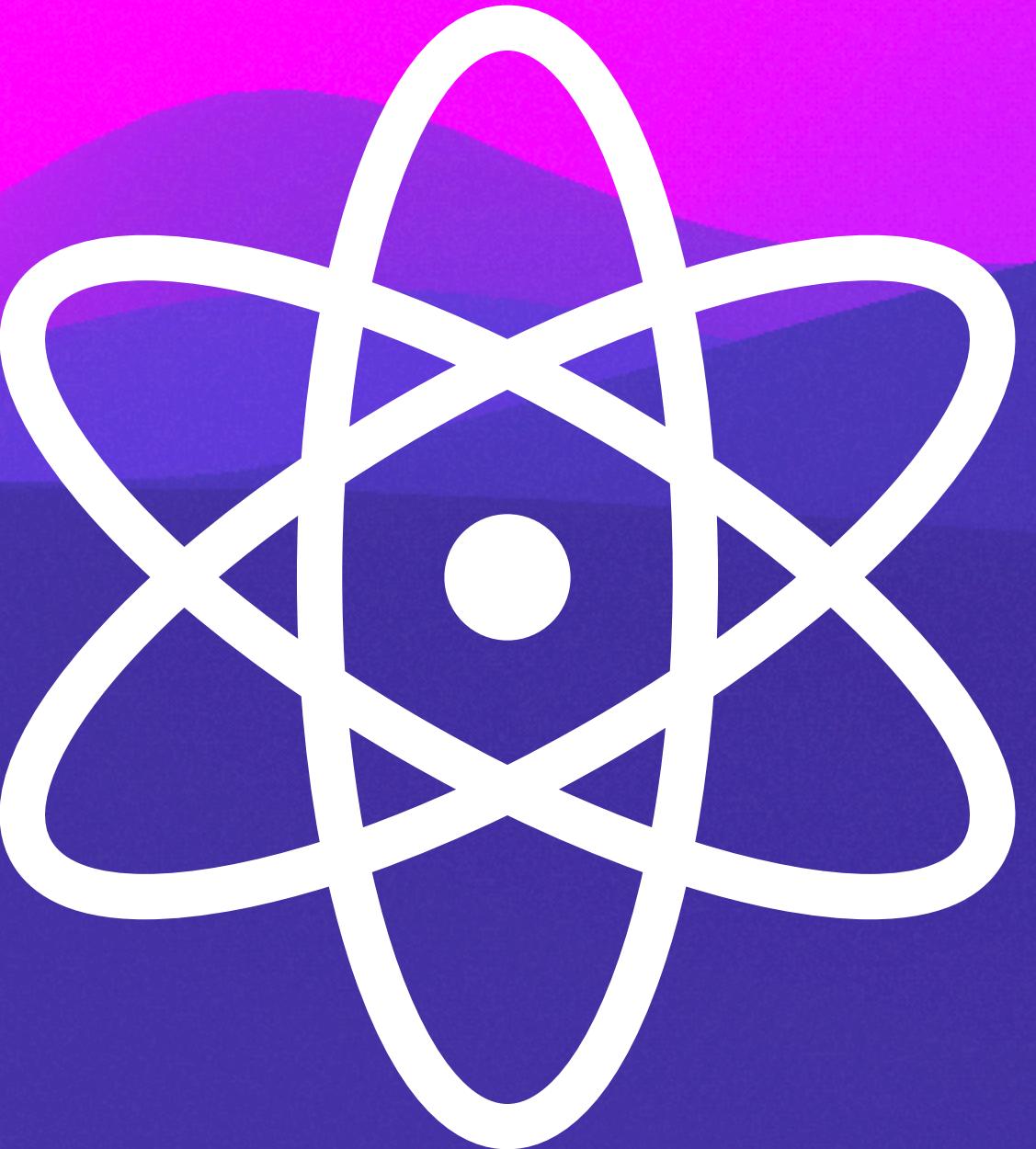


# Going Atomic

The Strengths and Weaknesses of a  
Technique-centric Purple Teaming Approach

Alfie Champion @ajpc500





# Atomic Purple Team?

# \$ whoami

- Adversary Emulation
- Previously MWR / F-Secure
- Previously Spoken at BH, RSA, T2.fi
- C3, Cobalt Strike, Mythic, Nim



@ajpc500 | [ajpc500.github.io](https://ajpc500.github.io)

Offense

Informs

Defense

# Red Team

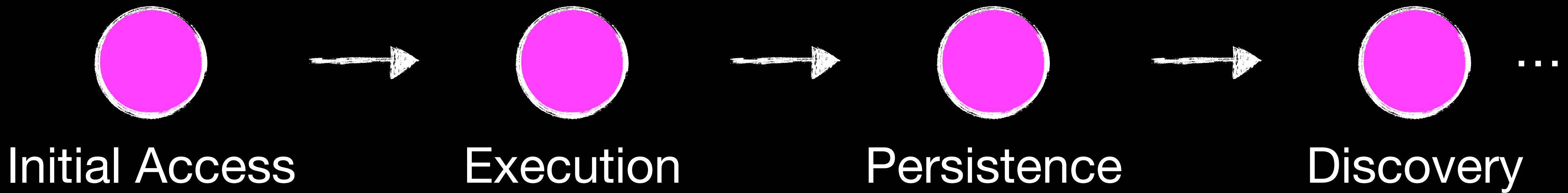
## Informs

# Defense

Table Top  
Informs  
Defense

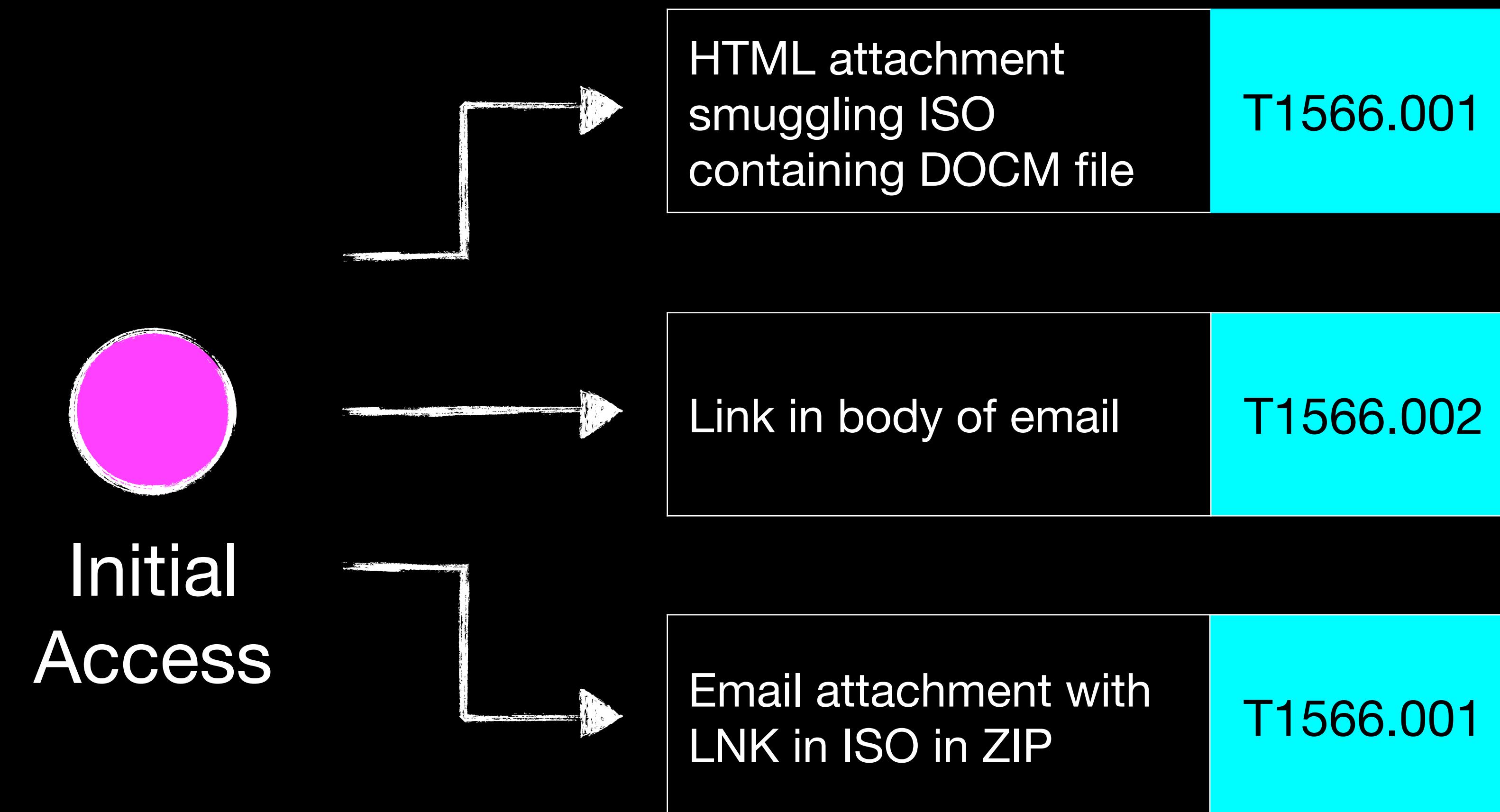
# Atomic Purple Team?

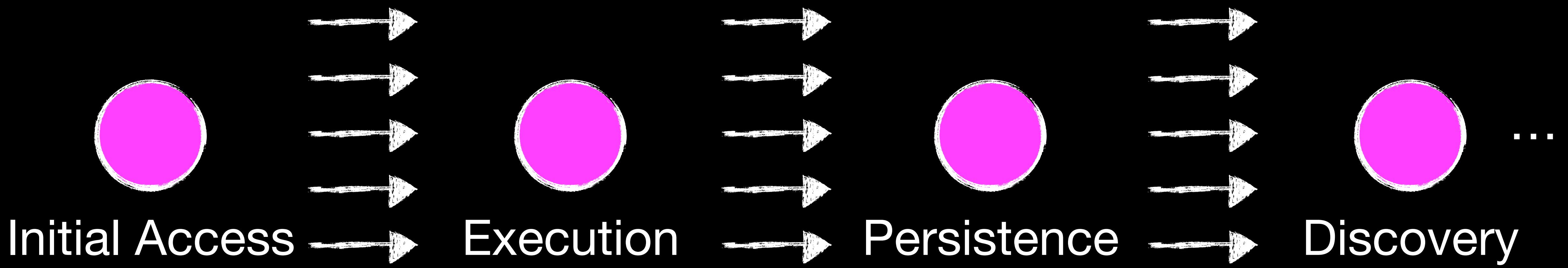
# Objective-Led Attack Path



# Objective-Led Attack Path

- Emulation potentially down to a procedural level 
- Evidence-based appraisal of defence against a given threat 
- Potential to exercise response playbooks and processes 





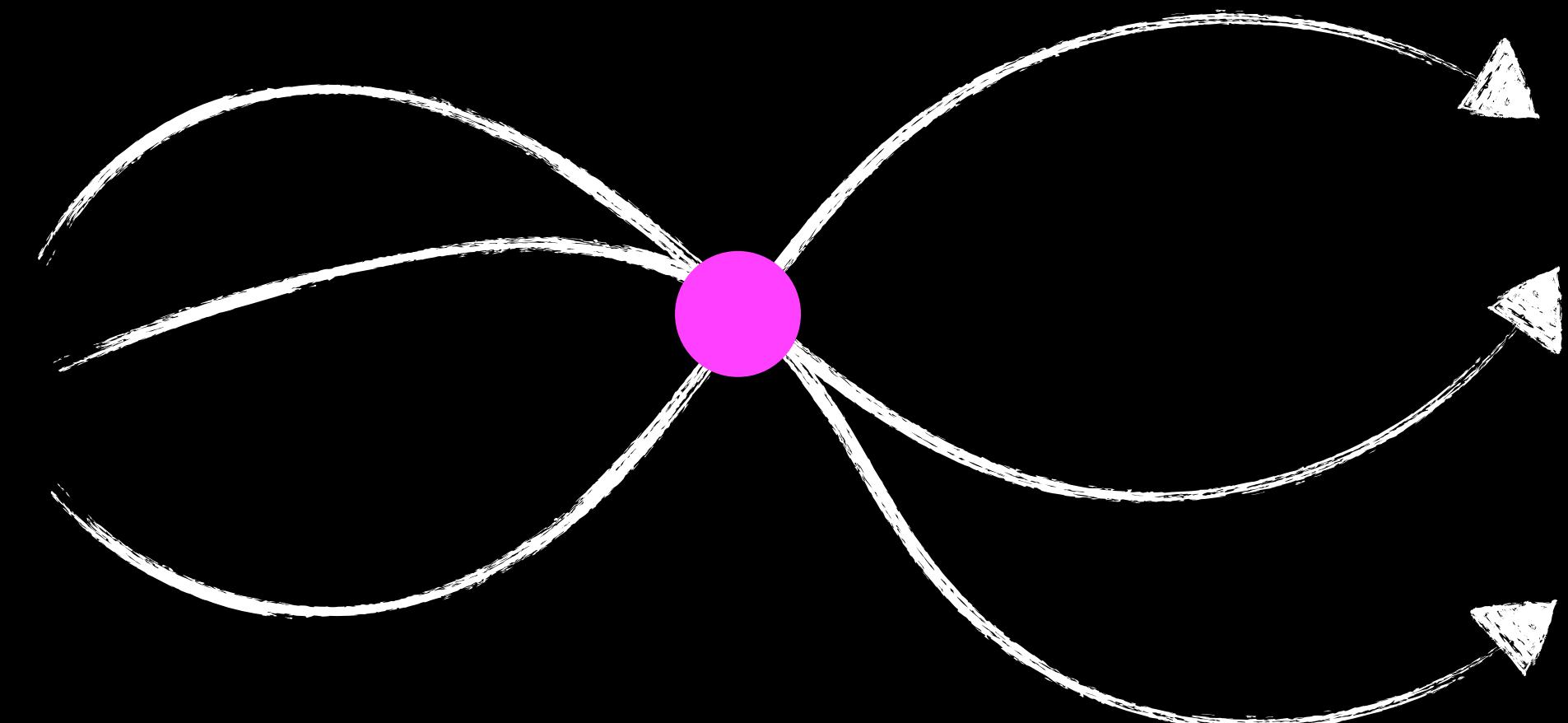


What should we  
execute?

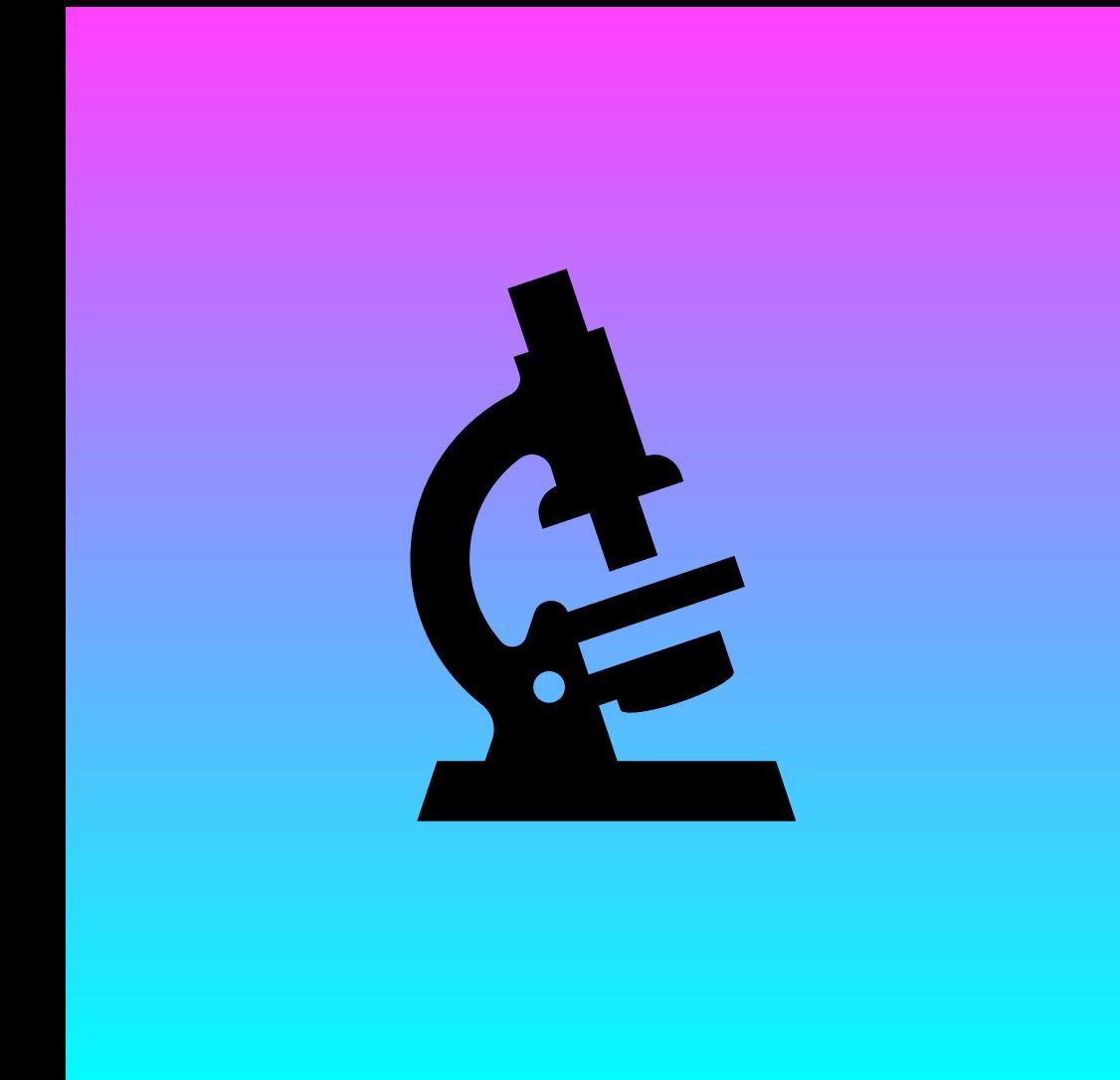
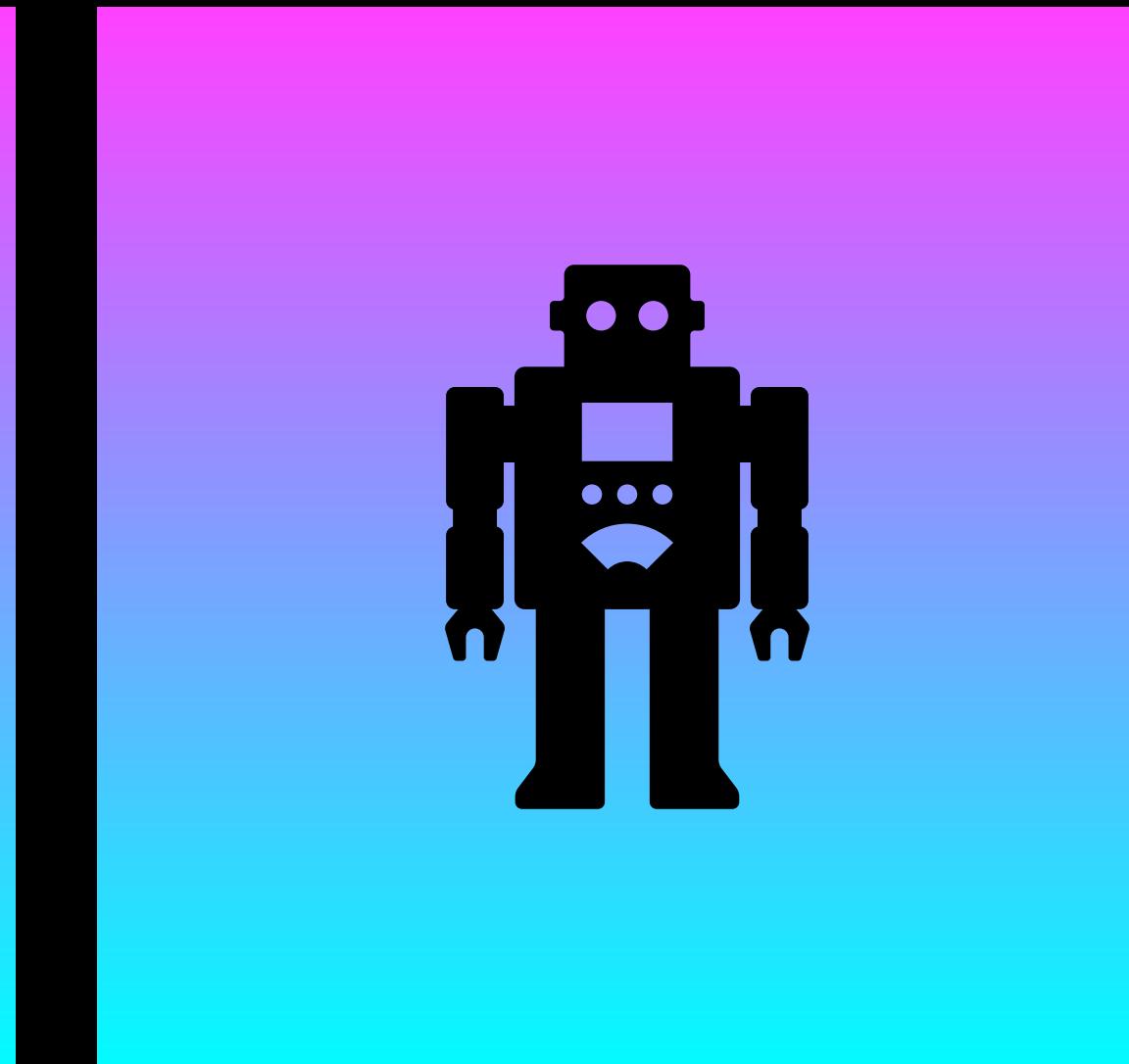
# What should we execute?

Sources of techniques:

- Threat Intelligence
- Incident Write-ups
- Offensive Testing Outputs
- Security Tooling Capability



# What should we execute?



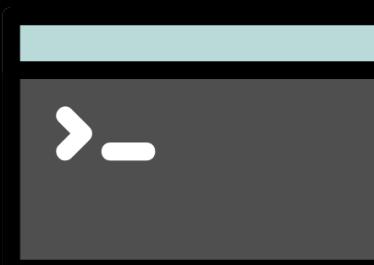
[P]

The screenshot shows the Operator Enterprise 1.5.3 interface. On the left, there's a sidebar with icons for CONNECT, TRAIN, DOCS, and SETTINGS. The main area has two search bars at the top: 'Filter the agents below' and 'Search the results'. Below these is a list of log entries from an agent named 'privateducky'. The log entries show multiple instances of the command 'Who am I, really? — sh' being run at different times. To the right of the log is a sidebar with several TTP (Technique-to-Procedure) cards:

- tactic:discovery name:python**: A card with a 'create' button and a link to 'Create a new TTP'.
- Use Python to enumerate domain users**: A card with a 'ttp' link and a description of enumerating domain users.
- Port Scan using python**: A card with a 'ttp' link and a description of scanning ports with python.
- Use Python to enumerate Service Principal Names**: A card with a 'ttp' link and a description of finding Service Principal Names.
- Grab python version**: A card with a 'ttp' link and a description of determining the current python version.

# T1087.002 - Domain Account Discovery

*The attacker will attempt to discovery who is a member of the privileged “Domain Admins” Active Directory group.*



```
net group "Domain Admins" /domain
```



```
Get-ADGroupMember -Identity "Domain Admins"
```

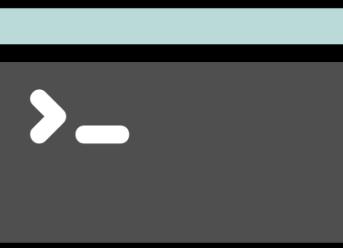


```
AdFind.exe -b "CN=Domain Admins,CN=Users,DC=Contoso,DC=com" member
```



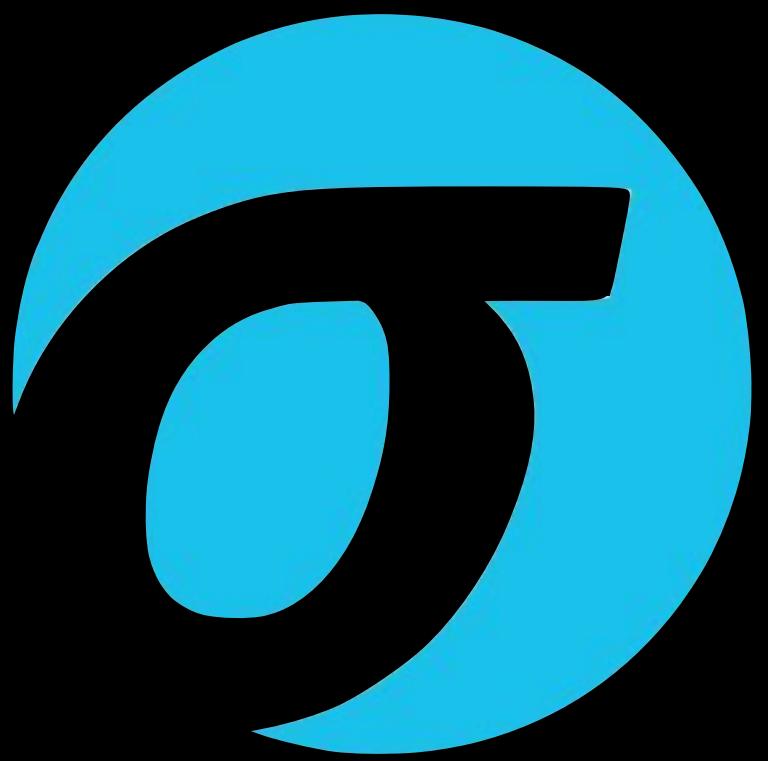
```
ldapsearch "CN=Domain Admins" member
```

# T1087.002 - Domain Account Discovery



```
net group "Domain Admins" /domain
```

# T1087.002 - Domain Account Discovery

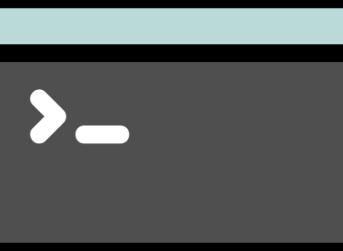


34 lines (34 sloc) | 1.03 KB

Raw Blame   

```
1 title: Suspicious Reconnaissance Activity
2 id: d95de845-b83c-4a9a-8a6a-4fc802ebf6c0
3 status: experimental
4 description: Detects suspicious command line activity on Windows systems
5 author: Florian Roth, omkar72, @svch0st
6 date: 2019/01/16
7 modified: 2022/06/09
8 references:
9   - https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
10  - https://thedefirreport.com/2020/10/18/ryuk-in-5-hours/
11 tags:
12   - attack.discovery
13   - attack.t1087.001
14   - attack.t1087.002
15 logsource:
16   category: process_creation
17   product: windows
18 detection:
19   selection:
20     CommandLine|contains:
21       - net group "domain admins"
22       - net localgroup administrators
23       - net group "enterprise admins"
24       - net accounts /do
25   condition: selection
26 fields:
27   - CommandLine
28   - ParentCommandLine
29 falsepositives:
30   - Inventory tool runs
31   - Administrative activity
32 analysis:
33   recommendation: Check if the user that executed the commands is suspicious (e.g. service accounts, LOCAL_SYSTEM)
34 level: medium
```

# T1087.002 - Domain Account Discovery

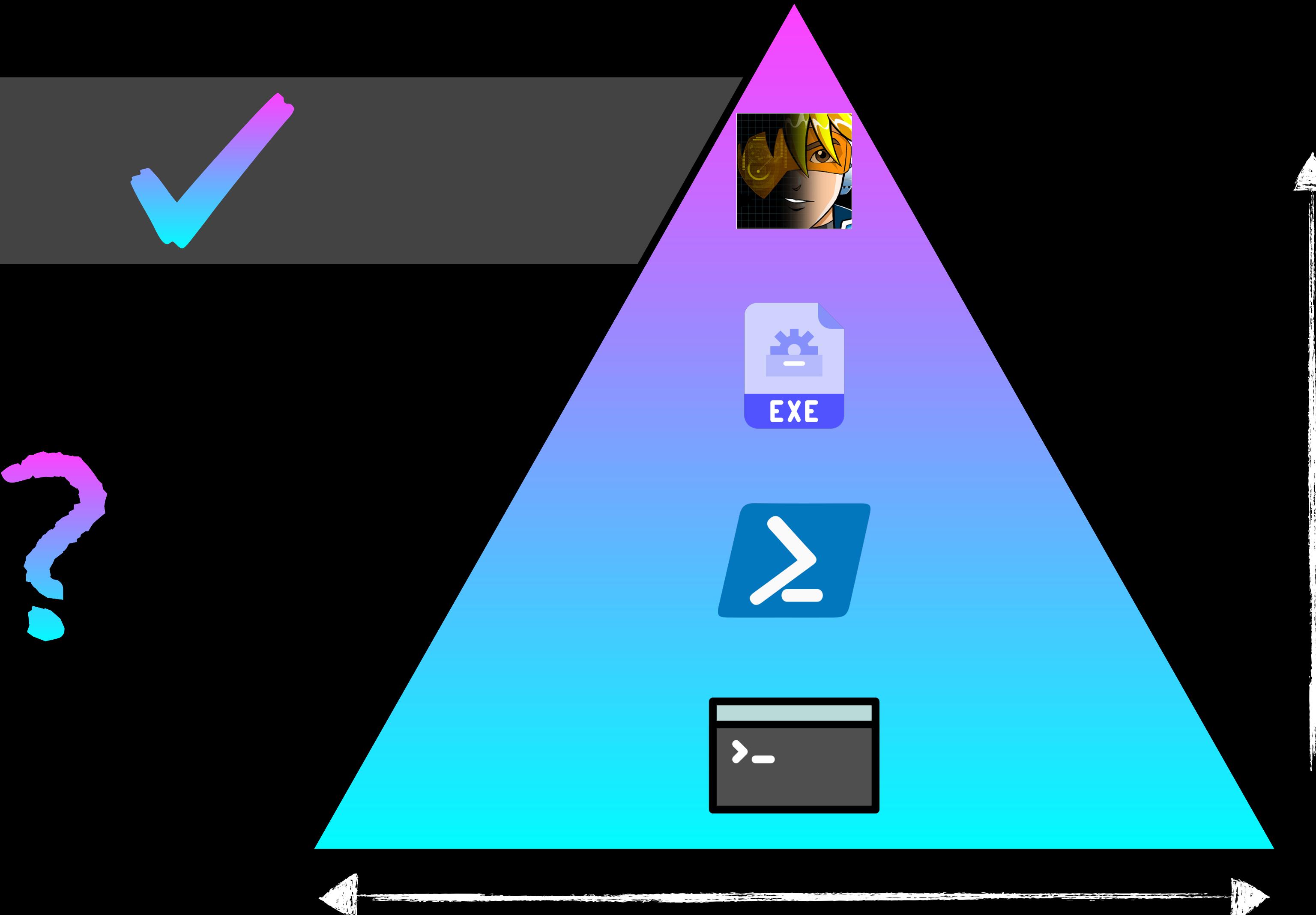


```
Set GROUP="Domain Admins" /domain  
n^e^t g^r^o^u^p %GROUP% /d^o
```

# T1087.002 - Domain Account Discovery



ldapsearch "CN=Domain Admins" member

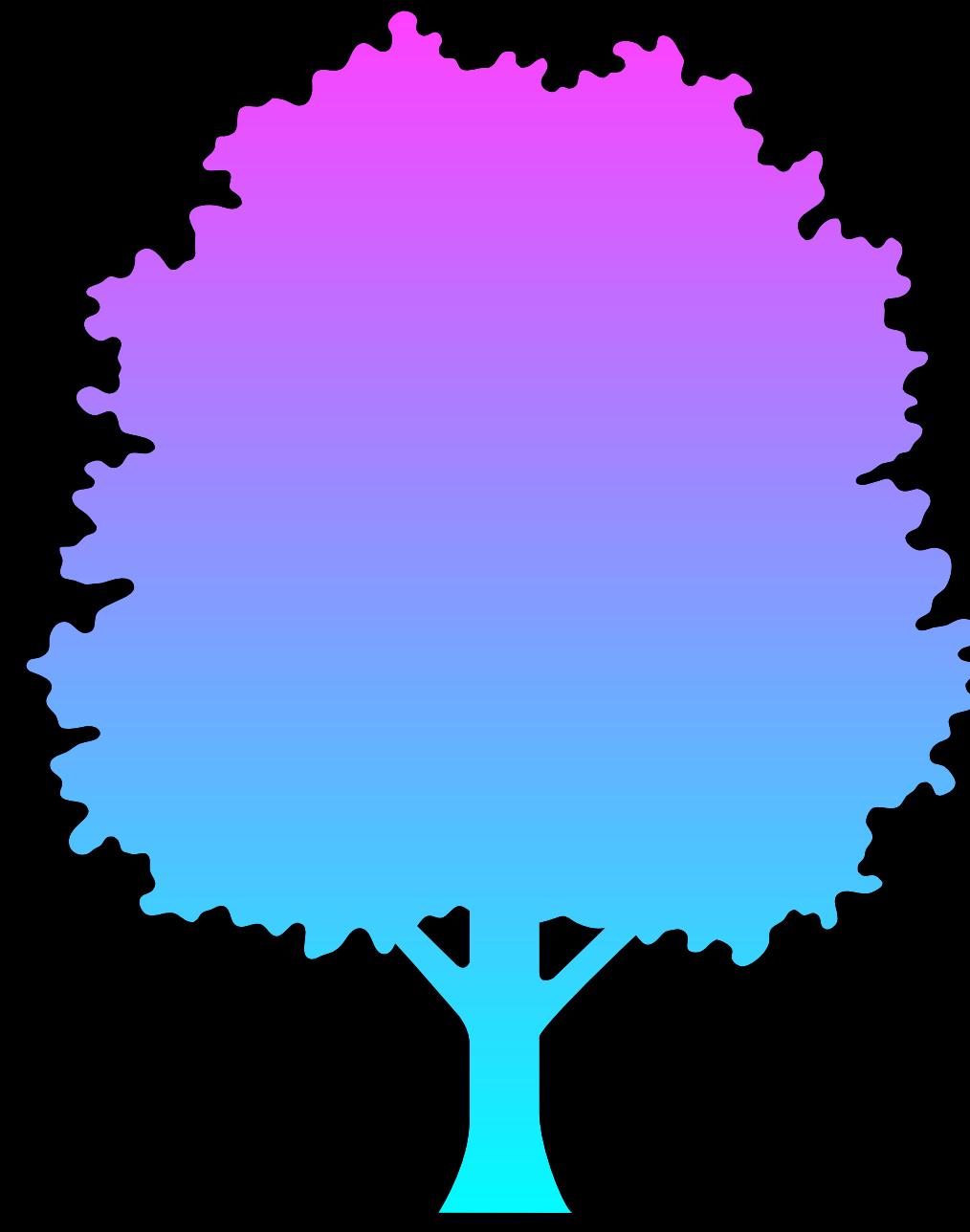


Technique  
Sophistication\*

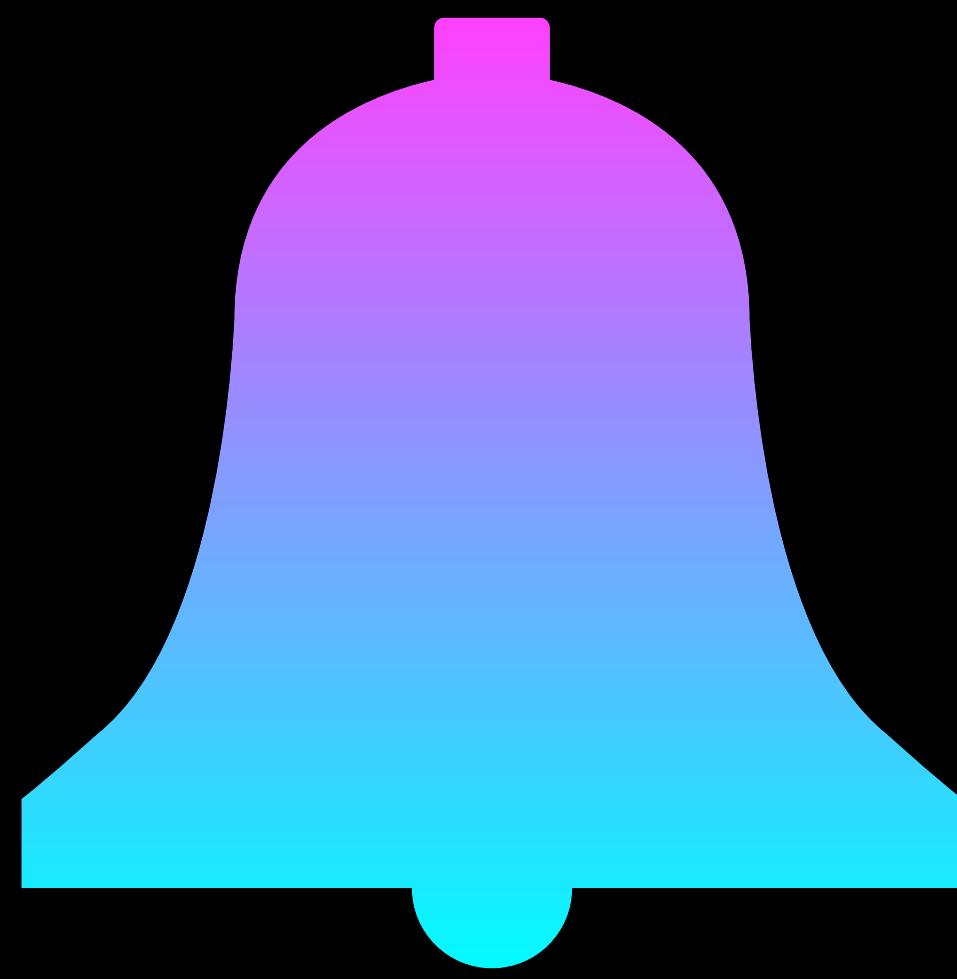
Technique Prevalence



# What data should we be collecting?



Telemetry



Alerting



Prevention

### Edit Domain Enumeration - LDAP using PowerShell Test Case

Status: Completed

Attack Start

01/16/2019 13:30:59  
status changed to InProgress

Attack Stop

01/16/2019 15:13:50  
status changed to Completed

Source IPs

Build/Run

Attacker Tools

PowerView

Target Assets

Red Team Details

Name: Domain Enumeration - LDAP using PowerShell

Description: Use PowerView v3 to perform queries against the Windows domain for common groups.

Blue Team Details

Outcome:  TBD  Blocked  Detected  NotDetected

Detecting Blue Tool(s):

Falcon Insight

Splunk

What was the alert severity?  Info  Low  TBD  Med  High  Critical

Outcome Notes: outcomeNotes

Tags:

Rules:

Sigma
Sigma
Sigma
Sigma
Sigma
Sigma
Sigma
Sigma

Detection Time

01/28/2019 17:25:59  
outcome changed to Detected

Expected Detection Layers

SIEM

Behavior Analytics

EDR

Detection

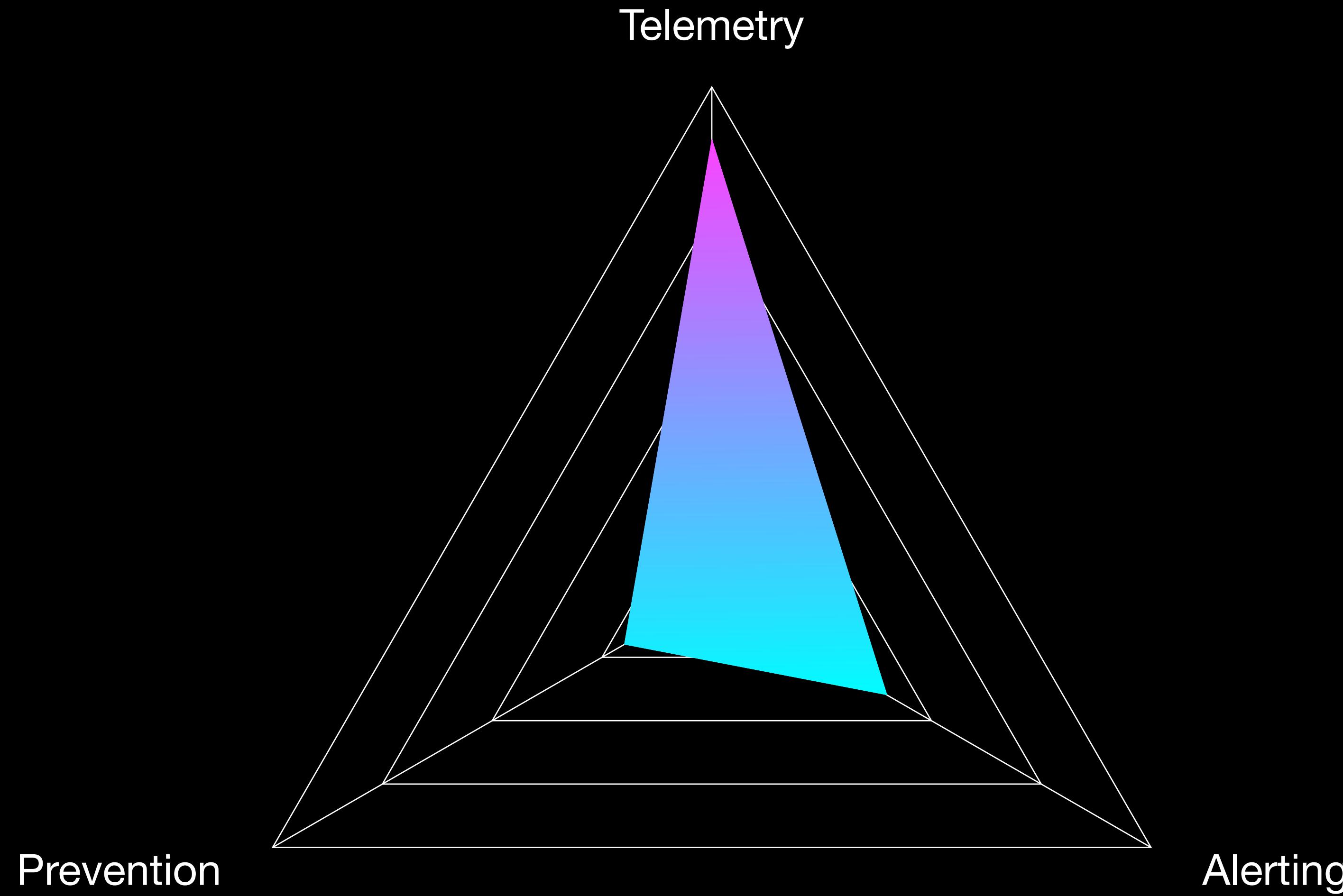
1) Windows enumeration activities detected from large amount of network traffic (SMB, ARP requests) from UEBA or network monitoring tools

2) Legacy Windows and native PowerShell commands used for enumeration are detected by EDR and/or SIEM rules

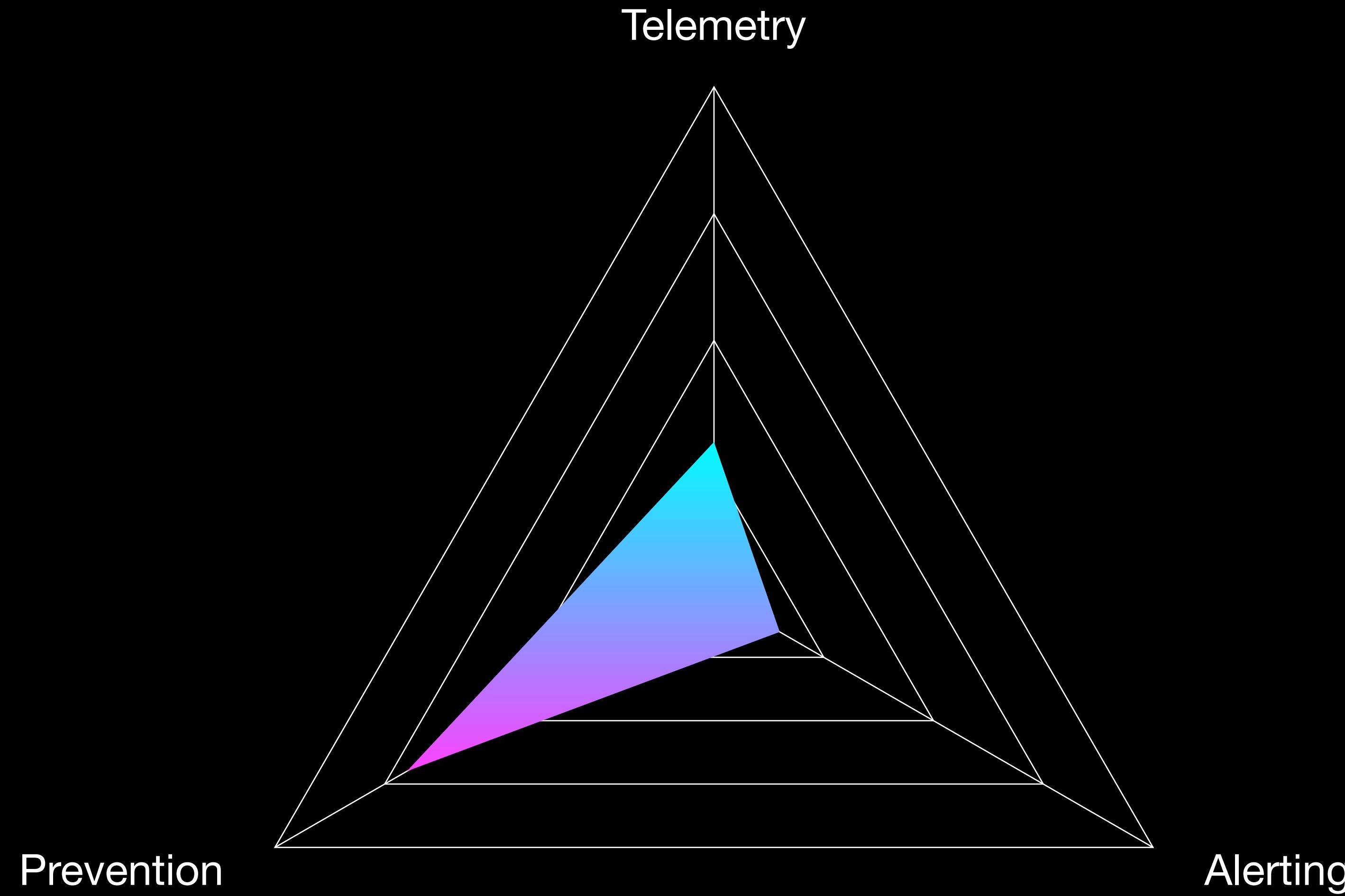
Prevention

# vector

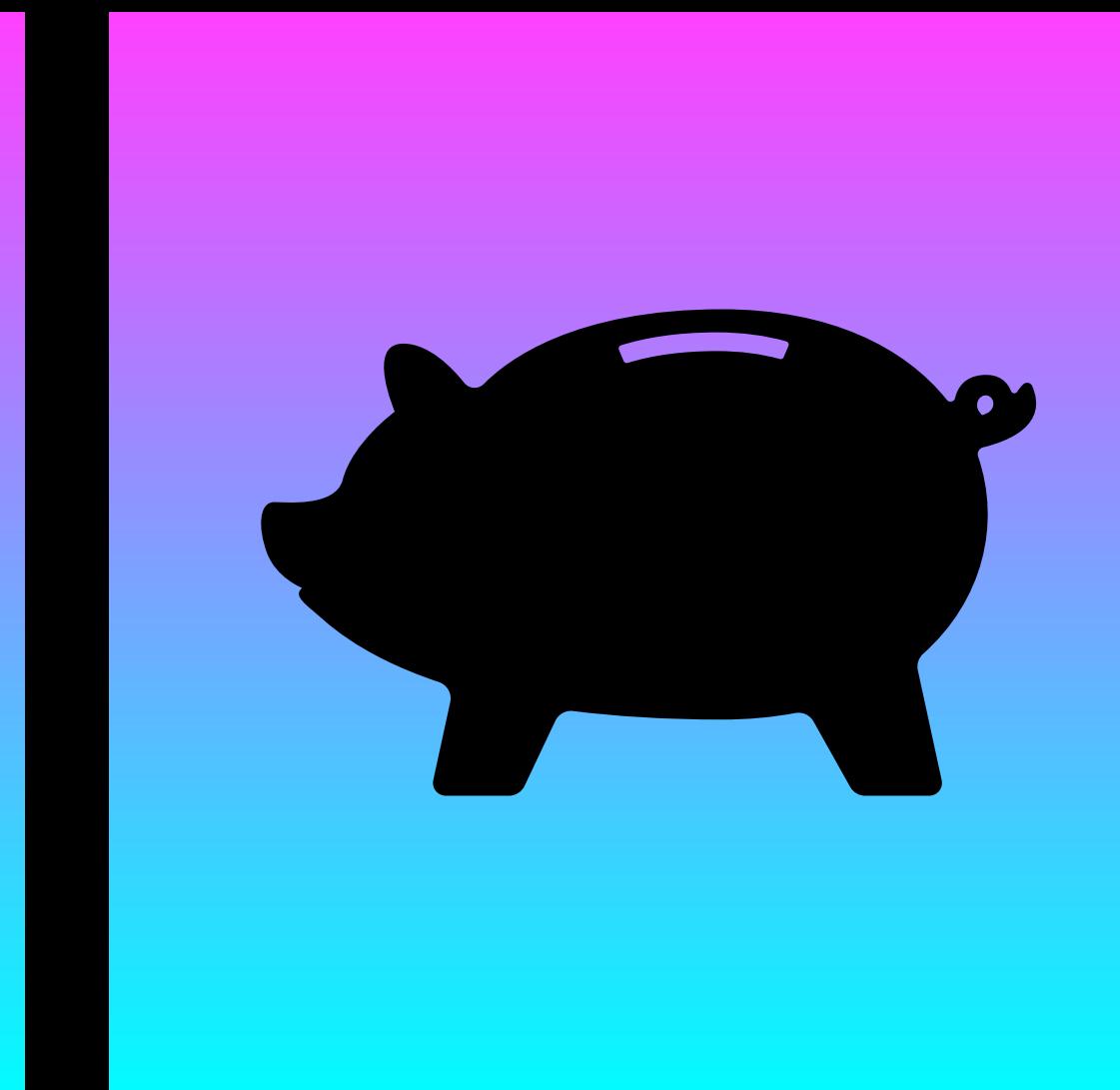
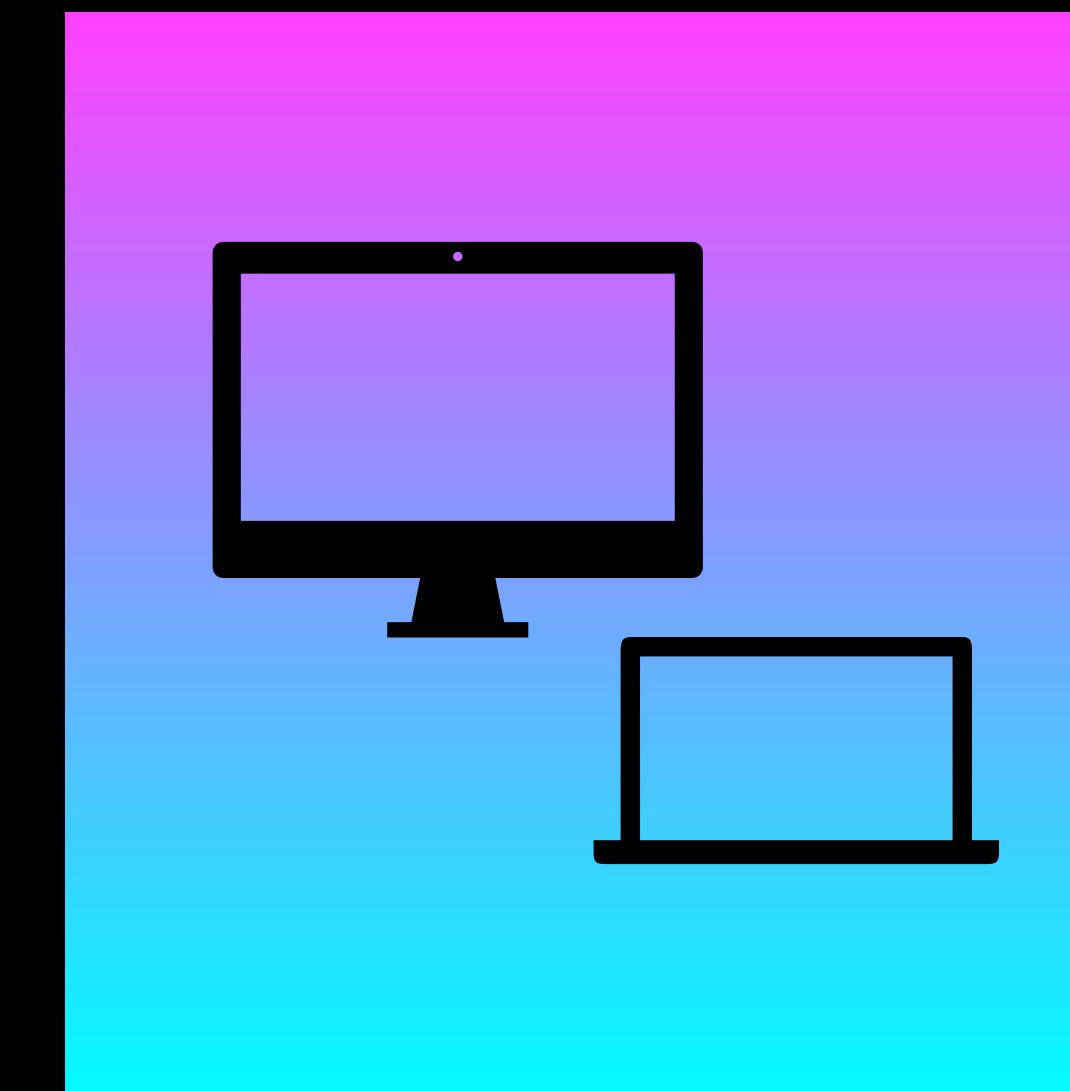
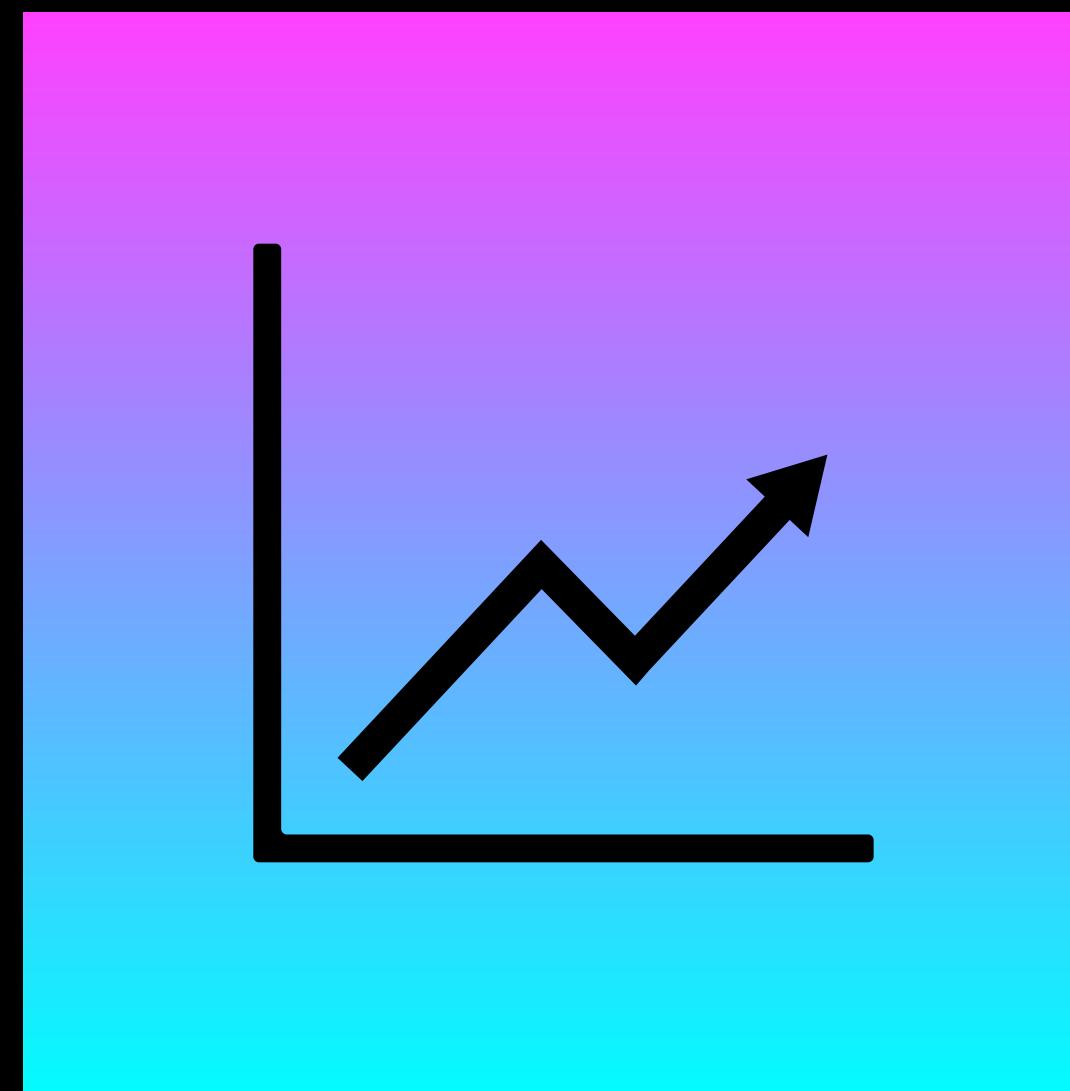
# Applying Results



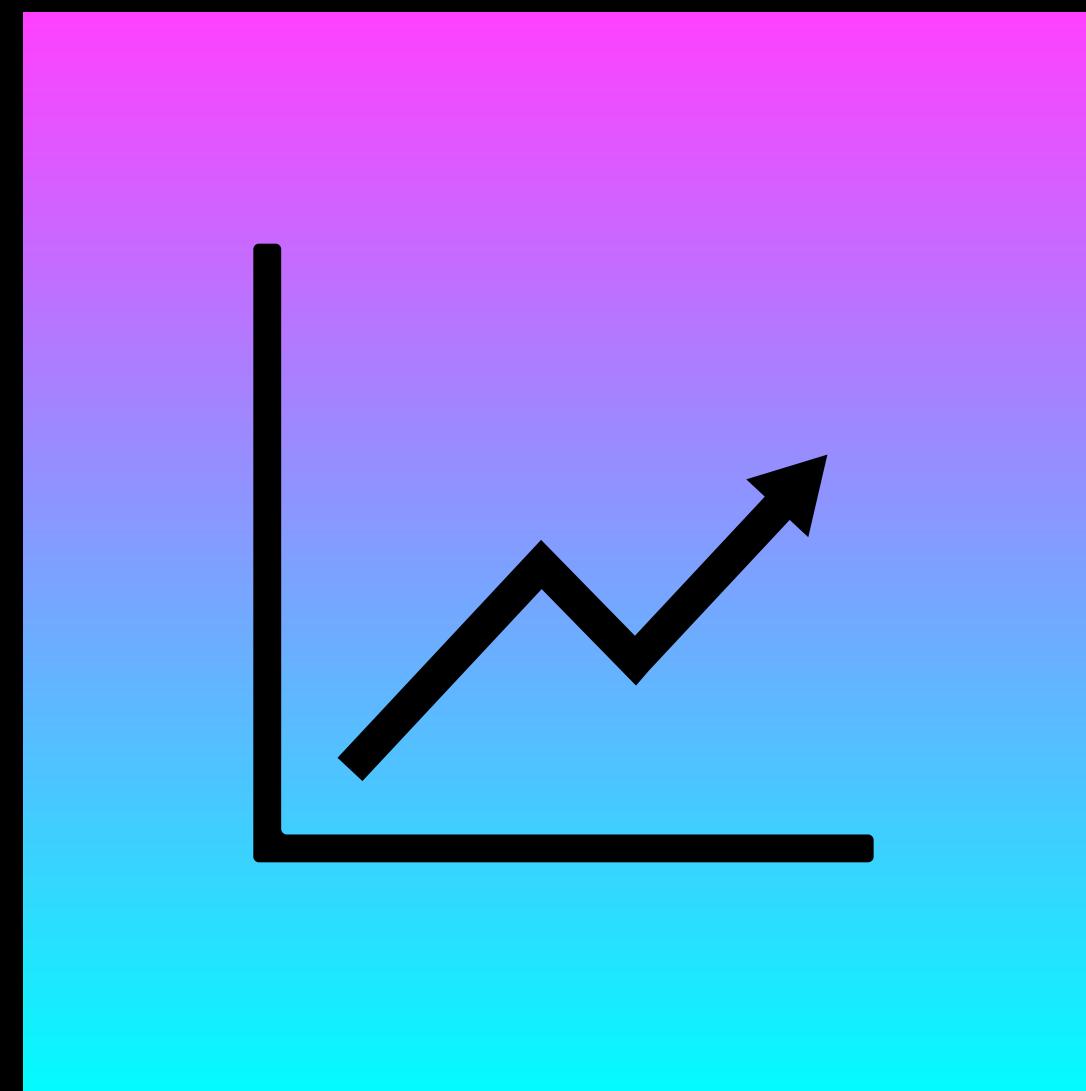
# Applying Results



# Applying Results

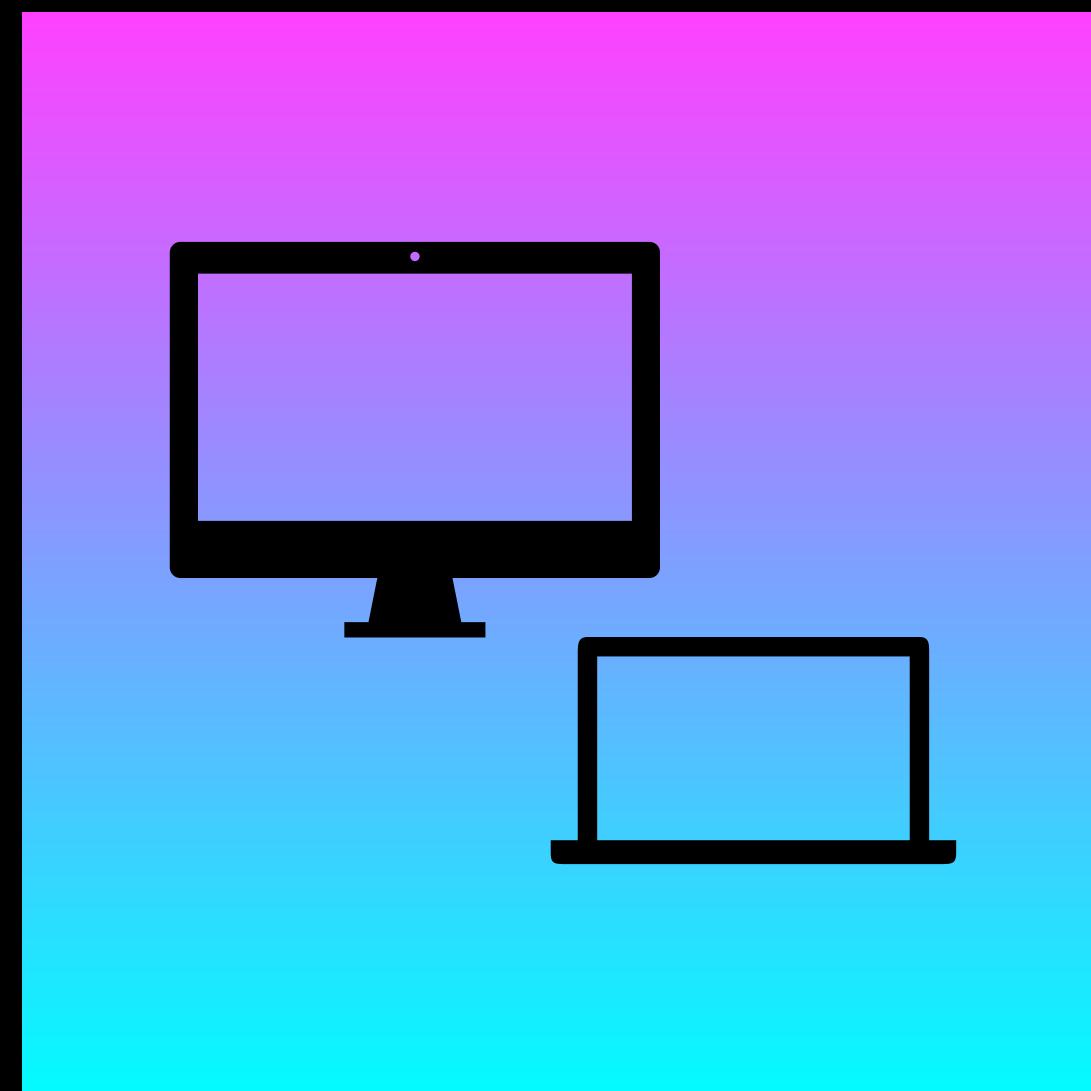


# Performance Benchmarking



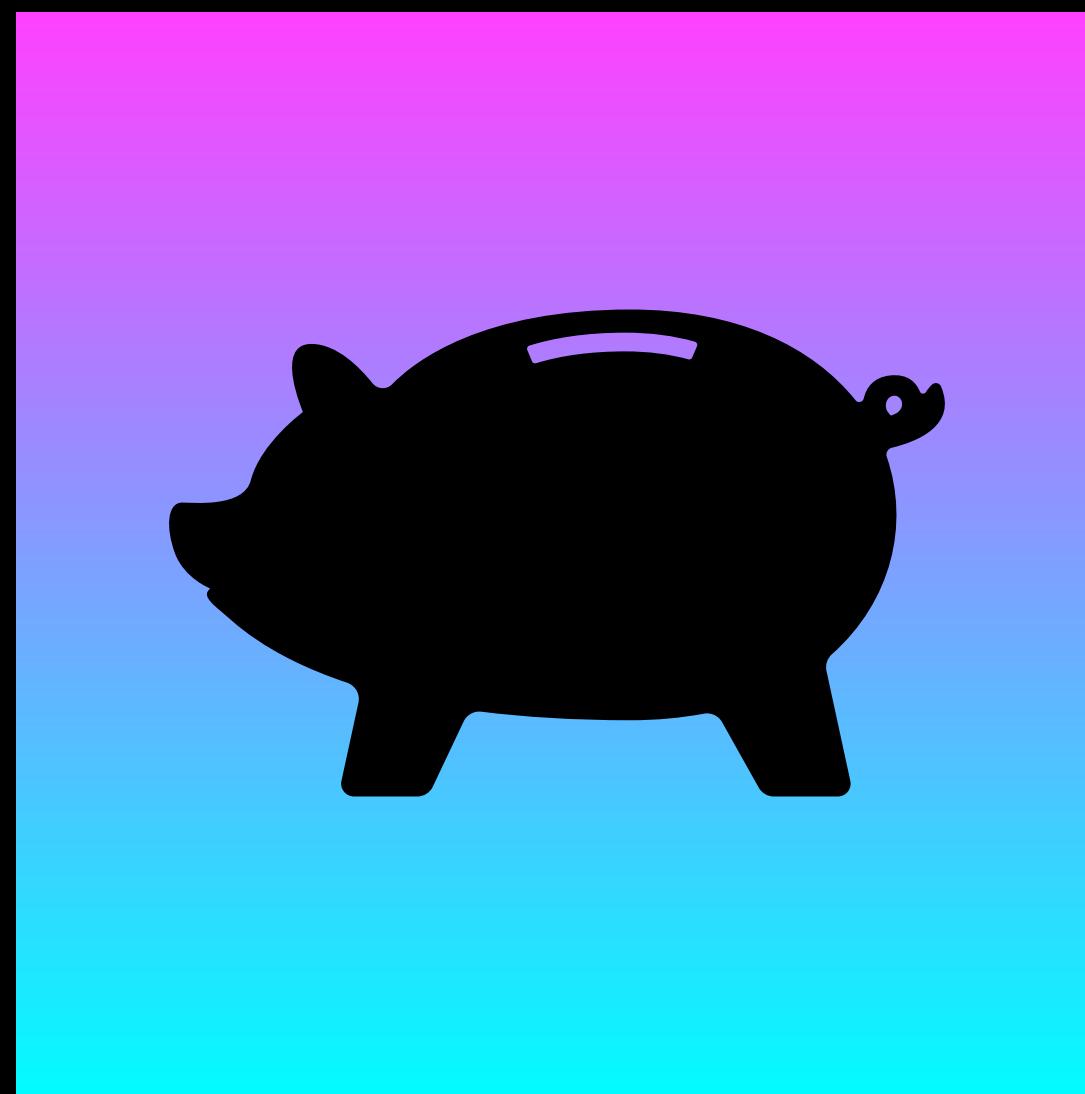
- Data-driven evidence of detective/preventative improvement.
- Challenge: TTPs evolve over time.
- Challenge: Importance of tests chosen.

# Environment Comparison



- Is there variance in your capability across regions? Across endpoint builds? On-premise vs. Virtualised?
- Challenge: Relevance of TTPs across infrastructure.

# Return on Investment



- Out of the box detections? Custom rule capability?  
Are we getting the most out of what we've paid for?
- Challenge: Raw Telemetry != Viable Alert.
- Challenge: DCSync > Whoami

# Industry Comparison



- Benchmark comparison against your peers.
- Challenge: Pleasing senior leadership!
- Challenge: Experience in capability development.

# Weaknesses of Atomic Testing

- Plays into a ‘MITRE ATT&CK Whac-A-Mole’ mindset
- Doesn’t test response playbooks and processes
- Good ‘atomic’ performance isn’t the whole story
- Maturity required to gain value and digest results



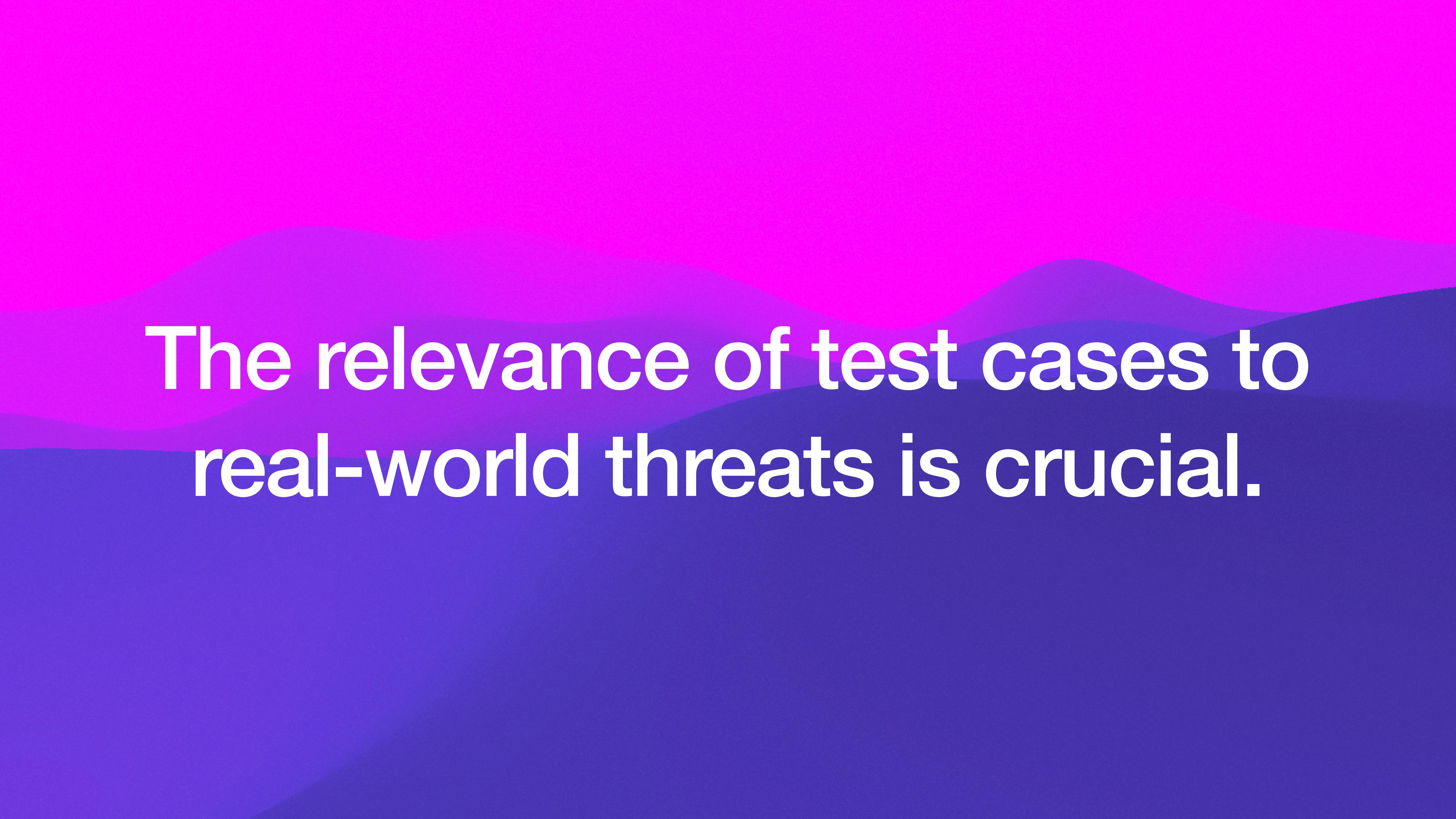
# Takeaways



Atomic testing can inform strategy,  
prioritisation and investment.



Atomic testing is invaluable to  
detection engineering.



The relevance of test cases to  
real-world threats is crucial.



Automation makes atomic  
testing scalable and repeatable.



Atomic testing is not a replacement  
for other offensive testing.

# Questions?



@ajpc500



[github.com/ajpc500](https://github.com/ajpc500)



[ajpc500.github.io](http://ajpc500.github.io)

