SPECTEROPS

State of Attack Path Management

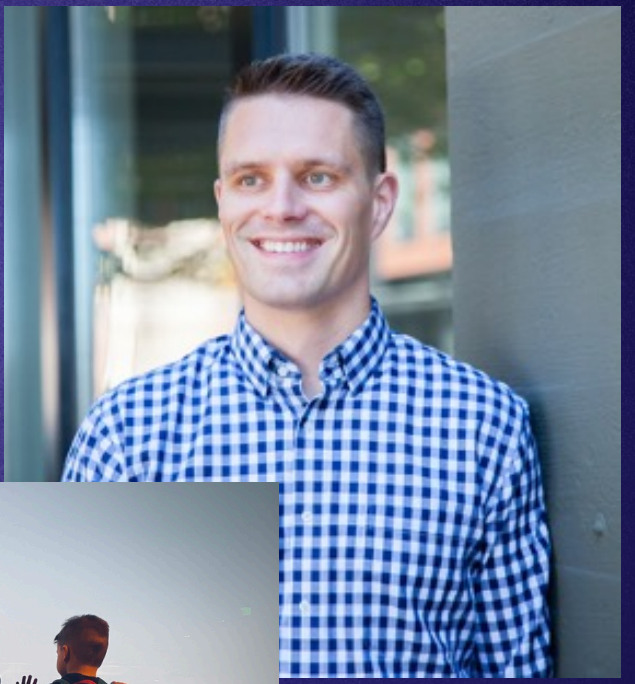
BLOODHOUND ENTERPRISE

Justin Kohler

VP of Product, SpecterOps

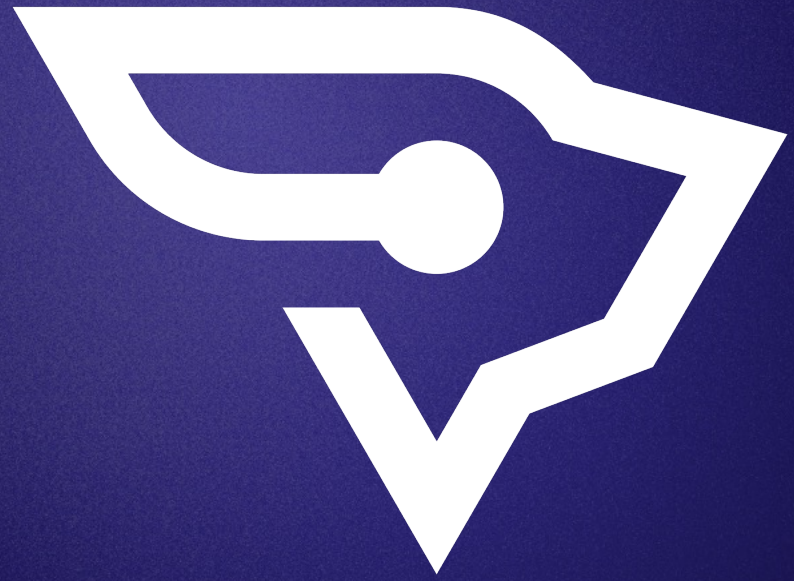
Who am I

- Product Leader at SpecterOps
- Former Air Force, Network Security
- Father of 4
- I love anything outside
- X: @JustinKohler10



Agenda

- What is Attack Path Management
- 3 Years of Attack Paths
- Lessons Learned
- Where do we go from here



What is Attack Path Management

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

Foundations

Continuous, Comprehensive Attack Path Mapping

Empirical Impact Assessment of Risk

Practical, Precise, and Safe Remediation Guidance

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 Community For Asm - Tenable Commu
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

Assess Security Configuration of Azure Environment

CISA created the Secure Cloud and Business Applications (SCuBA) assessment tool to help Federal Civilian Executive Branch (FCEB) agencies to verify that a M365 tenant configuration conforms to a minimal viable secure configuration baseline. Although the SCuBA assessment tool was developed for FCEB, other organizations can benefit from its output. CISA and MS-ISAC recommend the following:

- **Use tools that identify attack paths**. This will enable defenders to identify common attack paths used by threat actors and shut them down before they are exploited.
- **Review the security recommendations list provided by Microsoft 365 Defender**. Focus remediation on critical vulnerabilities on endpoints that are essential to mission execution and contain sensitive data.

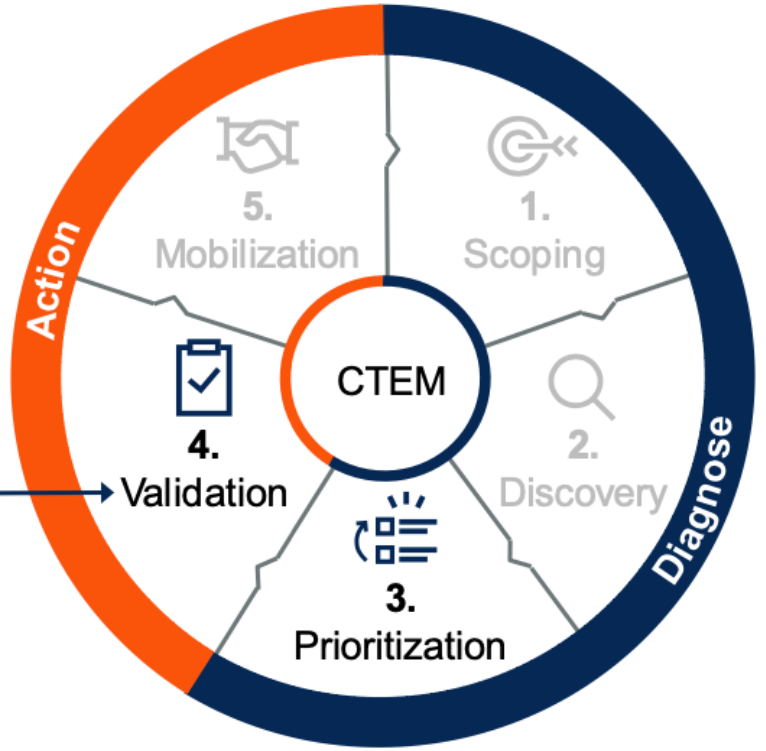
CISA
CYBER+INFRASTRUCTURE

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-046a

Continuous Threat Exposure Management

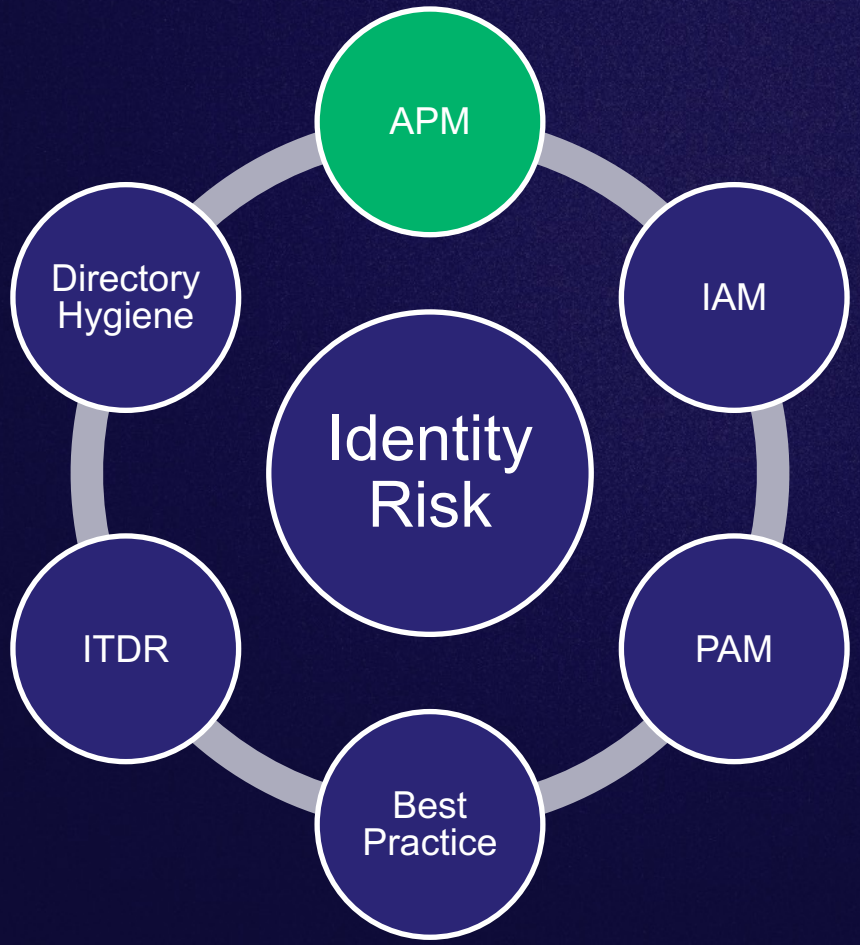
- Initiate or expand Cybersecurity Validation approaches.
- Validate to foster improved mobilization.
- Monitor progress from automated tools.

Security Posture Validation	Attack Path Mapping	Security Control Validation



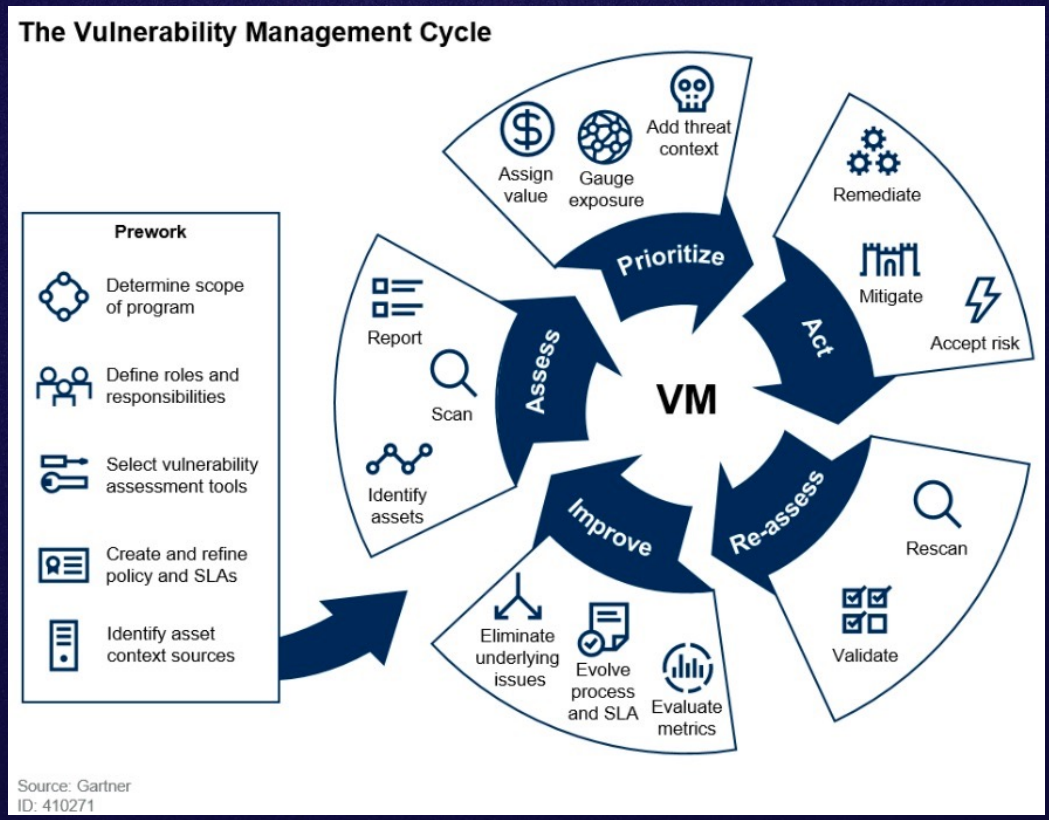
Gartner

APM is the missing capability in Identity Risk



APM has a familiar process

APM has a familiar process



APM has clear benefits

- ✓ Proactive, comprehensive visibility
- ✓ Single fixes to sever multiple Attack Paths
- ✓ Prioritized by exposure and impact
- ✓ Step-by-step remediations
- ✓ Measurable, meaningful progress

Attack Path Management will be the standard

What does 3 years of Attack Paths look like?

2 Billion

Abuseable configurations and behaviors

30M
Users

12M
Groups

5M
Azure Devices

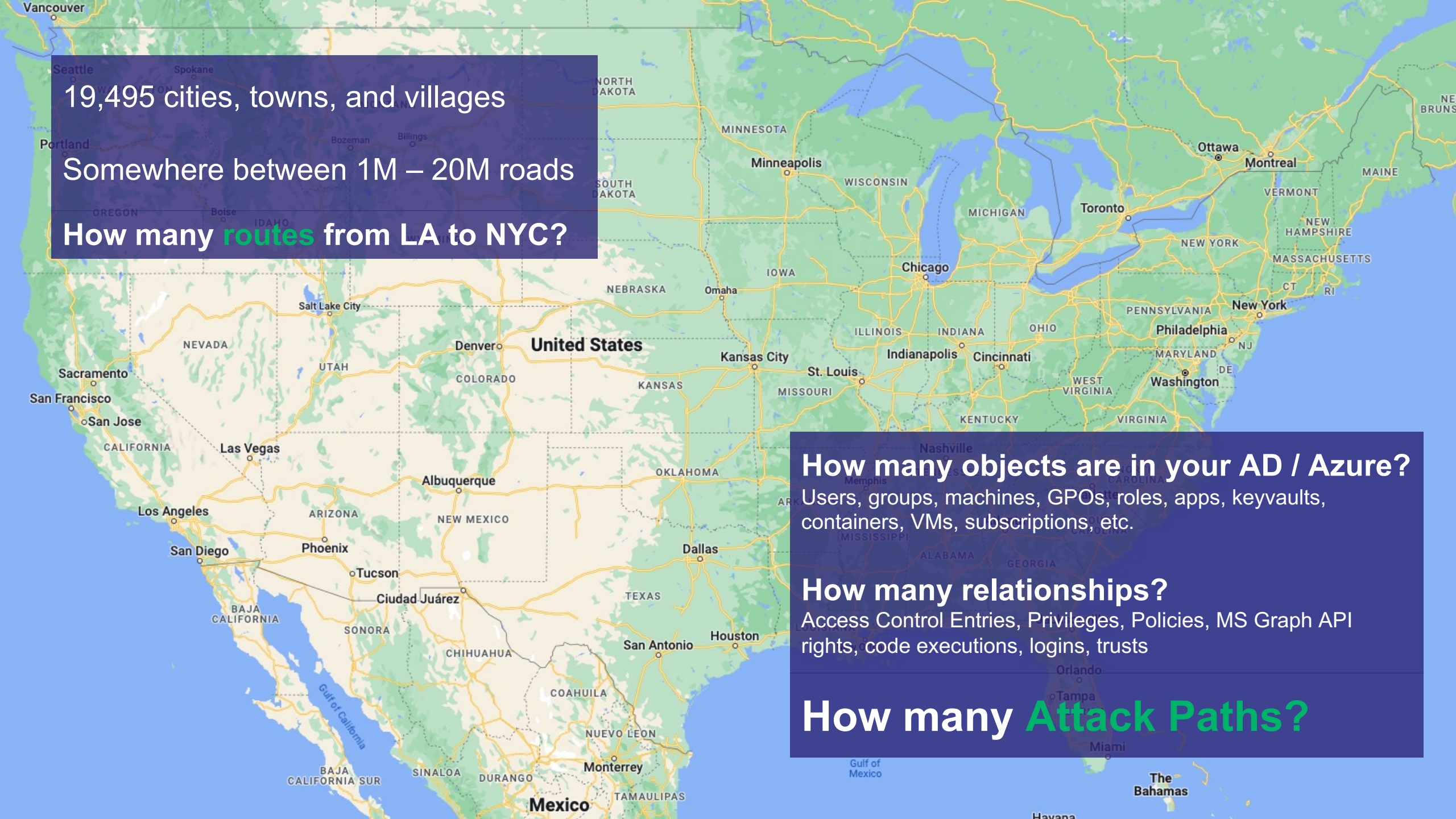
600K
Service Principals

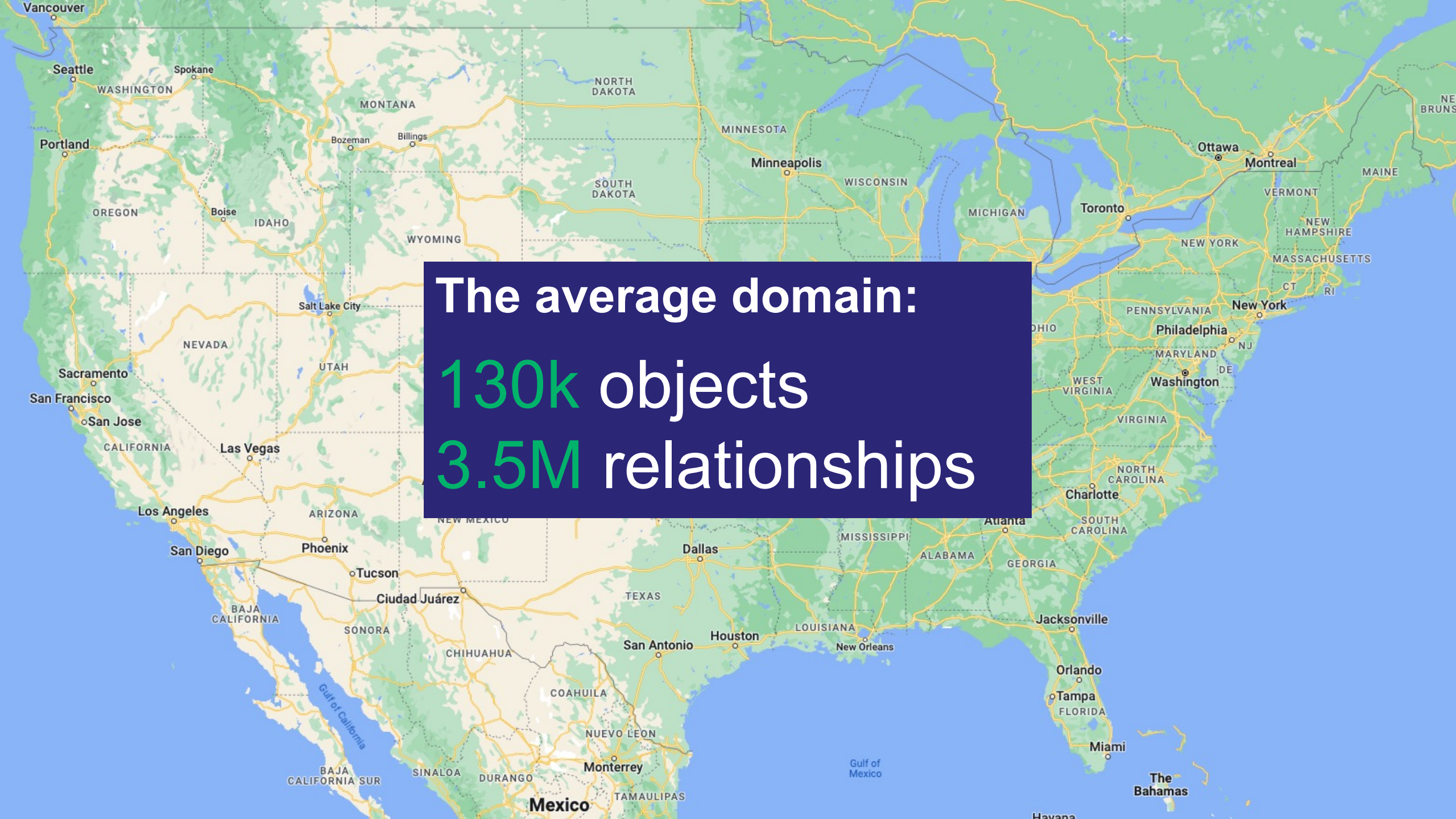
500K
OUs

200K
Azure Apps

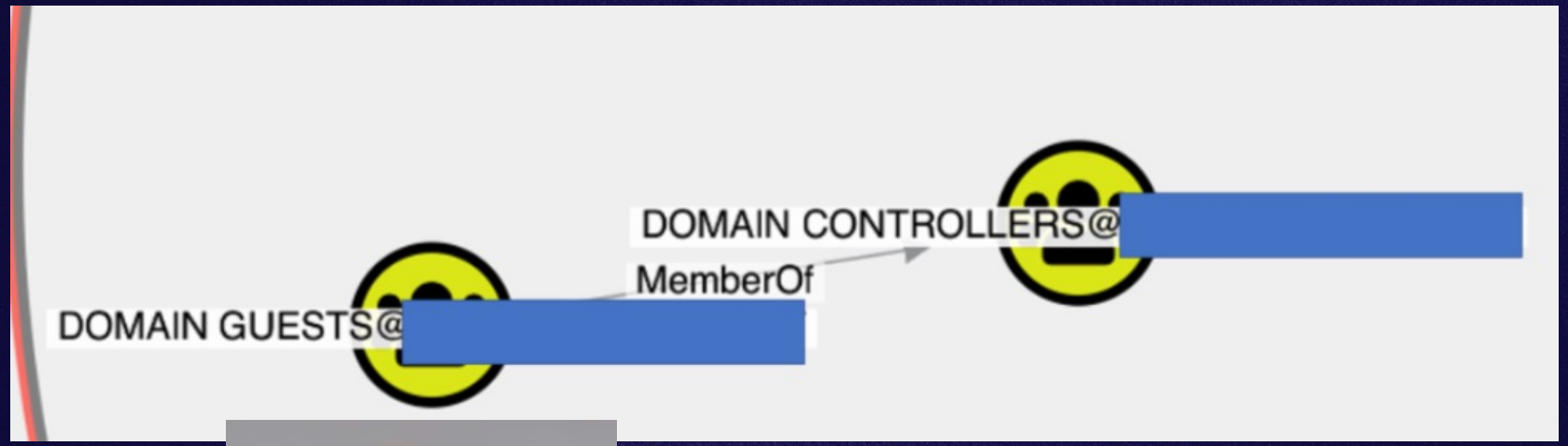
150K
GPOs

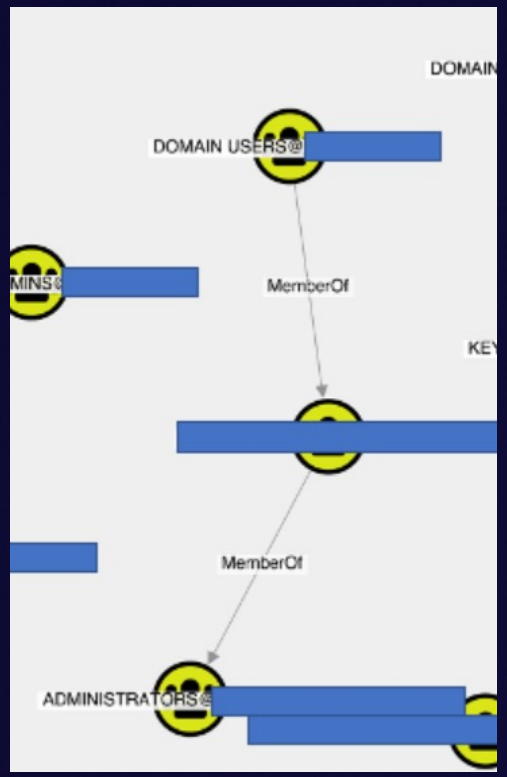
50K
Key Vaults

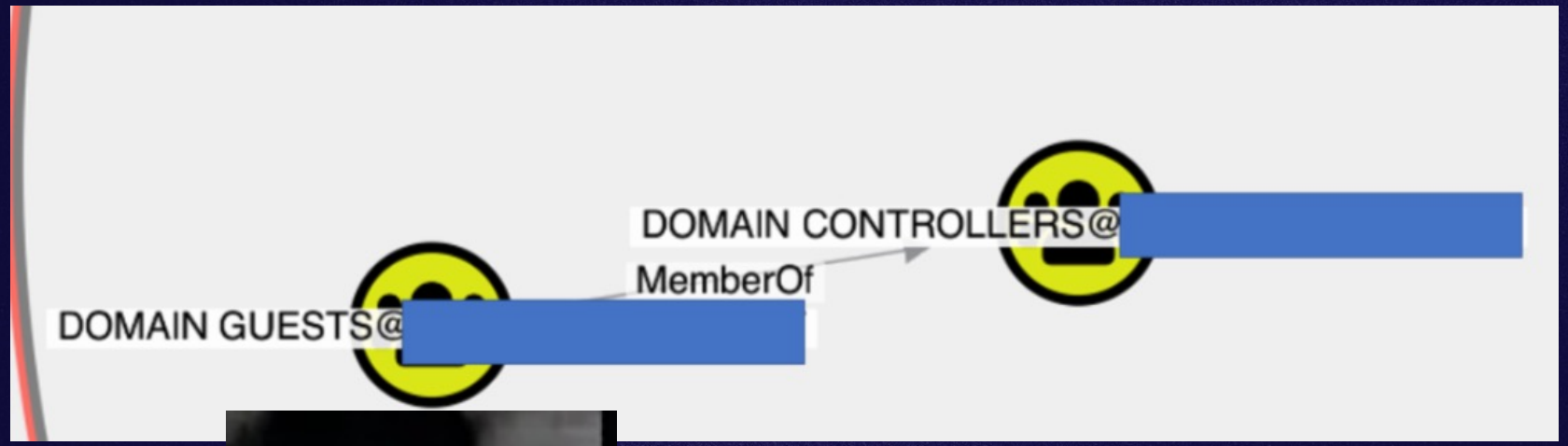

19,495 cities, towns, and villages
Somewhere between 1M – 20M roads
How many routes from LA to NYC?
How many objects are in your AD / Azure?
Users, groups, machines, GPOs, roles, apps, keyvaults, containers, VMs, subscriptions, etc.
How many relationships?
Access Control Entries, Privileges, Policies, MS Graph API rights, code executions, logins, trusts
How many Attack Paths?
United States
Mexico
Vancouver
Seattle
Spokane
Portland
Bozeman
Billings
Boise
Salt Lake City
Denver
Sacramento
San Francisco
San Jose
Las Vegas
Albuquerque
Los Angeles
San Diego
Phoenix
Tucson
Ciudad Juárez
Dallas
San Antonio
Houston
Minneapolis
Omaha
Kansas City
St. Louis
Chicago
Indianapolis
Cincinnati
Toronto
Ottawa
Montreal
New York
Philadelphia
Washington
Nashville
Memphis
Orlando
Tampa
Miami
Monterrey
Gulf of California
Gulf of Mexico
The Bahamas
Havana
NORTH DAKOTA
SOUTH DAKOTA
MINNESOTA
WISCONSIN
MICHIGAN
NEBRASKA
IOWA
ILLINOIS
INDIANA
OHIO
PENNSYLVANIA
NEW YORK
VERMONT
NEW HAMPSHIRE
MASSACHUSETTS
MAINE
CT
RI
NJ
DE
MARYLAND
WEST VIRGINIA
VIRGINIA
KENTUCKY
MISSOURI
KANSAS
OKLAHOMA
TEXAS
NEVADA
UTAH
COLORADO
ARIZONA
NEW MEXICO
CALIFORNIA
OREGON
IDAHO
BAJA CALIFORNIA
BAJA CALIFORNIA SUR
SONORA
CHIHUAHUA
COAHUILA
NUEVO LEON
SINALOA
DURANGO
TAMAULIPAS
MISSISSIPPI
ALABAMA
GEORGIA

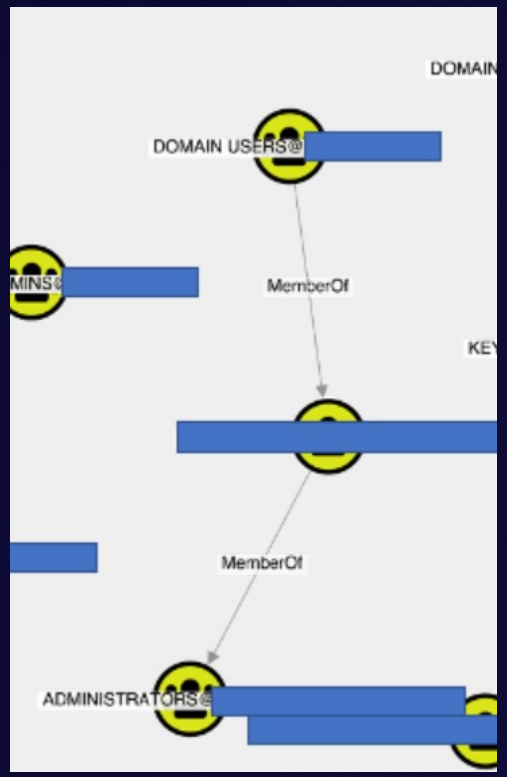

The average domain:
130k objects
3.5M relationships

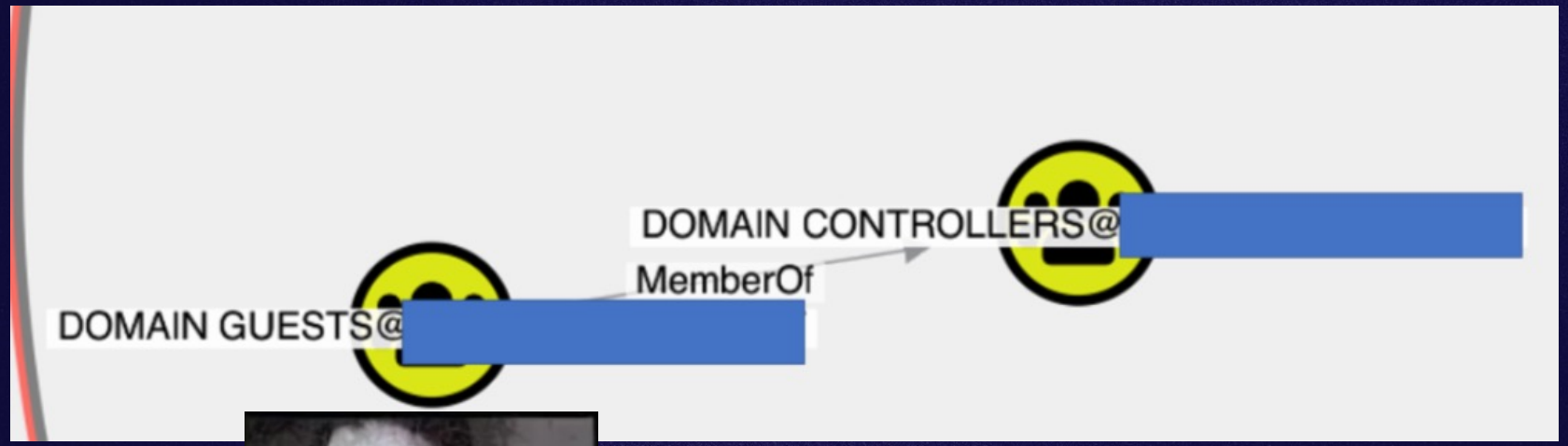
What does 3 years of Attack Paths actually look like?

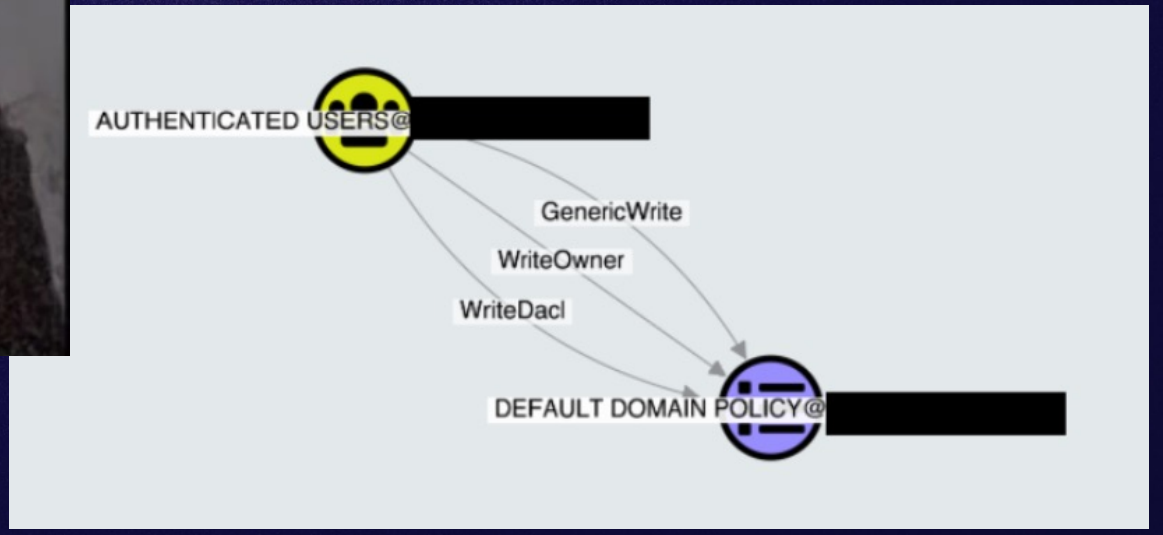

DOMAIN CONTROLLERS@
MemberOf
DOMAIN GUESTS@

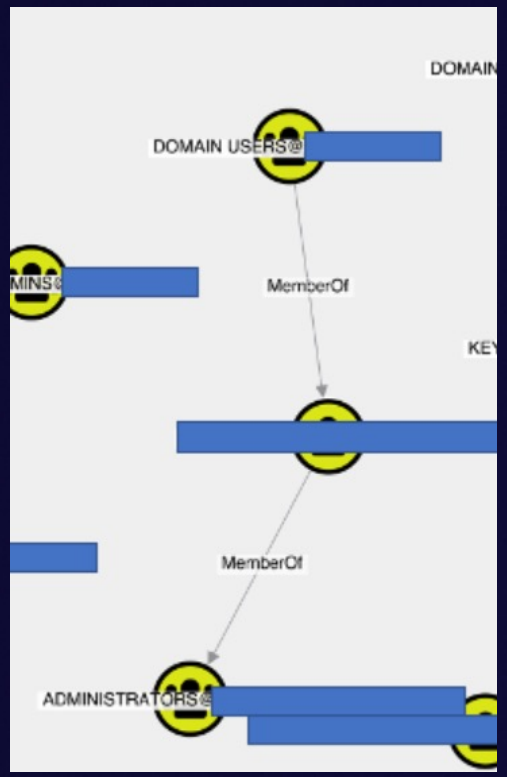

DOMAIN
DOMAIN USERS@
MemberOf
MemberOf
ADMINISTRATORS@

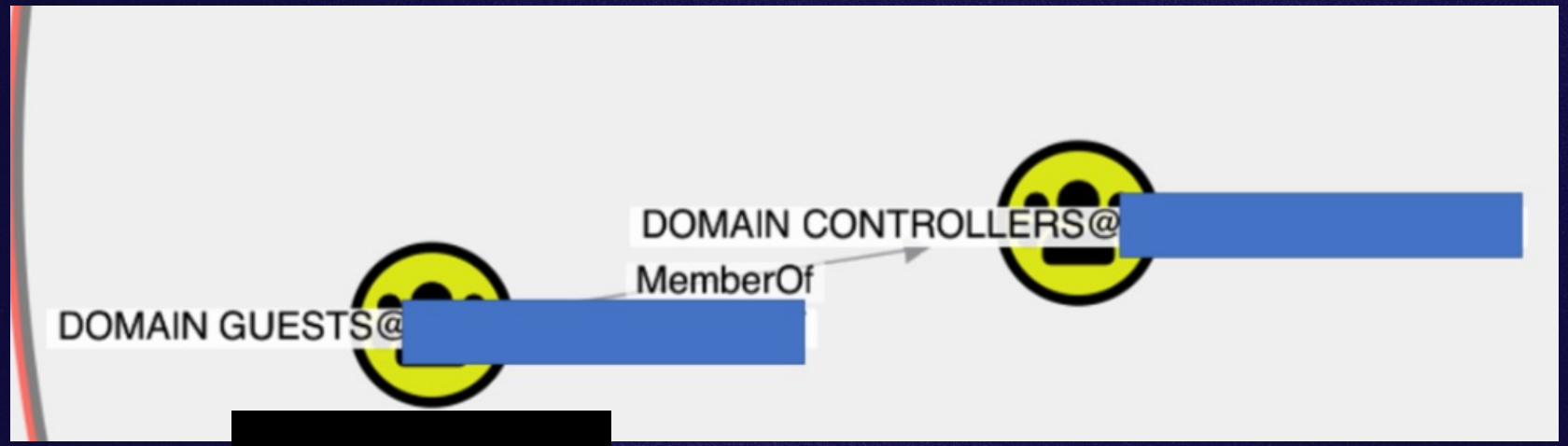

DOMAIN GUESTS@
MemberOf
DOMAIN CONTROLLERS@

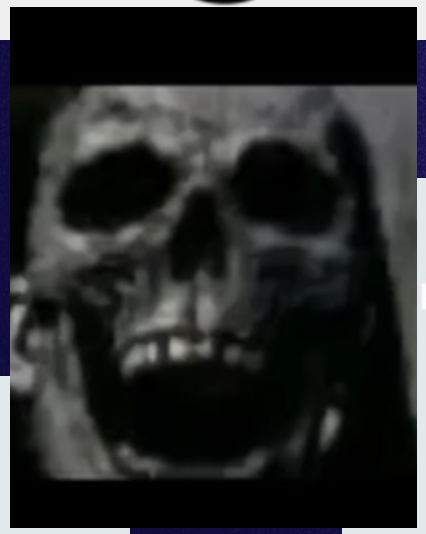

DOMAIN
DOMAIN USERS@
MemberOf
MemberOf
ADMINISTRATORS@

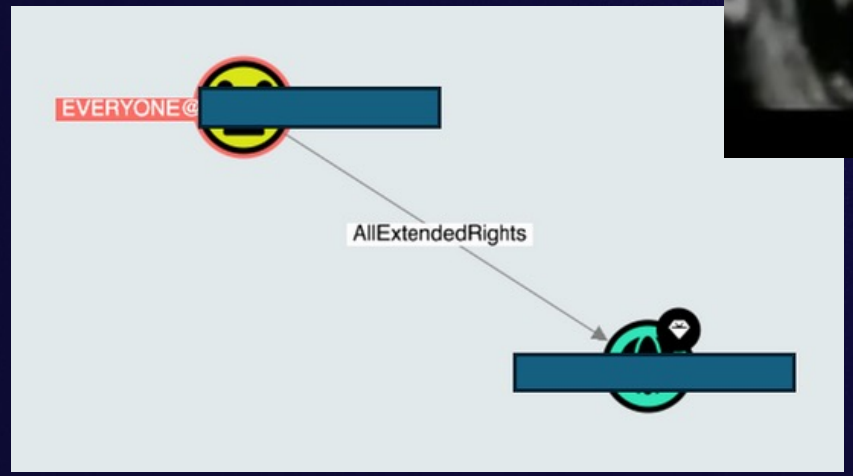

DOMAIN CONTROLLERS@
MemberOf
DOMAIN GUESTS@

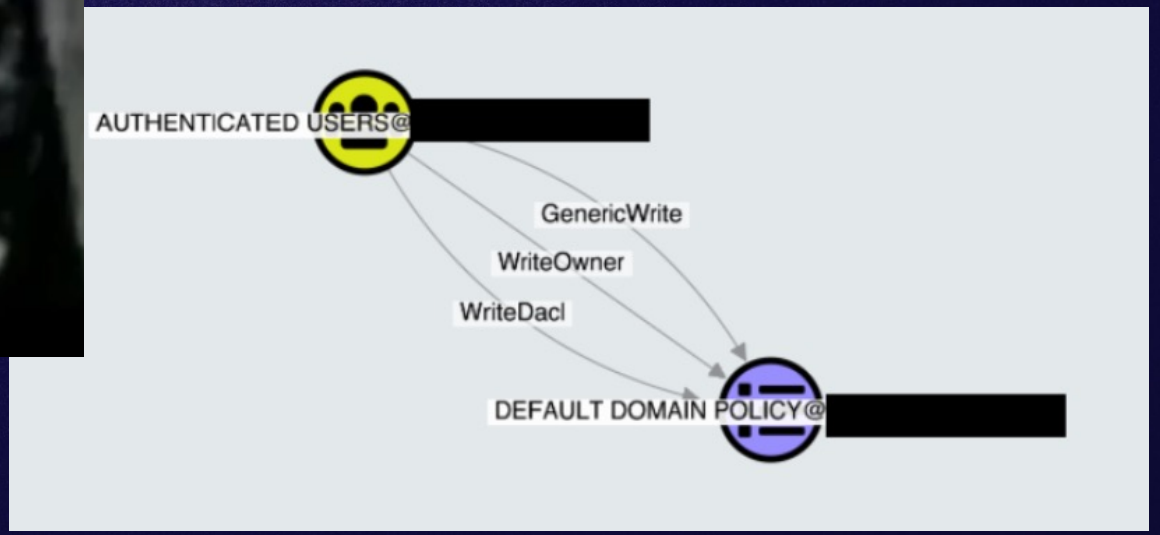

AUTHENTICATED USERS@
GenericWrite
WriteOwner
WriteDacl
DEFAULT DOMAIN POLICY@

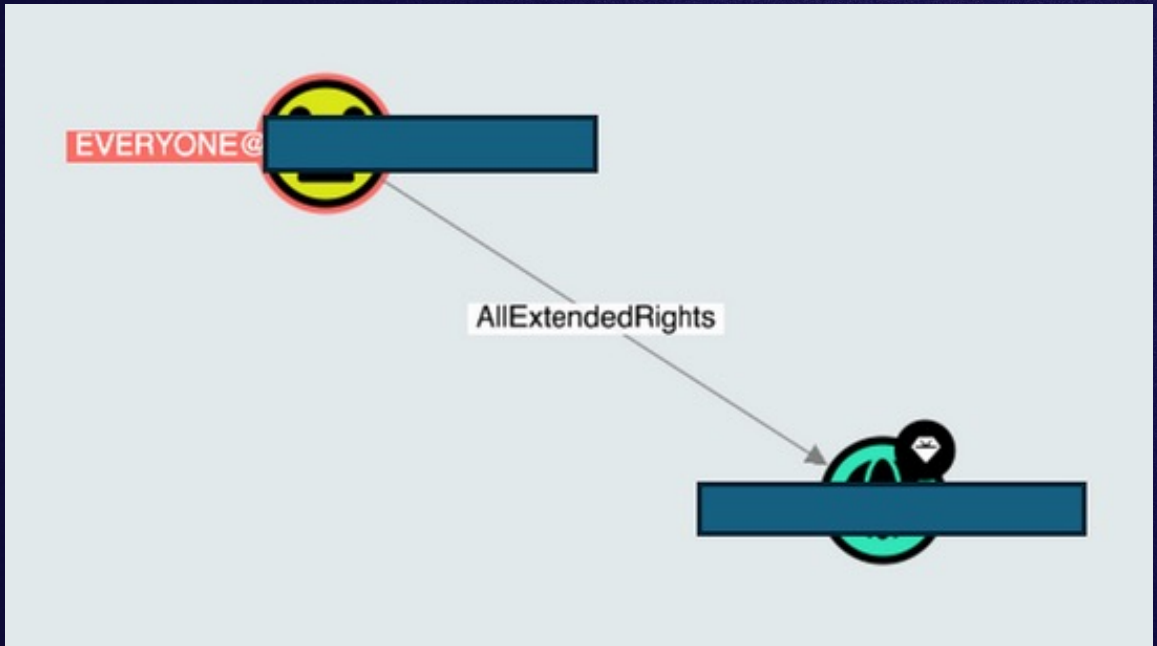

DOMAIN
DOMAIN USERS@
MemberOf
MemberOf
ADMINISTRATORS@


DOMAIN GUESTS@
MemberOf
DOMAIN CONTROLLERS@

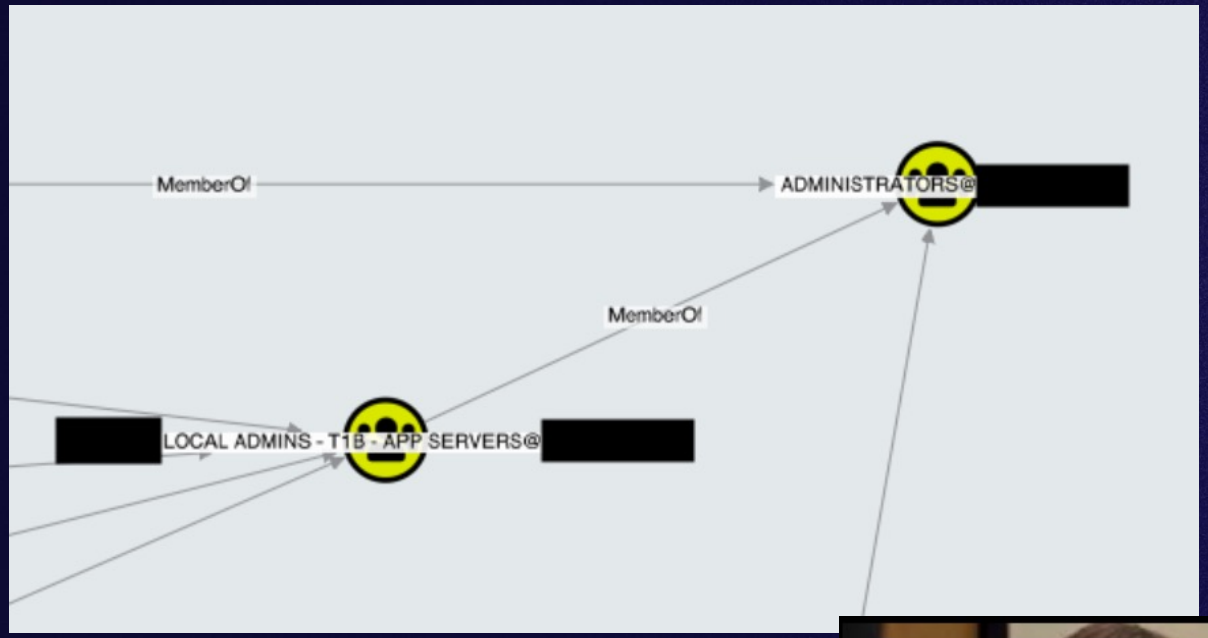


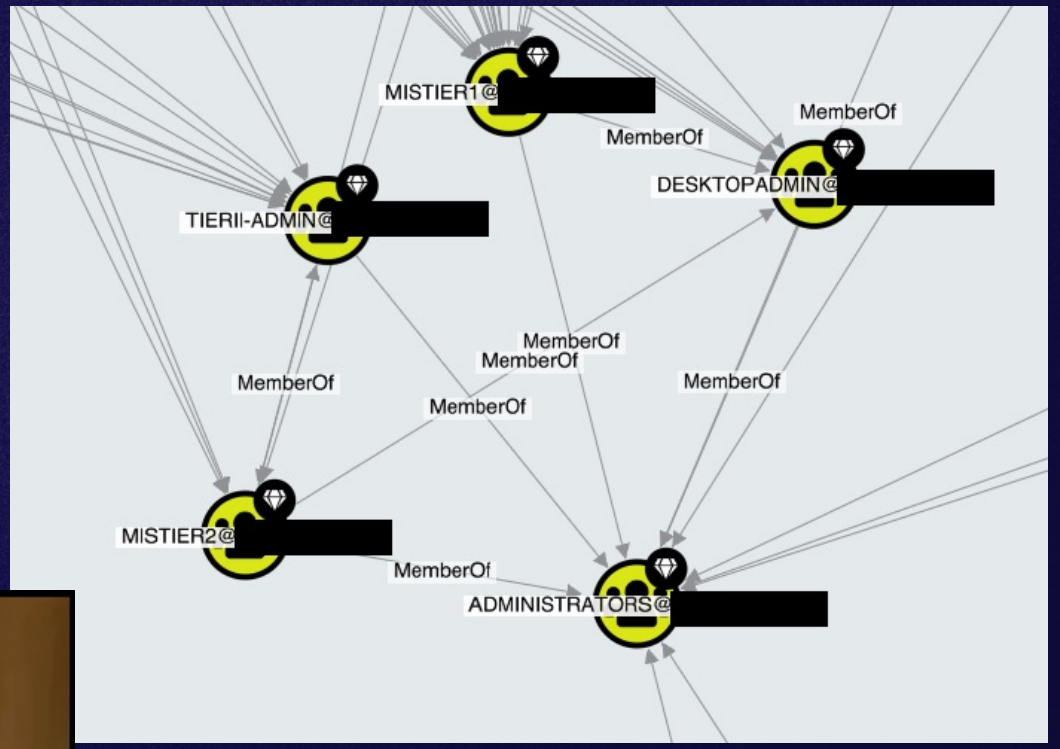

EVERYONE@
AllExtendedRights


AUTHENTICATED USERS@
GenericWrite
WriteOwner
WriteDacl
DEFAULT DOMAIN POLICY@

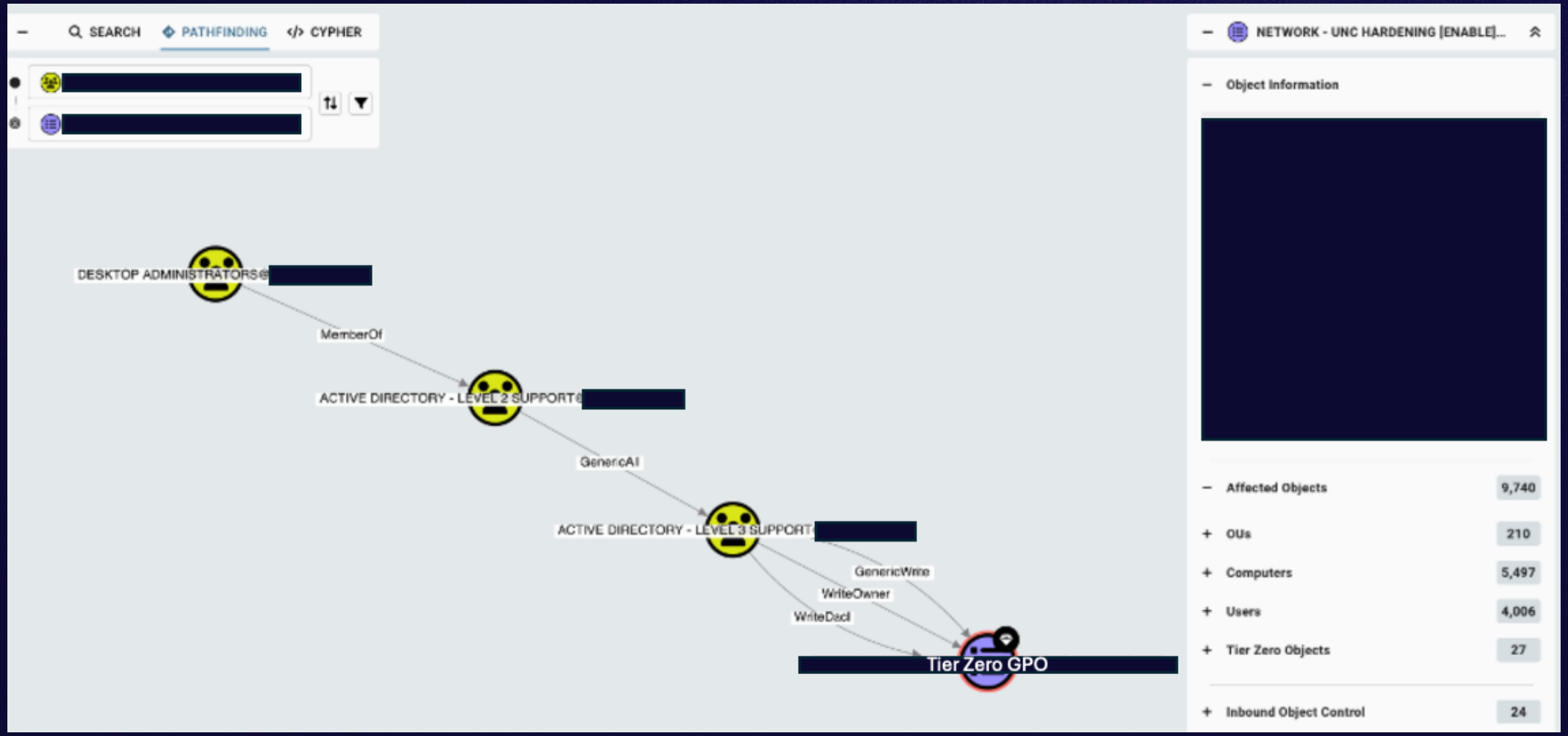

EVERYONE@
AllExtendedRights

People tried to do the right thing

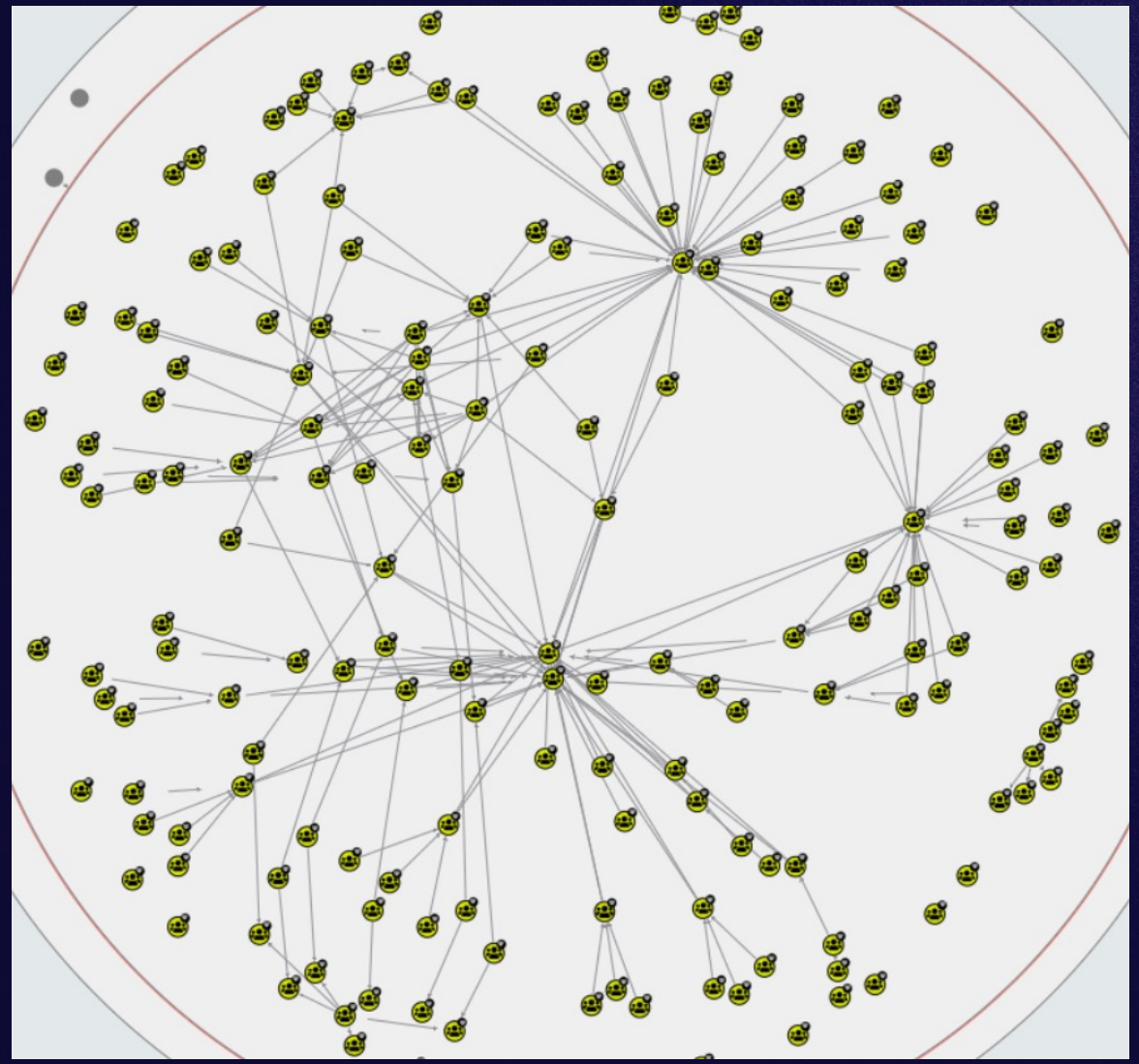




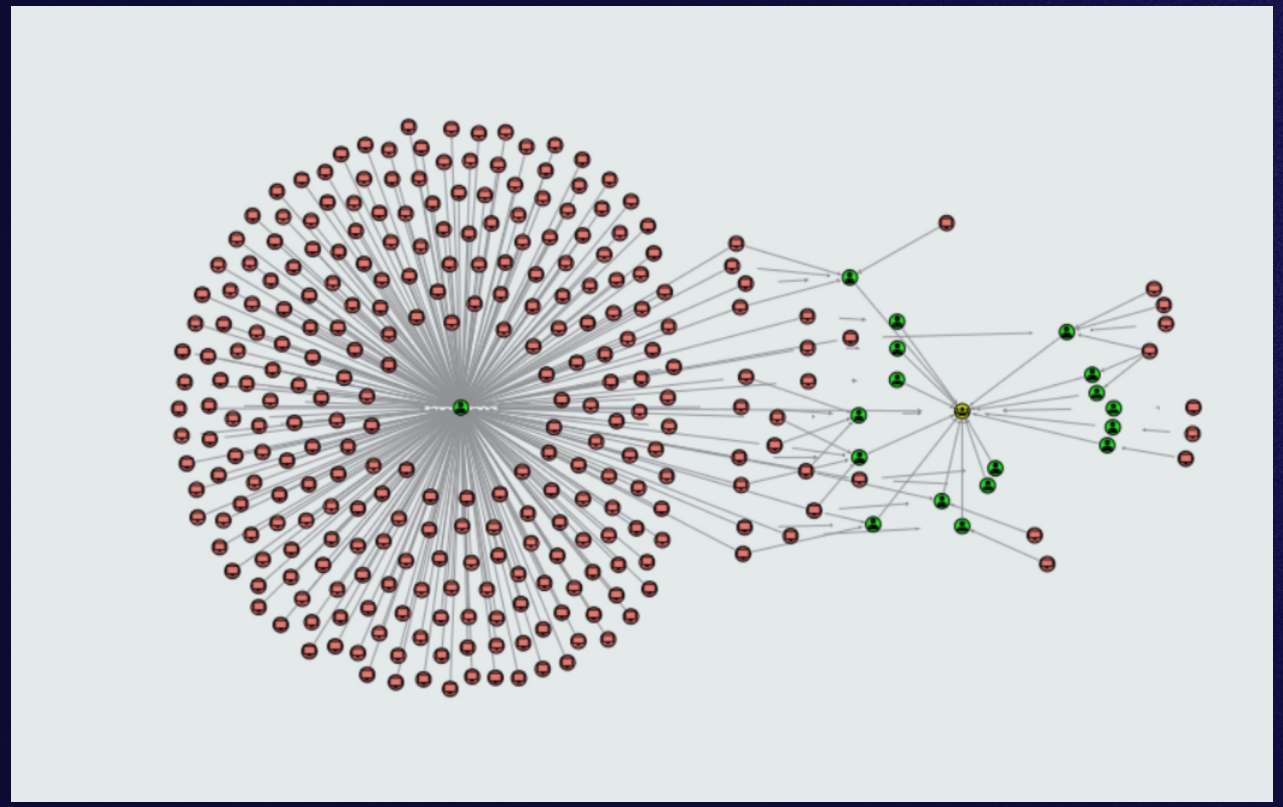
But the details matter

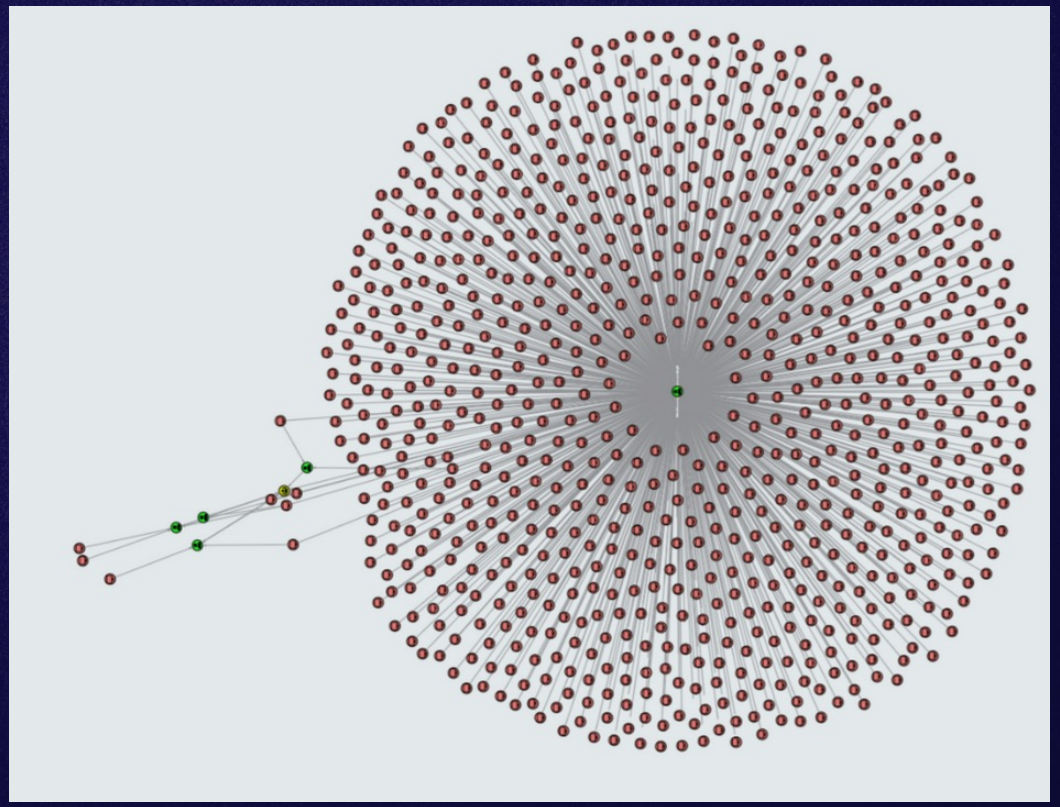


Can’t have Attack Paths if everyone is Tier Zero

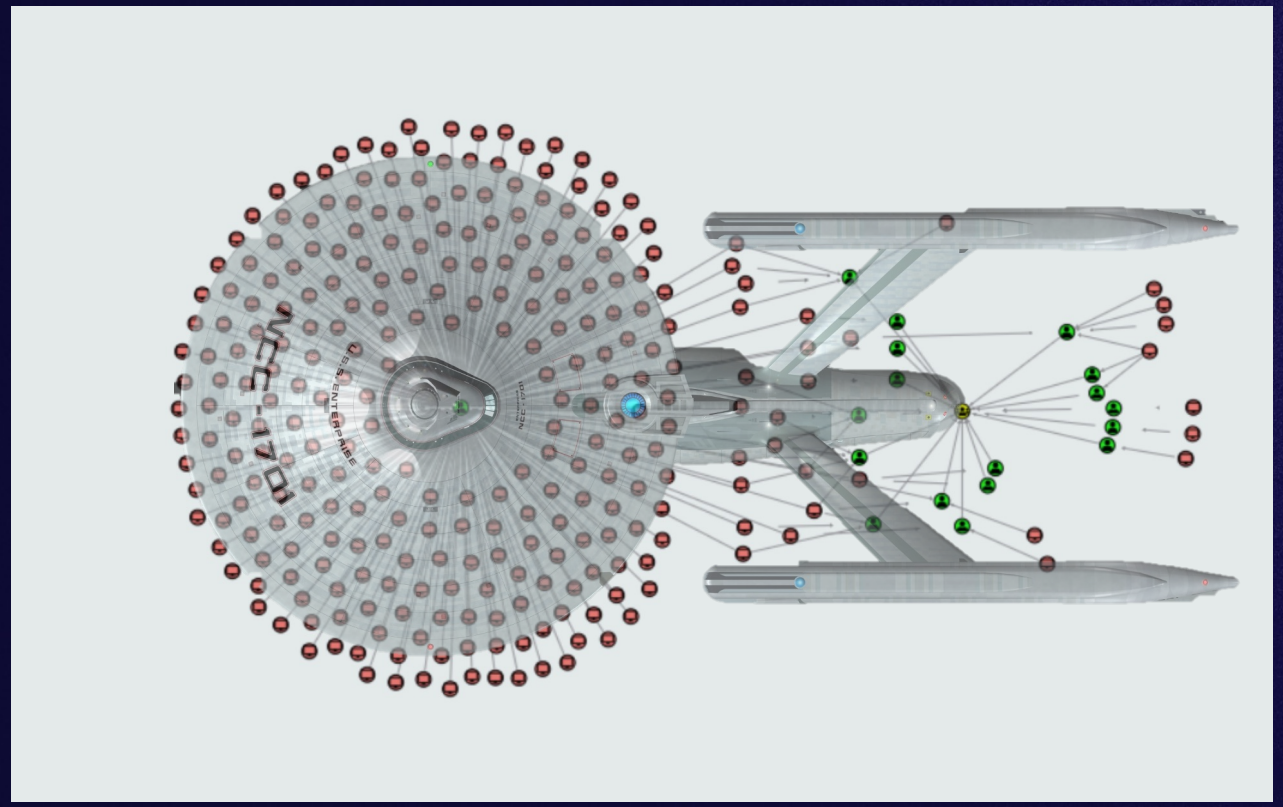


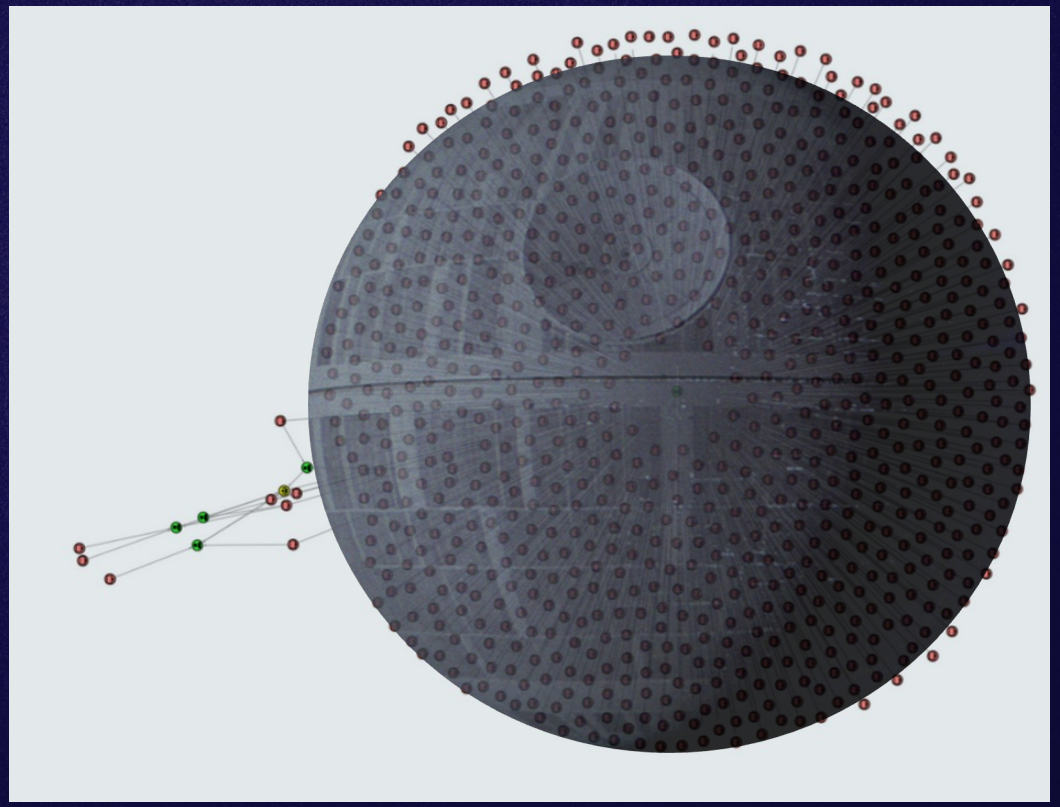
Security software making us safe



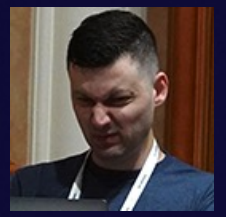


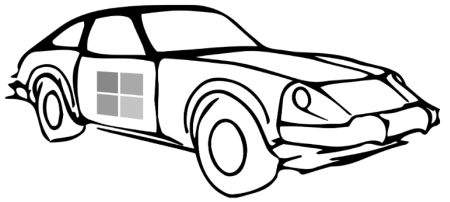
Security software making us safe





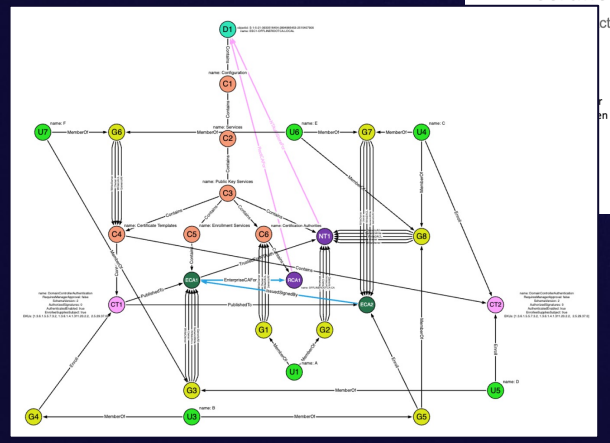
ADCS gave new meaning to complexity

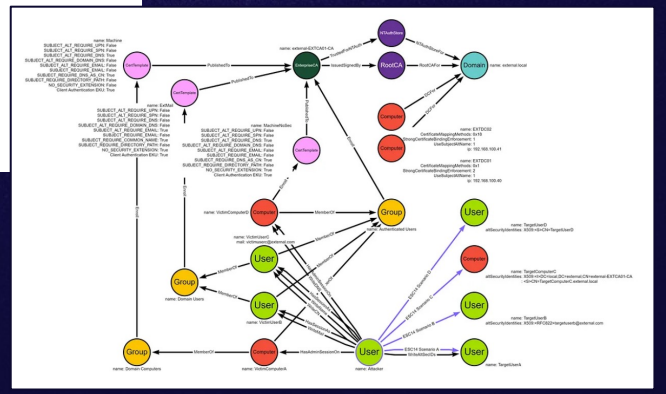




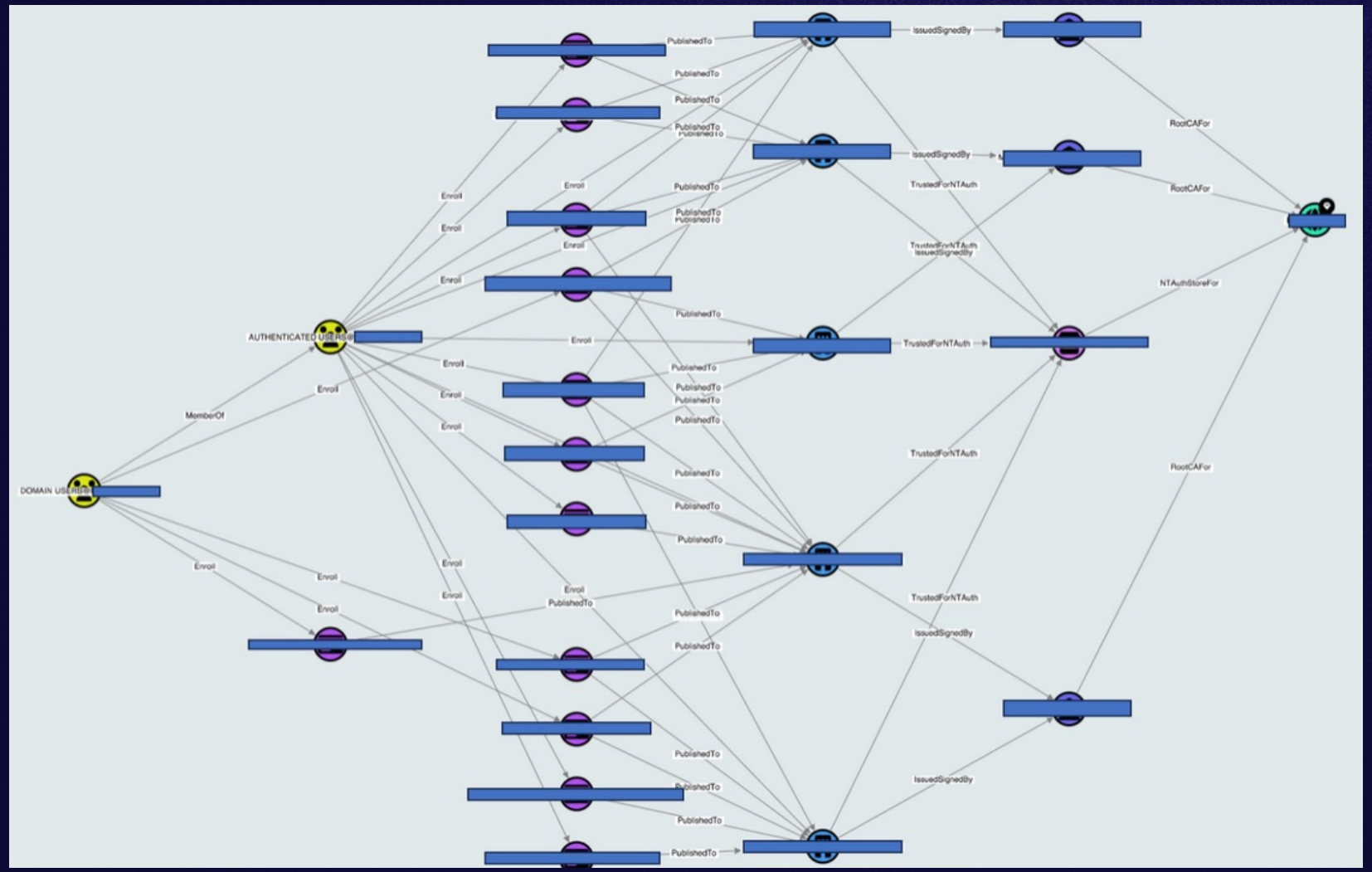
Certified Pre-Owned

ctive Directory Certificate Services



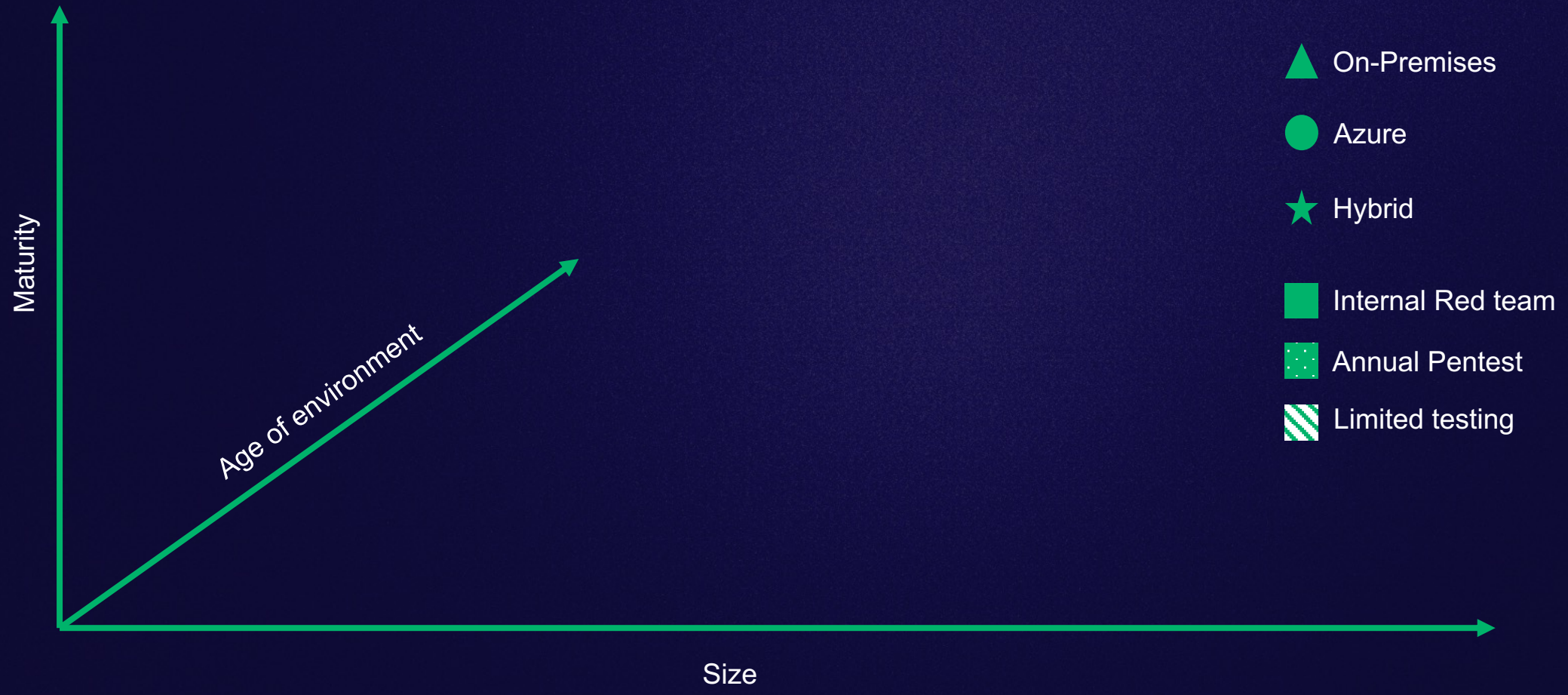


And closed critical gaps

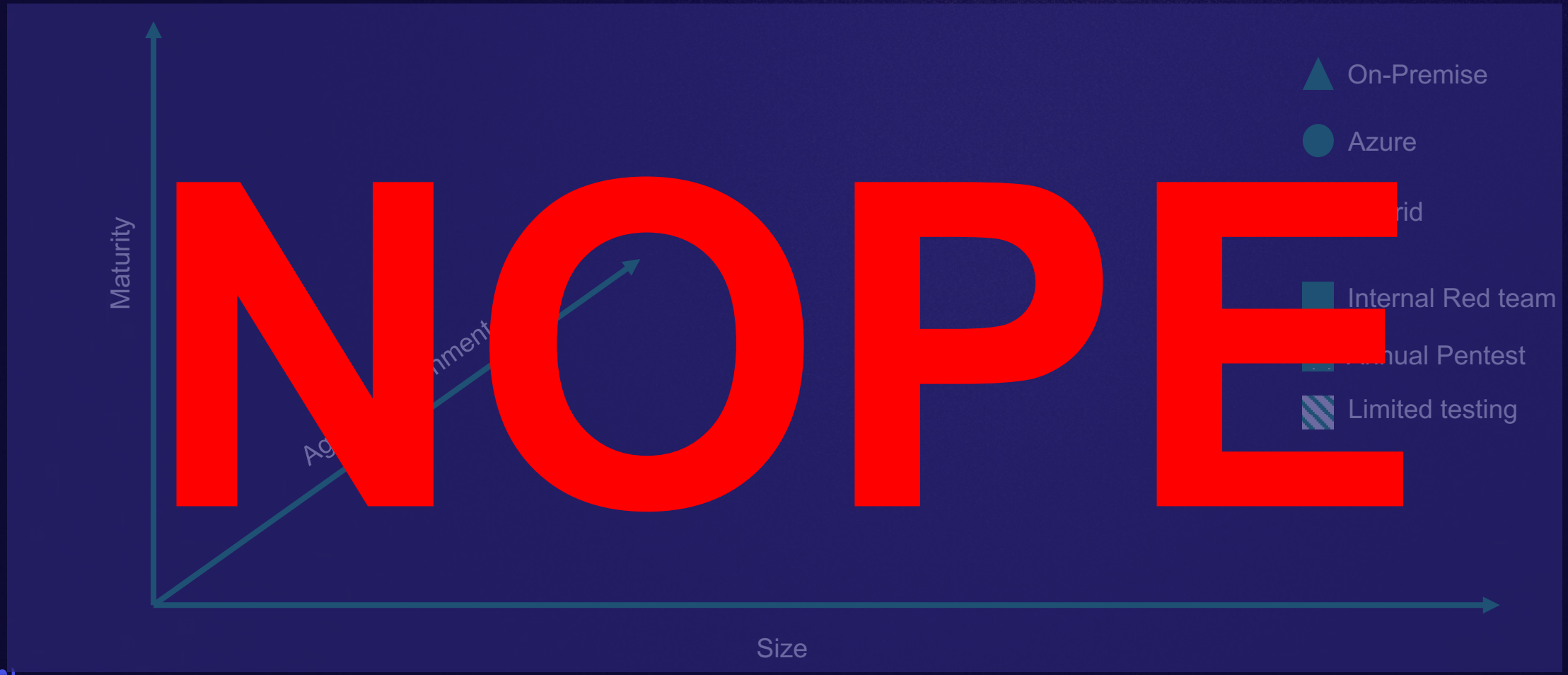


Lessons Learned

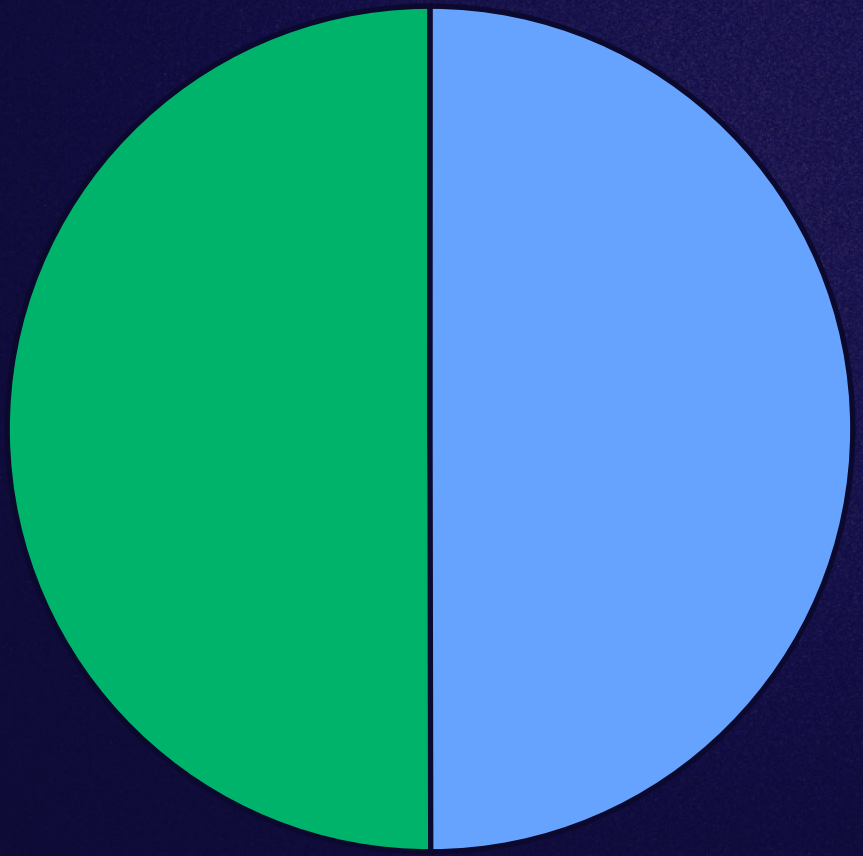
Attack Path distribution analysis



Attack Path distribution analysis



Organizations with Attack Paths



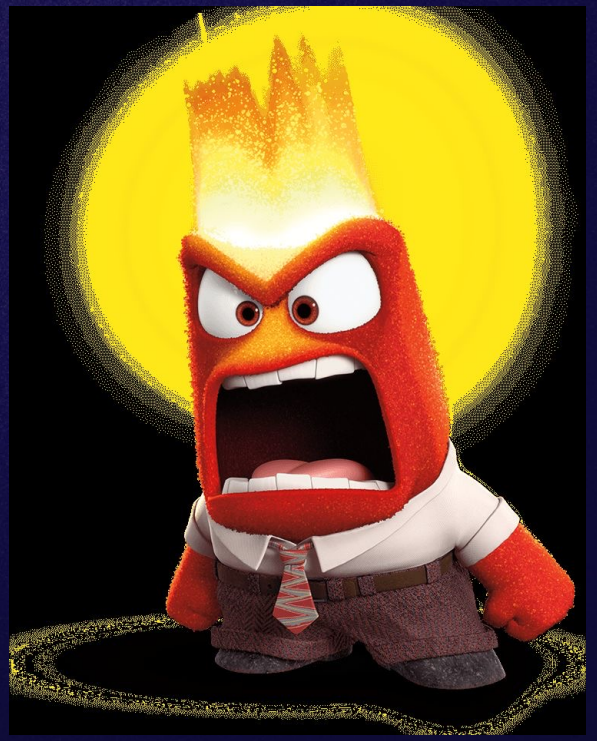
Those that haven’t deployed yet

AD is *still* not going away

- AD is more complex than anyone imagines
- It’s always worse than you think
- AD SMEs are disappearing
- Common knowledge is not common

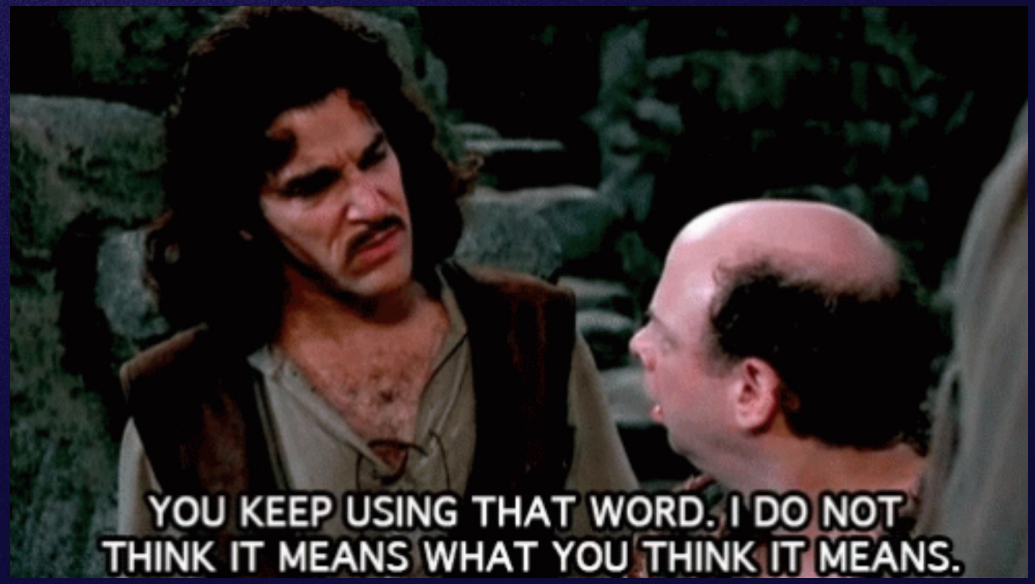
Azure is *still* a foreign language

- The amount of knowledge to maintain is extreme
- Constant updates exacerbate this
- Hybrid environments have 3x the risk
- You can do everything right today to have it undone tomorrow



Least Privilege is not possible without visibility

- Introduced 50 years ago
- Recommended during every breach or annual report
- “We separate our admin accounts”
- Perception vs reality can be a real shock

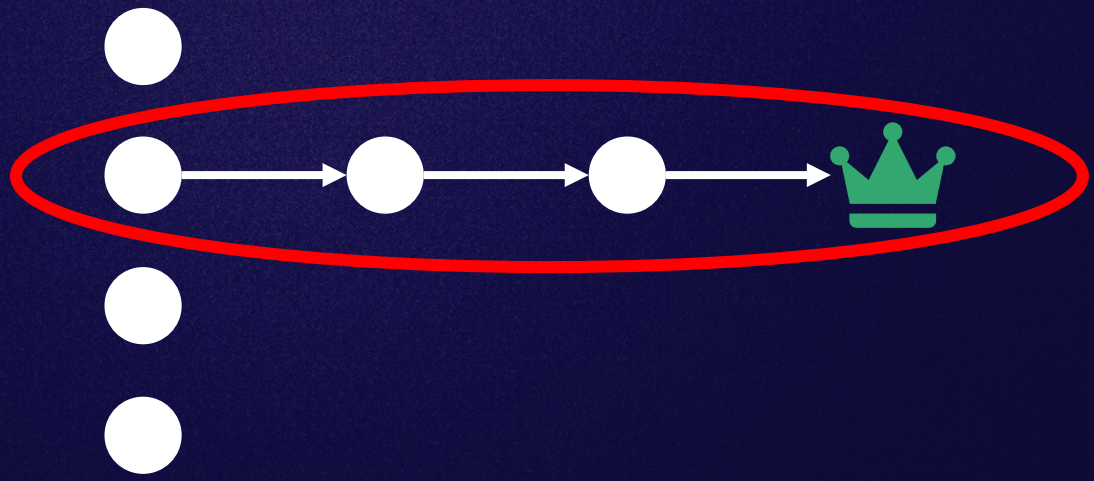


Who owns this problem?

- New problem without clear owner
- Red Team > Operationalized
- Evolution of existing processes

Visualizing Attack Paths is powerful

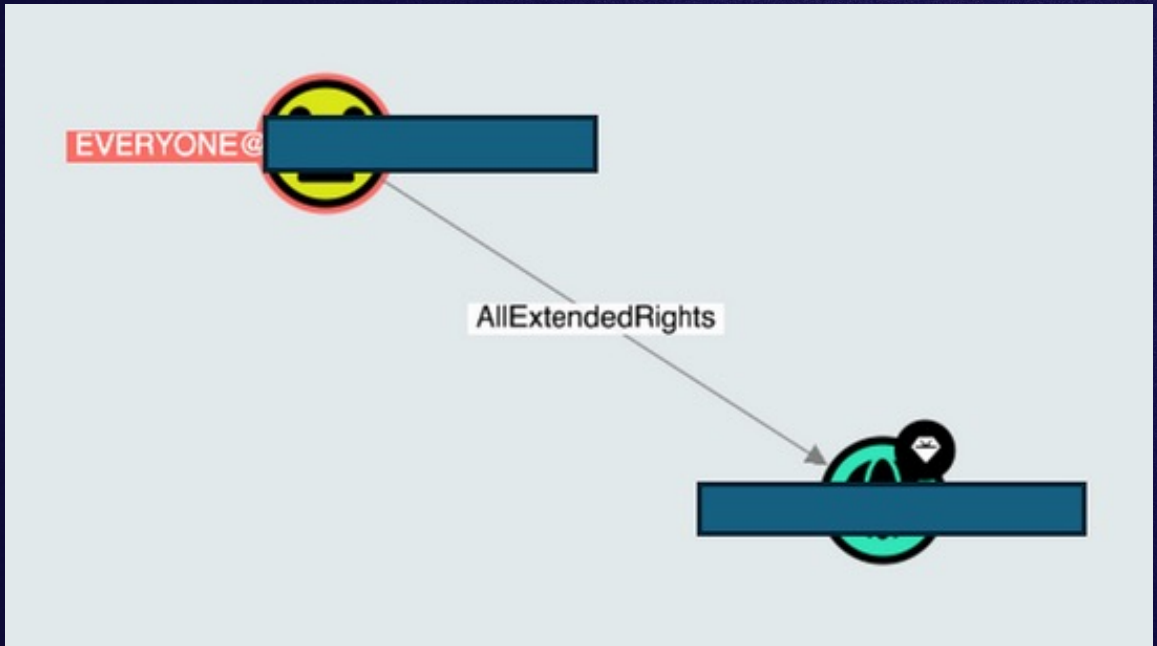
- AD Administrators and GPOs
- Incident Response
- Mergers and Acquisitions
- SOC Enrichment



APM Steps for Success

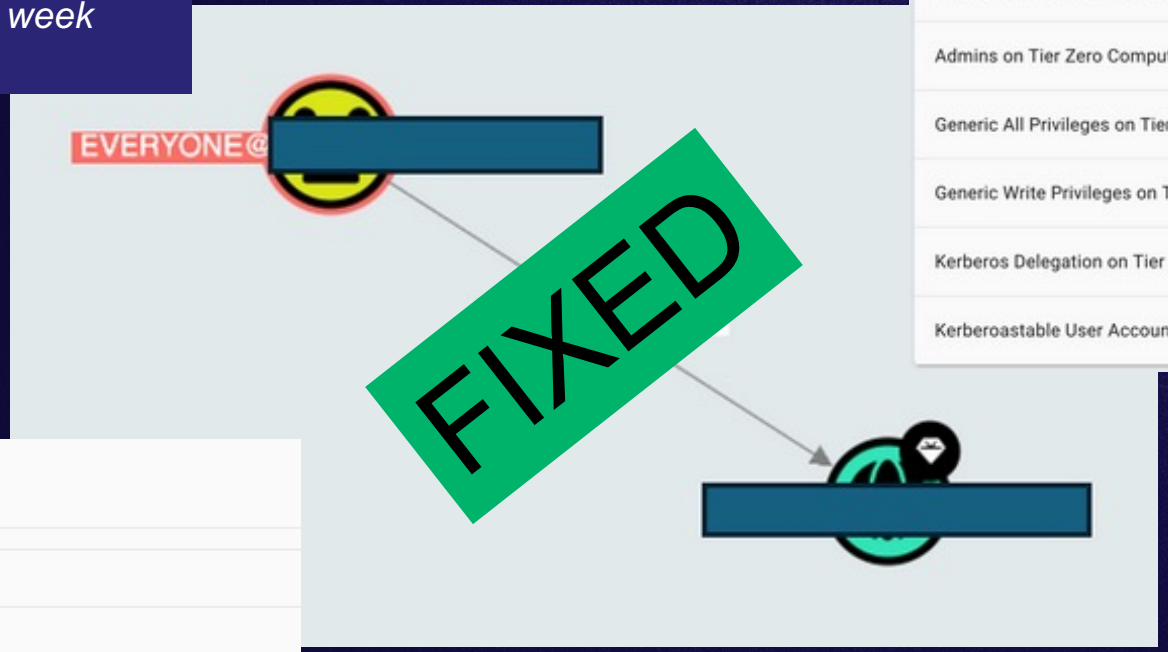
- Recognize it’s a new capability
- Build a repeatable program with stakeholder buy-in
- It’s no one’s fault (for now)
- Start small: fix one, then two, then ten
- Crawl, Walk, Run on expanding use cases

We can take back control


EVERYONE@
AllExtendedRights

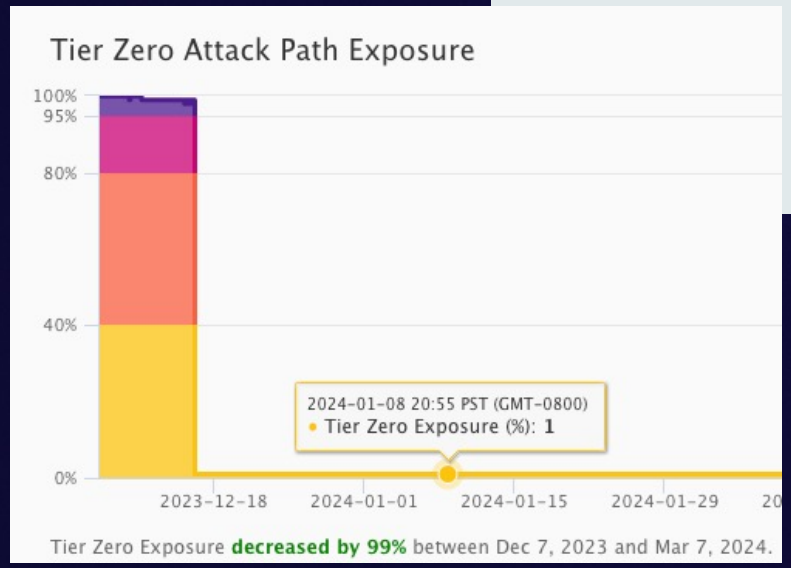
"BloodHound Enterprise has easily been the greatest reduction of risk in our organization to advanced attackers in the last year"

"I've learned more about our Active Directory environment in the past week than in the previous 4 years"



Active Attack Paths

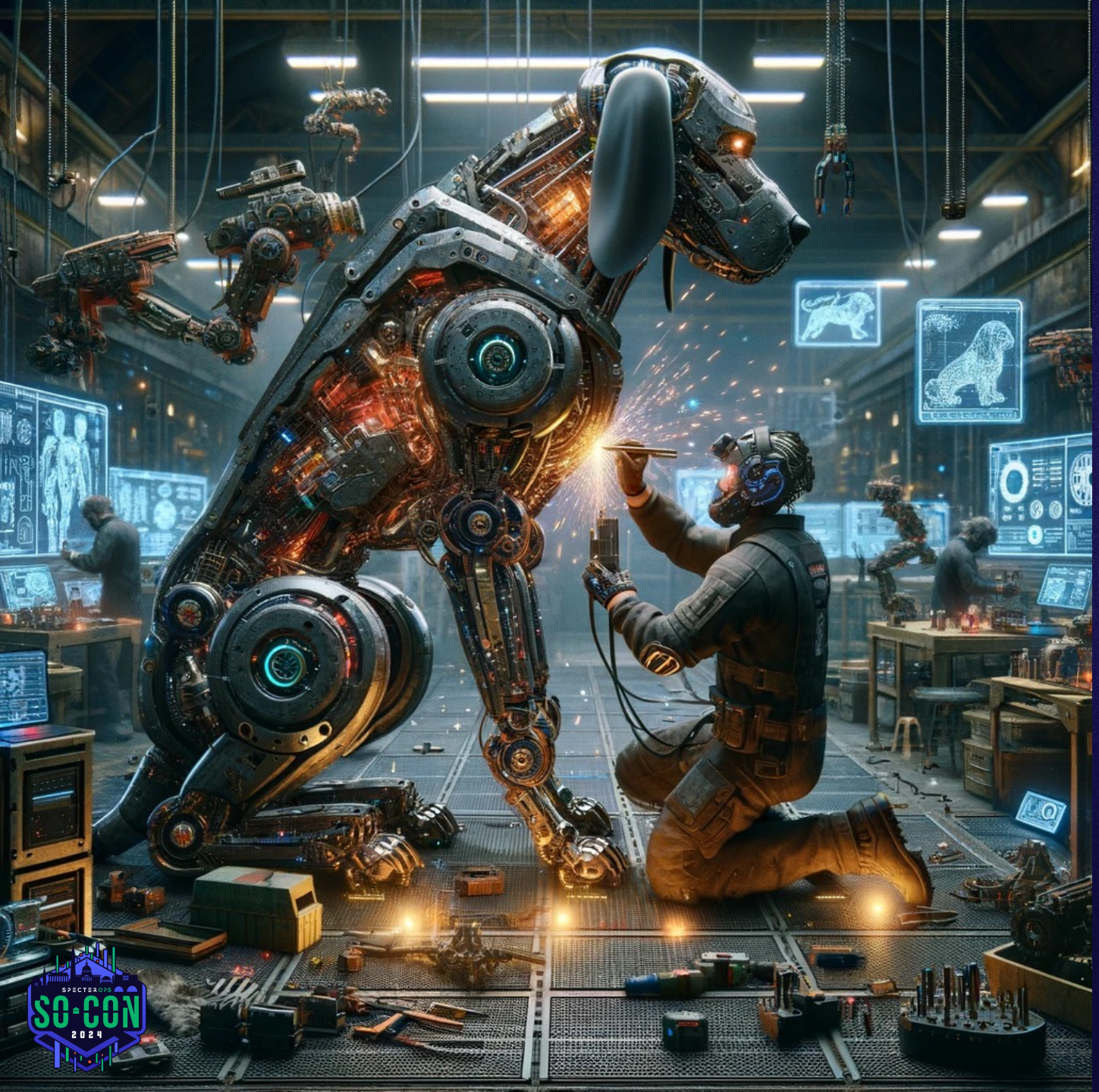
Attack Path	Impacted Principals	Change over 90 days
Add Member Privileges on Tier Zero Security Groups	1	-3
Read LAPS Password Privileges on Tier Zero Objects	4	-1
Logons from Tier Zero Users	54	-1,552
Admins on Tier Zero Computers	8	-6
Generic All Privileges on Tier Zero Objects	15	-21
Generic Write Privileges on Tier Zero Objects	4	-8
Kerberos Delegation on Tier Zero Objects	8	-8
Kerberoastable User Accounts	3	-11



Tier Zero Attack Paths	Impacted Principals	Change over 90 days	Severity
Logons from Tier Zero Users	294	-86	Low
Add Member Privileges on Tier Zero Security Groups	1	-1	Low
Generic Write Privileges on Tier Zero Objects	42	-4	Low
RDP Users on Tier Zero Computers	0	-518	Resolved
Write DACL Privileges on Tier Zero Objects	0	-5	Resolved
Write Owner Privileges on Tier Zero Objects	0	-4	Resolved

0.02% of Attack Paths actually matter

Where we go from here



BLOODHOUND COMMUNITY EDITION

- Supportive Community

  https://ghst.ly/BHSlack

- So easy I can deploy it

  https://github.com/BloodHoundAD/BloodHound

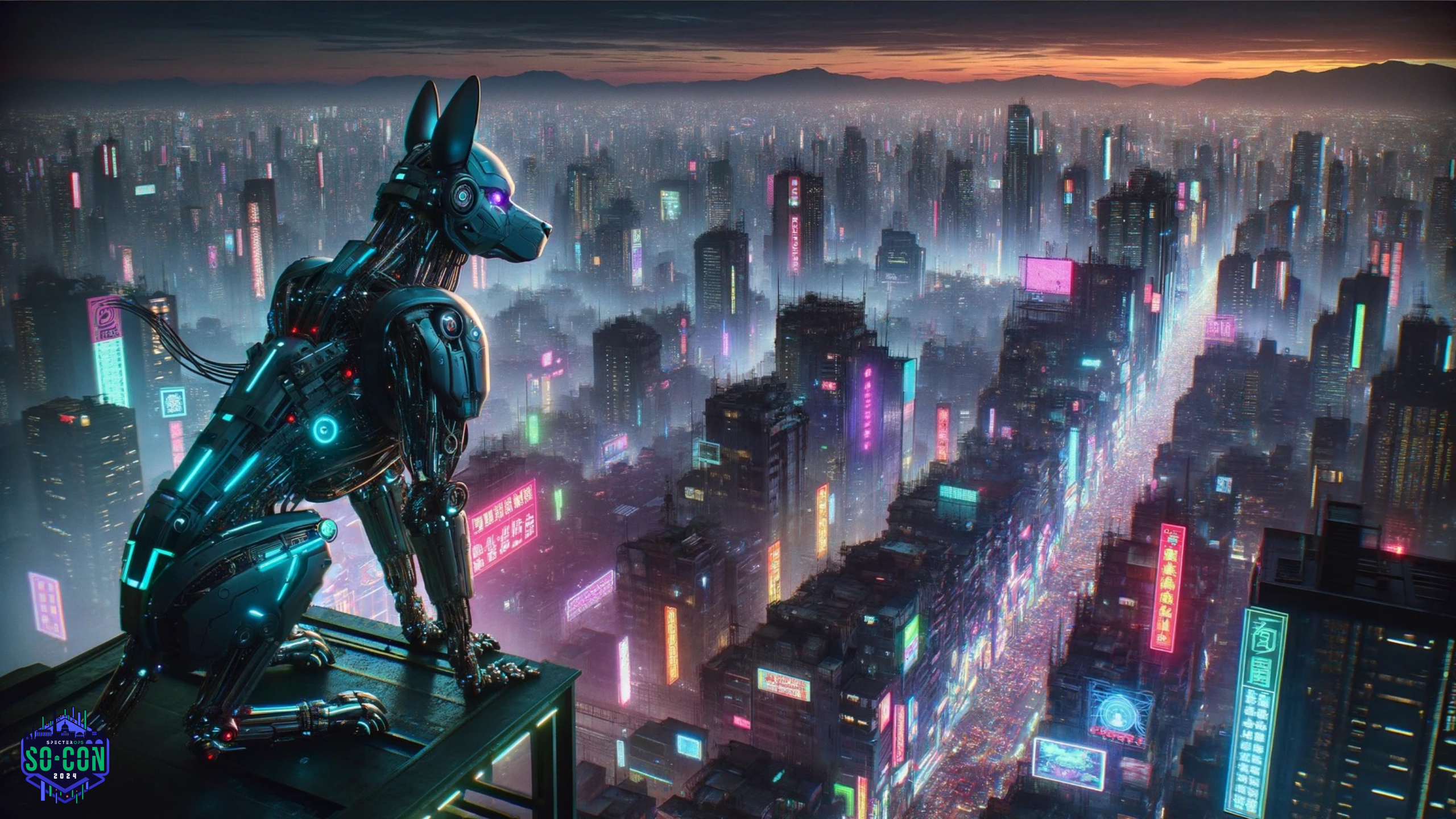
- Remove these today:

  https://www.linkedin.com/pulse/find-fix-three-common-ad-issues-andy-robbins/

BLOODHOUND ENTERPRISE

- Demo today
- See what we see
- https://bloodhoundenterprise.io/demo/

SPECTEROPS SO-CON 2024


SPECTEROPS
SO-CON
2024

Thank you