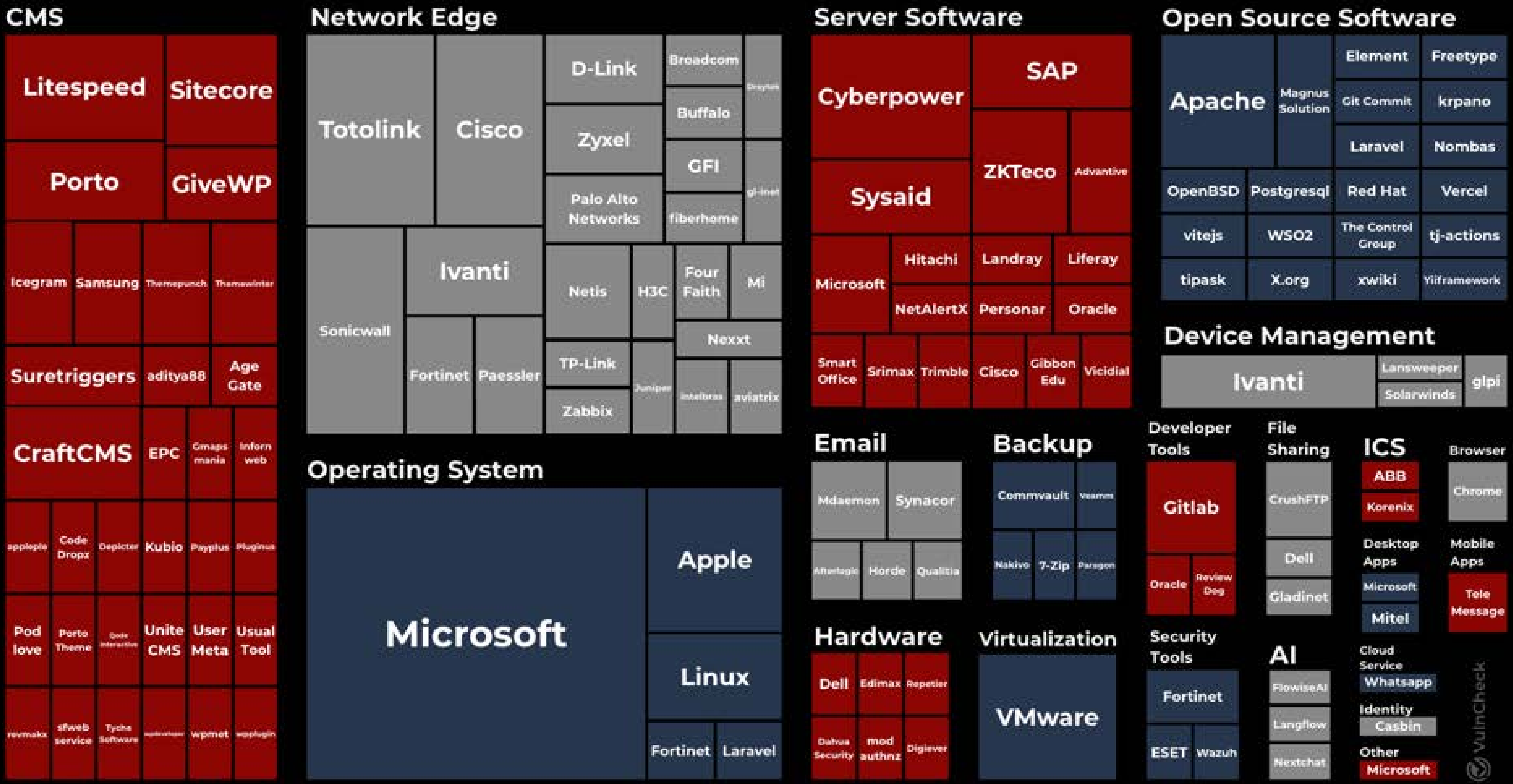
Deepfakes have enabled more sophistication in remote-worker scams and social engineering

Regulatory

Reporting requirements on breaches and ransom payments

Increased privacy standards that may have additional penalties or lawsuits

What Types of Technologies Have Known Exploited Vulnerabilties (2025 H1)



Limitations of Traditional Vulnerability Management Strategy

"Add it to the bucket"

2

The Shift to Autonomous Workflows

The Shift to Autonomous Workflows

Automate the Essential Eight

- **Continuous Discovery:** Make ongoing baselining a standard practice.
- **Accelerate Maturity:** Use automation and real-time feedback for Essential Eight
  - *“Patches in office productivity suites, browsers, extensions, email clients, PDF Software and security products are applied within 48-hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist”*
  - *“Applications that are no longer supported by vendors are removed”*
  - *“A vulnerability scanner is used at least fortnightly to identify missing patches in operating systems, applications, drivers, and firmware”*
  - *…and more!*
- **Proactive Configuration:** Reduce exploitable risk with autonomous workflows that don’t wait for the vulnerability scan

Don’t wait for reports & scans when you can proactively configure automation with confidence.

- Patch Applications
- Patch Operating Systems
- Enforce Multi-Factor Authentication
- Restrict Administrative Privileges
- Enforce Application Control
- Restrict Microsoft Office Macros
- Harden User Applications

Vulnerability Reduction Funnel

Automation Bucket

Configuration Management

Scan for and apply policies to enforce secure, compliant configurations

Standard Operating Environments (SOEs)

Apply OS and applications patches and secure configurations via standardised images

Removing Applications

Identify and removes unauthorised, unused, or outdated applications to reduce the attack surface

Replacing Vulnerable Certificates

Inventory & replace outdated or vulnerable certificates to ensure secure communication channels

Operating System Patching

Automate the testing and rollout of OS patches

Common Software Upgrades

Automate and deploy enterprise & third-party software patches in most-common ‘low-hanging fruit’ applications

High-Touch Bucket

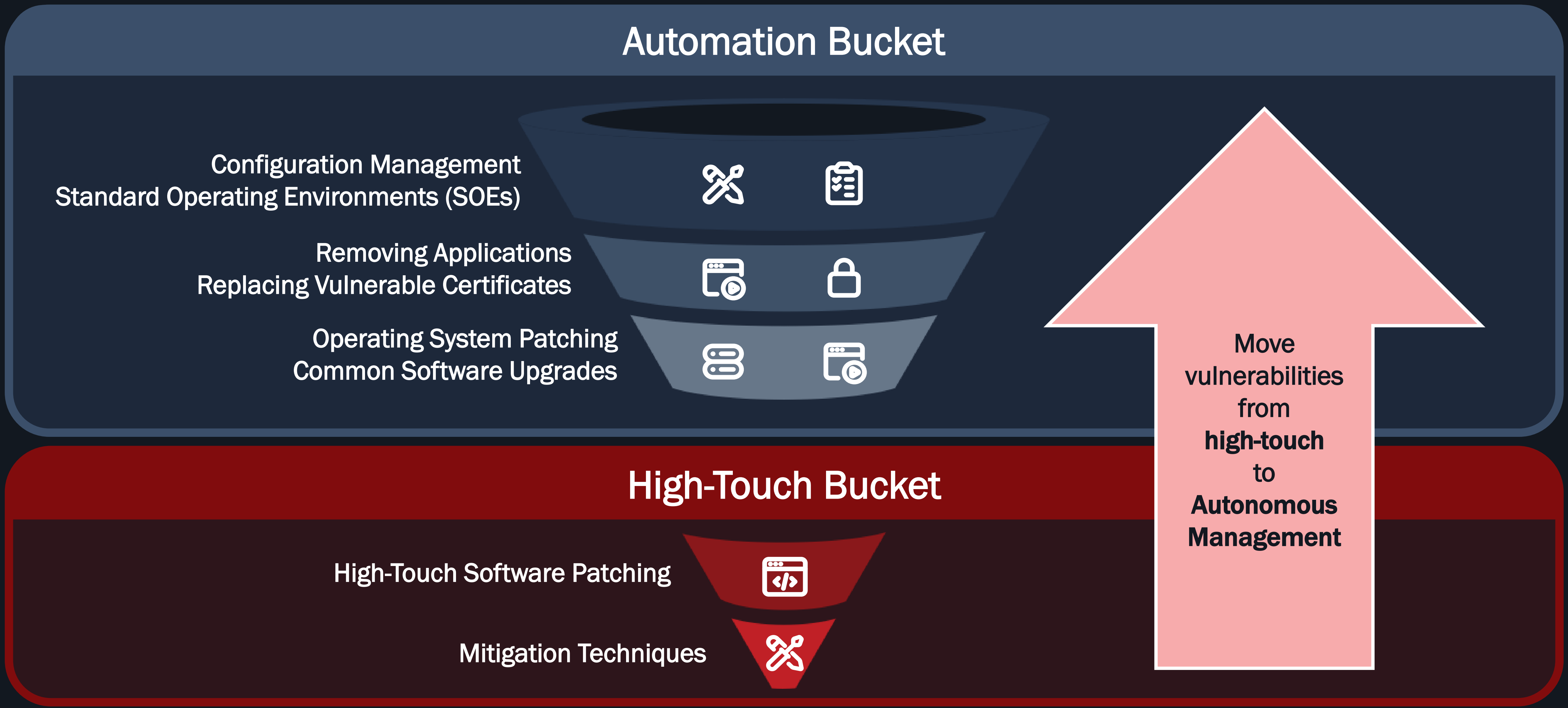
High-Touch Software Patching

Timely updates and extensive testing for enterprise software and custom-developed applications to minimise the attack surface.

Mitigation Techniques

Implement configuration changes, hardening, and mitigation techniques for ‘unpatchable’ vulnerabilities.

Vulnerability Reduction Funnel



Automation Bucket

Configuration Management
Standard Operating Environments (SOEs)

Removing Applications
Replacing Vulnerable Certificates

Operating System Patching
Common Software Upgrades

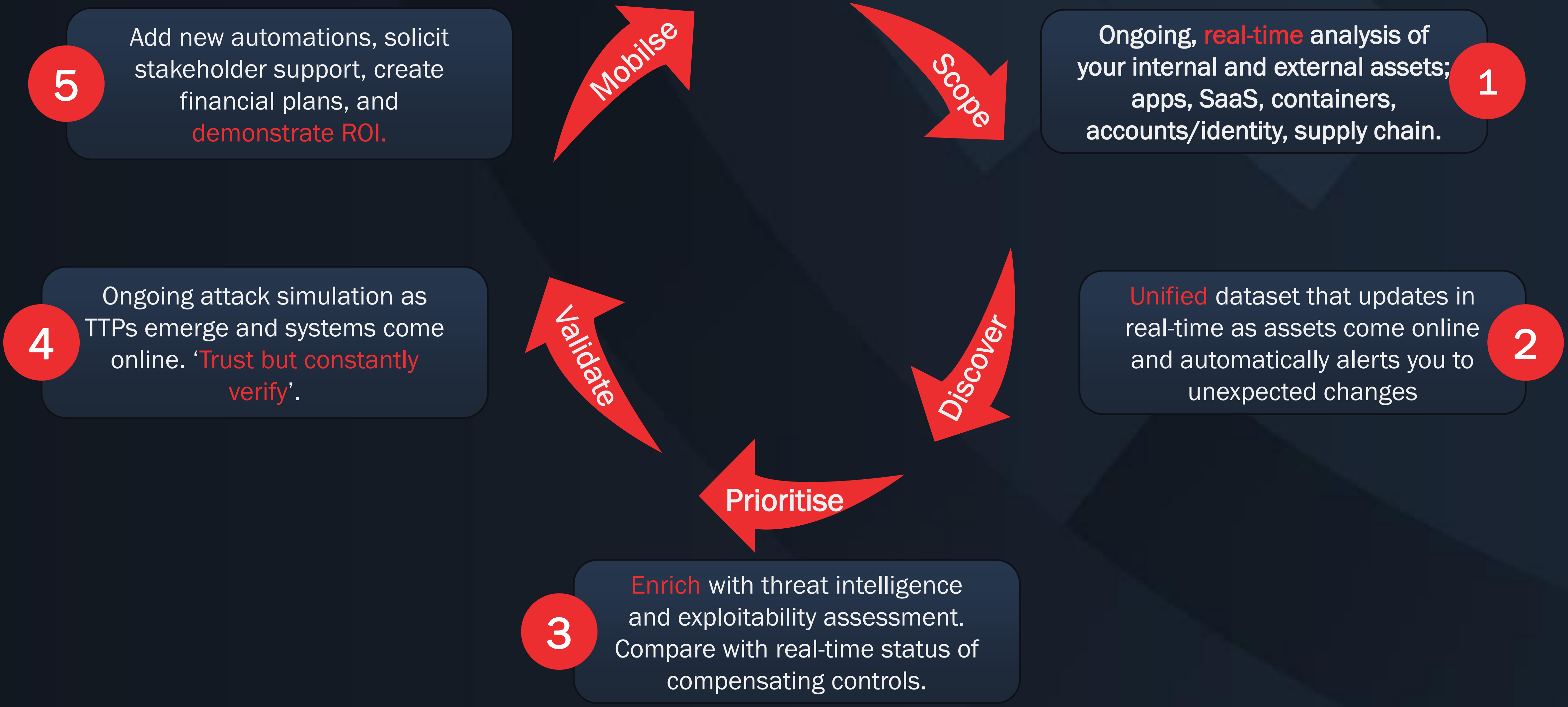
High-Touch Bucket

High-Touch Software Patching

Mitigation Techniques

Move vulnerabilities from **high-touch** to **Autonomous Management**

The Shift to Autonomous Workflows



1 Ongoing, real-time analysis of your internal and external assets; apps, SaaS, containers, accounts/identity, supply chain.

2 Unified dataset that updates in real-time as assets come online and automatically alerts you to unexpected changes

3 Enrich with threat intelligence and exploitability assessment. Compare with real-time status of compensating controls.

4 Ongoing attack simulation as TTPs emerge and systems come online. 'Trust but constantly verify'.

5 Add new automations, solicit stakeholder support, create financial plans, and demonstrate ROI.

3

Data-Driven Decisions for Risk Reduction

Exploit Intelligence Reduces Noise

Automation Bucket

Configuration Management
Standard Operating Environments (SOEs)

Removing Applications
Replacing Vulnerable Certificates

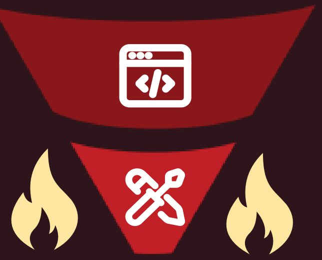
Operating System Patching
Common Software Upgrades

The essentials in this bucket can resolve be tens of thousands of vulnerabilities proactively and without manual, human intervention.

High-Touch Bucket

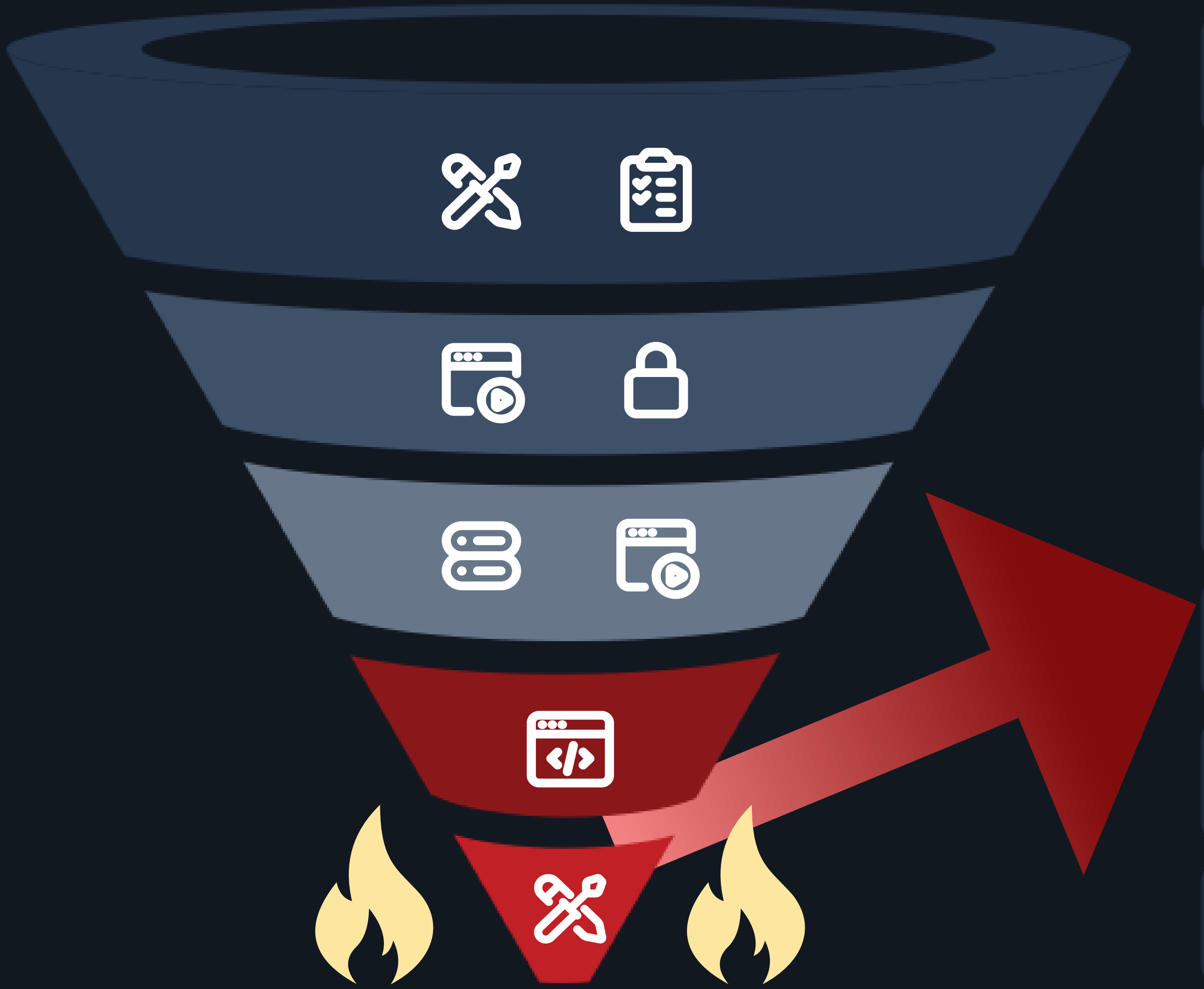
High-Touch Software Patching

Mitigation Techniques



These will be high-effort initiatives for the most urgent risks and may be less than 5% of the vulnerabilities in your environment.

Exploit Intelligence for Prioritisation



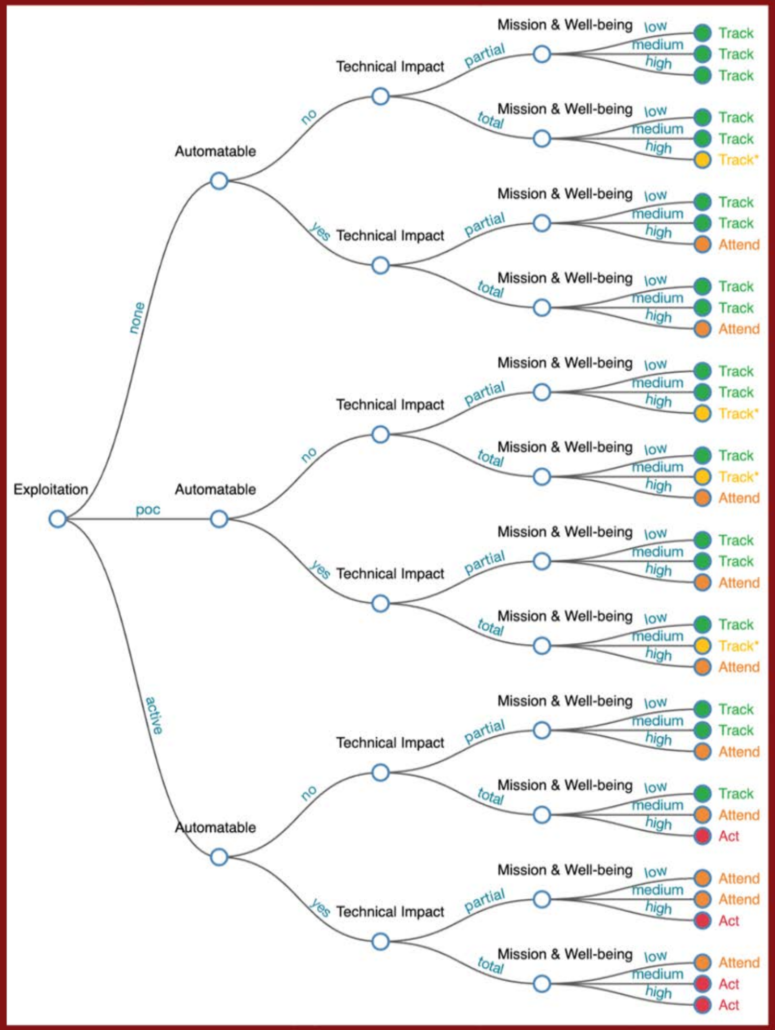
1. Ransomware
2. Botnets
3. APTs
4. Unattributed, but KEV
5. Weaponised
6. Proof-of-Concept
7. Everything else

Stakeholder-Specific Vulnerability Categories

Track, Attend, Act

- Developed by Carnegie Mellon University SEI and collaboration with the US Cybersecurity & Infrastructure Security Agency
- Track, Attend, or Act based on:
  - — Exploitation status
  - — Exploit automation capabilities
  - — Technical Impact
  - — Mission & well-being impact

When coupled with real time intelligence & environmental data you can act quickly on what matters and not get lost in a sea of reports & spreadsheets



4

Operational Impact: Unlock Resources & Reduce Costs

Challenge	Opportunity
- Teams are overwhelmed with manual work	- Automation reduces manual tasks, enabling teams to achieve more.
- Complexity of AI & automation	- Use low-code/no-code tools for simpler implementation
- Businesses lack real-time data for reliable outcomes.	- Implement tools that utilize real-time data for decision-making. Focus on the active state, not stale results.
- Need for significant developer resources	- Leverage low code/no code platforms to reduce dev overhead.
- Risk could be increased without controls and reliable data.	- Using tools that provide inbuilt confidence scoring based on data at scale can help to futureproof and mitigate risk.
- Automation libraries require highly skilled experts	- Automation, once enabled, allows skilled staff to ‘pass the torch’ of some tasks on to more junior staff to operate.

Operational Impact: Unlock Resources & Reduce Costs

Where do you start?

Consult Experts

Identify tedious or risky tasks that could benefit from automation.

Align with Priorities

Ensure stakeholder support by aligning with business goals.

Define KPIs

Set and track key performance indicators early.

Strategic Approach

Start with simple tasks and gradually move to advanced workflows.

Integrate Seamlessly

Incorporate automation into existing tools and workflows.

Operational Impact: Unlock Resources & Reduce Costs

How can you measure ROI for Autonomous Workflows?

Time Savings

- Metric: Reduction in time required to complete tasks.
- Example: Automation of software provisioning and setup reduces desktop support load and the time it takes for a new hire to use their equipment.

Cost Reduction

- Metric: Decrease in operational costs due to automation.
- Example: Automation of patch windows and deployment rings reduces the number of staff required for after-hours patching.

Increased Throughput

- Metric: Increase in the volume of output or transactions processed.
- Example: Admins can solve problems without developer resources and with less risk of adverse impact.

Customer Satisfaction

- Metric: Improvement in customer service and satisfaction levels.
- Example: Automation of policy and configuration enables 'self-healing' environments, reducing the number of helpdesk tickets.

Thank You!

Ivan Ortiz

Solution Engineer

November 2025