



# BloodHound: A Year in Review

Justin Kohler, Chief Product Officer





# The Impact of Attack Path Management



# Development Updates



# 2025 Preview

**Attack Path Management** is the continuous discovery, mapping, and risk assessment of Attack Path Choke Points.

**Tenable**  
<https://www.tenable.com/source/attack-path-management>

## What is Attack Path Management?

Attack path management (APM) is a process you can use to identify security weaknesses as seen through the eyes of an attacker. Tenable Community For Attack Path Management

**jumpsec**  
<https://www.jumpsec.com/attack-path-mapping>

## Attack Path Mapping

If you can understand potential attack paths you can build strategies that enable you to cut off these attack paths.

**Proofpoint**  
<https://www.proofpoint.com/identity-threat-defense/identity-attack-path-management>

## Importance of Continuous Attack Path

Nov 8, 2023 — Attack path management. This refers to the process of identifying, analyzing, understanding and remediating attack paths within a business.

[Key Terms](#) · [Data Exfiltration](#) · [Why An Attack Path...](#)

**traxion.com**  
<https://www.traxion.com/offensive-security-services/attack-path-management>

## Attack Path Management - Traxion

With Attack Path Management services from Traxion, you can map your network through the eyes of an attacker and simulate potential attack paths.

**NCC Group**  
<https://www.nccgroup.com/is-attack-path-mapping-part-of-your-cyber-security-strategy>

## Is Attack Path Mapping Part of Your Cyber Security Strategy?

Feb 15, 2024 — Continuous testing collaboration and evolution of attack path mapping methods. The best form of defence is to know the types of attacks that could be used against your organization.

**Dark Reading**  
<https://www.darkreading.com/exposure-management-lives-in-attack-paths>

## Exposure Management Looks to Attack Paths, Identity ...

Jul 7, 2023 — "With attack path analysis, organizations can understand how assets are interconnected, how a vulnerability in an asset might relate to a certain asset, and how it might be exploited."

**BloodHound Enterprise**  
<https://bloodhoundenterprise.io/what-is-attack-path-management>

## What is Attack Path Management?

Microsoft Research published a paper in 2009 describing Attack Paths as "Identity sniping". These attacks [that] leverage the users logged in to a first compromised account to gain access to other accounts ...

[Why Active Directory Is The...](#) · [Why Attack Paths Are...](#) · [What Is Attack Path...](#)

**Tarlogic**  
<https://www.tarlogic.com/cybersecurity/attack-path-management>

## Attack Path Management

May 10, 2023 — In short, Attack Path Management is a way to identify and mitigate ransomware attacks against company assets.

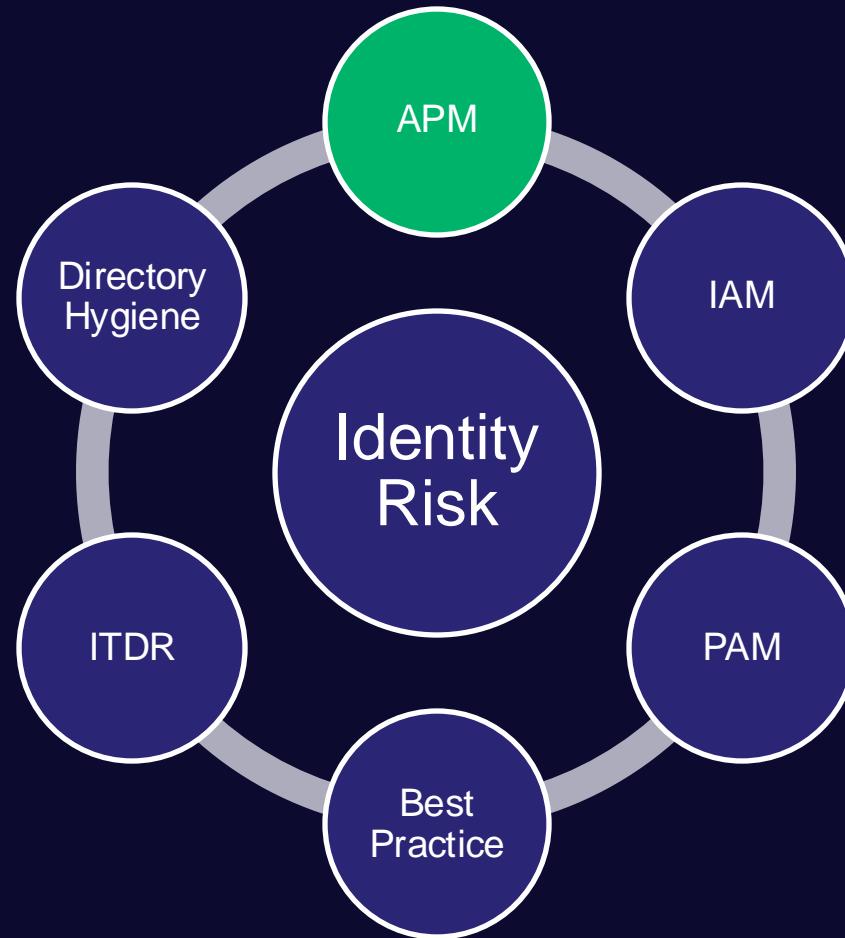
**TechTarget**  
<https://www.techtarget.com/searchsecurity/tip/close-security-gaps-with-attack-path-analysis>

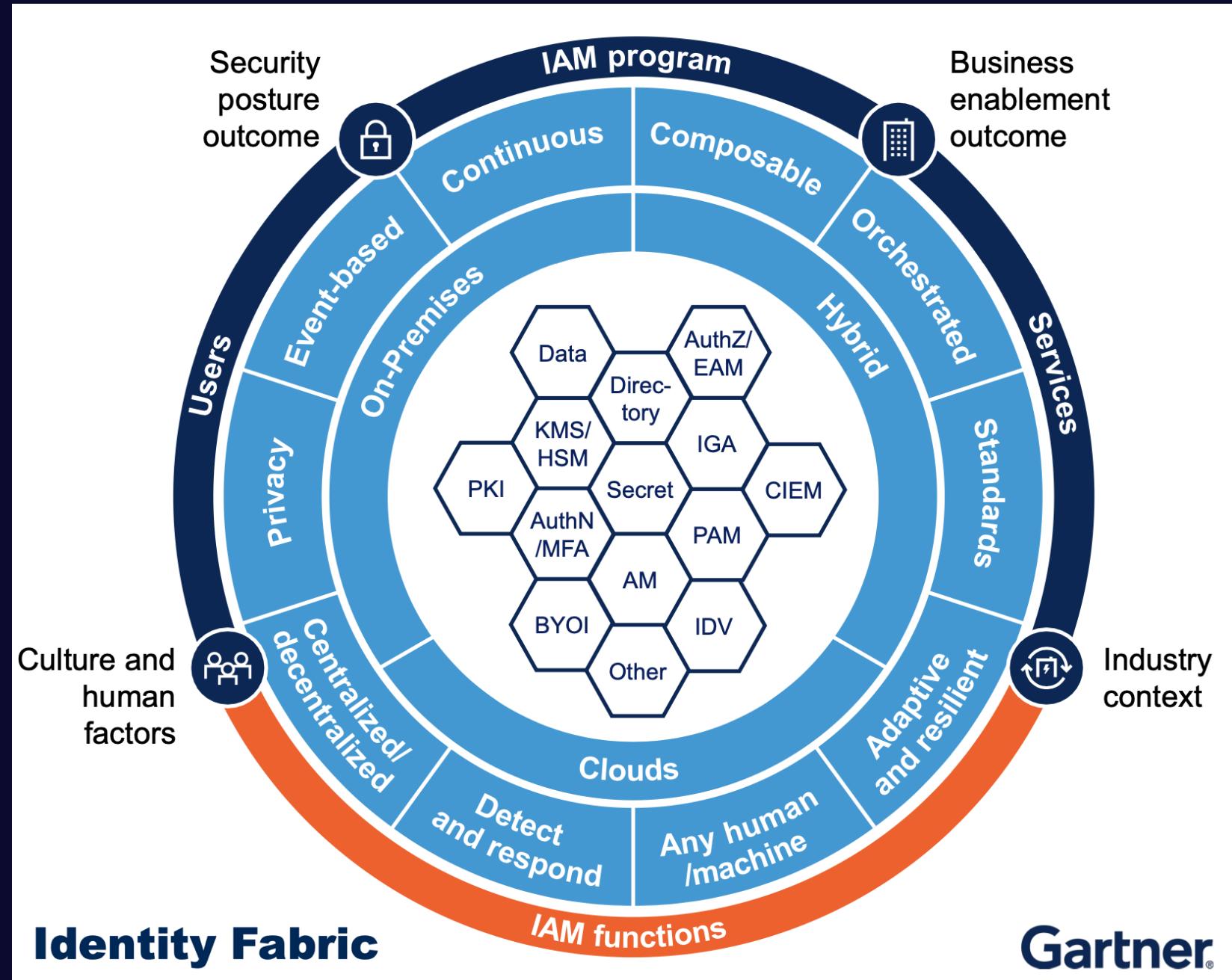
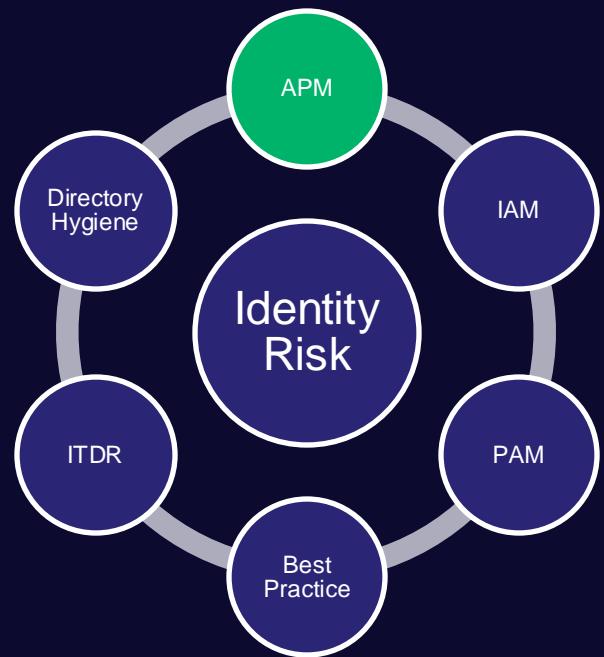
## Close security gaps with attack path analysis

Feb 6, 2024 — Penetration testing and red team exercises can help identify potential attack paths. Tenable Community For Attack Path Management



# **APM** is the missing capability in Identity Risk





**Gartner**



CyberArk

<https://www.cyberark.com> › what-is › identity-security

## What is Identity Security?

**Identity Security** is a comprehensive solution for securing all identities— human or machine throughout the cycle of accessing critical assets.



Veza

<https://www.veza.com>

## Future of Identity Security | Veza Identity Security

Go beyond groups and roles to get full visibility into all access permissions across 250+ systems in minutes...



Silverfort

<https://www.silverfort.com> › Glossary

## What is Identity Security? | Silverfort Glossary

Identity security is the practice of **protecting digital identities from manipulation, or misuse**. It involves a comprehensive set of ...



Duo Security

<https://duo.com> › Resources › InfoSec Glossary

## What is Identity Security?

Identity security means **safeguarding organizations**. This involves implem



CrowdStrike

<https://go.crowdstrike.com> › identity › protection

## CrowdStrike Identity - Secure Identities Faster

Only A Unified **Identity Protection** Strategy Delivers Robust Cyber



Grip Security

<https://www.grip.security> › glossary › id

## What is Identity Security and Why Is It Important?

**Identity security is a critical part of modern business**, especially when managing user identities across all systems.



SailPoint

<https://www.sailpoint.com> › Identity Library

## What is identity security? - Article

**Identity security** enables you to manage and govern accounts, applications, systems, data and cloud services, all while ...



Ping Identity

<https://www.pingidentity.com> › ...

## Ping Identity: Identity Security 101

Ping **Identity** helps you protect your users and experiences frictionless.



BeyondTrust

<https://www.beyondtrust.com> › Resources › Glossary

## Identity Security

**Identity security**, also called identity protection, refers to managing and secure enterprise digital identities.



Delinea

<https://delinea.com> › Glossary

## What is Identity Security?

Identity security **protects the digital identities of humans** as they interact with data, applications, and infrastructure.

How Do Identities Typically... · Here Are Some Common Examples



Saviynt

<https://www.saviynt.com>

## Leader in Identity Security

Secure Identity Management — Saviynt Help Program. Request a Demo

# How IAM Vendors Define “Identity Security”

## Authentication vendor

“... The practice of protecting digital identities from unauthorized access, manipulation or misuse.”

## PAM vendor

“Identity security is a comprehensive solution for securing all identities used in an organization. It assumes that any identity [...] **can become privileged** under certain conditions, creating an attack path to an organization’s most valuable assets.”

## IGA vendor

“Identity security (also known as **identity governance** and **identity management**) protects against the cyberthreats associated with providing technology access to a diverse workforce. It does this by enabling the management and governance of access for every digital identity within an organization.”

# Our Verdict ... “Identity Security” Is Just a Buzzword

- Many vendors with widely **different capabilities** have branded/rebranded as “identity security vendors.”
- Thus ... “identity security” is meaningless ... ask **vendors** what they **really** do.

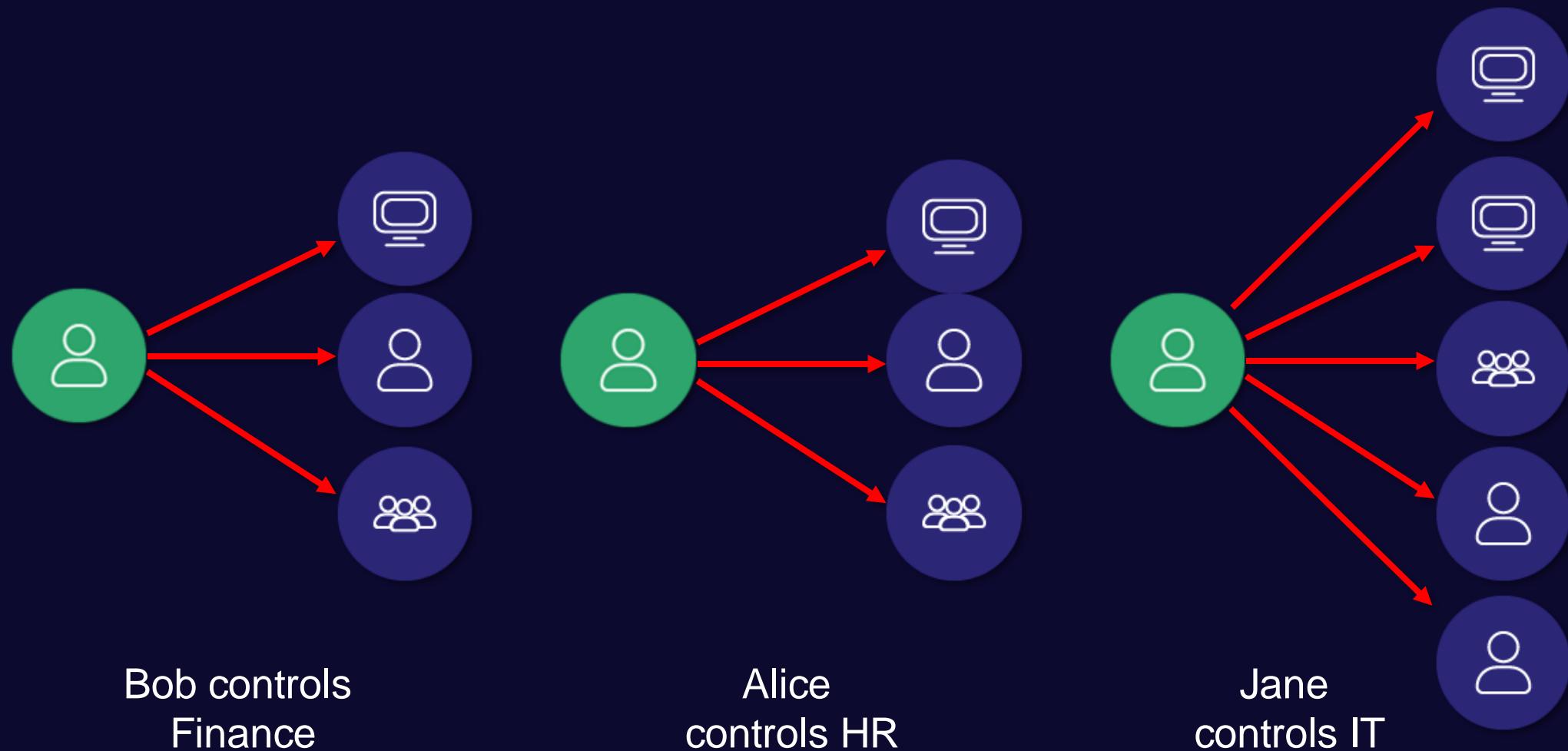


Attack Paths are **how** we attack identities

Attack Paths are how we attack [human] identities

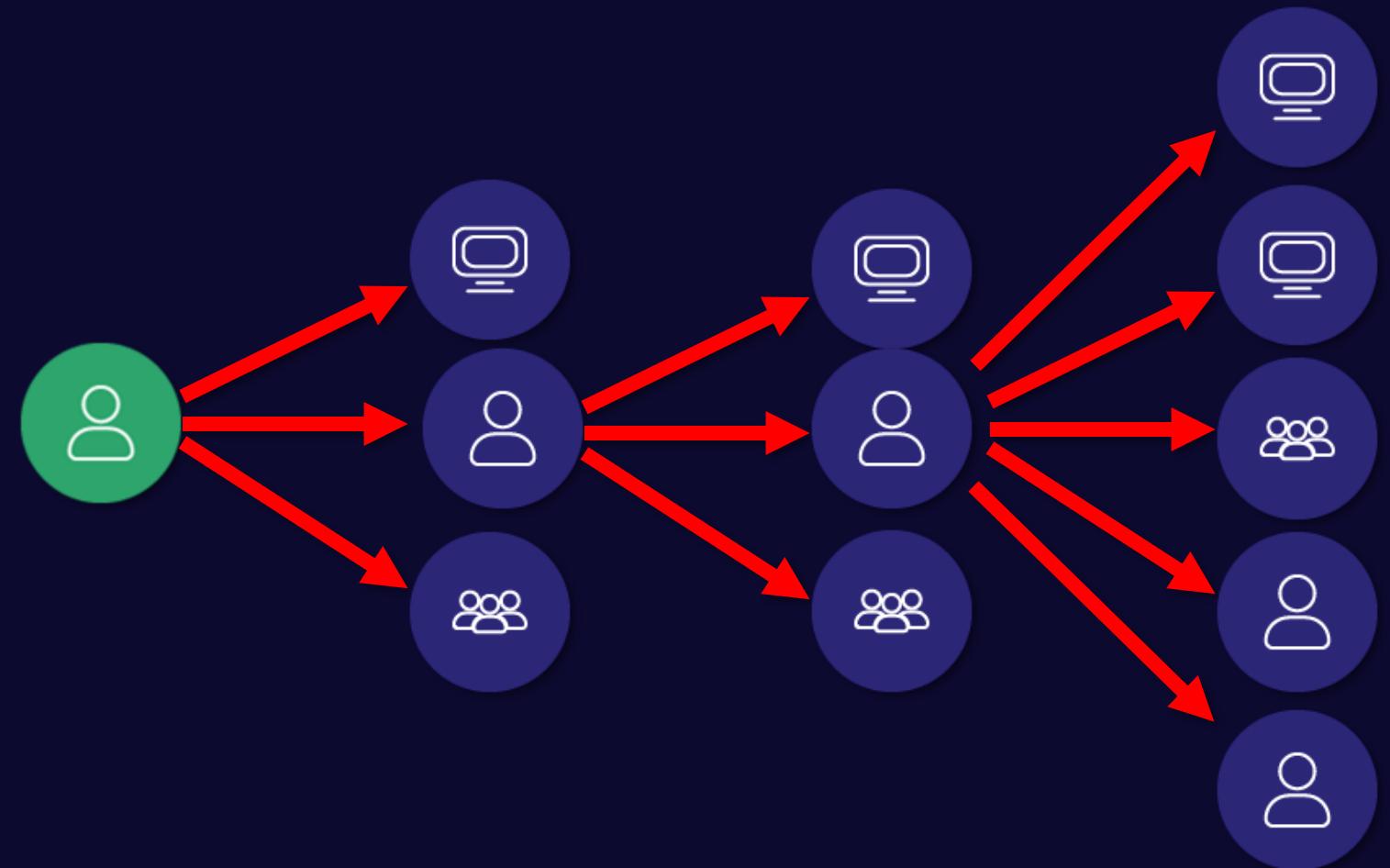
Attack Paths are how we attack [machine] identities

Attack Paths are how we attack **[all]** identities  
to compromise resources and disrupt business-  
critical operations





Bob controls *everything*



**“It’s not about the access I have now...  
it’s about the access I can **attack** my way to”**

**Attack Path Management** is the continuous discovery, mapping, and risk assessment of Attack Path Choke Points.

This is **how** we reduce Identity Risk

# Outcomes: Augmenting Existing IAM Capabilities

- Streamline remote access.
- Identify and manage the life cycle of machine identities.
- Detect and suppress lateral movement.
- Provide visibility and reduce risk from disconnected or complex infrastructure.
- Detect and manage unknown privilege.
- Analyze complex relationships across IAM data to reduce the attack surface.
- Implement the principle of least privilege.

## Pre-breach attack path analysis

Traditionally, organizations have leaned on all sorts of different security tools to manage threat exposure across their estate. This messy patchwork of approaches however, can lead to exposure visibility gaps and efficiency challenges.

This makes it imperative for security leaders to reach a unified and comprehensive view of their estate and to both continuously and smartly prioritize exposure reduction efforts. Prioritization should seek to understand threats and attacker perspective, identify "crown jewels" of interest to the attacker, and both identify and mitigate any paths that lead to them.

Three key components are required for threat-informed defense: single pane of glass, critical asset protection, and attack path management.

### Single pane of glass

Organizations should consolidate threat exposure insights across their estate into a single view covering cloud assets, on-prem devices, data, identities, applications, network, and the Internet of Things (IOT). This should then be used to manage top threats such as ransomware and business email compromise, as well as exposure to threat campaigns and actors.

**80%**

of organizations have attack paths that expose critical assets

## Critical asset management

It is imperative to thoroughly map an estate's "crown jewels." This can include critical servers, highly privileged identities, sensitive data, or other assets. Microsoft data indicates that an average <1% of organizational assets are of high interest to attackers.

### Attack path management

Organizations should identify the most likely attack paths leading to critical assets and continuously mitigate them. An attack path calculation incorporates things such as asset inventories, vulnerability/weakness data, and external attack surfaces to construct a possible attack chain leading to a critical asset.

### Links

[Introducing Security Exposure Management - Microsoft Community Hub | Mar 2024](#)

[Identifying and Protecting the Crown Jewels of your Cloud | Aug 2024](#)

[Exposure insights and secure score in Microsoft Security Exposure Management | Aug 2024](#)

[One graph of everything - Microsoft Security Exposure Management Graph | May 2024](#)

## Attack path insights for threat-informed defense (June 2024)

10%

of attack paths contain three steps or less

61%

of attack paths lead to a sensitive user account

40%

of attack paths include lateral movement based on non-interactive remote code execution

14%

of attack paths allow attackers to move from on-premises to cloud environments

1%

of attack paths start with a critically vulnerable internet-facing device

90%

of organizations are exposed to at least one attack path

3%

of organizations are exposed to more than 1,000 attack paths

80%

of organizations have attack paths that expose critical assets

22%

of organizations had an attack path identified in the cloud

8%

of organizations have a chokepoint that is involved in at least 10 attack paths

<1%

of organizational assets are of high interest to attackers

Source: Microsoft Security Exposure Management

**Attack path management**

Organizations should identify the most likely attack paths leading to critical assets and continuously mitigate them. An attack path calculation incorporates things such as asset inventories, vulnerability/weakness data, and external attack surfaces to construct a possible attack chain leading to a critical asset.

**Attack path management**

80% of organizations have attack paths to their most critical assets

**Attack path insights for threat informed defense (June 2020)**

Insight	Percentage
Attack paths exist from 99%	99%
Attack paths exist from 99% of organizations that have at least one	99%
Attack paths exist from 80%	80%
Attack paths exist from 80% of organizations that have at least one	80%
Attack paths exist from 60%	60%
Attack paths exist from 60% of organizations that have at least one	60%
Attack paths exist from 40%	40%
Attack paths exist from 40% of organizations that have at least one	40%
Attack paths exist from 20%	20%
Attack paths exist from 20% of organizations that have at least one	20%
<1%	<1%
Attack paths exist from <1% of organizations that have at least one	<1%

# Operationalizing APM

The screenshot displays the BloodHound Enterprise web interface. On the left, a network graph shows various user accounts connected to a central 'PHANTOM.CORP Tier Zero' node. The connections are color-coded: red for high-risk paths and yellow for lower-risk or informational paths. Some nodes have a count next to them, such as '59' for several red nodes and '3' for some yellow nodes. On the right, a summary card for 'PHANTOM.CORP' indicates it is 'Idle' with the last analysis date as '2025-03-30 20:02 EDT (GMT-0400)'. Below the card is a list of security findings categorized by risk level:

- Kerberoastable User Accounts**: 2 Findings, Critical
- Kerberos Delegation on Tier Zero Objects**: 13 Findings, Critical
- Computers Vulnerable to Coercion-based NTLM Relay to LDAP Attack**: 1 Finding, Critical
- Large Default Groups with Generic Write Privileges**: 1 Finding, Critical
- Computers Vulnerable to Coercion-based NTLM Relay to SMB Attack**: 1 Finding, Critical
- Computers Vulnerable to Coercion-based NTLM Relay to LDAPS Attack**: 1 Finding, Critical
- Large Default Groups in Local Administrator Groups**: 8 Findings, Critical
- AS-REP Roastable User Accounts**: 1 Finding, Critical
- Logons from Tier Zero Users**: 24 Findings, High
- Tier Zero Computer Vulnerable to Coercion-based NTLM Relay to SMB Attack**: 1 Finding, High
- Tier Zero Computer Vulnerable to Coercion-based NTLM Relay to LDAP Attack**: 1 Finding, High

A vertical sidebar on the far left contains various navigation icons. At the bottom left is a 'Reset View' button.

# Operationalizing APM

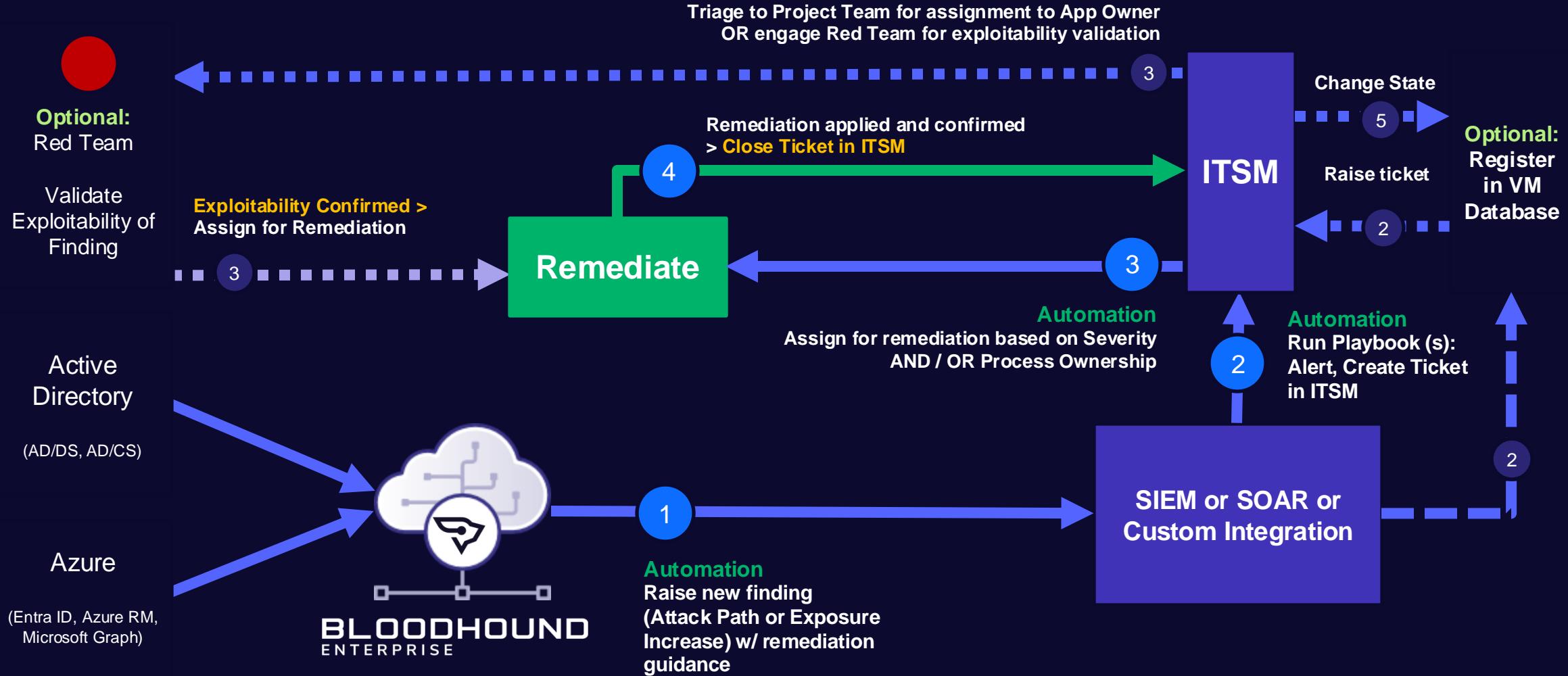
The screenshot shows the BloodHound Enterprise web interface. On the left is a network graph with nodes representing users and groups, and edges representing relationships like Kerberos delegation and AS-REP Roastability. A central node is labeled "PHANTOM.CORP Tier Zero 99% Exposed". On the right is a list of findings categorized by privilege escalation methods:

- Kerberoastable User Accounts: 2 Findings (Critical)
- Kerberos Delegation on Tier Zero Objects: 13 Findings (Critical)
- Computers Vulnerable to Coercion-based NTLM Relay to LDAP Attack: 1 Finding (Critical)
- Large Default Groups with Generic Write Privileges: 1 Finding (Critical)
- Computers Vulnerable to Coercion-based NTLM Relay to SMB Attack: 1 Finding (Critical)
- Computers Vulnerable to Coercion-based NTLM Relay to LDAPS Attack: 1 Finding (Critical)
- Large Default Groups in Local Administrator Groups: 8 Findings (Critical)
- AS-REP Roastable User Accounts: 1 Finding (Critical)
- Logons from Tier Zero Users: 24 Findings (High)
- Tier Zero Computer Vulnerable to Coercion-based NTLM Relay to SMB Attack: 1 Finding (High)
- Tier Zero Computer Vulnerable to Coercion-based NTLM Relay to LDAPS Attack: 1 Finding (High)

At the bottom left is a "Reset View" button.



# Operationalizing APM



# Attack Path Management is effective



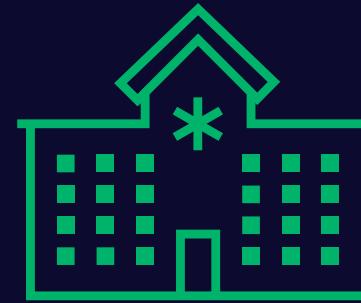
2M Identities

54% reduction in 6 months



50 Domains

T0 paths gone in 6 months



4M Identities

90% reduction in 18 months



Ann & Robert H. Lurie  
Children's Hospital of Chicago

BREAKING NEWS

MORE THAN 791,000 PEOPLE  
IMPACTED BY LURIE CHILDREN'S DATA BREACH



RANSOMWARE ATTACKS SURGE

▲ 20%

RANSOMWARE

# Ransomware Cyberattack Associated With Cardiac Arrest Incidence and Outcomes at Untargeted, Adjacent Hospitals

**OBJECTIVES:** Healthcare ransomware cyberattacks have been associated with major regional hospital disruptions, but data reporting patient-oriented outcomes in critical conditions such as cardiac arrest (CA) are limited. This study examined the CA incidence and outcomes of untargeted hospitals adjacent to a ransomware-infected healthcare delivery organization (HDO).

**DESIGN, SETTING, AND PATIENTS:** This cohort study compared the CA incidence and outcomes of two untargeted academic hospitals adjacent to an HDO under a ransomware cyberattack during the pre-attack (April 3–30, 2021), attack (May 1–28, 2021), and post-attack (May 29, 2021–June 25, 2021) phases.

**INTERVENTIONS:** None.

**MEASUREMENTS AND MAIN RESULTS:** Emergency department and hospital mean daily census, number of CAs, mean daily CA incidence per 1,000

Thaidan T. Pham, MD<sup>1</sup>

Theoren M. Loo, MS<sup>2</sup>

Atul Malhotra, MD<sup>3</sup>

Christopher A. Longhurst, MD,  
MS<sup>4,5</sup>

Diana Hylton, MD<sup>6</sup>

Christian Dameff, MD, MS<sup>4,7,8</sup>

Jeffrey Tully, MD<sup>6</sup>

Gabriel Wardi, MD, MPH<sup>3,7</sup>

Rebecca E. Sell, MD<sup>9</sup>

Alex K. Pearce, MD<sup>3</sup>

BREAKING NEWS  
JUSTICE DEPT. TO ELEVATE RANSOMWARE  
CASES TO SIMILAR PRIORITY AS TERRORISM

4:13A  
PACIFIC

HACK DISRUPTS HEALTH CARE SYSTEM





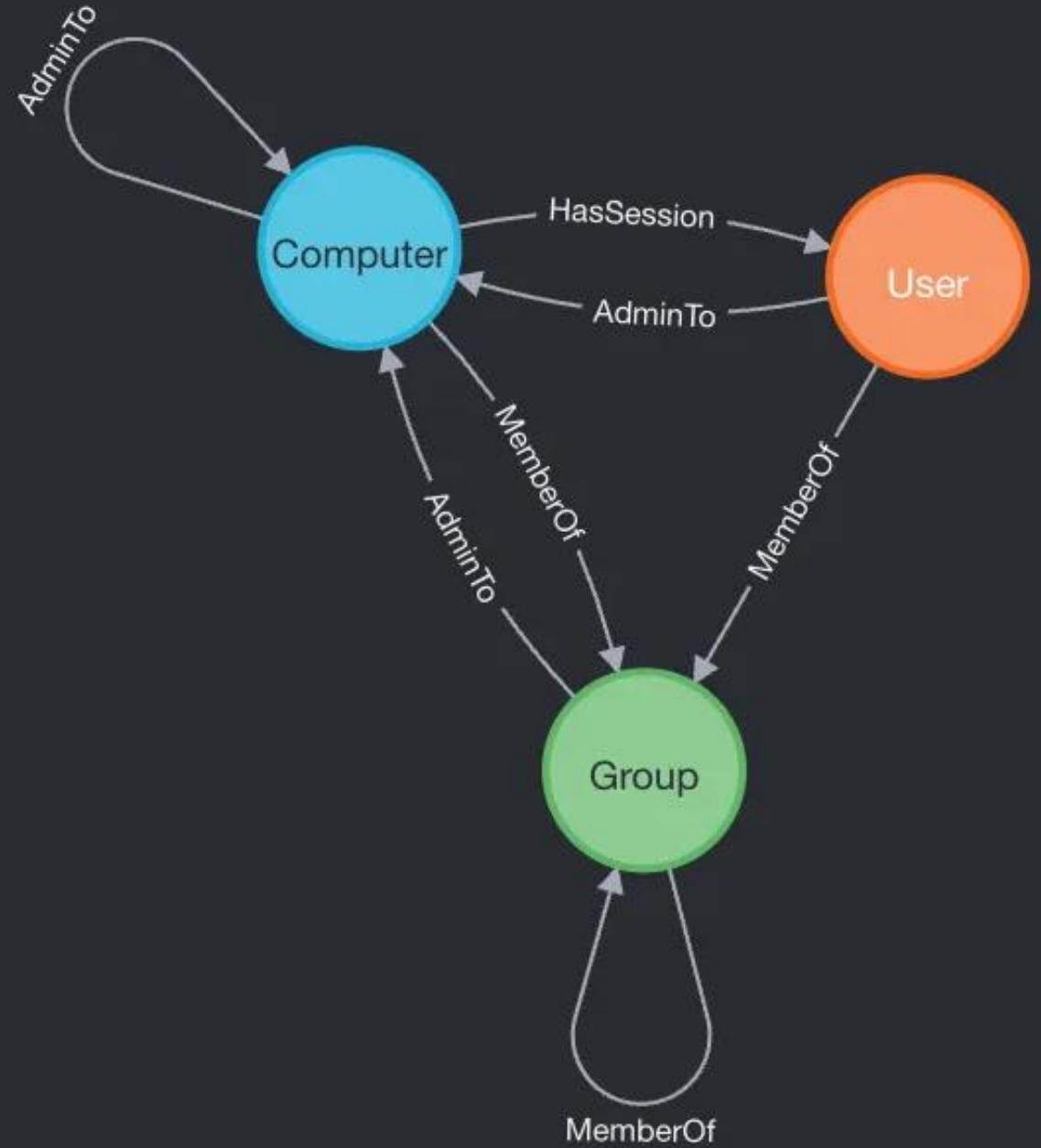
## The Impact of Attack Path Management



## Development Updates



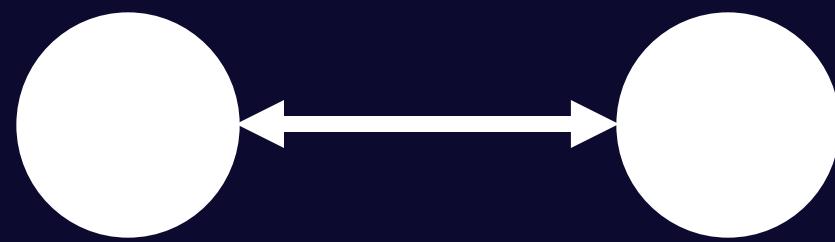
2025  
Preview



# BloodHound Graph 2016

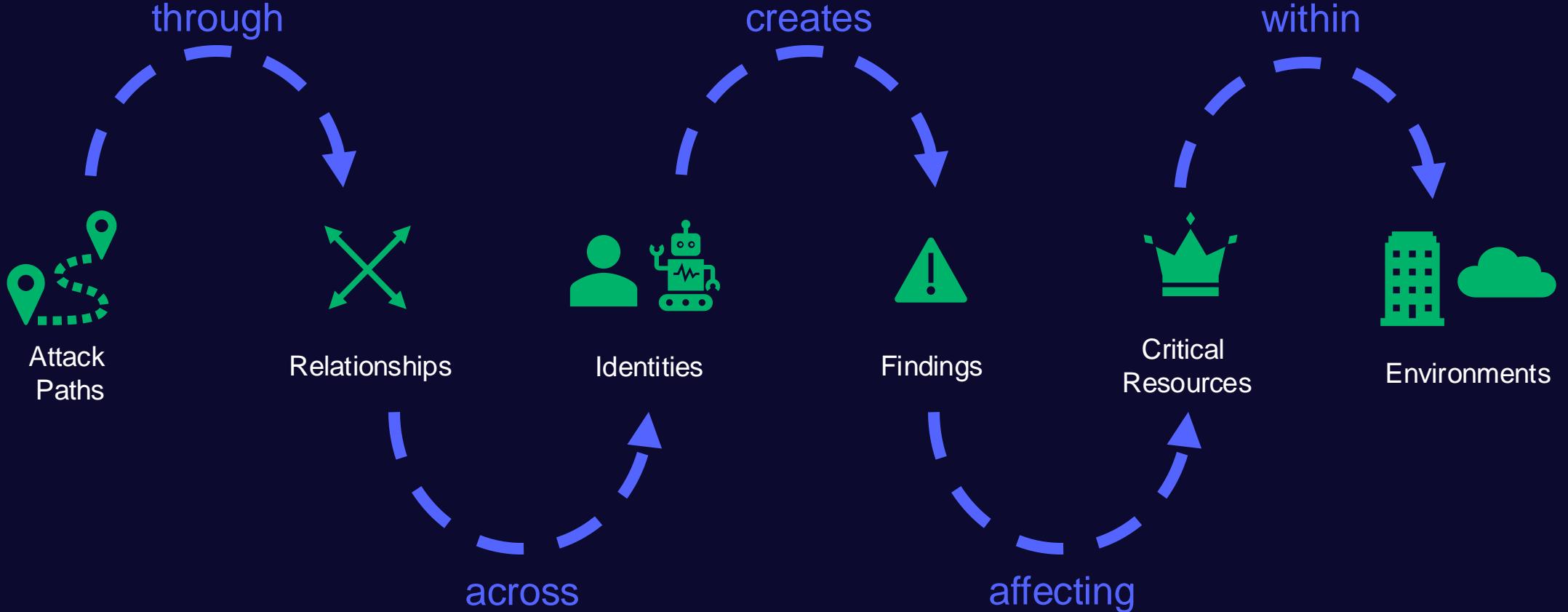
- 3 Nodes
- 3 Edges

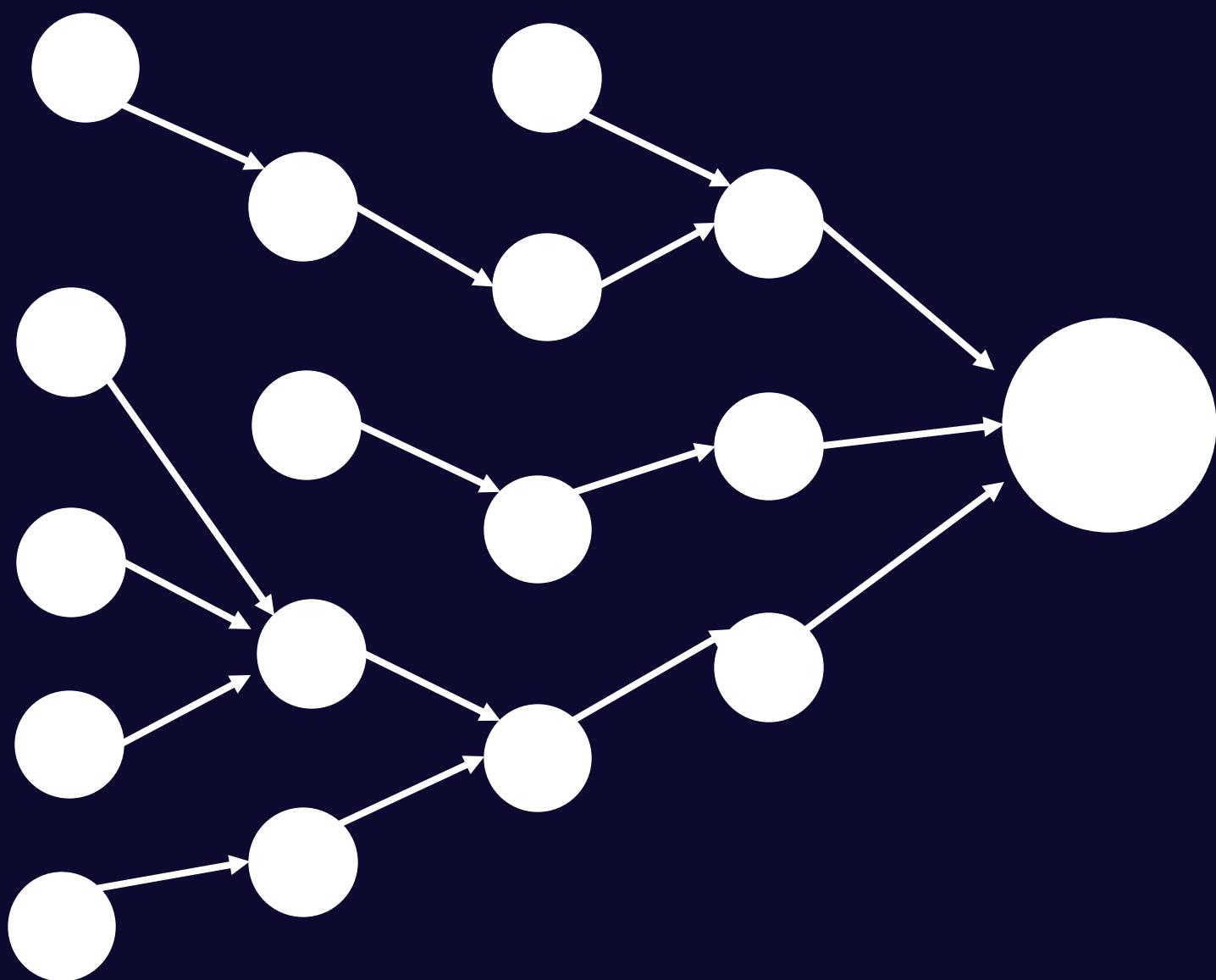






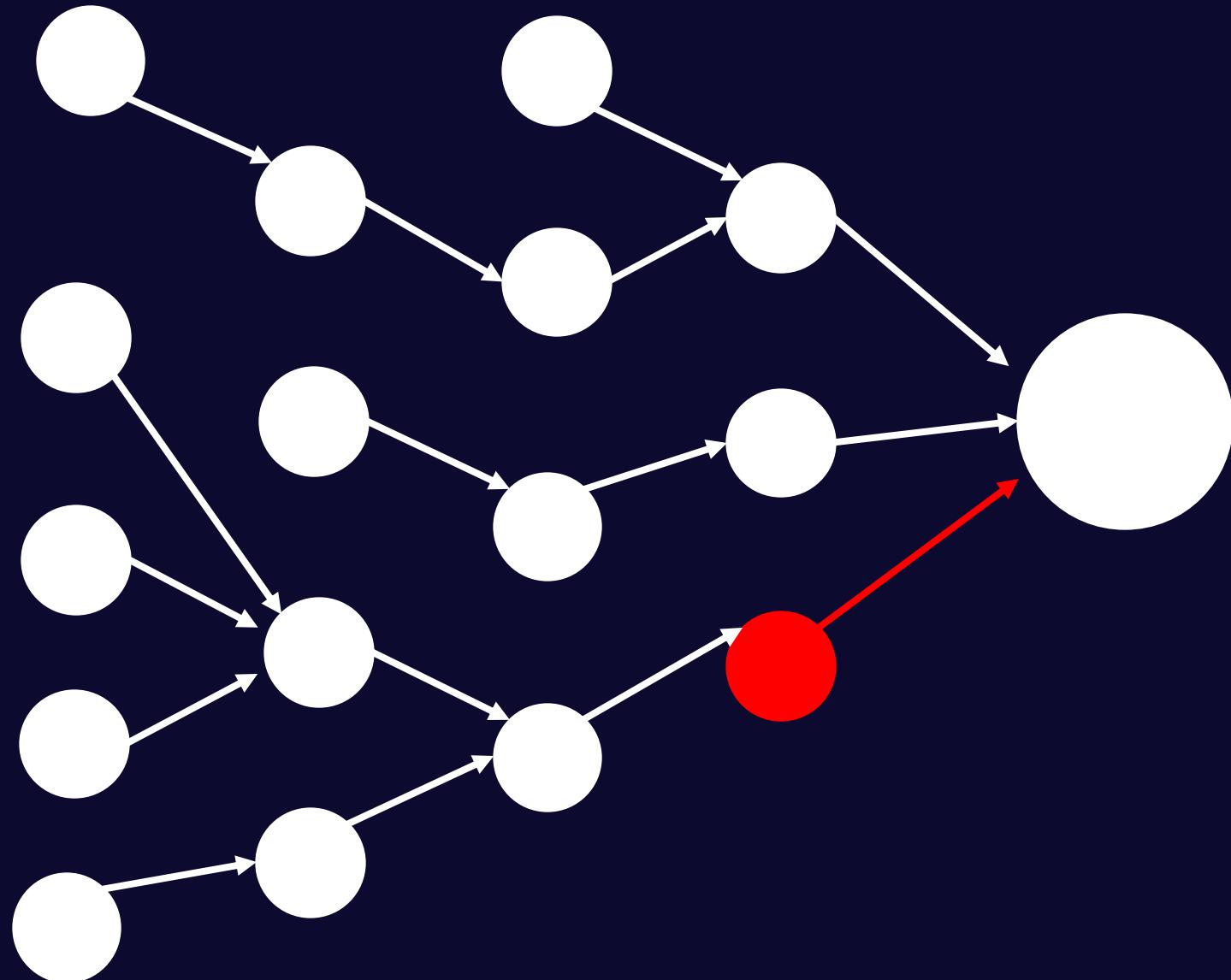






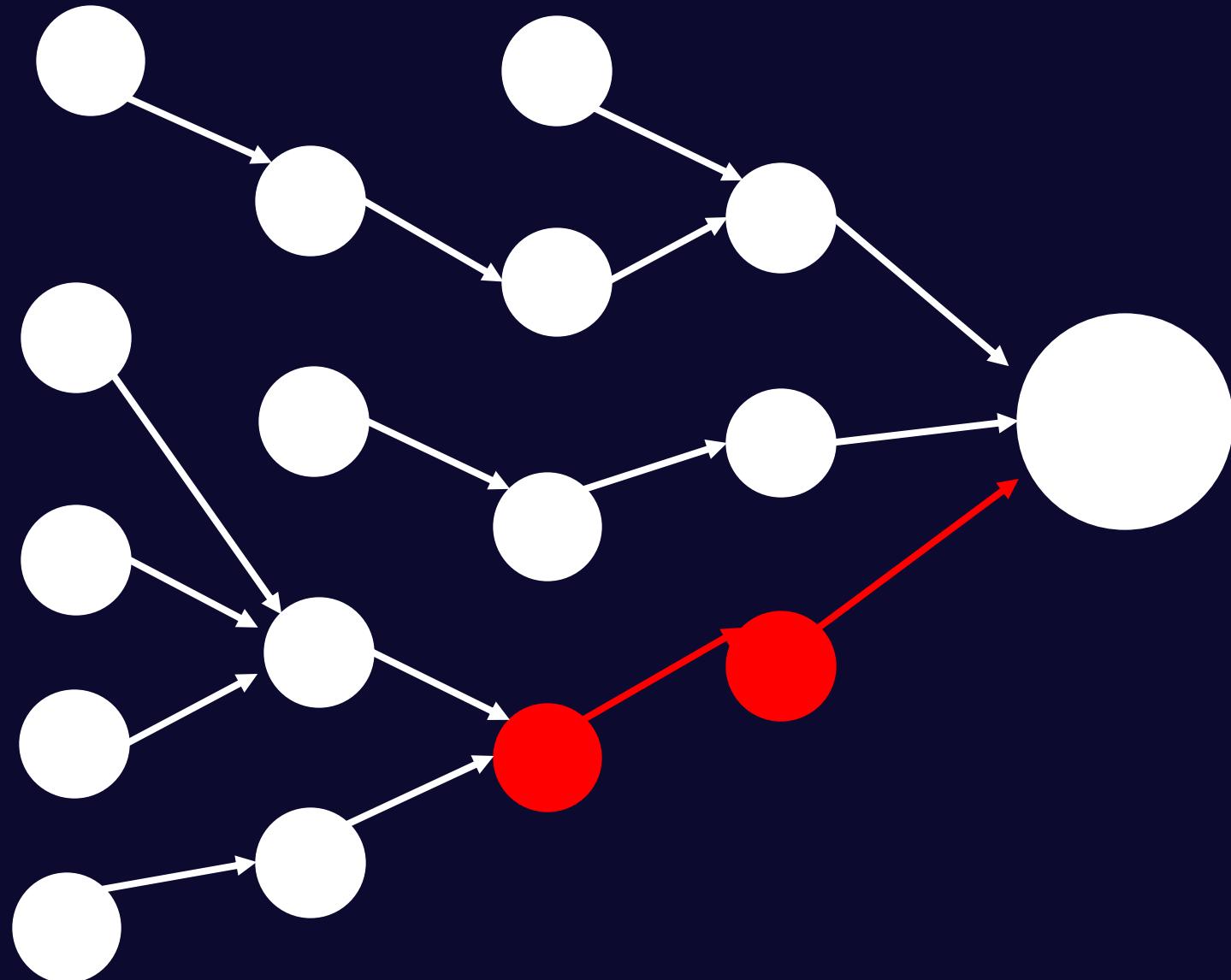
Attack Path  
Count:

**1**

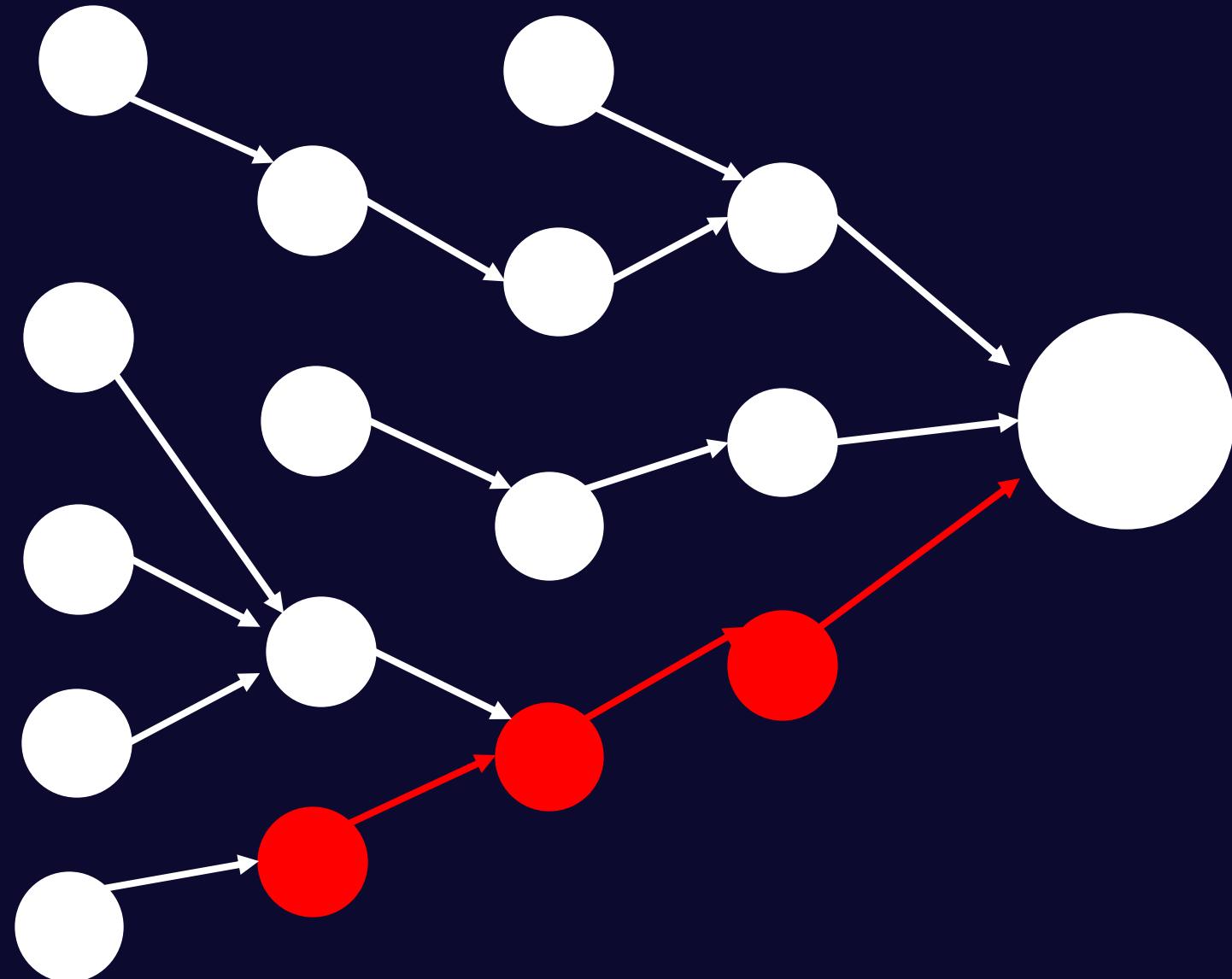


Attack Path  
Count:

**2**

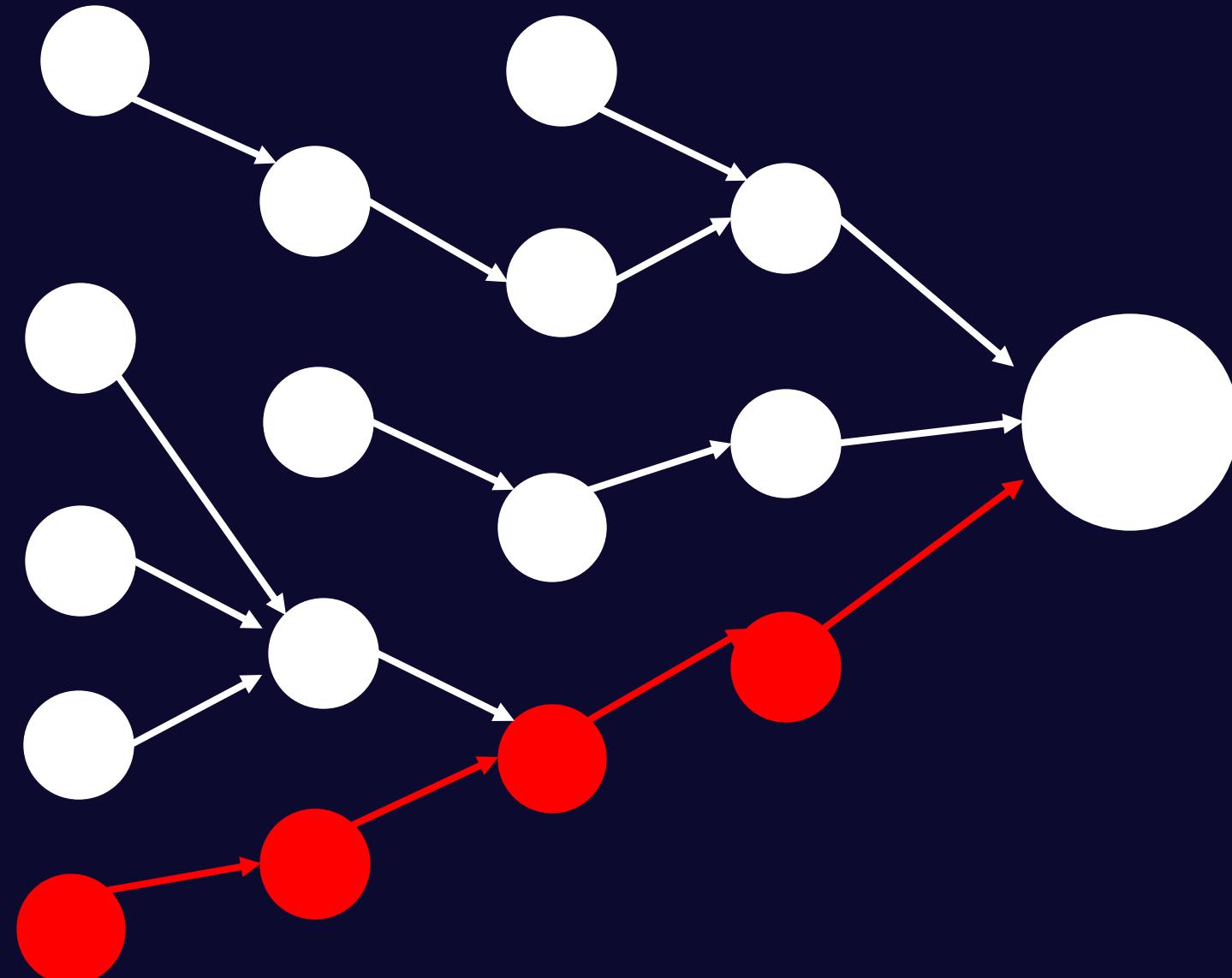


Attack Path  
Count:  
**3**

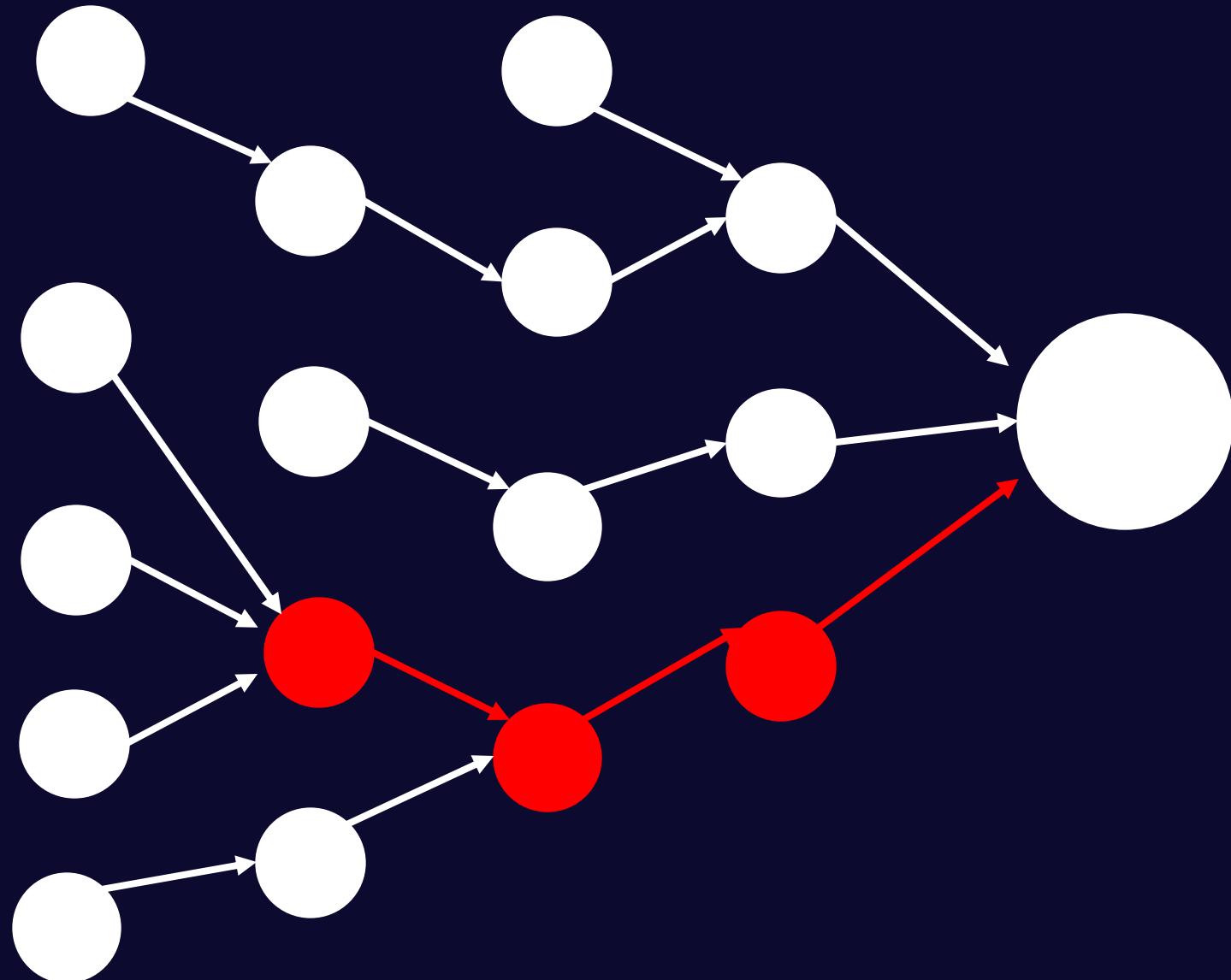


Attack Path  
Count:

**4**

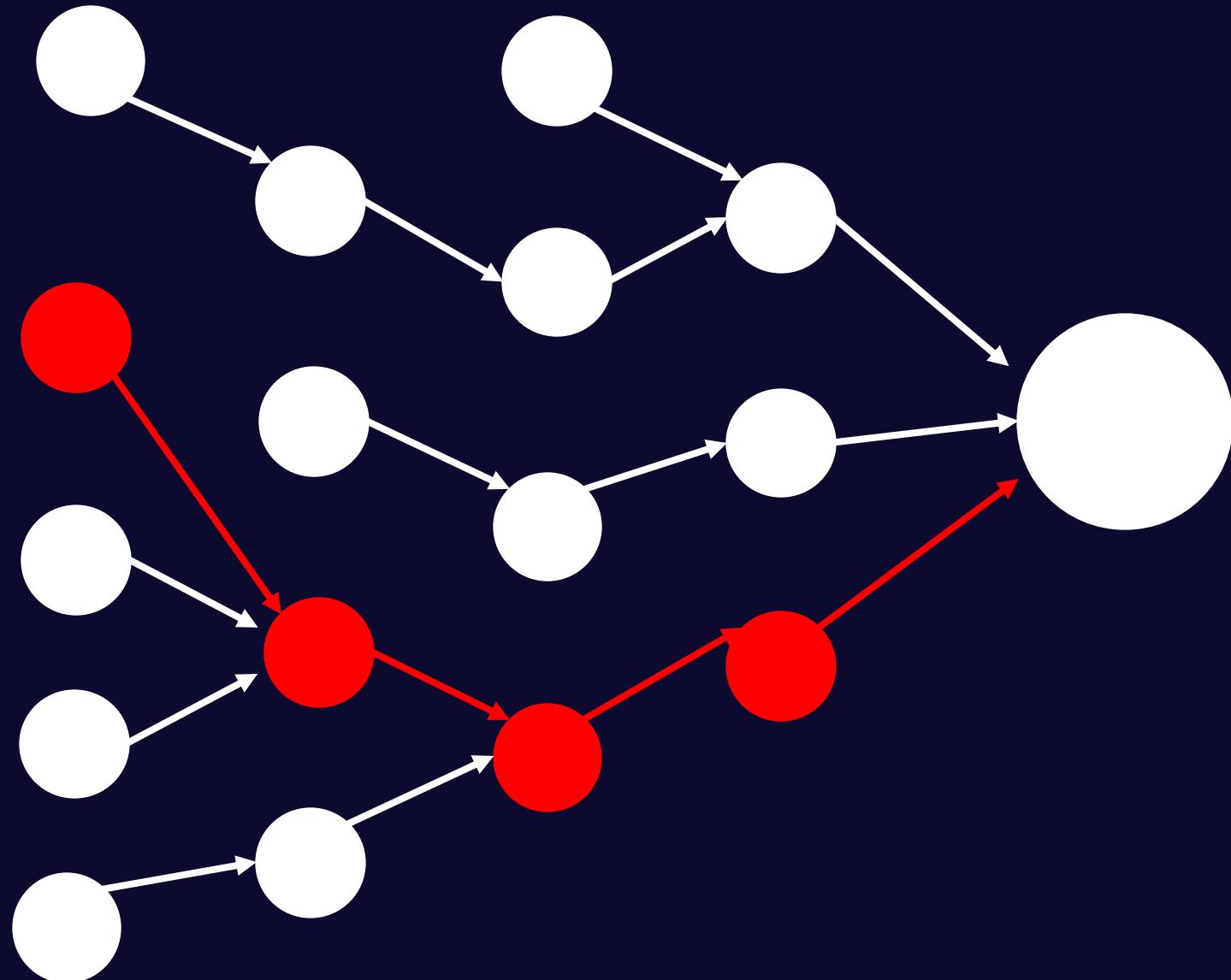


Attack Path  
Count:  
**5**



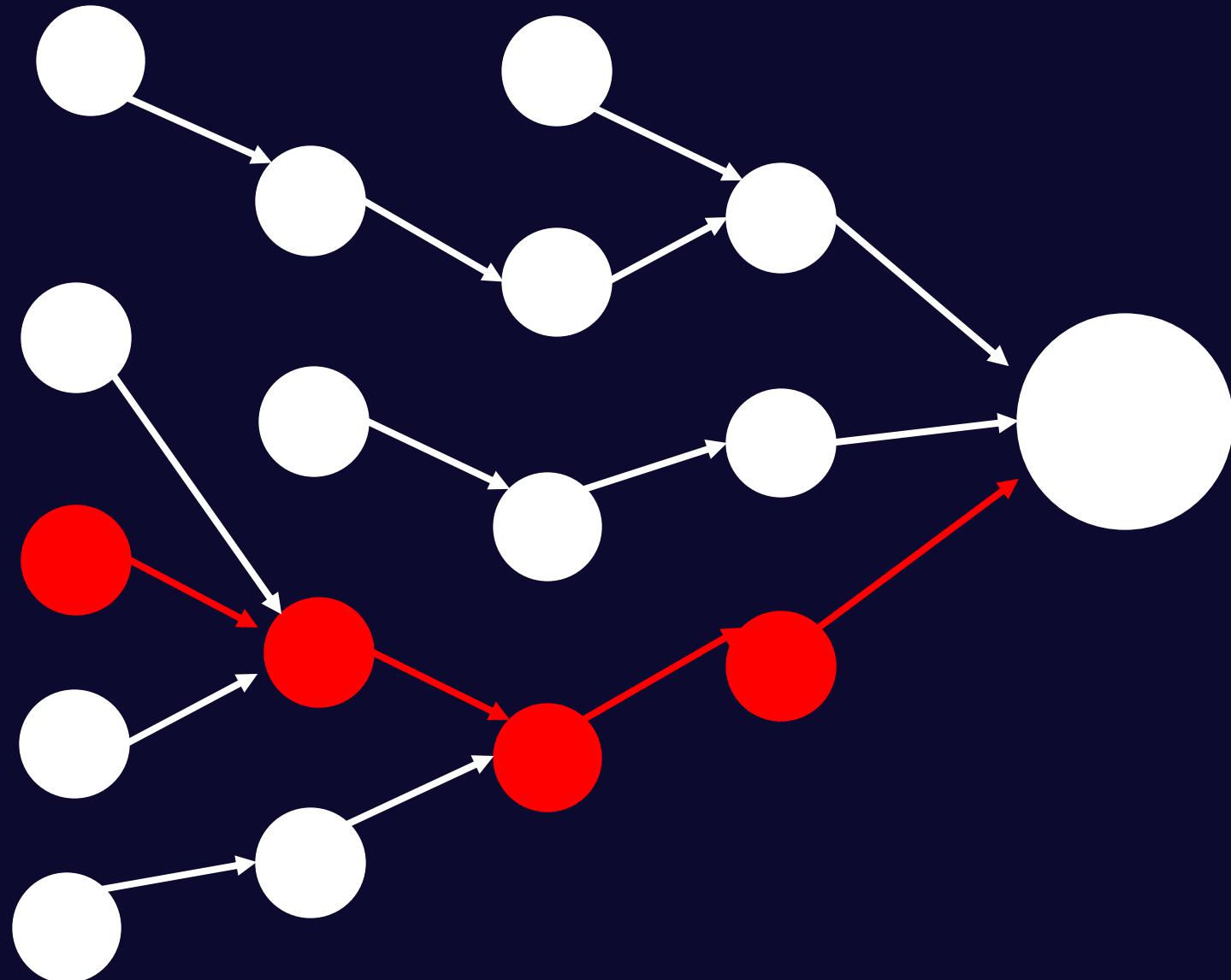
Attack Path  
Count:

**6**

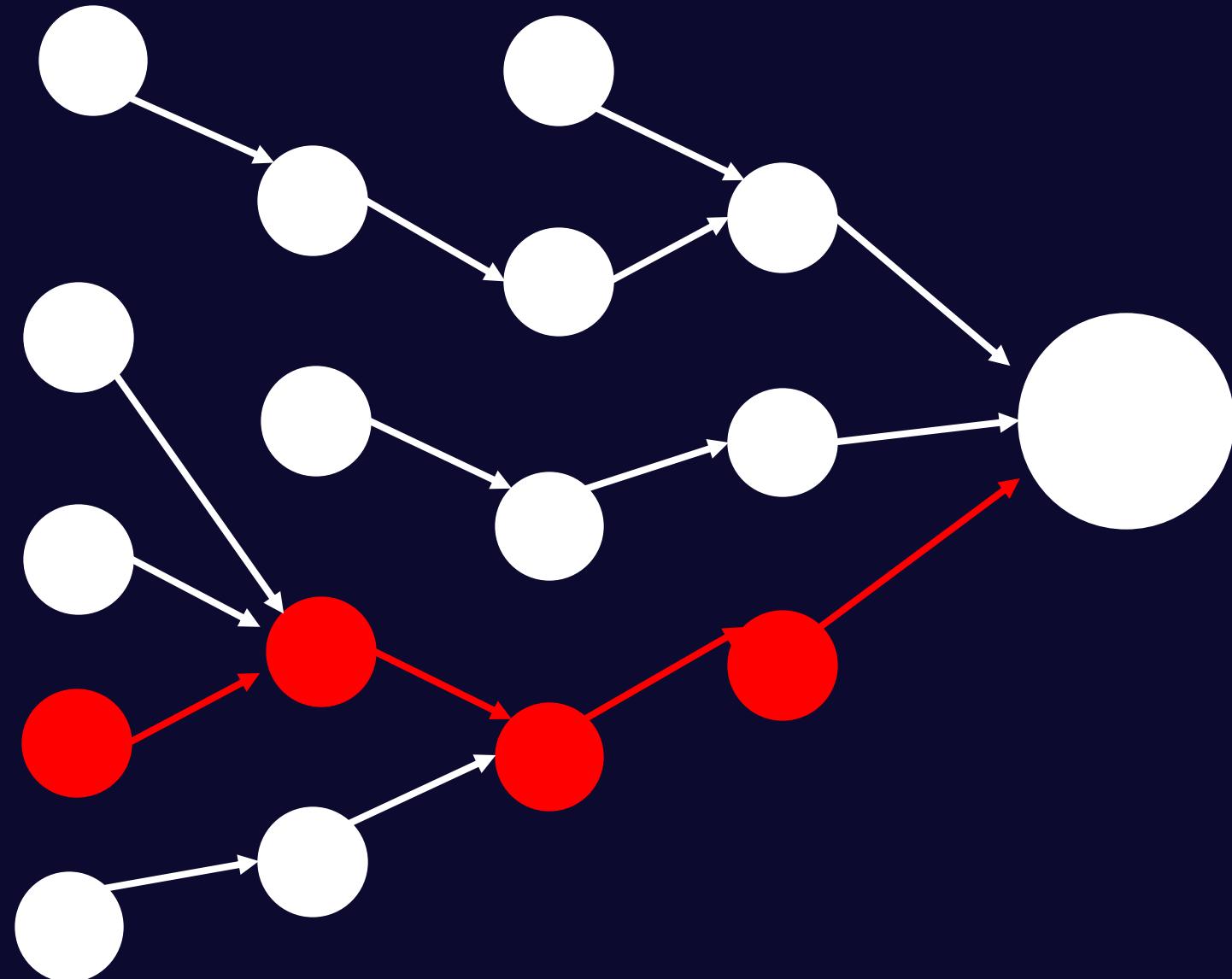


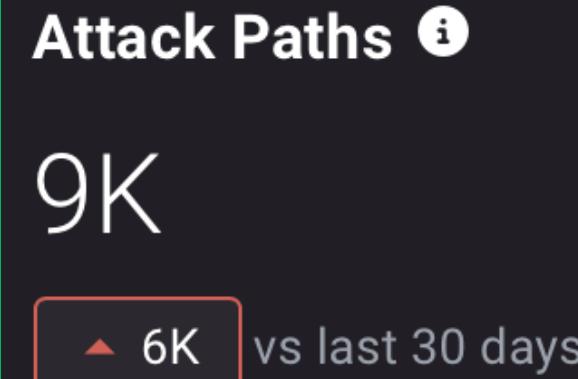
Attack Path  
Count:

7



Attack Path  
Count:  
**8**





# New Attack Path Quantification

## Understanding Posture

BloodHound Enterprise analyzes the attack path risk across your environment. Lateral movement and privilege escalation opportunities are analyzed to determine risk based on exposure (principals that can attack an object) or impact (what principals an object can attack). Learn more [here](#).

## Attack Paths

Search



Severity	Name	Category	Count	Change
Large Default Groups with Generic All Privileges	Least Privilege	Least Privilege	3	▲ 3
Kerberos Delegation on Tier Zero Objects	Kerberos	Kerberos	15	▲ 2
Large Default Groups with Write GPLink Privilege	Least Privilege	Least Privilege	16	▲ 16
Large Default Groups with Generic Write Privileges	Least Privilege	Least Privilege	2	▲ 1
Kerberoastable User Accounts	Kerberos	Kerberos	2	--
AS-REP Roastable User Accounts	Kerberos	Kerberos	1	--
Non Tier Zero Principals with ADCS ESC13 Privileges Against Tier Zero Group	AD Certificate Services	AD Certificate Services	5	▲ 5
Write Account Restrictions Privileges on Tier Zero Objects	Tier Zero	Tier Zero	3	--
		AD Certificate Services	5	▲ 4
		AD Certificate Services	12	▲ 12
		AD Certificate Services	11	▲ 10
		AD Certificate Services	6	▲ 2

# New Security Posture view

New Tier Zero Principals with ADCS  
ESC9 Scenario A Privileges

## Attack Path Summary

SpecterOps identified that 98% of all principals in the DUMPSTER.FIRE environment have at least one viable attack path leading to the compromise of a Tier Zero principal and thus absolute control of the entire environment.

### Attack Paths

9K

▲ 6K vs last 30 days

### Findings

167

▲ 84 vs last 30 days

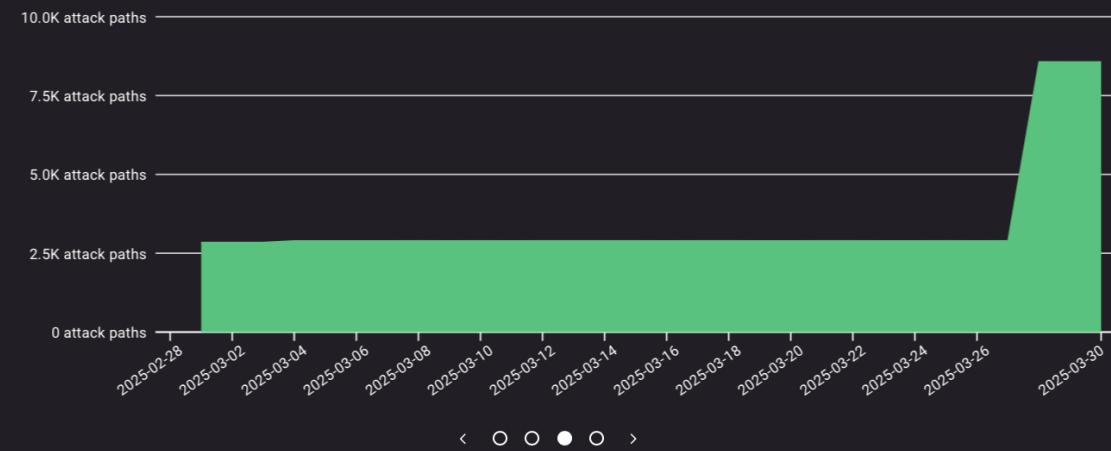
### Tier Zero Objects

86

▲ 21 vs last 30 days

## Total Attack Paths

Number of individual Attack Paths increased by 5725 between February 28, 2025 and March 30, 2025.



### Group Completeness

16%

▼ 24%

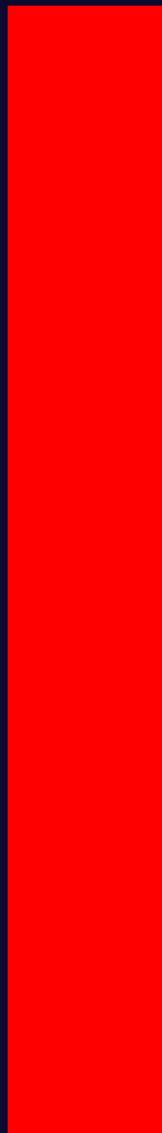
### Session Completeness

38%

= 0%

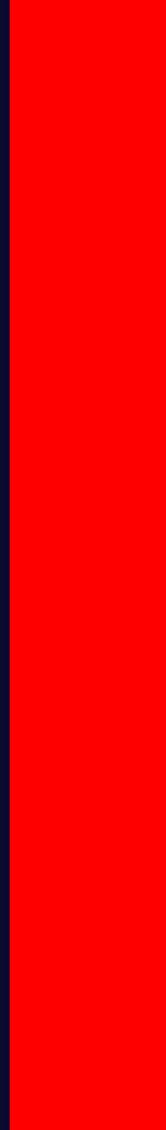
5K Identities =

5M



**5 Million  
Attack Paths**

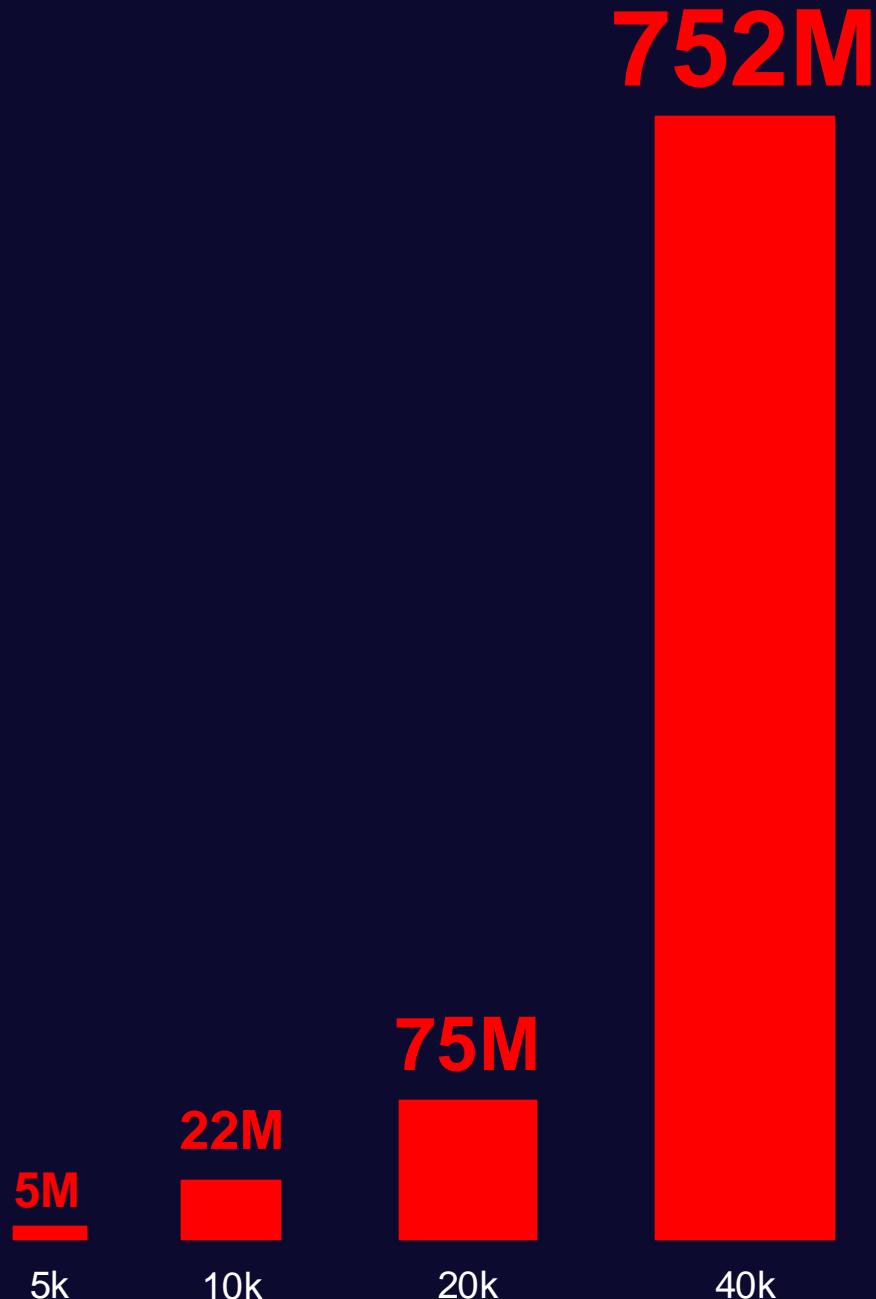
**5M**



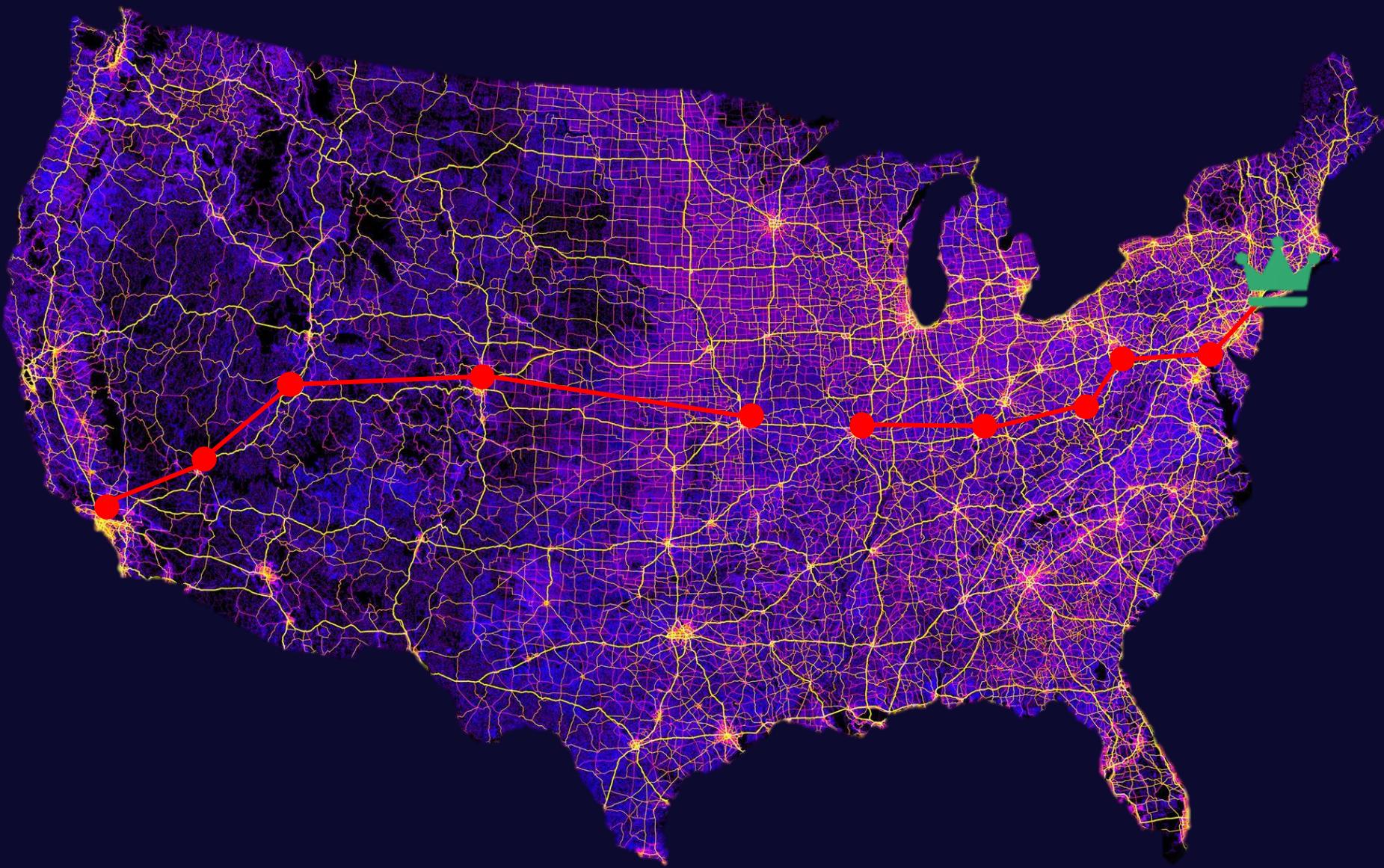
**5M**

5k

More Identities  
More Problems



**151 Billion  
Problems  
(to be exact)**



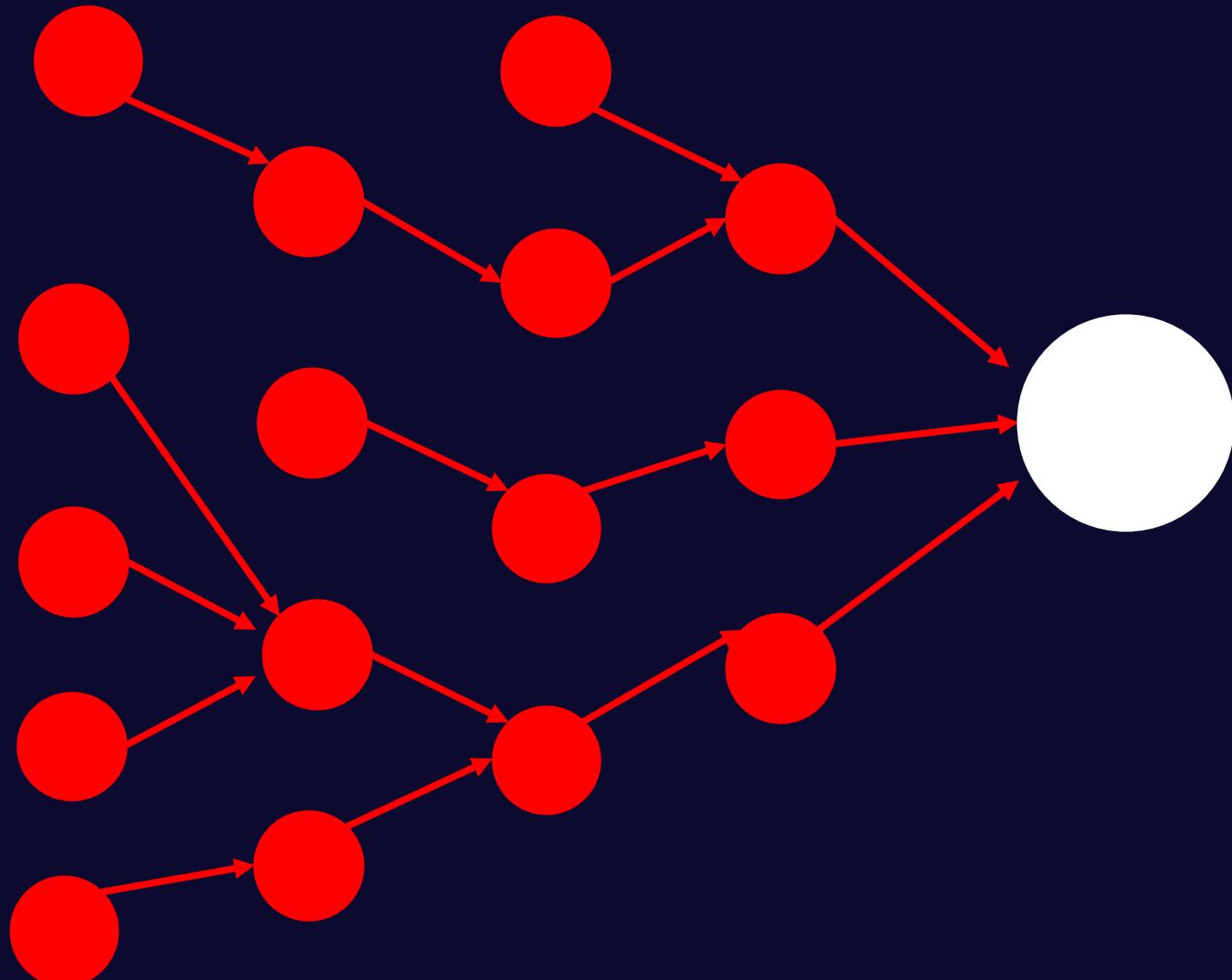
Billions of routes  
Billions of Attack Paths

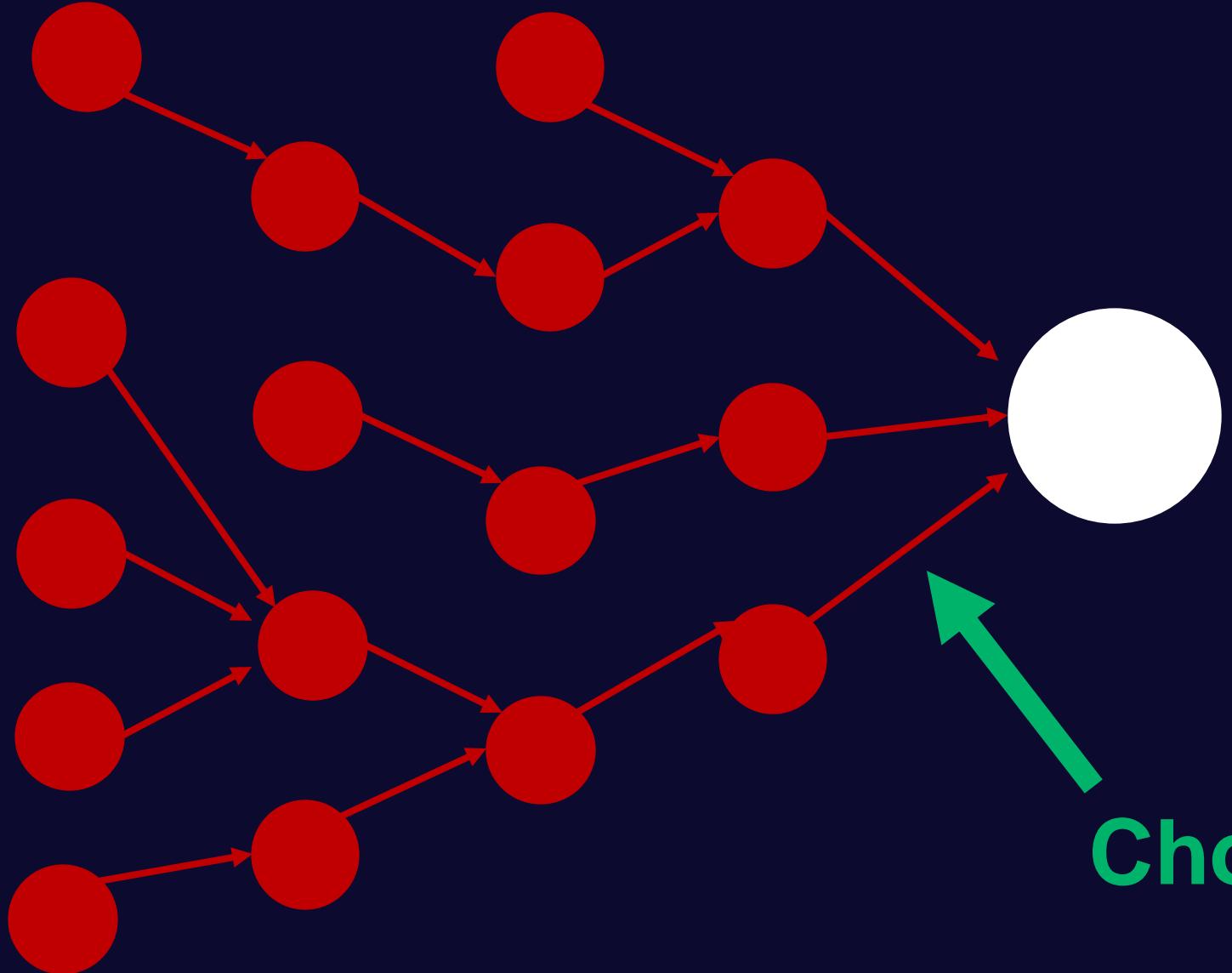
through millions of roads  
through millions of relationships

connecting thousands of cities  
connecting thousands of identities

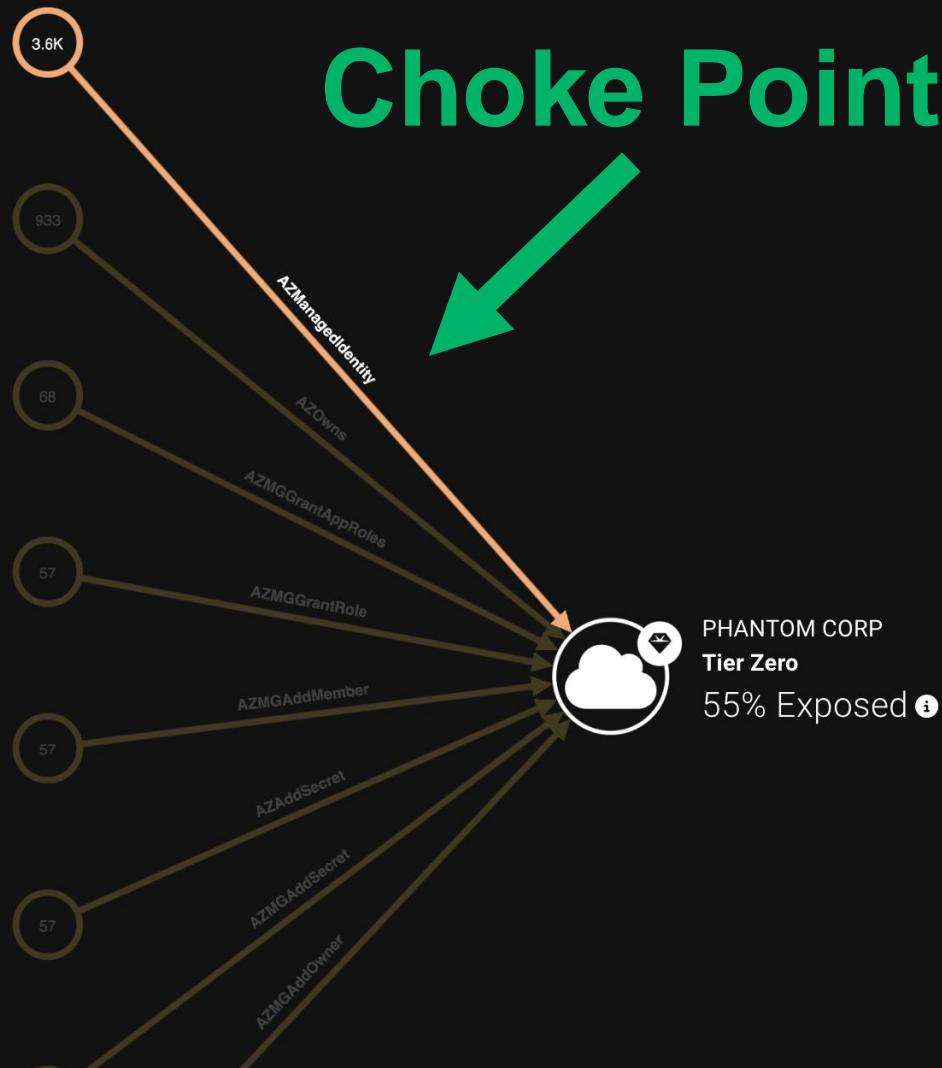
to Manhattan  
to critical resources

Attack Path  
Count:  
**16**





Choke Point



## New Attack Paths view

Reset View

PHANTOM CORP ⚙️

Status: Idle Last Analysis: 2025-03-29 17:02 PDT (GMT-0700)

Non Tier Zero Resource Assigned to Tier Zero Service Principal

2 Findings 2 vs last month Moderate

Description

This Attack Path exposes Tier Zero to 3.6K principals. ⓘ

Azure resources like Virtual Machines, Logic Apps, and Automation Accounts can be assigned to either System- or User-Assigned Managed Identities. This assignment allows the Azure resource to authenticate to Azure services as the Managed Identity without needing to know the credential for that Managed Identity. Managed Identities, whether System- or User-Assigned, are AzureAD Service Principals.

Only those Azure resources that are trusted to authenticate as a Tier Zero asset should be assigned to a System- or User-Assigned Managed Identity which is itself a Tier Zero Service Principal.

2 Findings Timeline

Accepted

Severity ⓘ	Exposure	Non Tier Zero Resource	Tier Zero Principal	Impact
●	3.6K	JOHNSAUTOMATIONAC...	SERVICEPRINCIPALE@P...	3
●	0	MYCOOLAUTOMATIONA...	MYCOOLAUTOMATIONA...	11

REMEDIALION

Re-assign the Azure resource to a non Tier Zero Managed Identity

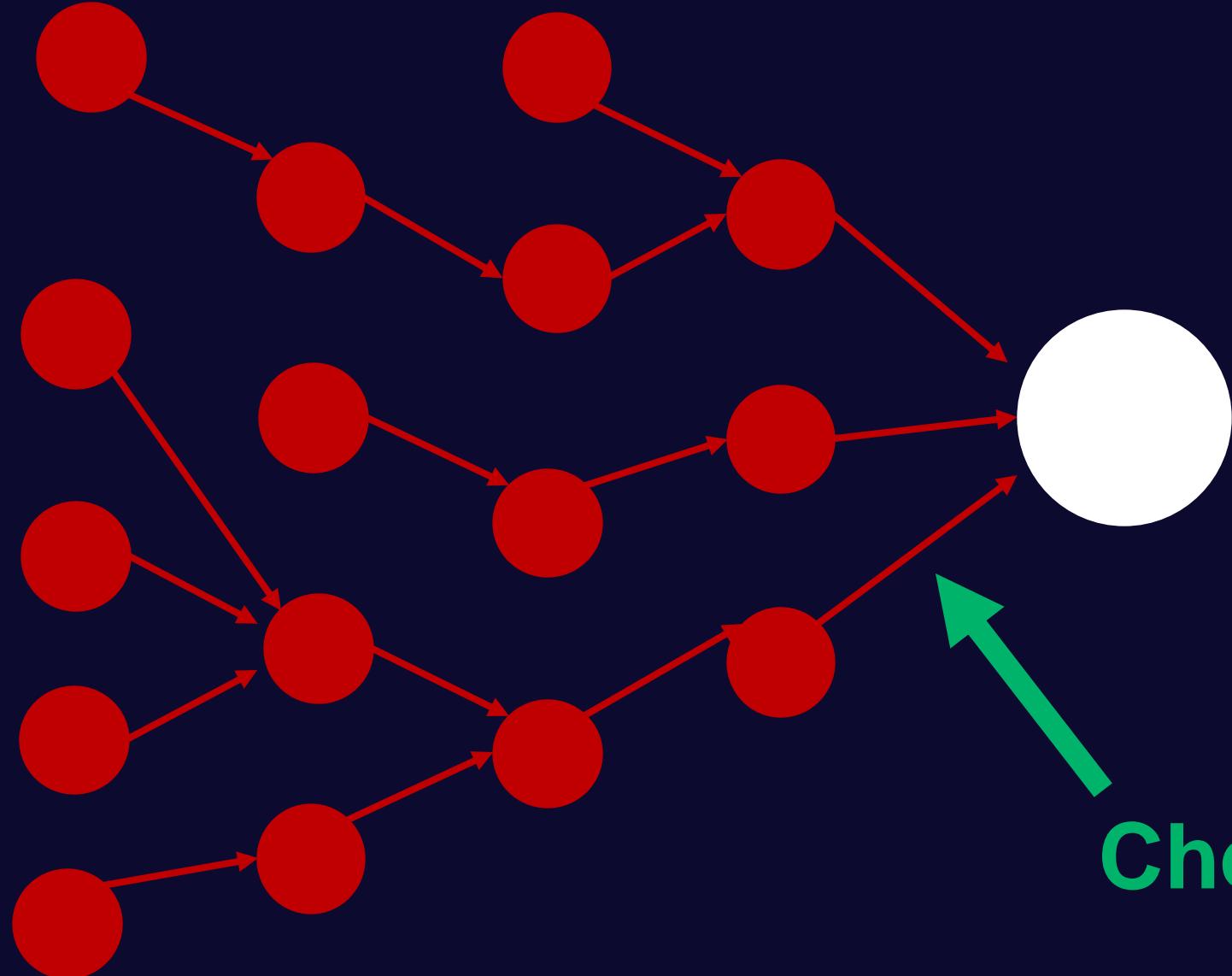
View / Export Full Remediation Plan Export CSV

Ownership of Tier Zero Principal

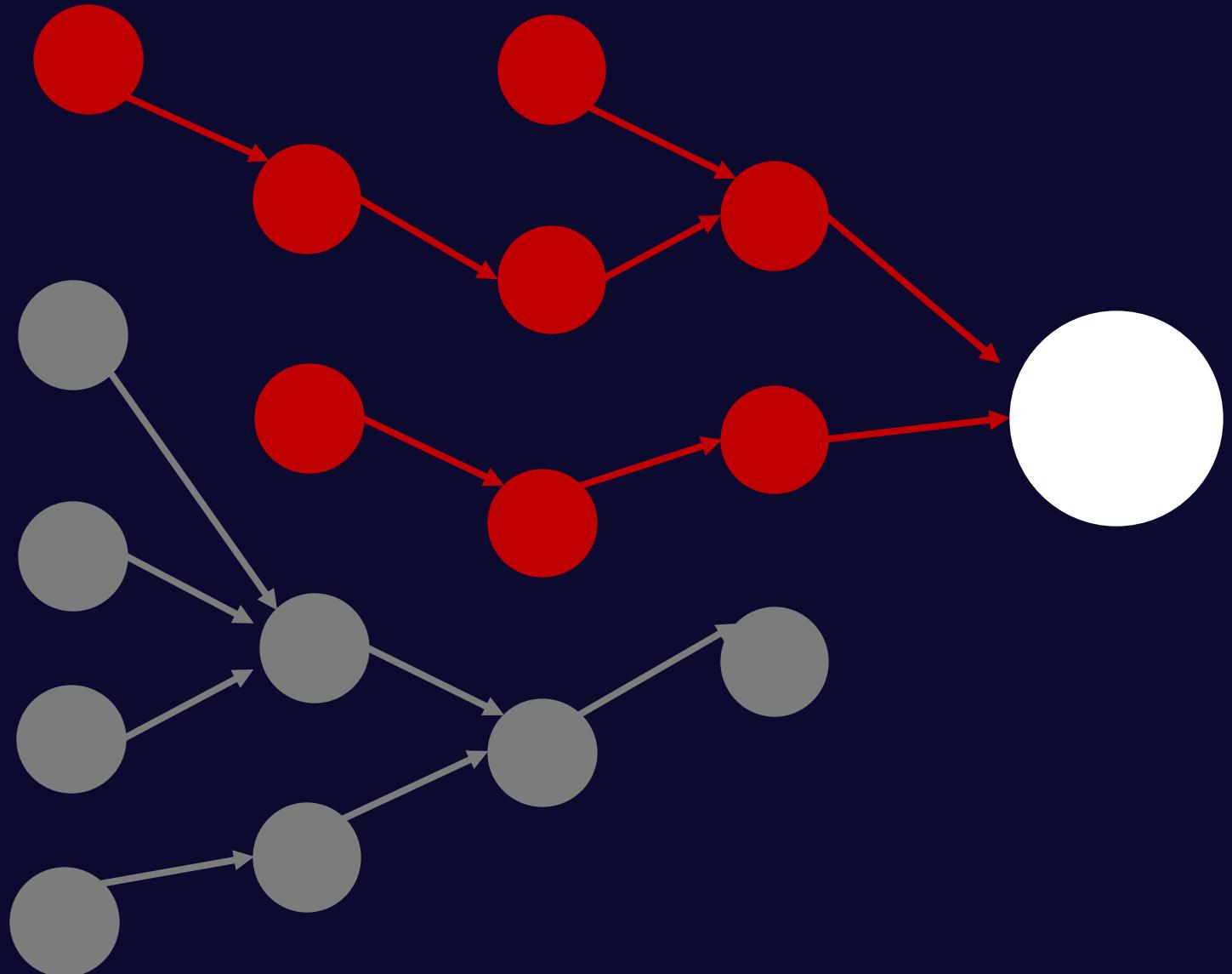
2 Findings ± 0 vs last month Low

Non Tier Zero Principal Can Grant Tier Zero App Roles

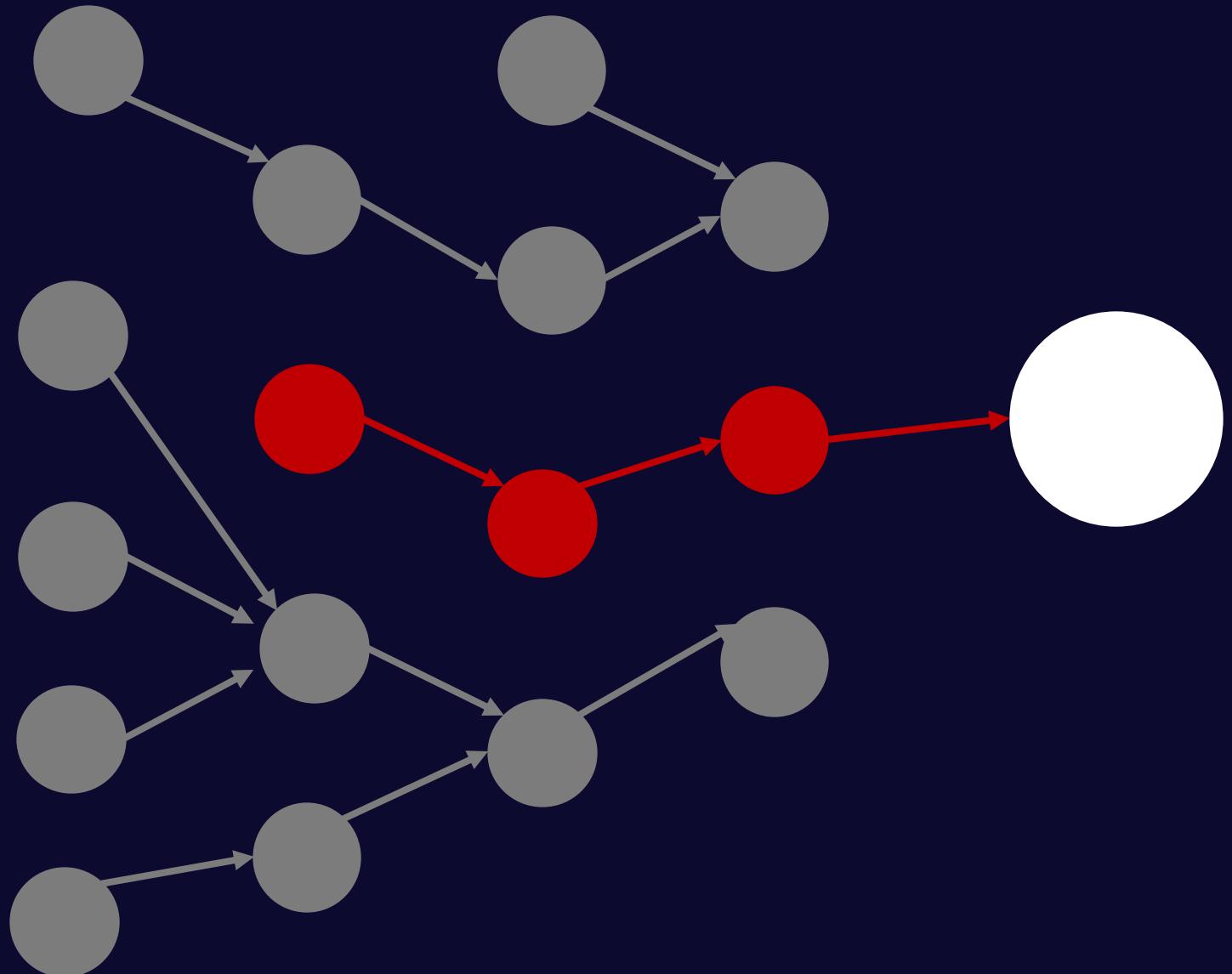
26 Findings 6 vs last month Low



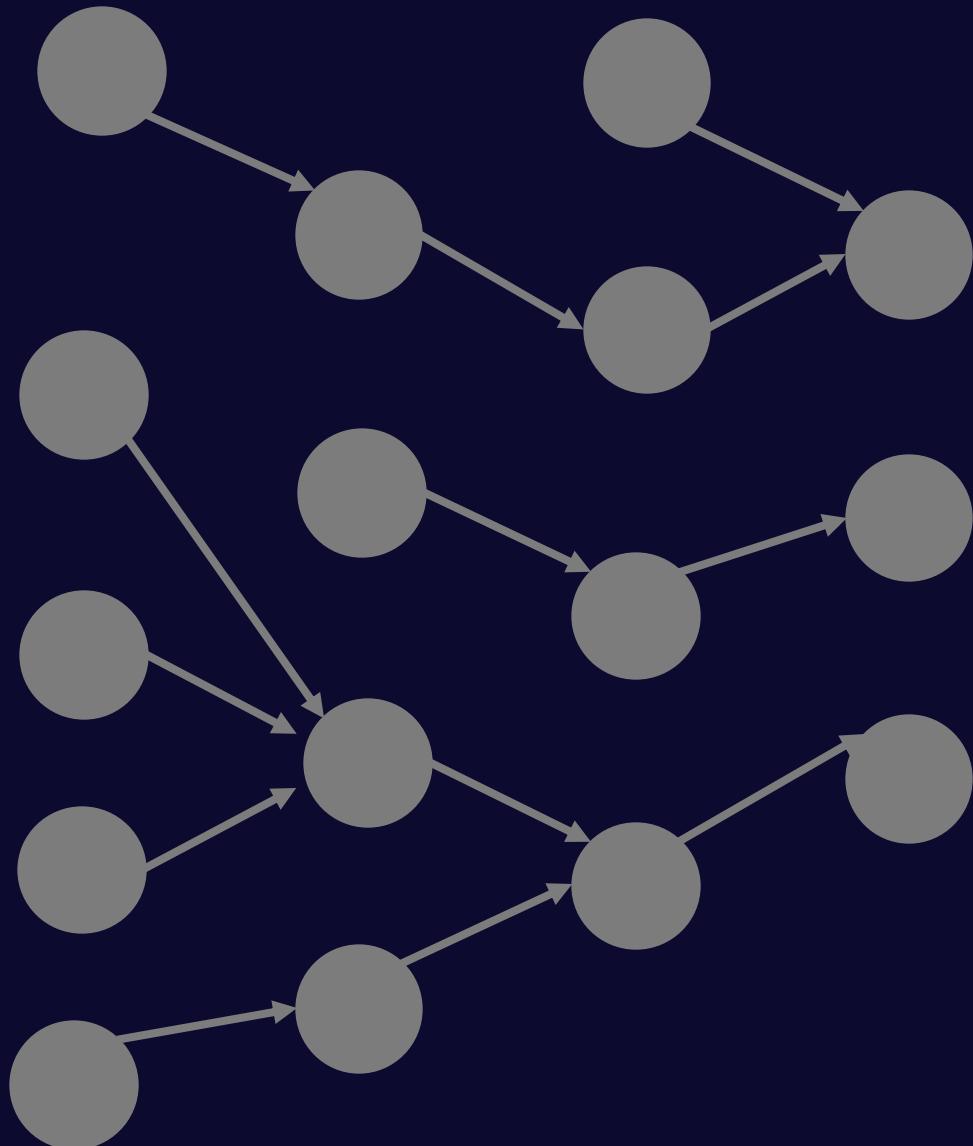
Choke Point



Attack Paths  
Removed:  
**8**



Attack Paths  
Removed:  
**13**

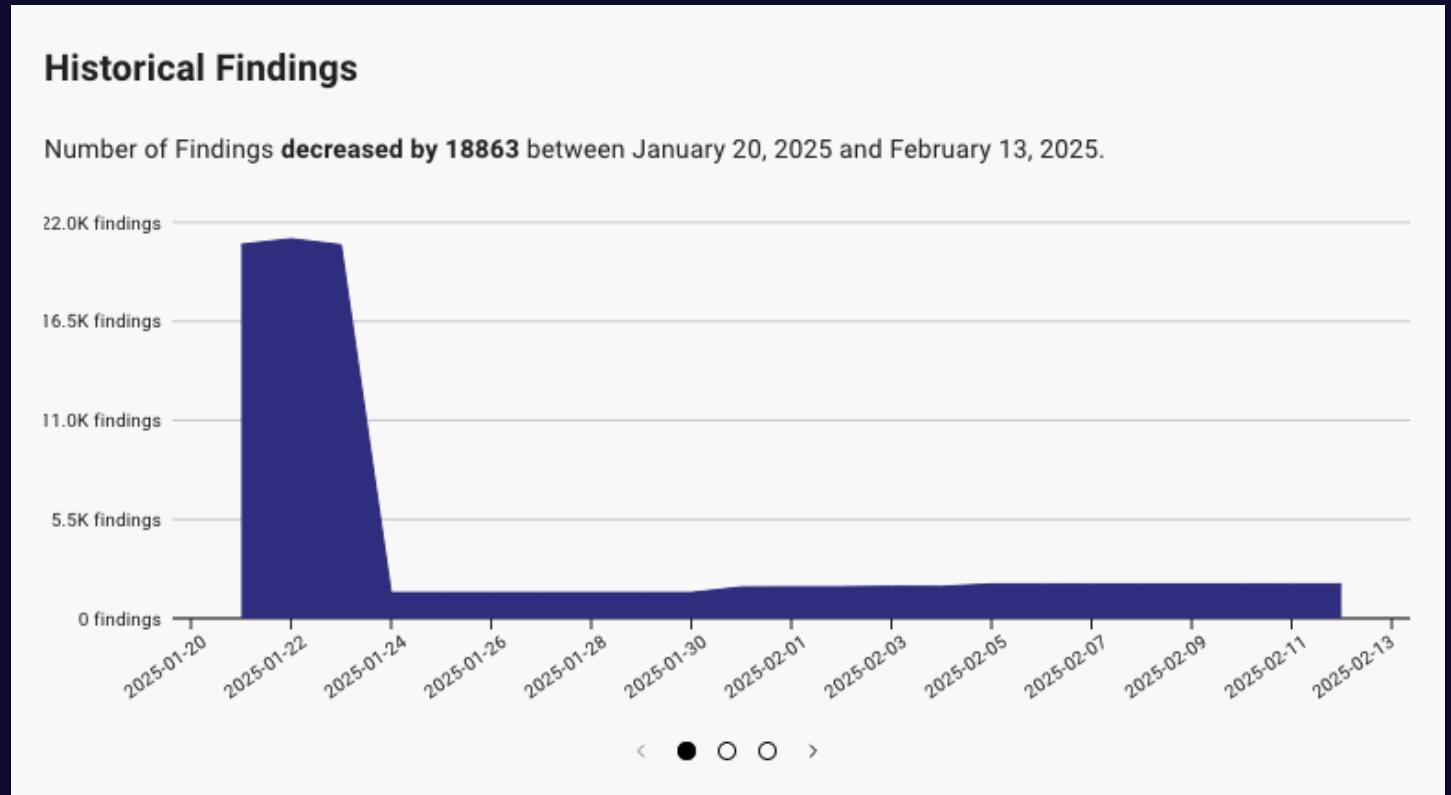


Attack Paths  
Removed:  
**16**



Fixing one finding  
**cuts 300,000**  
Attack Paths

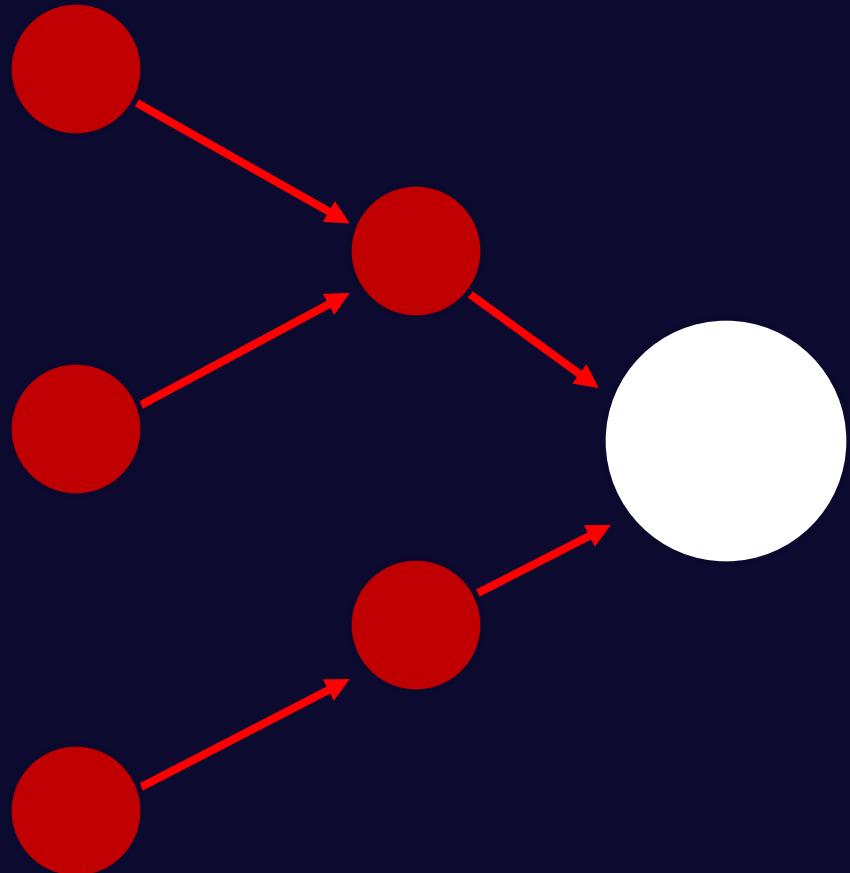
# Findings Resolved

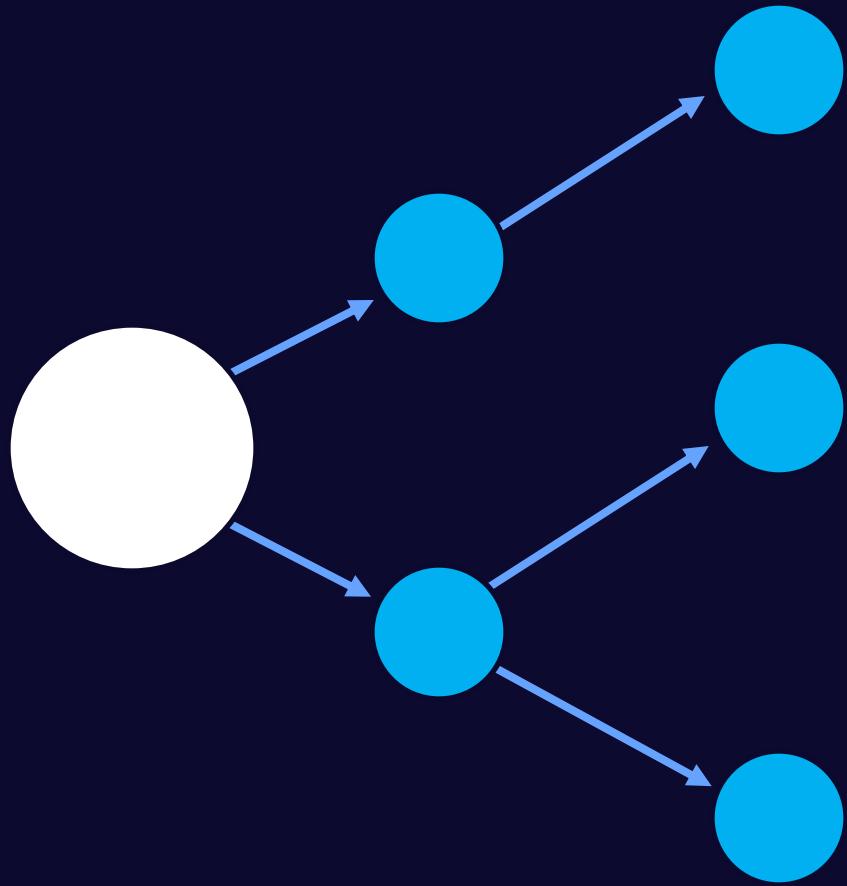


Finding reduction during trial

## Exposure

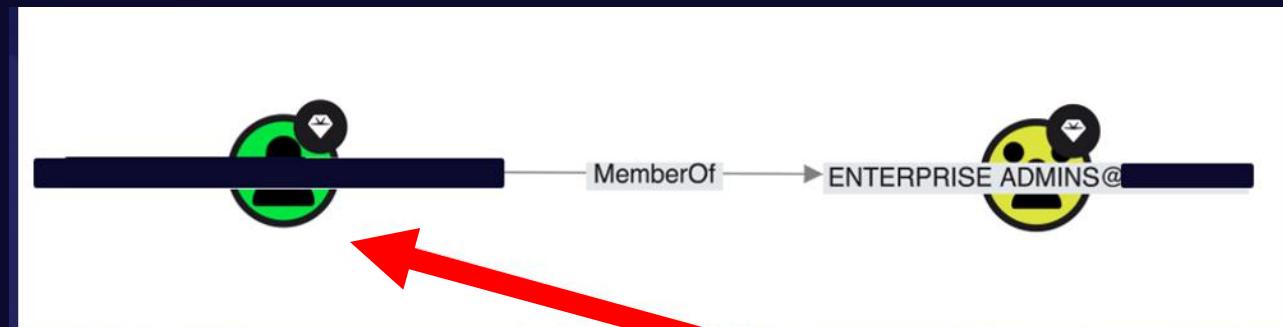
The Attack Paths to  
a target node





**Impact**  
The attack paths  
from a target node

# New Attack Path Impact



Kerberoastable User Accounts    53 Findings    4 vs last month    Critical

Description

Services hosted on Windows systems that support Kerberos authentication should use computer accounts as the service principal. During the Kerberos authentication process, principals may request a ticket-granting service (TGS) ticket for a service from a domain controller. The validity of that TGS ticket is validated by the service principal due to the TGS ticket being signed and encrypted with the NT hash of the service principal's password.

This process makes the service principal's password susceptible to offline brute force attacks, as the TGS ticket may be requested by any domain authenticated user or computer. Then, an attacker with possession of this TGS ticket may perform an offline brute force attack which, if successful, recovers the plaintext password of the service principal.

53 Findings    Timeline

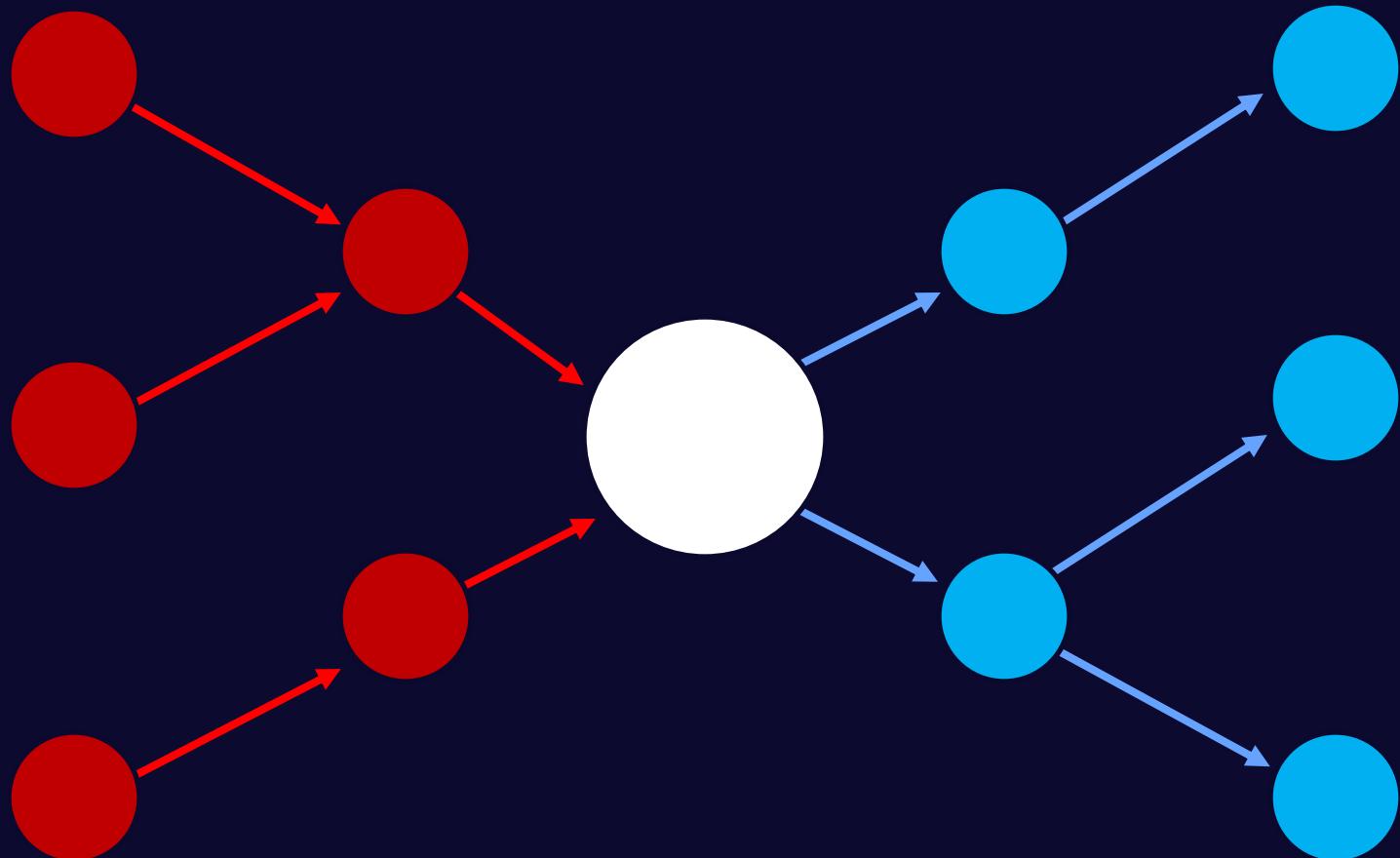
Accepted

Severity	User	Password Last Set	Last Login	Impact
Low	[User]	2008-12-15	2020-02-27	167.6K
Low	[User]	2014-05-09	2024-12-10	167.6K
Low	[User]	2012-05-29	2020-02-27	167.6K
Low	[User]	2019-05-03	2023-11-03	167.6K
Low	[User]	2010-05-20	2020-02-27	167.6K
Low	[User]	2024-12-11	2024-12-11	167.6K
Low	[User]	2010-05-20	2020-02-27	167.6K
Medium	[User]	2003-11-29	2022-10-22	167.6K   99%
Low	[User]	2013-03-13	2024-12-10	167.6K
Low	[User]	2006-12-09	2024-12-10	167.6K

Password Last Set: **2003-11-29**

## Exposure

The Attack Paths to  
a target node



## Impact

The attack paths  
from at target node

# New Granular Attack Path Risk

Logons from Tier Zero Users

23 Findings 10 ↗ vs last month Critical

Description

This Attack Path exposes Tier Zero to 2.7K principals. ⓘ

Only use user accounts belonging to the "Domain Admins," "Enterprise Admins," and "Administrators" domain groups, and other Tier Zero user accounts for tasks that require the higher privileges in Active Directory. Those users should only log onto the Domain Controllers or special systems such as Privileged Access Workstations.

Whenever a user performs an interactive logon on a system, that system may store the user's password in plain text in memory. Even with mitigations against plaintext password storage, interactive logons also result in processes running on the system with primary (or "process") tokens for that user. Such tokens can be used to authenticate to other systems without the need to re-type a password.

An attacker with administrative access on the system may abuse plaintext password storage or the Windows token model to impersonate the user, performing actions as that user and abusing whatever privileges that user may have.

23 Findings Timeline

Accepted

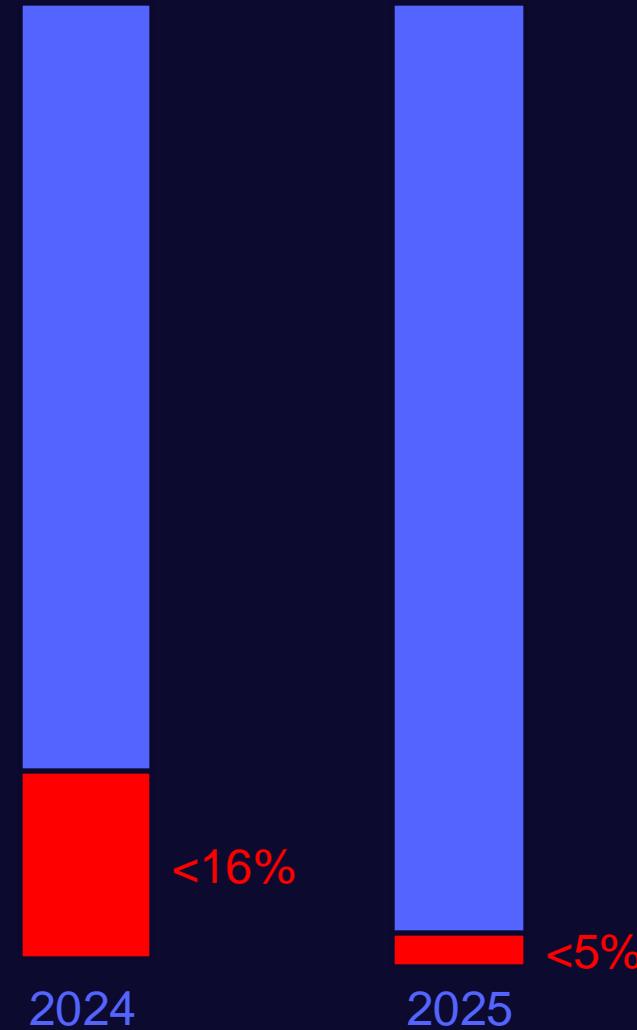
Severity ⓘ	Exposure	Non Tier Zero Principal	Tier Zero User	Impact
High	2.7K	CX-A	RY	2.8K
Medium	67	CS-F	RY	2.8K
Medium	65	CS-S	RY	2.8K
Medium	61	CC-V	RY	2.8K

# Active Directory Certificate Services (ADCS)



65% of critical ADCS ESC1  
have been remediated

Now found in 5% of  
environments

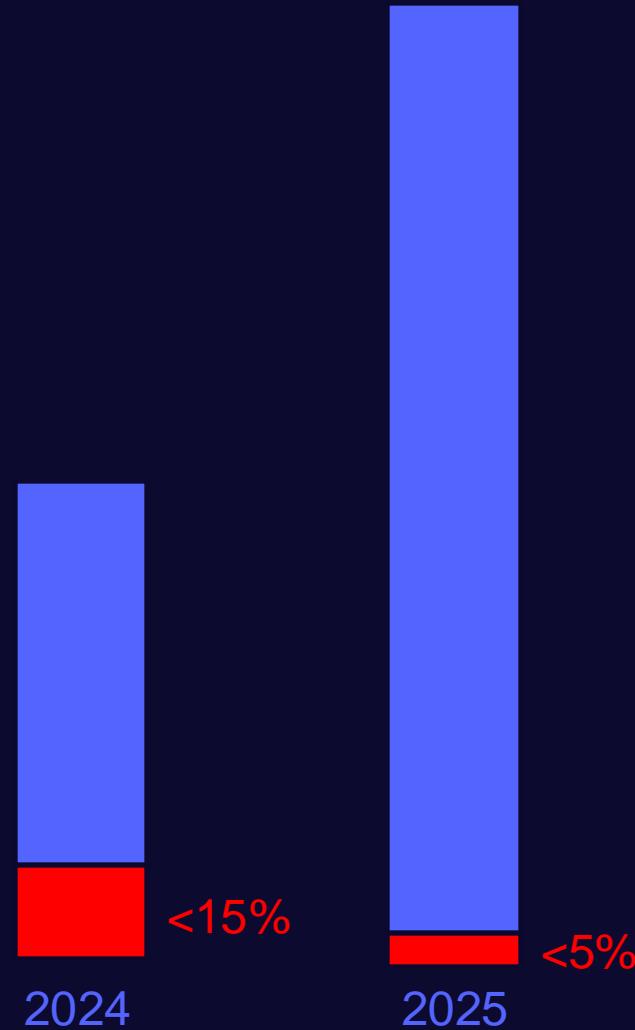


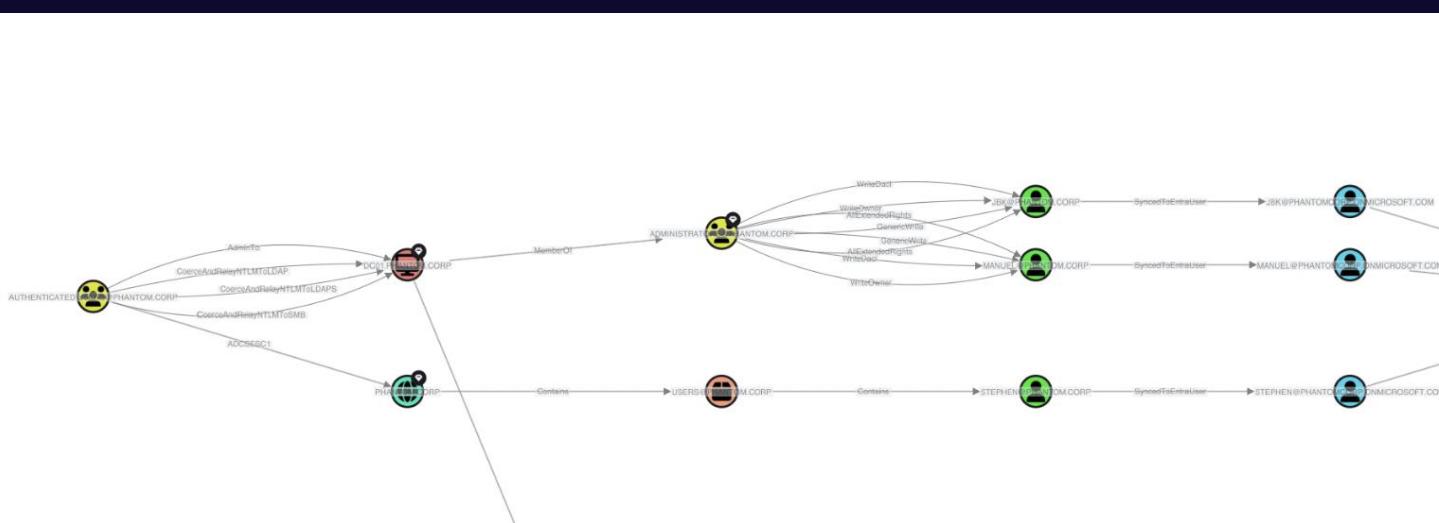
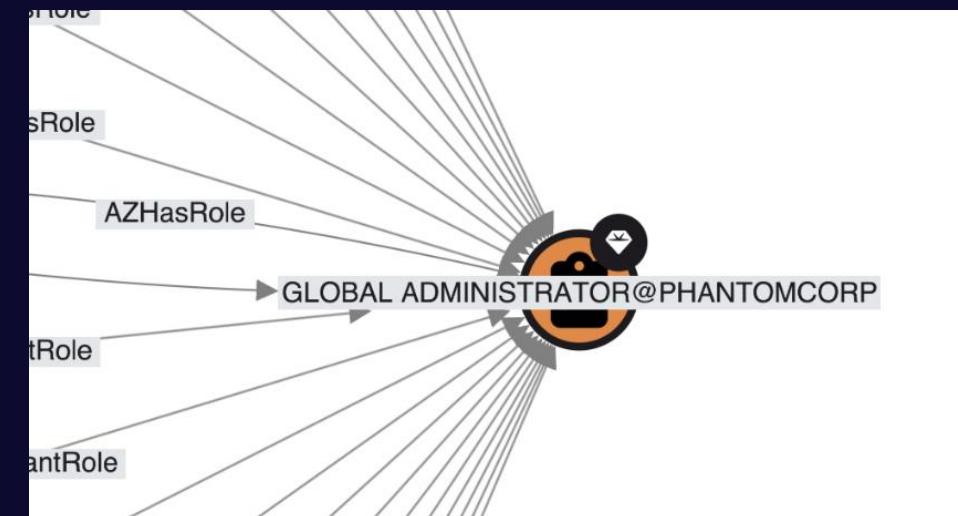
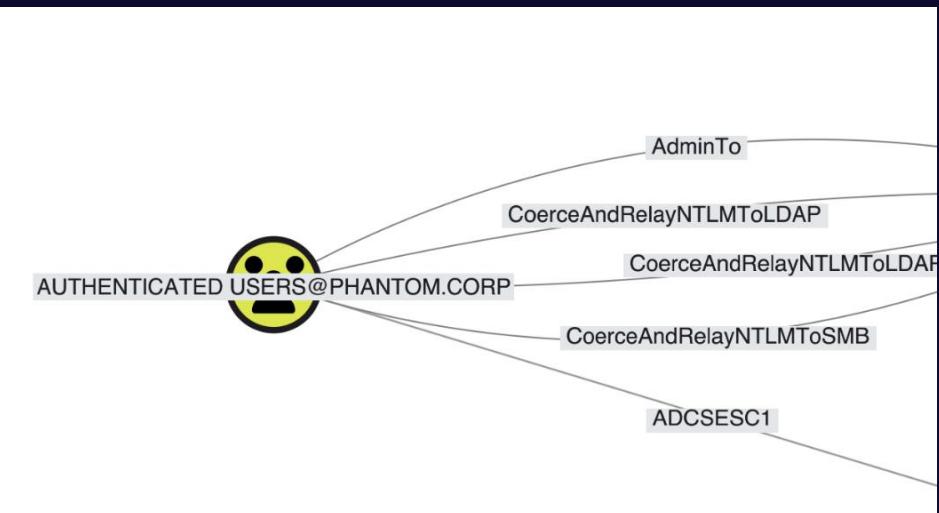
65% of critical ADCS ESC1  
have been remediated

Now found in 5% of  
environments

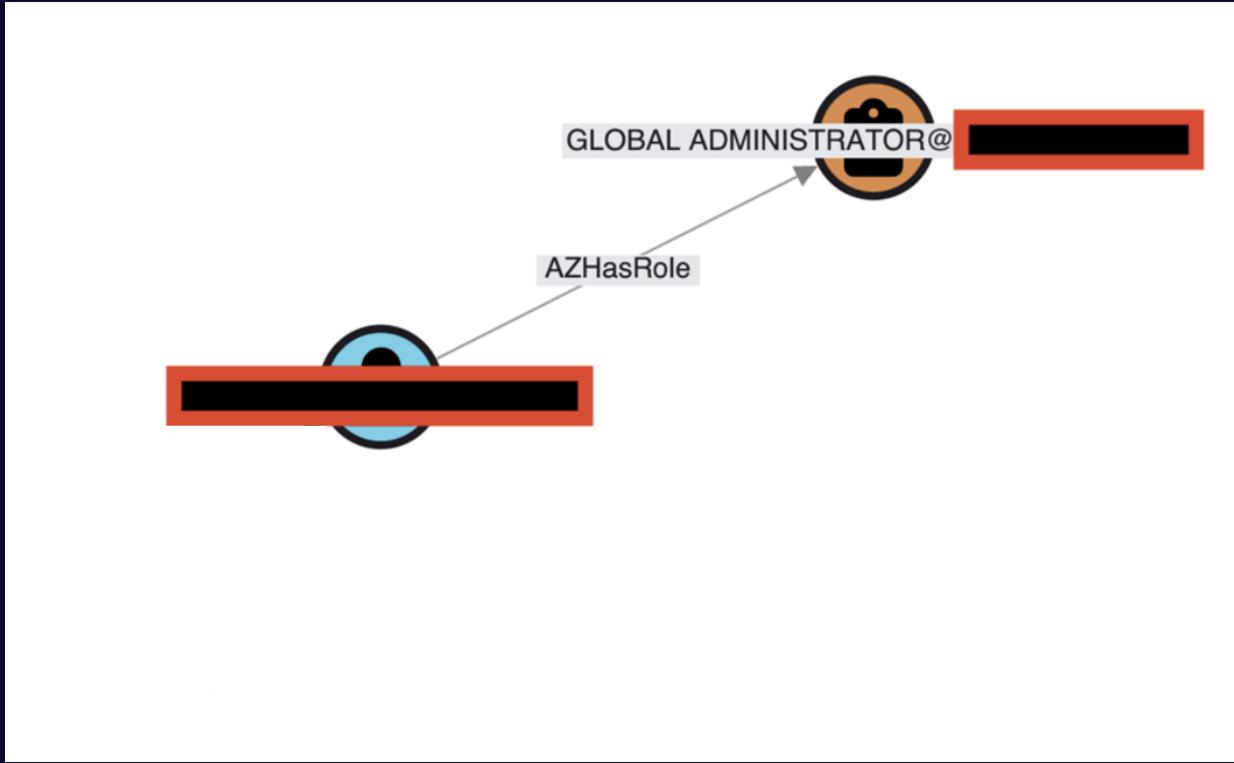
We also doubled monitored  
environments

*(identified and remediated even more)*

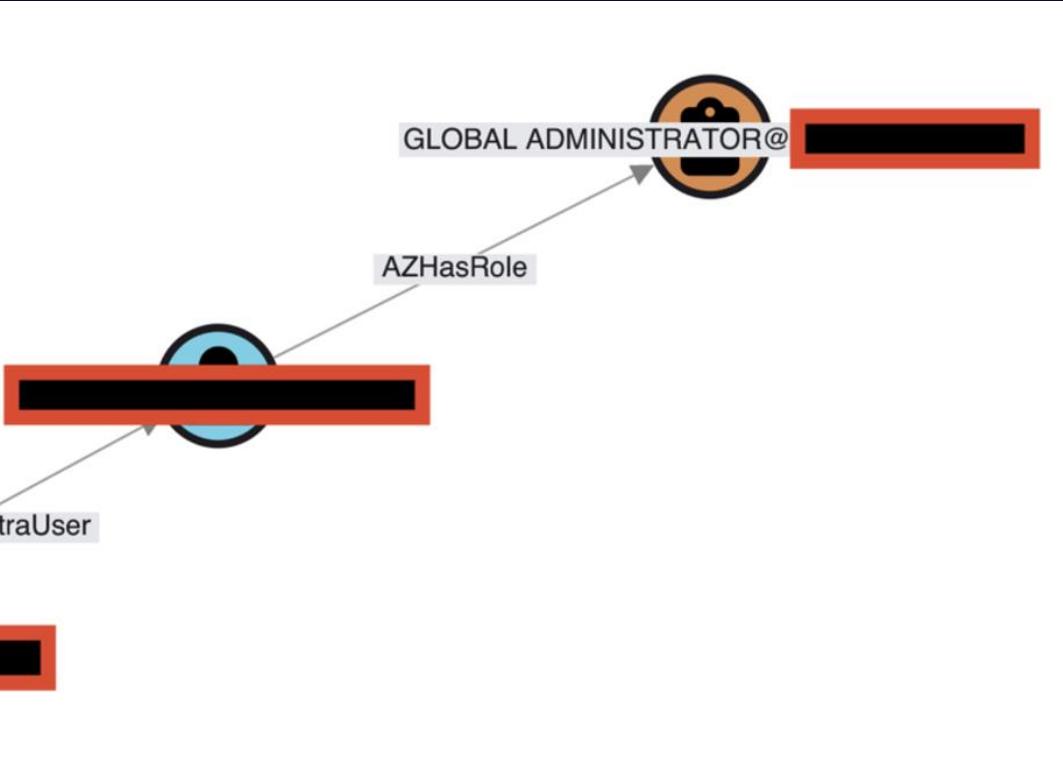




# Azure's biggest security problem is Active Directory



**5%**  
Azure Tier Zero  
Exposure



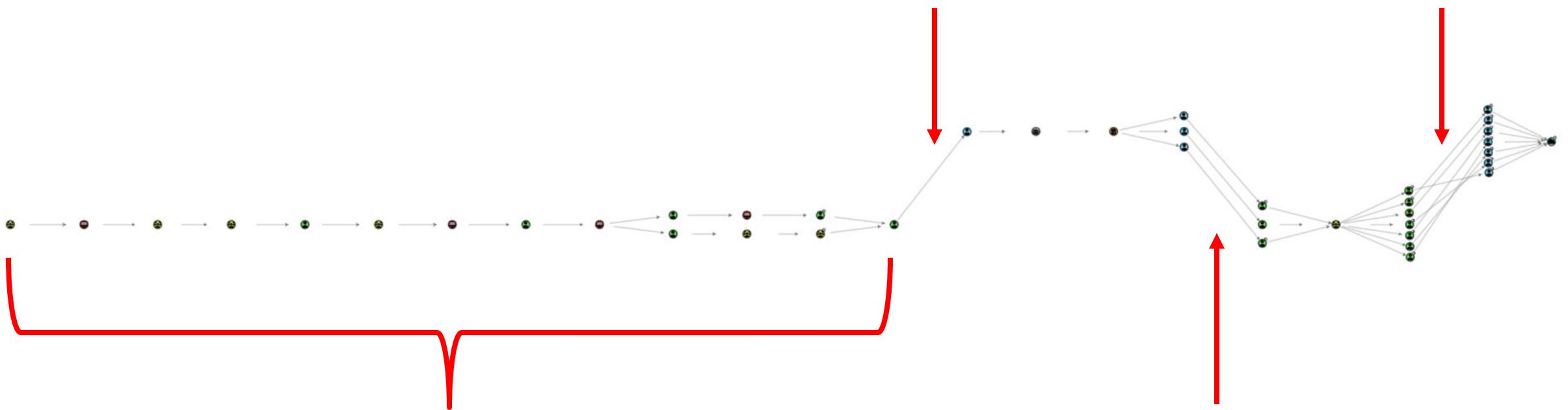
**97%**  
Azure Tier Zero  
Exposure

Pivot back to  
Entra ID for  
Global Admin

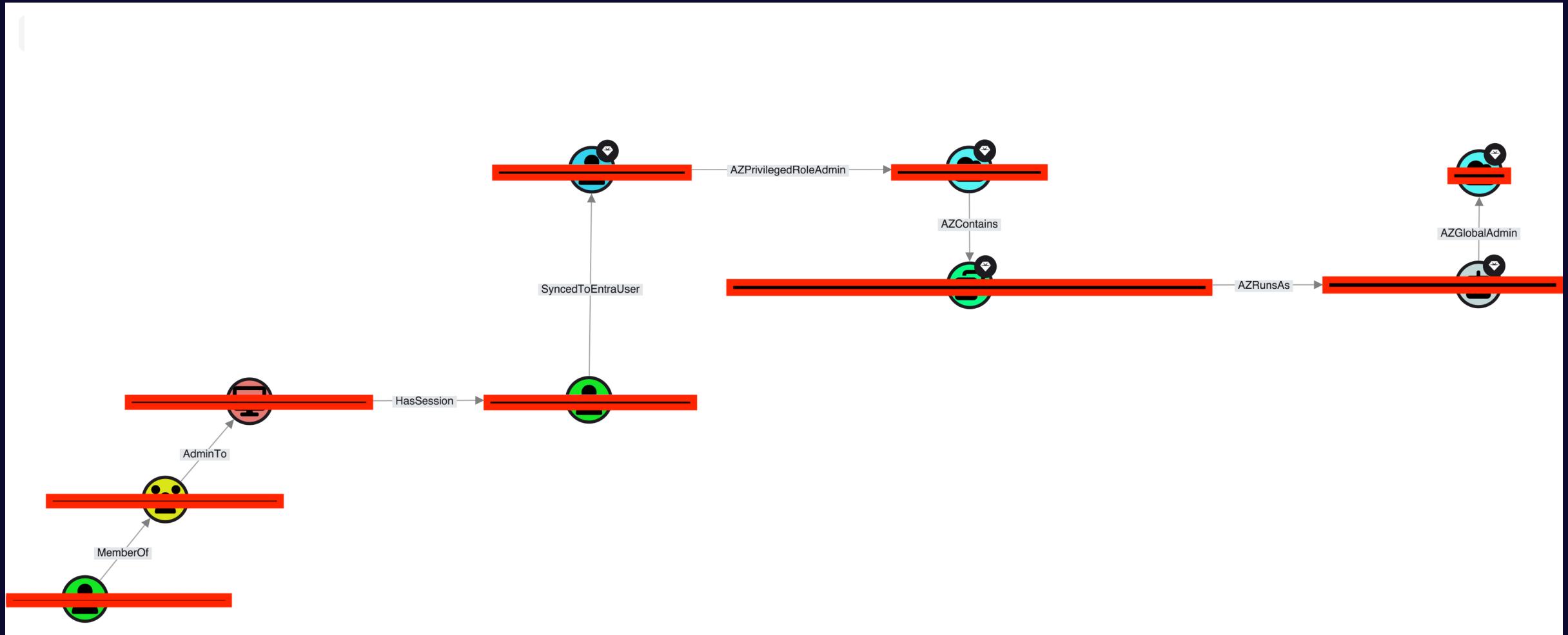
Pivot to Entra ID

Cross three domain trusts

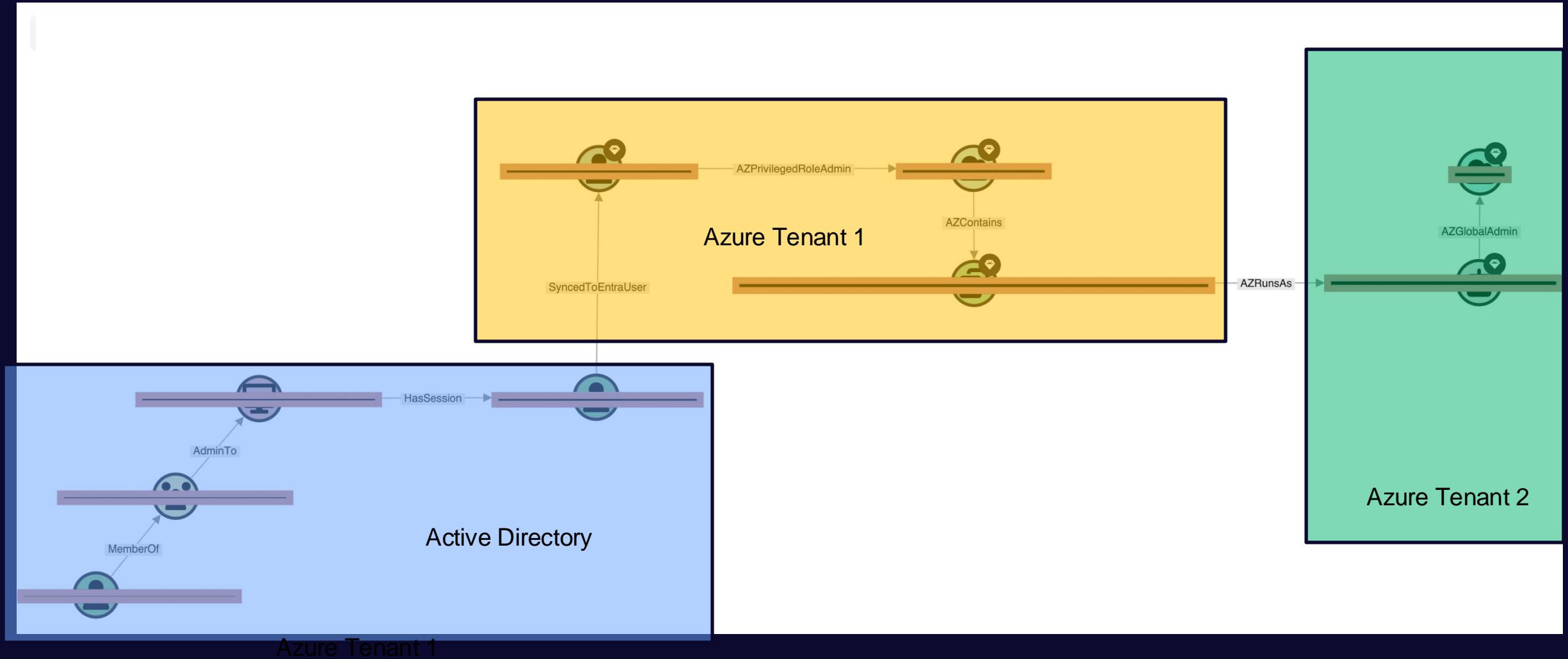
Pivot to back to AD

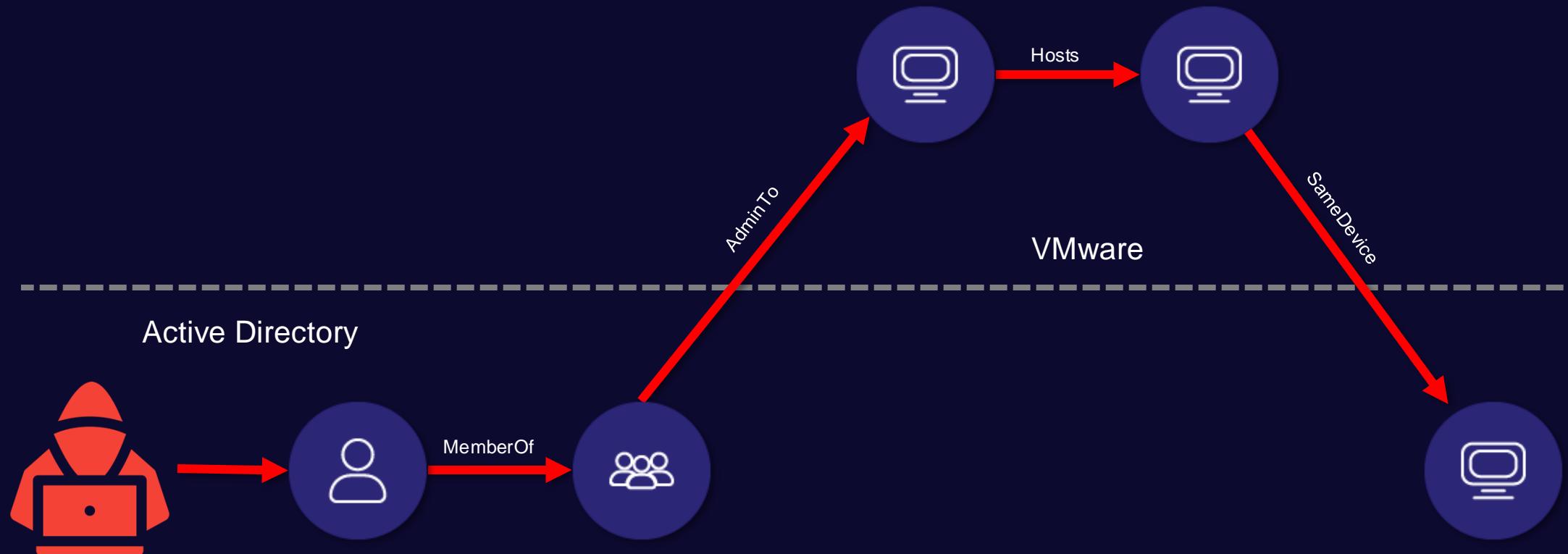


# Cross-tenant Attack Paths are a problem



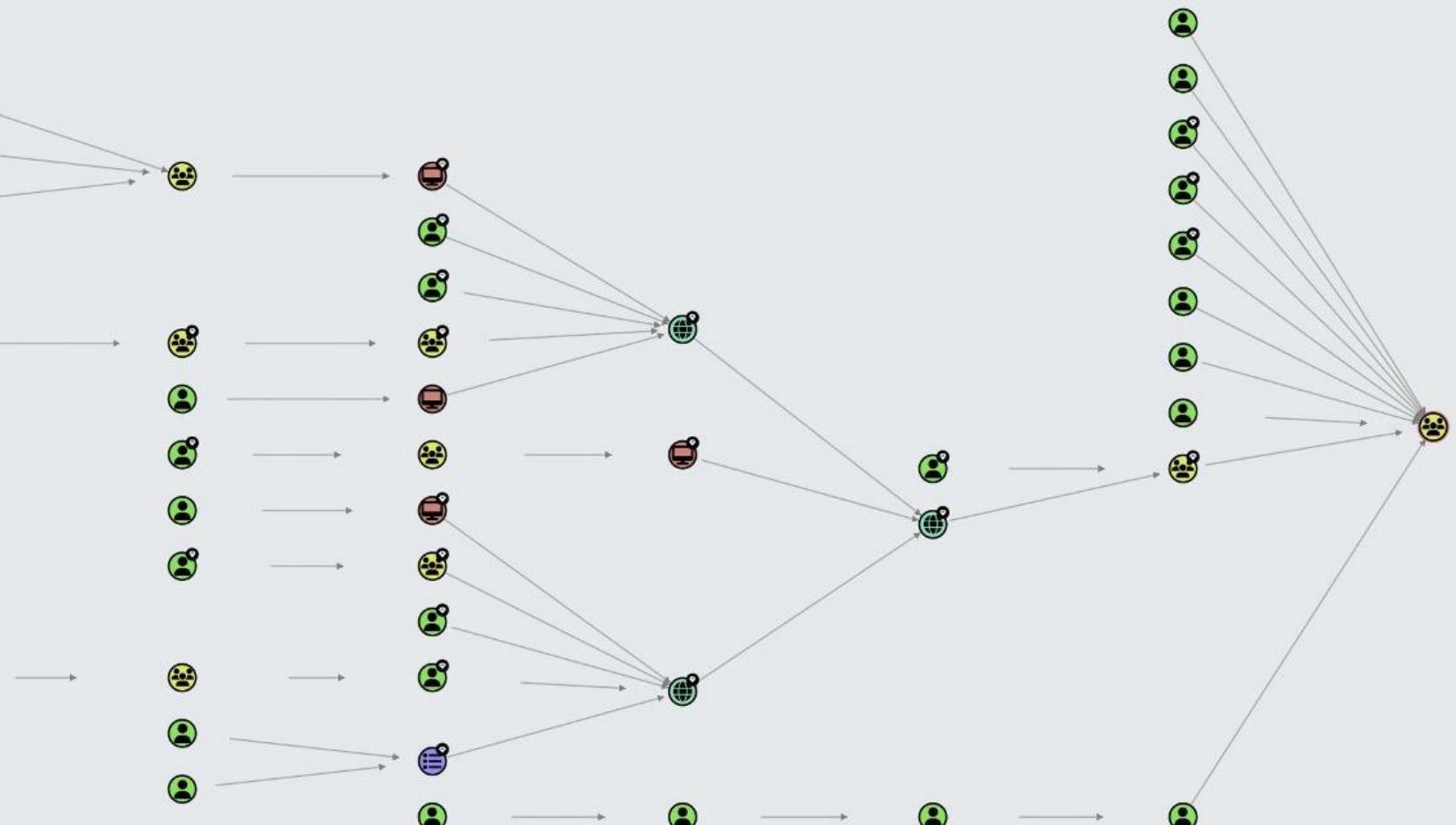
# Cross-tenant Attack Paths are a problem





+ SEARCH ◆ PATHFINDING </> CYpher

+  ESX ADMINS@SEVENKINGDOMS.LOCAL ⌂



+

SEARCH

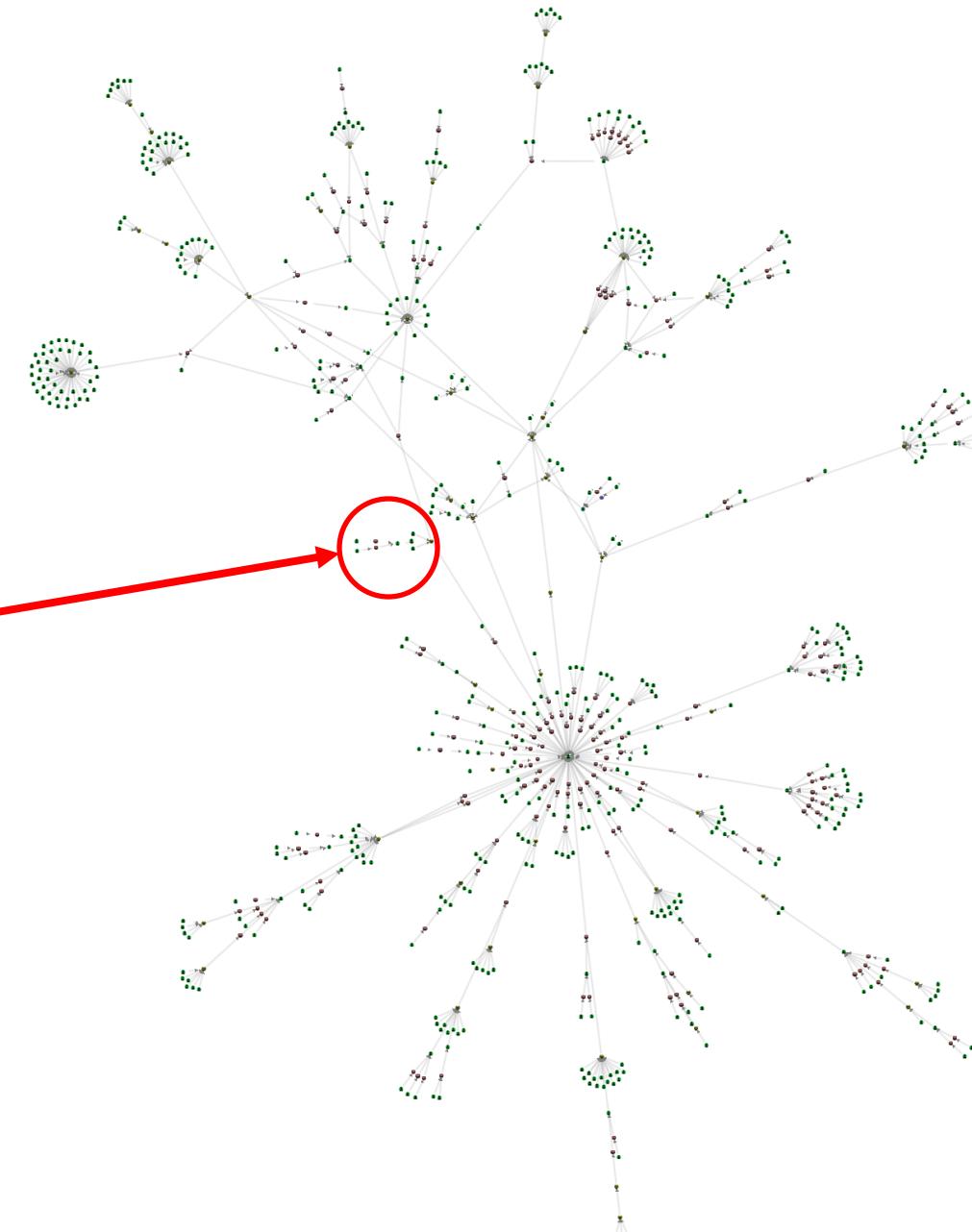
PATHFINDING

CYPER

+



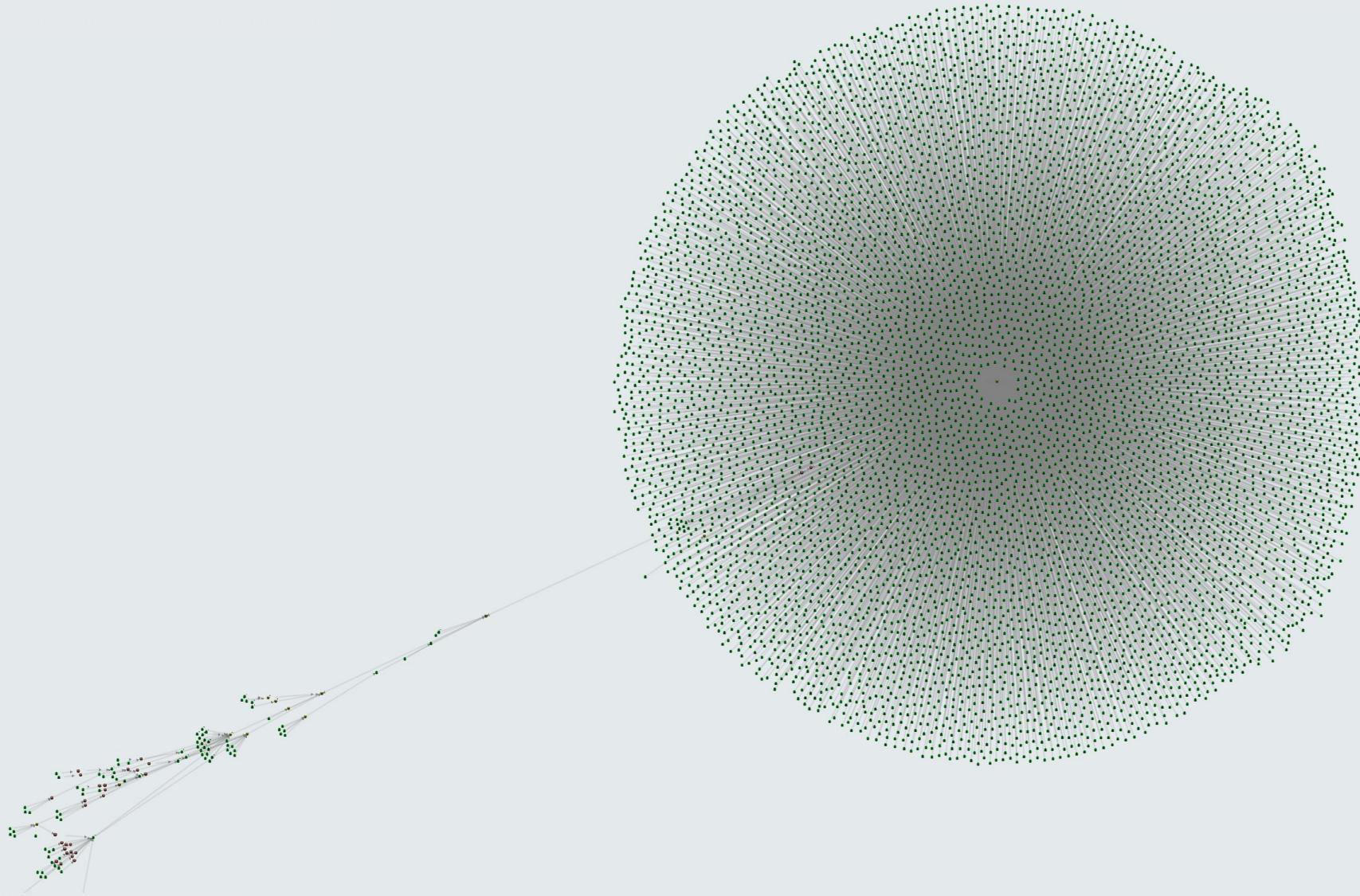
ESX ADMINS@

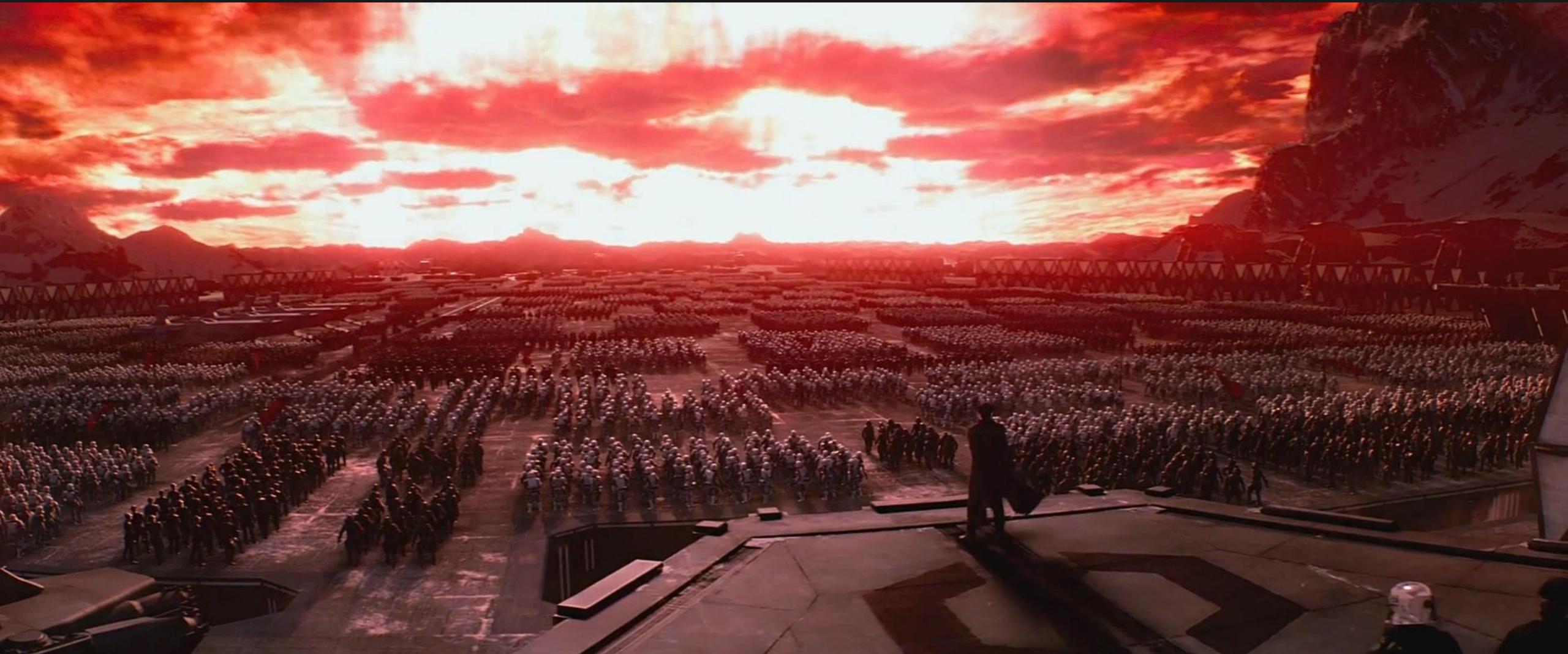


Layout

Export

Search Current Results



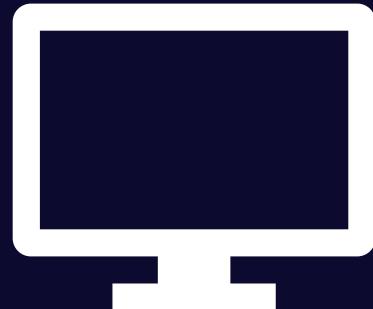


We are ESX Admins



Your “Least Privilege”

# NTLM in BloodHound

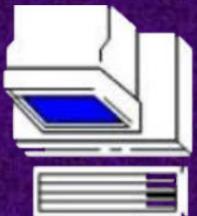


BLOODHOUND

# *NTLM and BloodHound*

---

Fighting 1993 in 2025

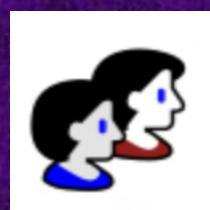




# NTLM In BloodHound



- The average exposure introduced by NTLM Attack Paths is 97%



Authenticated  
Users



Coerce & relay



Computer



Jane



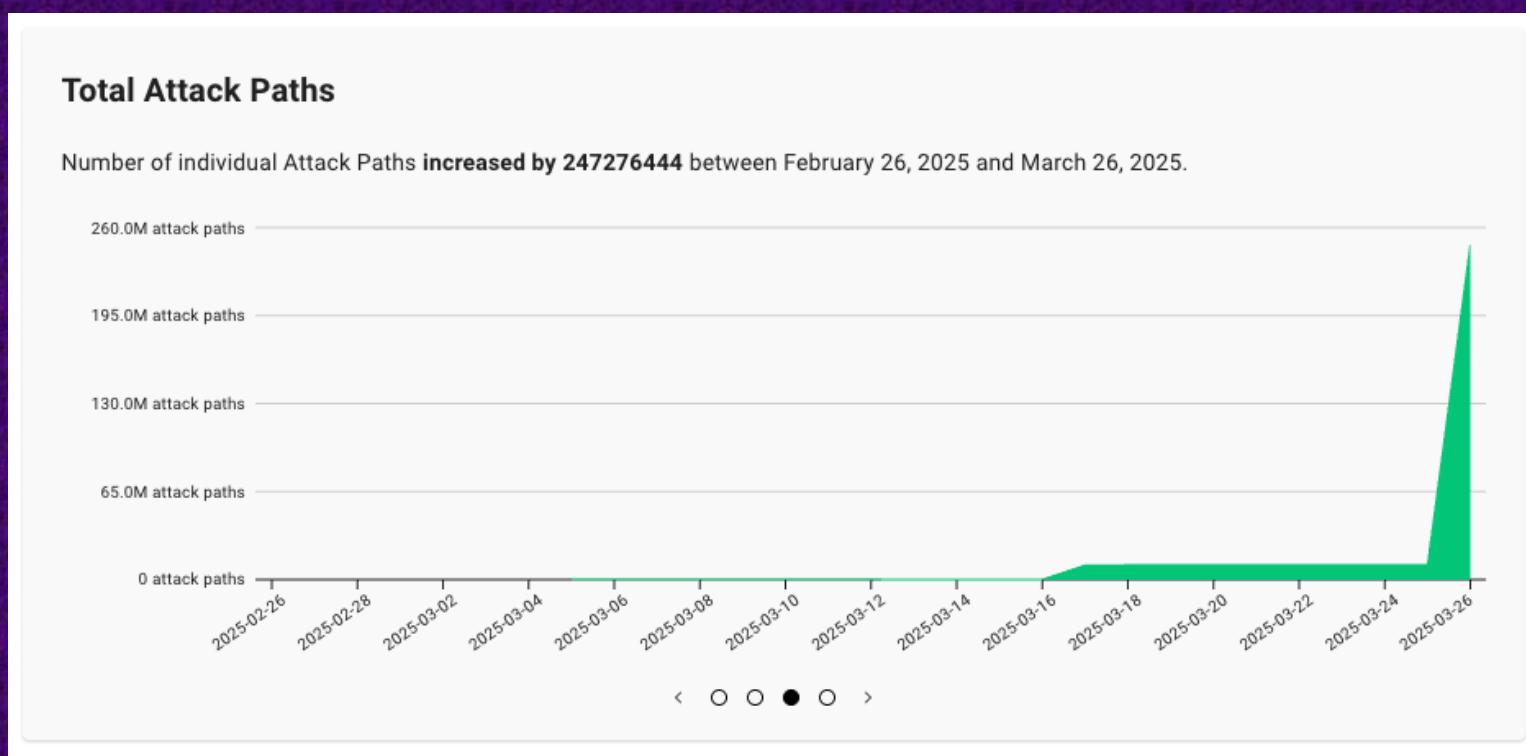
Domain  
Admins



# NTLM In BloodHound



- The average exposure introduced by NTLM Attack Paths is 97%





# NTLM In BloodHound



# Continuous Improvement of the Attack Graph

**CoerceToTGT**

**Relationship Information**

Source Node: AADMIN.TITANCORP.LOCAL  
Target Node: TITANCORP.LOCAL  
Is ACL: FALSE

Last Collected by BloodHound: 2025-03-31 11:01 EDT (GMT-0400)

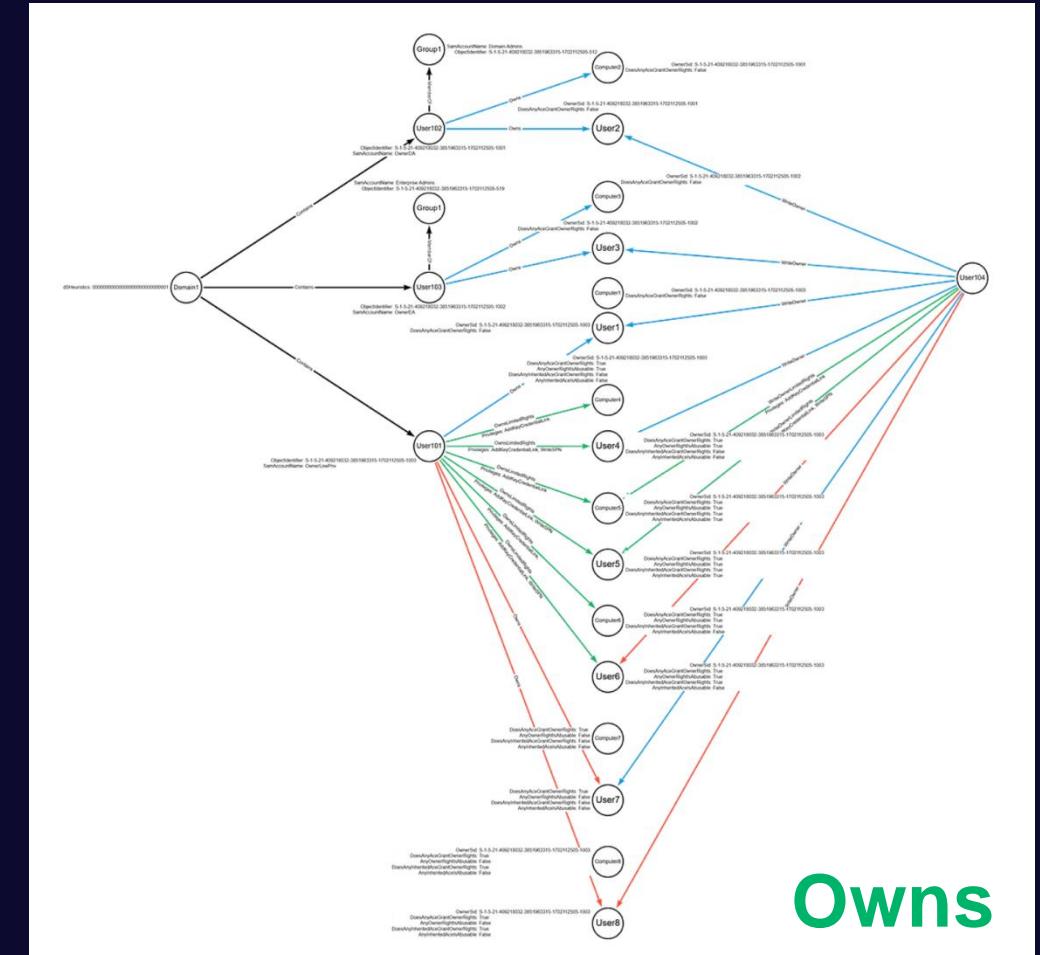
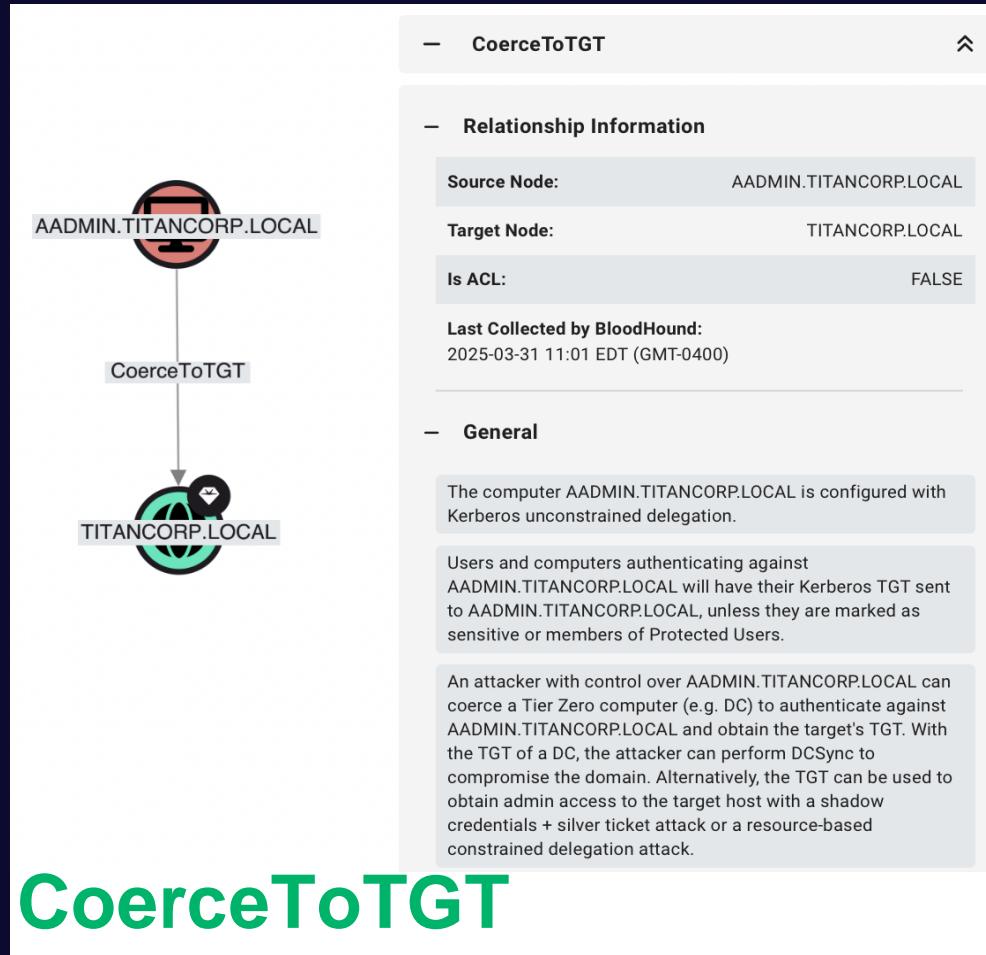
**General**

The computer AADMIN.TITANCORP.LOCAL is configured with Kerberos unconstrained delegation.

Users and computers authenticating against AADMIN.TITANCORP.LOCAL will have their Kerberos TGT sent to AADMIN.TITANCORP.LOCAL, unless they are marked as sensitive or members of Protected Users.

An attacker with control over AADMIN.TITANCORP.LOCAL can coerce a Tier Zero computer (e.g. DC) to authenticate against AADMIN.TITANCORP.LOCAL and obtain the target's TGT. With the TGT of a DC, the attacker can perform DCSync to compromise the domain. Alternatively, the TGT can be used to obtain admin access to the target host with a shadow credentials + silver ticket attack or a resource-based constrained delegation attack.

**CoerceToTGT**



CoerceToTGT: <https://bloodhound.specterops.io/resources/release-notes/2024-12-09-v6-3-0>

Owns: <https://posts.specterops.io/do-you-own-your-permissions-or-do-your-permissions-own-you-c829a91f5e45>

# Community contributions to the Attack Graph – Thanks @q-roland

The image displays a network diagram and a corresponding attack analysis interface. On the left, a graph shows a central node labeled "DUMPSTER.FIRE Tier Zero" with a globe icon and a "99% Exposed" status. Numerous arrows point from various principal nodes (represented by colored circles) towards this central node. The arrows are labeled with specific privilege names: "ADCSync", "WriteGPLink", "GenericAll", "ReadGMSAPassword", "DCSync", "GenericWrite", "AllowedToDelegate", "Owns", "WriteAccountRestrictions", and "ADCSyncA". The principal nodes have counts associated with them: 53 (purple), 4 (yellow), 3 (yellow), 3 (yellow), 3 (yellow), 2 (yellow), 2 (yellow), and 1 (yellow). On the right, a detailed analysis window for the "DUMPSTER.FIRE" object is shown. The top bar indicates the object is "Idle" with its last analysis date as "2024-08-27 10:11 GMT+2 (GMT+0200)". Below this, a section titled "Write GPLink Privileges on Tier Zero Objects" is highlighted in purple, showing 10 findings, 0 changes from the previous month, and a "Critical" severity level. A descriptive text states: "This Attack Path exposes Tier Zero to 53 principals." Further details explain that the "WriteGPLink" privilege allows altering gPLink attributes of organizational units or domain objects, enabling malicious GPO application and child principal command execution. A table below lists 10 findings, all marked as "Accepted". The columns are "Non Tier Zero Principal", "Tier Zero Container", and "First Seen". The findings are:

Non Tier Zero Principal	Tier Zero Container	First Seen
DOMAIN COMPUTERS@DUMPSTER.FIRE	DUMPSTER.FIRE	2024-08-26
DOMAIN COMPUTERS@DUMPSTER.FIRE	SERVICEACCOUNTS@DUMPSTER.FIRE	2024-08-26
DOMAIN COMPUTERS@DUMPSTER.FIRE	USERS@DUMPSTER.FIRE	2024-08-26
DOMAIN COMPUTERS@DUMPSTER.FIRE	TIER1@DUMPSTER.FIRE	2024-08-26
DOMAIN COMPUTERS@DUMPSTER.FIRE	TIER0@DUMPSTER.FIRE	2024-08-26
DOMAIN USERS@DUMPSTER.FIRE	TIER0@DUMPSTER.FIRE	2024-08-26
DOMAIN COMPUTERS@DUMPSTER.FIRE	DOMAIN CONTROLLERS@DUMPSTER.FIRE	2024-08-26

# ATTACK PATHS



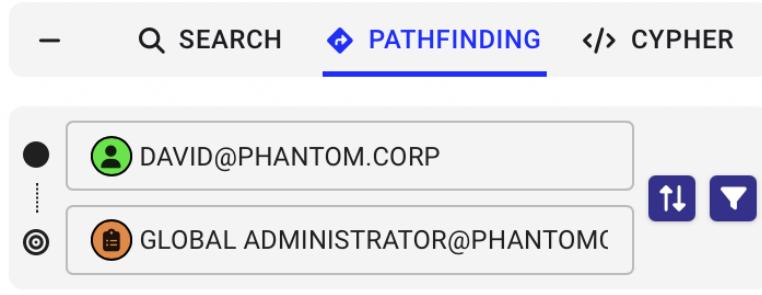
# ATTACK PATHS EVERYWHERE

# ATTACK PATHS



# ATTACK PATHS EVERYWHERE

# Dealing with Scale



Database Agnostic Wrapper for Graphs (DAWGS)

MATCH path = (u:User {name: "DAVID"})-[:HAS\_ROLE|MEMBER\_OF\*1..]->(r:Role {name:...})

SELECT g.name AS group\_name  
FROM Users u  
JOIN Memberships m ON u.id = m.user\_id



# ARE WE GETTING RID OF NEO4J?

- Eventually, yes
- Cypher will be supported on Postgres (cysql)
- We will communicate a deprecation timeline

# So many other enhancements

- Complete rewrite of SharpHound
- Massively sped up AzureHound
- Dark Mode
- Group Management View
- Completely new analysis algorithm
- Integrations: SplunkSOAR, Splunk v2
- Saved Custom Queries
- OIDC support with JIT Users / Roles
- Citrix Direct Access Users Support
- Numerous performance enhancements
- Numerous bugs squashed
- Palt - Toggle labels option
- Palt - Owned object visual representation
- yannis-srl - Fix healthcheck to not use env variable
- Roltere - BP-881: Update README.md ]
- Daniel Underhay - update AZUserAccessAdministrator helptexts
- PJ - Update LinuxAbuse.tsx
- Spyro - Fixed LAPS attributes
- Hoshea - Update WellKnownPrincipal.cs
- q-roland - Write gPLink abuse

*many more to list*

*We're also excited to share...*

# BloodHound Enterprise is now FedRAMP® High Authorized



# What is FedRAMP®?

*Federal security standardization for cloud services*



Standardized US Government program for federal agencies to securely adopt cloud technologies and services



Leverages National Institute of Standards and Technology (NIST) guidelines for uniform security and compliance





# Challenges of FedRAMP®

*Time and resource intensive*

- FedRAMP® Authorization is a **hard requirement** to work with the federal government for cloud hosted tech
- **On average**, zero to authorization takes:
  - **Years** for agency sponsorship, engineering, compliance, accreditation
  - **Millions of dollars** for infrastructure, technical, people, audits
  - **Security and compliance experts**
  - **Many people and teams**
- For **Palantir...**
  - **4.5 years**
  - **700+** security controls implemented
  - **25** different teams
  - **60** full time staff just for authorizations



## BRIEFING ROOM

Office of Management and Budget Releases Draft Federal Strategy For Moving the U.S. Government Towards a Zero Trust Architecture

SEPTEMBER 07, 2021 • PRESS RELEASES

OMB and CISA are requesting public comment on key zero trust strategic and technical guidance to enhance enterprise security across the federal government

Today, the Office of Management and Budget (OMB) released a [draft federal strategy](#) designed to move the U.S. government towards a zero trust architecture. The Cybersecurity and Infrastructure Security Agency (CISA) also released their Cloud Security Technical Reference Architecture and Zero Trust Maturity Model to guide and assist agencies in their implementation planning.

OMB's zero trust strategy complements the Executive Order on Improving the Nation's Cybersecurity

## BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1. Policy.** The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

draft  
e  
d

# Introducing FedStart

*Bring innovation to the government fast*

- Palantir's SaaS offering for cloud companies and startups to get solutions to the government ***fast***
  
- Deploy into Palantir's secure Federal Cloud Services infrastructure to inherit ***~80% of NIST security controls***
  
- Inclusion in Palantir's authorized package means companies are FedRAMP® High Authorized in a ***few months***

The screenshot shows the FedRAMP Marketplace interface. At the top, there is a search bar labeled "Search FedRAMP.gov" and a navigation bar with links for "UPDATES & PRIORITIES", "GET AUTHORIZED", "PARTNERS", "RESOURCES", "MARKETPLACE" (which is highlighted in blue), and "DEV HUB". Below the navigation bar, the title "PALANTIR FEDERAL CLOUD SERVICE – SUPPORTING SERVICES (PFCS-SS)" is displayed. On the left, the Palantir logo is shown. To the right, there is a summary section with the following details:

- Package ID: FR2315464863
- Authorizations: 1
- Reuse: 9

This screenshot shows the detailed view of the Palantir package. It includes sections for "System Profile", "Dependent Products", and "Service Description".

- System Profile:**
  - Service Model: SaaS
  - Deployment Model: Public Cloud
  - Impact Level: High
- Dependent Products:**
  - Palantir Technologies Inc.
  - [Palantir Federal Cloud Service - High](#)

This screenshot shows the "Service Description" section of the package details. It provides a brief overview of the service and its features:

The PFCS-SS is a dedicated environment for the purpose of delivering best-of-breed commercial software to federal government customers as a secure cloud service at the FedRAMP High baseline. The software deployed to PFCS-SS is commercially available software configured to run on PFCS' Kubernetes infrastructure and leverage PFCS' management plane services. This includes:

PFCS-SS Telemetry and Monitoring (PFCS-TM) - an observability and monitoring platform that allows users to visualize, query, and analyze metrics from various data sources through interactive dashboards.

**SpecterOps BloodHound Enterprise** - See your organization from the attacker's view, BloodHound Enterprise is an Attack Path Management solution that continuously maps and quantifies identity Attack Paths in Active Directory and Azure.

# Introducing FedStart

*The first FedStart partner*



Palantir  
→ FedStart



# SpecterOps: Zero to ATO

Getting BHE FedRAMP® High Authorized

1. **Deploy** BHE into Palantir's secure infrastructure (inherit ~80% of NIST controls from Palantir Federal Cloud Services)
2. **Meet compliance requirements** for the remaining ~20% of requisite BHE- and SpecterOps-specific controls
3. **Third party audit** to verify NIST control implementation and test BHE security
4. **FedRAMP® High Authorization** after FedRAMP® PMO reviews successful audit and inclusion in Palantir's FedRAMP High package
5. **Federal agency ATO** of BHE (Palantir-supported government ATO conversations)



Palantir  
↳ FedStart



# SpecterOps: Zero to ATO

*FedRAMP® High in a year*

1. **Deploy** BHE into Palantir's secure infrastructure (inherit ~80% of NIST controls from Palantir Federal Cloud Services)
2. **Meet compliance requirements** for the remaining ~20% of requisite BHE- and SpecterOps-specific controls
3. **Third party audit** to verify NIST control implementation and test BHE security
4. **FedRAMP® High Authorization** after FedRAMP® PMO reviews successful audit and inclusion in Palantir's FedRAMP High package
5. **Federal agency ATO** of BHE (Palantir-supported government ATO conversations)

in 1 year



# FedStart Today: Zero to ATO

*Decreased time to FedRAMP® High*

1. Deploy application into Palantir's secure infrastructure (inherit ~80% of NIST controls from Palantir Federal Cloud Services)
2. Meet compliance requirements for the remaining ~20% of requisite app- and org-specific controls
3. Third party audit to verify NIST control implementation and test application security
4. FedRAMP® High Authorization after FedRAMP® PMO reviews successful audit and inclusion in Palantir's FedRAMP High package
5. Federal agency ATOs (Palantir-supported government ATO conversations)

in less than  
6 months



# FedRAMP® Benefits



Support our Federal Agencies

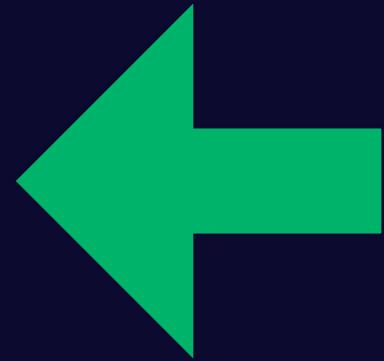


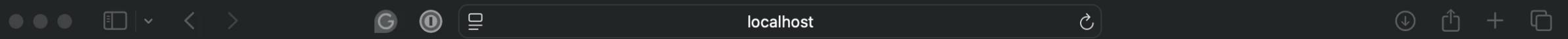
Support enterprise clients with federal data

Learn more: [info@specterops.io](mailto:info@specterops.io) / [specterops.io/industry-public-sector](https://specterops.io/industry-public-sector)

See the Authorization & ATO: <https://marketplace.fedramp.gov/products/FR2315464863>

One more thing...





SEARCH PATHFINDING CYPHER



Search Nodes



localhost



- None Selected



Select a node to view the associated information

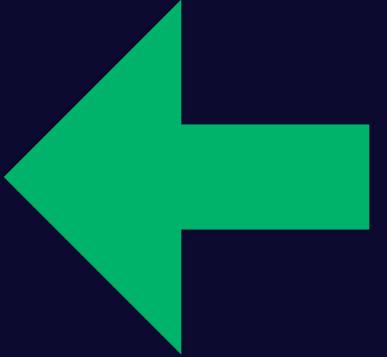


Hide Labels

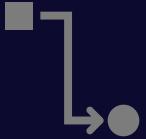
Layout

Export

Search Current Results



I'm sorry it's taken this long



## The Impact of Attack Path Management

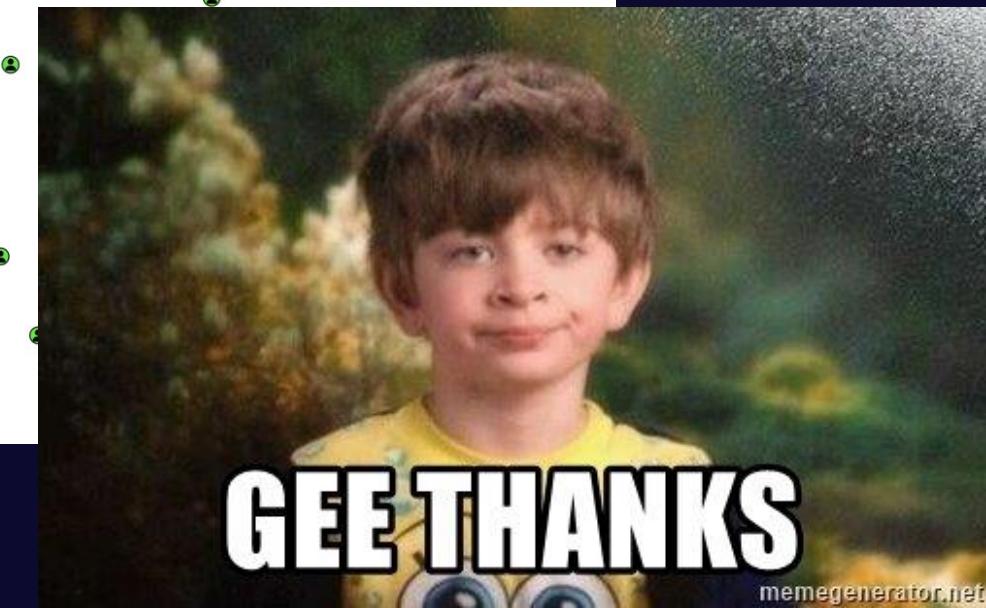
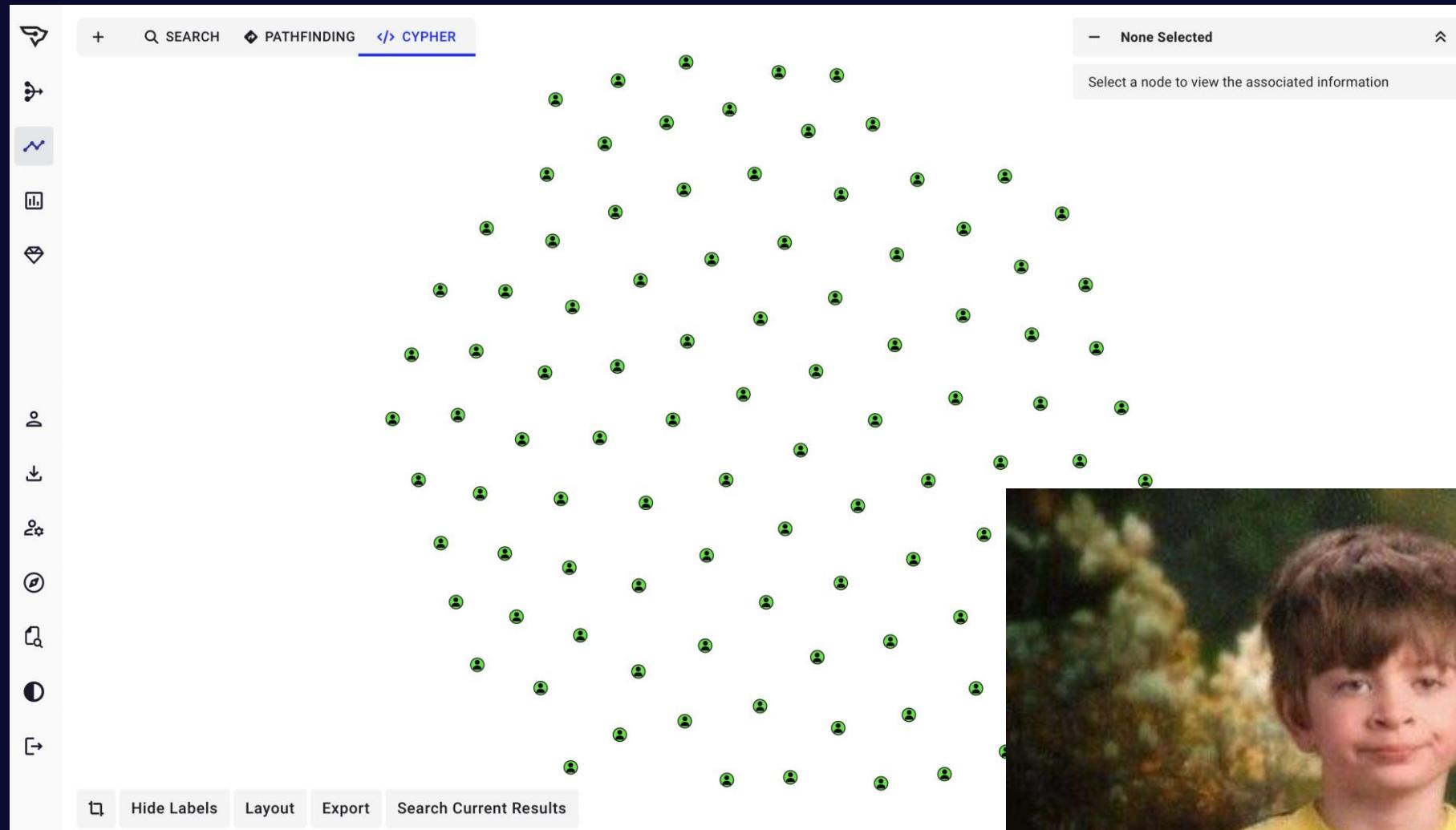


## Development Updates



2025  
Preview

# “Show me all Kerberoastable users”



# “Show me all Kerberoastable users”

Explore ⓘ

Results  
200 results

Search  Manage Columns ✖

Type	Object Name	Object ID	Last Collected	Domain SID	Admin Count	Allows Unconstrained Delegation	Enabled	Created
: 🚩	BIN.DUMPSTER.FIRE	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GMSA_SHS\$@DUM...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GGOOFBALL@TITANC...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	BIN.DUMPSTER.FIRE	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GMSA_SHS\$@DUM...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GGOOFBALL@TITANC...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	BIN.DUMPSTER.FIRE	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GMSA_SHS\$@DUM...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GGOOFBALL@TITANC...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	BIN.DUMPSTER.FIRE	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GMSA_SHS\$@DUM...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	GGOOFBALL@TITANC...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	BIN.DUMPSTER.FIRE	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRUE	2024-07-30 17:53 EDT (GMT-0400)
: 🚩	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FALSE	2024-07-30 17:53 EDT (GMT-0400)

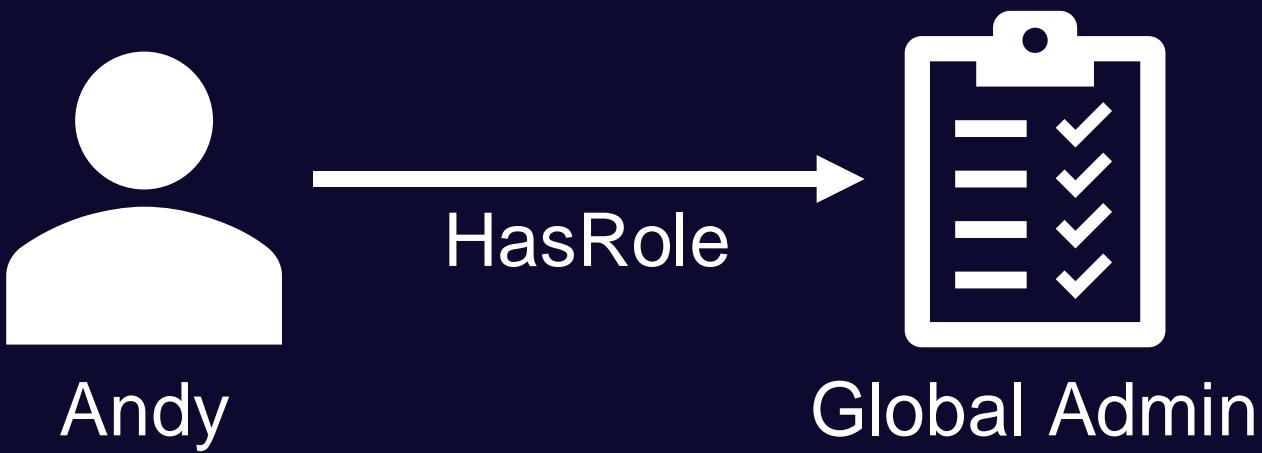


Defenders can think in graphs

*but sometimes interpret results in lists*

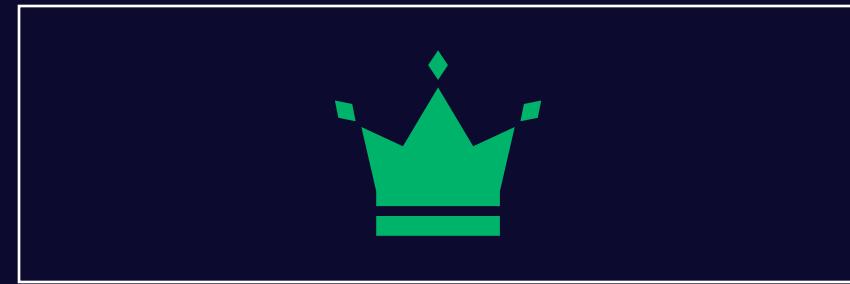


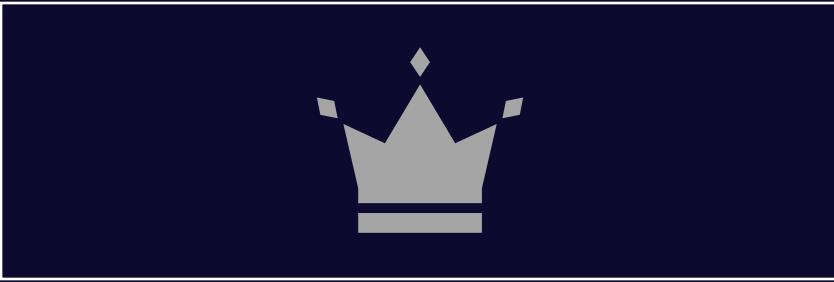
Table View Coming this Summer

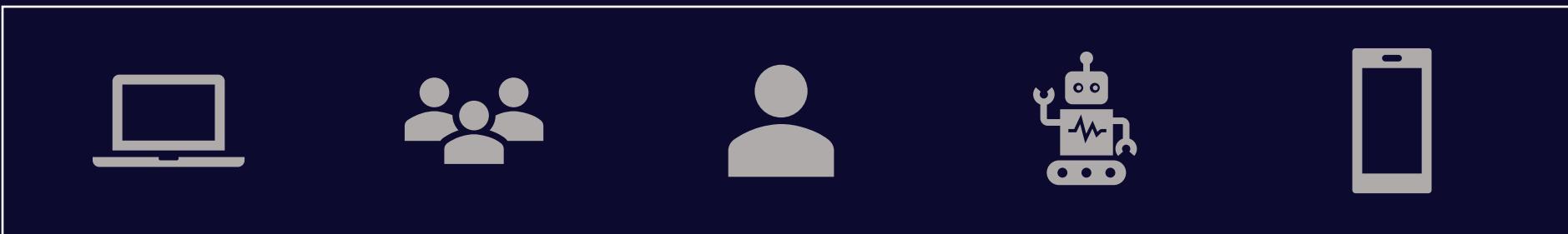
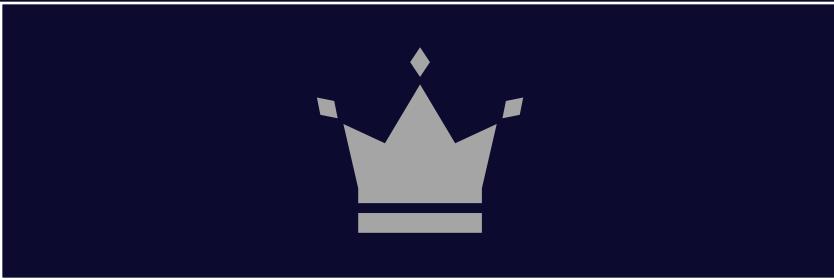


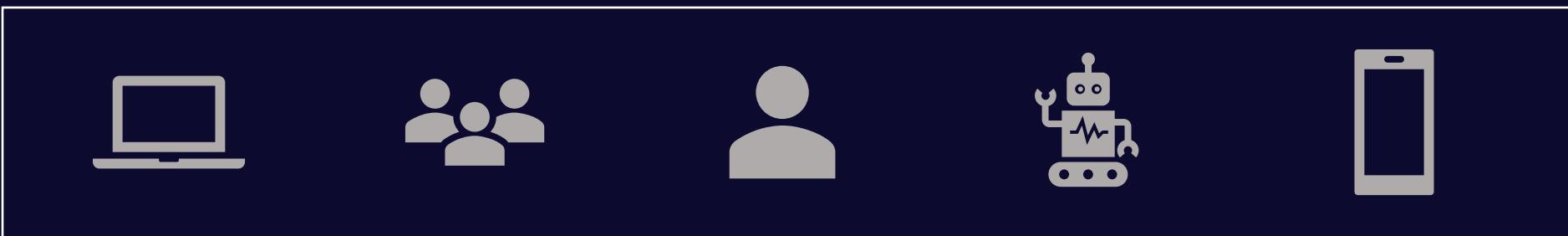
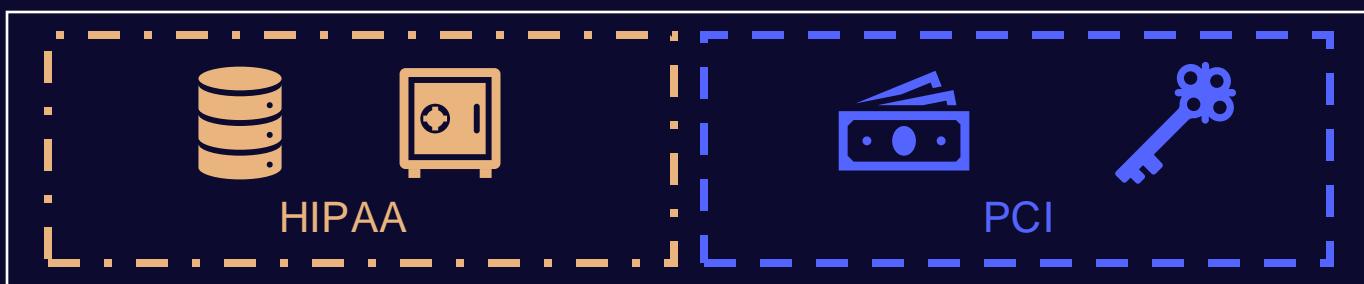
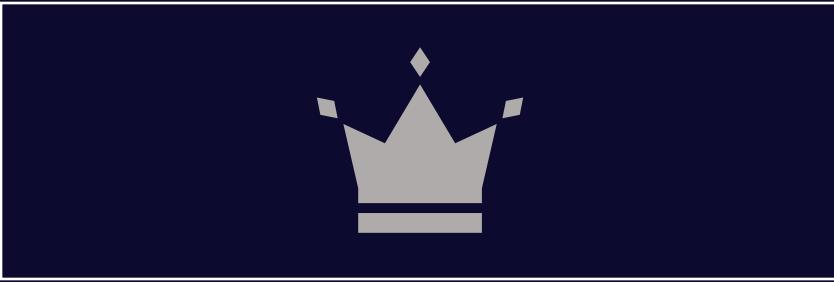


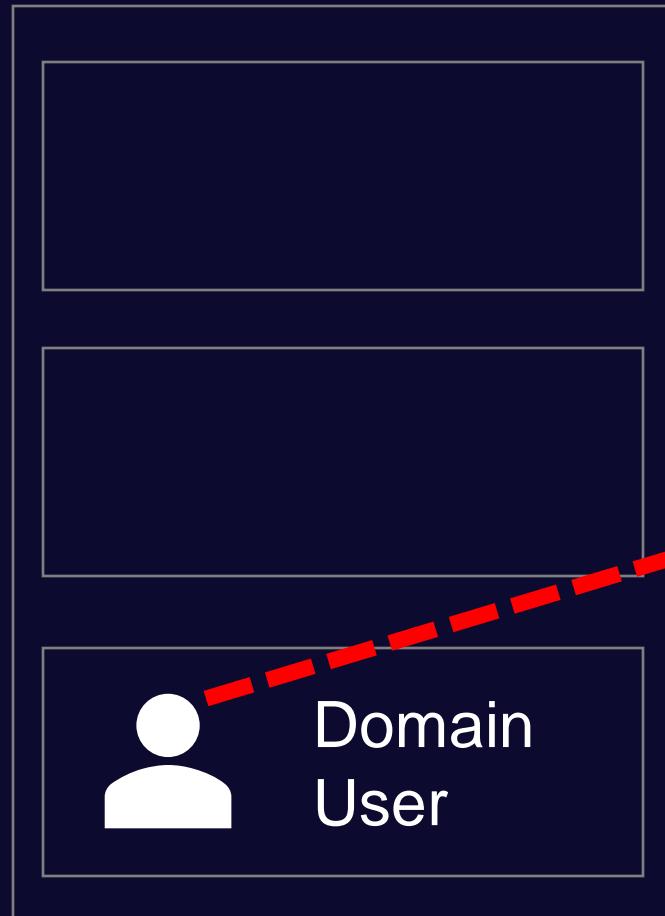
PIM Roles coming this summer



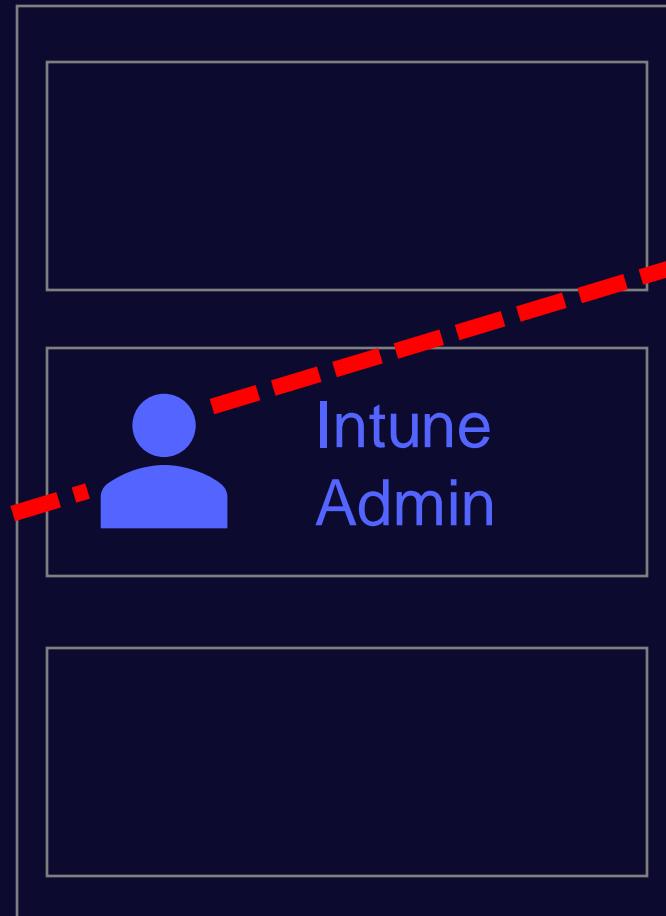




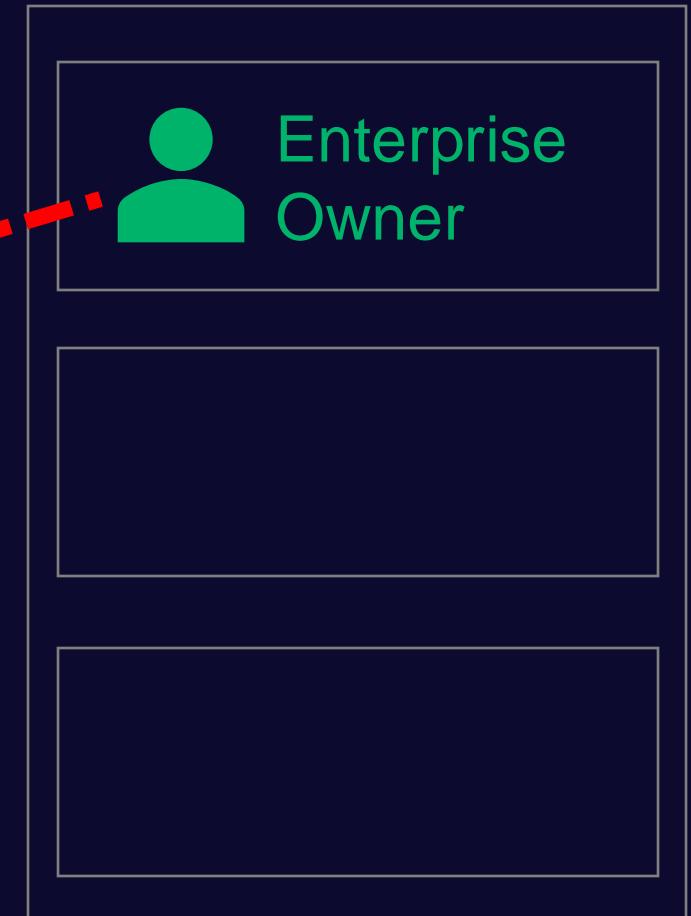




Active Directory



Entra ID



GitHub

**Tier Management**

**Tiers** Labels Certification History

**Create Tier** Summary View

Tier	Selectors	Members	Actions
Tier Zero	4	50	<a href="#">View Details</a> <a href="#">View Certifications</a>
Tier One	2	100	<a href="#">View Details</a> <a href="#">View Certifications</a>
Tier Two	1	1k	<a href="#">View Details</a> <a href="#">View Certifications</a>
Tier Three	1	12k	<a href="#">View Details</a> <a href="#">View Certifications</a>

**Posture**

TESTLAB.LOCAL Tier 1 1 Week 1 Month 3 Months 6 Months 1 Year Custom Range

**Understanding Posture**

Your security posture is created by analyzing the configuration of user groups and session completeness within your environment. Refer to [the documentation](#) to ensure all groups and sessions are accurately established for a comprehensive security overview.

**Attack Paths**

Severity	Name	Category	Findings	Change
Purple	Logons from Tier One Users	Tier Zero	3	-
Purple	Non Tier Zero Principals with DC Sync Privileges	Tier Zero	268	- 68
Purple	Add RBCD Privileges on Tier One Computers	Tier Zero	59	- 10
Purple	Legacy SID History on Tier One Objects	Abusable Kerberos	2	- 8
Red	Force change Password Privileges on Tier One Objects	Least Privilege	1,864	- 100
Red	Non Tier Zero Principals with DC Sync Privileges	Tier Zero	268	-
Orange	Add RBCD Privileges on Tier Zero Computers	Abusable Kerberos	59	- 12
Orange	Legacy SID History on Tier Zero Objects	Abusable Kerberos	2	- 6
Orange	Force change Password Privileges on Tier Zero Objects	Tier Zero	1,864	- 15
Orange	Non Tier Zero Principals with DC Sync Privileges	Least Privilege	268	- 18
Orange	Add RBCD Privileges on Tier Zero Computers	Least Privilege	59	- 1
Orange	Legacy SID History on Tier Zero Objects	Abusable Kerberos	2	-
Cyan	Force change Password Privileges on Tier Zero Objects	Tier Zero	0	- 10

Severity: ● Critical ● High ● Moderate ● Low ● Resolved

**Attack Path Summary**

SpecterOps identified that 100.0% of all users and computers in the TESTLAB.LOCAL domain have at least one viable attack path leading to the compromise of a Tier One principal and thus absolute control of the entire Active Directory environment.

**Findings** 20K - 10 vs last month

**Attack Paths** 8.9M - 10 vs last week

**Tier One Objects** 500 - 10 vs last month

**Historical Findings**

Number of Findings decreased by 10 between date 1 and date 2.

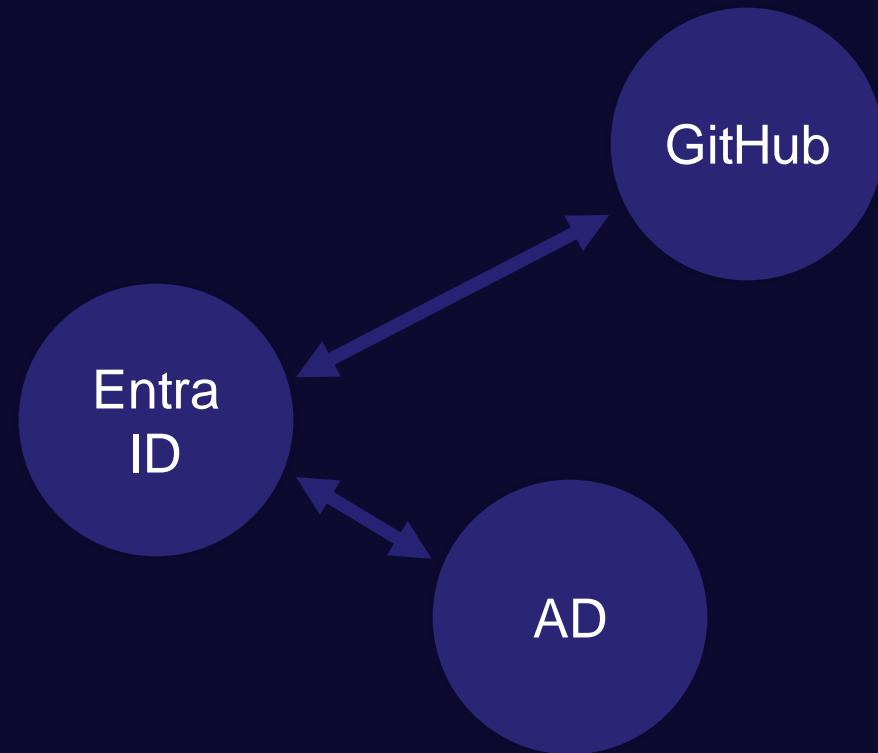
**Group Completeness** 50%

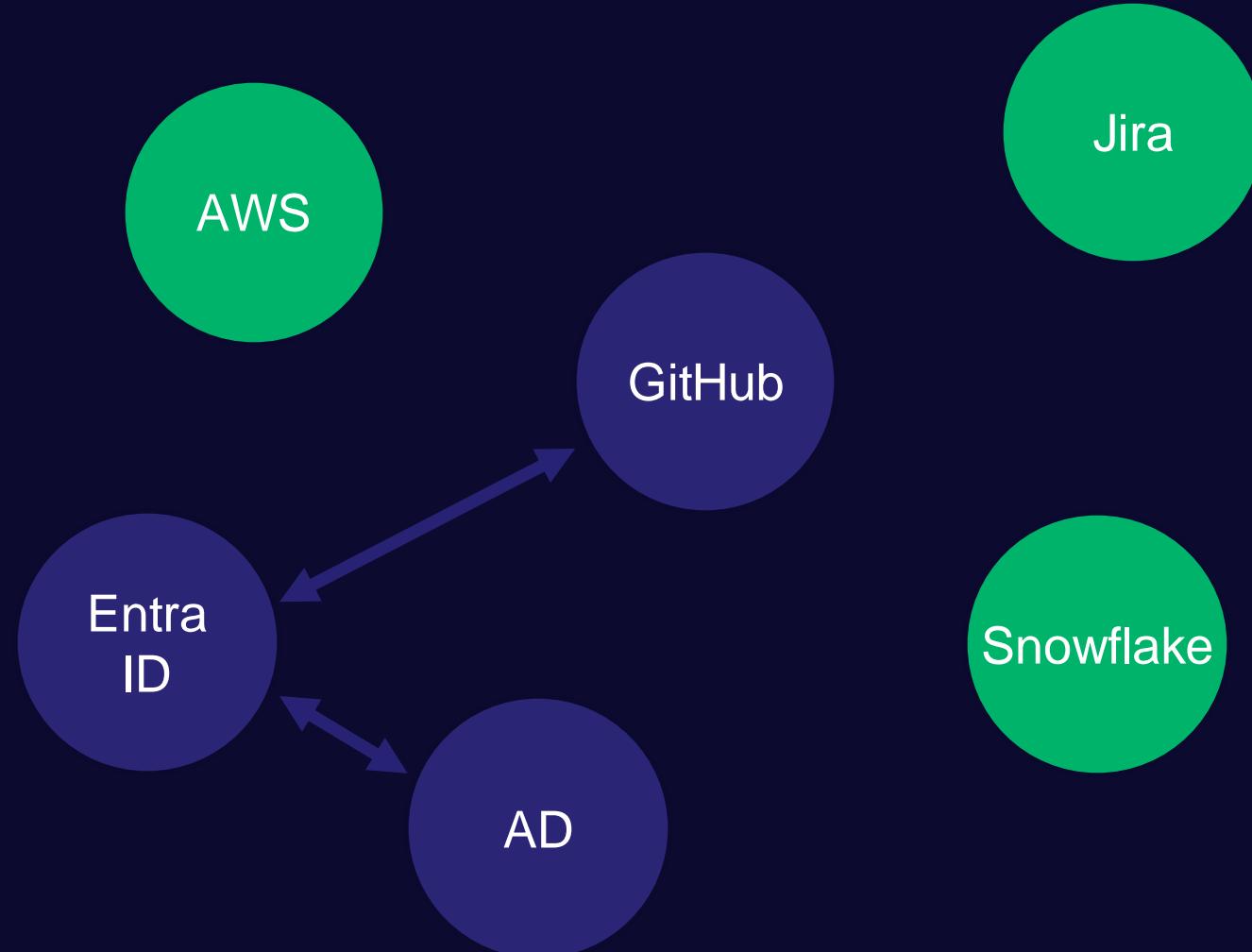
**Session Completeness** 60%

# Multi-Tier Management and Analysis

## Coming this Summer

But when are you going to \_\_\_\_\_?







Salesforce

GCP

Ping

Entra  
ID

AWS

AD

GitHub

Snowflake

Workday

Jira

Okta

BloodHound is where Attack Path research is done

BloodHound is where [AD] Attack Path research is done

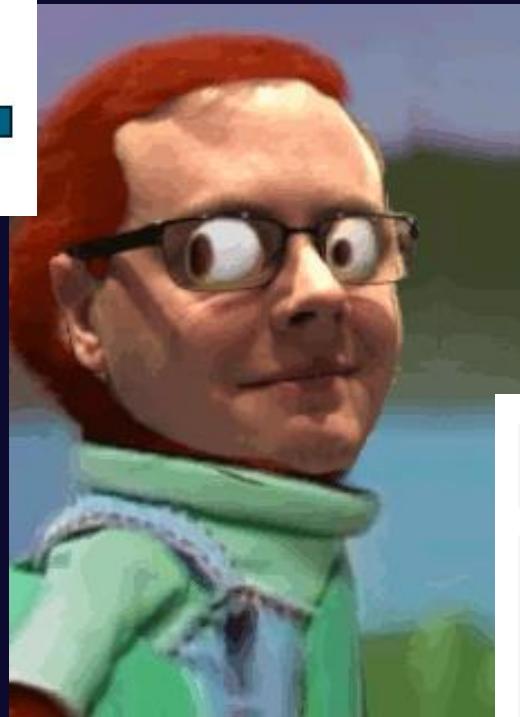
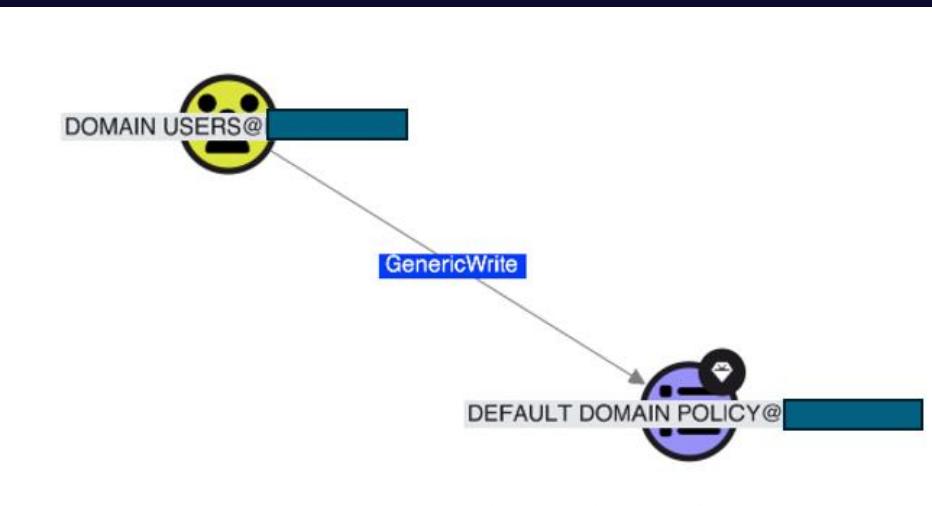
BloodHound is where [Azure] Attack Path research is done

BloodHound is where [GitHub] Attack Path research is done

BloodHound is where [AWS] Attack Path research is done

BloodHound is where [Okta] Attack Path research is done

BloodHound is where **[All]** Attack Path research is done



Meanwhile.....  
we still have a lot to fix

A screenshot of a user profile interface. At the top, there is a minus sign, a user icon, and the text 'HELPDESK ADMINISTRATOR@...' followed by a red rectangular box covering the end of the email address. To the right of the box is an upward-pointing arrow. Below this, there are two expandable sections: '+ Object Information' and '+ Active Assignments'. To the right of '+ Active Assignments' is a grey box containing the number '25,034'.



# Questions

Justin Kohler, Chief Product Officer

