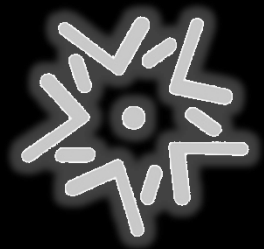
REQUIEM FOR AN ADMIN



PowerShell Conference
Singapore 2017

Microsoft

KEMP APPLICATION DELIVERY

SAPIEN Technologies, Inc.

CHEF CHEF.IO

Konfx. www.konfx.io

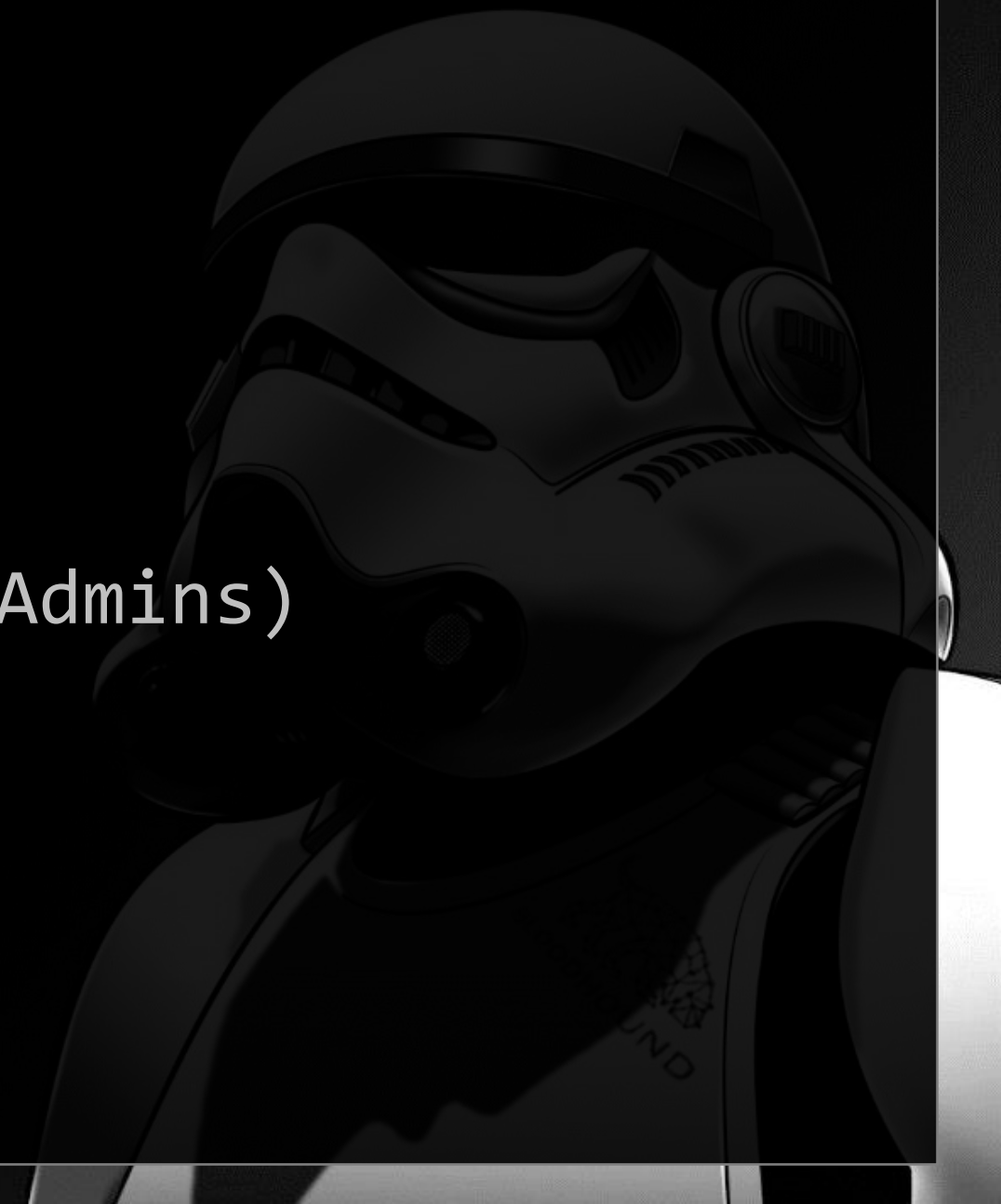
Whois

Walter Legowski

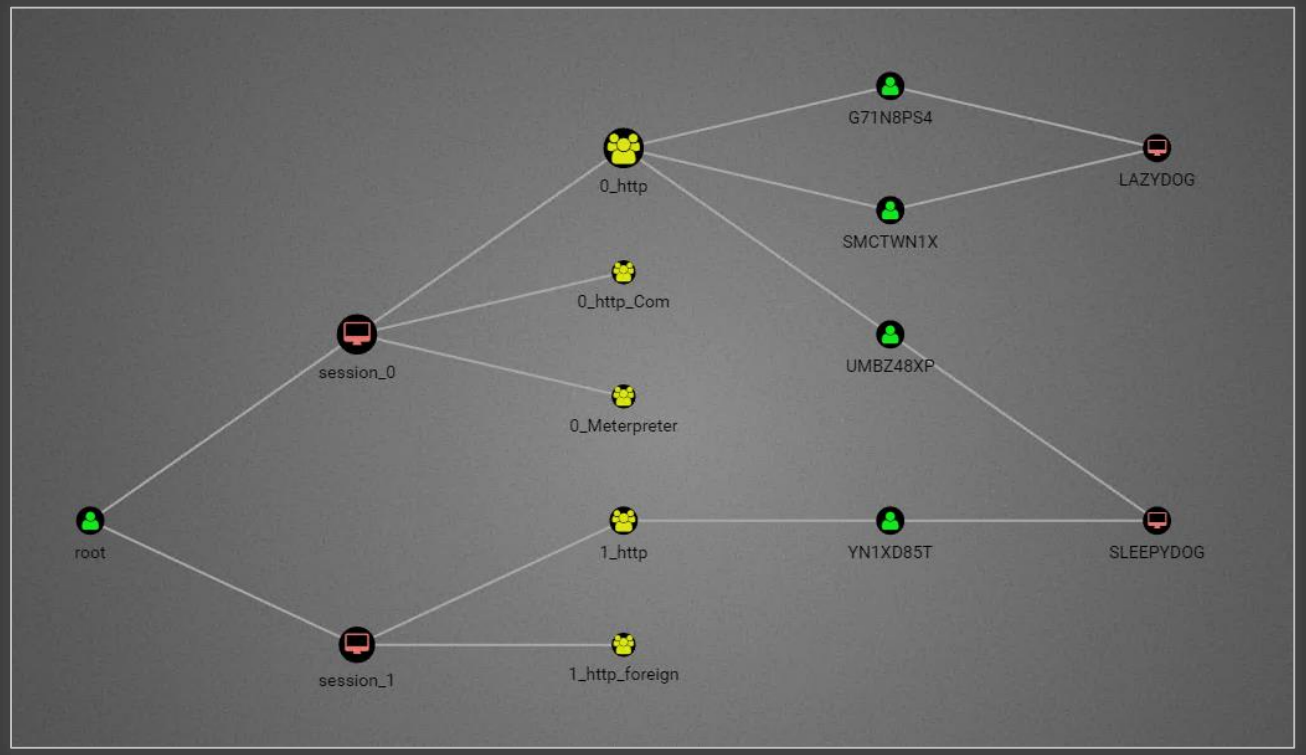
@SadProcessor

- ♥ PowerShell
- ♥ More PowerShell
- ♥ (Offensive) Tools
- ♥ Corporate Stuff (Admins)

- ♥ Wife & ♥♥♥ Kids
- ♥ Digital Arts
- ♥ Lego Bricks



Demo/POC



> Map Empire in Bloodhound

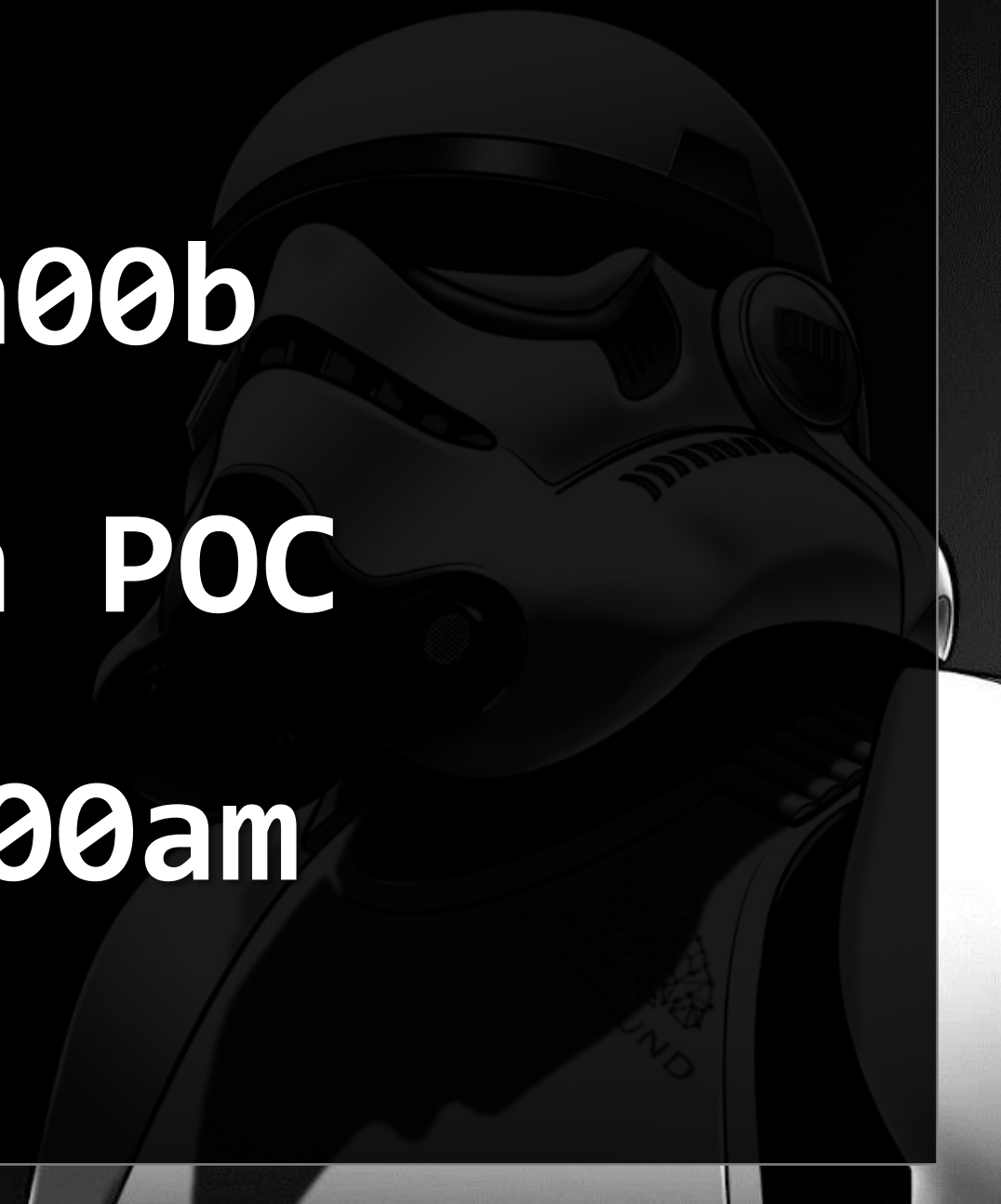
> Query “Agent Aware” Paths
>> PowerShell All Things...

Disclaimer

I am a n00b

This is a POC

It’s 10:00am



Plan

0 - Building Blocks

Orchestrating BloodHound & Empire

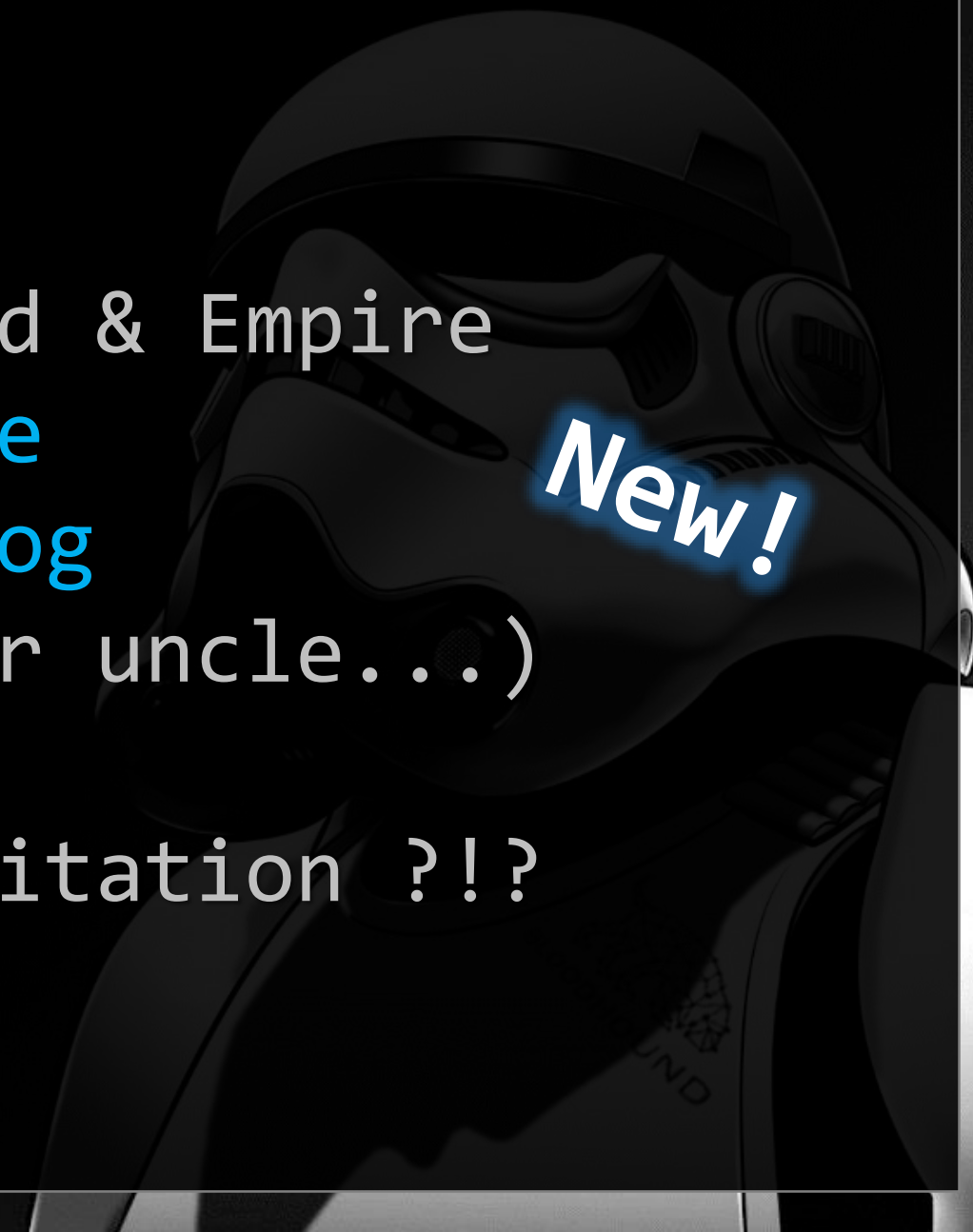
1 - Empire & EmpireStrike

2 - BloodHound & CypherDog

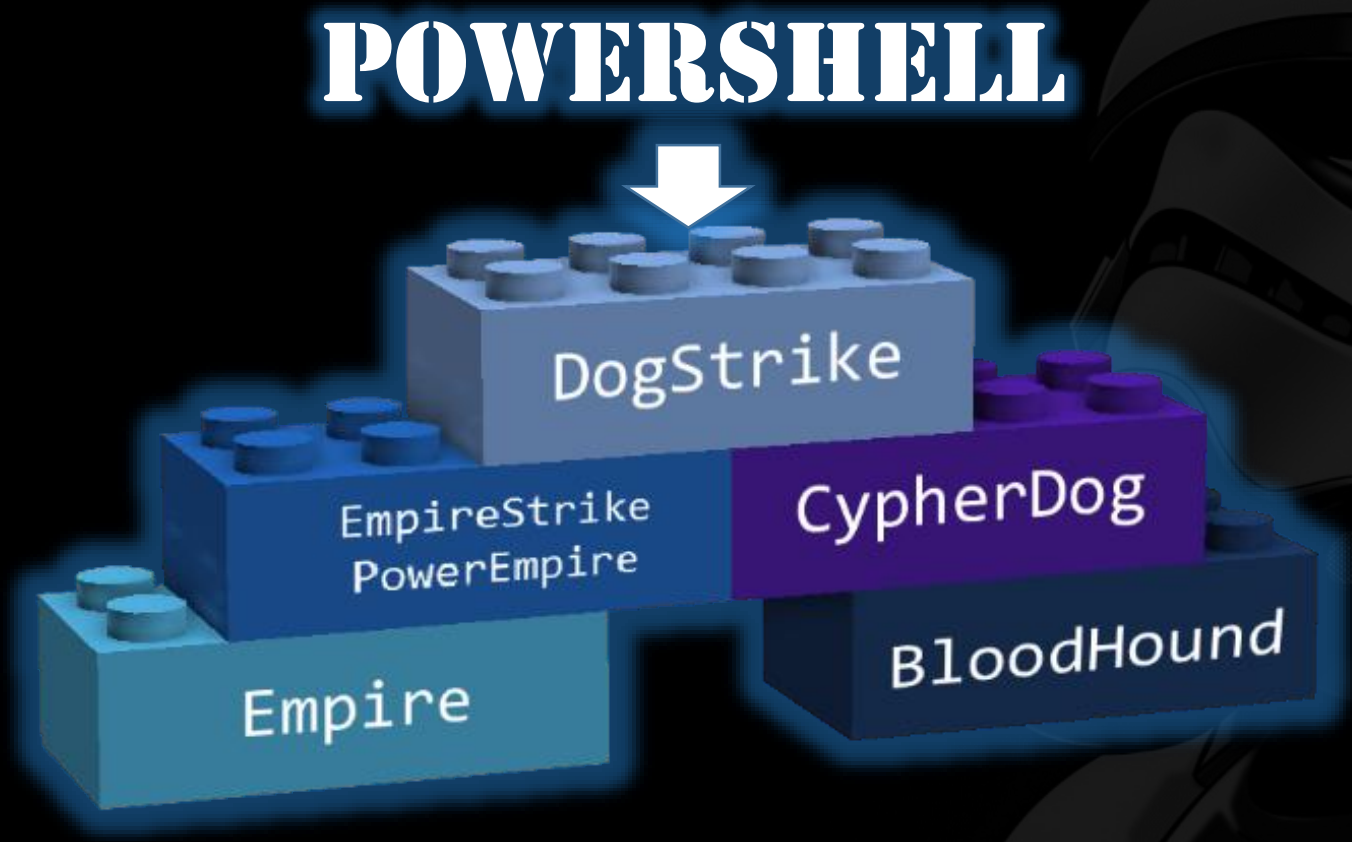
3 - DogStrike & Bob (your uncle...)

Automated AD Post-Exploitation ?!?

4 - Q&A / Open Mic



Building Blocks



Building Blocks

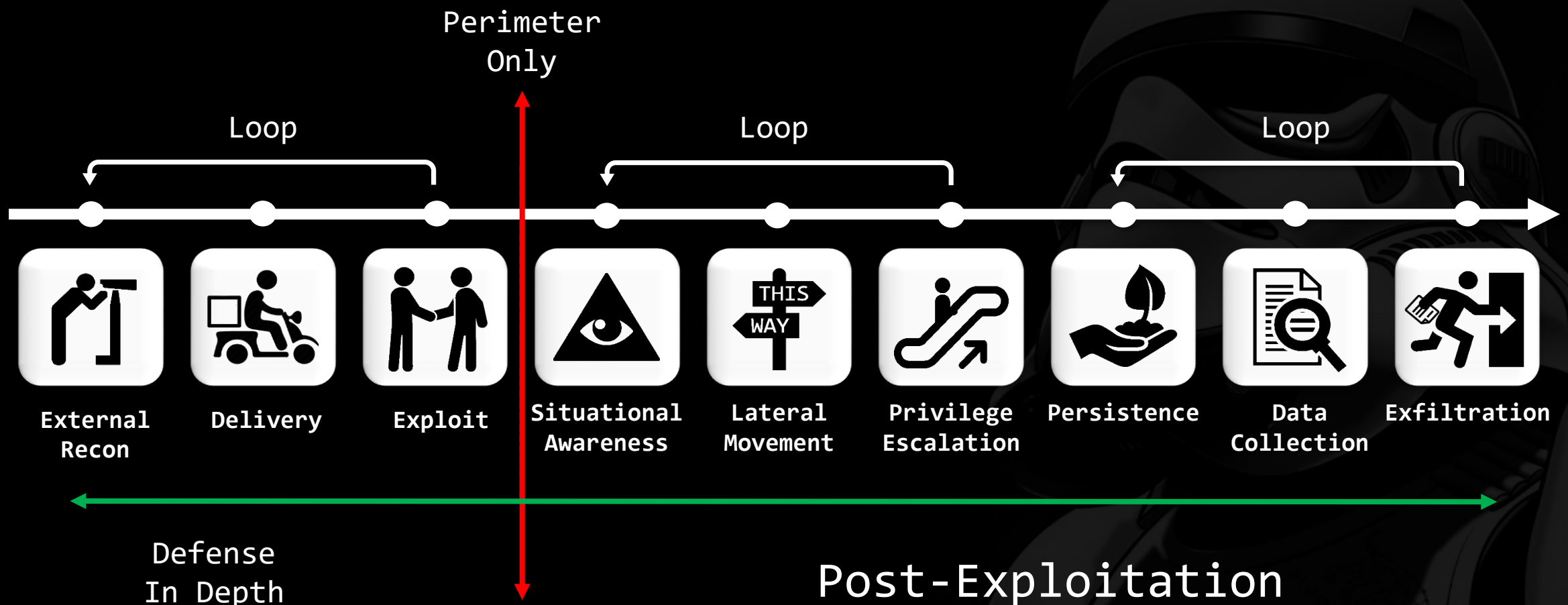
“ Standing on shoulders of Giants... ”

PART 1

Orchestrating BloodHound & Empire

> Empire & EmpireStrike

Attacker KillChain

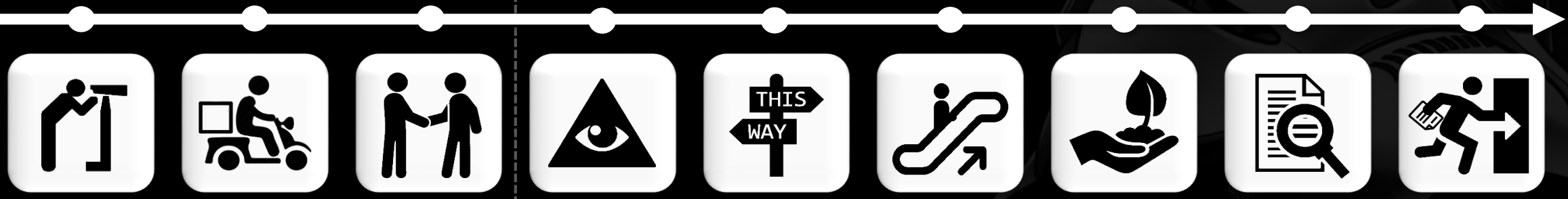


Empire - What?

```
=================================================================
 [Empire]  Post-Exploitation Framework
=================================================================
 [Version] 2.0 | [Web] https://theempire.io
=================================================================
```

First release: Aug 2015

Empire - What?



Assume Breach

Situational Awareness

Lateral Movement

Privilege Escalation

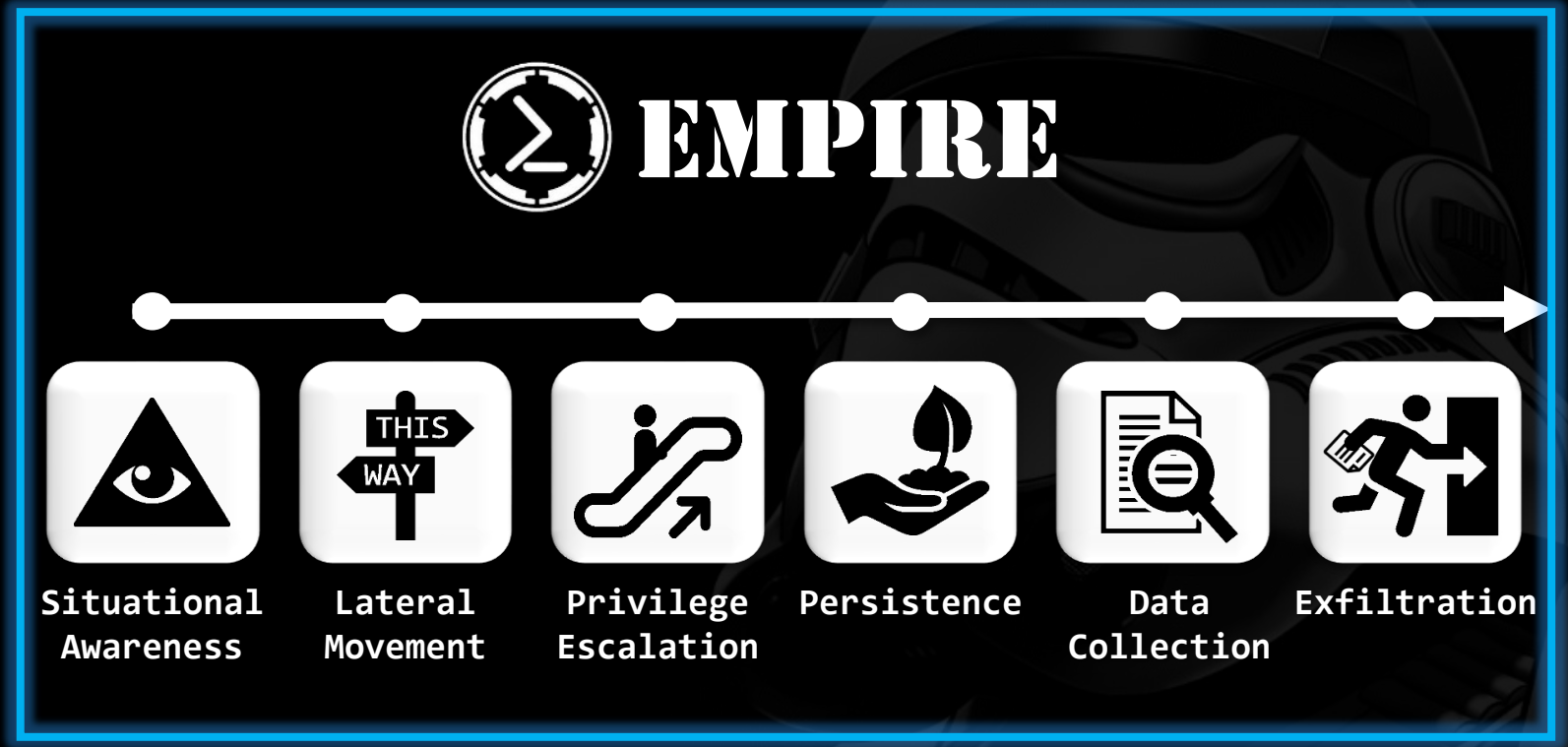
Persistence

Data Collection

Exfiltration

Empire - What?

Features
- 267 Modules
- PS & more...
- ...
- REST API <-



Post-Exploitation Framework

version 2.1 - 2017

Empire - Who?

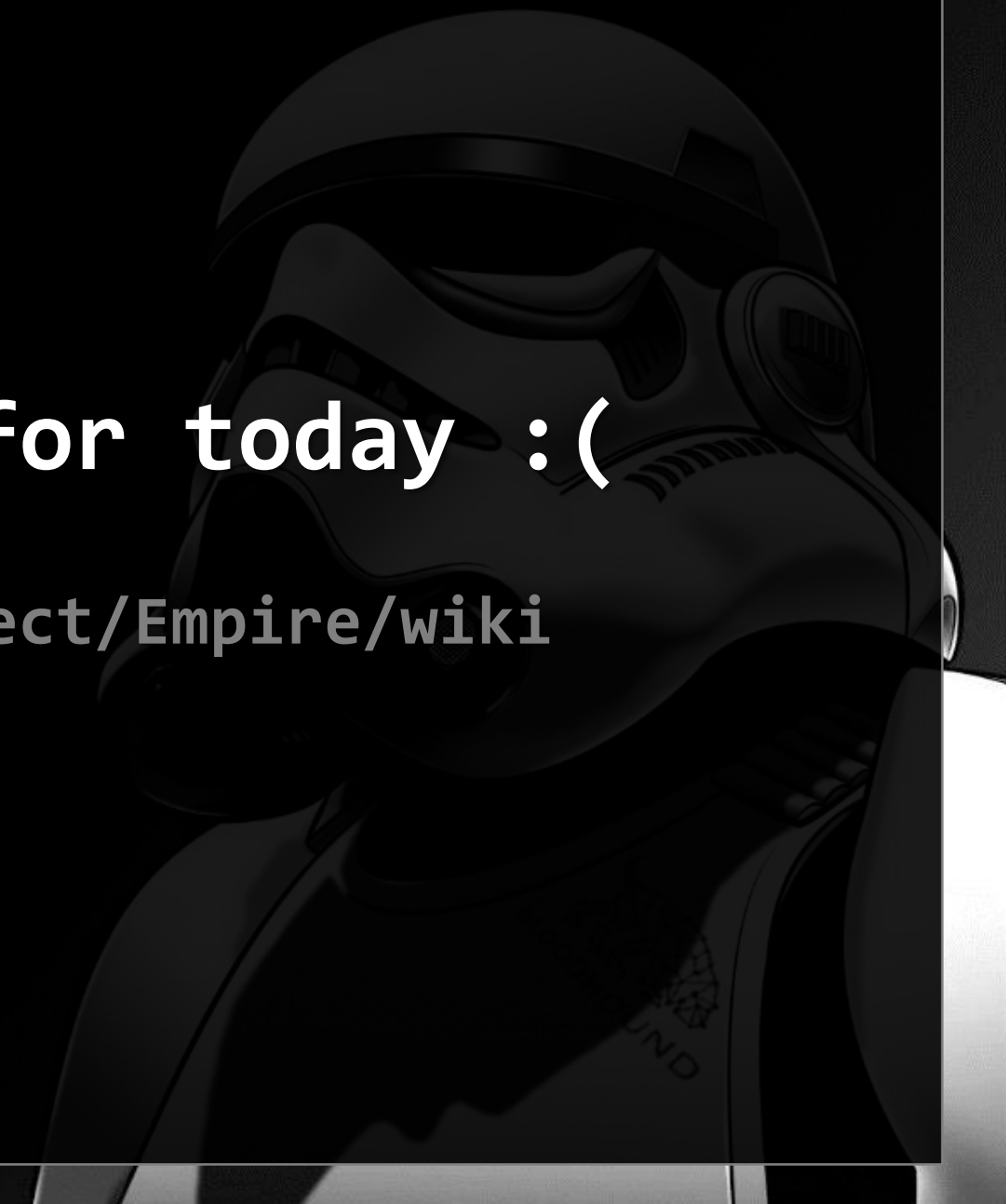
@harmj0y
@sixdub
@enigma0x3
@killswitch_gui
@xorrior
@424f424f
aka rvrsh3ll

+ Crème de la crème
Module Contributors

Empire - How?

Sorry, out of scope for today :(

https://github.com/EmpireProject/Empire/wiki



PowerEmpire - Who?

DarkOperator

@Carlos_Perez

Info & Original Source Code:
https://gitlab.com/carlos_perez/PowerEmpire/wikis/home

PowerEmpire - What?

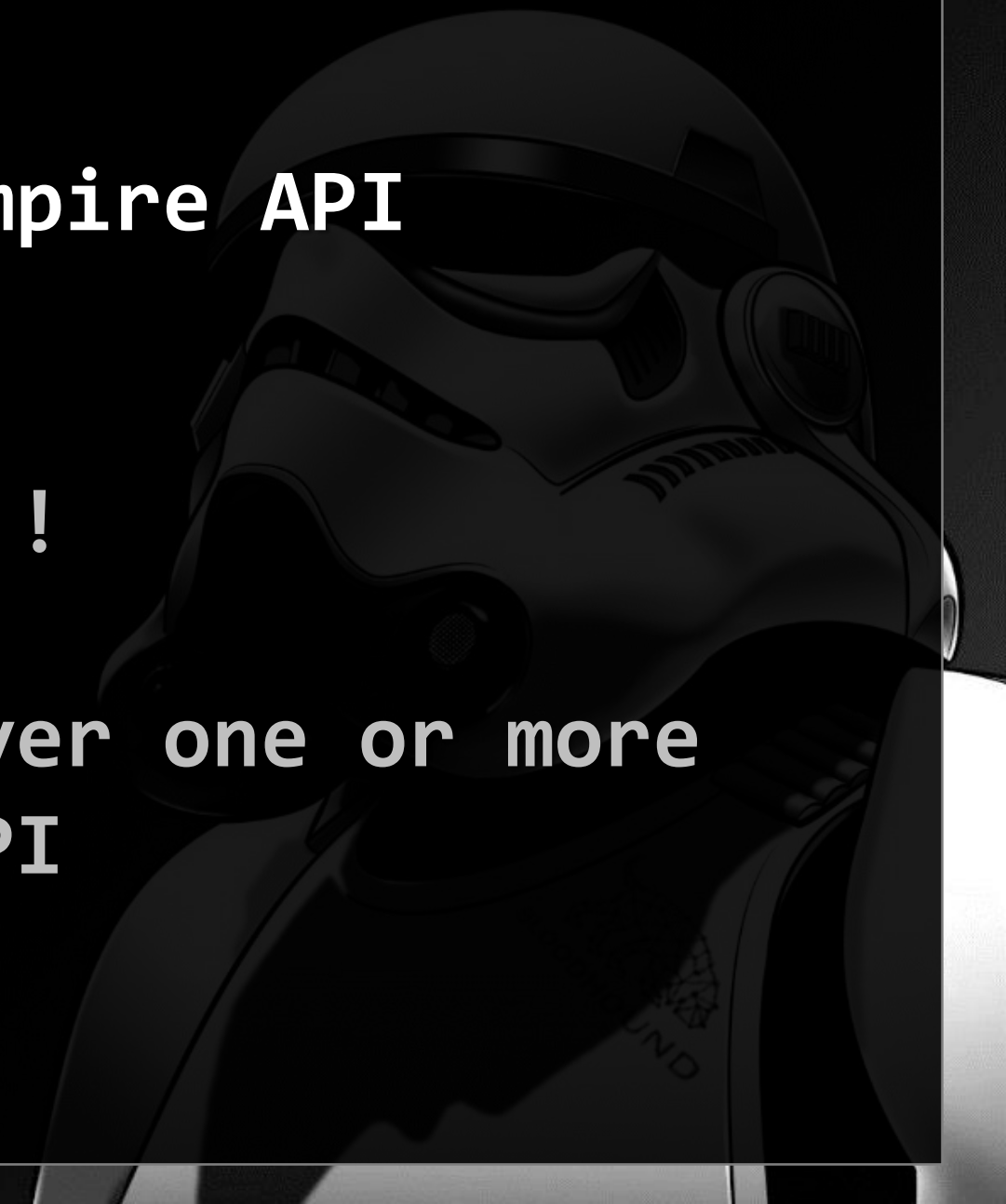
PowerShell Module for Empire API

> **27 Cmdlets**

> Multiple Sessions

> Do it with PowerShell!!

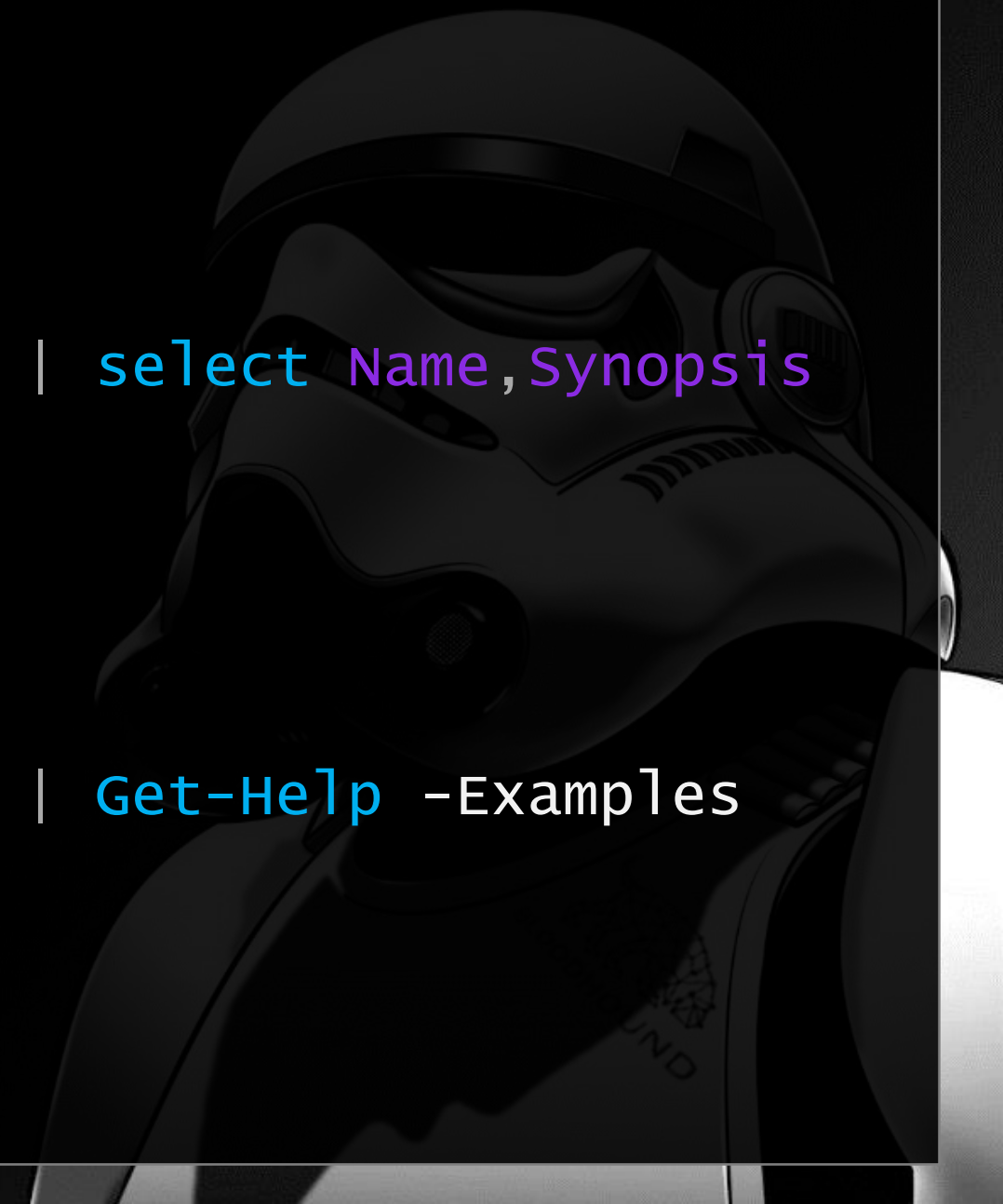
>> Allow full control over one or more Empire Servers via API



PowerEmpire - How?

RTFM

```
# List all Module Commands
gcm -Mod PowerEmpire2.0* | Get-Help | select Name,Synopsis

# Get Help for specific command
Get-Help Get-EmpireAgent -full

# tl;dr
Get-Command -Module PowerEmpire2.0* | Get-Help -Examples
```



EmpireStrike - What?

PowerEmpire Wrapper

> 17 Cmdlets
> Tab-Completion
> Dynamic Params
> Pipeline Input / Multiple Targets
> Short Syntax

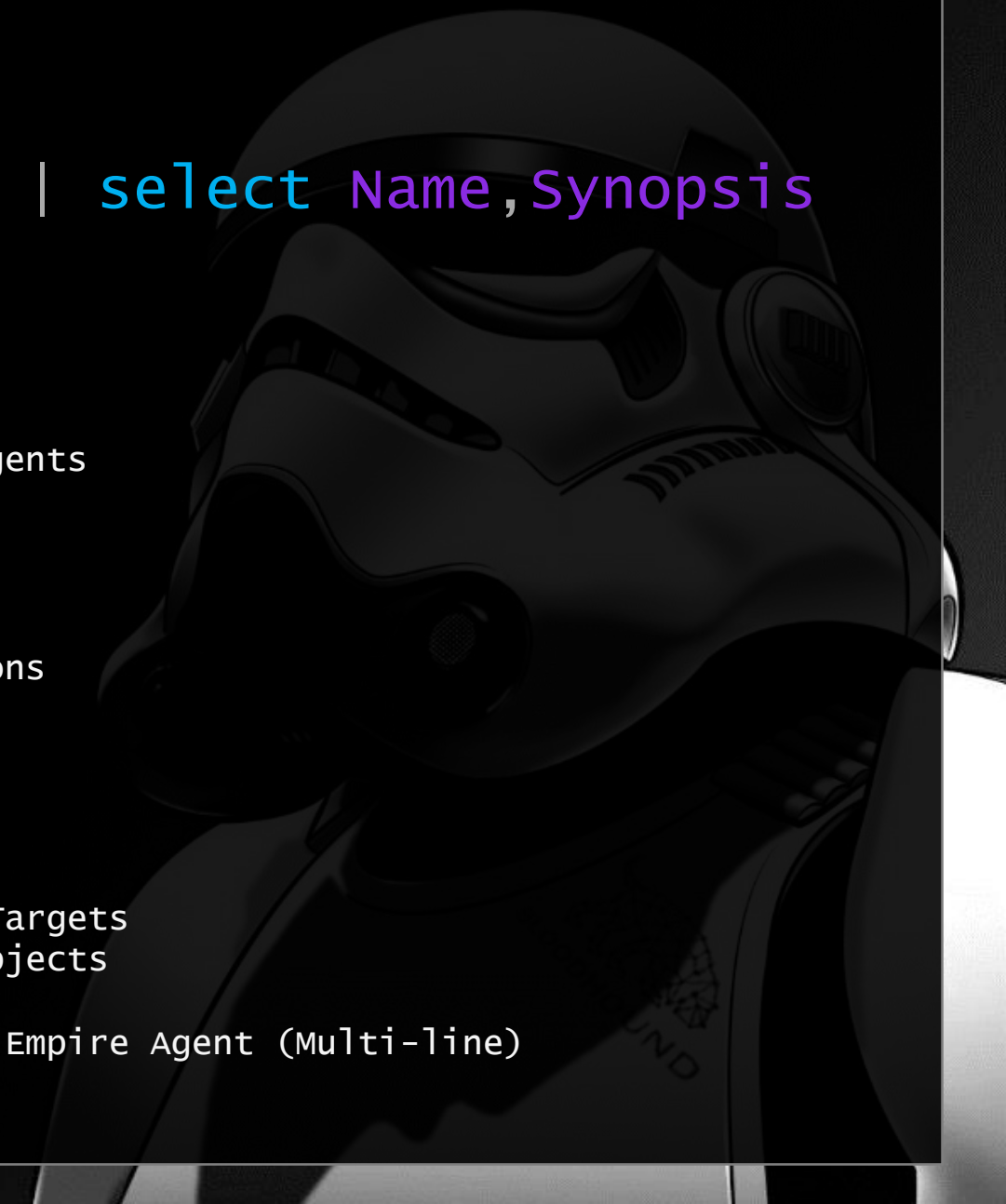
>> Shortcut Commands for PowerEmpire

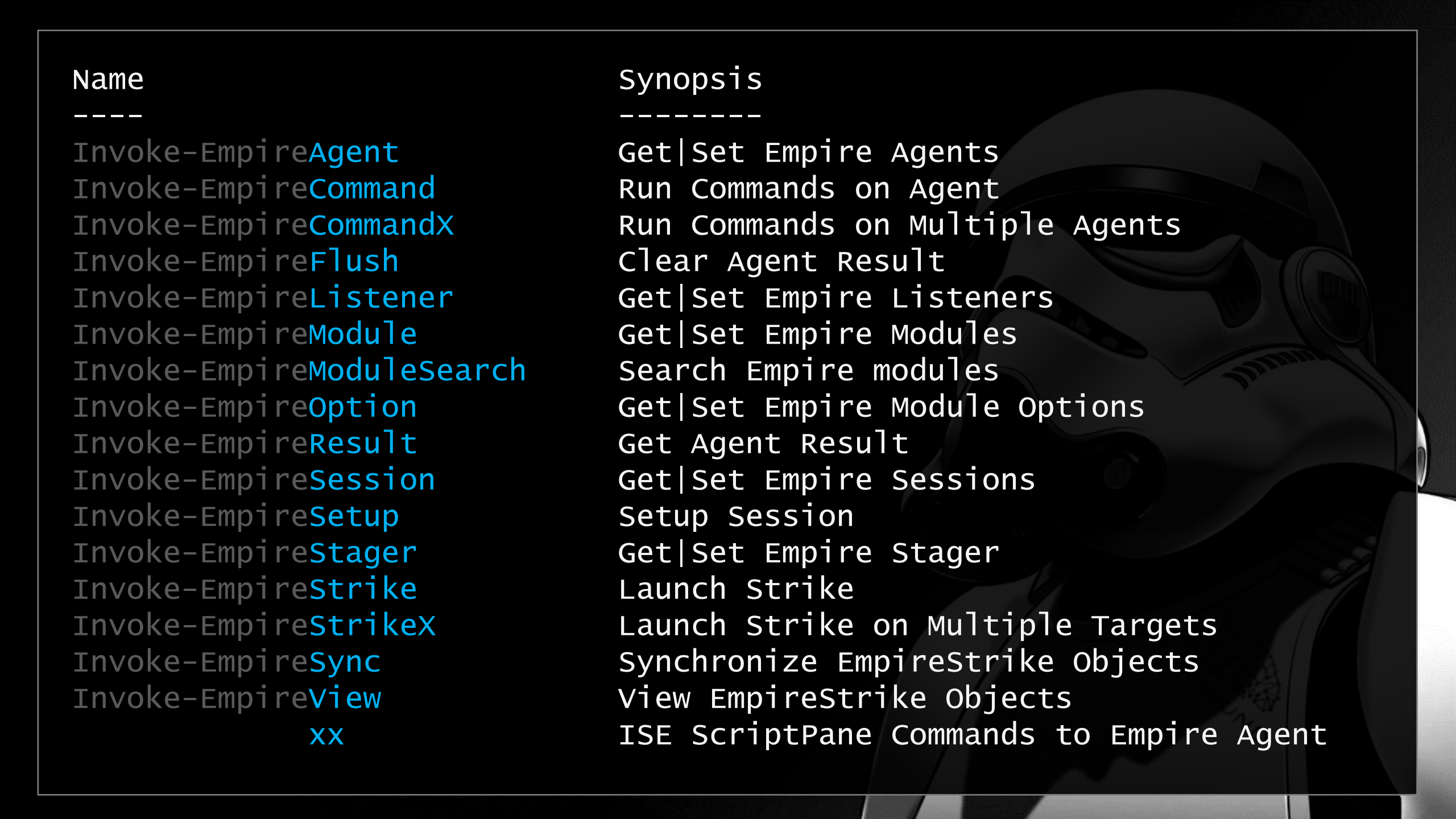
EmpireStrike - How?

Commands

```
gcm -Mod EmpireStrike2.0 | Get-Help | select Name,Synopsis
```

Name	Synopsis
Invoke-EmpireAgent	Get|Set Empire Agents
Invoke-EmpireCommand	Run Commands on Agent
Invoke-EmpireCommandX	Run Commands on Multiple Agents
Invoke-EmpireFlush	Clear Agent Result
Invoke-EmpireListener	Get|Set Empire Listeners
Invoke-EmpireModule	Get|Set Empire Modules
Invoke-EmpireModuleSearch	Search Empire modules
Invoke-EmpireOption	Get|Set Empire Module Options
Invoke-EmpireResult	Get Agent Result
Invoke-EmpireSession	Get|Set Empire Sessions
Invoke-EmpireSetup	Setup Session
Invoke-EmpireStager	Get|Set Empire Stager
Invoke-EmpireStrike	Launch Strike
Invoke-EmpireStrikeX	Launch Strike on Multiple Targets
Invoke-EmpireSync	Synchronize EmpireStrike Objects
Invoke-EmpireView	View EmpireStrike Objects
Invoke-SniperISEr	ISE ScriptPane Commands to Empire Agent (Multi-line)

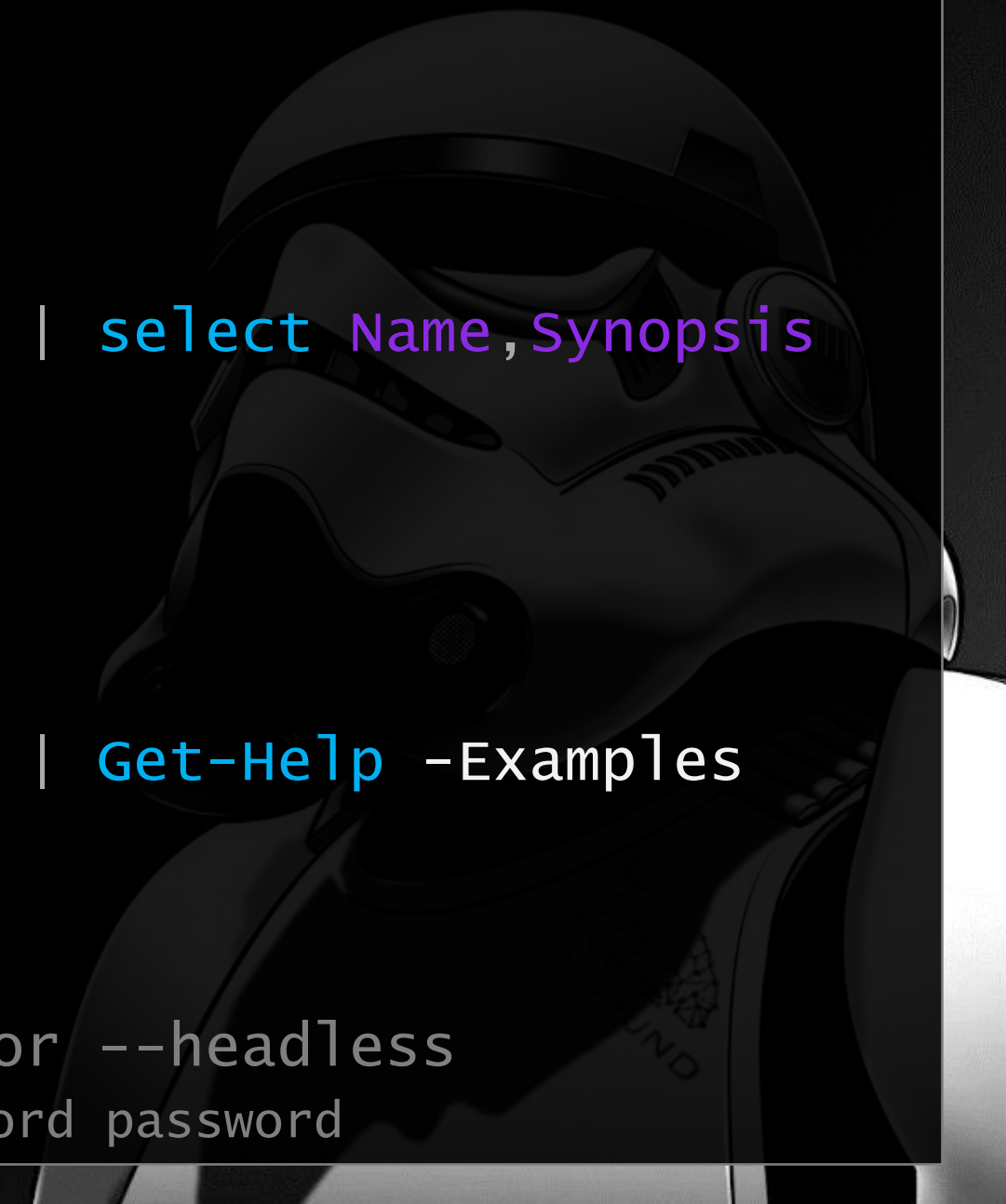


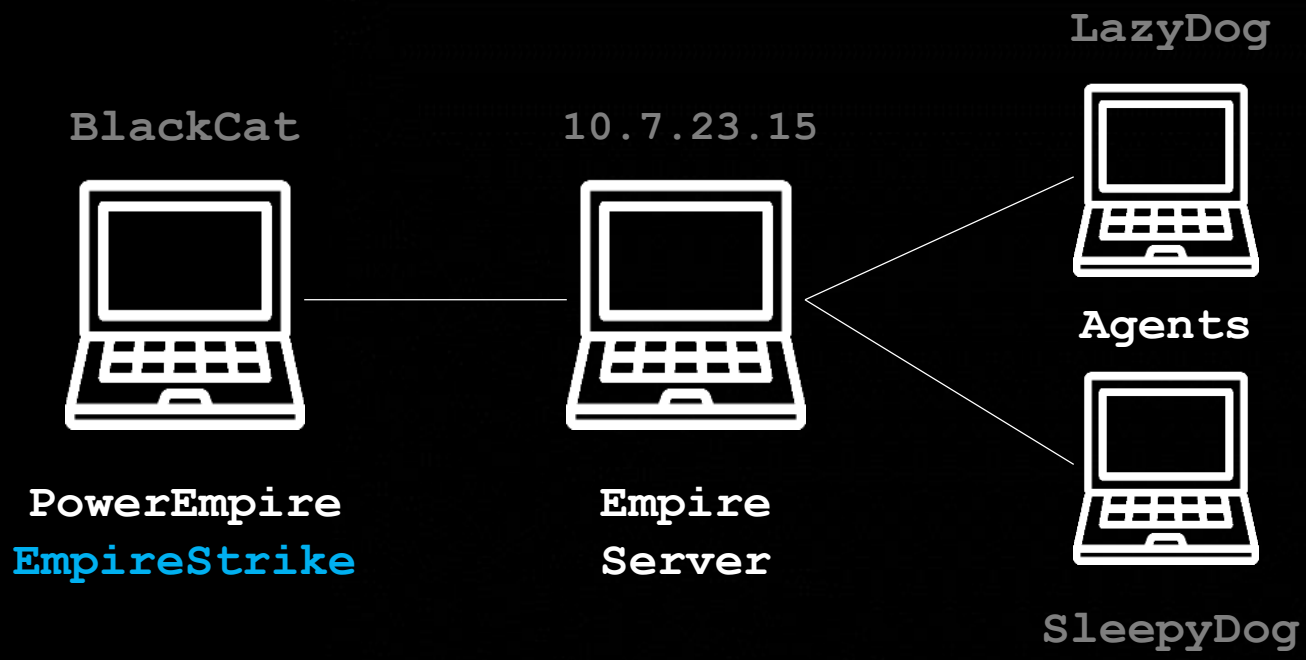


Name	Synopsis
Invoke-EmpireAgent	Get|Set Empire Agents
Invoke-EmpireCommand	Run Commands on Agent
Invoke-EmpireCommandX	Run Commands on Multiple Agents
Invoke-EmpireFlush	Clear Agent Result
Invoke-EmpireListener	Get|Set Empire Listeners
Invoke-EmpireModule	Get|Set Empire Modules
Invoke-EmpireModuleSearch	Search Empire modules
Invoke-EmpireOption	Get|Set Empire Module Options
Invoke-EmpireResult	Get Agent Result
Invoke-EmpireSession	Get|Set Empire Sessions
Invoke-EmpireSetup	Setup Session
Invoke-EmpireStager	Get|Set Empire Stager
Invoke-EmpireStrike	Launch Strike
Invoke-EmpireStrikeX	Launch Strike on Multiple Targets
Invoke-EmpireSync	Synchronize EmpireStrike Objects
Invoke-EmpireView	View EmpireStrike Objects
xx	ISE ScriptPane Commands to Empire Agent

EmpireStrike - How?

```
## RTFM

# List all Module Commands
gcm -Mod EmpireStrike2.0 | Get-Help | select Name,Synopsis

# Get Help for specific command
Get-Help Invoke-EmpireAgent -full

# tl;dr
Get-Command -Module EmpireStrike2.0 | Get-Help -Examples



# /!\ Start Empire API with --rest or --headless
#> ./empire --rest --username user --password password
```




LazyDog
BlackCat
10.7.23.15
Agents
PowerEmpire
EmpireStrike
Empire
Server
SleepyDog

DEMO

EmpireStrike Basics

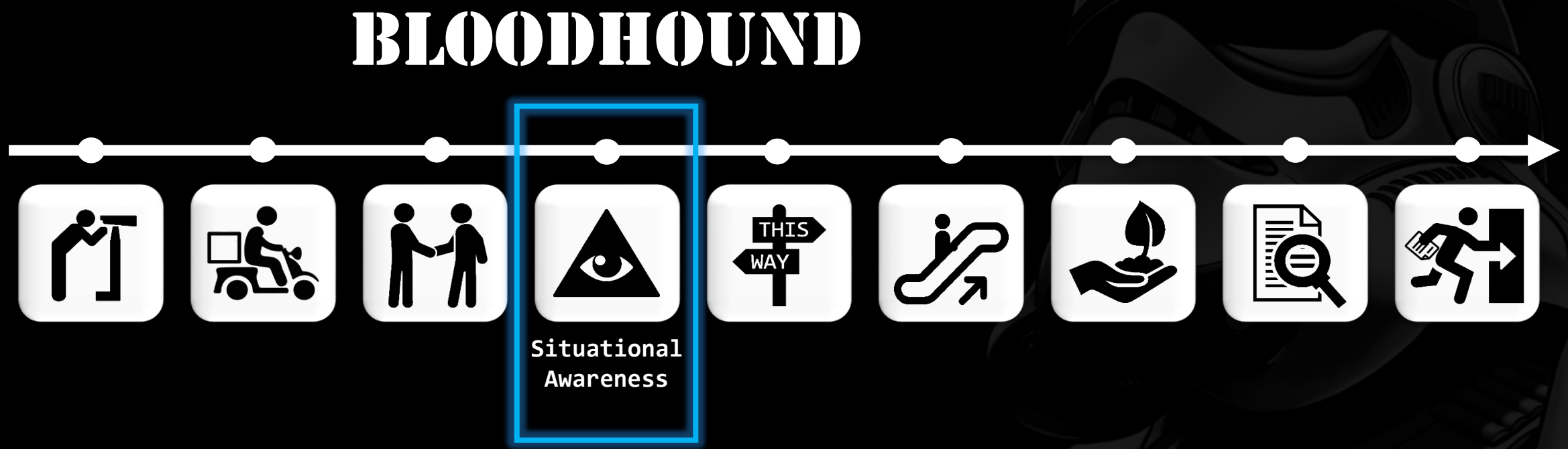
https://www.youtube.com/watch?v=eok_NgFOnmc

PART 2

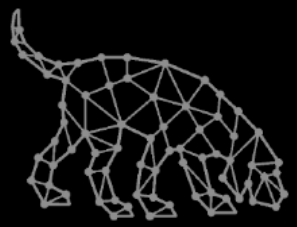
Orchestrating BloodHound & Empire

> BloodHound & CypherDog

BloodHound - What?



Active Directory
Objects & Relationships
Graphing Tool



BloodHound - What?

Graphical front-end to a Neo4j DB

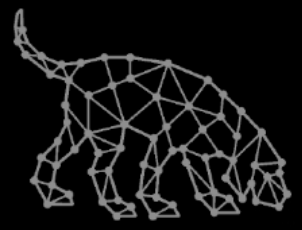
> PowerShell (or C#)* to collect AD data

> Stored in DB / displayed in graph

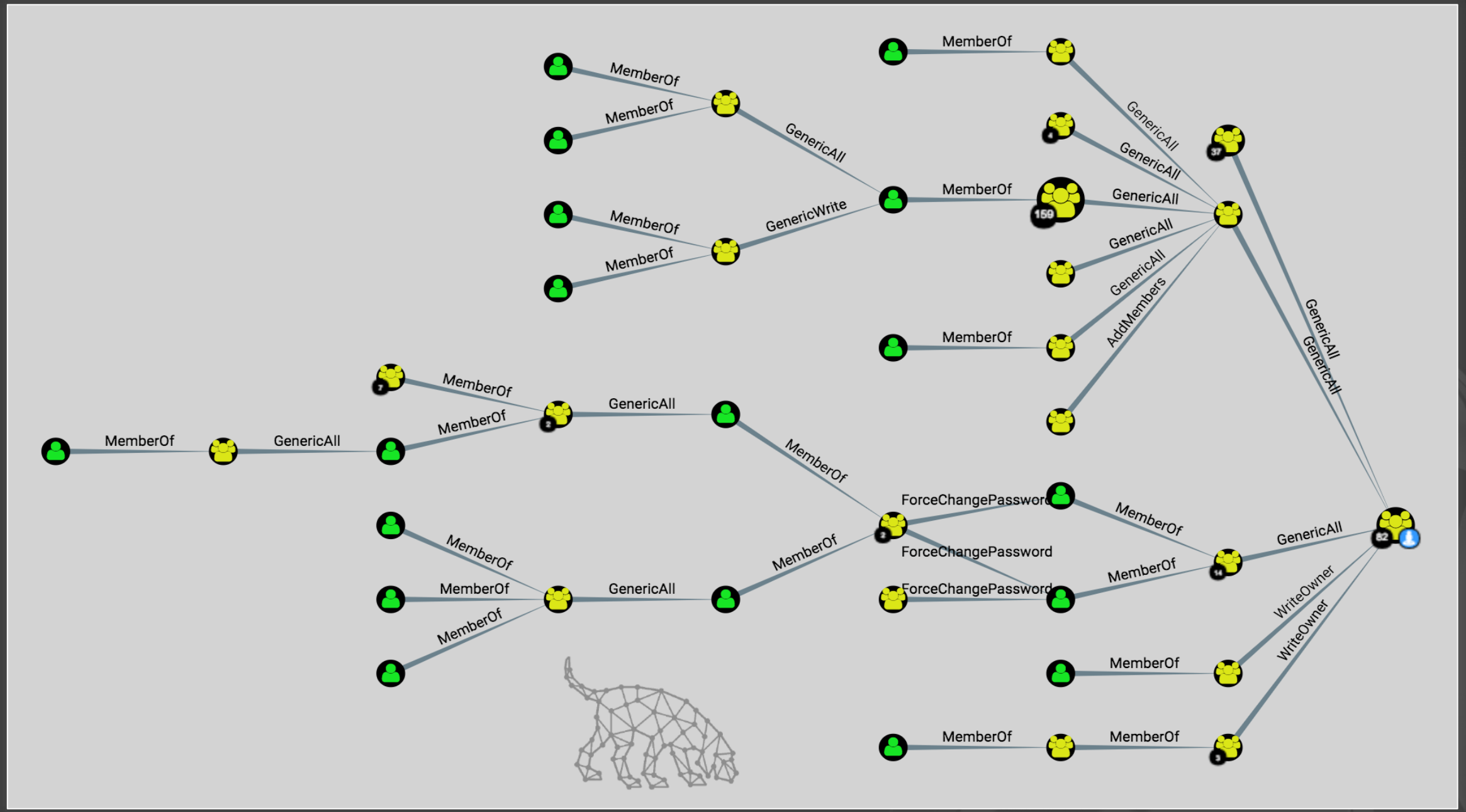
> Cypher Queries = Neo4j language

>> Concept: Node/Edge(ACL)**/Path

see ref for more info

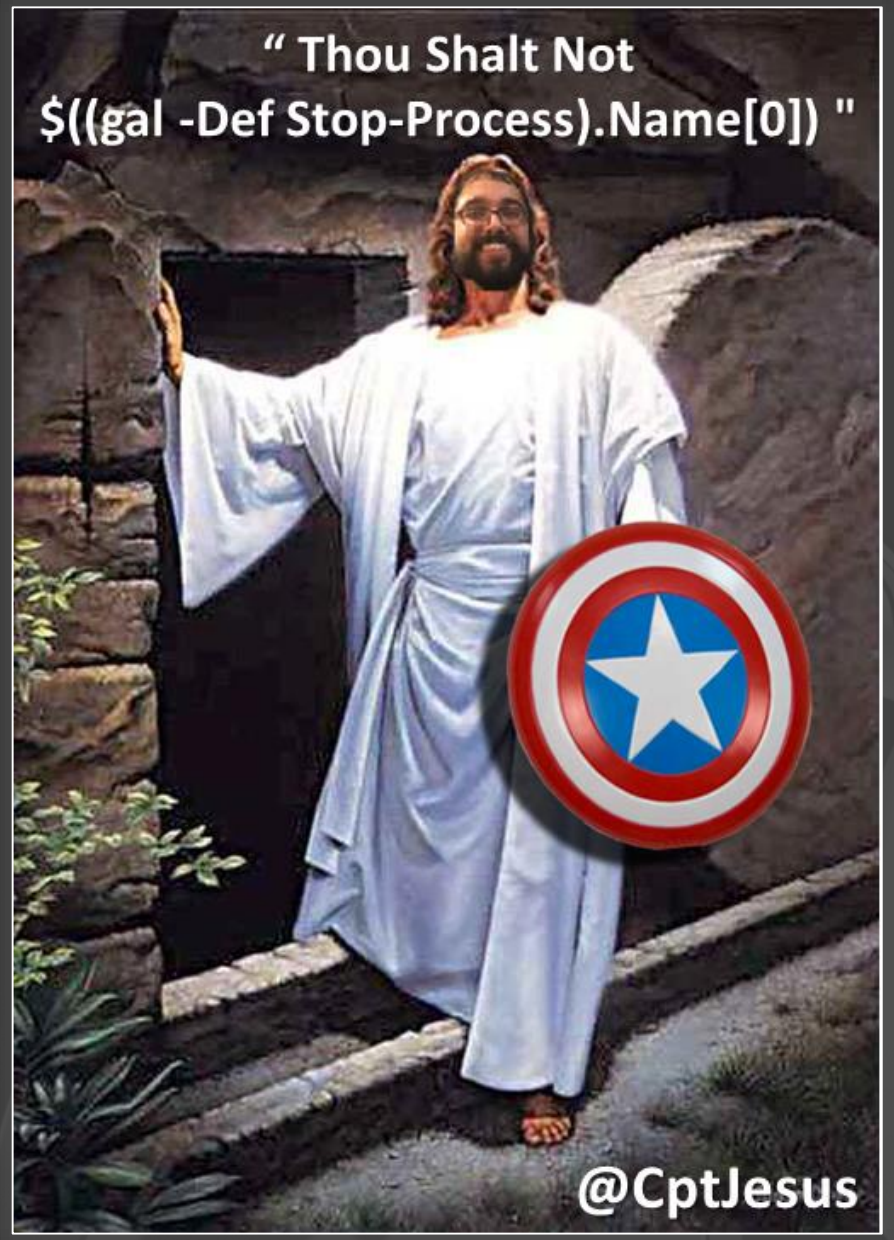


*Beta **New2017


MemberOf
GenericAll
MemberOf
MemberOf
GenericAll
MemberOf
MemberOf
GenericWrite
MemberOf
MemberOf
MemberOf
GenericAll
GenericAll
GenericAll
GenericAll
GenericAll
AddMembers
MemberOf
MemberOf
MemberOf
GenericAll
MemberOf
MemberOf
GenericAll
MemberOf
MemberOf
MemberOf
GenericAll
ForceChangePassword
ForceChangePassword
ForceChangePassword
MemberOf
MemberOf
GenericAll
WriteOwner
WriteOwner
MemberOf
MemberOf
MemberOf

BloodHound - Who?

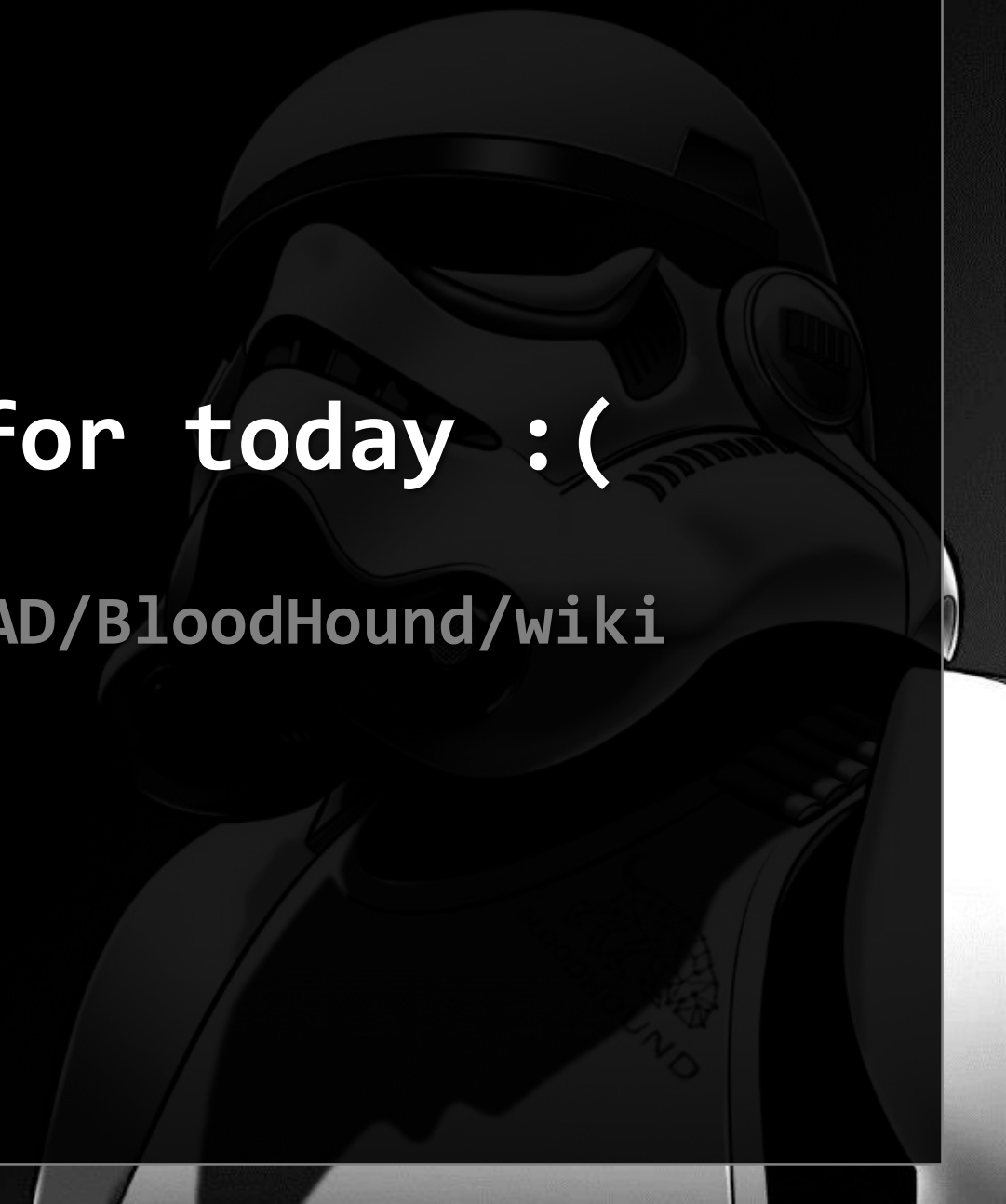
@_wald0



BloodHound - How?

Sorry, out of scope for today :(

https://github.com/BloodHoundAD/BloodHound/wiki

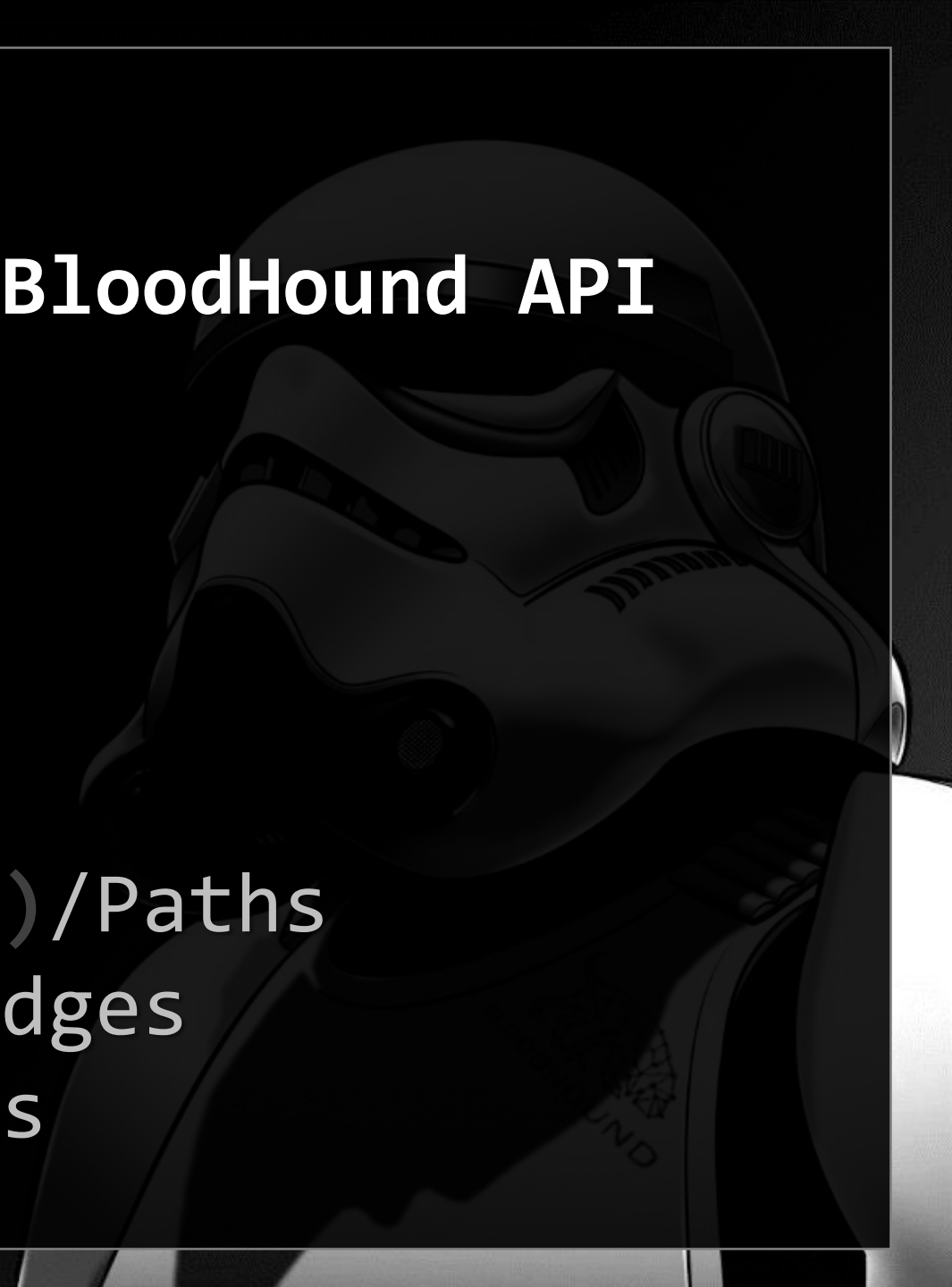


CypherDog - What?

A PowerShell Module for BloodHound API

> 11 Cmdlets
> Tab-Completion
> Dynamic Params
> Pipeline Input

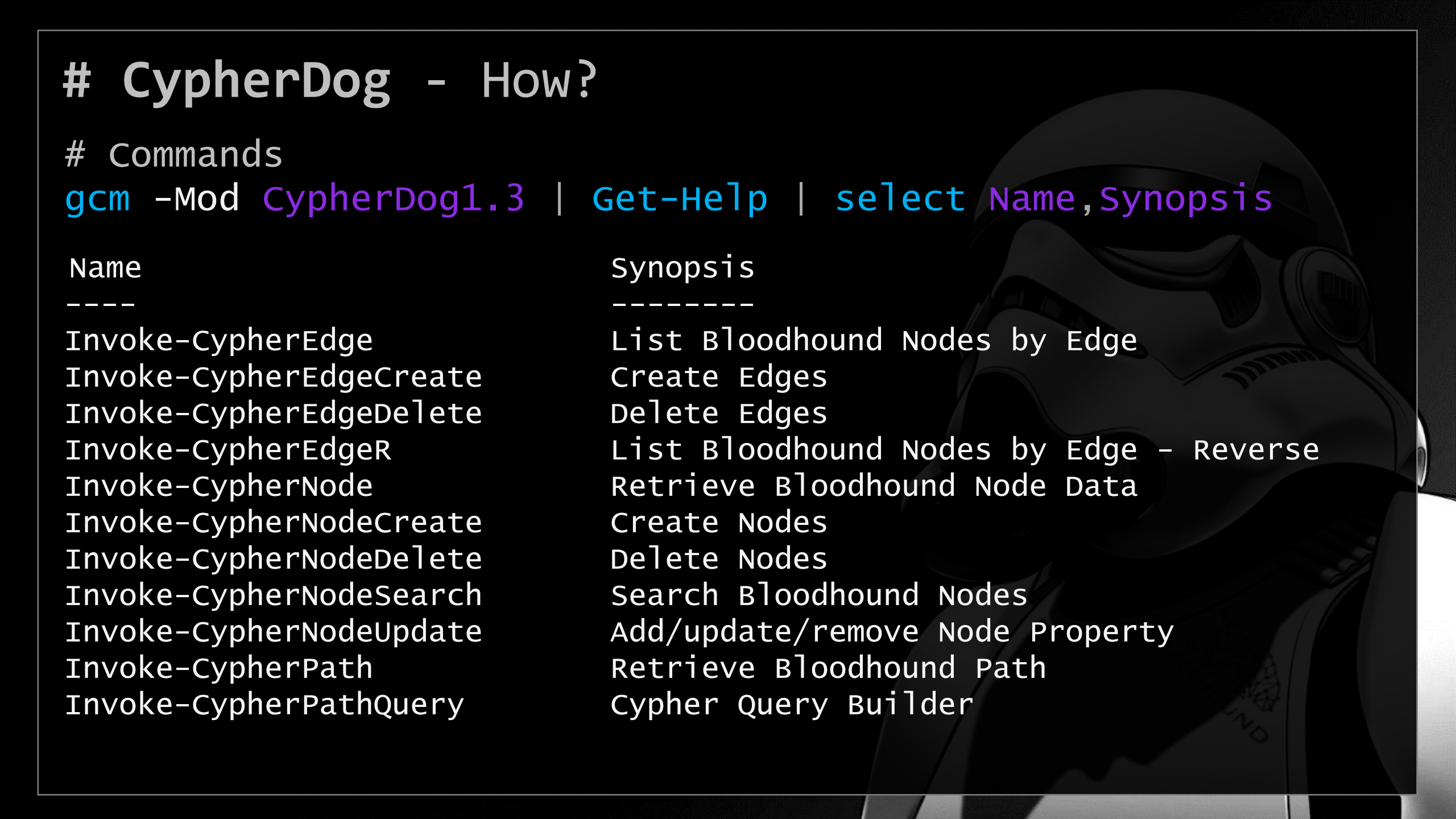
>> Check Nodes/Edges(ACL)/Paths
>> Create/Delete Nodes/Edges
>> Update Node Properties



CypherDog - How?

```
# Commands
gcm -Mod CypherDog1.3 | Get-Help | select Name,Synopsis
```

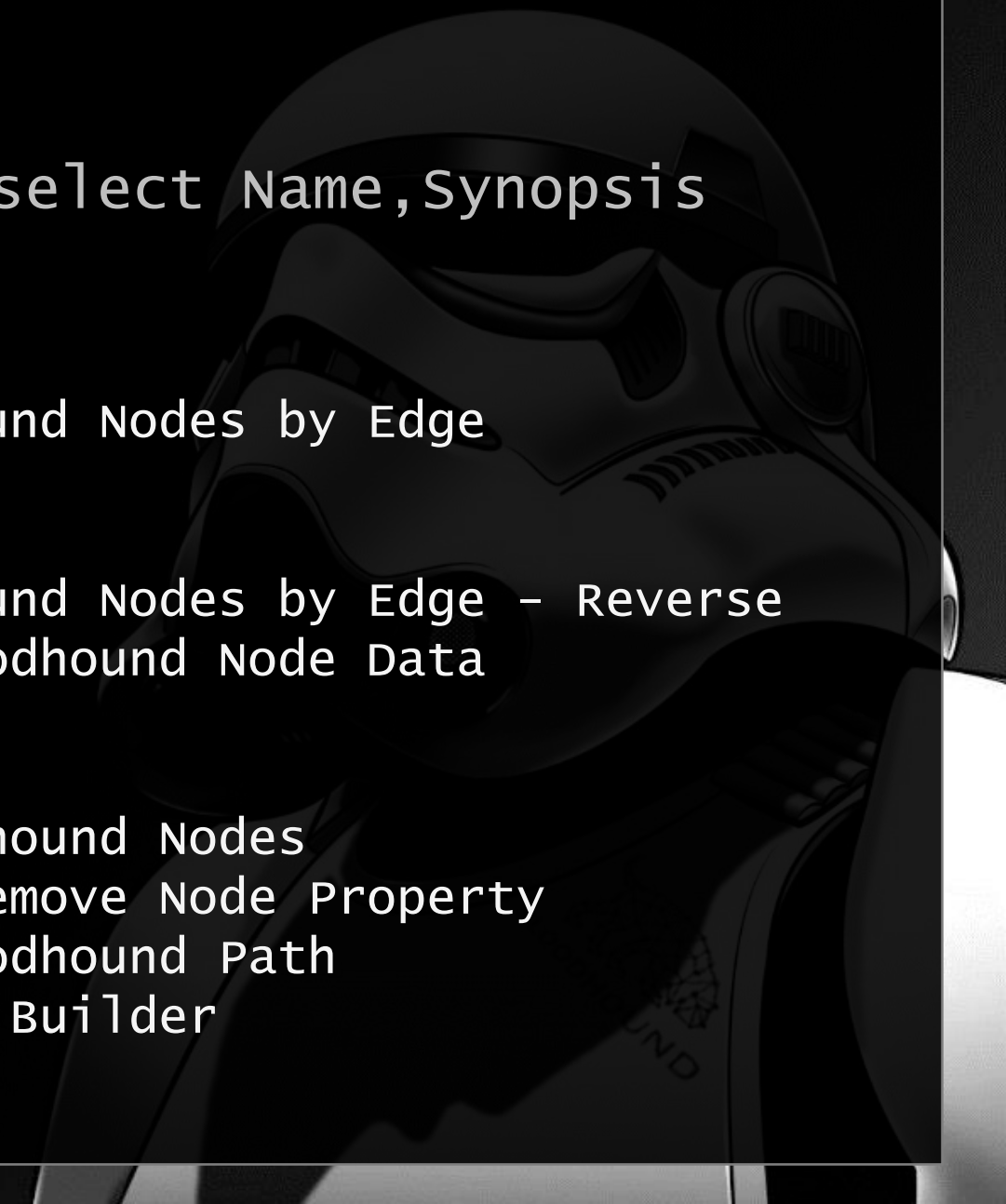
Name	Synopsis
Invoke-CypherEdge	List Bloodhound Nodes by Edge
Invoke-CypherEdgeCreate	Create Edges
Invoke-CypherEdgeDelete	Delete Edges
Invoke-CypherEdgeR	List Bloodhound Nodes by Edge - Reverse
Invoke-CypherNode	Retrieve Bloodhound Node Data
Invoke-CypherNodeCreate	Create Nodes
Invoke-CypherNodeDelete	Delete Nodes
Invoke-CypherNodeSearch	Search Bloodhound Nodes
Invoke-CypherNodeUpdate	Add/update/remove Node Property
Invoke-CypherPath	Retrieve Bloodhound Path
Invoke-CypherPathQuery	Cypher Query Builder



CypherDog - How?

```
# Commands
gcm -Mod CypherDog1.3 | Get-Help | select Name,Synopsis
```

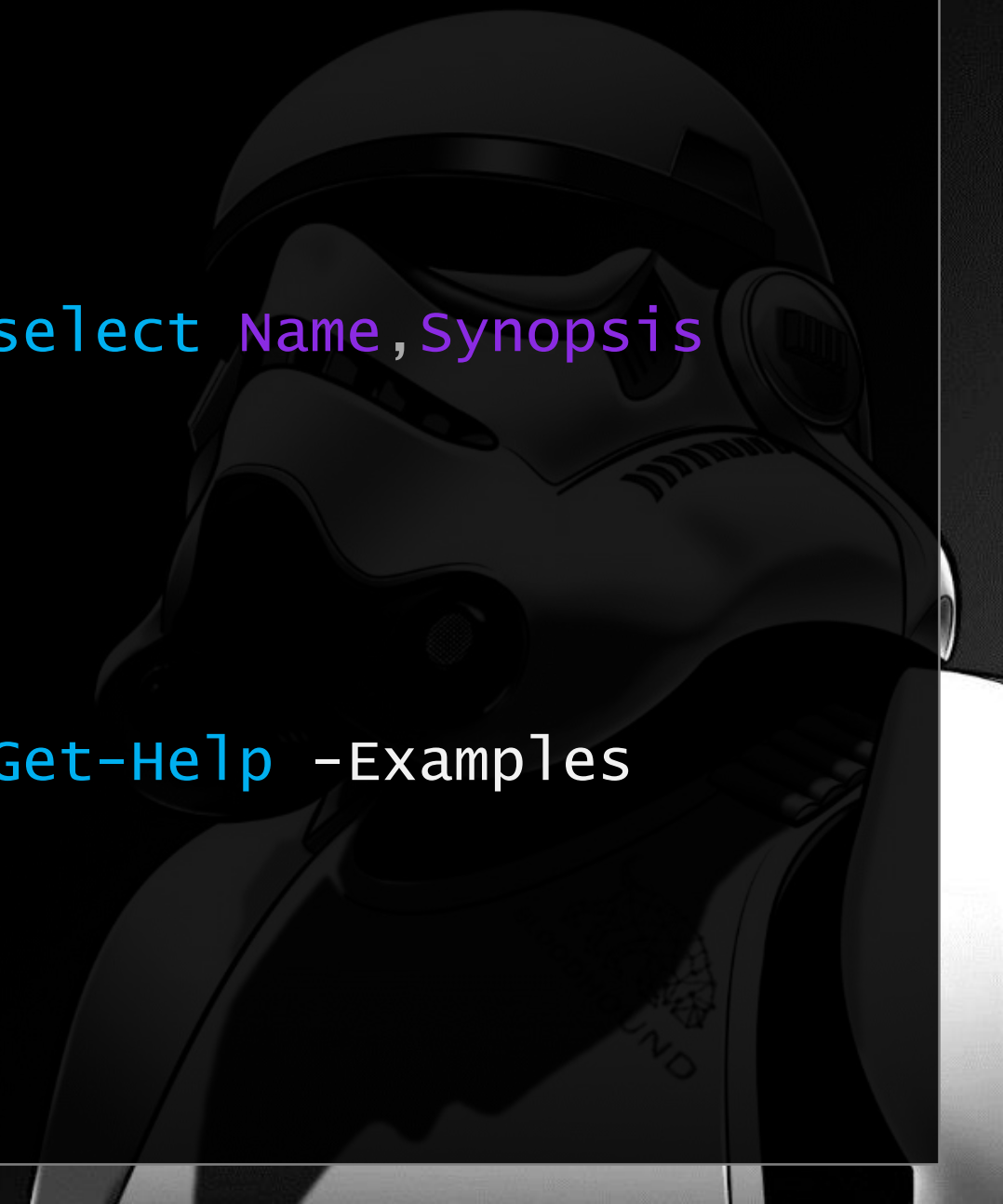
Name	Synopsis
Invoke-CypherEdge	List Bloodhound Nodes by Edge
Invoke-CypherEdgeCreate	Create Edges
Invoke-CypherEdgeDelete	Delete Edges
Invoke-CypherEdgeR	List Bloodhound Nodes by Edge - Reverse
Invoke-CypherNode	Retrieve Bloodhound Node Data
Invoke-CypherNodeCreate	Create Nodes
Invoke-CypherNodeDelete	Delete Nodes
Invoke-CypherNodeSearch	Search Bloodhound Nodes
Invoke-CypherNodeUpdate	Add/update/remove Node Property
Invoke-CypherPath	Retrieve Bloodhound Path
Invoke-CypherPathQuery	Cypher Query Builder



CypherDog - How?

RTFM

```
# List all Module Commands
gcm -Mod CypherDog1.3 | Get-Help | select Name,Synopsis

# Get Help for specific command
Get-Help Invoke-CypherPath -full

# tl;dr
Get-Command -Module CypherDog1.3 | Get-Help -Examples
```



BlackCat

BloodHound

CypherDog

DEMO

CypherDog Basics

https://www.youtube.com/watch?v=SPgkgeOY40Y

PART 3

Orchestrating BloodHound & Empire

> DogStrike & More

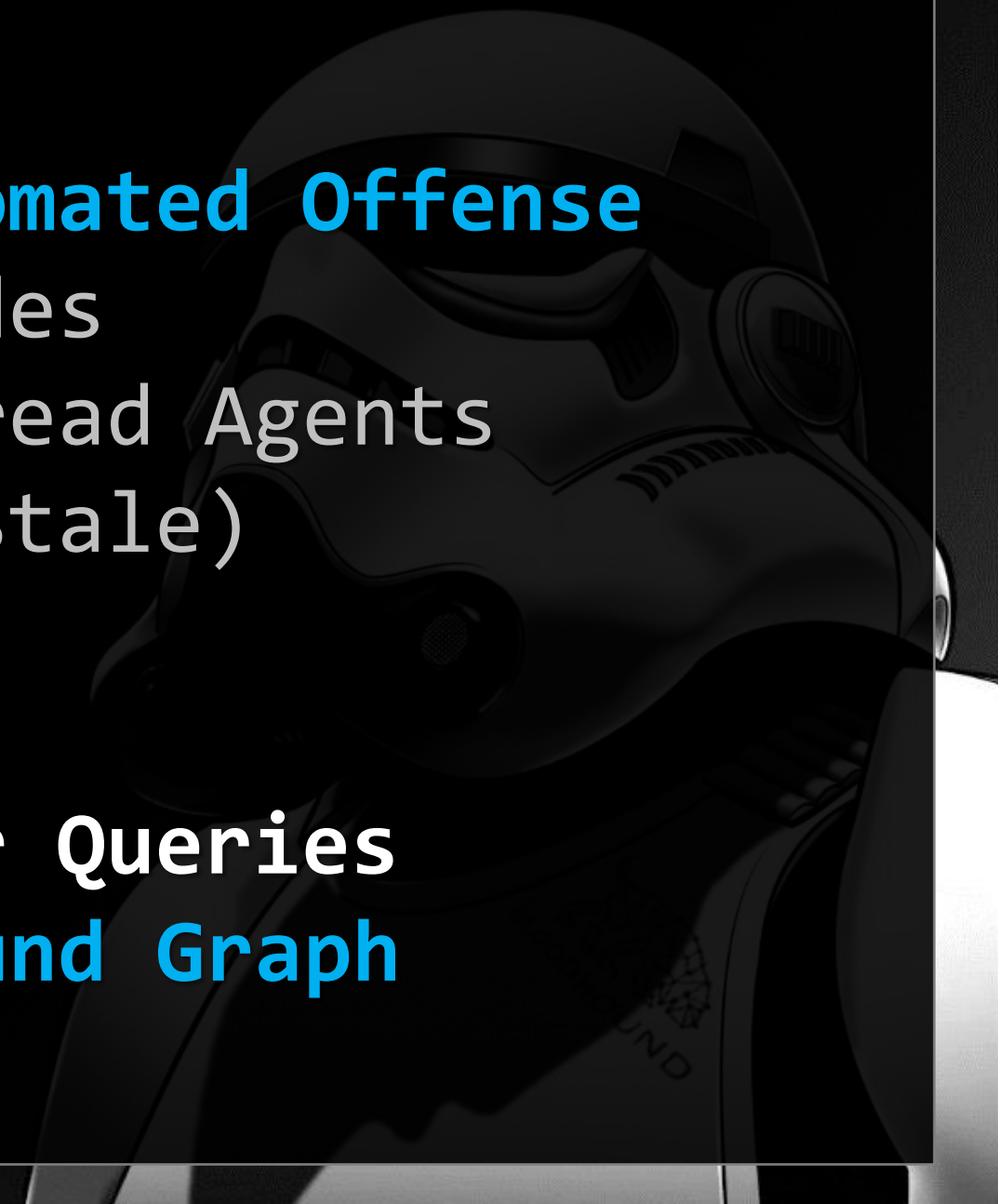
DogStrike - What?

Scripts/Cmdlets for Automated Offense

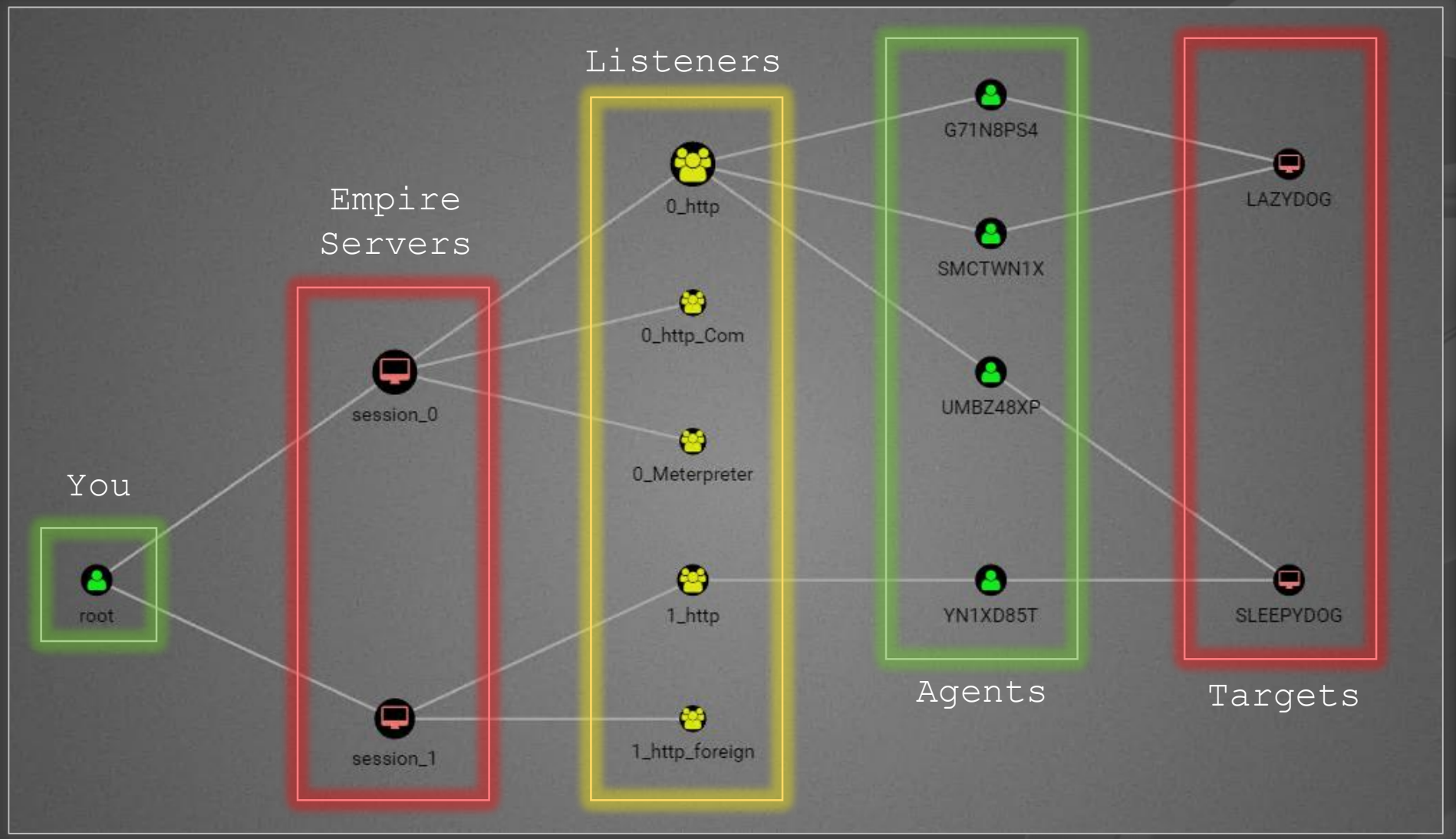
> Auto Map Empire as Nodes
> Auto Elevate/Spawn/Spread Agents
> Auto Clean Sessions (Stale)
> More cool stuff...

Custom Bloodhound Cypher Queries

> **Map Empire in BloodHound Graph**



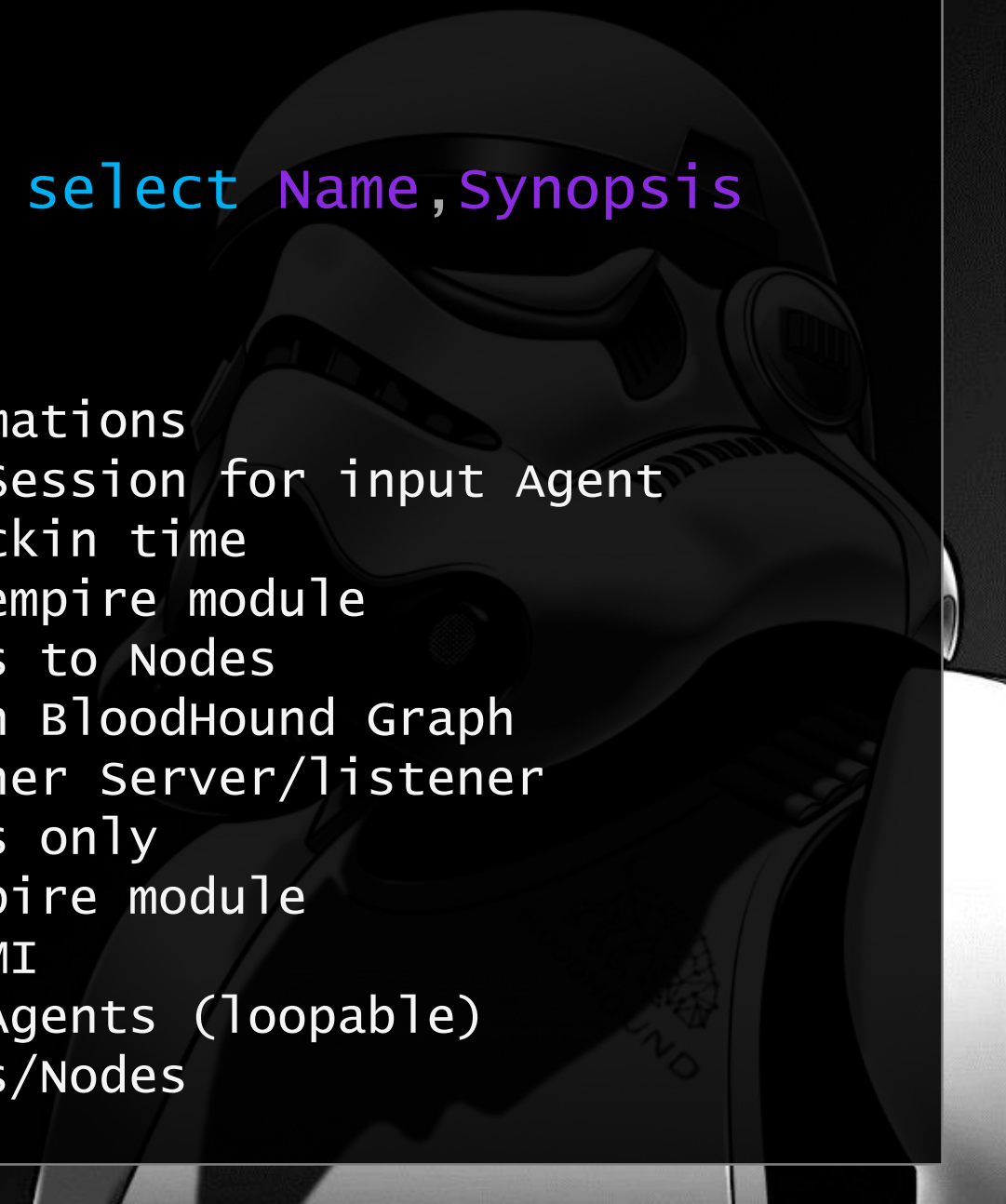
DogStrike - What?



DogStrike - How?

```
# Commands
gcm -Mod DogStrike2.13 | Get-Help | select Name,Synopsis
```

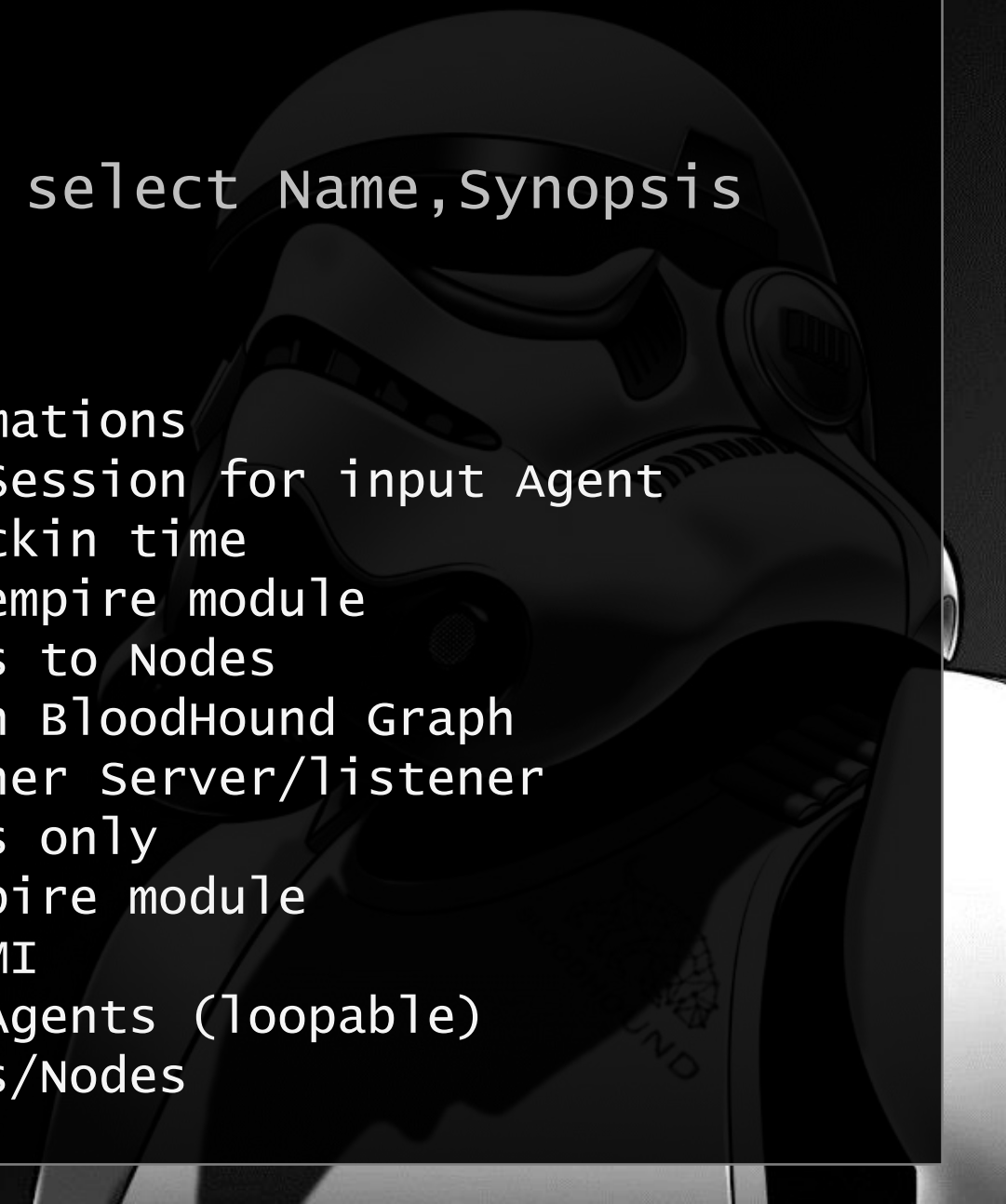
```
 Name                   Synopsis
----                   --------
Invoke-DogBark          Add Speech to automations
Invoke-DogBite          Return Listener & Session for input Agent
Invoke-DogClock         Get Agent last checkin time
Invoke-DogElevate       Elevate Agent via empire module
Invoke-DogFetch         Bulk Add Properties to Nodes
Invoke-DogMap           Map Empire Nodes in BloodHound Graph
Invoke-DogPass          Pass Agent to another Server/listener
Invoke-DogSearch        Search Empire Nodes only
Invoke-DogSpawn         Spawn agent via empire module
Invoke-DogSpread        Spread agent via WMI
Invoke-DogWatch         Map/Update Empire Agents (loopable)
Invoke-DogWipe          Remove Stale Agents/Nodes
```



DogStrike - How?

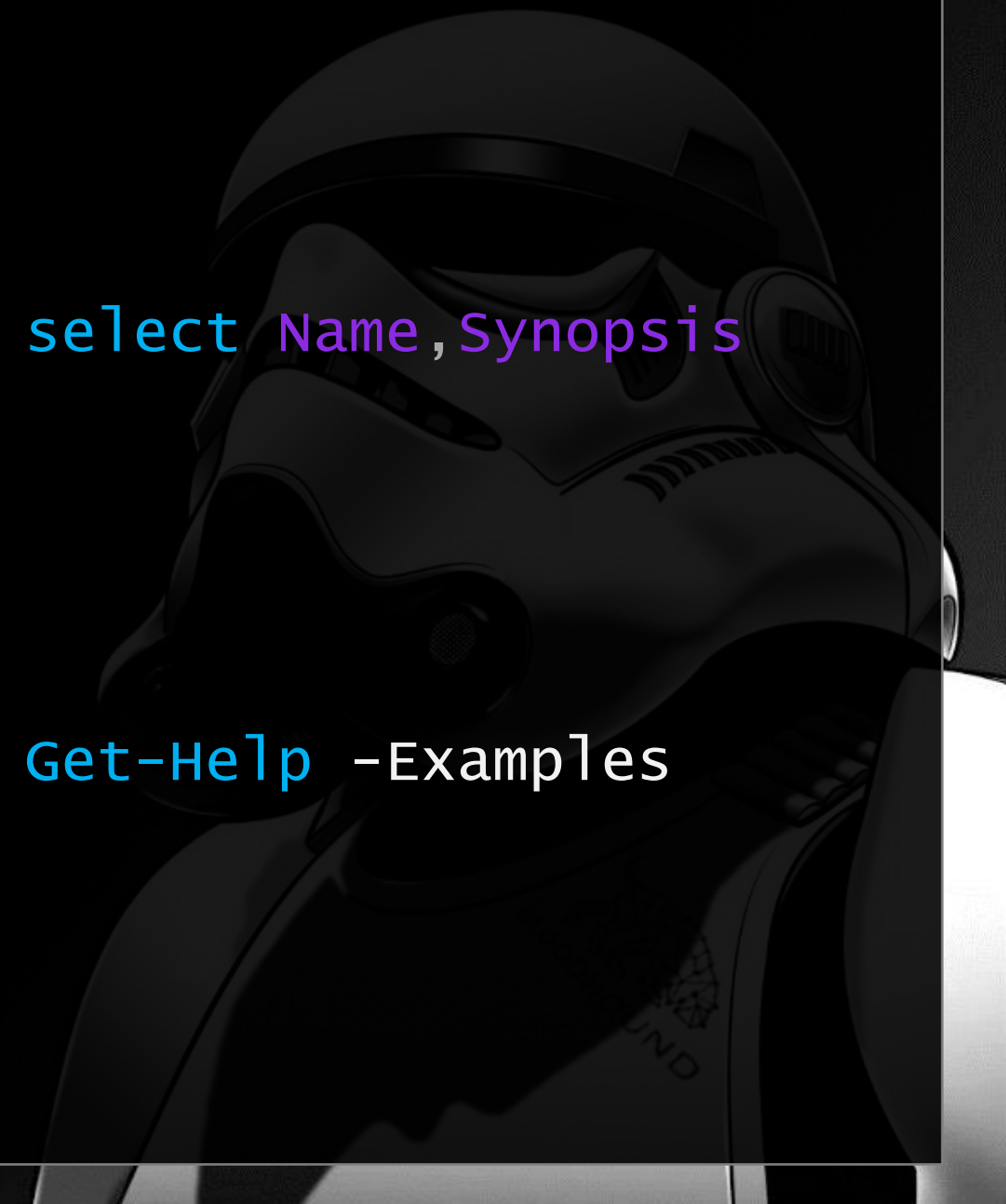
```
# Commands
gcm -Mod DogStrike2.13 | Get-Help | select Name,Synopsis
```

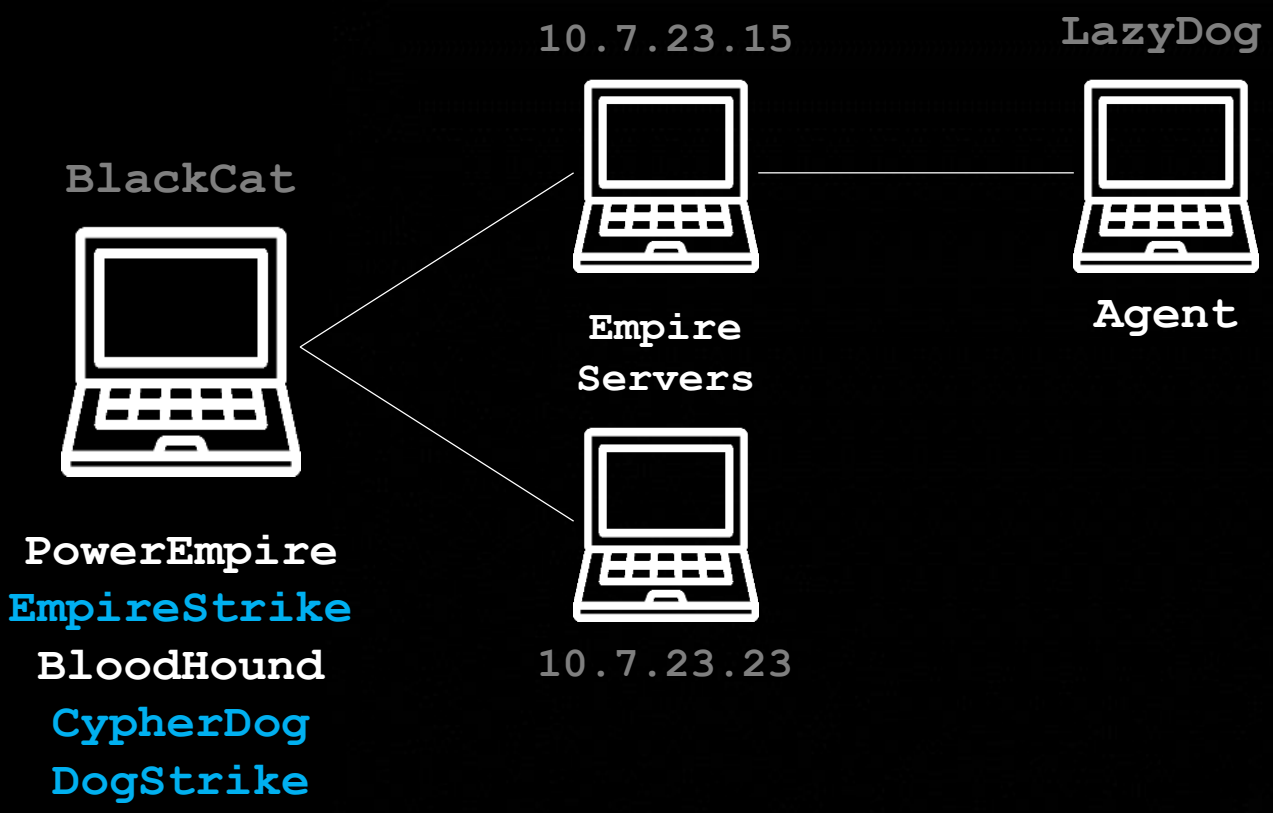
Name	Synopsis
Invoke-DogBark	Add Speech to automations
Invoke-DogBite	Return Listener & Session for input Agent
Invoke-DogClock	Get Agent last checkin time
Invoke-DogElevate	Elevate Agent via empire module
Invoke-DogFetch	Bulk Add Properties to Nodes
Invoke-DogMap	Map Empire Nodes in BloodHound Graph
Invoke-DogPass	Pass Agent to another Server/listener
Invoke-DogSearch	Search Empire Nodes only
Invoke-DogSpawn	Spawn agent via empire module
Invoke-DogSpread	Spread agent via WMI
Invoke-DogWatch	Map/Update Empire Agents (loopable)
Invoke-DogWipe	Remove Stale Agents/Nodes



DogStrike - How?

```
## RTFM

# List all Module Commands
gcm -Mod DogStrike2.13 | Get-Help | select Name,Synopsis

# Get Help for specific command
Get-Help Invoke-DogMap -full

# tl;dr
Get-Command -Module DogStrike2.13 | Get-Help -Examples
```





PowerEmpire
EmpireStrike
BloodHound
CypherDog
DogStrike

DEMO

Mapping Empire in Bloodhound
Adding New Server
Passing Agent to New Server

https://www.youtube.com/watch?v=IcbCYy7IiNE

Spawning Agents (at Scale)...

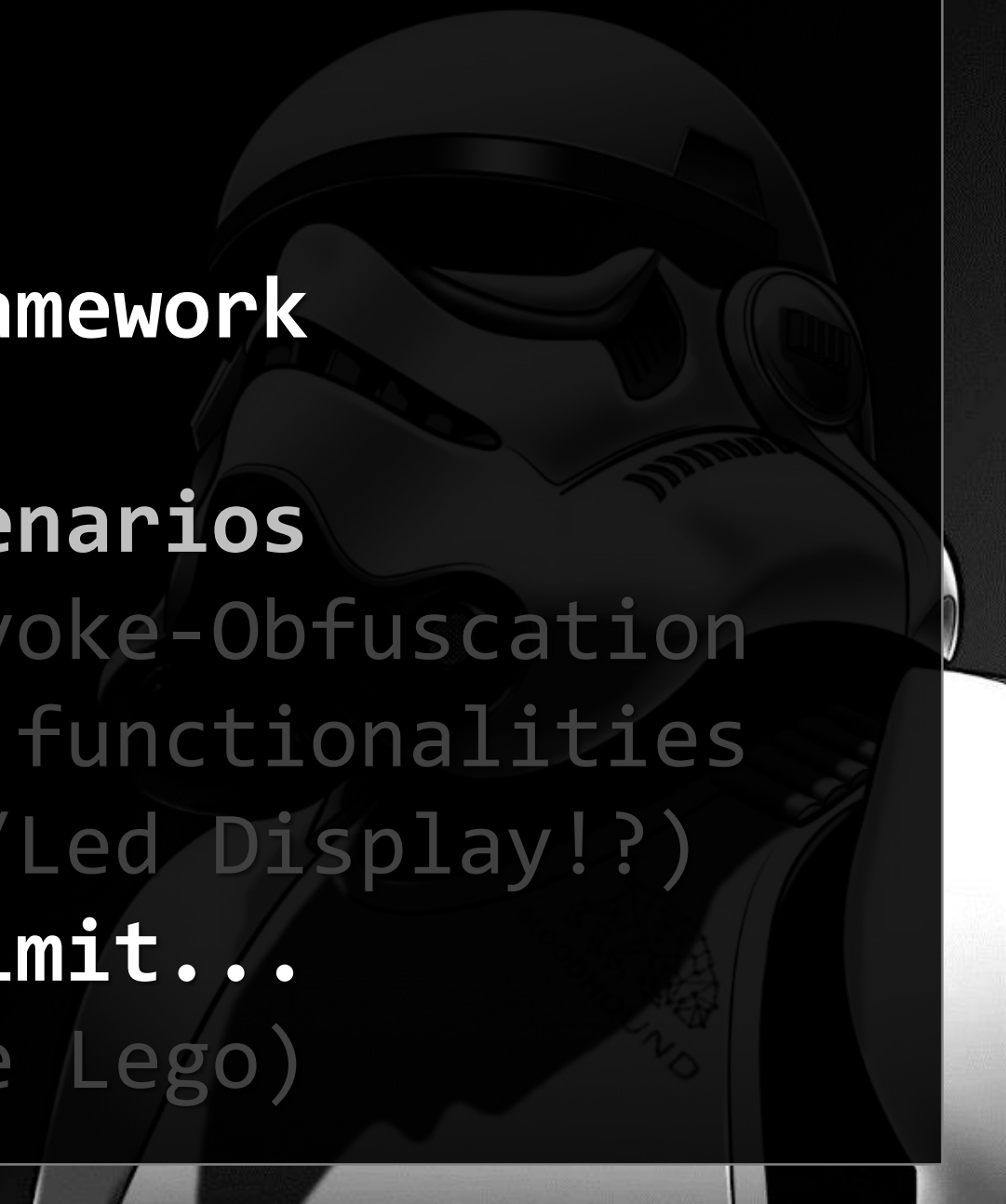
https://www.youtube.com/watch?v=oHMt1_YwQfA

Rolling Your Own Automations...

https://www.youtube.com/watch?v=a4EtEY37ImQ

Your Uncle Bob...

Use PowerShell as
Offensive Automation Framework
> Live Action
> Scripted Sequences/Scenarios
> Other PoSh Modules Invoke-Obfuscation
> DIY Cmdlets / Add New functionalities
(Notifications/Slackbot/Led Display!?)
>> Imagination is the limit...
(PowerShell is just like Lego)



```
Foreach($Agt in $Agent){
    # Set Session & Target Agent
    DogBite -Agent $Agt -Select

    # trollsploit/wallpaper
    Module powershell/trollsploit/wallpaper
    Option LocalImagePath $ImagePath
    Strike -Agent $Agt -Blind

    # trollsploit/get-swchifty
    Module powershell/trollsploit/get_schwifty
    if($VideoURL){Option VideoURL $VideoURL}
    Strike -Agent $Agt -Blind
    }
```

Tool Drop

Code available on GitHub

> https://github.com/SadProcessor/EmpireDog

DIY Guide (PDF)

> https://www.bsidesams.nl/

Video Demos

> Youtube : Brick.IT+Powershell+Empire+Bloodhound

What Next...

More dev projects

> More automated sequences/Cmdlets
> Pass output to **Go-Fetch/DeathStar?**
> Bloodhound **GUI Hacks** by **@porterhau5**

> Automated RedTeam CookBook for BlueTeam
> Auto generate Attack report
> ???

More Tools...

Other Auto AD post-Exploitation tools

> DeathStar by @Byt3Bl33d3r

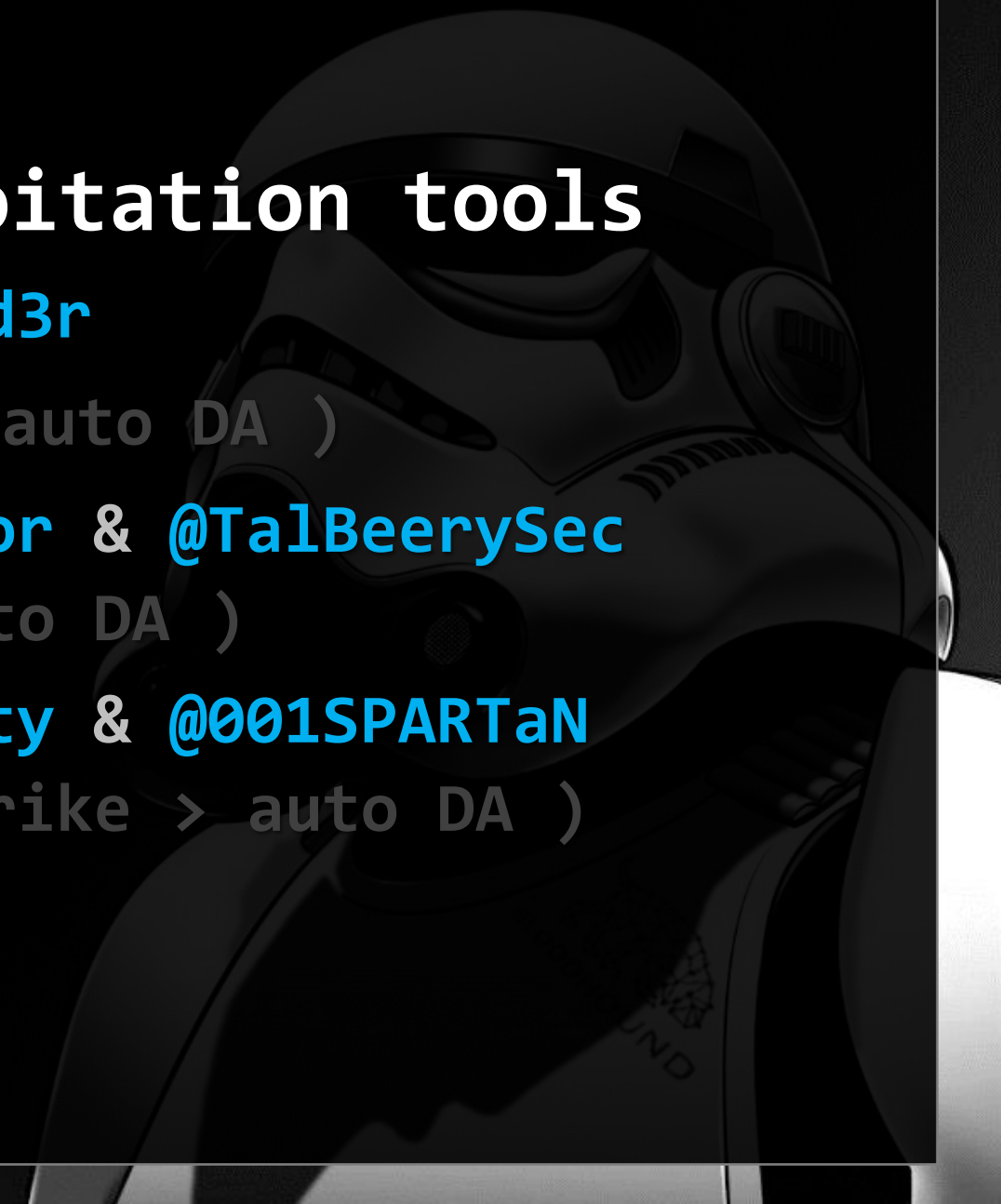
(Bootleg Empire + Python > auto DA)

> Go-Fetch by @TalTheMaor & @TalBeerySec

(Bloodhound Path + PS > auto DA)

> AngryPuppy by @VySecurity & @001SPARTaN

(BloodHound Path + CobaltStrike > auto DA)



Refs

Empire by @HarmjOy & Co.

GitHub	https://github.com/EmpireProject
Wiki	https://github.com/EmpireProject/Empire/wiki
Slack	https://adaptiveempire.slack.com

PowerEmpire by DarkOperator

GitLab	https://gitlab.com/carlos_perez/PowerEmpire

BloodHound by @_wald0 @CptJesus & @HarmjOy

GitHub	https://github.com/BloodHoundAD/BloodHound
Wiki	https://github.com/BloodHoundAD/BloodHound/wiki
Slack	https://bloodhoundhq.slack.com

Blogs

Empire & More	https://blog.harmjOy.net/
BloodHound & More	https://wald0.com/?p=68
Cypher & More	https://blog.cptjesus.com/posts/introtocypher
SpecterOps Blogs	https://posts.specterops.io/
BH Hacks by @PorterHau5	http://porterhau5.com/blog/
ADSecutity by @PyroTek3	https://adsecurity.org/
Invoke-Obfuscation by @danielBohannon	https://github.com/danielbohannon/Invoke-Obfuscation

Other Tools

DeathStar	https://github.com/byt3bl33d3r/DeathStar
GoFetch	https://github.com/GoFetchAD/GoFetch
AngryPuppy	https://github.com/vysec/ANGRYPUPPY

PART 4

Automated AD Post-Exploitation ?!?

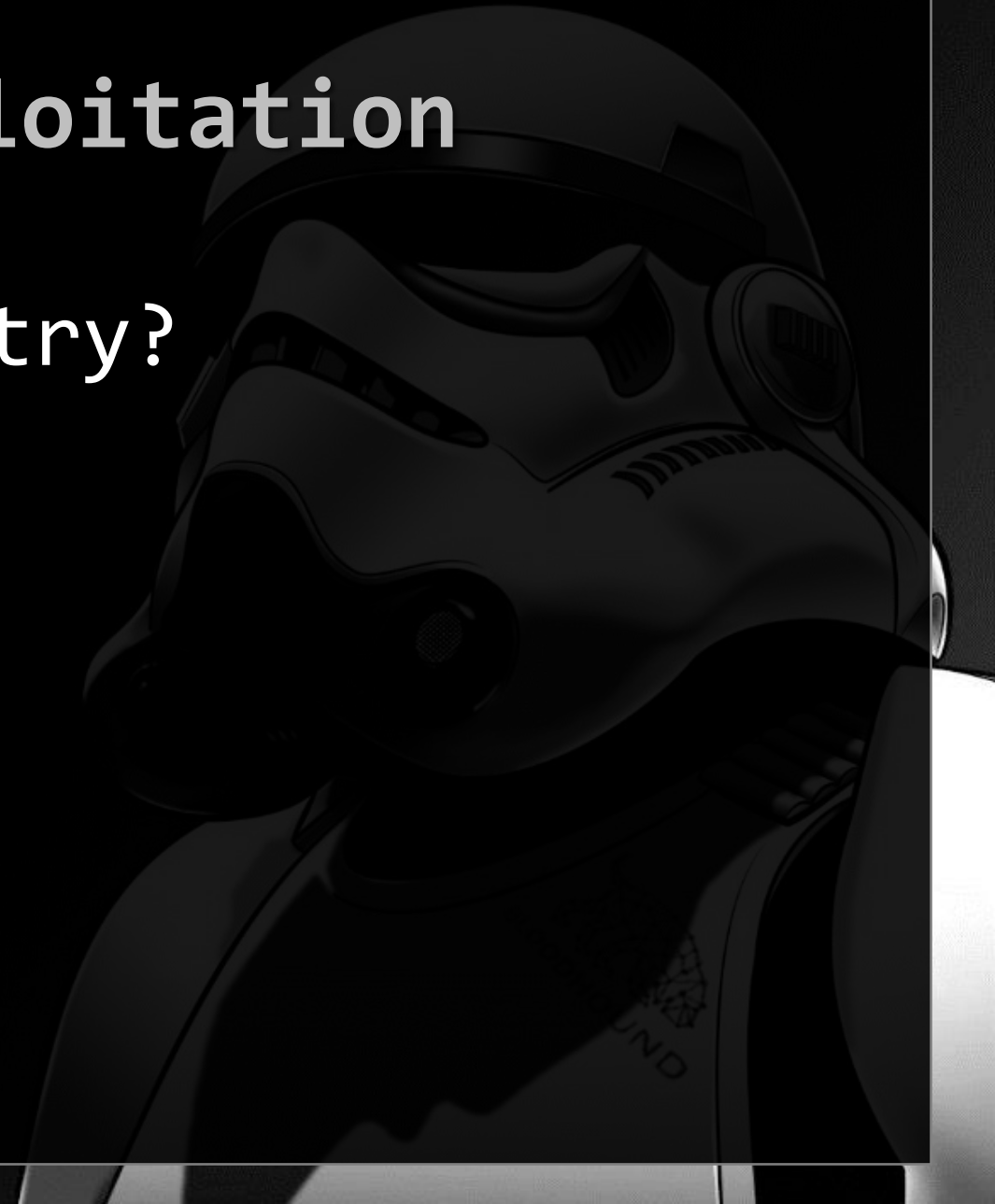
> Q&A


Matt Graeber
@mattifestation
Following
I think Deathstar and GoFetch represent an important inflection point in attack automation that I hope all EDR vendors are taking seriously.
7:07 PM - 6 Jun 2017
Josh Pitts
@midnite_runr
Follow
Replying to @nikhil_mitt
A lot of what pentesters do can be automated. It's time. Pilots use automated systems but we still call them pilots not skiddies.
2:49 PM - 4 Aug 2017
Nikhil Mittal
@nikhil_mitt
Following
Not liking the automation of lateral movement. Not that the tools are not good but "fire and forget" is not a good way of security testing.
1:58 PM - 4 Aug 2017
Lee Christensen
@tifkin_
Following
Replying to @Carlos_Perez @SadProcessor @nikhil_mitt
Devil's advocate: "Stealthy" isn't the only valid form of tradecraft :)
10:05 PM - 4 Aug 2017
Darkoperator
@Carlos_Perez
Following
Replying to @nikhil_mitt @SadProcessor
Agree, shows lack of tradecraft when proper controls and mitigations have not been identified. Action and tools should be dictated by env
3:11 PM - 4 Aug 2017
scot berner
@slobtresix0
Following
Replying to @nikhil_mitt
I secretly like keeping those skills as magic, but lowering the bar helps less skilled defenders learn and get better...
2:38 PM - 5 Aug 2017

Q&A

Automated AD Post-Exploitation

> Pros/Cons?
> Good/Bad for the industry?
> Dangerous? Pointless?
> The future?
> The end of my job?
> ...



What Do You Think??