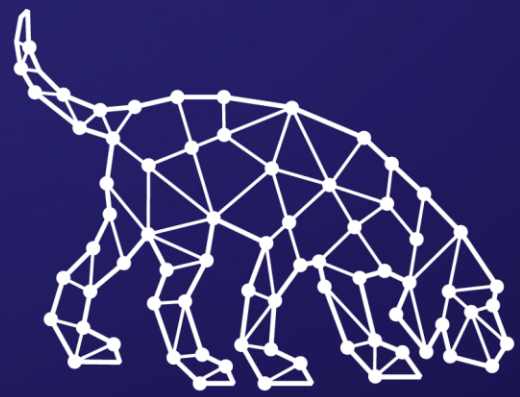
SPECTEROPS

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-manage...

What is Attack Path Management?

Attack path management (APM) is a process y
security weaknesses as seen through the eyes o
Tenable
world **attacks**, but they do so

NCC Group
https://www.nccgroup.com › is-attack-path-mapping-part...

Is Attack Path Mapping Part of Your Cyber S

Feb 15, 2024 — Continuous testing collaboration and evolution
methods. The best form of defence is to know the types of **attac**

Dark Reading
https://www.darkreading.com › exposure-management-l...

Exposure Management Looks to Attack Paths, Identity ...

Jul 7, 2023 — "With **attack path** analysis, organizations can understand how **atta**
chained, how a vulnerability in an asset might relate to a certain ...

jumpsec
https://www.jumpsec.com › attack-path-mapping

Attack Path Mapping

If you can understand potential **attack paths** you can build str
enables you to cut off these **attack** pa

XM Cyber
https://xmcyber.com › attack-path-management

Attack Path Management

Give teams an intuitive platform for discovering, understandin

BloodHound Enterprise
https://bloodhoundenterprise.io › what-is-attack-path-ma...

What is Attack Path Management?

Microsoft Research published a paper in 2009 describing **Attack Paths** as "Identity sno
attacks [that] leverage the users logged in to a first compromised ...
Why Active Directory Is The... · Why Attack Paths Are... · What Is Attack Path...

Proofpoint
https://www.proofpoint.com › identity-threat-defense › i...

Importance of Continuous Attack Path

Nov 8, 2023 — **Attack path management**. This refers to the process of identifying, analyz
understanding and remediating attack paths within a business.
Key Terms · Data Exfiltration · Why An Attack Path...

Tarlogic
https://www.tarlogic.com › Cyb

Attack Path Manageme

May 10, 2023 — In short, **Attack**
ransomware attacks against com

traxion.com
https://www.traxion.com › ... › Offensive Security Services

Attack Path Management - Traxion

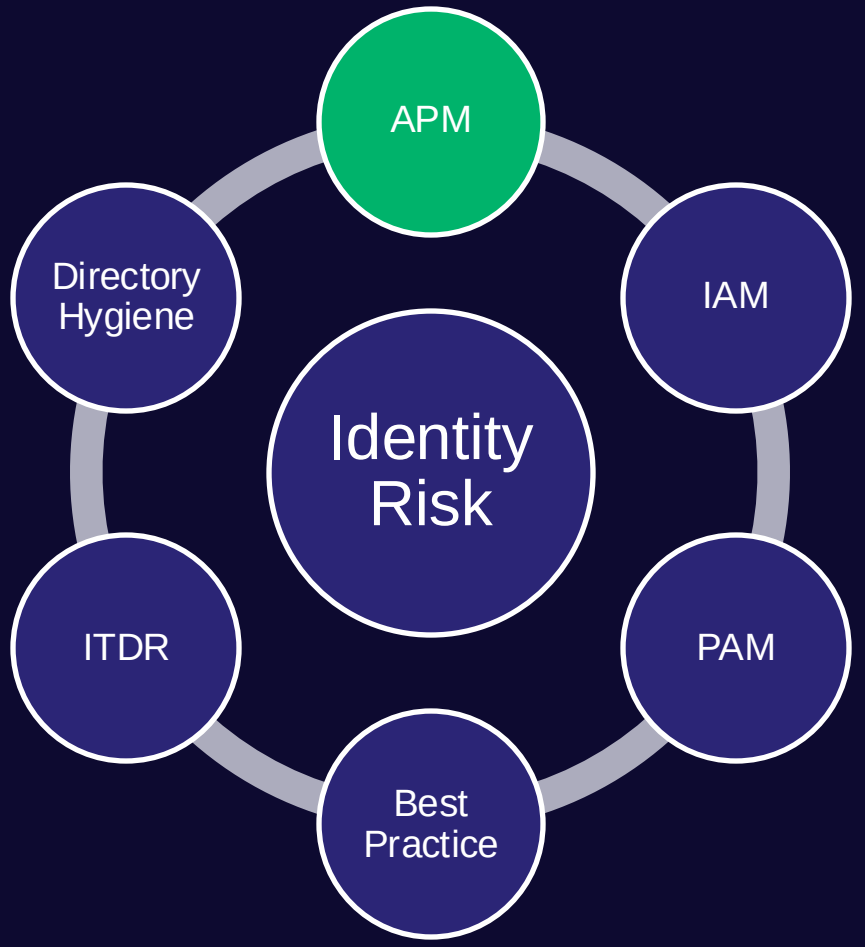
With **Attack Path Management** services from Traxion, y
network through the eyes of an attacker and simulate po

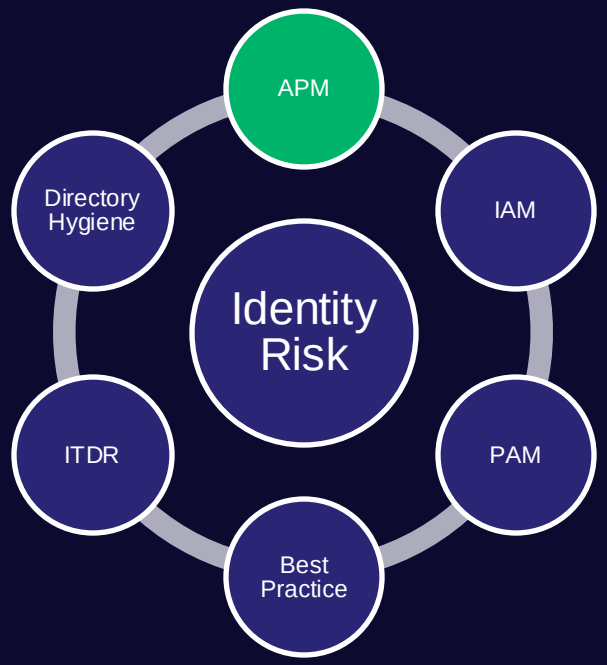
TechTarget
https://www.techtarget.com › searchsecurity › tip › Close

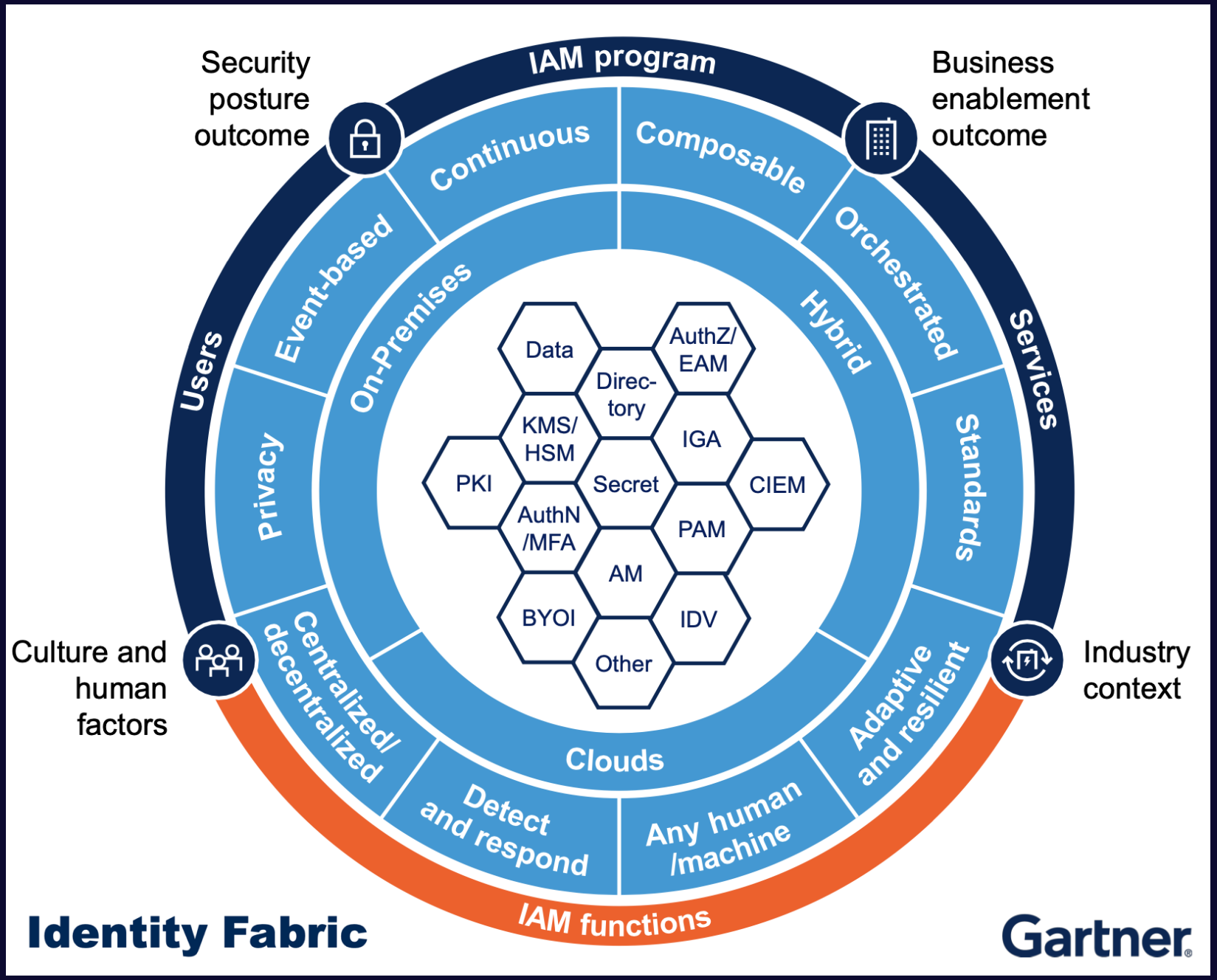
Close security gaps with attack path a

Feb 6, 2024 — Penetration testing and red team exerc
world **attacks**, but they do so one **attack** vector at a ti

APM is the missing capability in Identity Risk




APM
Directory Hygiene
IAM
Identity Risk
ITDR
PAM
Best Practice


IAM program
Security posture outcome
Business enablement outcome
Users
Services
Continuous
Composable
Event-based
Orchestrated
On-Premises
Hybrid
Privacy
Standards
Data
Direc-tory
AuthZ/ EAM
KMS/ HSM
IGA
PKI
Secret
CIEM
AuthN /MFA
PAM
AM
BYOI
IDV
Other
Culture and human factors
Industry context
Centralized/ decentralized
Clouds
Adaptive and resilient
Detect and respond
Any human /machine
IAM functions
Identity Fabric
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 the cycle of accessing critical assets.

CrowdStrike
https://go.crowdstrike.com › identity › protection

CrowdStrike Identity - Secure Identities Faster

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

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 ...

Grip Security
https://www.grip.security › glossary › id

What is Identity Security and

Identity security is a critical part of m
managing user identities across all syste

Ping Identity
https://www.pingidentity.com › ...

Ping Identity: Identity Security

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

Veza
https://www.veza.com

Future of Identity Security | Veza Identity Security

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

BeyondTrust
https://www.beyondtrust.com › Resources › Glossary

Identity Security

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

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 ...

Delinea
https://delinea.com › Glossary

What is Identity Security?

Identity security **protects the digital identities of hu** interact with data, applications, and infrastructure.
How Do Identities Typically... · Here Are Some Comm

Duo Security
https://duo.com › Resources › Info

What is Identity Security?

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

Saviynt
https://www.saviynt.com

Leader in Identity Security

Secure Identity Management — Saviynt Hel 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.”

Gartner

Source: Gartner - Demystifying the Hype: Identity Security, Posture Management, Threat Detection and Response - Felix Gaehtgens

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.

Gartner

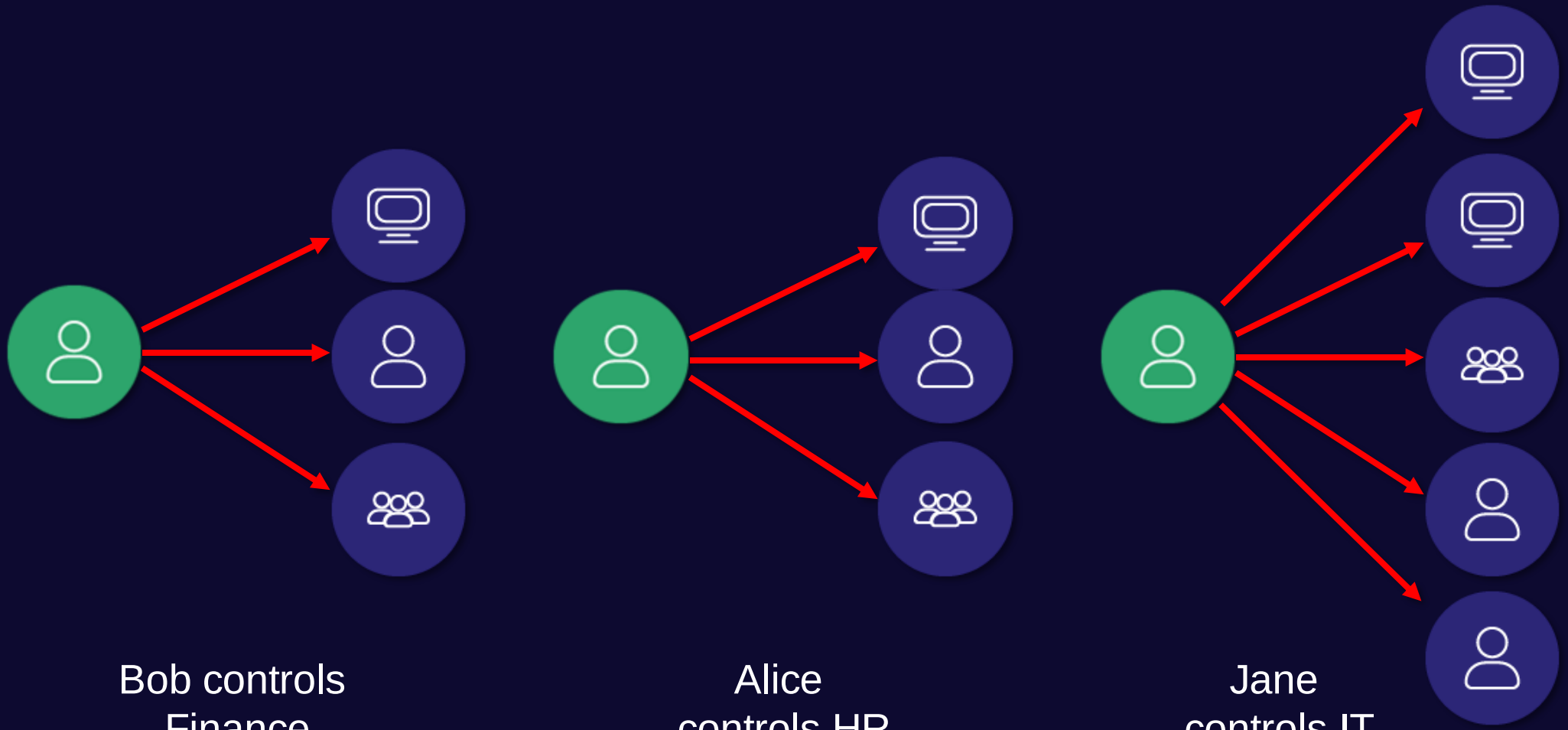
Source: Gartner - Demystifying the Hype: Identity Security, Posture Management, Threat Detection and Response - Felix Gaehtgens

Attack Paths are **how** we attack identities

Attack Paths are how we attack [human] identities

Attack Paths are how we attack [machine] identities

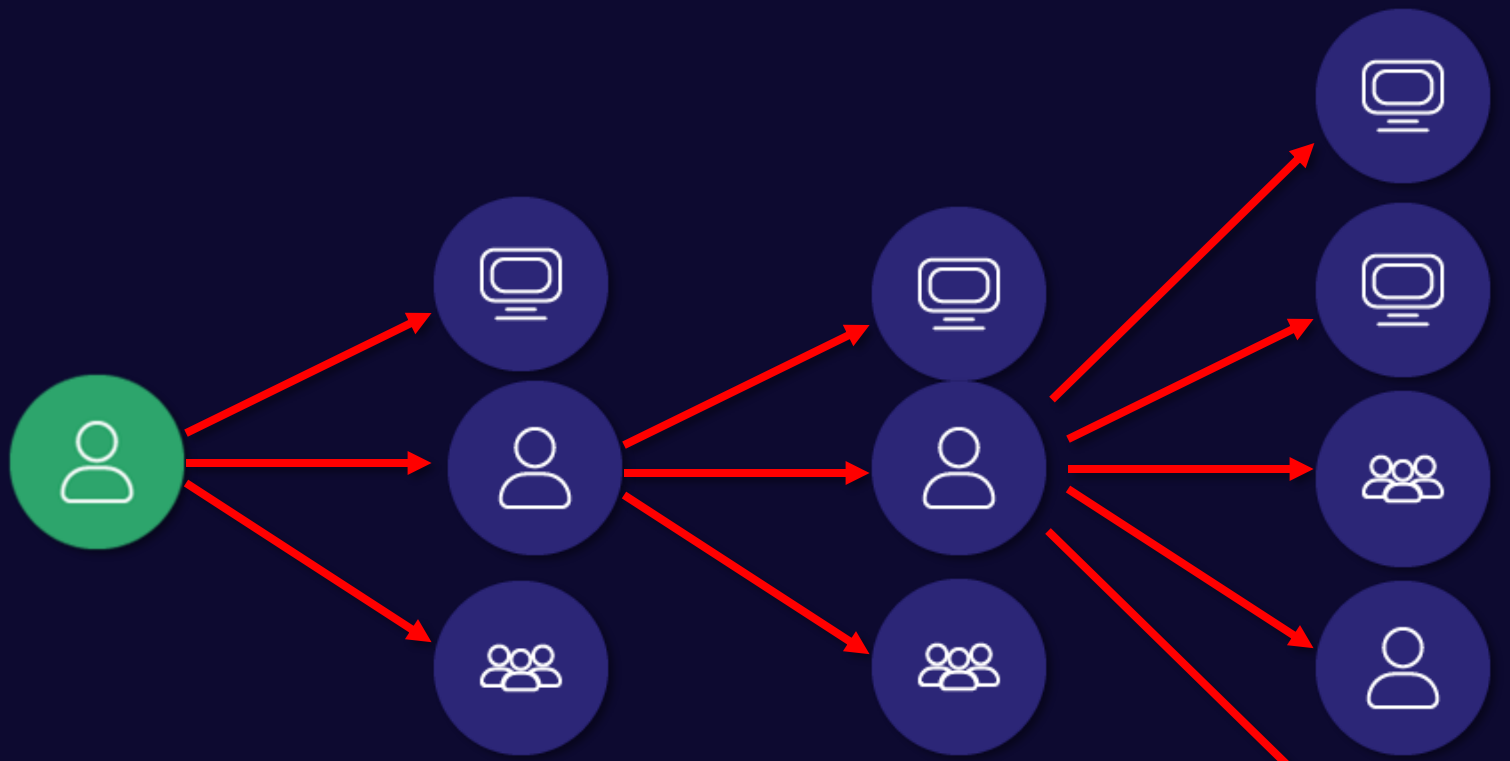
Attack Paths are how we attack **[all]** identities to compromise resources and disrupt business-critical operations



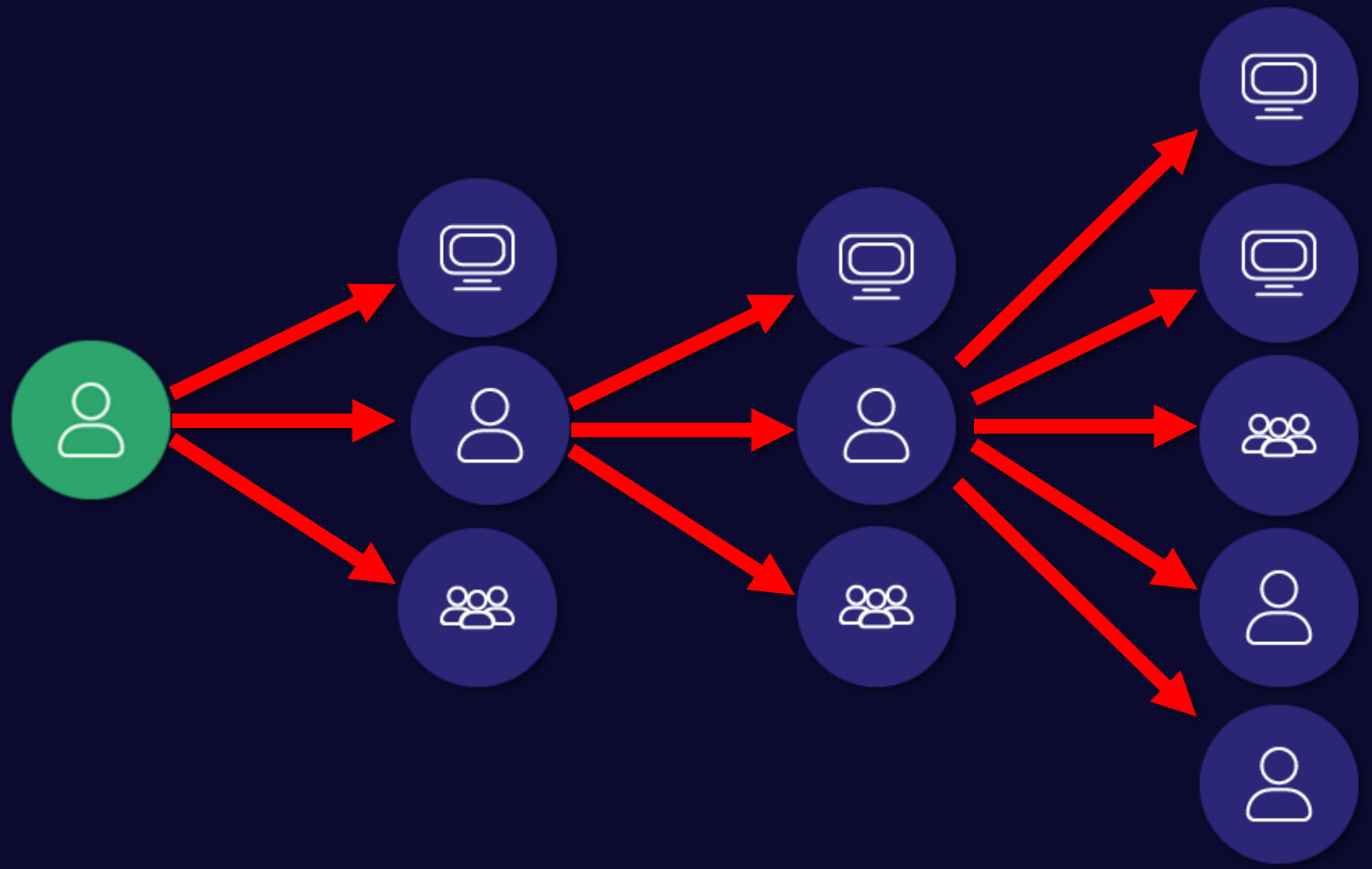
Bob controls Finance

Alice controls HR

Jane controls IT



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 visi[illegible] reduce risk from disco[illegible] complex ps/infrastructure.
- Detect and manage unknown privilege.
- Analyze complex relationships across IAM data to reduce the attack surface.
- Implement the principle of least privilege.

Gartner

Source: Gartner - Demystifying the Hype: Identity Security, Posture Management, Threat Detection and Response - Felix Gaehtgens

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

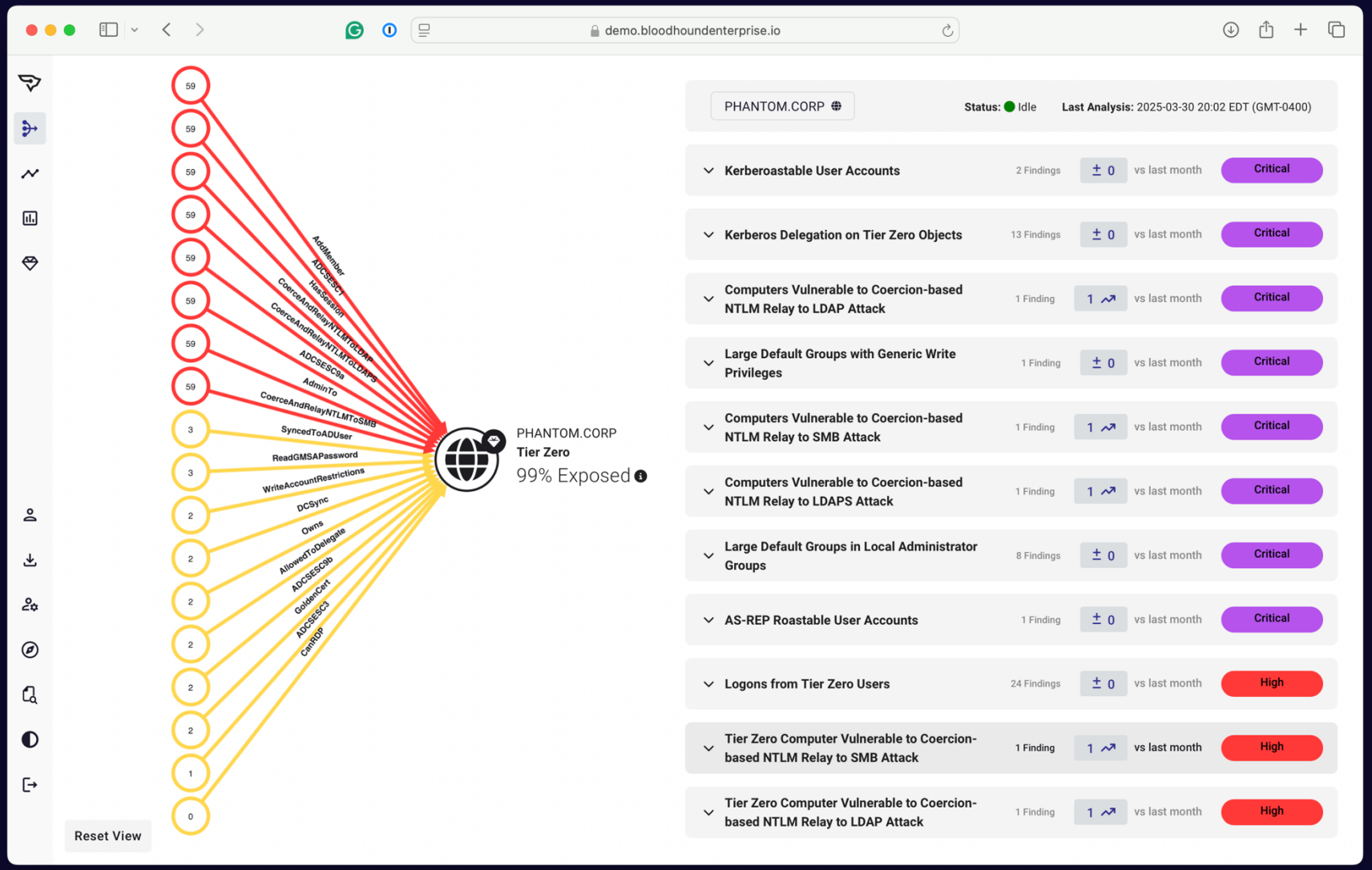
Source: Gartner - Demystifying the Hype: Identity Security, Posture Management, Threat Detection and Response - Felix Gaehtgens

Attack path management

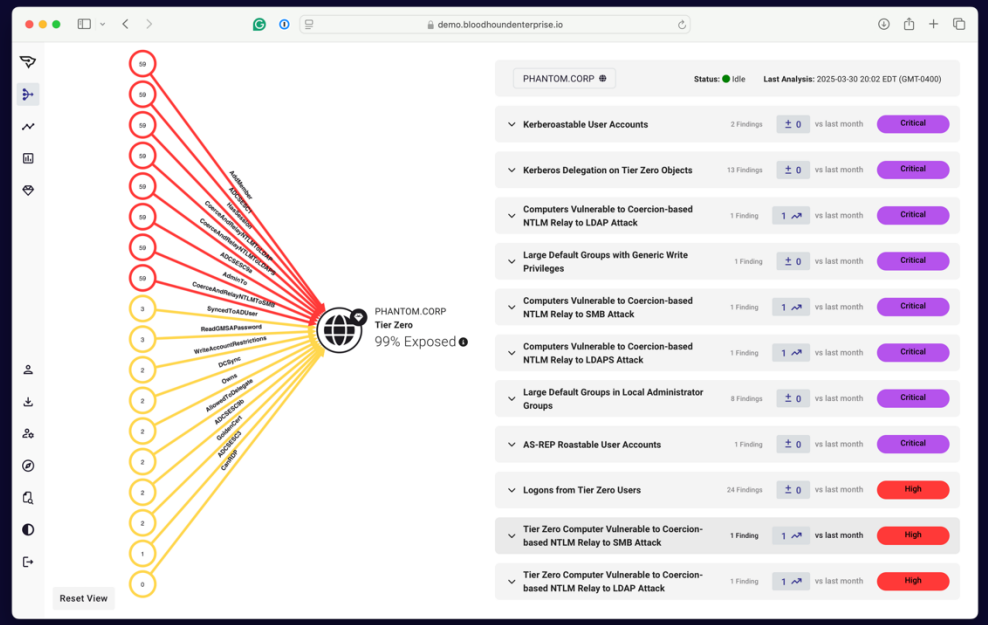
Organizations should identify the most likely attack paths leading to critical assets and continuously mitigate them. An attack path calculation incorporates things such as asset inventories, vulnerability/weakness data, and external attack surfaces to construct a possible attack chain leading to a critical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

Source: Gartner - Demystifying the Hype: Identity Security, Posture Management, Threat Detection and Response - Felix Gaehtgens

Operationalizing APM



Operationalizing APM

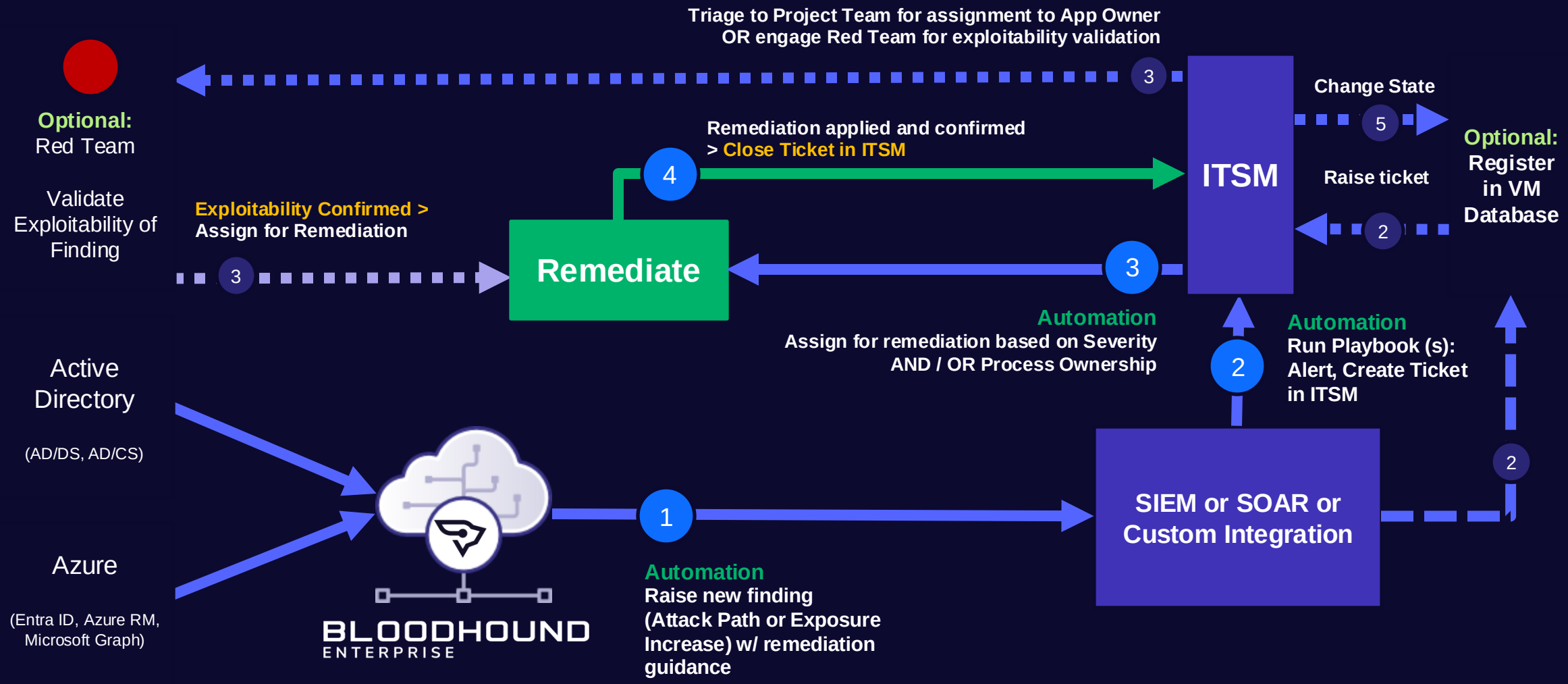


splunk>

Microsoft Sentinel

CORTEX XSOAR
BY PALO ALTO NETWORKS

Operationalizing APM



Attack Path Management is effective

2M Identities

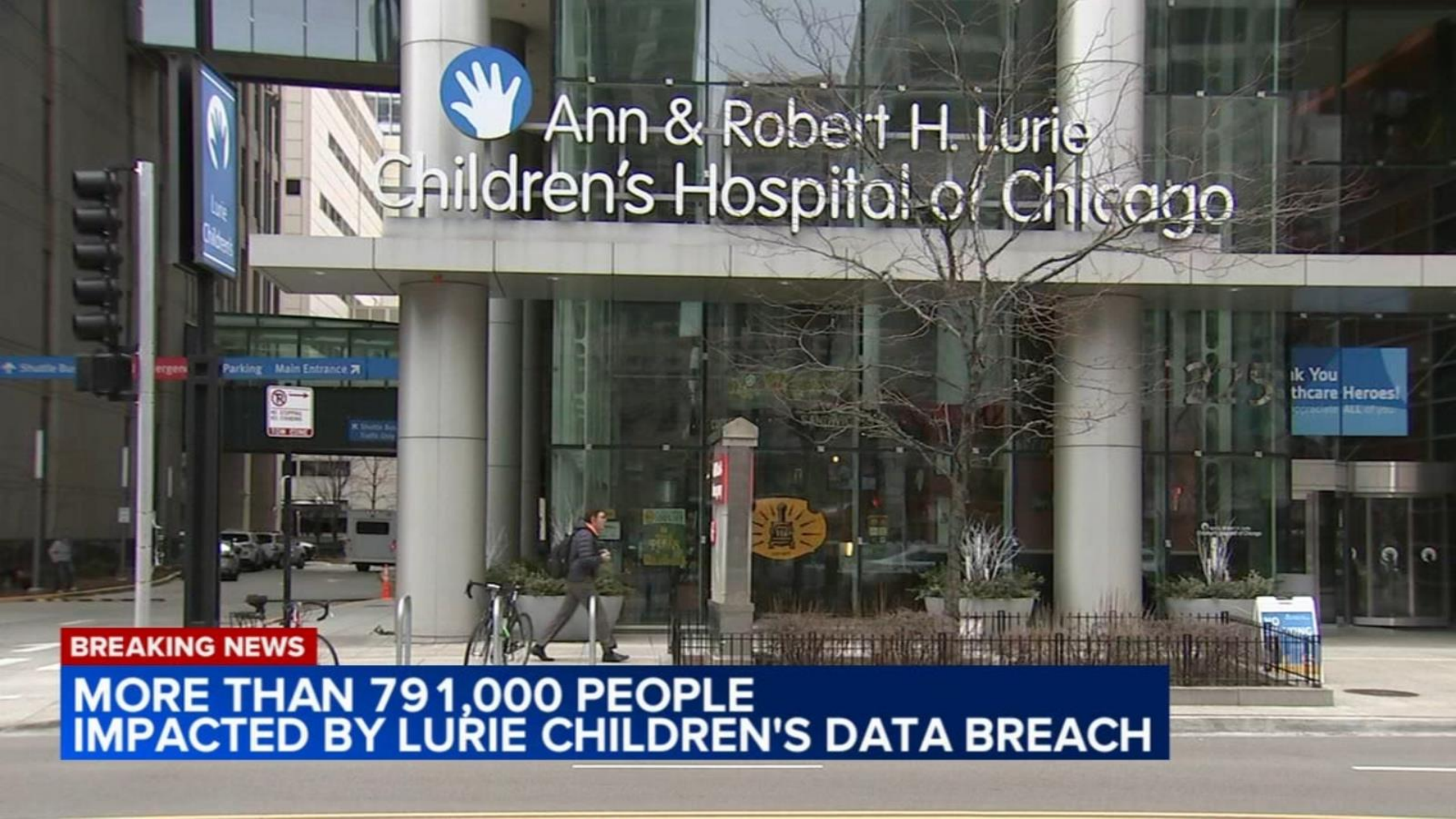
54% reduction in 6 months

50 Domains

T0 paths gone in 6 months

4M Identities

90% reduction in 18 months

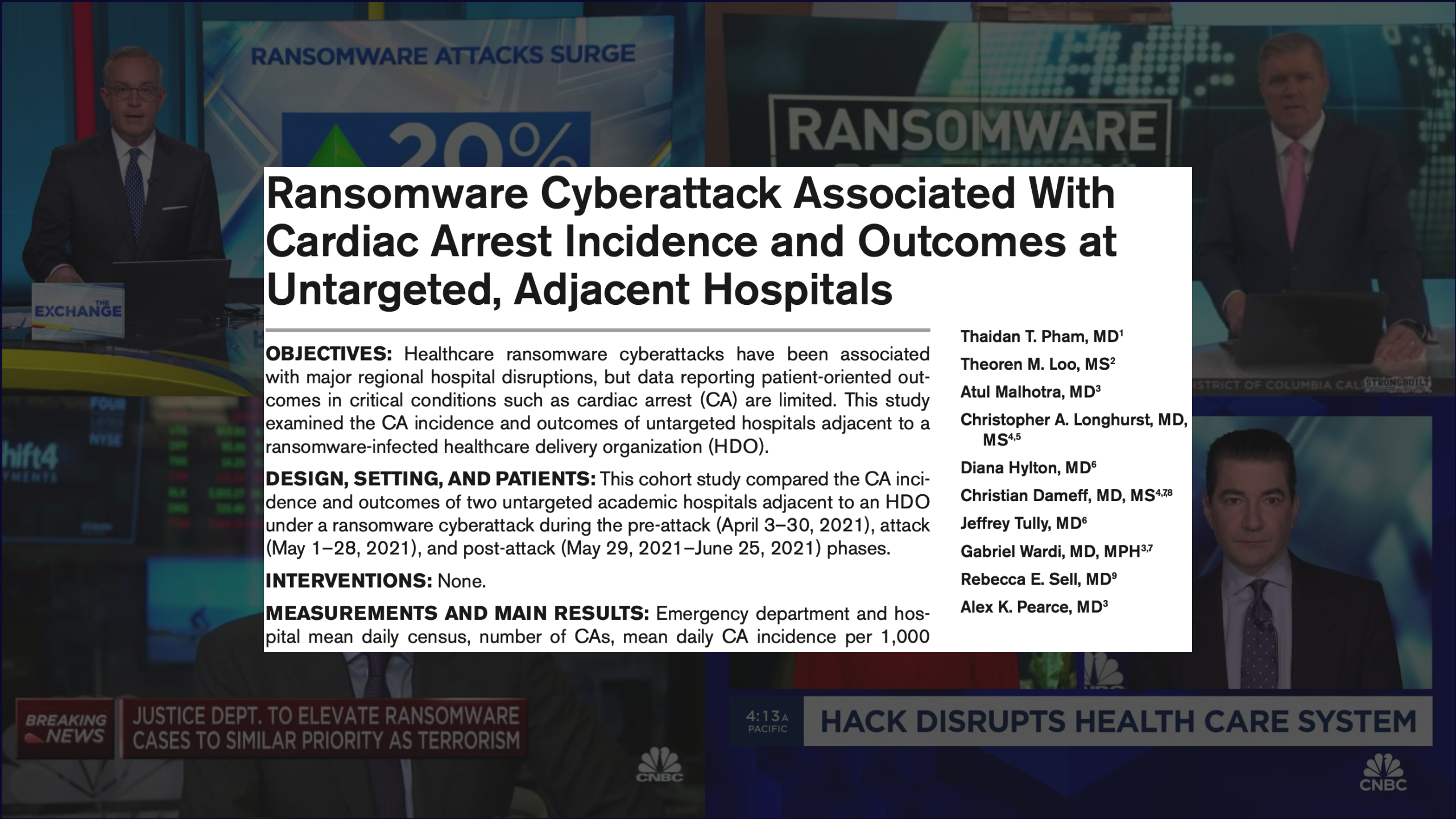

Ann & Robert H. Lurie
Children's Hospital of Chicago
Parking
Main Entrance
BREAKING NEWS
MORE THAN 791,000 PEOPLE
IMPACTED BY LURIE CHILDREN'S DATA BREACH


RANSOMWARE ATTACKS SURGE
20%
YEAR-OVER-YEAR
SOURCE: CHECKPOINT SOFTWARE
THE EXCHANGE
CNBC


RANSOMWARE ATTACK
NEWS 4 TUCSON
10:00 | 69°
ATTORNEY GENERAL KRIS MAYES HAS TEAMED UP WITH 17 STATES AND THE DISTRICT OF COLUMBIA CAL
STRONGBUILT


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


4:13A PACIFIC
HACK DISRUPTS HEALTH CARE SYSTEM
CNBC



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

Thaidan T. Pham, MD[1]

Theoren M. Loo, MS[2]

Atul Malhotra, MD[3]

Christopher A. Longhurst, MD, MS[4,5]

Diana Hylton, MD[6]

Christian Dameff, MD, MS[4,7,8]

Jeffrey Tully, MD[6]

Gabriel Wardi, MD, MPH[3,7]

Rebecca E. Sell, MD[9]

Alex K. Pearce, MD[3]

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.

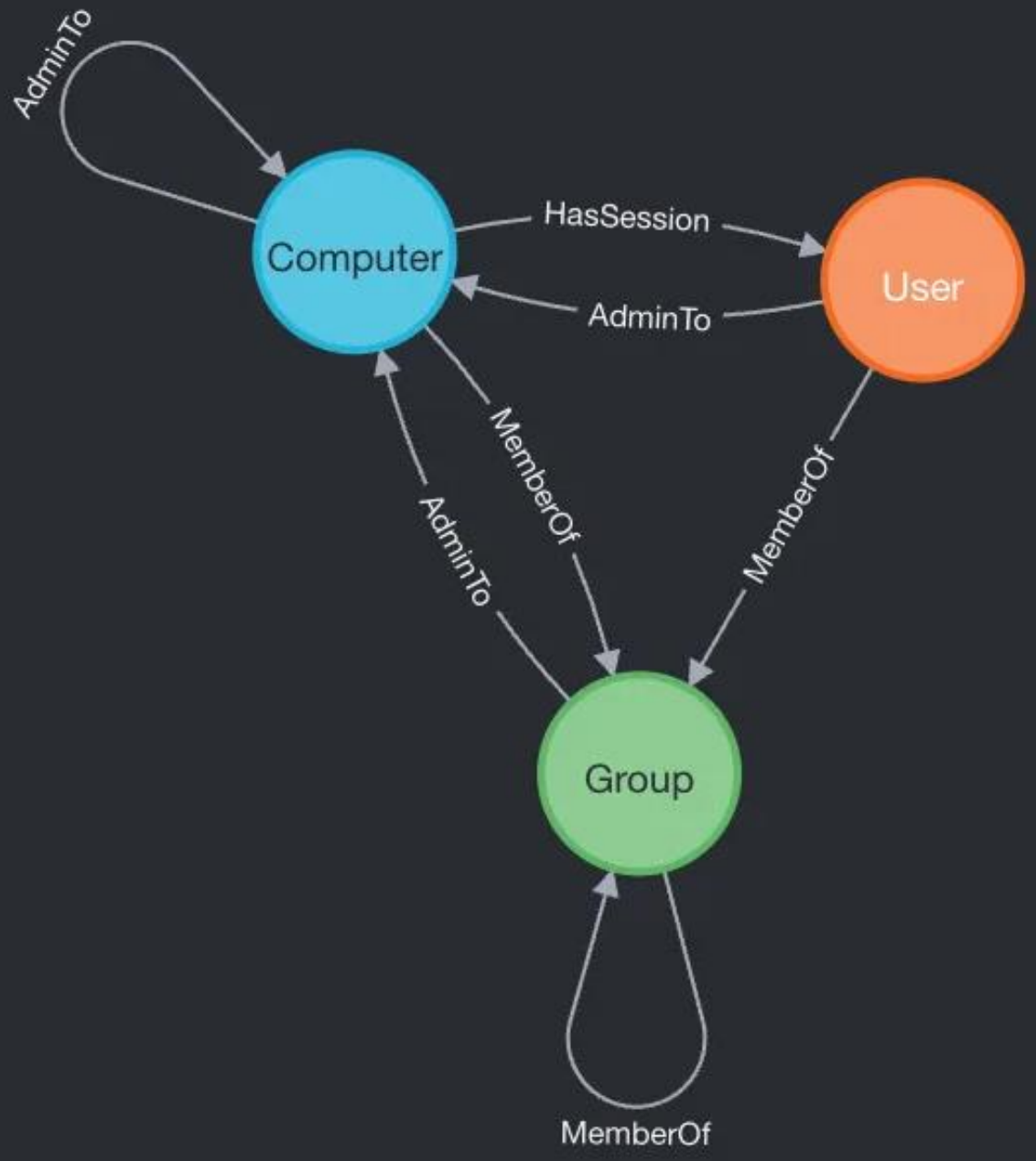
INTERVENTIONS: None.

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

The Impact of Attack Path Management

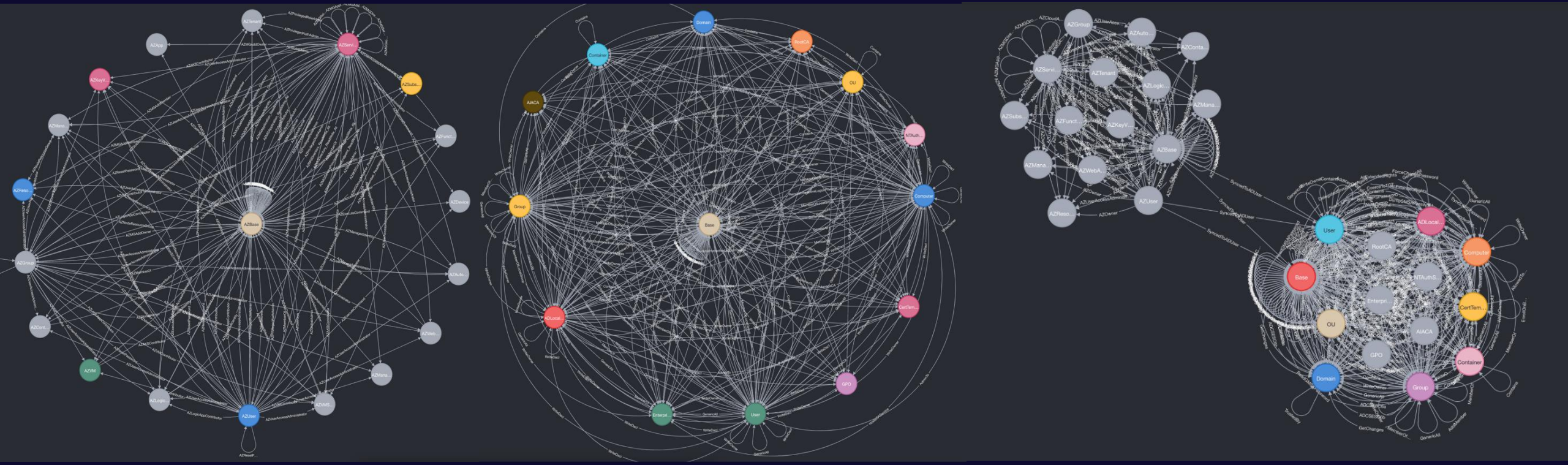
Development Updates

2025 Preview

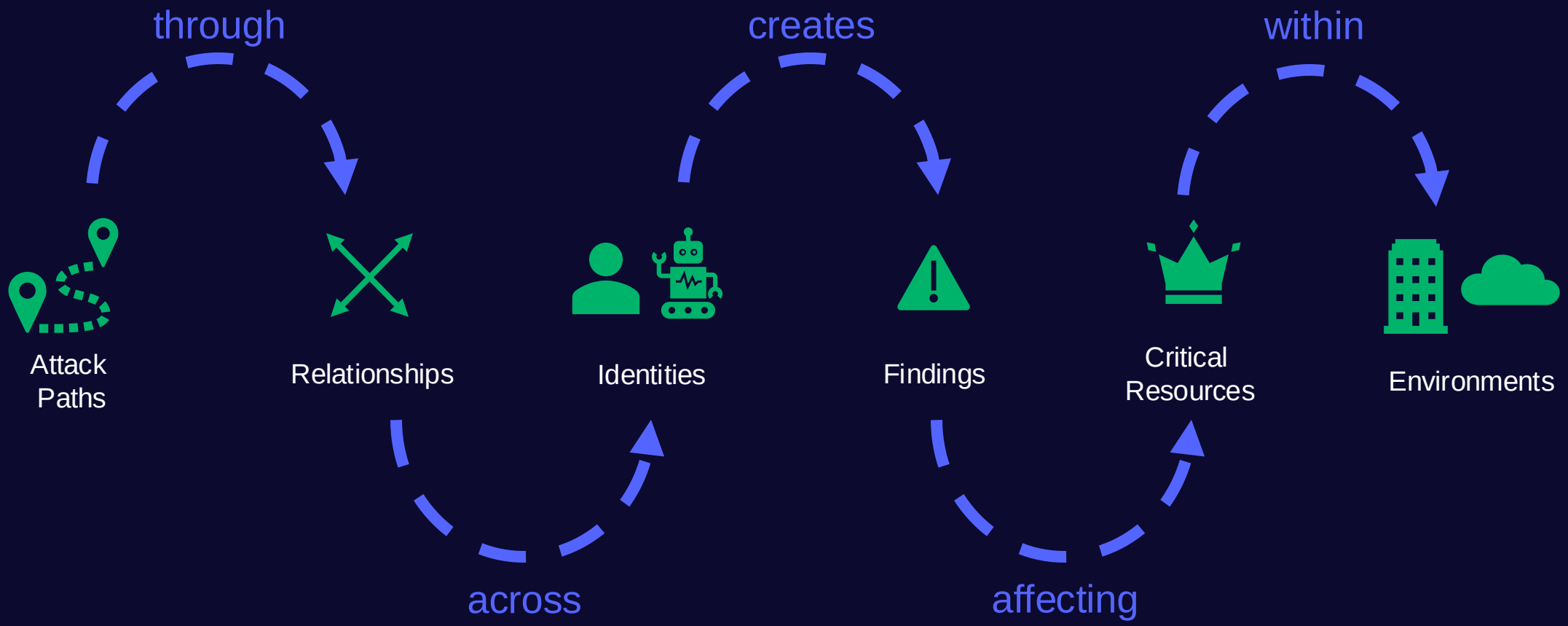


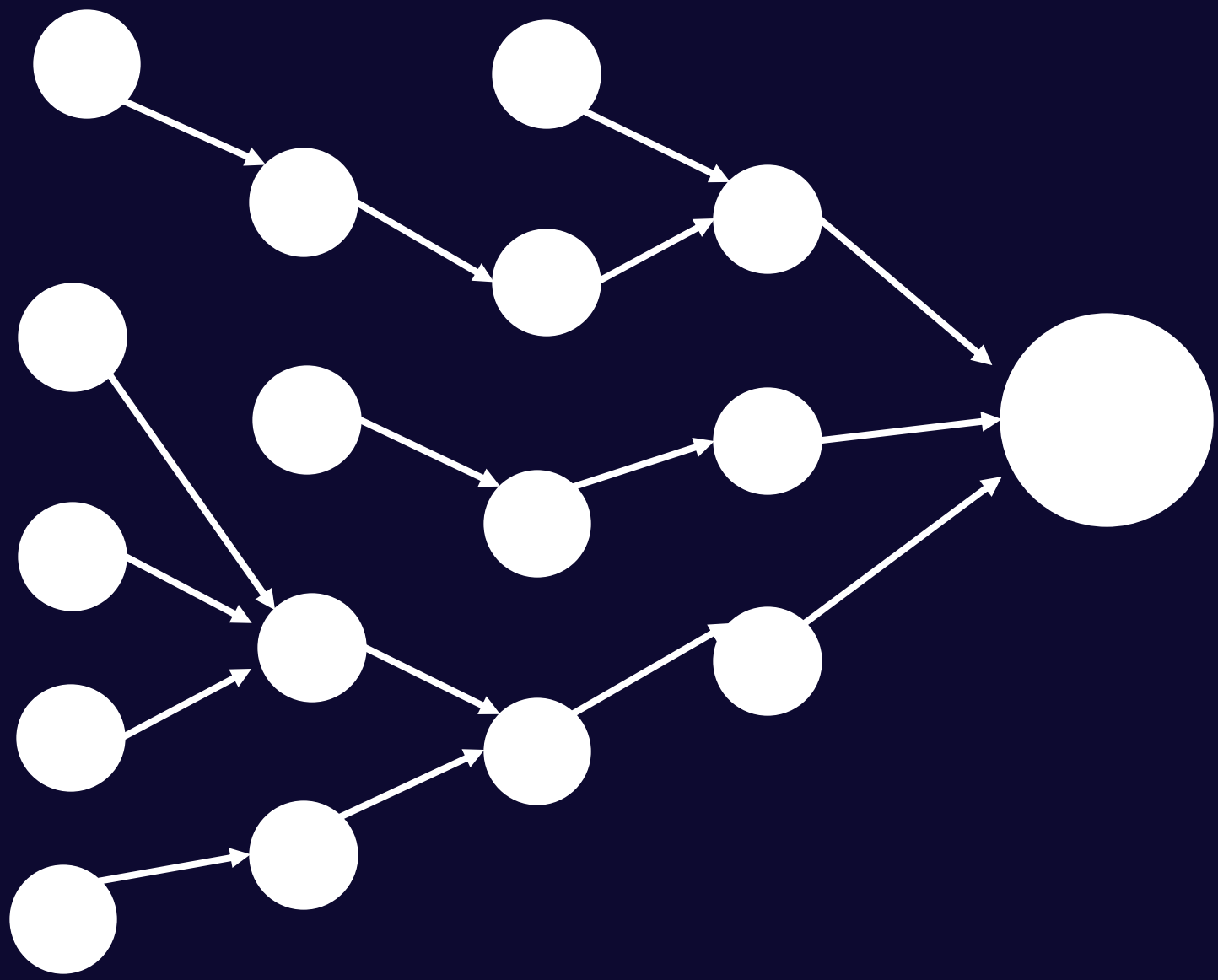
BloodHound Graph 2016

- 3 Nodes
- 3 Edges



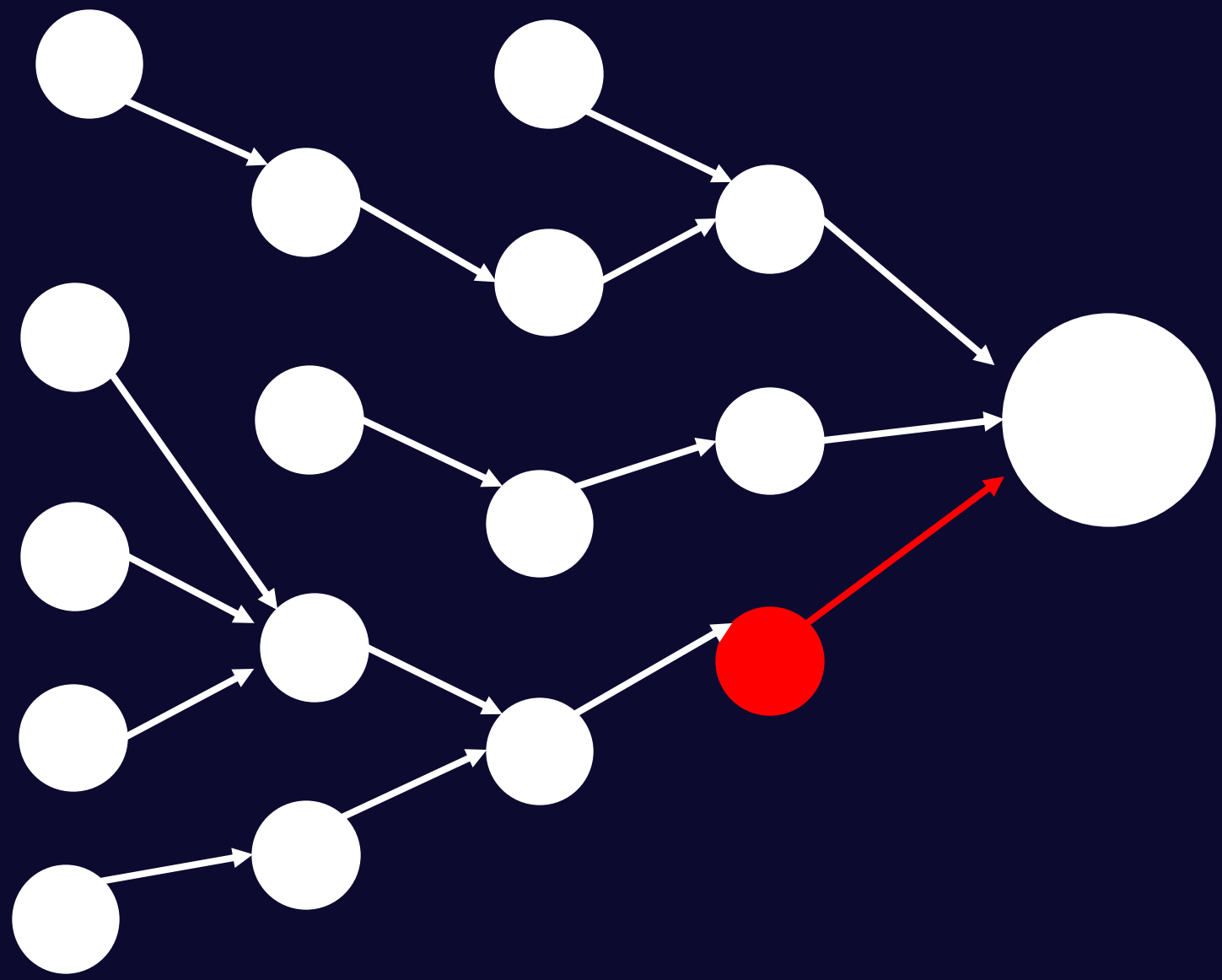
Today: ● 36 Nodes → 121 Edges


through
creates
within
Attack Paths
Relationships
Identities
Findings
Critical Resources
Environments
across
affecting



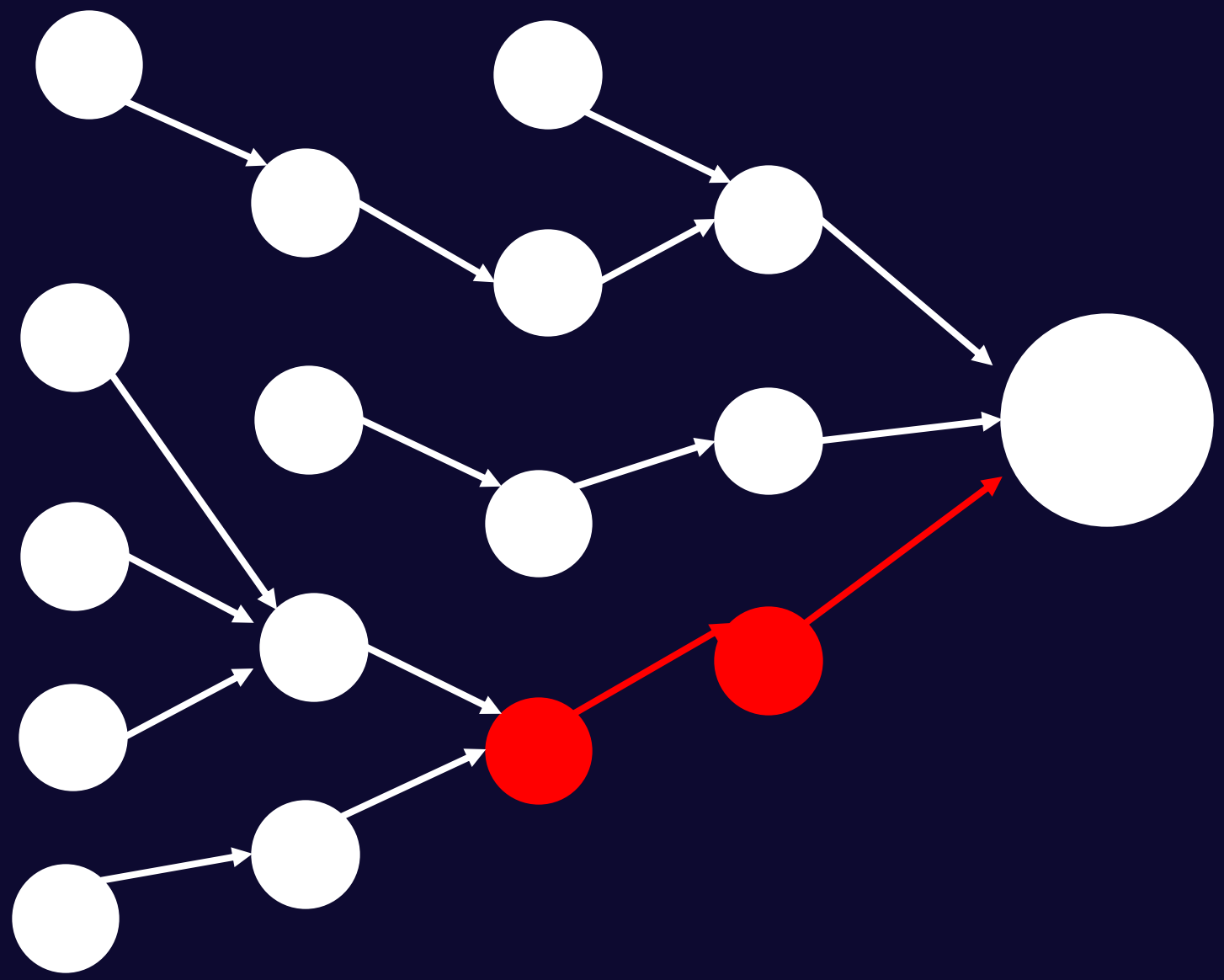
Attack Path Count:

1



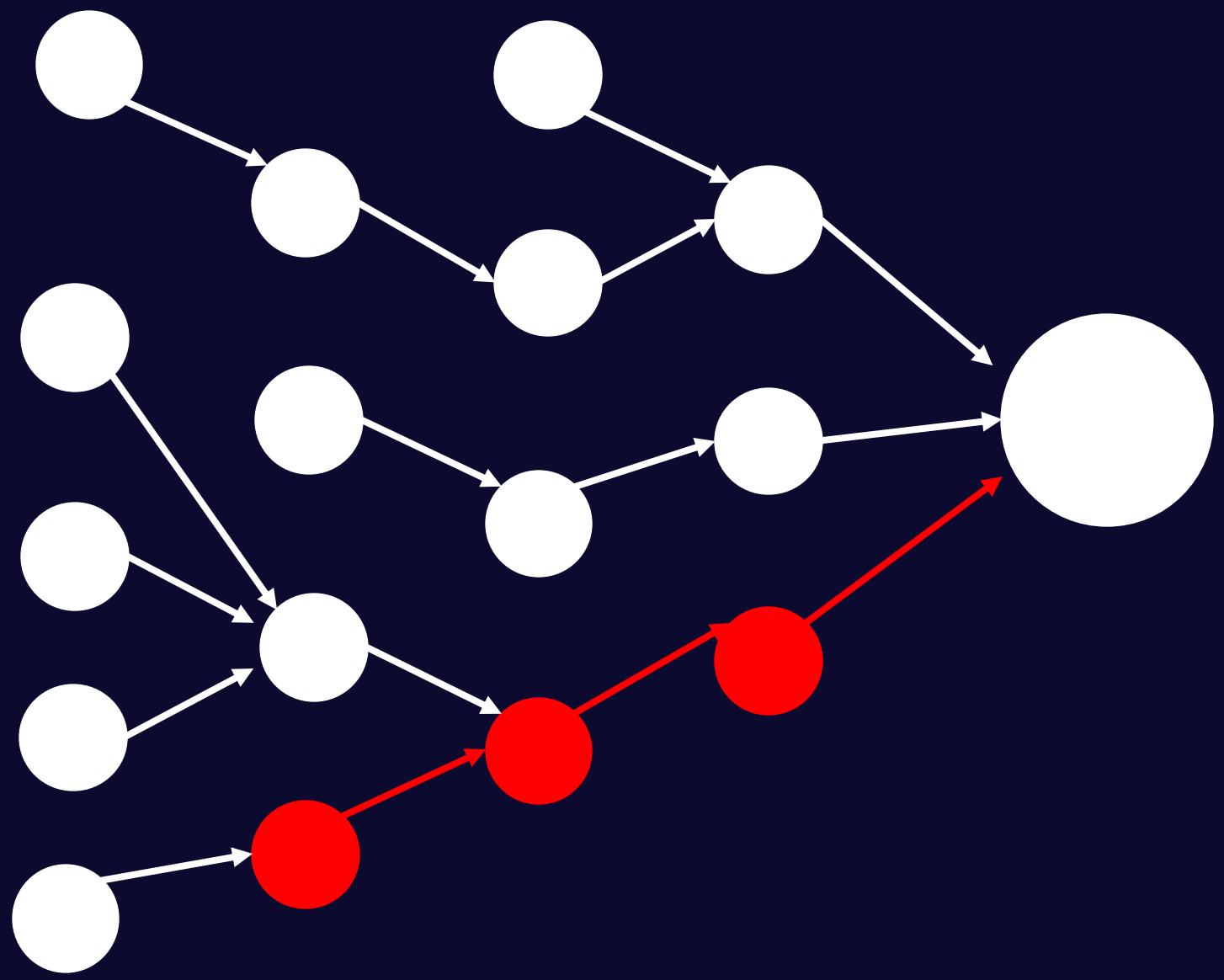
Attack Path Count:

2



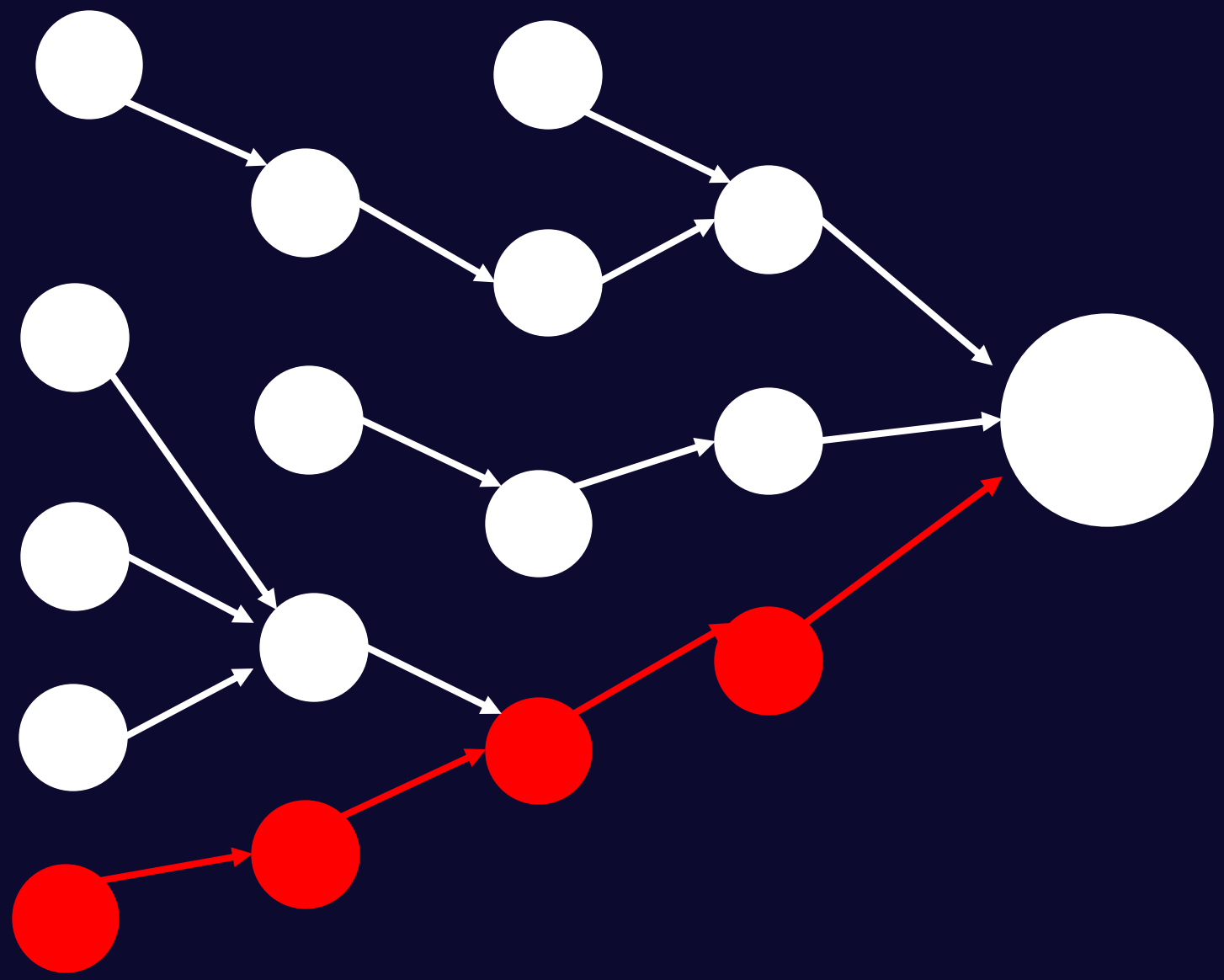
Attack Path Count:

3



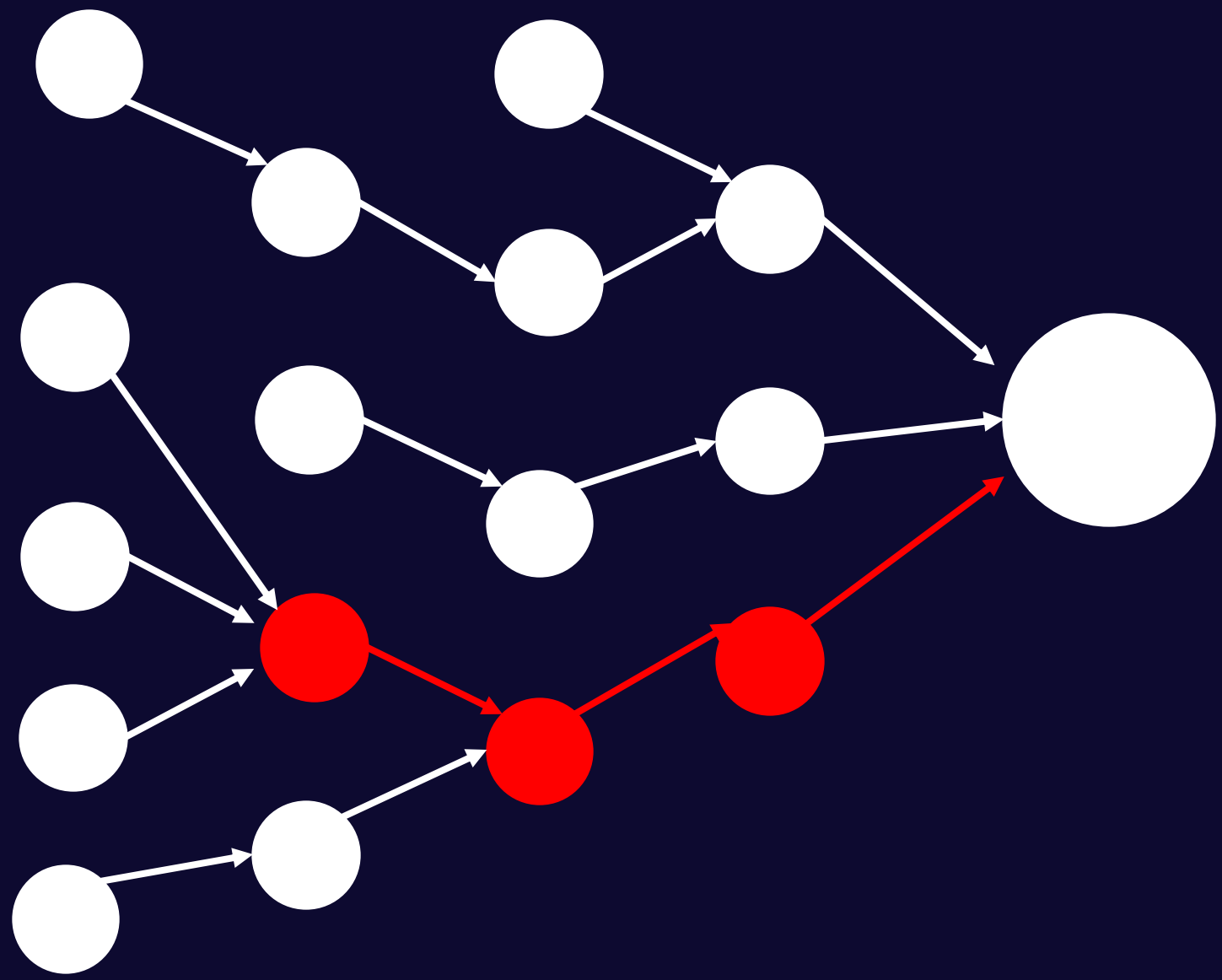
Attack Path Count:

4



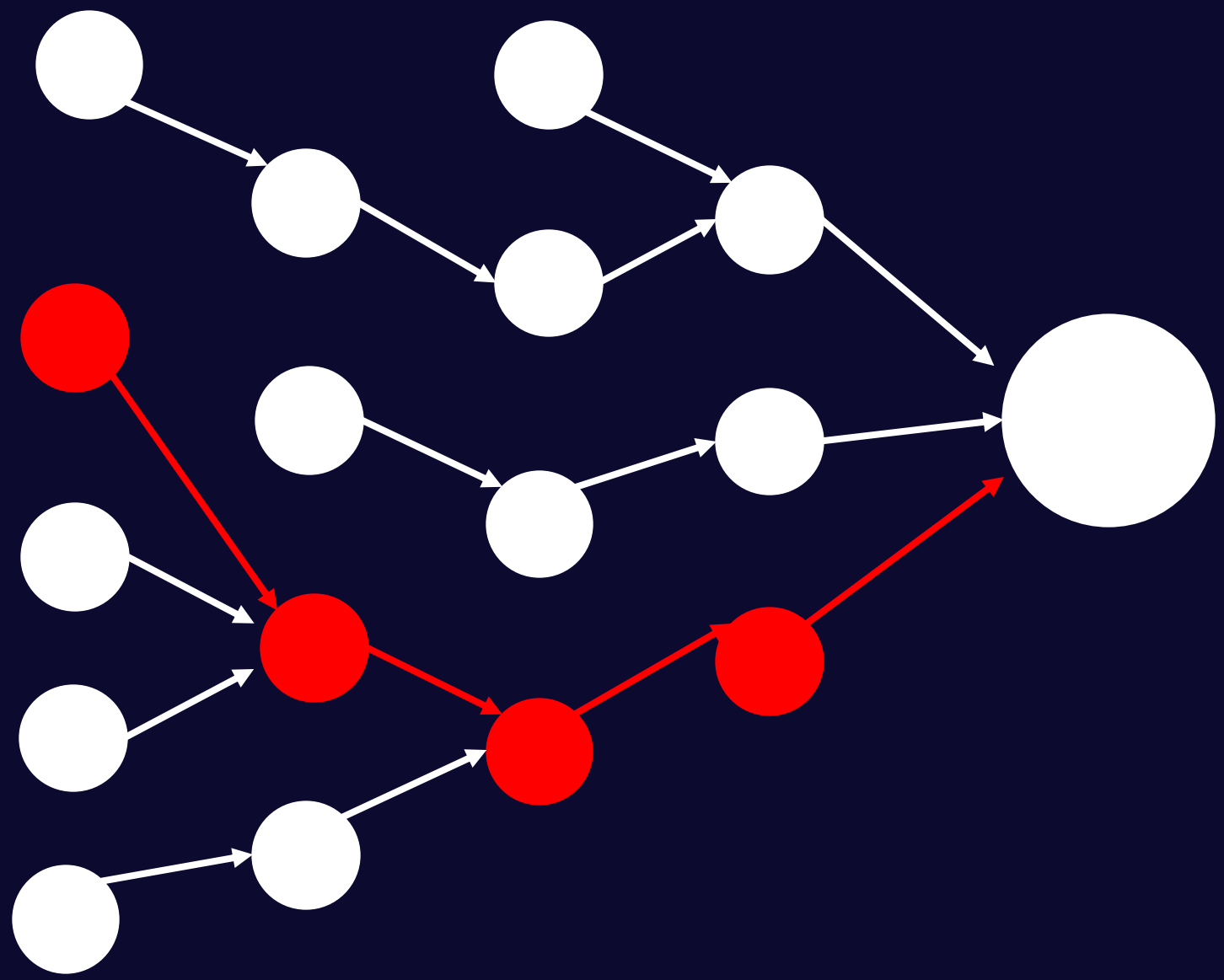
Attack Path Count:

5



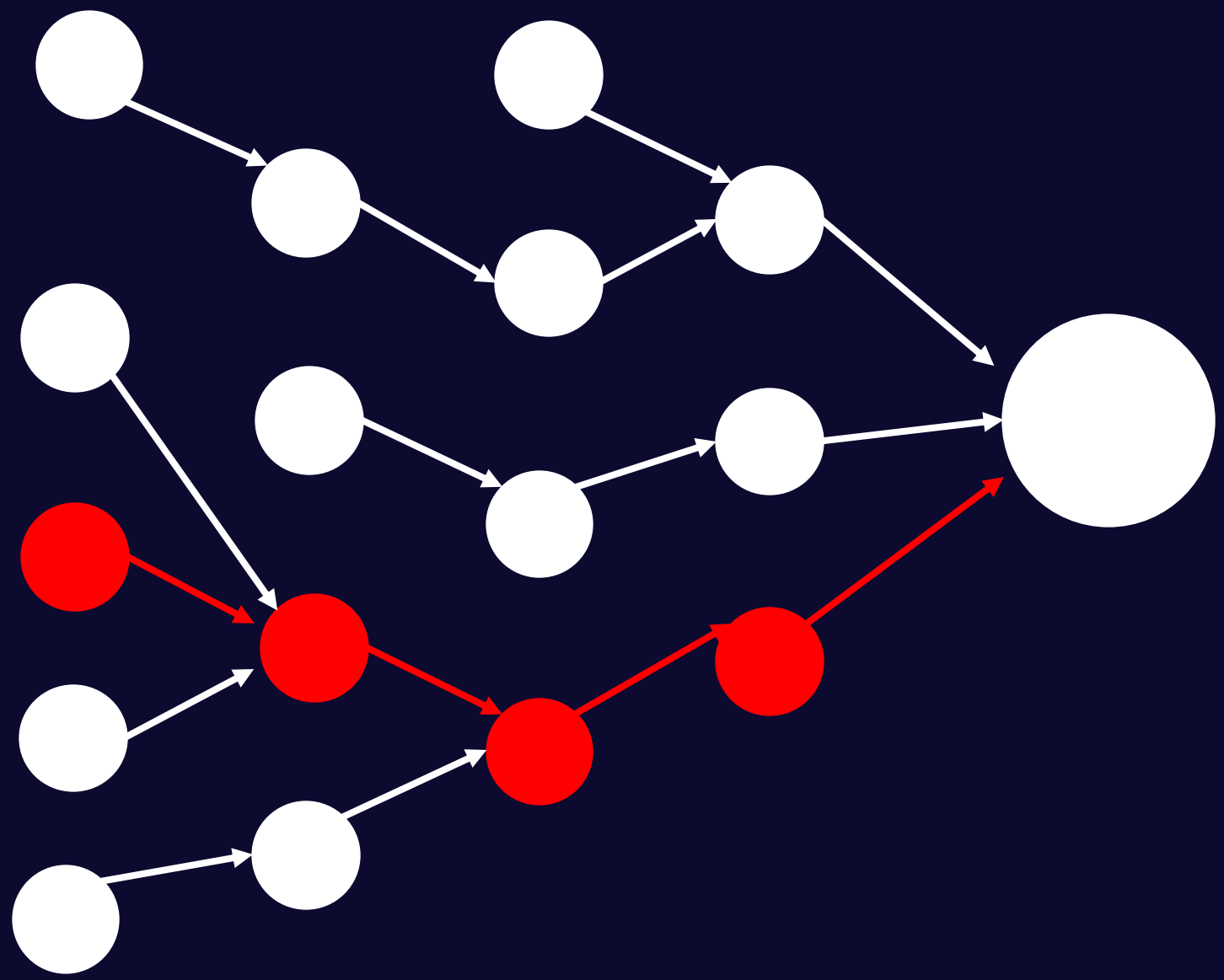
Attack Path Count:

6



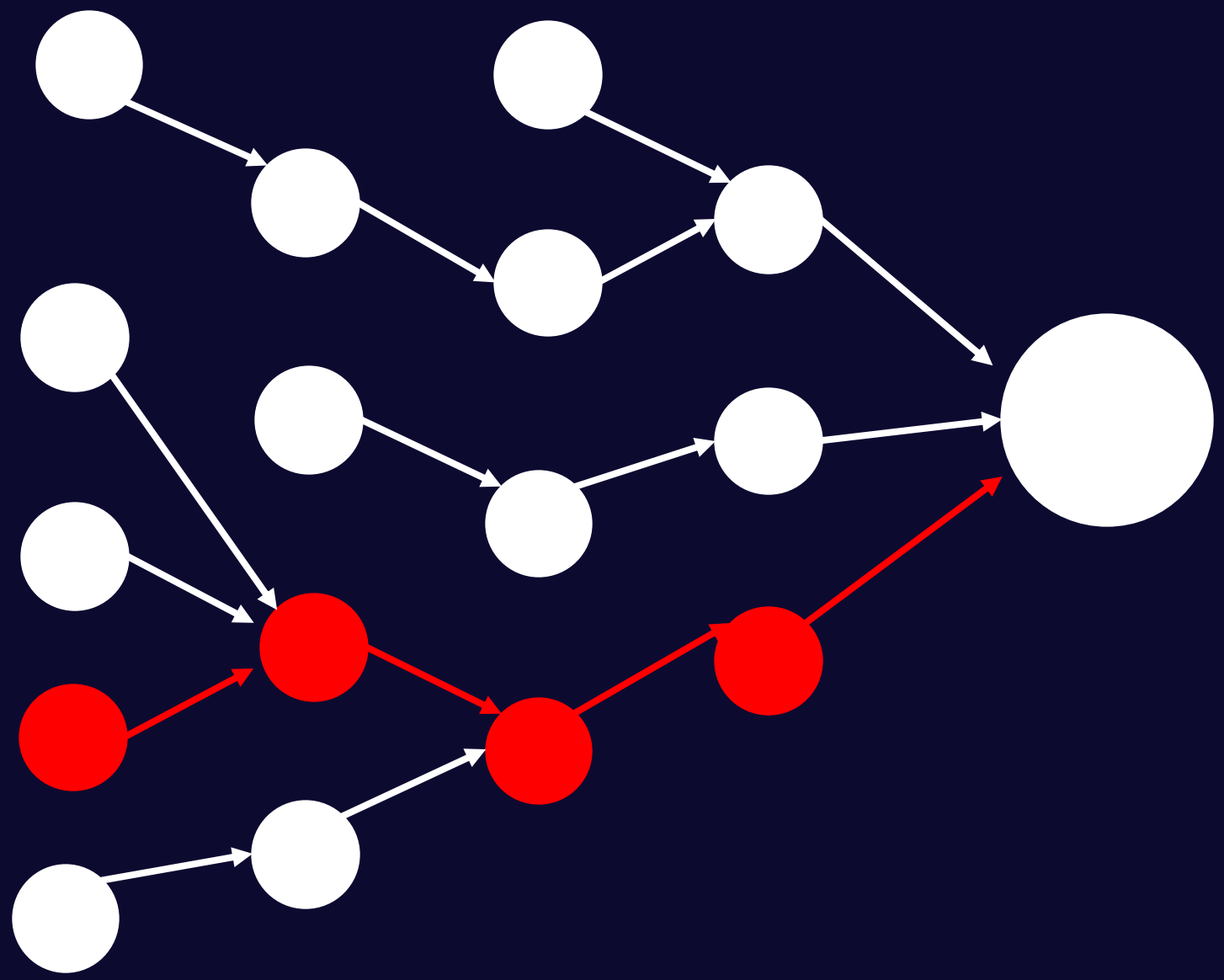
Attack Path Count:

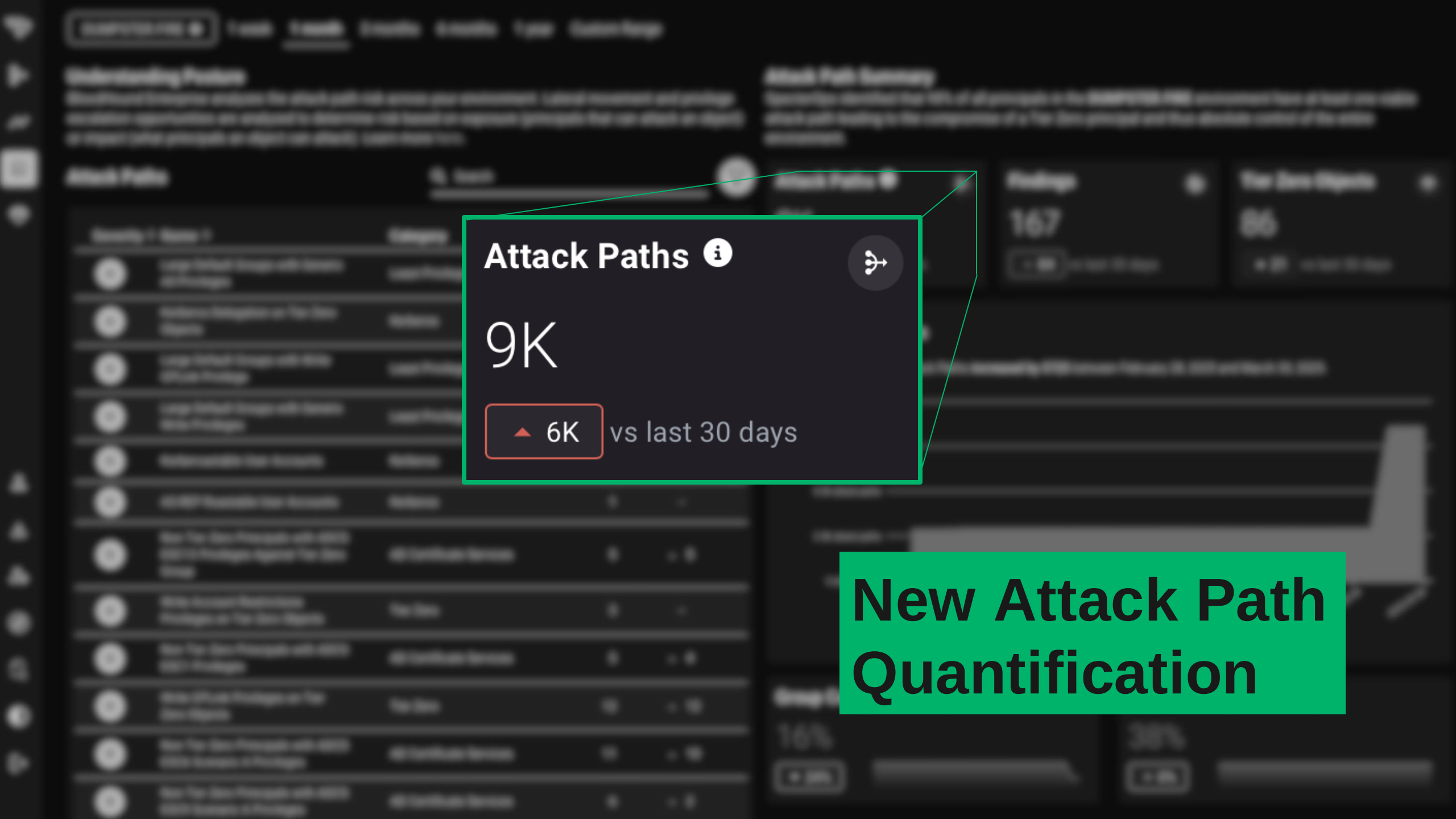
7



Attack Path Count:

8




Attack Paths
9K
6K
vs last 30 days
New Attack Path Quantification

DUMPSTER.FIRE | 1 week | **1 month** | 3 months | 6 months | 1 year | Custom Range

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 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

Search

Severity	Name	Category	Count	Change
	Large Default Groups with Generic All Privileges	Least Privilege	3	▲ 3
	Kerberos Delegation on Tier Zero Objects	Kerberos	15	▲ 2
	Large Default Groups with Write GPLink Privilege	Least Privilege	16	▲ 16
	Large Default Groups with Generic Write Privileges	Least Privilege	2	▲ 1
	Kerberoastable User Accounts	Kerberos	2	--
	AS-REP Roastable User Accounts	Kerberos	1	--
	Non Tier Zero Principals with ADCS ESC13 Privileges Against Tier Zero Group	AD Certificate Services	5	▲ 5
	Write Account Restrictions Privileges on Tier Zero Objects	Tier Zero	3	--
		cate Services	5	▲ 4
			12	▲ 12
		cate Services	11	▲ 10
	ESC9 Scenario A Privileges	AD Certificate Services	6	▲ 2

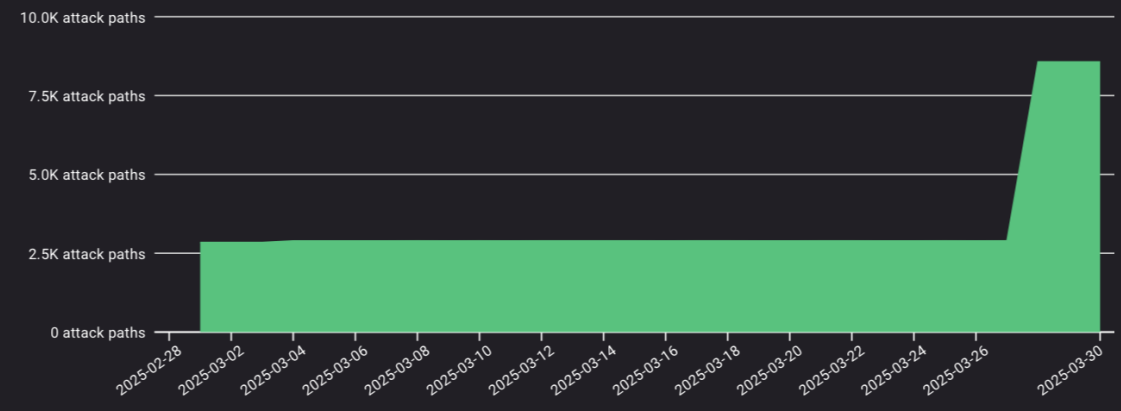
Attack Paths 9K ▲ 6K vs last 30 days

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

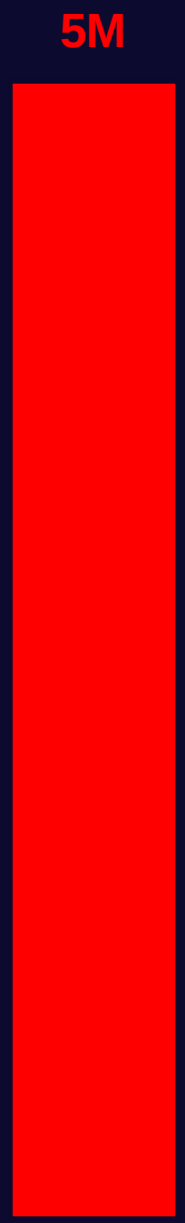
16% ▼ 24%

Session Completeness

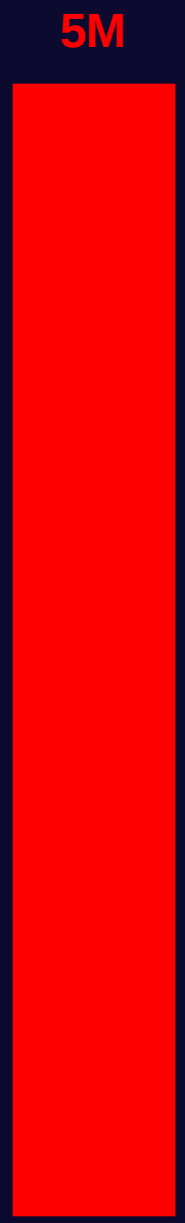
38% = 0%

New Security Posture view

5K Identities =



5 Million Attack Paths

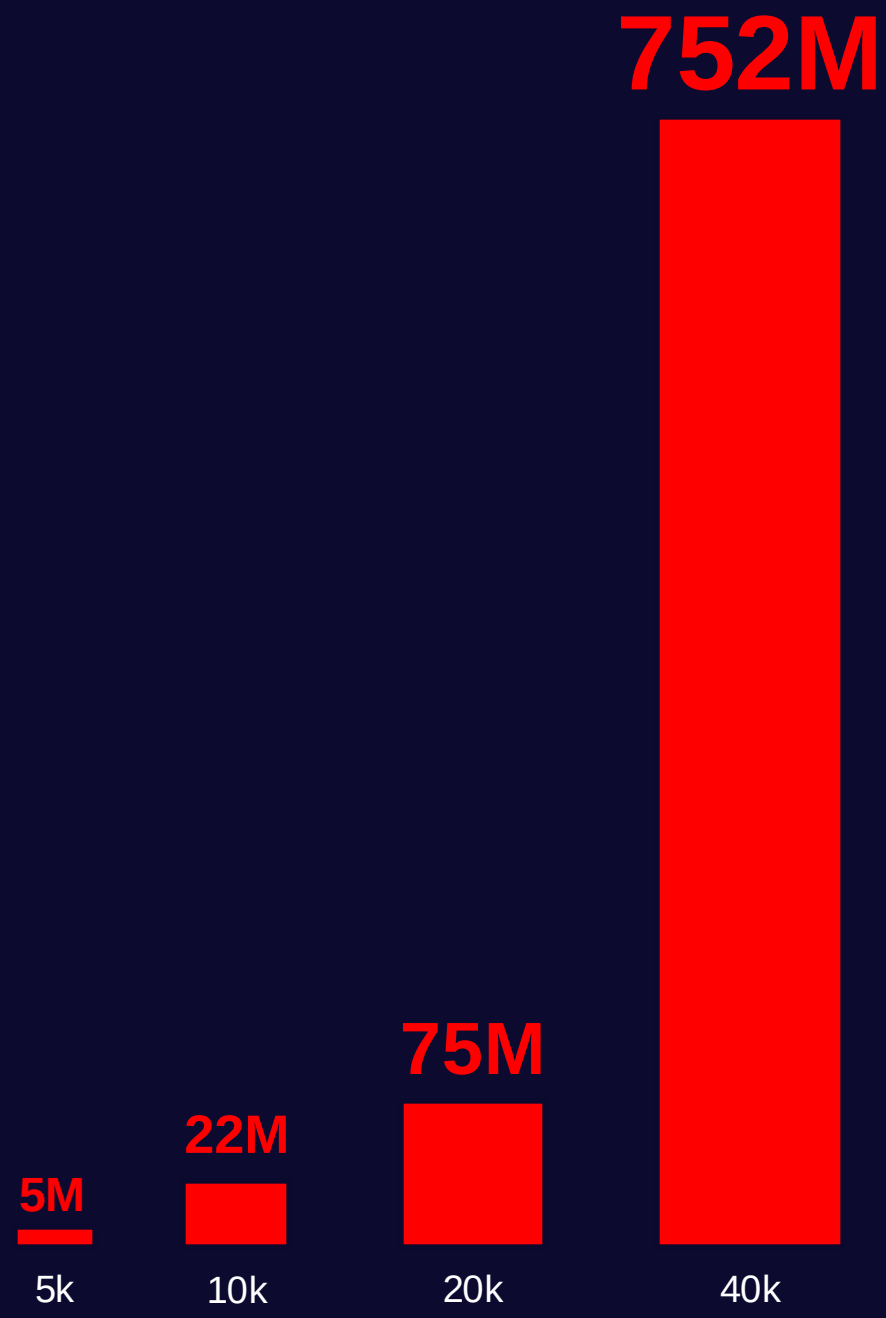

5M

5M

5k

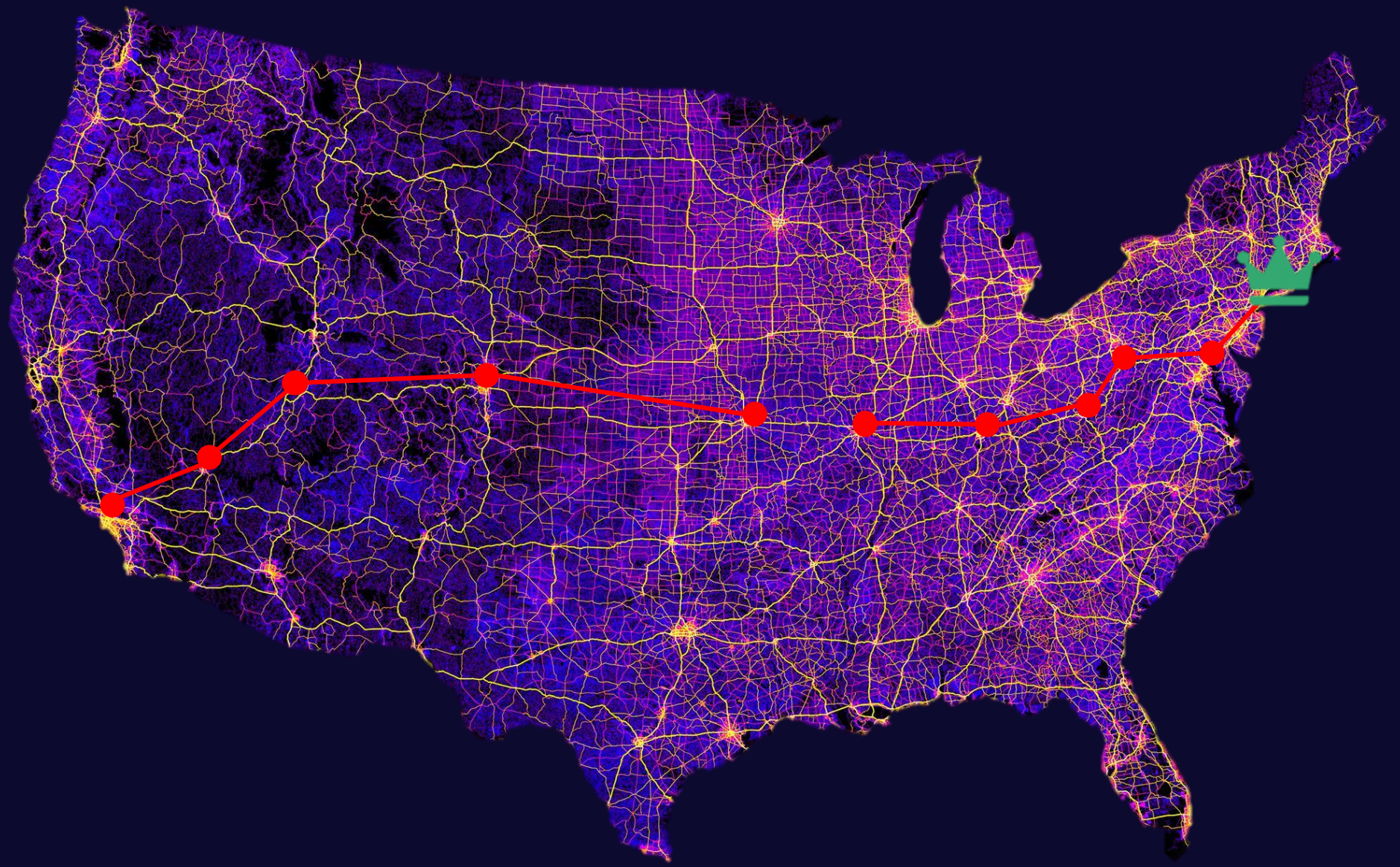
More Identities

More Problems



151 Billion Problems

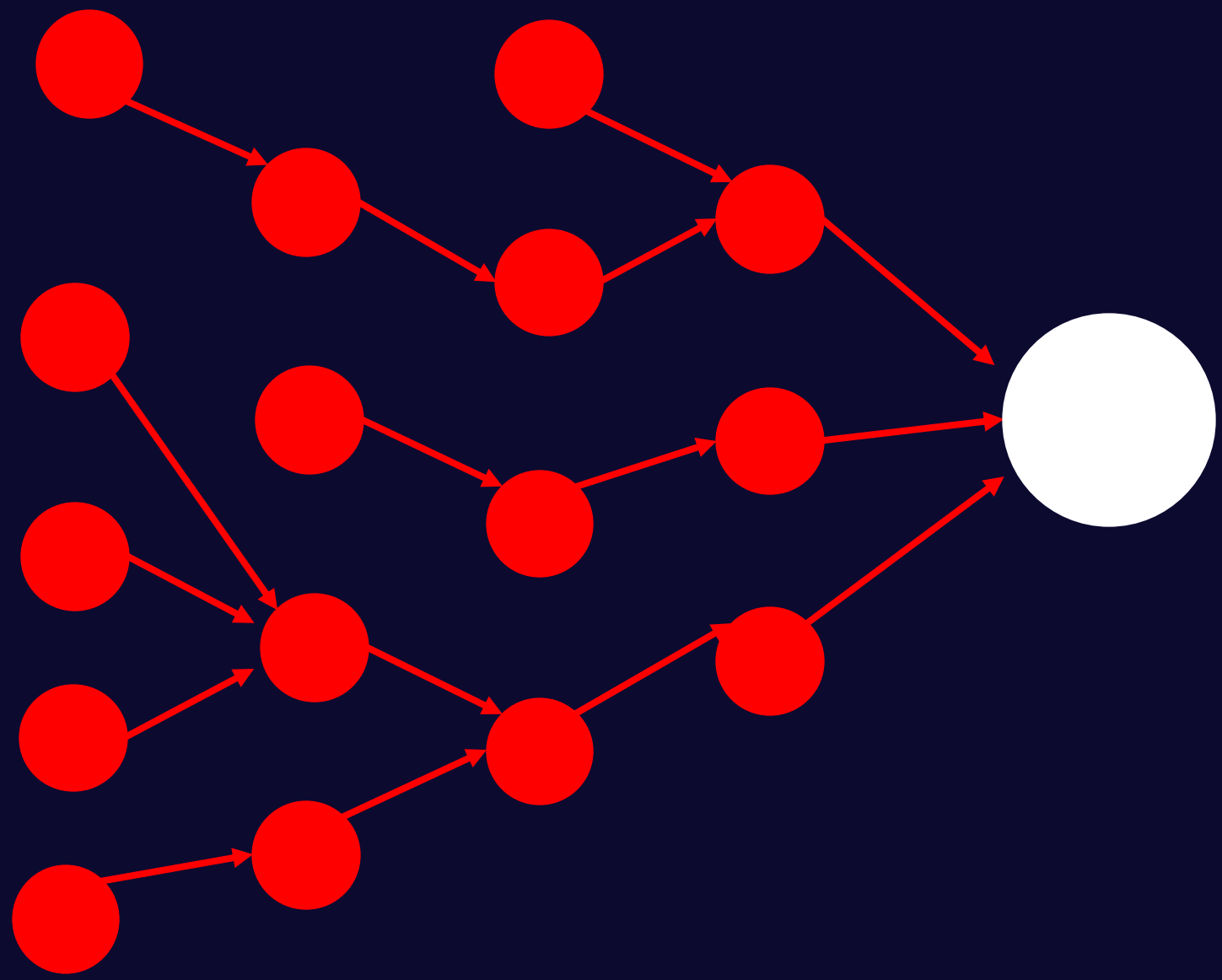
(to be exact)

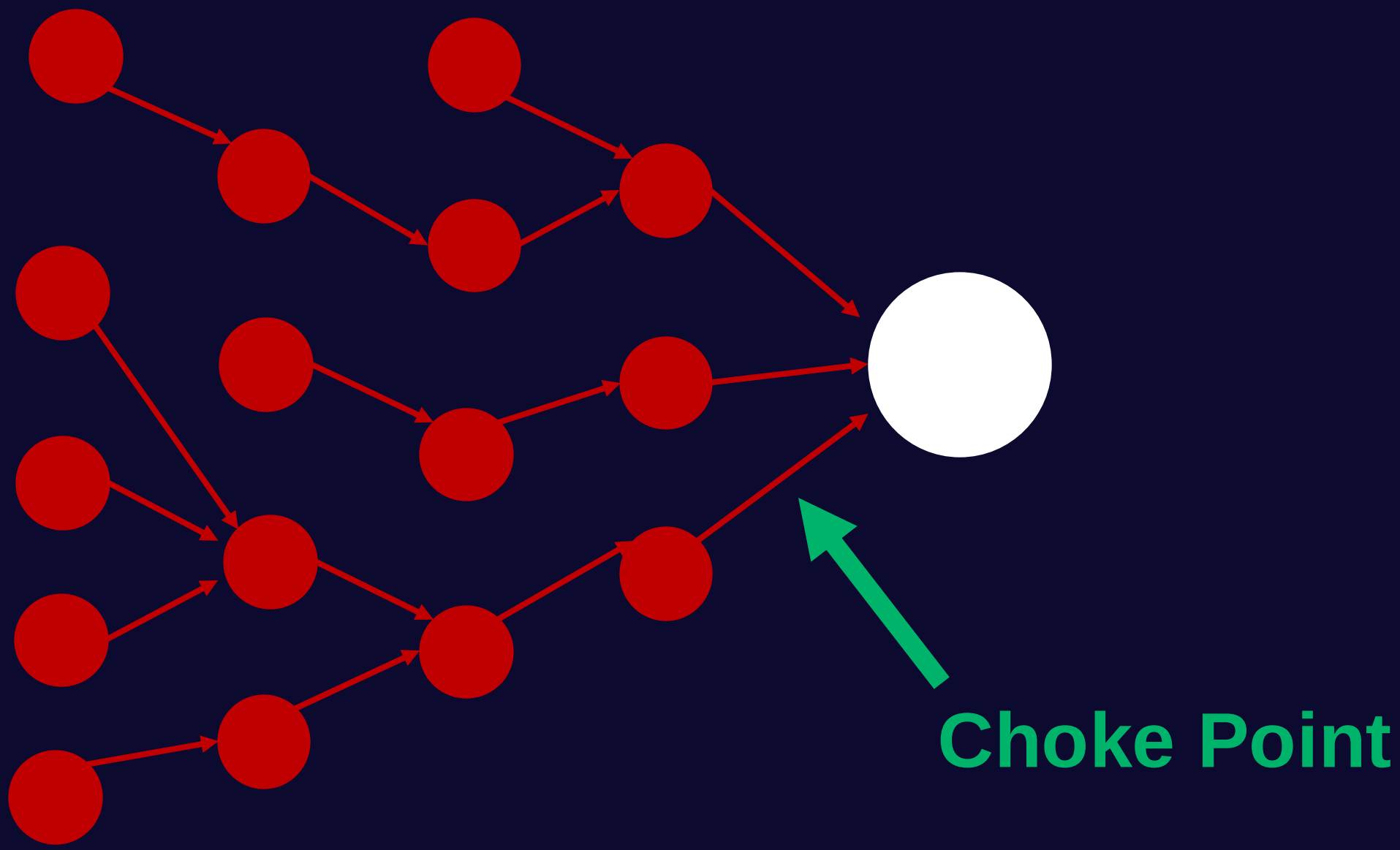


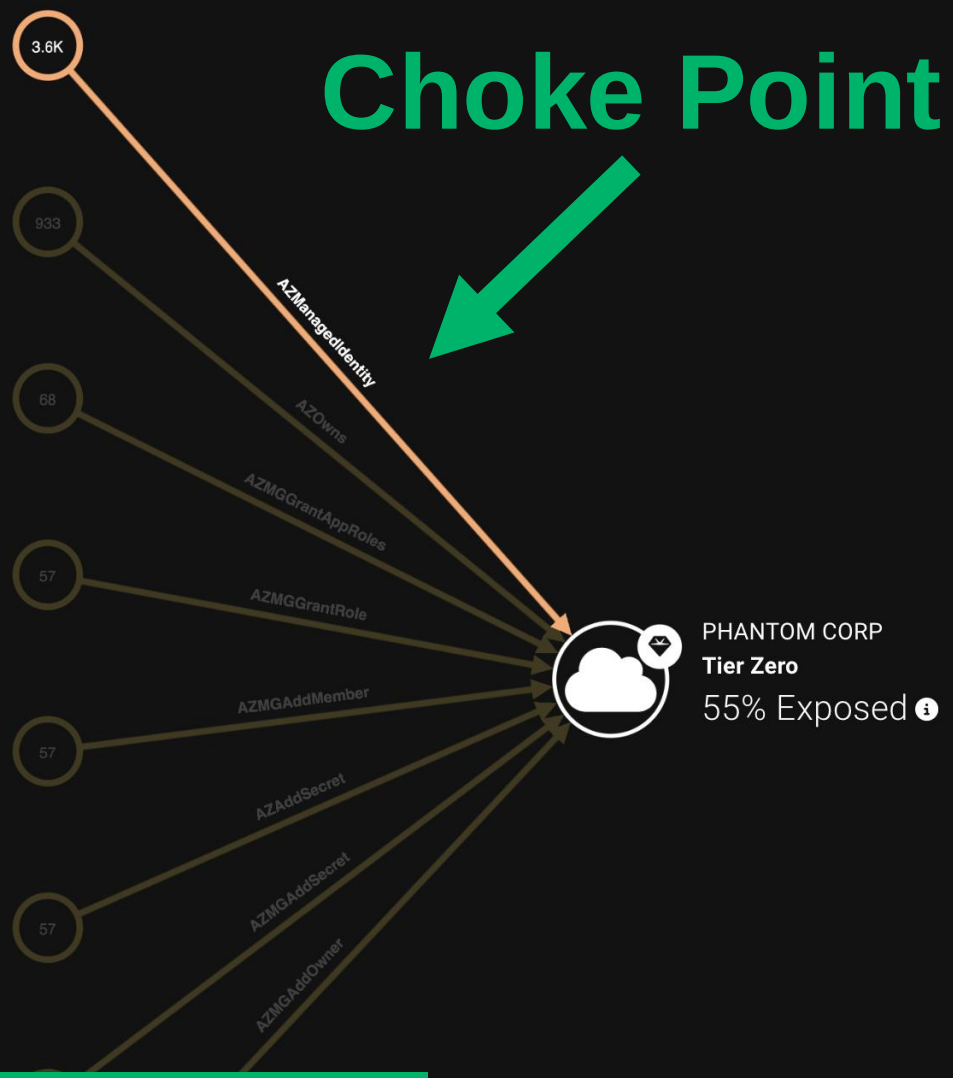
Billions of routes	through millions of roads	connecting thousands of cities	to Manhattan
Billions of Attack Paths	through millions of relationships	connecting thousands of identities	to critical resources

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

REMEDIATION

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

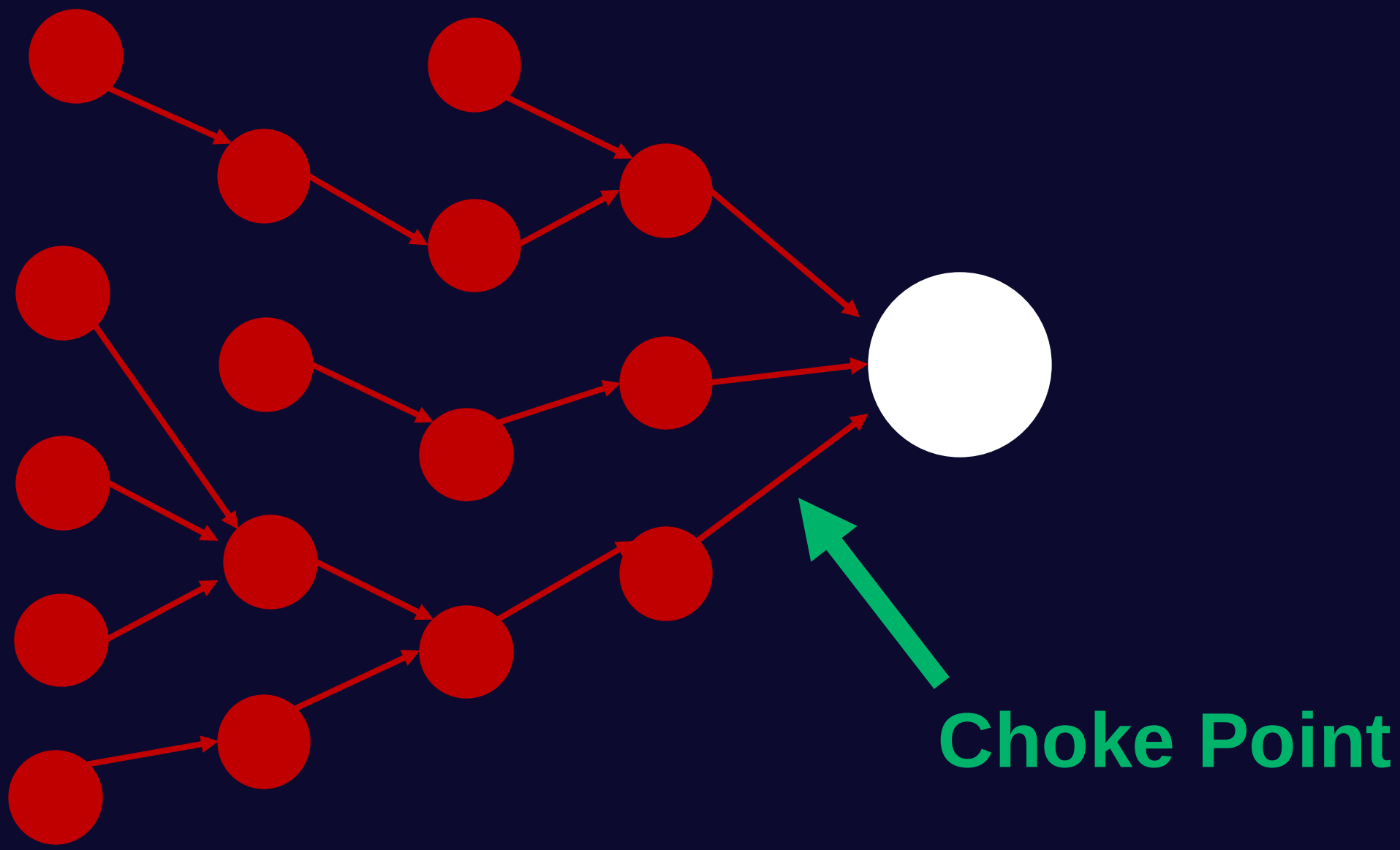
View / Export Full Remediation Plan | Export CSV

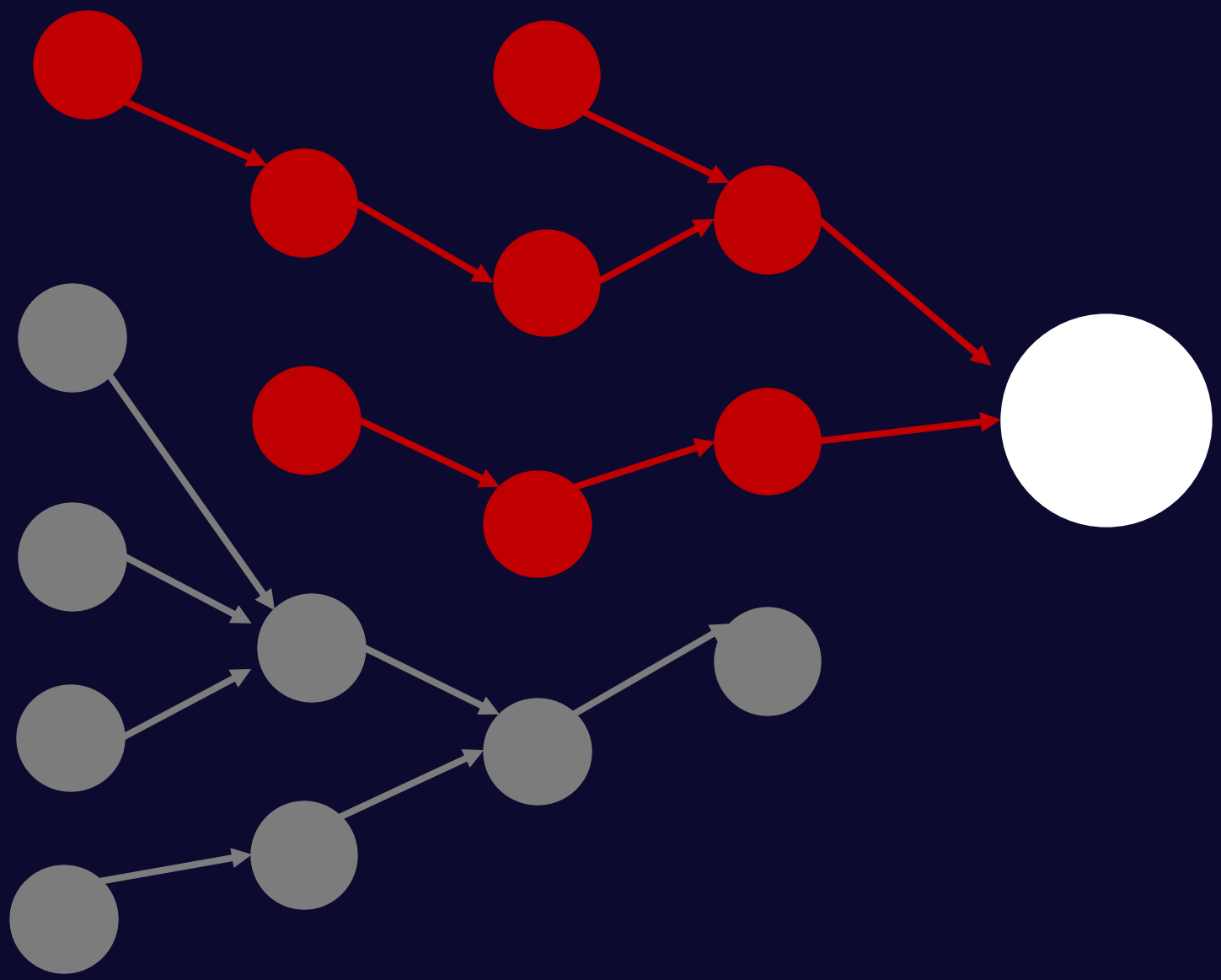
Ownership of Tier Zero Principal

2 Findings | ± 0 vs last month | Low

Non Tier Zero Principal Can Grant Tier Zero App Roles

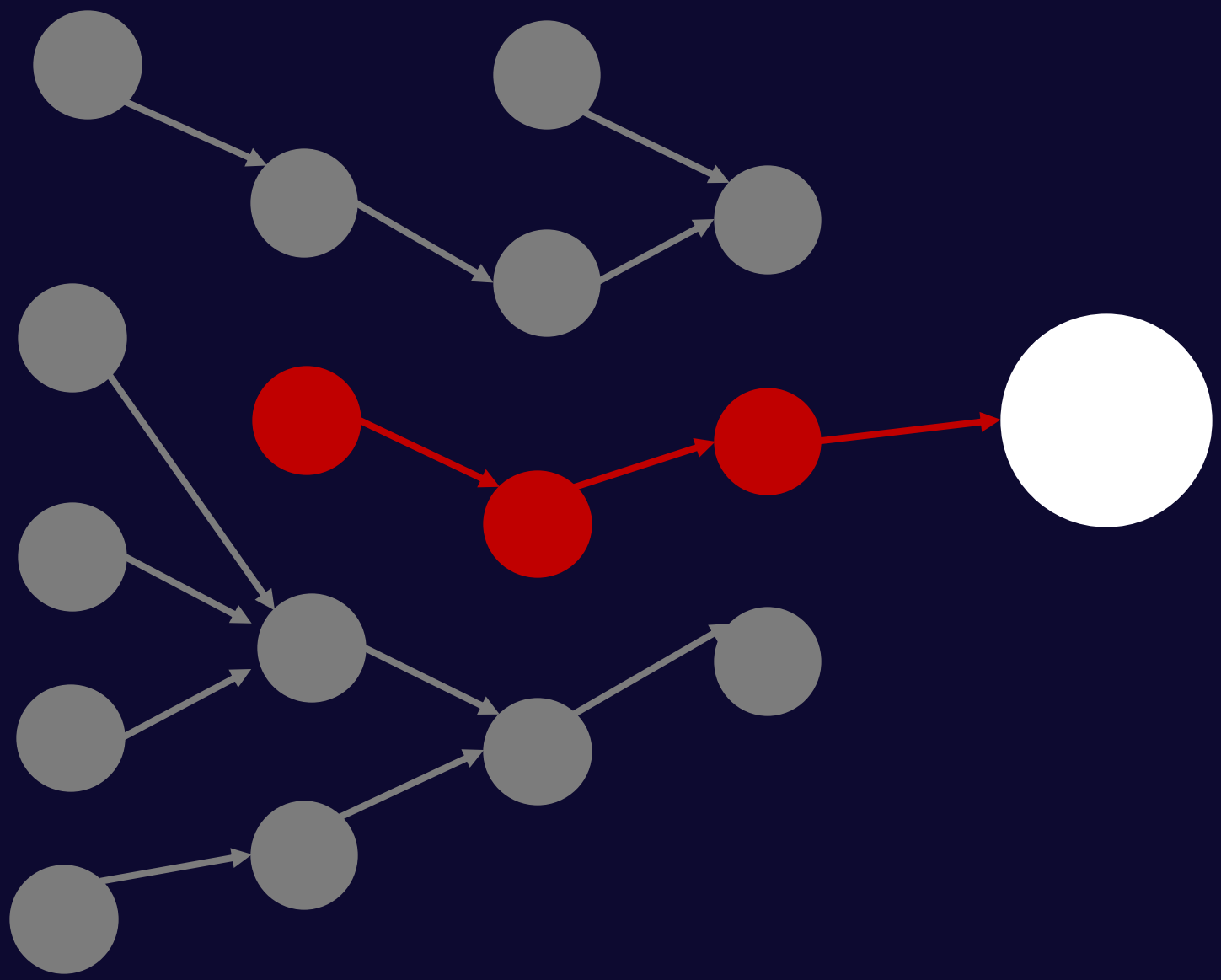
26 Findings | 6 ↘ vs last month | Low


Choke Point



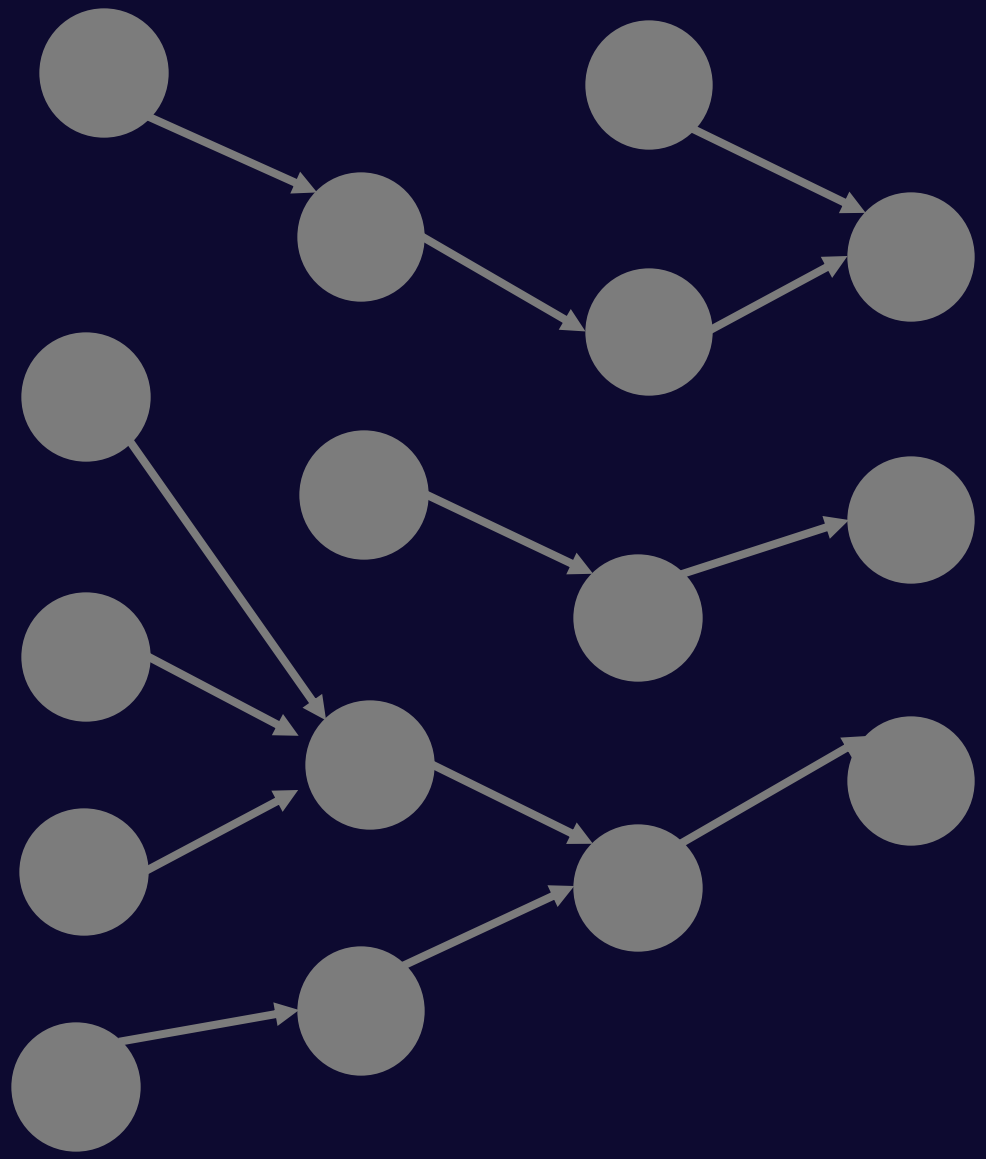
Attack Paths Removed:

8



Attack Paths Removed:

13

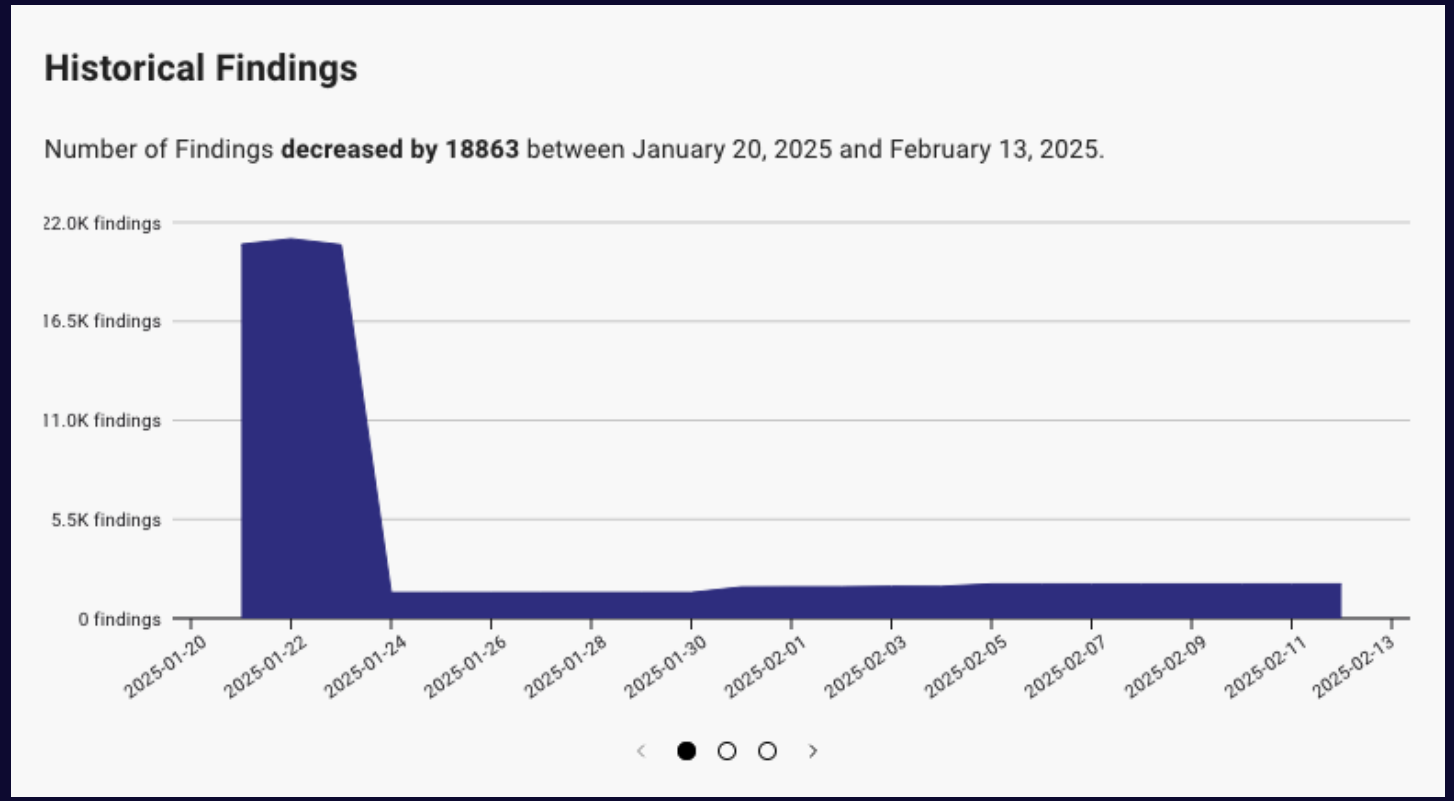


Attack Paths Removed:

16

Fixing one finding
cuts 300,000
Attack Paths

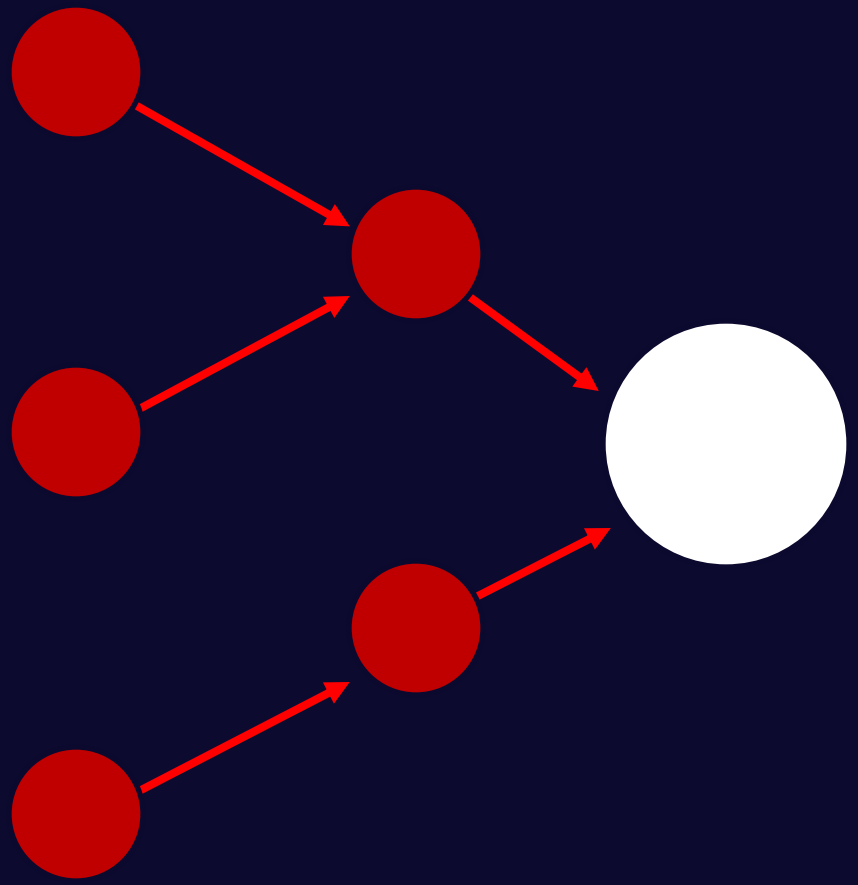
Findings Resolved

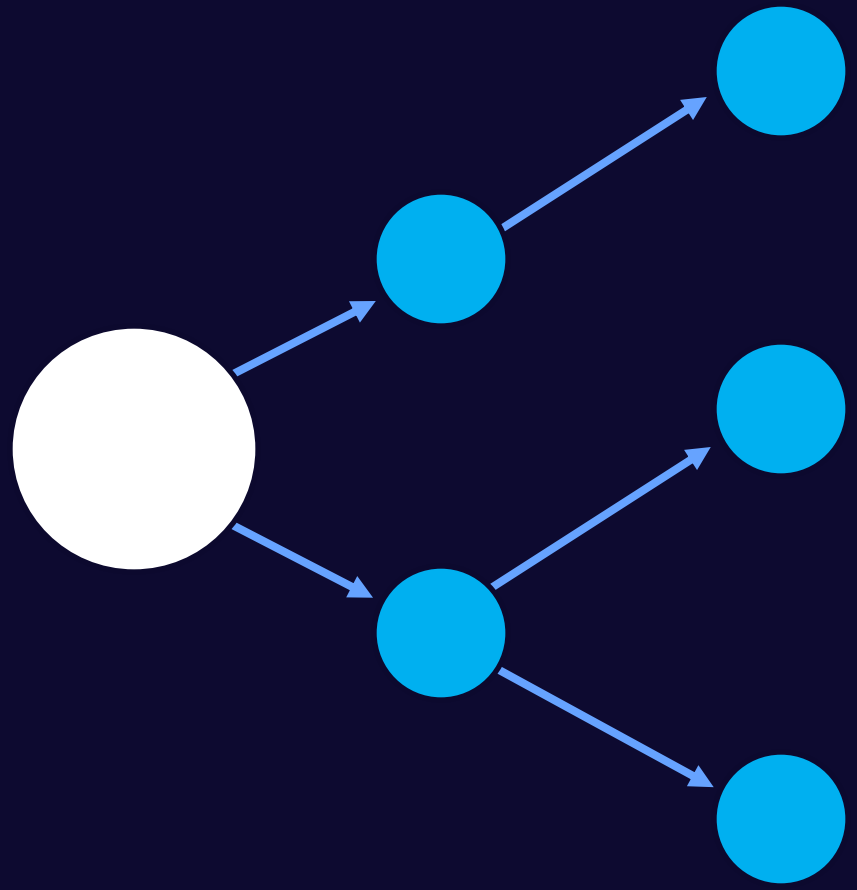


Finding reduction during trial

Exposure

The Attack Paths to
a target node

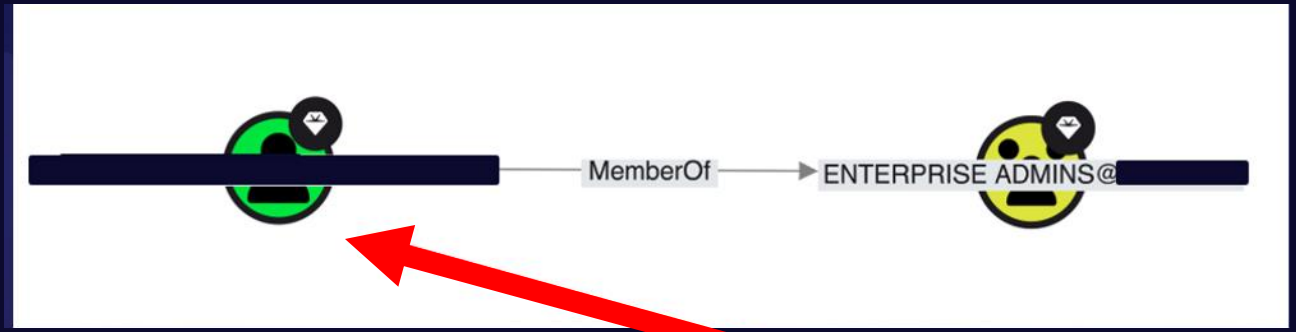




Impact

The attack paths from at 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

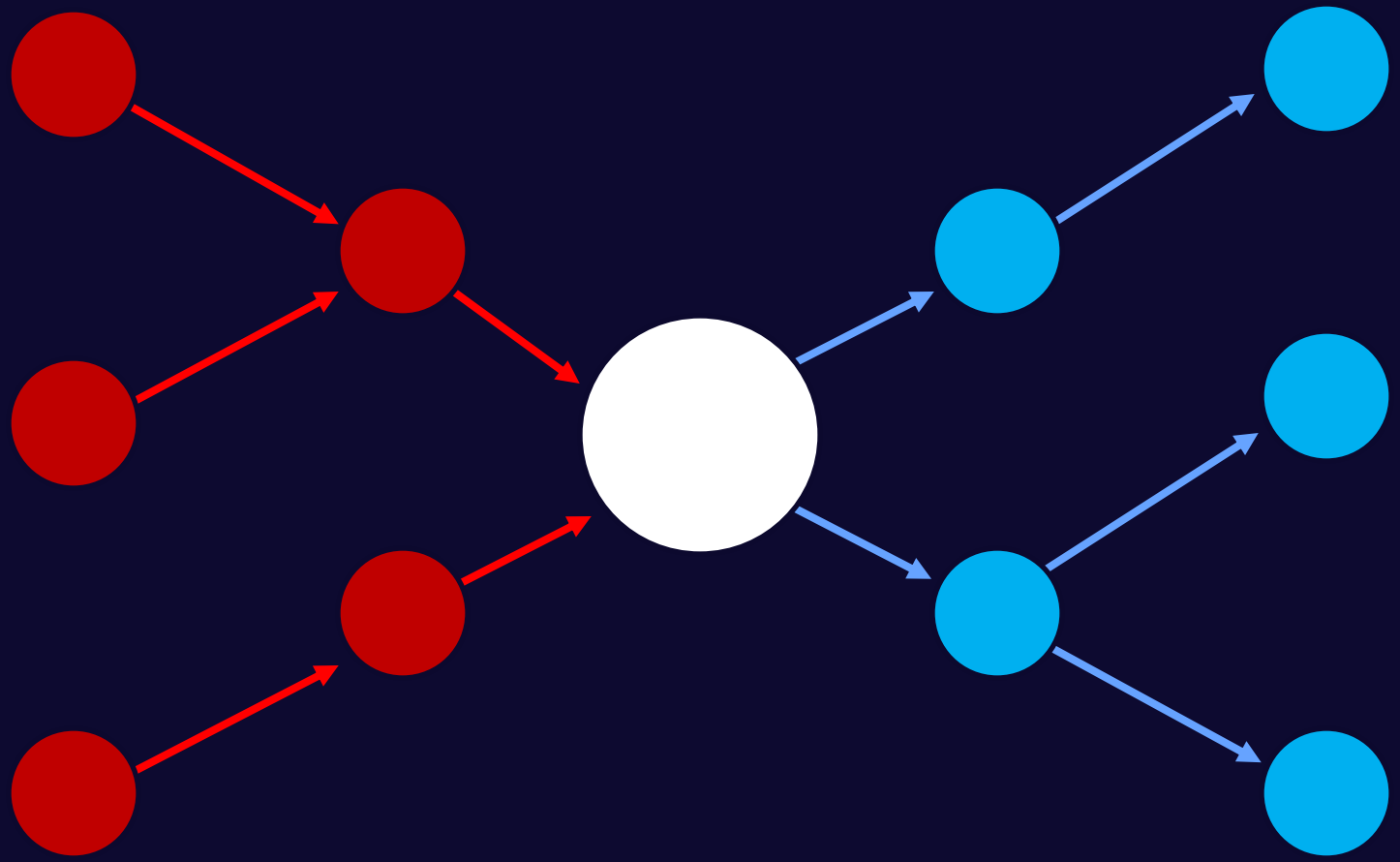
Accepted

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

Password Last Set: 2003-11-29

Exposure

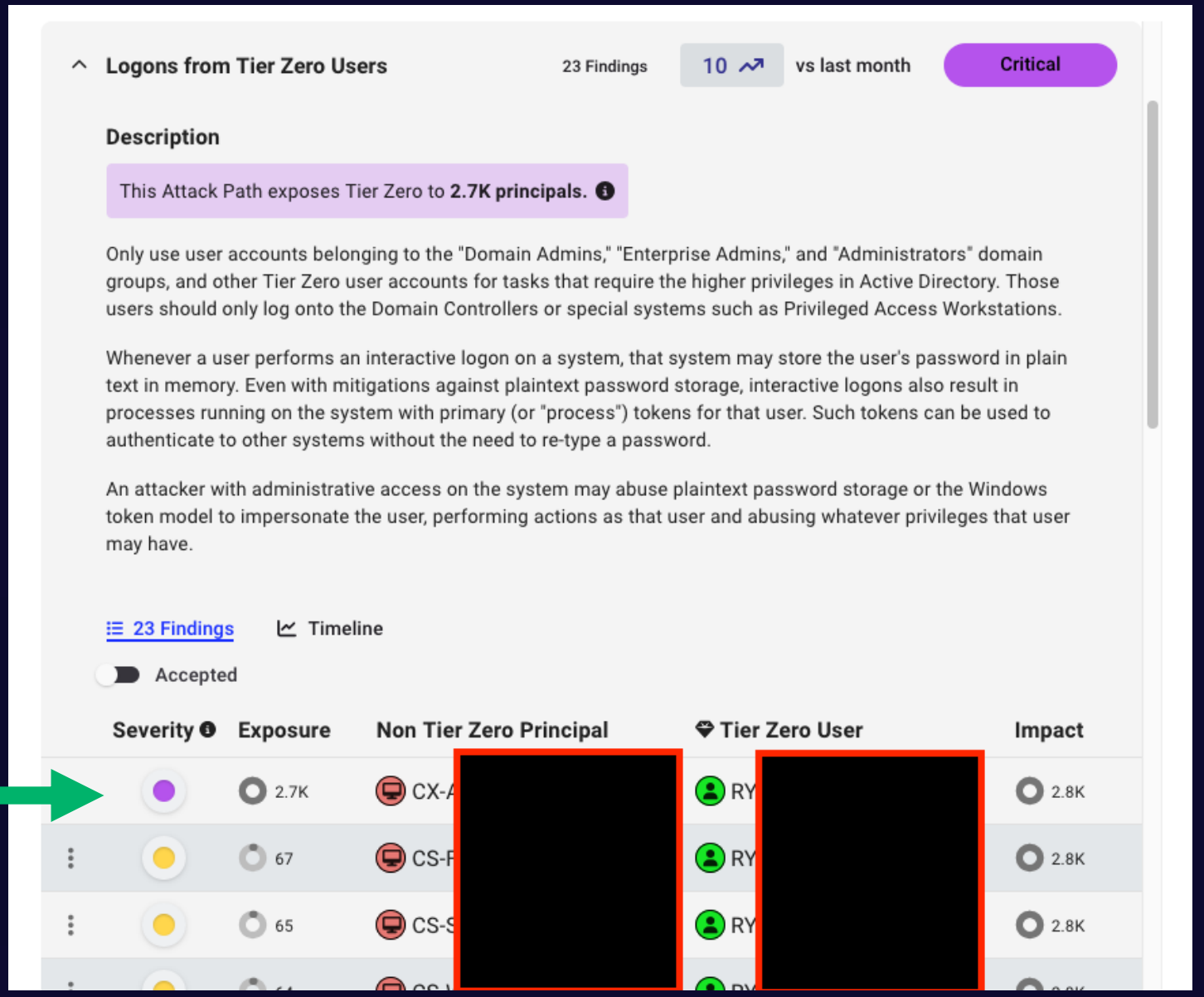
The Attack Paths to
a target node



Impact

The attack paths
from at target node

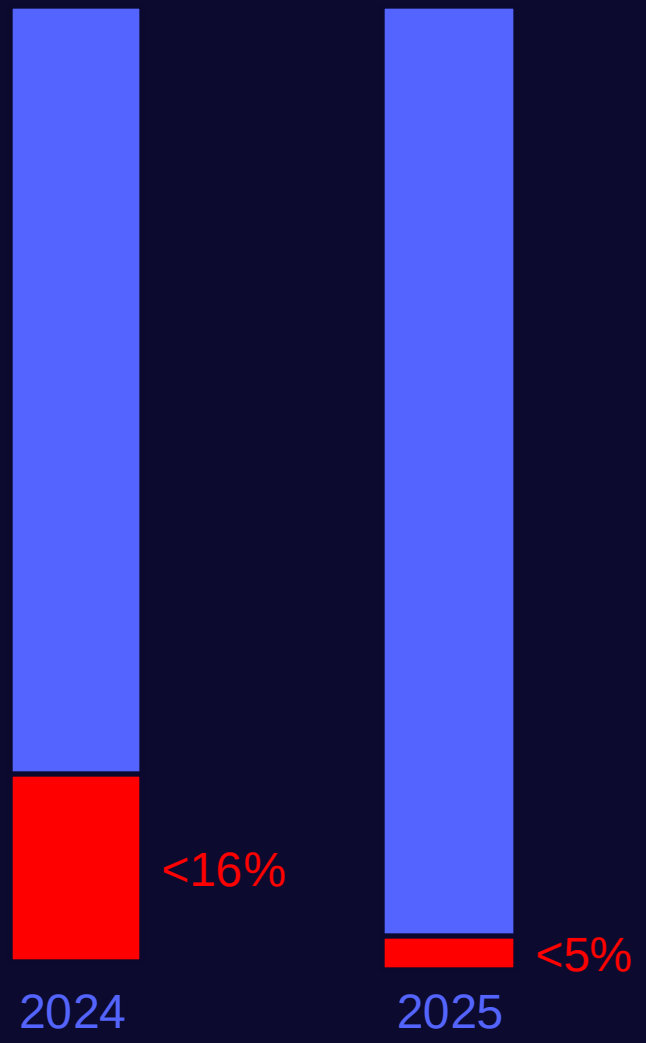
New Granular Attack Path Risk



Active Directory Certificate Services (ADCS)

65% of critical ADCS ESC1 have been remediated

Now found in 5% of environments

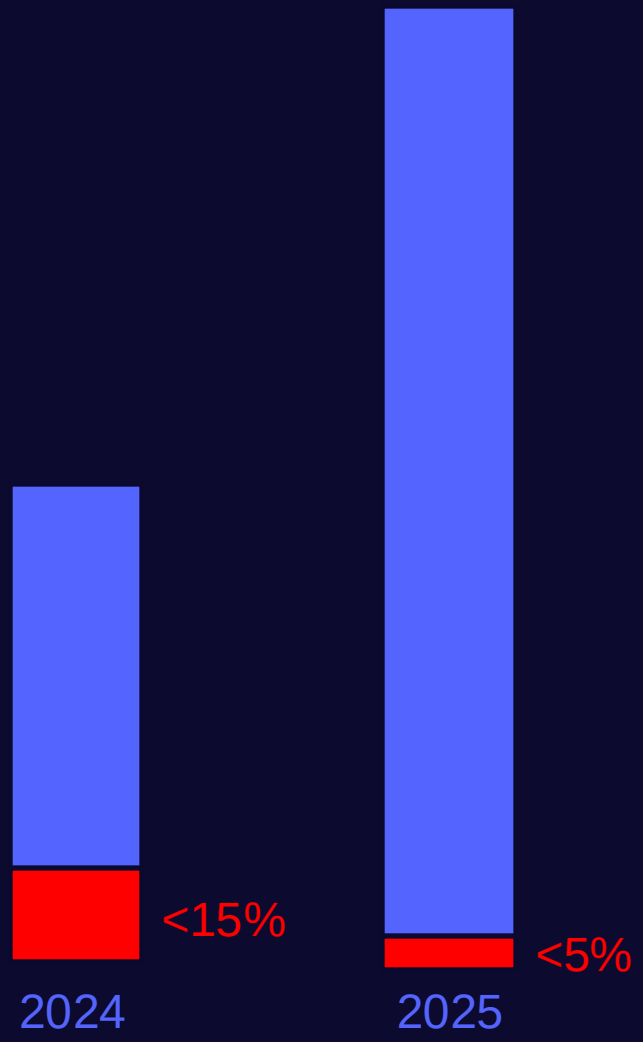


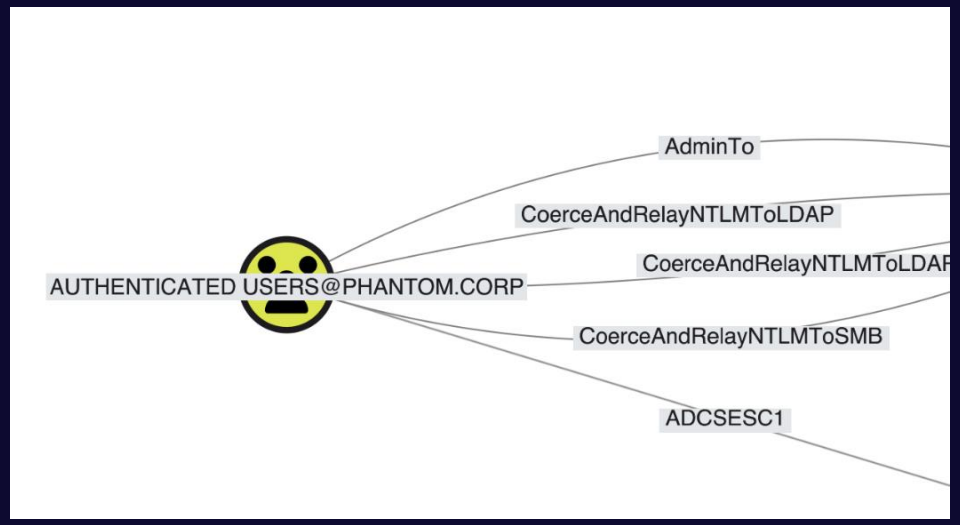
65% of critical ADCS ESC1 have been remediated

Now found in 5% of environments

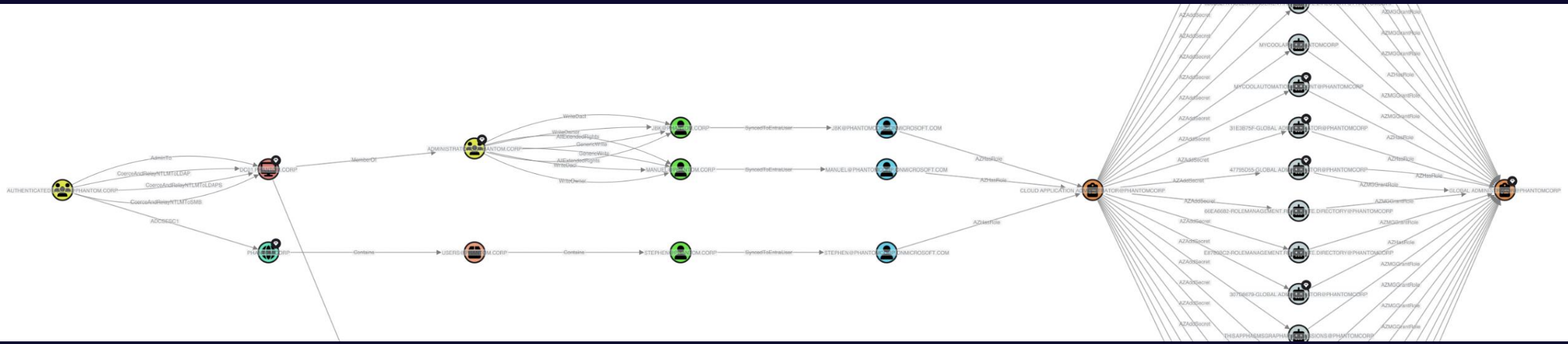
We also doubled monitored environments

(identified and remediated even more)

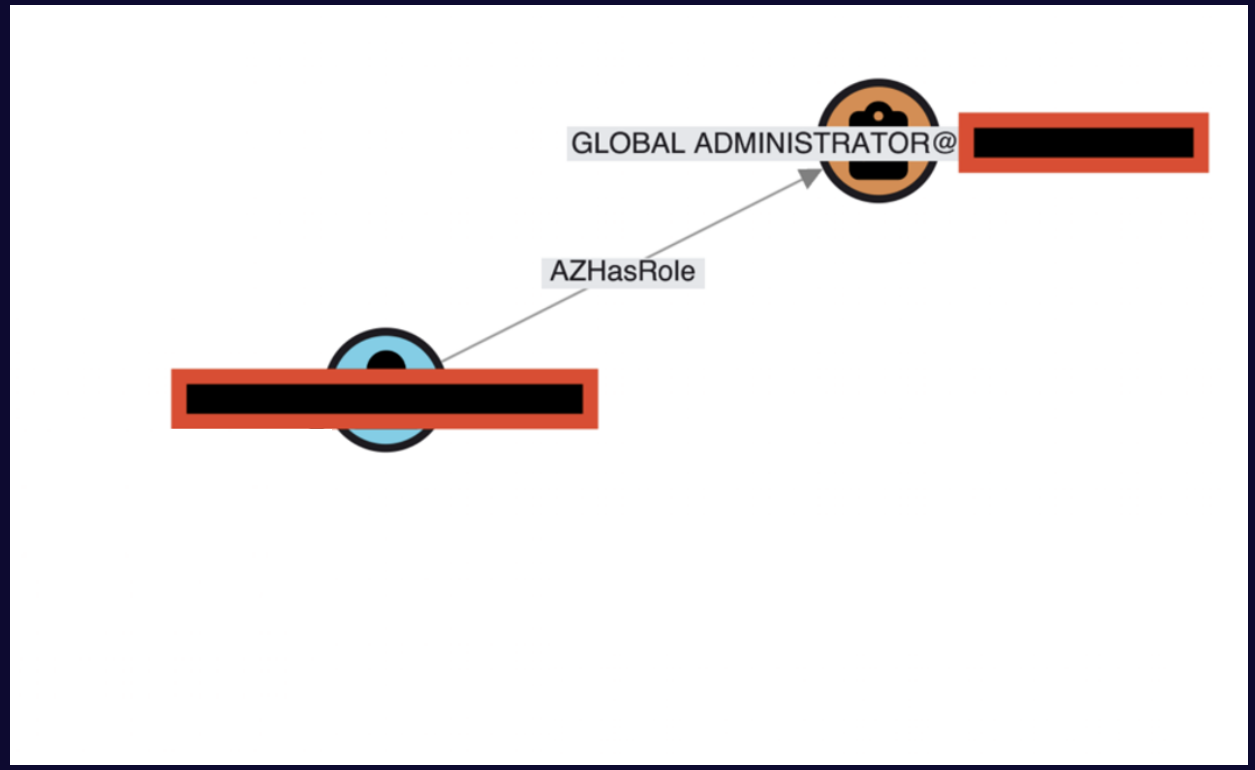




Hybrid Attack Paths

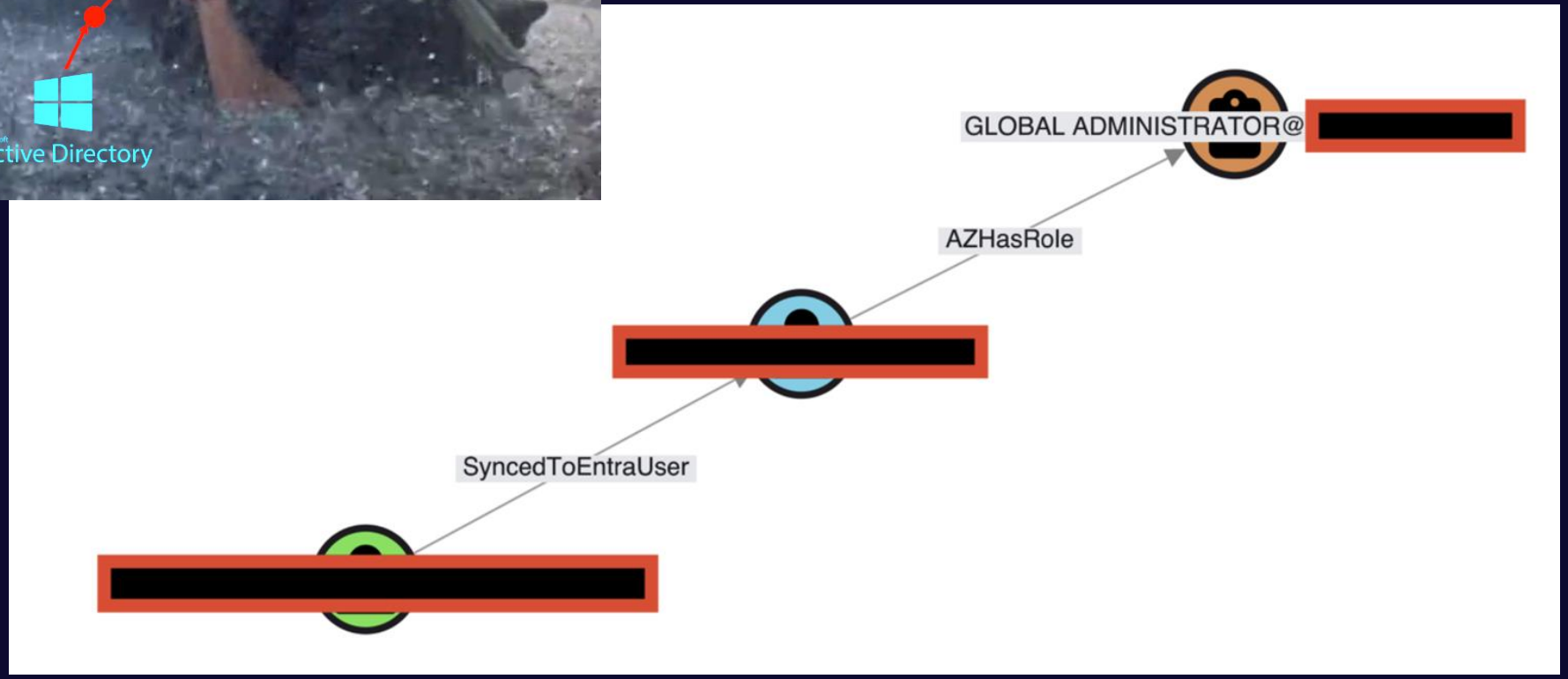


Azure’s biggest security problem is Active Directory



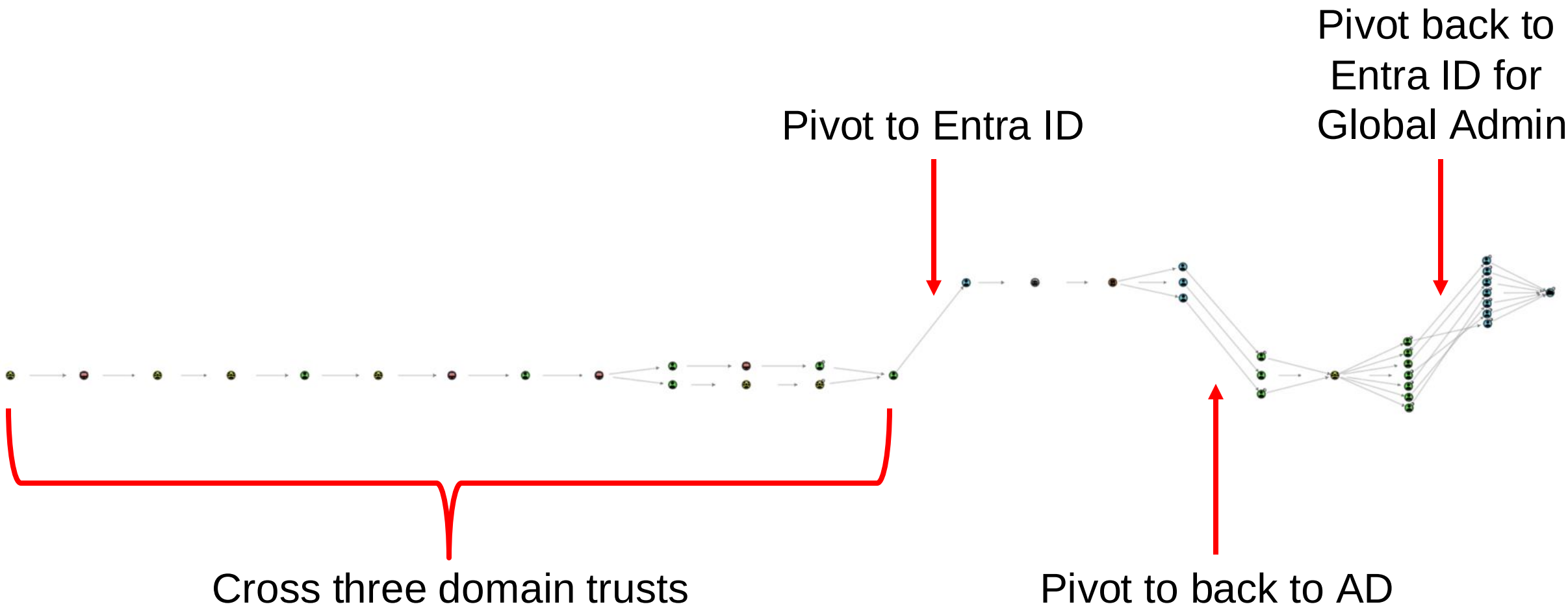
5%

Azure Tier Zero Exposure

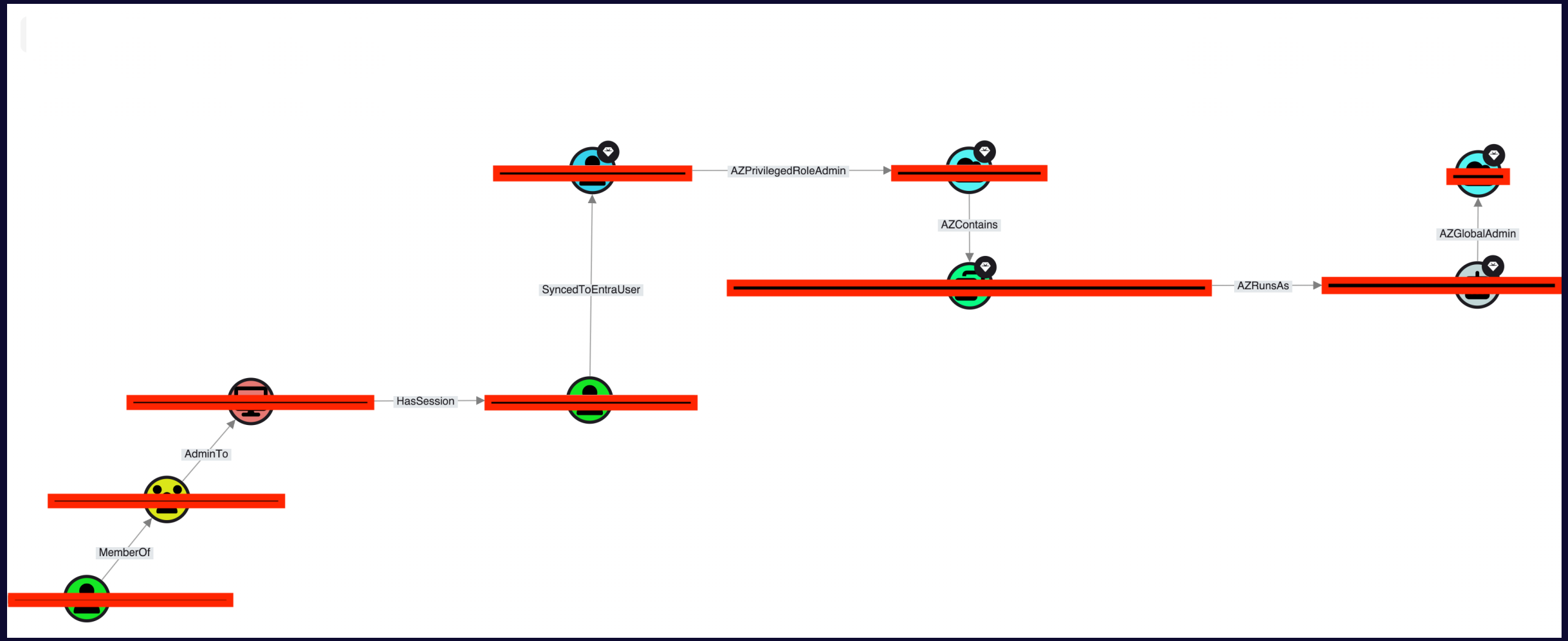


97%

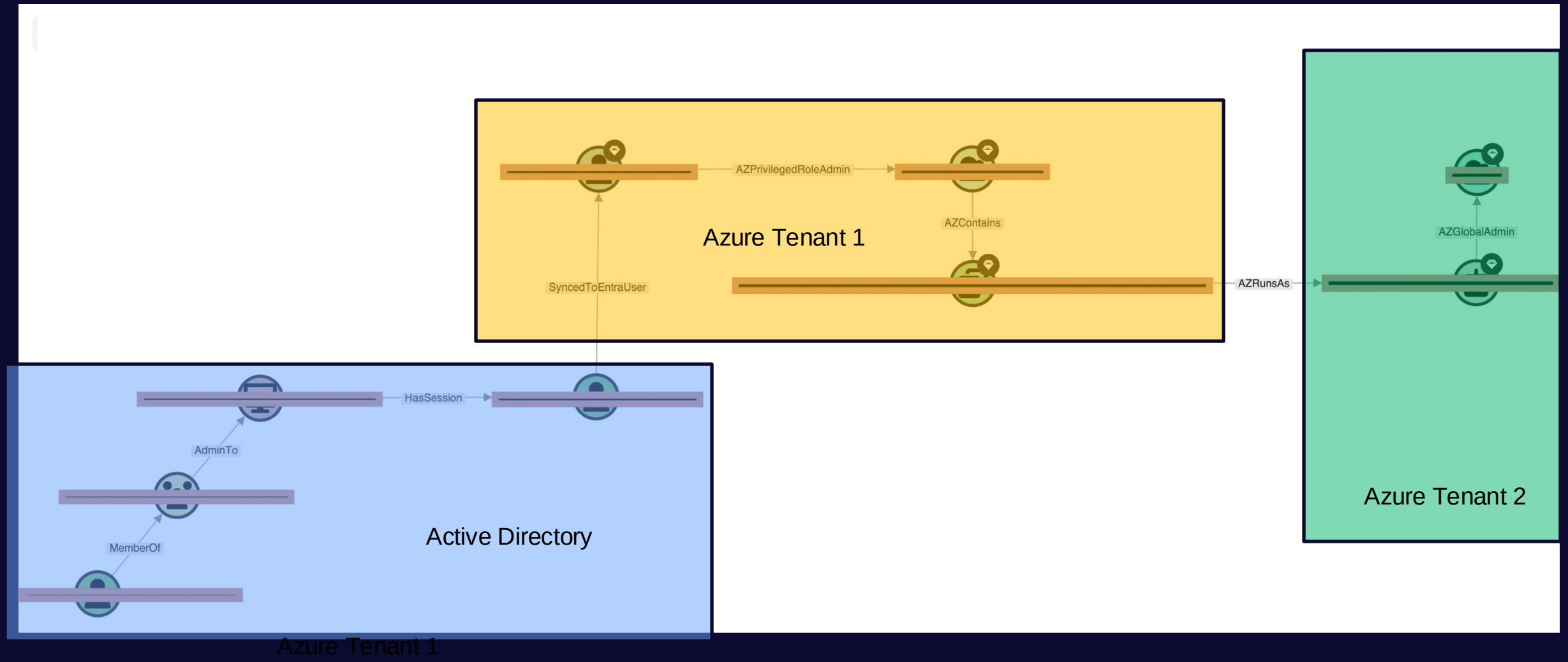
Azure Tier Zero Exposure

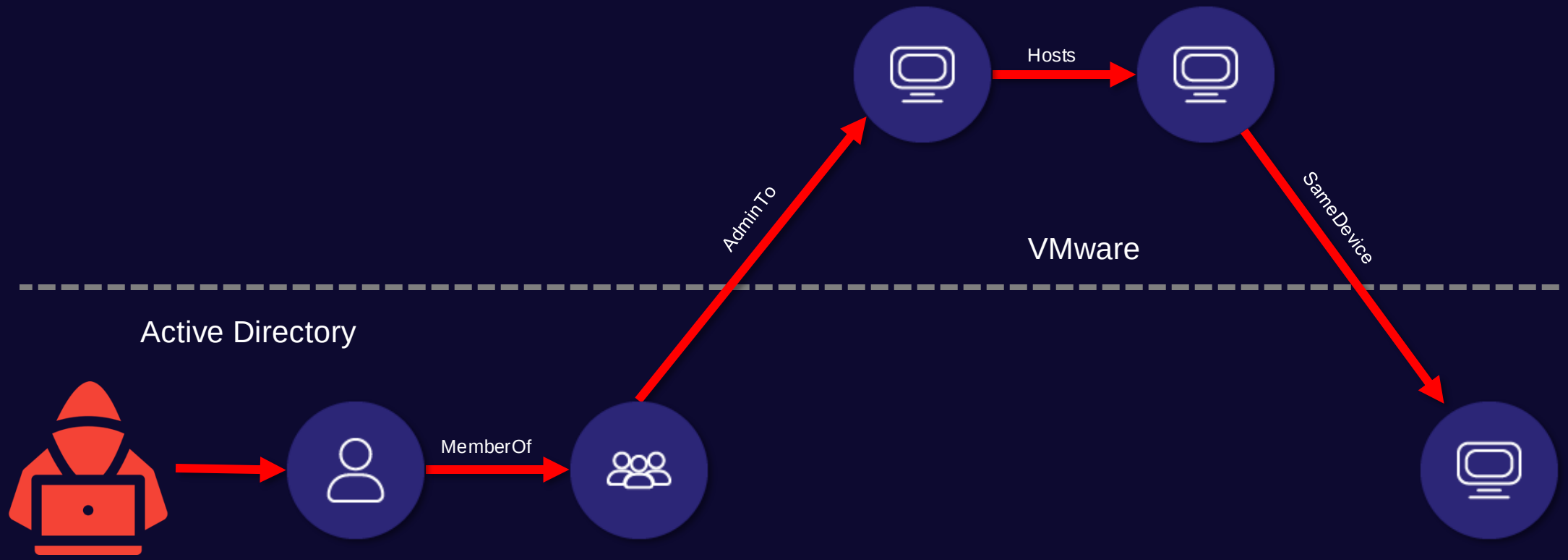

Pivot back to Entra ID for Global Admin
Pivot to Entra ID
Cross three domain trusts
Pivot to back to AD

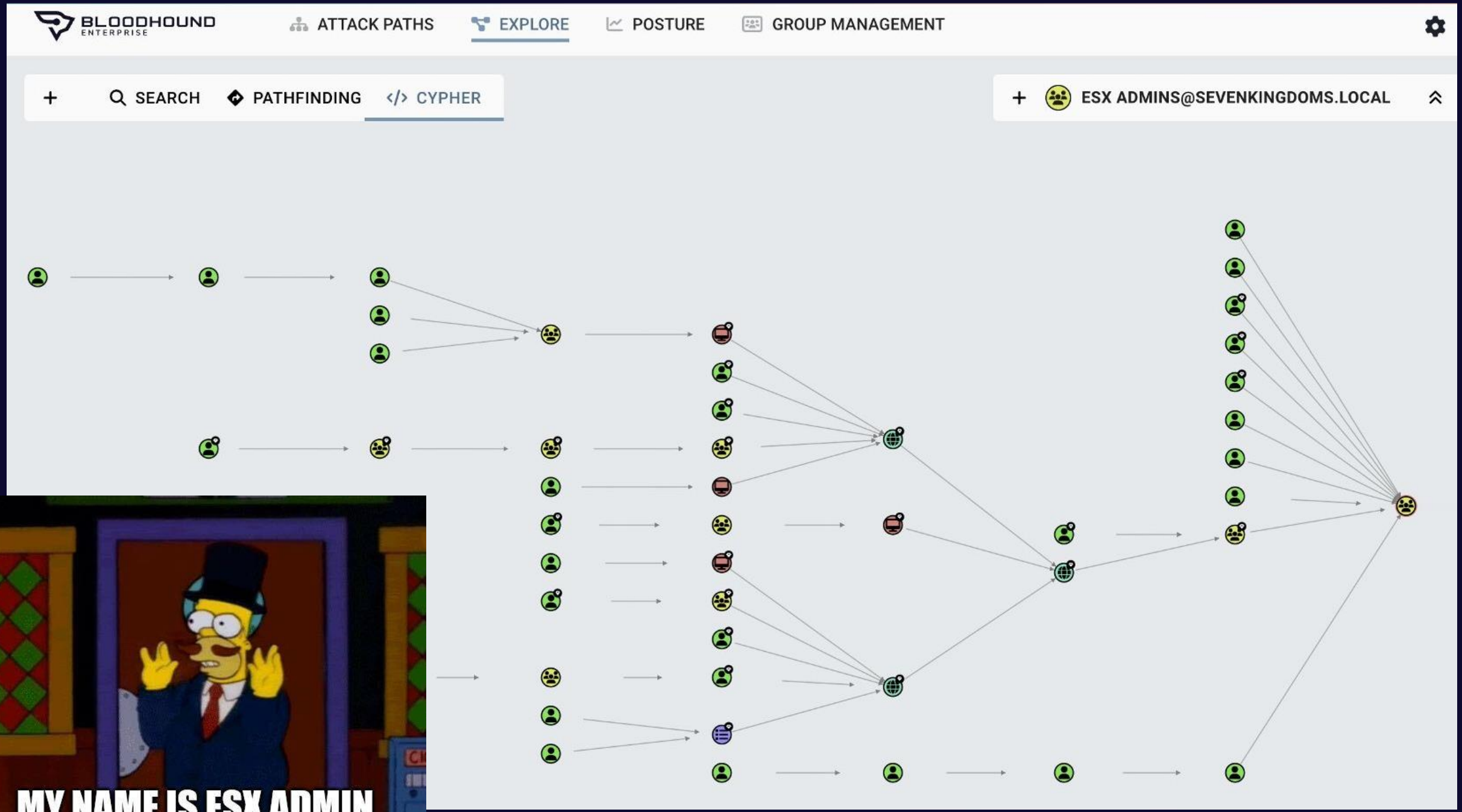
Cross-tenant Attack Paths are a problem

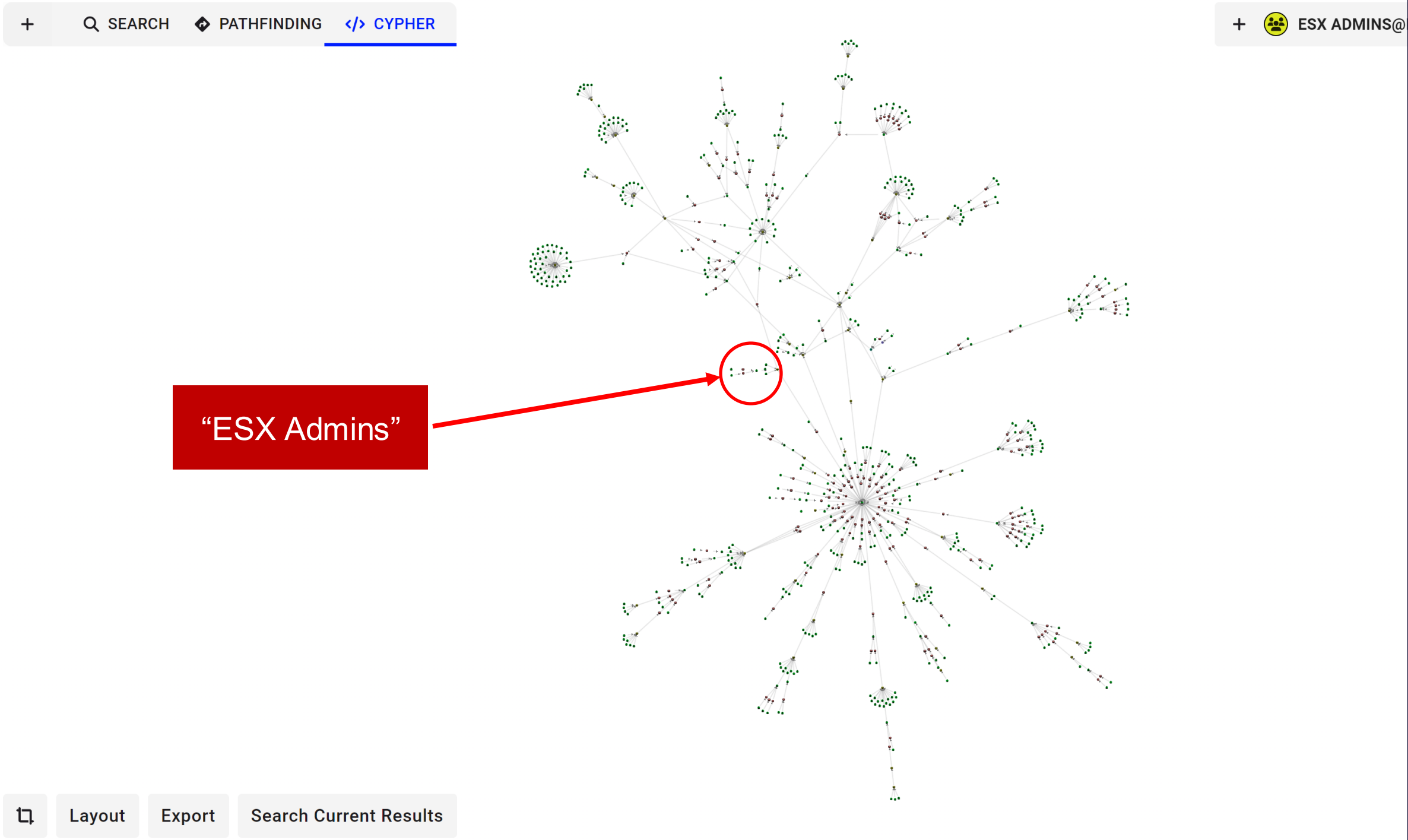


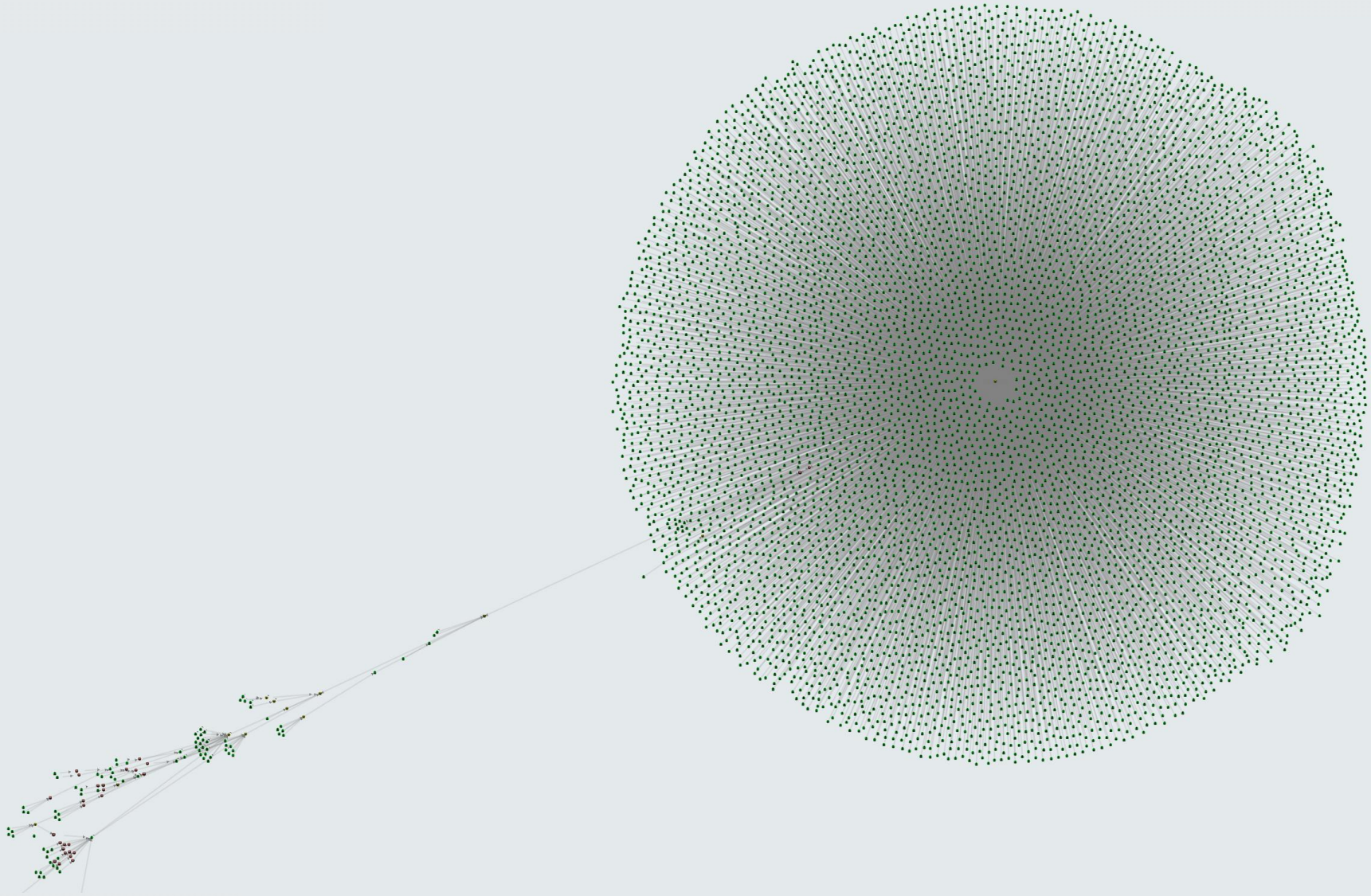
Cross-tenant Attack Paths are a problem

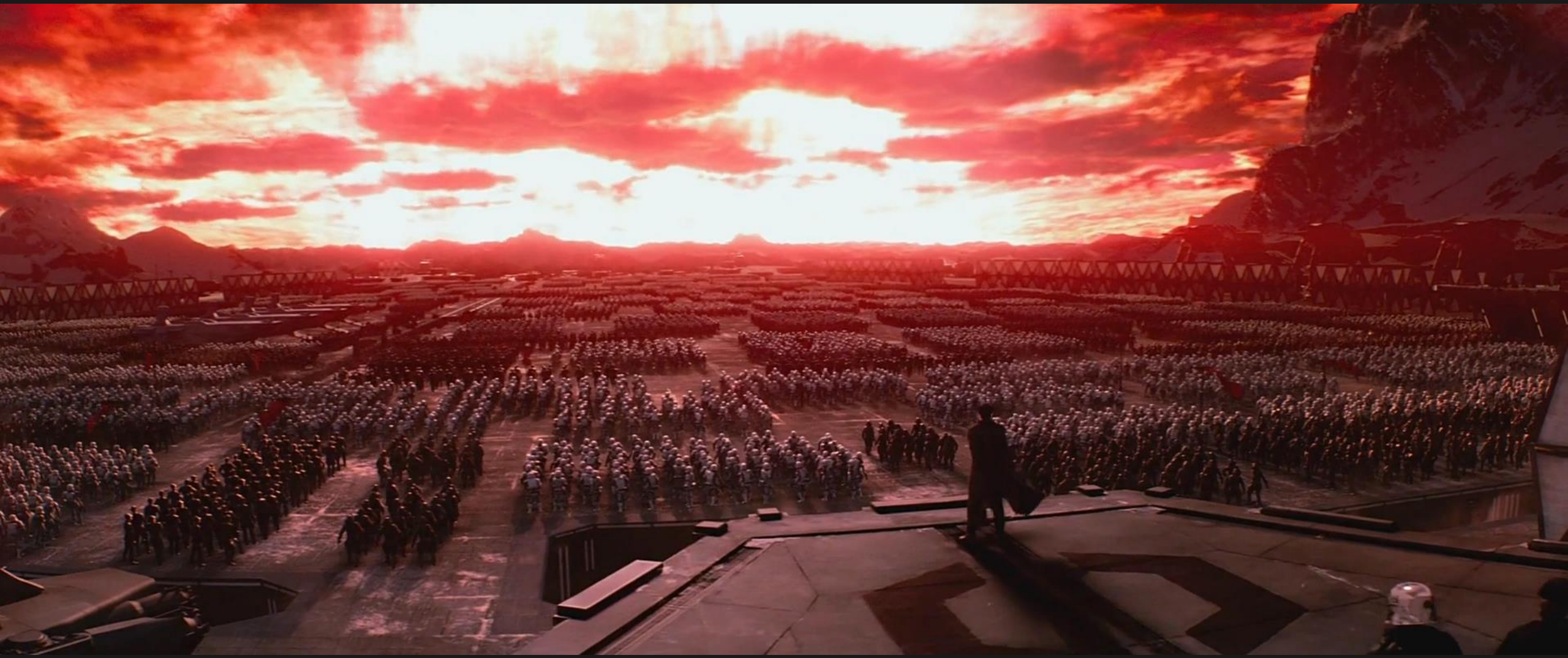



Hosts
AdminTo
SameDevice
VMware
Active Directory
MemberOf


BLOODHOUND
ENTERPRISE
ATTACK PATHS
EXPLORE
POSTURE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
ESX ADMINS@SEVENKINGDOMS.LOCAL
MY NAME IS ESX ADMIN
imgflip.com


SEARCH
PATHFINDING
CYPHER
ESX ADMINS@
"ESX Admins"
Layout
Export
Search Current Results





We are ESX Admins

Your “Least Privilege”

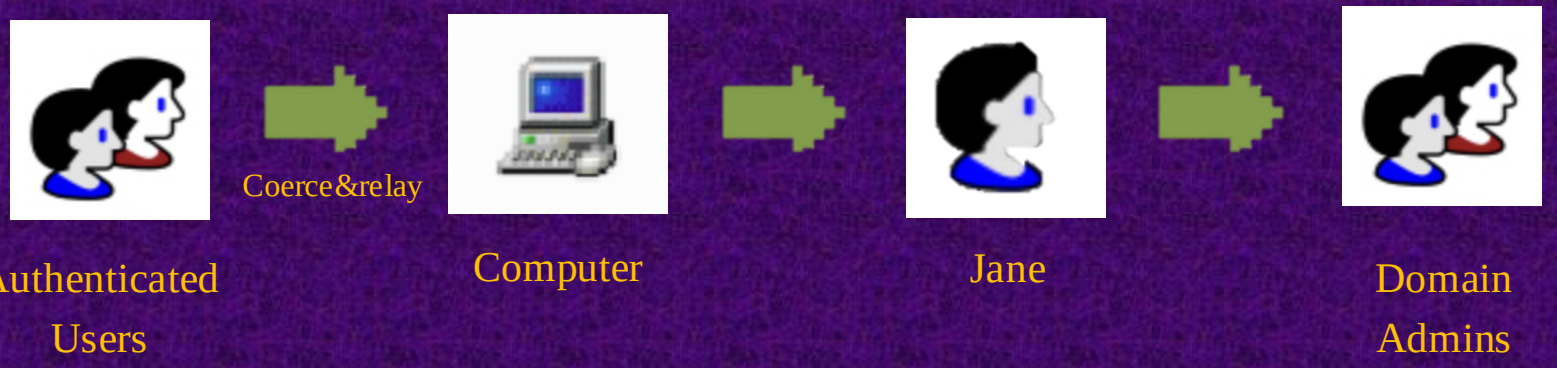
NTLM in BloodHound

NTLM and BloodHound

Fighting 1993 in 2025

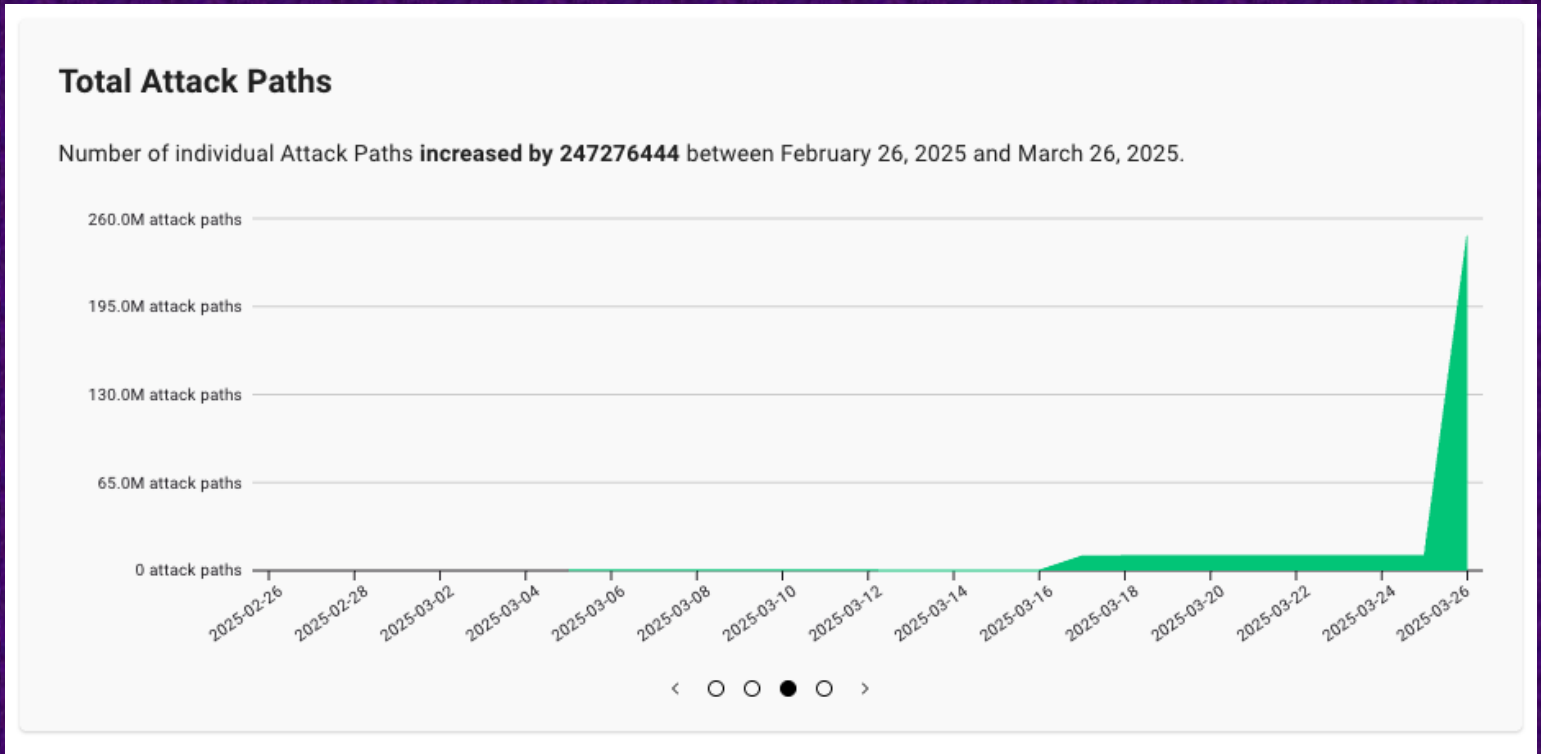
NTLM In BloodHound

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



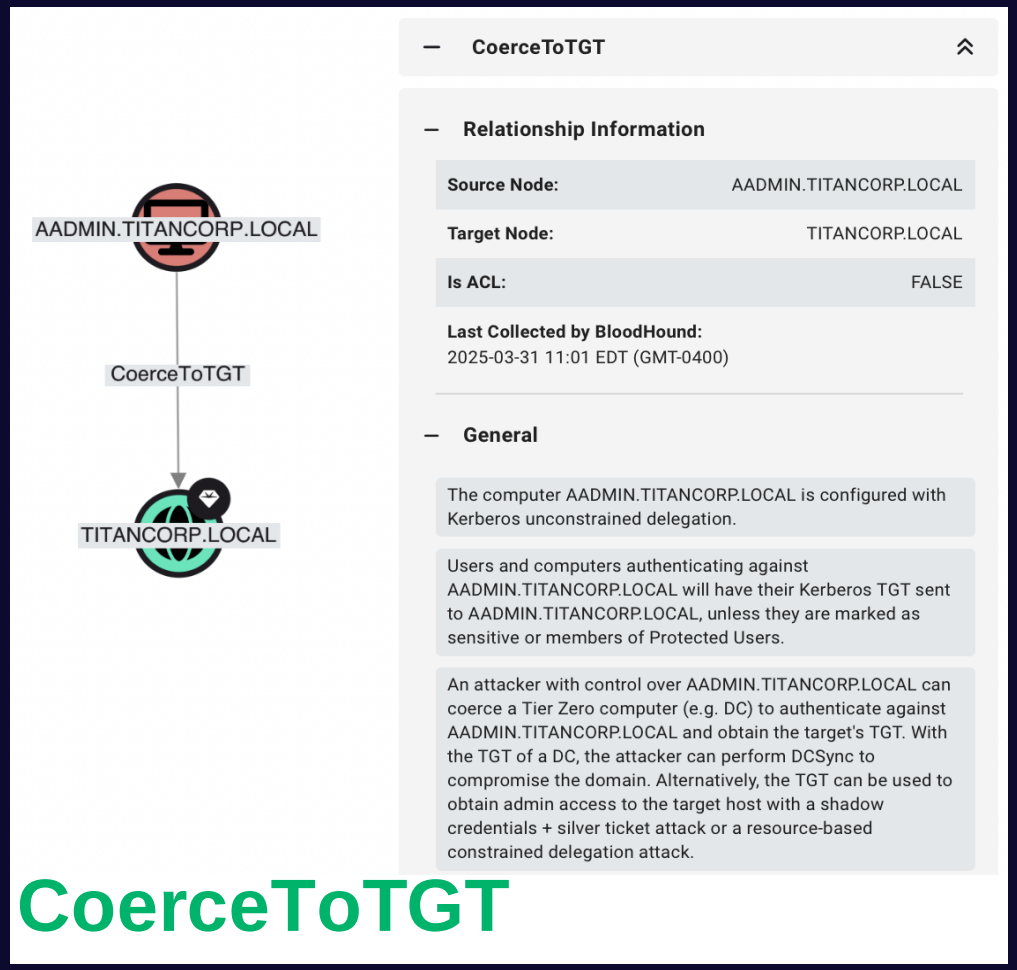
NTLM In BloodHound

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

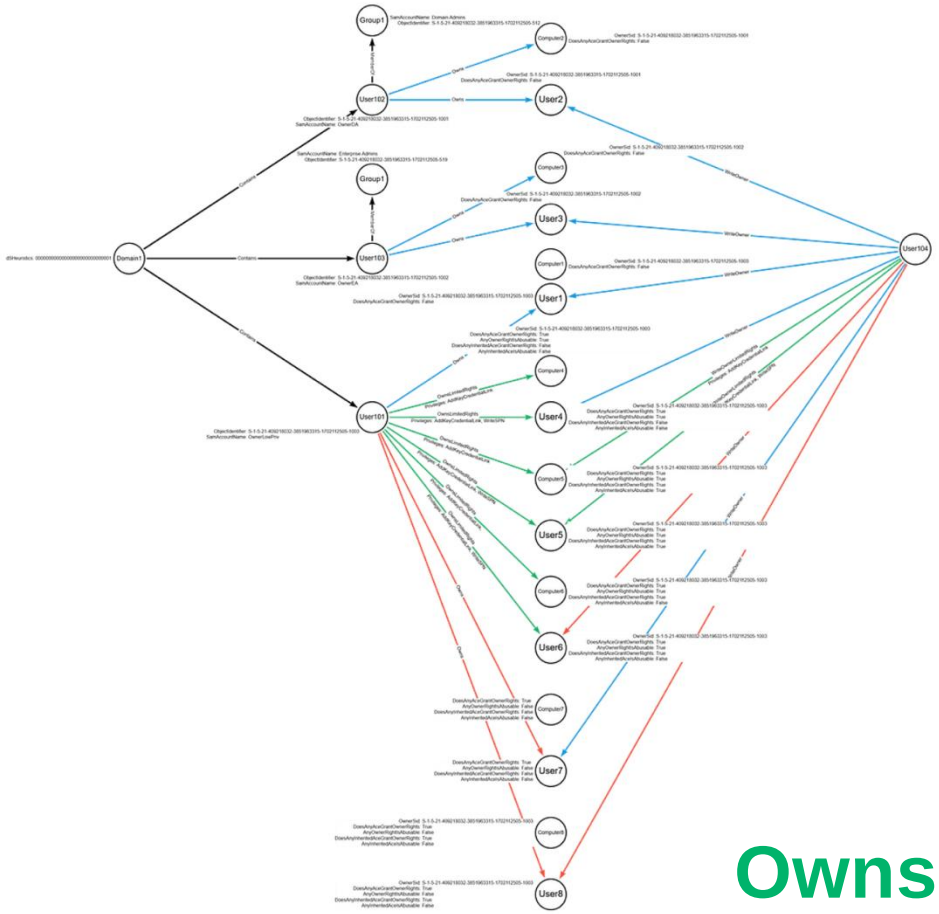


NTLM In BloodHound

Continuous Improvement of the Attack Graph



CoerceToTGT

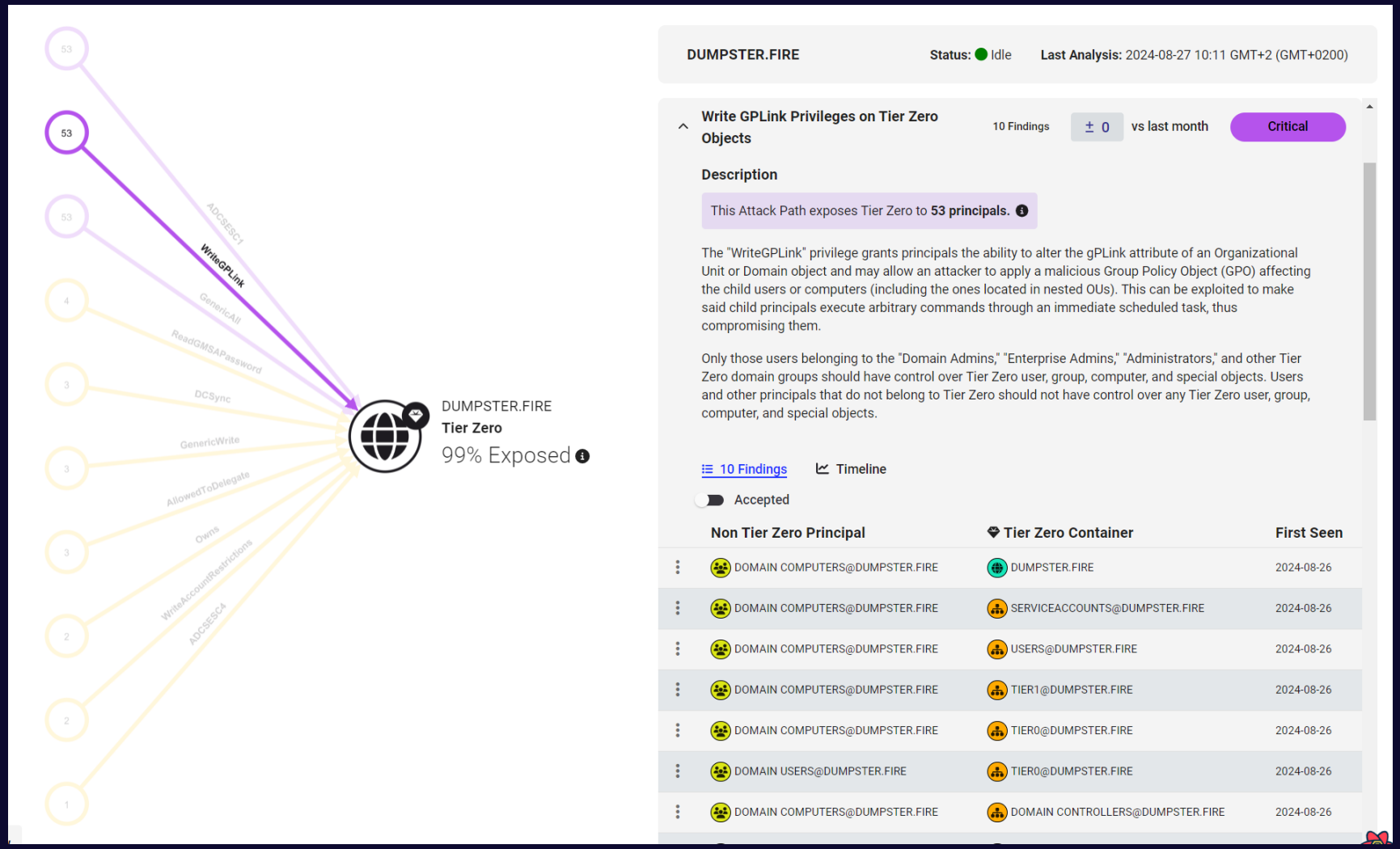


Owns

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

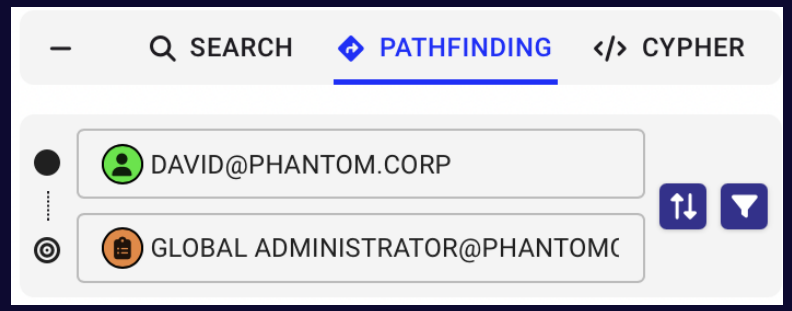
Community contributions to the Attack Graph – Thanks @q-roland




ATTACK PATHS
LIGHTYEAR
ATTACK PATHS EVERYWHERE


ATTACK PATHS
LIGHTYEAR
ATTACK PATHS EVERYWHERE

Dealing with Scale



Database **A**gnostic **W**rapper for **G**raph**s** (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
```

neo4j

PostgreSQL

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
- Spyr0 - 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

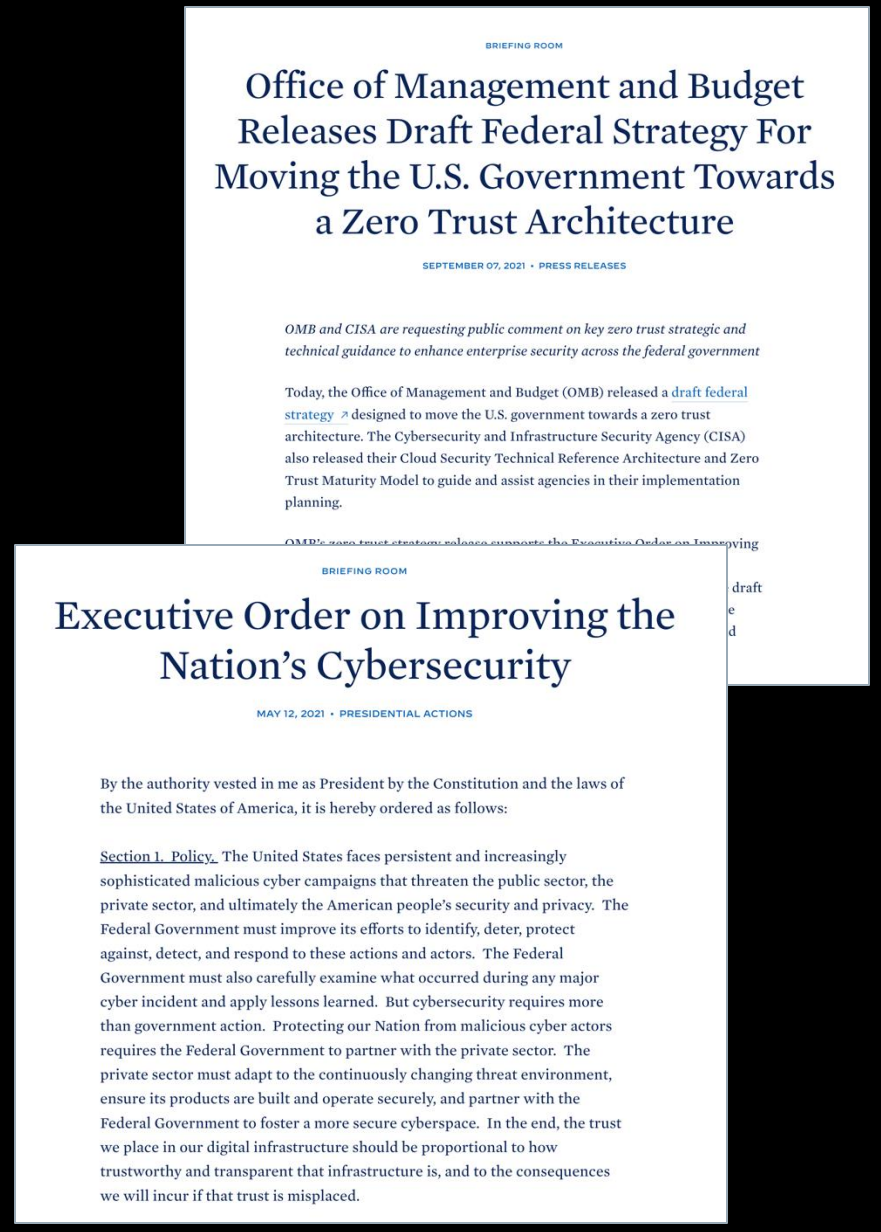
Leverages National Institute of Standards and Technology (NIST) guidelines for uniform security and compliance

FedRAMP™

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.

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:

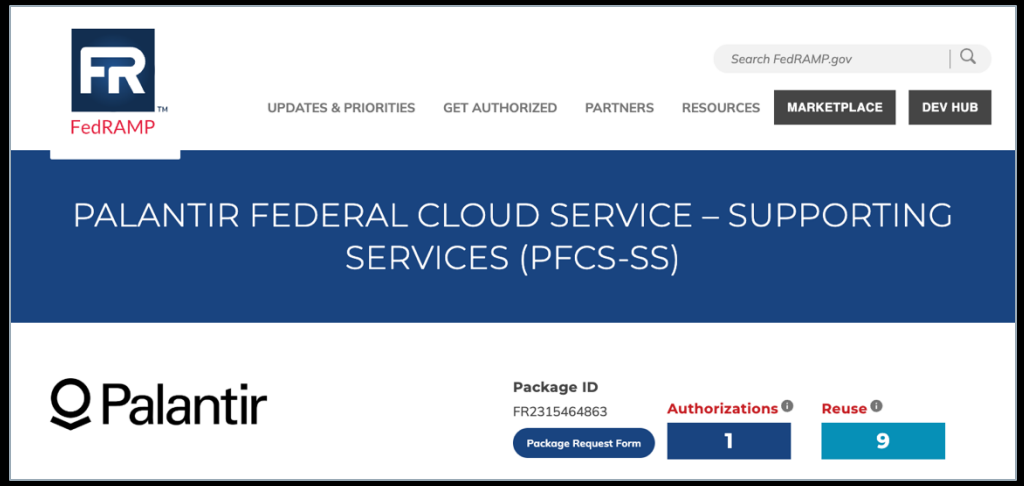
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, 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.

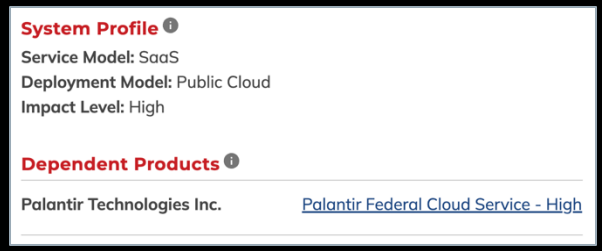
SpecterOps & Palantir FedStart Partnership

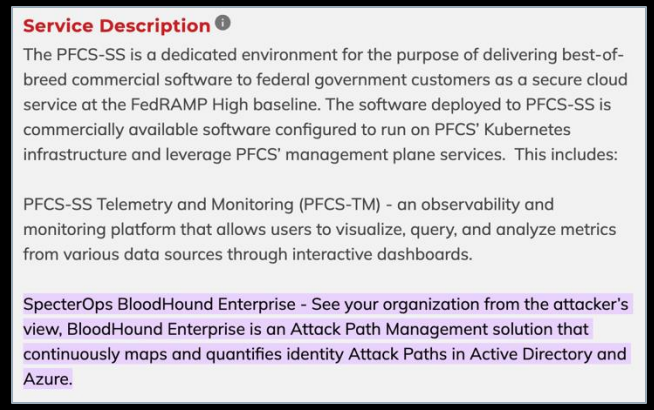
Introducing FedStart

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***







Introducing FedStart

The first FedStart partner

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

BLOODHOUND ENTERPRISE

SPECTEROPS

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

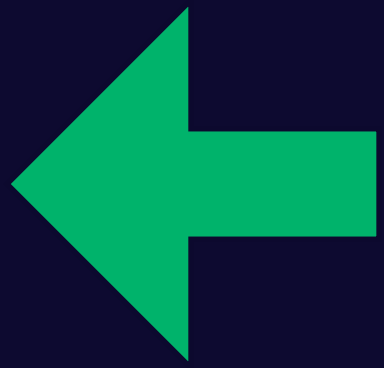
FedRAMP® Benefits

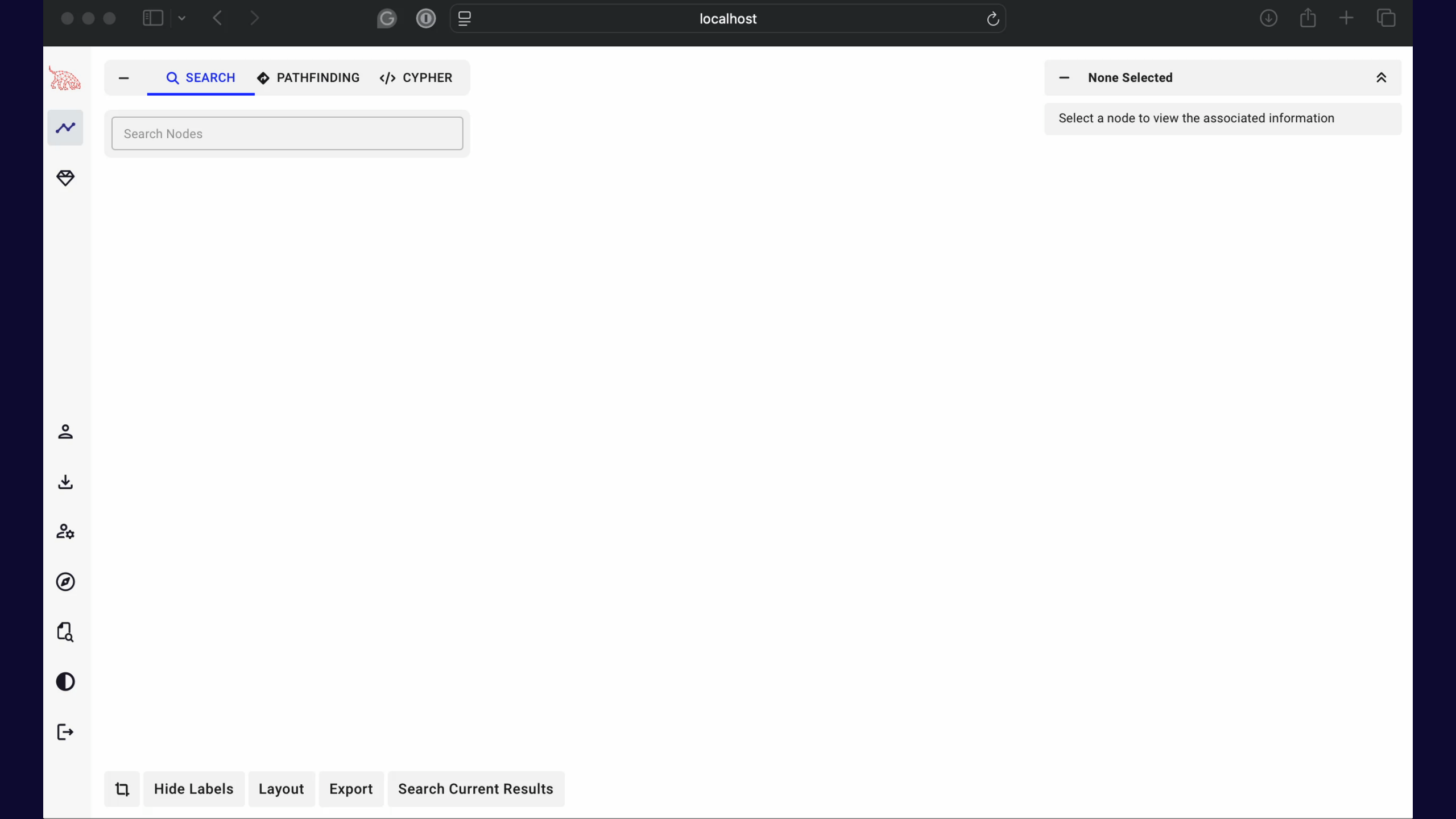
Support our Federal Agencies

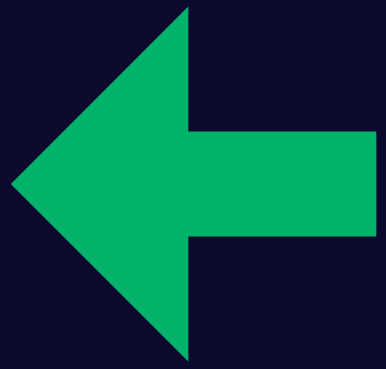
Support enterprise clients with federal data

Learn more: info@specterops.io / specterops.io/industry-public-sector
See the Authorizatio & ATO: https://marketplace.fedramp.gov/products/FR2315464863

One more thing…




localhost
SEARCH
PATHFINDING
CYPHER
Search Nodes
None Selected
Select a node to view the associated information
Hide Labels
Layout
Export
Search Current Results



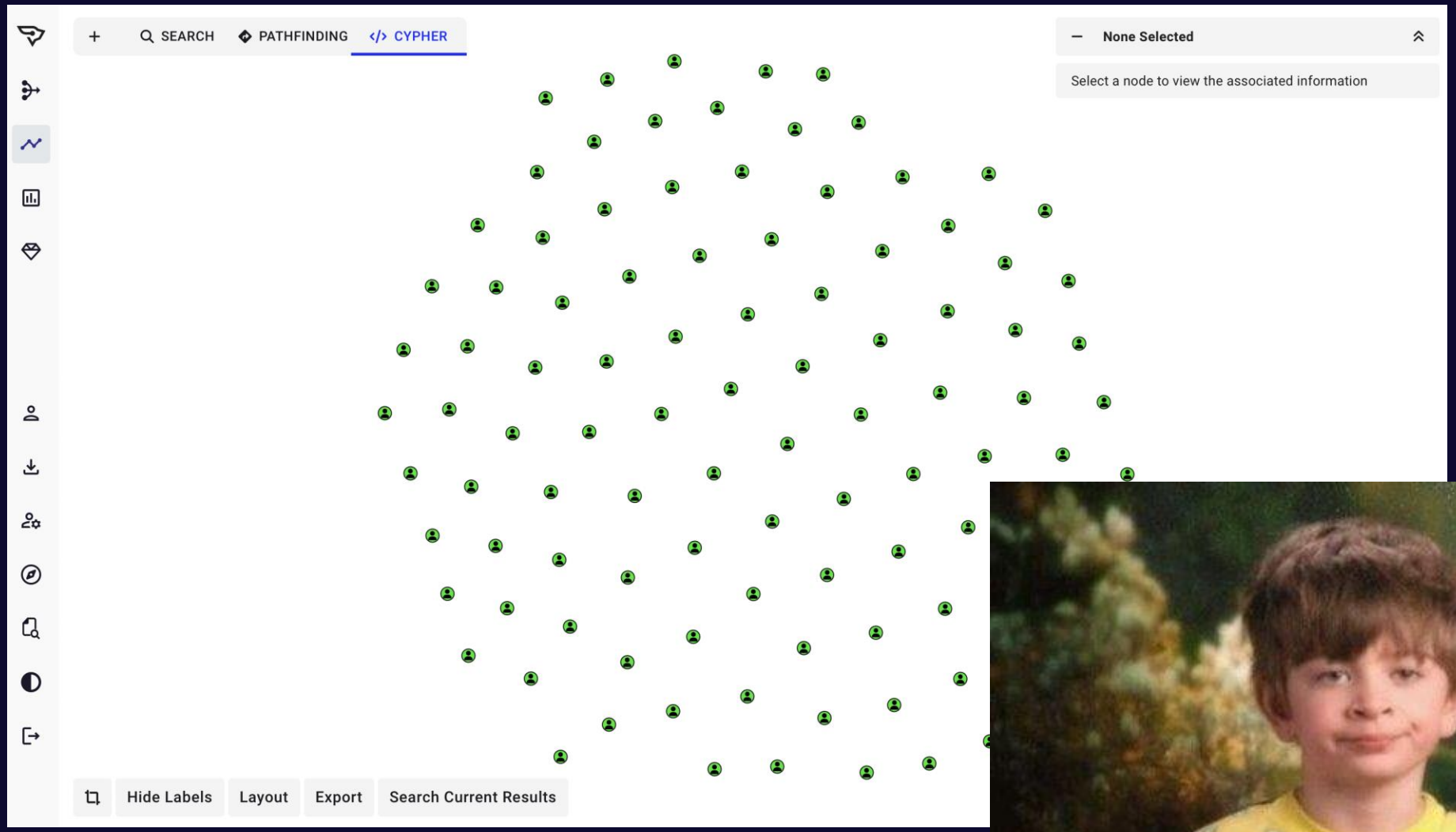
I’m sorry it’s taken this long

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	TRU	
	GMSA_SHS$@DUM...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRU	
	GGOOFBALL@TITANC...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FAL	
	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FAL	
	BIN.DUMPSTER.FIRE	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRU	
	GMSA_SHS$@DUM...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	TRU	
	GGOOFBALL@TITANC...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FAL	
	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FAL	
	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	TRU	
	SVCCAAD@TITANCOR...	TESTLAB.LOCAL-S-1-5-32-544	2021-04-14 14:57 EDT (GMT-0400)	S-1-5-21-3130019616	TRUE	FALSE	FAL	

Defenders can think in graphs

but sometimes interpret results in lists

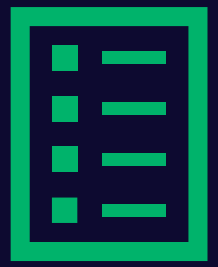
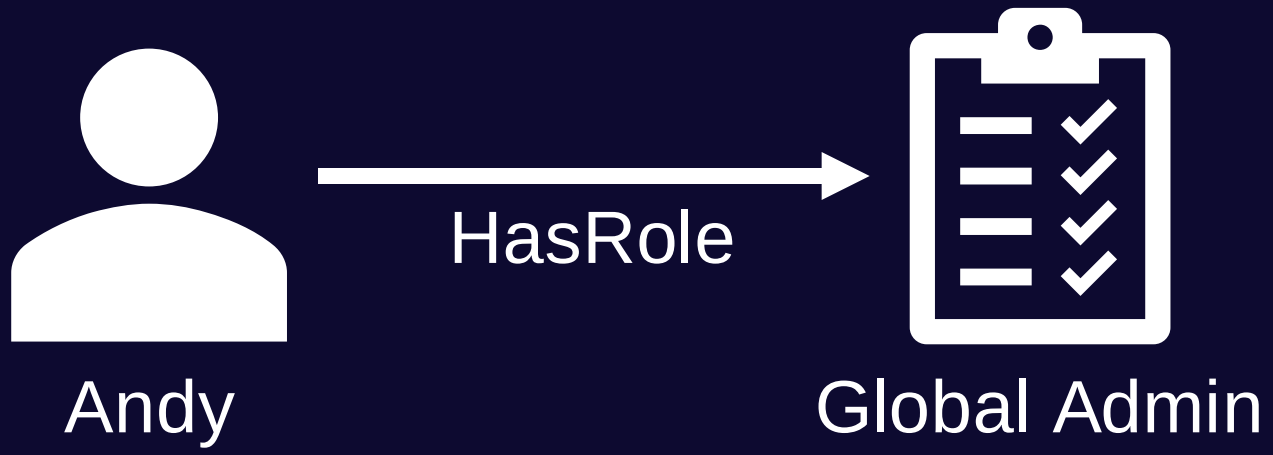
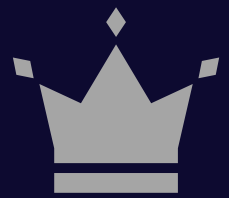
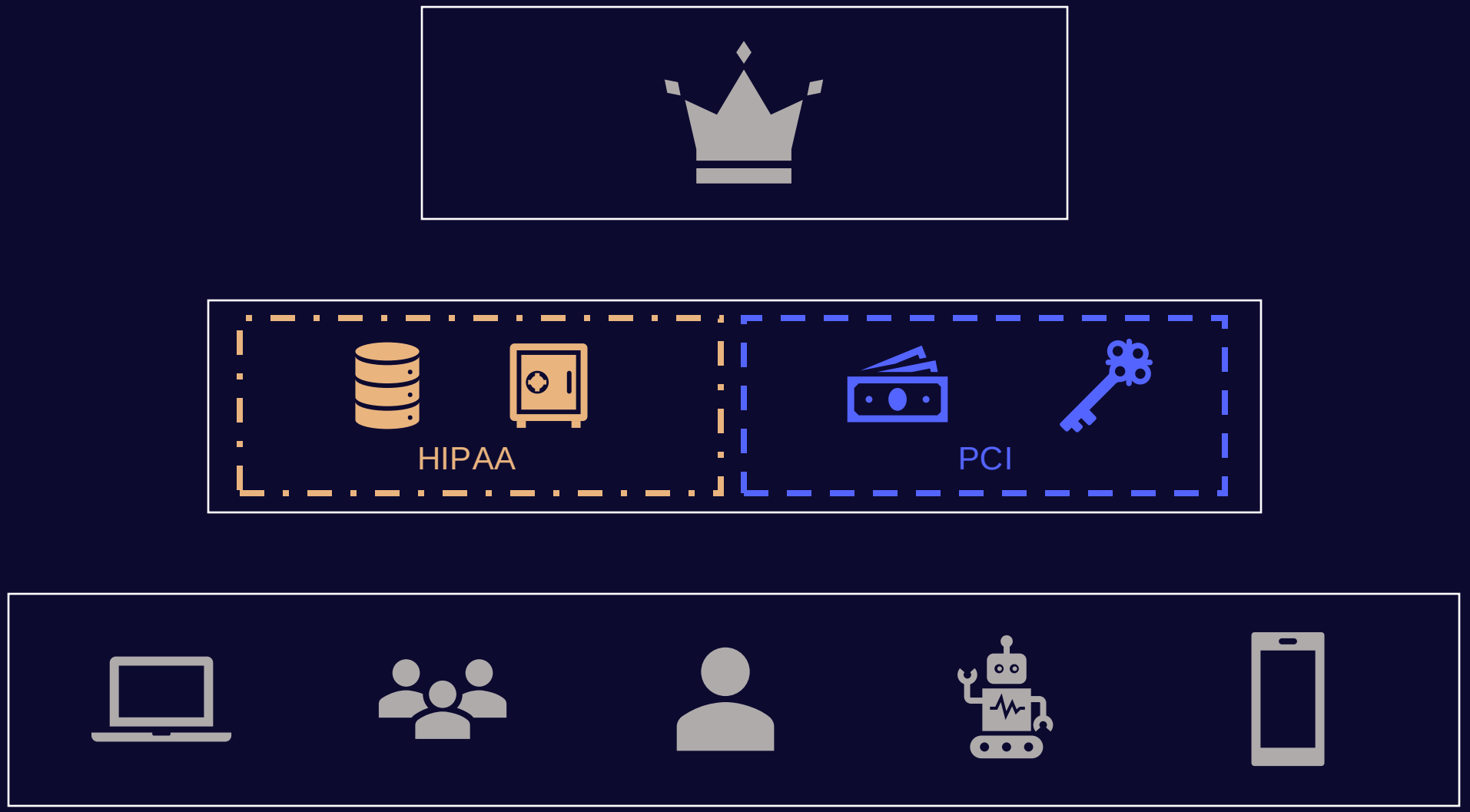


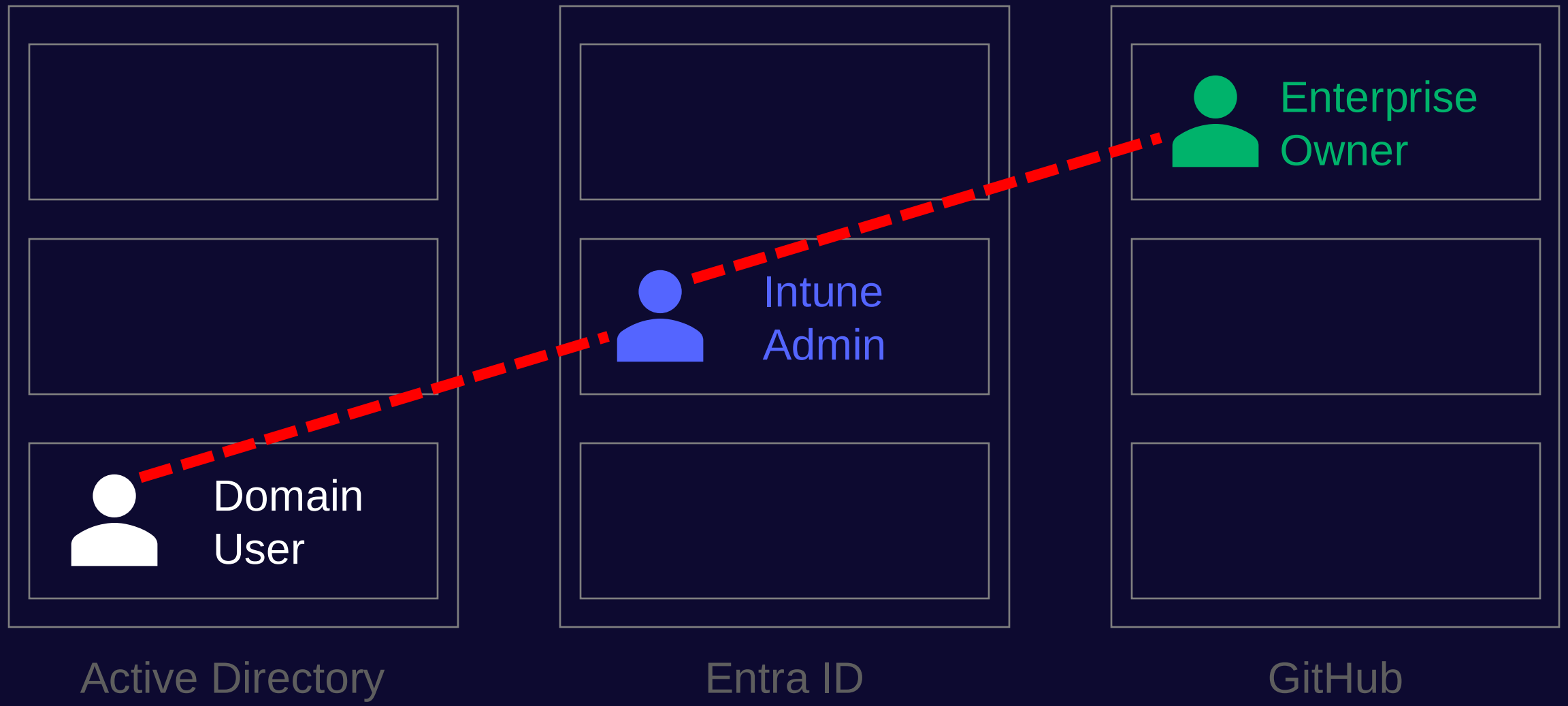
Table View Coming this Summer

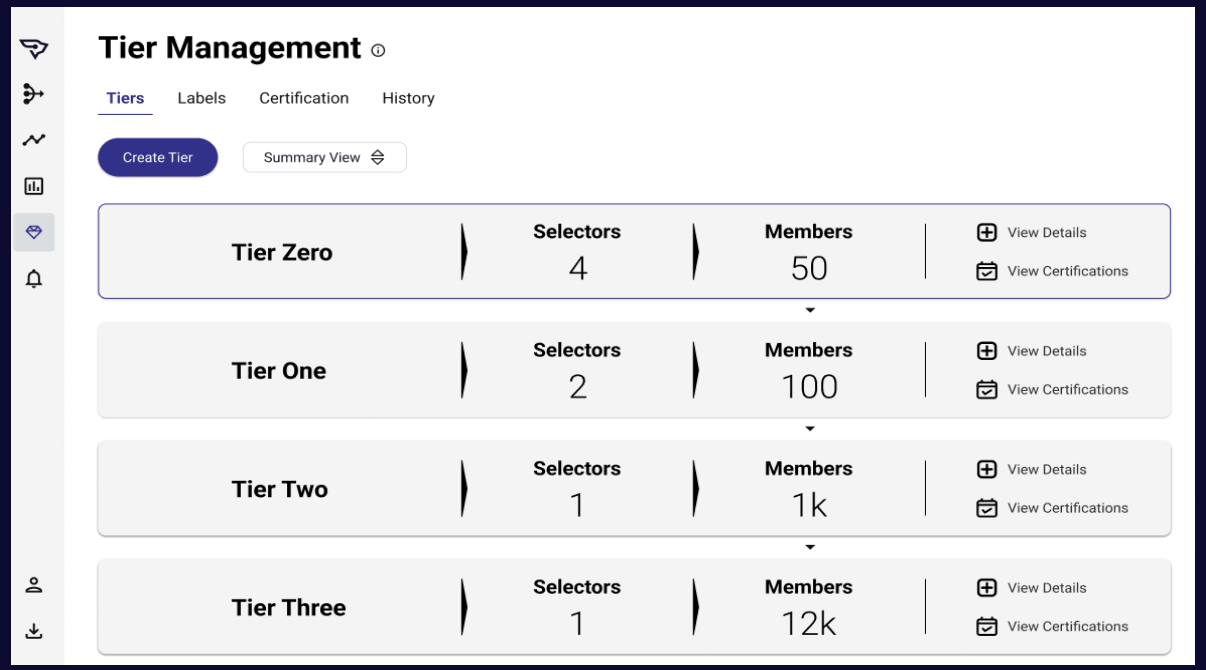

HasRole
Andy
Global Admin

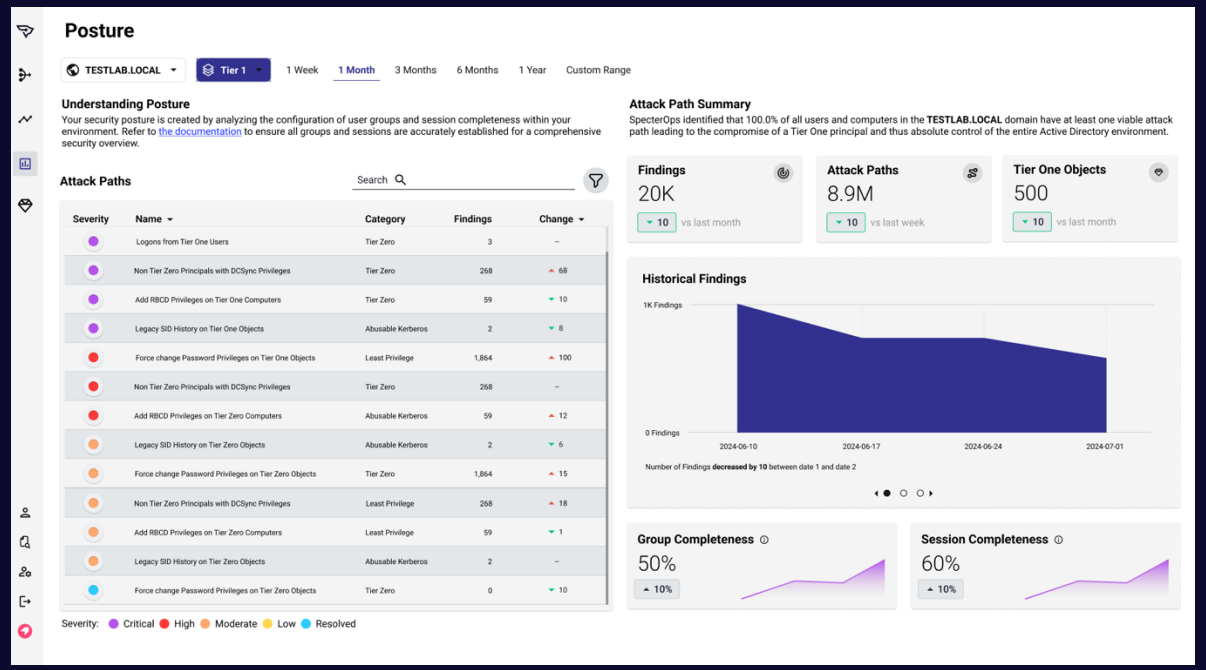
PIM Roles coming this summer




HIPAA
PCI

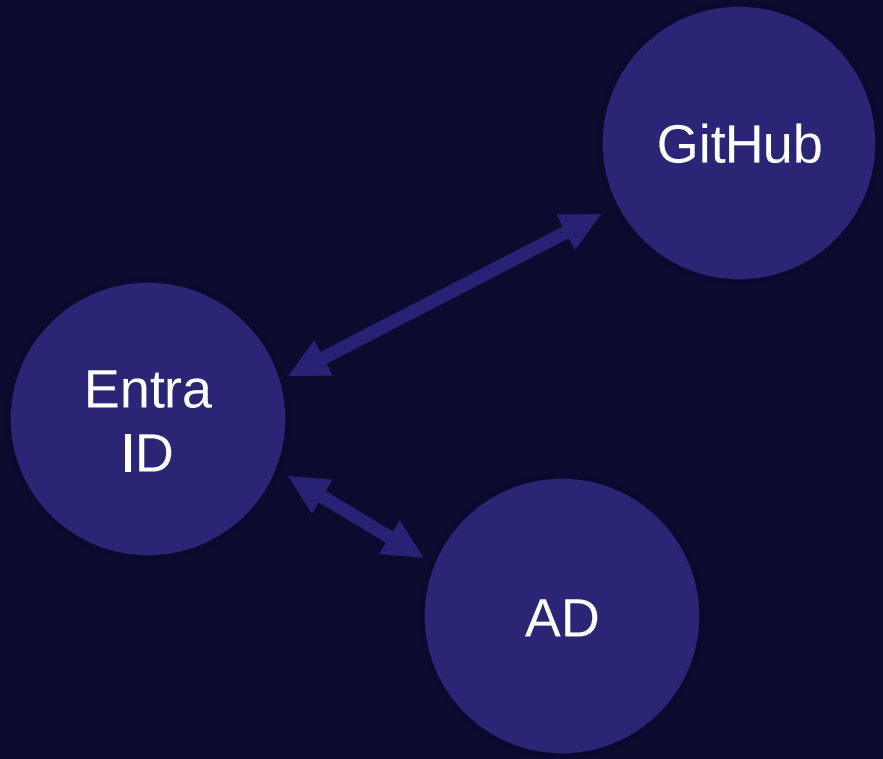

Enterprise
Owner
Intune
Admin
Domain
User
Active Directory
Entra ID
GitHub

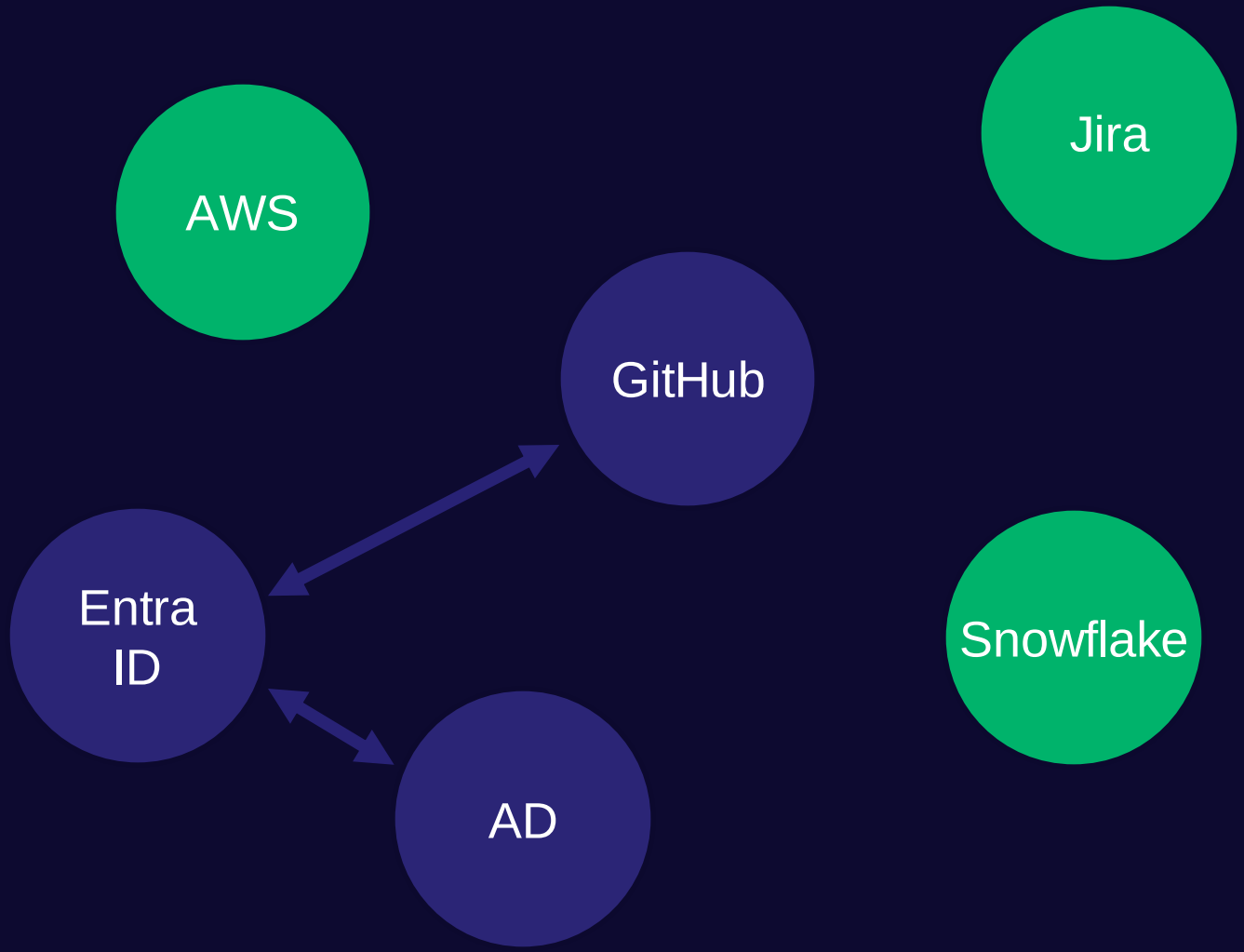




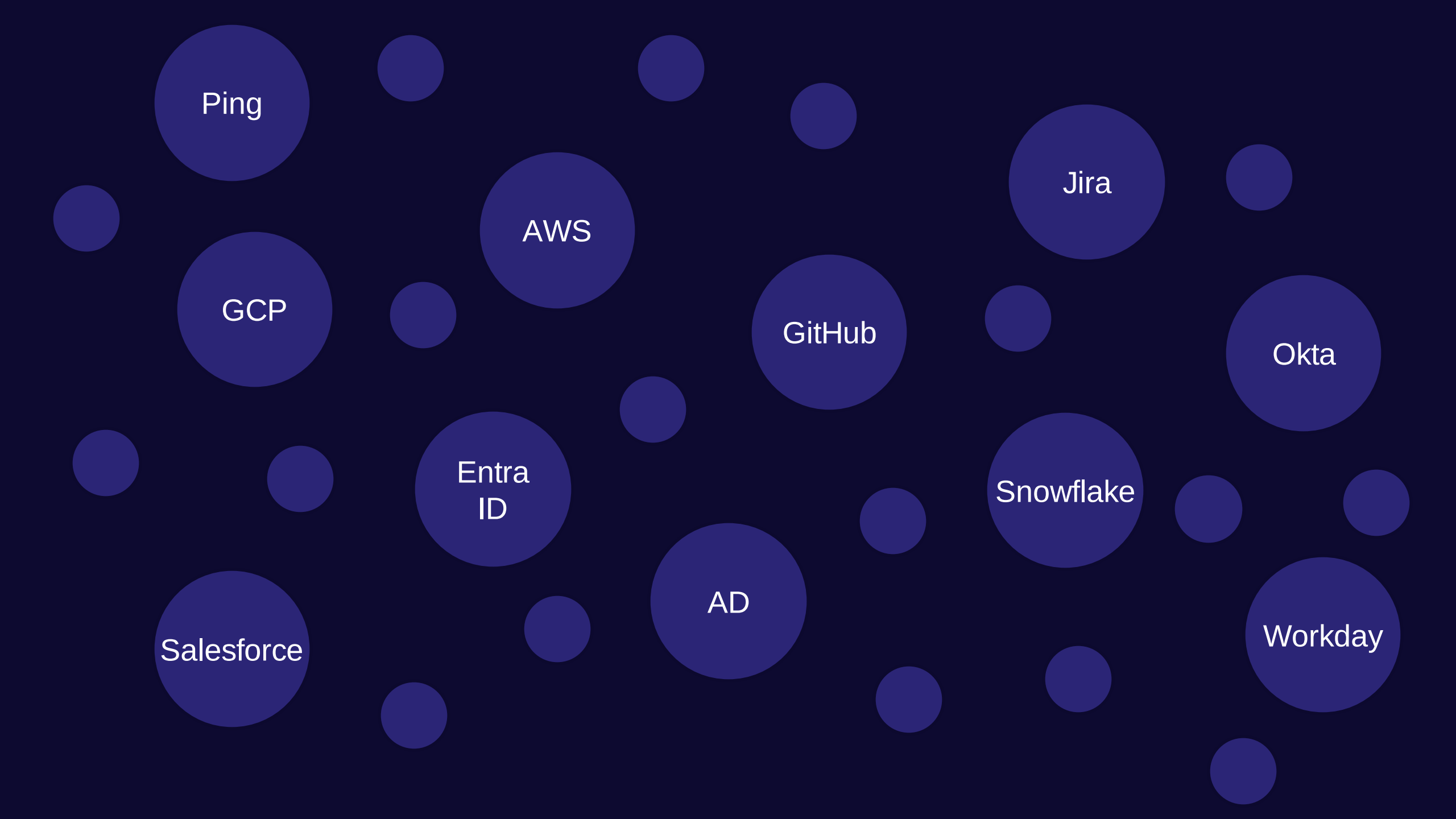
Multi-Tier Management and Analysis Coming this Summer

But when are you going to _____?


GitHub
Entra
ID
AD


AWS
Jira
GitHub
Entra
ID
Snowflake
AD


Ping
AWS
Jira
GCP
GitHub
Okta
Entra
ID
Snowflake
AD
Salesforce
Workday


Ping
AWS
Jira
GCP
GitHub
Okta
Entra
ID
Snowflake
AD
Salesforce
Workday

BloodHound is where Attack Path research is done

BloodHound is where [AD] Attack Path research is done

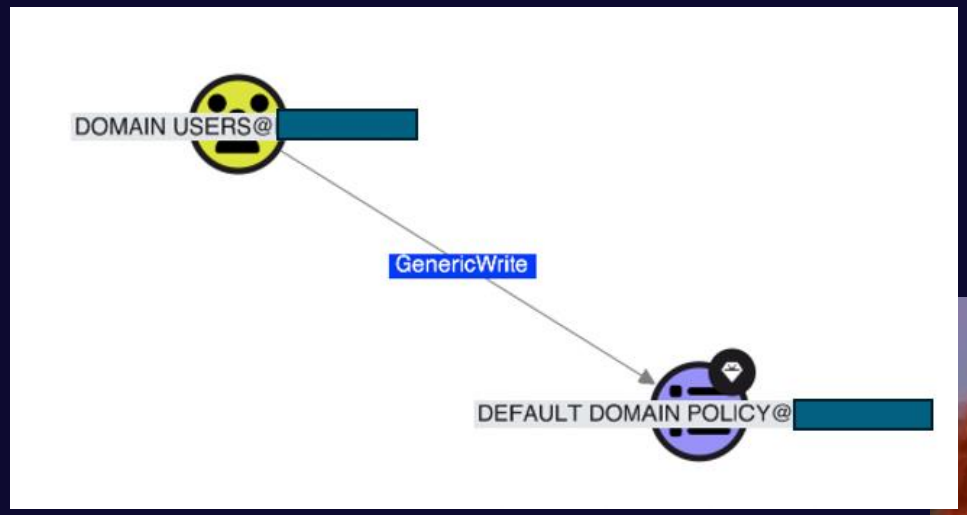
BloodHound is where [Azure] Attack Path research is done

BloodHound is where [GitHub] Attack Path research is done

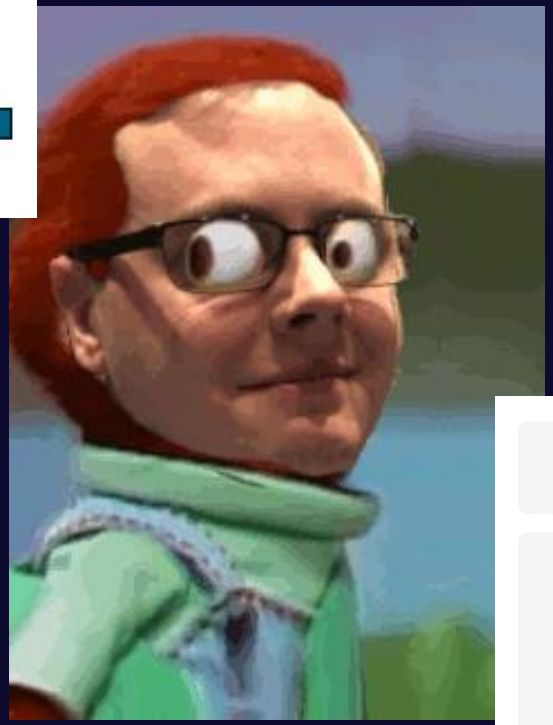
BloodHound is where [AWS] Attack Path research is done

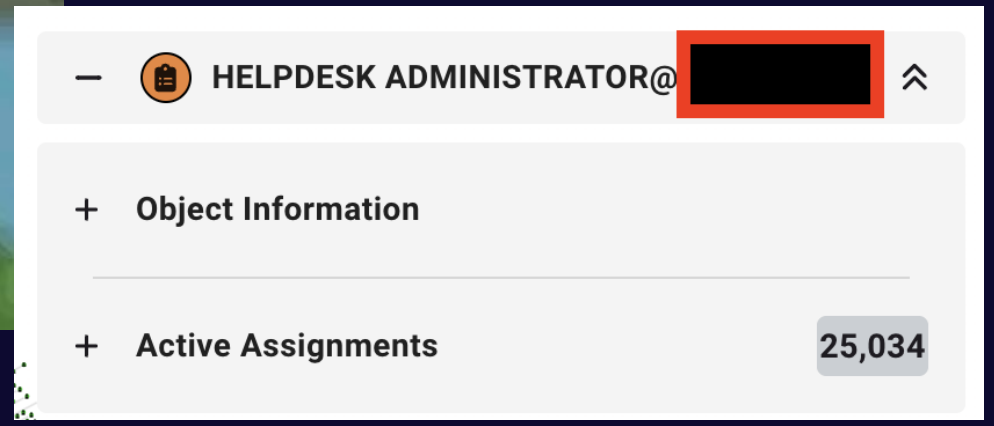
BloodHound is where [Okta] Attack Path research is done

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



Meanwhile…..
we still have a lot to fix





SPECTEROPS

Questions

Justin Kohler, Chief Product Officer