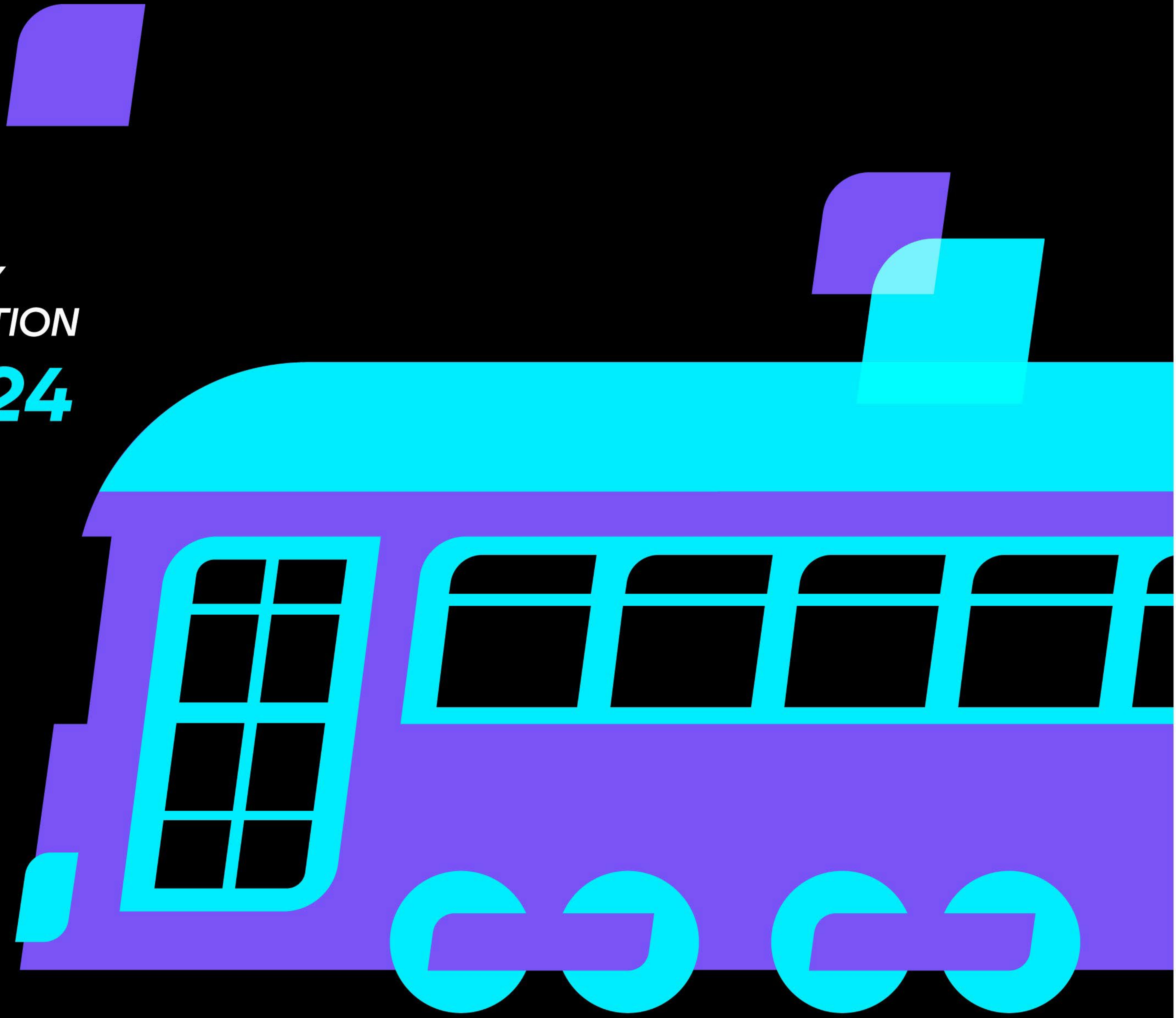
HYBRID
IDENTITY
PROTECTION

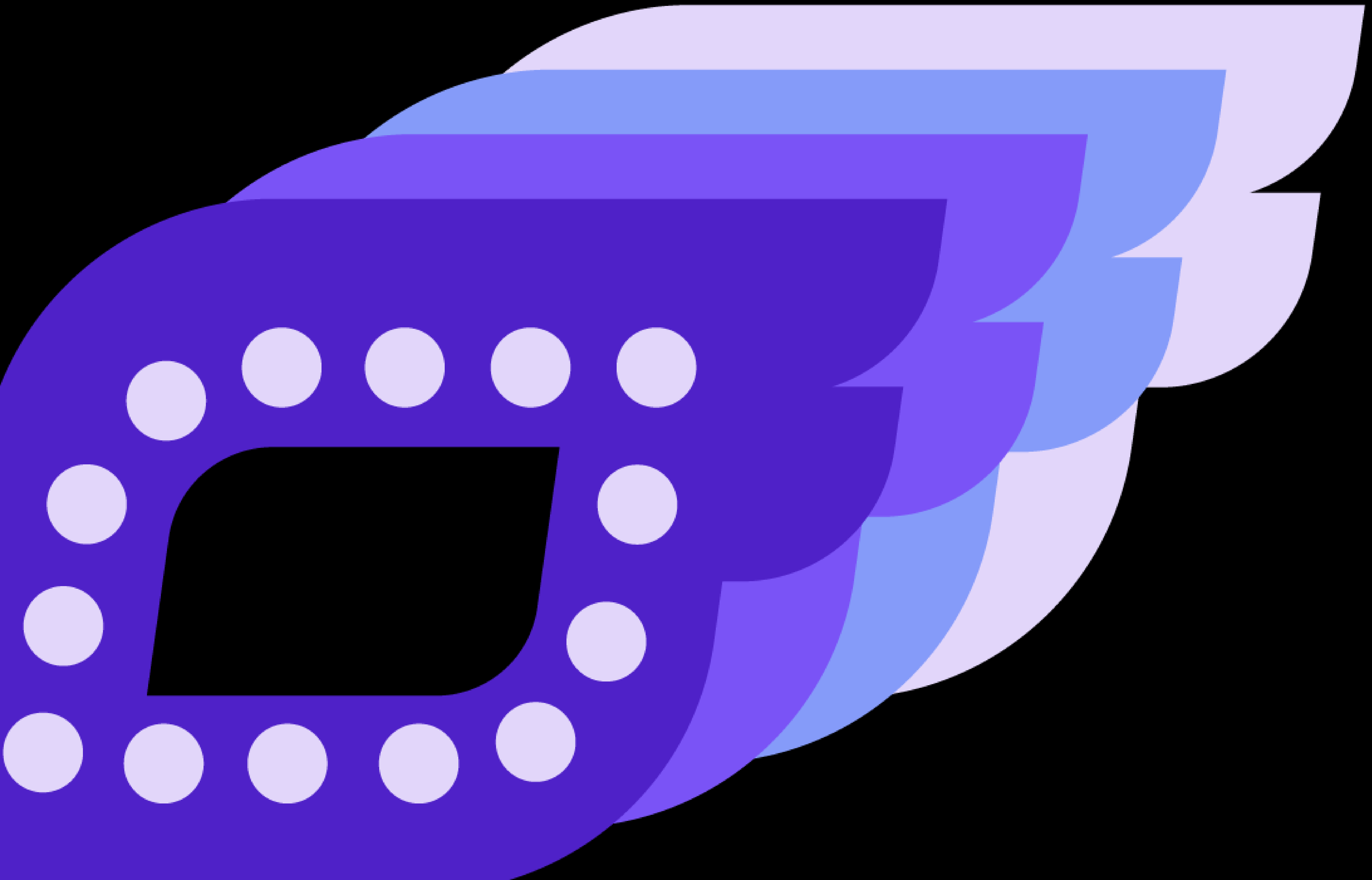
conf24

NEW ORLEANS



HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS



Beyond Tier0

The Forest Druid Journey

Darren Mar-Elia
VP Products

Ran Harel
AVP Security Products

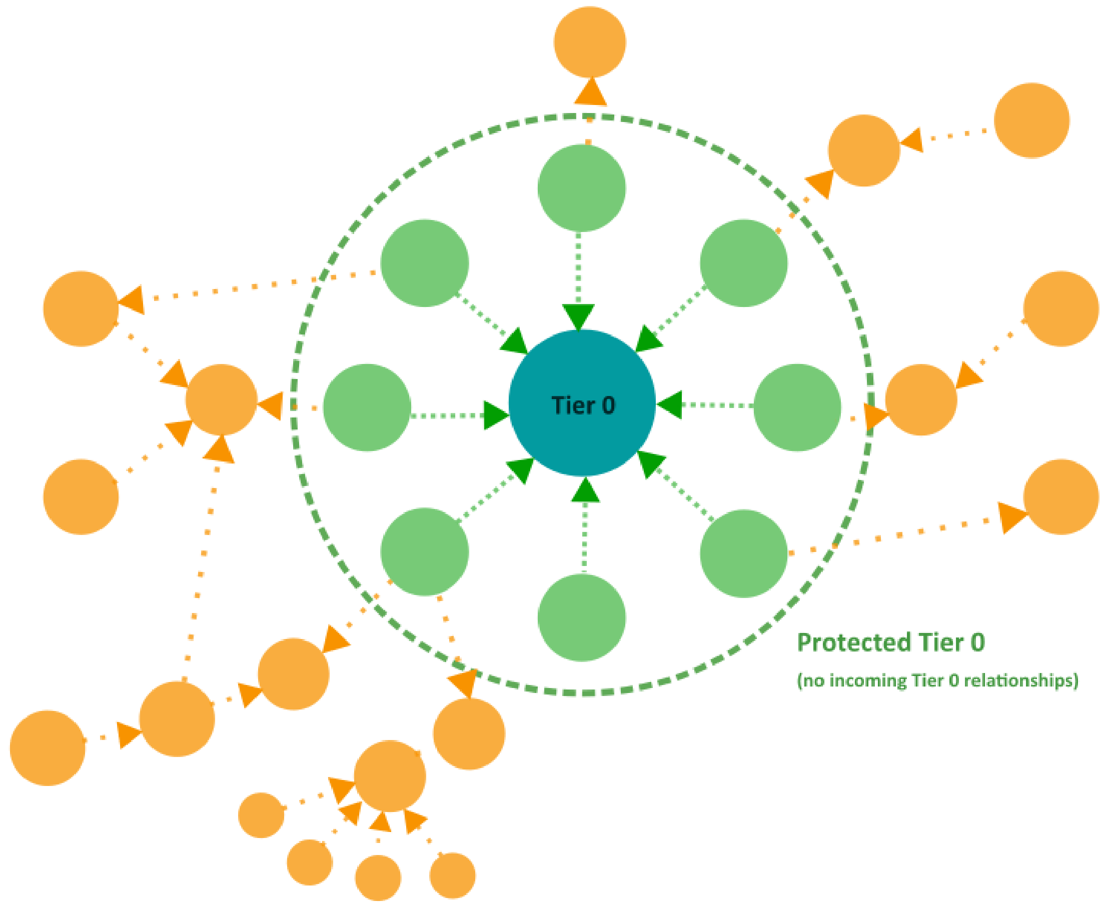
Part I

The beginning

August 2022 – Mission Statement

Goal – Identify and Protect Tier 0

- Objective 1 – Identify all attack paths into “known” Tier 0
- Objective 2 – Classify paths into Tier 0 as “legitimate” or “illegitimate”
- Objective 3 – Define a “Privilege-defined Perimeter” of <u>actual</u> Tier 0 for monitoring

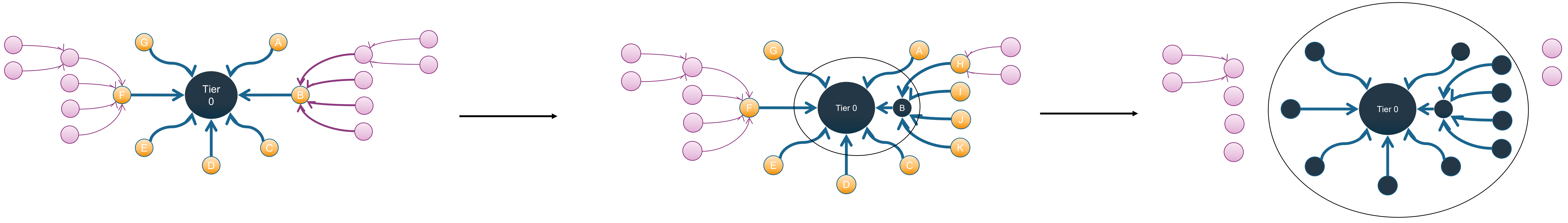


HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

forest druid powered by semperis

The Forest Druid hypotheses

- Risk boundaries are defined by an “Identity Perimeter”
- Given enough time and activity, all environments experience “access creep”
- The existing red-team methods of attack path analysis are insufficient



1. Mapping attack paths

2. Inside-out Analysis … discovering the perimeter

3. Protecting the identity-defined perimeter

Part II

The Journey

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

forest druid powered by semperis

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

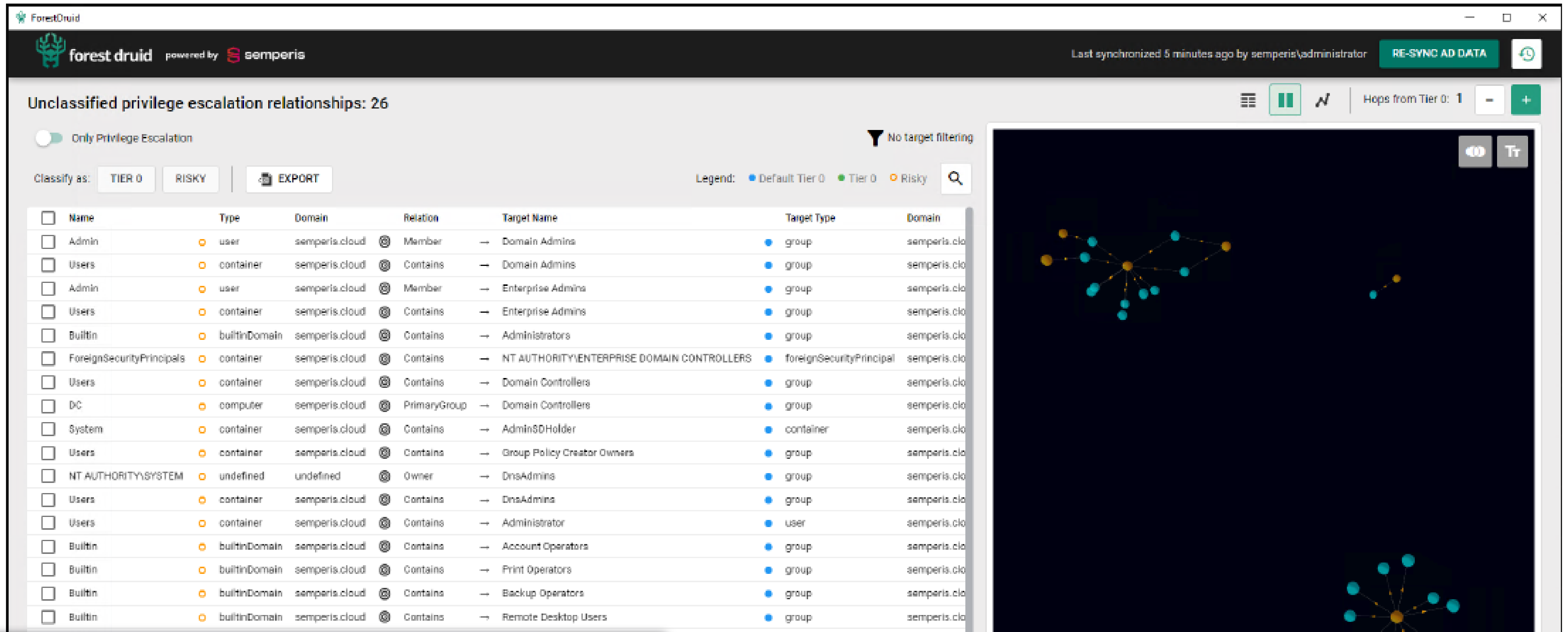
forest druid powered by semperis

Forest Druid v1 (12/22)

- Single-screen “galaxy view”
- Classify and list

What we learned:

- Prioritization is critical (need a metric)
- Must have a search / filter
- 3-D can get … messy



ForestDruid

forest druid powered by semperis

Last synchronized 5 minutes ago by semperis\administrator

Unclassified privilege escalation relationships: 26

Hops from Tier 0: 1

Only Privilege Escalation

No target filtering

Classify as: TIER 0 RISKY EXPORT

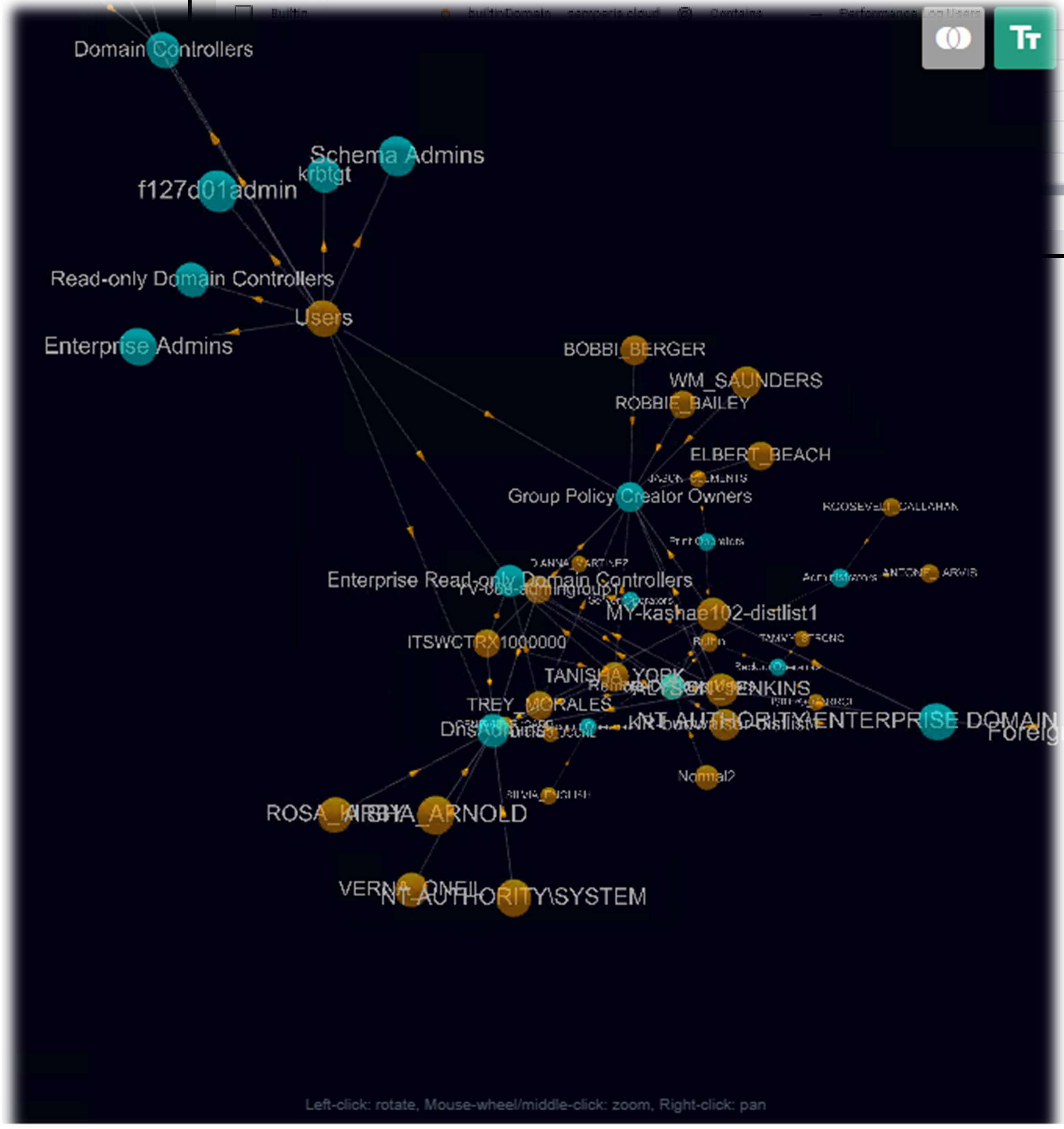
Legend: ● Default Tier 0 ● Tier 0 ○ Risky

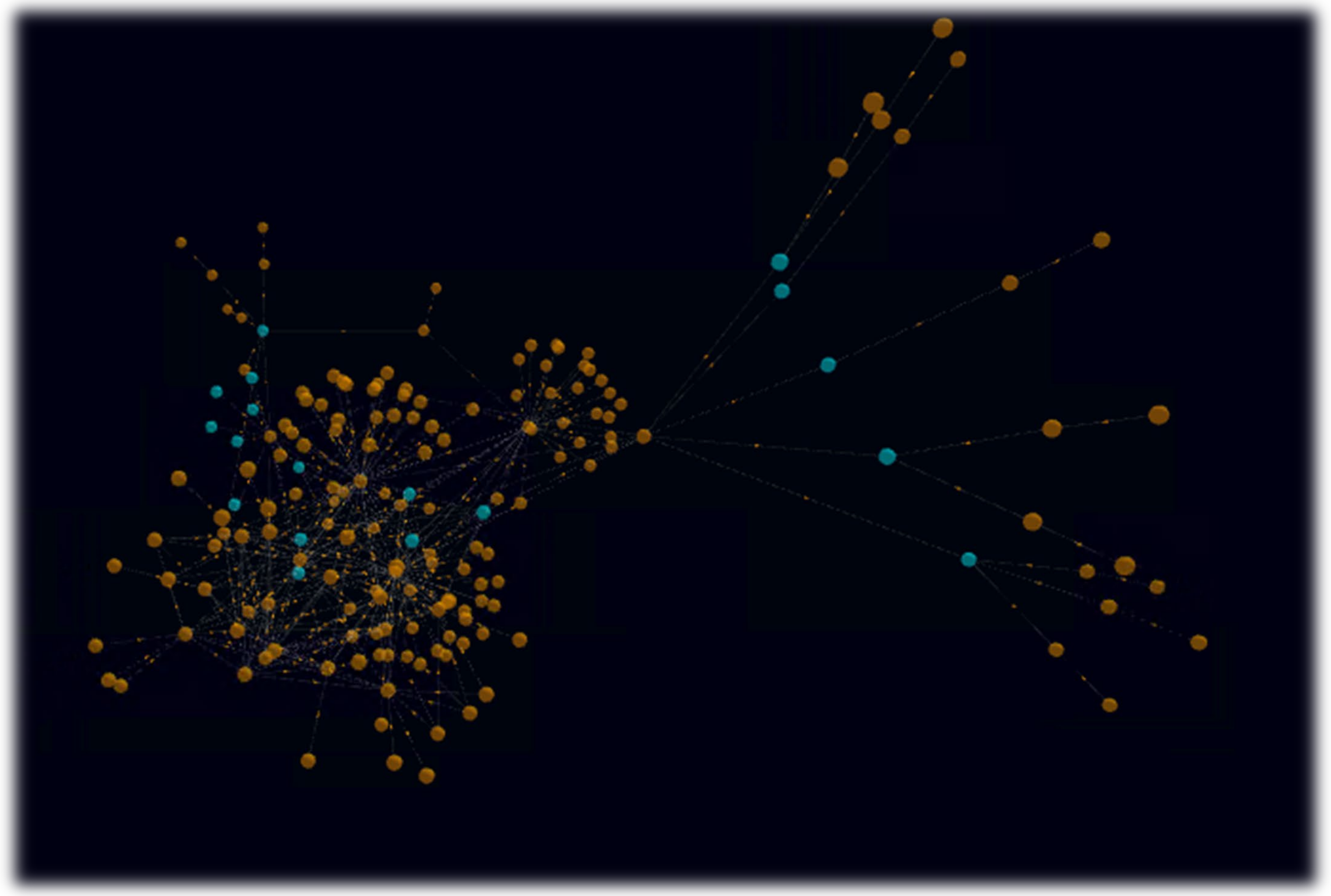
□	Name		Type	Domain		Relation		Target Name		Target Type	Domain
□	Admin	○	user	semperis.cloud	◎	Member	→	Domain Admins	●	group	semperis.clo
□	Users	○	container	semperis.cloud	◎	Contains	→	Domain Admins	●	group	semperis.clo
□	Admin	○	user	semperis.cloud	◎	Member	→	Enterprise Admins	●	group	semperis.clo
□	Users	○	container	semperis.cloud	◎	Contains	→	Enterprise Admins	●	group	semperis.clo
□	Builtin	○	builtinDomain	semperis.cloud	◎	Contains	→	Administrators	●	group	semperis.clo
□	ForeignSecurityPrincipals	○	container	semperis.cloud	◎	Contains	→	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	●	foreignSecurityPrincipal	semperis.clo
□	Users	○	container	semperis.cloud	◎	Contains	→	Domain Controllers	●	group	semperis.clo
□	DC	○	computer	semperis.cloud	◎	PrimaryGroup	→	Domain Controllers	●	group	semperis.clo
□	System	○	container	semperis.cloud	◎	Contains	→	AdminSDHolder	●	container	semperis.clo
□	Users	○	container	semperis.cloud	◎	Contains	→	Group Policy Creator Owners	●	group	semperis.clo
□	NT AUTHORITY\SYSTEM	○	undefined	undefined	◎	Owner	→	DnsAdmins	●	group	semperis.clo
□	Users	○	container	semperis.cloud	◎	Contains	→	DnsAdmins	●	group	semperis.clo
□	Users	○	container	semperis.cloud	◎	Contains	→	Administrator	●	user	semperis.clo
□	Builtin	○	builtinDomain	semperis.cloud	◎	Contains	→	Account Operators	●	group	semperis.clo
□	Builtin	○	builtinDomain	semperis.cloud	◎	Contains	→	Print Operators	●	group	semperis.clo
□	Builtin	○	builtinDomain	semperis.cloud	◎	Contains	→	Backup Operators	●	group	semperis.clo
□	Builtin	○	builtinDomain	semperis.cloud	◎	Contains	→	Remote Desktop Users	●	group	semperis.clo
□	Builtin	○	builtinDomain	semperis.cloud	◎	Contains	→	Performance Log Users	●	group	semperis.clo
									●	group	semperis.clo
									●	group	semperis.clo
									●	group	semperis.clo
									●	group	semperis.clo
									●	group	semperis.clo

1-26 of 26

Left-click: rotate, Mouse-wheel/middle-click: zoom, Right-click: pan

Version 1.0.173-62690 ©2022 Semperis. All rights reserved.





HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

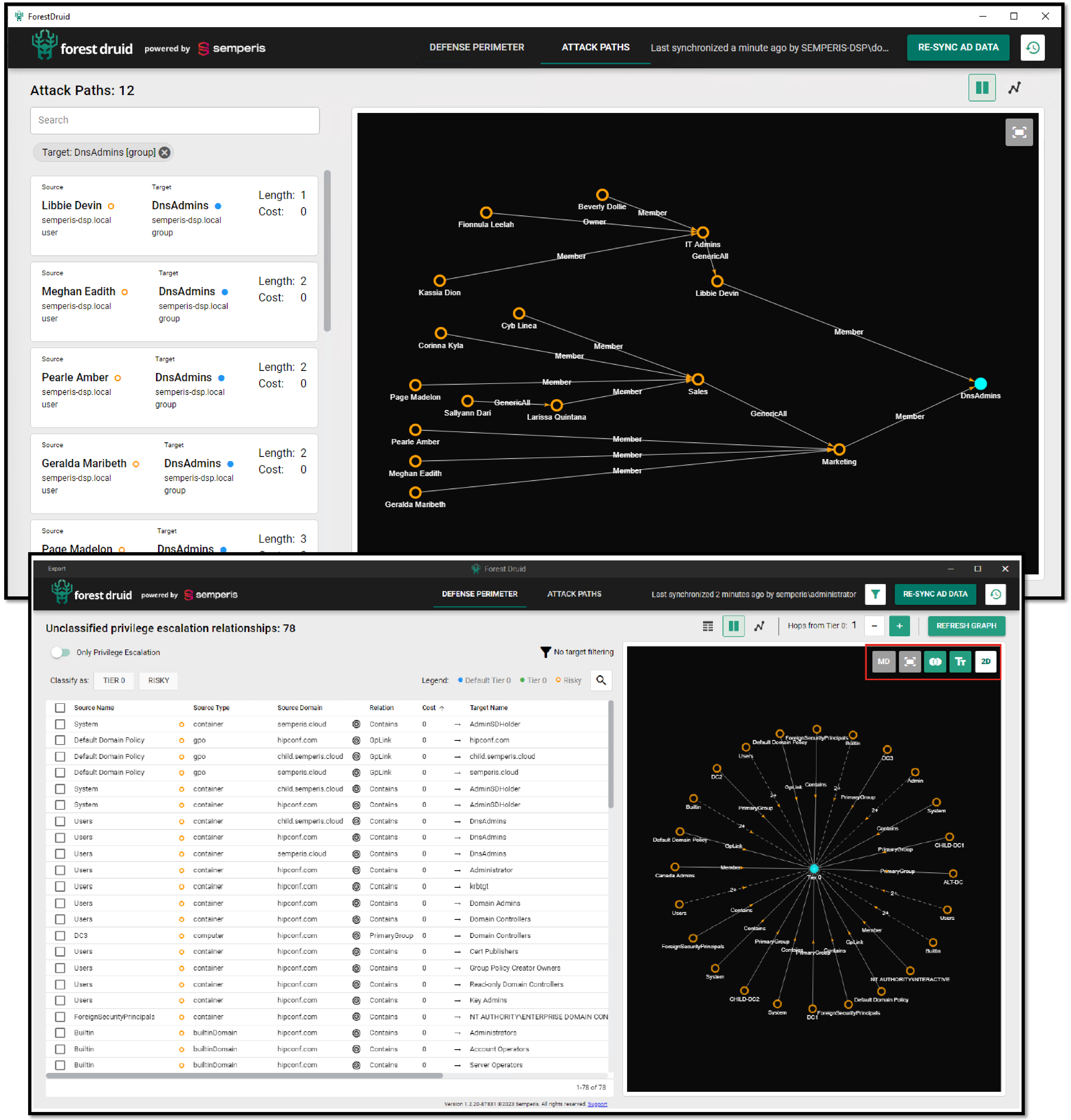
forest druid powered by semperis

Forest Druid v1.2 (4/23)

- 2-D View
- Attack Path Analysis UI
- Attack Cost (patented…)
  - NOT RISK

What we learned:

- Need more exploration tools
- Must have a search / filter
- Time to move beyond AD …



Attack Paths: 12

Search

Target: DnsAdmins [group] ⊗

Source	Target	
Libbie Devin ○ semperis-dsp.local user	DnsAdmins ● semperis-dsp.local group	Length: 1 Cost: 0
Meghan Eadith ○ semperis-dsp.local user	DnsAdmins ● semperis-dsp.local group	Length: 2 Cost: 0
Pearle Amber ○ semperis-dsp.local user	DnsAdmins ● semperis-dsp.local group	Length: 2 Cost: 0
Geralda Maribeth ○ semperis-dsp.local user	DnsAdmins ● semperis-dsp.local group	Length: 2 Cost: 0
Page Madelon ○	DnsAdmins ●	Length: 3

Last synchronized 2 minutes ago by semperis\administrator

RE-SYNC AD DATA

Unclassified privilege escalation relationships: 78

Hops from Tier 0: 1 − +

REFRESH GRAPH

Only Privilege Escalation

No target filtering

Classify as: TIER 0 RISKY

Legend: ● Default Tier 0 ● Tier 0 ○ Risky

□	Source Name		Source Type	Source Domain		Relation	Cost ↑		Target Name
□	System	○	container	semperis.cloud	◎	Contains	0	→	AdminSDHolder
□	Default Domain Policy	○	gpo	hipconf.com	◎	GpLink	0	→	hipconf.com
□	Default Domain Policy	○	gpo	child.semperis.cloud	◎	GpLink	0	→	child.semperis.cloud
□	Default Domain Policy	○	gpo	semperis.cloud	◎	GpLink	0	→	semperis.cloud
□	System	○	container	child.semperis.cloud	◎	Contains	0	→	AdminSDHolder
□	System	○	container	hipconf.com	◎	Contains	0	→	AdminSDHolder
□	Users	○	container	child.semperis.cloud	◎	Contains	0	→	DnsAdmins
□	Users	○	container	hipconf.com	◎	Contains	0	→	DnsAdmins
□	Users	○	container	semperis.cloud	◎	Contains	0	→	DnsAdmins
□	Users	○	container	hipconf.com	◎	Contains	0	→	Administrator
□	Users	○	container	hipconf.com	◎	Contains	0	→	krbtgt
□	Users	○	container	hipconf.com	◎	Contains	0	→	Domain Admins
□	Users	○	container	hipconf.com	◎	Contains	0	→	Domain Controllers
□	DC3	○	computer	hipconf.com	◎	PrimaryGroup	0	→	Domain Controllers
□	Users	○	container	hipconf.com	◎	Contains	0	→	Cert Publishers
□	Users	○	container	hipconf.com	◎	Contains	0	→	Group Policy Creator Owners
□	Users	○	container	hipconf.com	◎	Contains	0	→	Read-only Domain Controllers
□	Users	○	container	hipconf.com	◎	Contains	0	→	Key Admins
□	ForeignSecurityPrincipals	○	container	hipconf.com	◎	Contains	0	→	NT AUTHORITY\ENTERPRISE DOMAIN CON
□	Builtin	○	builtinDomain	hipconf.com	◎	Contains	0	→	Administrators
□	Builtin	○	builtinDomain	hipconf.com	◎	Contains	0	→	Account Operators
□	Builtin	○	builtinDomain	hipconf.com	◎	Contains	0	→	Server Operators

1-78 of 78

Version 1.2.20-87831 ©2023 Semperis. All rights reserved. Support

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

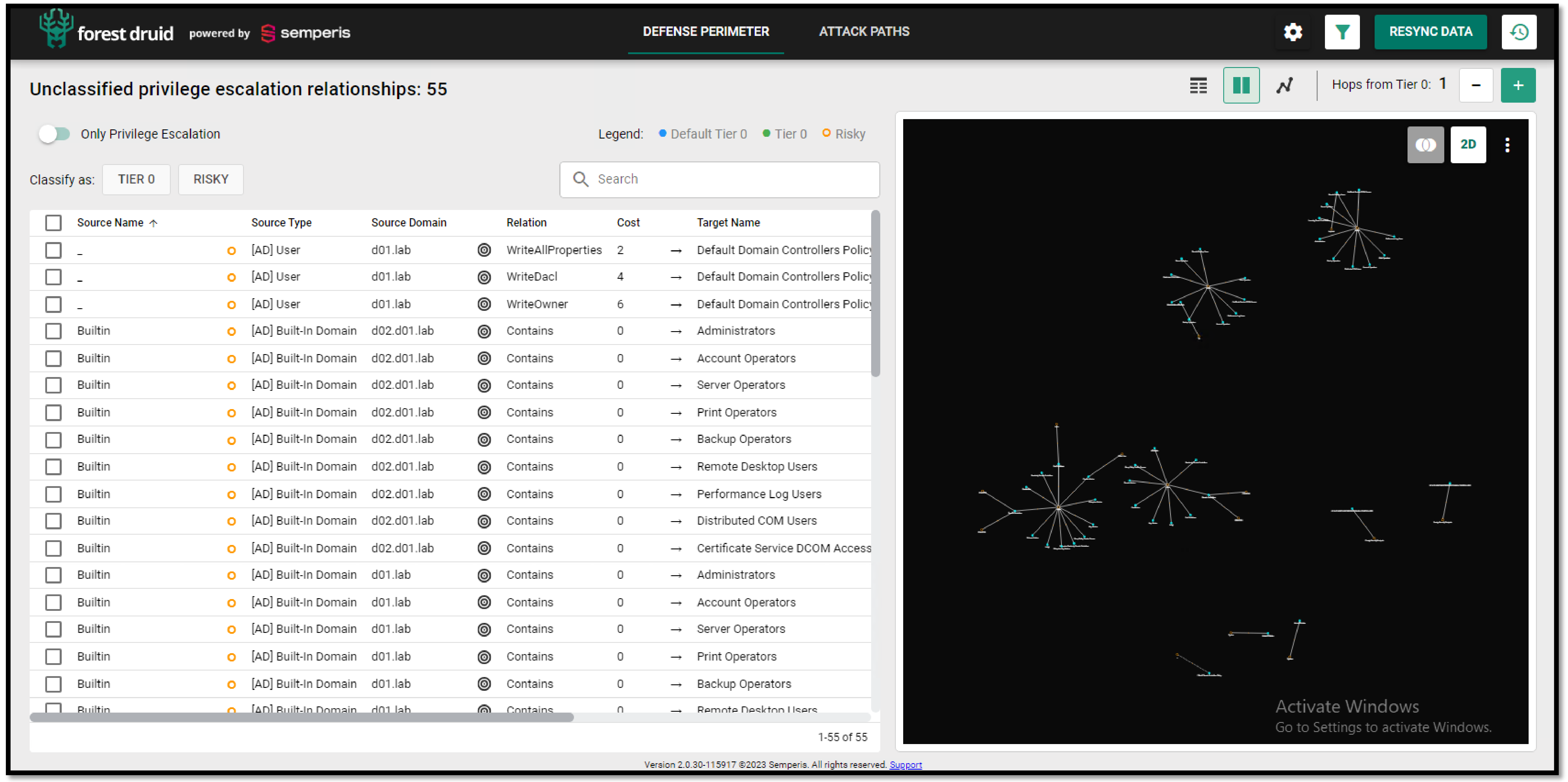
forest druid powered by semperis

Forest Druid v2 (10/23)

- **Entra ID Control Plane**
- Advanced Graph Controls
- Data Filters

What we learned:

- The UI is still clunky
- We need to move beyond the pre-defined perimeters …



Unclassified privilege escalation relationships: 55

Only Privilege Escalation

Legend: ● Default Tier 0 ● Tier 0 ○ Risky

Classify as: TIER 0 RISKY

Search

□	Source Name ↑		Source Type	Source Domain		Relation	Cost		Target Name
□	_	○	[AD] User	d01.lab	◎	WriteAllProperties	2	→	Default Domain Controllers Polic
□	_	○	[AD] User	d01.lab	◎	WriteDacl	4	→	Default Domain Controllers Polic
□	_	○	[AD] User	d01.lab	◎	WriteOwner	6	→	Default Domain Controllers Polic
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Administrators
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Account Operators
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Server Operators
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Print Operators
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Backup Operators
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Remote Desktop Users
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Performance Log Users
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Distributed COM Users
□	Builtin	○	[AD] Built-In Domain	d02.d01.lab	◎	Contains	0	→	Certificate Service DCOM Access
□	Builtin	○	[AD] Built-In Domain	d01.lab	◎	Contains	0	→	Administrators
□	Builtin	○	[AD] Built-In Domain	d01.lab	◎	Contains	0	→	Account Operators
□	Builtin	○	[AD] Built-In Domain	d01.lab	◎	Contains	0	→	Server Operators
□	Builtin	○	[AD] Built-In Domain	d01.lab	◎	Contains	0	→	Print Operators
□	Builtin	○	[AD] Built-In Domain	d01.lab	◎	Contains	0	→	Backup Operators
□	Builtin	○	[AD] Built-In Domain	d01.lab	◎	Contains	0	→	Remote Desktop Users

1-55 of 55

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

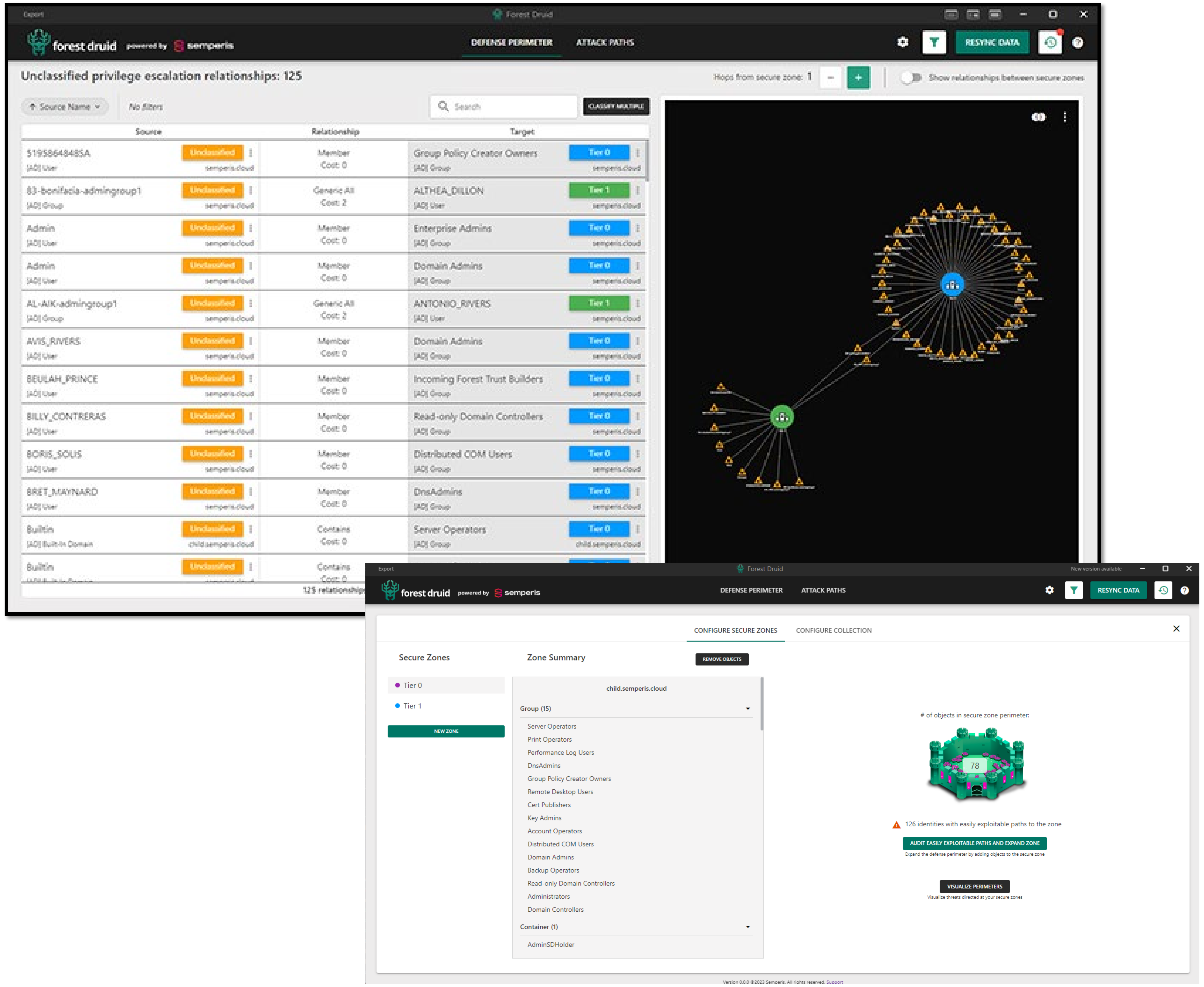
forest druid
powered by semperis

Forest Druid v3 (4/24)

- Custom zones
- UI overhaul

What we learned:

- Need “traversal” functionality
- Perimeters represent risk
- We need to scale …



Unclassified privilege escalation relationships: 125

Source		Relationship	Target	
5195864848SA [AD] User	Unclassified semperis.cloud	Member Cost: 0	Group Policy Creator Owners [AD] Group	Tier 0 semperis.cloud
83-bonifacia-admingroup1 [AD] Group	Unclassified semperis.cloud	Generic All Cost: 2	ALTHEA_DILLON [AD] User	Tier 1 semperis.cloud
Admin [AD] User	Unclassified semperis.cloud	Member Cost: 0	Enterprise Admins [AD] Group	Tier 0 semperis.cloud
Admin [AD] User	Unclassified semperis.cloud	Member Cost: 0	Domain Admins [AD] Group	Tier 0 semperis.cloud
AL-AIK-admingroup1 [AD] Group	Unclassified semperis.cloud	Generic All Cost: 2	ANTONIO_RIVERS [AD] User	Tier 1 semperis.cloud
AVIS_RIVERS [AD] User	Unclassified semperis.cloud	Member Cost: 0	Domain Admins [AD] Group	Tier 0 semperis.cloud
BEULAH_PRINCE [AD] User	Unclassified semperis.cloud	Member Cost: 0	Incoming Forest Trust Builders [AD] Group	Tier 0 semperis.cloud
BILLY_CONTRERAS [AD] User	Unclassified semperis.cloud	Member Cost: 0	Read-only Domain Controllers [AD] Group	Tier 0 semperis.cloud
BORIS_SOLIS [AD] User	Unclassified semperis.cloud	Member Cost: 0	Distributed COM Users [AD] Group	Tier 0 semperis.cloud
BRET_MAYNARD [AD] User	Unclassified semperis.cloud	Member Cost: 0	DnsAdmins [AD] Group	Tier 0 semperis.cloud
Builtin [AD] Built-In Domain	Unclassified child.semperis.cloud	Contains Cost: 0	Server Operators [AD] Group	Tier 0 child.semperis.cloud
Builtin	Unclassified	Contains Cost: 0		

125 relationships

Secure Zones

- Tier 0
- Tier 1

Zone Summary

child.semperis.cloud

Group (15)

Server Operators
Print Operators
Performance Log Users
DnsAdmins
Group Policy Creator Owners
Remote Desktop Users
Cert Publishers
Key Admins
Account Operators
Distributed COM Users
Domain Admins
Backup Operators
Read-only Domain Controllers
Administrators
Domain Controllers

Container (1)

AdminSDHolder

# of objects in secure zone perimeter:

⚠ 126 identities with easily exploitable paths to the zone

Expand the defense perimeter by adding objects to the secure zone

Visualize threats directed at your secure zones

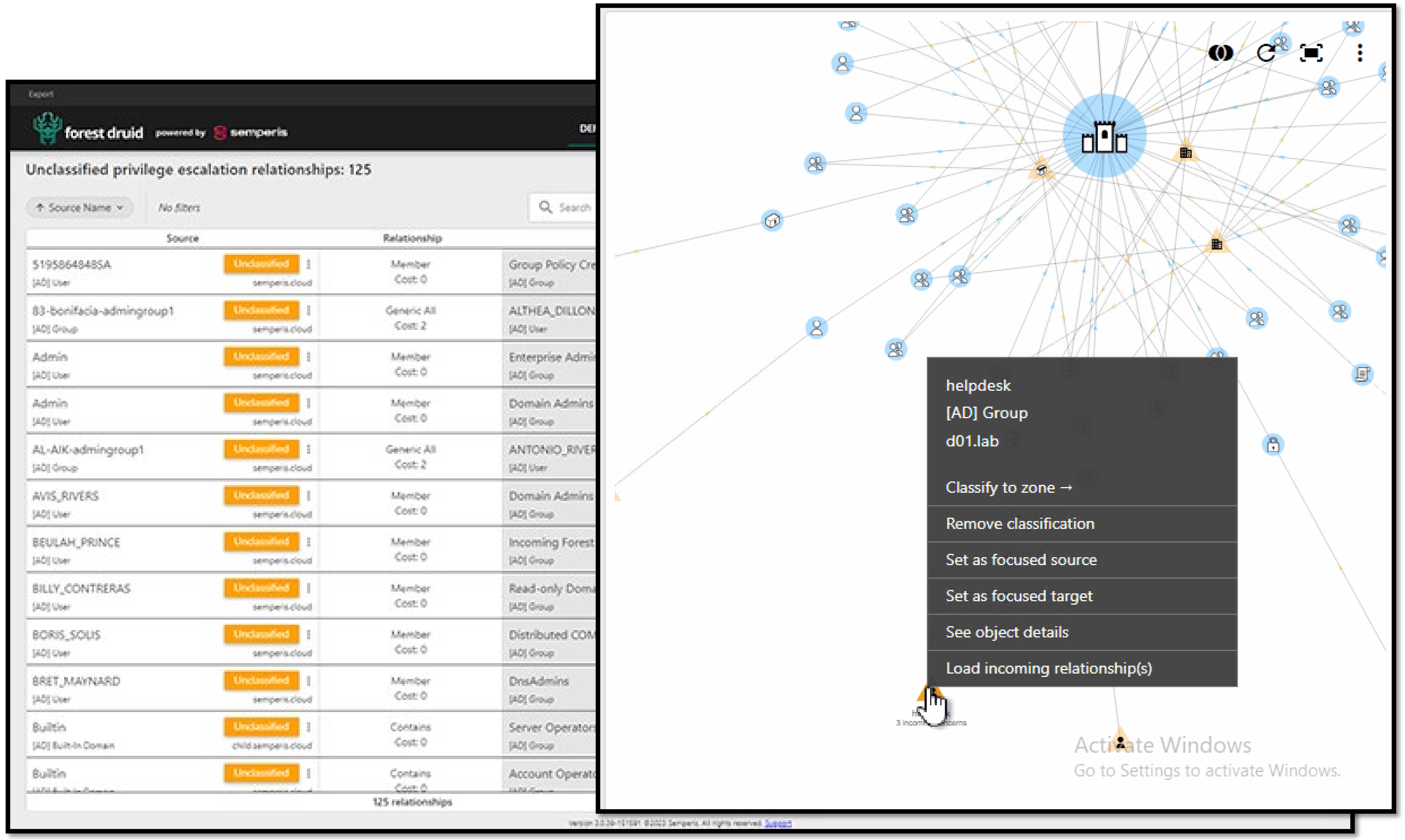
Version 0.0.0 ©2023 Semperis. All rights reserved. Support

Forest Druid v3.1 (7/24)

- Graph traversal
- Scale (2 million objects, 4 million relationships)

What we learned:

- Perimeters represent risk
- We need to scale …



Export

forest druid powered by semperis

Unclassified privilege escalation relationships: 125

↑ Source Name ⌄   No filters   Search

Source		Relationship	
51958648485A [AD] User	Unclassified semperis.cloud	Member Cost: 0	Group Policy Cre [AD] Group
83-bonifacia-admingroup1 [AD] Group	Unclassified semperis.cloud	Generic All Cost: 2	ALTHEA_DILLON [AD] User
Admin [AD] User	Unclassified semperis.cloud	Member Cost: 0	Enterprise Admi [AD] Group
Admin [AD] User	Unclassified semperis.cloud	Member Cost: 0	Domain Admins [AD] Group
AL-AIK-admingroup1 [AD] Group	Unclassified semperis.cloud	Generic All Cost: 2	ANTONIO_RIVER [AD] User
AVIS_RIVERS [AD] User	Unclassified semperis.cloud	Member Cost: 0	Domain Admins [AD] Group
BEULAH_PRINCE [AD] User	Unclassified semperis.cloud	Member Cost: 0	Incoming Forest [AD] Group
BILLY_CONTRERAS [AD] User	Unclassified semperis.cloud	Member Cost: 0	Read-only Doma [AD] Group
BORIS_SOLIS [AD] User	Unclassified semperis.cloud	Member Cost: 0	Distributed COM [AD] Group
BRET_MAYNARD [AD] User	Unclassified semperis.cloud	Member Cost: 0	DnsAdmins [AD] Group
Builtin [AD] Built-in Domain	Unclassified child.semperis.cloud	Contains Cost: 0	Server Operator [AD] Group
Builtin	Unclassified	Contains Cost: 0	Account Operat

125 relationships

helpdesk
[AD] Group
d01.lab

Where we are today…

- After 2 years of Forest Druid…
  - Hundreds of downloads
  - Dozens of user sessions
  - Massive scale (2 million nodes, 4 million edges)

- Major lessons learned
  - There is **always** privilege creep
  - Attack path analysis is an ongoing effort
  - There is more to identity risk than just Tier 0 ….

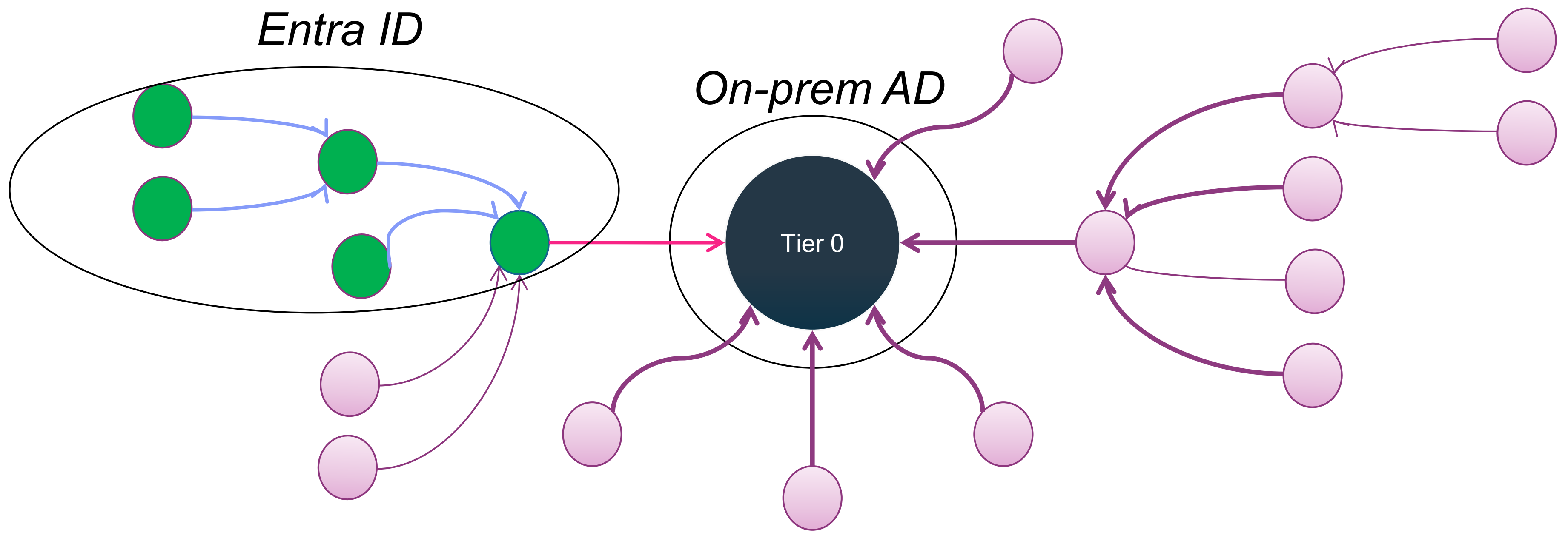
Part III

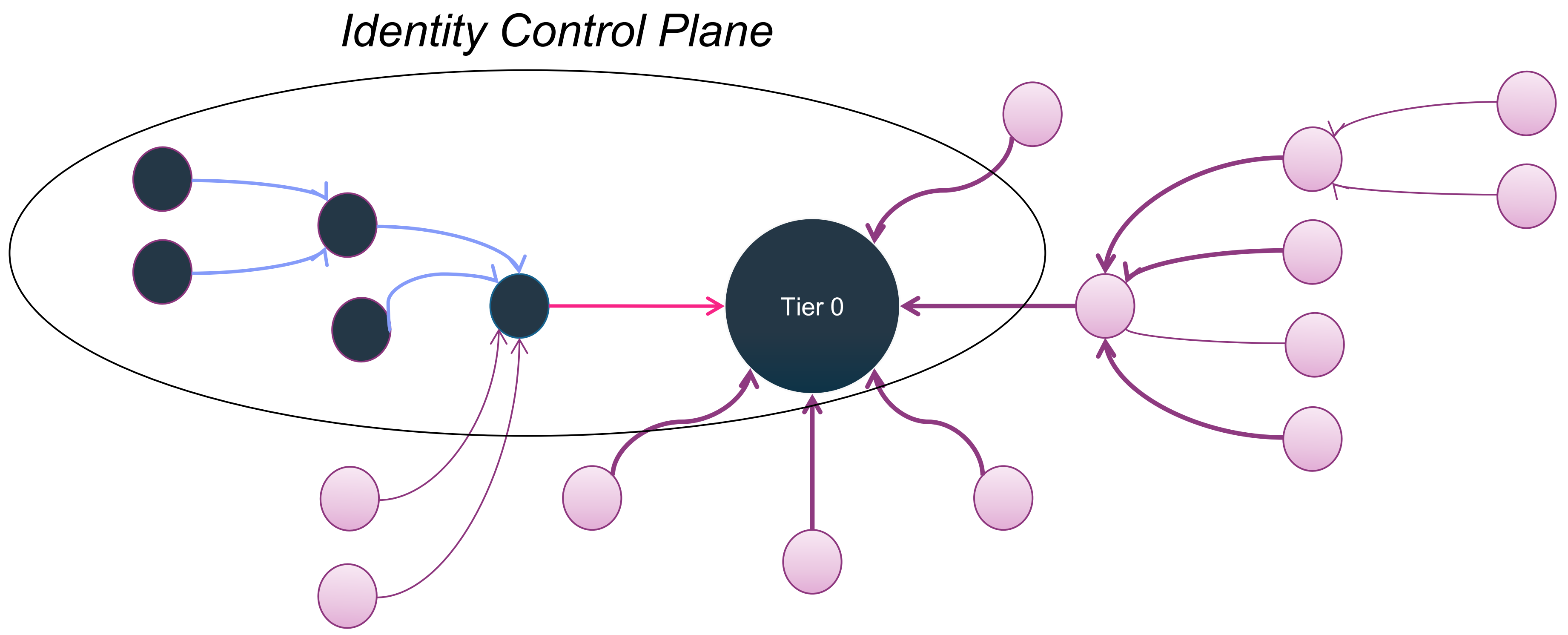
The Identity Defined Perimeter

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

forest druid powered by semperis

What are Security Zones?

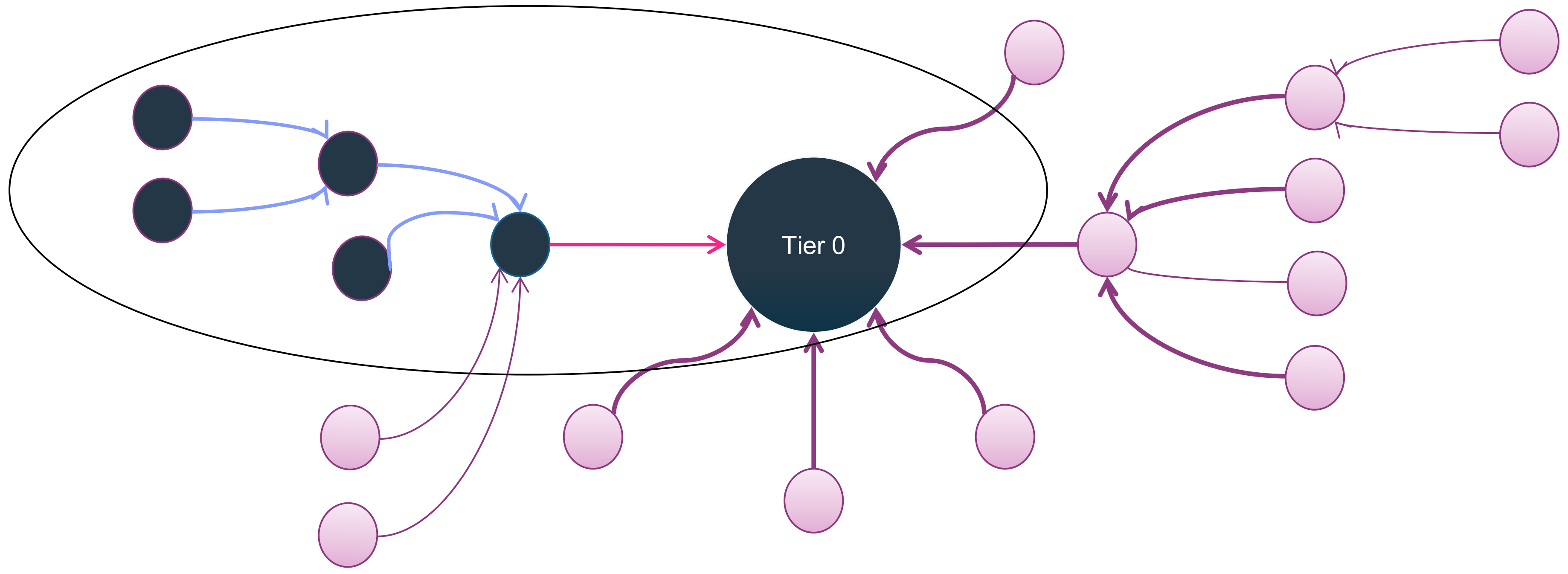




Use Case 1 - Identity Control Plane … Together but separate

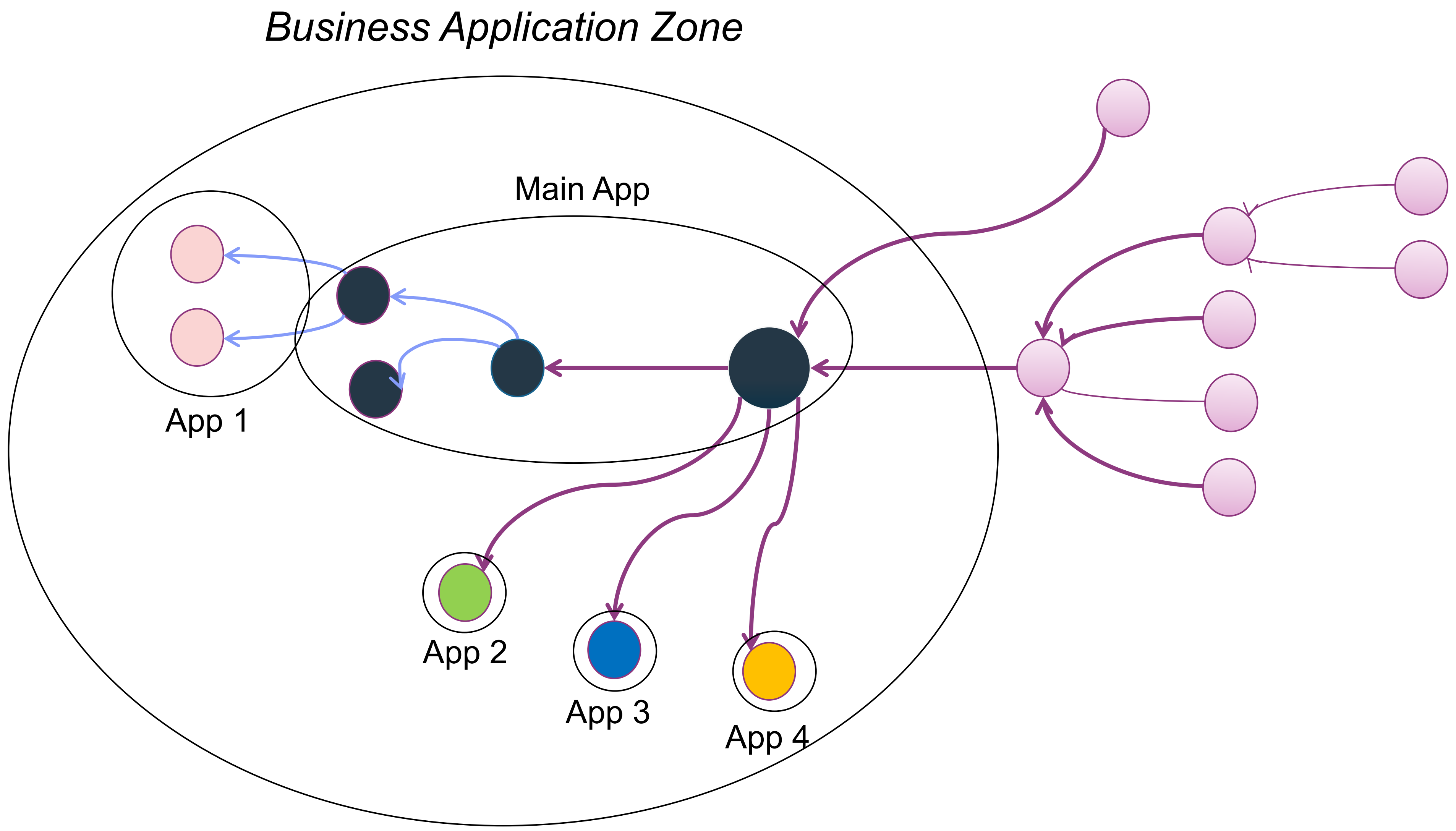
What are Security Zones?

Backup Zone



Use Case 2 – IT Infrastructure Resilience

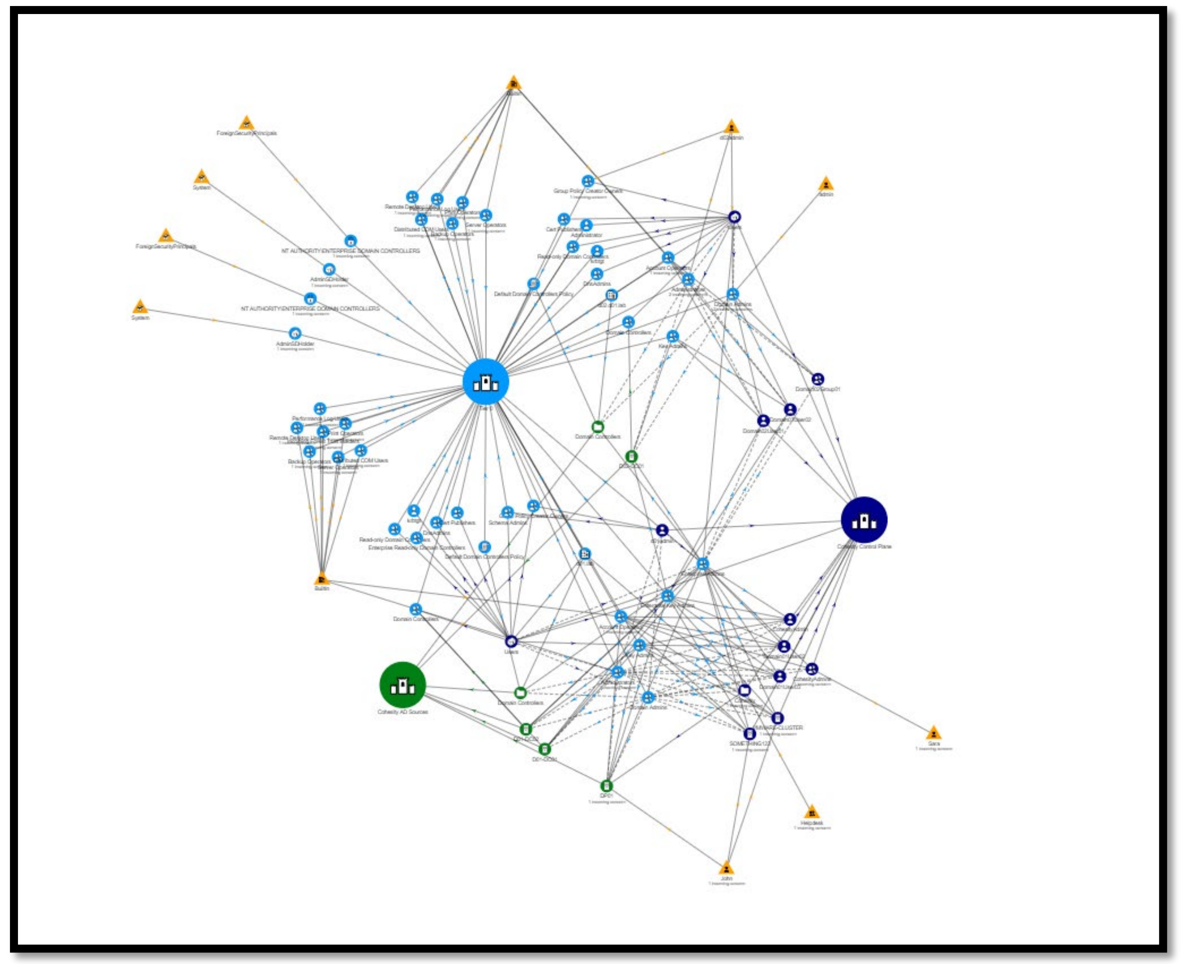
What are Security Zones?

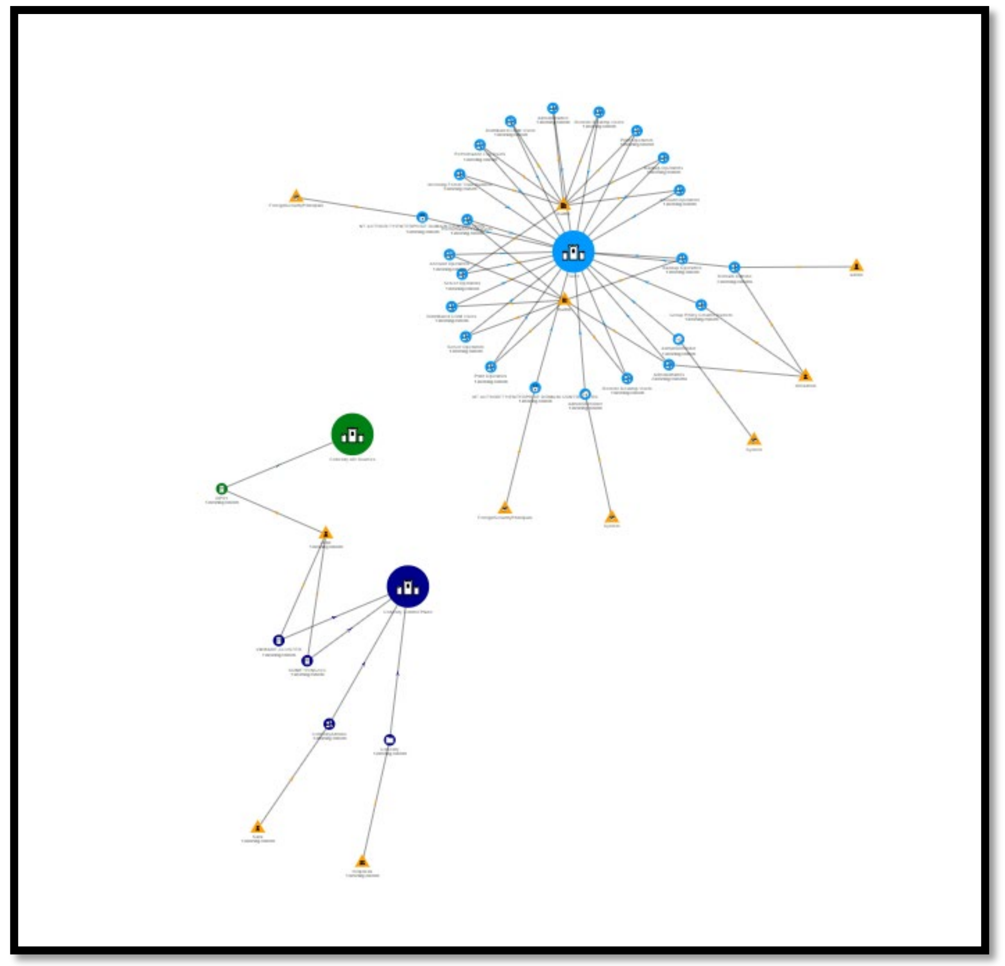


Use Case 3 – Cloud Applications

So what does that look like ?

- Version 3.2 … the Forest Druid SDK
- Add-on security zones – import “privilege lexicons” to map out perimeters of any application, infrastructure, etc..
- Cohesity demo…





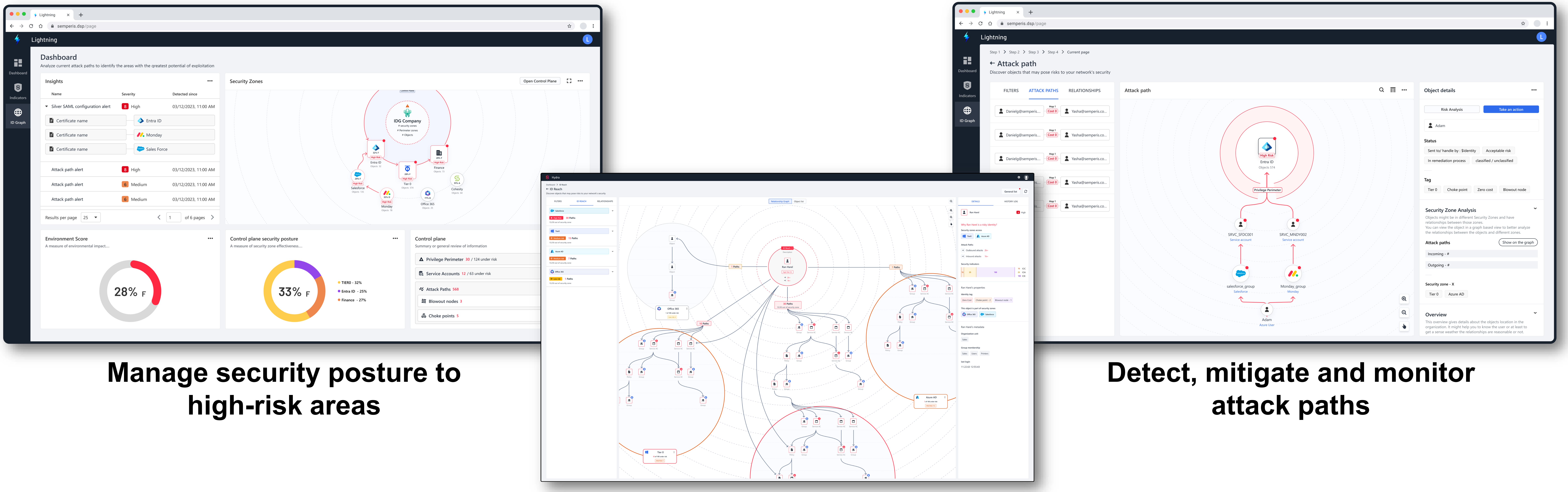
Part III

The (near) Future

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

Lightning

Welcome to Lightning



Lightning

semperis.dsp/page

Dashboard

Analyze current attack paths to identify the areas with the greatest potential of exploitation

Insights

Name	Severity	Detected since
Silver SAML configuration alert	8 High	03/12/2023, 11:00 AM
Certificate name	Entra ID	
Certificate name	Monday	
Certificate name	Sales Force	
Attack path alert	8 High	03/12/2023, 11:00 AM
Attack path alert	6 Medium	03/12/2023, 11:00 AM
Attack path alert	6 Medium	03/12/2023, 11:00 AM

Results per page 25 · 1 of 6 pages

Security Zones

Environment Score

A measure of environmental impact....

28% F

Control plane security posture

A measure of security zone effectiveness....

33% F

- TIER0 - 32%
- Entra ID - 25%
- Finance - 27%

Control plane

Summary or general review of information

- Privilege Perimeter 30 / 124 under risk
- Service Accounts 12 / 63 under risk
- Attack Paths 568
- Blowout nodes 3
- Choke points 5

Step 1 > Step 2 > Step 3 > Step 4 > Current page

← Attack path

Discover objects that may pose risks to your network's security

FILTERS · ATTACK PATHS · RELATIONSHIPS

Danielg@semperis....	Hop 1 Cost 0	Yasha@semperis.co...
Danielg@semperis....	Hop 1 Cost 0	Yasha@semperis.co...
Danielg@semperis....	Hop 1 Cost 0	Yasha@semperis.co...
	Hop 1 Cost 0	Yasha@semperis.co...
	Hop 1 Cost 0	Yasha@semperis.co...

Object details

Risk Analysis · Take an action

Adam

Status: Sent to/ handle by : $Identity · Acceptable risk · In remediation process · classified / unclassified

Tag: Tier 0 · Choke point · Zero cost · Blowout node

Security Zone Analysis

Objects might be in different Security Zones and have relationships between those zones. You can view the object in a graph based view to better analyze the relationships between the objects and different zones.

Attack paths — Show on the graph

- Incoming - #
- Outgoing - #

Security zone - X: Tier 0 · Azure AD

Overview

This overview gives details about the objects location in the organization. It might help you to know the user or at least to get a sense weather the relationships are reasonable or not.

Manage security posture to high-risk areas

Identify, remediate and manage risky identities – human and non-human (service accounts)

Detect, mitigate and monitor attack paths

HYBRID
IDENTITY
PROTECTION
conf24
NEW ORLEANS

Thank You !

Questions?