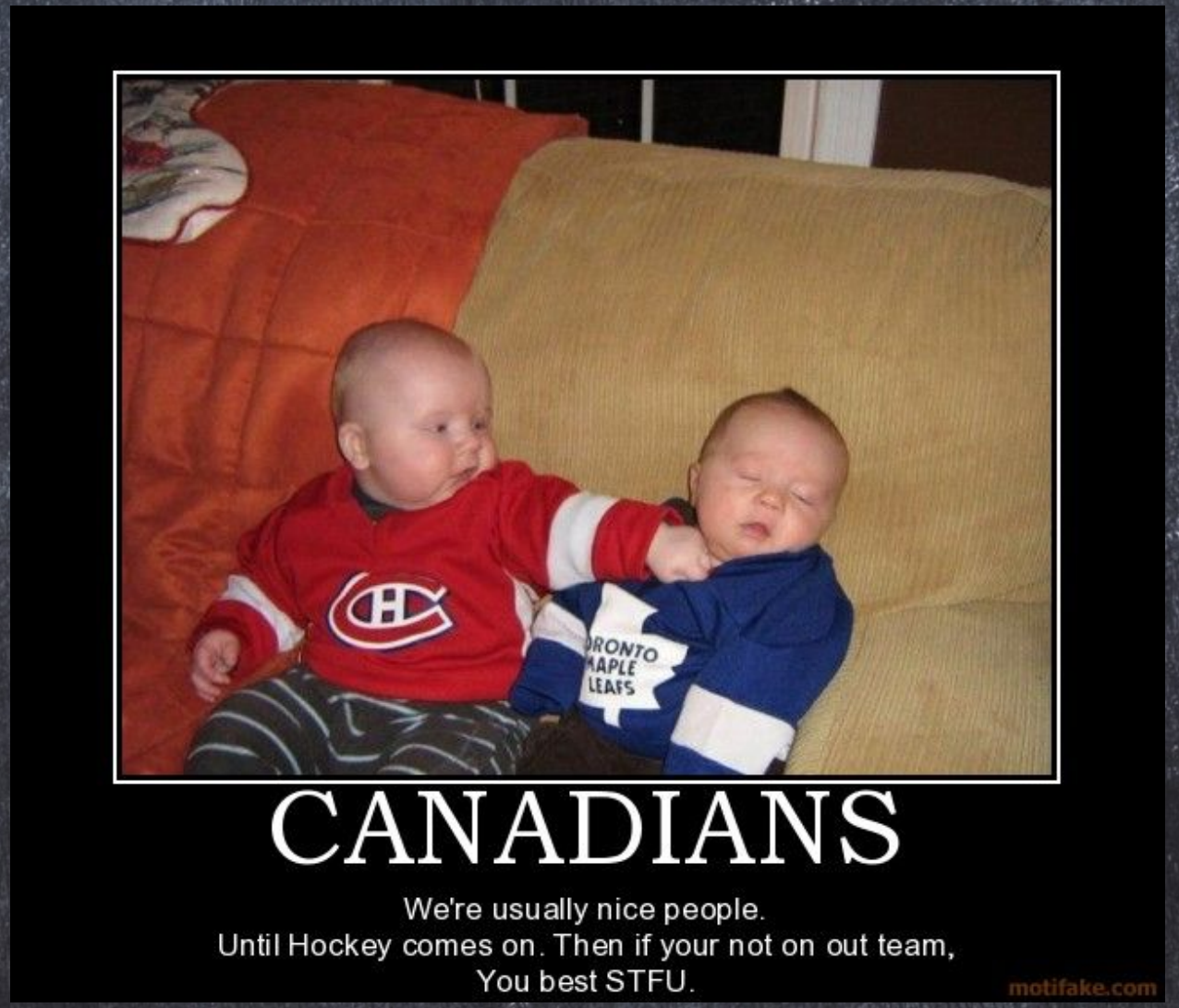
BloodHound From Red to Blue

By Mathieu Saulnier
@ScoubiMTL

BIO

- Work in InfoSec since 2000
- Blue Team since 7 years
- Sr Security Architect at Bell Canada
  - Adversary Detection Team Lead
  - Threat Hunting Team Lead
- Defcon Blue Team Village Volunteer
- Other passions
  - Travelling
  - Wine
- French Canadian



"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."

@JohnLaTwC

git.io/fpfZs

List?

Asset Management > Asset List Create New Asset

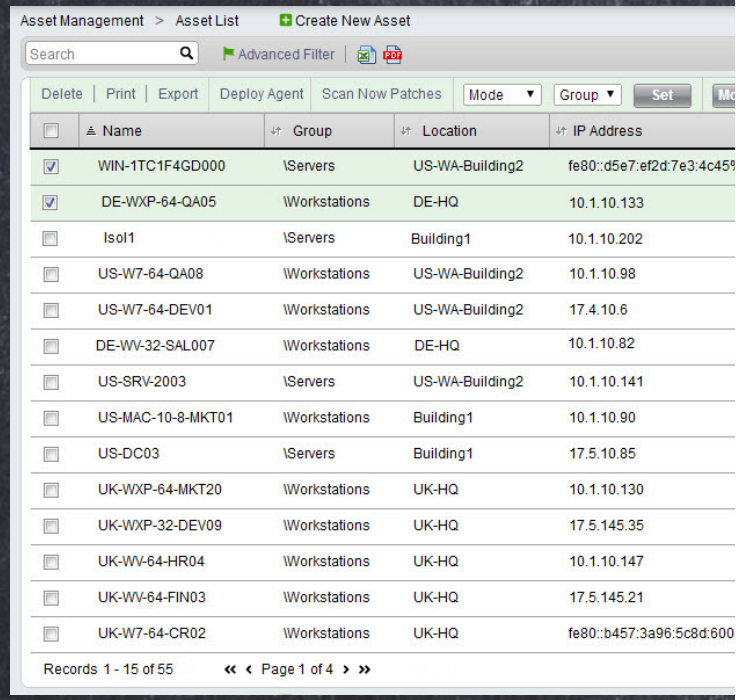
Search Advanced Filter View: DEFAULT Customize View

Delete | Print | Export | Deploy Agent | Scan Now Patches | Mode | Group | Set | More Actions Records 1 - 15 of 55 Page 1 of 4 Show All

Name	Group	Location	IP Address	Type	Manufacturer	Serial	Source
WIN-1TC1F4GD000	\Servers	US-WA-Building2	fe80::d5e7:ef2d:7e3:4c45%8	Server	VMware, Inc.	VMware-42 39 90 e7	Agent
DE-WXP-64-QA05	\Workstations	DE-HQ	10.1.10.133	Workstation	VMware, Inc.	VMware-42 39 75 05	Agent
Isol1	\Servers	Building1	10.1.10.202	Server	Sun		SNMP
US-W7-64-QA08	\Workstations	US-WA-Building2	10.1.10.98	Laptop	Dell Inc.	JHPZ93J	Agent
US-W7-64-DEV01	\Workstations	US-WA-Building2	17.4.10.6	Workstation	IBM		
DE-WV-32-SAL007	\Workstations	DE-HQ	10.1.10.82	Workstation	Phoenix	VMware-42 39 27 73	WMI
US-SRV-2003	\Servers	US-WA-Building2	10.1.10.141	Server	VMware, Inc.	VMware-42 39 50 e4	Agent
US-MAC-10-8-MKT01	\Workstations	Building1	10.1.10.90	Workstation	Apple	C07K91CMDY3H	Agent
US-DC03	\Servers	Building1	17.5.10.85	Server	HP		
UK-WXP-64-MKT20	\Workstations	UK-HQ	10.1.10.130	Workstation	Dell Inc.	4P3FW3J	Agent
UK-WXP-32-DEV09	\Workstations	UK-HQ	17.5.145.35	Workstation	HP		
UK-WV-64-HR04	\Workstations	UK-HQ	10.1.10.147	Workstation	Dell Inc.	JMGX83J	Agent
UK-WV-64-FIN03	\Workstations	UK-HQ	17.5.145.21	Workstation	HP		
UK-W7-64-CR02	\Workstations	UK-HQ	fe80::b457:3a96:5c8d:600a%14	Workstation	VMware, Inc.	VMware-42 39 26 a3	Agent

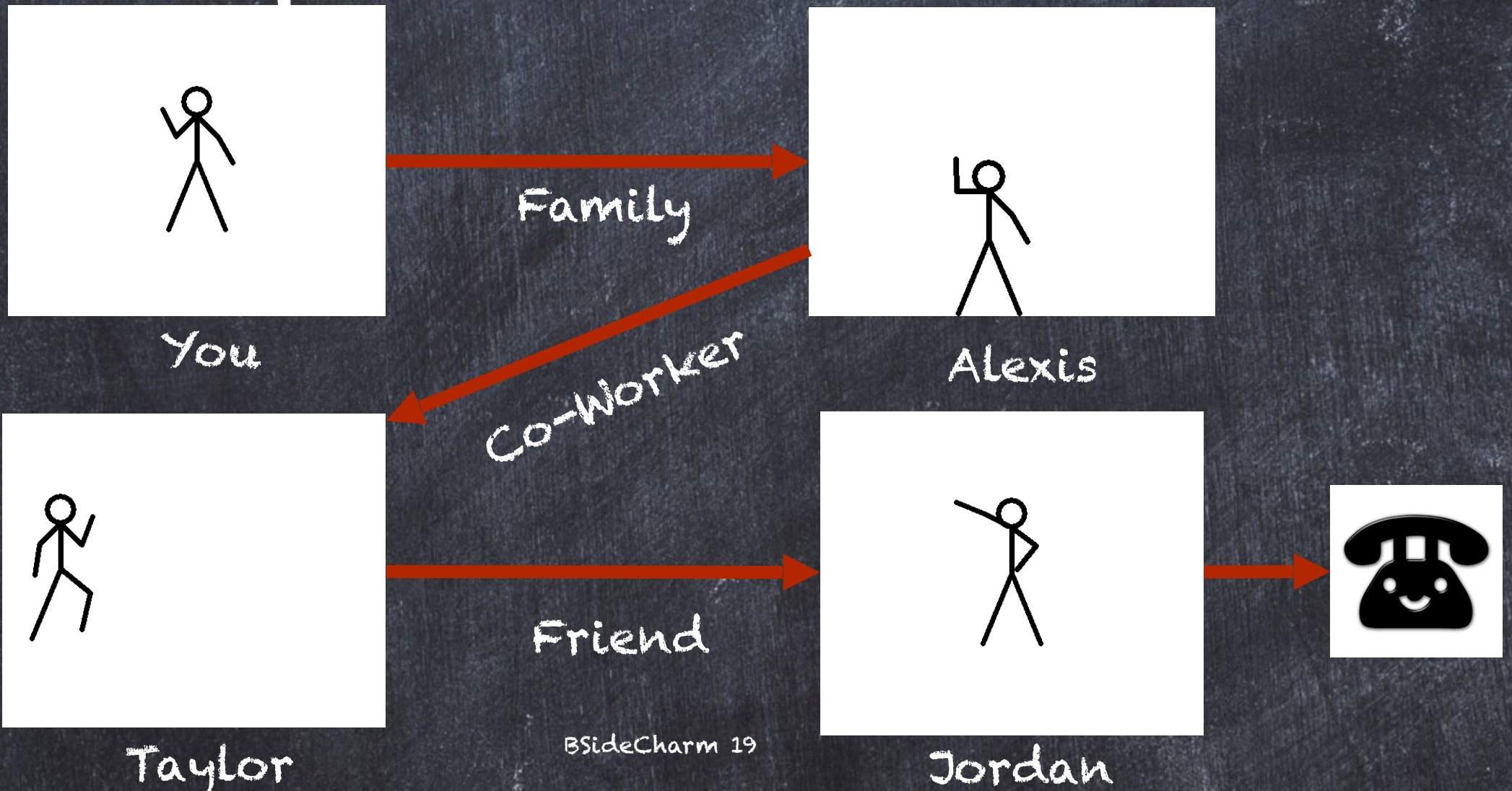
Records 1 - 15 of 55 Page 1 of 4

List?

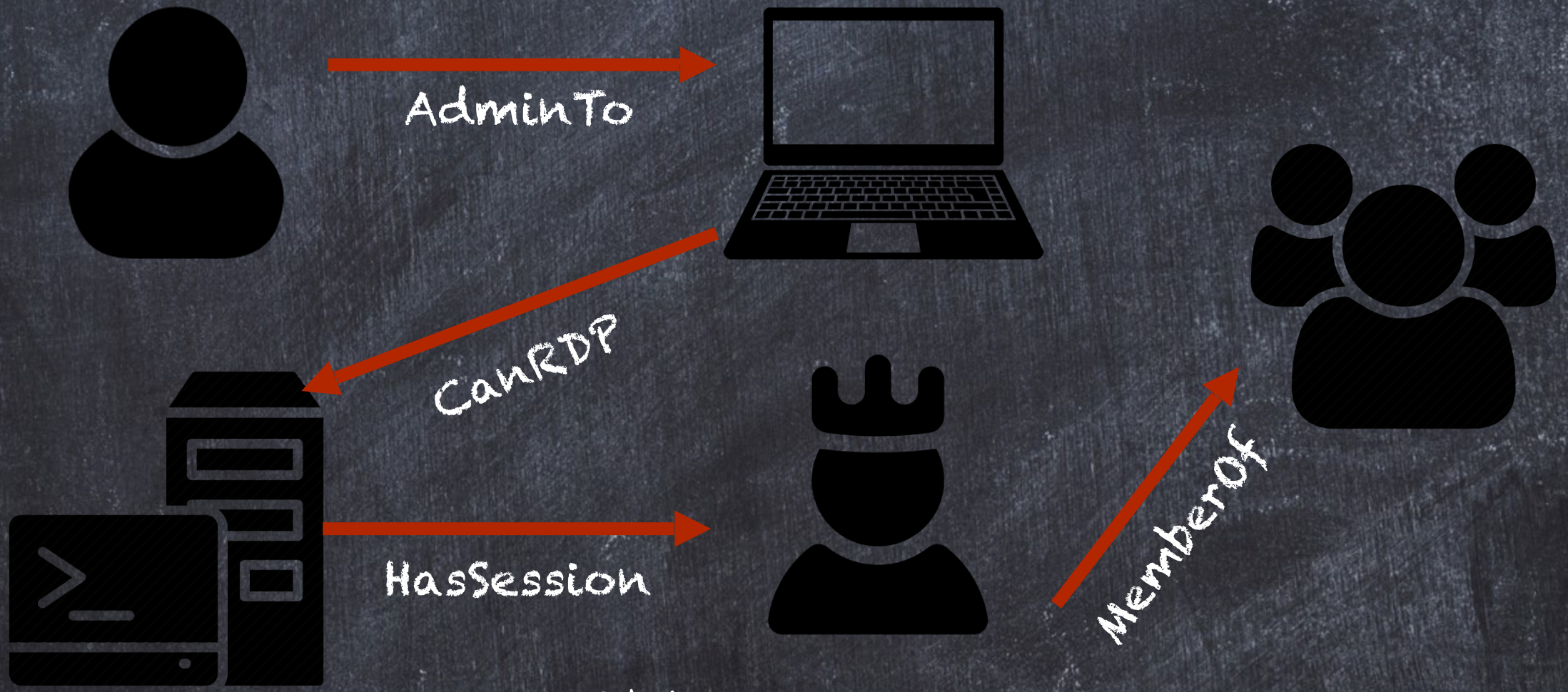


Model	Installation folder
HP Universal Discovery Agent 10	/opt/HP/Discovery/Plugins/
GSKit 8 x64	/usr/local/ibm/gsk8_64/lib64/
Network Security Services Tools 3	/usr/bin/
Lsof 4	/usr/sbin/
Python 2	/usr/bin/
IBM Tivoli Storage Manager API 7	/opt/tivoli/tsm/client/api/bin64/
DynaTrace Agent 6 x64	/opt/jboss/dynatrace/dynatrace-6.1.0/agent/lib64/
Dmidecode 3	/usr/sbin/
Puppet 3	/etc/NetworkManager/dispatcher.d/
IBM Spectrum Protect Client and VSS Requestor 7	/opt/tivoli/tsm/client/ba/bin/
hiera 1	/usr/bin/
Java SE Development Kit 8(64bit)	/opt/jboss/jdk1.8.0_92/bin/
Valgrind 3	/usr/bin/
Network Security Services 3	/usr/lib64/
Facter 1	/usr/bin/

Graph?



Graph?



Overview

What is BloodHound?

* DEF CON 24 - Six Degrees of Domain Admin

  https://youtu.be/Y8qu5NFKyrE

* Blackhat 2017 - The Industrial Revolution of Lateral Movement

  https://youtu.be/lbJPCnjQxCU

* BloodHound is developed by @_wald0, @CptJesus, and @harmjoy.

What does BloodHound do?

* It queries Active Directory
* Import the data in Neo4j
* Show relations between objects

Why use BloodHound?

* For Red
  * Use UI to build attack paths offline
  * Reduce noise on the network
* For Blue
  * Use queries to "busiest" attack paths
  * Destroy paths before they are exploited

The Basics

First Steps

Ingestors

* SharpHound
* Invoke-BloodHound
* bloodhound-python

--CollectionMethod | -C
all | LoggedOn | DCOnly

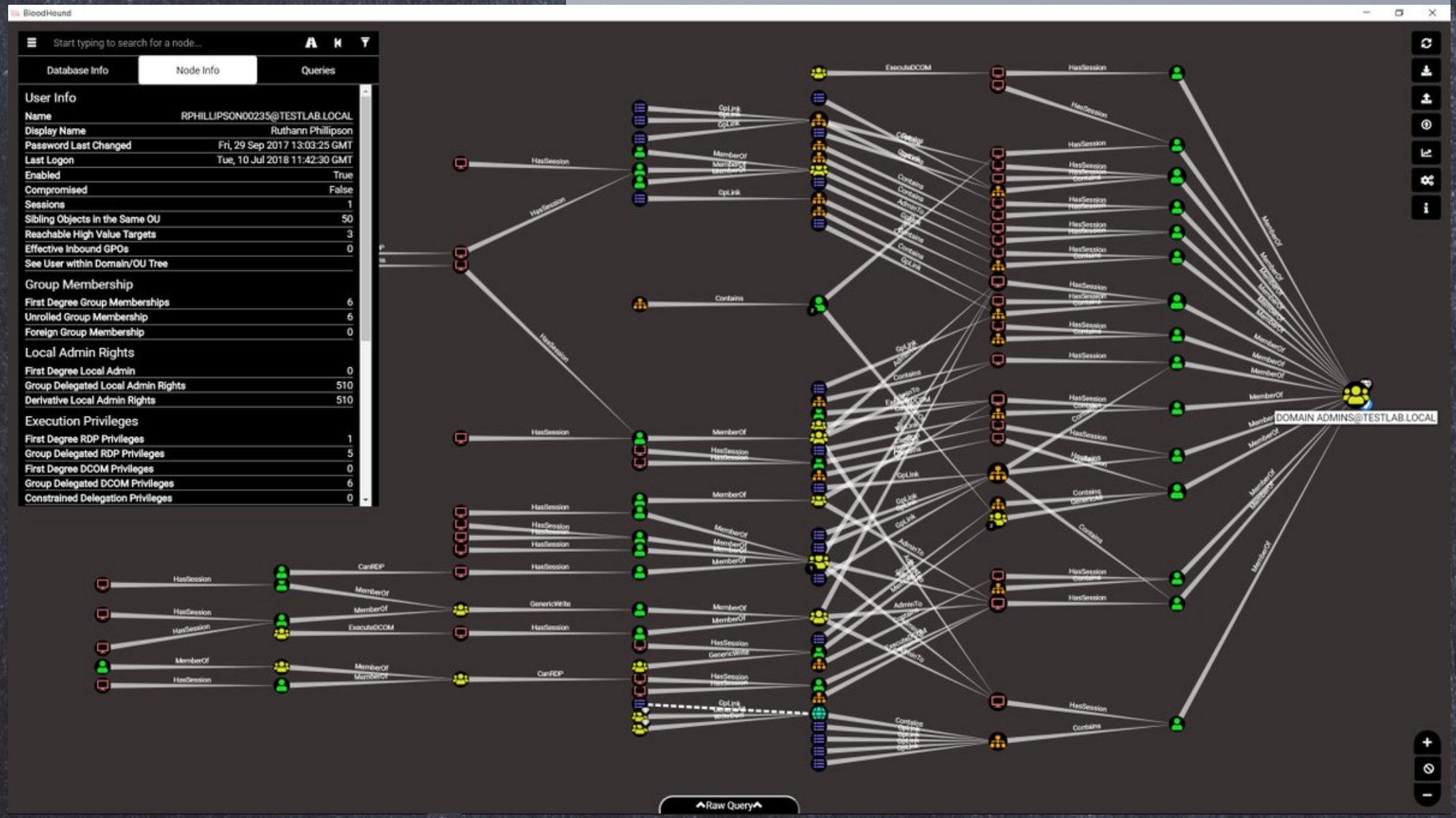
--MaxLoopTime
-c SessionLoop

--SearchForest

Sharphound -h

https://github.com/BloodHoundAD/SharpHound

The GUI


BloodHound
Start typing to search for a node...
Database Info
Node Info
Queries
User Info
Name RPHILLIPSON00235@TESTLAB.LOCAL
Display Name Ruthann Phillipson
Password Last Changed Fri, 29 Sep 2017 13:03:25 GMT
Last Logon Tue, 10 Jul 2018 11:42:30 GMT
Enabled True
Compromised False
Sessions 1
Sibling Objects in the Same OU 50
Reachable High Value Targets 3
Effective Inbound GPOs 0
See User within Domain/OU Tree
Group Membership
First Degree Group Memberships 6
Unrolled Group Membership 6
Foreign Group Membership 0
Local Admin Rights
First Degree Local Admin 0
Group Delegated Local Admin Rights 510
Derivative Local Admin Rights 510
Execution Privileges
First Degree RDP Privileges 1
Group Delegated RDP Privileges 5
First Degree DCOM Privileges 0
Group Delegated DCOM Privileges 6
Constrained Delegation Privileges 0
DOMAIN ADMINS@TESTLAB.LOCAL
Raw Query

Graph Database

Neo4j

Download : https://neo4j.com/download-center/#releases

Launch : $ neo4j-community-3.4.5/bin/neo4j start

Console : http://localhost:7474/

Graph Database

```
$ MATCH (g:Group {highvalue=true}) RETURN g.name
```

To enjoy the full Neo4j Browser experience, we advise you to use Neo4j Browser Sync

x

```
$ MATCH (g:Group {highvalue=true}) RETURN g.name
```

Error

ERROR

Neo.ClientError.Statement.SyntaxError

```
Neo.ClientError.Statement.SyntaxError: Invalid input '=': expected an identifier
character, whitespace, ':' or '}' (line 1, column 26 (offset: 25))
"MATCH (g:Group {highvalue=true}) RETURN g.name"
                          ^
```

Graph Database

```
$ MATCH (g:Group {highvalue:true}) RETURN g.name
```

To enjoy the full Neo4j Browser experience, we advise you to use Neo4j Browser Sync X

$ MATCH (g:Group {highvalue:true}) RETURN g.name

Table | Text | Code

g.name
"DOMAIN ADMINS@TESTLAB.LOCAL"
"DOMAIN CONTROLLERS@TESTLAB.LOCAL"
"ENTERPRISE DOMAIN CONTROLLERS@TESTLAB.LOCAL"
"ADMINISTRATORS@TESTLAB.LOCAL"
"ENTERPRISE ADMINS@TESTLAB.LOCAL"

Customization

Learning to run

Cypher Basics

- MATCH
- Objects : (u:User) u.name
- Relationship : -[:RelType]->
- Path Finding : shortestpath(u)-[:*1..]->(g)
- WHERE
- RETURN

Example

Explicit Where

```
1 MATCH (n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"}),
2 (m:Group {name: "DOMAIN ADMINS@TESTLAB.LOCAL"}),
3 p=shortestPath((n)-[r*1..]->(m))
4 RETURN p
```

Example

Explicit Where

```
1 MATCH (n:Group),(m:Group}),
2 p=shortestPath((n)-[r*1..]->(m))
3 WHERE n.name STARTS WITH "DOMAIN USERS"
4 AND m.name CONTAINS "DOMAIN ADM"
5 RETURN p
```

Example

Explicit

```
1 MATCH (n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"}),
2 (m:Group {name: "DOMAIN ADMINS@TESTLAB.LOCAL"}),
3 p=shortestPath((n)-[r*1..]->(m))
4 RETURN p
```

Where

```
1 MATCH (n:Group),(m:Group}),
2 p=shortestPath((n)-[r*1..]->(m))
3 WHERE n.name STARTS WITH "DOMAIN USERS"
4 AND m.name CONTAINS "DOMAIN ADM"
5 RETURN p
```

Example

Explicit

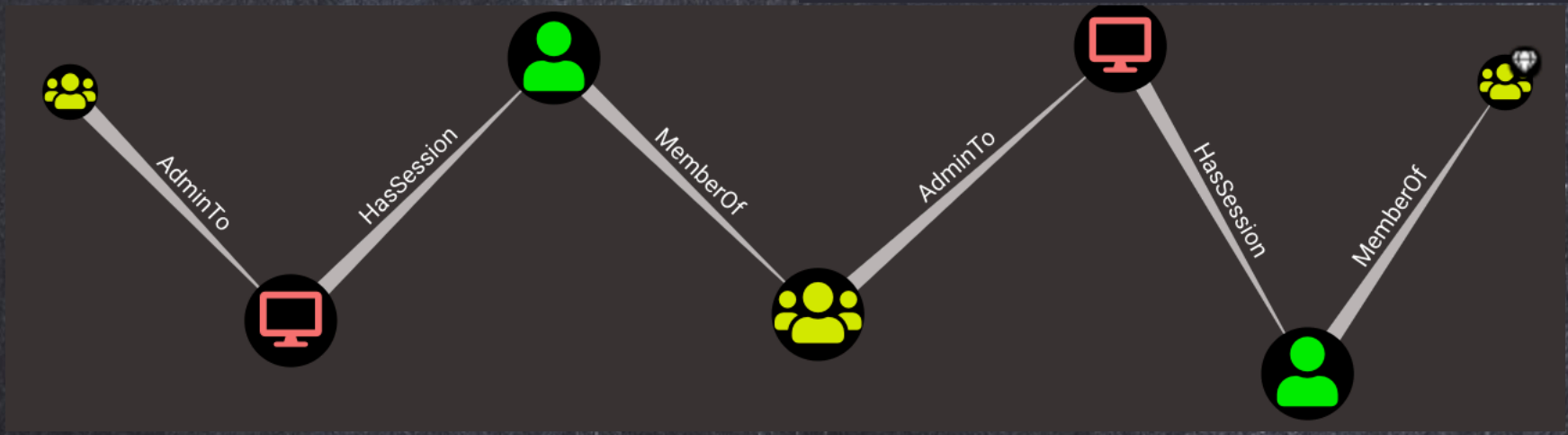
```
1 MATCH (n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"}),
2 (m:Group {name: "DOMAIN ADMINS@TESTLAB.LOCAL"}),
3 p=shortestPath((n)-[r*1..]->(m))
4 RETURN p
```

1 ms

Where

```
1 MATCH (n:Group),(m:Group}),
2 p=shortestPath((n)-[r*1..]->(m))
3 WHERE n.name STARTS WITH "DOMAIN USERS"
4 AND m.name CONTAINS "DOMAIN ADM"
5 RETURN p
```

81 ms



Improving Queries

```
1 MATCH (u:User),(g:Group {highvalue:true}),
2 p=shortestPath((u)-[r*1..]->(g))
3 RETURN COUNT (DISTINCT(u))
```

Improving Queries

WARNING

This feature is deprecated and will be removed in future versions.

Binding relationships to a list in a variable length pattern is deprecated. (Binding a variable length relationship pattern to a variable ('r') is deprecated and will be unsupported in a future version. The recommended way is to bind the whole path to a variable, then extract the relationships: MATCH p = (...)-[...]-(...) WITH *, relationships(p) AS r)

```
p=shortestPath((u)-[r*1..]->(g))
                                                    ^
```

WARNING

This query builds a cartesian product between disconnected patterns.

If a part of a query contains multiple disconnected patterns, this will build a cartesian product between all those parts. This may produce a large amount of data and slow down query processing. While occasionally intended, it may often be possible to reformulate the query that avoids the use of this cross product, perhaps by adding a relationship between the different parts or by using OPTIONAL MATCH (identifier is: (g))

```
EXPLAIN MATCH (u:User),(g:Group {highvalue:true}),
        ^
```

Improving Queries

```
1 MATCH p=shortestPath((u:User)-[*1..]->
2 (g:Group {highvalue:true}))
3 RETURN COUNT (DISTINCT(u))
```

Improving Queries

```
1 MATCH (u:User),(g:Group {highvalue:true}),
2 p=shortestPath((u)-[r*1..]->(g))
3 RETURN COUNT (DISTINCT(u))
```

```
1 MATCH p=shortestPath((u:User)-[*1..]->
2 (g:Group {highvalue:true}))
3 RETURN COUNT (DISTINCT(u))
```

Pro Tip

EXPLAIN

execution plan but not run the statement

PROFILE

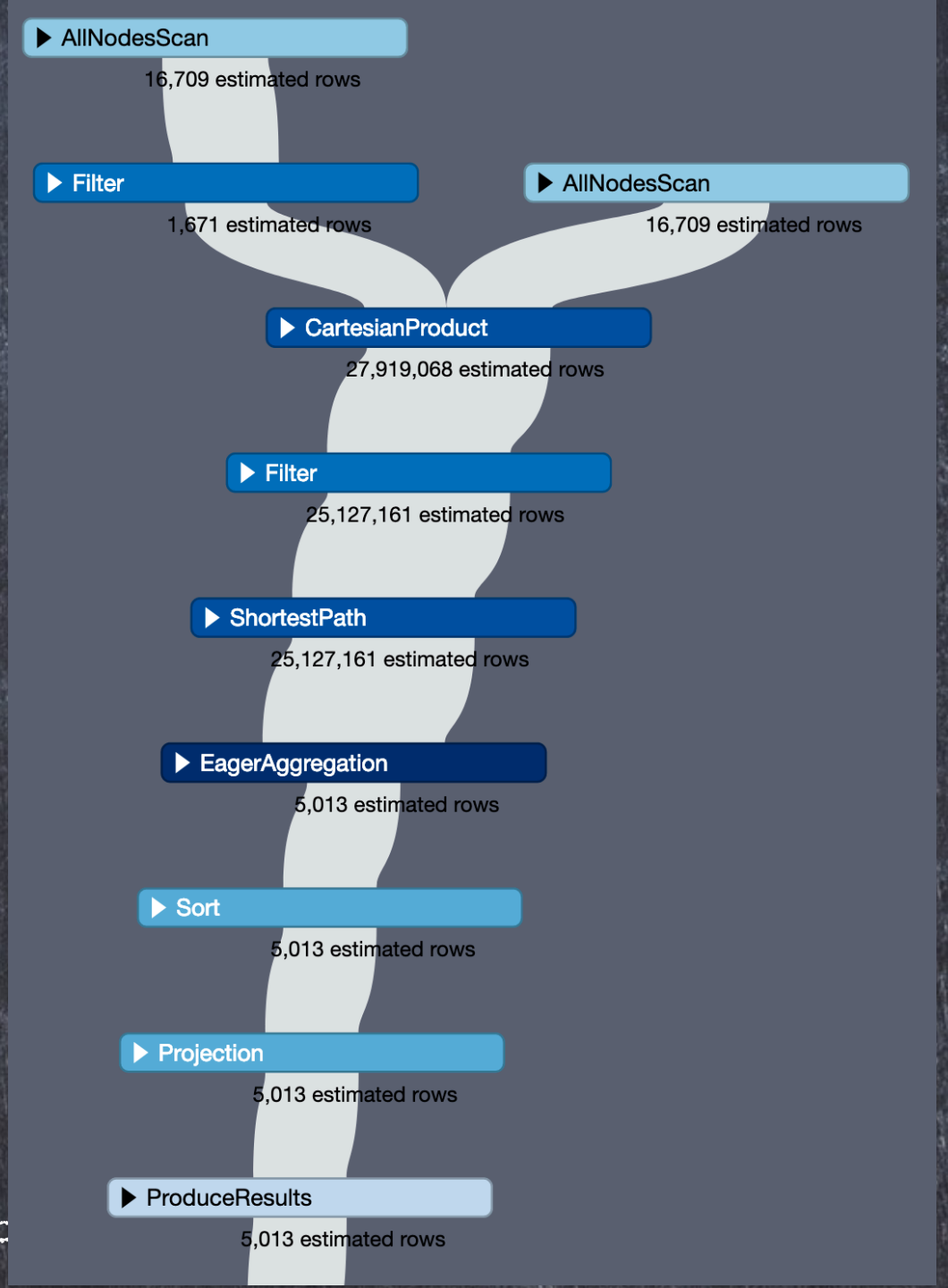
run the statement and see which operators are doing most of the work

Pro Tip

```
1 MATCH p = shortestPath((n)-[*1..]->(m {highvalue:true}))
2 WHERE NOT n = m
3 RETURN DISTINCT(m.name),LABELS(m)[0],COUNT(DISTINCT(n))
4 ORDER BY COUNT(DISTINCT(n)) DESC
```

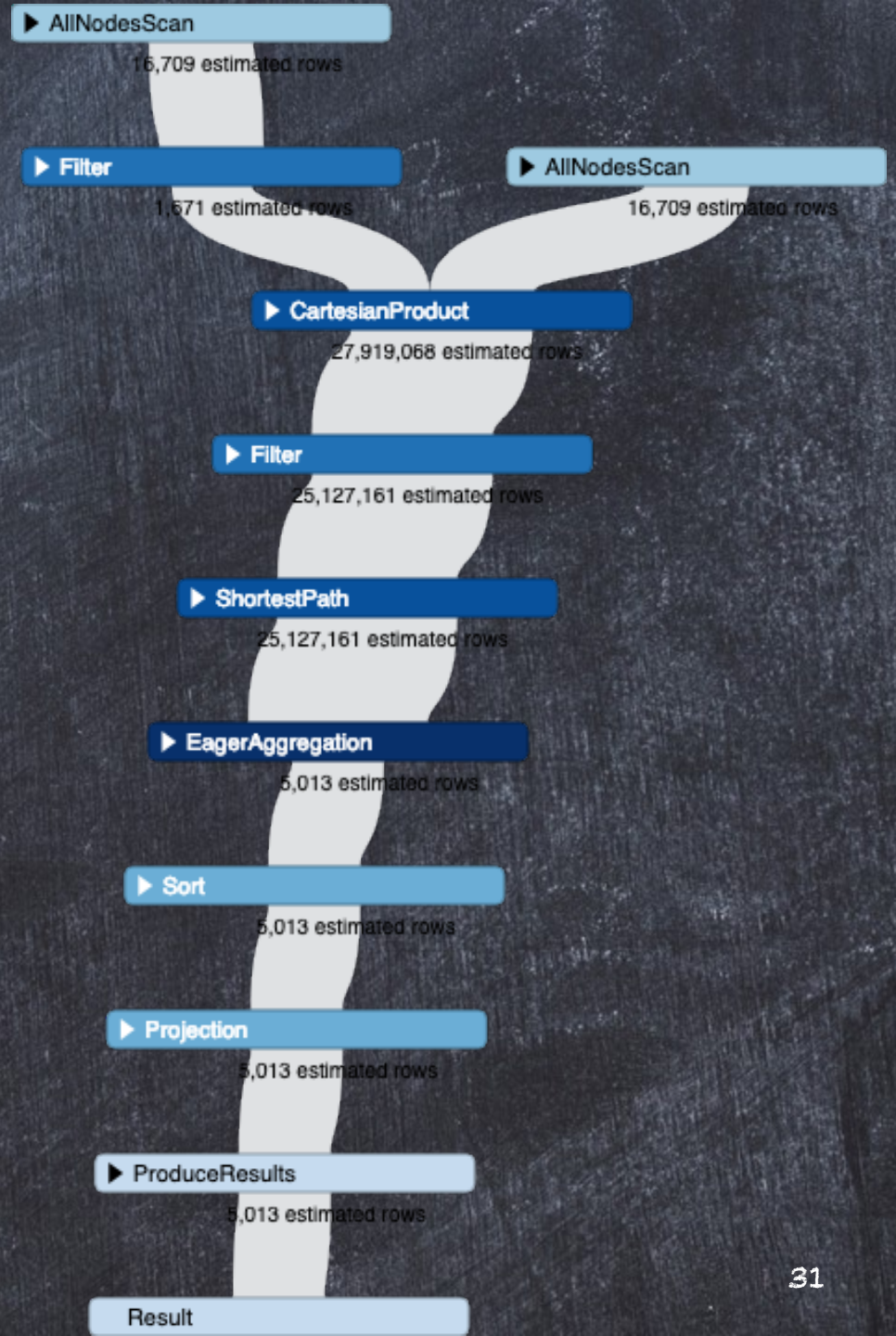
Pro Tip

EXPLAIN MATCH



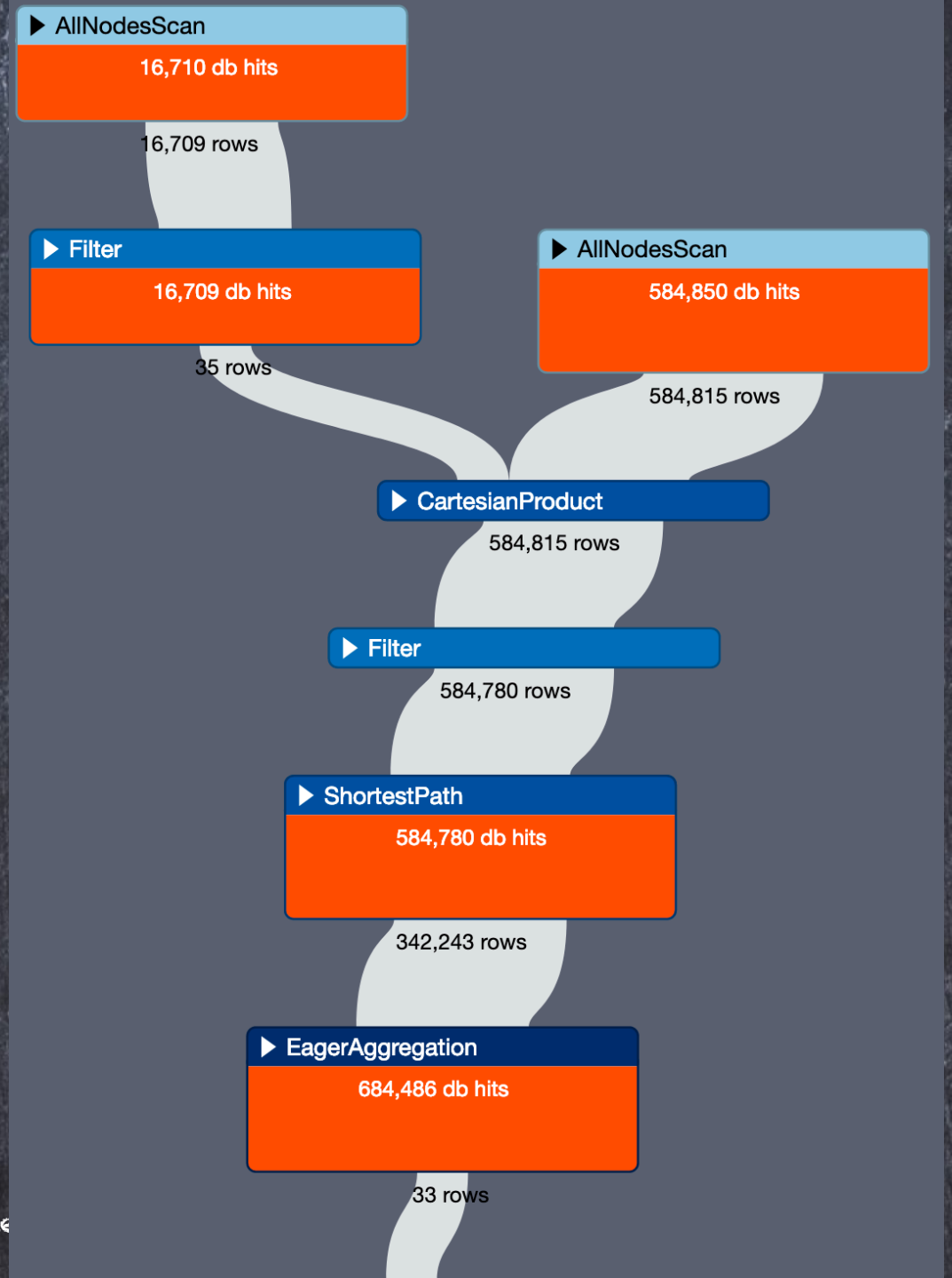
Pro Tip

EXPLAIN



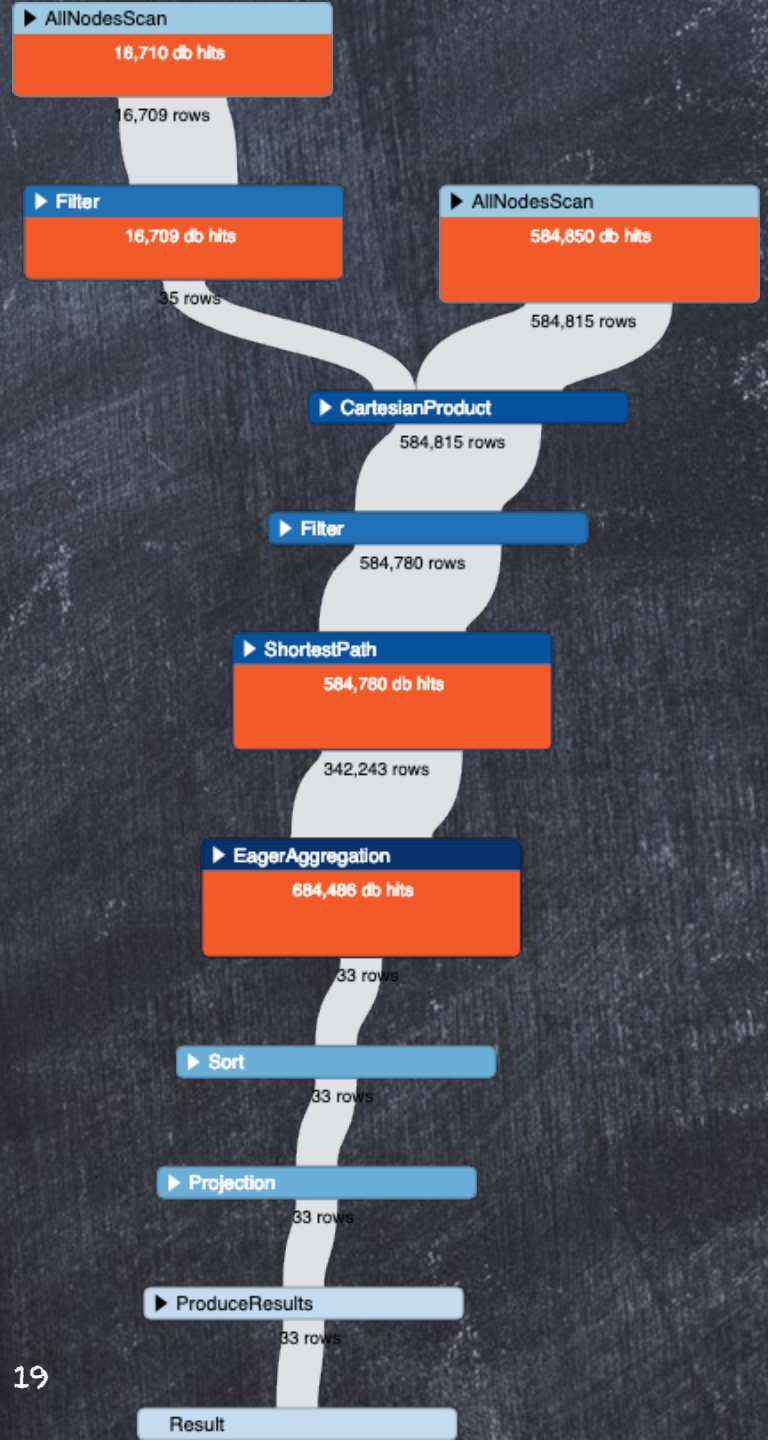
Pro Tip

PROFILE



Pro Tip

PROFILE MATCH



Advanced Queries

```
********** Computer where the most users can RDP to
MATCH (c:Computer)
OPTIONAL MATCH (u1:User)-[:CanRDP]->(c)
OPTIONAL MATCH (u2:User)-[:MemberOf*1..]->(:Group)-[:CanRDP]->(c)
WITH COLLECT(u1) + COLLECT(u2) as tempVar,c
UNWIND tempVar as users
RETURN c.name,COUNT(DISTINCT(users))
ORDER BY COUNT(DISTINCT(users)) DESC
**********

********** Avrage Lenght of Path
MATCH (g:Group {name:'DOMAIN ADMINS@CONTOSO.LOCAL'})
MATCH p = shortestPath((u:User)-[r:AdminTo|MemberOf|HasSession*1..]->(g))
WITH EXTRACT(n in NODES(p) | LABELS(n)[0]) as pathNodes
WITH FILTER(x IN pathNodes WHERE x = "Computer") as filteredPathNodes
RETURN AVG(LENGTH(filteredPathNodes))
**********
```

Useful queries you ~~can run~~

1. Domain Users
    1. Authenticated users

2. Kerberoasting

3. Top 10 X

https://github.com/Scoubi/BloodhoundAD-Queries

1.1 Are Local Admin
1.2 Shortest path to High Value
1.3 Can RDP to
1.4 Other "bad" Rights
2.1 High Value Accounts
2.2 List all
3.1 User with sessions
3.2 Computer with Admin
3.3 Computer with Sessions
3.4 User with Admin Rights

Cypher Cheat Sheet

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

Destroy Paths

Controlled Environment

Create a problem

Create a link

```
1 MERGE (n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 WITH n MERGE (m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
3 WITH n,m MERGE (n)-[:AdminTo]->(m)
```

Create a problem

```
$ MERGE (n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
```

Table

Code

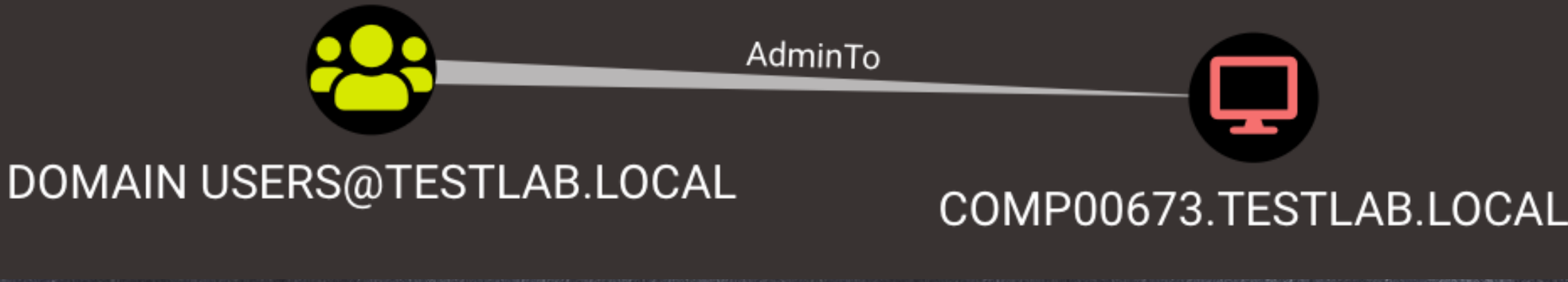
Created 1 relationship, completed after 8 ms.

```
1 MER
2 WIT
3 WIT
```

Test New Relation

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->(m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
3 RETURN p
```

Test New Relation



Filter Out Relation

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->(m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
3 WHERE ALL(x in relationships(p)
4 WHERE type(x) <> "AdminTo")
5 RETURN p
```

Delete a Relation

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->
3 (m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
4 DELETE r
```

Test Remediation

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->(m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
3 WHERE ALL(x in relationships(p)
```

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->
3 (m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
4 RETURN p
```

```
3 (m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
4 DELETE r
```

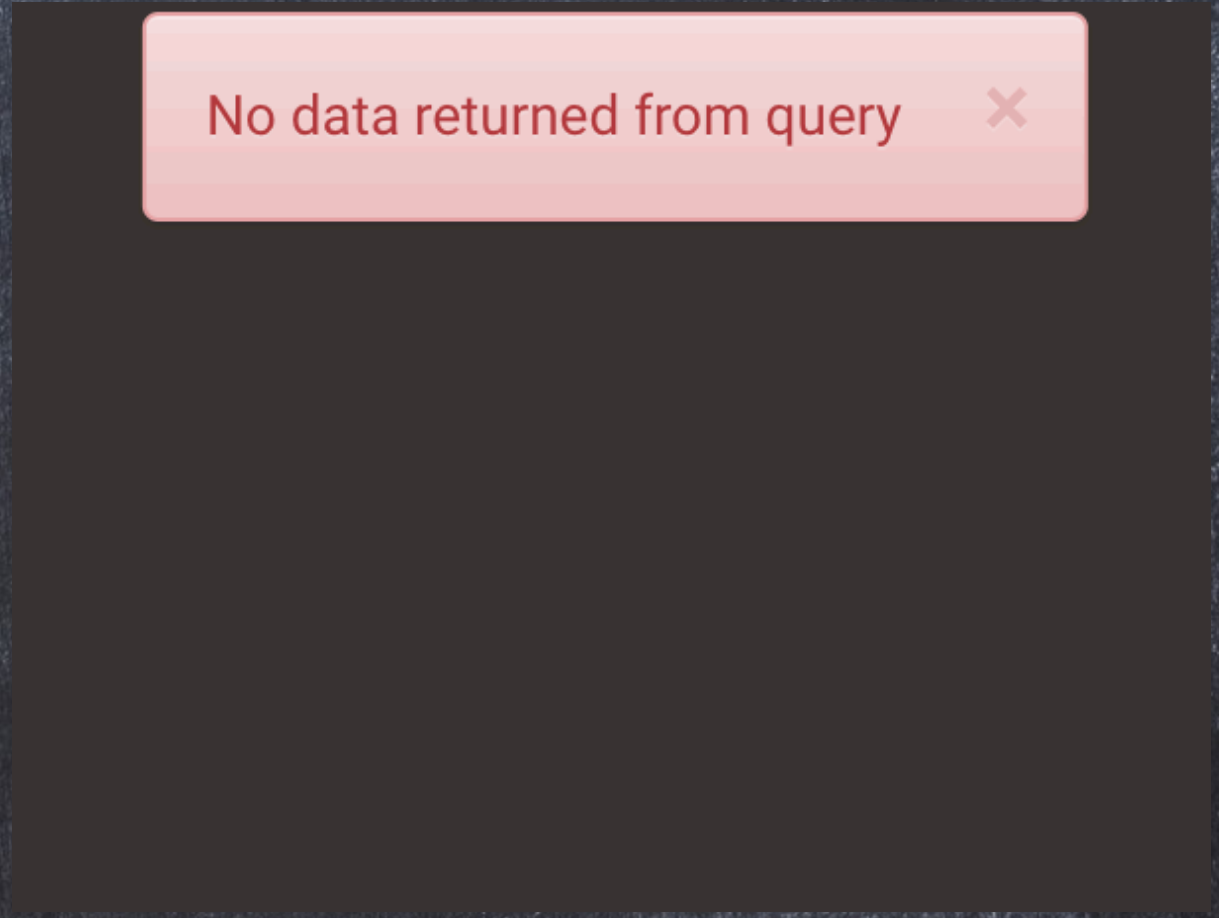
Test remediation

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->(m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
3 WHERE ALL(x in relationships(p)
4 WHERE type(x) <> "AdminTo")
5 RETURN p
```

OR

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->
3 (m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
4 DELETE r
```

```
1 MATCH p=(n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"})
2 -[r:AdminTo]->
3 (m:Computer {name:"COMP00673.TESTLAB.LOCAL"})
4 RETURN p
```



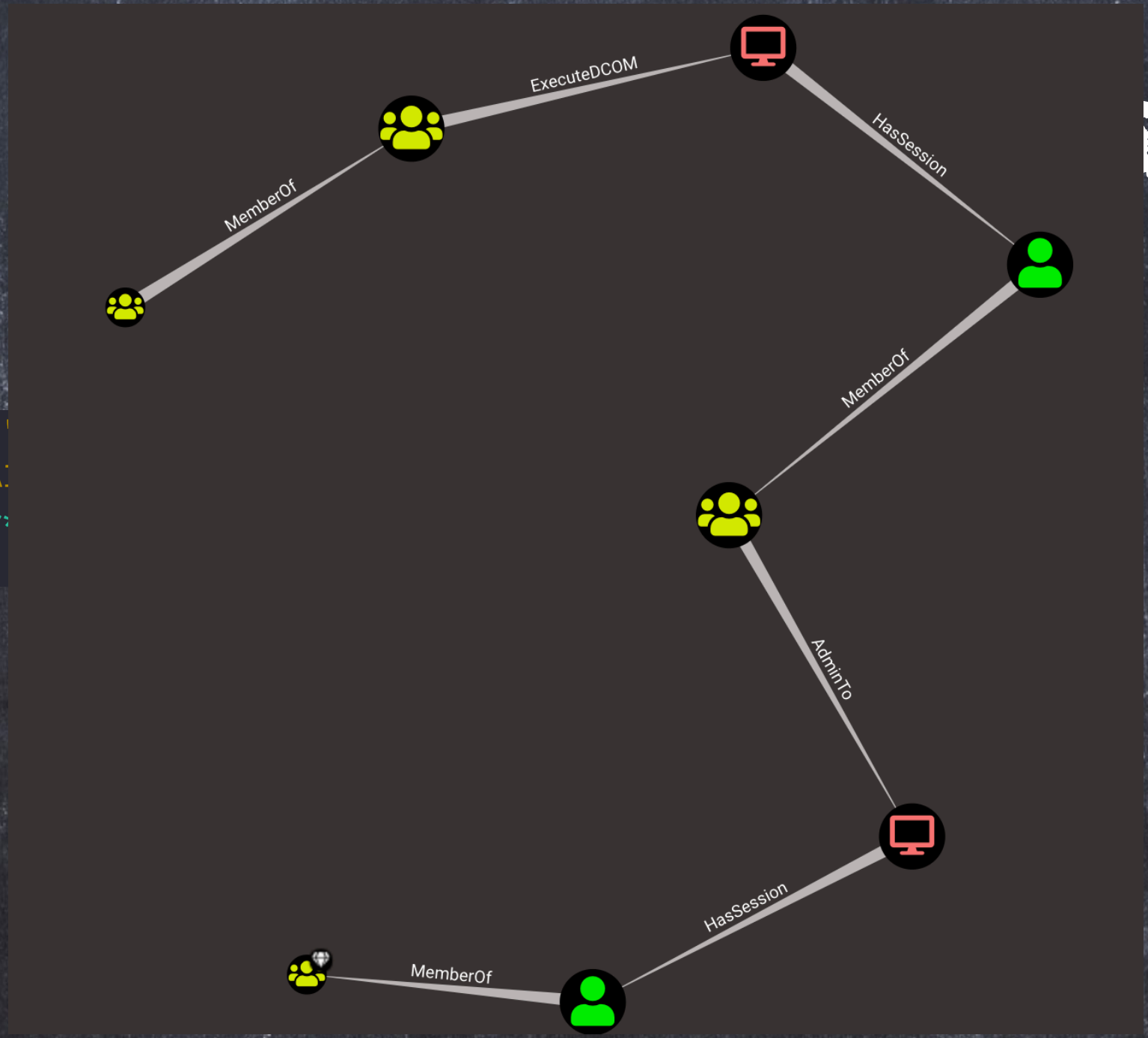
Against Our Data

Test Result of Prosed Fix

```
1 MATCH (n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"}),
2 (m:Group {name: "DOMAIN ADMINS@TESTLAB.LOCAL"}),
3 p=shortestPath((n)-[r*1..]->(m))
4 RETURN p
```

Test

```
1 MATCH (n:Group {name:'
2 (m:Group {name: "DOMA
3 p=shortestPath((n)-[r
4 RETURN p
```

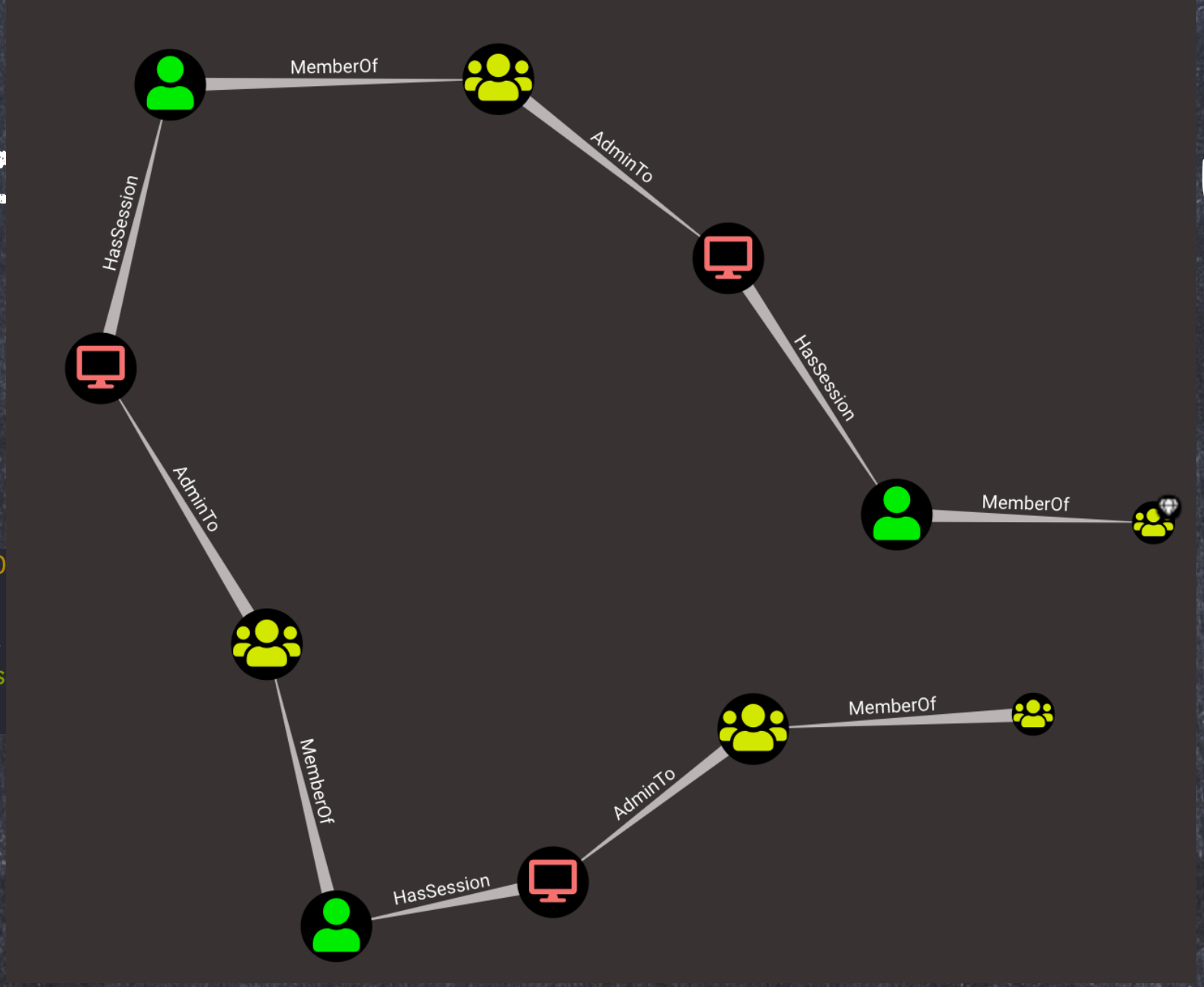


Test result of prosed fix

```
1 MATCH (n:Group {name:"DOMAIN USERS@TESTLAB.LOCAL"}),
2 (m:Group {name: "DOMAIN ADMINS@TESTLAB.LOCAL"}),
3 p=shortestPath((n)-[r*1..]->(m))
4 WHERE ALL(x in relationships(p) WHERE type(x) <> "ExecuteDCOM")
5 RETURN p
```

Test ix

```
1 MATCH (n:Group {name:"DO
2 (m:Group {name: "DOMAIN
3 p=shortestPath((n)-[r*1.
4 WHERE ALL(x in relations
5 RETURN p
```



Pro Tip #1

```
1 MATCH (g:Group)
2 WHERE g.name CONTAINS "ADMIN"
3 AND g.highvalue is null
4 RETURN g.name
```

Pro Tip #1

```
1 MATCH (g:
2 WHERE g.n
3 AND g.hig
4 RETURN g.
```

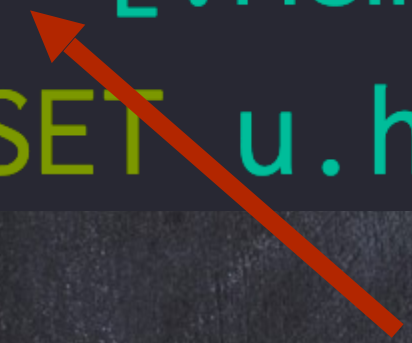
g.name
"ASIA_ADMINS@TESTLAB.LOCAL"
"EUROPE_ADMINS@TESTLAB.LOCAL"
"NORTHAMERICA_ADMINS@TESTLAB.LOCAL"

Pro Tip #1

```
1 MATCH (g:Group)
2 WHERE g.name CONTAINS "ADMIN"
3 AND g.highvalue is null
4 SET g.highvalue=true
```

Pro Tip #2

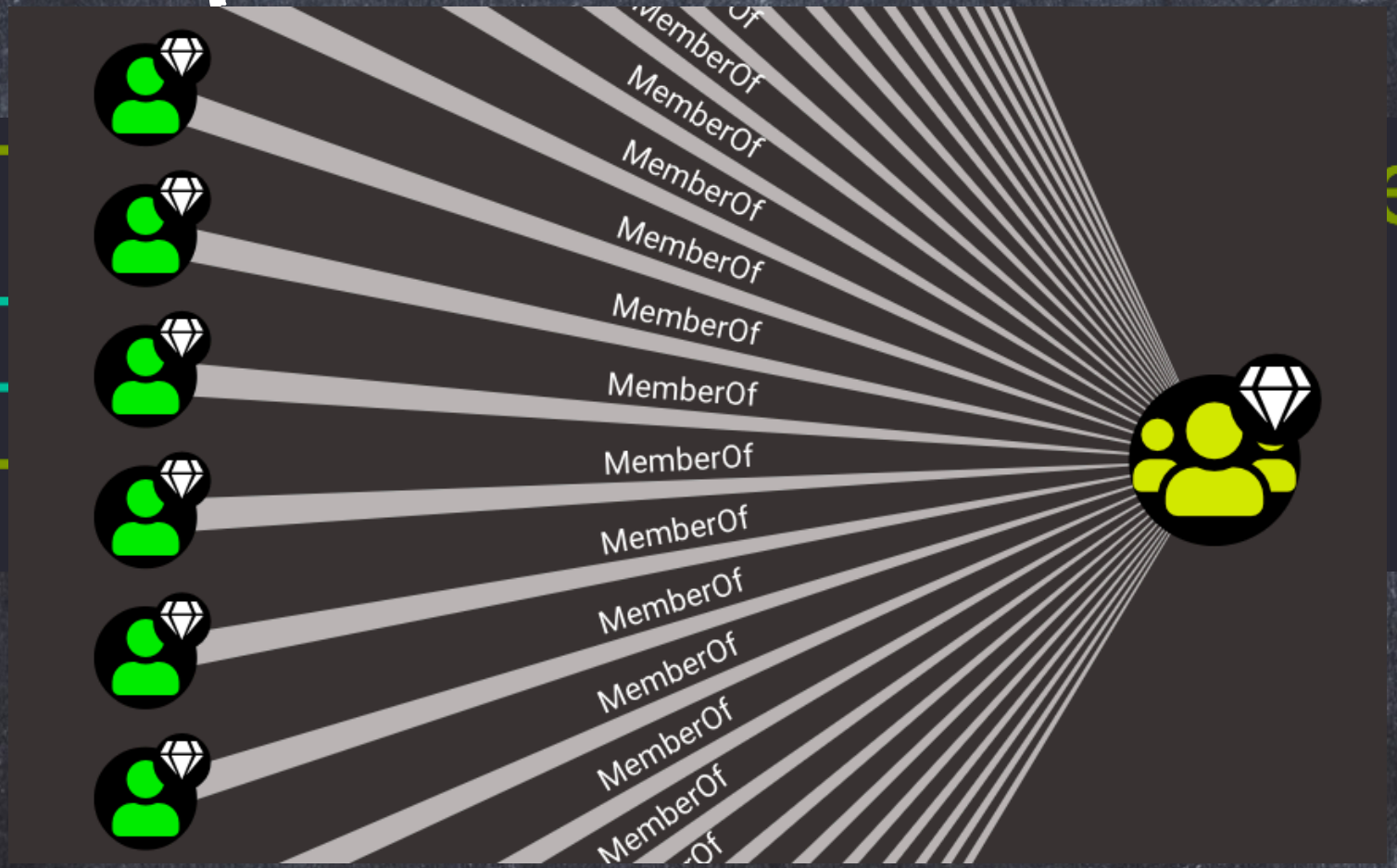
```
MATCH p=(g {highvalue:true})
<-[:MemberOf]-(u:User)
SET u.highvalue=true
```



Pro Tip #2

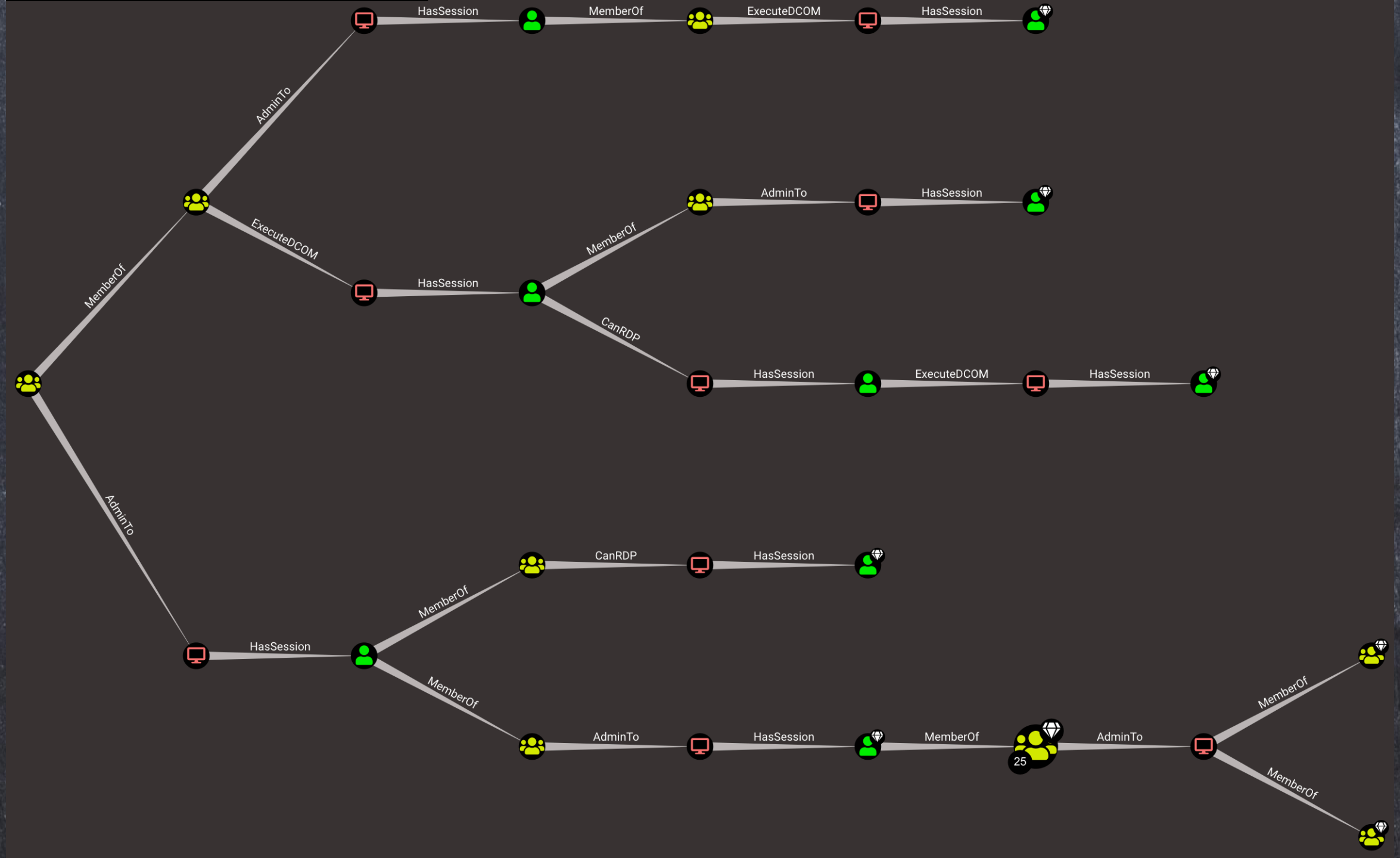

MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf

Pro Tip #2


MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf

Pro Tip #2


AdminTo
HasSession
MemberOf
AdminTo
HasSession
MemberOf
AdminTo
MemberOf
MemberOf


HasSession
MemberOf
ExecuteDCOM
HasSession
AdminTo
MemberOf
ExecuteDCOM
HasSession
AdminTo
HasSession
MemberOf
CanRDP
HasSession
ExecuteDCOM
HasSession
AdminTo
CanRDP
HasSession
HasSession
MemberOf
MemberOf
AdminTo
HasSession
MemberOf
25
AdminTo
MemberOf
MemberOf

PrivExchange

Want to Learn More?

* Operationalizing BloodHound's Attack Graph for Defense
  https://register.gotowebinar.com/register/5012887211059506187
* @SadProcessor
  https://insinuator.net/2019/01/2019-year-of-the-blue-dog/
  https://insinuator.net/2018/11/the-dog-whisperers-handbook/
* BH Slack
  bloodhoundgang.herokuapp.com
  #cypher_queries

Reporting

% of users with path to DA

```
1 OPTIONAL MATCH p=shortestPath((u:User)-[*1..]->
2 (m:Group {name: "DOMAIN ADMINS@TESTLAB.LOCAL"}))
3 OPTIONAL MATCH (uT:User)
4 WITH COUNT (DISTINCT(uT)) as uTotal,
5 COUNT (DISTINCT(u)) as uHasPath
6 RETURN uHasPath / uTotal * 100 as Percent
```

% of users with path to DA

```
1 OPTIONAL
2 (m:Group
3 OPTIONAL
4 WITH COUN
5 COUNT (DI
6 RETURN uH
```

```
$ OPTIONAL MATCH p=shortestPath((u:User)-[*1..]->
```

Table

Text

Percent
100

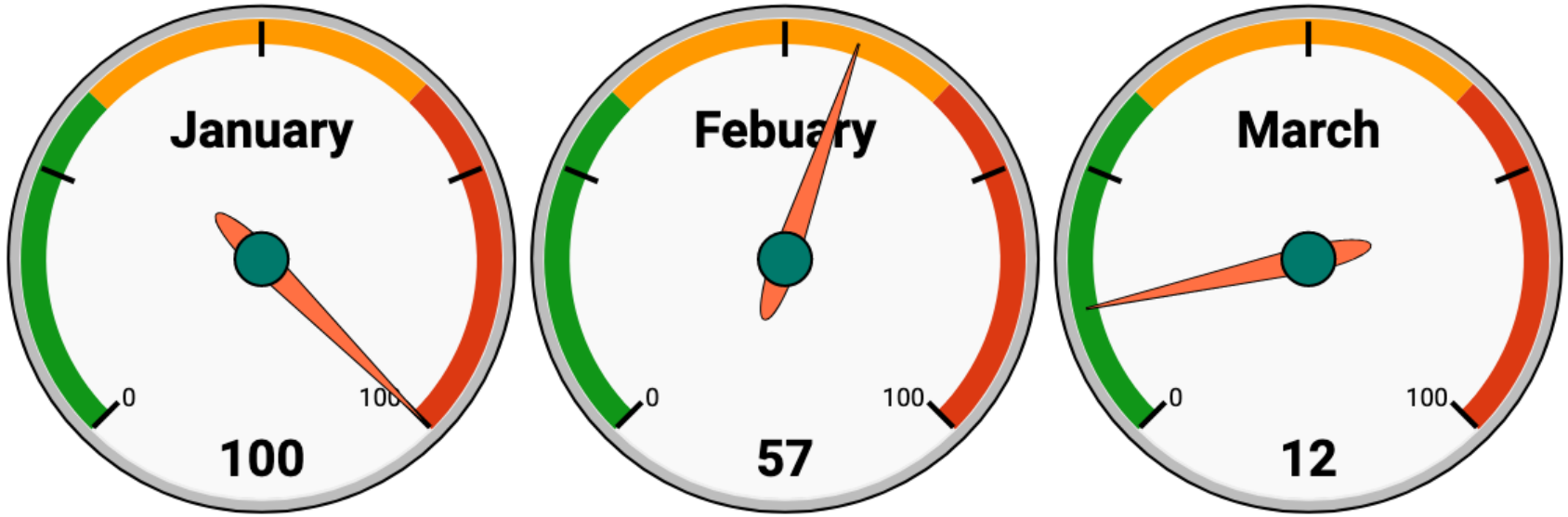
% of users with path to DA

Queries	January	Febuary	March	April
Percentage of users with path to DA	100	57	12	
List Computers where DOMAIN USERS are Local Admin	3	0	1	
Shortest Path from DOMAIN USERS to High Value Targets	1	0	0	
ALL Path from DOMAIN USERS to High Value Targets	5	0	0	
Find Workstations where DOMAIN USERS can RDP To	6	0	2	
Find Servers where DOMAIN USERS can RDP To	111	68	21	
Find all other Rights DOMAIN USERS shouldn't have	8	0	0	
Kerberoastable Accounts member of High Value Group	3	4	0	
List all Kerberoastable Accounts	196	206	213	

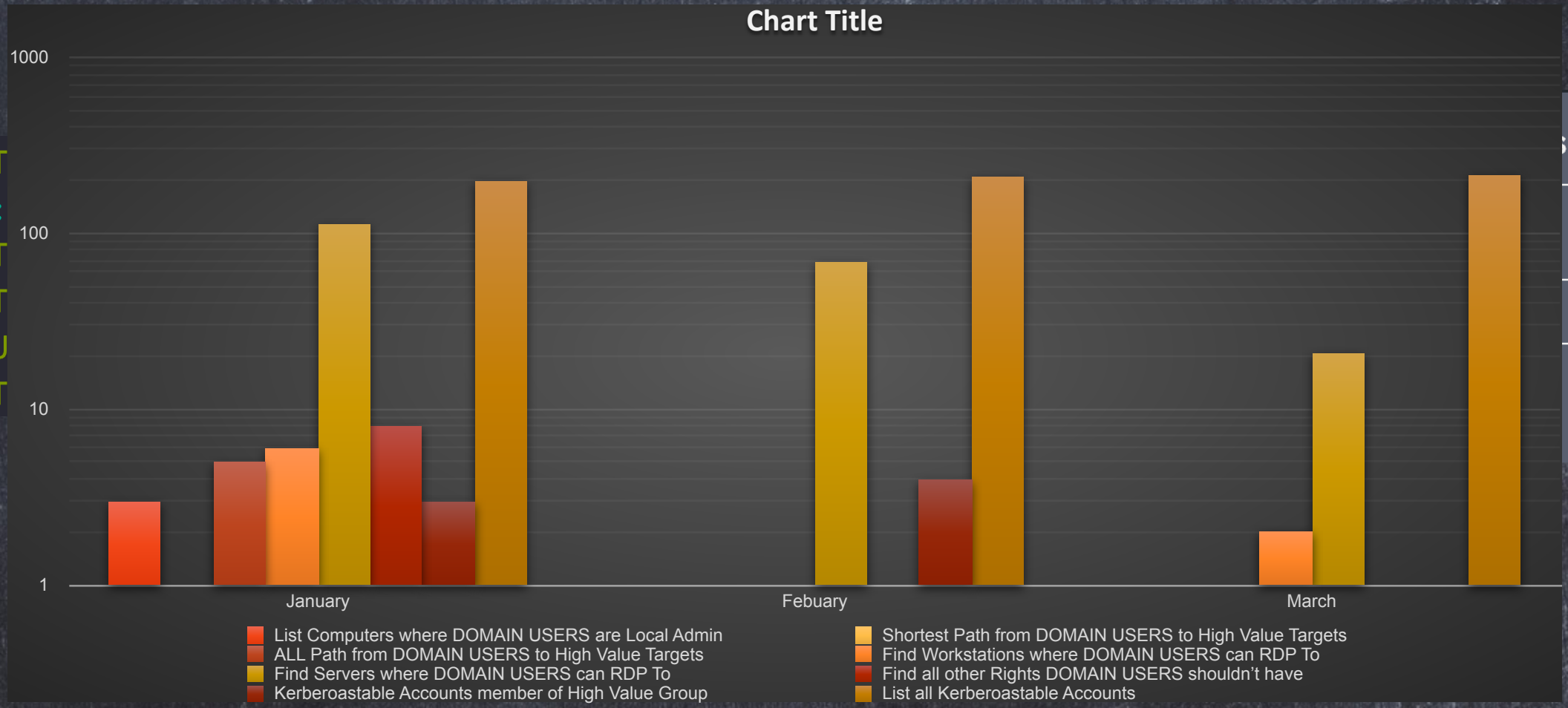
% of users with path to DA

```
1 OPTIONAL MAT
2 (m:Group {na
3 OPTIONAL MAT
4 WITH COUNT (
5 COUNT (DISTI
6 RETURN uHasP
```

```
User)-[*1..]->
```



% of users with path to DA




```
1 OPT
2 (m:
3 OPT
4 WIT
5 COU
6 RET
```

```
ser)-[*1..]->
```

Automation

Automation

```
Hunter:bin mats$ pwd
/Users/mats/neo4j-community-3.4.5/bin
Hunter:bin mats$ export NEO4J_USERNAME='neo4j'
Hunter:bin mats$ export NEO4J_PASSWORD='[redacted]'
Hunter:bin mats$ ./cypher-shell 'MATCH (n:User)-[r:MemberOf]->(g:Group)
WHERE g.highvalue=true AND n.hasspn=true RETURN n, g, r;'
```

Automation

```
+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| n                                                                                                        | g                                                                                                                              | r              |
+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| (:User {highvalue: TRUE, hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: -1, displayname: "Jesusita Noa", lastlogon: -1, name: "JNOA00093@TESTLAB.LOCAL", objectsid: "S-1-5-21-883232822-274137685-4173207997-1093", enabled: TRUE}) | (:Group {name: "DOMAIN ADMINS@TESTLAB.LOCAL", highvalue: TRUE, objectsid: "S-1-5-21-883232822-274137685-4173207997-512", domain: "TESTLAB.LOCAL"}) | [:MemberOf] |
+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------+

1 row available after 1 ms, consumed after another 5 ms
```

Automation

```
+-------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------+
| n
                                                                                  | g
                                                                                          | r          |
+-------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------+
| (:User {highvalue: TRUE, hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: -1, displayname: "Jesusita Noa", lastlogon: -1
, name: "JNOA00093@TESTLAB.LOCAL", objectsid: "S-1-5-21-883232822-274137685-4173207997-1093", enabled: TRUE}) | (:Group {name: "DOMAIN ADM
INS@TESTLAB.LOCAL", highvalue: TRUE, objectsid: "S-1-5-21-883232822-274137685-4173207997-512", domain: "TESTLAB.LOCAL"}) | [:MemberOf] |
+-------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------+

1 row available after 1 ms, consumed after another 5 ms
```

Automation

```
n, g, r
(:User {highvalue: TRUE, hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: -1,
displayname: "Jesusita Noa", lastlogon: -1, name: "JNOA00093@TESTLAB.LOCAL", objectsid: "S-1-5
-21-883232822-274137685-4173207997-1093", enabled: TRUE}), (:Group {name: "DOMAIN ADMINS@TESTL
AB.LOCAL", highvalue: TRUE, objectsid: "S-1-5-21-883232822-274137685-4173207997-512", domain:
"TESTLAB.LOCAL"}), [:MemberOf]
```

Automation

```
Hunter:bin mats$ ./cypher-shell 'MATCH (n:User)-[r:MemberOf]->(g:Group) WHERE n.hasspn=true
RETURN n, g, r;' > Q2.csv
Hunter:bin mats$ echo "User; Group; Relation" > Query2.csv
Hunter:bin mats$ grep -v "n, g, r" Q2.csv >> tmp2.csv
Hunter:bin mats$ sed 's/),/);/g' tmp2.csv >> Query2.csv
```

Automation

Query2

User	Group	Relation
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT05305@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT04556@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT01491@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT02031@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT04395@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT04246@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT04112@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT05364@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "IT02954@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]
(:User {hasspn: TRUE, owned: FALSE, domain: "TESTLAB.LOCAL", pwdlastset: 0, displayname	(:Group {name: "DOMAIN USERS@TESTLAB.LOCAL", domain: "TESTLAB.LOCAL"})	[:MemberOf]

Alerting

- Query
- Compare Last Results
- Alert if increase

Conclusion

- Defenders can use Graph too
- Cypher is a very flexible language
- Important to test real impact of remediation
- Not all queries are worth automating

Thank You

- BSideCharm
- @Pyrotek, @TalBeerySec, @danielhbohannon
- @_waldo, @CptJesus