
PSCONF.EU

PSCONF.EU

2018

Invoke-CypherDog

BloodHound Dog Whispering with PowerShell

Walter Legoswki aka @SadProcessor

Agenda

I - What is BloodHound
II - What is Cypher
III - What is CypherDog
IV - What is Next…

PSCONF.EU

Whois/Disclaimer

n00b

Whois/Disclaimer

n00b

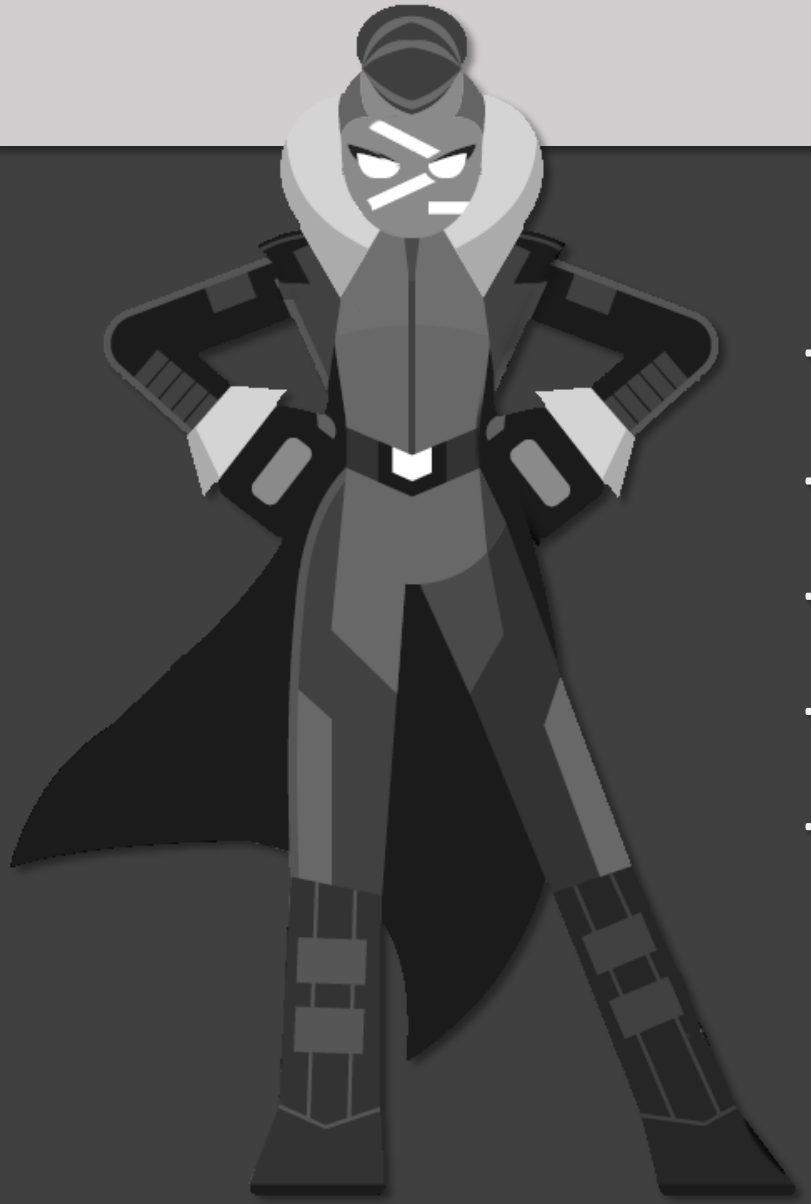
PSCONF.EU

Whois/Disclaimer

n00b

PSCONF.EU

Goal

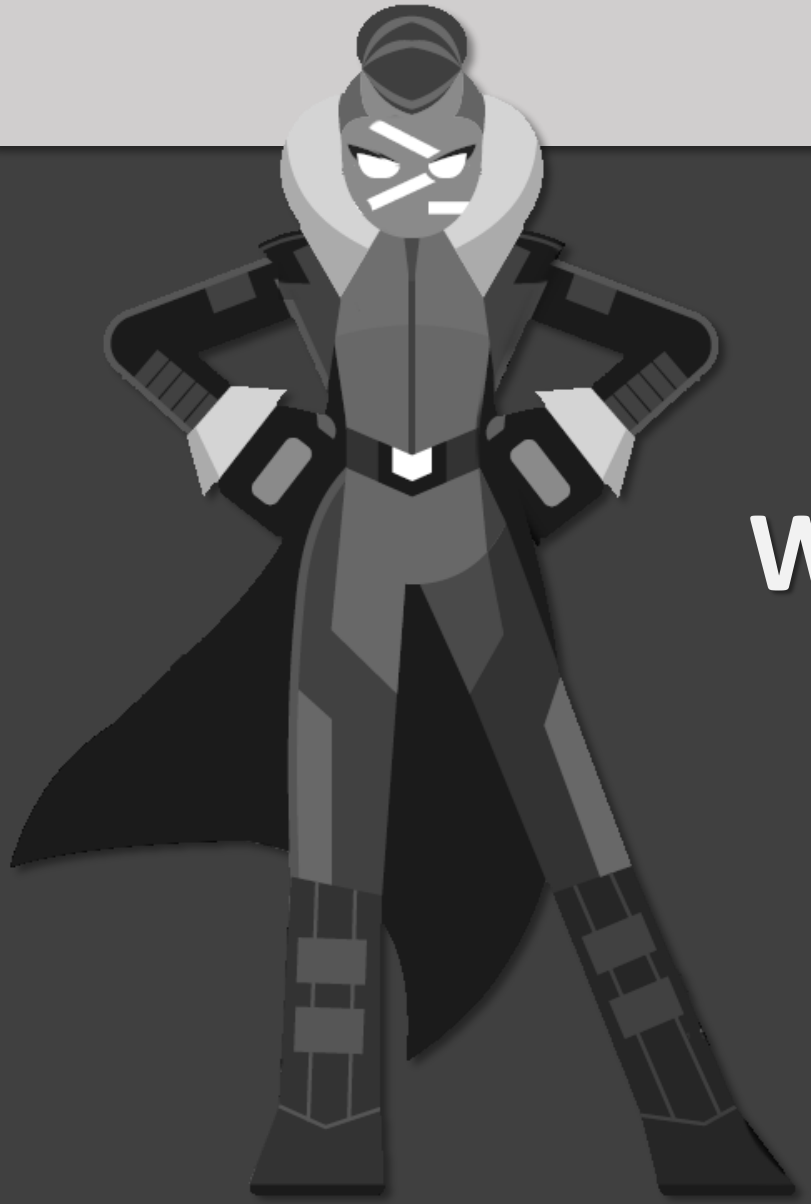


- Share **Passion**
- Share **Ideas**
- Share **Tools**
- Share **Joys & Pains**
- Share **Tips & Tricks**

(take home what you like…)

PSCONF.EU

Part I



What is BloodHound ?

PSCONF.EU

Famous Quote – @JohnLaTwC

"Defenders think in Lists, Attackers think in Graphs..."

John Lambert
MS Threat Intel

BloodHound – Definition

Active Directory
Object Relationship
Graphing Tool

PSCONF.EU

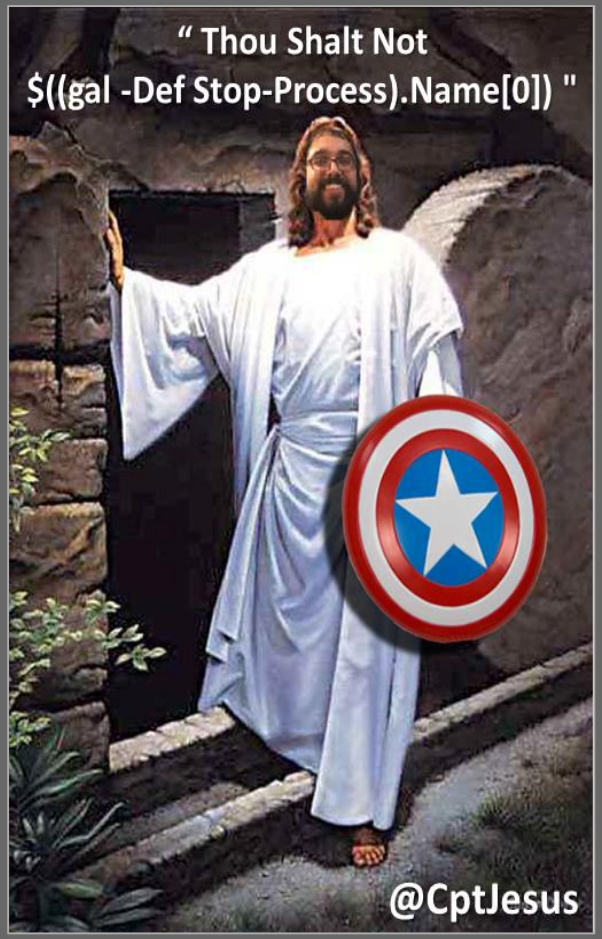
BloodHound – Definition

RED & BLUE

Active Directory Object Relationship Graphing Tool

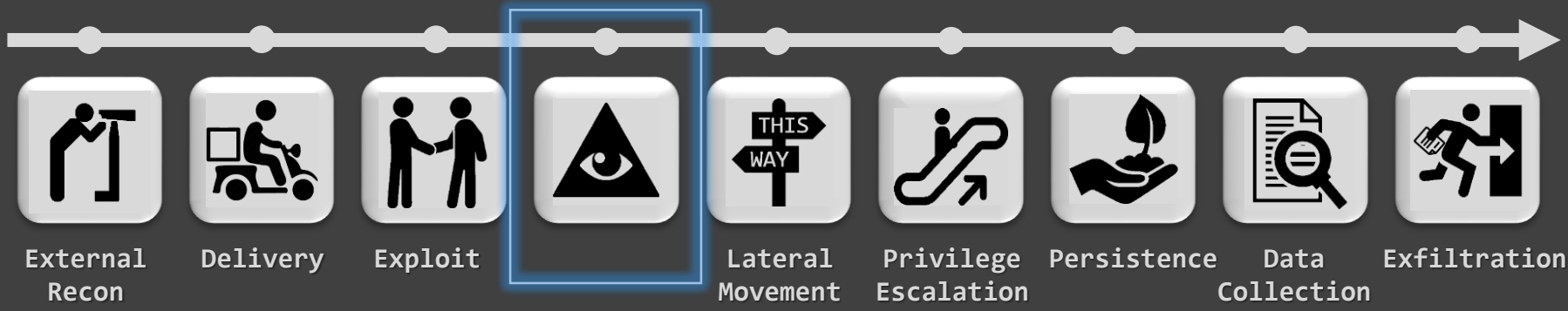
PSCONF.EU

BloodHound – Credits



@_Wald0

BloodHound – Kill Chain



Situational Awareness

PSCONF.EU

BloodHound – Components

- **SharpHound** = Data Collector (C#)
- **Neo4j Database** << AD Data
- **JS / Electron** >> Web UI
- Cypher = Neo4j DB Query

WIN/TUX/OSX

PSCONF.EU

BloodHound – Terminology

Node: Active Directory Object

NEW 1.5
GPO & OU !!

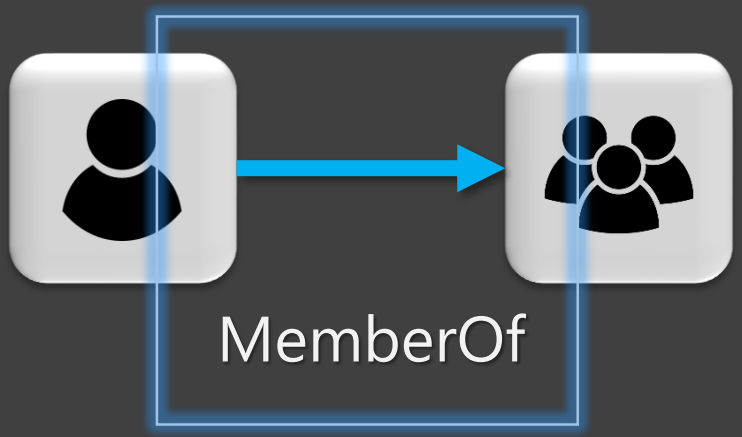
PSCONF.EU

BloodHound – Terminology

Edge: Relationship between 2 Nodes

 # Basics: (v1.0)
MemberOf
AdminTo
HasSession
TrustedBy

 # ACL: (v1.3)
ForceChangePassword
AddMembers
GenericAll
GenericWrite
WriteOwner
WriteDACL
AllExtendedRights

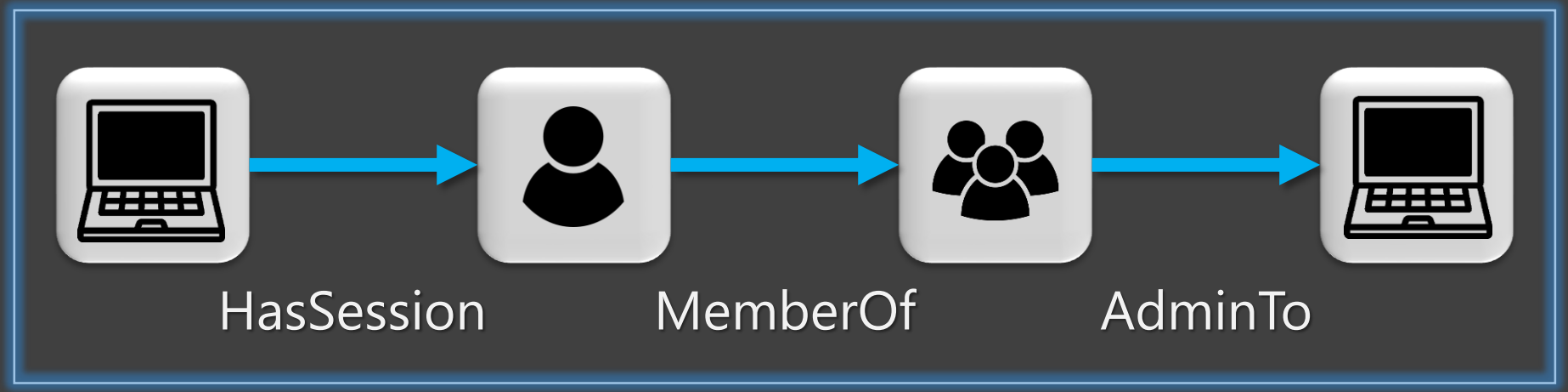


 # GP: NEW 1.5 GPO & OU !!
GpLink
Contains
Owns

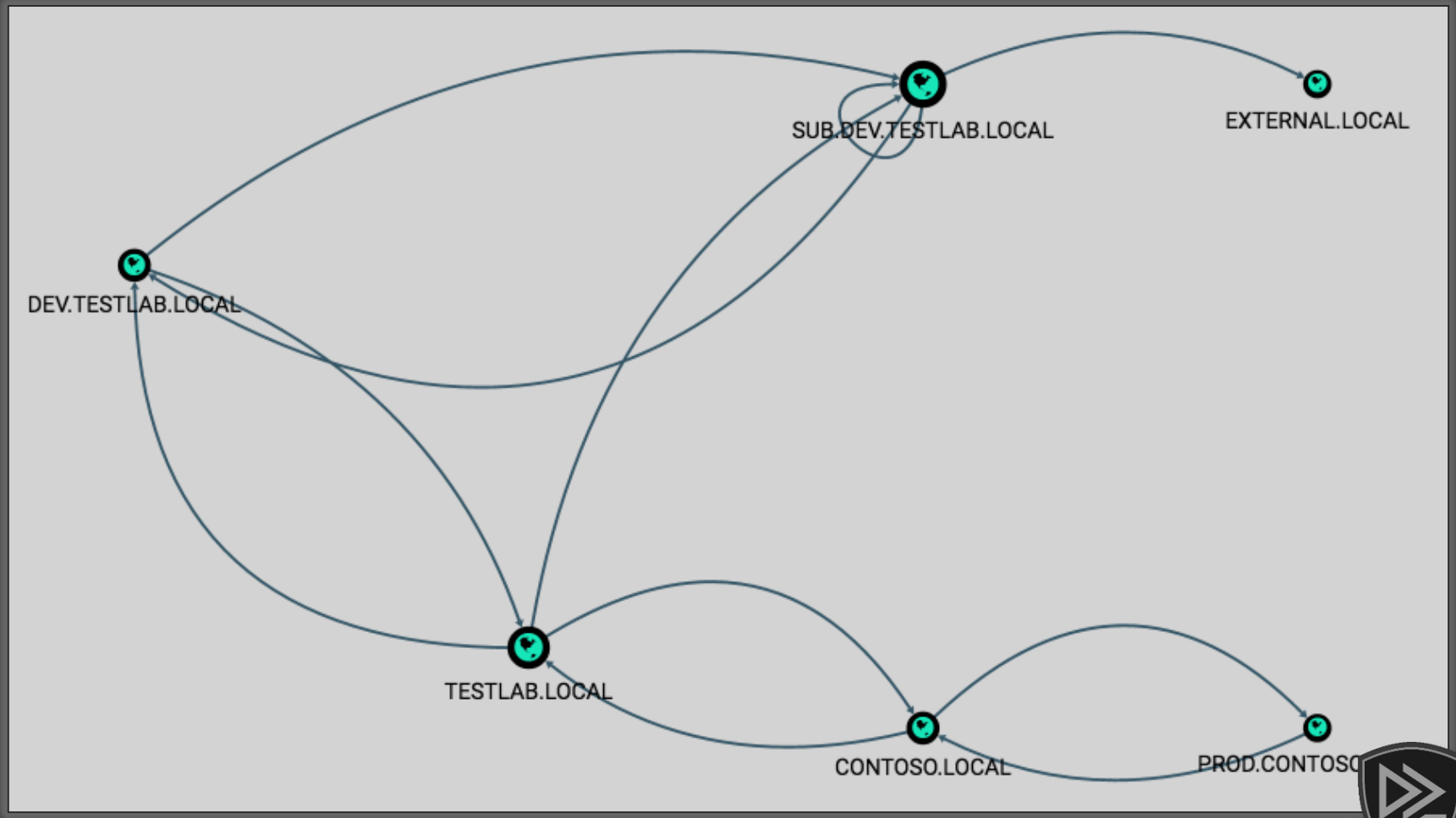
PSCONF.EU

BloodHound – Terminology

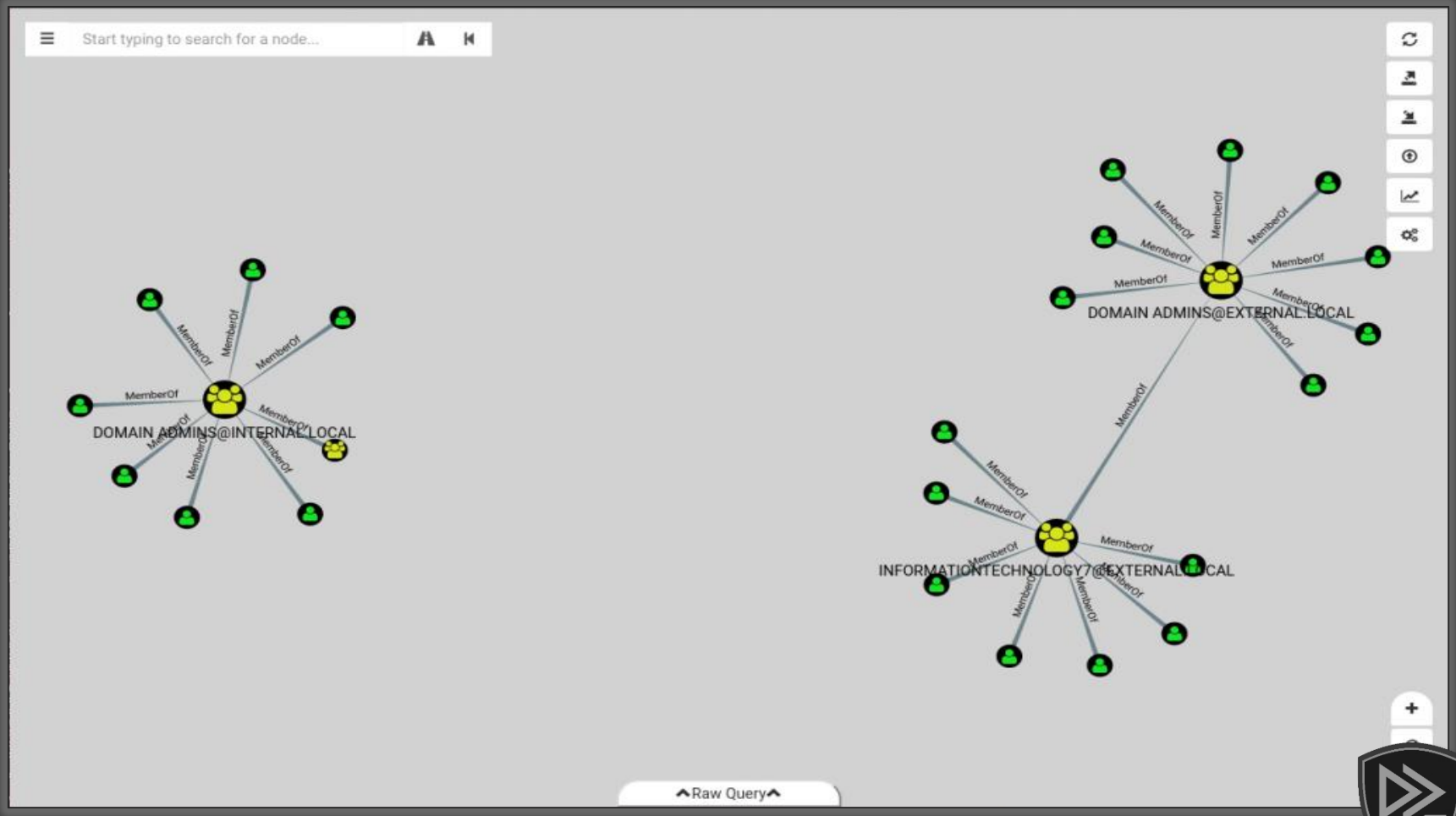
Path: Chain of connected Nodes



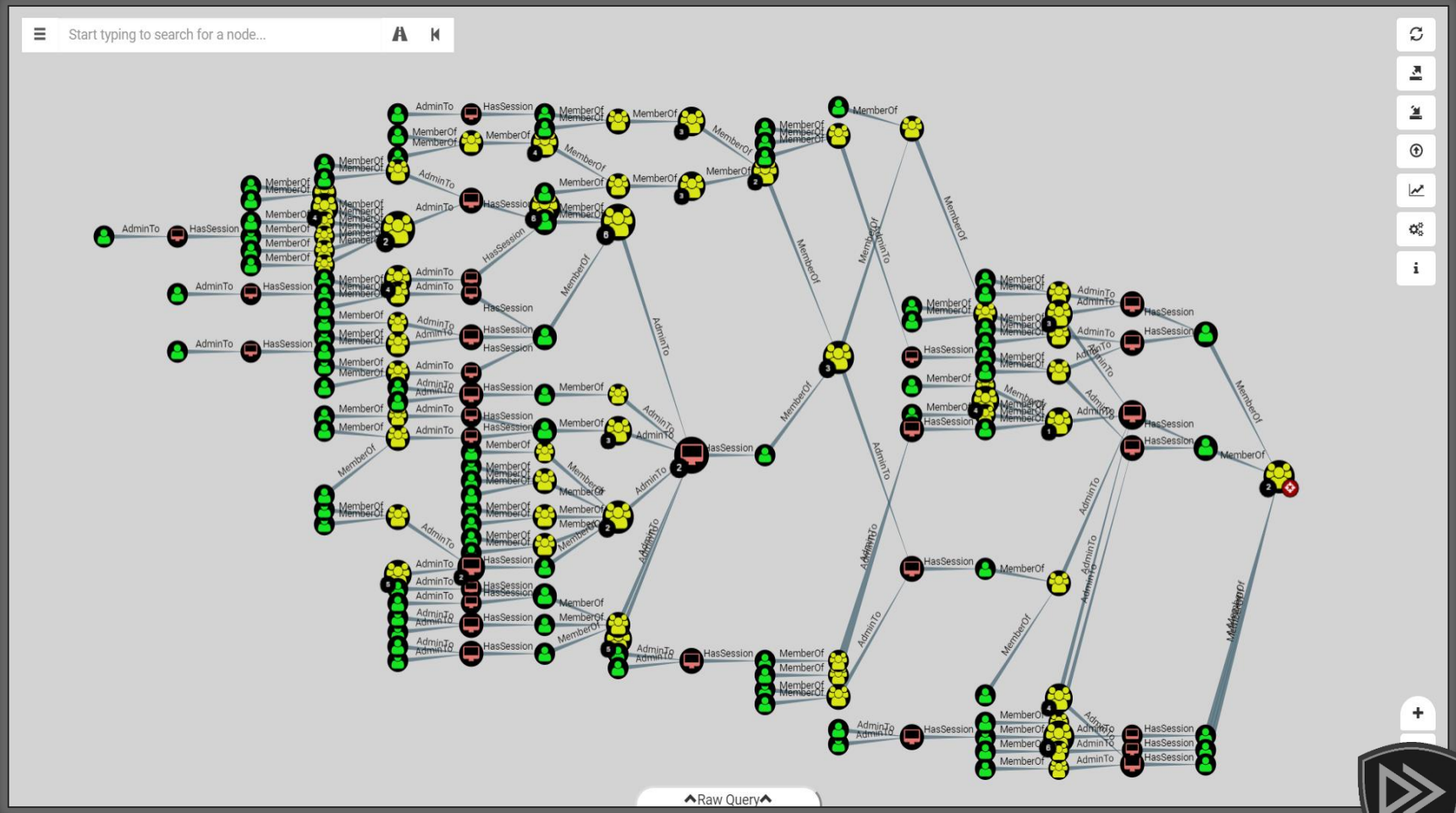
BloodHound – Look & Feel



BloodHound – Look & Feel



BloodHound – Look & Feel



SadJoey – meme

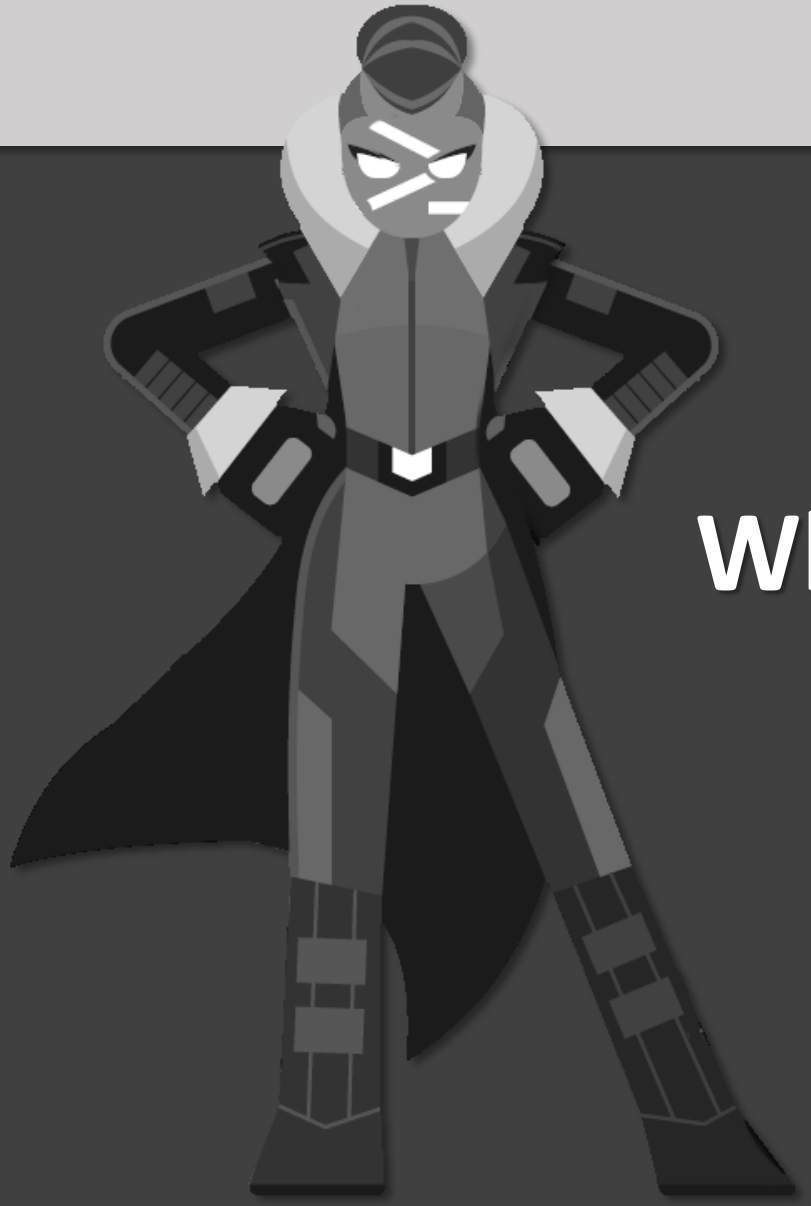
BloodHound

Demo

PSCONF.EU

DEMO – BLOODHOUND UI

Part II



What is Cypher ?

PSCONF.EU

Cypher – Definition

Neo4j Database
Query Language

Cypher – Basics

(Node)-[Edge]->(Node)

/!\ Not Real Code...

Cypher – Basics

(Node)-[Edge]->(Node)

Source

/!\ Not Real Code...

Cypher – Basics

(Node)-[Edge]->(Node)

Relationship

/!\ Not Real Code...

Cypher – Basics

(Node)-[Edge]->(Node)

Target

/!\ Not Real Code...

Cypher – Basics

(Bob)-[Knows]->(Alice)

Data

/!\ Not Real Code...

Cypher – Basics

(X)-[Knows]->(Alice)

Who knows Alice?

/!\ Not Real Code...

Cypher – Basics

(Bob)-[Knows]->(X)

Who does Bob Know?

/!\ Not Real Code...

Cypher – Basics

(Bob)-[X]->(Alice)

What Edge from Bob to Alice?

/!\ Not Real Code...

Cypher – Basics

(Bob)-[Knows]->(Alice)
(Alice)-[Knows]->(John)

Data

/!\ Not Real Code...

Cypher – Basics

Path((Bob)-[X]->(John))

Path from Bob to John?

/!\ Not Real Code...

Cypher – Basics

(Bob)-[Knows]->(Alice)-[Knows]->(John)

Resulting Path

/!\ Not Real Code...

Cypher – Real Example - Path

```
MATCH
(A:User {name: 'ACHAVARIN@EXTERNAL.LOCAL'}),
(B:Group {name: 'DOMAIN ADMINS@INTERNAL.LOCAL'}),
P=shortestPath((A)-[*1..]->(B))
RETURN P
```

"Shortest Path with any edges from specified User to DA Group"

Cypher – Real Example - Metrics

```
MATCH
(U:User)-[r:MemberOf|:AdminTo*1..]->(C:Computer)
WITH
U.name as n,
COUNT(DISTINCT(C)) as c
RETURN {Name: n, Count: c} as SingleObj
ORDER BY c DESC
LIMIT 5
```

"Top 5 users with most Unrolled AdminTo on Computers"

Cypher – Real Example - Metrics

```
MATCH
(U:User)<-[r:HasSession*1..]-(C:Computer)
WITH
U.name as n,
COUNT(DISTINCT(C)) as c
RETURN {Name: n, Count: c} as SingleObj
ORDER BY c DESC
LIMIT 10
```

"Top 10 Users with most HasSession from Computers"

Questions?

?

PSCONF.EU

OK, cool...

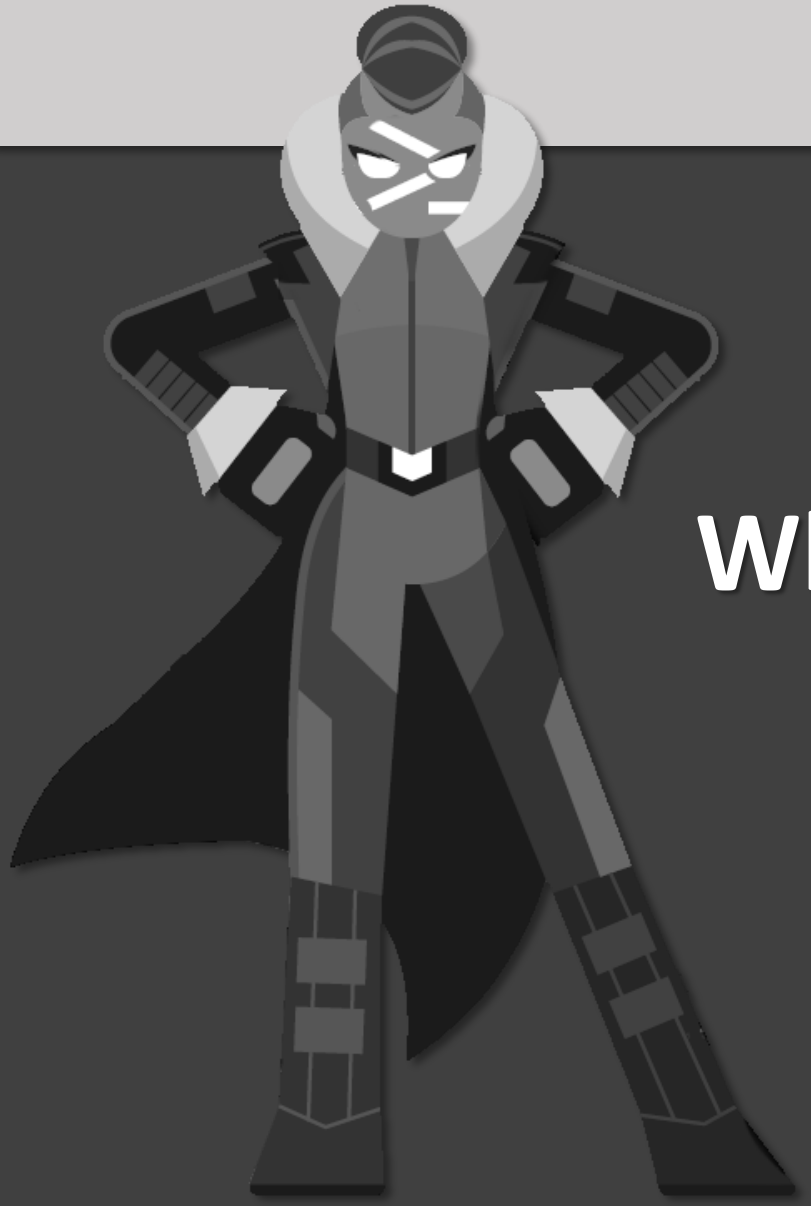
... but what about PowerShell ?!?

Cypher – Query via API

Demo

DEMO – CYPHERISER

Part III



What is CypherDog ?

PSCONF.EU

CypherDog – Definition

A set of Cmdlets to interact with BloodHound DB via REST API

CypherDog – Cmdlets

```
PS @:\> BloodHound-Help

Cmdlet                 Synopsis                                  Help
------                 --------                                  ----
BloodHound-Node        Get Node by Name                          Help Node
BloodHound-NodeSearch  Search Node by Key|Prop|PropValue         Help NodeSearch
BloodHound-NodeCreate  Add Node to DB                            Help NodeCreate
BloodHound-NodeUpdate  Add/Update Node Properties                Help NodeUpdate
BloodHound-NodeDelete  Remove Node from DB                       Help NodeDelete
BloodHound-Edge        Get Node by Edge                          Help Edge
BloodHound-EdgeReverse Get Node by Reverse Edge                  Help EdgeReverse
BloodHound-EdgeCustom  Get Node by Custom Edge                   Help EdgeCustom
BloodHound-EdgeCreate  Create Edge between Nodes                 Help EdgeCreate
BloodHound-EdgeDelete  Remove Edge between Nodes                 Help EdgeDelete
BloodHound-Path        Shortest Path - Node to Node              Help Path
BloodHound-PathVia     Shortest Path - Node to Node via Node     Help PathVia
BloodHound-PathCypher  Generate Cypher | WaldOIndex              Help Cypher
```

CypherDog – Cmdlets

```
PS @:\> BloodHound-Help

Cmdlet                Synopsis
------                --------
          Node        Get Node by Name
          NodeSearch  Search Node by Key|Prop|PropValue
          NodeCreate  Add Node to DB
          NodeUpdate  Add/Update Node Properties
          NodeDelete  Remove Node from DB
          Edge        Get Node by Edge
          EdgeReverse Get Node by Reverse Edge
          EdgeCustom  Get Node by Custom Edge
          EdgeCreate  Create Edge between Nodes
          EdgeDelete  Remove Edge between Nodes
          Path        Shortest Path - Node to Node
          PathVia     Shortest Path - Node to Node via Node
          PathCypher  Generate Cypher | WaldOIndex
```

CypherDog – Cmdlets

CypherDog – Features

- Short Syntax
- Tab-Completion
- Dynamic Params
- Pipeline Input
- Return Objects

Think
Ty<TAB>
Get

Demo

DEMO – CYPHERDOG

Questions?

What next?

PSCONF.EU

What next...

THIS POWERSHELL ADVENTURE JUST BEGINS MORTY,
AND THERE IS NO ENDING...

What next…

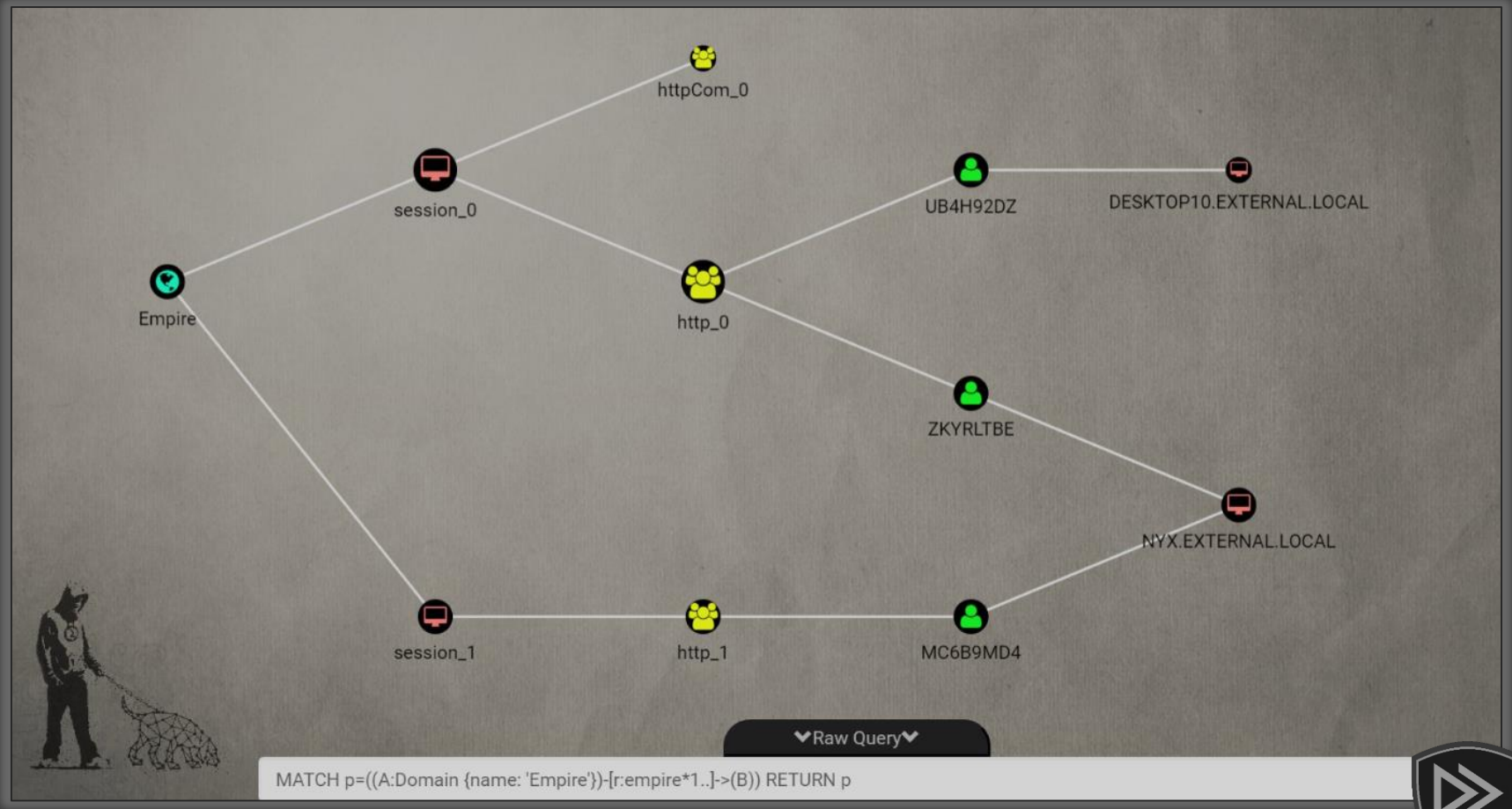
You:

- Download **BloodHound** and play with it
- Use **PowerShell** to query BloodHound via **API**
- Find relevant **metrics** & use PoSh to pimp output
- **Simulate** changes to AD in Graph
- **Apply** Changes with some PowerShell ???

Me:

- **Update Module** for BloodHound 1.5
- Merge **Empire & BloodHound** (+ATT&CK)

What next...


httpCom_0
session_0
UB4H92DZ
DESKTOP10.EXTERNAL.LOCAL
Empire
http_0
ZKYRLTBE
NYX.EXTERNAL.LOCAL
session_1
http_1
MC6B9MD4
Raw Query
MATCH p=((A:Domain {name: 'Empire'})-[r:empire*1..]->(B)) RETURN p

What next…

Each BloodHound Edge has matching Modules in Empire that could be used to automate that move… just sayin'…

What next...

To Be Continued...

BloodHound– Google it…

- **Attackers Think in Graphs…** - J. Lambert
- **Active Directory Control Paths** - Gras & Bouillot
- **Automated Derivative Admin Search** - @_Wald0
- **Introducing BloodHound** - @_Wald0
- **Intro to Cypher** - @CptJesus
- **The ACL Attack Path Update** (1.3) - @_Wald0
- **Evolution of the BloodHound Ingestor** - @CptJesus
- **The Object Properties Update** (1.4) - @CptJesus
- **SharpHound: Technical Details** - @CptJesus
- **The Container Update** (1.5) - @CptJesus
- **A Red Teamer's Guide to GPOs & OUs** - @_Wald0
- Anything by **@harmj0y** (Powerview & Co)
- Anything by **@PyroTek3** (ADSecurity.org)

More Info – Google it…

VIDEOS

- **Six Degrees of Domain Admin** - BSides LasVegas 2016
- **Here be Dragons…** - DerbyCon 2017
- **An ACE up the sleeve…** - WeAreTroopers 2018
- **+ SpecterOps** YouTube channel

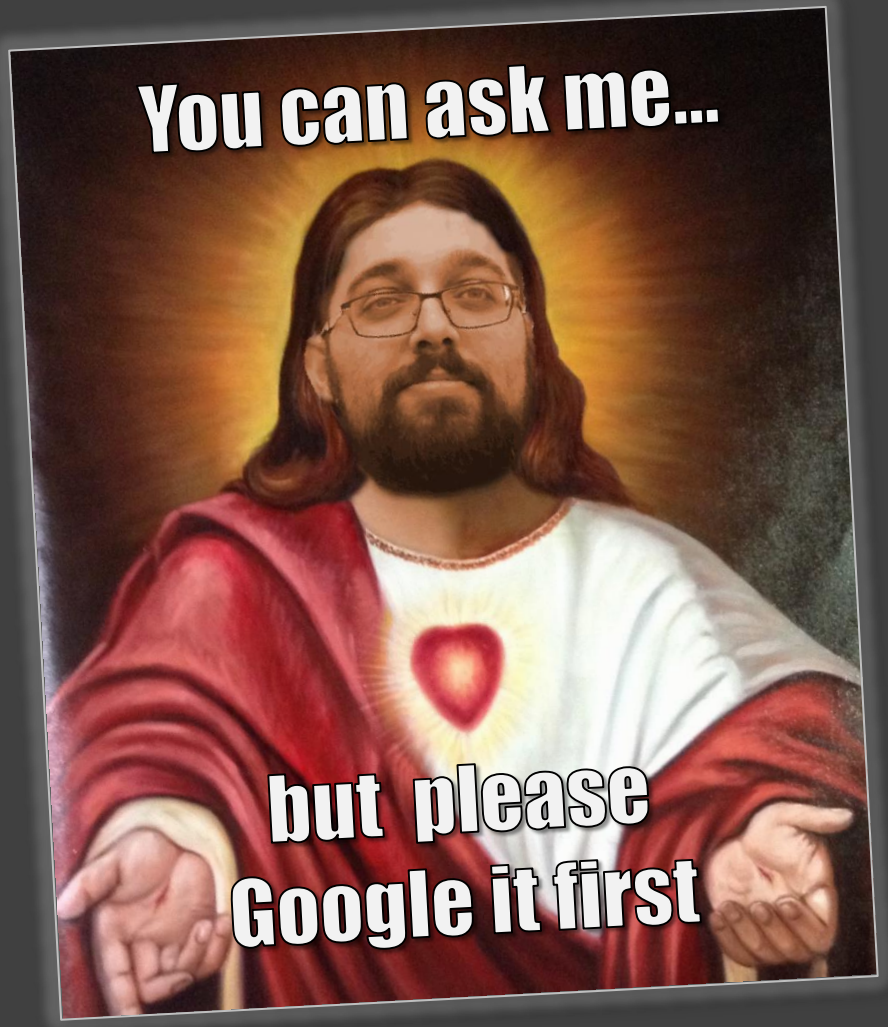
Wald0Index

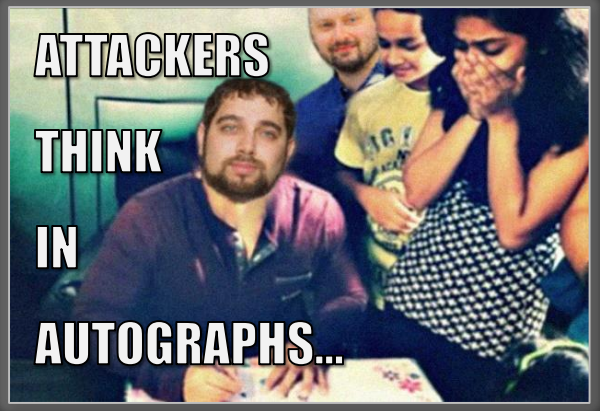
- **How to Build Adversary Resilience into your AD Environment** - Video
- **Introducing the adversary resilience methodology** - pt1/pt2 - Posts

NEO4J - CYPHER

- Neo4j Cypher Cheat Sheet
- Neo4j Dev Docs

BloodHound – Fan Club (Slack)





PSCONF.EU

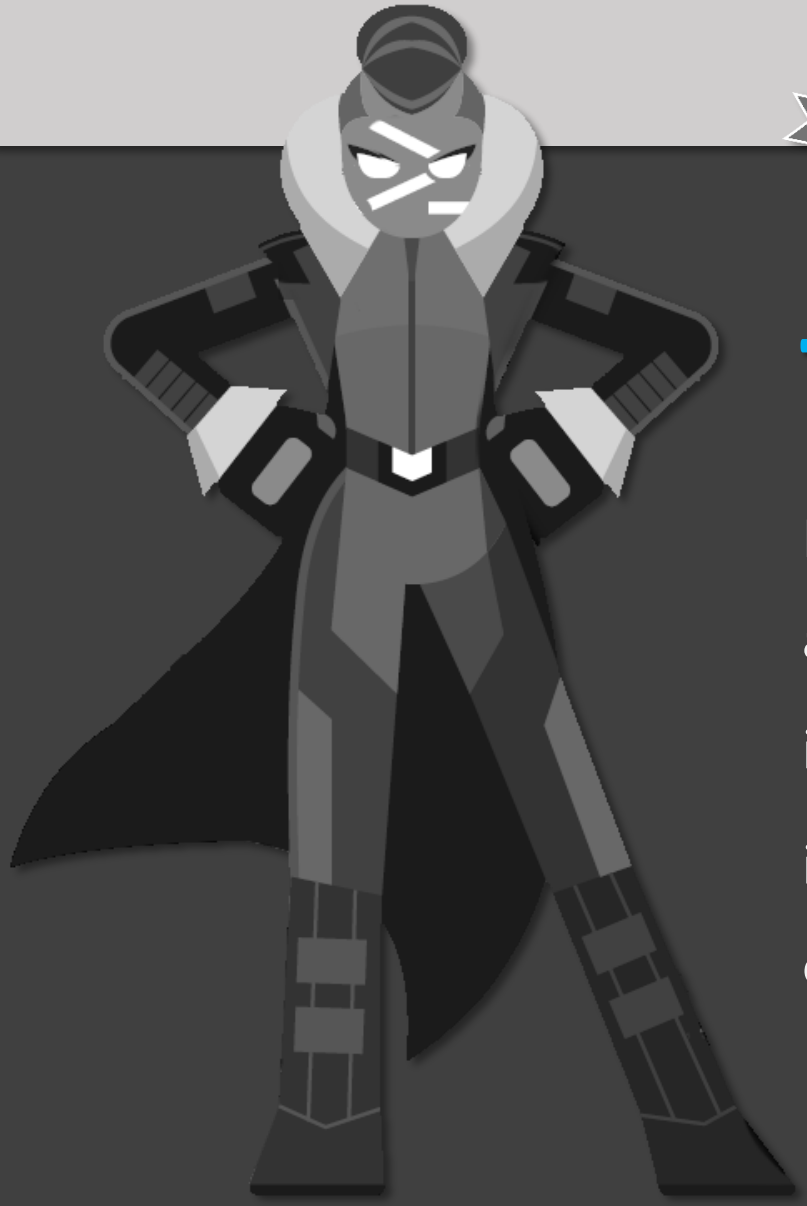
Summary

- **BloodHound is awesome** (Red/Blue/Any…)
- API + PowerShell >> loads of options

- Tool-Making with **PowerShell is awesome**
- If this guy can do it, so can I… (Make it so!)

- **PSConfEU is awesome !!**

Summary



PSCONF.EU

2018

Thank you

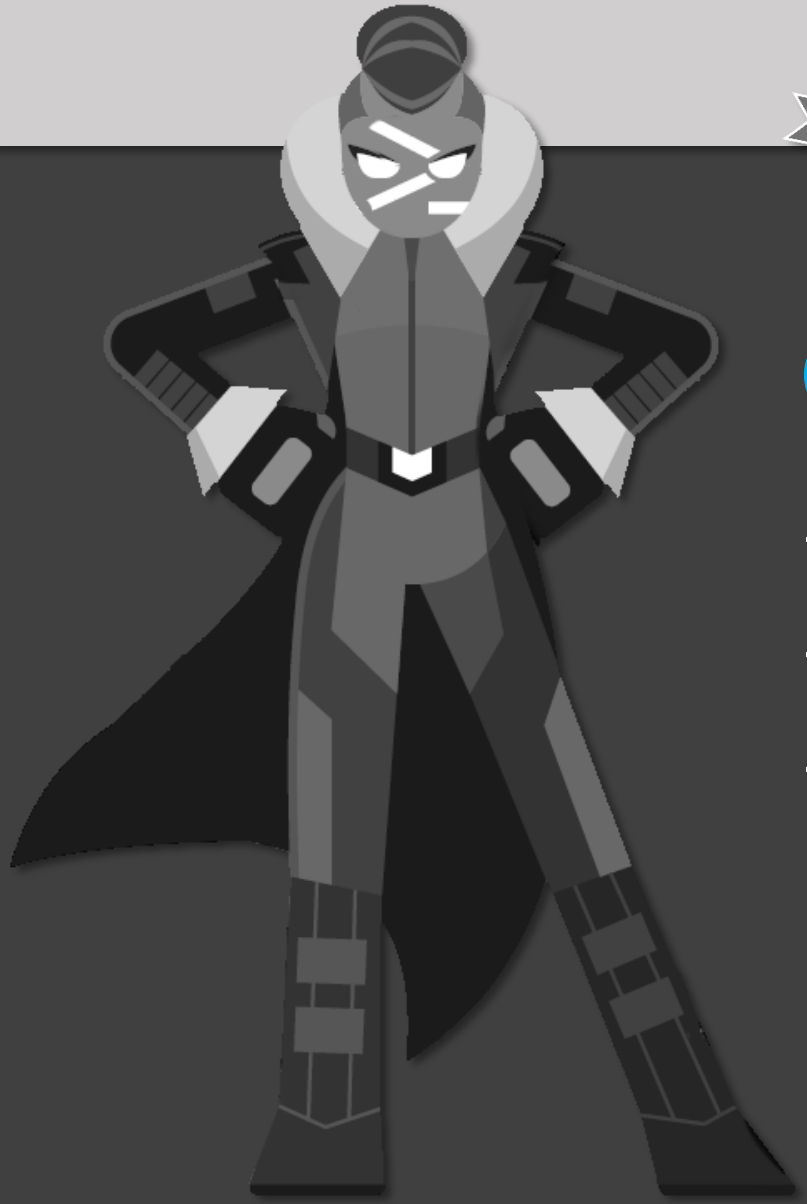
Meetup in the **breakout room**

after this session

if you have **more questions**

if you want to **test this tool**

or simply for a chat/drink...



Now…

PSCONF.EU

2018

Get-Break -Min 15

- Grab a coffee / Have a Chat
- Change Room/Track
- Stay here for next talk

Enjoy **PSConfEU 2018**…


PSCONF.EU