ERNW
providing security.

Hands-On BloodHound

BloodHound & Cypher Workshop - ERNW - 2021

@SadProcessor

ERNW
providing security.

Agenda – Day 1

- **M1 – Introduction**
  - Thinking in Graphs
- **M2 - BloodHound Basic**
  - BloodHound Data Types
  - Data Collection and Ingestion
  - Ui Components & Features
  - Edge Abuse Info
- **M3 - Cypher Language Basic**
  - What is Cypher?
  - Basic Node & Path Queries

ERNW
providing security.

Agenda – Day 2

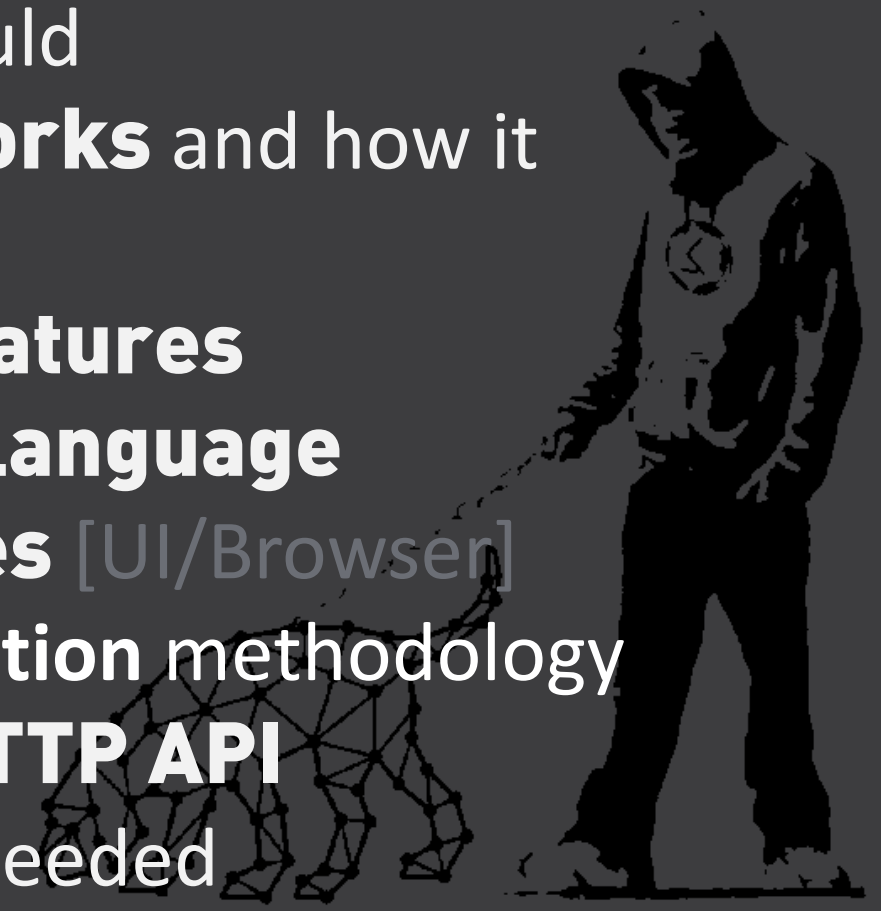
- **M4 - BloodHound Advanced**
  - Build-In / Custom Queries
  - Attack Path Reduction
- **M5 - Cypher Advanced**
  - Modifying data
  - Calculating metrics
  - Debugging Queries
- **M6 - Expanding BloodHound**
  - HTTP API Basics
  - Tool: CypherDog / WatchDog

ERNW
providing security.

Goal

At the end of this workshop, you should

- Understand **how BloodHound works** and how it could be useful for you [Red/Blue]
- Feel familiar with the **UI & tool features**
- Understand the basics of **Cypher language**
- **Create/Debug your own queries** [UI/Browser]
- Understand the **Attack Path Reduction** methodology
- Understand the workings of the **HTTP API**
- Know where to find **Info/Help** if needed



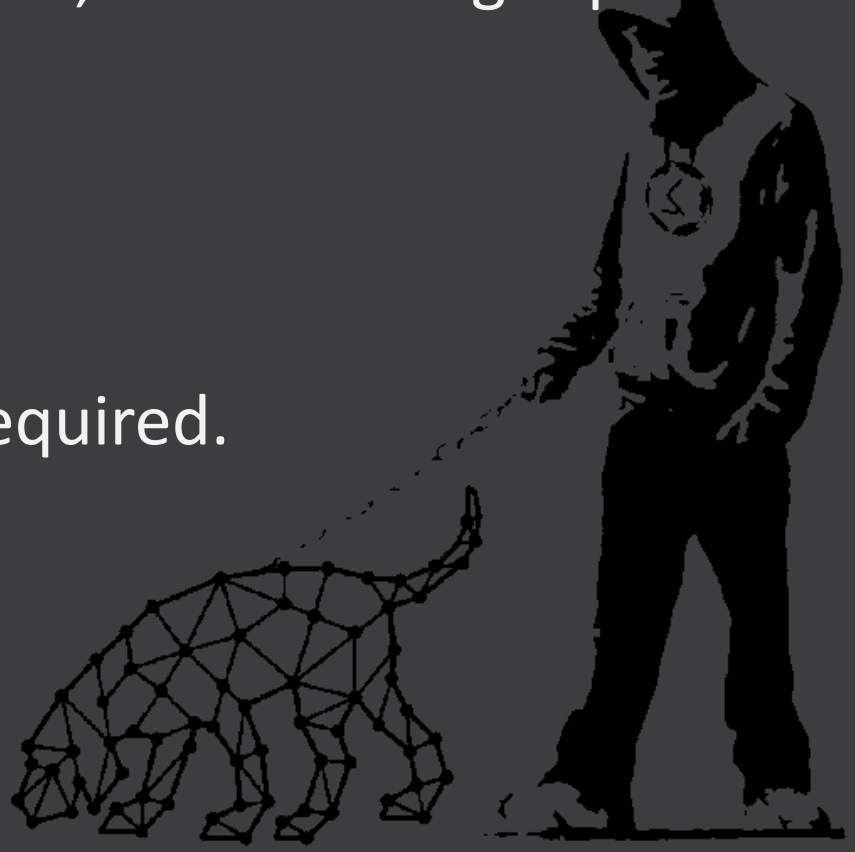
ERNW
providing security.

Scope

This training is about **Bloodhound & Cypher**, the following topics will not be covered in this workshop:

- Active Directory & Hardening in General
- Specific Attack Scenario

Basic understanding of Active Directory is required.

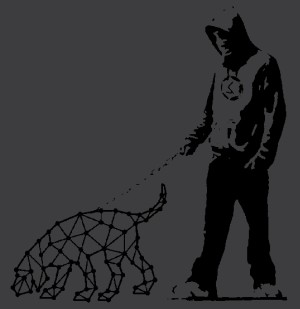


ERNW
providing security.

Whois

Walter Legowski - @SadProcessor

- Windows Security Consultant [ERNW]
- Born FR, Live NL, Work DE
- Like Windows/Cats/Trees
- Love my 3 kids
- Don't like Dogs
- Made exception for **BloodHound**

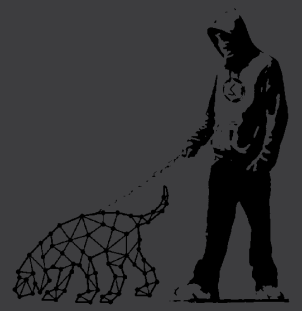


ERNW
providing security.

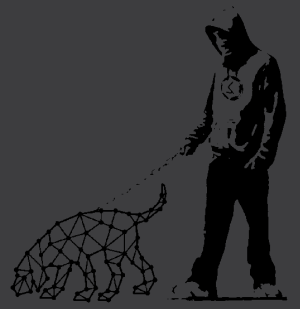
Disclaimer

- **I am not a Cypher expert**
- Training only scratches the surface
- Excuses if any errors/typos in material

- **DO NOT SCAN A CORPORATE NETWORK WITHOUT PROPER AUTHORISATION**




NO TIME TO EXPLAIN
GET IN THE TRUCK



ERNW
providing security.

M1 - Introduction

- What is BloodHound
- “Attackers think in Graphs”
- Graph DB Concept & terminology

[Alice & Bob example]

ERNW
providing security.

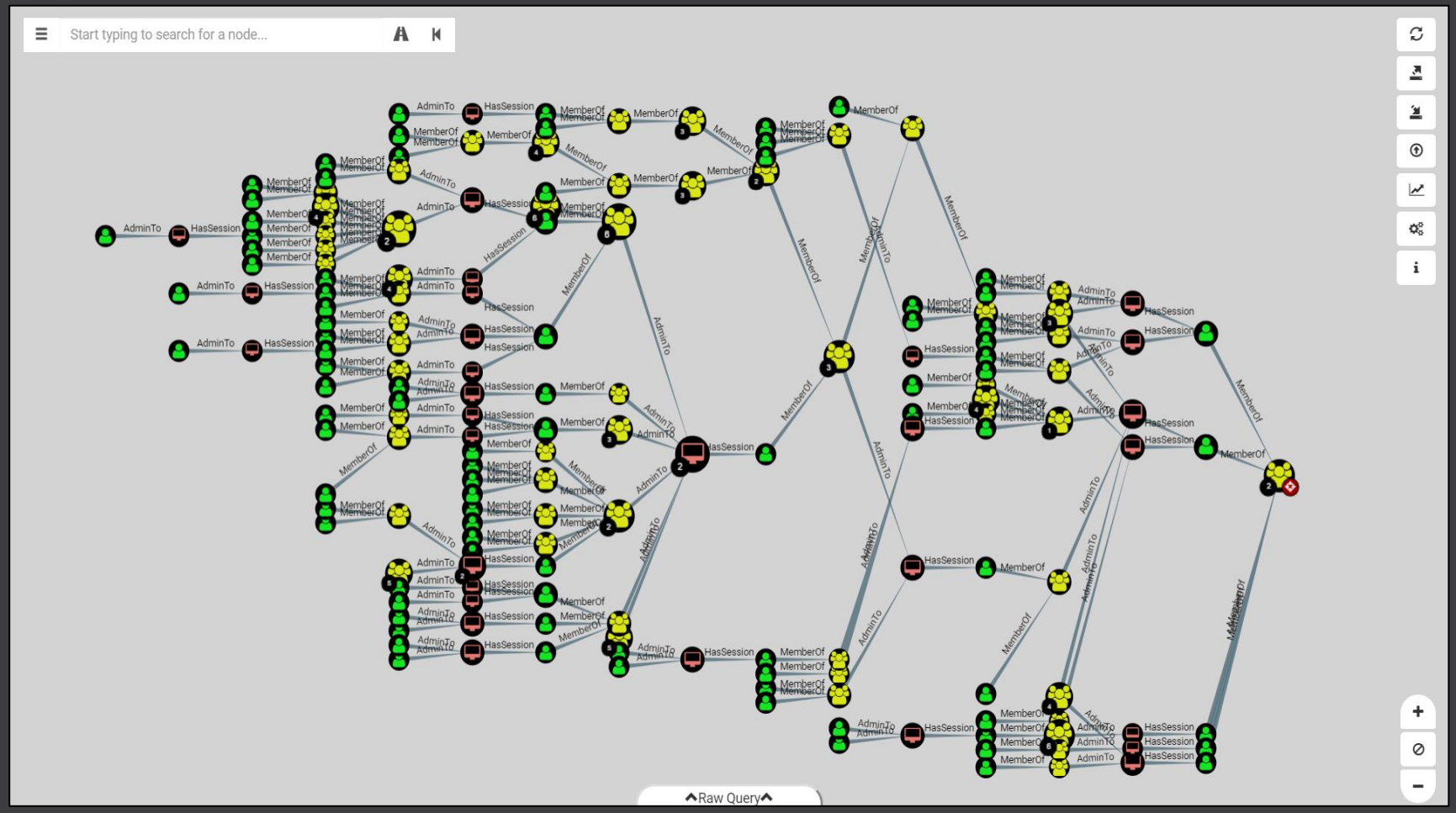
BloodHound - What?

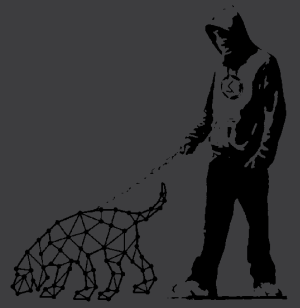
Defenders think in lists,
Attackers think in graphs,
As long as this is true,
Attackers win...
[John Lambert, MS Threat Intel]

Read: https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/

ERNW
providing security.

BloodHound – What?





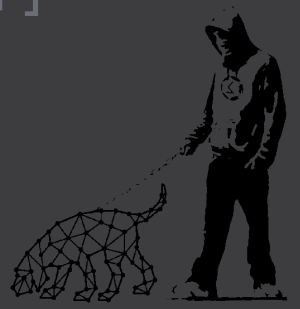
ERNW
providing security.

BloodHound – Who?

Created by

- @_WaldO
- @CptJesus
- @harmj0y

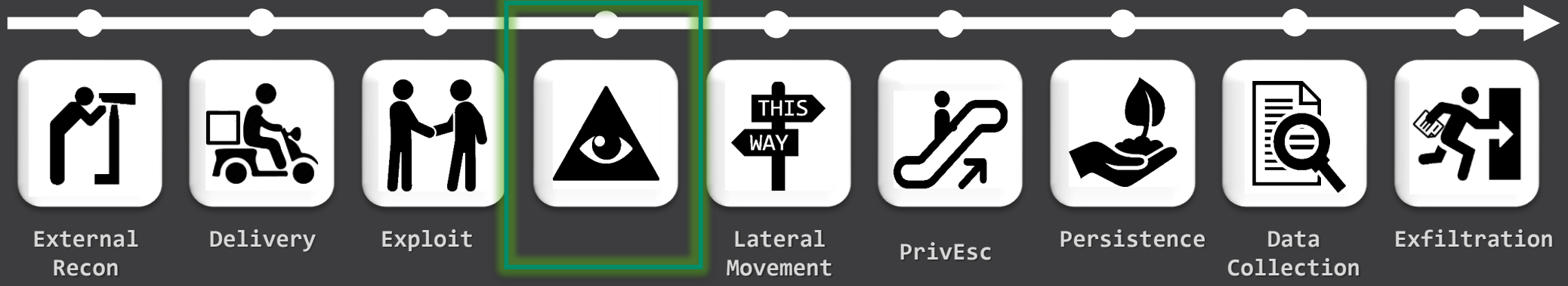
[follow on Twitter]



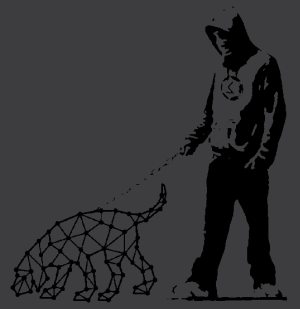
ERNW
providing security.

BloodHound – What?

Attacker Kill Chain

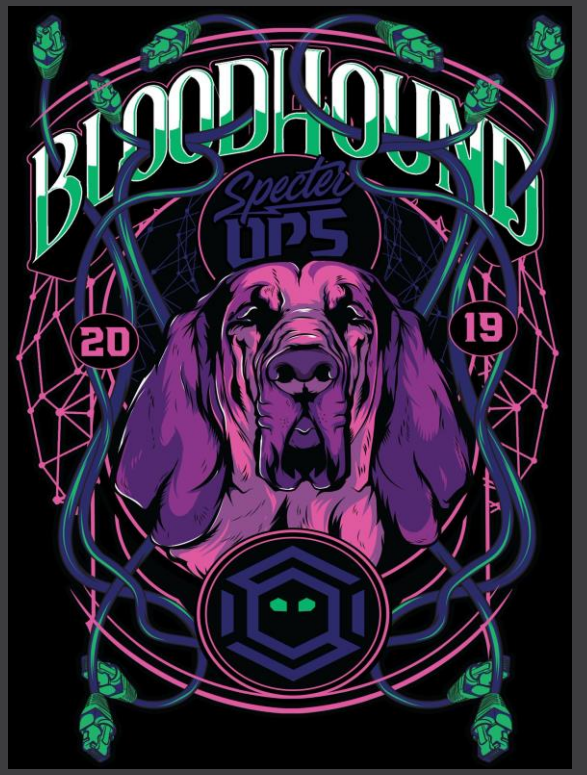


External Recon | Delivery | Exploit | **Internal Recon** | Lateral Movement | PrivEsc | Persistence | Data Collection | Exfiltration



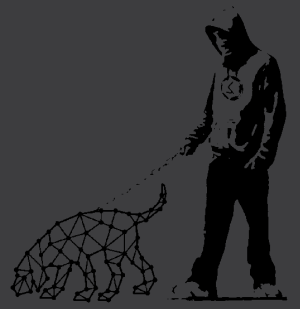
ERNW
providing security.

BloodHound – What?



An **AD attack path** mapping tool...

- **Open Source** [all OS flavor]
- Based on **neo4j** graph DB
- Initial release: 2016
- Current version: 4.1
- Well maintained & documented
- User Community ++



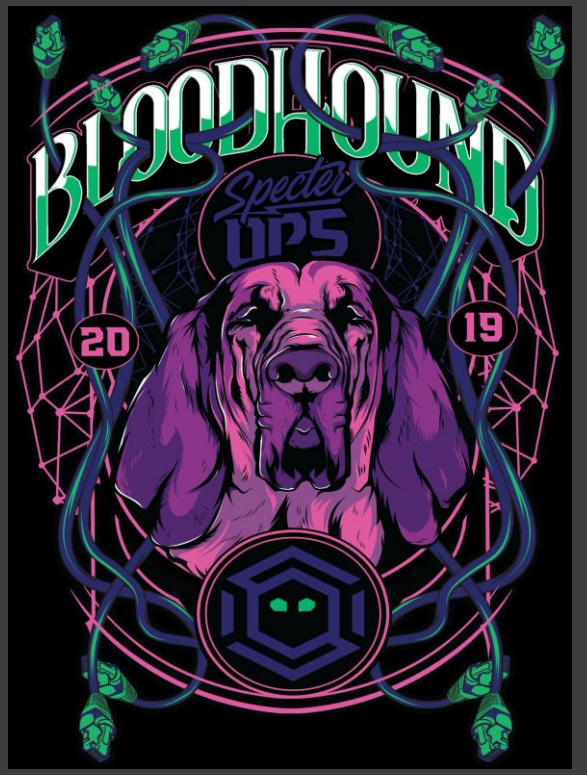
Wiki: https://bloodhound.readthedocs.io/en/latest/index.html

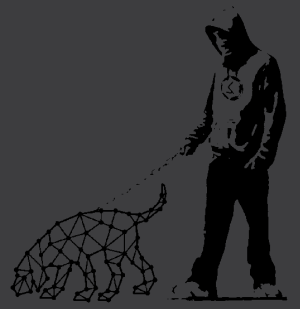
ERNW
providing security.

BloodHound –What?

An **AD Hardening** tool…

- Originally designed for **Red Team** reconnaissance [Post-Exploitation]
- Gaining popularity in **Blue Teams**
- Can be used for Security **Consulting** and **AD Auditing**
- **Expandable** & **Automatable**





Wiki: https://bloodhound.readthedocs.io/en/latest/index.html

ERNW
providing security.

BloodHound - Where?

Tool & Resources...

- Neo4j Community Edition

https://neo4j.com/download-center/#community

- BloodHound Source code

https://github.com/BloodHoundAD/BloodHound

- BloodHound Online Documentation

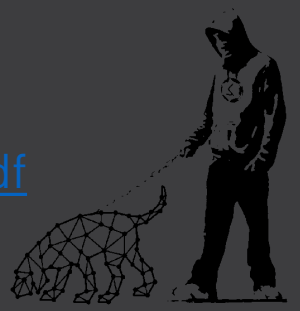
https://bloodhound.readthedocs.io/en/latest/index.html

- Neo4j Cypher Reference Card

https://neo4j.com/docs/cypher-refcard/current/

- Dog Whisperer Handbook

https://www.ernw.de/download/BloodHoundWorkshop/ERNW_DogWhispererHandbook.pdf



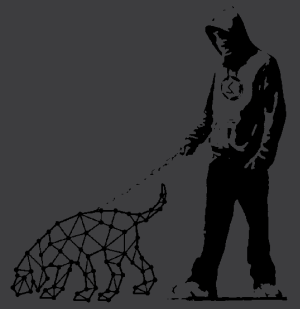
ERNW
providing security.

BloodHound - How?

Install... [Windows64]

- [Install Java64bit]
- Unzip Neo4j Community Edition
- Install & Start neo4j service
- Go to **http://localhost:7474**
- Set new password
- Unzip BloodHound Source
- Start bloodhound.exe & enter password

Wiki: https://bloodhound.readthedocs.io/en/latest/index.html

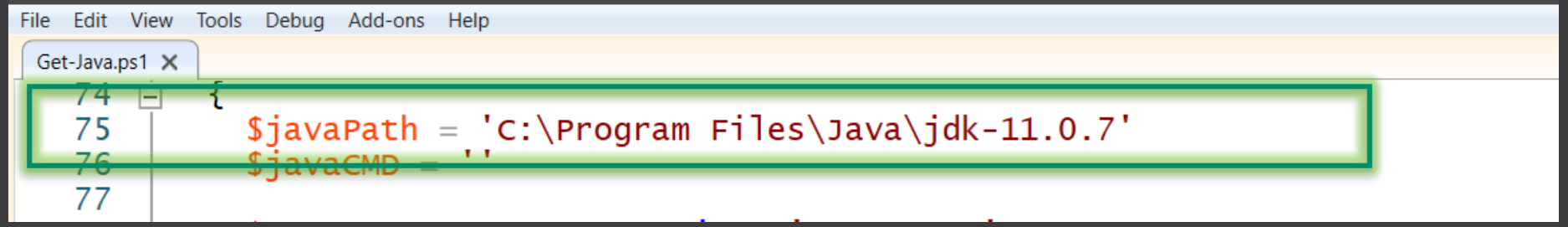


ERNW
providing security.

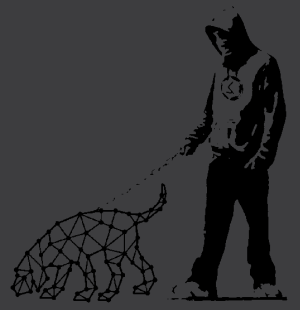
BloodHound - How?

Install... [Windows64]

- To avoid error due to multiple Java installs
  > Hard-code JavaPath in **Get-Java.ps1**



C:\[...]\neo4j-community-4.1.0\bin\Neo4j-Management\Get-Java.ps1



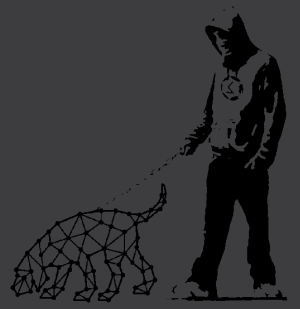
ERNW
providing security.

BloodHound – Where?

Join the BloodHound Slack…

- Read tons of **interesting stuff**
- Meet tons of **interesting people** [6000+]
- Ask Wald0 about **#cypher_queries**
- Speak **#kerberos** with Harmj0y
- Ask Jesus anything
- **+ Many more AD/Pentest/Tool channels**

Invite: https://bloodhoundgang.herokuapp.com/



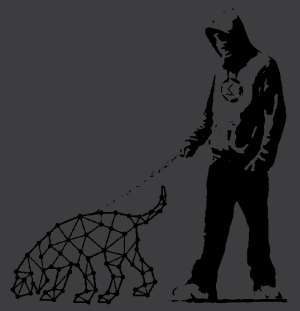
ERNW
providing security.

Hands-On: Think In Graphs...

Read blog post by J. Lambert to start thinking in graphs...

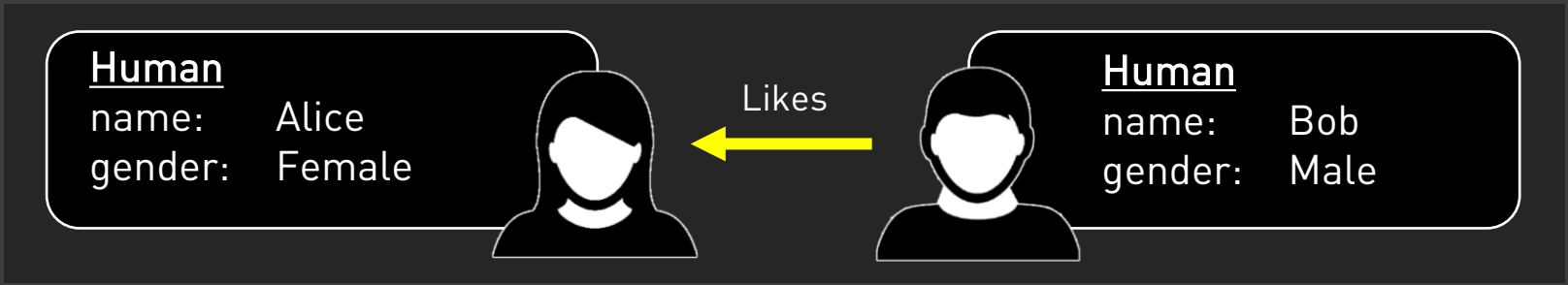
+ Join the BloodHound Gang... [if you like]

[E1.1 + E1.2]

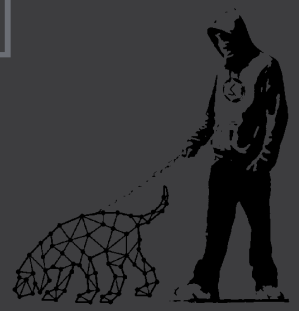


ERNW
providing security.

Alice & Bob - Terminology

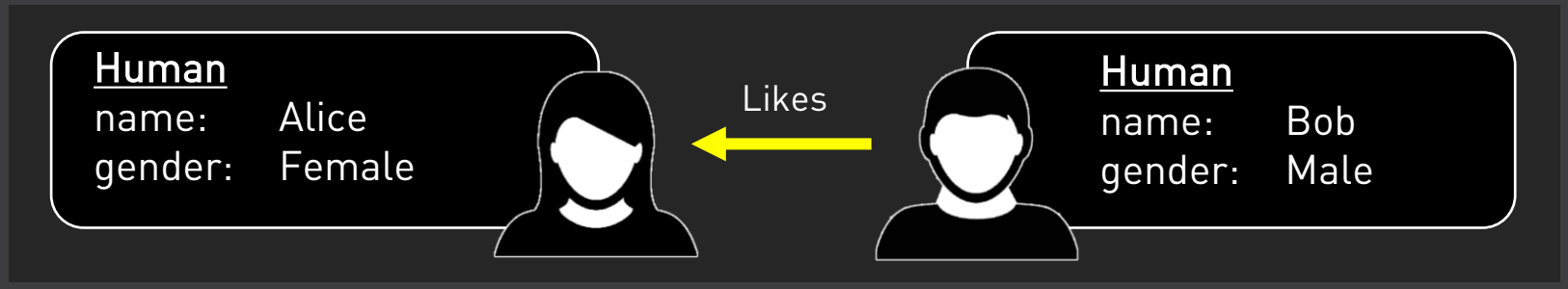


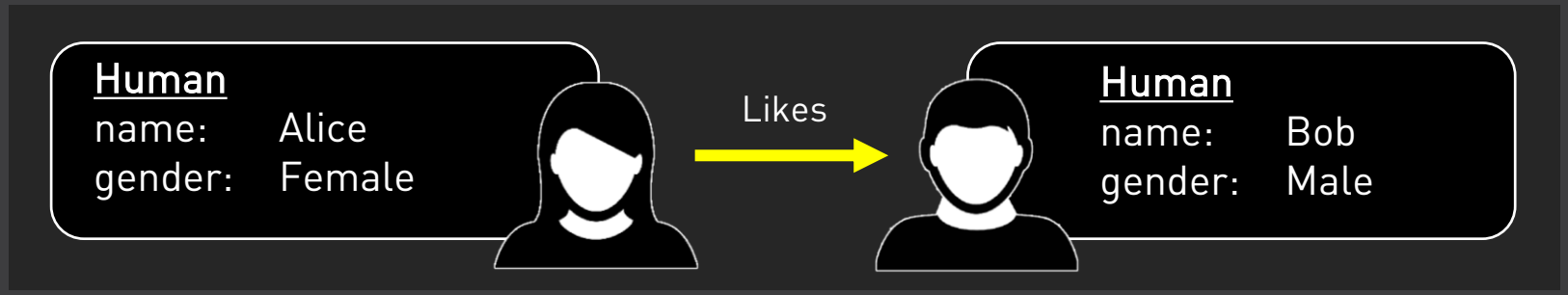
- Objects are called **Nodes** [Humans Alice & Bob]
- Nodes have a type aka **Label** [Human]
- Nodes have **properties** [name/gender]
- Relationships are called an **Edges** [Likes]
- Edges can also have properties

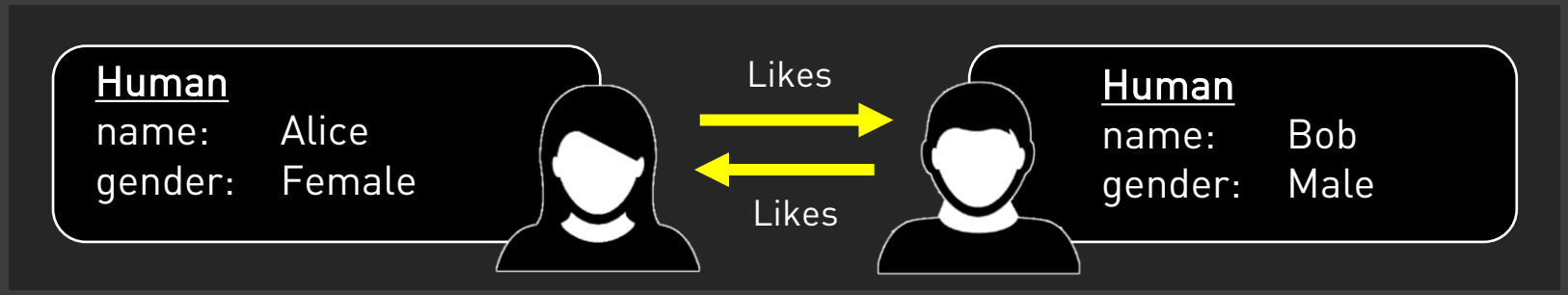


ERNW
providing security.

Alice & Bob - Terminology

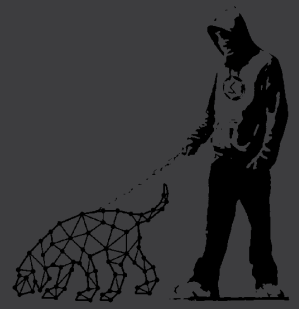






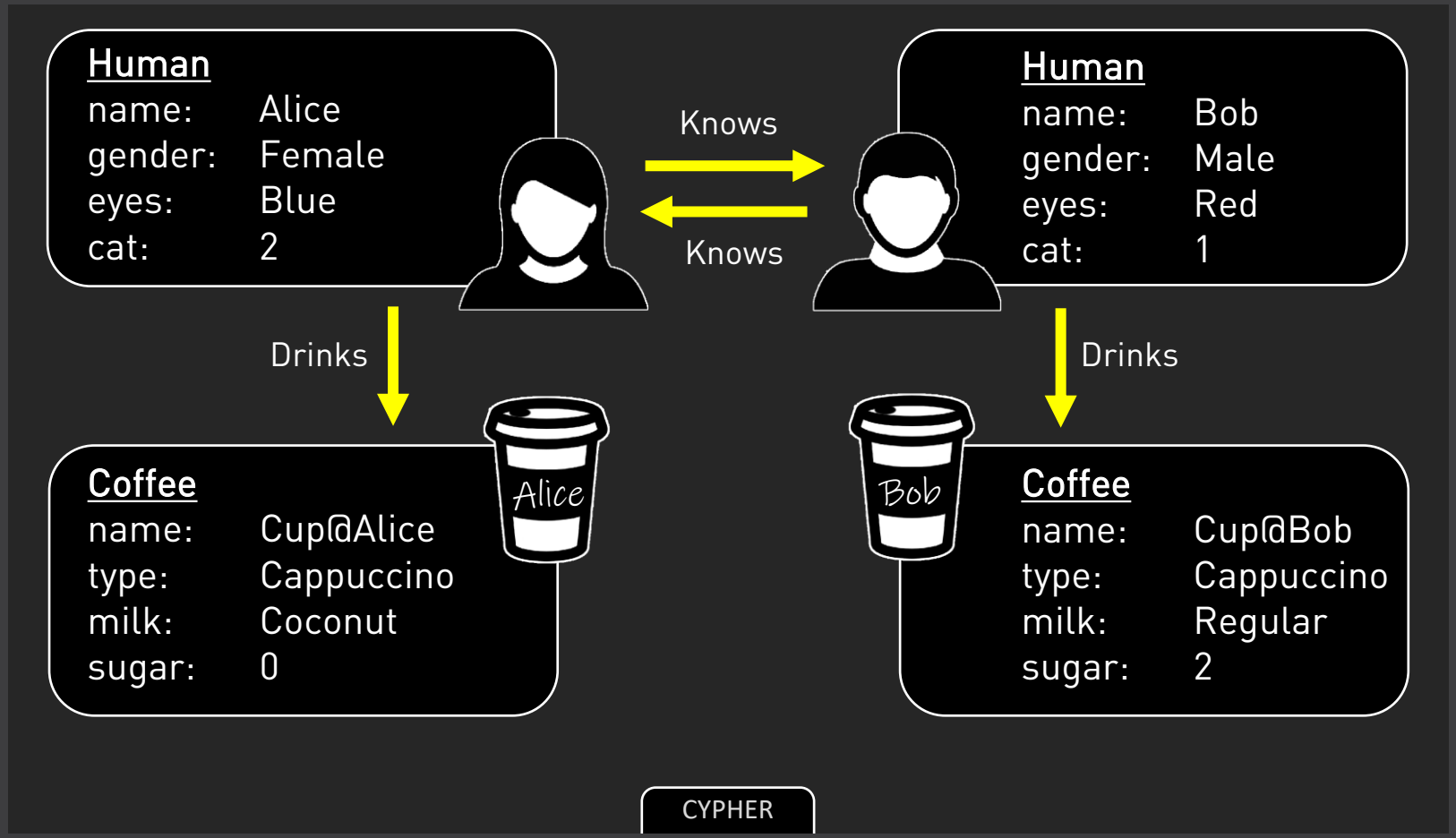
Important:
Edges are directional

[Need two Edges for relationship to go both ways...]

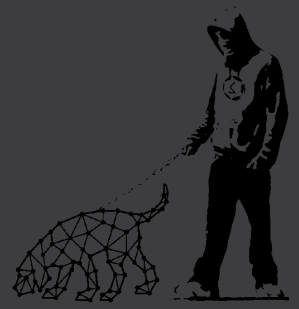


ERNW
providing security.

Alice & Bob - Dataset

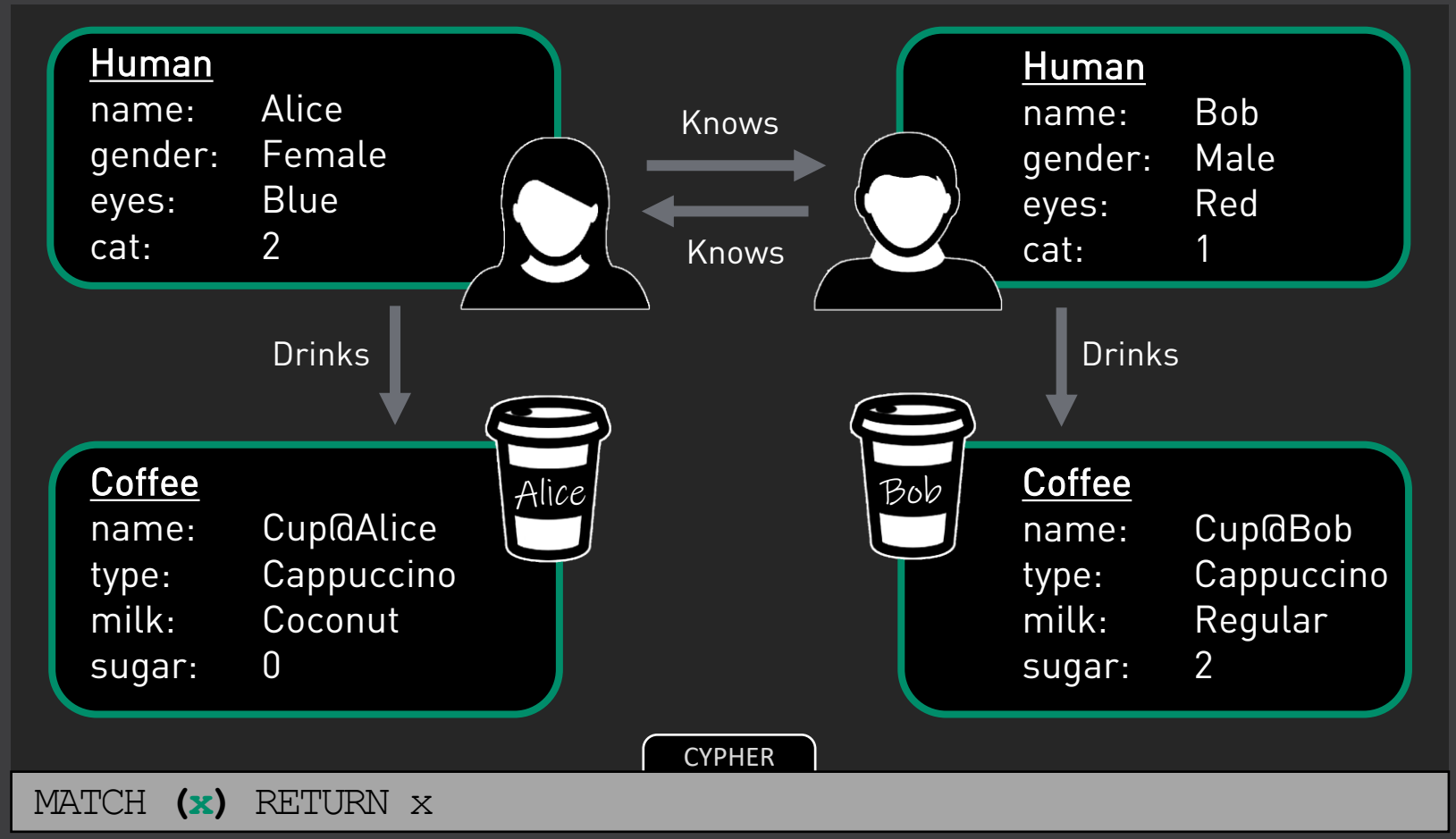


Now let's imagine this is our data. **Let's see what we can ask neo4j...**

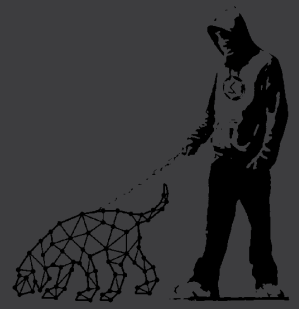


ERNW
providing security.

Alice & Bob - Queries

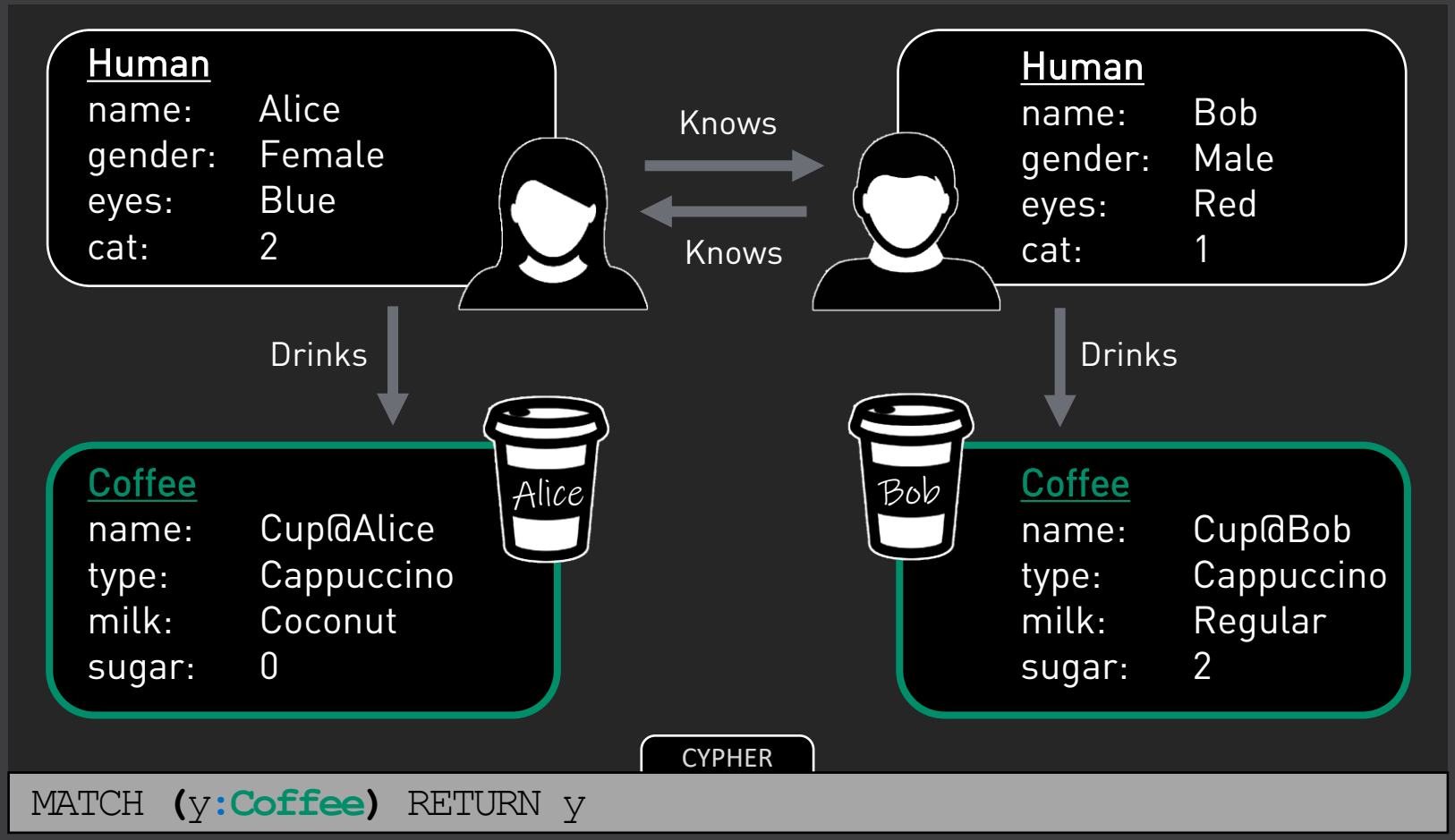


Return all Objects... [Nodes]

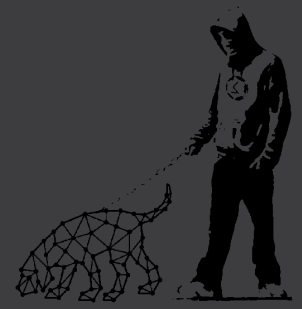


ERNW
providing security.

Alice & Bob - Queries

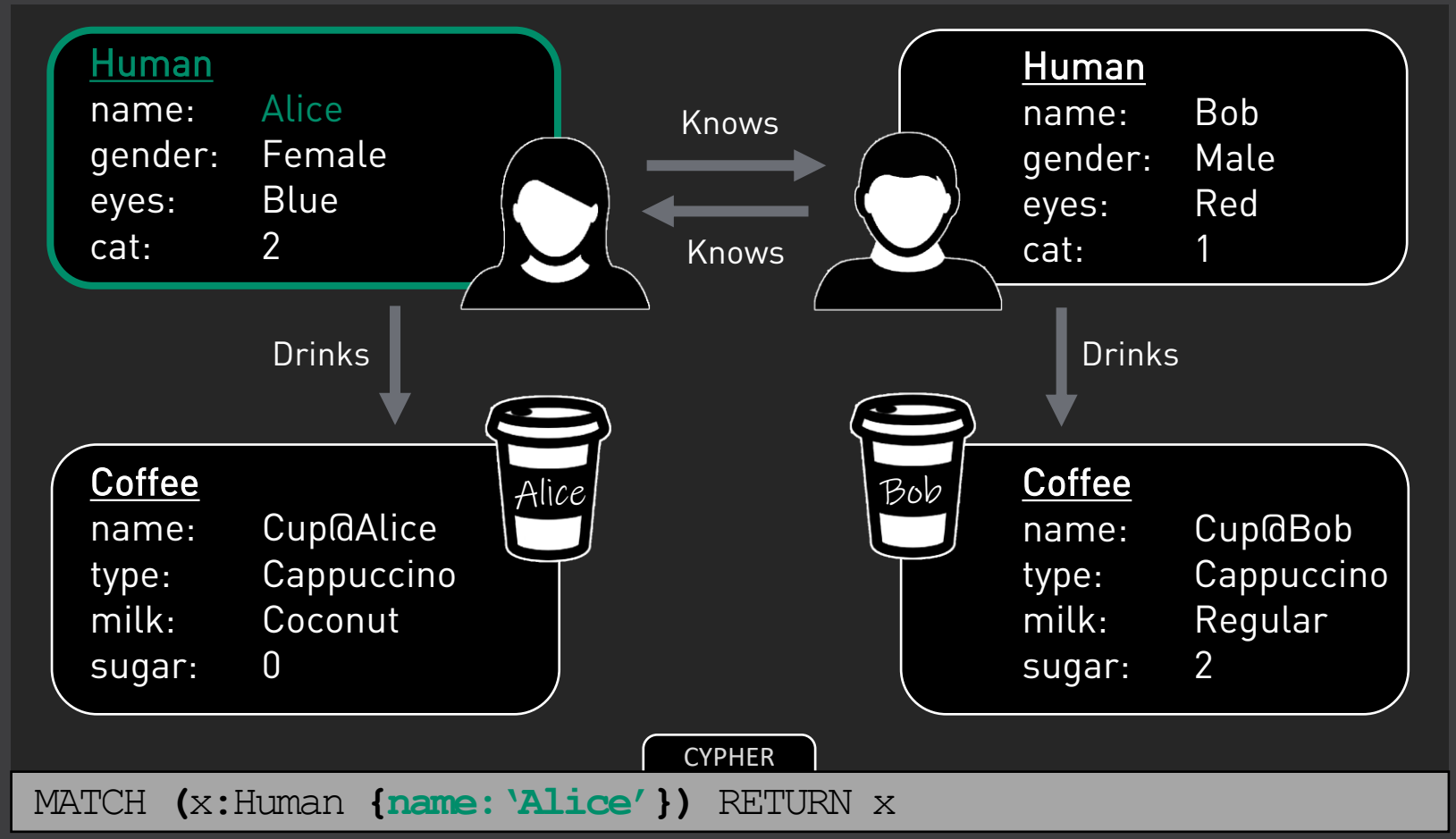


Return all Nodes of type Coffee [Label]

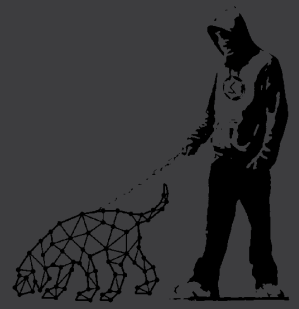


ERNW
providing security.

Alice & Bob - Queries

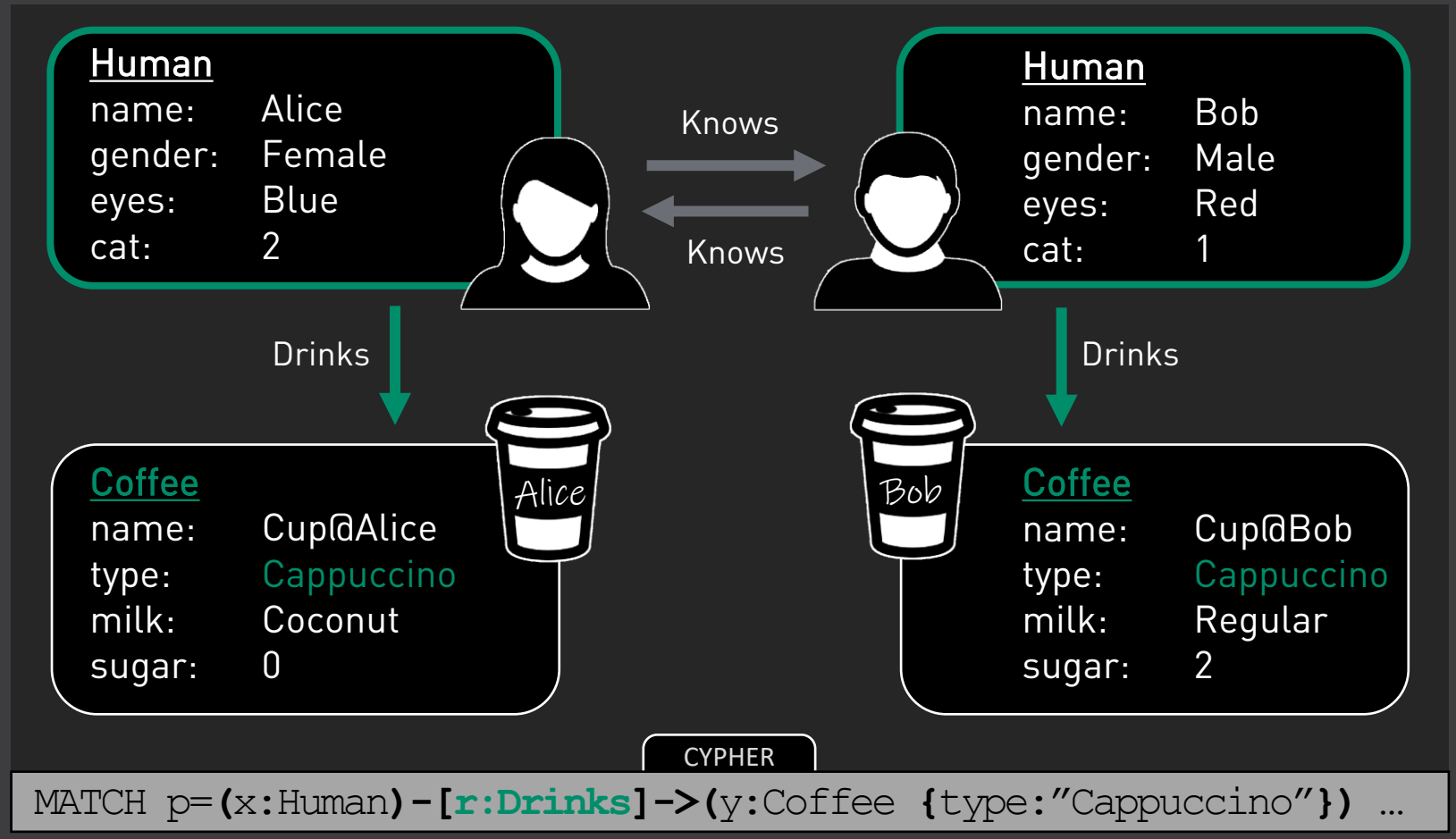


Is there a Human with name Alice?
[Property]



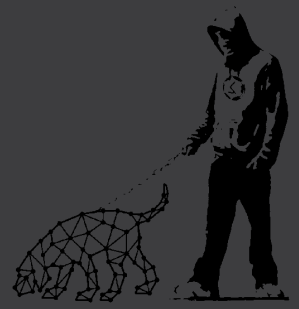
ERNW
providing security.

Alice & Bob - Queries



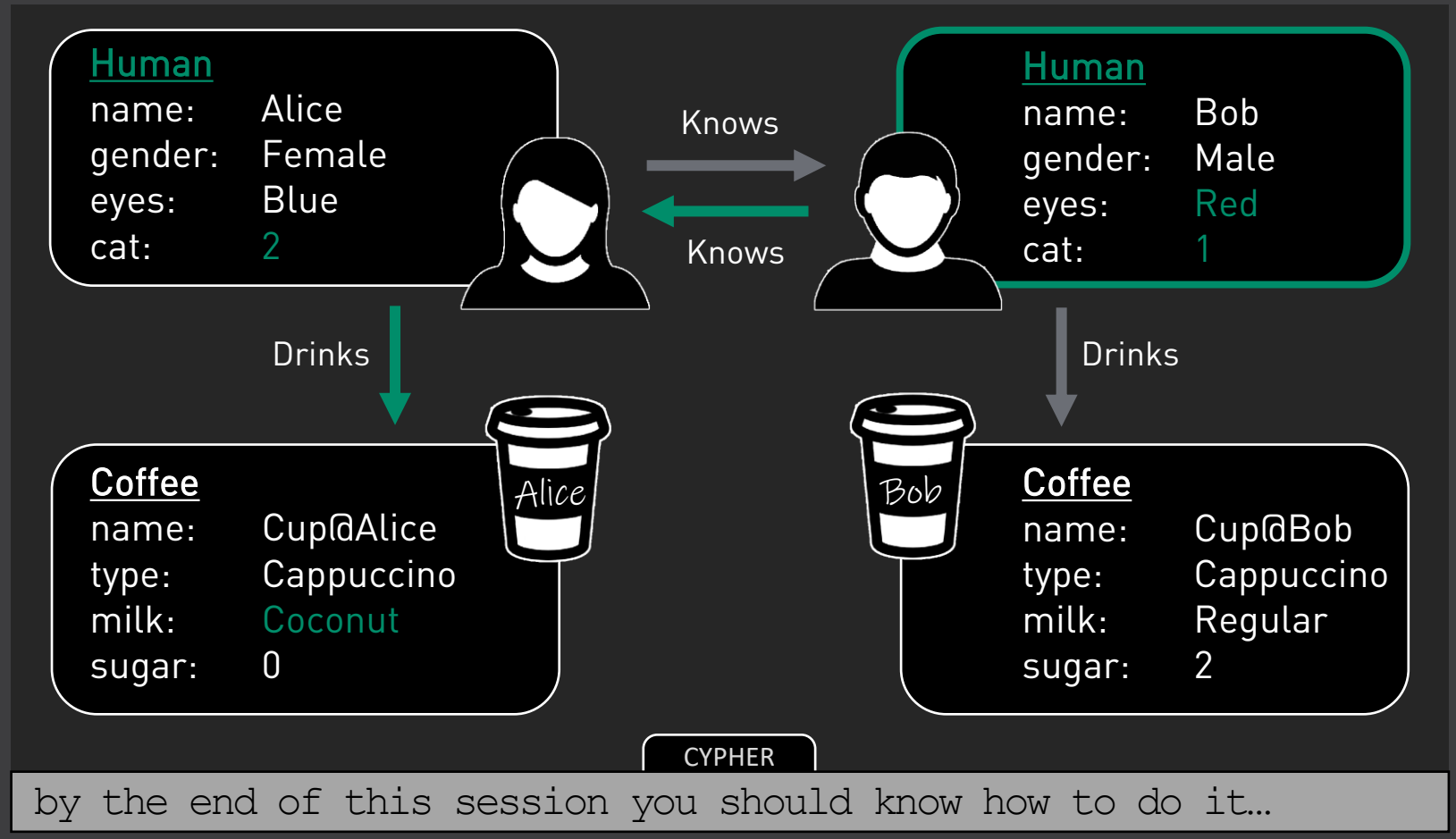
Who Drinks Cappuccino?

[Edge]

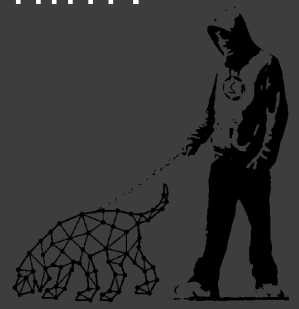


ERNW
providing security.

Alice & Bob - Queries



Does anyone with red eyes know somebody that drinks cappuccino with coconut milk and that has more cats than him?



ERNW
providing security.

M2 – BloodHound Basics

- BloodHound data type
- Data Collection & Ingestion
- UI Features
- Querying Nodes & Path (UI)

ERNW
providing security.

BloodHound Data

ERNW
providing security.

BloodHound Data - Nodes

BloodHound uses **6 Node types** [aka Node Labels]


:Domain


:Group

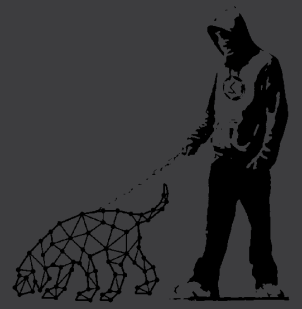

:OU


:Computer


:GPO


:User

Each Node type has matching set of **properties**

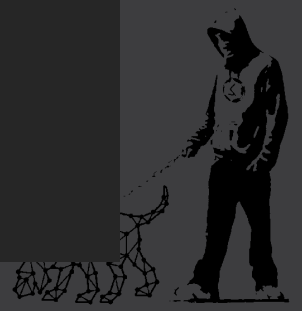


ERNW
providing security.

BloodHound Data - Nodes

BloodHound 4.+ extends to **Azure** and adds following node types:

- :AZTenant
- :AZApp
- :AZUser
- :AZSubscription
- :AZDevice
- :AZVM
- :AZResourceGroup
- :AZServicePrincipal
- :AZServicePrincipal
- :AZGroup



ERNW
providing security.

BloodHound Data - Edges

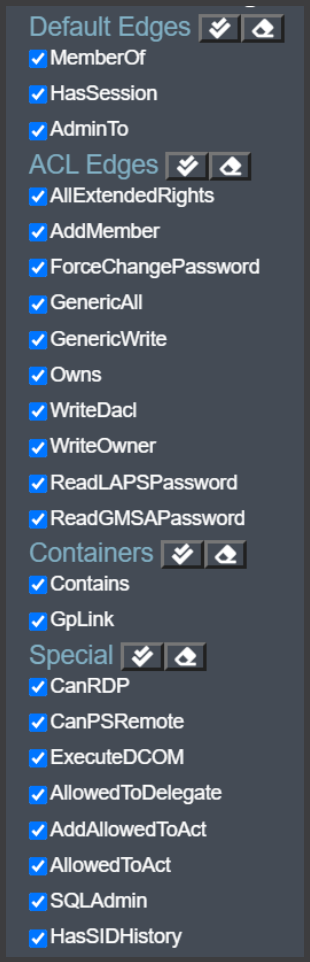
BloodHound uses **23 Edge types**

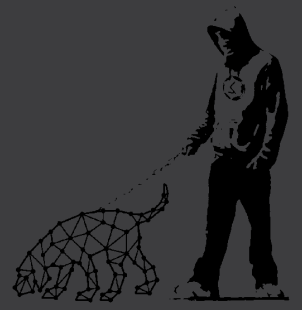
Default
MemberOf
HasSession
AdminTo

Special
CanRDP
CanPSRemote
ExecuteDCOM
AllowedToDelegate
AddAllowedToAct
AllowedToAct
SQLAdmin
HasSIDHistory

ACL
AllExtendedRights
AddMember
ForceChangePassword
GenericAll
GenericWrite
Owns
WriteDacl
WriteOwner
ReadLAPSPassword
ReadGMSAPassword

Container
Contains
GpLink



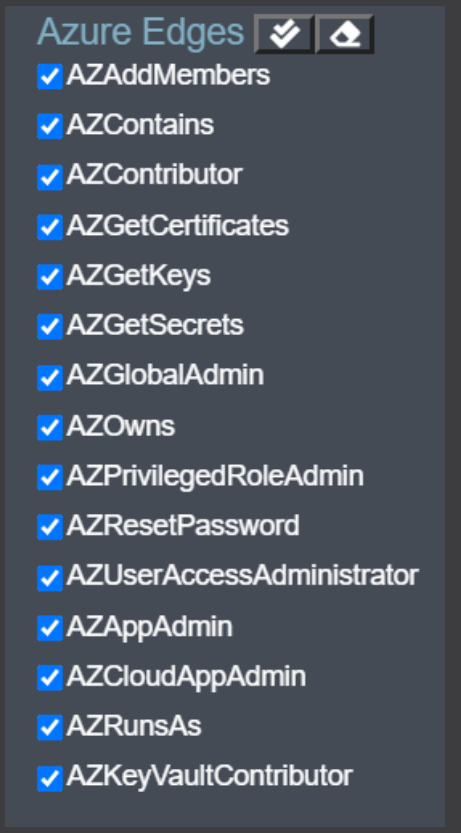


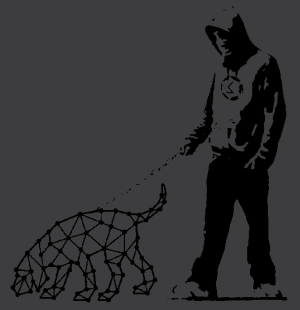
ERNW
providing security.

BloodHound Data - Edges

BloodHound 4+ adds following relationships for Azure Related Nodes:

Azure Edges
AZAddMembers
AZContains
AZContributors
AZGetCretificates
AZGetKeys
AZGetSecrets
AZGlobalAdmin
AZOwns
AZPriviledgedRoleAdmin
AZResetPassword
AZUserAccessAdministrator
AZAppAdmin
AZCloudAppAdmin
AZRunAs
AZKeyVaultContributor

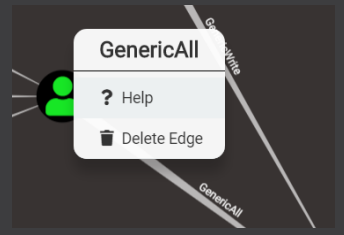




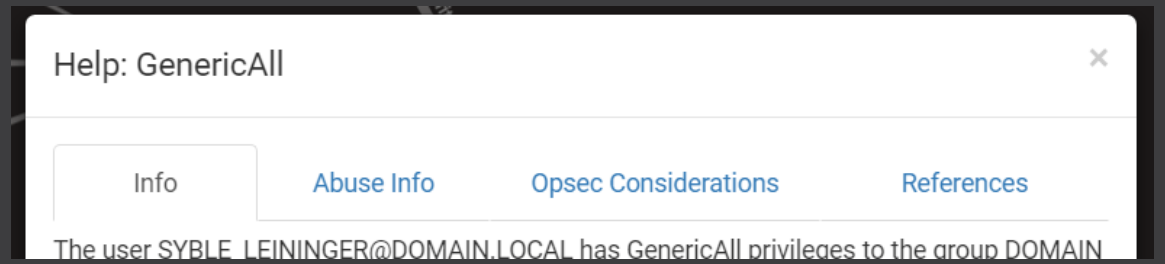
ERNW
providing security.

BloodHound Data - Edges

Each Edge represents a [one]way to move

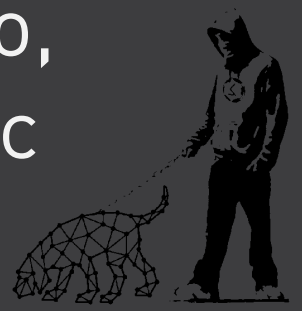


Right-Click Edge for Edge Help



This will open a contextual menu with General Info, Attack Info, OpSec Info, and Extra Refs on the topic

Wiki: https://bloodhound.readthedocs.io/en/latest/data-analysis/edges.html



ERNW
providing security.

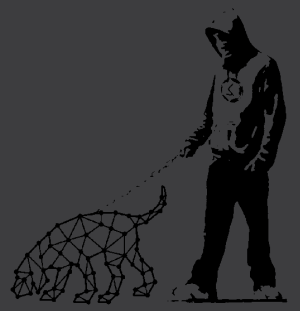
BloodHound - Components

Data Collection = SharpHound

- Runs on targeted network
- Ouputs ZIP file containing data

Data Consumption = BloodHound

- Runs on attacker machine [not target network]
- Ingest ZIP file and consume AD data

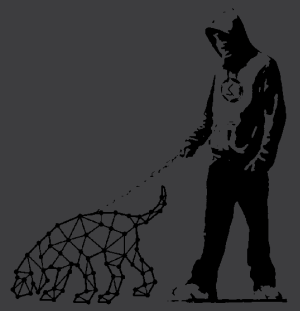


ERNW
providing security.

BloodHound - Components

New: Azure Data Collection = AzureHound

- Runs on targeted tenant
- Ouputs ZIP file containing data
- Uses PowerShell to contact Azure APIs



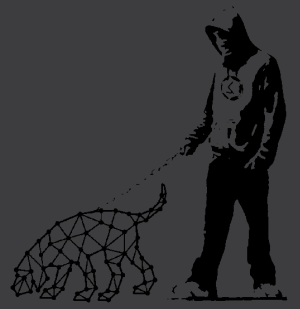
ERNW
providing security.

SharpHounds - Info

SharpHound is the BloodHound Data Collector

- [Re]Written in **C#** for better performances
- Uses **LDAP & win32 API Calls** to gather info
- Data can be collected at user level
- Comes in two flavors [.exe/.ps1]
- Various **Collection Methods** [switches]

Read: https://blog.cptjesus.com/posts/sharphoundtargeting



ERNW
providing security.

Collection Methods - Overview

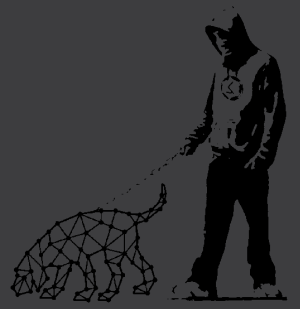
Data collected depends on Collection Method chosen

- To collect everything: [no admin needed]

Invoke-BloodHound –CollectionMethod **All**

- Make sure to read Wiki & CptJesus's post on the topic
- Check .ps1 code & Help pages

Read: https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound.html

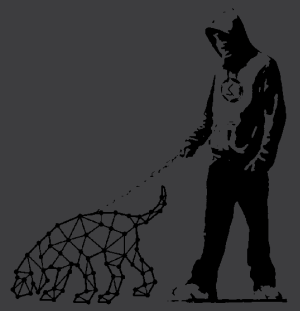


ERNW
providing security.

Hands-On: Collection Methods

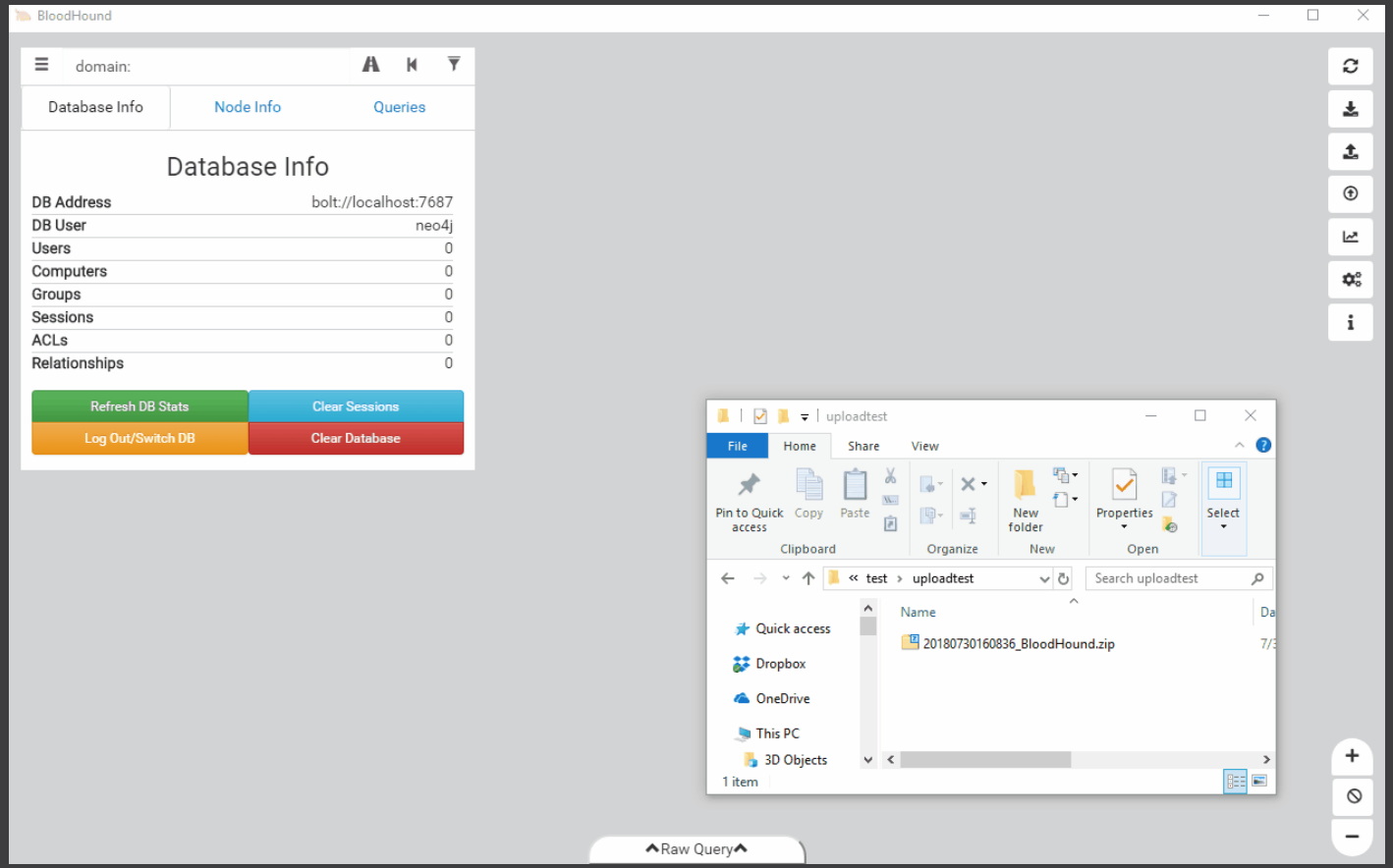
Answer the following questions using information found in help pages and online...

[E2.1]

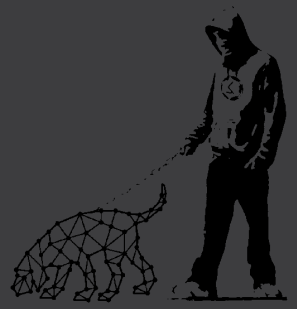


ERNW
providing security.

Data Import – HowTo?

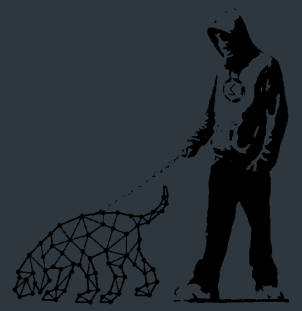


To Import [more] collected data, simply **drag** [extra] **zip files into the UI**



ERNW
providing security.

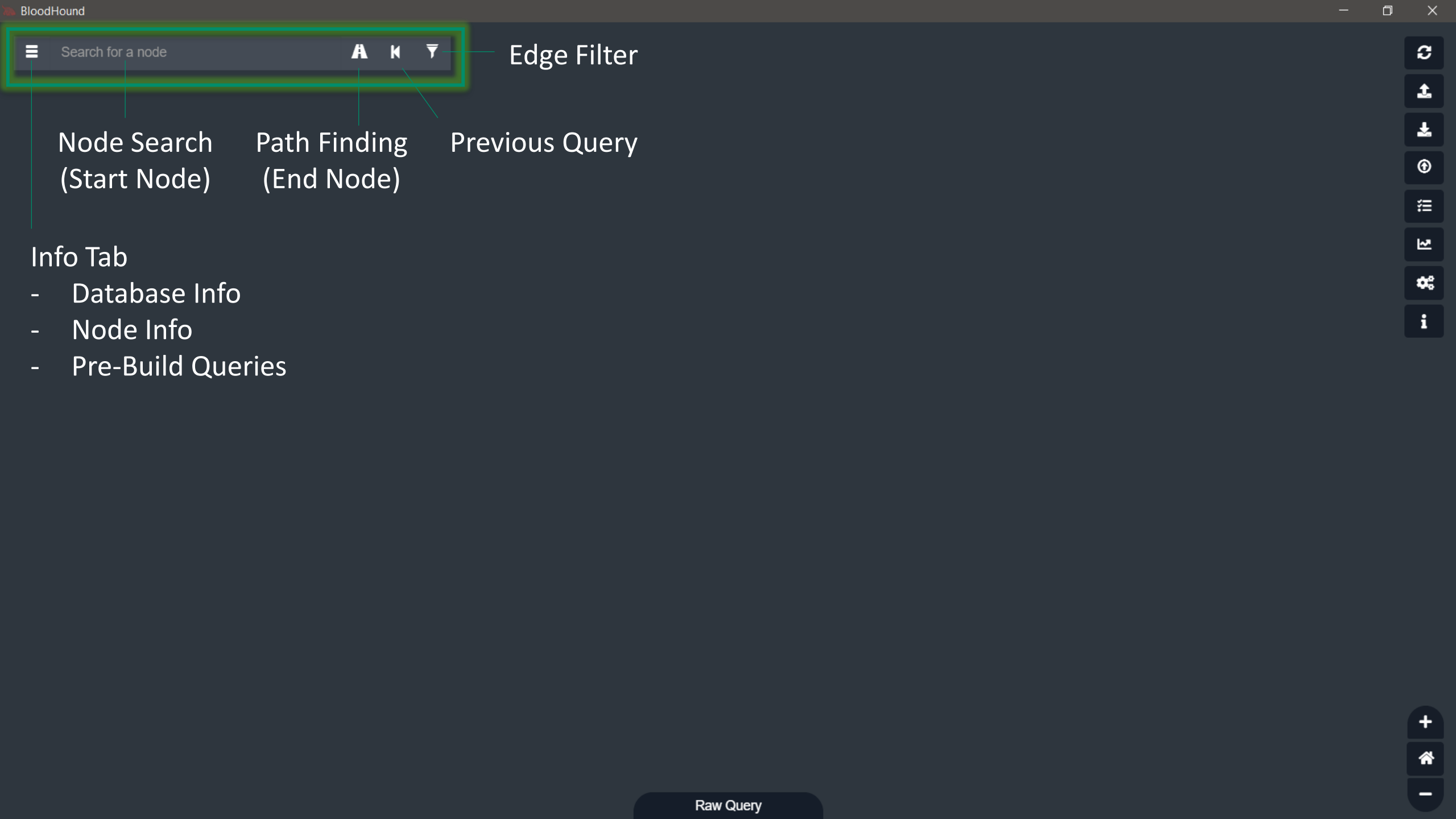
BloodHound - UI

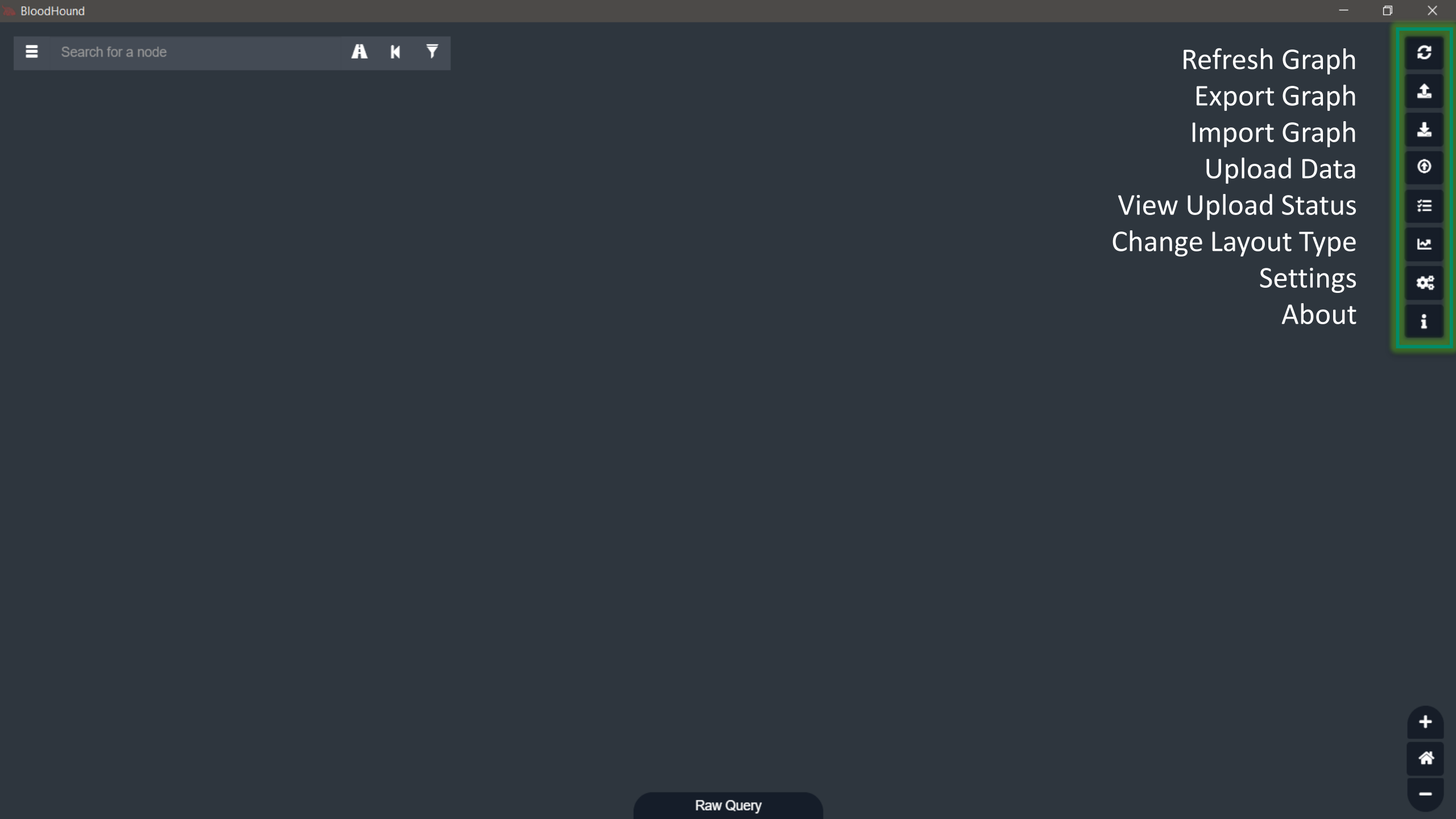


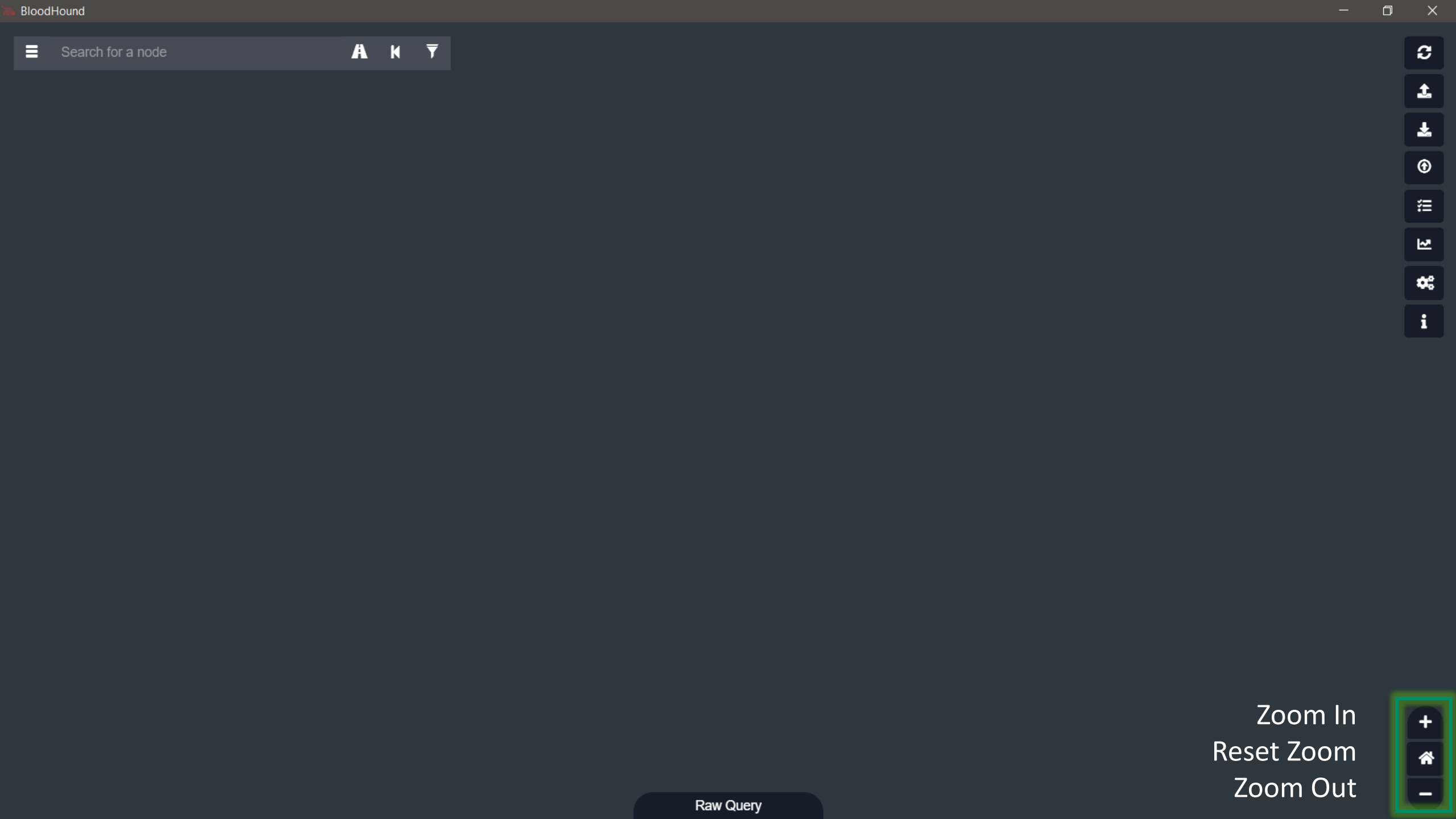
BloodHound

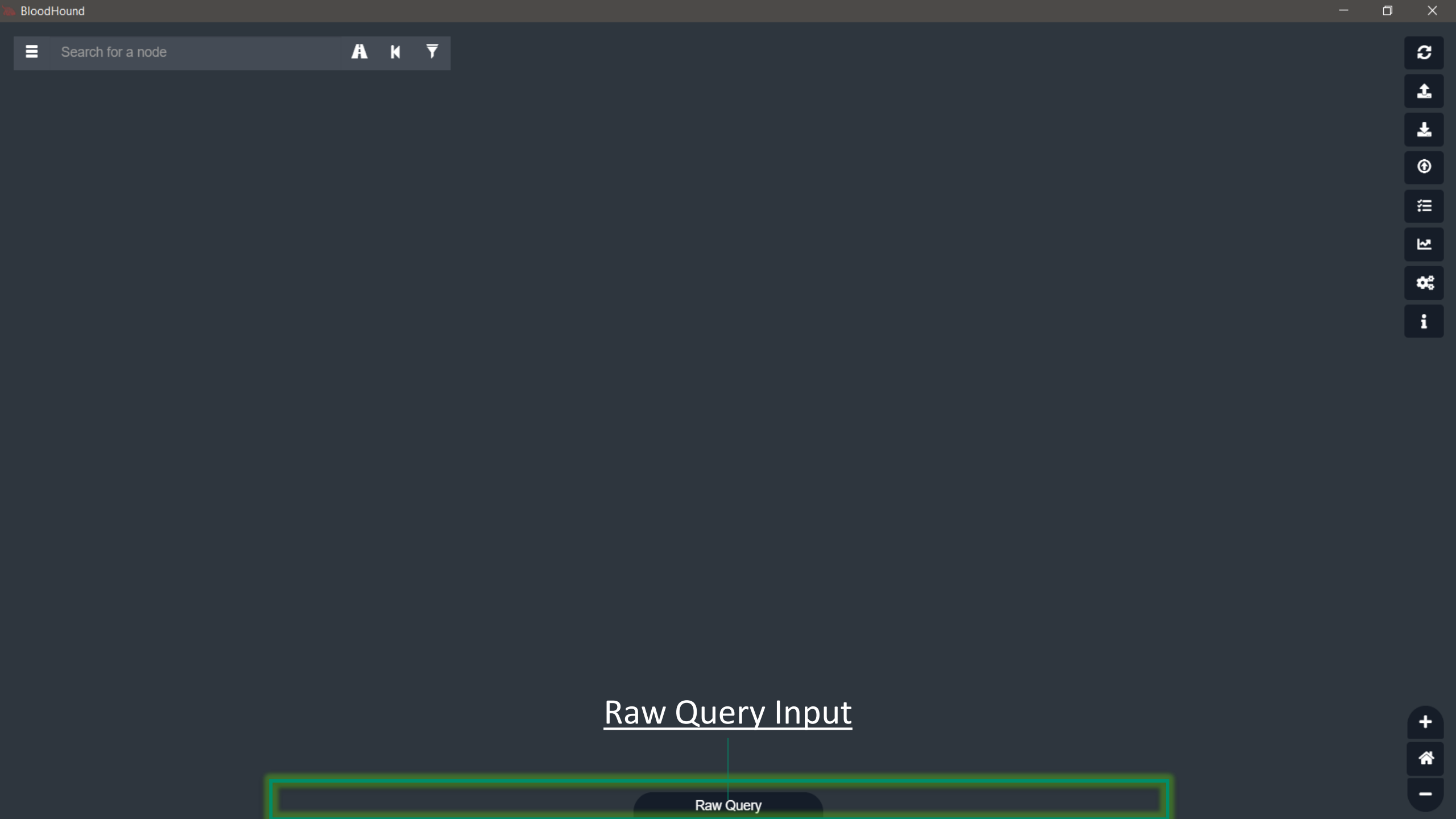
Search for a node

Raw Query


BloodHound
Search for a node
Edge Filter
Node Search
(Start Node)
Path Finding
(End Node)
Previous Query
Info Tab
- Database Info
- Node Info
- Pre-Build Queries
Raw Query


BloodHound
Search for a node
Refresh Graph
Export Graph
Import Graph
Upload Data
View Upload Status
Change Layout Type
Settings
About
Raw Query


BloodHound
Search for a node
Zoom In
Reset Zoom
Zoom Out
Raw Query

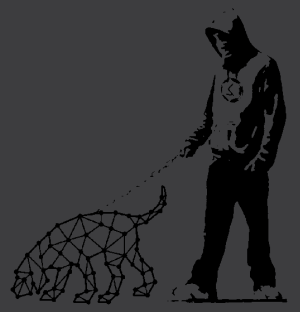

BloodHound
Search for a node
Raw Query Input
Raw Query

ERNW
providing security.

Hands-On: UI Discovery

Click everywhere in the **BloodHound UI** to answer the following questions...

[E2.2]

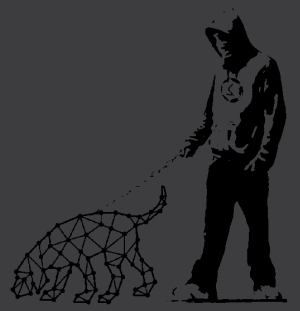


ERNW
providing security.

Hands-On: Nodes & Paths (UI)

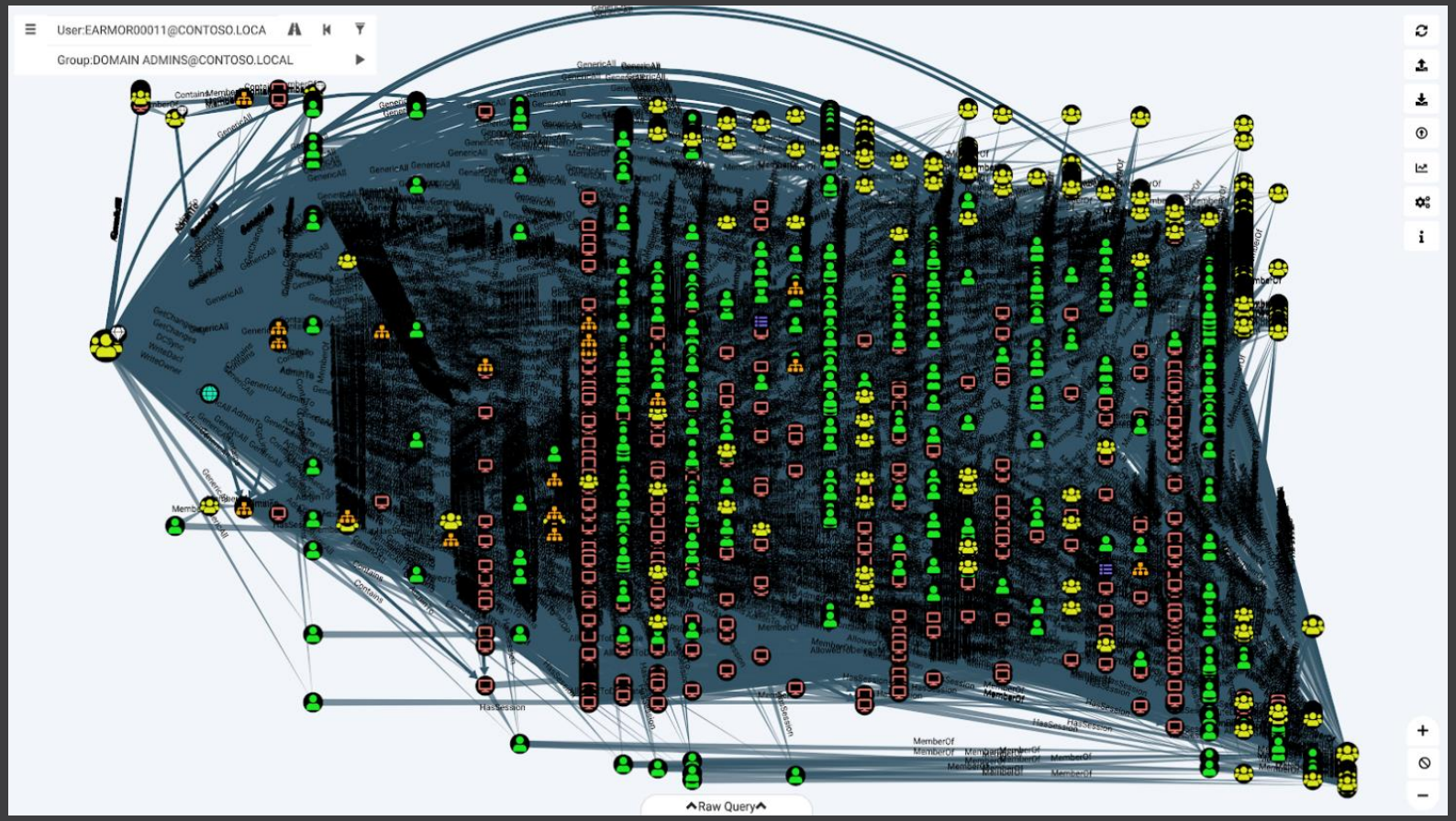
Click in **BloodHound UI** to answer the following questions...

[E2.3 + E2.4]

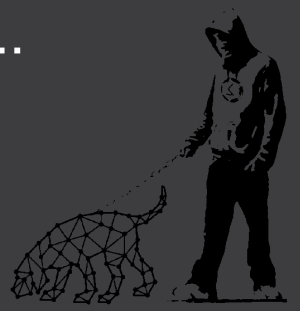


ERNW
providing security.

Data – too much data...



How to navigate all this?? **LEARN CYPHER**...



ERNW
providing security.

M3 – Cypher Basics

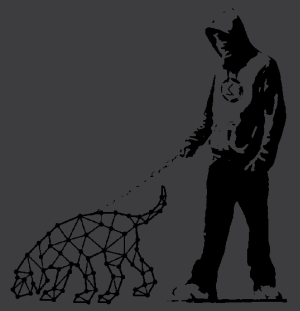
- What is Cypher
- Node Queries
- Path Queries
- Tips & tricks

ERNW
providing security.

What is Cypher?

Cypher is the neo4j DB query language.

- Not specific to BloodHound
- Specific to neo4j
- Quite widely used (info ++ online)
- Easy to get started
- Powerful but hard to master
- Fun ASCII like syntax

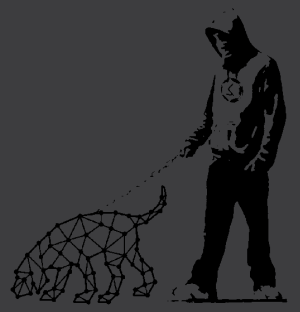


ERNW
providing security.

Node Queries - Basic

Example of basic Node Queries

```
// All Nodes
MATCH (x) RETURN x

// All User Nodes
MATCH (x:User) RETURN x

// Node by Property
MATCH (x:User {name: 'BOB@DEMO.LAB'}) RETURN x
```

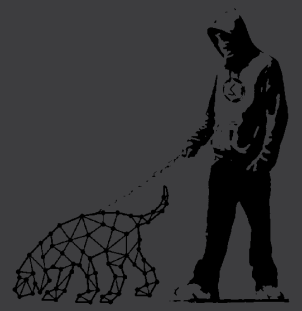


ERNW
providing security.

Path Queries - Basic

Example of Basic Path Query

```
// Path User Bob to DA
MATCH (u:User {name:'BOB@DEMO.LAB'})
MATCH (g:Group {name:'DOMAIN ADMINS@DEMO.LAB'})
MATCH p=shortestPath((u)-[r*1..]->(c))
RETURN p
```

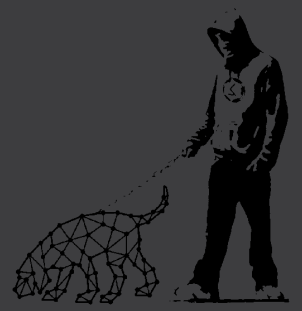


ERNW
providing security.

Path Queries - Basic

Example Path – Owned to HighValue

```
// Path Own to High Value – All Shortest
MATCH (u:User {owned:true})
MATCH (g:Group {highvalue:true})
MATCH p=allShortestPaths((c)-[r*1..]->(u))
RETURN p
```



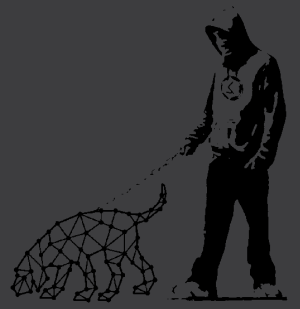
ERNW
providing security.

Filtering - WHERE

The WHERE clause can be used to filter after a MATCH:

```
MATCH (x:User {name: 'BOB@DEMO.LAB'}) RETURN x
// same as
MATCH (x:User)
WHERE x.name='BOB@DEMO.LAB'
RETURN x
```

WHERE can be used with other operators than equal



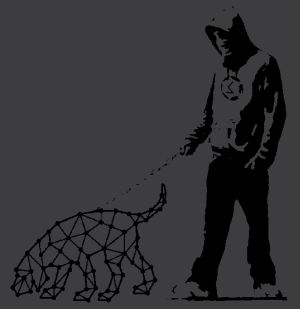
ERNW
providing security.

Comparing - Operators

List of Comparaison Operators:

OPERATOR	SYNTAX
Is Equal To	=
Is Not Equal To	<>
Is Less Than	<
Is Greater Than	>
Is Less or Equal	<=
Is Greater or Equal	>=
Is Null	IS NULL
Is Not Null	IS NOT NULL
Prefix Search*	STARTS WITH
Suffix Search*	ENDS WITH
Inclusion Search*	CONTAINS
RegEx*	=~

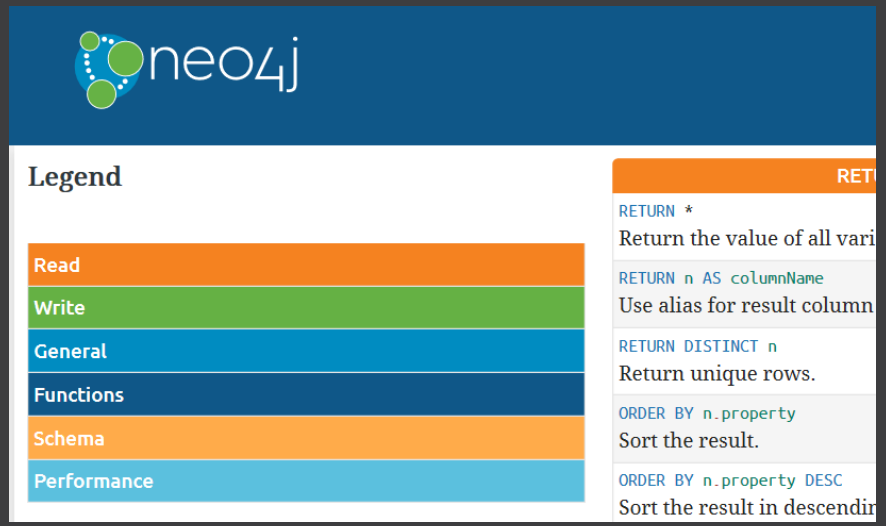
* String specific



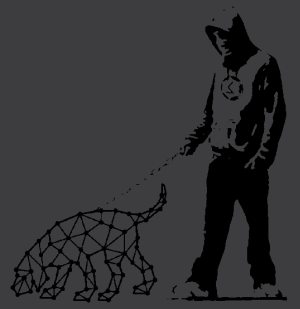
ERNW
providing security.

More Syntax - Ref Card

There are many Functions available...
Check out the **cypher Reference Card** for a quick overview...



Ref: https://neo4j.com/docs/cypher-refcard/current/

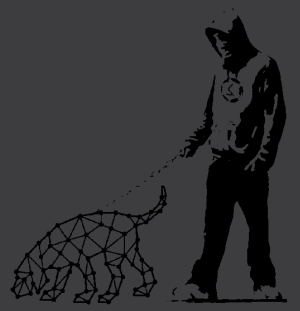


ERNW
providing security.

Hands-On: Node Queries

Use the **Cypher** to answer the following questions on nodes...

[E3.1]

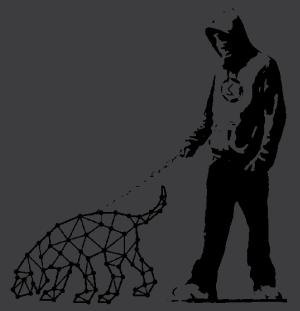


ERNW
providing security.

Hands-On: Path Queries

Use the **Cypher** to answer the following questions on paths...

[E3.2]



ERNW
providing security.

M4 – BloodHound Advanced

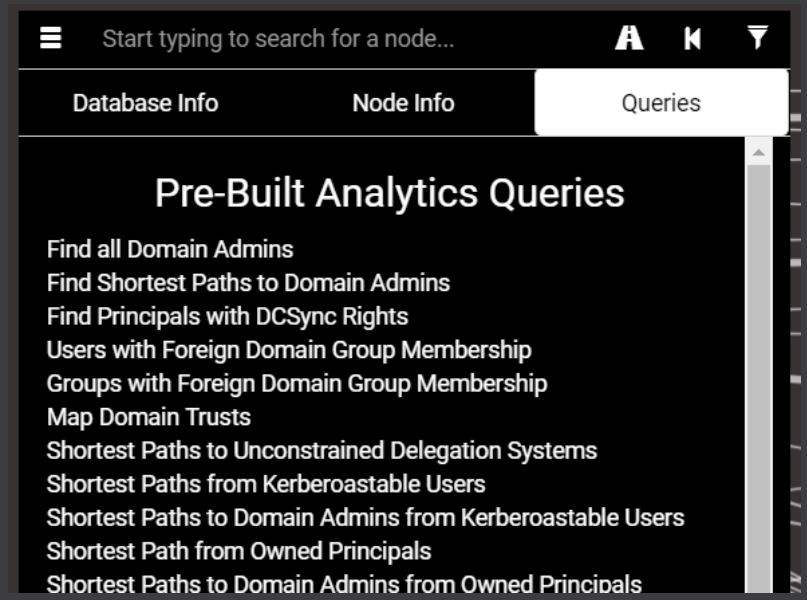
- Build-In Queries
- Custom Queries
- Attack Path Reduction Methodology
- Tips & tricks

ERNW
providing security.

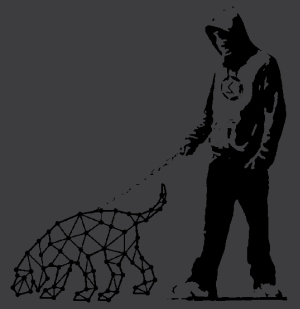
Build-In Queries

Many advanced queries built-in to UI

- DA members/Path to DA
- Kerberoastable
- DC Sync
- ...



[Turn debug mode on to visualize query syntax]

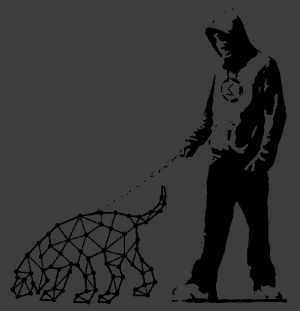


ERNW
providing security.

Hands-On: Build-In Qs

With the Debug mode turned On, navigate to the query tab and answer the following questions...

[E4.1]

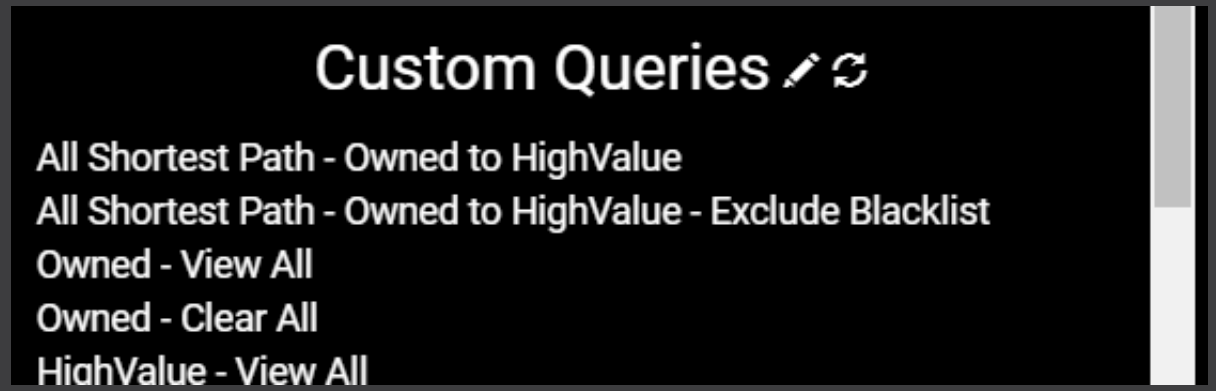


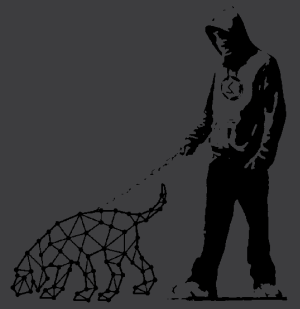
ERNW
providing security.

Custom Queries

Can be added to UI to match specific environment / needs

- Click on pen icon to add queries
- Remember to save when modifying
- Click on refresh icon after adding new query



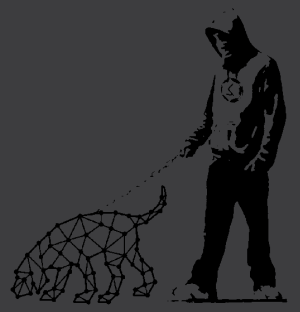


ERNW
providing security.

Hands-On: Custom Qs

Click on the Pen Icon and add a custom query to the UI...

[E4.2]

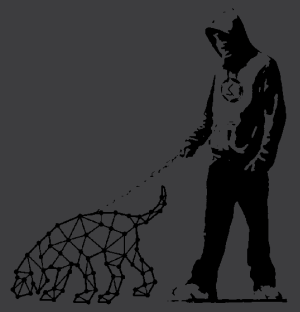


ERNW
providing security.

Attack Path Reduction

BloodHound can (should) be used for defense

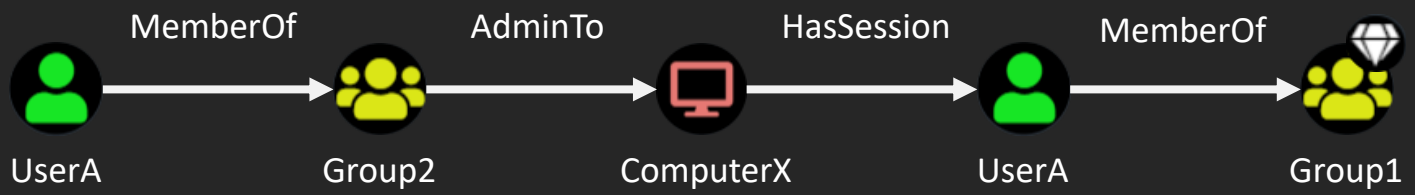
- Think in Graph
- Visualize what attacker would see
- Understand how attacker would move
- Identify weak points and misconfigurations
- Simulate consequences of changes

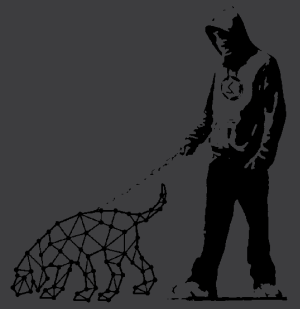


ERNW
providing security.

Attack Path Reduction

Basic Example of Tier Model Breach:

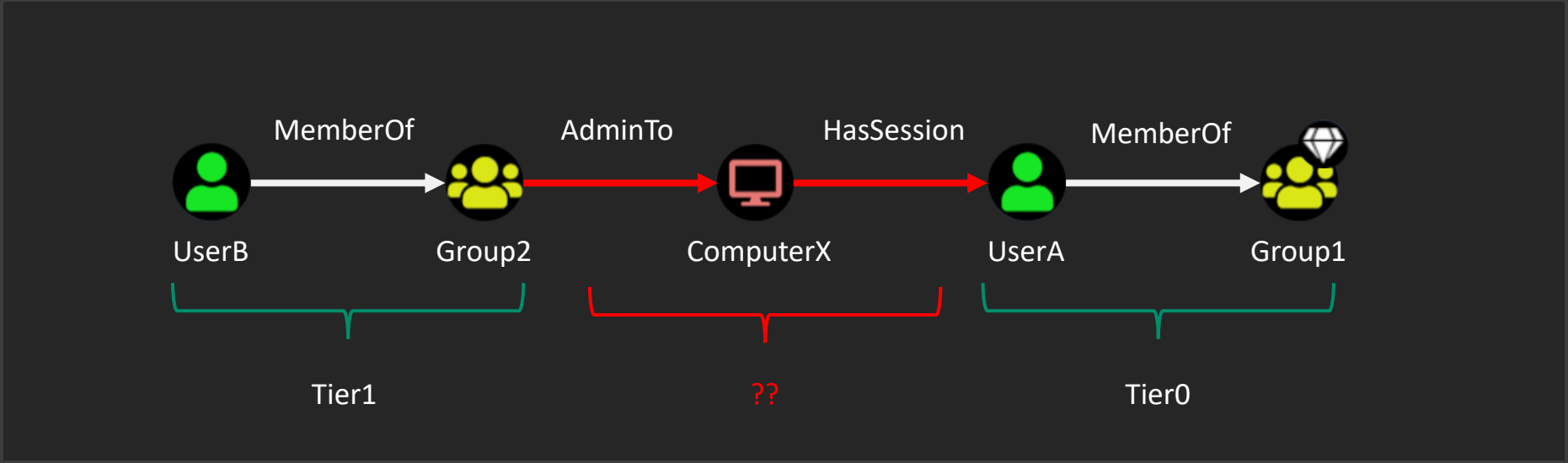




ERNW
providing security.

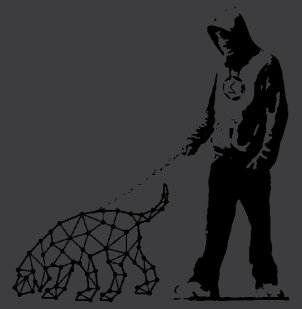
Attack Path Reduction

Basic Example of Tier Model Breach:



Control restriction? -> | <- Login Restriction?

(Asset Classification ComputerX ?)



ERNW
providing security.

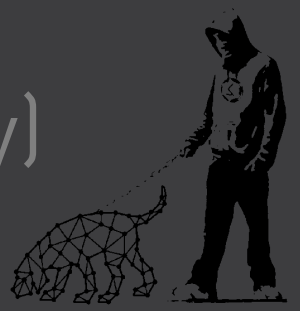
Attack Path Reduction

Limitations to be taken in considerations:

- Not a silver bullet

[Limited to data collected at time of collection]

- Not designed to be a monitoring tool
- Iterative process [work in cycles]
- Requires solid Asset Classification
- Can be overwhelming at first [where to start?]
- Remediation not always possible (politics/legacy)

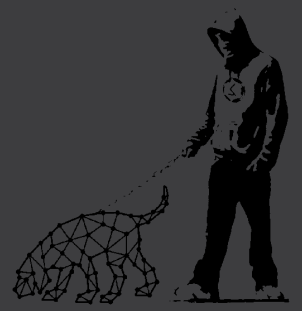


ERNW
providing security.

Attack Path Reduction

Methodology:

- Start with low hanging fruits
  (e.g. Group Membership DA // Domain Root Object ACL)
- Isolate Tier 0 assets first and move away
  [Prevent elevation vs lateral mvmt same tier]
- Focus on domain level first (keep interdomain rels in mind)
- Go one step at a time
- Measure progress to get management support
  [Use metrics]

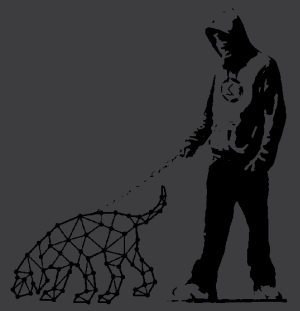


ERNW
providing security.

Tips & Tricks – Large DBs

When working with large datasets

- Use modern hardware with RAM ++
- Collect each domain in separate DB
- Tweak allocated memory and heap size in neo4j config
- Fine tune query syntax for performance [use browser]
- Use PROFILE/EXPLAIN to see what query does
- Ask for help on Slack if needed...



ERNW
providing security.

M5 – Cypher Advanced

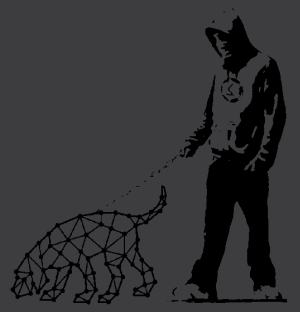
- Adding/Updating/Deleting data
- Calculating Metrics [neo4j browser]
- Debugging Queries

ERNW
providing security.

Adding - Node

The following syntax is used to create a Node & Add props

```
// Create Node
MERGE (u:User {name: 'BOB'})

// Add Props
MATCH (u:User {name: 'BOB'})
SET u.age=23, u.hair='Black'
```

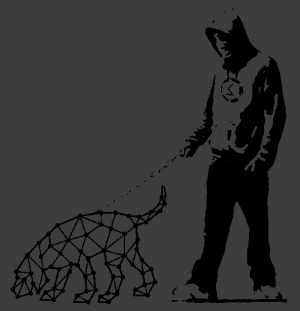


ERNW
providing security.

Adding - Edge

The following syntax is used to create an Edge:

```
// Create Edge Between Nodes
MATCH (b:Human {name: 'BOB'})
MATCH (a:Human {name: 'ALICE'})
MERGE (b)-[r:Likes]->(a)
```

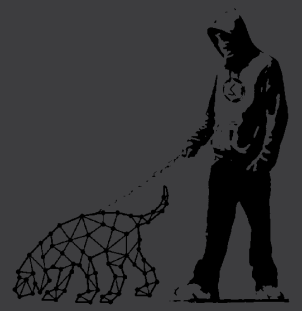


ERNW
providing security.

Deleting - Edge

The following syntax is used to delete an Edge:

```
// Delete Relationship
MATCH (b:Human {name: 'BOB'})-[r:Likes]->(a:Human {name: 'ALICE'})
DELETE r
```



ERNW
providing security.

Deleting - Node

The following syntax is used to delete a Node:

```
// Delete Node
MATCH (u:User {name: 'BOB'})
DETACH DELETE u
```

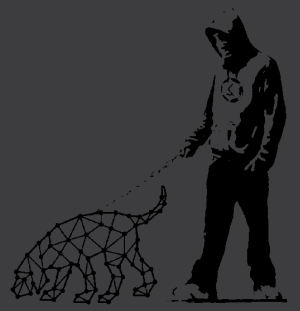
More: https://www.ernw.de/download/BloodHoundWorkshop/ERNW_DogWhispererHandbook.pdf

ERNW
providing security.

Hands-On: Modifying Data

Perform the following actions using **Cypher**...

[E5.1]

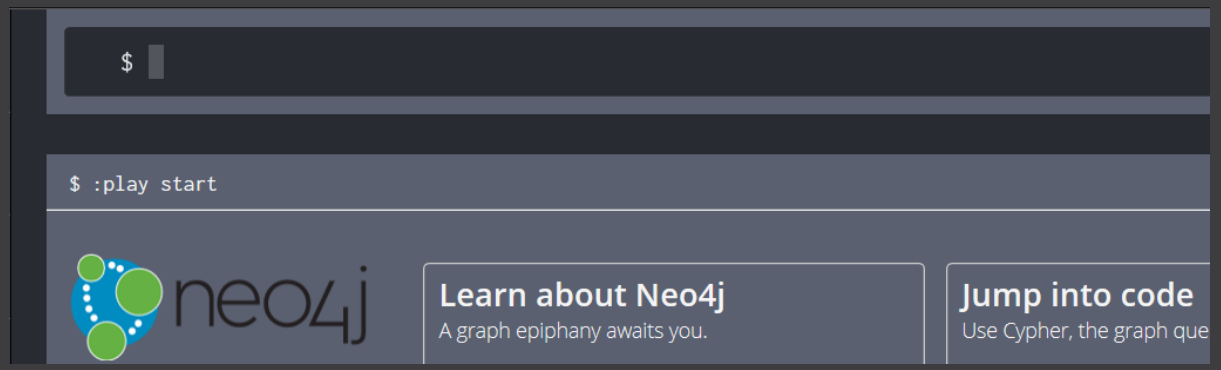


ERNW
providing security.

Neo4j Browser – Cypher IDE

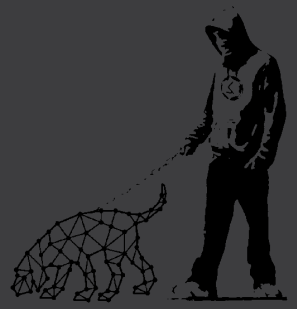
The Neo4j Browser is the best place to work on queries:

- Bigger font
- Syntax coloring
- Error messages
- **Return metrics**



And more...

It is located at http://localhost:7474



ERNW
providing security.

Counting - COUNT()

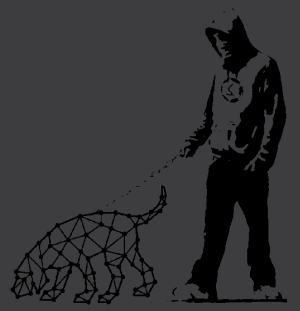
The following syntax can be used to count Nodes

```
MATCH
(g:Group {name: 'DOMAIN ADMINS@SUB.DOMAIN.LOCAL'}),
p=shortestPath((x:User)-[r*1..]->(g))
RETURN COUNT(DISTINCT(x))
```

ERNW
providing security.

Hands-On: Calculating Metrics

Calculate the following in the **neo4j browser**...

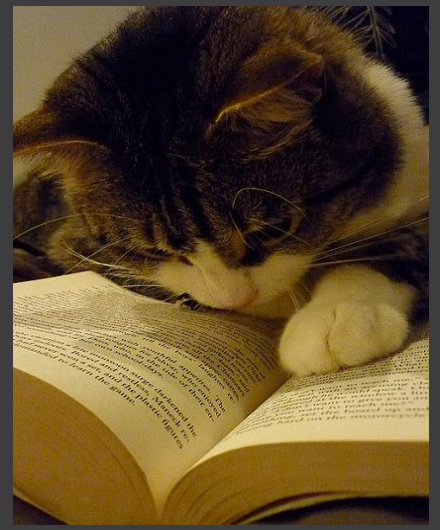


[E5.2]

ERNW
providing security.

Cypher Manual

Full Cypher language reference manual available online

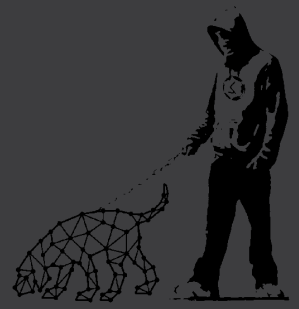


The Neo4j Cypher Manual v3.5

This is the Cypher manual for Neo4j version 3.5, authored by the Neo4j Team.

This manual covers the following areas:

- Chapter 1, *Introduction* — Introducing the Cypher query language.
- Chapter 2, *Syntax* — Learn Cypher query syntax.
- Chapter 3, *Clauses* — Reference of Cypher query clauses.
- Chapter 4, *Functions* — Reference of Cypher query functions.
- Chapter 5, *Schema* — Working with indexes and constraints in Cypher.
- Chapter 6, *Query tuning* — Learn to analyze queries and tune them for performance.
- Chapter 7, *Execution plans* — Cypher execution plans and operators.
- Chapter 8, *Deprecations, additions and compatibility* — An overview of language developments across



Manual: https://neo4j.com/docs/cypher-manual/current/

ERNW
providing security.

Cypher Gallery - Community

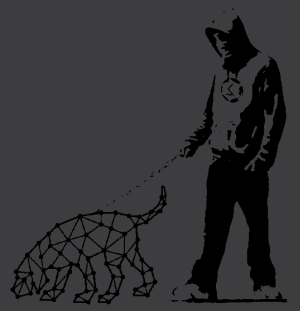
List of Cypher cheats by Community Members

https://gist.github.com/jeffmcjunkin/7b4a67bb7dd0cfbfbd83768f3aa6eb12

https://hausec.com/2019/09/09/bloodhound-cypher-cheatsheet/

https://github.com/BloodHoundAD/BloodHound/wiki/Cypher-Query-Gallery

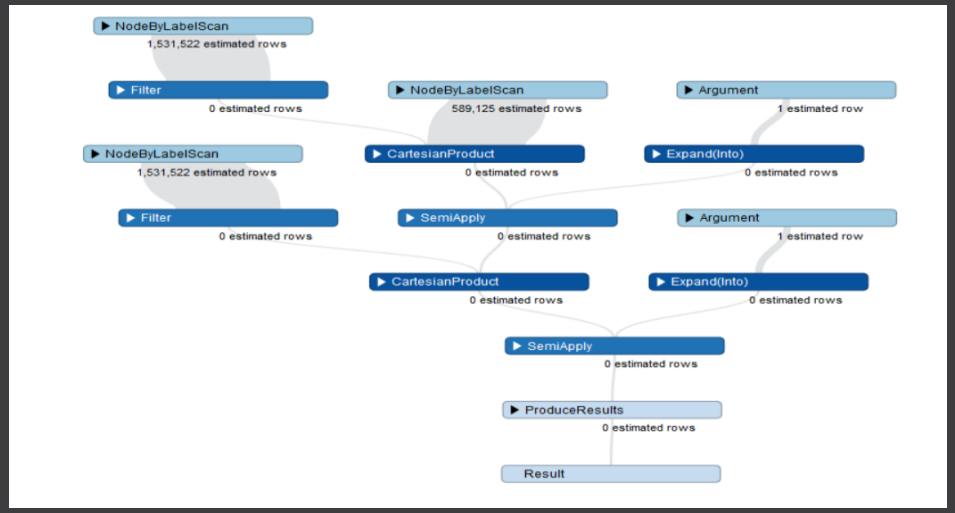
Share your queries on BloodHound slack...



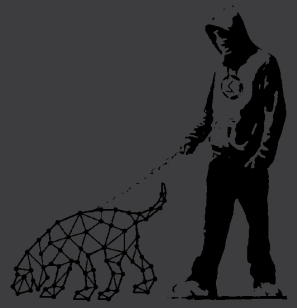
ERNW
providing security.

Query Tuning - Performance

Tip: Add **EXPLAIN** or **PROFILE** in front of your Cypher Query to understand how it performs under the hood... [Browser Only]



Manual: https://neo4j.com/docs/cypher-manual/4.1/query-tuning/



ERNW
providing security.

M6 – Extending BloodHound

- HTTP API basics
- Tool: CypherDog
- Tool: WatchDog

ERNW
providing security.

HTTP API - Basic Call

HTTP API / Cypher transaction API / Begin and commit a transaction in one request

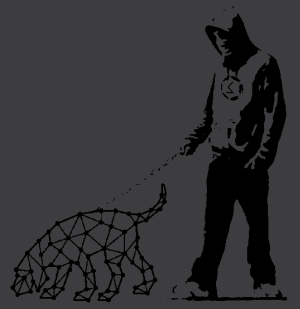
Example request

- **POST** http://localhost:41915/db/neo4j/tx/commit
- **Accept:** application/json;charset=UTF-8
- **Content-Type:** application/json

JavaScript Copy to Clipboard

```
{
  "statements" : [ {
    "statement" : "MATCH (n) WHERE ID(n) = $nodeId RETURN n",
    "parameters" : {
      "nodeId" : 6
    }
  } ]
}
```

[The Neo4j HTTP API Docs v4.2 - HTTP API]

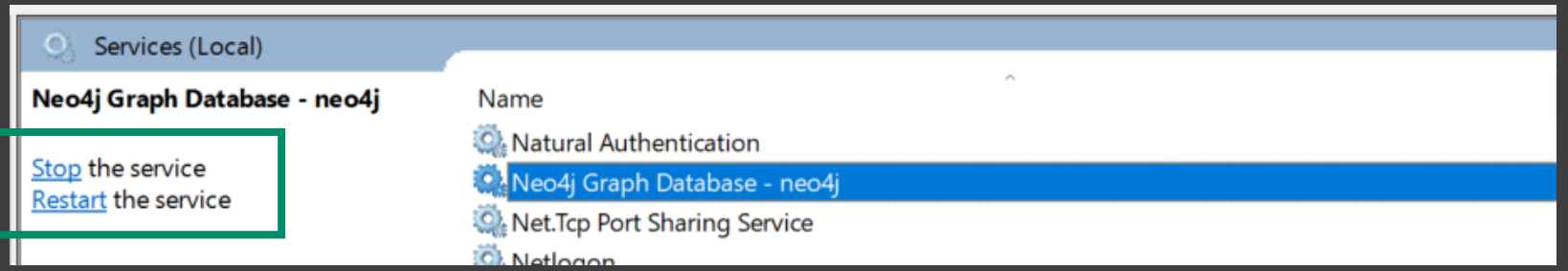


ERNW
providing security.

HTTP API - Setup

Enable **Unauthenticated** API requests [/!\ LocalHost Only /!\]

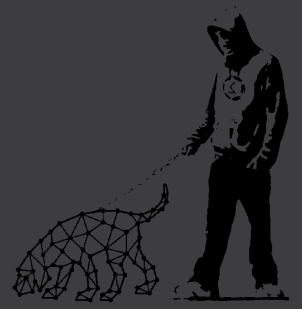
- Stop neo4j service



- Uncomment in neo4j\conf\neo4j.conf

```
24  # Whether requests to Neo4j are authenticated.
25  # To disable authentication, uncomment this line
26  dbms.security.auth_enabled=false
```

- Start neo4j service



ERNW
providing security.

Tool Demos

- CypherDog
- WatchDog

ERNW
providing security.

Invoke-Neo4jCypher - Cmdlet

Invoke-Neo4jCypher is a Cmdlet to send Cypher queries to the BloodHound HTTP API.

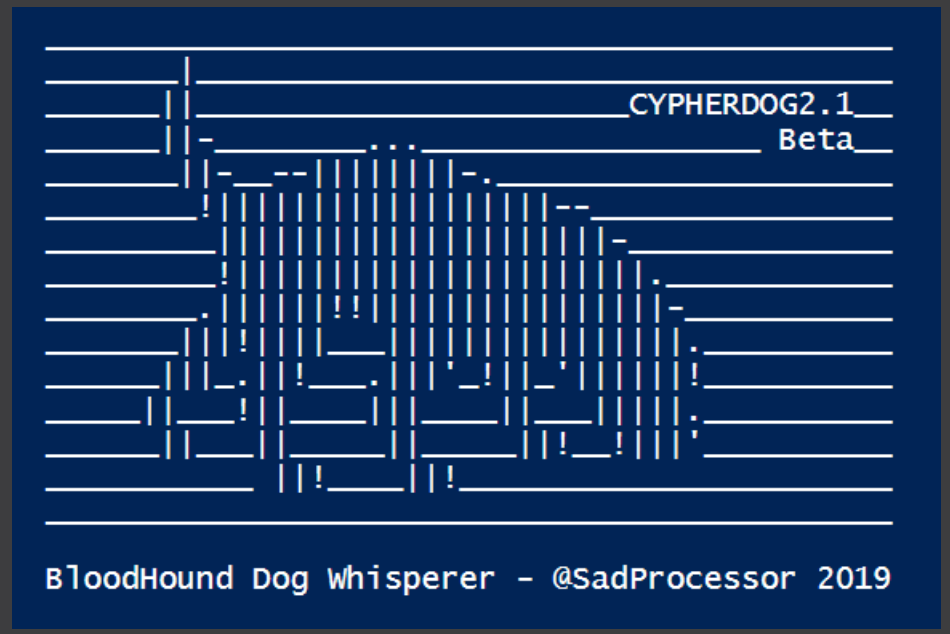
```
> help Invoke-Cypher

NAME
    Invoke-Cypher

SYNOPSIS
    Invoke Cypher


SYNTAX
    Invoke-Cypher [-Query] <String> [[-Params] <Hashtable>] [[-Expand] <String[]>] [<CommonParameters>]


DESCRIPTION
    Post Cypher Query to BloodHound REST API
```

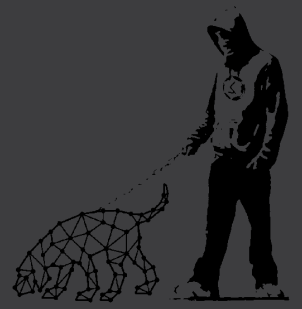
Code: https://github.com/SadProcessor/HandsOnBloodHound/blob/master/Workshop/Invoke-Cypher.ps1

ERNW
providing security.

CypherDog - Demo

CypherDog is a PowerShell BloodHound Client allowing Data Manipulation & Automation



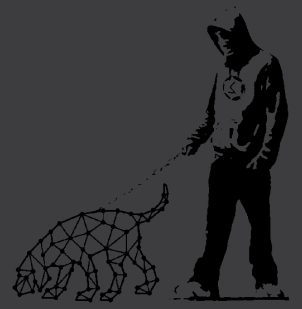


ERNW
providing security.

WatchDog - Demo

WatchDog is an BloodHound Data Scanner [POC/WiP]

```
Top20 Overall - TotalImpact [ 19 : 637 : 100 ]
--------------------------

Type     Name                                    Hit Weight Impact
----     ----                                    --- ------ ------
Group    ENTERPRISE ADMINS@DOMAIN.LOCAL           19    158   24.8
User     SYBLE_LEININGER@DOMAIN.LOCAL             19    143   22.4
Group    ACCOUNT OPERATORS@DOMAIN.LOCAL           18    141   22.1
User     HAZEL_DUNFEE@SUB.DOMAIN.LOCAL            19    104   16.3
Computer WS_4.DOMAIN.LOCAL                        19     95   14.9
Group    REMOTE MANAGEMENT USERS@DOMAIN.LOCAL     19     95   14.9
User     EUGENIE_HITES@DOMAIN.LOCAL               19     86   13.5
Computer WS_17.SUB.DOMAIN.LOCAL                   18     85   13.3
Computer WS_12.SUB.DOMAIN.LOCAL                   19     79   12.4
Group    DOMAIN GUESTS@SUB.DOMAIN.LOCAL           19     79   12.4
Group    DOMAIN ADMINS@DOMAIN.LOCAL               18     77   12.1
Group    DISTRIBUTED COM USERS@SUB.DOMAIN.LOCAL   16     66   10.4
User     SHERWOOD_ENDRES@DOMAIN.LOCAL             19     65   10.2
User     MICHEAL_MAURER@DOMAIN.LOCAL              19     55    8.6
Computer SRV_9.DOMAIN.LOCAL                       19     55    8.6
User     PENNI_ROGAN@DOMAIN.LOCAL                 19     54    8.5
Group    RAS AND IAS SERVERS@SUB.DOMAIN.LOCAL     19     54    8.5
User     SOLEDAD_UHRIG@DOMAIN.LOCAL               19     47    7.4
User     THI_RODKEY@DOMAIN.LOCAL                  19     47    7.4
User     LOREAN_EUGENE@DOMAIN.LOCAL               19     45    7.1
```



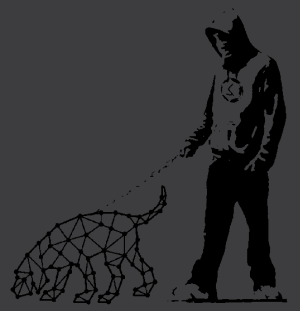
ERNW
providing security.

Hands-On: DIY

Try queries from previous exercises using the **Invoke-Neo4jCypher** cmdlet...

```
[Get-Help Invoke-Neo4jCypher -Full]
```

[E6.1]

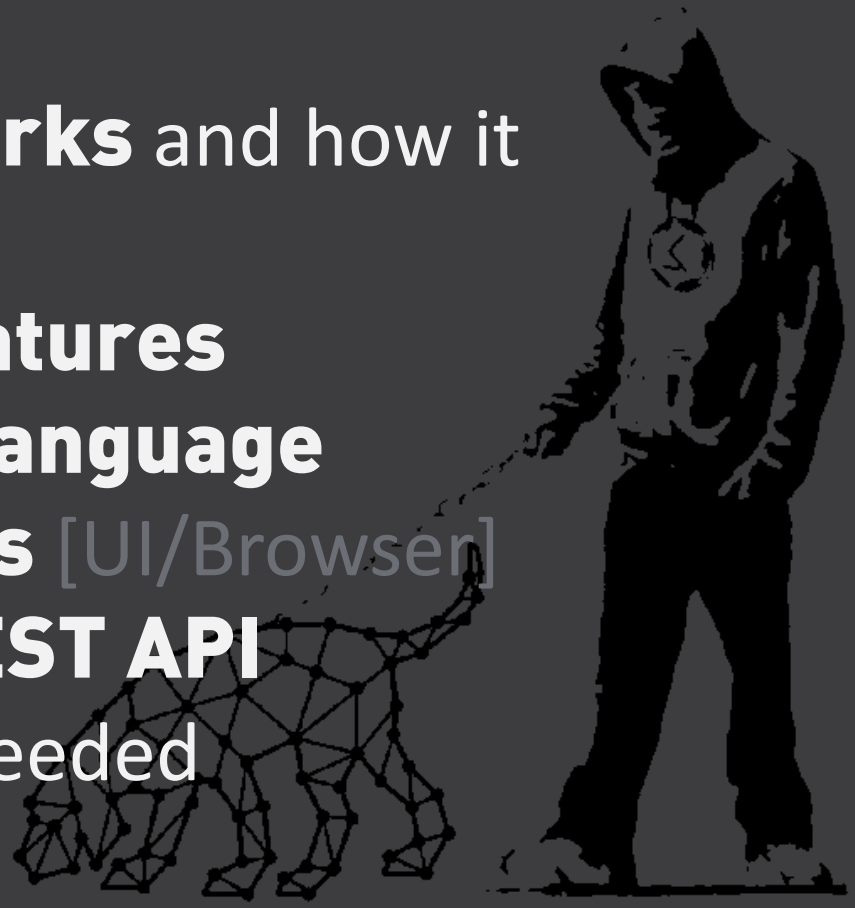


ERNW
providing security.

Goal...?

Now I hope you:

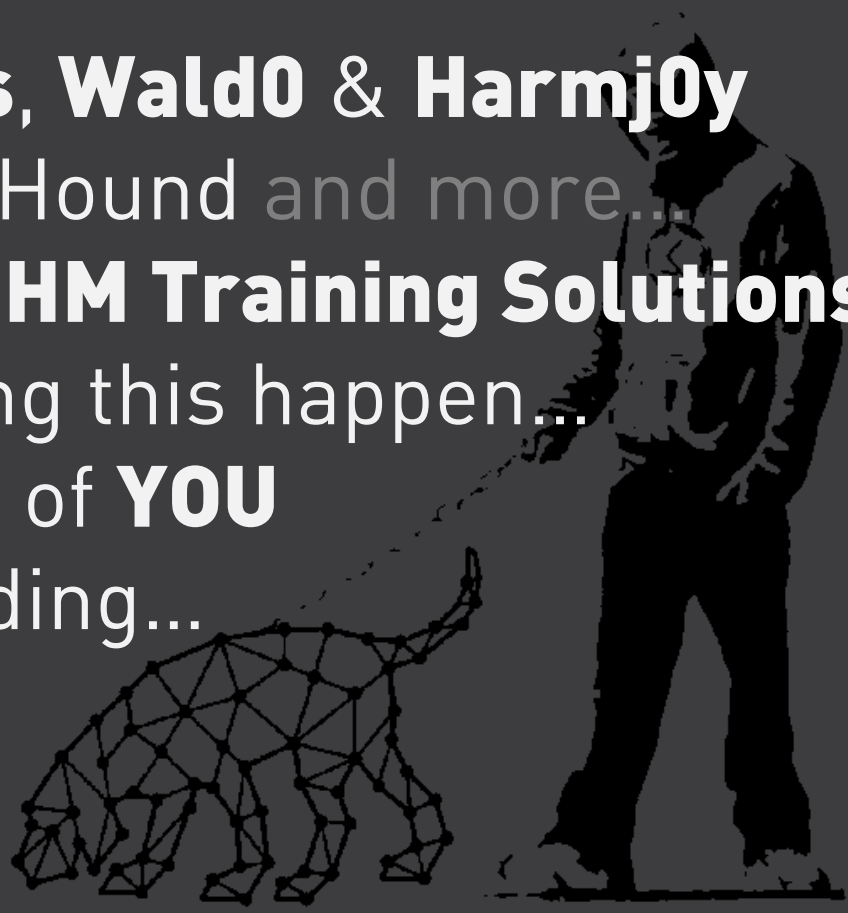
- Understand **how BloodHound works** and how it could be useful for you [Red/Blue]
- Feel familiar with the **UI & tool features**
- Understand the basics of **Cypher language**
- **Create/Debug your own queries** [UI/Browser]
- Understand the workings of the **REST API**
- Know where to find **Info/Help** if needed



ERNW
providing security.

Thank You...

- **CptJesus**, **Wald0** & **Harmj0y**
  for BloodHound and more...
- **ERNW** & **HM Training Solutions**
  for making this happen...
- Each one of **YOU**
  for attending...



Thank You...

ERNW
providing security.

Z1 – Title

Bold

- Bullet1
- Bullet2