Attack path-based Detection Engineering

Leveraging BloodHound for robust defense

Olaf Hartong

Detection Engineer and Security Researcher

- Purple teaming, Threat hunting
- IR and Compromise assessments

Former documentary photographer
Father of 2 boys
“I like **warm hugs**”

@olafhartong
github.com/olafhartong
olaf@falconforce.nl
olafhartong.nl / falconforce.nl

What can you expect today ?

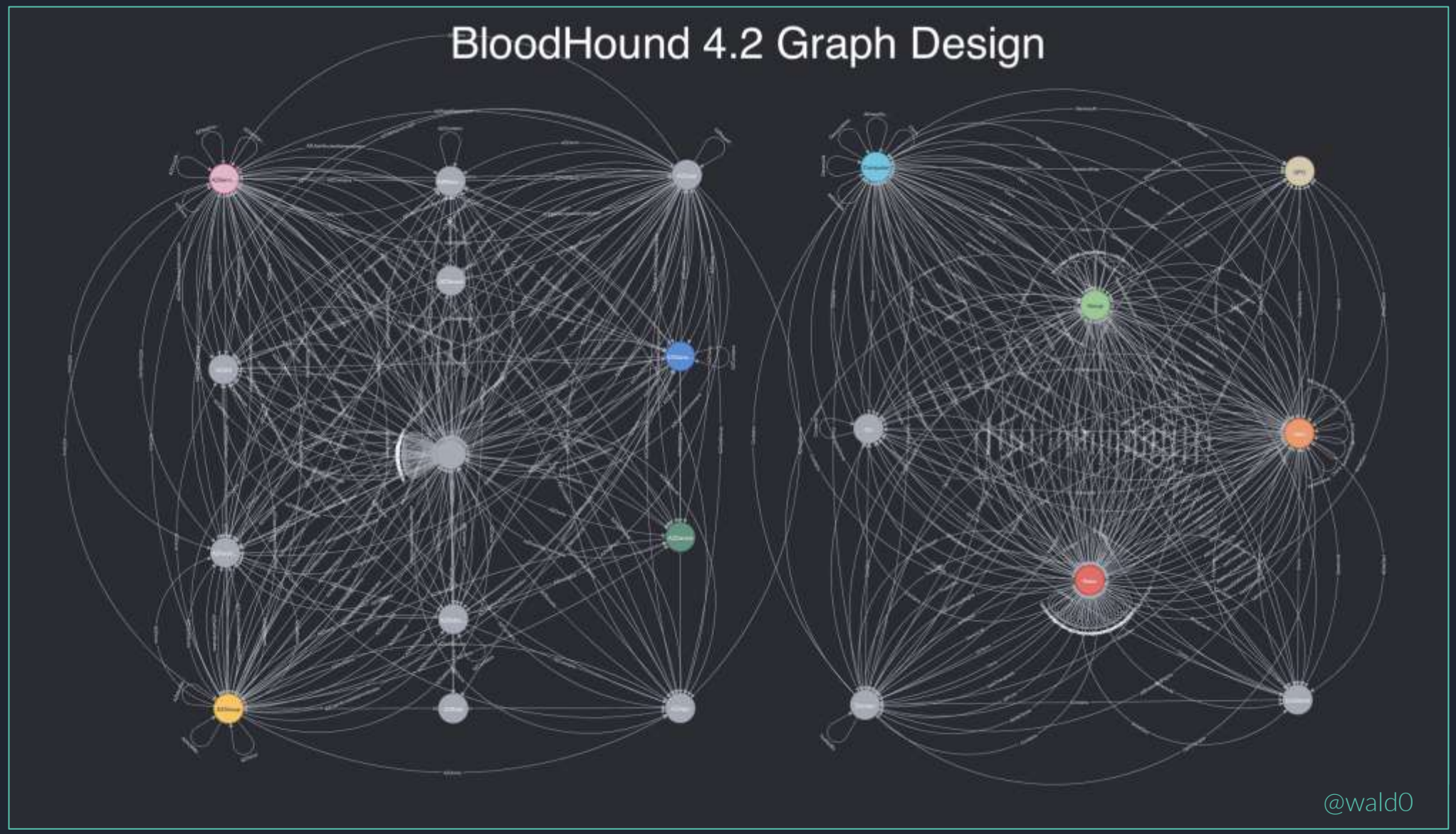
- Some slides with several lists
- Me, using some graphs to explain the value of lists
- Some more lists
- **Near real-time Blue team use cases for BloodHound**

This has always bugged me

“DEFENDERS THINK IN LISTS.
ATTACKERS THINK IN GRAPHS.
AS LONG AS THIS IS TRUE, ATTACKERS WIN”

John Lambert, 2015

A year later, BloodHound was released



Path based detection and enrichment

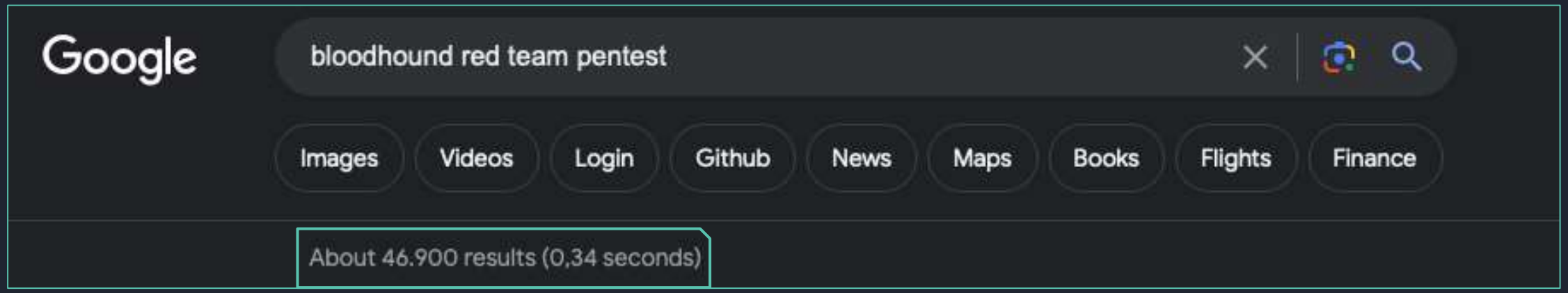
Most red teams rely on BloodHound in their operations for uncovering lateral movement paths.

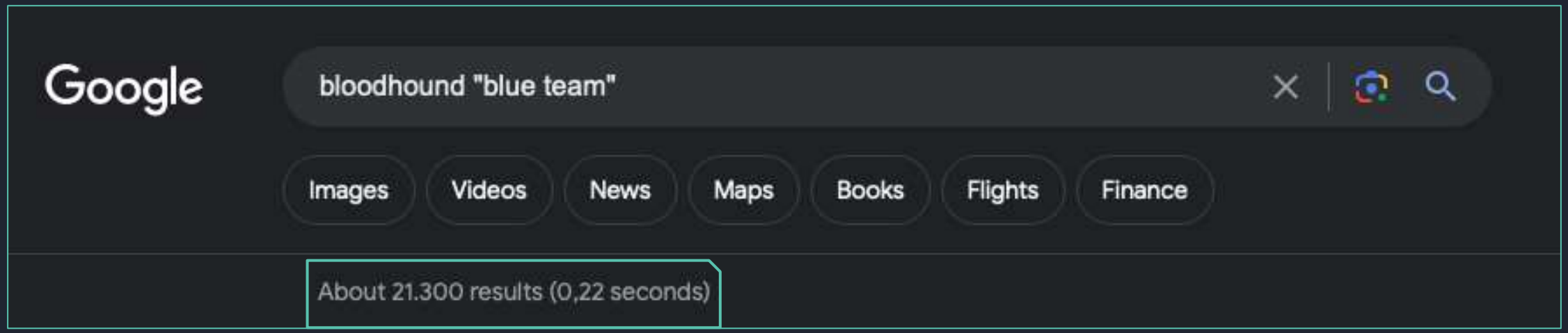
Sadly, we don't see many detection teams leverage it for mitigations and detections, not even talking about enrichment or alert investigations.

In some cases we see it being used, but only a hand-full times a year, in a very manual way.

There must be a better way.

It’s not the lack of documentation



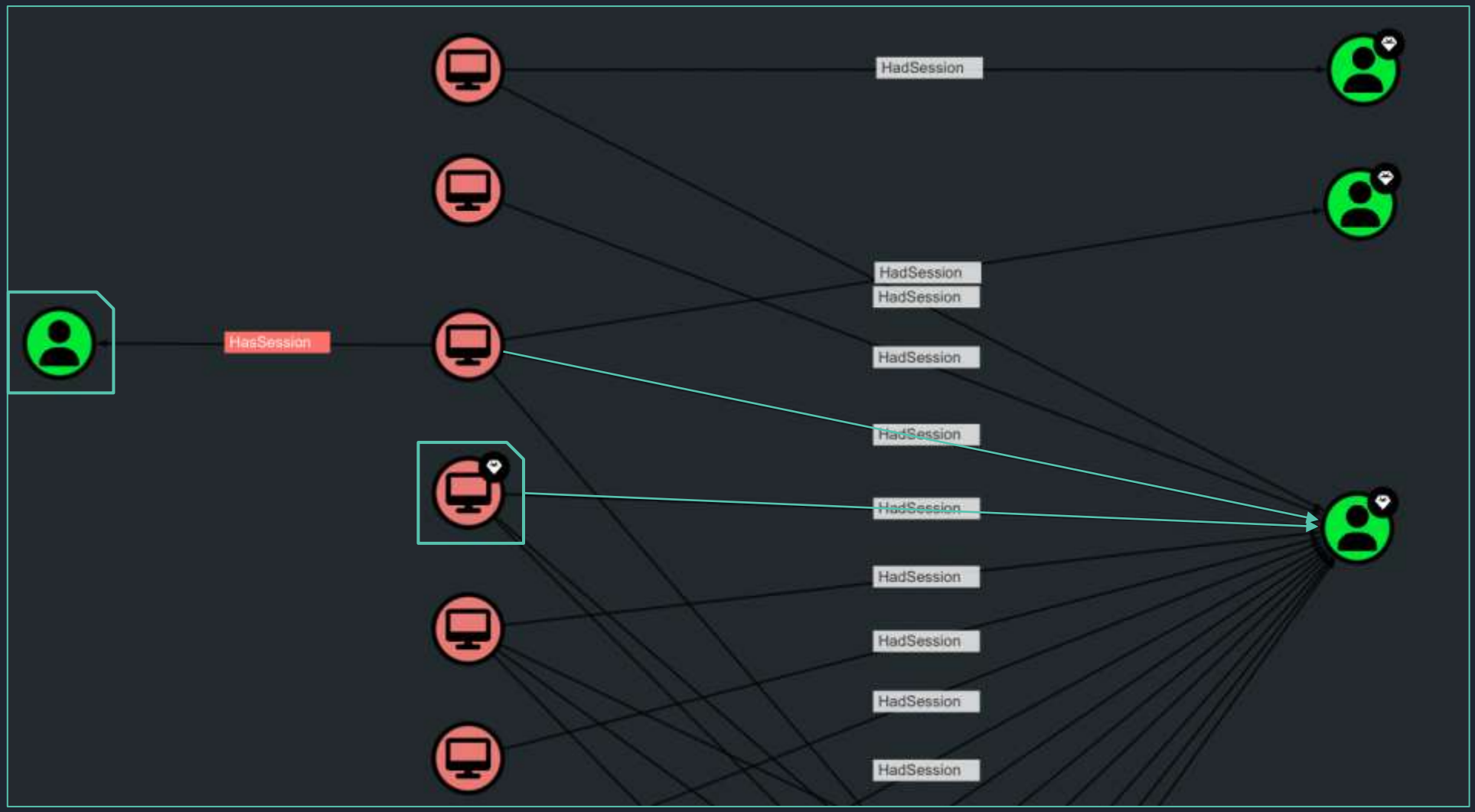


BloodHound for blue

BloodHound challenges for red and blue

- Frequently scanning adds complexity and sometimes friction between teams
- Hard to reach all subnets for session data
- It is always a moment in time snapshot
- Local user and group modifications are mostly invisible
- How do you know a session is still active? Or if there are more?

Why are sessions so important?



The power of ~~*love*~~ logs

As a blue team, we already have this information!

And with that... much, much more..

The power of ~~*love*~~ logs

- User logons / unlocks
- User / group / object modifications
- Alerts on entities
- (Eligible) Role assignments, MFA modifications
- All these events and much more in near-realtime, *all the time*!

FalconHound

Query

Neo4j
MDE
M365 Security
MS Graph API
Azure Data Explorer
Sentinel
Splunk
Elastic
Falcon Logscale
BloodHound API*

Process

FalconHound
Actions

Store

Sentinel table
Sentinel Watchlist
Neo4j
CSV / JSON / MD
Azure Data Explorer
Splunk
Falcon Logscale
Bloodhound API *
Elastic*

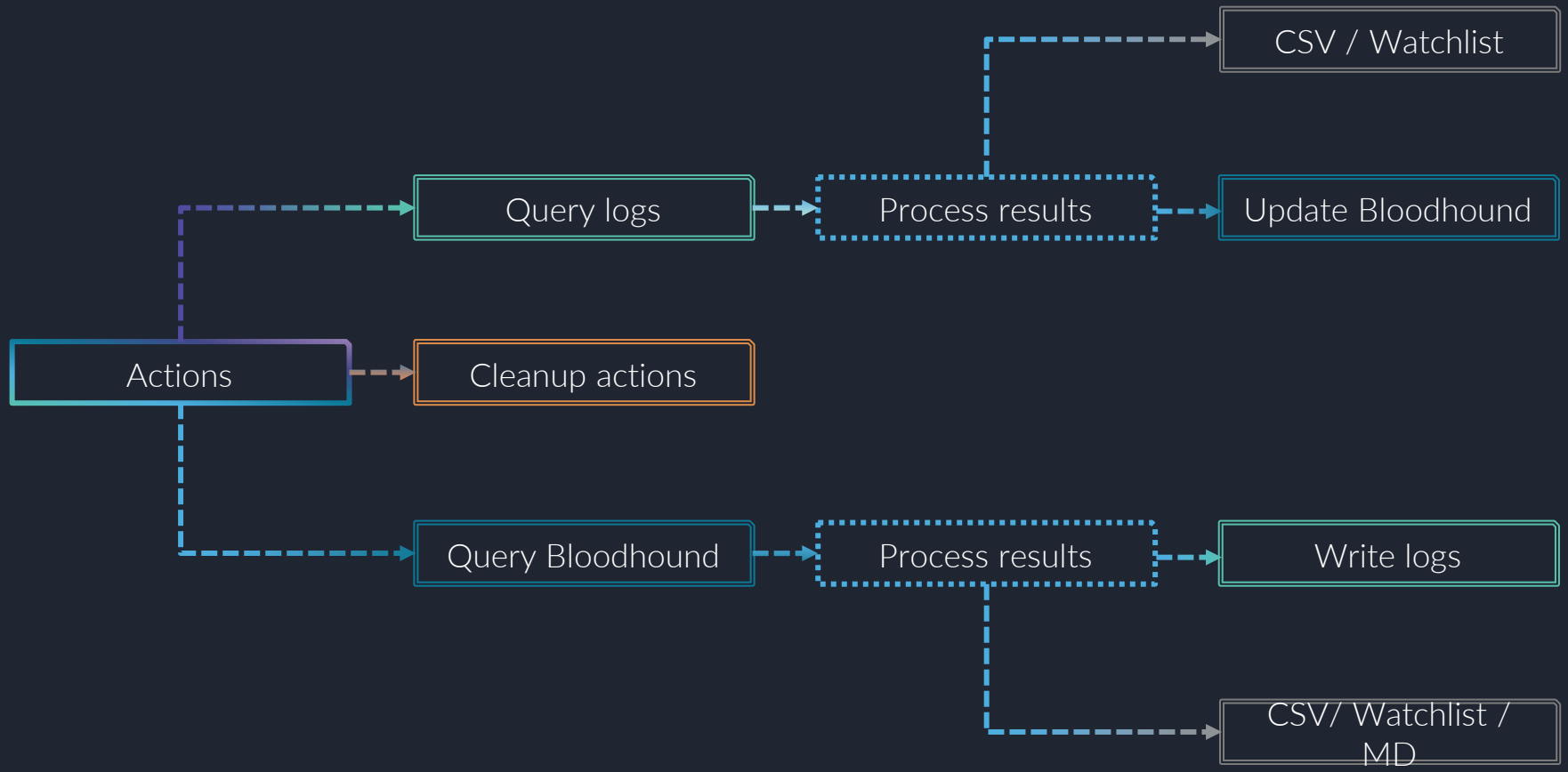
https://github.com/FalconForceTeam/FalconHound

* Under development, more connectors to follow

Built for easy implementation

- Builds for all major operating systems
- Configure your API creds
- Update the config file with your keys
- Define actions you want to run
- Schedule the agent to run every 5/10/15 mins, whichever you prefer and your env can take.

Process flow – simplified example



Some example actions

- Keep the session information in BloodHound up to date, without scanning!
- Mark machines/users with alerts as Owned
- Repeatedly query for paths to high value targets, for instance from owned to sensitive resource
- Add new users or group modifications
- Calculate new paths or chokepoints based on this information

YAML based configuration

```yaml
Active: true                    # Enable to run this action
Debug: false                     # Enable to see query results in the console
SourcePlatform: MDE             # Sentinel, Watchlist, Neo4j, CSV, MDE, Graph, Splunk
Query: |
    let timeframe = 15m;
    DeviceNetworkEvents
    | where Timestamp > ago(timeframe)
    | where ActionType == "InboundInternetScanInspected"
    | where RemotePort in (3389,445,389,636,135,139,161,53,21,22,23,1433)
    | summarize LastSeen=arg_max(Timestamp, * ), PublicPorts=make_set(RemotePort) by DeviceId,DeviceName, PublicIP=RemoteIP
    | project LastSeen,PublicPorts,DeviceId,DeviceName,PublicIP,LocalIP
```

```yaml
  - Name: Sentinel
Targets:
  - Name: Neo4j
    Enabled: true
    Query: |
      WITH toUpper($DeviceName) as DeviceName, $PublicPorts as PublicPorts
      MATCH (c:Computer {name:DeviceName}) SET c.exposed = true, c.ports = PublicPorts, c.exposedSince = $LastSeen
    Parameters:
      DeviceName: DeviceName
      PublicPorts: PublicPorts
      LastSeen: LastSeen
  - Name: Watchlist
    Enabled: true
    WatchlistName: FH_MDE_Exposed_Machines
    DisplayName: MDE Exposed Machines
    SearchKey: DeviceName
    Overwrite: false
```

Some practical blue uses

- Generate watchlists for users and devices with a known, harder to mitigate path
- Dynamically raise the severity of alerts for these entities
- Generate alerts based on new paths found in Bloodhound
- Tracking uncommon sessions across a path, as a lateral Movement indicator
- Uncover risky resources or unintentional paths

Demo

```
                  %????????;;'
                %??++;;;;??????'''+
              ++++%??%%???;;???''+;
           ???++++;??????%#%?????;;;'';
           +;;+?????????.'#.......?%%??
         +;;;+???????????.??.;%##%%%%%??
      ##??;;;???';;???????%%######%%%%#??.
      #?;;;??;;;';;?????+?+?%%... %???????'
     +;;';?'';'''';;;;;;;???????.. +''.????'
    ;##+';;;';';;''''';'''''........   .'++'
     #+;;;';''''''';;;''''........'      +'
     ';'';;';;;;;';;..''....'.''''.      ;
        ;;.''''.'''''..'....''''''..
         . '''..'''''''...'''....'..
           ''''''.''''''..''''......    FalconForce Sentry
            ' '''...'''''.........      FalconHound v1.3.0
                ;''.'''.........'.      ------------------
                  ''''.......'?         Usage: FalconHound -[options]
                     '''.''''           https://github.com/FalconForceTeam/FalconHound
                       ''
Usage: FalconHound -[options]
Options:
  -actionlist
        Get a list of all enabled actions, use in combination with -go
  -actionsdir string
        Path to the actions directory (default "actions/")
  -adxinit
        Initialize the Azure Dara Explorer table (requires database admin permissions) and -go
  -config string
        config file name (default "config.yml")
  -debug
        Enable debug mode, for all executed actions
  -go
        Run all actions in the actions directory
  -help
        Print this help message
  -ids string
        comma separated list of action IDs to run
  -keyvault
        Use the keyvault specified in the config for secrets
  -lookback string
        Override the timeframe in the queries, use the KQL supported format (1d,1h,15m,etc)
  -skip string
        Skip the input processor for the specified source platform, comma separated list of platforms
```

Running actions at a big corp

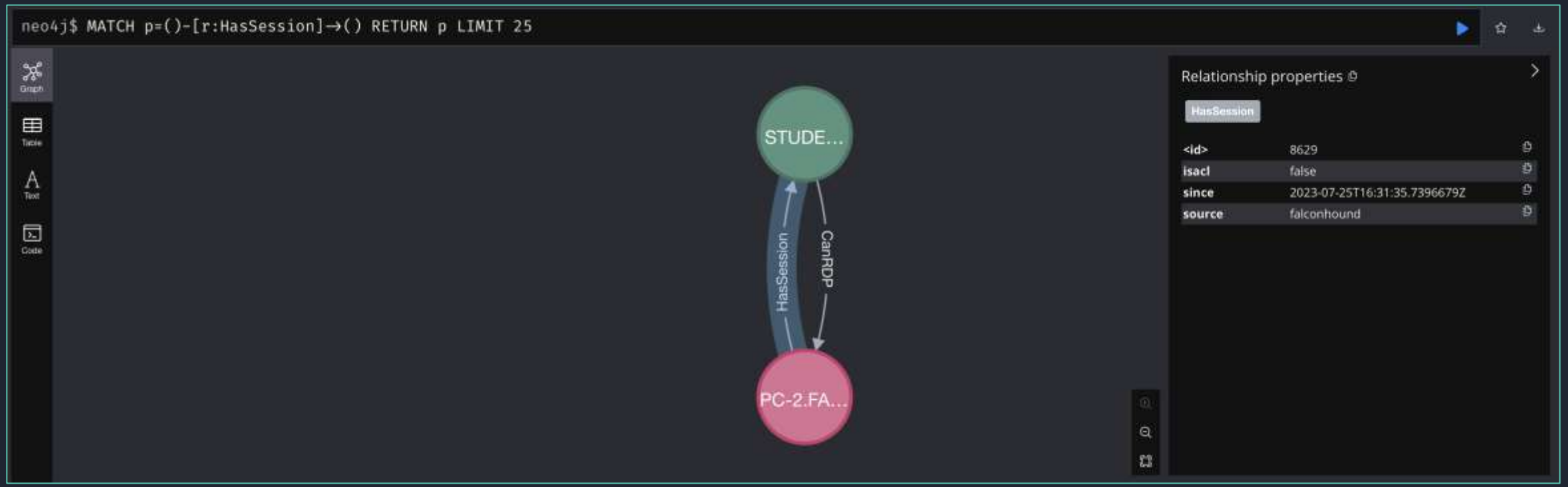
```
falconforce@0xff-neo4j:~/falconhound$ ./falconhound -go -ids SEN_New_Sessions -lookback 14d
                    %????????;;'
                  %??++;;;;??????'''+
                +++++%??%%%???;;???''+;
             ???++++;??????%#%?????;;;'';
             +;;+?????????.'#.......?%%??
          +;;;+???????????.??.;%##%%%%%??
       ##??;;;???';;???????%%%#####%%%%??.
       #?;;;??;;;';;?????+?+?%%... %???????'
      +;;';?'';'''';;;;;;;??????.. +''.????'
     ;##+';;;';';;;'''';;''''.......   .'++'
      #+;;;';''''''';;;''''........'      +'
       ';''';;;;;';;..''....'.''''.      ;
         ;;.''''.''''''..'....''''''..
           . ''''.''''''...'''.....'..
             ' '''...''''.........
                ;''.'''.........'.
                  ''''.......'?
                     '''.''''
                       ''

FalconForce Sentry
FalconHound v1.3.0
------------------
Usage: FalconHound -[options]
https://github.com/FalconForceTeam/FalconHound

2024/02/23 20:48:48 [>] Starting run
2024/02/23 20:48:48 [+] Found 17 .yml files in actions/
2024/02/23 20:48:49 [+] Running 1 active queries...
2024/02/23 20:48:49 [+] Using config file: /home/falconforce/falconhound/config.yml
2024/02/23 20:48:49 [i] Overriding timeframe to 14d for all active queries
2024/02/23 20:48:49 [Ξ] Running query "Get new logon sessions" (SEN_New_Sessions) in Sentinel
2024/02/23 20:49:14  ↳ [>] Processing 339319 results..
2024/02/23 20:49:14    ↳ [>] Writing to Neo4j
2024/02/23 20:52:28 [=] All done ... finished in 219 seconds
falconforce@0xff-neo4j:~/falconhound$
```

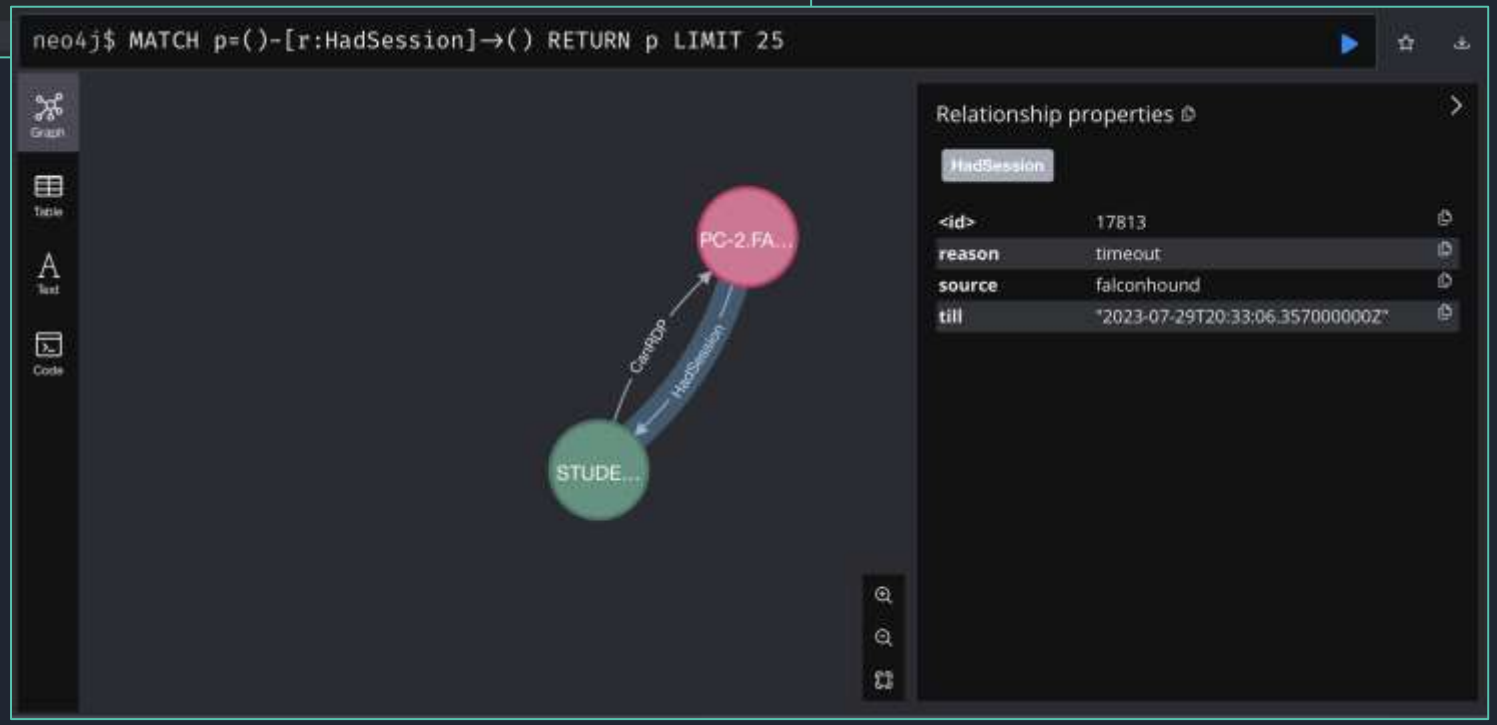
Creating new sessions

```
2023/07/28 22:30:10 [ Starting run
2023/07/28 22:30:10 [+] Found 9 files in actions/test/
2023/07/28 22:30:10 [+] Running 3 active queries...
2023/07/28 22:30:10 [<] Running query "Get Sessions from MDE" in MDE
{"AccountDomain":"FALCONFORCE","LogonType":"Interactive","Timestamp":"2023-07-25T16:31:35.7396679Z","min_Timestamp_arg1":0,"DeviceName":"PC-2.FALCONFORCE.LOCAL","AccountSid":"S-1-5-21-2953915480-1169422843-688089779-1103","Acc
ountName":"STUDENT-USER"}
2023/07/28 22:30:10 [>] Writing to Neo4j
MATCH (x:Computer {name:'PC-2.FALCONFORCE.LOCAL'}) MATCH (y:User {objectid:'S-1-5-21-2953915480-1169422843-688089779-1103'}) MERGE (x)-[r:HasSession]->(y) SET r.since='2023-07-25T16:31:35.7396679Z' SET r.source='falconhound'
```



Time out sessions and set new edge

```
Name: N4J_CLN_Remove_Older_Sessions
Synopsis: Removes the HasSession relation and replaces it with HadSession if the session is older than 3 days
ID: N4J_CLN_Remove_Owned
Description: Removes the HasSession relation and replaces it with HadSession if the session is older than 3 days
Author: FalconHound
Version: '0.8'
Info: |
  tbd
Active: true                # Enable to run this action
Debug: false                # Enable to see query results in the console
SourcePlatform: Neo4j
Query: |
    MATCH (c)-[R:HasSession]->(u)
    WHERE duration.between(datetime(R.since), datetime()).days > 3
    MERGE (c)-[r:HadSession]->(u) SET r.till=datetime() SET r.source='falconhound' SET r.reason='timeout' DELETE R
Enhance: |
Targets:
```



Cutting edge-stensions and property additions

- HadSession
- HasConsent
- MfaDeviceSharing
- MfaEmailSharing
- MfaPhoneSharing
- AZHasRole > Eligible

- AlertIds > Owned
- Publicly exposed ports
- Known exploitable CVEs
- Azure Dynamic Groups
- MFA Properties
- App Consent Scope
- And much more

How can we use this?

With this data we can build detections based on for example an increase in direct or nested paths from for example:

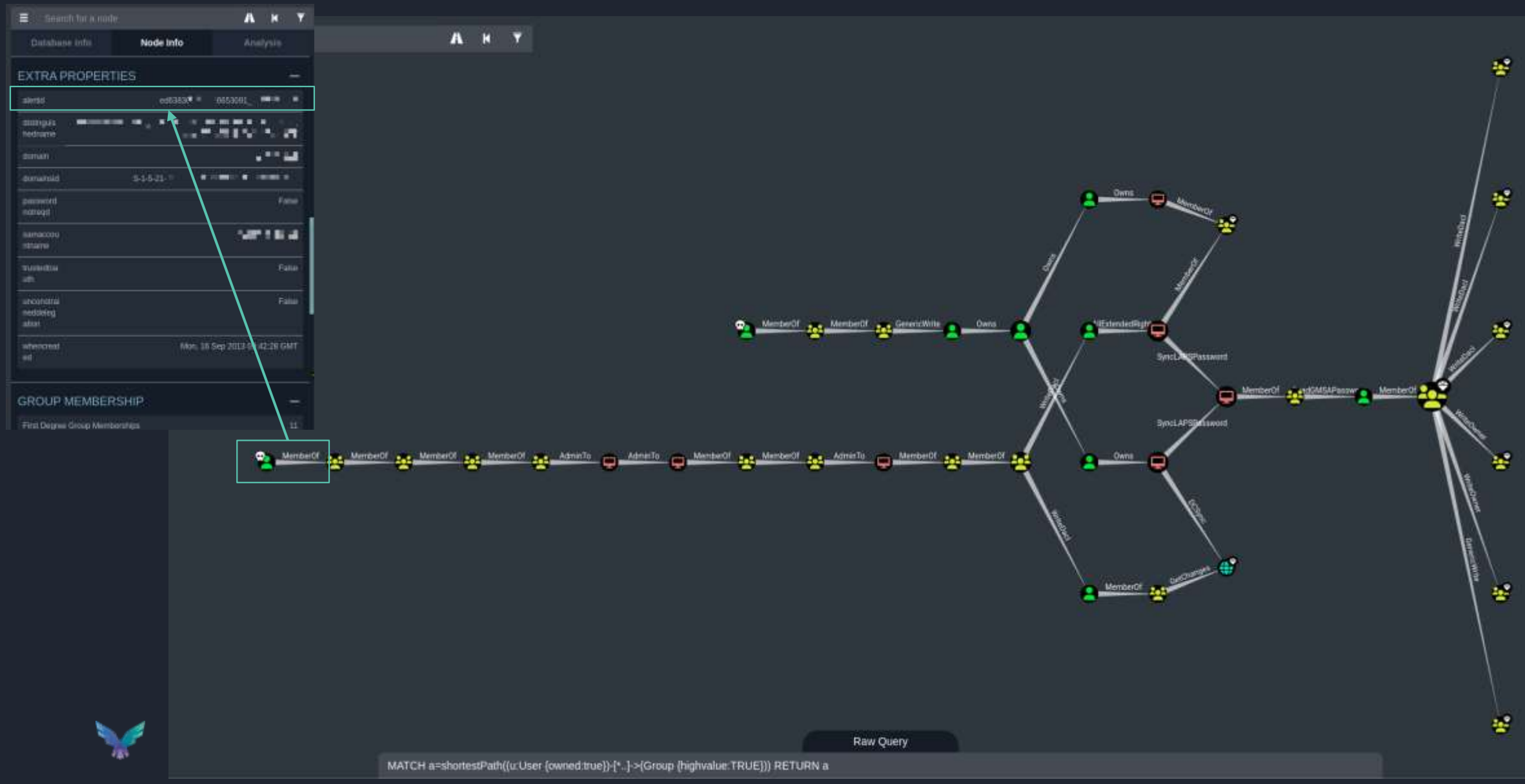
Owned users / computers to high value resources

```
DemoFalconHound_CL
| where EventID_s == "N4J_Owned_User_to_HighValue"
| where EventData_s != "[]"
| extend EventData=parse_json(EventData_s)
| sort by TimeGenerated asc
| extend PrevEventData=prev(EventData)
| extend diff=set_difference(EventData, PrevEventData)
| where diff!="[]"
| mv-expand diff
| extend TargetName=diff.Name,DirectCount=diff.Direct, DirectPath=diff.DirectNames, NestedCount=diff.Nested, NestedPath=diff.NestedNames
| project-away EventData,diff, EventData_s, PrevEventData
```

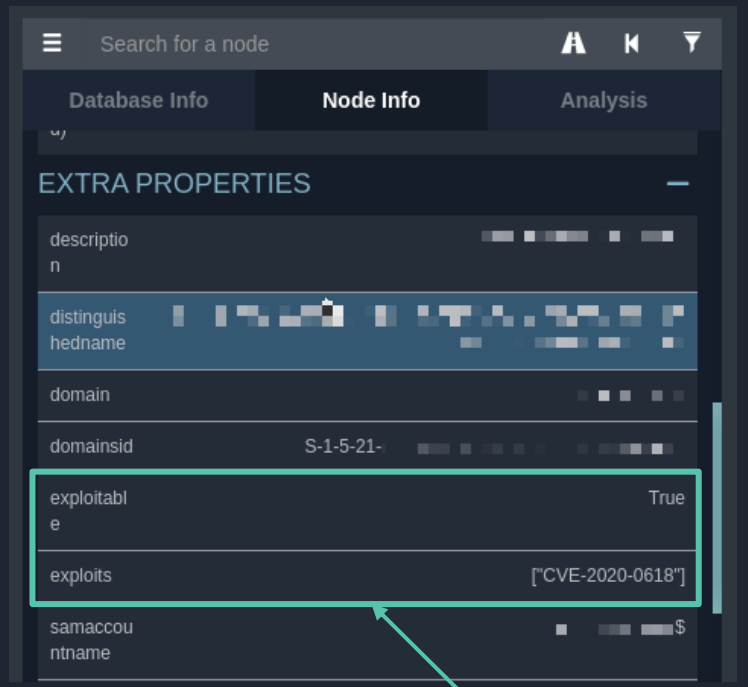
Results | Chart | Add bookmark

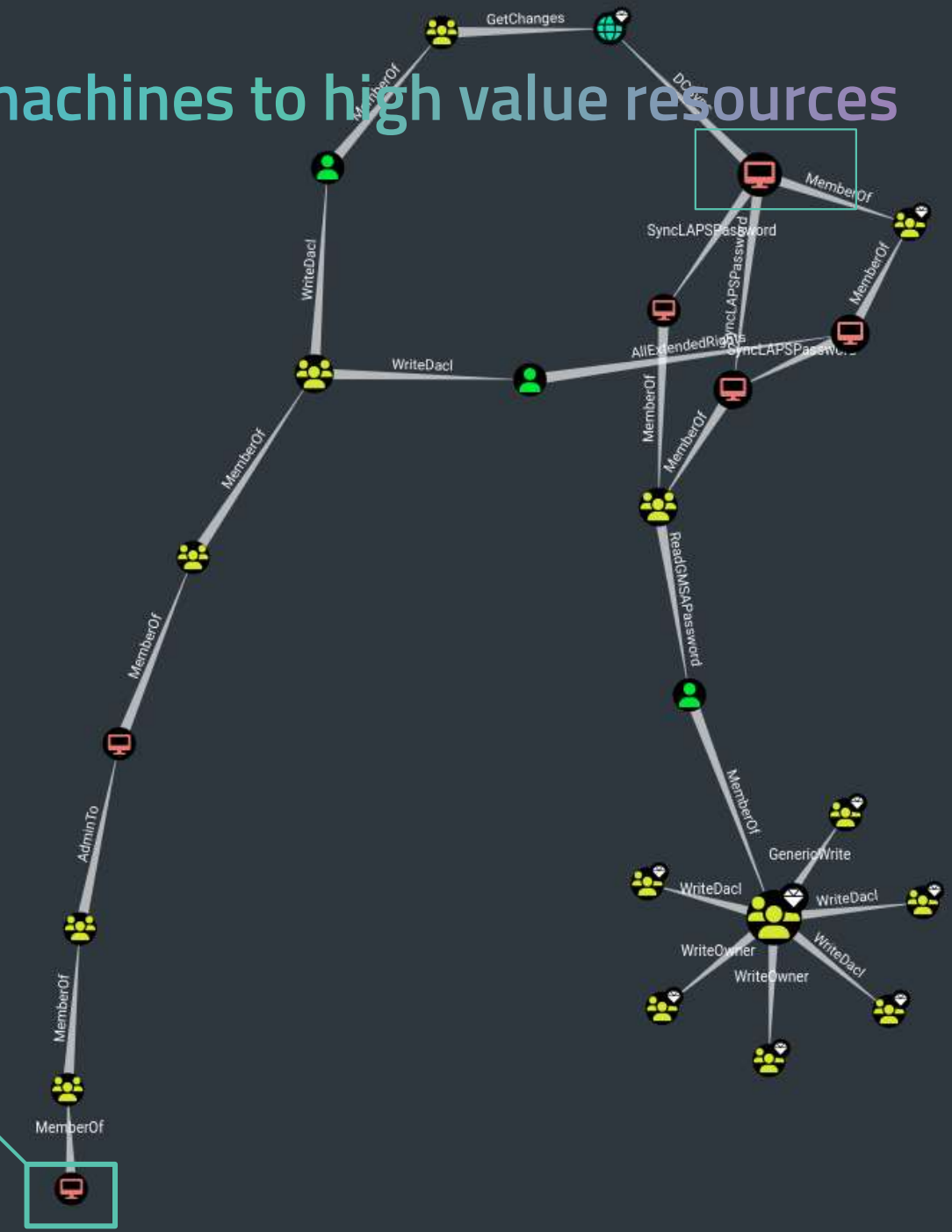
TimeGenerated [UTC]	TargetName	DirectCount	DirectPath	NestedCount	NestedPath	EventID_s	Description_s
01/09/2023, 13:04:18.788	ADMINISTRATORS@BALLPIT...	1	["ADMINISTRATOR@BALLPIT.INT","ADMINISTRA...	1	["ADMINISTRATOR@BALLPIT...	N4J_Owned_User_to_HighValue	Counts all direct and
01/09/2023, 13:04:18.788	DOMAIN ADMINS@BALLPIT.I...	1	["LYNX-ADM@BALLPIT.INT","DOMAIN ADMINS@...	1	["LYNX-ADM@BALLPIT.INT",...	N4J_Owned_User_to_HighValue	Counts all direct and
01/09/2023, 13:04:18.788	DOMAIN ADMINS@BALLPIT.I...	1	["SEAL-ADM@BALLPIT.INT","DOMAIN ADMINS@...	1	["SEAL-ADM@BALLPIT.INT","...	N4J_Owned_User_to_HighValue	Counts all direct and

Owned user to high value targets



Exploitable machines to high value resources





Unexpected sessions from accounts with SPN

```
let KerberoastableUsers=_GetWatchlist('FH_Kerberoastable_Users') | project Sid;
SecurityEvent
| where EventID in (4624,4625)
| where LogonType !in (3,7)
| where not(SubjectUserName endswith "$" or TargetUserName endswith "$")
| where TargetUserSid in (KerberoastableUsers)
```

Results | Chart | Add bookmark

TenantId	TimeGenerated [UTC]	SourceSystem	Account	AccountType	Computer	EventSourceName	Channel
3b6c13cd-041d-41d5-88b4-32742a558494	01/12/2023, 10:41:03.165	OpsManager	NORTH\jon.snow	User	ws02.essos.local	Microsoft-Windows-Security...	Security
3b6c13cd-041d-41d5-88b4-32742a558494	01/12/2023, 10:41:03.165	OpsManager	NORTH\jon.snow	User	ws02.essos.local	Microsoft-Windows-Security...	Security

01/12/2023, 10:45:27.311	Searches for kerberoastable users with a session on a computer	[{"Computer":"WS02.ESSO...	N4J_Kerberoastable_U

TenantId	3b6c13cd-041d-41d5-88b4-32742a558494
SourceSystem	RestAPI
TimeGenerated [UTC]	2023-12-01T10:45:27.3112562Z
Description_s	Searches for kerberoastable users with a session on a computer
EventData_s	[{"Computer":"WS02.ESSOS.LOCAL","ComputerHasAlerts":false,"ComputerIsExposed":true,"ComputerIsVulnerable":null,"UserHasAlerts":false,"UserName":"JON.SNOW@NORTH.SEVENKINGDOMS.LO
EventID_s	N4J_Kerberoastable_User_with_Session
Name_s	Kerberoastable User with a Session on a Computer
Type	FalconHound_CL

Follow-up query in the data

Query results can be augmented with BloodHound queries for further analysis

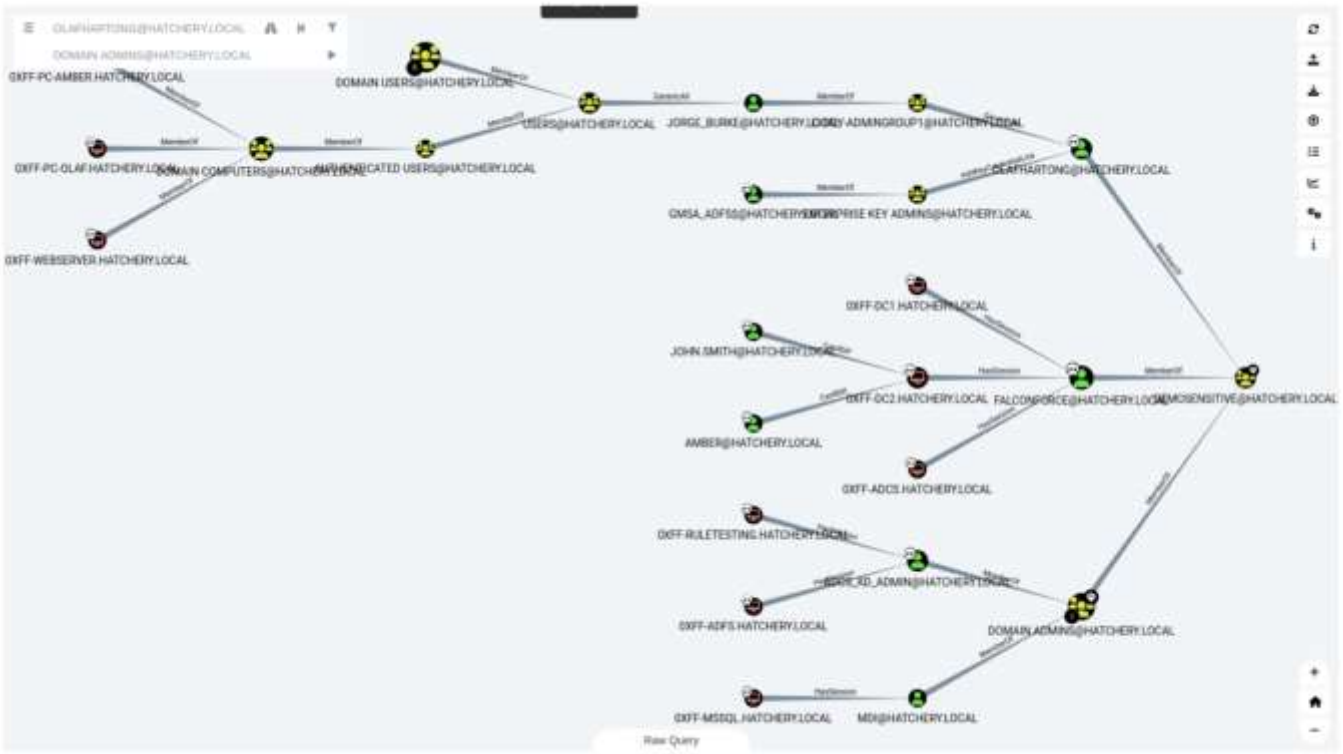
TenantId	
SourceSystem	RestAPI
TimeGenerated [UTC]	2023-10-13T14:55:07.6708278Z
BHQuery_s	MATCH a=shortestPath((u:User {owned:true})-[*..]->({highvalue:TRUE})) RETURN a
EventID_s	N4J_Owned_User_to_HighValue
Description_s	Counts all direct and nested shortest paths to HighValue nodes from owned users
EventData_s	[{"Direct":1,"DirectNames":[' [redacted] T","Nested":1,"N
Name_s	AD Owned User with a path to high value assets
Type	DemoFalconHound_CL

How can we use this?

BloodHound details

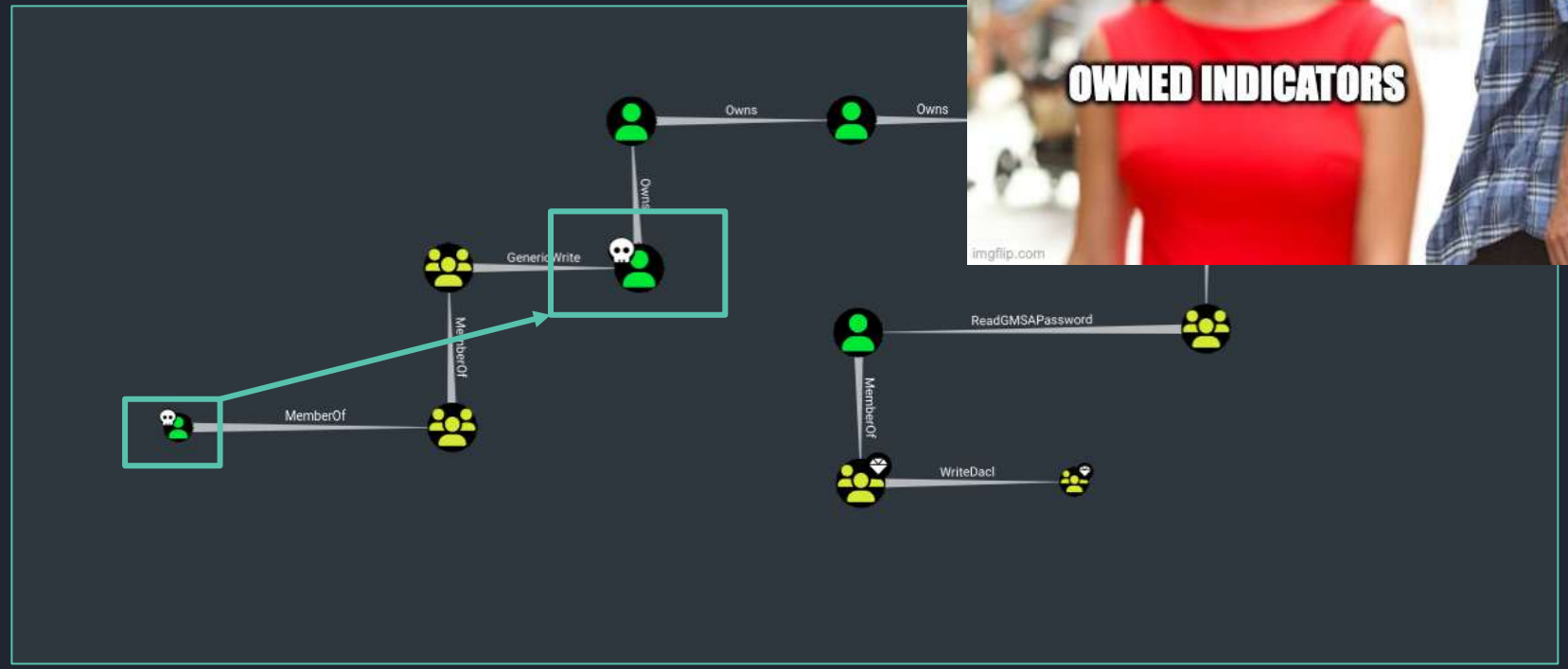
Name	Value
Outbound transitive objects	5024
Inbound transitive objects	6
Total objects in BloodHound	7203
Path to sensitive resources	TRUE

Bloodhound paths to sensitive resources:



How can we use this?

- Alert on a lateral movement path being traversed
- **AND** *(attempt to)* predict the next steps to investigate



Real-world example - Bears reading emails

January 25, 2024

Microsoft Defender for Cloud Apps

Microsoft Defender XDR

Microsoft Entra

more

The Microsoft security team dete
systems on January 12, 2024, an
investigate, disrupt malicious act
actor further access. The Microso
threat actor as Midnight Blizzard
as NOBELIUM. The latest inform
Center (MSRC) is posted here.

As stated in the MSRC blog, give
resourced and funded by nation
strike between security and busi
no longer sufficient. For Microso
to move even faster.

SPECTEROPS

Microsoft Breach:
What happened?
What should Azure admins do?

ANDY ROBBINS
Principal Product Architect

0:00 / 1:01:20

Microsoft Breach: What Happened? What Should Azure Admins Do?

SpecterOps
4.63K subscribers

Subscribe

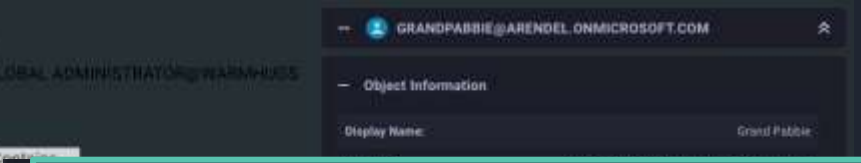
138

Share

Save

4.5K views 1 month ago
Microsoft disclosed the details of their breach at the hands of Midnight Blizzard. In this video, we explain and demonstrate what happened, and provide some analysis on what the real impact of this breach could be.
...more

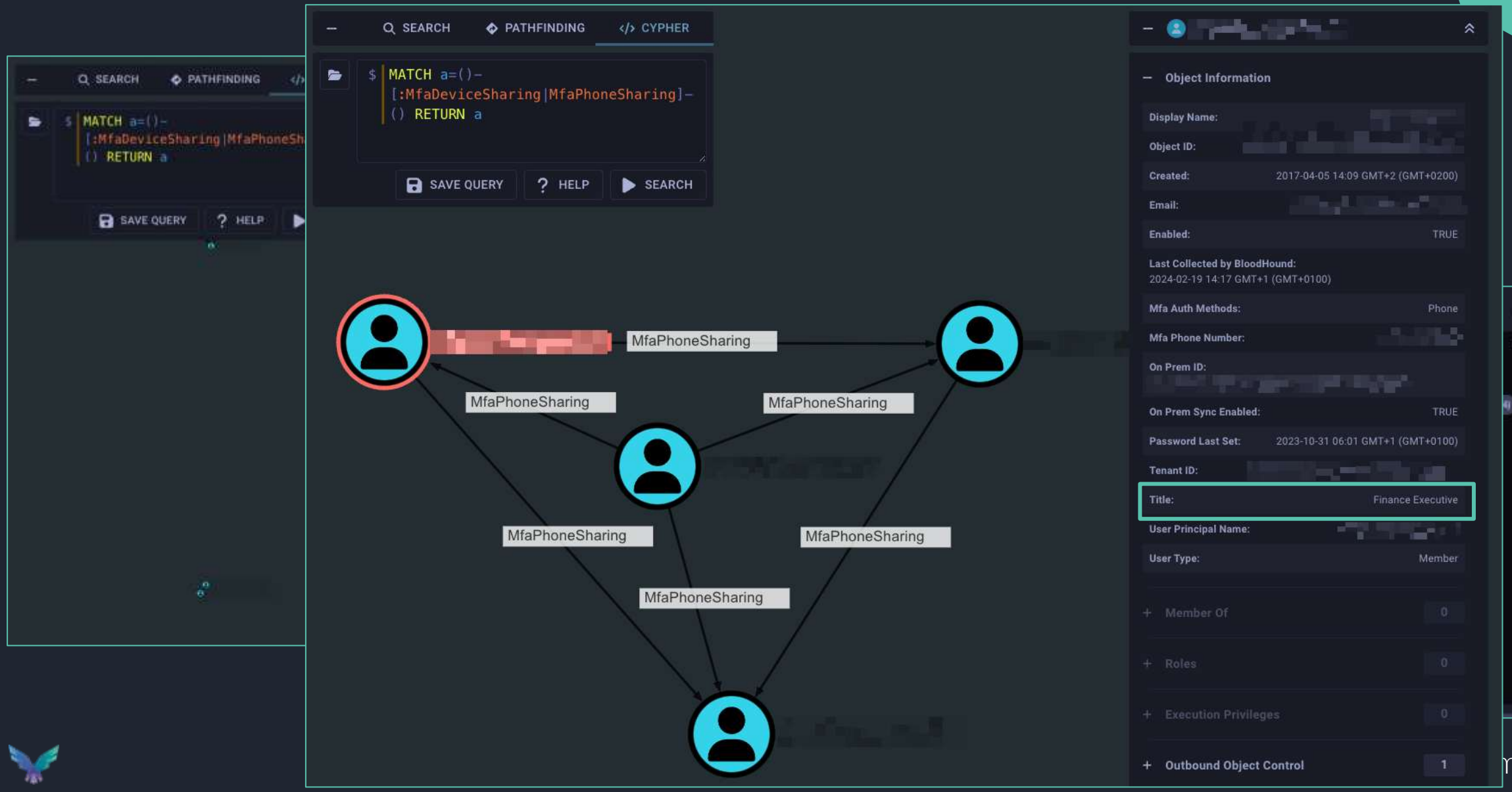
Bears reading emails



Mfa Auth Methods:	Phone
	Email
Mfa Email Address:	ROAR@G.RU
Mfa Phone Number:	+1 5055034455
Mfa Sign In Preference:	sms
Mfa Sms Method:	notAllowedByPolicy
On Prem Sync Enabled:	FALSE
Password Last Set:	2024-02-08 20:11 GMT+1 (GMT+0100)
Tenant ID:	597A06D3-53DA-4BAF-B808-673573EB31A6
Title:	King of the Trolls
User Principal Name:	GrandPabbie@arendel.onmicrosoft.com
User Type:	Member

Bears reading emails – and potentially more

Hunt down account sharing or hijacking



Implementation recommendation

Sharphound & Azurehound

Periodically

- Not all details are in the logs
- Incremental collections with LDAP filter
- Sessions not needed
- Run it every week/month

FalconHound

Every 15 minutes

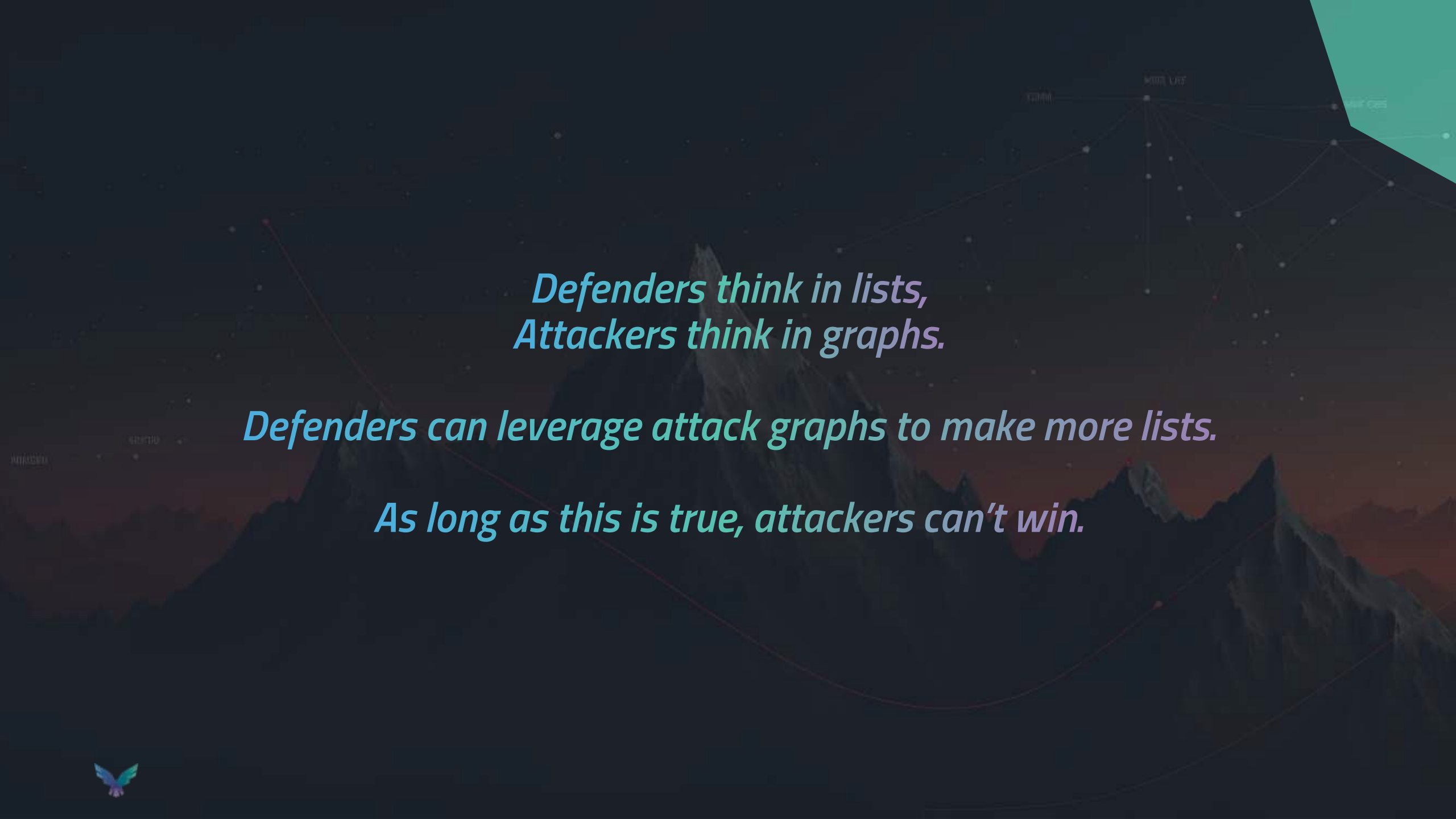
- Set as a scheduled task / cron job
- Collects sessions, new objects
- New / updated path calculations
- Watchlists / Lookup lists for detections

BloodHound Community/Enterprise

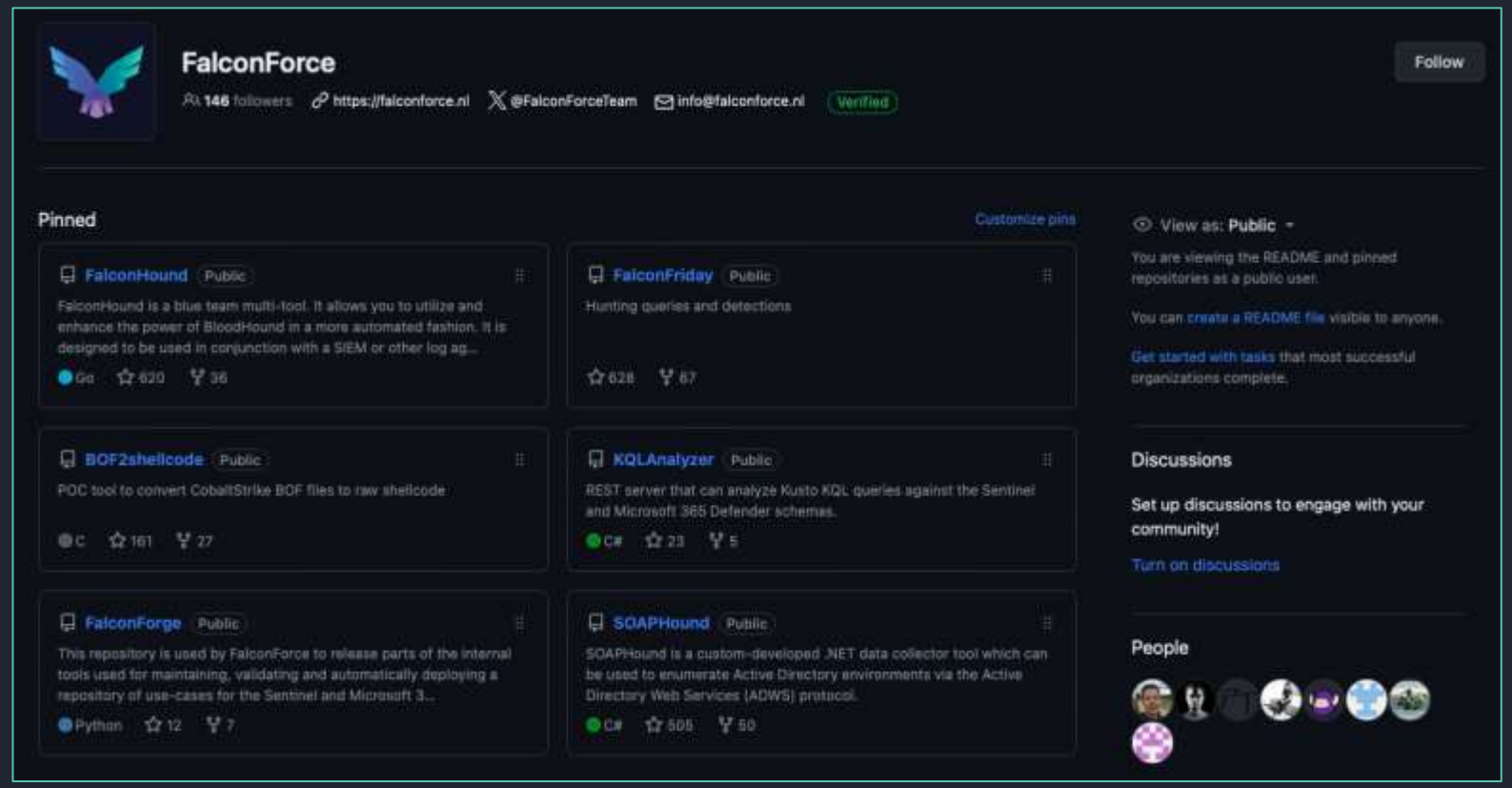
- BloodHound CE / Enterprise APIs rely on objectids (SIDs)
- Logs don't contain SIDs
- BloodHound CE is currently supported through Neo4j
- BH API support is under development

Why you should consider implementation

- Up to date sessions, MFA settings, Alerts, Vulnerability info etc
- Coverage for unexpected account sharing
- Continuous attack-path detection, including lateral movement detection
- Input for detection enrichment and dynamic alert prioritization
- Great resource for incident investigations and impact assessments


Defenders think in lists,
Attackers think in graphs.
Defenders can leverage attack graphs to make more lists.
As long as this is true, attackers can't win.

FalconHound, available now!



https://github.com/FalconForceTeam/FalconHound

Contributions welcome!

Thank you! <3

olaf@falconforce.nl

https://falconforce.nl

@olafhartong
@falconforceteam

https://linkedin.com/in/olafhartong
https://linkedin.com/company/falconforce