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

Offense

Informs

Defense

Red Team

Informs

Defense

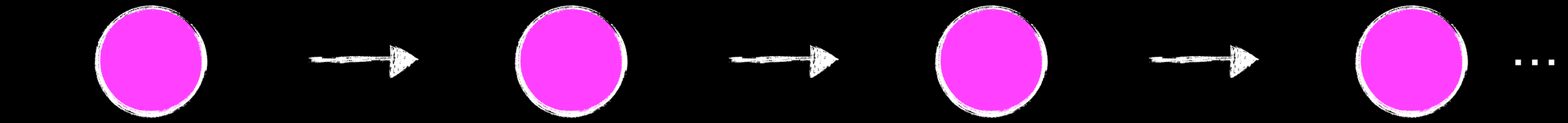
Table Top

Informs

Defense

Atomic Purple Team?

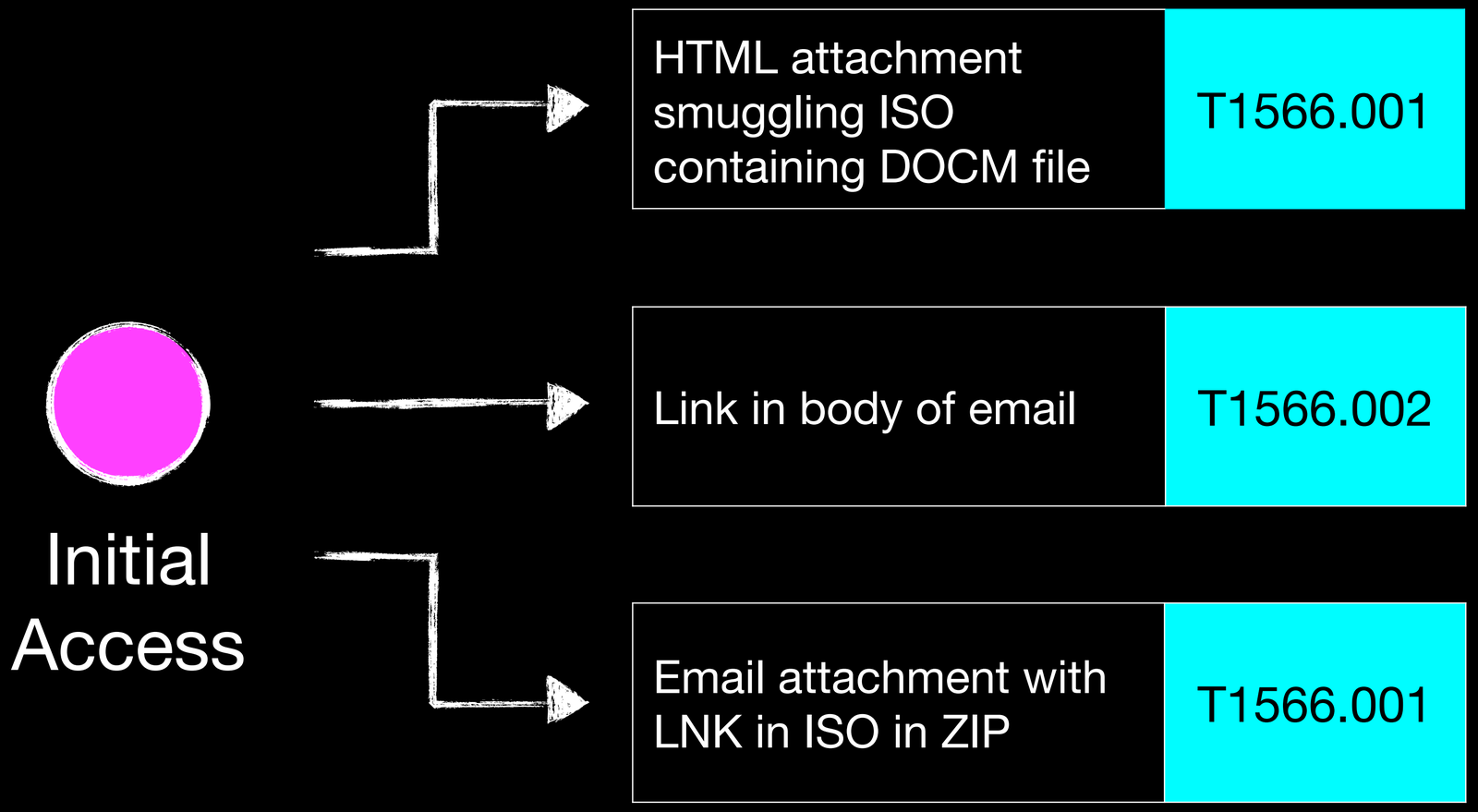
Objective-Led Attack Path

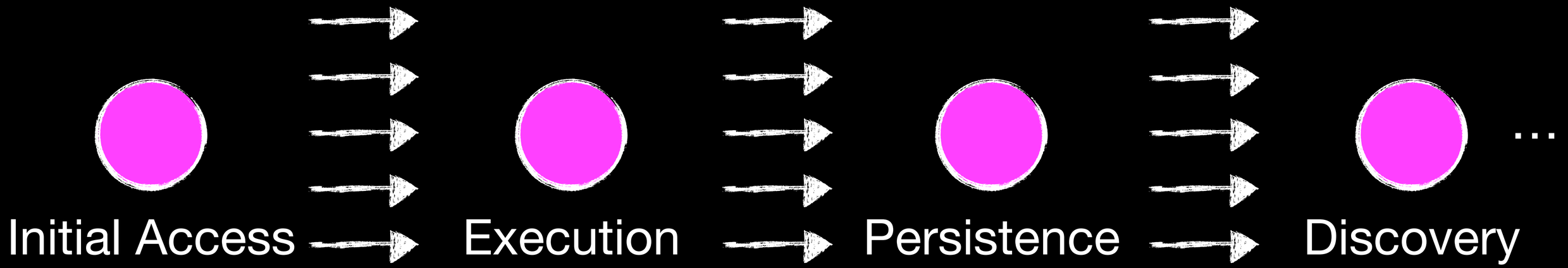


Initial Access → Execution → Persistence → Discovery → ...

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 


Initial Access
HTML attachment smuggling ISO containing DOCM file
T1566.001
Link in body of email
T1566.002
Email attachment with LNK in ISO in ZIP
T1566.001

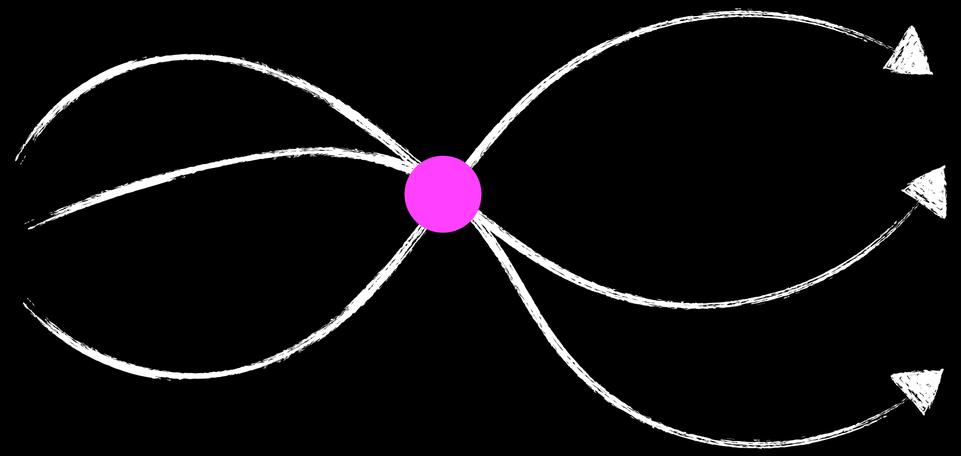

Initial Access
Execution
Persistence
Discovery
...

What should we execute?

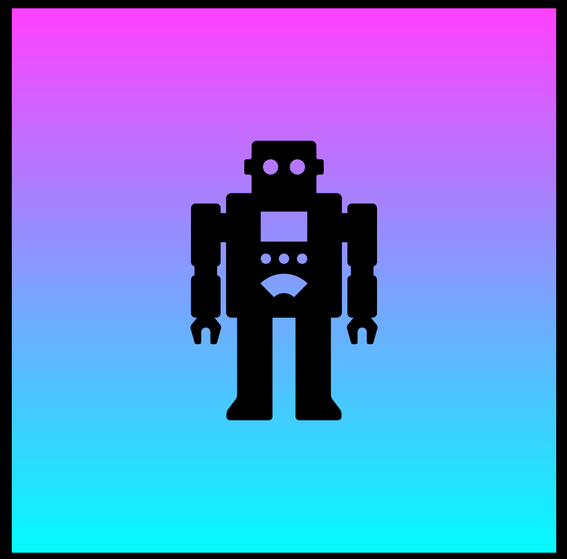
What should we execute?

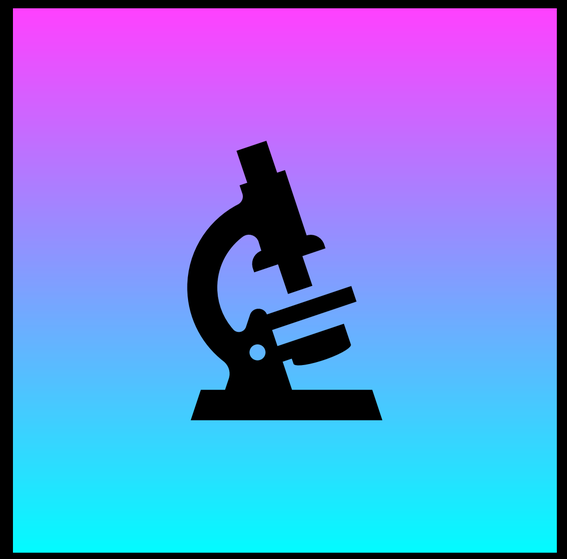
Sources of techniques:

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

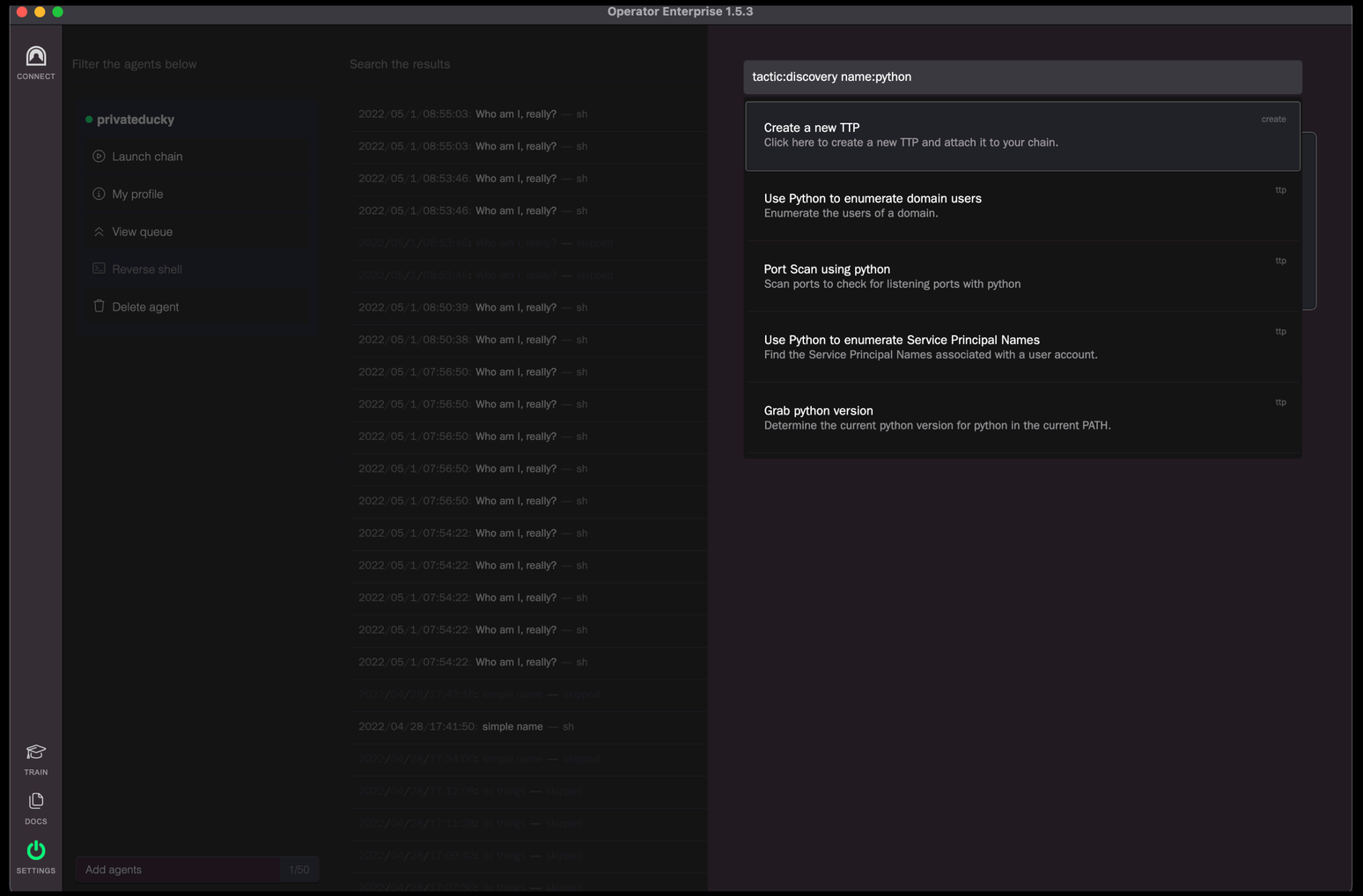


What should we execute?





[P]



https://www.prelude.org

T1087.002 - Domain Account Discovery

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

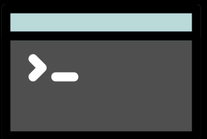
```
net group “Domain Admins” /domain
```

```
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

```yaml
title: Suspicious Reconnaissance Activity
id: d95de845-b83c-4a9a-8a6a-4fc802ebf6c0
status: experimental
description: Detects suspicious command line activity on Windows systems
author: Florian Roth, omkar72, @svch0st
date: 2019/01/16
modified: 2022/06/09
references:
    - https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
    - https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/
tags:
    - attack.discovery
    - attack.t1087.001
    - attack.t1087.002
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - net group "domain admins"
            - net localgroup administrators
            - net group "enterprise admins"
            - net accounts /do
    condition: selection
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Inventory tool runs
    - Administrative activity
analysis:
    recommendation: Check if the user that executed the commands is suspicious (e.g. service accounts, LOCAL_SYSTEM)
level: medium
```

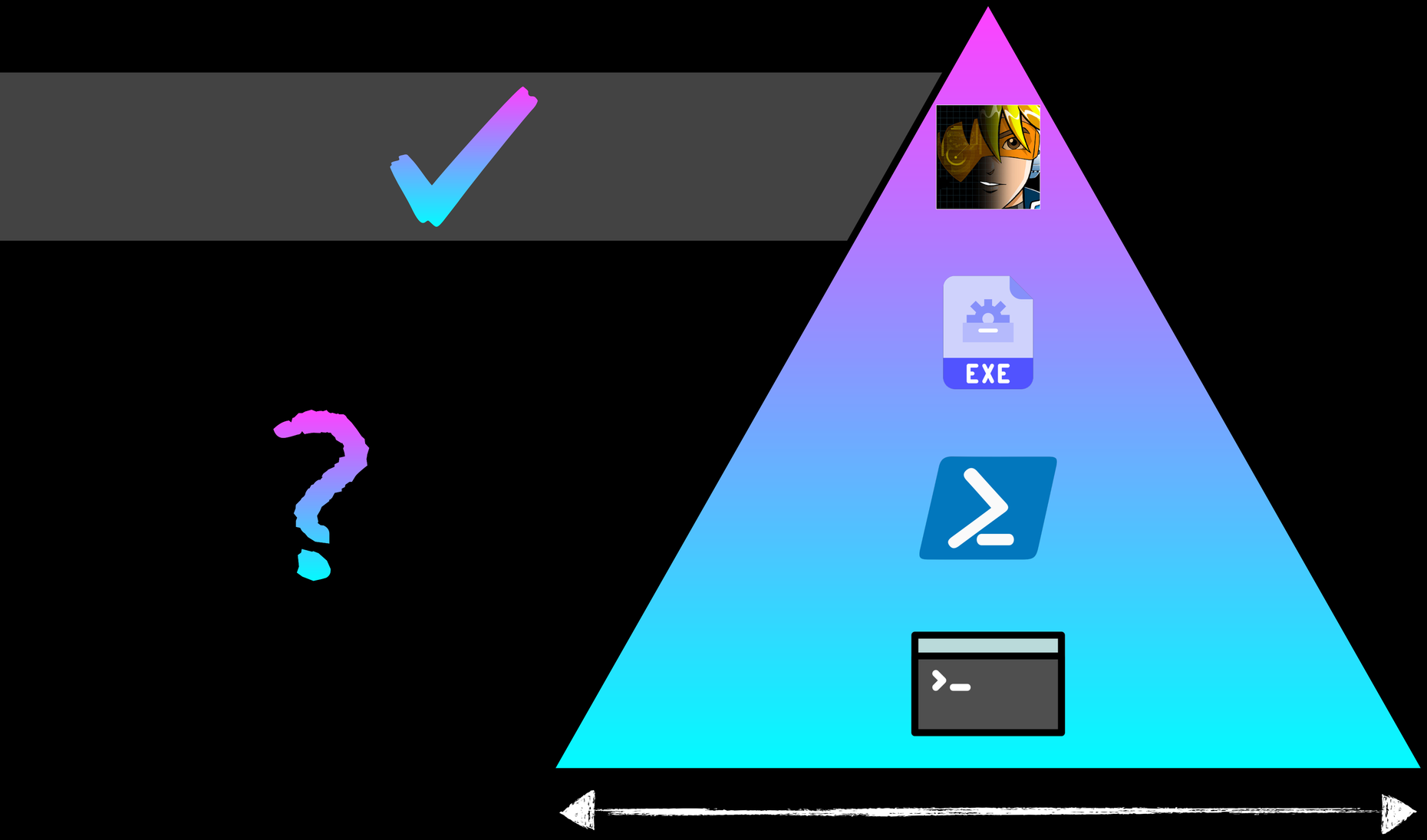
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_susp_recon_activity.yml

T1087.002 - Domain Account Discovery

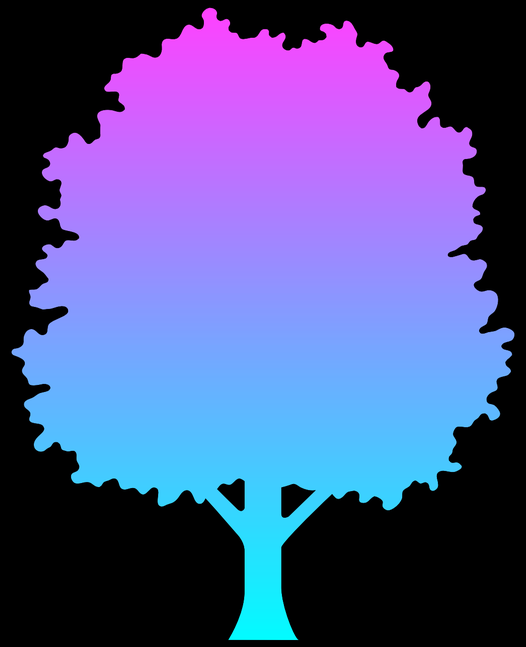
```
set GROUP="Domain Admins" /domain
n^e^t g^r^o^u^p %GROUP% /d^o
```

T1087.002 - Domain Account Discovery

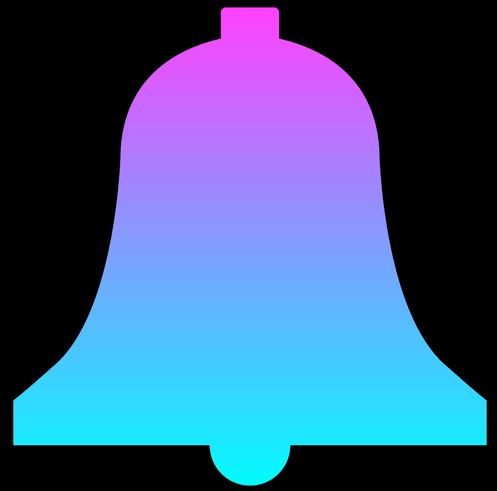
```
ldapsearch “CN=Domain Admins” member
```


EXE
Technique Sophistication*
Technique Prevalence

What data should we be collecting?

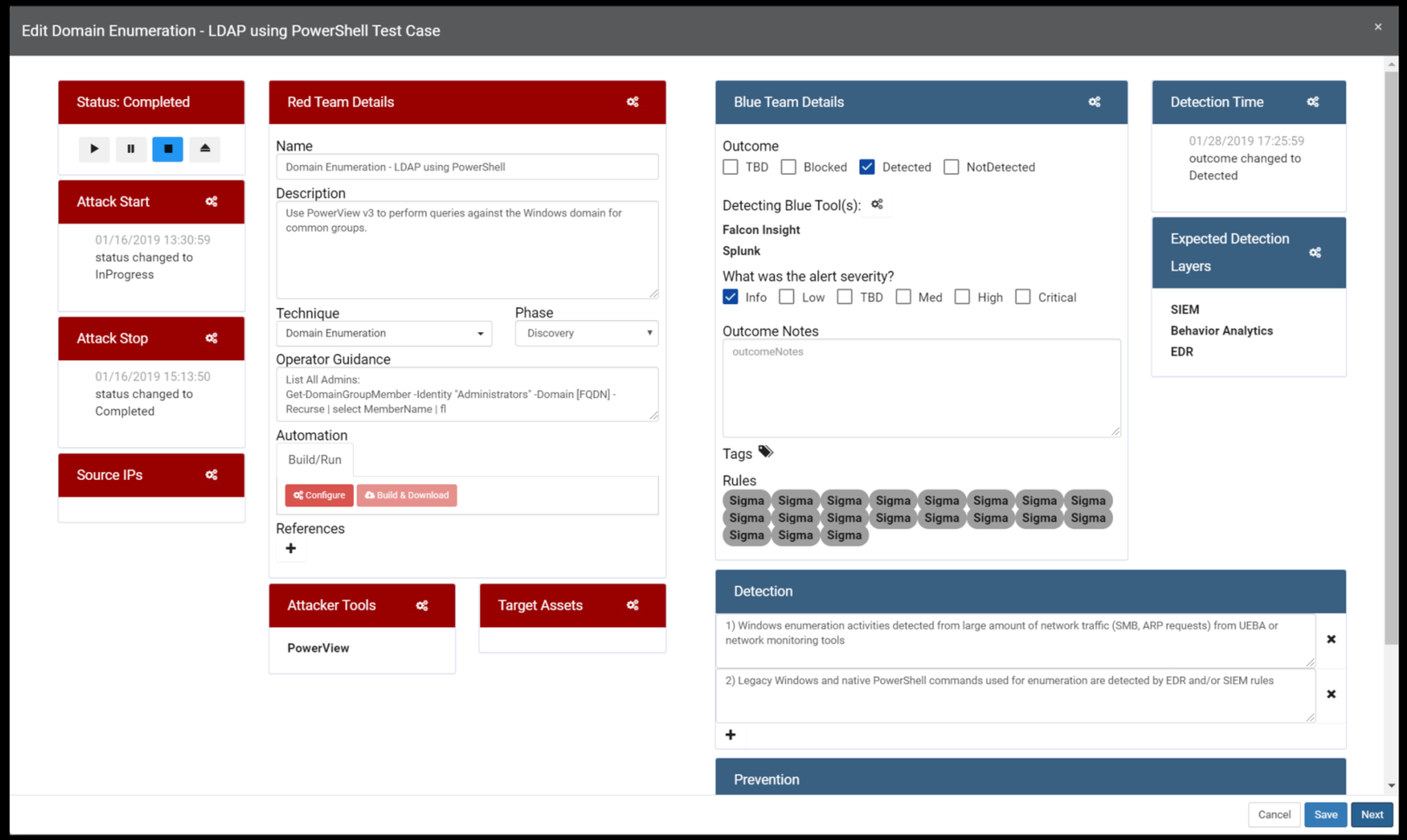


Telemetry



Alerting

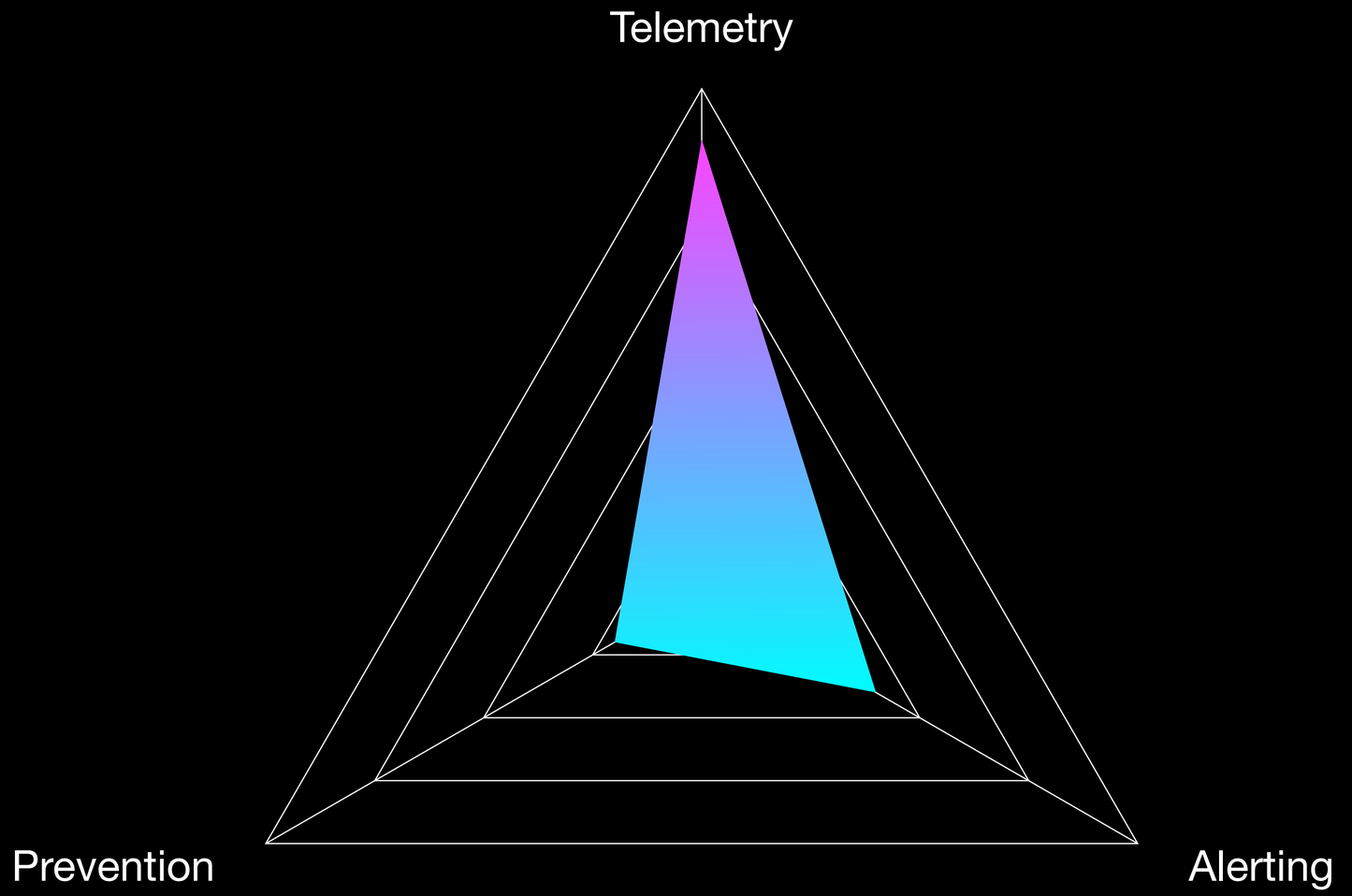
Prevention



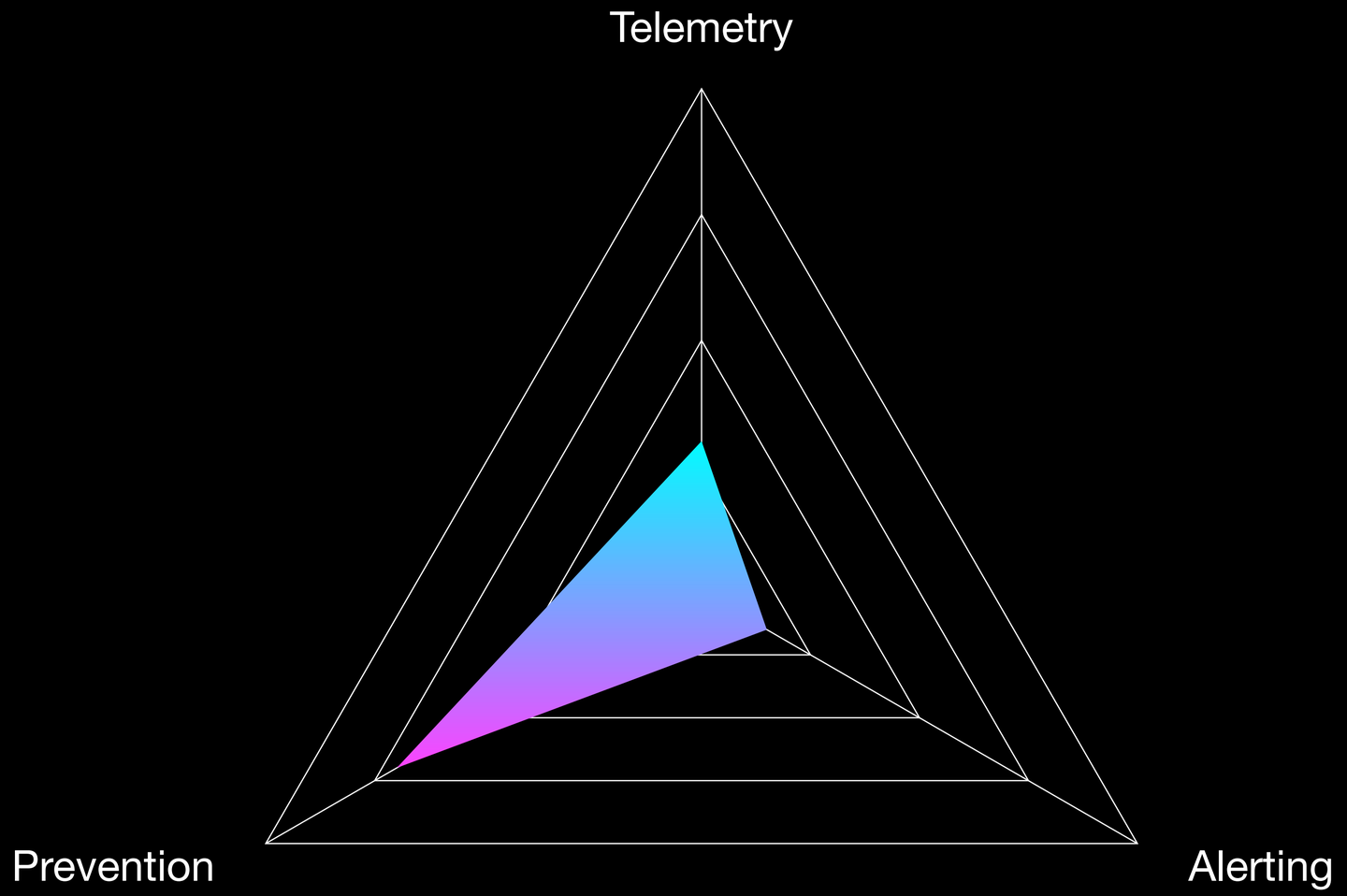
vectr

https://github.com/SecurityRiskAdvisors/VECTR

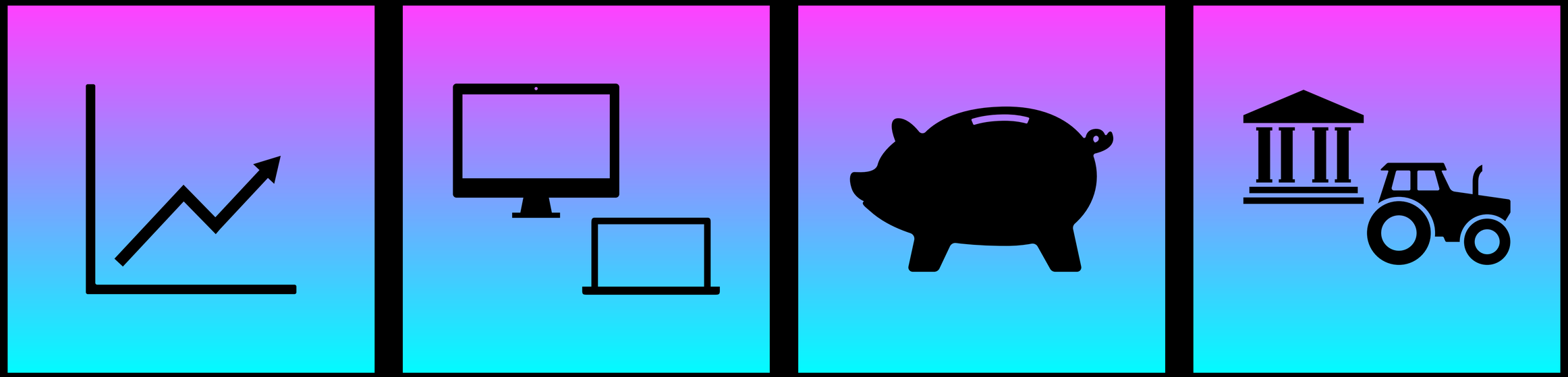
Applying Results



Applying Results



Applying Results

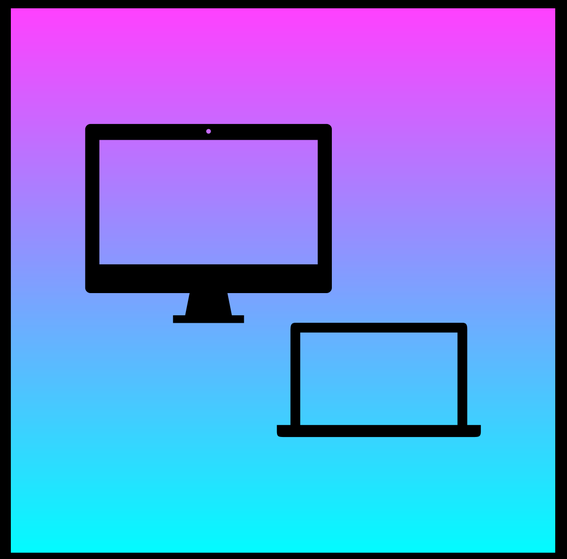


Performance Benchmarking

- 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

ajpc500.github.io