

# DOUBLE YOUR PROFIT WITH THESE TOOLS FOR ACTIVE DIRECTORY SECURITY

SEMPERIS FREE TOOLS  
COMMUNITY DRIVEN

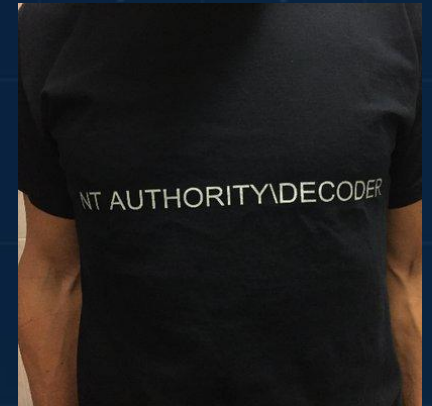
Andrea Pierini

Marco Magnaguagno



# Who am I: Andrea Pierini

- Senior IR and BP consultant @ Semperis
- IT security enthusiast and independent researcher
- Microsoft Most Valuable Researcher top #100 – 2022
- \*potato saga contributor ;)
- C64, MS-DOS, Windows 3.1, NT 4.0 & Linux Slackware 1.00 lover



*@decoder\_it | <https://decoder.cloud> | [www.linkedin.com/in/andrea-pierini](https://www.linkedin.com/in/andrea-pierini)*

# Who am I: Marco Magnaguagno

- **Solution Architect @ Semperis**
- **Microsoft CE/PFE**
- **Consulting on Microsoft technology**
- **More than 17 years in tech industry**



*@Il\_MMagna | [www.linkedin.com/in/marco-magnaguagno/](https://www.linkedin.com/in/marco-magnaguagno/)*

# AGENDA

- Why it is important to protect identity



- What is Purple Knight?
- How it works
- Requirement
- Demo



- What is Forest Druid?
- How it works
- Requirement
- Demo

## KEYS TO THE KINGDOM

# Identity is the new perimeter

For over 90% of the enterprise, **identity starts with Active Directory.**



## KEYS TO THE KINGDOM

# If AD isn't secure, nothing is

**Cloud identity is extended from Active Directory.** If tampered with, it will have a ripple effect across the entire identity infrastructure.

**Zero trust model assumes** that the only component that you can trust is the identity.





# Purple Knight

**Free tools for securing AD and AAD  
hybrid environments.**

# What is Purple Knight?




## AD security posture

- Free to use
- Safe to use (read only)
- Offline (no data sent outside)
- Easy to use (GUI and Report)
- Built and improved with community involvement

**PURPLE KNIGHT (Community edition)**

Agreement 1 — Environment 2 — Indicators 3 — Progress 4 — Summary 5

Select one or both options

☒  AZURE ACTIVE DIRECTORY


Fill in the details from the Azure application [Learn more](#)

Tenant ID


Application ID

Application Secret


TEST CONNECTION

☒  ACTIVE DIRECTORY

Select forest and domains to assess ⓘ



SELECT

Available: 0 Unreachable: 0 Selected: 0 |  AAD Disconnected

BACK NEXT

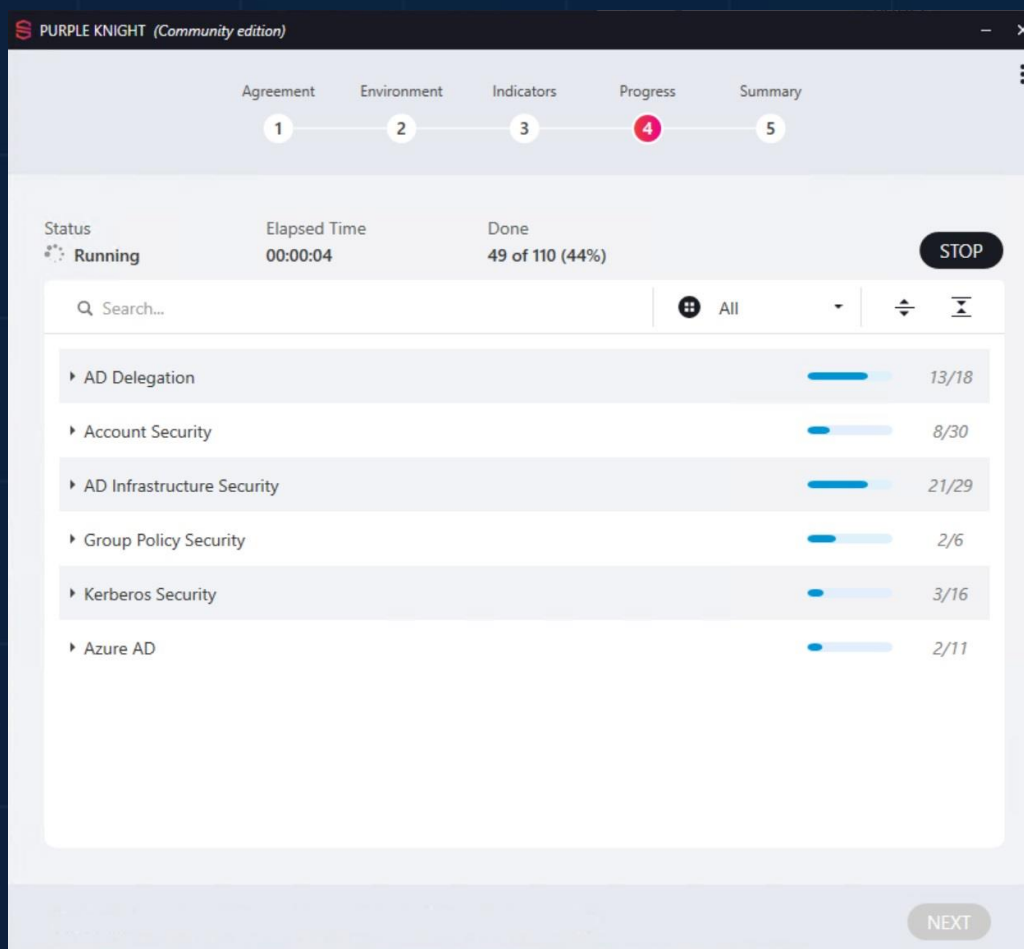


# How it work?



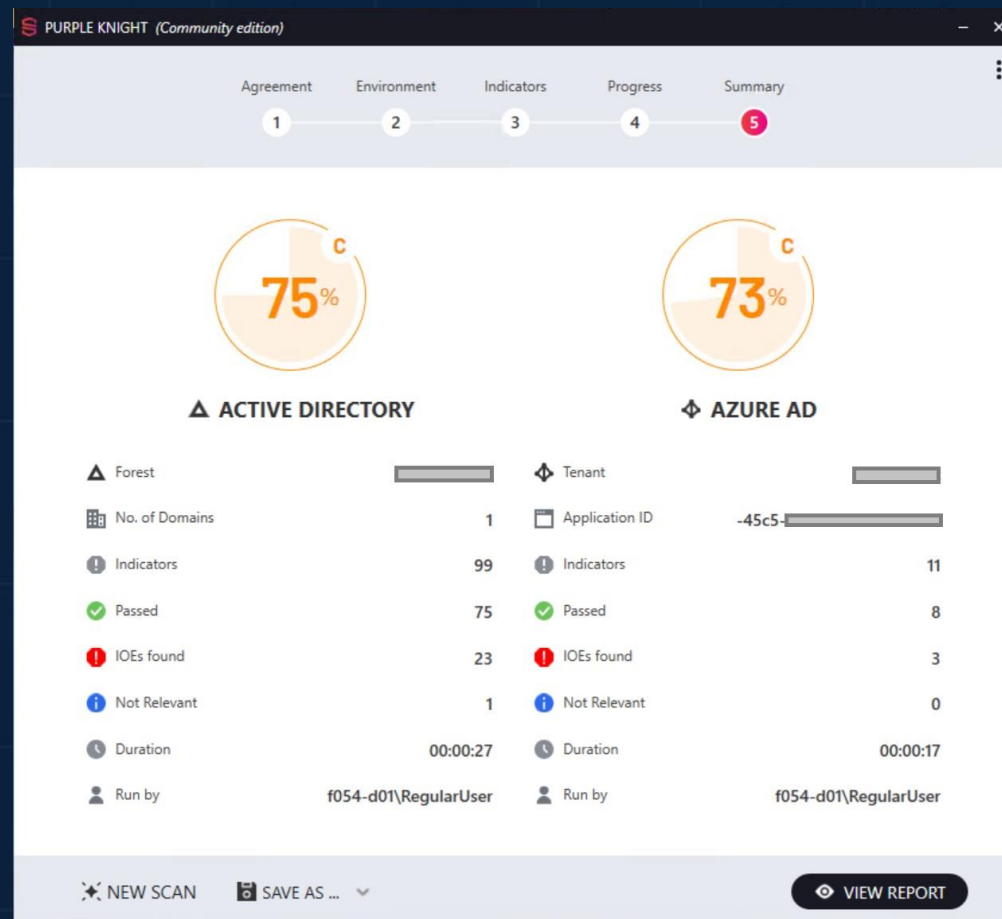
## IoE and IoC Scanner

- 120+ Indicators of Exposure and Compromise for AD and AAD
- Security posture scorecard reports (HTML and PDF)
- Portable (no installation)
- No admin right



# Requirements

- **Domain-joined PC**
  - Windows 8.1+, Server 2012R2+
- **Normal domain user (supports runas)**
  - Script execution policy – Remote Signed
- **Open ports to DC**
  - LDAP, SMB (389, 445)
  - Certain indicators may require additional ports (e.g. 443 for Web Enrollment Services scanning)
- **Internet connection required only for:**
  - Check for Updates
  - Azure connectivity



**Download at**  
<https://it.purple-knight.com>



**Slack:**  
[purpleknight.slack.com](https://purpleknight.slack.com)

**Email:**  
[pk-community@semperis.com](mailto:pk-community@semperis.com)



## Scoprite le vulnerabilità di Active Directory prima che lo facciano gli aggressori.

Con l'accesso ad Active Directory o Azure AD, gli attori delle minacce possono ottenere il dominio sull'intera infrastruttura. Liberatene con Purple Knight- uno strumento gratuito di valutazione della sicurezza di AD e Azure AD realizzato da esperti di sicurezza delle identità - per colmare le lacune di sicurezza che lasciano il vostro ambiente AD ibrido aperto ai cyberattaccanti.

Scaricalo ora

Versione: Purple Knight 2.1.1 Comunità

# DEMO

- Single forest, multi domain
- Azure AD synched with AD



# DEMO AD



## SECURITY INDICATOR Certificate templates that allow requesters to specify a subjectAltName

SEVERITY  
Critical

WEIGHT  
8

### Security Frameworks

- MITRE ATT&CK
- Credential Access
  - Privilege Escalation
- MITRE D3FEND
- Detect - Certificate Analysis

### Description

This indicator checks if certificate templates are enabling requesters to specify a subjectAltName in the CSR.

### Likelihood of Compromise

When certificate templates allow requesters to specify a subjectAltName in the CSR, the result is that they can request a certificate as anyone. For example, a domain admin. When that is combined with an authentication EKU present in the certificate template it can become extremely dangerous.

### Result

Found 1 certificate templates that allow the requester to specify a subjectAltName in the CSR

DistinguishedName	CertificateTemplateName	SANEnabled	CertificateCanBeUsedForAuthentication
CN=BadCert,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=mylab,DC=local	BadCert	Requester can specify a subjectAltName	True

Showing 1 of 1

### Remediation Steps

Ensure that when a SAN is allowed on a certificate template it is absolutely required on the template, so that the certificate must specify a subjectAltName. If not absolutely required, it should be disabled. This configuration can be viewed under the "Supply in request" option in the "Subject Name" tab in certtmpl.msc. When an authentication EKU is also present on the certificate template this becomes very dangerous and action should be taken to disable SAN on it.

MITRE D3fend based on the reference: [NIST-SP1800-16B](#)

# DEMO AD



## SECURITY INDICATOR Permission changes on AdminSDHolder object

SEVERITY  
Critical

WEIGHT  
10

### Security Frameworks

MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

ANSSI

- vuln1\_permissions\_adminsdholder
- vuln1\_privileged\_members\_perm

### Description

This indicator looks for Access Control List (ACL) changes on the AdminSDHolder object, which could indicate an attempt to modify permissions on privileged objects that are subject to AdminSDHolder (e.g. users or groups with adminCount=1).

### Likelihood of Compromise

Changes to the AdminSDHolder object are very rare. An admin should know that the change was made and be able to articulate the reason for the change. If the change was not intentional, the likelihood of compromise is very high.

### Result

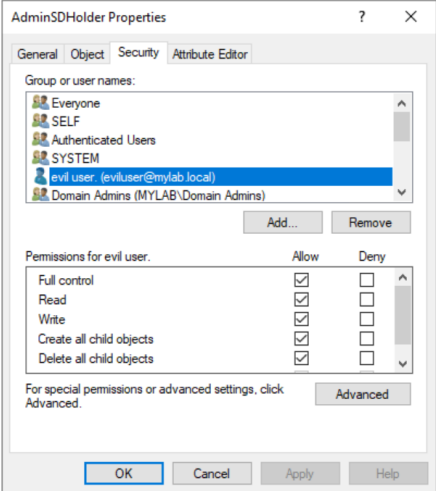
Found 3 domains with AdminSDHolder container permission changes in the last 6 months.

DistinguishedName	Attribute	EventTimestamp
CN=AdminSDHolder,CN=System,DC=lab1,DC=mylab,DC=local	nTSecurityDescriptor	8/30/2022 9:32:31 AM
CN=AdminSDHolder,CN=System,DC=lab2,DC=mylab,DC=local	nTSecurityDescriptor	10/25/2022 7:36:21 AM
CN=AdminSDHolder,CN=System,DC=mylab,DC=local	nTSecurityDescriptor	8/30/2022 9:22:03 AM

Showing 3 of 3

### Remediation Steps

Check the permissions on the AdminSDHolder container and search for abnormal ACE \ owner.



# DEMO AD



## SECURITY INDICATOR

### Accounts with Constrained Delegation configured to ghost SPN

#### SEVERITY

Warning



#### WEIGHT

6

#### Security Frameworks

##### MITRE ATT&CK

- Privilege Escalation

##### ANSSI

- vuln1\_delegation\_a2d2

#### Description

When computers are decommissioned, delegation configuration to them is often not cleaned up. Such a delegation could allow an attacker that has the privileges to write to the ServicePrincipalName attribute of another service account, to escalate privileges on those services. This could result in escalating privileges by moving laterally across the infrastructure. This indicator looks for accounts that have Constrained Delegation configured to ghost SPNs.

#### Likelihood of Compromise

This type of attack should be easy to spot as the configured SPN within the msds-allowedtodelegateto attribute will not exist on the domain. However, if they are found, they would represent a significant risk and should be mitigated quickly.

#### Result

Found 1 account(s) with Constrained Delegation configured to ghost SPN(s).

DistinguishedName	ServicePrincipalName	DomainName
CN=WEBSERVER,CN=Computers,DC=lab2,DC=mylab,DC=local	CIFS/OLDSERVER	lab2.mylab.local

Showing 1 of 1

#### Remediation Steps

Remove any Kerberos delegations to ghost SPN(s).

# DEMO AZUREAD



## SECURITY INDICATOR MFA not configured for privileged accounts

SEVERITY

Warning



WEIGHT

7

### Security Frameworks

MITRE ATT&CK

- Credential Access

### Description

This indicator checks that MFA (Multi-Factor Authentication) is enabled for users with administrative rights. Required permissions: RoleManagement.Read.Directory, Reports.Read.All

### Likelihood of Compromise

Accounts having privileged access are more valuable targets to attackers. A compromise of a privileged user represents a significant risk. As a result, these accounts require extra protections.

### Result

1 privileged user(s) found without MFA configured.

UserName	MFARegistered
AlexW@z8k3g.onmicrosoft.com	False

Showing 1 of 1

### Remediation Steps

It is recommended to configure MFA for privileged user(s).



# DEMO AZUERAD



SECURITY INDICATOR  
**Non-synced AAD user that is eligible for a privileged role**

SEVERITY                      WEIGHT  
Warning                      5

Security Frameworks

- MITRE ATT&CK
- Privilege Escalation

Description

This indicator checks for Azure AD users that are eligible for a high-privilege role and have the proxyAddress attribute, but are not synchronized with an AD account. For more information see the following [Semperis blog entry](#). Required permissions: User.Read.All, RoleManagement.Read.Directory, Directory.Read.All

Likelihood of Compromise

An attacker might use SMTP matching to synchronize controlled AD users with AAD users that are eligible for high-privilege roles. This process overwrites the AAD password and could result in privilege escalation over AAD.

Result

Found 2 eligible to hight privilege role users that are not sychronized with on-prem.

displayName	UPN	ProxyAddresses	Roles
Alex Wilber	AlexW@z8k3g.onmicrosoft.com	SMTP:AlexW@z8k3g.onmicrosoft.com	Global administrator
Adele Vance	AdeleV@z8k3g.onmicrosoft.com	SMTP:AdeleV@z8k3g.onmicrosoft.com	Global administrator

Showing 2 of 2

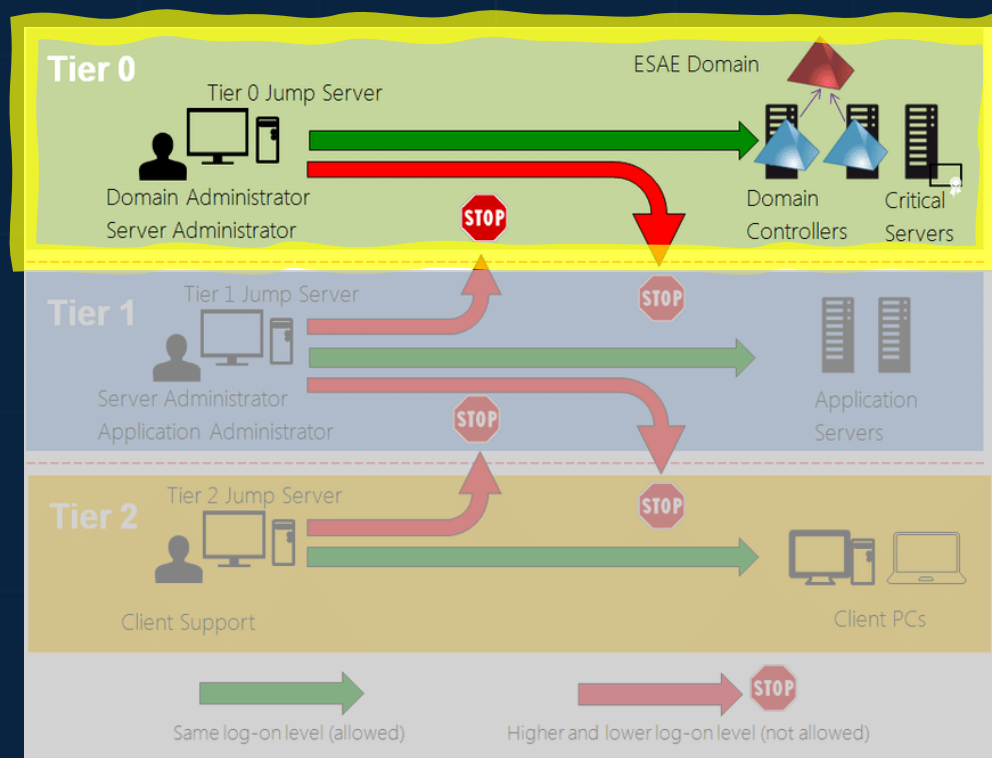


# Forest Druid

**Attack Path analysis  
“Inside-out” approach**

## THE QUESTION – WHO HAS ACCESS?

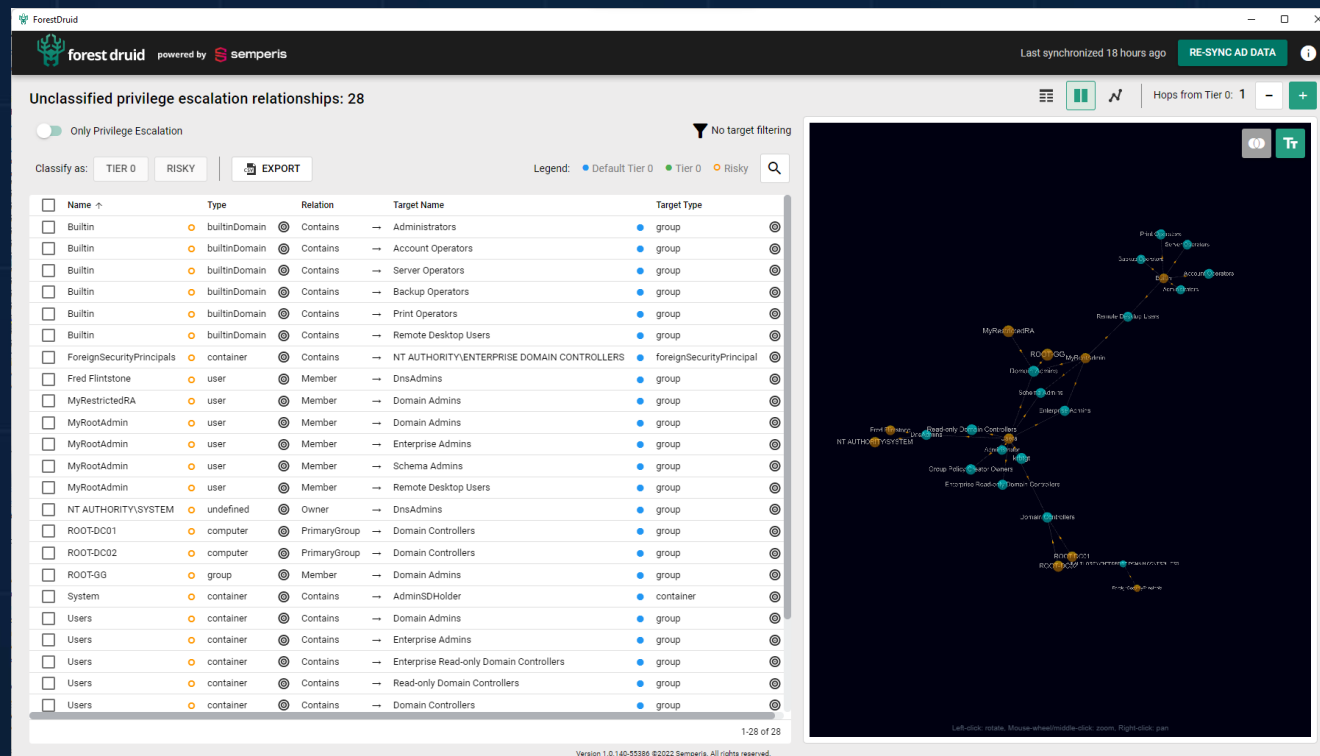
Permission models are very complex, and permission “creep” is endemic.  
**Identity Attack Paths** are chains of permissions that allow privilege escalation into an “Identity Perimeter”, e.g. AD Tier 0:



Source: Microsoft

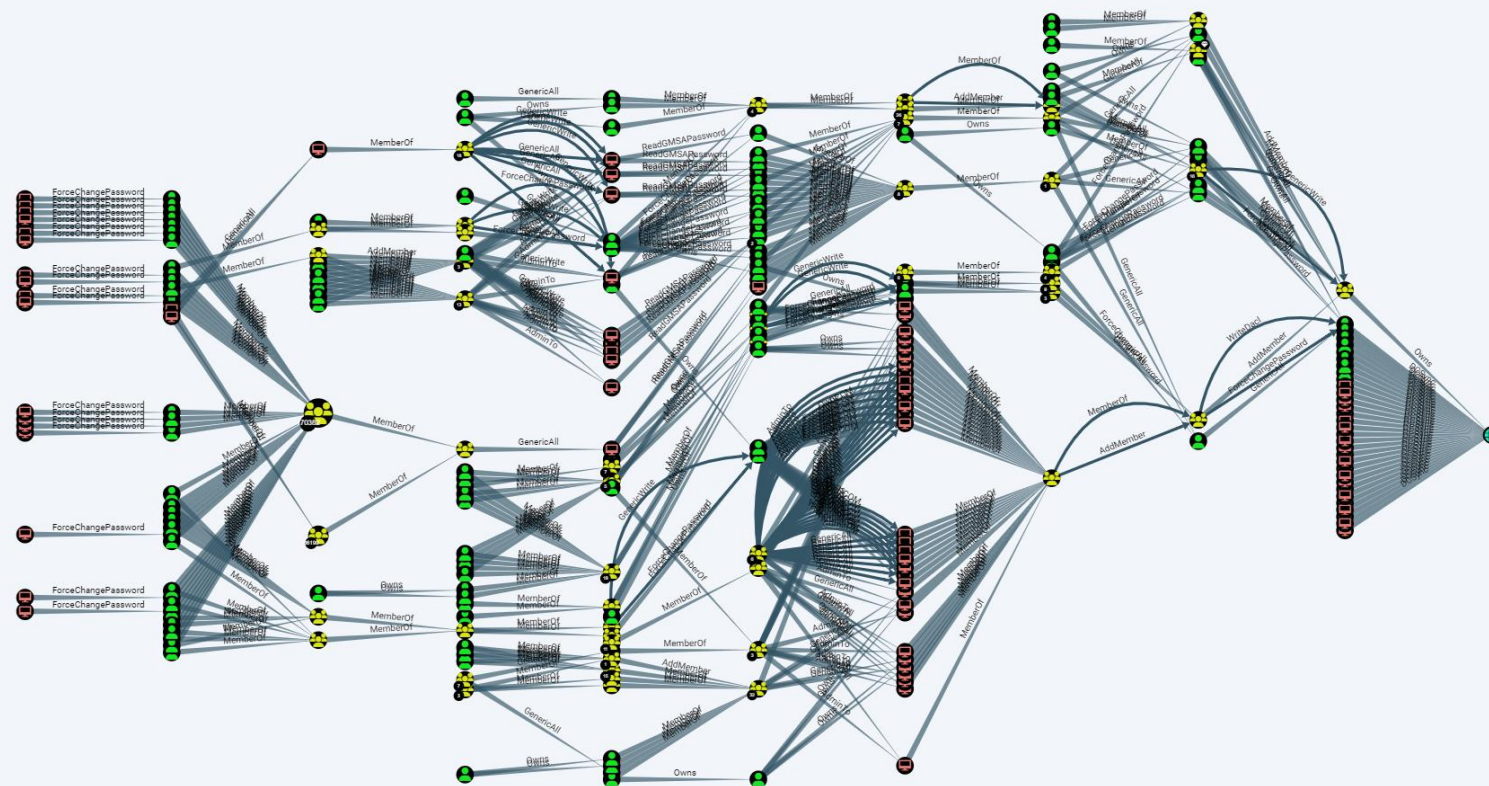
# What is Forest Druid ?

- Free attack path analysis tool  
Identifies risky access to Tier 0
- Designed for defenders  
Technical tool for AD practitioners
- Easy to setup and efficient to run
- Multi domain support



The screenshot displays the Forest Druid web interface, powered by semperis. The main view shows "Unclassified privilege escalation relationships: 28". A table lists various entities and their relationships, categorized by Tier 0 and Risky. A legend indicates the color coding for Default Tier 0 (blue), Tier 0 (green), and Risky (orange). On the right, a network graph visualizes these relationships, showing a complex web of connections between different system components.

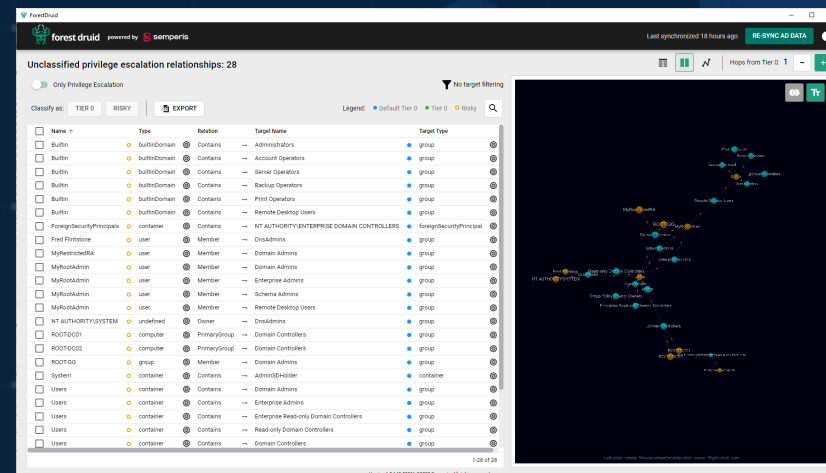
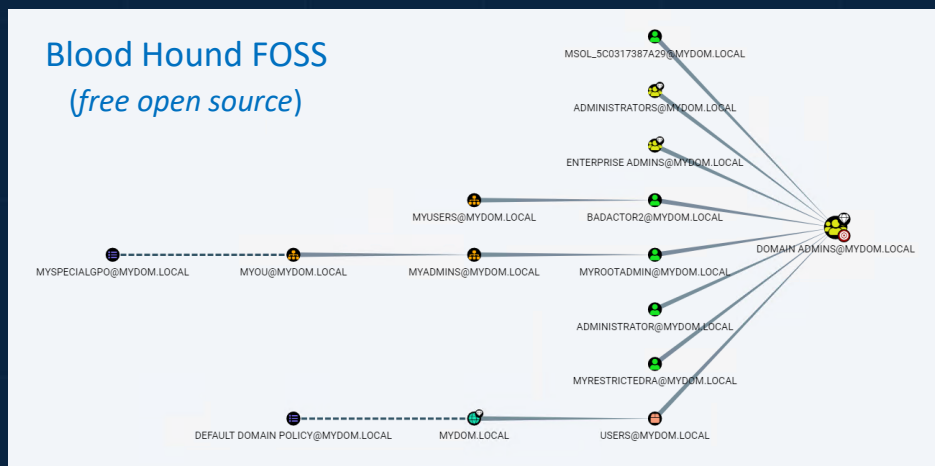
Name	Type	Relation	Target Name	Target Type
Builtin	builtinDomain	Contains	Administrators	group
Builtin	builtinDomain	Contains	Account Operators	group
Builtin	builtinDomain	Contains	Server Operators	group
Builtin	builtinDomain	Contains	Backup Operators	group
Builtin	builtinDomain	Contains	Print Operators	group
Builtin	builtinDomain	Contains	Remote Desktop Users	group
ForeignSecurityPrincipals	container	Contains	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	foreignSecurityPrincipal
Fred Flintstone	user	Member	DnsAdmins	group
MyRestrictedRA	user	Member	Domain Admins	group
MyRootAdmin	user	Member	Domain Admins	group
MyRootAdmin	user	Member	Enterprise Admins	group
MyRootAdmin	user	Member	Schema Admins	group
MyRootAdmin	user	Member	Remote Desktop Users	group
NT AUTHORITY\SYSTEM	undefined	Owner	DnsAdmins	group
ROOT-DC01	computer	PrimaryGroup	Domain Controllers	group
ROOT-DC02	computer	PrimaryGroup	Domain Controllers	group
ROOT-GG	group	Member	Domain Admins	group
System	container	Contains	AdminSDHolder	container
Users	container	Contains	Domain Admins	group
Users	container	Contains	Enterprise Admins	group
Users	container	Contains	Enterprise Read-only Domain Controllers	group
Users	container	Contains	Read-only Domain Controllers	group
Users	container	Contains	Domain Controllers	group



## BLOODHOUND vs. FOREST DRUID

# How does Forest Druid relate to the free version of BloodHound?

## Forest Druid and BloodHound are complementary



### Better for red-team

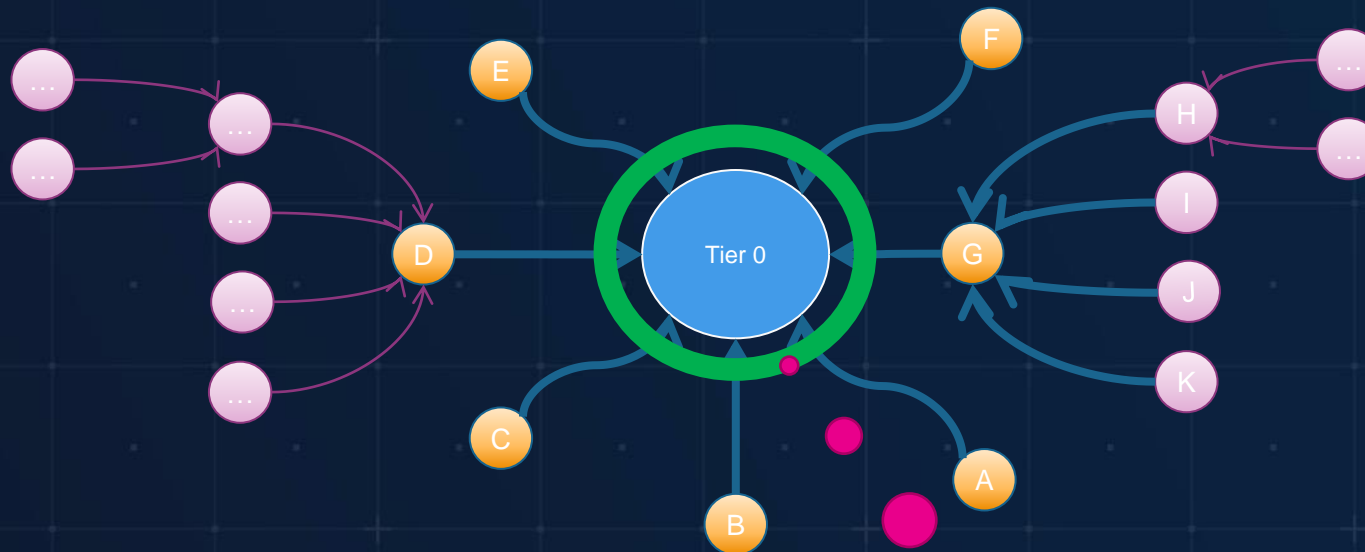
- Out-inside way
- Requires Neo4J DB
- Shows all possible and complete paths

### Better for blue-team

- Inside-out method
- Identity perimeters
- No installation, All in-one

# Forest Druid: how it works?

## The (Tier 0) Identity Perimeter



Here's some  
privileged access.  
Is it legitimate?

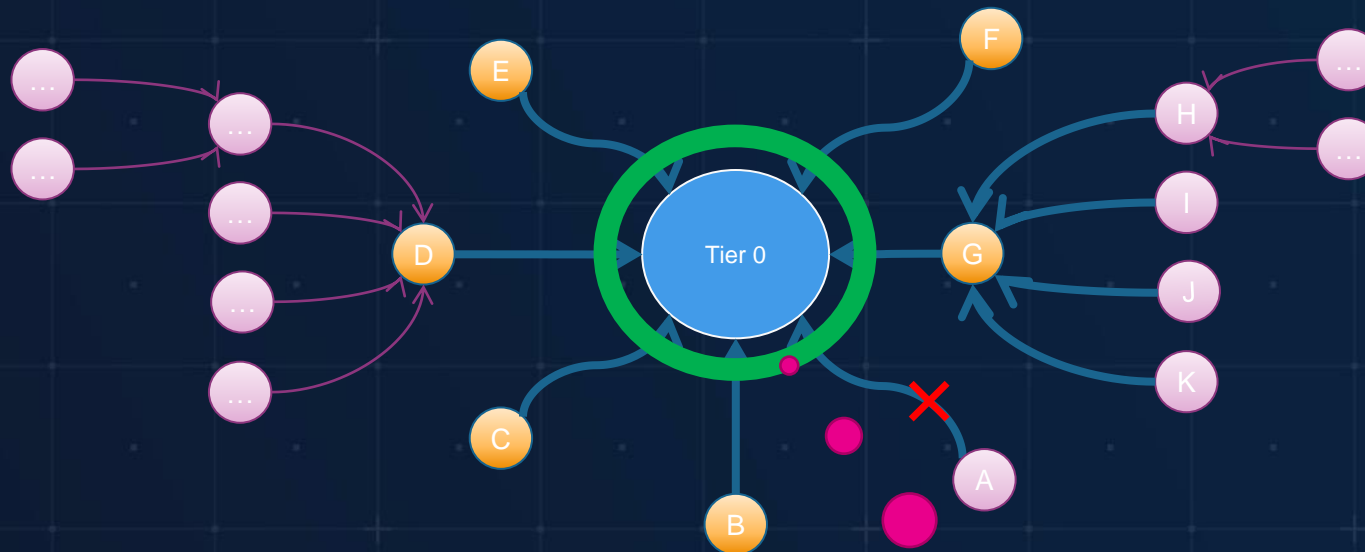
### RELATIONSHIPS COLLECTED:

- GenericAll
- GetChangesAll
- GpLink
- Member
- ReadLAPSPassword
- WriteSPN
- ...



# Forest Druid: how it works?

## The (Tier 0) Identity Perimeter



Here's some  
privileged access.  
Is it legitimate?

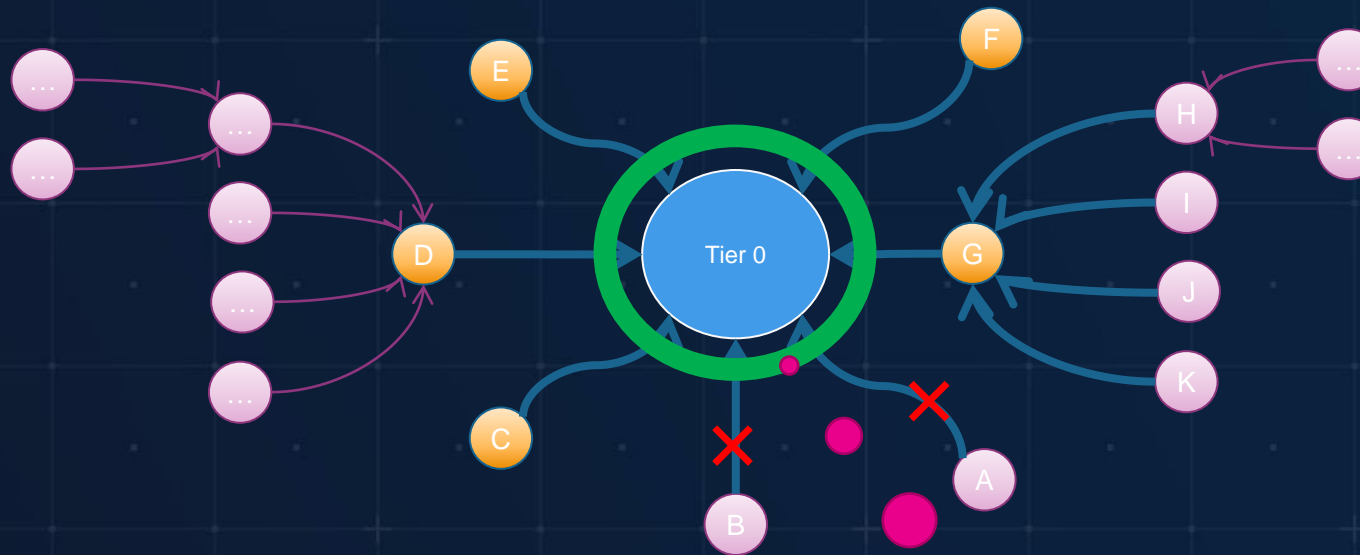
### RELATIONSHIPS COLLECTED:

- GenericAll
- GetChangesAll
- GpLink
- Member
- ReadLAPSPassword
- WriteSPN
- ...



# Forest Druid: how it works?

## The (Tier 0) Identity Perimeter



### RELATIONSHIPS COLLECTED:

- GenericAll
- GetChangesAll
- GpLink
- Member
- ReadLAPSPassword
- WriteSPN
- ...

Here's some  
privileged access.  
Is it legitimate?

# Forest Druid: how it works?

## The (Tier 0) Identity Perimeter



### RELATIONSHIPS COLLECTED:

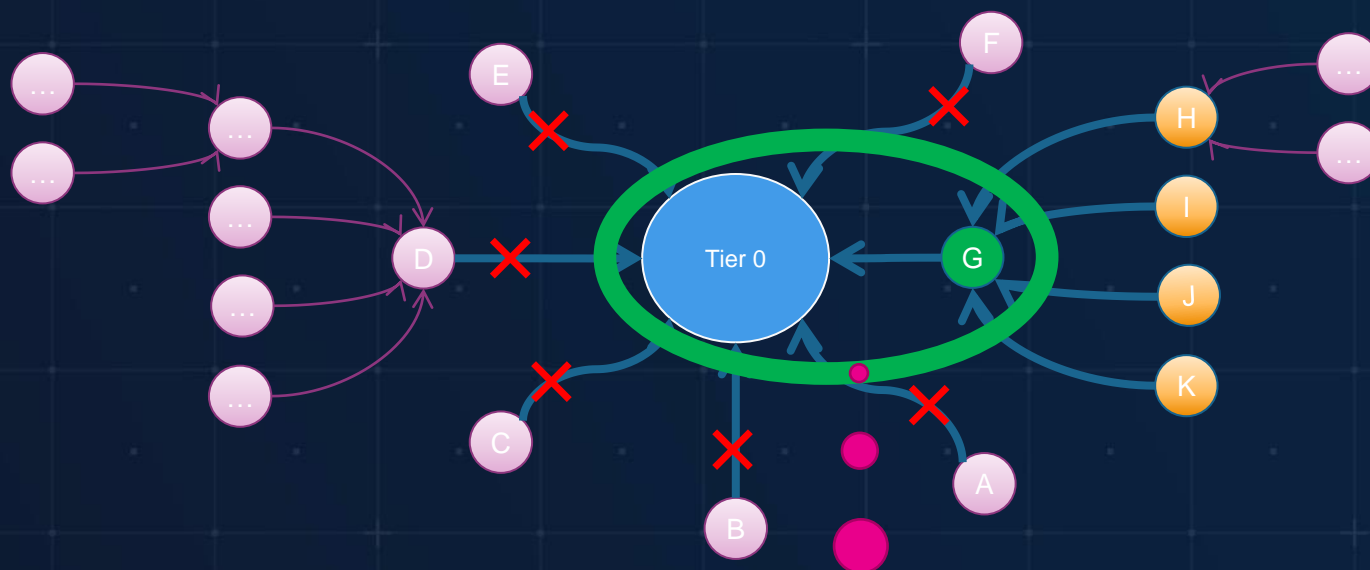
- GenericAll
- GetChangesAll
- GpLink
- Member
- ReadLAPSPassword
- WriteSPN
- ...

Here's some  
privileged access.  
Is it legitimate?



# Forest Druid: how it works?

## The (Tier 0) Identity Perimeter



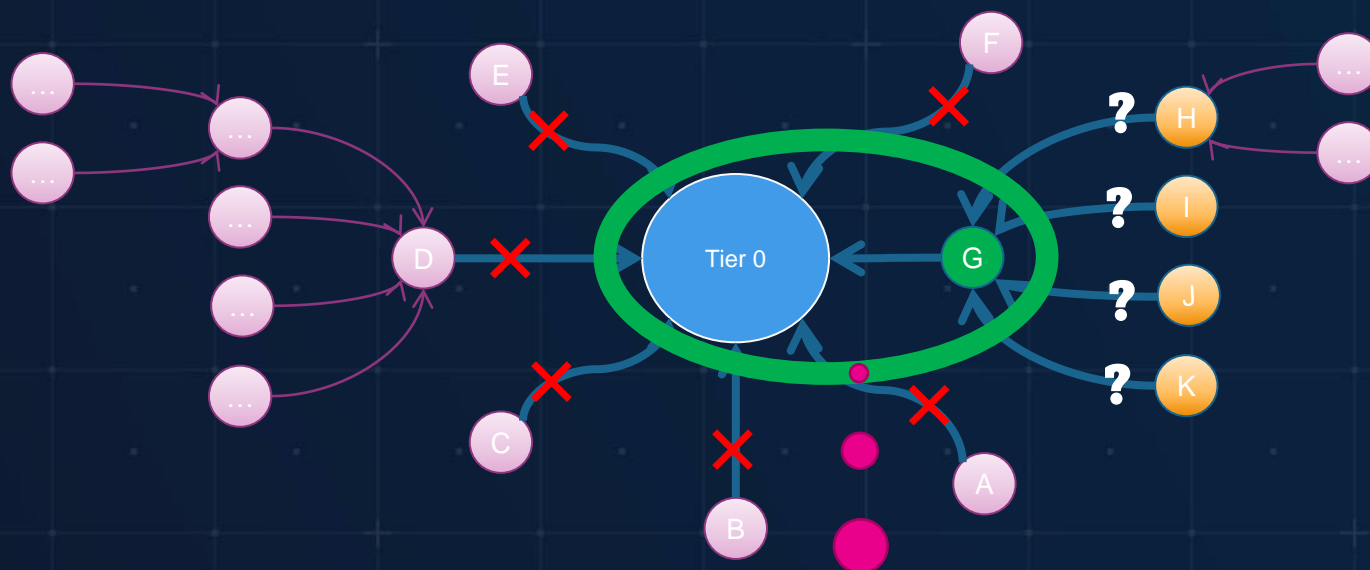
My actual Tier 0  
perimeter. I need to  
monitor and defend this  
(with DSP of course)

### RELATIONSHIPS COLLECTED:

- GenericAll
- GetChangesAll
- GpLink
- Member
- ReadLAPSPassword
- WriteSPN
- ...

# Forest Druid: how it works?

## The (Tier 0) Identity Perimeter



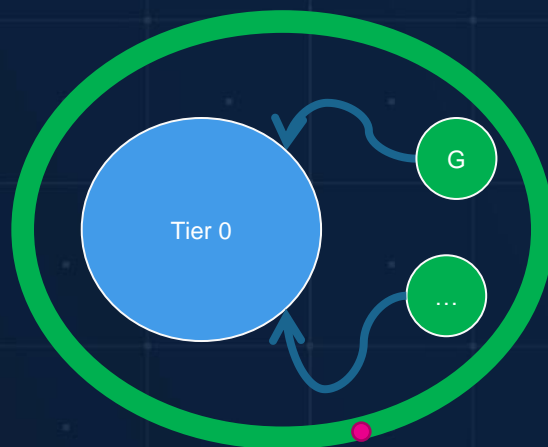
My actual Tier 0  
perimeter. I need to  
monitor and defend this  
(with DSP of course)

### RELATIONSHIPS COLLECTED:

- GenericAll
- GetChangesAll
- GpLink
- Member
- ReadLAPSPassword
- WriteSPN
- ...

# Forest Druid: how it works?

## The (Tier 0) Identity Perimeter



Desidered state.  
Tier 0 isolated



# DEMO



# FROM 7<sup>th</sup> DECEMBER 2022

**DATASHEET:** <https://www.semperis.com/wp-content/uploads/PDFs/datasheet-forest-druid.pdf>

**WEBSITE:** <https://www.purple-knight.com/forest%20druid/>



SCAN ME

 forest druid  
powered by semperis

## Introducing Forest Druid

### Stop chasing AD attack paths. Focus on your Tier 0 perimeter.

In a typical organization's Active Directory, there are literally millions of attack paths an adversary can take to arrive at domain dominance. The problem is clear—excessive privileges—but sifting through every group and user relationship is an impossible task. **Forest Druid flips the script**—taking an inside-out approach to attack path management. Forest Druid focuses on attack paths leading into the Tier 0 perimeter—saving time and resources by prioritizing your most critical assets.

- △ You can't manage millions of attack paths—focus on the Tier 0 perimeter
- △ Vulnerable Tier 0 assets often remain undiscovered until it's too late
- △ Unnecessary privileges create 99% of attack paths into Tier 0 assets
- △ Most common attack paths are not always the most dangerous ones

**Attack paths aren't created equal. Effective defense starts from inside the Tier 0 perimeter.**

  
Identify the true Tier 0 perimeter

  
Cut down excessive privileges

  
Prioritize attack paths by severity, not commonality

  
Monitor what matters—critical assets

  
Save time and resources

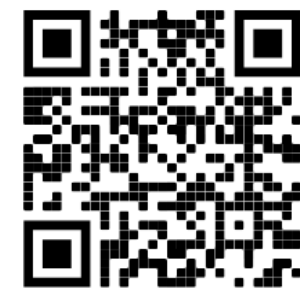
 forest druid  
powered by semperis

## Stop chasing AD attack paths. Focus on your Tier 0 perimeter.

Active Directory has countless paths adversaries can take to achieve domain dominance. The problem is clear—excessive permissions—but sifting through every group and user relationship is impossible. Forest Druid flips the script, taking an inside-out approach to attack path management. Forest Druid focuses on attack paths leading into the Tier 0 perimeter—saving time by prioritizing your most critical assets.

[Request early access](#)

Define what matters—Tier 0 assets.



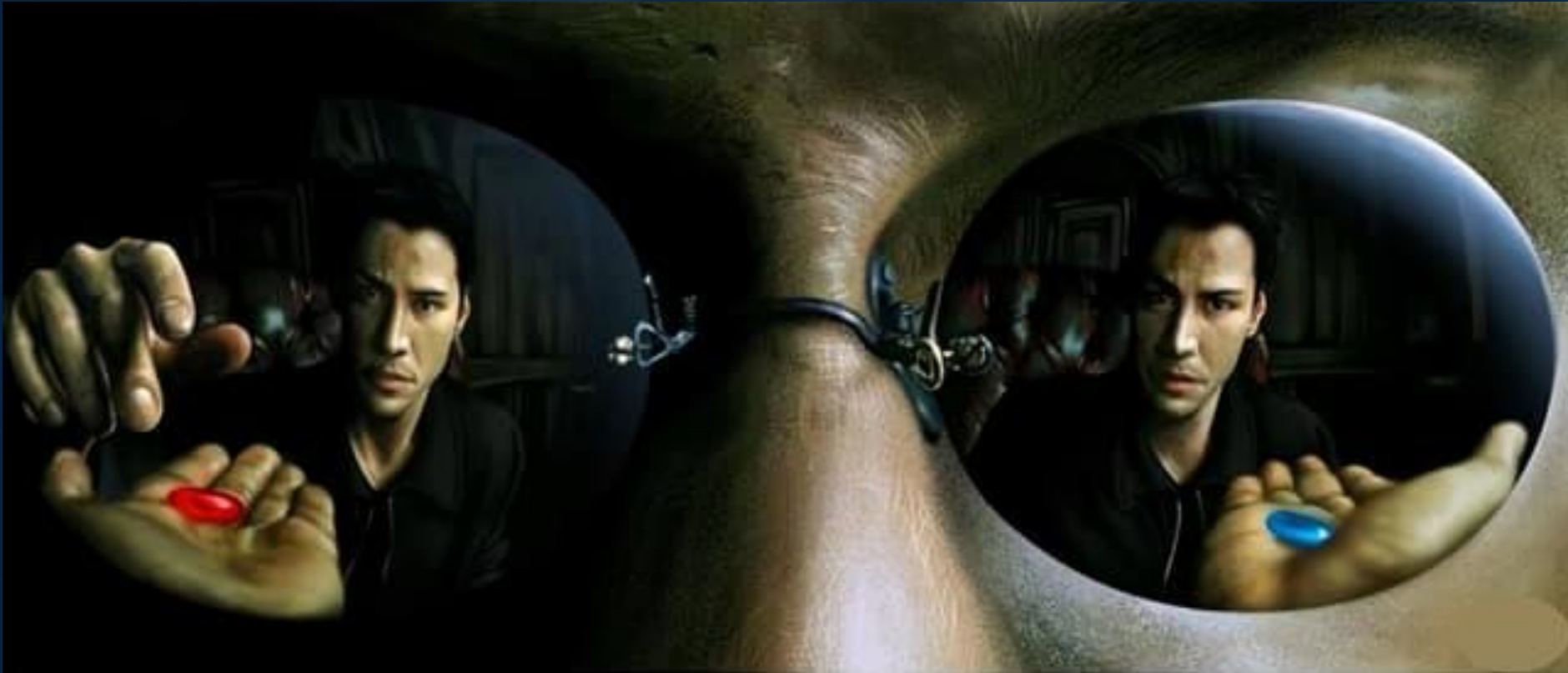
SCAN ME

# Quick take-away

- Continuous assessment on AD & AAD is mandatory!
- Monitor and review your changes
- “Hide” your tier-0 assets making the life for attackers harder ;-)



# FIND THE TRUE



ANY QUESTIONS?

# We hope you enjoyed our talk... did you?

Marco  
Magnaguagno



@ll\_MMagna



marcom@semepris.com



Andrea  
Pierini



@decoder\_it



andreap@semepris.com

Thank you and feel free to reach out! :)