





The Dog Ate My Homework...

(re)Building a PowerShell Module for the New BloodHound

SadProcessor

SpecterOps







Some say
I love the Captain...



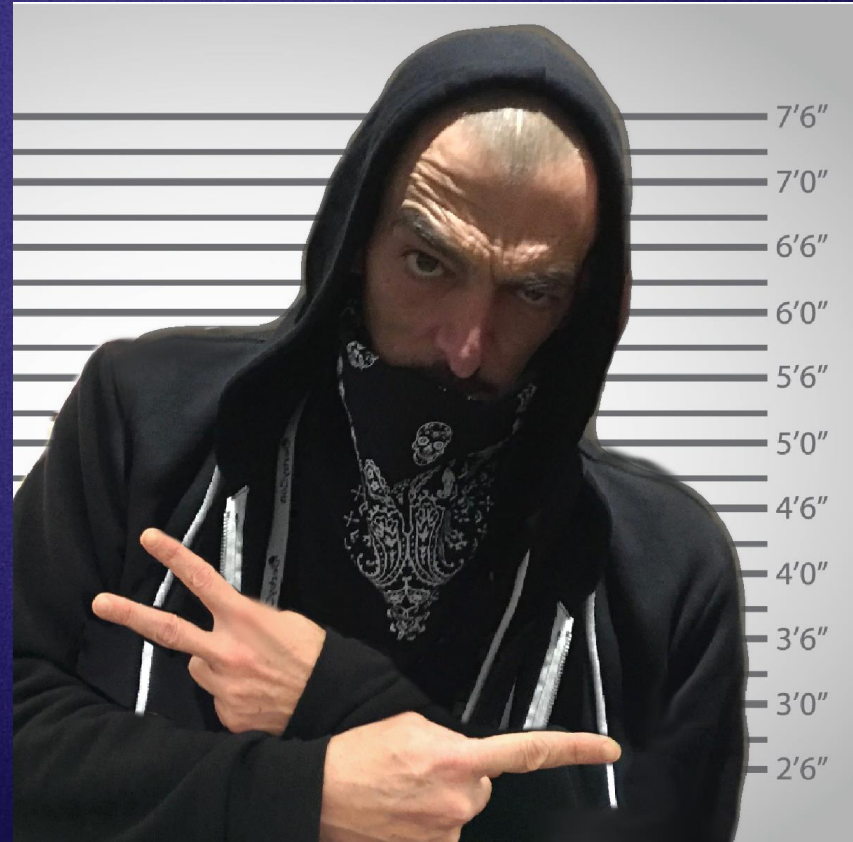


Some say
I dream in Graphs...



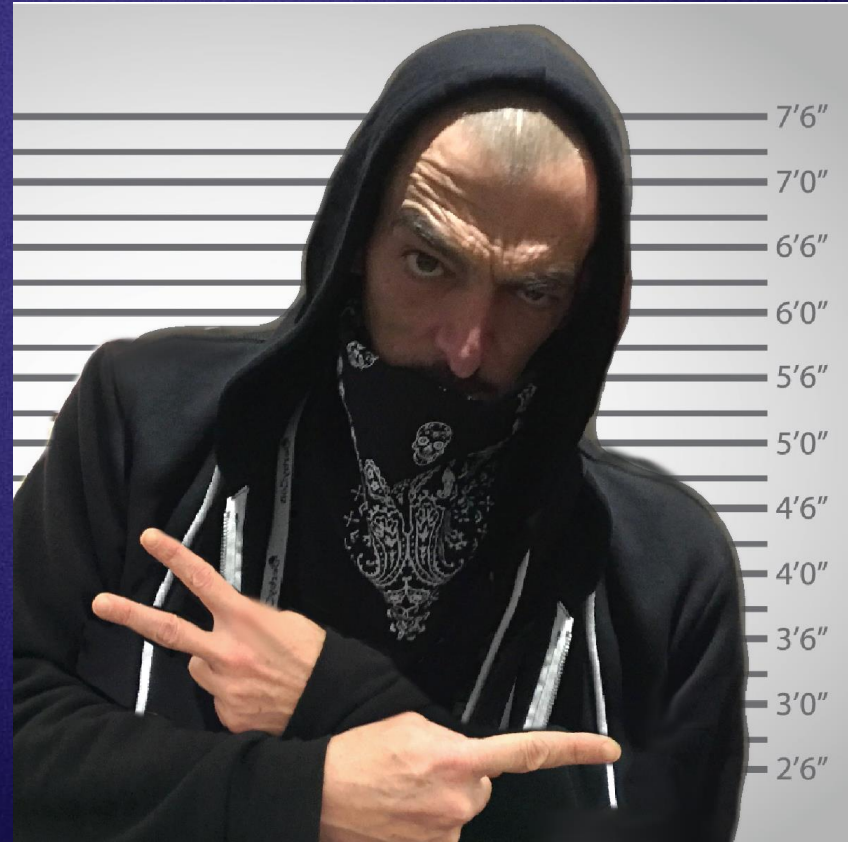


Others say
I'm just a PowerShell
Bad Boy...



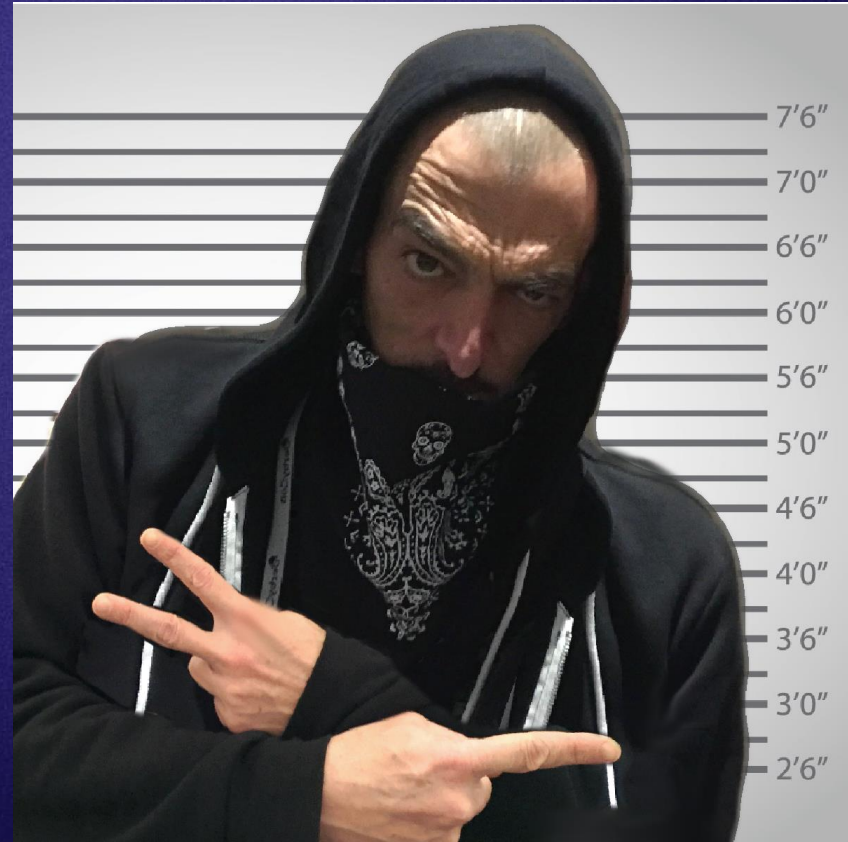


*I can
neither confirm
nor deny
any of these
statements...*





- SadProcessor – Walter Legowski
- Born FR / Home NL / Father x3
- ERNW / FalconForce / SpecterOps
- PowerShell all the Things!!
- Dog Whisperer Handbook
- CypherDog / WatchDog / ZipHound
BHQlib / FalconHound





- SadProcessor – Walter Legowski
- Born FR / Home NL / Father x3
- ERNW / FalconForce / SpecterOps
- PowerShell all the Things!!
- Dog Whisperer Handbook
- CypherDog / WatchDog / ZipHound
BHQlib / FalconHound





- SadProcessor – Walter Legowski
- Born FR / Home NL / Father x3
- ERNW / FalconForce / SpecterOps
- PowerShell all the Things!!
- Dog Whisperer Handbook
- PowerShell BloodHound Operator





Agenda

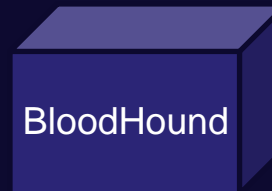
- Intro
- Old BloodHound vs. New BloodHound
- New BloodHound REST API
- PowerShell BloodHound Operator
- What Next...
- Q&A



Old BloodHound vs. New BloodHound



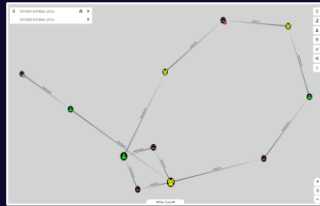
Old vs. New – Components



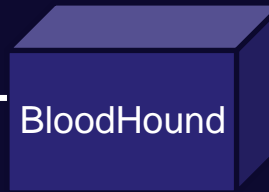


Old vs. New – Components: Old BloodHound

BH Legacy

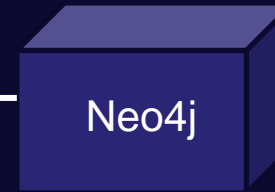


UI



BloodHound

bin

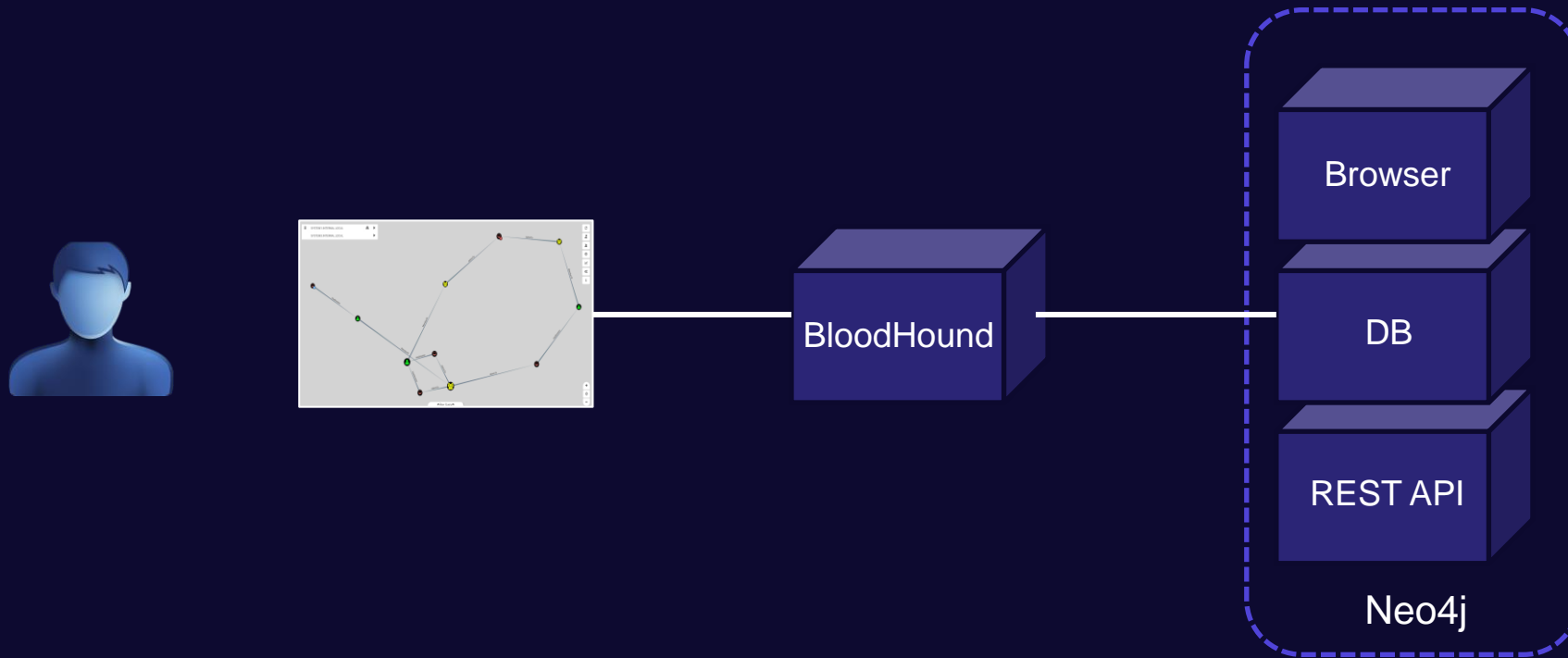


Neo4j

DB

Old vs. New – Components: Old BloodHound

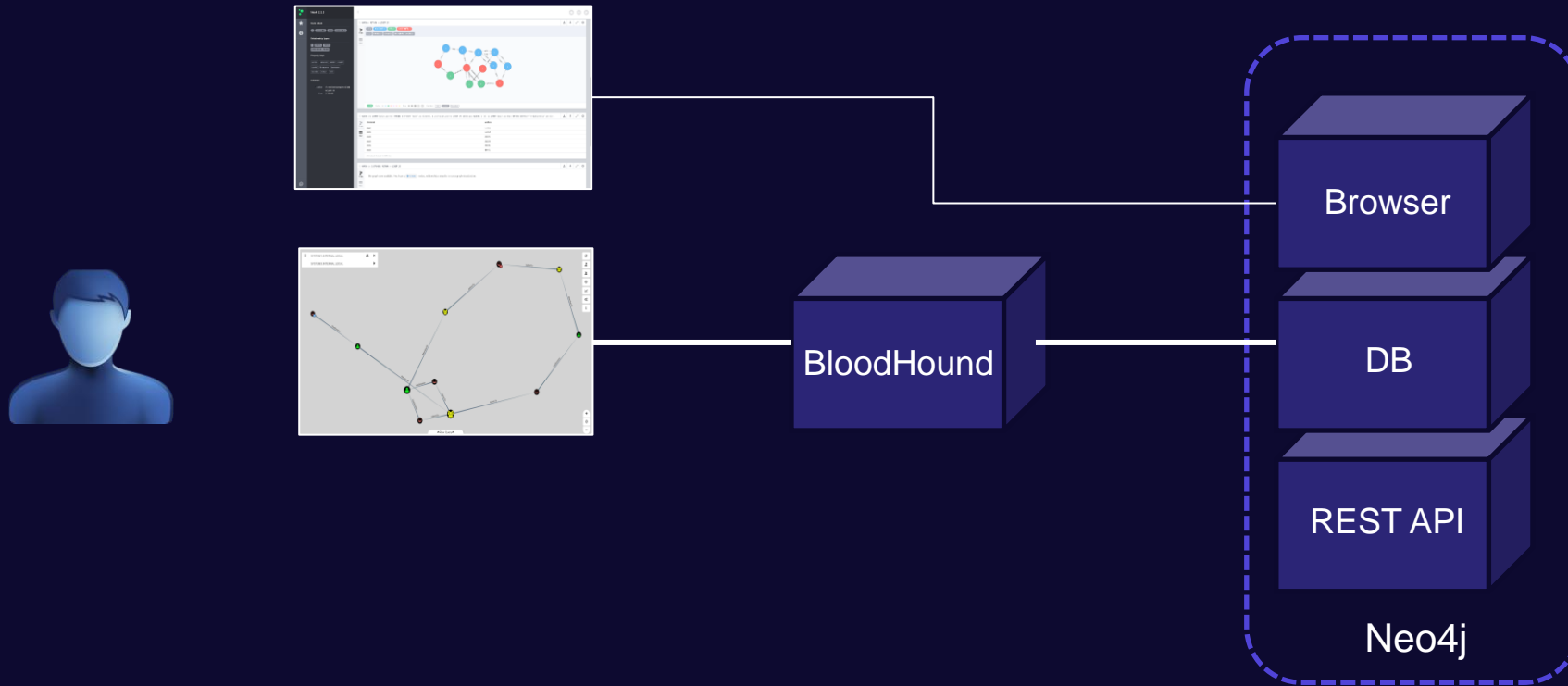
BH Legacy





Old vs. New – Components: Old BloodHound

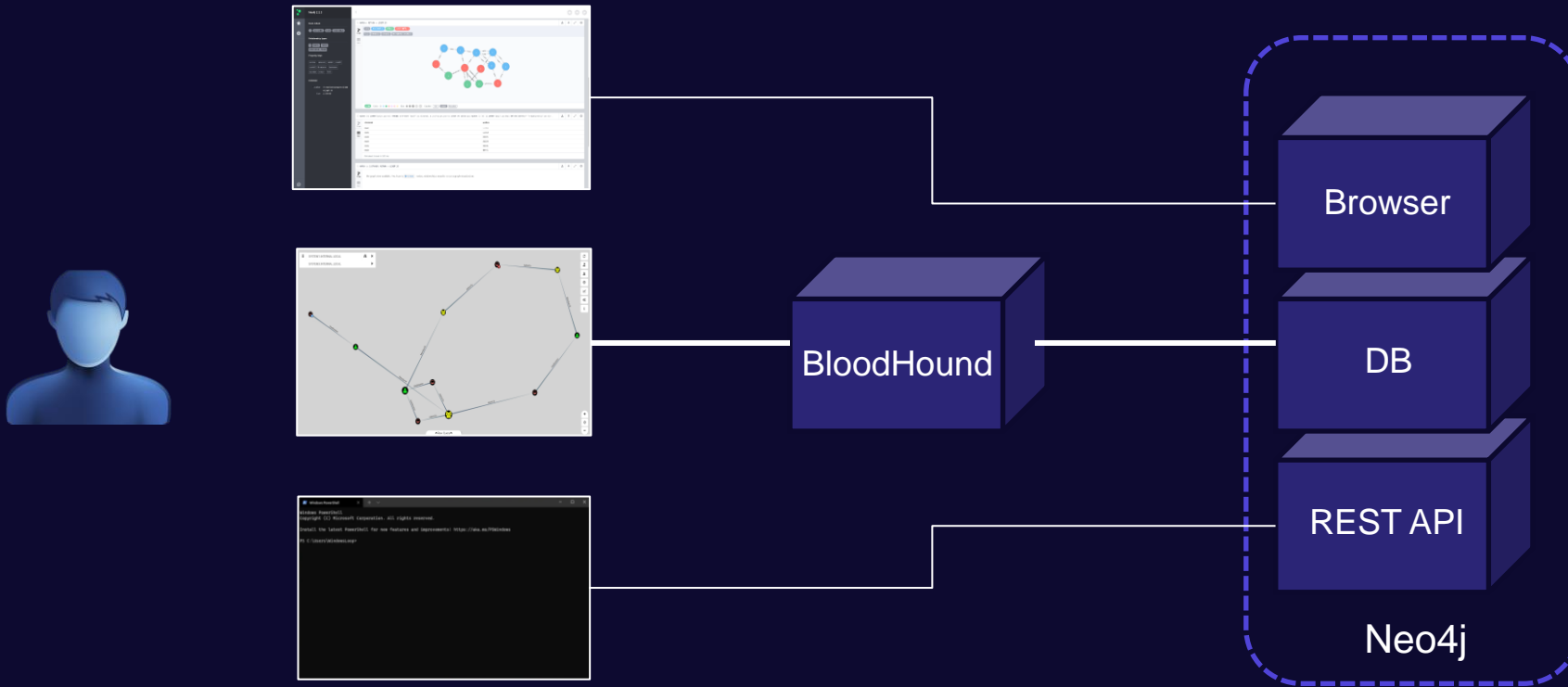
BH Legacy





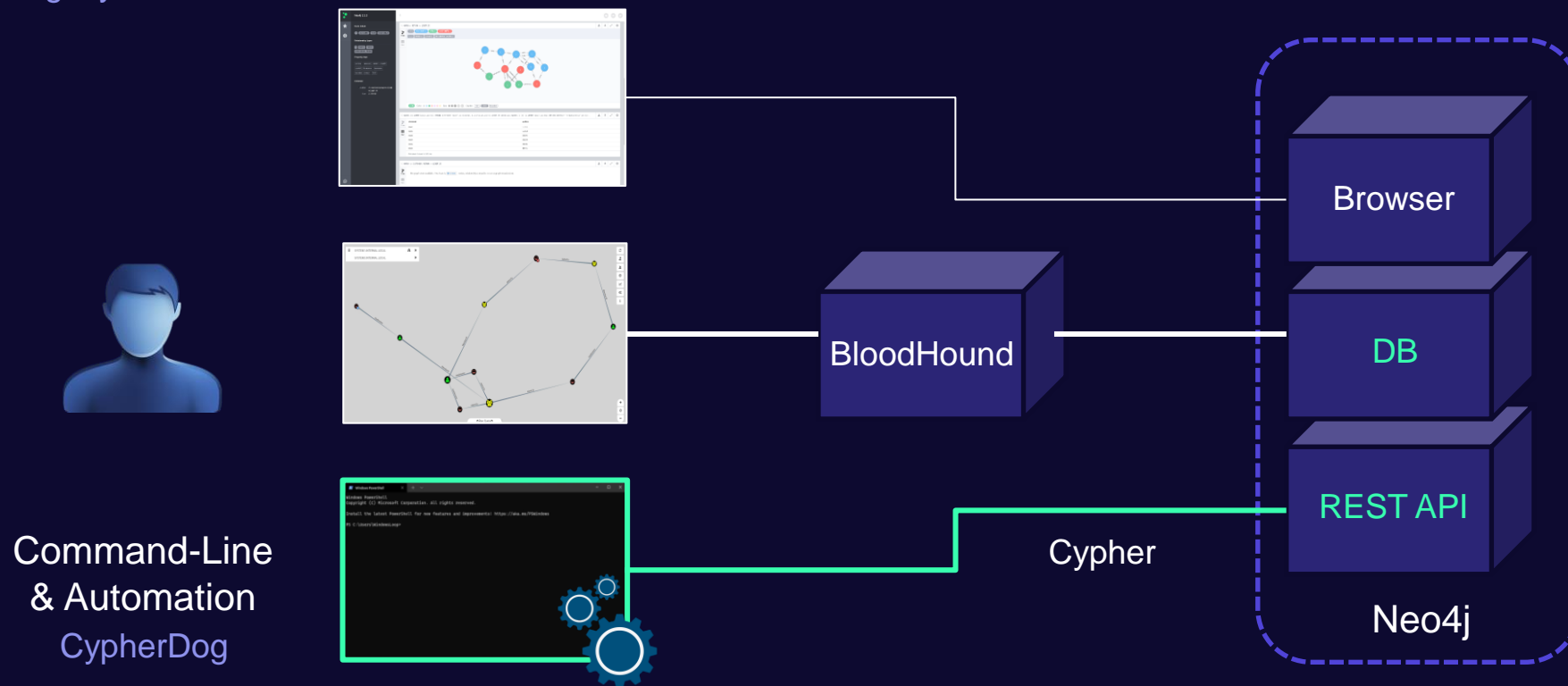
Old vs. New – Components: Old BloodHound

BH Legacy



Old vs. New – Components: Old BloodHound

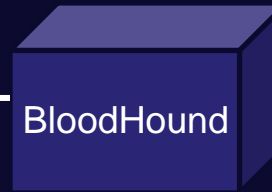
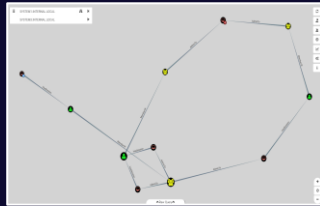
BH Legacy



Command-Line
& Automation
CypherDog

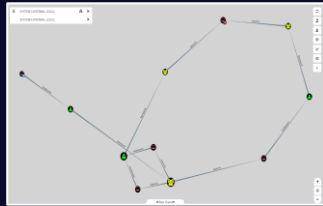
Old vs. New – Components: New BloodHound

BHE / BHCE



Old vs. New – Components: New BloodHound

BHE / BHCE



BloodHound

PostgreSQL

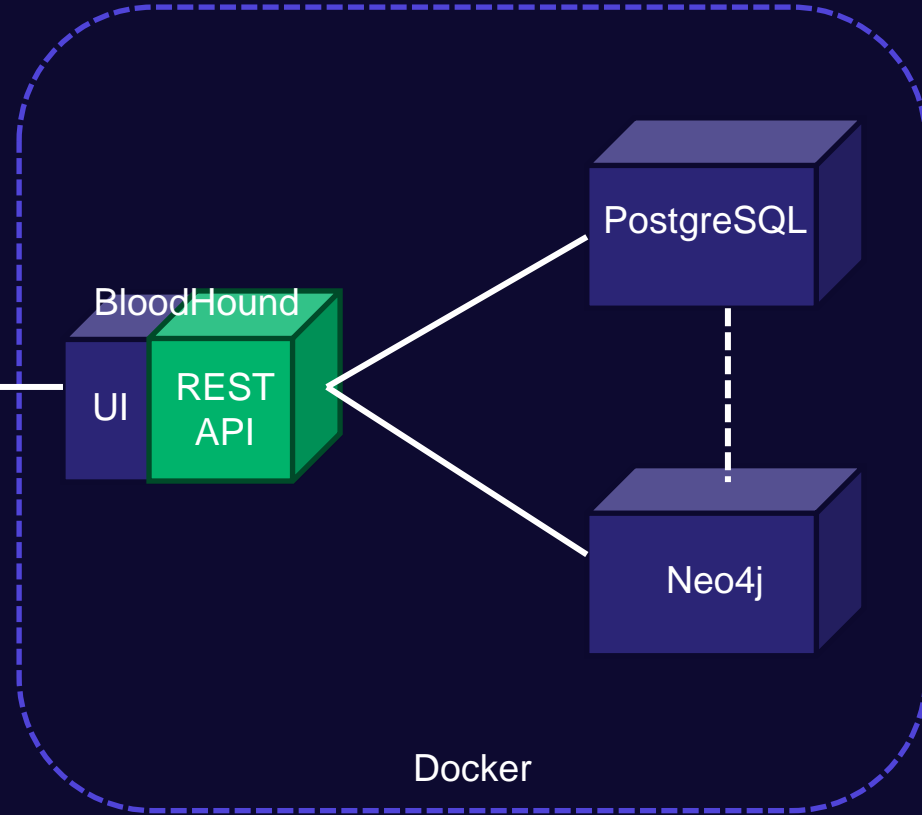
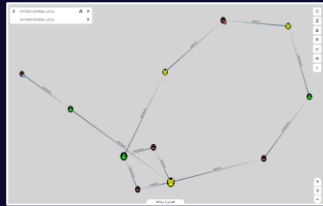
Neo4j

Docker



Old vs. New – Components: New BloodHound

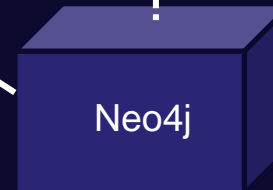
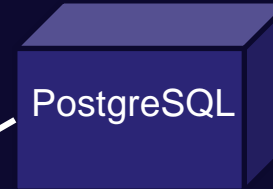
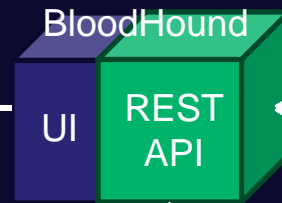
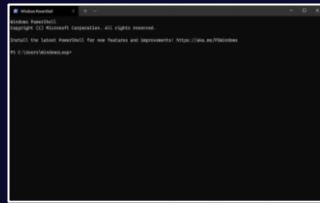
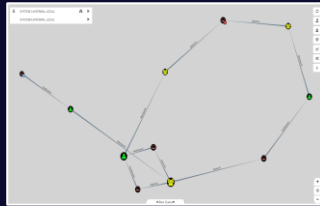
BHE / BHCE





Old vs. New – Components: New BloodHound

BHE / BHCE

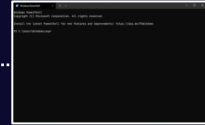
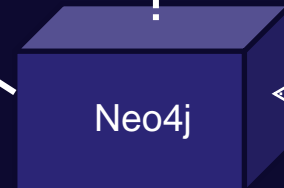
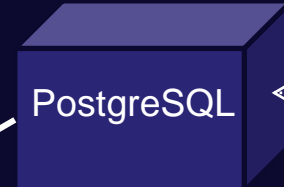
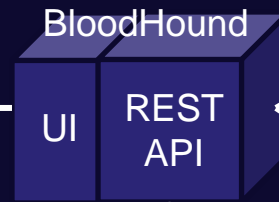
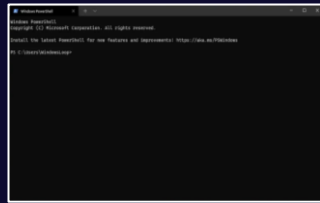
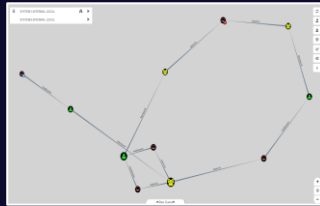


Docker

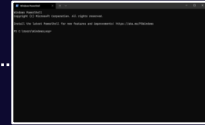


Old vs. New – Components: New BloodHound

BHE / BHCE



Exposable in
BHCE
via Config

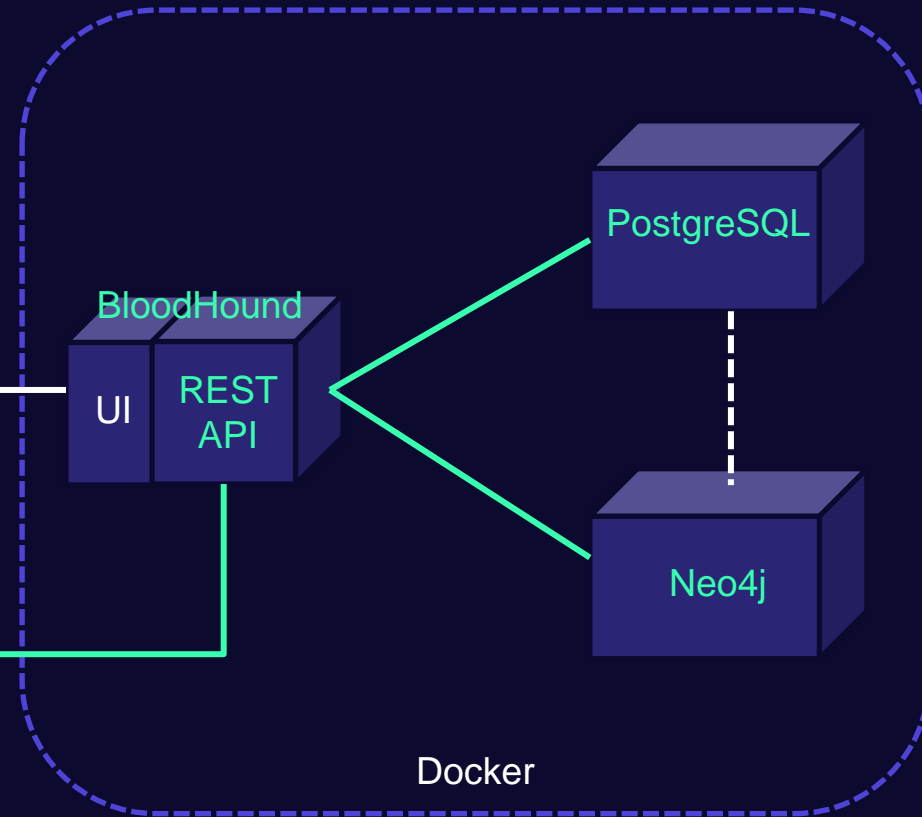
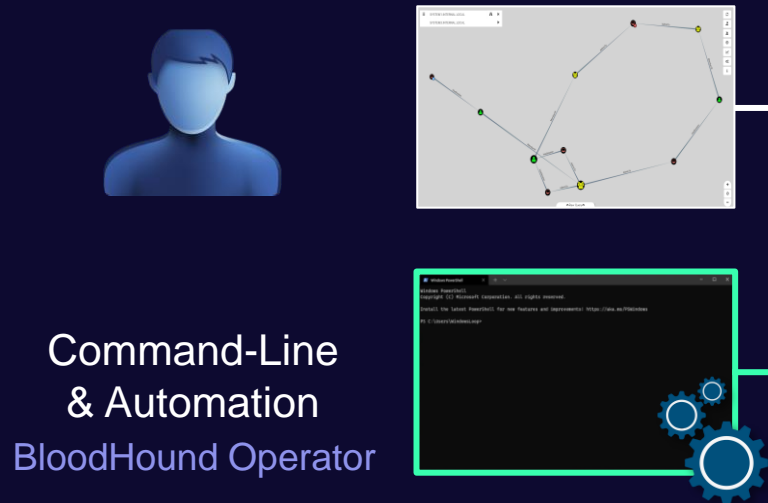


Docker



Old vs. New – Components: New BloodHound

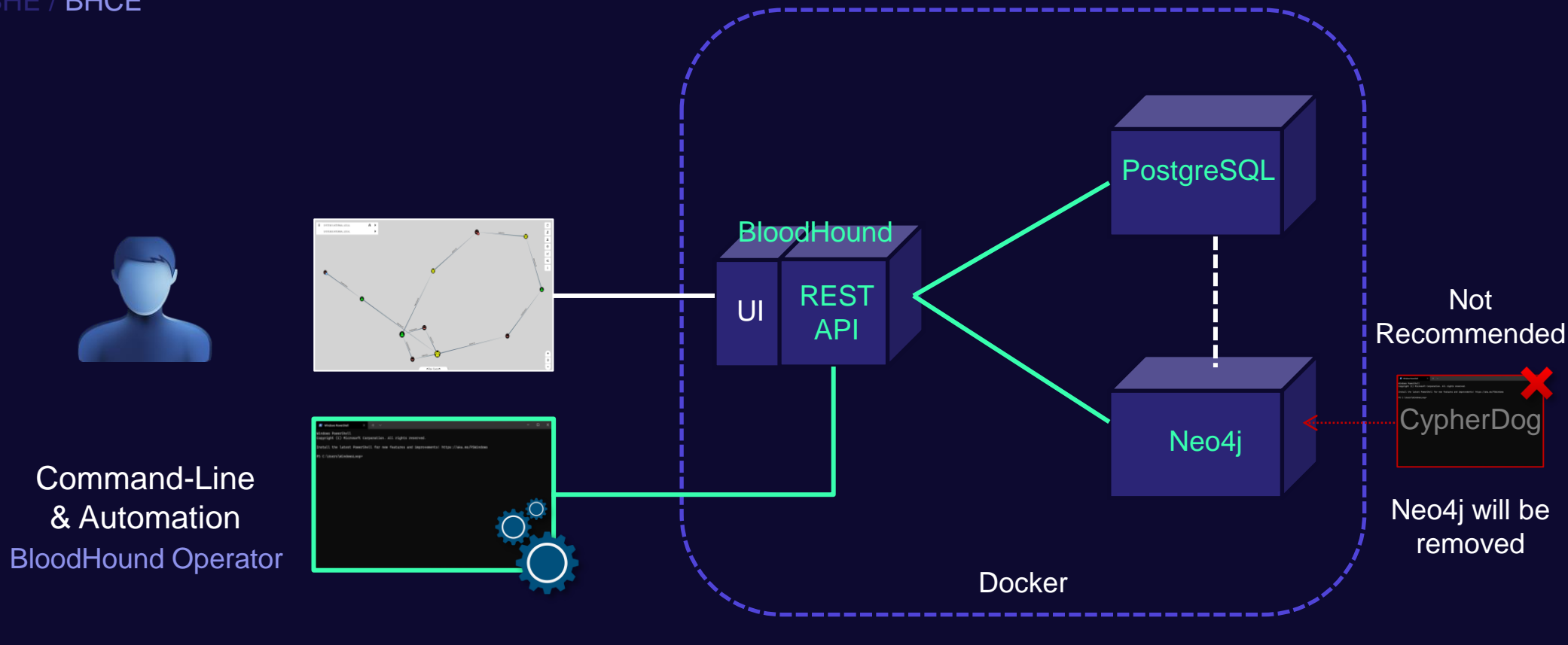
BHE / BHCE





Old vs. New – Components: New BloodHound

BHE / BHCE



Old vs. New – Feature Comparison

FEATURE	LEGACY	COMMUNITY
Easy Install	✗	✓
User Management	n/a	✓
Secure Authentication	✗	✓
Custom Queries via REST API	✓	✓ *
Data Ingestion via REST API	✗	✓
Other Actions via REST API	✗	✓



Old vs. New – Feature Comparison

FEATURE	LEGACY	COMMUNITY
Easy Install	✗	✓
User Management	n/a	✓
Secure Authentication	✗	✓
Custom Queries via REST API	✓	✓ *
Data Ingestion via REST API	✗	✓
Other Actions via REST API	✗	✓
ADCS Attack Paths	✗	✓



New BloodHound REST API





BloodHound REST API – Overview

- Exposes all functionalities of UI
- Follows OpenAPI specs
- Secure Authentication
- Shared BHCE / BHE structure
- Endpoints: BHCE=142 / BHE=195
- Explorable in UI

API Explorer

Filter by tag

Method	Endpoint	Description	Icon
GET	/api/v2/accept-eula	Accept EULA	
GET	/api/v2/bloodhound-users	List Users	
POST	/api/v2/bloodhound-users	Create a New User	
DELETE	/api/v2/bloodhound-users/{user_id}	Delete a User	
GET	/api/v2/bloodhound-users/{user_id}	Lookup User	
PATCH	/api/v2/bloodhound-users/{user_id}	Update a User	
DELETE	/api/v2/bloodhound-users/{user_id}/mfa	Disenroll user from multi-factor authentication	
POST	/api/v2/bloodhound-users/{user_id}/mfa	Enroll user in MFA	
GET	/api/v2/bloodhound-users/{user_id}/mfa-activation	Returns MFA activation status for a user	
POST	/api/v2/bloodhound-users/{user_id}/mfa-activation	Activates MFA for an enrolled user	
DELETE	/api/v2/bloodhound-users/{user_id}/secret	Remove User Secret	
PUT	/api/v2/bloodhound-users/{user_id}/secret	Create or Set User Secret	
POST	/api/v2/login	Login to BloodHound	
POST	/api/v2/logout	Logout of BloodHound	
GET	/api/v2/permissions	List Permissions	
GET	/api/v2/permissions/{permission_id}	Get Permission	
GET	/api/v2/roles	List Roles	
GET	/api/v2/roles/{role_id}	Get Role	
GET	/api/v2/saml	List SAML Providers	
POST	/api/v2/saml/providers	Create a New SAML Provider from Metadata	
DELETE	/api/v2/saml/{provider_id}	Delete a SAML Provider	
GET	/api/v2/saml/{provider_id}	Get SAML Provider	
GET	/api/v2/sso	Lookup SSO	
GET	/api/v2/tokens	List Auth Tokens	
POST	/api/v2/tokens	Create Token for User	
DELETE	/api/v2/tokens/{token_id}	Delete a User Token	
GET	/api/v2/saml/sso	Get all SAML sign-on endpoints	

Data Quality Stats

GET	/api/v2/ad-domains/{domain_id}/data-quality-stats	Time series list of data quality stats for a given AD domain	
GET	/api/v2/azure-tenants/{tenant_id}/data-quality-stats	Time series list of data quality stats for a given Azure tenant	
GET	/api/v2/platform/{platform_id}/data-quality-stats	Time series list of aggregate data quality stats for a given platform	

AIACA Entity API

GET	/api/v2/aiacas/{object_id}	Get aiaca entity info	
GET	/api/v2/aiacas/{object_id}/controllers	List aiaca controllers	



BloodHound REST API – Roles & Permissions

Authority	Permission	Read-Only	Upload-Only	User	Power User	Admin
App	ReadAppConfig	✓		✓	✓	✓
App	WriteAppConfig				✓	✓
Auth	CreateToken	✓		✓	✓	✓
Auth	ManageAppConfig					✓
Auth	ManageProviders					✓
Auth	ManageSelf	✓		✓	✓	✓
Auth	ManageUsers					✓
GraphDB	Read	✓		✓	✓	✓
GraphDB	Write		✓		✓	✓
Saved_Queries	Read			✓	✓	✓
Saved_Queries	Write			✓	✓	✓
Clients	Manage				✓	✓
Clients	Read			✓	✓	✓
Clients	Taskings		✓		✓	✓
Collection	ManageJobs				✓	✓
Risks	GenerateReport	✓		✓	✓	✓
Risks	ManageRisks				✓	✓

Access to API endpoints is determined by role and associated permissions in the application

BHE only





BloodHound REST API – Authentication

- Uses **TokenID + TokenKey** (incl. User Token Lifecycle)
- Each request must be signed
- 3x HMAC SHA256
- Signature = [Hash:(((TokenKey x Operation) x Timestamp) x Body)].ToBase64
- Headers must include TokenID, Signature and Timestamp
- Server validates signature against request



[Working with the BloodHound API – BloodHound \(bloodhoundenterprise.io\)](https://bloodhoundenterprise.io)



BloodHound REST API – Authentication

```
# Signature
```

PowerShell

```
$Timestamp = [Datetime]::utcnow.toString('o')
$KeyByte   = [Text.Encoding]::UTF8.GetBytes($TokenKey)
$OpByte    = [Text.Encoding]::UTF8.GetBytes("$Method/$URI")
$DateByte  = [Text.Encoding]::UTF8.GetBytes(-join $Timestamp[0..12])
$BodyByte  = [Text.Encoding]::UTF8.GetBytes("$Body")
$HMAC      = [Security.Cryptography.HMACSHA256]::new($KeyByte).ComputeHash($OpByte)
$HMAC      = [Security.Cryptography.HMACSHA256]::new($HMAC).ComputeHash($DateByte)
$HMAC      = [Security.Cryptography.HMACSHA256]::new($HMAC).ComputeHash($BodyByte)
$Sign      = [Convert]::ToBase64String($HMAC)
```

```
# Headers
```

```
$Headers = @{
    Authorization = "BHESignature $TokenID"
    Signature     = $Sign
    RequestDate   = $Timestamp
}
```



PowerShell BloodHound Operator





BloodHound Operator – Features



PowerShell Cmdlets for the BloodHound REST API (50+)

- Verb-BHNoun Syntax / Pipeline Input / Output Objects / Tab-Completion / ...
- All application features are accessible
- Allows for scripted deployments
- Allows for full Ingest-Query-Analyze automation (DIY)
- Experimental: Multiple sessions



BloodHound Operator – Disclaimer

- Still a **Work-In-Progress...**
- ADCS / BHE endpoints not included **yet**
- Some things will change = **Break**
- Provided as Gist for beta testers / No Support (**feedback via BH Slack**)
- Not an official SpecterOps tool
- Use at your own risks...

—_ (ツ) _ /

DEMO

BloodHound Operator – Basic Usage



What's Next ?







- On my side:
- Add ADCS / BugFix / Docs
- Add BHE functionalities
- Format as proper Module
- Publish to PS Gallery
- Present at PSConfEU





- On my side:

- Add ADCS / BugFix / Docs
- Add BHE functionalities
- Format as proper Module
- Publish to PS Gallery
- Present at PSConfEU

- On your side:

- Download Gist
- Test-drive
- Feedback via BH Slack
- Wait for release
- Automate all the things...



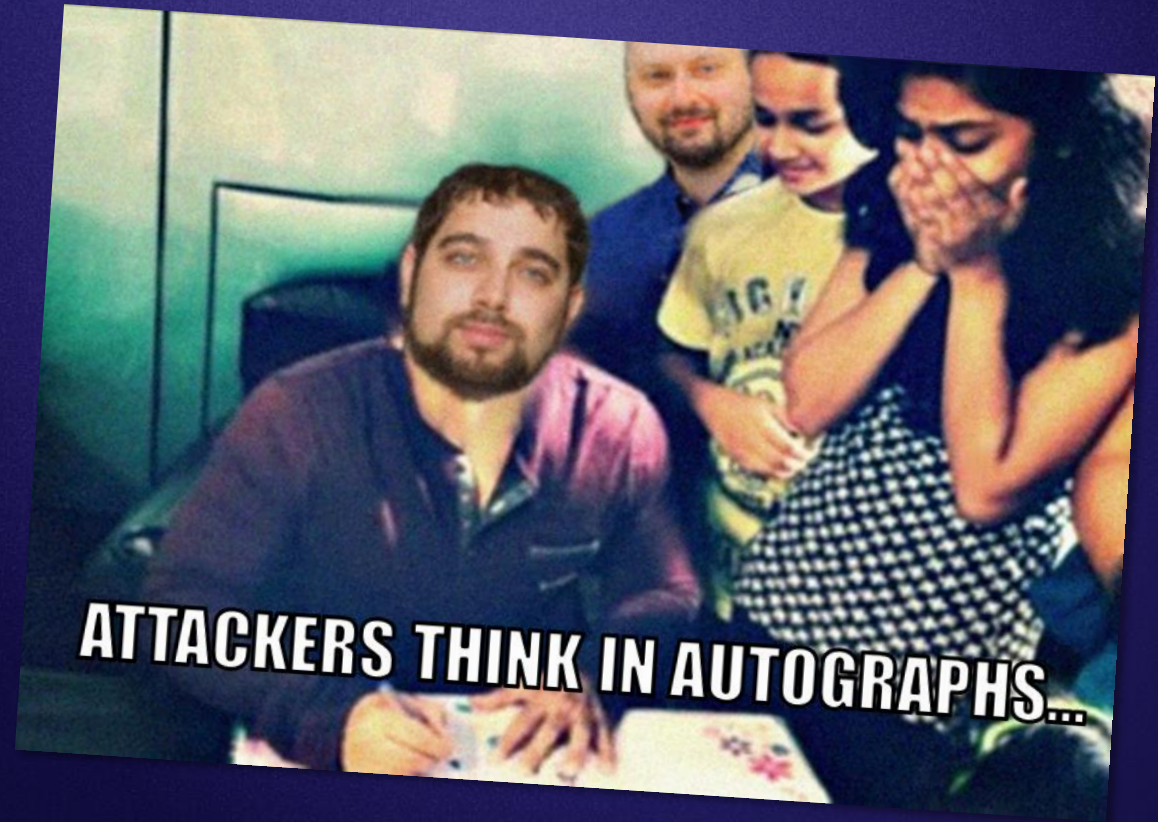
Questions ?



Reminder

CptJesus will be signing autographs in the lobby later this afternoon...

Come and get yours!





Thank you

Catch me in the lobby if you want to chat...
Enjoy the rest of SO-CON!



SadProcessor

