Breaking Boundaries, Securing Perimeters: A Pragmatic Approach to Attack Surface Management

Katie Inns 🐦 @J3lly____

Hello!

Katie Inns

Security Consultant @ WithSecure

🐦 @J3lly____

W/TH
secure

Vulnerability Management

"

Vulnerability management is the process of **identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them**.
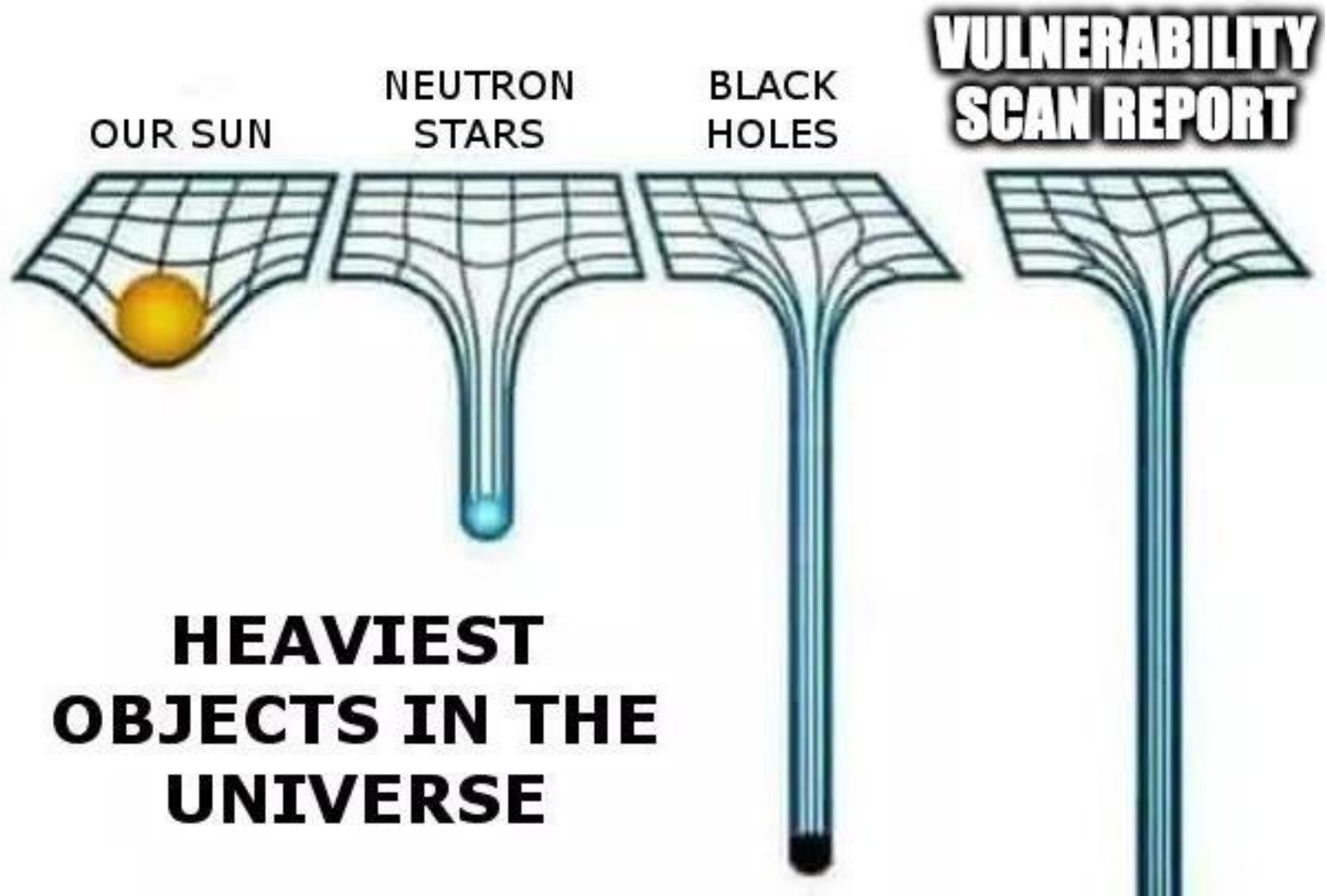
-- Rapid7

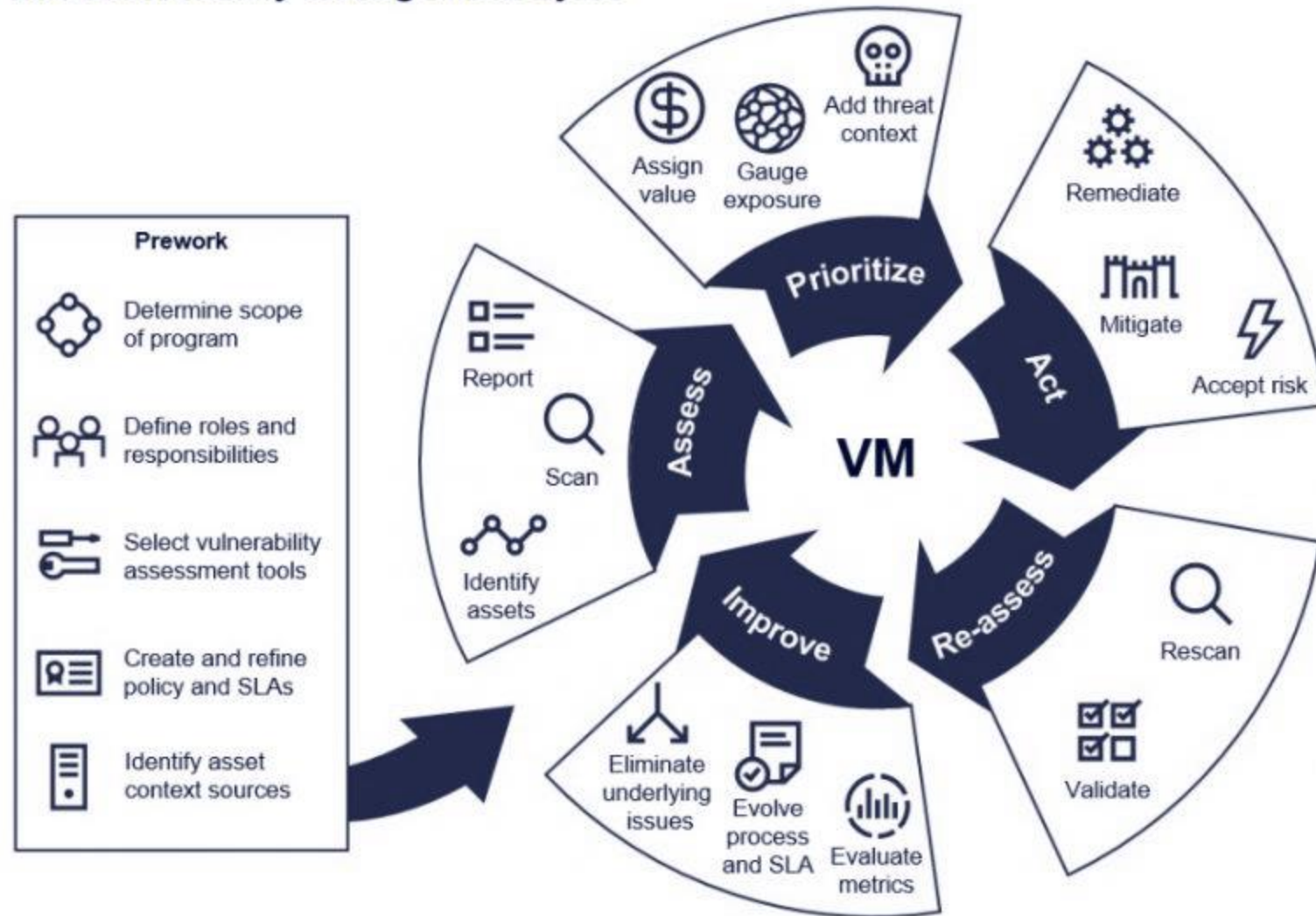"

W / TH
secure

Monthly Scanning

- Vulnerabilities drop between scan periods
- Time taken to add new plugins

Scope

- Restricted to defined target list
- New assets not considered

OUR SUN · NEUTRON STARS · BLACK HOLES · VULNERABILITY SCAN REPORT

HEAVIEST OBJECTS IN THE UNIVERSE

WithSecure

The Vulnerability Management Cycle

Prework
- Determine scope of program
- Define roles and responsibilities
- Select vulnerability assessment tools
- Create and refine policy and SLAs
- Identify asset context sources

Assess
- Report
- Scan
- Identify assets

Prioritize
- Assign value
- Gauge exposure
- Add threat context

Act
- Remediate
- Mitigate
- Accept risk

Re-assess
- Rescan
- Validate

Improve
- Eliminate underlying issues
- Evolve process and SLA
- Evaluate metrics

VM

Source: Gartner
ID: 410271

W/TH secure

Image: https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/

'Prioritise'

- 'Top-down' approach

- Exploitation in the wild not considered

- Ignored threats not included by vulnerability scanners

Windows RDP / Terminal Services Detection

`INFO` Nessus Network Monitor Plugin ID 5935

Prioritising Vulnerabilities

Utilise threat intelligence

Understand threats to organisation and industry

Remediate based on likelihood of exploitation

Bug Bounty
Program

WITH
secure

Cool & interesting techniques

Some zero-days

Research driven

A ... monetary reward give...
hacke... successfully discovering a...
vulnerability or bug to the application's...
Bug bounty programs allow companies...
**the hacker community to improve their...
security posture ... continuously**

-- HackerOne

BUG BOUNTY

LAUNCH

MUCH SUCCESS

WOW

WITH secure

Response Efficiency

about 1 day
Average time to first response

2 days
Average time to triage

7 days
Average time to bounty

6 months
Average time to resolution

🟢 **98% of reports**
Meet response standards
Based on last 90 days

Inconsistent

- Gaps in submissions
- Could be controlled with scope, bounty amount etc.
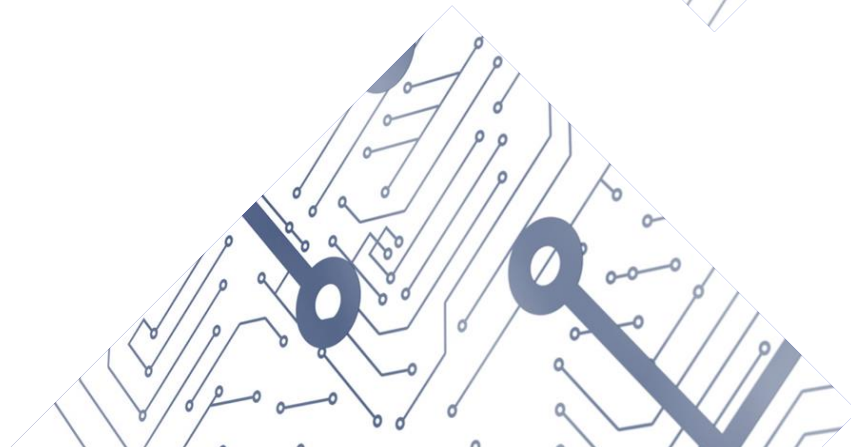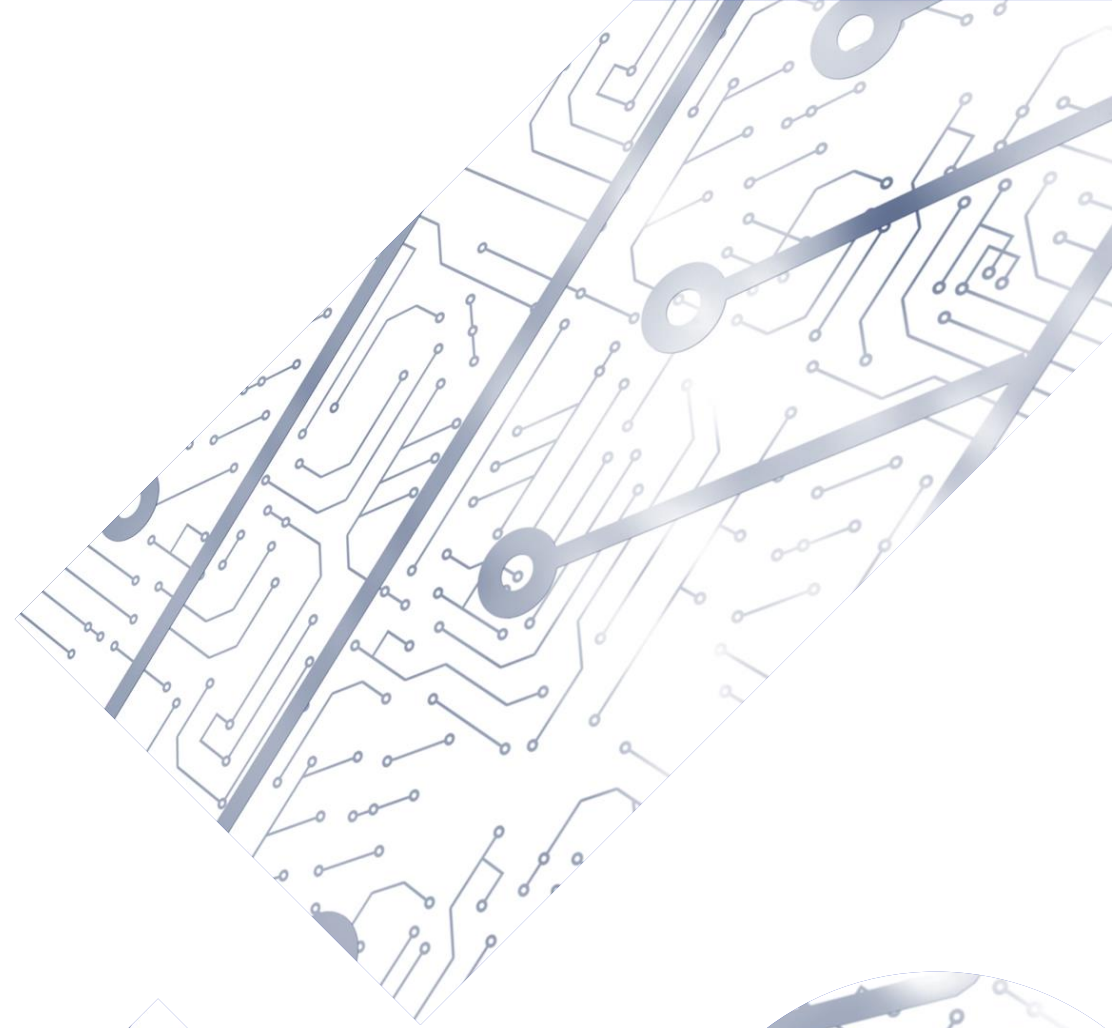
Scope

Scopes

In Scope

Other	**Uber Assets** If you have found a vulnerability in an Uber app or site that is not in the Out of Scope list below, please submit a report for triage and review.	▬ Critical	💲 Eligible

Out of Scope

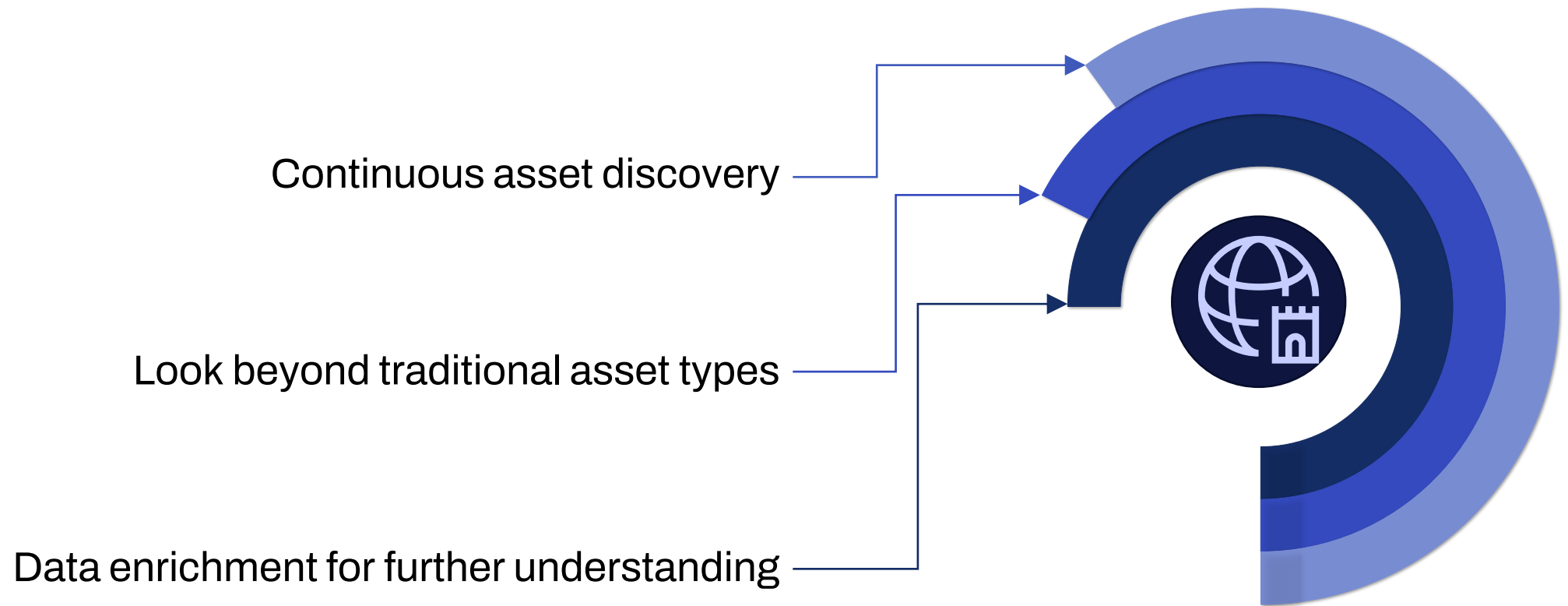|		
Domain	***.support-uber.com** This asset is not eligible for Uber bounty programs.	
Domain	***.lioncityrentals.com.sg** This asset is not eligible for Uber bounty programs.	
Domain	***.xchangeleasing.com** This asset is not eligible for Uber bounty programs.	

Scopes

In Scope

Domain	**slack.com** The slack.com site and application.	▬ Critical	💲 Eligible
Domain	**api.slack.com** The Slack API	▬ Critical	💲 Eligible
Domain	**status.slack.com** The Slack status site	▬ Critical	💲 Eligible
Domain	**slackb.com**	▬ Critical	💲 Eligible
Domain	**app.slack.com**	▬ Critical	💲 Eligible
Domain	**edgeapi.slack.com**	▬ Critical	💲 Eligible

W/THsecure

Dynamic Scope

Continuous asset discovery

Look beyond traditional asset types

Data enrichment for further understanding

Attack Surface Management

"Attack surface management is the **continuous discovery, monitoring, evaluation, prioritisation and remediation** of attack vectors within an organization's IT infrastructure.
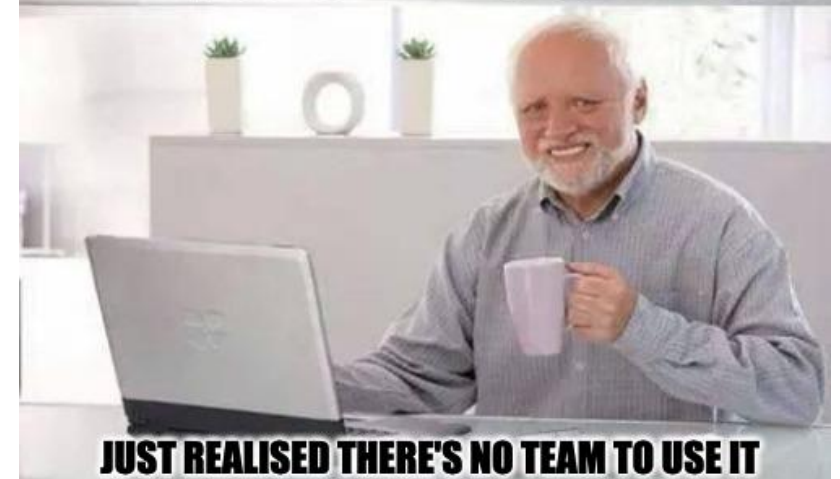
-- CrowdStrike

SaaS

- Needs a team behind it
- Lots of data
- Trends & statistics

Human driven

- Orgs valuing consultation & expert advice
- Ability to apply more context
- Humans aren't 24/7

SECURITY MANAGERS BE LIKE

SPENT $100K ON A NEW SECURITY TOOL
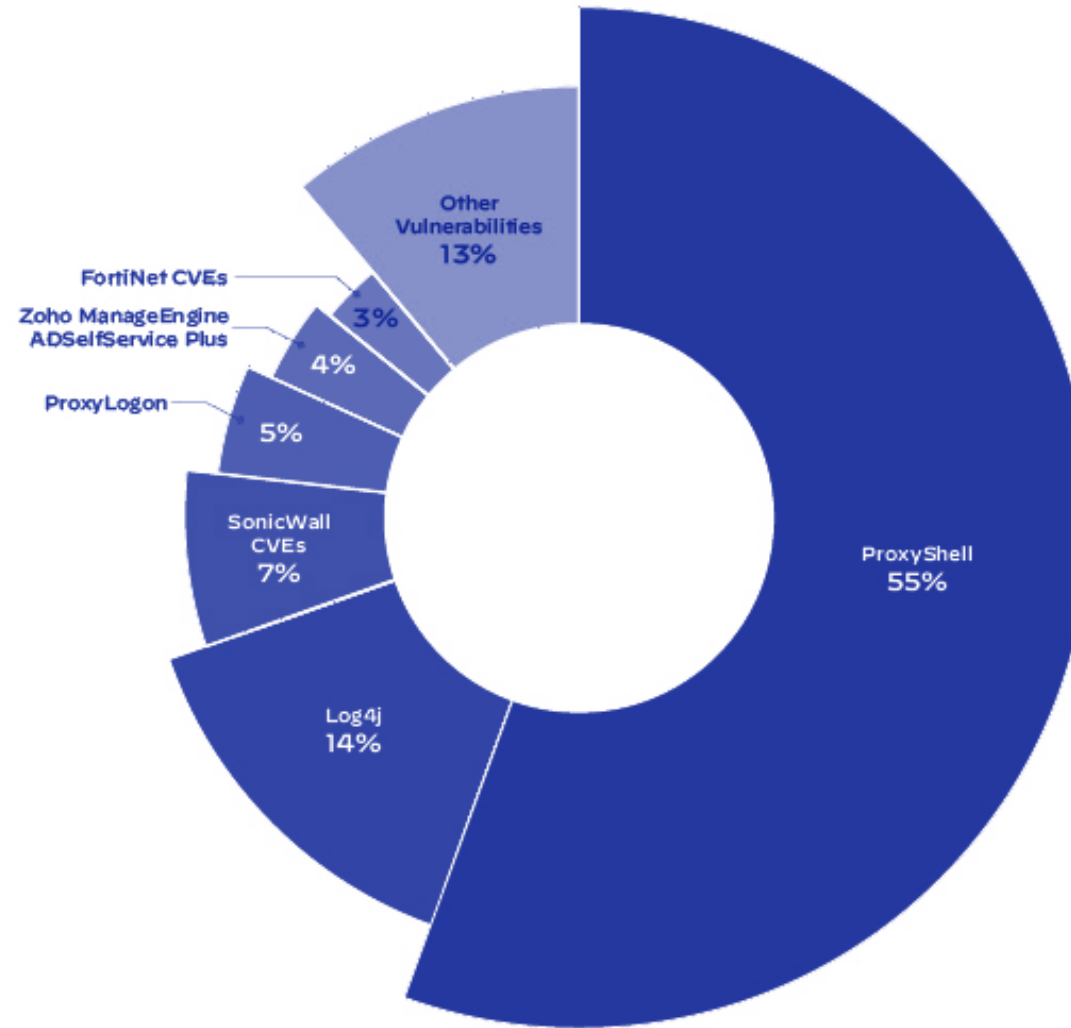
JUST REALISED THERE'S NO TEAM TO USE IT

Dynamic Scope

- Continuous asset discovery
- Extended to unconventional asset types

Only **22.4%** of CVE's have published exploit code, of which **1.8%** are actively exploited in the wild.

WITH secure

Exploited Vulnerabilities in Unit 42 Cases

- ProxyShell 55%
- Log4j 14%
- Other Vulnerabilities 13%
- SonicWall CVEs 7%
- ProxyLogon 5%
- Zoho ManageEngine ADSelfService Plus 4%
- FortiNet CVEs 3%

Insights From the 2022 Unit 42 Incident Response Report: https://unit42.paloaltonetworks.com/incident-response-report/
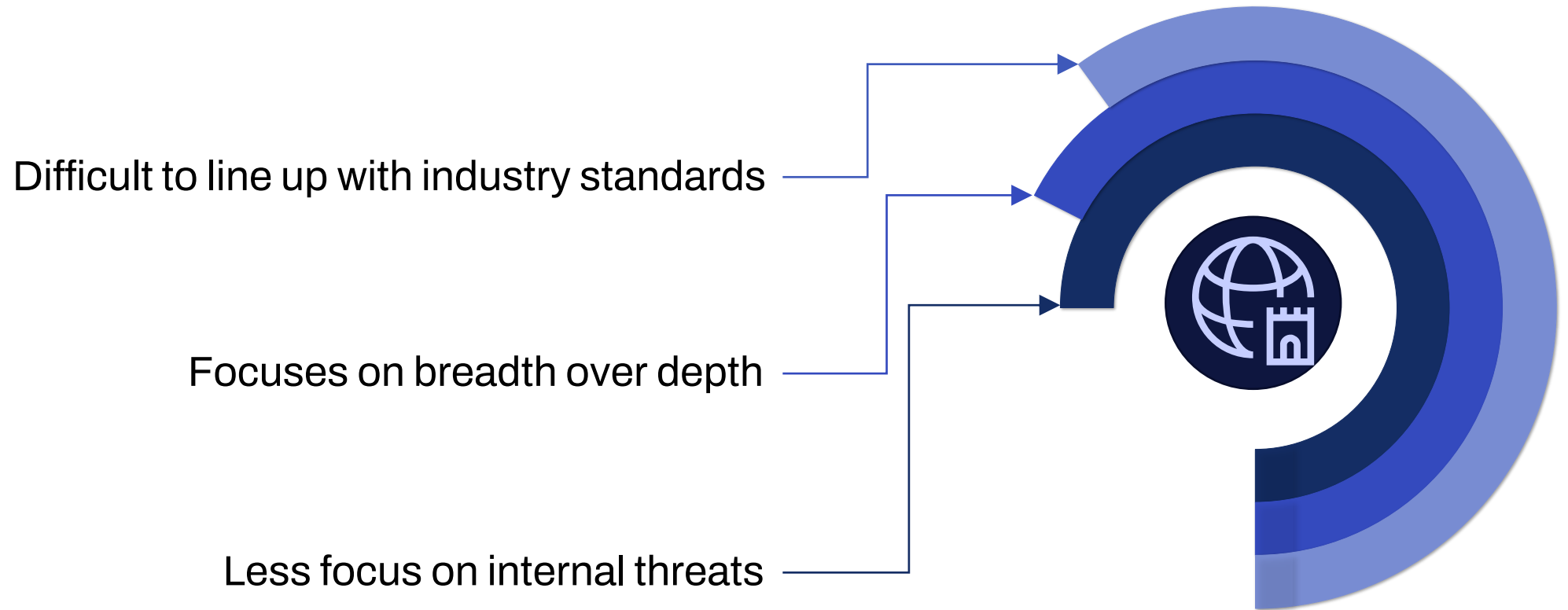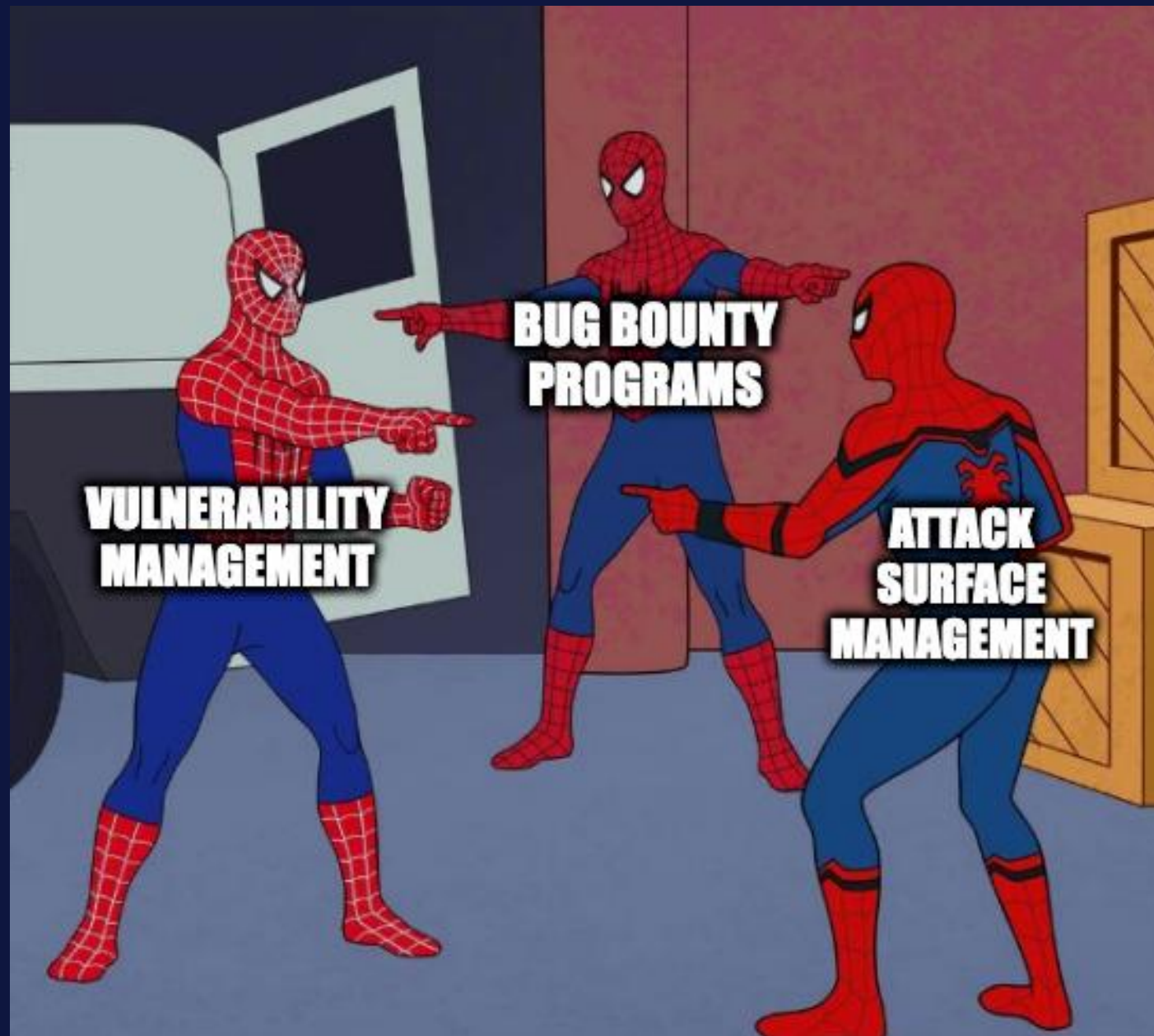
W I T H secure

Adapt based on emerging threats

- Defence against new styles of attack

- Newer and more targeted technologies

- Less considered types of attack surface

Unsolved challenges...

Difficult to line up with industry standards

Focuses on breadth over depth

Less focus on internal threats

Takeaways

01 Apply context and prioritise vulnerabilities

02 Carry out continuous testing and asset discovery

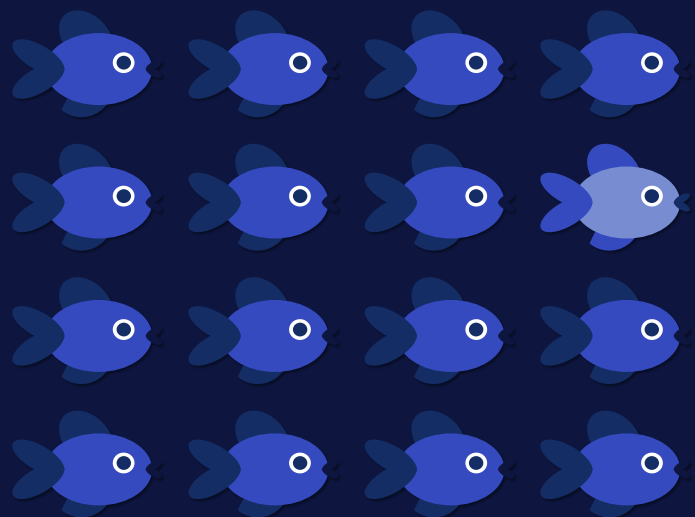**03** Be innovative and adapt to the changing threat landscape

Resources

Exploring Unconventional Attack Surfaces:

https://www.withsecure.com/gb-en/expertise/resources/unconventional-attack-surfaces

Managing Your True Attack Surface:

https://www.withsecure.com/gb-en/expertise/resources/managing-your-true-attack-surface

WITH secure

Thank you!

Any questions?

Katie Inns   @J3lly____

W/TH
secure