Adversary Village at DEF CON 33

LETTHEMIN

Facilitating High-Value Purple Teams Using an Assumed Compromise Approach

Sarah Hume



Adversary Village at DEF CON 33



#WHOAMI

- Sarah Hume
- Purple Team Service Lead @ Security Risk Advisors
- Certifications: CISSP, CRTO, AWS CCP, Google CDL
- Philadelphia, PA (go birds)
- Dog mom

Adversary Village at DEF CON 33



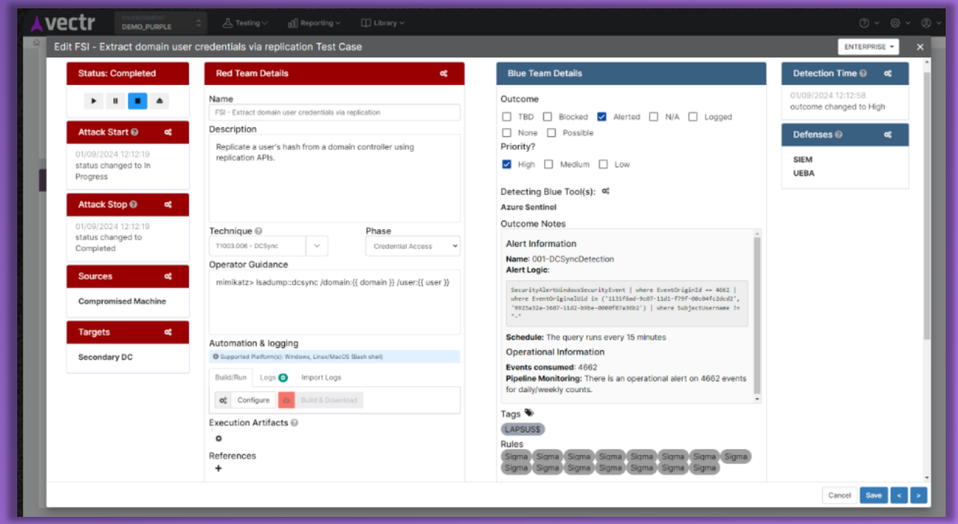
AGENDA

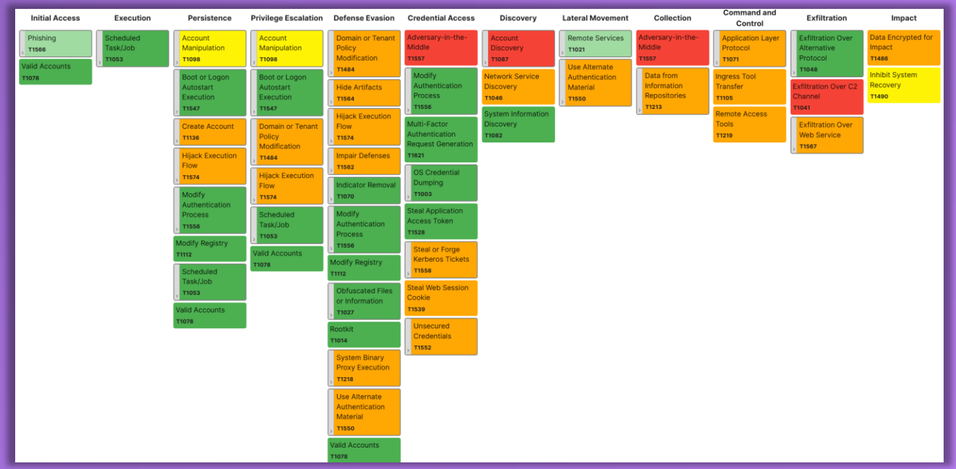
1. Introduction
2. Defining Purple Team Terminology
3. Applying the Assumed Compromise Approach
4. Collecting and Analyzing Results
5. Conclusion

Adversary Village at DEF CON 33

PURPLE TEAM TERMINOLOGY

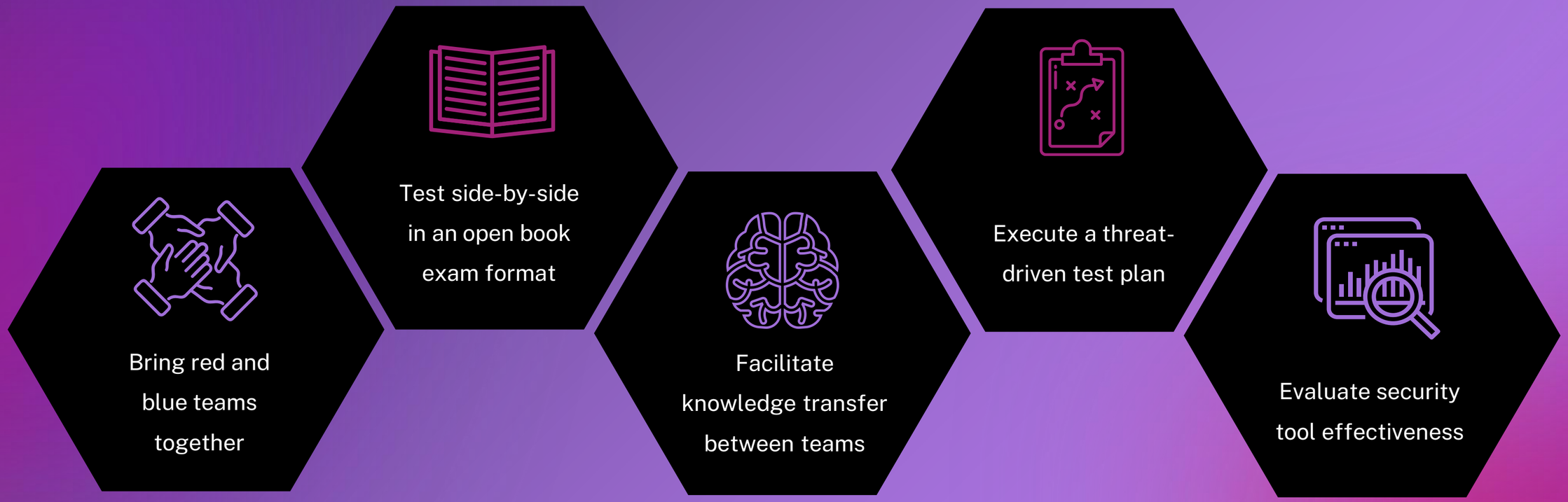
- Threat Intelligence
- MITRE ATT&CK Framework
  - Tactics, Techniques, and Procedures (TTPs)
  - Adversary PEMDAS
- Red Team
  - Red team engagement vs pen test
- Blue Team
- Red + Blue = Purple Team
- Purple Team Engagement = Collaborative Workshop
- Assumed Compromise Approach





Adversary Village at DEF CON 33

PURPLE TEAM IS



Adversary Village at DEF CON 33

PURPLE TEAM IS NOT

BAS

Adversaries cannot fully automate their operations, and neither should your approach to realistic simulations.

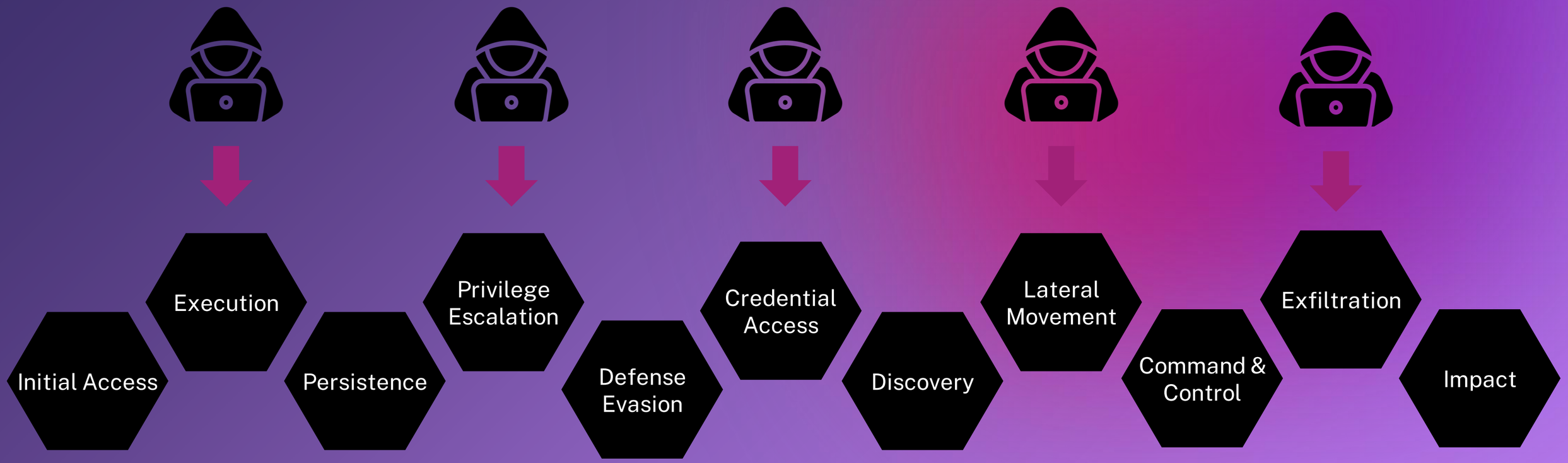
RED

Tests your incident response processes by demonstrating realistic paths to compromise of pre-set flags.

PENTEST

Identifies vulnerabilities and risky configurations that could allow access to sensitive data or cause business impact.

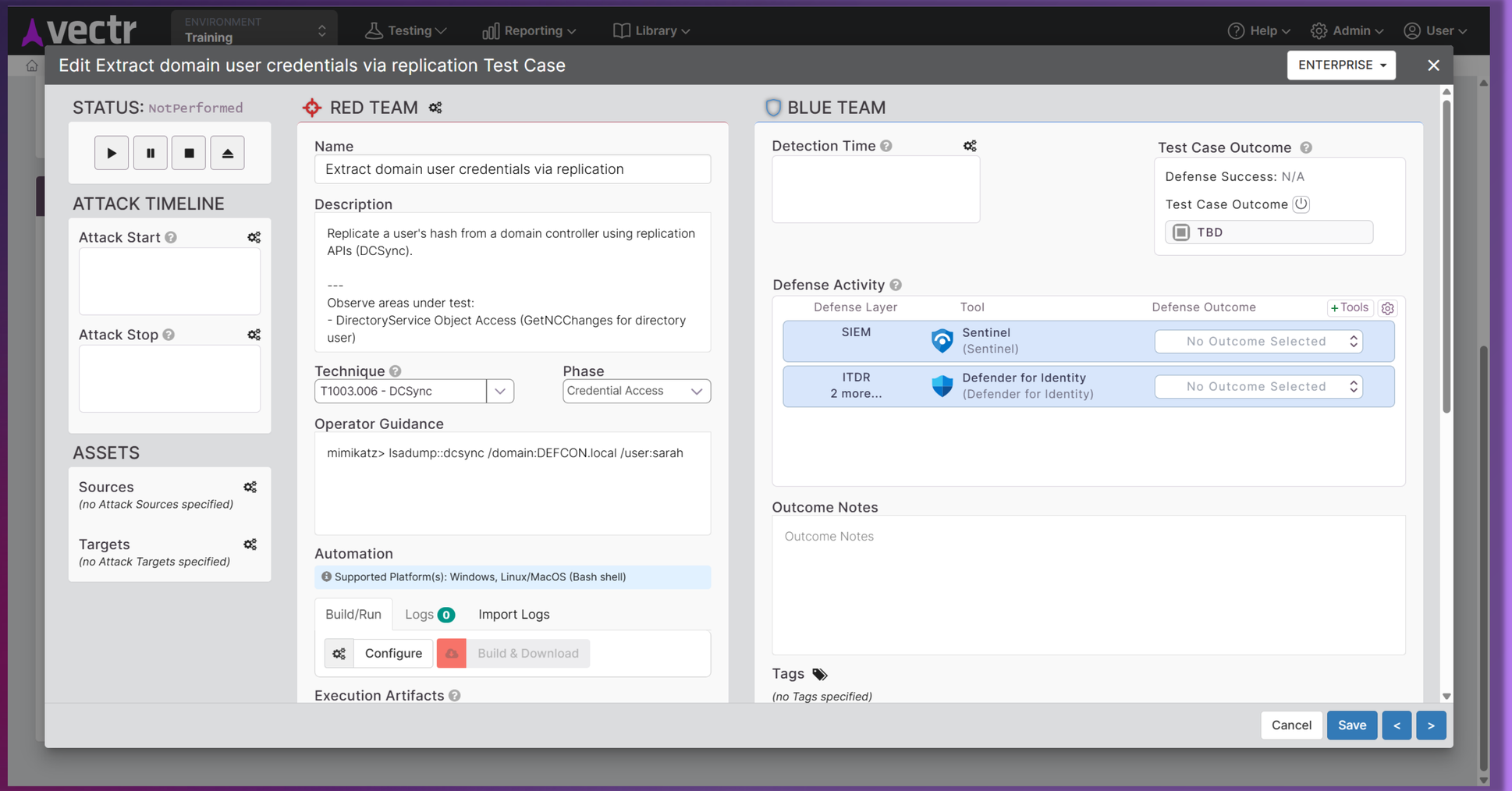
Adversary Village at DEF CON 33



ASSUMED COMPROMISE APPROACH

Adversary Village at DEF CON 33

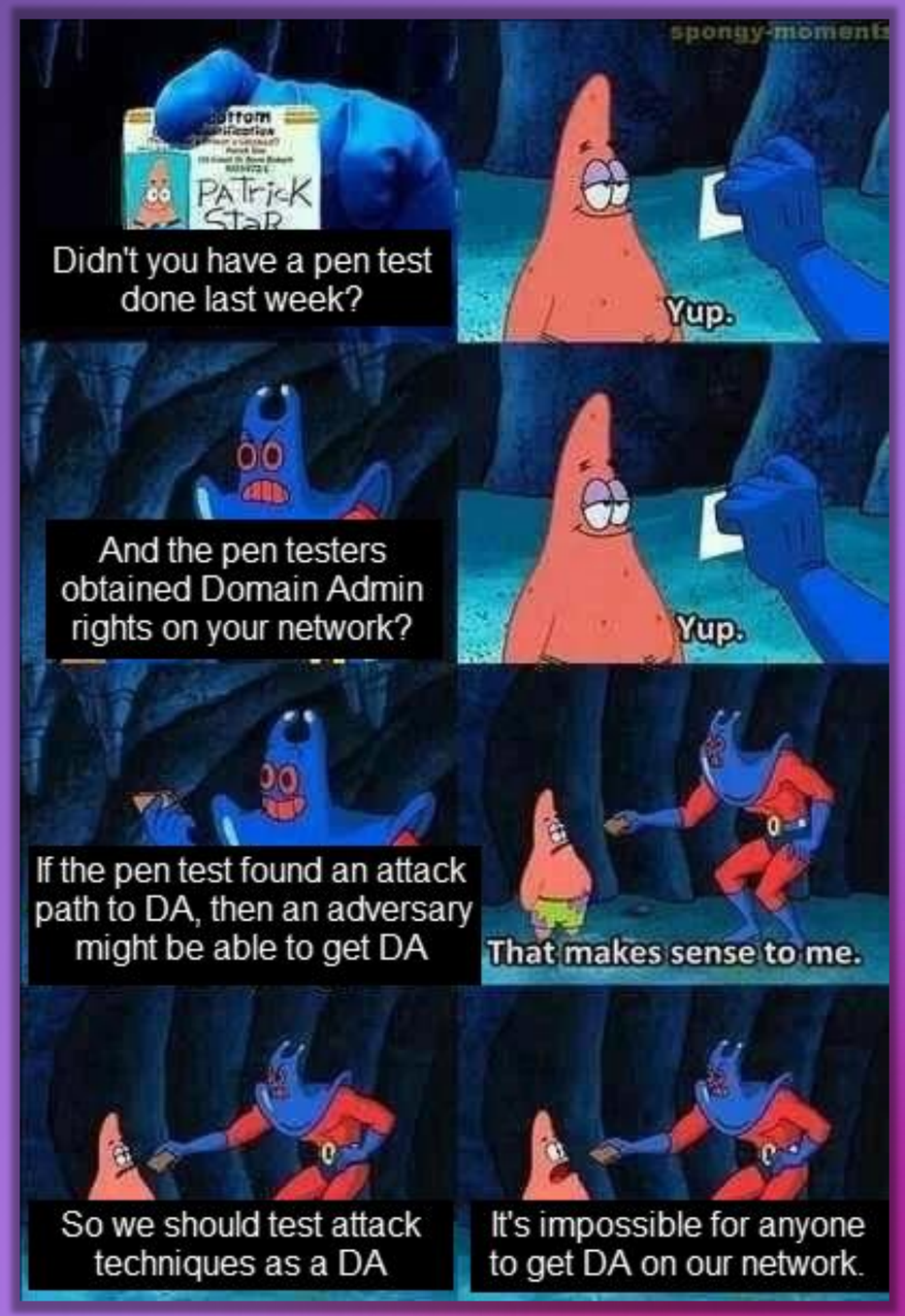
EXAMPLE SCENARIO:



Adversary Village at DEF CON 33

VISIBILITY, NOT VULNERABILITY

- We know any organization can be vulnerable at a point in time
- Assume the stage is set for the attack to run
- Focus on attacker visibility following their entry into a network
- If the worst happens, what can we detect? What can we prevent? (Do our security tools really do what we think they do / what we paid for them to do?)
- Full supervision = low risk
- Lower likelihood (often)= higher impact
  - Take DCSync, for example…

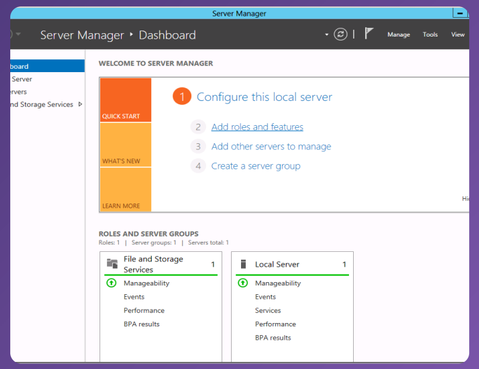


Adversary Village at DEF CON 33

RUNNING DCSYNC

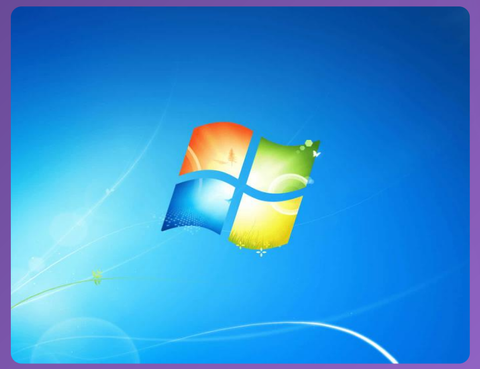
We've granted our red operators DA rights. Now they are running DCSync...

DOMAIN CONTROLLER



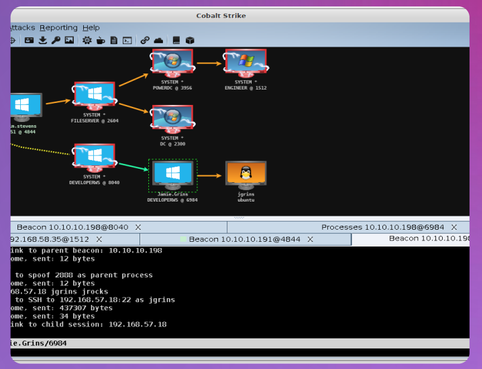
Blocked by Privileged Access Management solution

USER WORKSTATION



Blocked by Endpoint Detection & Response

COBALT STRIKE C2



Blocked by Next Generation Firewall

BUT WHAT IF THE ADVERSARY...?

Adds a rogue workstation to the domain

Breaks into your office building and plugs into your network

Is an insider threat

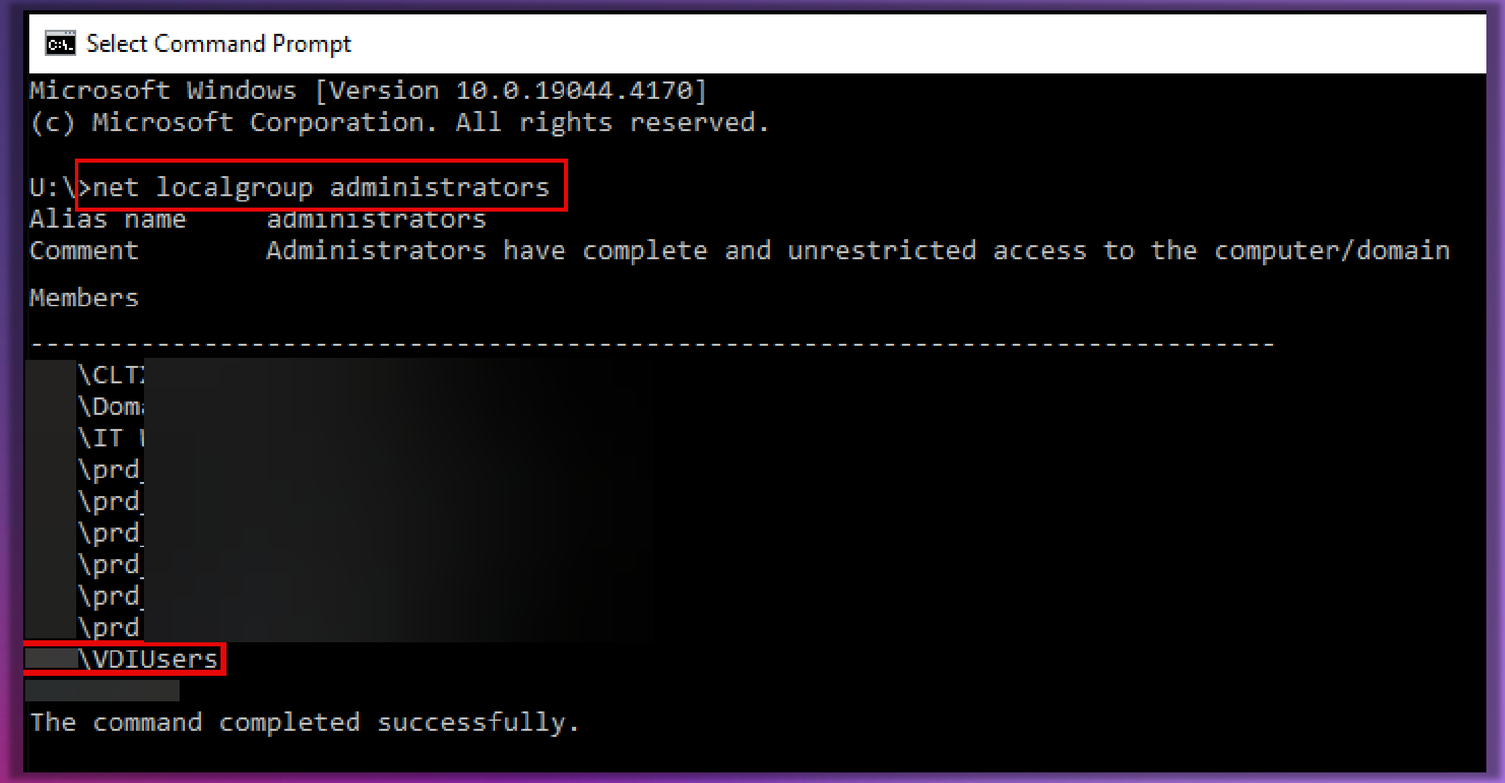
Makes direct RPC calls from a SOCKS proxy or C2 with unsignatured traffic patterns

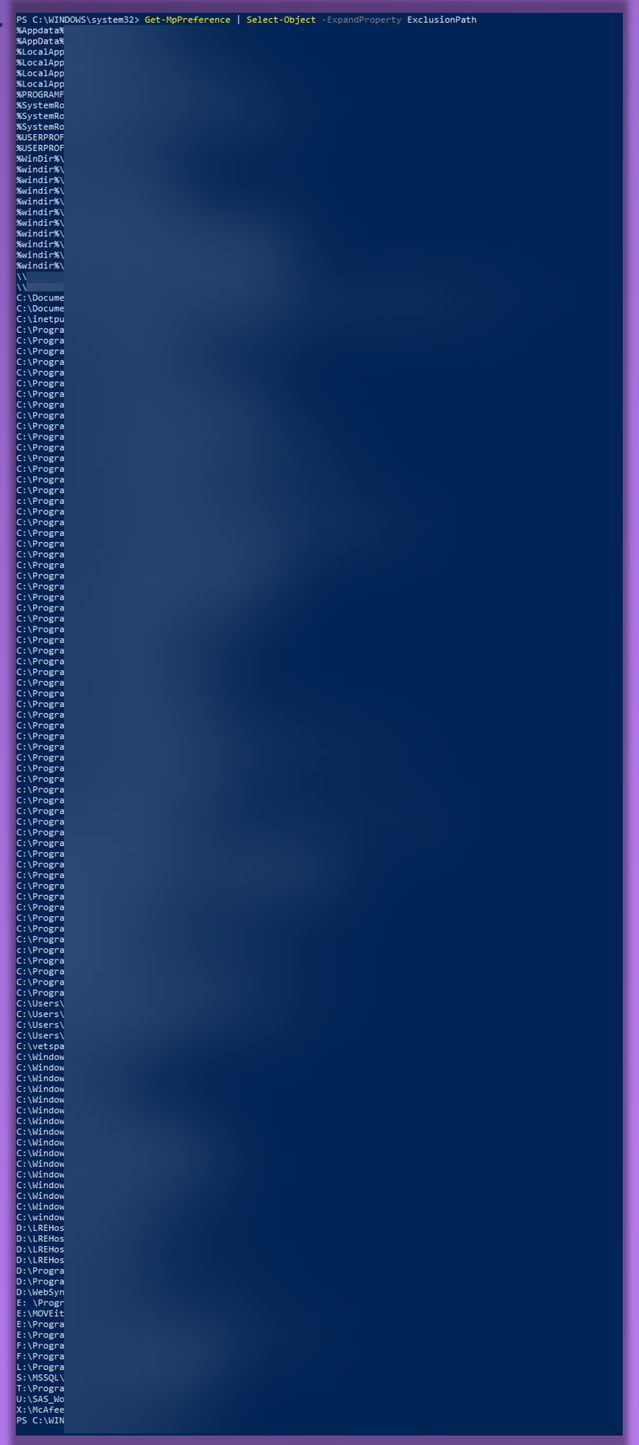
Runs from a Linux server with lackluster endpoint protection

Uses a payload unrecognized by AV static signatures (WHAT?!?!?!?)

```
PS C:\Windows\system32>  Get-MpPreference | Select-Object -ExpandProperty ExclusionPath
```

Adversary Village at DEF CON 33





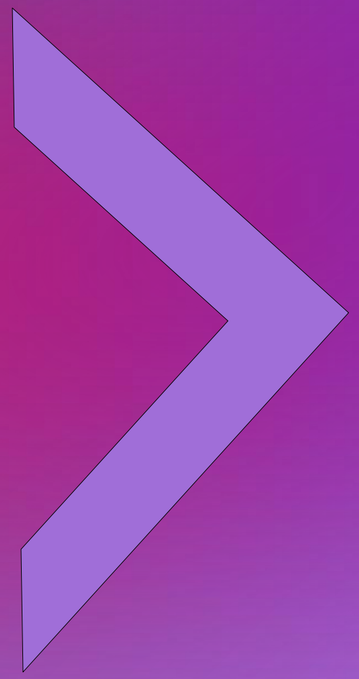
IT MAY NOT BE AS CHALLENGING AS YOU THINK...

Adversary Village at DEF CON 33

PLS HELP WHAT DO

No matter how the attacker tweaks their approach...

Mimikatz
Secretsdump
PowerShell script
Fancy custom-built tool
On a DC
On a workstation
Remote from a C2
Workstation added to the domain
Rogue device on the network
..and more variations..

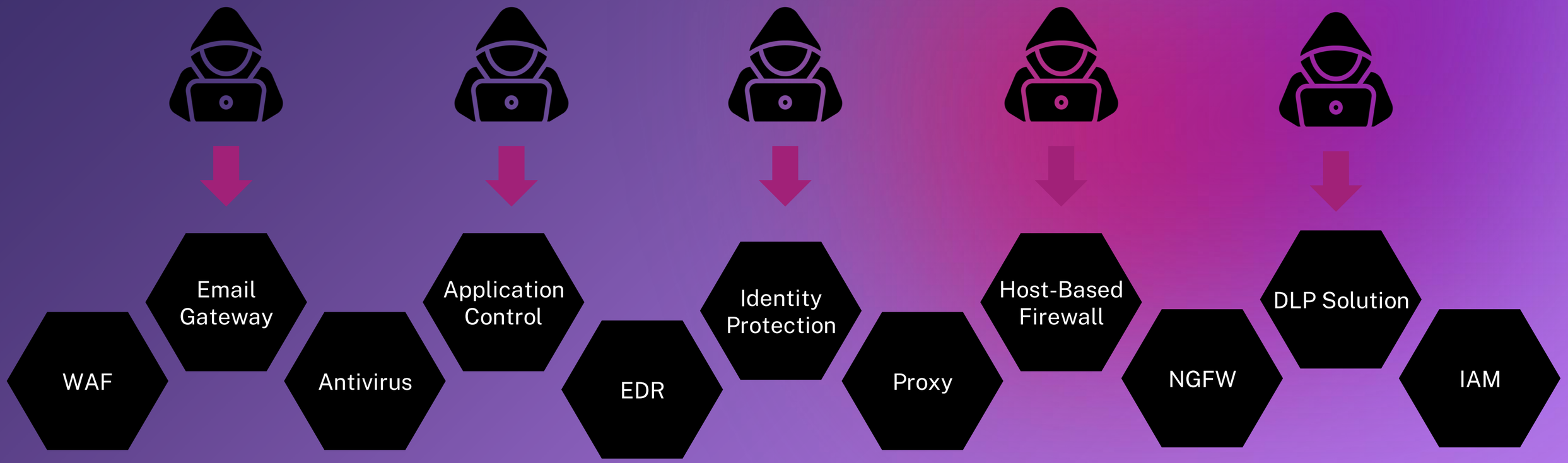


The underlying activity is the same...

Directory Service Object Log
Windows Security Event ID 4662
AccessMask 0x100
GUID
1131f6ad-9c07-11d1-f79f-00c04fc2dcd2 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2
9923a32a-3607-11d2-b9be-0000f87a36b2
89e95b76-444d-4c62-991a-0facbeda640c

RPC Call
Interface: DRSUAPI RPC interface
Function: IDL_DRSGetNCChanges

Adversary Village at DEF CON 33

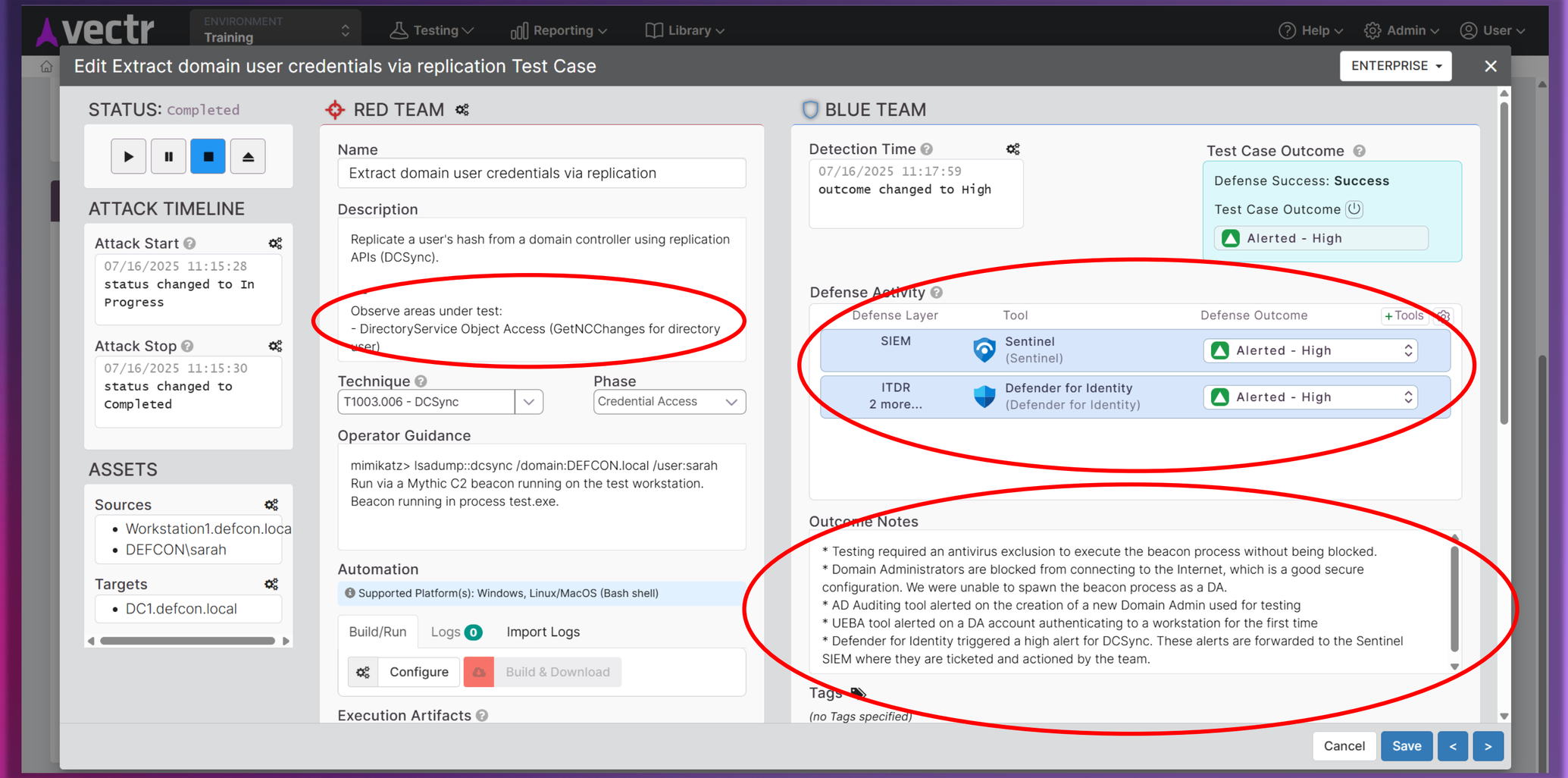


ASSUMED COMPROMISE APPROACH

Doesn't stop at just the user/system access level

Adversary Village at DEF CON 33

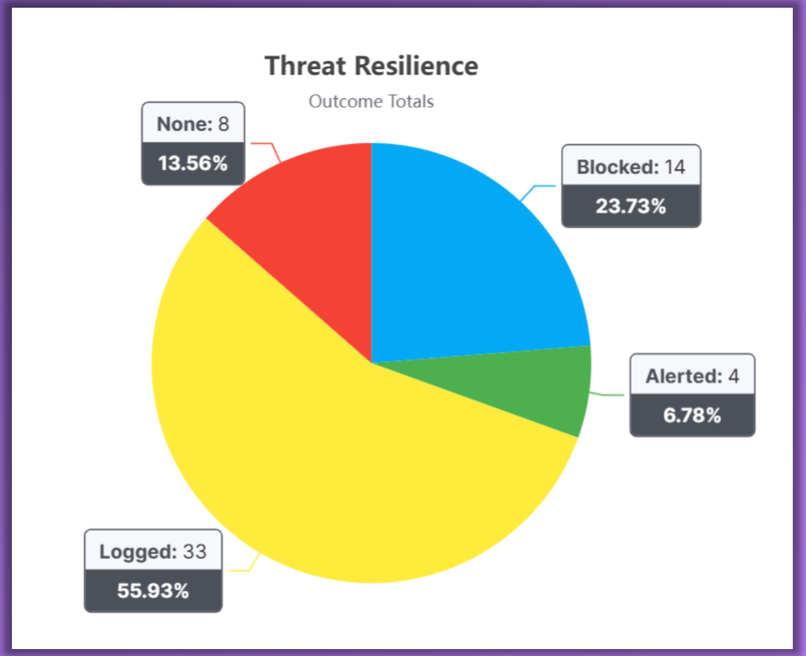
EXAMPLE SCENARIO:

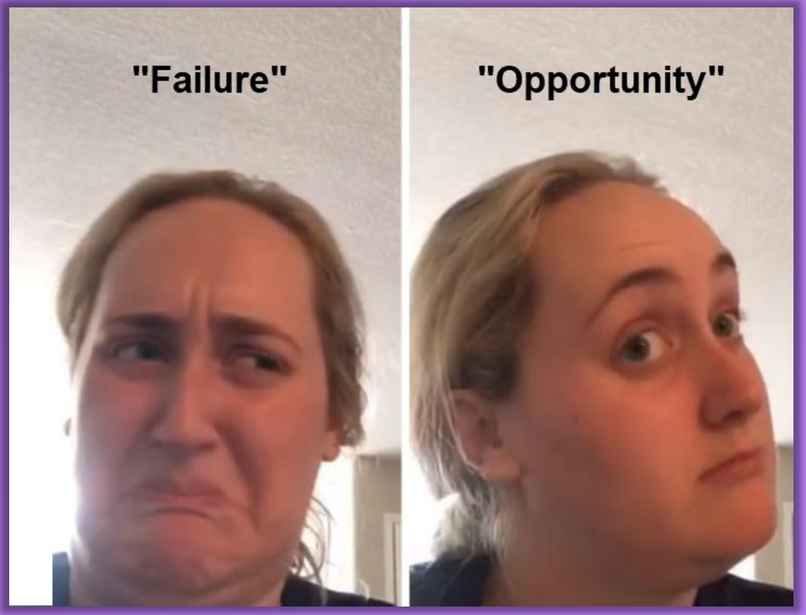


Adversary Village at DEF CON 33

SCORING YOUR PURPLE TEAM

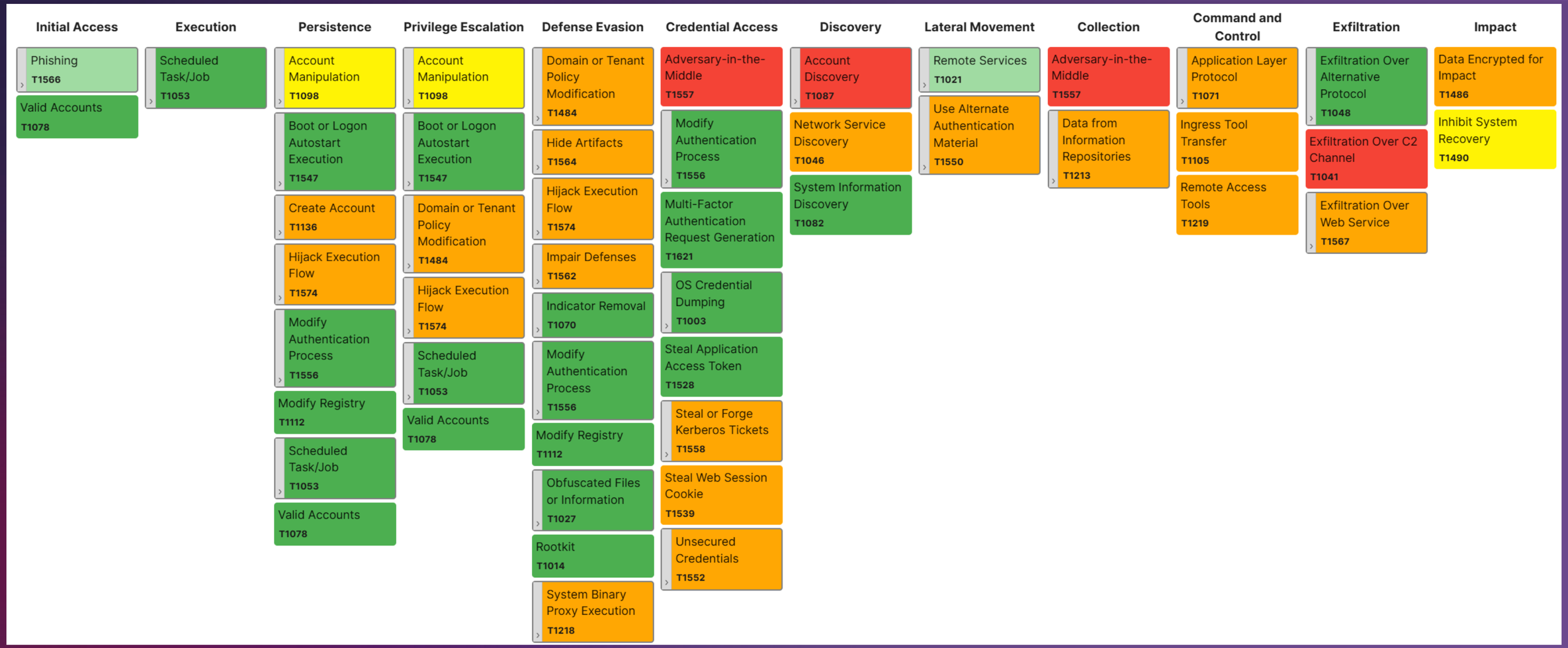
1. Choose a threat intelligence-driven, high priority test plan
2. Use the assumed compromise approach to isolate the security area under test
3. Identify the security tool outcome for each test case
4. Successful (blocked/alerted) outcomes count toward the score, unsuccessful outcomes (logged/none) do NOT count against the score
5. The successful outcomes / total test cases = SCORE





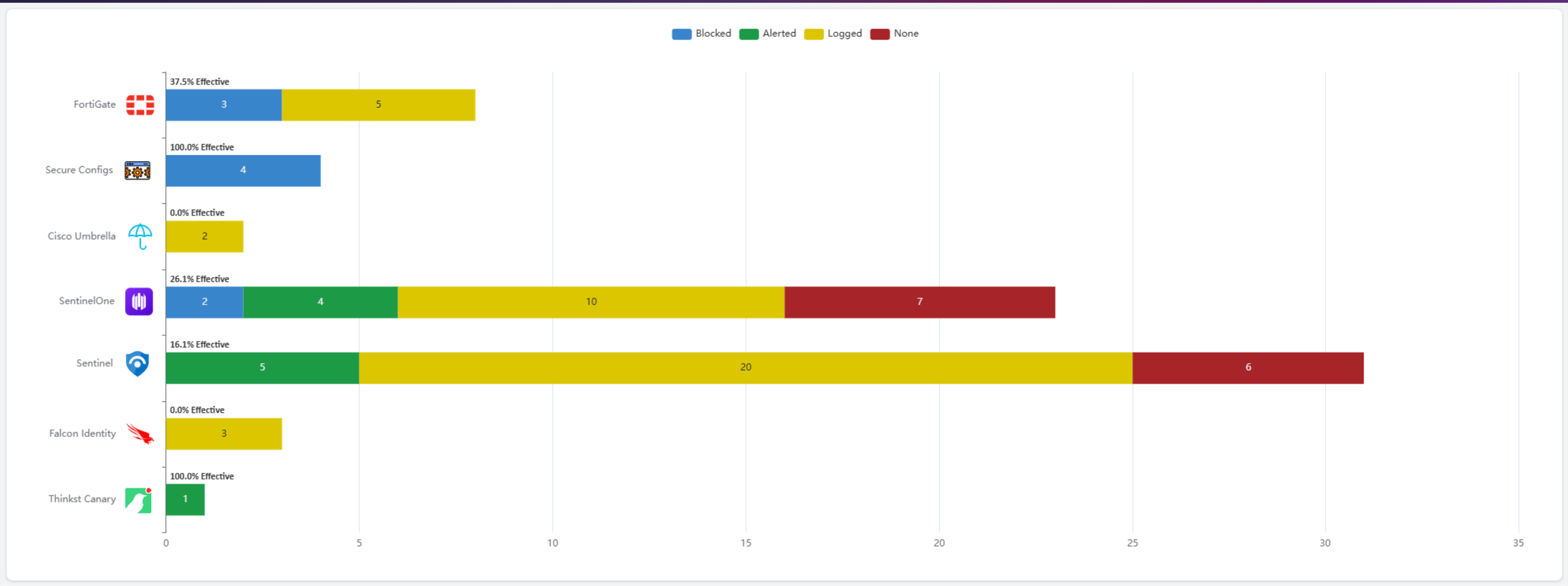
Adversary Village at DEF CON 33

PRIORITIZE REMEDIATION EFFORTS



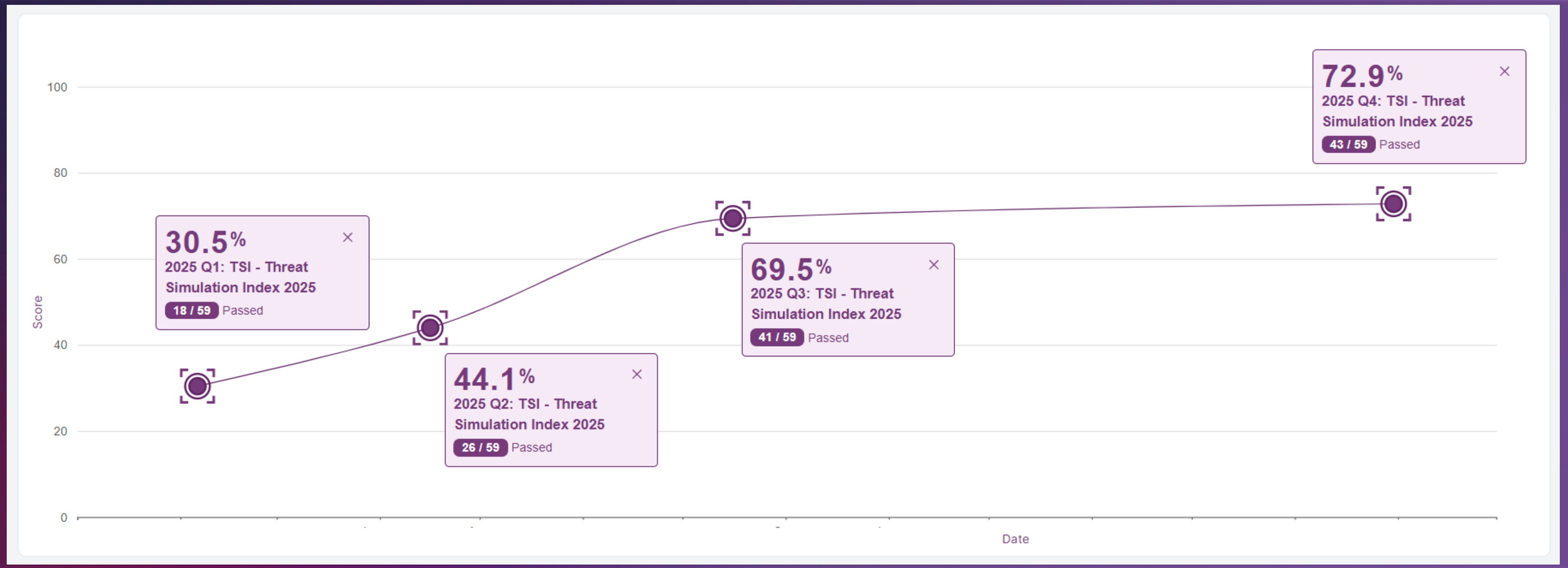
Adversary Village at DEF CON 33

IDENTIFY THEMES



Adversary Village at DEF CON 33

TRACK SUCCESS OVER TIME

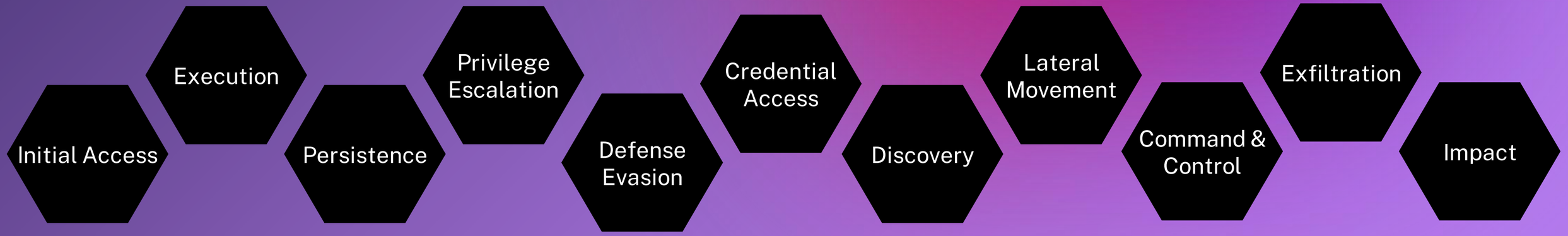


Adversary Village at DEF CON 33

CLOSING THOUGHTS

Keep focus on the purpose

- Improve your resilience against adversaries
- Protect your organization against current & future threats
- Break the chain
- Flip the burden of perfection



Adversary Village at DEF CON 33

THANK YOU



Let’s connect!

https://www.linkedin.com/in/sarah-hume-353898126/

@sarah__hume

https://github.com/SecurityRiskAdvisors/VECTR