



# Exposing Hidden Attack Paths: How Threats Get Past Your Best Defenses

Justin Kohler  
Chief Product Officer

# A Quick Shoutout to Dirk-Jan Mollema



 Pinned

 **Dirk-Jan**  
@\_dirkjan Follow  

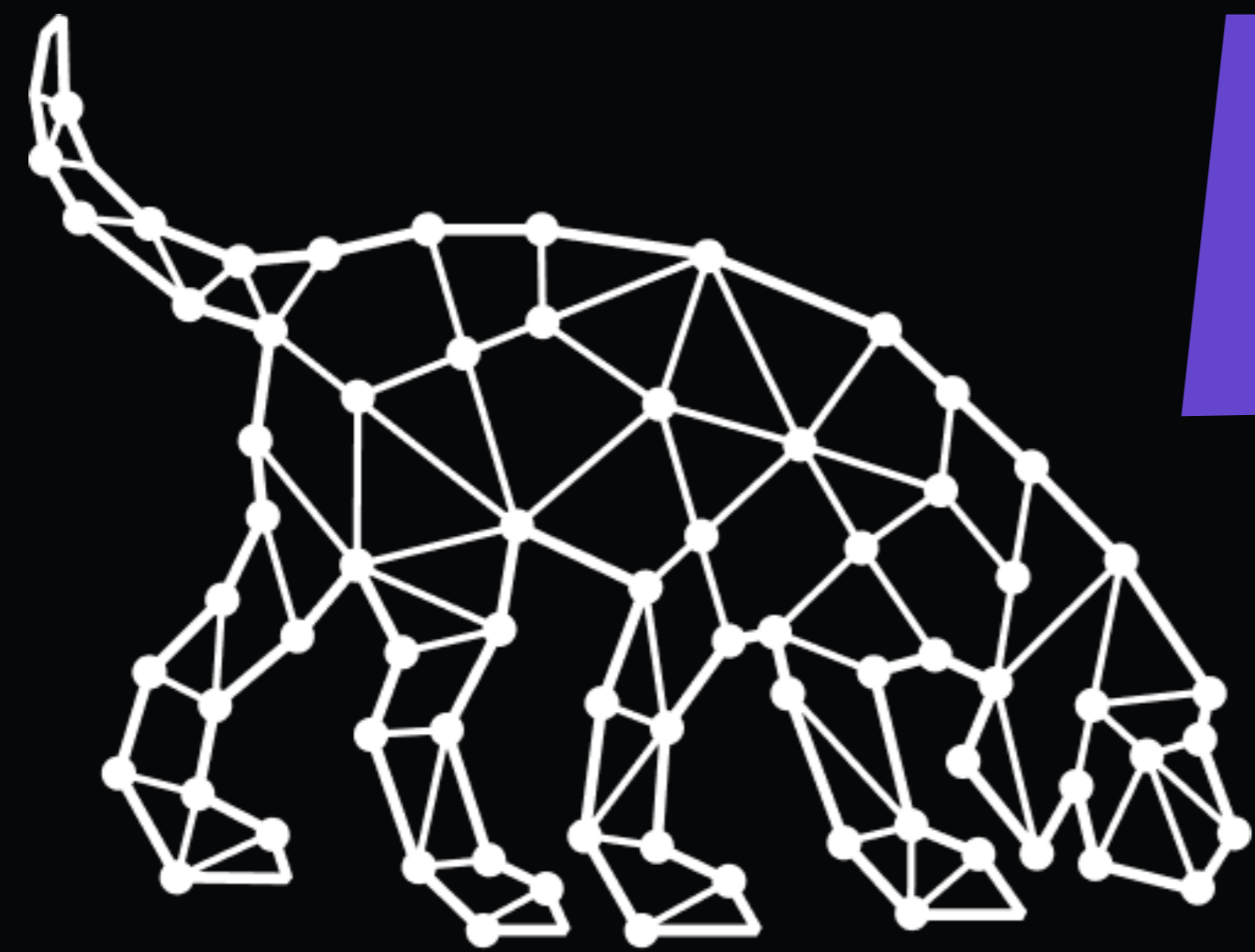
I've been researching the Microsoft cloud for almost 7 years now. A few months ago that research resulted in the most impactful vulnerability I will probably ever find: a token validation flaw allowing me to get Global Admin in any Entra ID tenant. Blog:

 [dirkjanm.io](https://dirkjanm.io)  
**One Token to rule them all - obtaining Global Ad...**  
While preparing for my Black Hat and DEF CON talks in July of this year, I found the most ...

6:20 AM · Sep 17, 2025 · **424.3K** Views

 142  988  3K  1.4K 

<https://dirkjanm.io/obtaining-global-admin-in-every-entra-id-tenant-with-actor-tokens/>



BLOODHOUND

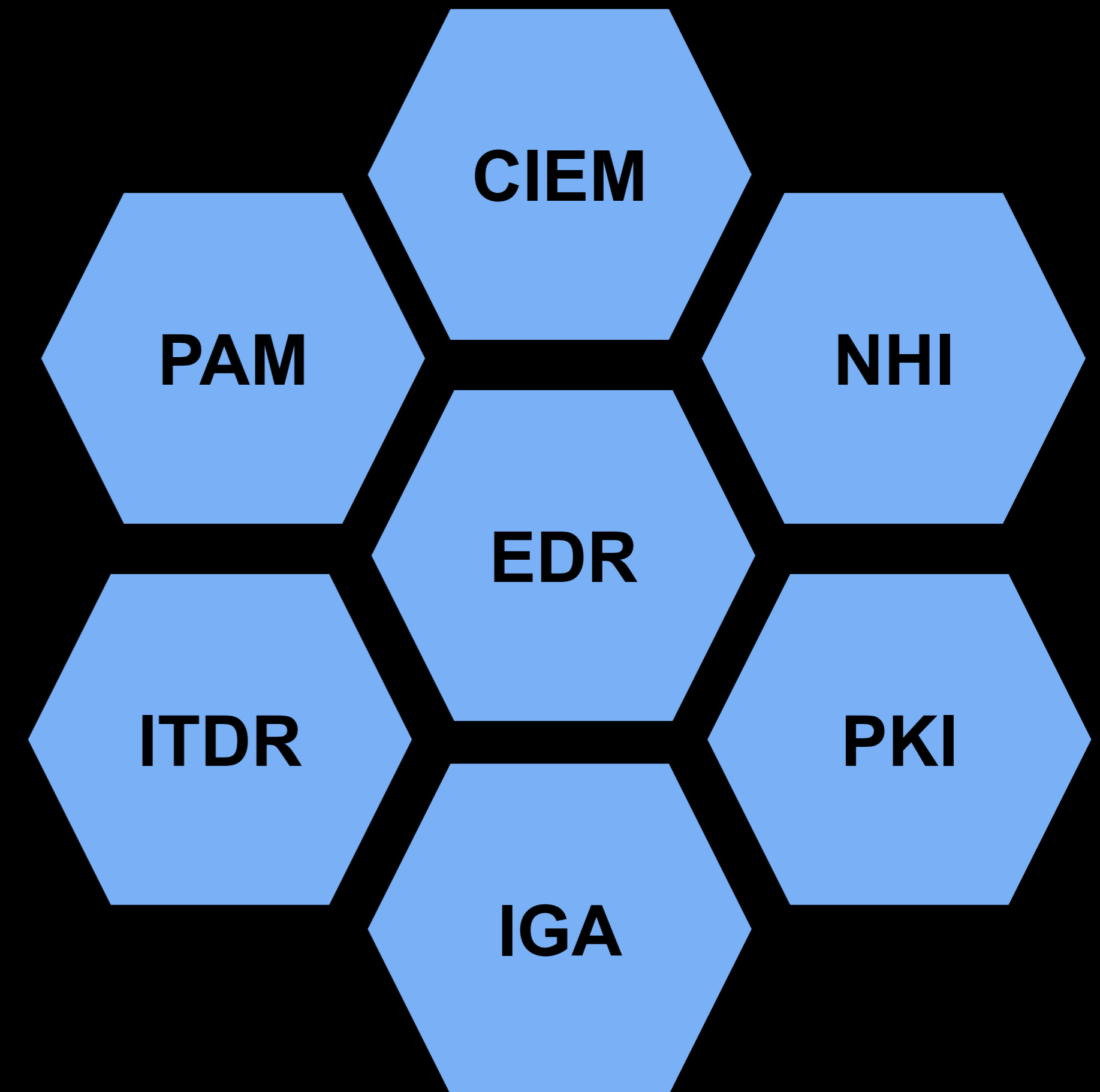
## Justin Kohler

Chief Product Officer @  SPECTEROPS

- Leads development for BloodHound Community Edition and BloodHound Enterprise
- Former Network Forensics, Detection and Response
- Air Force SIGINT Veteran
- Various speaking engagements, podcasts, etc

# ***“We Did Everything Right...”***

- Built a security-aware culture
- Aligned to NIST, MITRE, Zero Trust
- Implemented best-in-class tools



# “.....So Why Are We Still Getting Breached?”

**275%**

increase in human-operated **ransomware**

**71%**

of detections were **malware-free**,

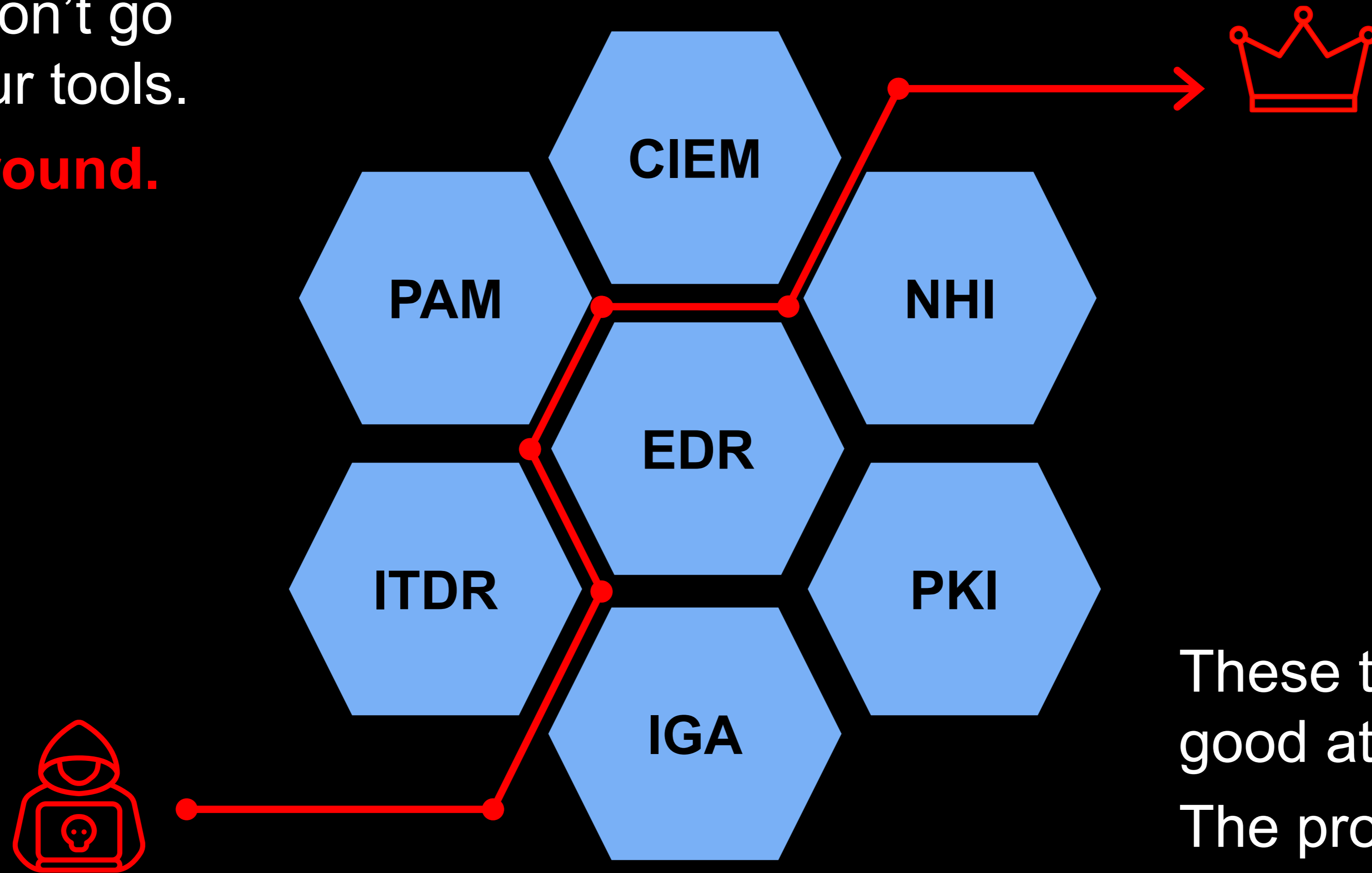
**80%**

of organizations have attack paths that expose **critical assets**

Even with modern tooling, attackers are succeeding.

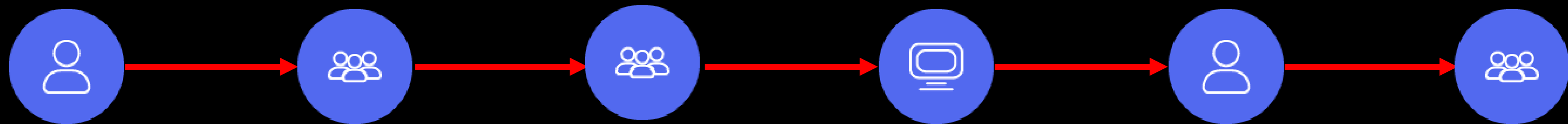
Attackers don't go through your tools.

**They go around.**

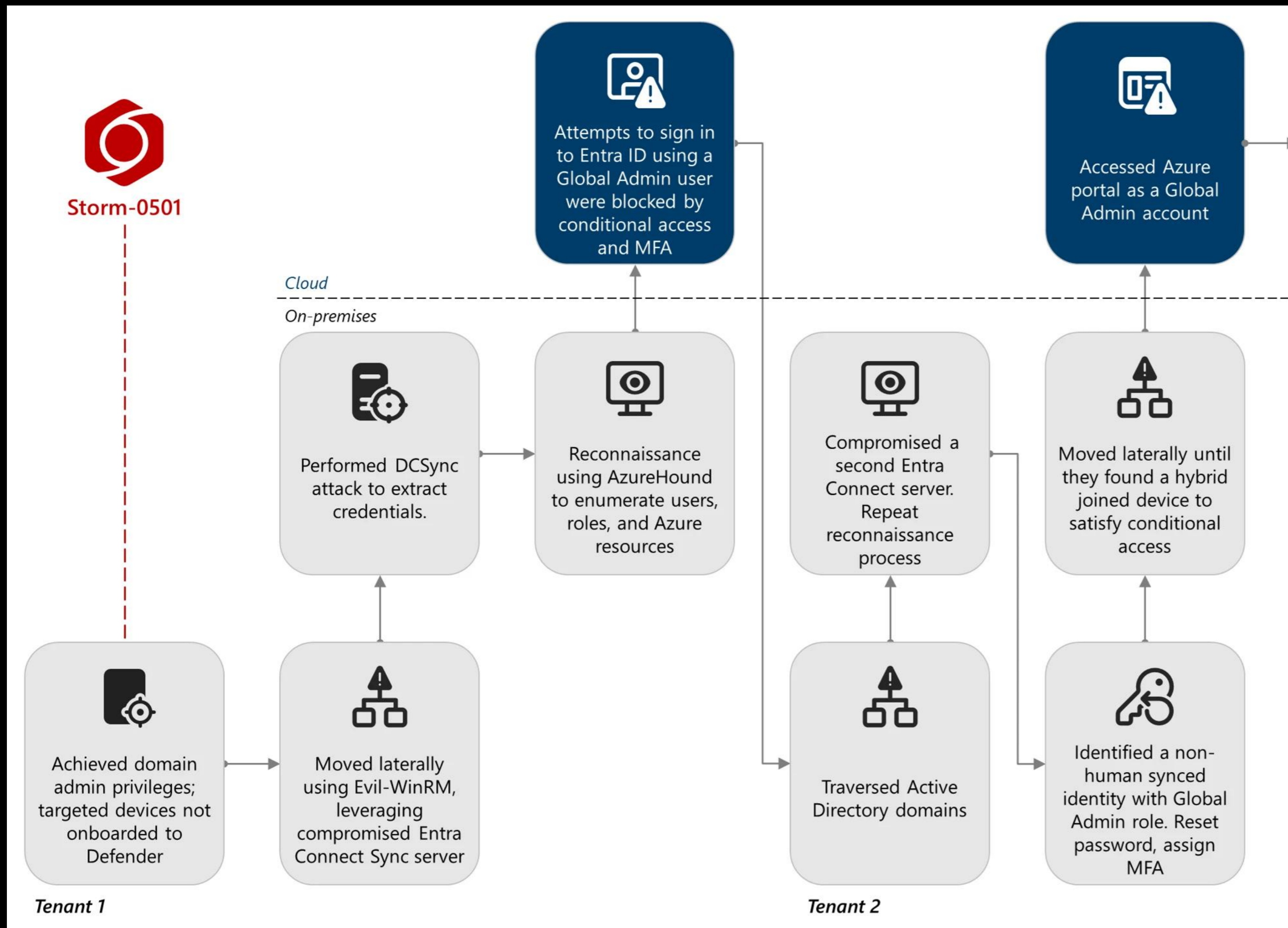


These tools are good at what they do. The problem is what they **don't do**.

Attack Paths are chains of **abusable privileges and user behaviors** that create connections between identities and resources.



# Attack Paths pivot through hybrid environments



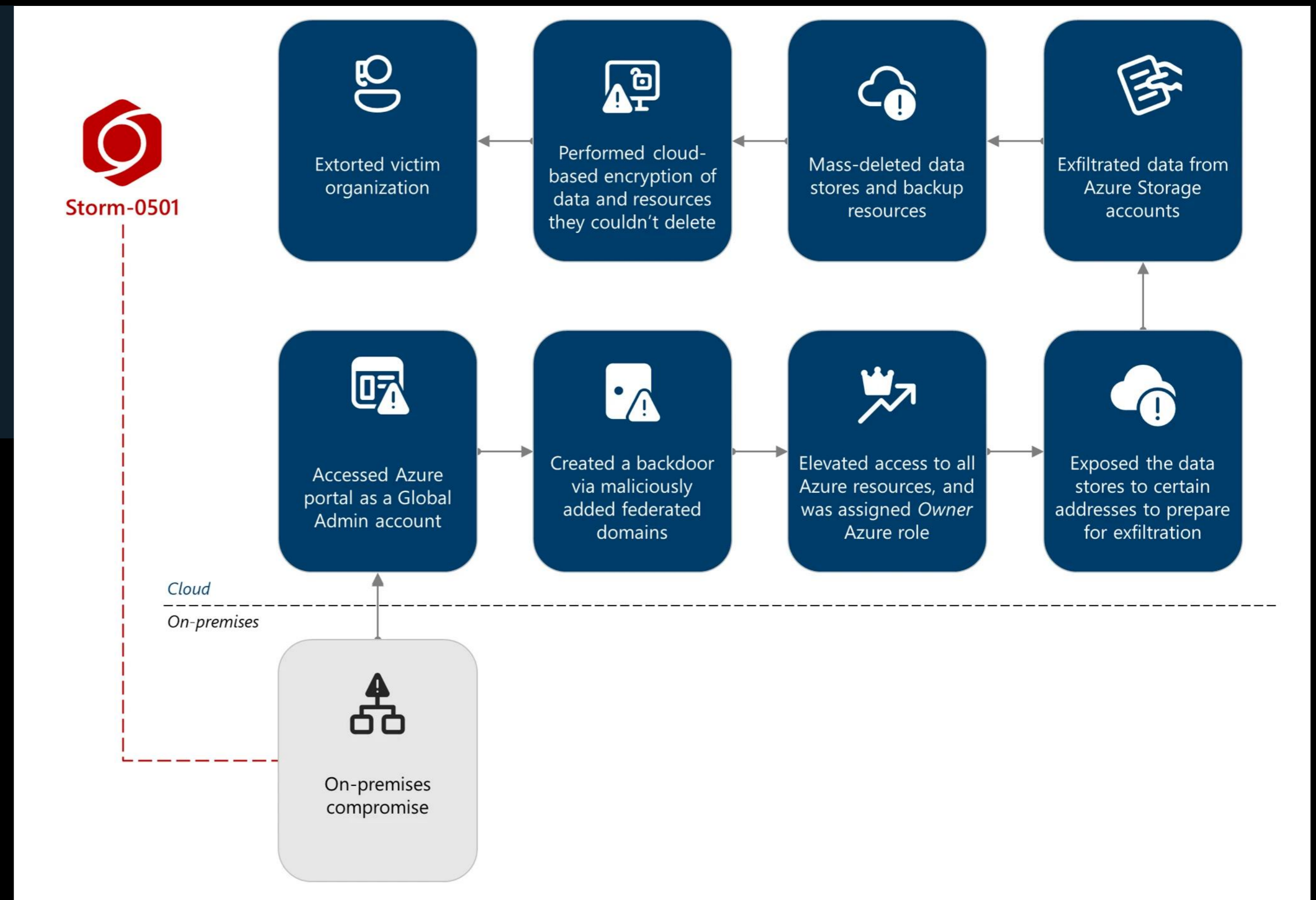
Storm-0501's evolving techniques lead to cloud-based ransomware

By [Microsoft Threat Intelligence](#)

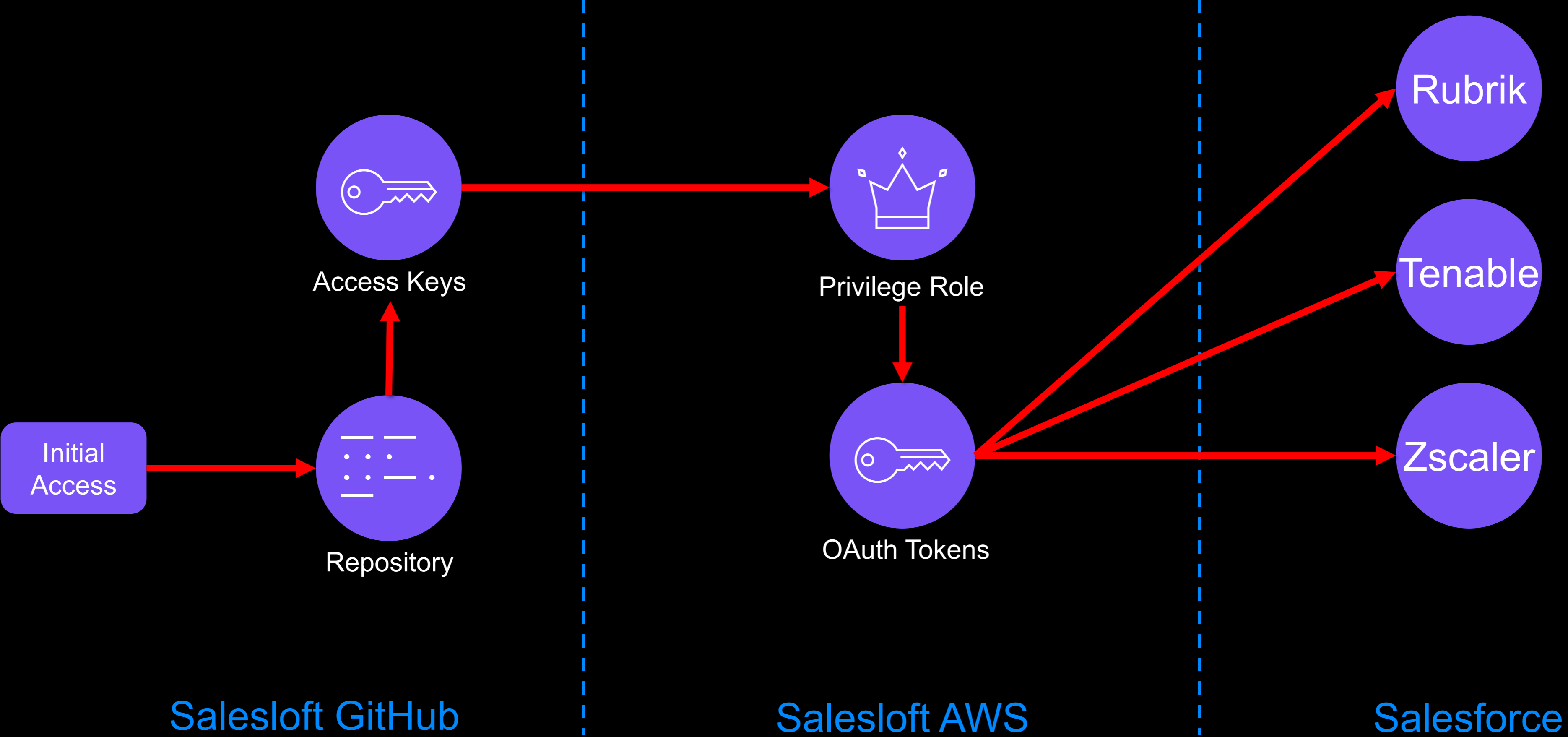
# Attack Paths pivot through hybrid environments

## Storm-0501's evolving techniques lead to cloud-based ransomware

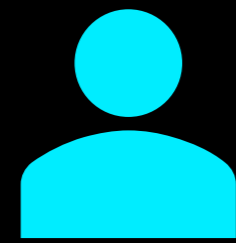
By [Microsoft Threat Intelligence](#)



# Salesloft Breach Attack Path



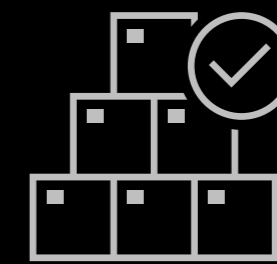
Source: [Widespread Data Theft Targets Salesforce Instances via Salesloft Drift](#)



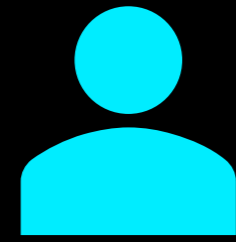
How  
Attack Paths  
Bypass Controls



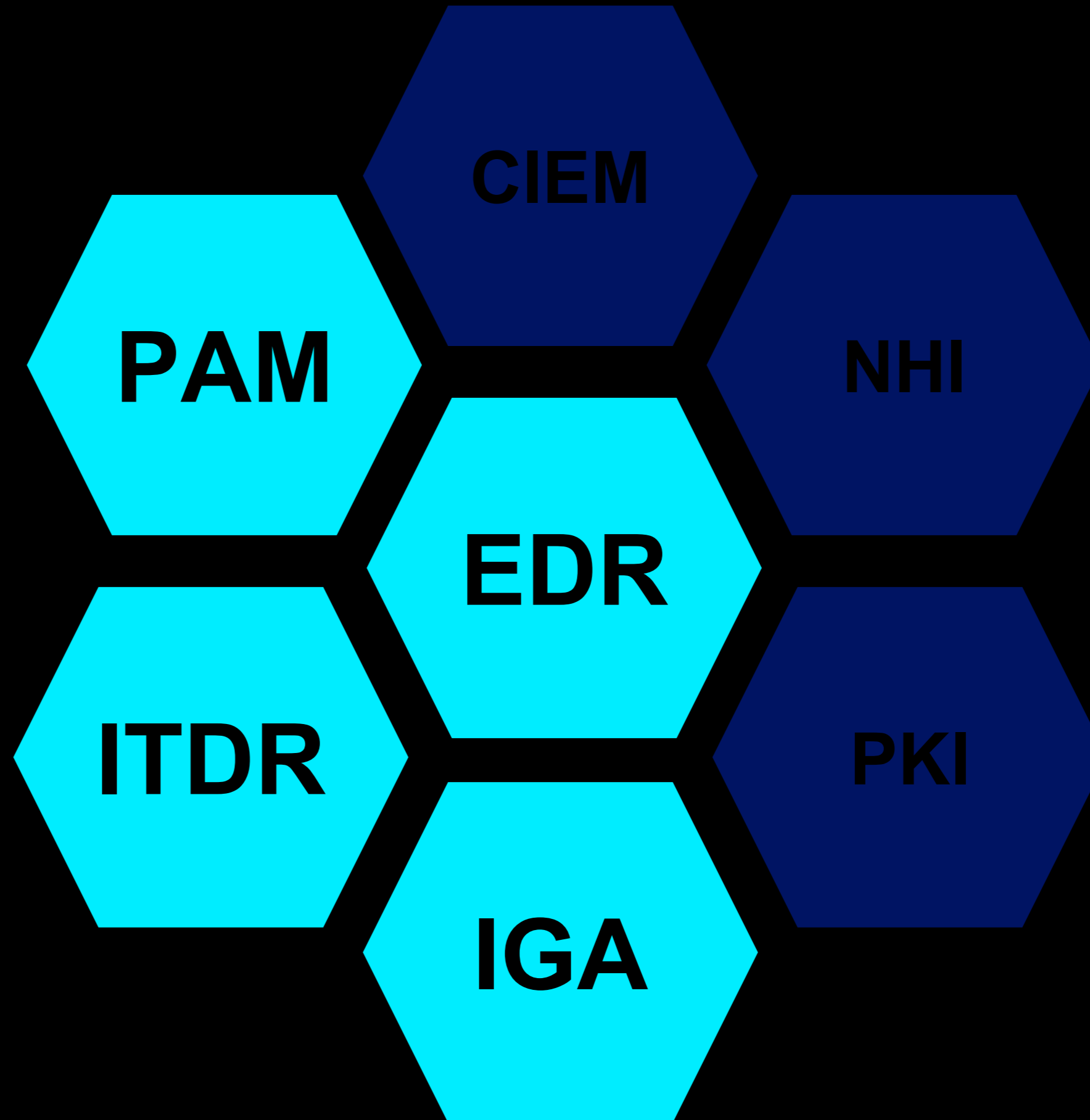
The Scale of  
Attack Paths

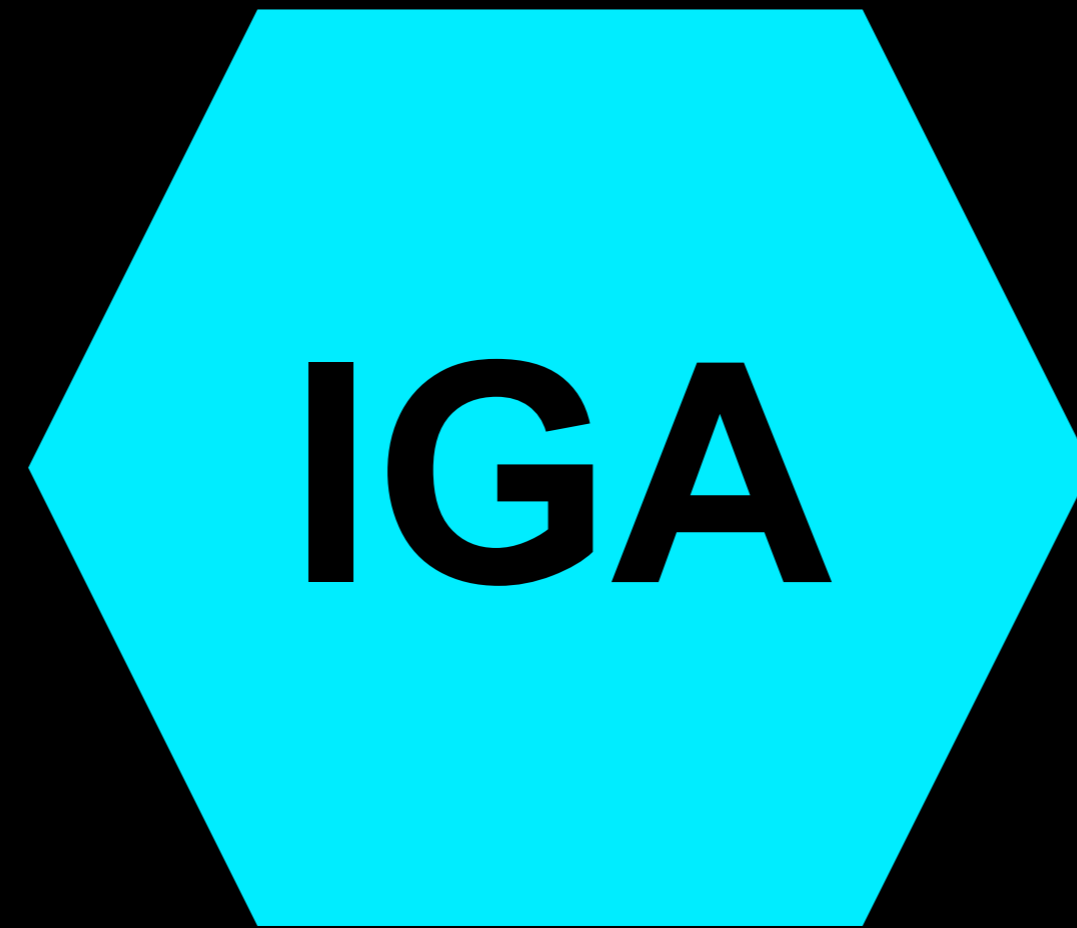


Attack Path  
Management



How  
Attack Paths  
Bypass Controls

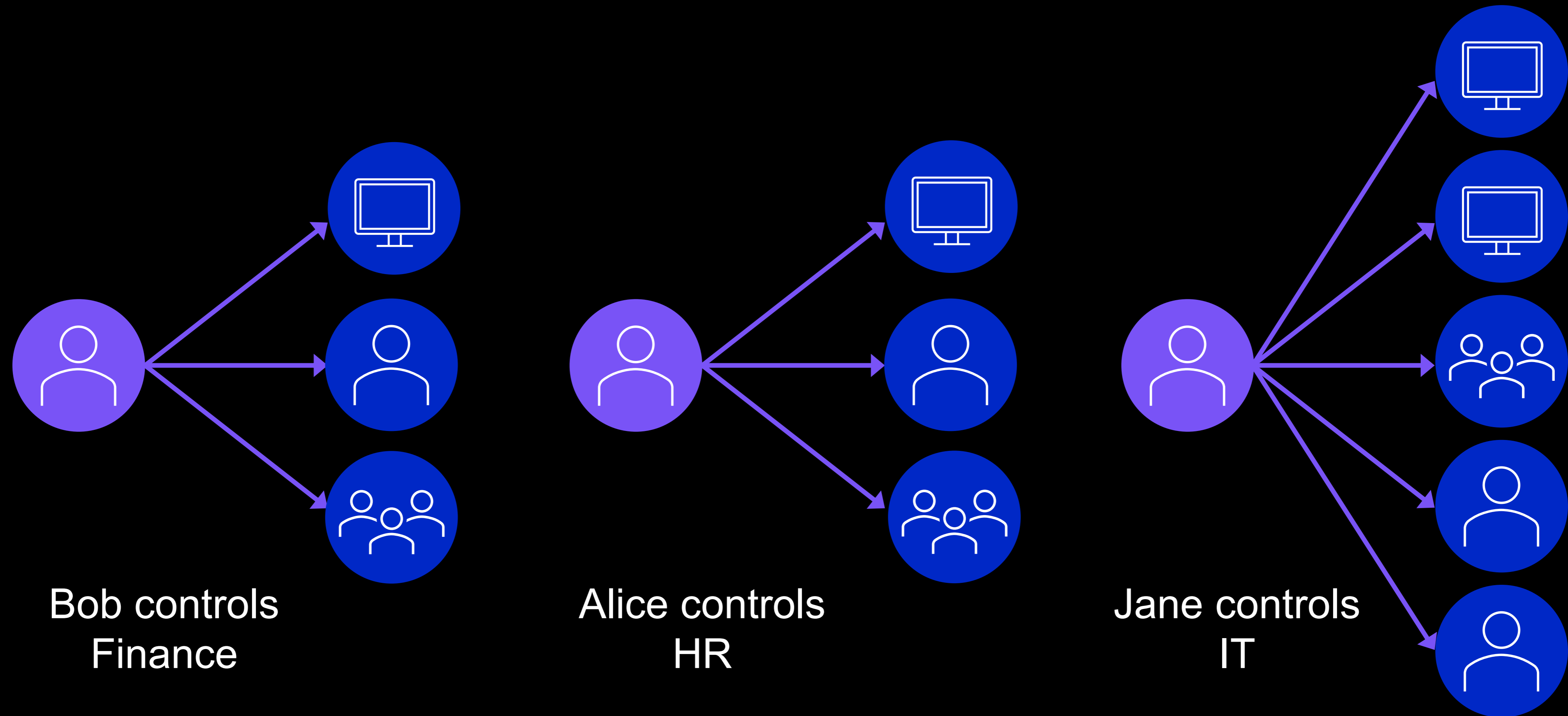




**Identity Governance and Administration**

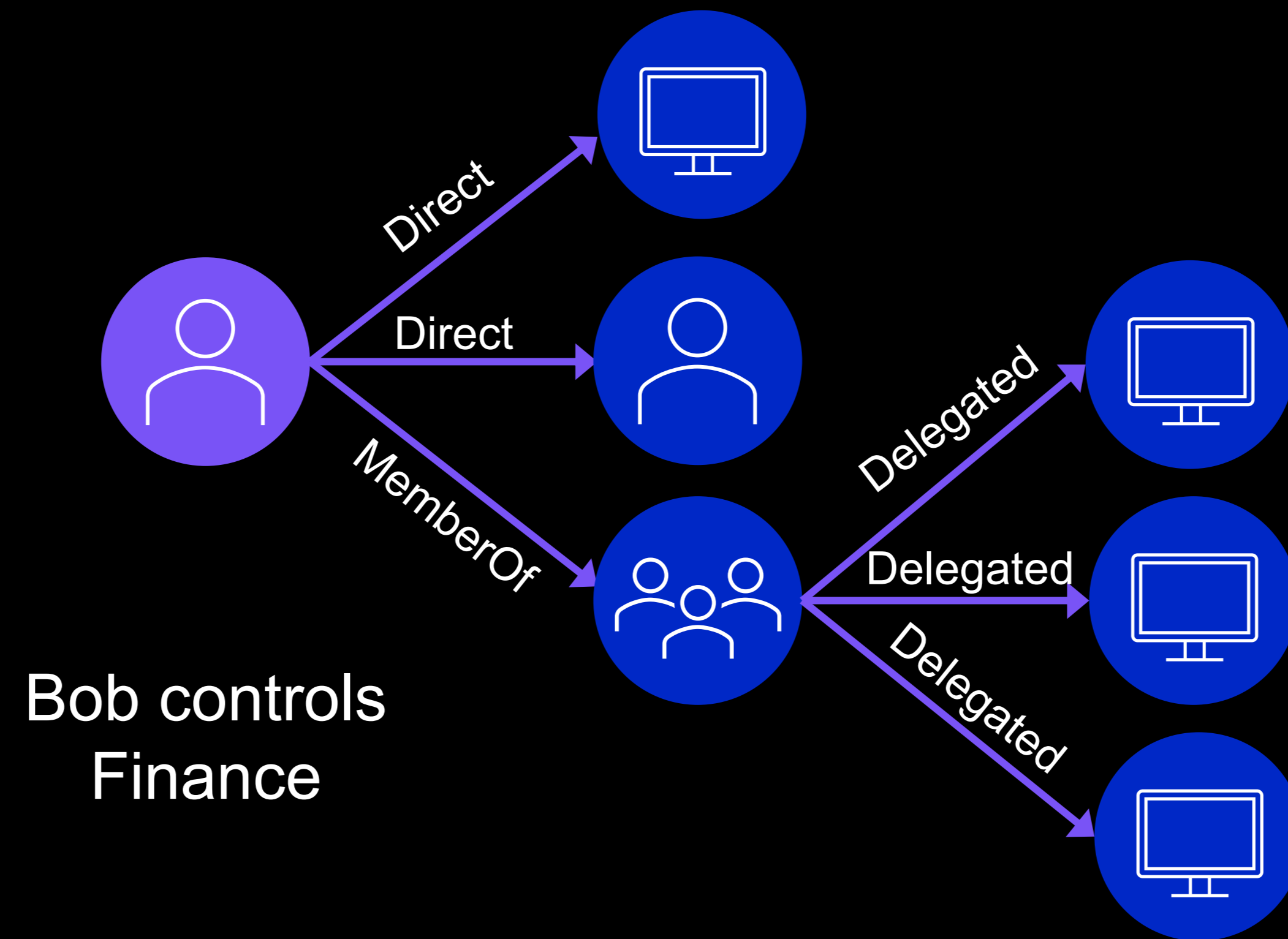
# Identity Governance and Administration

Identities are analyzed in silos

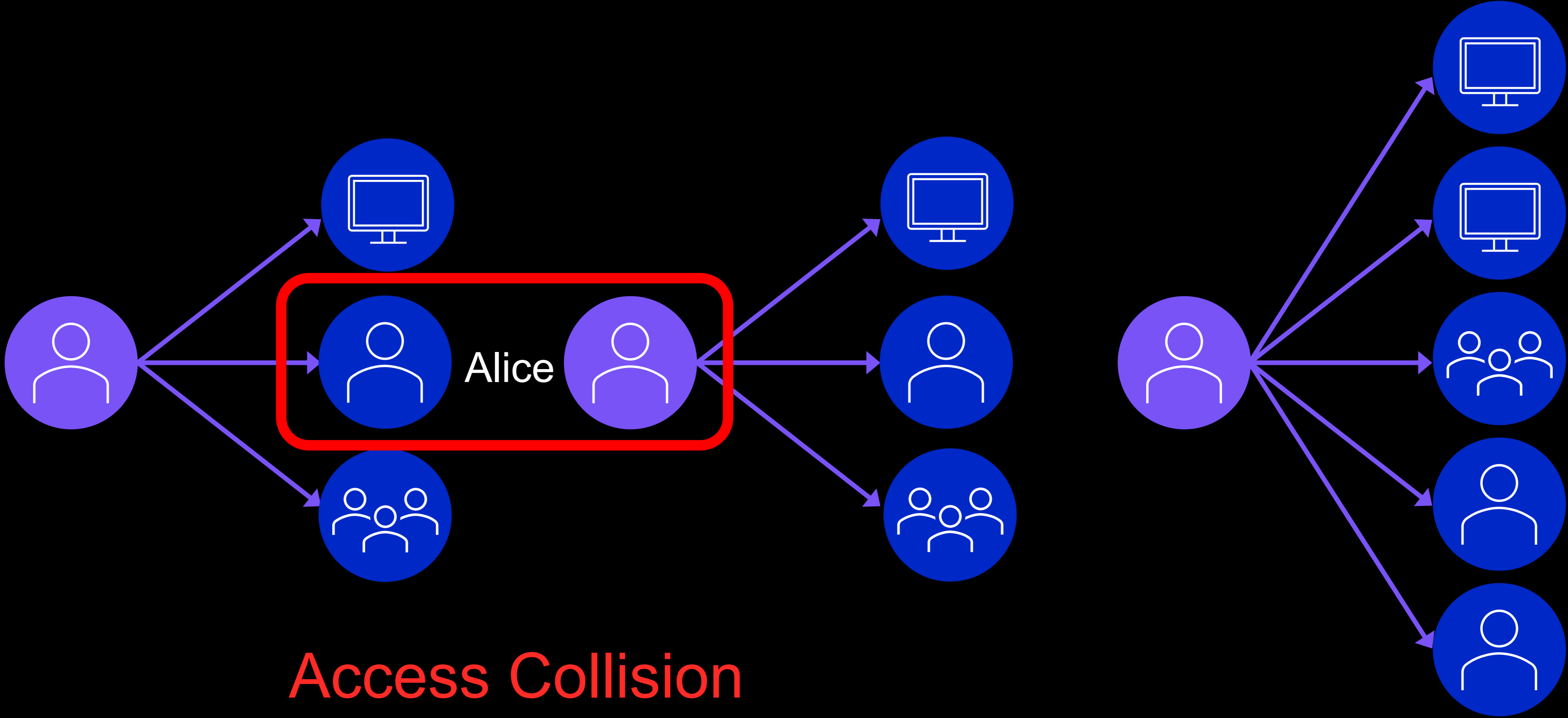


# Identity Governance and Administration

## Access Graphs

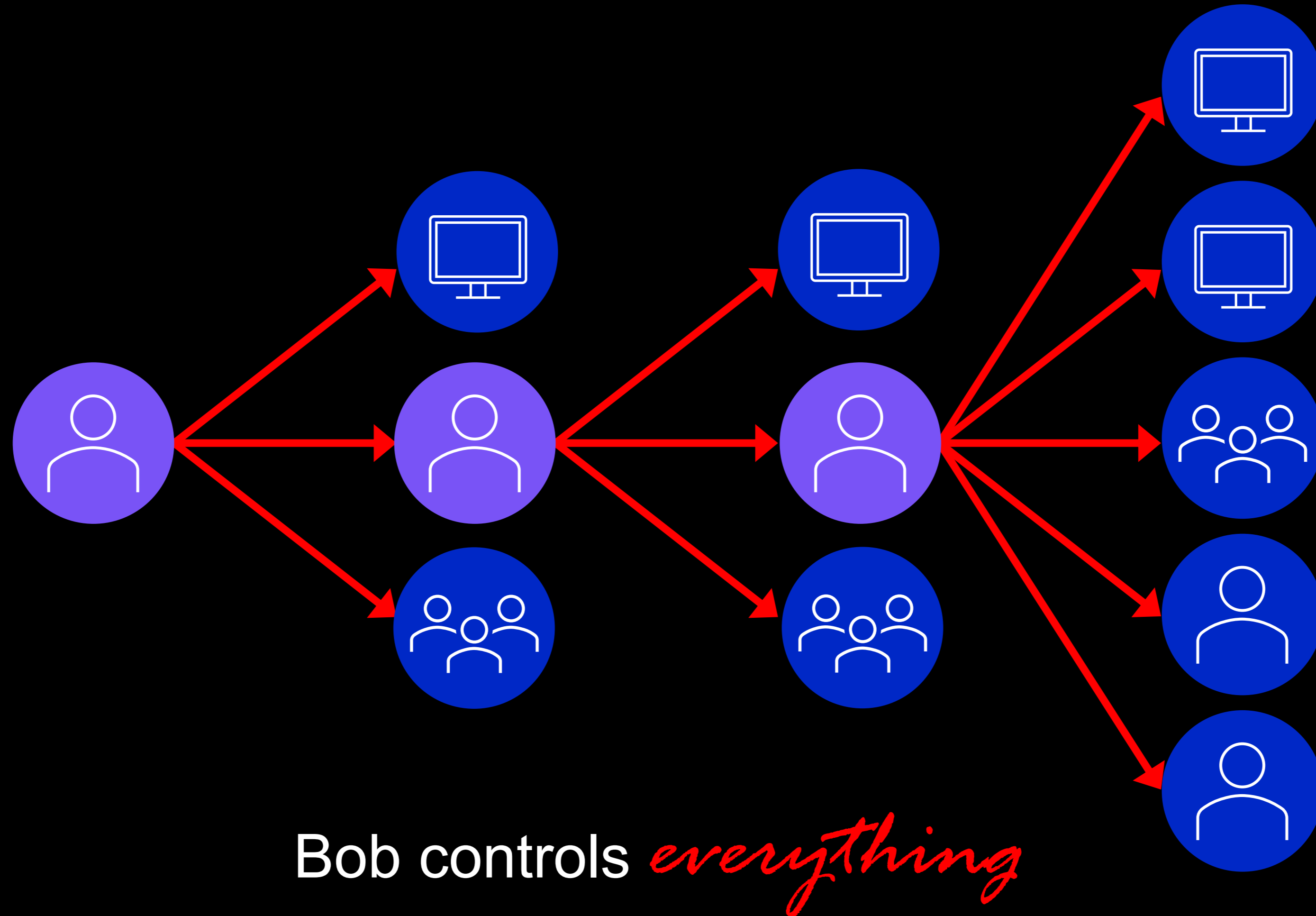


# Identity Governance and Administration

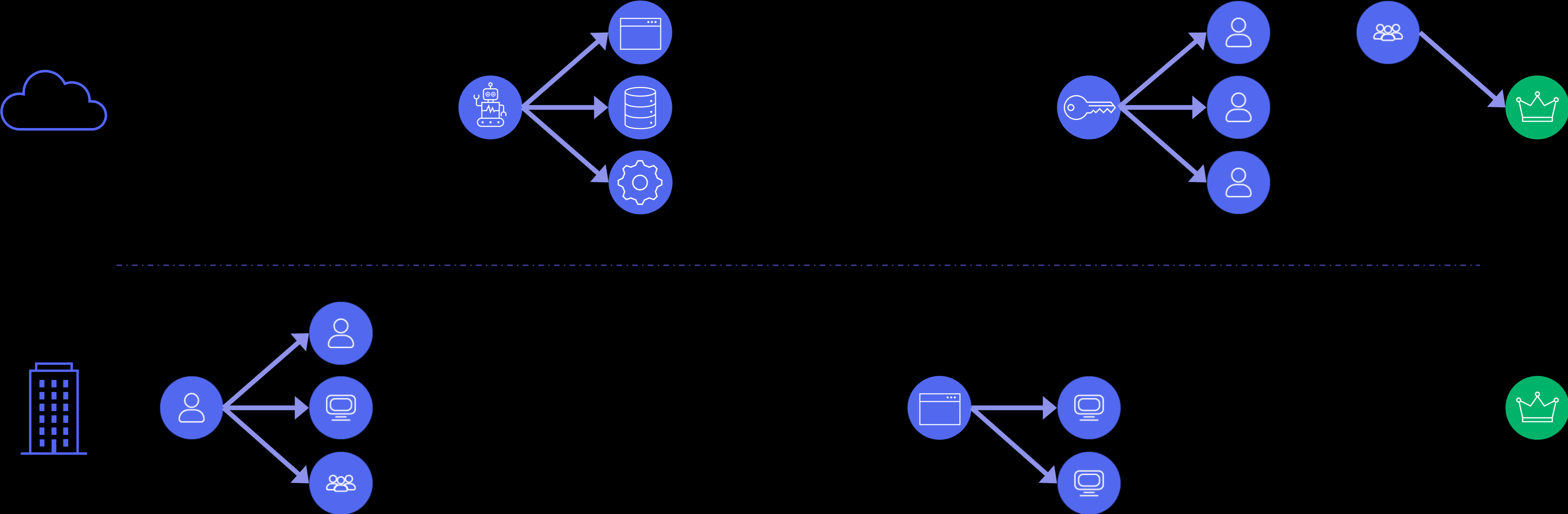


# Identity Governance and Administration

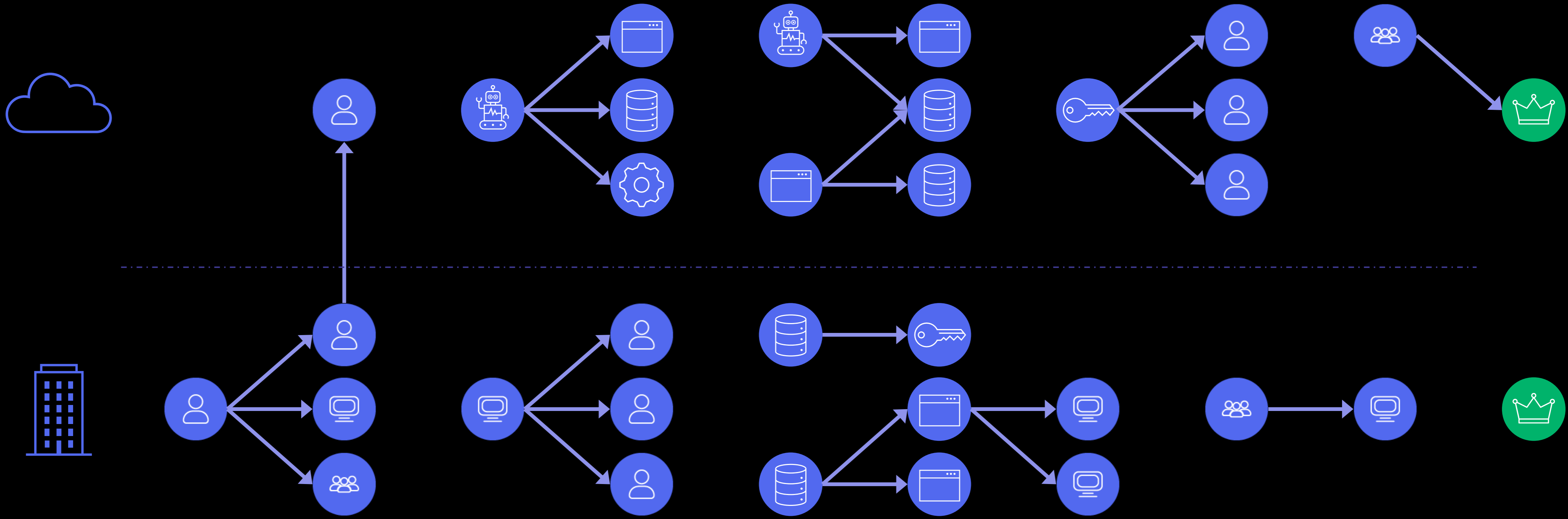
## Attack Graph



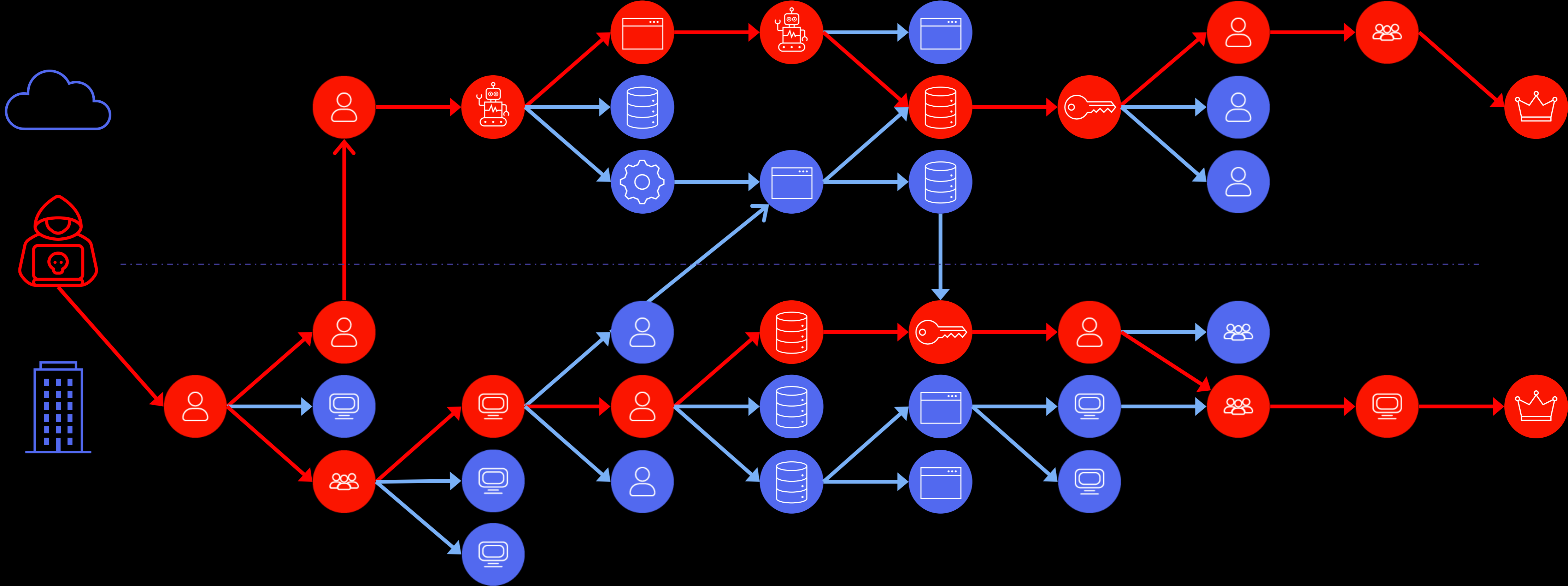
# Individual access decisions appear benign



# ...but form access collisions invisible to IGA



# Which form Attack Paths



# Identity Governance and Administration

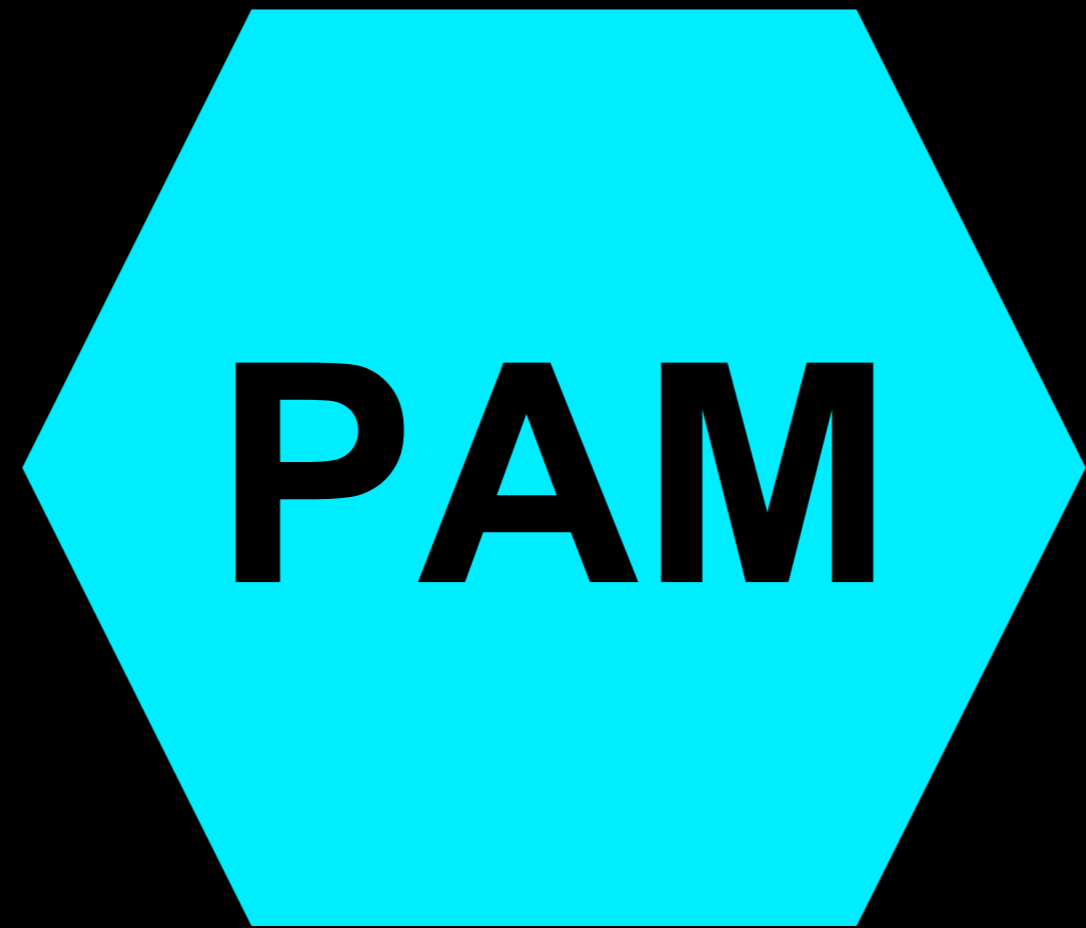
- IGA is great for provisioning access at scale

# Identity Governance and Administration

- IGA is great for provisioning access at scale
- Assigned Access  $\neq$  Effective Access

# Identity Governance and Administration

- IGA is great for provisioning access at scale
- Assigned Access  $\neq$  Effective Access
- Access Collisions create Attack Paths for adversaries



**Privileged Access Management**

# Privileged Access Management

**Identity At Rest**

**Identity In Transit**

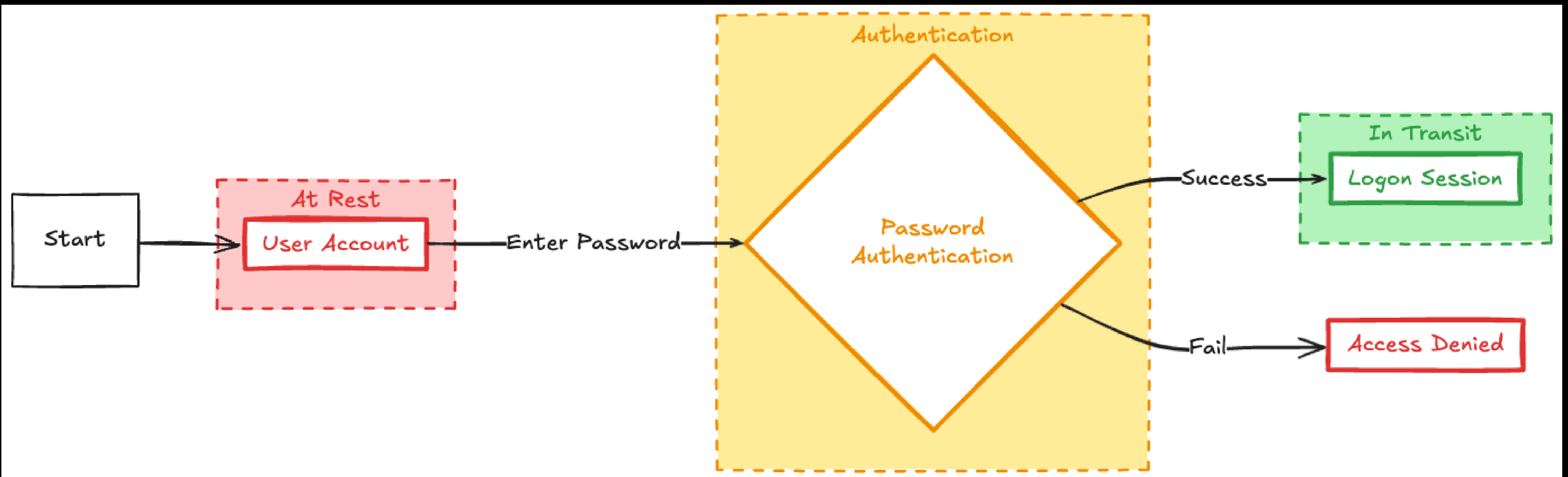
# Privileged Access Management

	Identity At Rest	Identity In Transit
Definition	A pre-authentication account with a credential	Sessions, Tokens, Processes. Created post authentication.

# Privileged Access Management

	Identity At Rest	Identity In Transit
Definition	A pre-authentication account with a credential	Sessions, Tokens, Processes. Created post authentication.
Attacks	Password Dumping, Brute Forcing	Token Impersonation, Session hijacking, process injection, Cookie Theft, Pass-the-Ticket

# Identity States during Authentication Flow



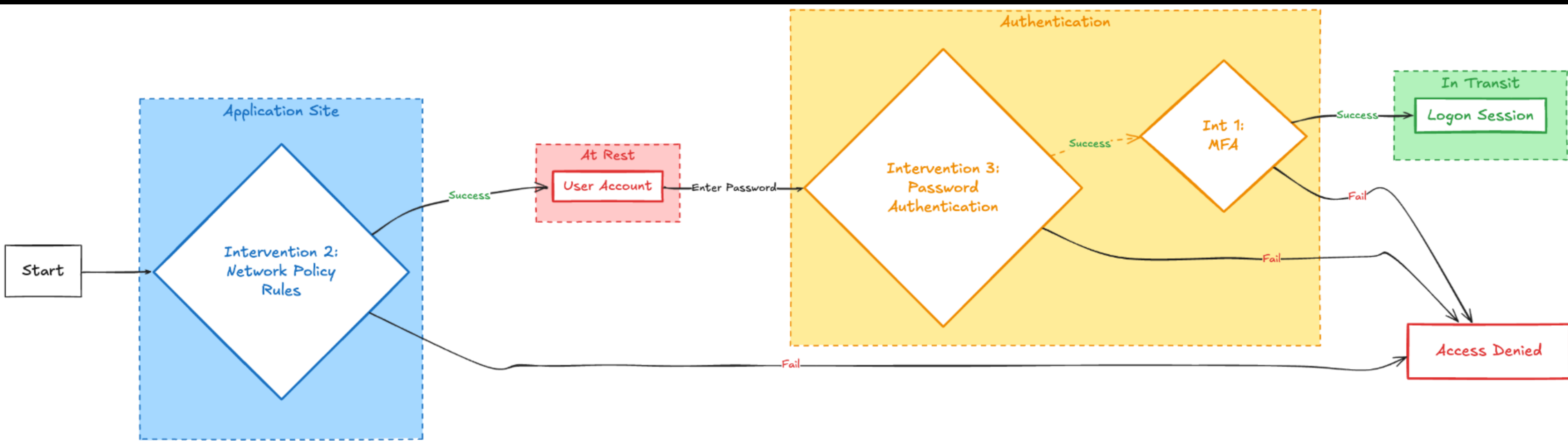
# Case Study: 2024 Snowflake Attack

*According to Mandiant, these victims' Snowflake identities were compromised via a contractor's laptop also used for personal activities.*

Snowflake and Mandiant recommendations:

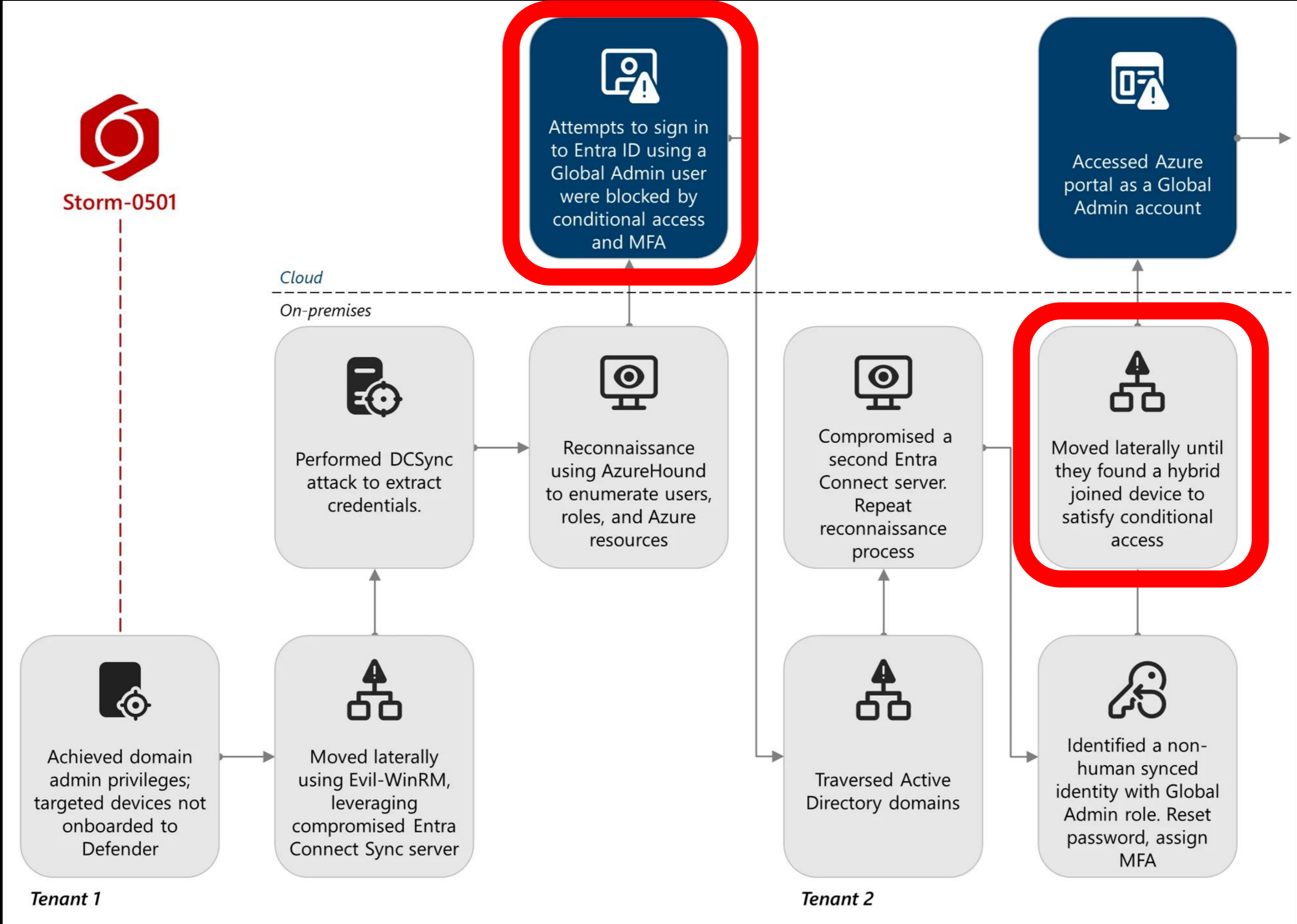
1. Enforce Multi-Factor Authentication on all accounts
2. Set up Network Policy Rules to allow authorized users & locations
3. Reset and rotate Snowflake credentials

# Recommendations in the Authentication Flow



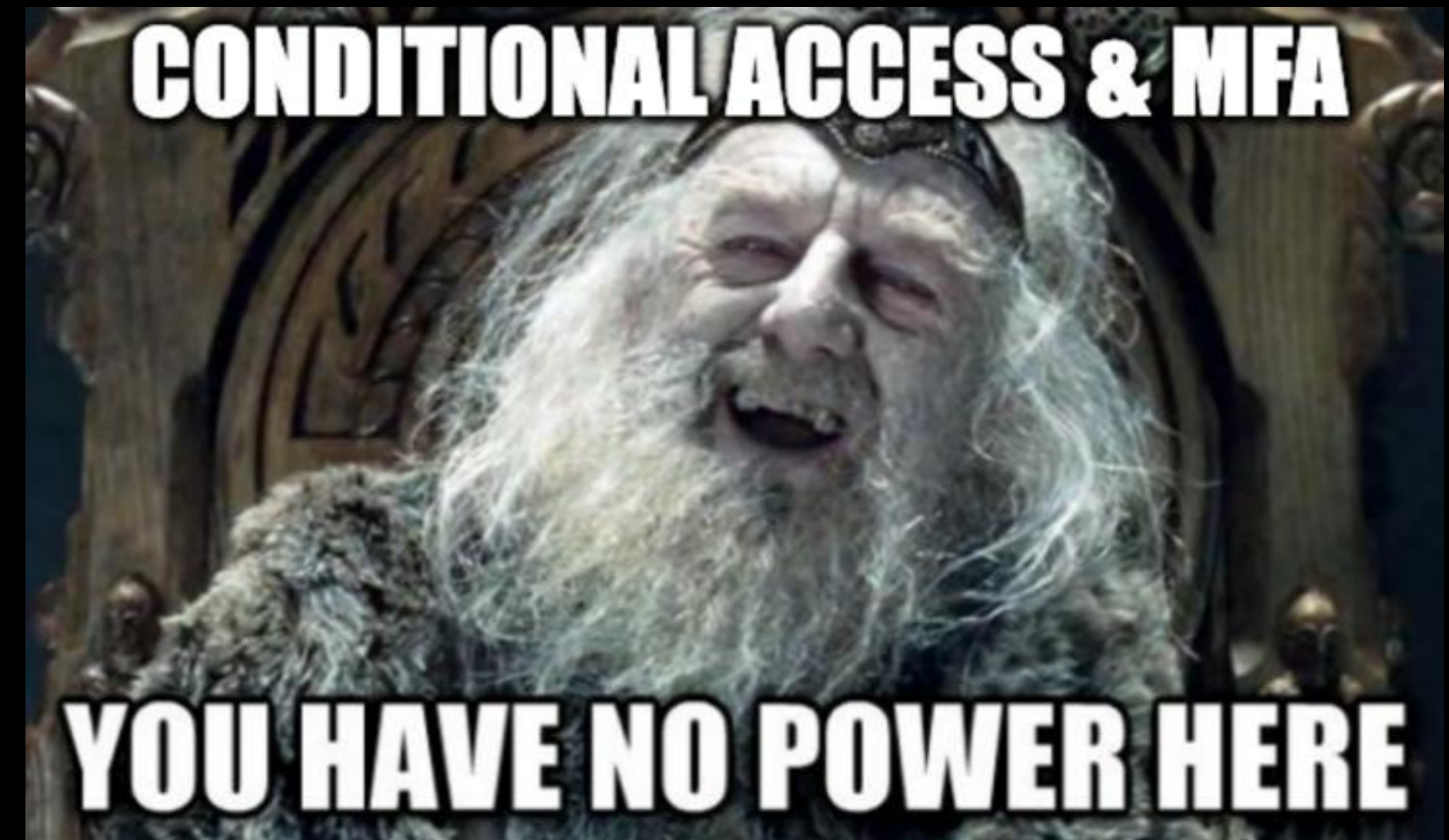
Nothing for the In Transit identity = I can still pivot

# But we use Conditional Access!



# Identity In Transit attacks & Conditional Access

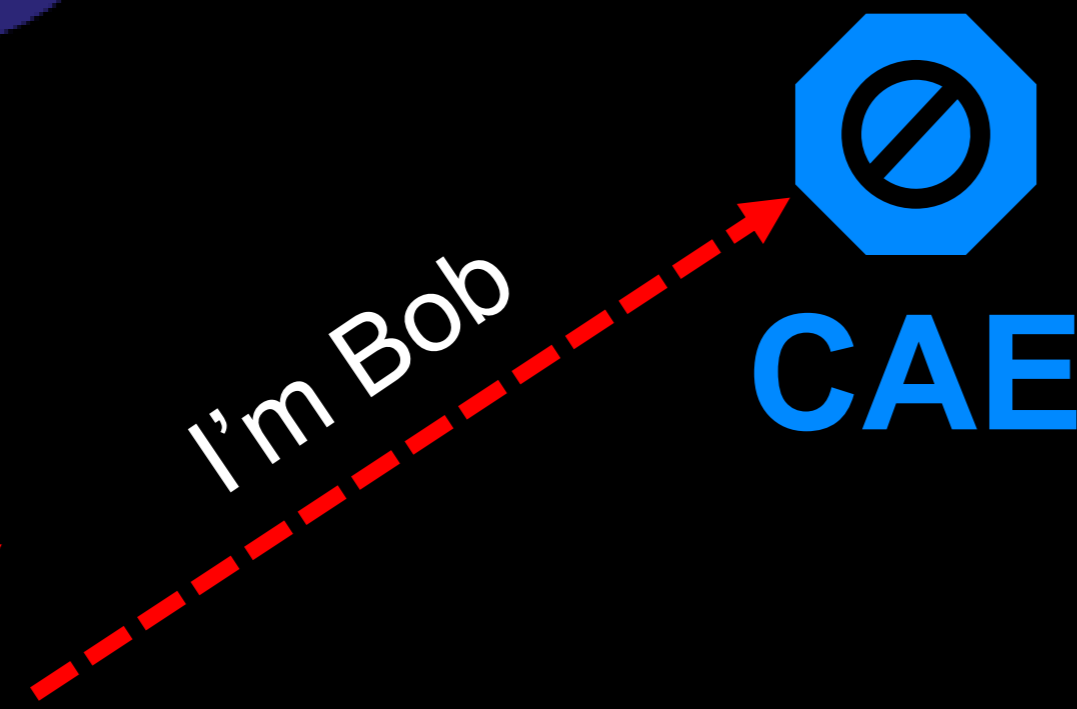
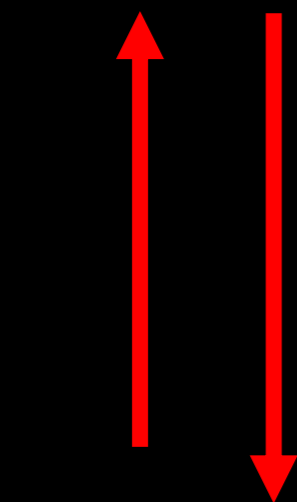
- Bob logs in
- Satisfies Conditional Access + MFA
- Bearer token / JWT created on host
- Attacker harvests token
- Attacker uses token from their host
- *Attacker is Bob*



# But we use Conditional Access *with* Continuous Access Evaluation

BOB's Workstation

Azure

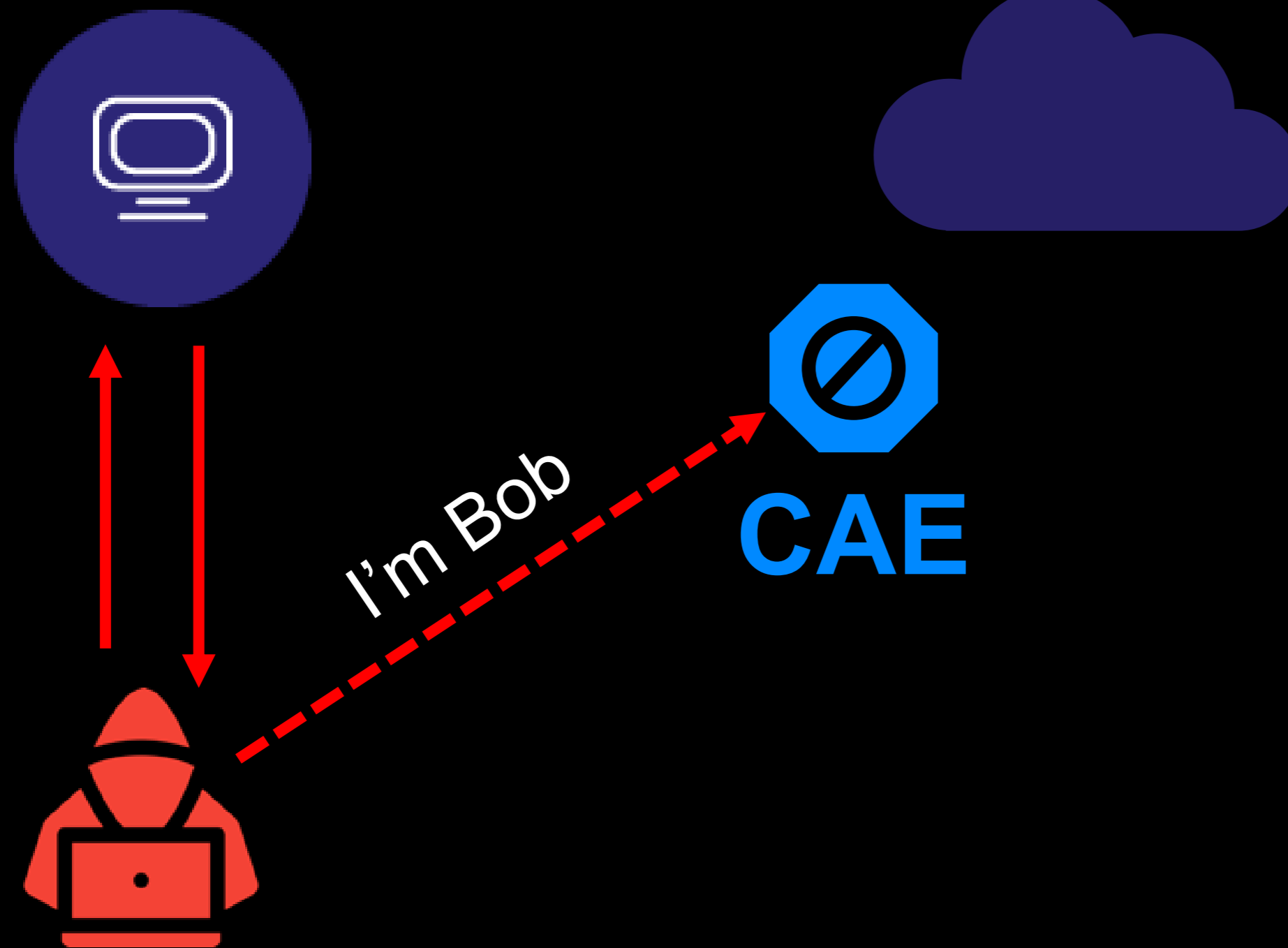


CAE

# But we use Conditional Access *with* Continuous Access Evaluation

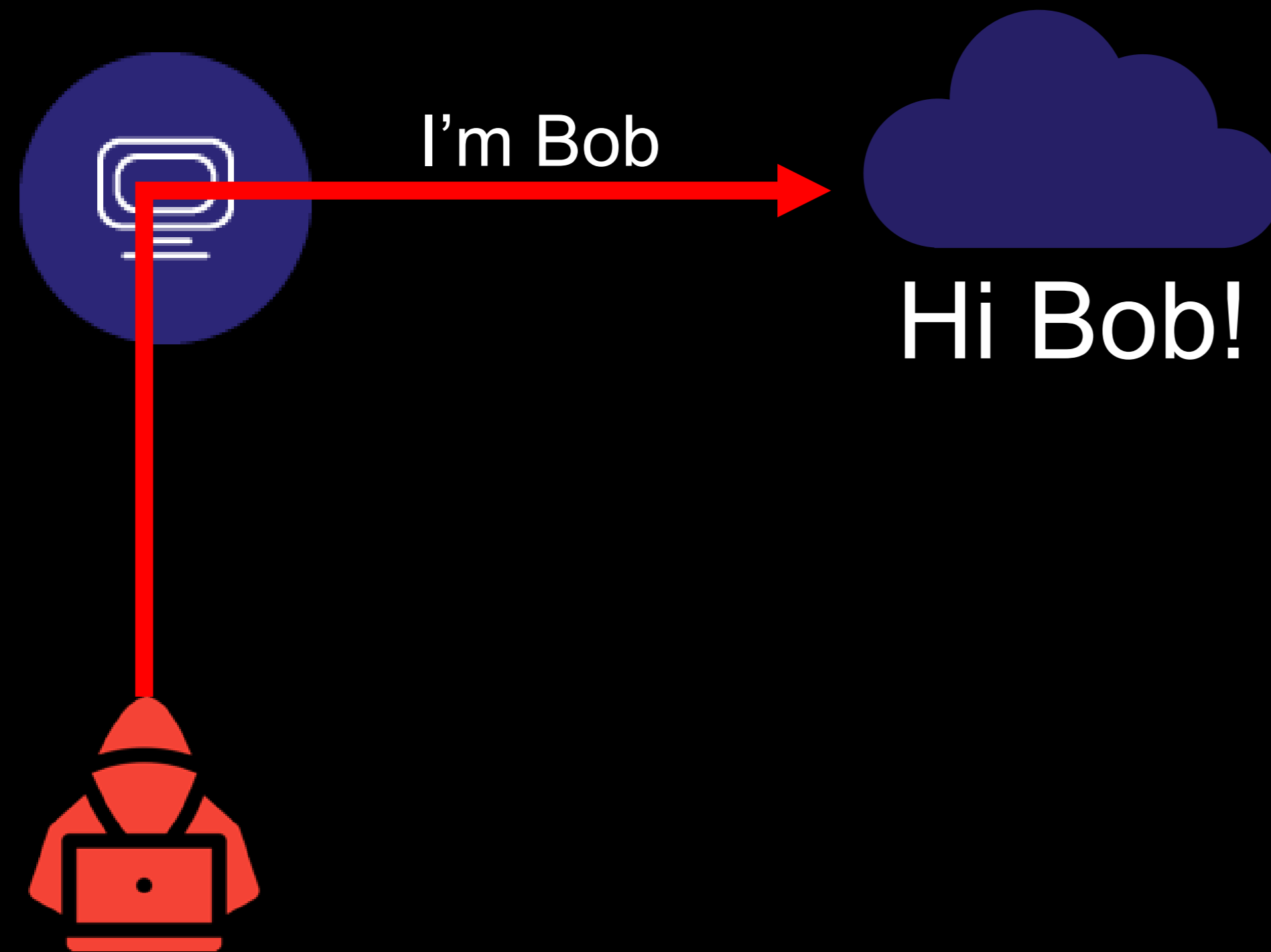
BOB's Workstation

Azure



*I'll just use your host*

# But we use Conditional Access *with* Continuous Access Evaluation



I'll just use *your* host

# Privileged Access Management

- PAM / JIT / CAP are all powerful tools that should be used

# Privileged Access Management

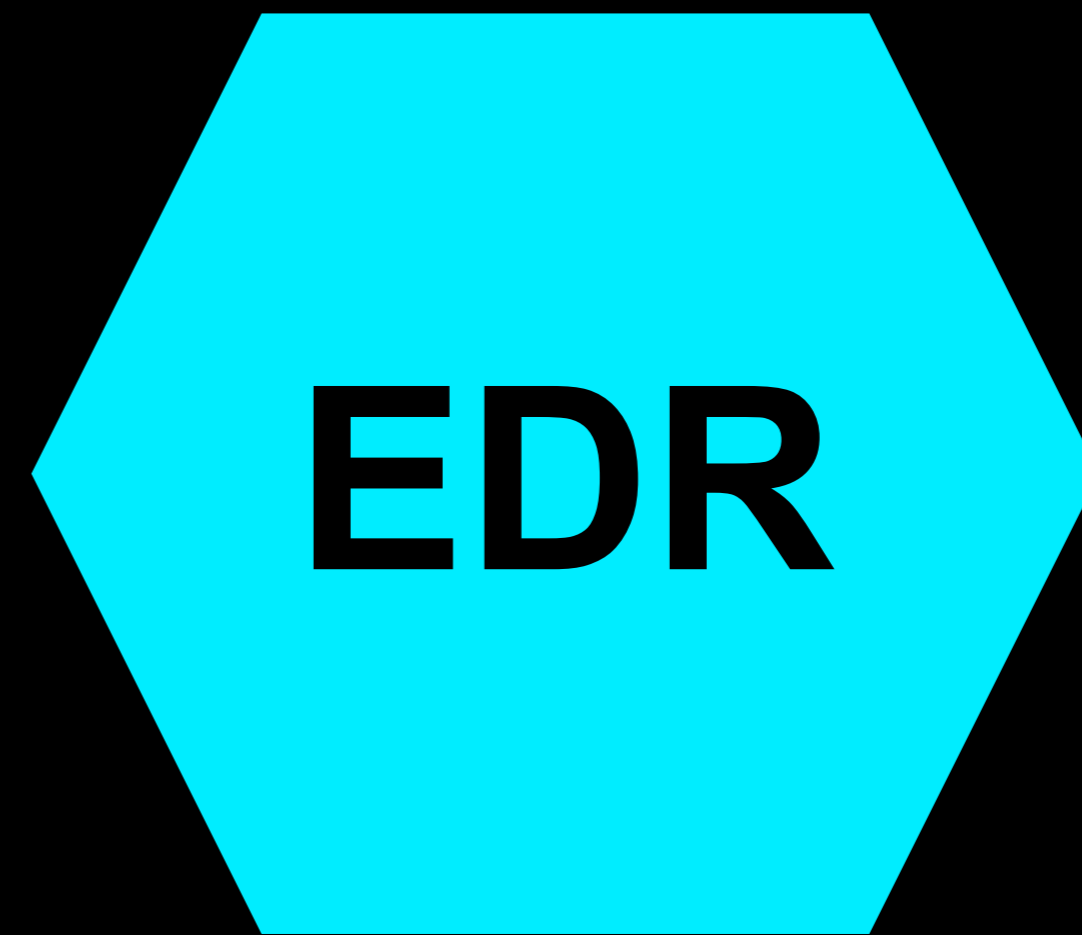
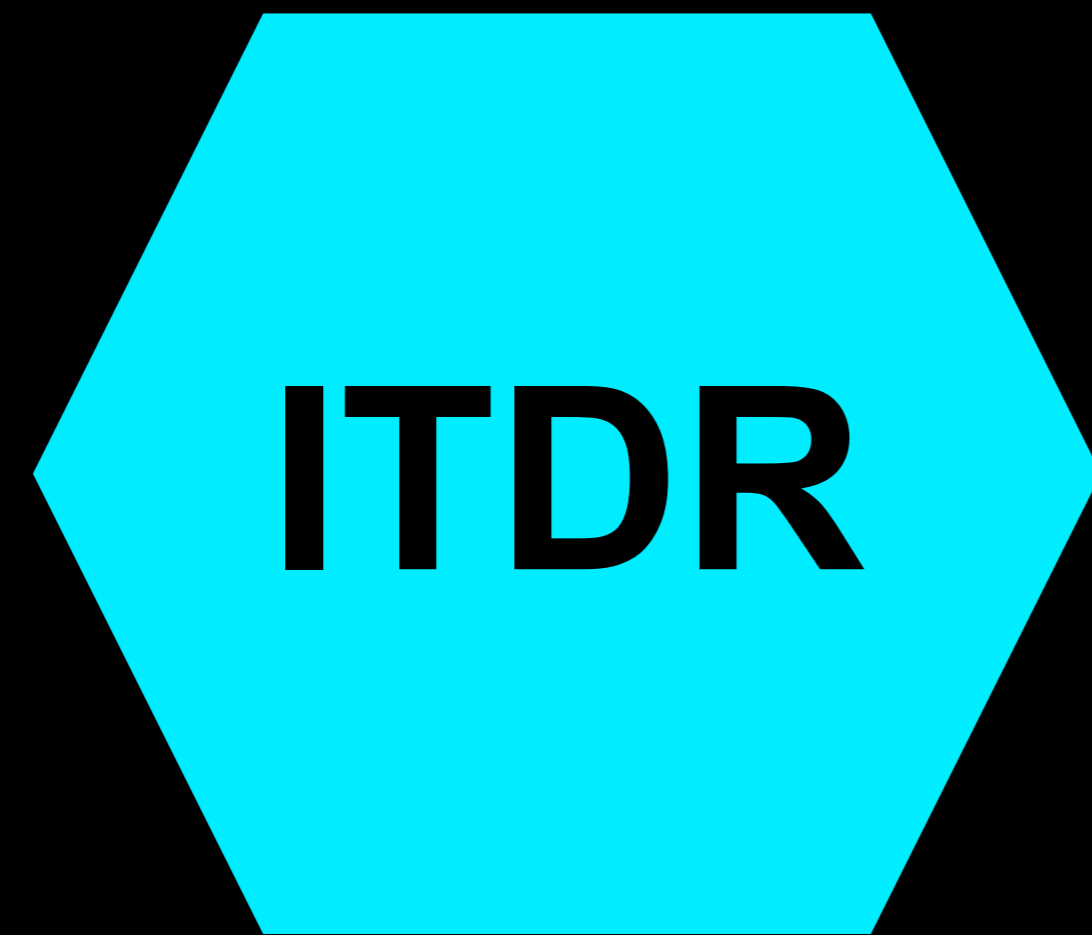
- PAM / JIT / CAP are all powerful tools that should be used
- User login sessions create artifacts that can be abused

# Privileged Access Management

- PAM / JIT / CAP are all powerful tools that should be used
- User login sessions create artifacts that can be abused
- Attackers don't need the password, they steal sessions

# Privileged Access Management

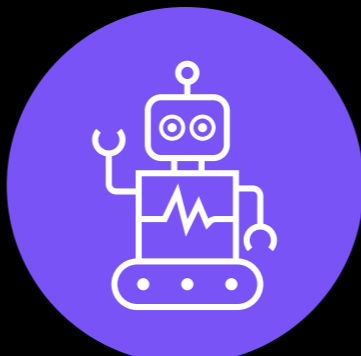
- PAM / JIT / CAP are all powerful tools that should be used
- User login sessions create artifacts that can be abused
- Attackers don't need the password, they steal sessions
- PAM secures Identities At Rest, not what happens next



**Endpoint & Identity Detection Response**

# Endpoint & Identity Detection and Response

Anonymous Login

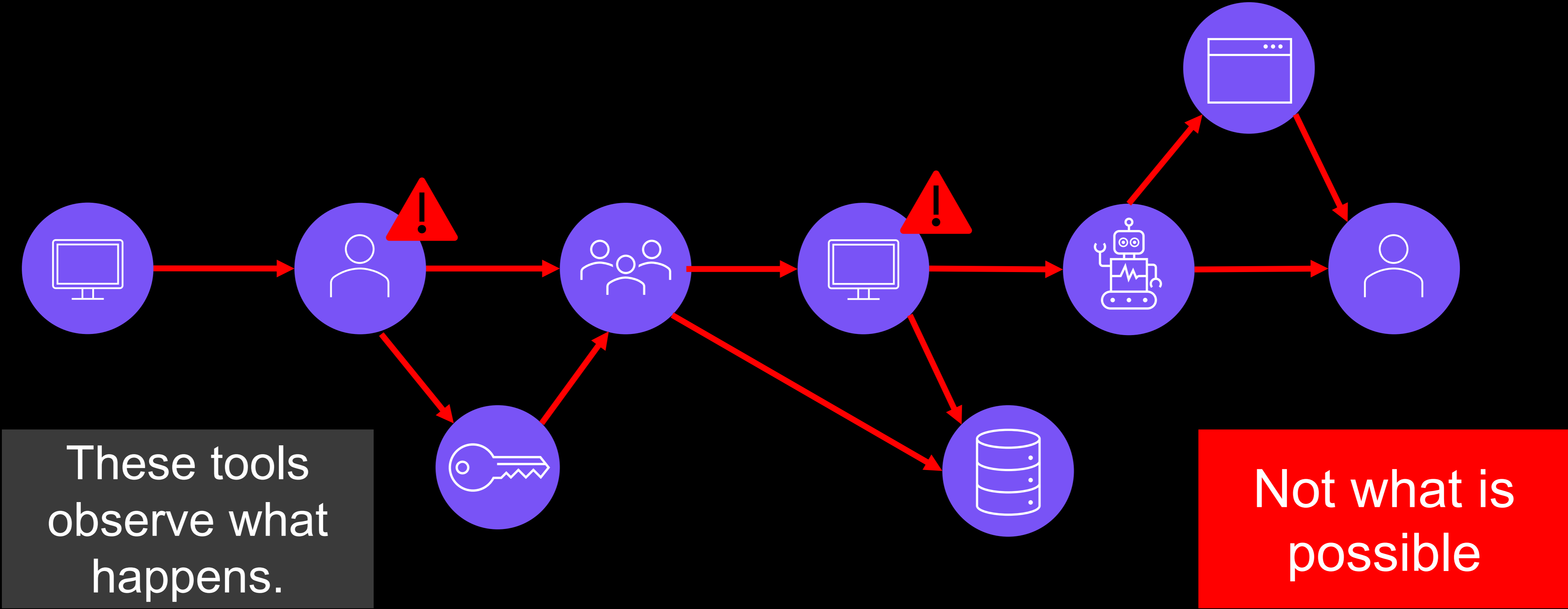


These tools observe what happens.

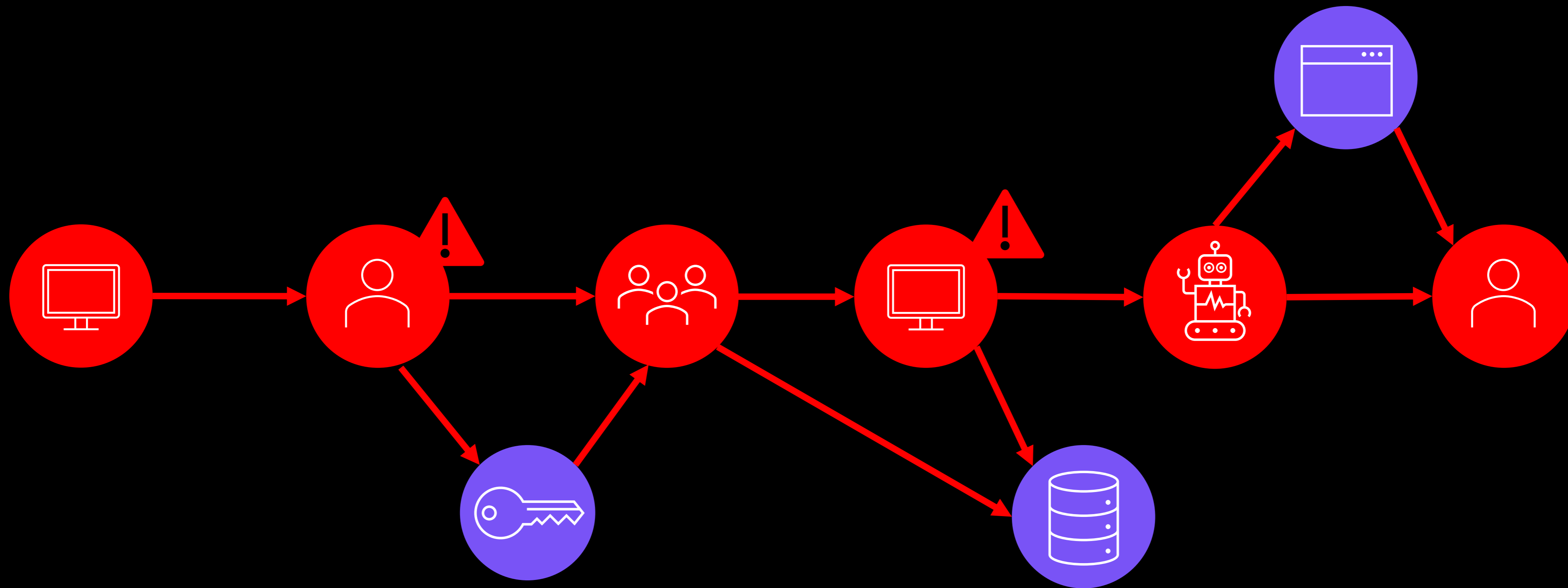


Process Injection

# Endpoint & Identity Detection and Response



# Endpoint & Identity Detection and Response



They detect the *symptom*, not the *condition*.

# Case Study: **Red Team Engagement**

- Advanced organization, modern controls, strong defense

# Case Study: **Red Team Engagement**

- *Advanced organization, modern controls, strong defense*
- How about Command and Control (C2) in Perl?

# Case Study: **Red Team Engagement**

- Advanced organization, modern controls, strong defense
- How about Command and Control (C2) in Perl?
- Attackers are now only limited by their creativity

# Nation state attacker tradecraft, for everyone!



## Yesterday's Attacker:

Manual

Expensive

Repeatable TTPs



## Today's Attacker:

Agentic

Cheap

Customized

# Endpoint & Identity Detection and Response

I don't need to beat the E/ITDR, I just need to beat *you*

# Endpoint & Identity Detection and Response

- E/ITDR monitor systems & behaviors – often miss structure

# Endpoint & Identity Detection and Response

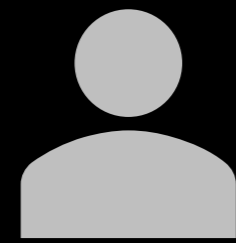
- E/ITDR monitor systems & behaviors – often miss structure
- Lateral movement can look legitimate and go undetected

# Endpoint & Identity Detection and Response

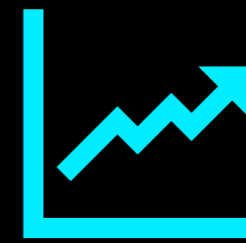
- E/ITDR monitor systems & behaviors – often miss structure
- Lateral movement can look legitimate and go undetected
- AI/LLMs are lowering the bar for advanced attacks

# Endpoint & Identity Detection and Response

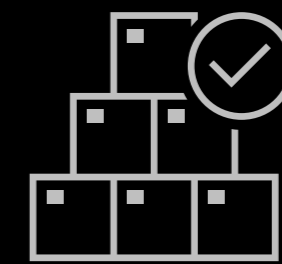
- E/ITDR monitor systems & behaviors – often miss structure
- Lateral movement can look legitimate and go undetected
- AI/LLMs are lowering the bar for advanced attacks
- Even once detected, attacker may have moved on



How  
Attack Paths  
Bypass Controls

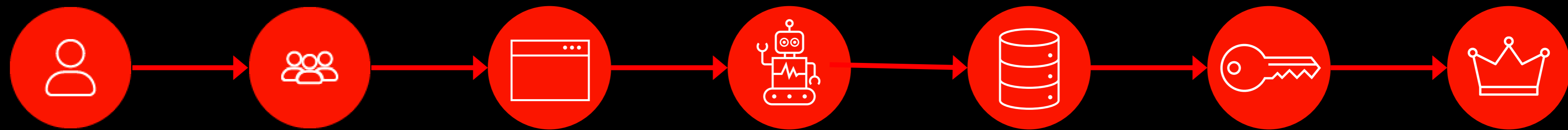


The Scale of  
Attack Paths



Attack Path  
Management

# How can we quantify this problem?



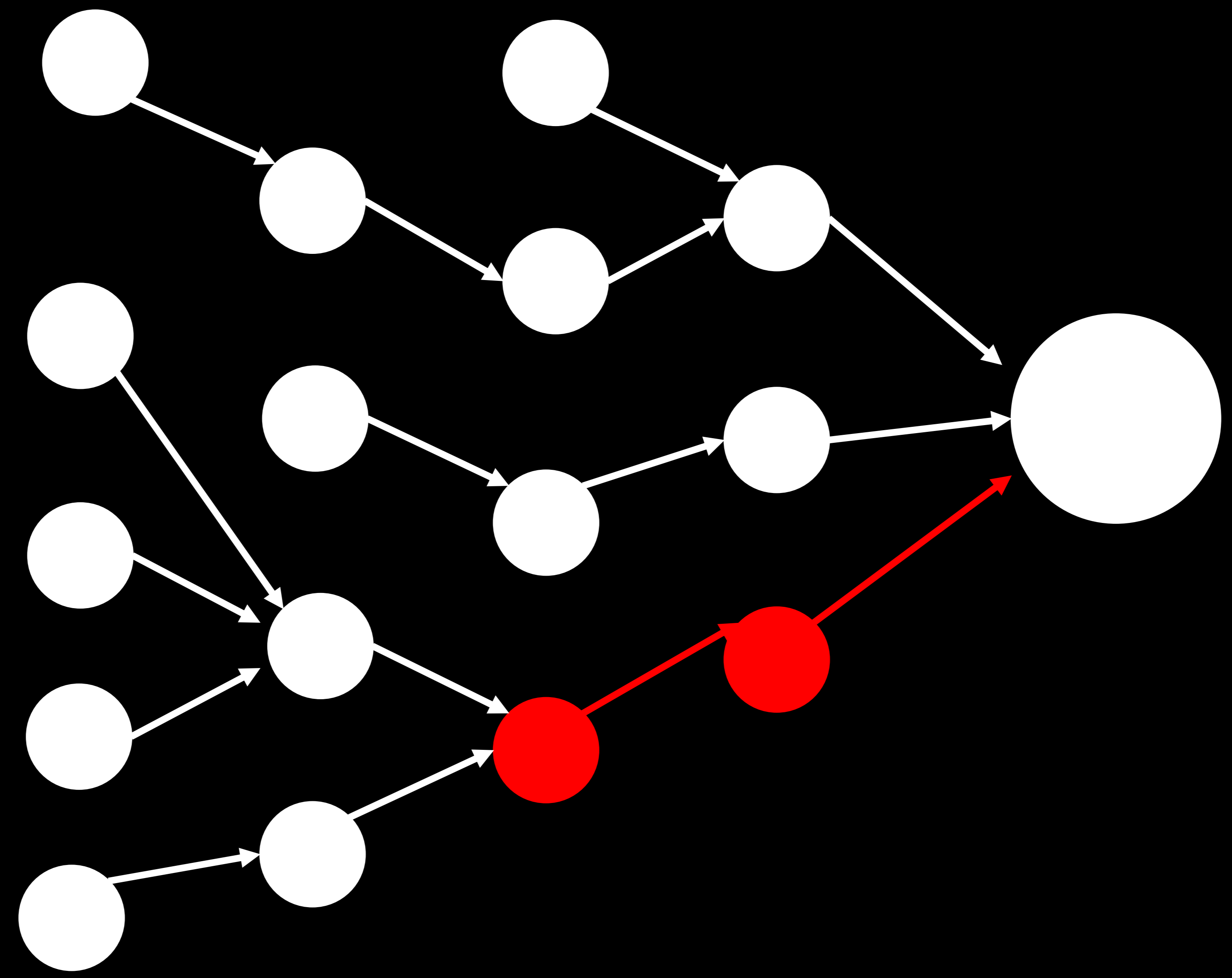
The count of unique attack paths...  
using any available abuseable relationship...  
between any identity to a destination





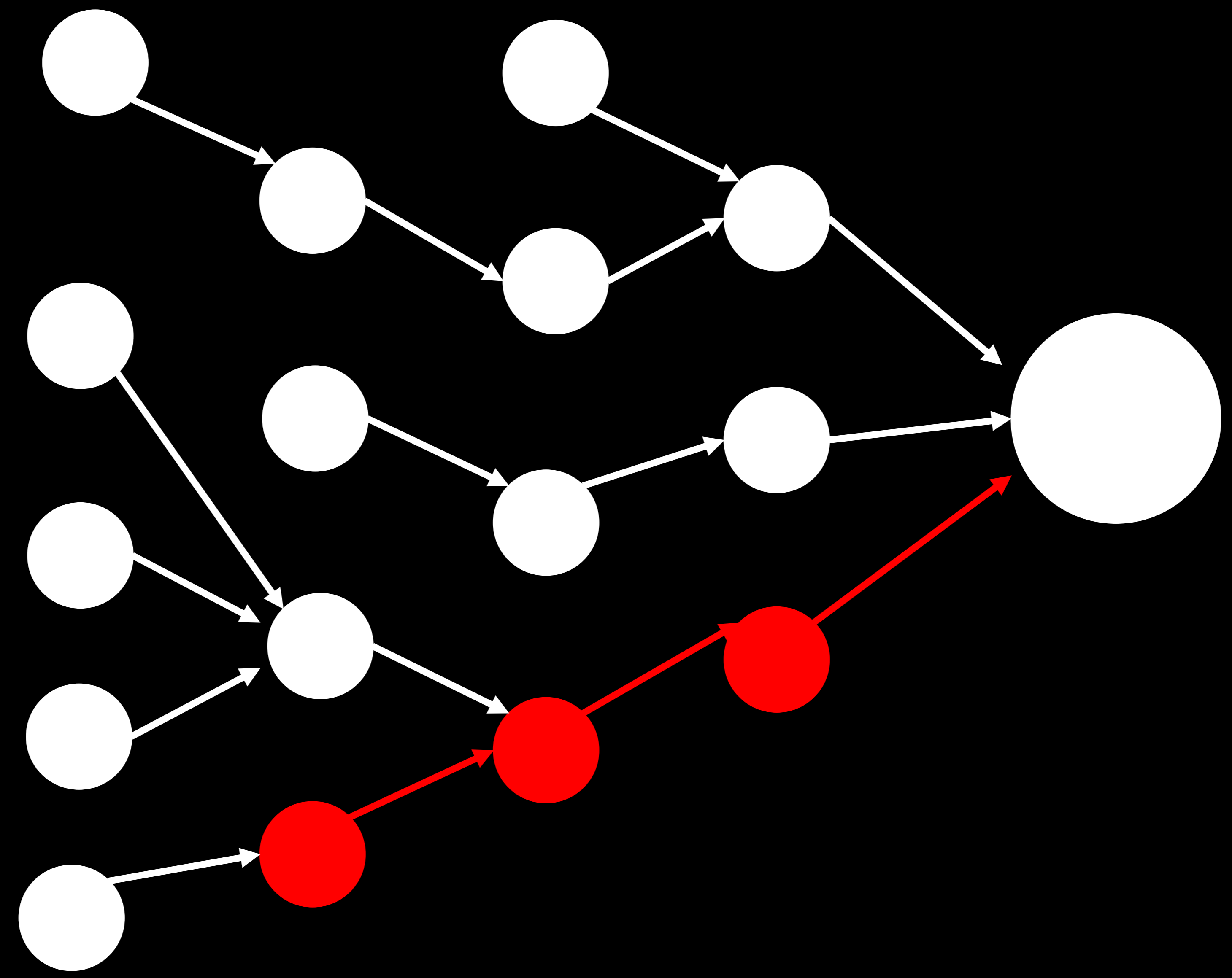
Attack Path  
Count:

**2**



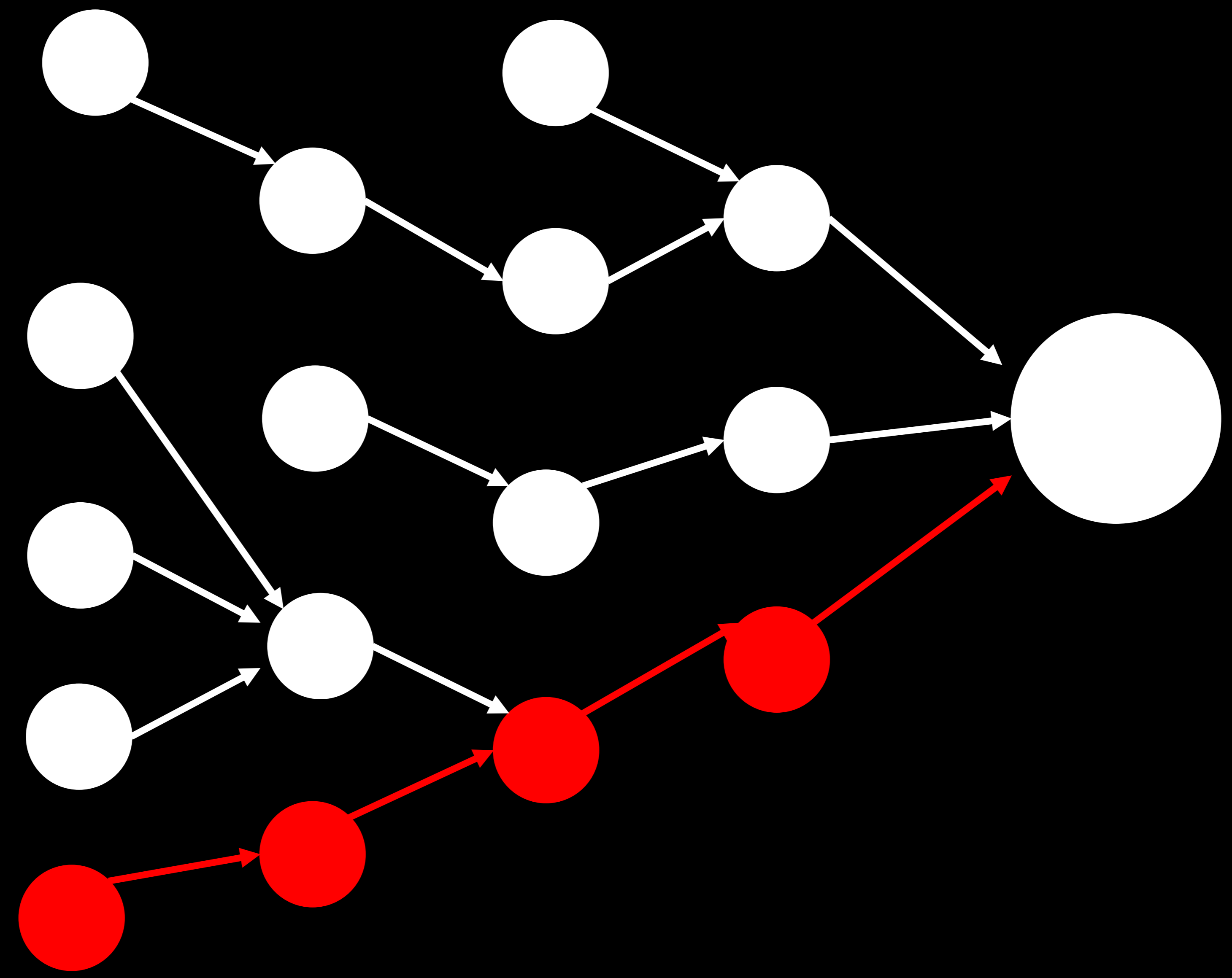
Attack Path  
Count:

**3**



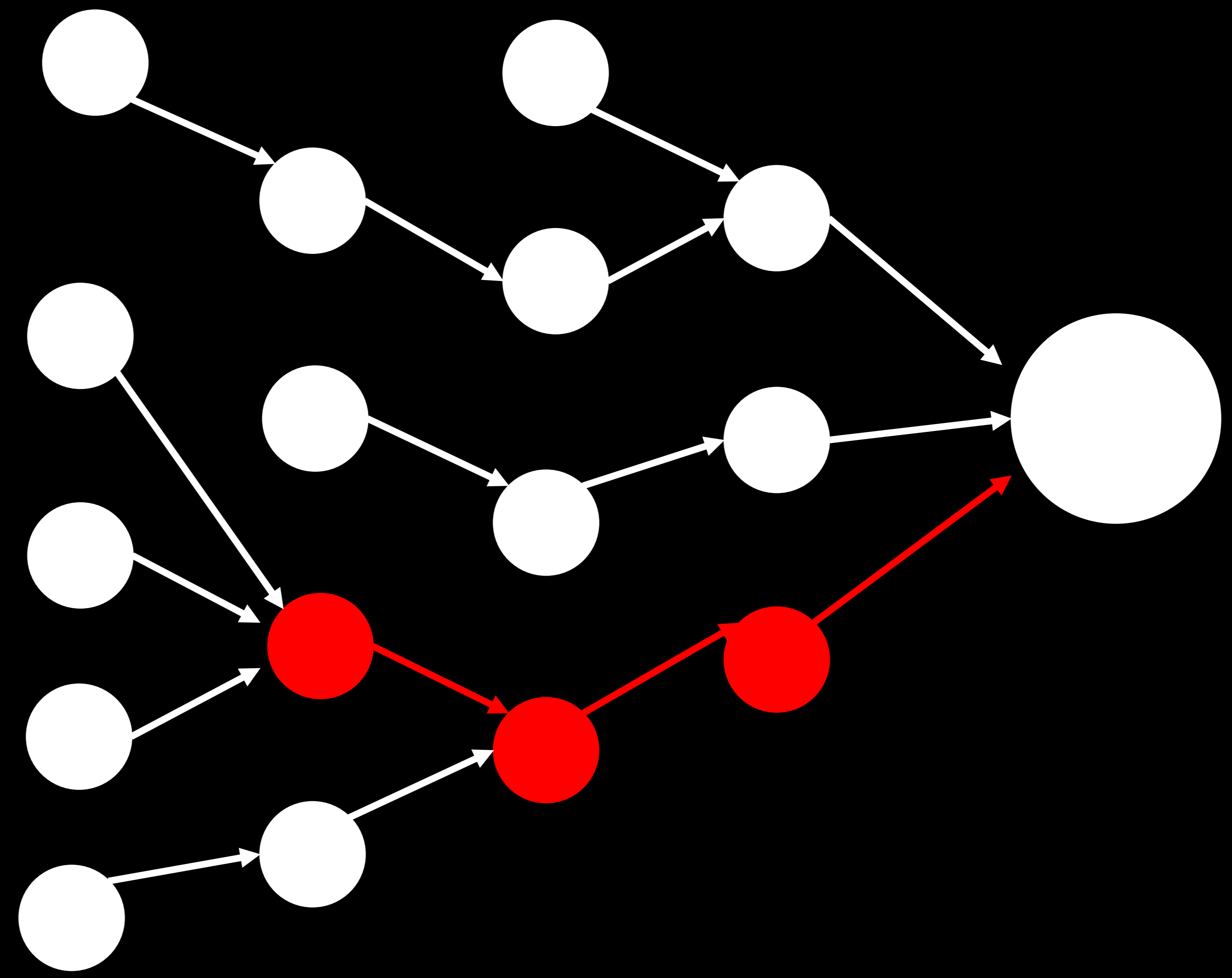
Attack Path  
Count:

4



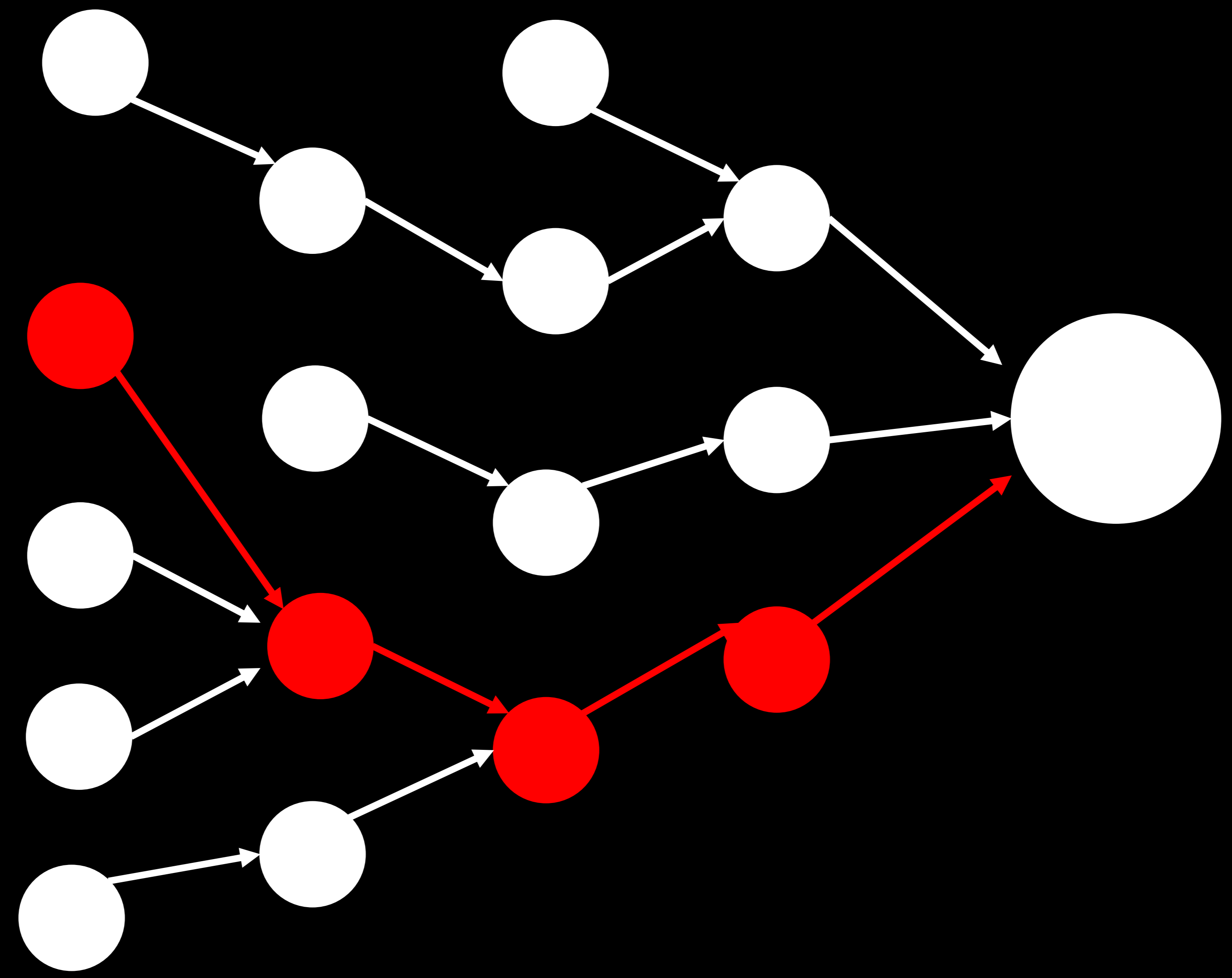
Attack Path  
Count:

**5**



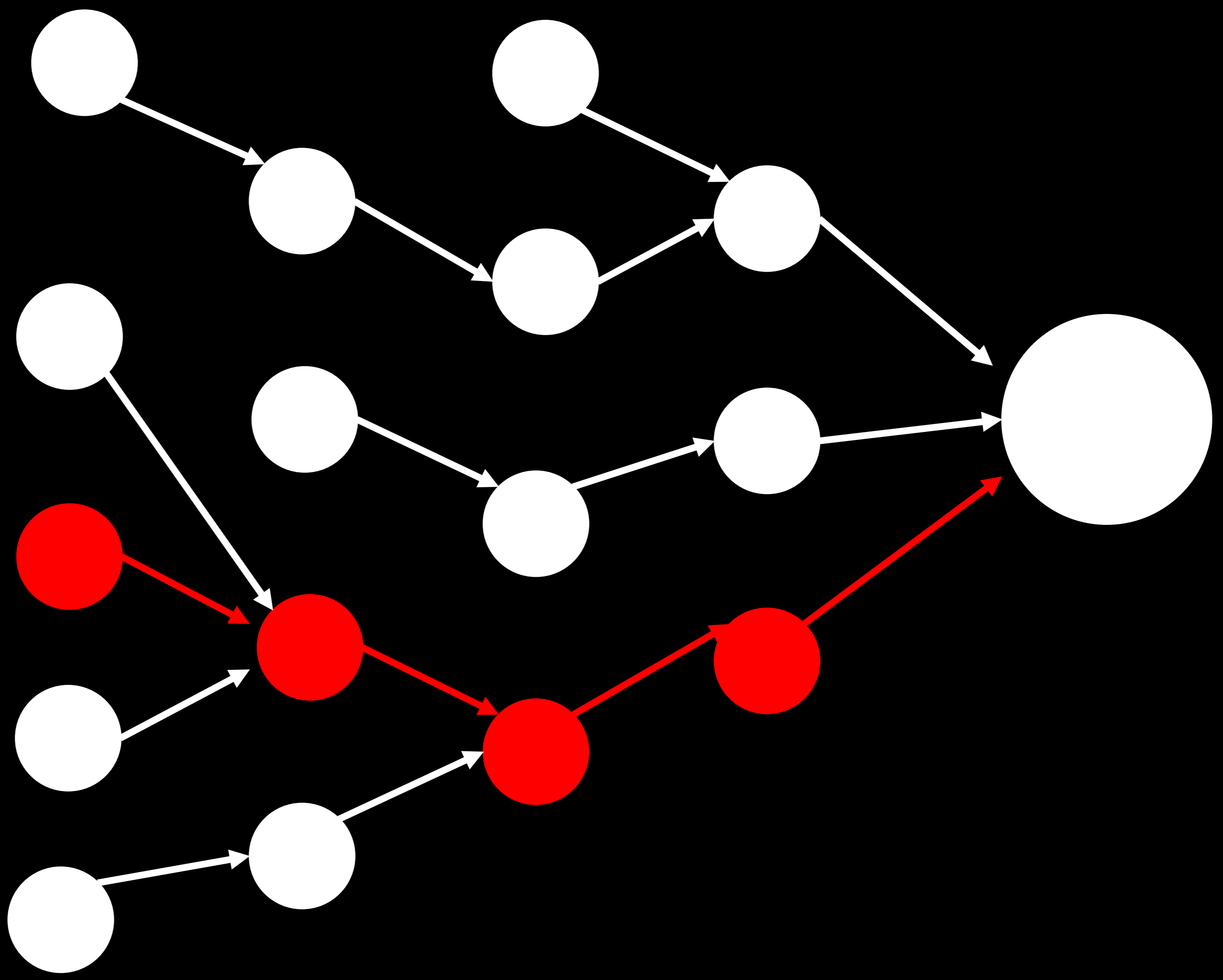
Attack Path  
Count:

6



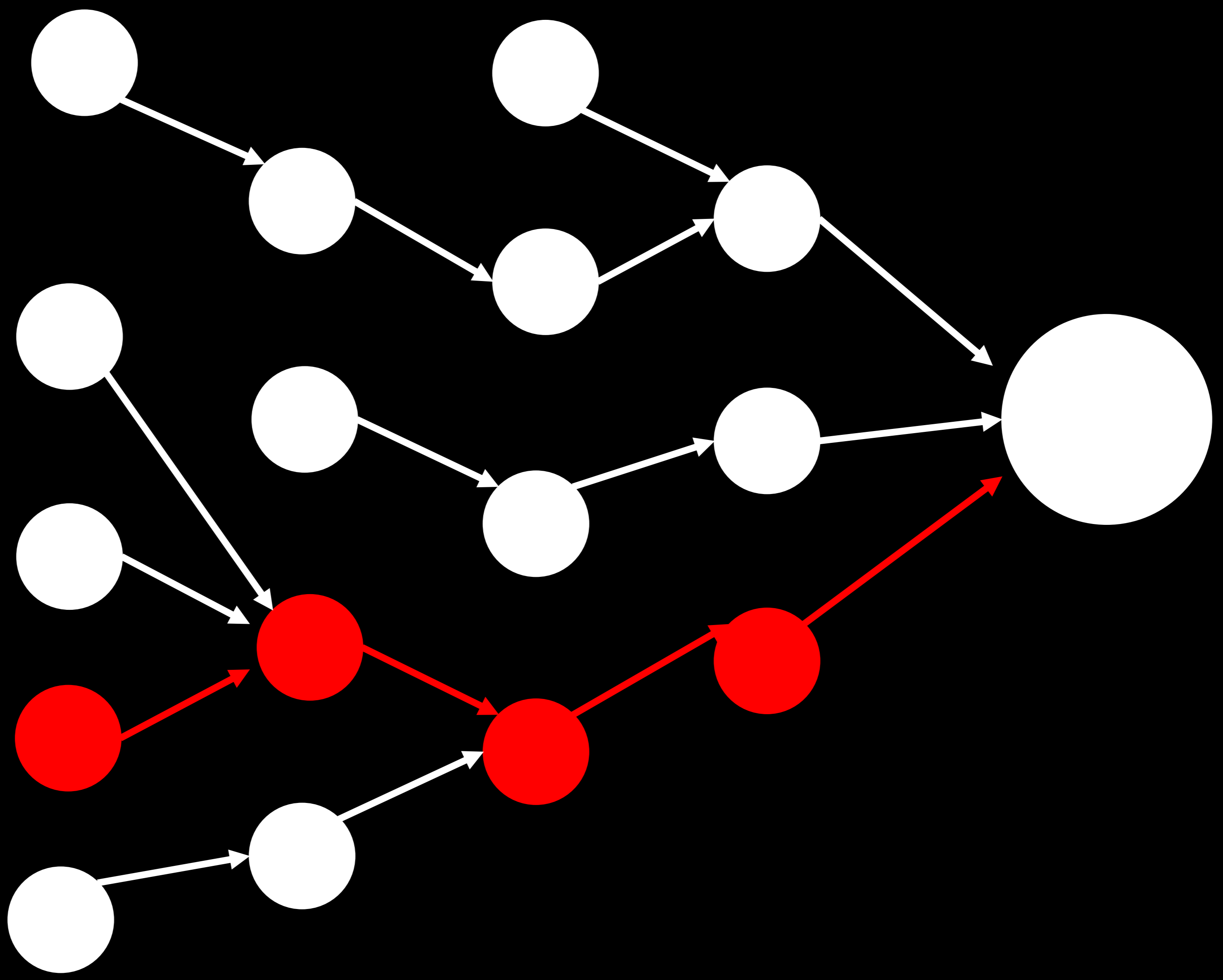
Attack Path  
Count:

7



Attack Path  
Count:

8



More  
Identities

More  
Attack Paths

5k

| 5M

10k

■ 22M

20k

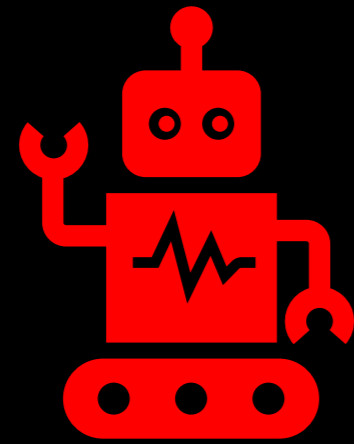
■ 75M

40k

■ 752M

Average unique Attack Path count to Privileged Identities/Resources in Microsoft AD / Entra ID

# And like all problems, worse with AI



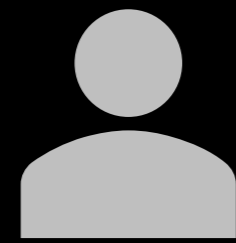
Every AI agent needs an identity

**20:1**

NHIs outnumber Humans 20-to-1

**150%**

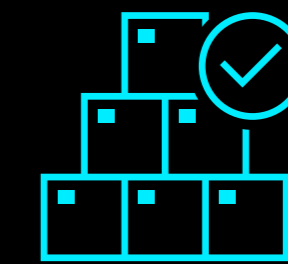
Growth in NHIs this year



How Attack Paths  
Bypass Controls

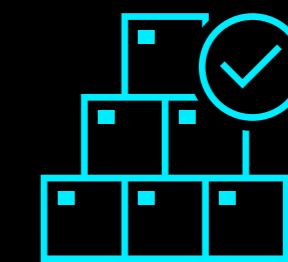


The Scale of  
Attack Paths



Attack Path  
Management

The continuous discovery,  
mapping, and risk assessment  
of Attack Path Choke Points.



Attack Path  
Management

# Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword

# Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound (**FREE**) to visualize attack paths

# Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound (**FREE**) to visualize attack paths
3. Identify and prioritize attack path choke points

# Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound (**FREE**) to visualize attack paths
3. Identify and prioritize attack path choke points
4. Once established, address hybrid attack path risk

# Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound (**FREE**) to visualize attack paths
3. Identify and prioritize attack path choke points
4. Once established, address hybrid attack path risk
5. Track and report Key Performance Indicators (KPIs)



2025 Data Breach  
Investigations Report

Microsoft  
Defense  
The founda  
frontiers of



verizon  
business

CROWDSTRIKE

2025  
GLOBAL THREAT  
REPORT

***“Implement least-privilege  
access principles.”***

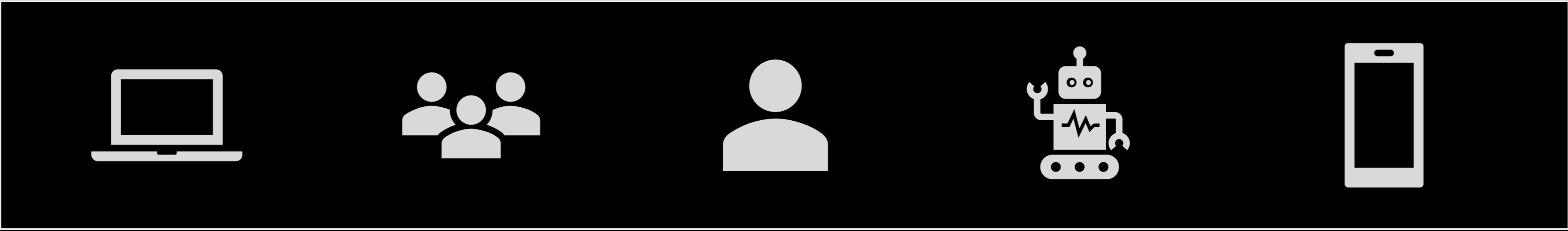
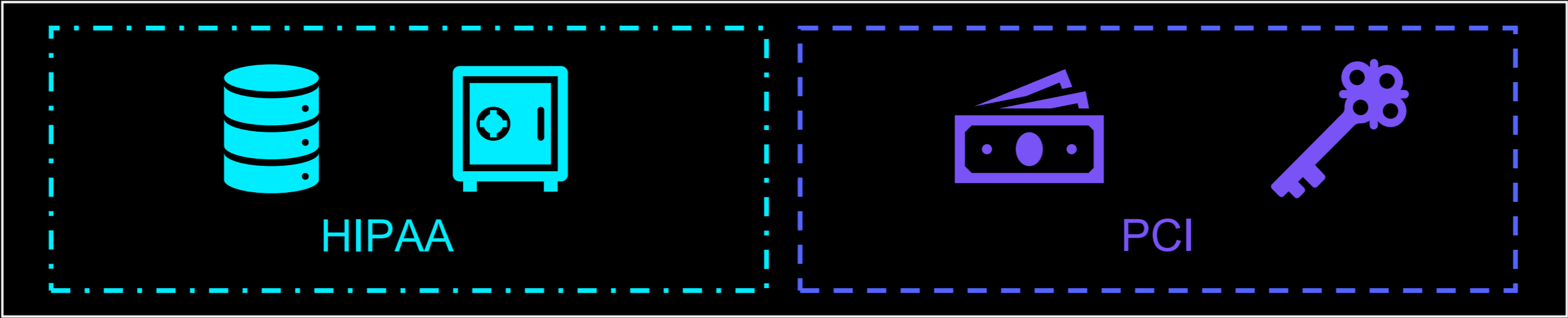
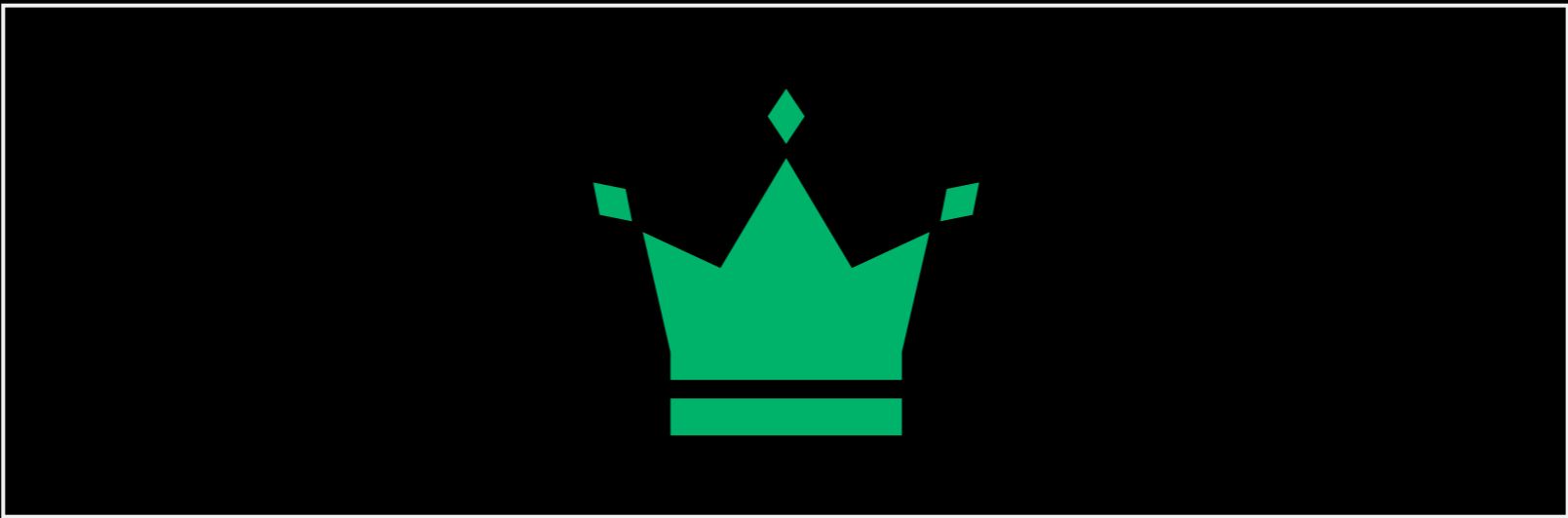
*CrowdStrike 2025 Global Threat Report*

***“Restrict Administrator  
Privileges to Dedicated  
Administrator Accounts”***

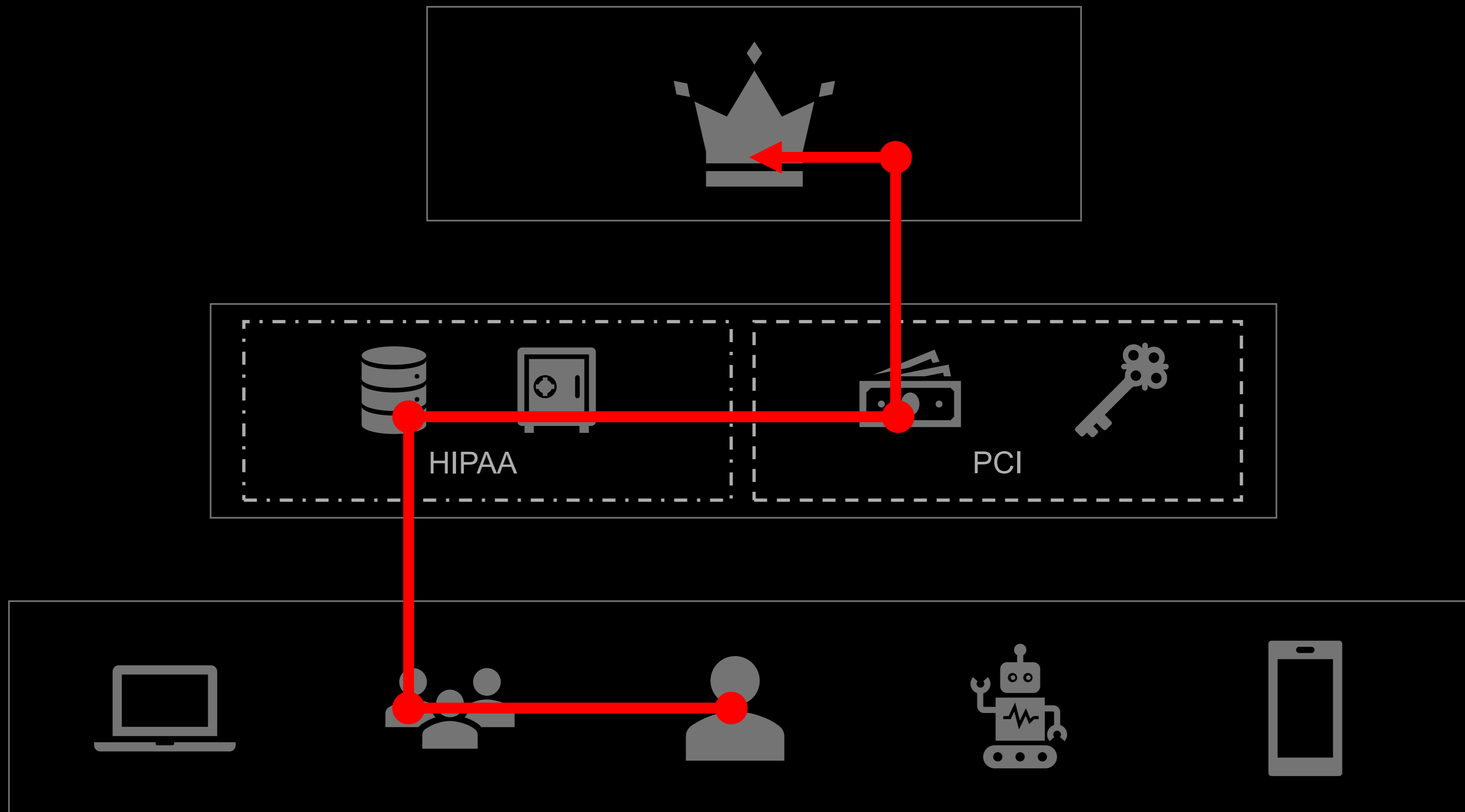
*Verizon 2025 DBIR*

***“Govern permissions to ensure  
identities have only the  
privileges they need.”***

*Microsoft 2024 Digital Defense Report*



# 1. “Attack Path” is not a red team buzzword



Attack Paths are violations/vulnerabilities of privilege boundaries

# 2. Use BloodHound to visualize Attack Paths

The screenshot displays the BloodHound interface with a network graph and a detailed view of the user JASON@PHANTOM.CORP.

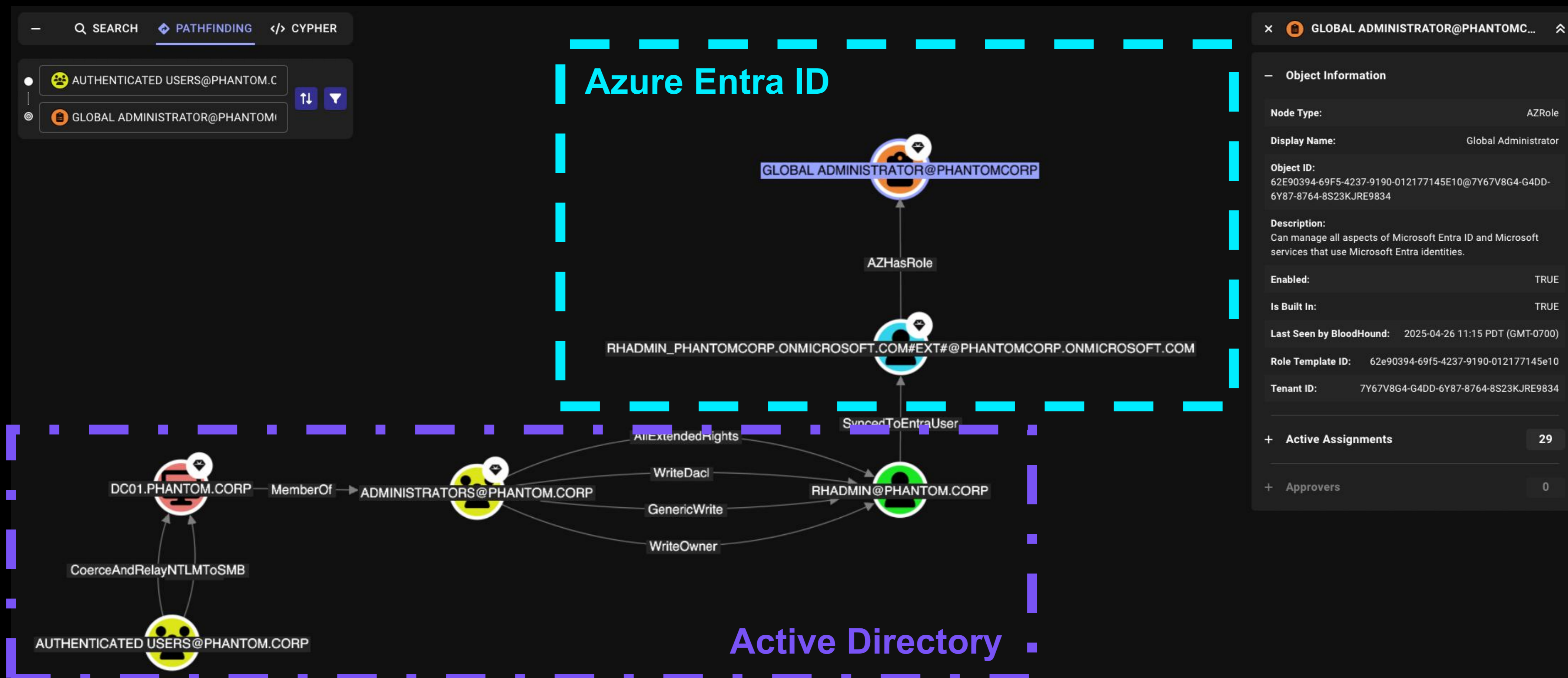
**Network Graph:**

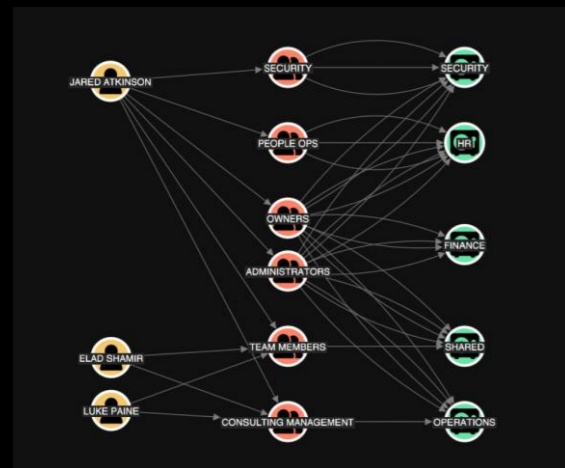
- Nodes:** JASON@PHANTOM.CORP (User), DOMAIN USERS@PHANTOM.CORP (Group), AUTHENTICATED USERS@PHANTOM.CORP (Group), DC01.PHANTOM.CORP (DC), PAYMENT01.PHANTOM.CORP (DC), ALICE-LAPTOP.PHANTOM.CORP (Laptop), AM-WIN10-DEV02.PHANTOM.CORP (Laptop), JD@PHANTOM.CORP (User), ADMINISTRATORS@PHANTOM.CORP (Group), SVC\_PAYADMIN@PHANTOM.CORP (Service), ANDY@PHANTOM.CORP (User), ADMINISTRATOR@PHANTOM.CORP (User), DOMAIN ADMINS@PHANTOM.CORP (Group).
- Relationships:**
  - JASON@PHANTOM.CORP is a member of DOMAIN USERS@PHANTOM.CORP.
  - DOMAIN USERS@PHANTOM.CORP is a member of AUTHENTICATED USERS@PHANTOM.CORP.
  - AUTHENTICATED USERS@PHANTOM.CORP has administrative rights (AdminTo) over DC01.PHANTOM.CORP, PAYMENT01.PHANTOM.CORP, ALICE-LAPTOP.PHANTOM.CORP, and AM-WIN10-DEV02.PHANTOM.CORP.
  - DC01.PHANTOM.CORP has a session (HasSession) with JD@PHANTOM.CORP and is a member of ADMINISTRATORS@PHANTOM.CORP.
  - PAYMENT01.PHANTOM.CORP has sessions (HasSession) with SVC\_PAYADMIN@PHANTOM.CORP and ADMINISTRATOR@PHANTOM.CORP.
  - ALICE-LAPTOP.PHANTOM.CORP has sessions (HasSession) with ADMINISTRATOR@PHANTOM.CORP and ANDY@PHANTOM.CORP.
  - AM-WIN10-DEV02.PHANTOM.CORP has sessions (HasSession) with ANDY@PHANTOM.CORP and ADMINISTRATOR@PHANTOM.CORP.
  - JD@PHANTOM.CORP has administrative rights (WriteDacl, GenericWrite, WriteOwner) over DOMAIN ADMINS@PHANTOM.CORP.
  - ADMINISTRATORS@PHANTOM.CORP is a member of DOMAIN ADMINS@PHANTOM.CORP.
  - SVC\_PAYADMIN@PHANTOM.CORP has administrative rights (AddMember) over DOMAIN ADMINS@PHANTOM.CORP.
  - ADMINISTRATOR@PHANTOM.CORP is a member of DOMAIN ADMINS@PHANTOM.CORP.

**User Information: JASON@PHANTOM.CORP**

Property	Value
Node Type	User
Display Name	jason
Object ID	S-1-5-21-2697957641-2271029196-387917394-2249
ACL Inheritance Denied	TRUE
Admin Count	FALSE
Allows Unconstrained Delegation	FALSE
Created	2023-11-07 01:03 PST (GMT-0800)
Distinguished Name	CN=DC01.PHANTOM.CORP,CN=USERS,DC=PHANTOM,DC=C...
Do Not Require Pre-Authentication	FALSE
Domain FQDN	PHANTOM.CORP
Domain SID	S-1-5-21-2697957641-2271029196-387917394
Enabled	TRUE
Last Logon (Replicated)	2024-02-21 01:32 PST (GMT-0800)
Last Logon	2024-02-21 01:34 PST (GMT-0800)
Last Seen by BloodHound	2025-04-26 11:15 PDT (GMT-0700)
Marked Sensitive	FALSE
Owner SID	S-1-5-21-2697957641-2271029196-387917394-512
Password Last Set	2023-11-07 09:03 PST (GMT-0800)
Password Never Expires	TRUE
Password Not Required	FALSE
SAM Account Name	jason
Trusted For Constrained Delegation	FALSE

# 2. Use BloodHound to visualize Attack Paths

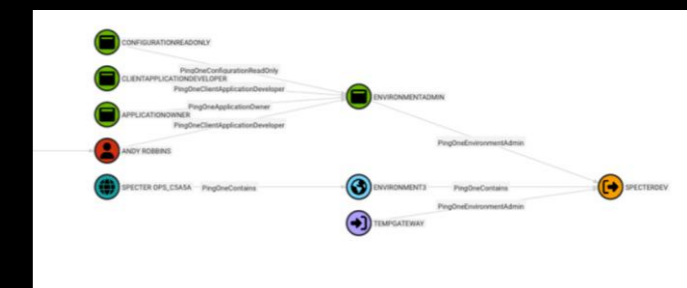


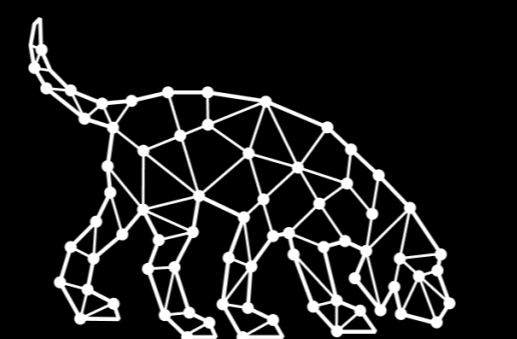


 **1Password**

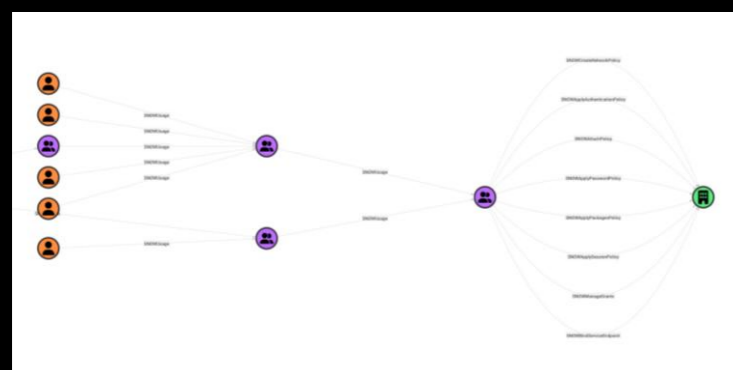
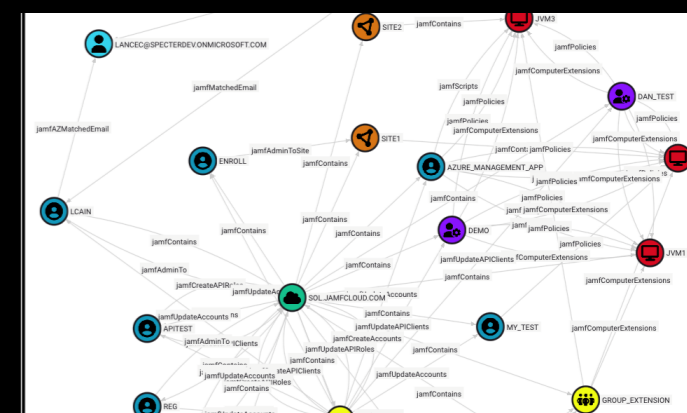
 **Microsoft**

 **PingIdentity**



  
**BLOODHOUND  
OpenGraph**

 **jamf**



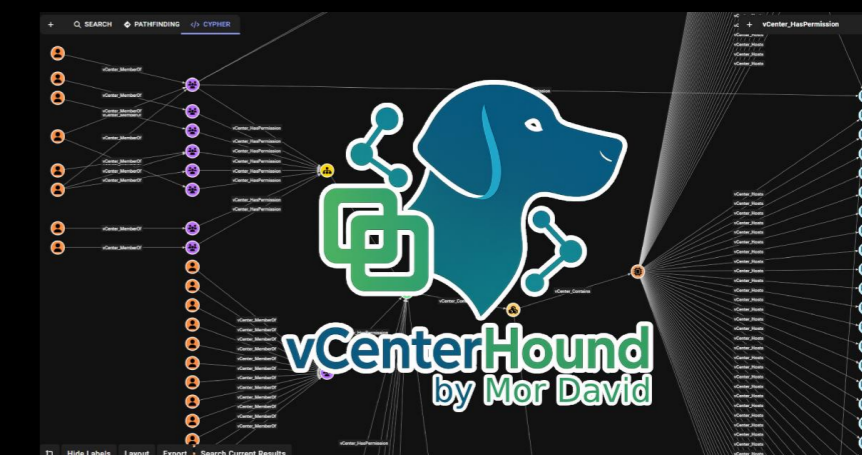
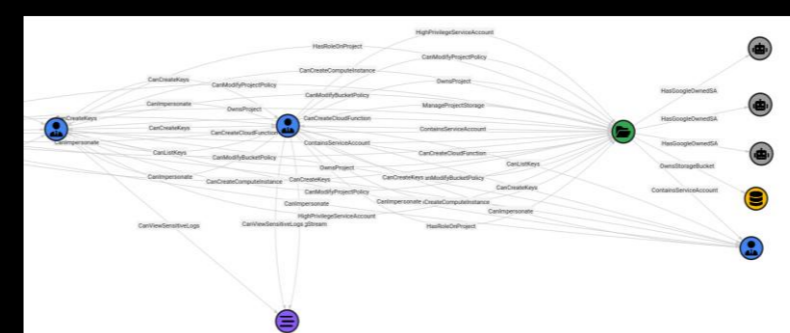
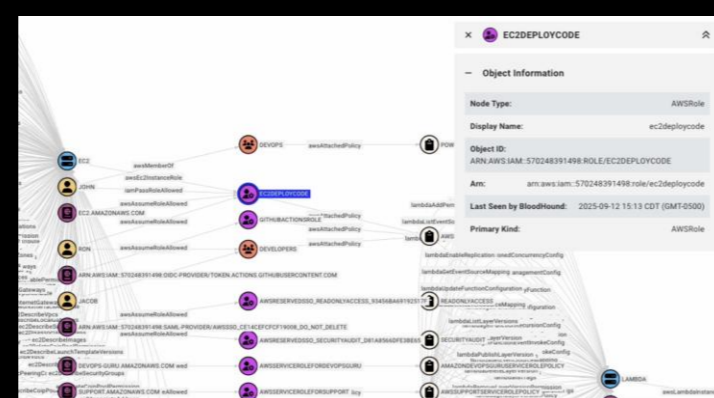
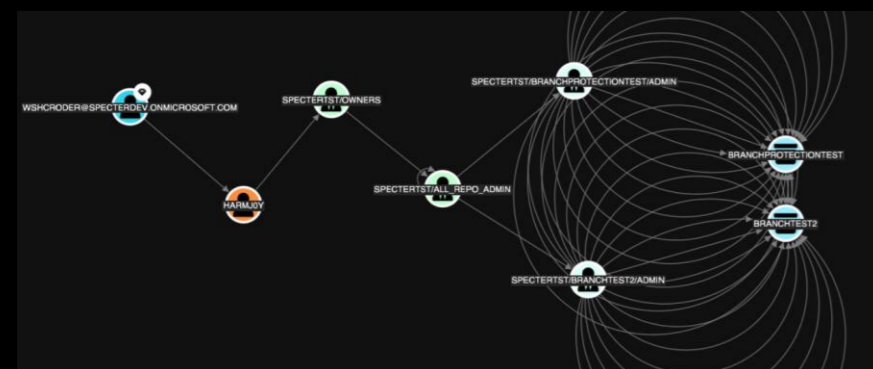
 **snowflake**

  
**GitHub**

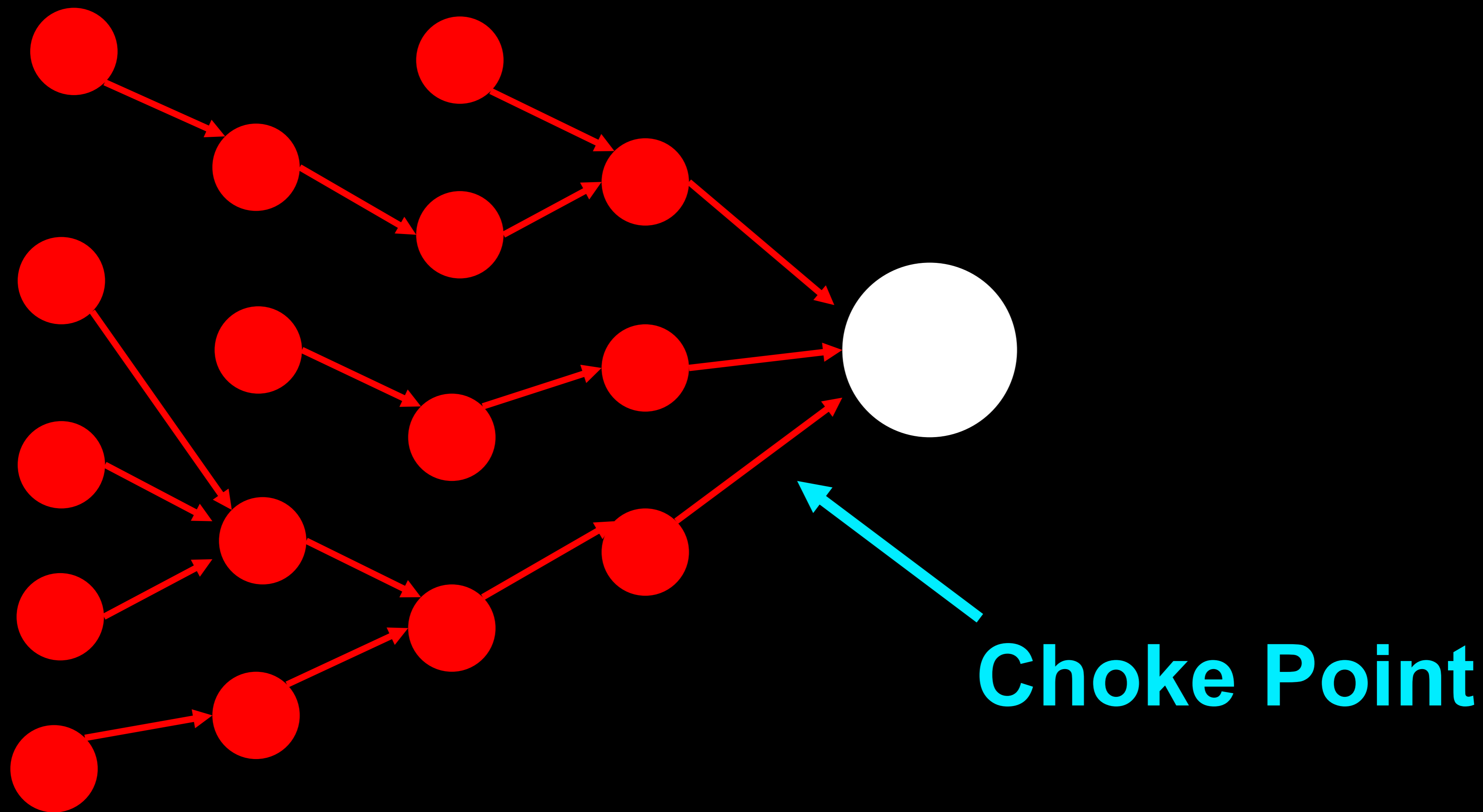
  
**aws**

  
**Google Cloud**

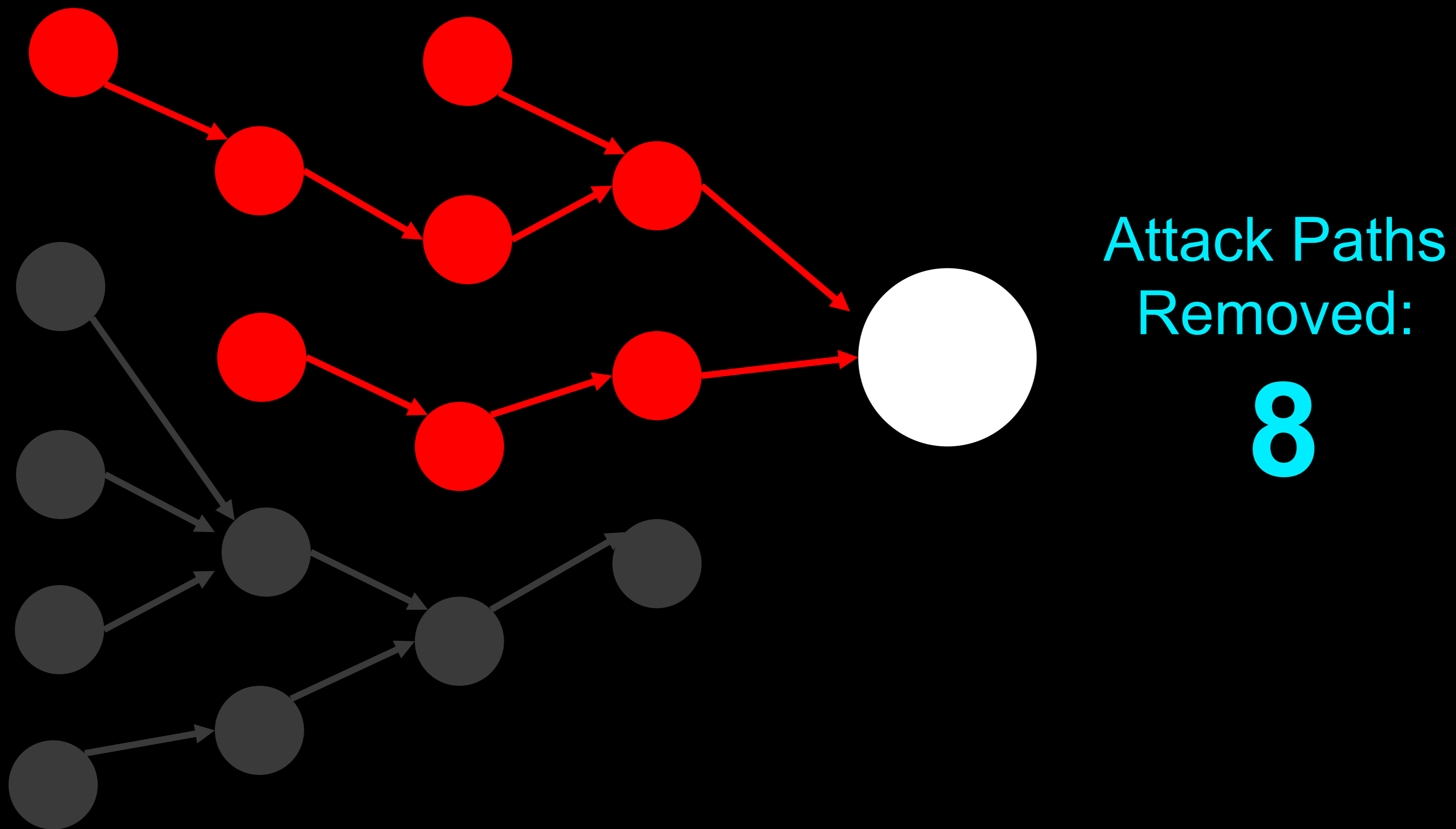
  
**vmware**  
by Broadcom



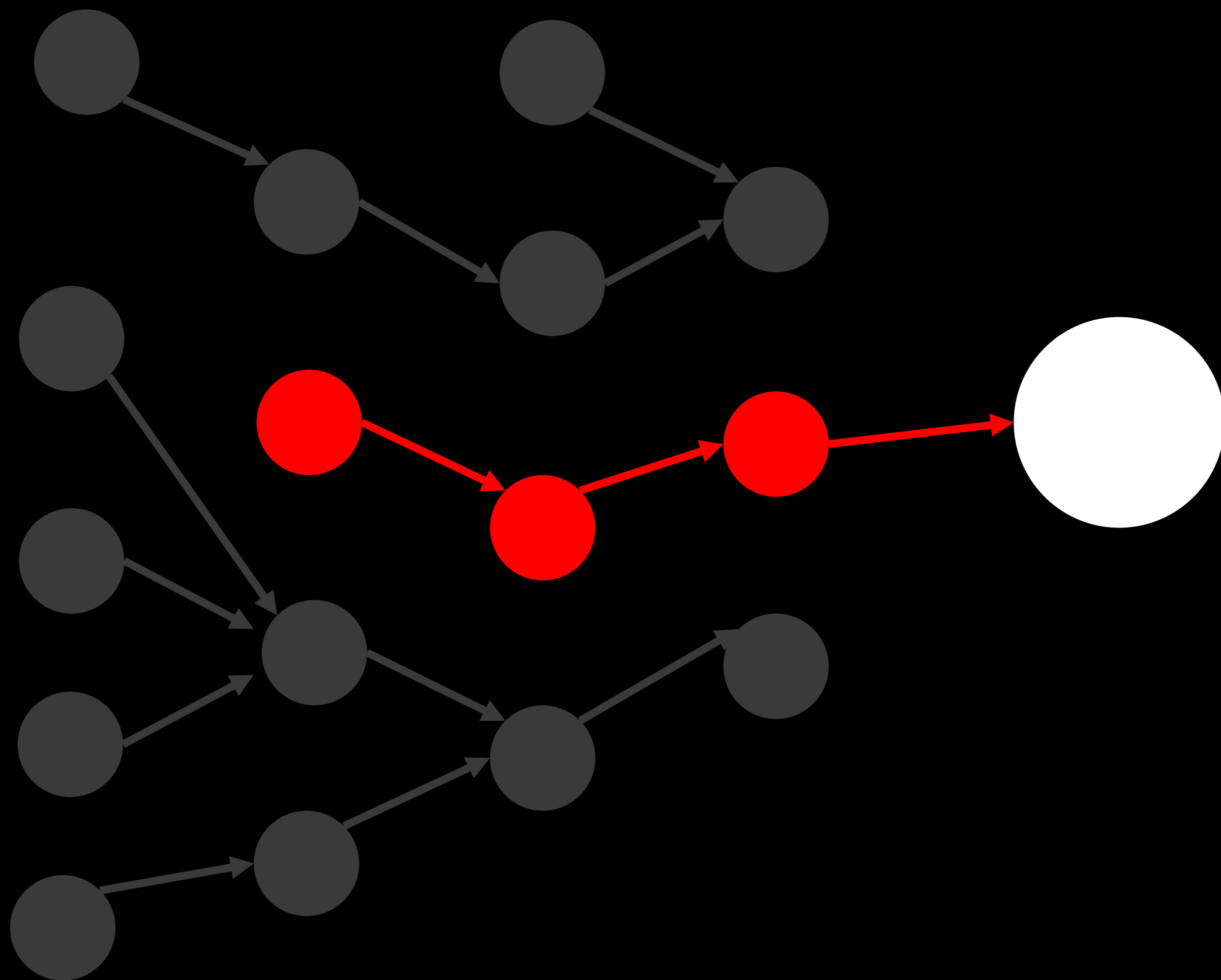
### 3. Identify and Prioritize Attack Path Choke Points



### 3. Identify and Prioritize Attack Path Choke Points



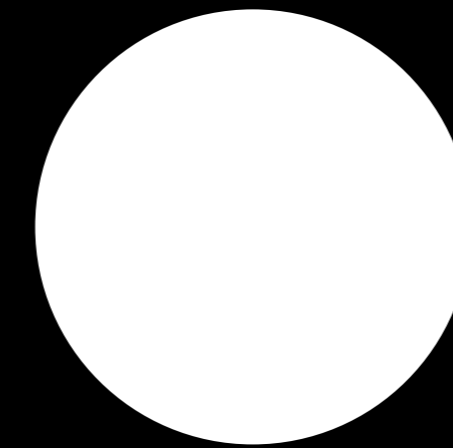
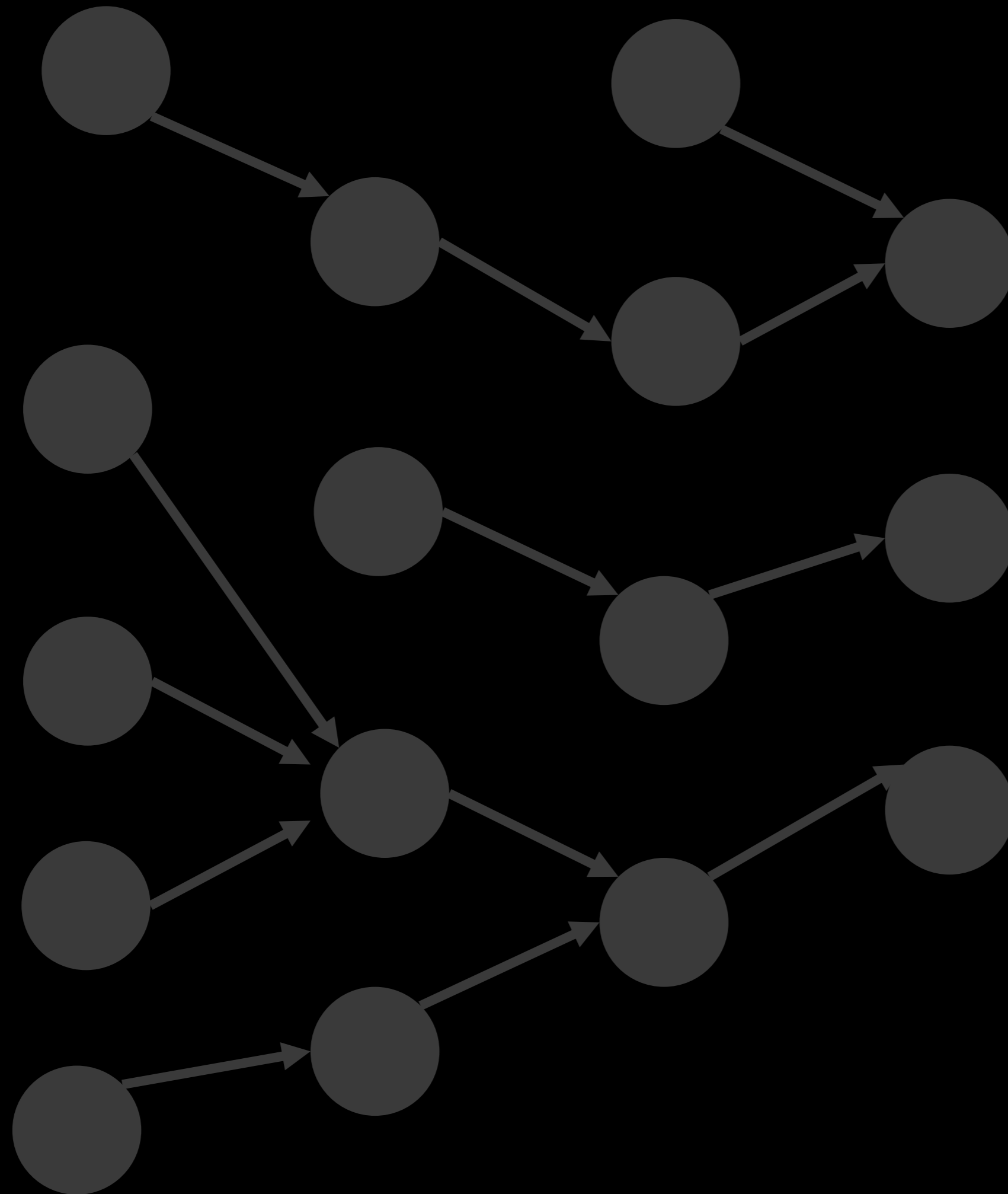
### 3. Identify and Prioritize Attack Path Choke Points



Attack Paths  
Removed:

**13**

### 3. Identify and Prioritize Attack Path Choke Points



Attack Paths  
Removed:

**16**

# 3. Identify and Prioritize Attack Path Choke Points

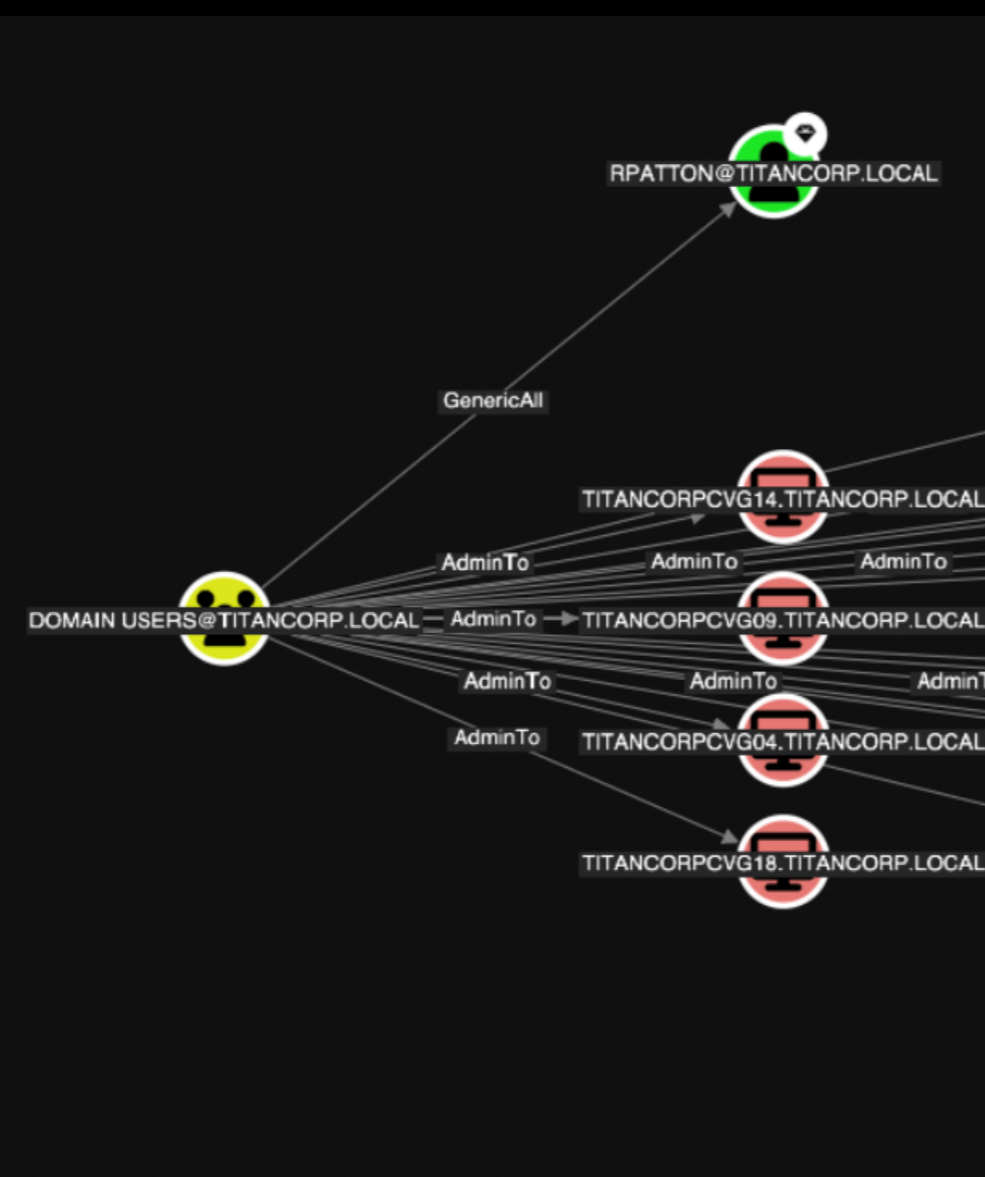
▼ Saved Queries

Search [ ] Import Export [ ]

Platforms: Active Directory Categories Source

Active Directory

- Servers where Domain Users can RDP  
*Active Directory, Dangerous Privileges*
- Dangerous privileges for Domain Users groups  
*Active Directory, Dangerous Privileges*
- Domain Admins logons to non-Domain Controllers  
*Active Directory, Dangerous Privileges*
- Kerberoastable members of Tier Zero / High Value groups  
*Active Directory, Kerberos Interaction*
- All Kerberoastable users  
*Active Directory, Kerberos Interaction*
- Kerberoastable users with most admin privileges  
*Active Directory, Kerberos Interaction*
- AS-REP Roastable users (DontReqPreAuth)  
*Active Directory, Kerberos Interaction*
- Shortest paths to systems trusted for unconstrained delegation  
*Active Directory, Shortest Paths*



Initial Access Choke Points:  
Privileges held by large groups

SEARCH PATHFINDING CYPHER

^ Saved Queries

Auto-run selected query

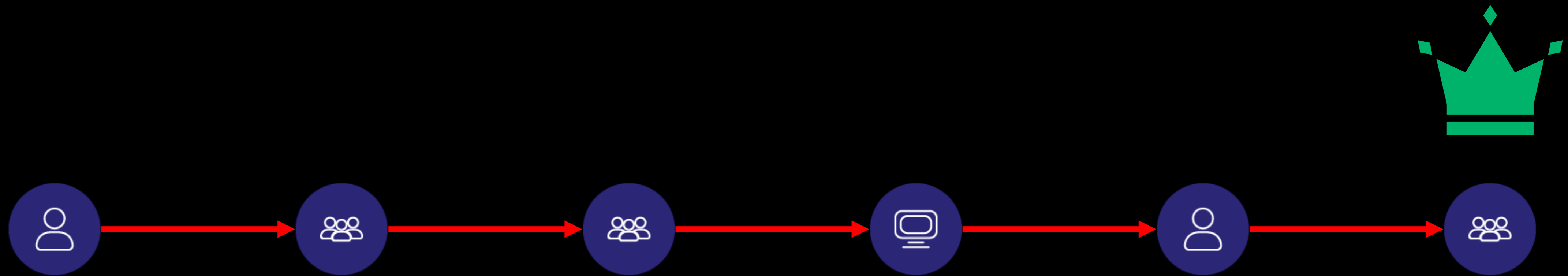
```
1 MATCH p = (n:User)-[:Owns]->(c:Computer)
2 WHERE c.isdc = True
3 RETURN p
```

Tag Save Run

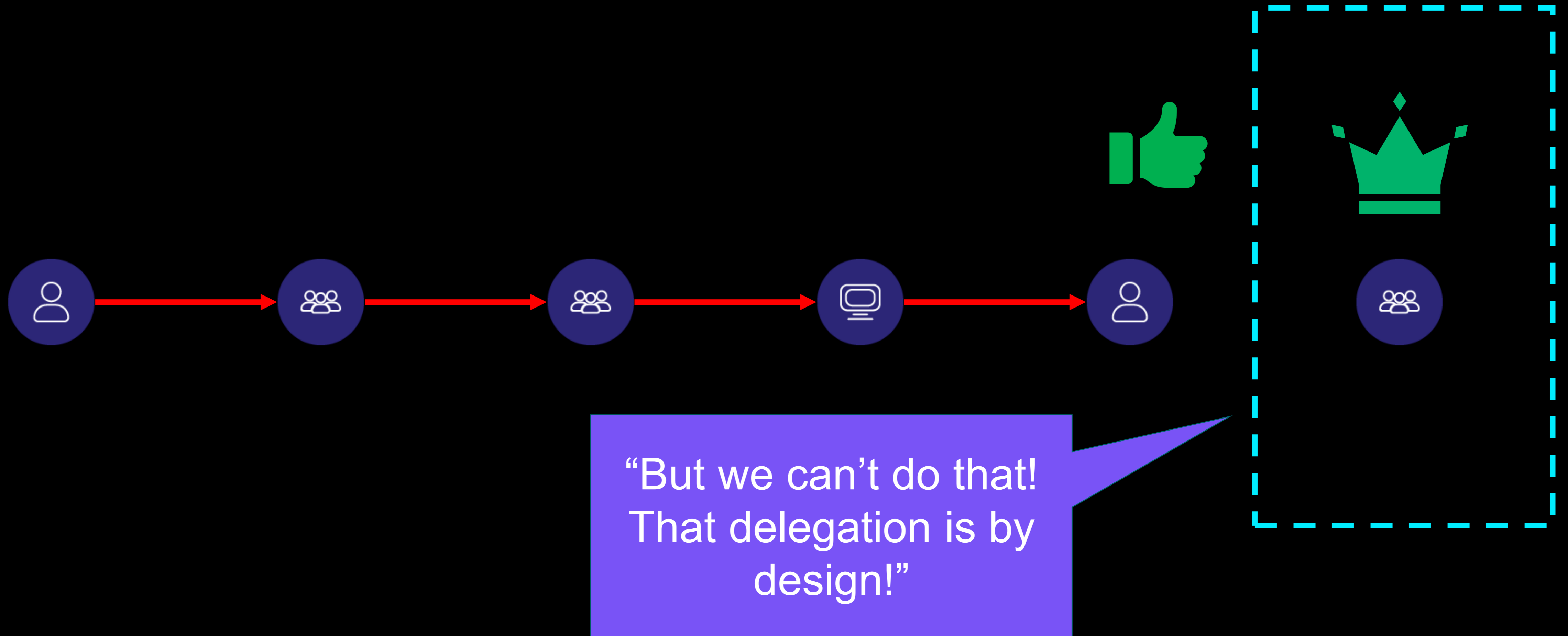
SVC\_DOMAINJOIN@PHANTOM.CORP Owns DC01.PHANTOM.CORP

Destination Choke Points:  
Privileges over critical identities  
and resources

# 3. Identify and Prioritize Attack Path Choke Points

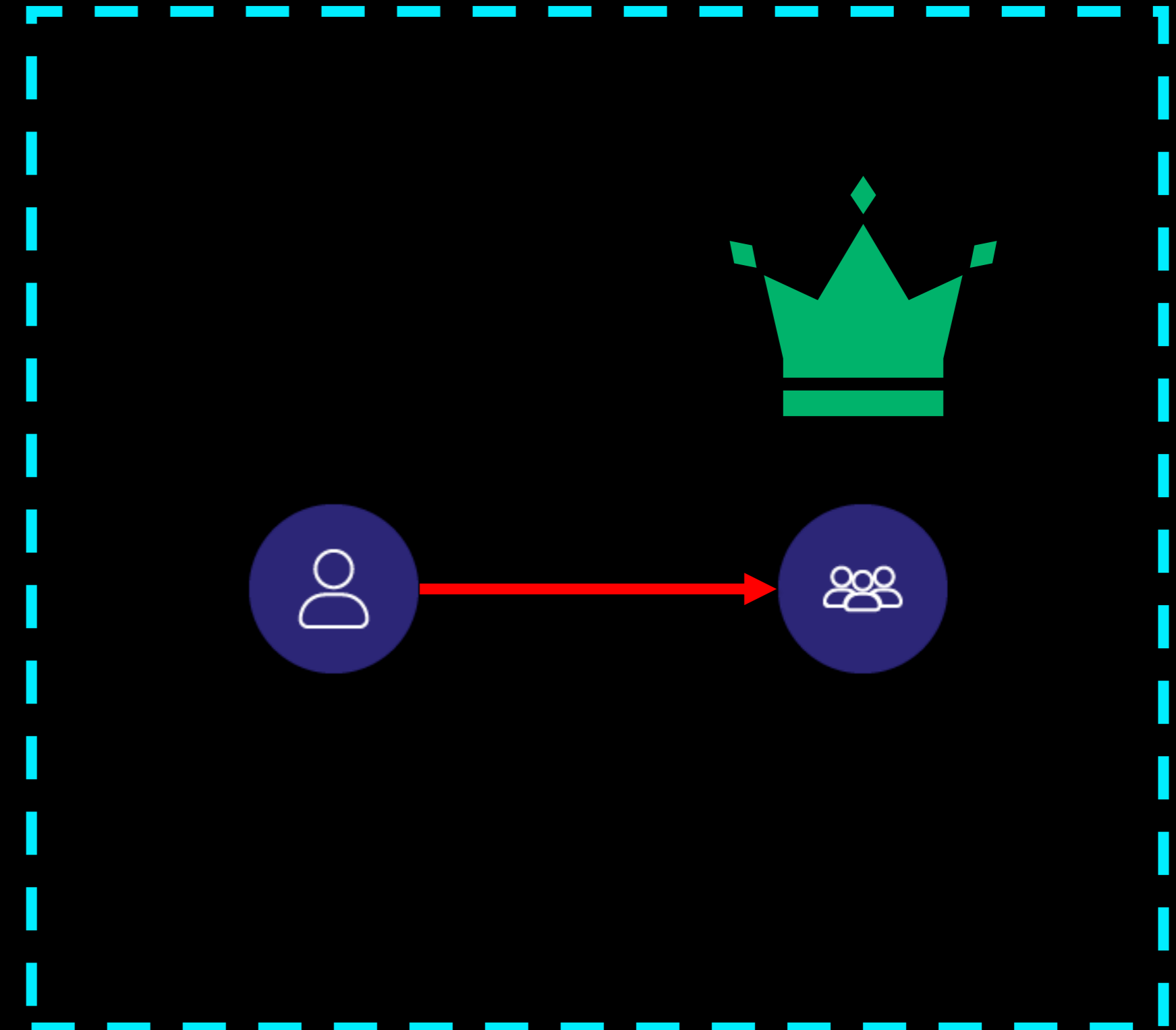


# 3. Identify and Prioritize Attack Path Choke Points



# 3. Identify and Prioritize Attack Path Choke Points

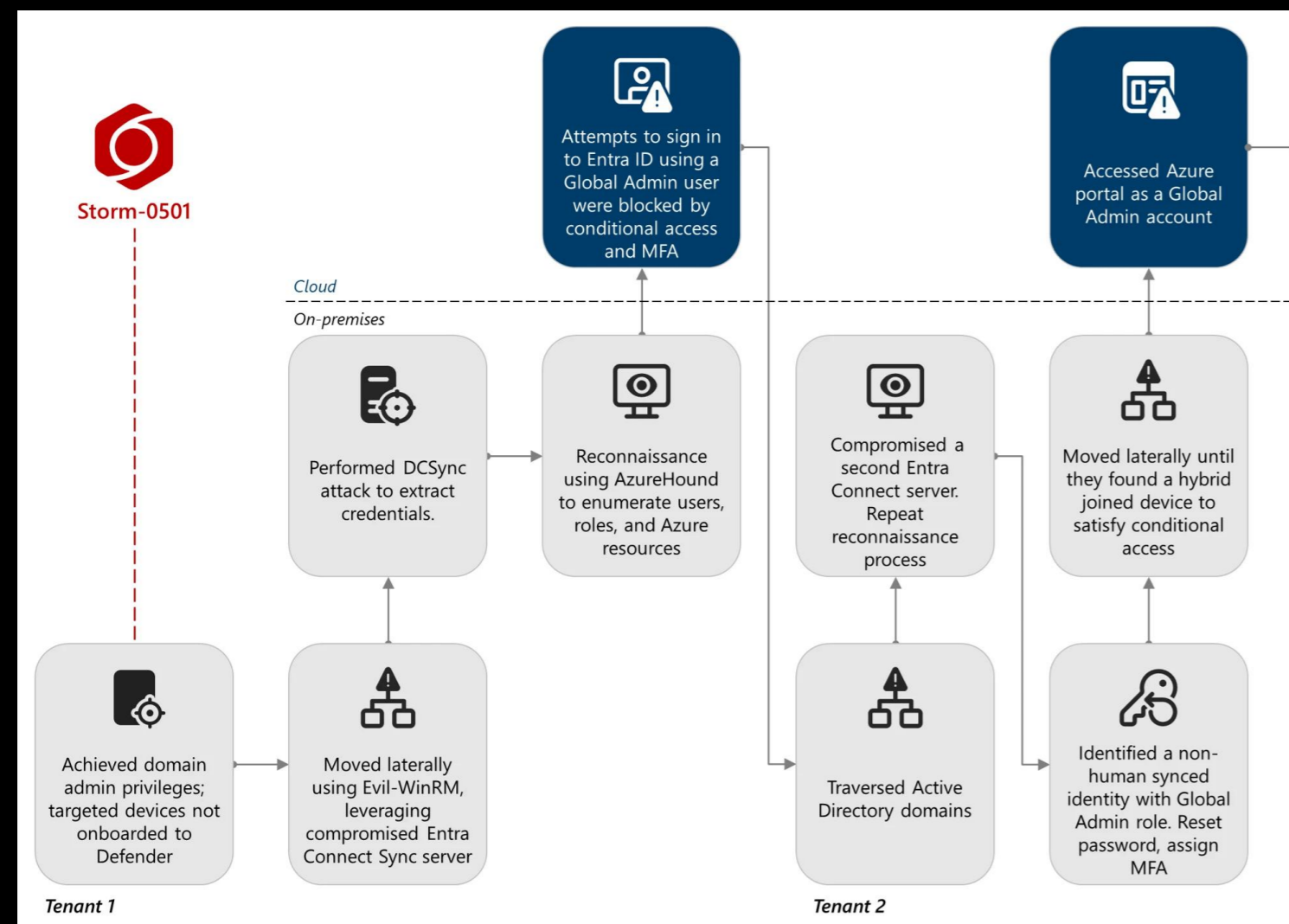
Also 



# 4. Once Established, Address Hybrid Attack Path Risk

Storm-0501's evolving techniques lead to cloud-based ransomware

By [Microsoft Threat Intelligence](#)



## Ensure separate user accounts and mail forwarding for Global Administrator accounts

Personal email accounts are regularly phished by cyber attackers, a risk that makes personal email addresses unacceptable for Global Administrator accounts. To help separate internet risks from administrative privileges, create dedicated accounts for each user with administrative privileges.

- Be sure to create separate accounts for users to do Global Administrator tasks.
- Make sure that your Global Administrators don't accidentally open emails or run programs with their administrator accounts.
- Be sure those accounts have their email forwarded to a working mailbox.
- Global Administrator (and other privileged groups) accounts should be cloud-only accounts with no ties to on-premises Active Directory.

# 4. Once Established, Address Hybrid Attack Path Risk

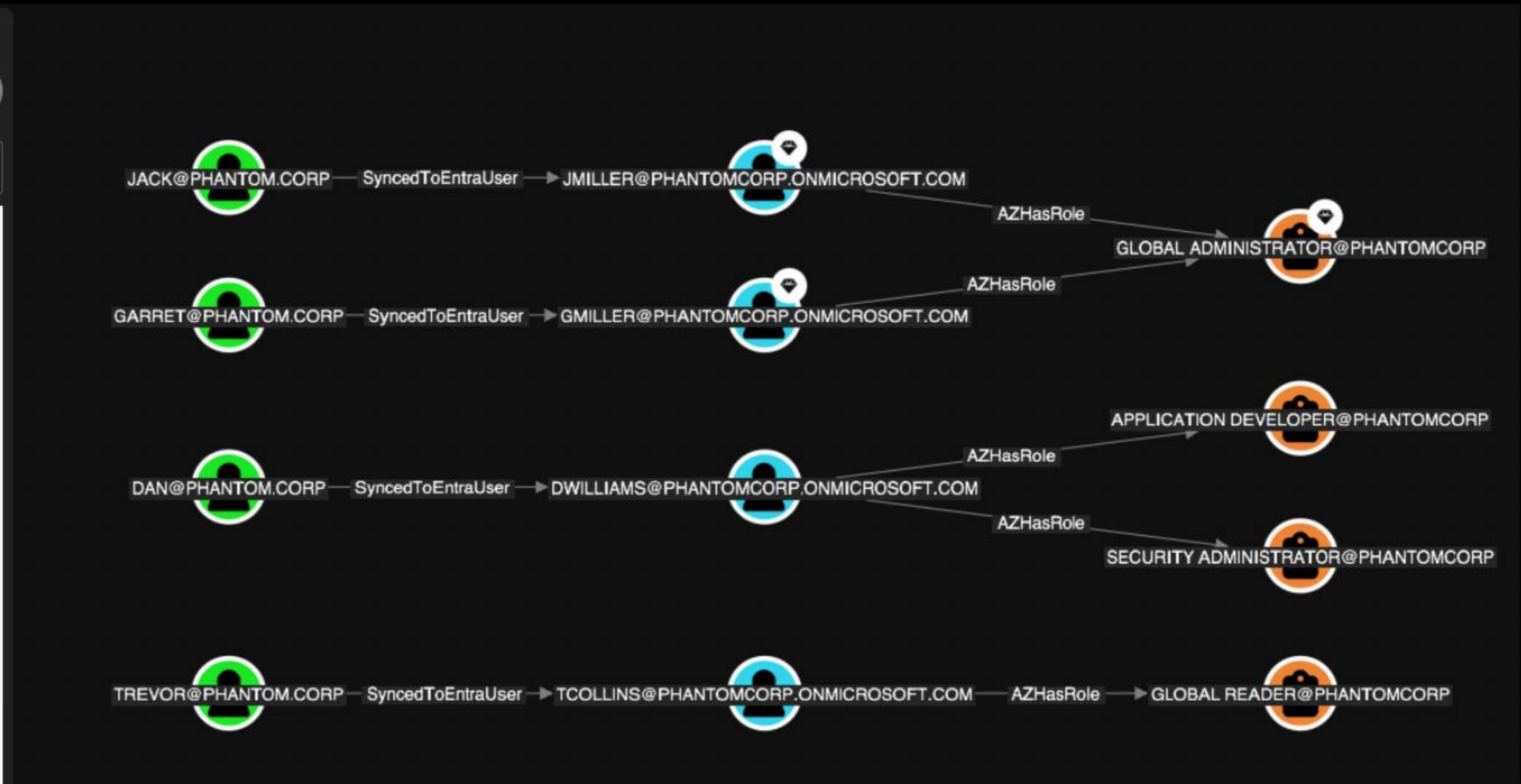
▼ **Saved Queries**

Search

Platforms  Categories  Source

**Azure**  
*Azure, Cross Platform Attack Paths*

- On-Prem Users synced to Entra Users with Entra Admin Roles (direct)  
*Azure, Cross Platform Attack Paths*
- On-Prem Users synced to Entra Users with Entra Admin Roles (group delegated)  
*Azure, Cross Platform Attack Paths*
- On-Prem Users synced to Entra Users with Azure RM Roles (direct)  
*Azure, Cross Platform Attack Paths*
- On-Prem Users synced to Entra Users with Azure RM Roles (group delegated)  
*Azure, Cross Platform Attack Paths*
- On-Prem Users synced to Entra Users that Own Entra Objects  
*Azure, Cross Platform Attack Paths*
- On-Prem Users synced to Entra Users with Entra Group Membership  
*Azure, Cross Platform Attack Paths*



## 6. Track Key Performance Indicators (KPIs)

### Baseline

- # of attack paths to privileged identities
- # of Choke Points (findings)

### Remediations

- # of resolved choke points
- # of resolved attack paths
- Remediation cycle time

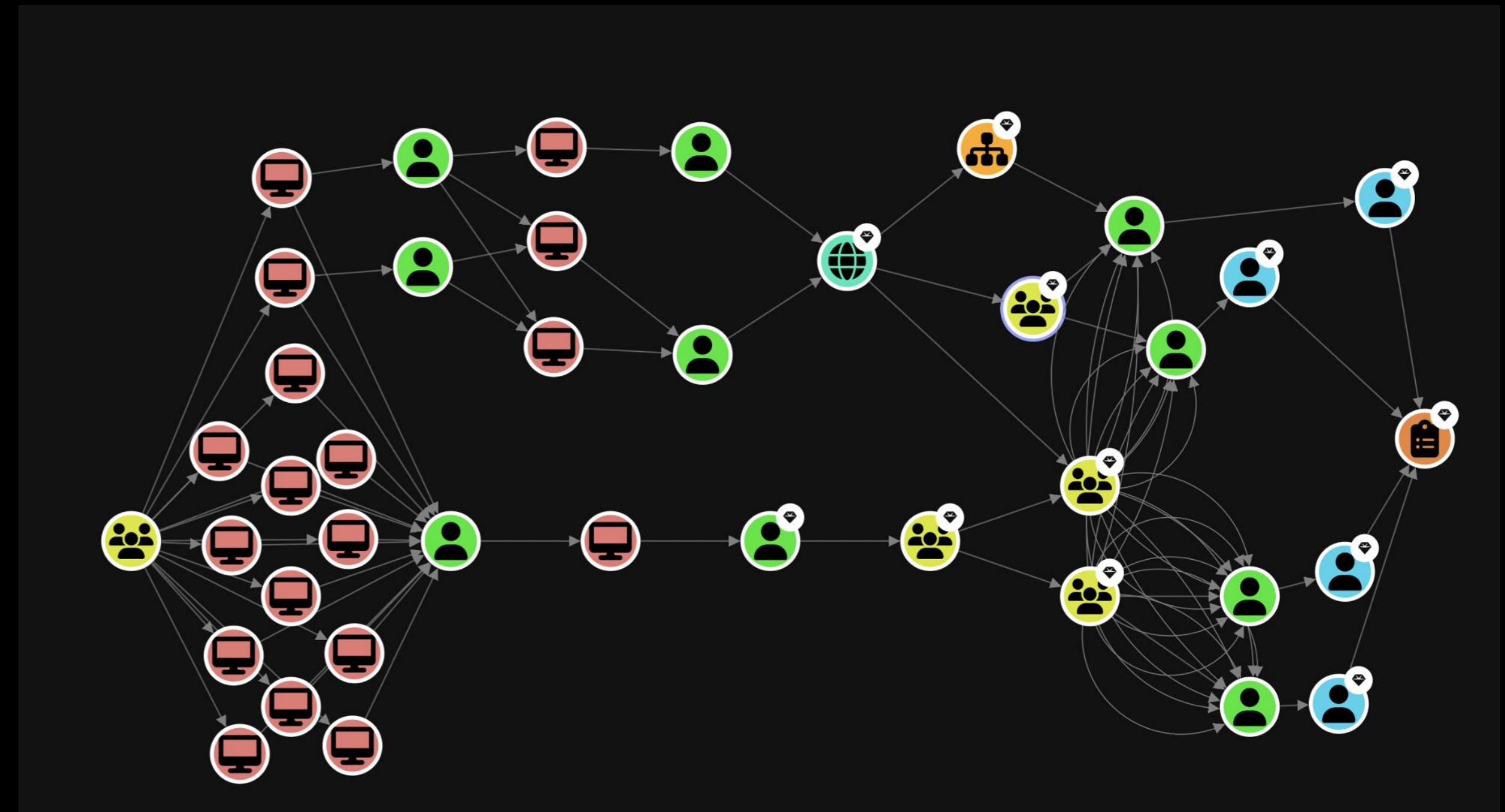
### Scope

- # of identities
- # of privileged identities
- # of relationships

# Attackers see a map, do you?

The collage includes several news items:

- MGM Resorts to Pay \$45M to Settle Data Breach Lawsuit** (January 29, 2025)
- Change Healthcare Increases Ransomware Victim Count to 192.7 Million Individuals** (The HIPAA Journal)
- Salesloft Breached via GitHub Account Compromise** (The breach kickstarted a massive supply chain attack that led to the compromise of hundreds of Salesforce accounts through stolen OAuth tokens.)
- Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard** (MSRC / By MSRC / March 8, 2024)
- What we know about the Snowflake customer attacks** (Published June 17, 2024)



“How did this happen?”

“How did this **[take so long to]** happen?”

### **1. Attackers bypass tools, not break them.**

Even the strongest security stack (MFA, Conditional Access, EDR, PAM) can be sidestepped through *identity attack paths* across hybrid environments.

### **2. Identity Attack paths are the real risk surface.**

Individual access or privilege decisions may look safe in isolation but combined they create *invisible collisions* that attackers exploit like the SalesLoft Breach

### **3. Attack Path Management is essential.**

Treat attack paths as measurable, trackable risks. Use BloodHound Community Edition to get started **visualizing** attack paths, BloodHound Enterprise to **automatically identify choke points and remediate continuously**. What you can see, you can control.

# Exposing Hidden Attack Paths: How Threats Get Past Your Best Defenses



*Questions?*