SPECTEROPS

Beyond the Shell

Unconventional Agents for Red Teaming Success

Cody Thomas

SpecterOps

Cody Thomas

- @its_a_feature_
- macOS Red Teaming/Researcher/Teacher
- Sr. Software Developer at SpecterOps
- Mythic C2 Developer

Overview

SO-CON 2024 Outline

- Mythic Command and Control Framework
- Normal Operational Flow
- Unconventional Agents
  - Arachne
- Mythic 3rd Party Service Agents
  - Ghostwriter
  - Bloodhound
  - Nemesis

What is Mythic?

Why does it matter?

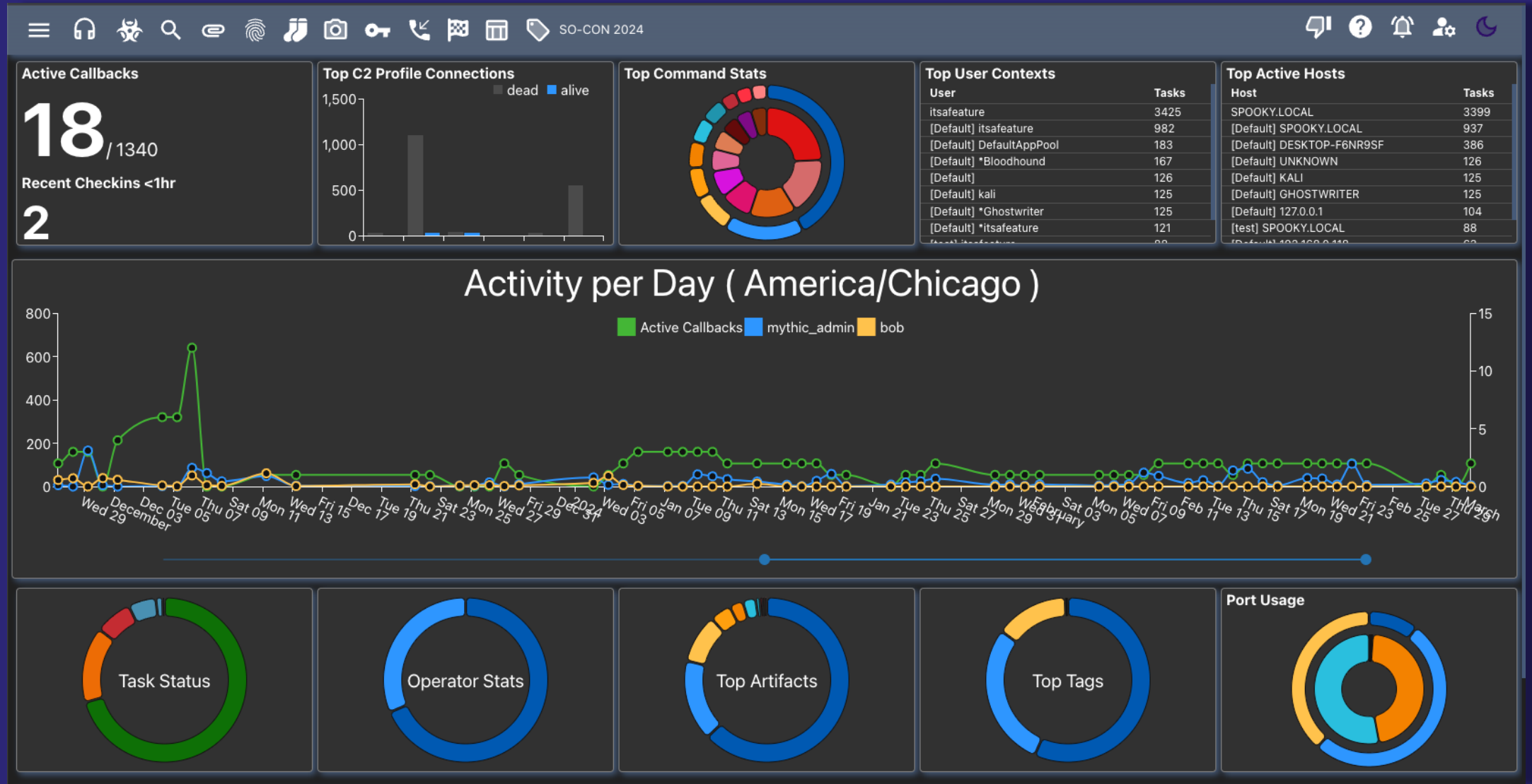
Mythic Command and Control

Open Source C2 Framework – https://github.com/its-a-feature/Mythic

- Microservice Architecture (Docker)
- Collaborative Web UI (React)
- Plug-n-play Payload Types/C2 Profiles
  - https://mythicmeta.github.io/overview
- RabbitMQ/gRPC for inter-service comms
- PostgreSQL Database
- GraphQL (Hasura) API access

Mythic

Home Dashboard



Mythic Community Overview

⭐ indicates update in the last 30 days.

For agent comparison, check out the Agent Capability Matrix.

Show 50 entries

Search:

Last Update	Branch	Category	Docker Image		Name	Description	Commit Message	Stars	Clones	URL
2024-03-10 ⭐	master	Agent			freyja	Freyja is a Golang, Purple Team agent that compiles into Windows, Linux and macOS x64 executables.	Merge pull request #7 from MythicAgents/V3.2.2 V3.2.2	15	105	
2024-03-08 ⭐	master	Agent	ghcr.io/mythicagents/poseidon:v0.0.0.8		poseidon	Poseidon is a Golang agent targeting Linux and macOS	Bump Dockerfile tag to match release 'v0.0.0.8'	86	243	
2024-03-07 ⭐	2024Q1-Dev	Agent			Apollo	A .NET Framework 4.0 Windows Agent	adding coff options for modal use	416	293	
2024-03-02 ⭐	rewrite	Agent	ghcr.io/mythicagents/thanatos:v0.1.8		thanatos	Mythic C2 agent targeting Linux and Windows hosts written in Rust	Linux things	259	167	
2024-03-01 ⭐	main	Agent	ghcr.io/mythicagents/athena:v2.0.3		Athena		Update load.py spelling	161	238	
2024-02-29 ⭐	master	Agent	ghcr.io/mythicagents/apfell:v0.0.1.3		apfell	JavaScript for Automation (JXA) macOS agent	Bump Dockerfile tag to match release 'v0.0.1.3'	50	144	
2024-02-27 ⭐	main	Agent			hermes	Swift 5 macOS agent	Added Dockerfile in comments if people want to DIY	91	53	
2024-02-20 ⭐	master	C2	ghcr.io/mythicc2profiles/websocket:v0.0.1.1		websocket	Websocket communications with Push and Poll messages	Bump Dockerfile tag to match release 'v0.0.1.1'	11	124	
2024-02-20 ⭐	master	C2	ghcr.io/mythicc2profiles/dynamichttp:v0.0.1.2		dynamichttp	Complex and extendable http messages with dynamic modifications in client and server	Bump Dockerfile tag to match release 'v0.0.1.2'	7	92	
2024-02-19 ⭐	winhttp	Agent			merlin	Cross-platform post-exploitation HTTP Command & Control agent written in golang	Updated merlin-agent	66	193	
2024-02-13 ⭐	master	C2	ghcr.io/mythicc2profiles/http:v0.0.1.4		http	Simple HTTP async comms using standard GET/POST requests	Bump Dockerfile tag to match release 'v0.0.1.4'	17	427	
2024-02-12 ⭐	main	Webhook	ghcr.io/mythicc2profiles/basic_webhook:v0.0.4		basic_webhook	Basic webhook container for Mythic 3.0.0	Bump Dockerfile tag to match release 'v0.0.4'	3	28	
2024-02-12 ⭐	main	Logger	ghcr.io/mythicc2profiles/basic_logger:v0.0.3		basic_logger	Basic stdout/file logger for Mythic	Bump Dockerfile tag to match release 'v0.0.3'	2	44	
2024-02-07	main	Agent	ghcr.io/mythicagents/arachne:v0.0.0.5		arachne	Webshell agent in aspx and php	Bump Dockerfile tag to match release 'v0.0.0.5'	13	33	
2024-01-29	main	C2	ghcr.io/mythicc2profiles/smb:v0.0.1		smb	P2P Communications of Named Pipes	Bump Dockerfile tag to match release 'v0.0.1'	5	96	
2024-01-21	master	Wrapper	ghcr.io/mythicagents/service_wrapper:v0.0.1		service_wrapper	.NET Service EXE wrapper for shellcode payloads	Bump Dockerfile tag to match release 'v0.0.1'	5	30	
2024-01-10	dependabot/npm_and_y...	Agent			venus	A Visual Studio Code Extension agent for Mythic C2	Bump follow-redirects in /Payload_Type/venus/agent_code Bum...	57	22	
2023-12-27	master	Agent			atlas		adding agent capabilities json	14	17	

https://mythicmeta.github.io/overview/agent_matrix.html

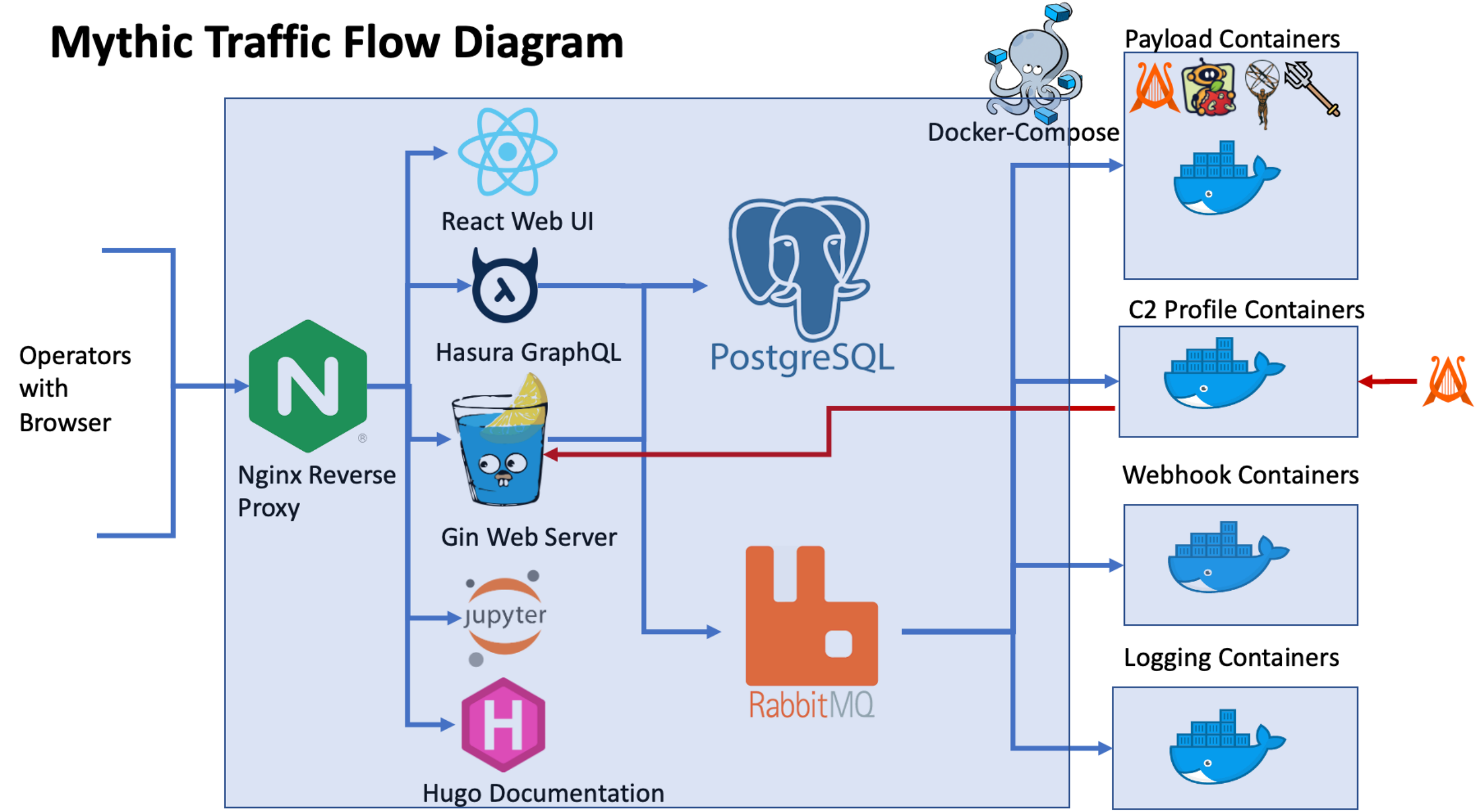
Mythic Community Agent Feature Matrix

For agent overview and update frequency, check out the [Overview Matrix](). Mythic feature descriptions and documentation is at the bottom of the page.

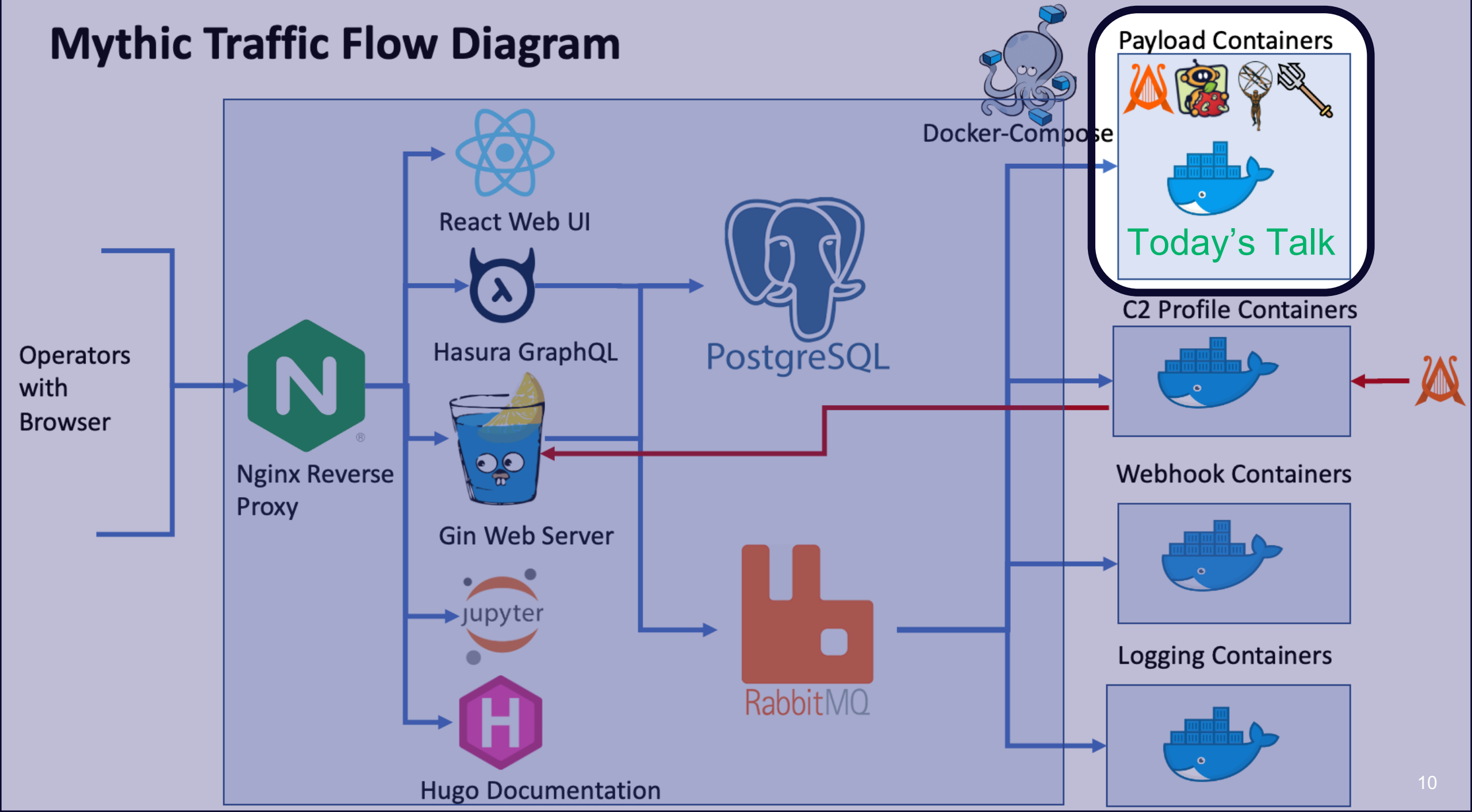
Show 100 entries

01. Version Information																					
Mythic Version	3.2	3.2	3.2	3.2	✗	✗	✗	3.2	✗	3.2	3.2	✗	✗	✗	✗	2.3	✗	3.2	3.2	✗	✗
Agent Version	0.1.3	2.2.4	2.0.2	2.0	✗	✗	✗	2.2.0	✗	2.0.27	0.1.8	✗	✗	✗	✗	✗	✗	0.0.1	✗	✗	✗
02. Operating Systems																					
FreeBSD	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Linux	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
OpenBSD	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Solaris	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Windows	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗
macOS	✓	✗	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
03. Supported C2 Profiles																					
discord	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
dynamichttp	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
freyja_tcp	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Mythic Traffic Flow Diagram



Mythic Traffic Flow Diagram



Mythic Command and Control

Why does it matter?

- Agent Developers Get Full Control
  - Tasking
  - Building
  - Processing Responses
  - Data Display*
    - Tables, Buttons, Inline-Viewers, more…
  - Message Formats

Normal Operational **Tasking** Flow

What are **agents** doing on an op?

Mythic Command and Control

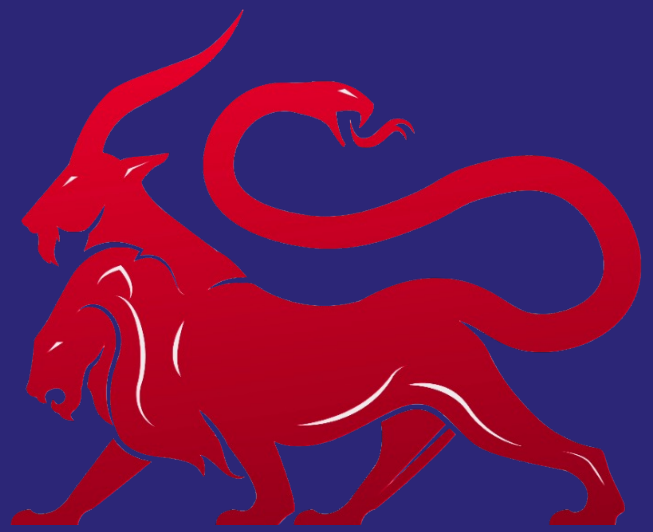
Normal Operational Tasking Flow Pt. 1

1. Install C2 Framework
2. Install Payload Types and C2 Profiles
3. Generate Payloads
4. Execute Payloads on Target

Mythic Command and Control

Normal Operational Tasking Flow Pt. 2-a (Polling C2 – ex: HTTP)

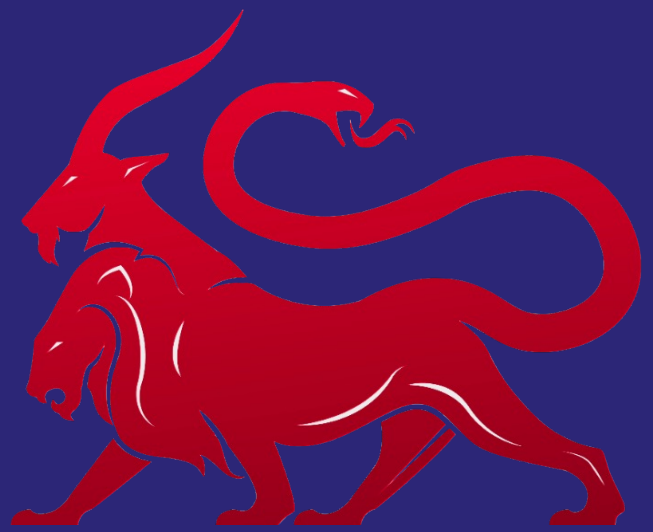
5. Agent Phones Home (new connection)
6. Callback Created
7. Operator Issues Task (saved in database)
8. Agent Phones Home (new connection) (gets task)
9. Agent Phones Home (new connection) (sends response)



Mythic Command and Control

Normal Operational Tasking Flow Pt. 2-b (Push C2 – ex: Websocket)

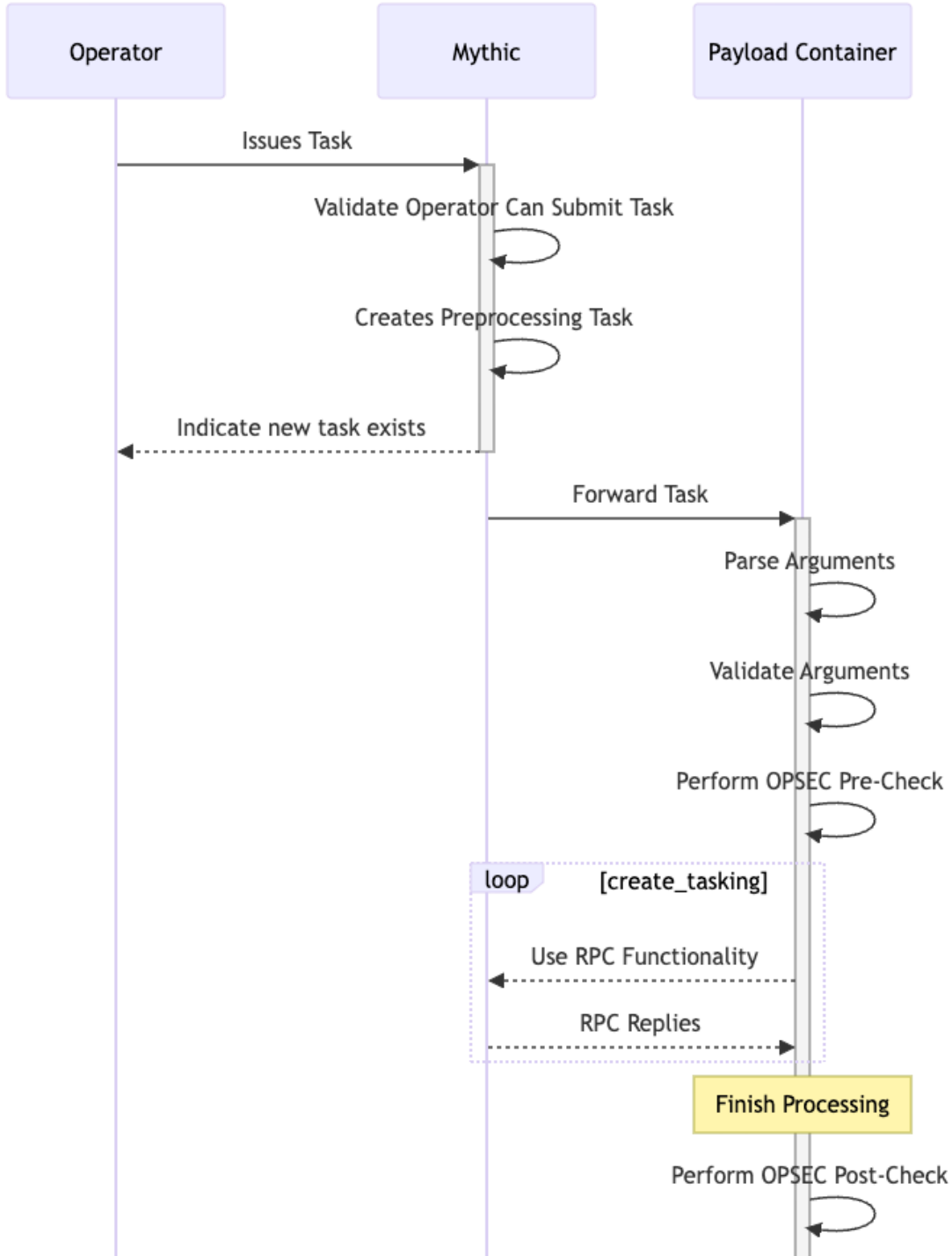
5. Agent Phones Home (new connection) and Waits
6. Callback Created
7. Operator Issues Task (saved in database)
8. Mythic Pushes Task to Agent (same connection)
9. Agent Sends Response and Waits (same connection)



Mythic Command and Control

Normal Operational Tasking Flow Pt. 2 – Tasking Control

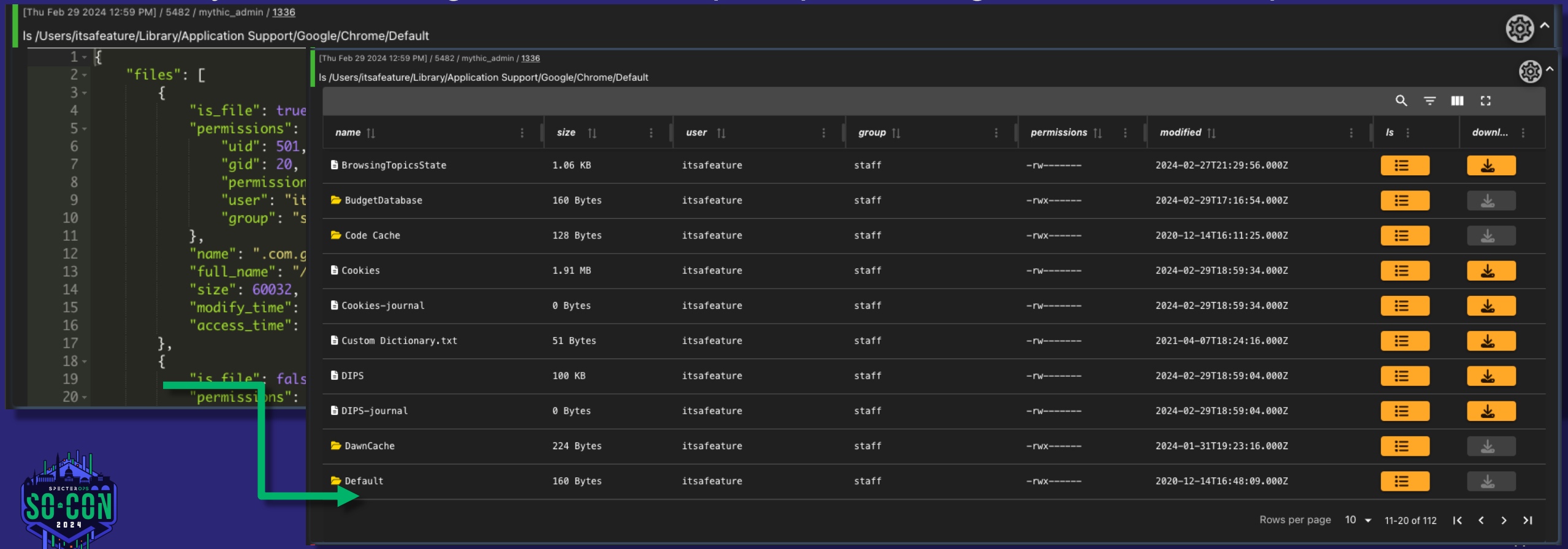
- Mythic allows developers to define all processing
  - How arguments are parsed / defined
  - OPSEC pre/post checks
  - RPC Functionality to Mythic Server
  - Full execution
    - Python
    - GoLang



Mythic Command and Control

Normal Operational Tasking Flow Pt. 2 – Browser Scripting

- Mythic allows agents to define post-processing in the UI for responses



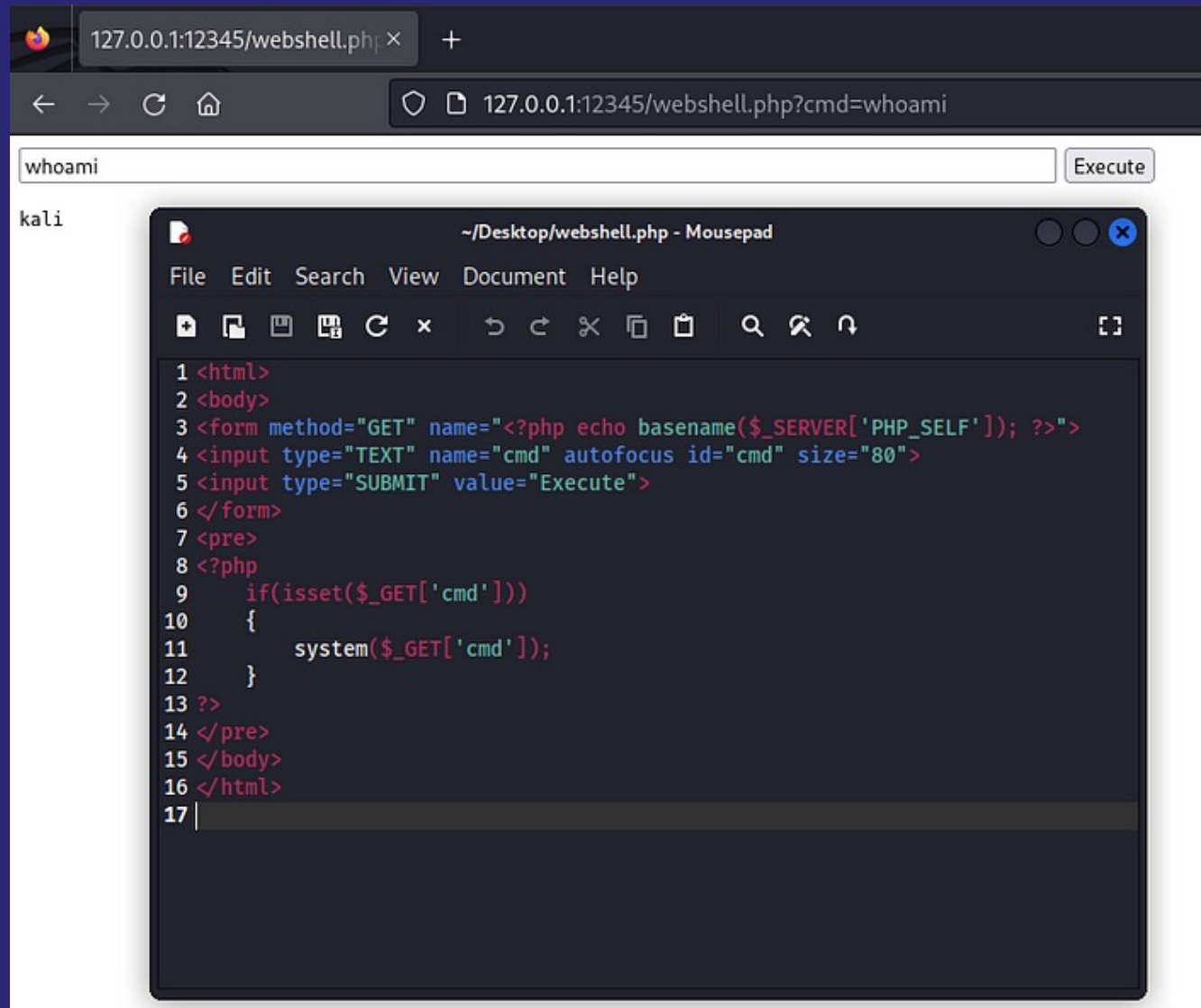
Unconventional Operational **Tasking** Flow

What **could agents** do on an op?

Unconventional Agents

Web Shells

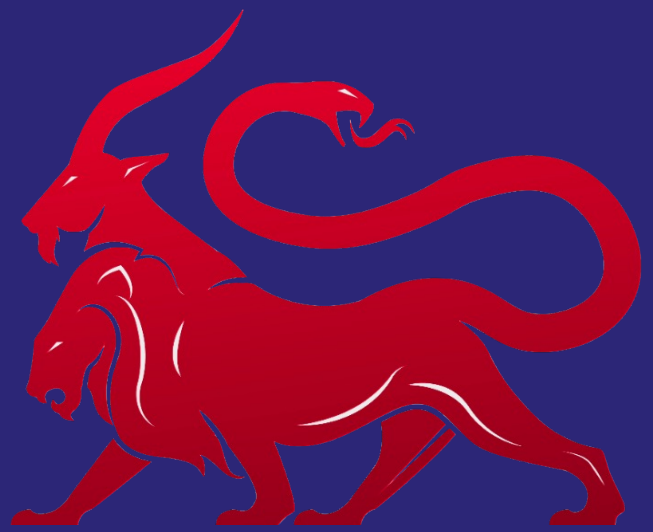
- Web page that allows execution of system commands based on HTTP parameters
  - Typically, a special query parameter or cookie value
- Usually some form of injection or upload allows custom code on the server



Unconventional Agents

Web Shells – The Problems for C2

1. Web shells don't Phone Home to the server
   - How do you get a Callback for it on your server?
2. How do you issue tasks?
   - Nothing is Phoning Home to pick up a task
3. What if the web shell isn't internet accessible?
   - How do you task through another agent?



Unconventional Agents

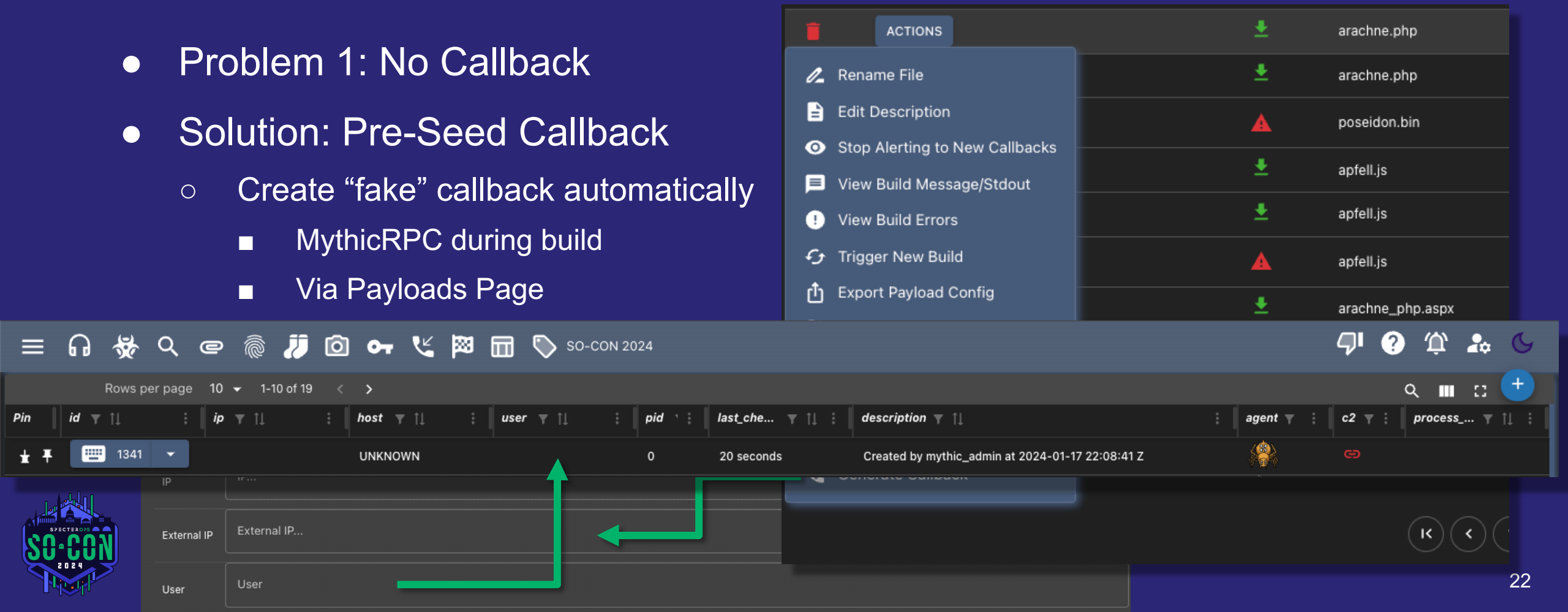
Introducing - Arachne

- https://github.com/MythicAgents/Arachne
- Web Shell agent for Mythic C2
- ASPX and PHP versions
- AES256 Encryption (no key exchange)
- Execute Assembly, Upload, Download, Shell, Ls

Unconventional Agents - Arachne

Web Shells – Solutions

- Problem 1: No Callback
- Solution: Pre-Seed Callback
  - Create “fake” callback automatically
    - MythicRPC during build
    - Via Payloads Page



Unconventional Agents - Arachne

Web Shells – Solutions

```
encrypted_resp = await SendMythicRPCCallbackEncryptBytes(MythicRPCCallbackEncryptBytesMessage(
    AgentCallbackUUID=taskData.Callback.AgentCallbackID,
    Message=message.encode(),
```

1. Encrypt the message

Rows per page 10 11-19 of 19

Pin	id	ip	host	user	domain	last_che...	description	agent	c2
	1244	127.0.1.1	KALI	kali		a month	Created by mythic_admin at 2024-02-07 17:49:13 Z		

CALLBACK: 1244

[Wed Feb 07 2024 12:49 PM] / 4877 / mythic_admin / 1244

ls .

[Wed Feb 07 2024 12:49 PM] / 4878 / mythic_admin / 1244

checkin

```
1 IP: 127.0.1.1
2 OS: Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64
3 User: kali
4 Host: kali
5 Domain:
6 PID: 16235
7 Arch: x86_64
```

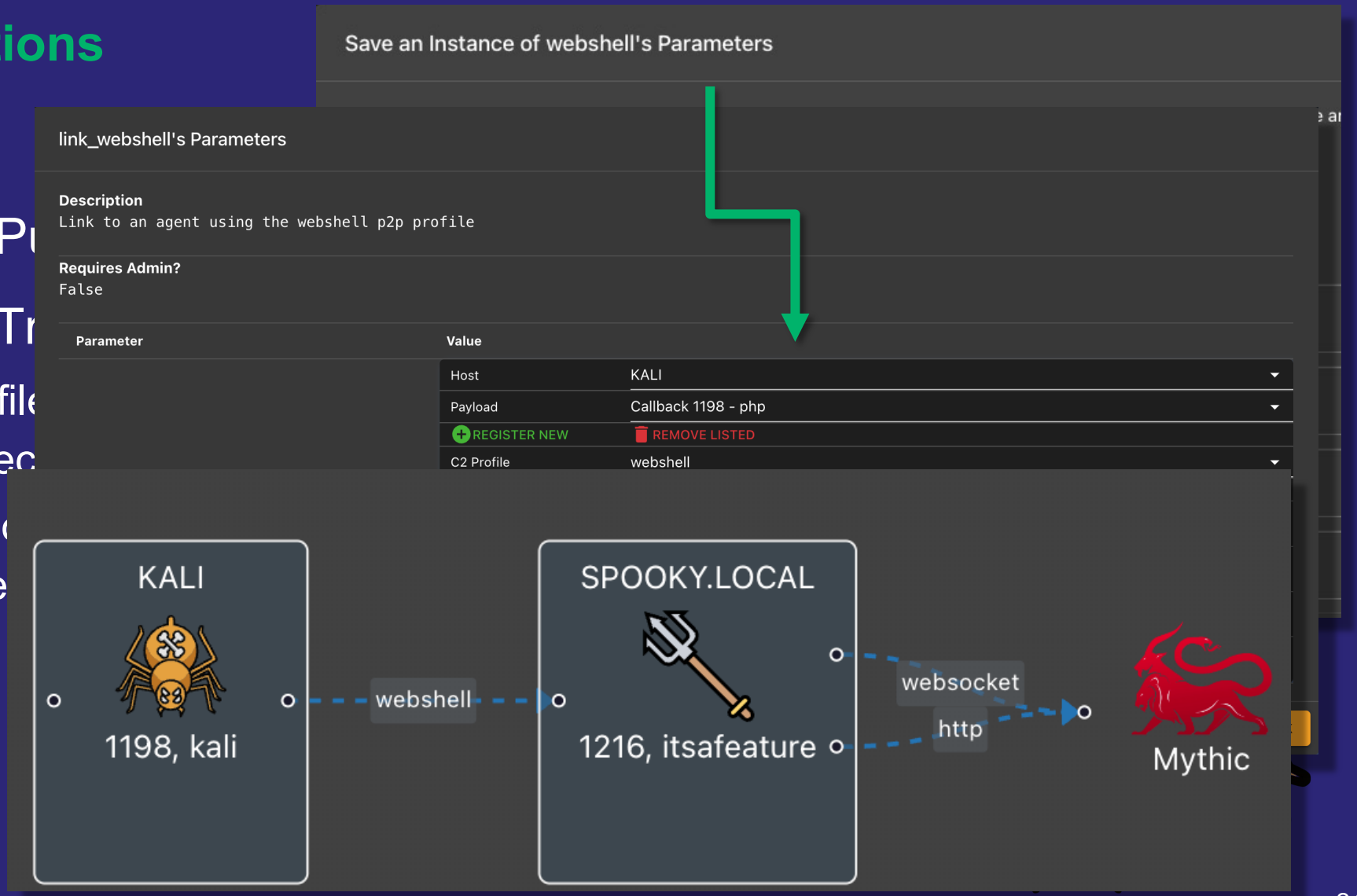
```
OS=info[2],
User=info[3],
Host=info[4],
Domain=info[5],
PID=int(info[6]),
Architecture=info[7]
))
```

4. MythicRPC Update Callback from “checkin”

Unconventional Agents - Arachne

Web Shells – Solutions

- Problem 3: Non-Pu
- Solution: P2P & Tr
  - Create P2P Profile
    shell comms spec
  - Create Translati
    convert web she
    JSON



Unconventional Agents - Arachne

Web Shells – Solutions

- Webshell expects encrypted, ”|” separated messages
- Mythic expects JSON

- Translation container converts between the two so that P2P generated messages

```
async def translate_to_c2_format(self,  its-a-feature *
                                 inputMsg: TrMythicC2ToCustomMessageFormatMessage) -> TrM
    response = TrMythicC2ToCustomMessageFormatMessageResponse(Success=True)
    if "tasks" in inputMsg.Message:
        if len(inpu
            response.Message = inputMsg.Message["tasks"][0]["parameters"].encode("UTF8")
        else:
            response.Message = b""
    else:
        response.Message = b""
    return response

async def translate_from_c2_format(self,  its-a-feature *
                                   inputMsg: TrCustomMessageToMythicC2FormatMessage) -> T
    response = TrCustomMessageToMythicC2FormatMessageResponse(Success=True)
    response_pieces = inputMsg.Message.decode("UTF8").split("|")
    response.Message = {
        "action": "post_response",
        "responses": [
            {
                "task_id": response_pieces[0],
                "process_response": "|".join(response_pieces[1:]),
                "completed": True
            }
        ]}
    return response
```

Remove JSON and return just custom parameters

Create JSON back from custom parameters

Unconventional Agents - Arachne

Recap - https://posts.specterops.io/spinning-webs-unveiling-arachne-for-web-shell-c2-26c40f570ea1

1. Create “callbacks” without needing an agent to phone home
2. Task these “callbacks” with custom execution logic
3. Gained collaboration for traditionally non-collaborative web shells

Mythic 3rd Party Service Agents

What **could help** on an op?

Normal Operational Flow

3rd Party Services

Operating isn't JUST interacting with a C2 platform

- Tracking logs, objectives, findings, artifacts (Ghostwriter)
- Additional Tooling (Bloodhound, Nemesis)
- Team coordination (Slack, Mattermost, Rocketchat, etc)
- Report Writing (Ghostwriter)
- Infrastructure Management

Normal Operational Flow

Problems

- Duplicated data entry between multiple platforms
- Context switching between applications / tools
- Many tools are non-collaborative
- Error prone and tedious to copy paste between applications

Normal Operational Flow

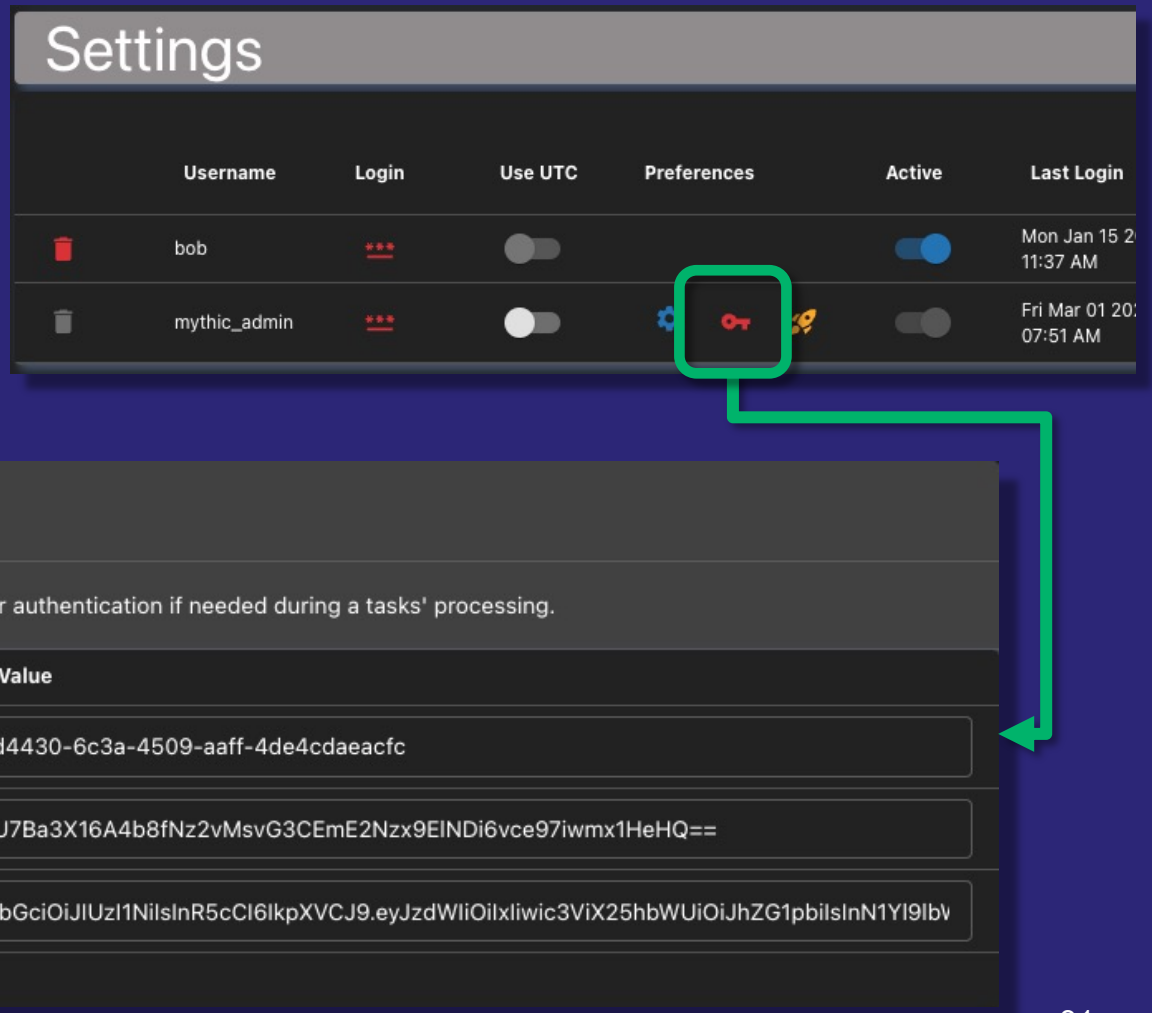
Mythic's 3rd Party Service Solution

- Interacting with 3rd Party services is no different than tasking a web shell
  - Services offer a set of web-based API endpoints
  - Authenticate in some way and display data back to the user
  - Full custom control in Python or GoLang for processing
- Create a taskable agent for each service
  - One problem – still need per-user authentication to 3rd party services

Mythic 3rd Party: Authentication

Secrets Management

- Don’t hardcode each user’s API Tokens
- Don’t store API Tokens in .env
- Dynamically allow new user auth
- Sent as part of tasking



Mythic 3rd Party - Ghostwriter

What **could help** on an op?

Mythic 3rd Party: Ghostwriter

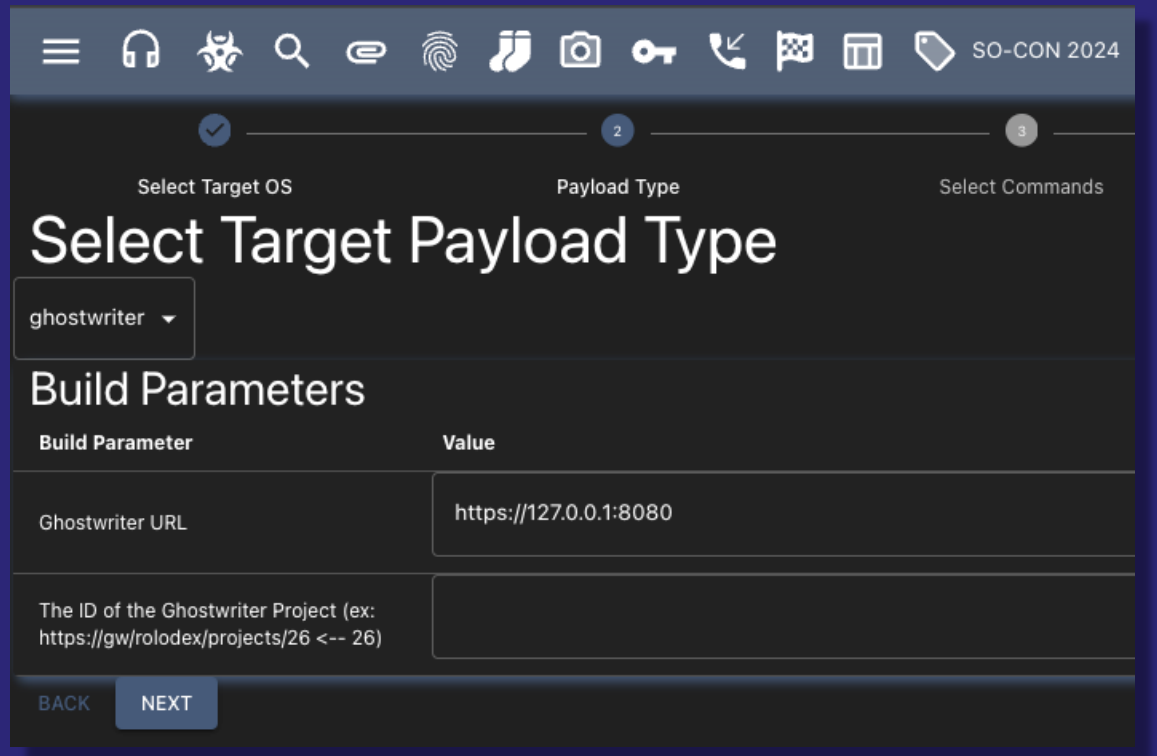
Beyond MythicSync

- Internally, we use Ghostwriter for many things:
  - Aggregated operational logging from terminals, C2, and more
  - Tracking objectives, projects, and clients
  - Report writing with custom findings
  - Evidence for findings
  - Deconfliction
- Some of this is captured in MythicSync for Ghostwriter

Mythic 3rd Party: Ghostwriter

Beyond MythicSync

- Ghostwriter offers an extensive GraphQL API
- An agent needs three things:
  - Location of Ghostwriter server
  - User-specific API JWT
  - Project ID
- Container needs networking access to Ghostwriter server



Mythic 3rd Party: Ghostwriter Commands

findings_*

Work with the findings library and create/attach findings to current reports for the specified project.

objectives_*

Manipulate objectives for the current project. Create new ones, update status, and even create new subtasks.

evidence_*

Create evidence for findings or the report overall. Can't upload files yet

oplog_*

Search the oplog for a variety of information as well as creating new oplog entries.

reports_*

Get information about reports and generate artifacts to include in an appendix.

Mythic 3rd Party: Ghostwriter

findings_*

[Fri Mar 01 2024 03:56 PM] / 5497 / mythic_admin / 1326

findings_get -title ""

Reported Findings

title	severity	complete	reviewer	type	report	actions
1212	Critical(11)	False	tester	Cloud	2024 Q1 Internal Assessment	ACTIONS
Blank Template	Low(2.9)	False	tester	Cloud	Client2 Penetration Test (2023-08-14)	ACTIONS
custom finding2	Informational(null)	False	TBD	Network	Client2 Penetration Test (2023-08-14)	ACTIONS
Blank Template	Informational(null)	False	admin	Cloud	Client2 Penetration Test (2023-08-14)	ACTIONS
custom finding	Informational(null)	False	TBD	Network	Client2 Penetration Test (2023-08-14)	ACTIONS
new finding?	High(null)	False	admin	Host	Client2 Penetration Test (2023-08-14)	ACTIONS
test	Medium(null)	False	admin	Web	Client2 Penetration Test (2023-08-14)	ACTIONS
Test	Critical(10)	False	admin	Cloud	2024 Q1 Internal Assessment	ACTIONS
test	Critical(5.4)	False	admin	Network	Client2 Penetration Test (2023-08-14)	ACTIONS
Test	Critical(10)	False	admin	Cloud	Client2 Penetration Test (2023-08-14)	ACTIONS

Rows per page 10 1-10 of 13

Mythic 3rd Party: Ghostwriter

objectives_*

[Fri Mar 01 2024 04:02 PM] / 5503 / mythic_admin / 1326

objectives_get

Project Objectives

type	objective	complete	due	description	status	priority	actions
objective	make trouble	False	2023-08-19	to make it double	In Progress	Primary	ACTIONS
subtask	second task for primary	True	2023-08-19		Active	Primary	ACTIONS
subtask	updated subtask?	2024-02-08	2023-08-19		In Progress	Primary	ACTIONS
objective	and make it double	False	2023-08-19		Active	Secondary	ACTIONS
objective	defeat team rocket	False	2023-08-19		Active	Tertiary	ACTIONS

CREATE OBJECTIVE

Rows per page 10 1-6 of 6

Mythic 3rd Party: Ghostwriter

oplog_*

[Fri Mar 01 2024 04:06 PM] / 5505 / mythic_admin / 1326

oplog_search {"command":"shell","tool":"beacon"}

Findings

command	comments	des...	ips	tool	userContext	actions
shell id	From beacon 351829956		->	Beacon		ACTIONS
shell whoami		PID: 10120	DESKTOP-F6NR9SF (10.20.16.139)->	Beacon	itsafeature	ACTIONS
shell ok, for real?		PID: 5716	DESKTOP-F6NR9SF (10.20.16.139)->	Beacon	itsafeature	ACTIONS
shell whoami			192.168.53.133->192.168.53.133	beacon	itsafeature	ACTIONS
shell whoami	From beacon 351829956		->	Beacon		ACTIONS
shell whoami	From beacon 351829956		->	Beacon		ACTIONS
run powershell.exe Get-Date		Callback: 14339	10.1.10.101->10.1.10.101	beacon	SYSTEM *	ACTIONS
Tasked beacon to run: powershell.exe Get-Date	T1059	Callback: 14339	10.1.10.101->10.1.10.101	beacon	SYSTEM *	ACTIONS
Tasked beacon to import: /root/Tools/KeeThief/P	T1086,T1064	Callback: 66482	->	beacon	SYSTEM *	ACTIONS
powershell-import /root/Tools/PowerSploit/Recon,		Callback: 16941	10.1.10.25->10.1.10.25	beacon	SYSTEM *	ACTIONS

Rows per page 10 1-10 of 1,624

Mythic 3rd Party: Ghostwriter

evidence_*

[Fri Mar 08 2024 01:52 PM] / 5684 / mythic_admin / 1326

evidence_get

Reported Evidence

name	description	caption	document	finding/report	actions
my new report evidence	descr	capt?	original file	Client2 Penetration Test (2023-08-14) Rep	ACTIONS
new report-wide finding?	just updated the description	what about a fancy new caption?		Client2 Penetration Test (2023-08-14) Rep	ACTIONS
just added this one			just added this one	test	ACTIONS
general report evidence	mydescription	general report evidence caption	evidence/1/dpapi_blob_b64_s	Client2 Penetration Test (2023-08-14) Rep	ACTIONS
backupkey	my description here	found backupkey	evidence/1/dpapi_blob_b64.t	new finding?	ACTIONS
my friendly name?	description	caption	document?	test	ACTIONS

NEW REPORT EVIDENCE

Rows per page 10 1-7 of 7

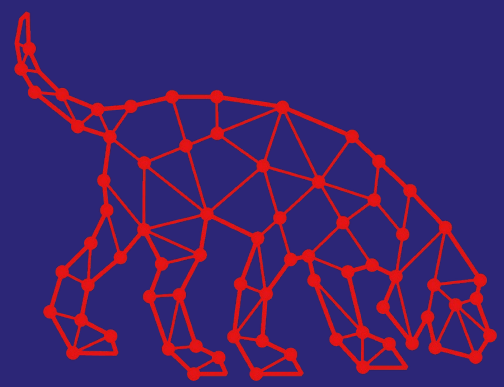
Mythic 3rd Party - Bloodhound

What **could help** on an op?

Mythic 3rd Party: Bloodhound Community Edition

Bloodhound CE

- Bloodhound helps find attack paths in Microsoft Active Directory
- Uses Graph Theory to construct shortest paths between nodes
- Focuses on practically abusable edges
- Community Edition uses Docker to coordinate between:
  - Neo4j and PostgreSQL Databases
  - A React Web UI



BLOODHOUND
COMMUNITY EDITION

Mythic 3rd Party: Bloodhound Community Edition

Bloodhound CE UI Pros / Cons

Bloodhound CE UI Pros:

- Displays a lot of nodes / edges
- Easy to click around and dive into nodes / paths
- Clean UI for displaying enriching text

Bloodhound CE UI Cons:

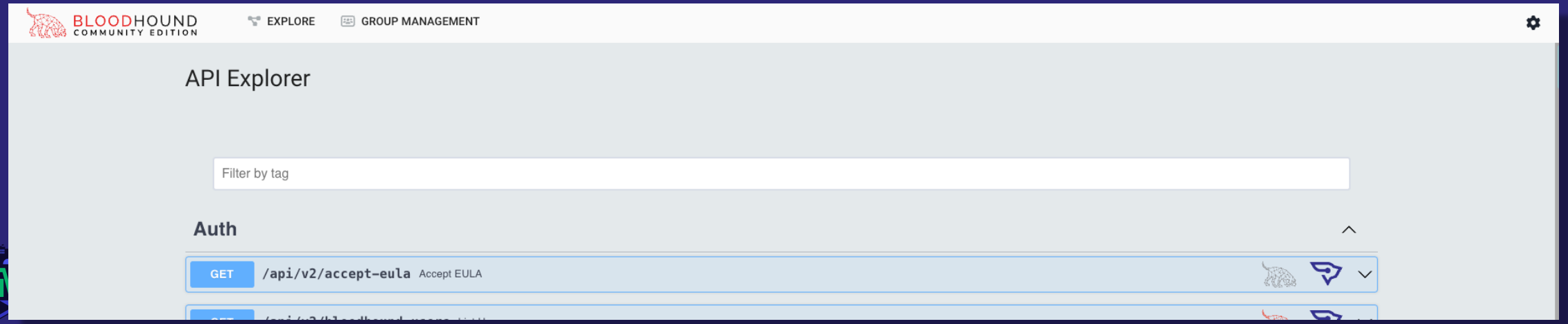
- Not collaborative
- Can’t back-track
- Can’t prune results
- Can’t automatically task agents
- Requires a lot of context switching for ops

Mythic 3rd Party: Bloodhound Community Edition

Bloodhound CE API

Bloodhound CE now offers an API!

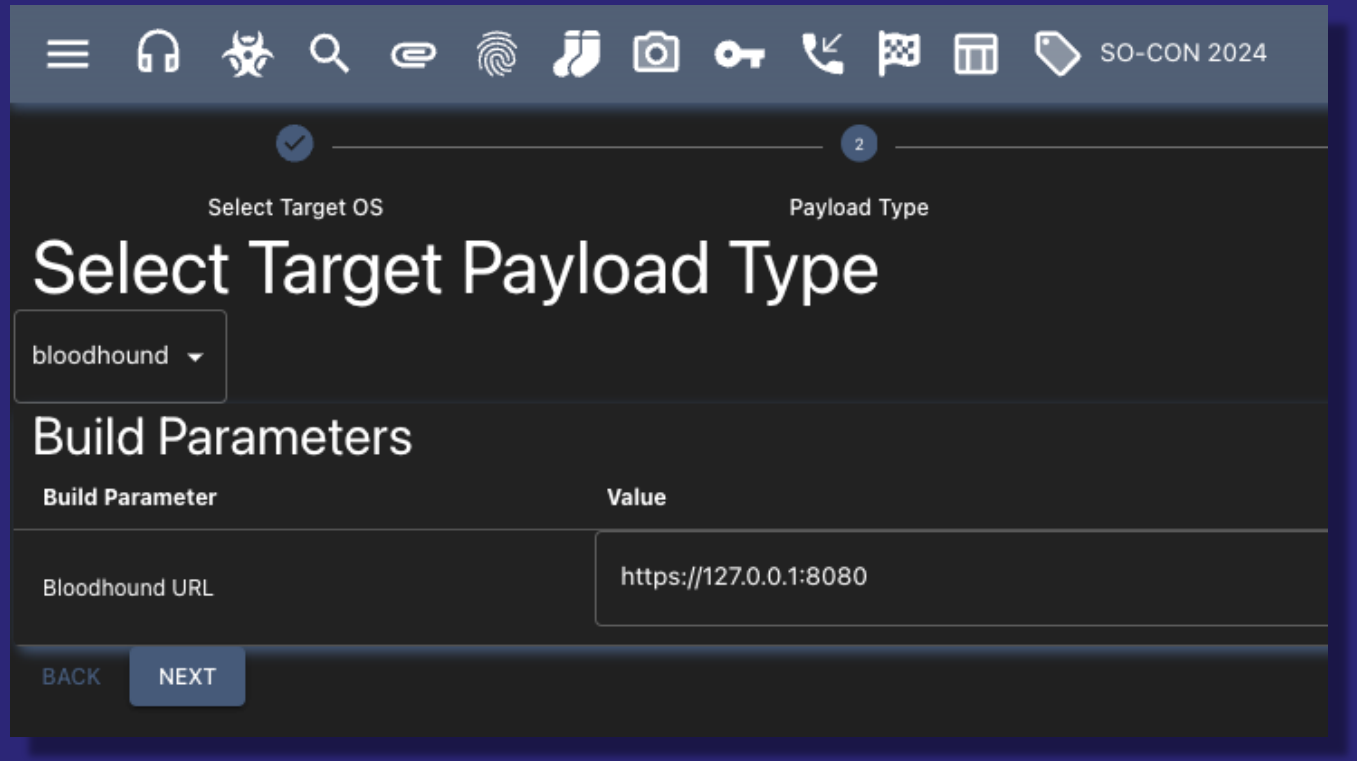
- Documented REST API included with Bloodhound CE installs
- Easy example Python script provided for how to interact
- Uses API Token and ID generated for your user



Mythic 3rd Party: Bloodhound Community Edition

Bloodhound CE Agent

- Query Bloodhound's API and process it in Mythic
- Every query is saved as a new Task
- Responses seen by everybody in an operation
- Agent needs URL
  - Each user provides API Secret



Mythic 3rd Party: Bloodhound Commands

cypher_*

Execute raw custom Cypher queries, leverage user-specified custom queries, or use Bloodhound's pre-defined queries.

get_*

Get information about objects, users, owned entities, and groups.

upload_*

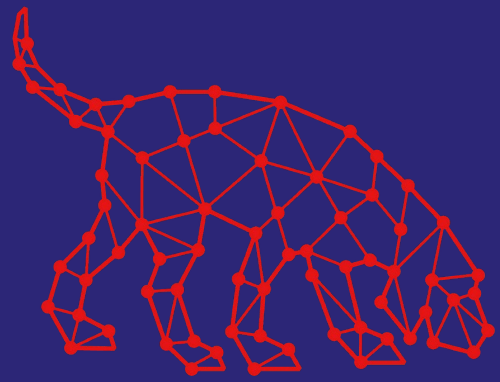
Upload and track upload status for ingesting JSON data into Bloodhound. Fetches data downloaded by Mythic agents or uploaded manually.

shortest_path

Calculate shortest paths between two objects

controllables

Get controllable information about an object.

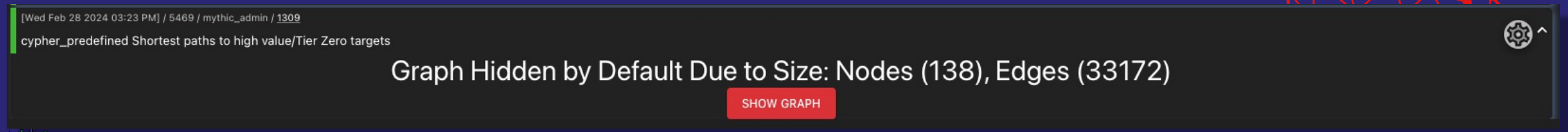


BLOODHOUND
COMMUNITY EDITION

Mythic 3rd Party: Bloodhound Community Edition

Browser Scripting Graphs

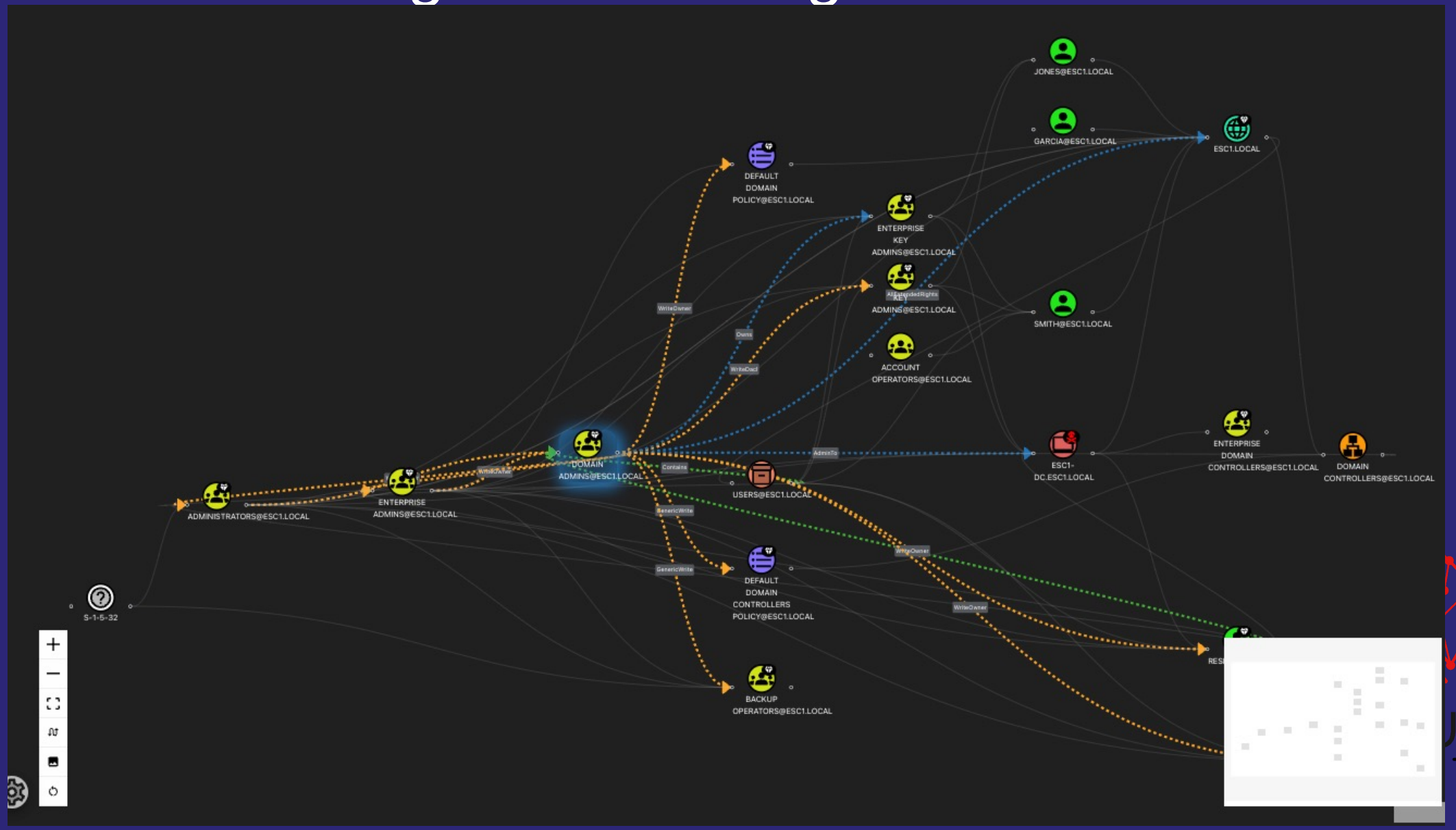
- Bloodhound works in graphs while most other things use tables
- Mythic's Browser Scripting now offers a "graph" option
  - Specify Nodes, Edges, Icons, Overlay Icons
  - Specify custom node and edge context menu actions
  - Specify custom Node and Edge styling
  - Auto-hiding graphs with > 50 nodes



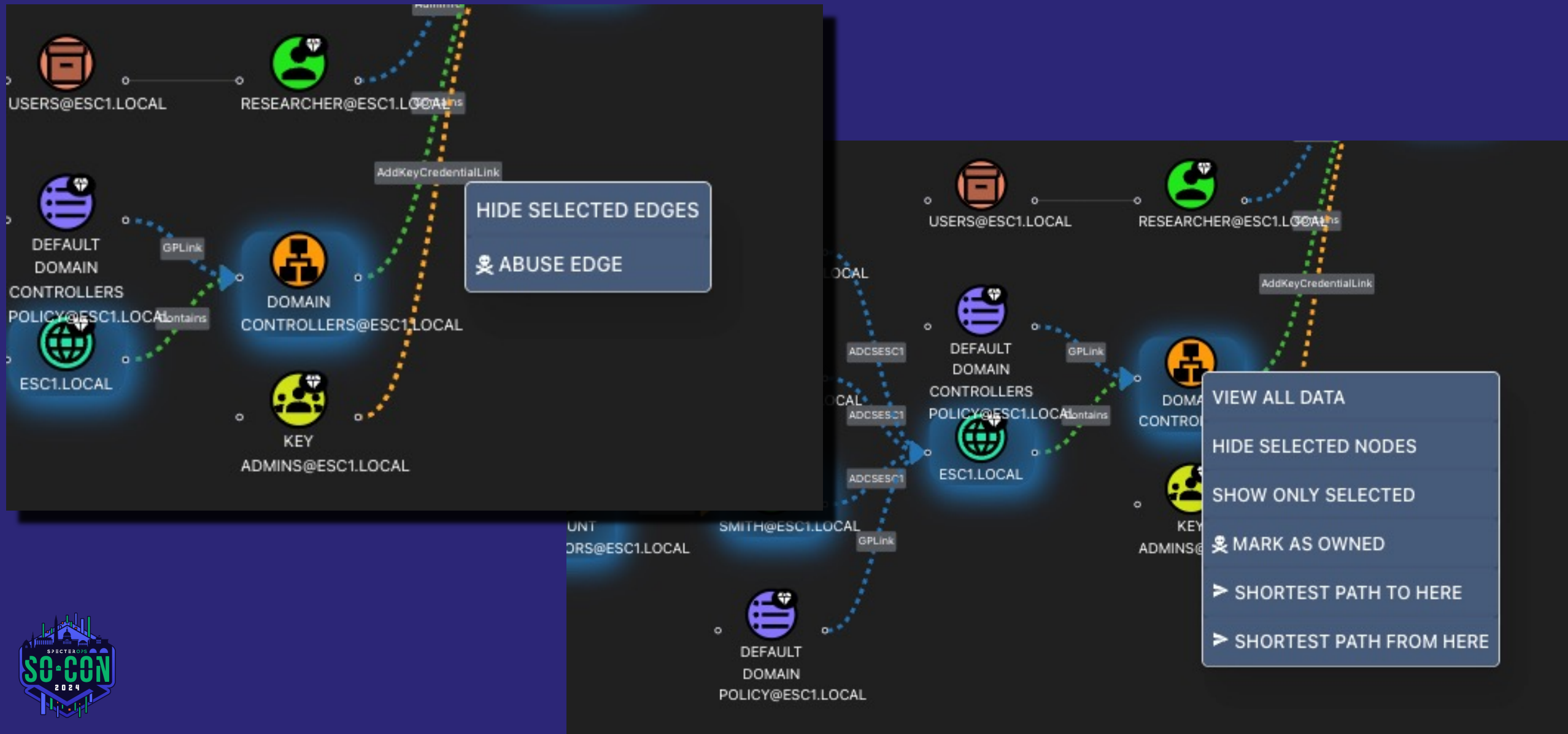
Bloodhound Agent: Rendering Graphs

Graph Controls and Minimap

Bloodhound Agent: Selecting Nodes

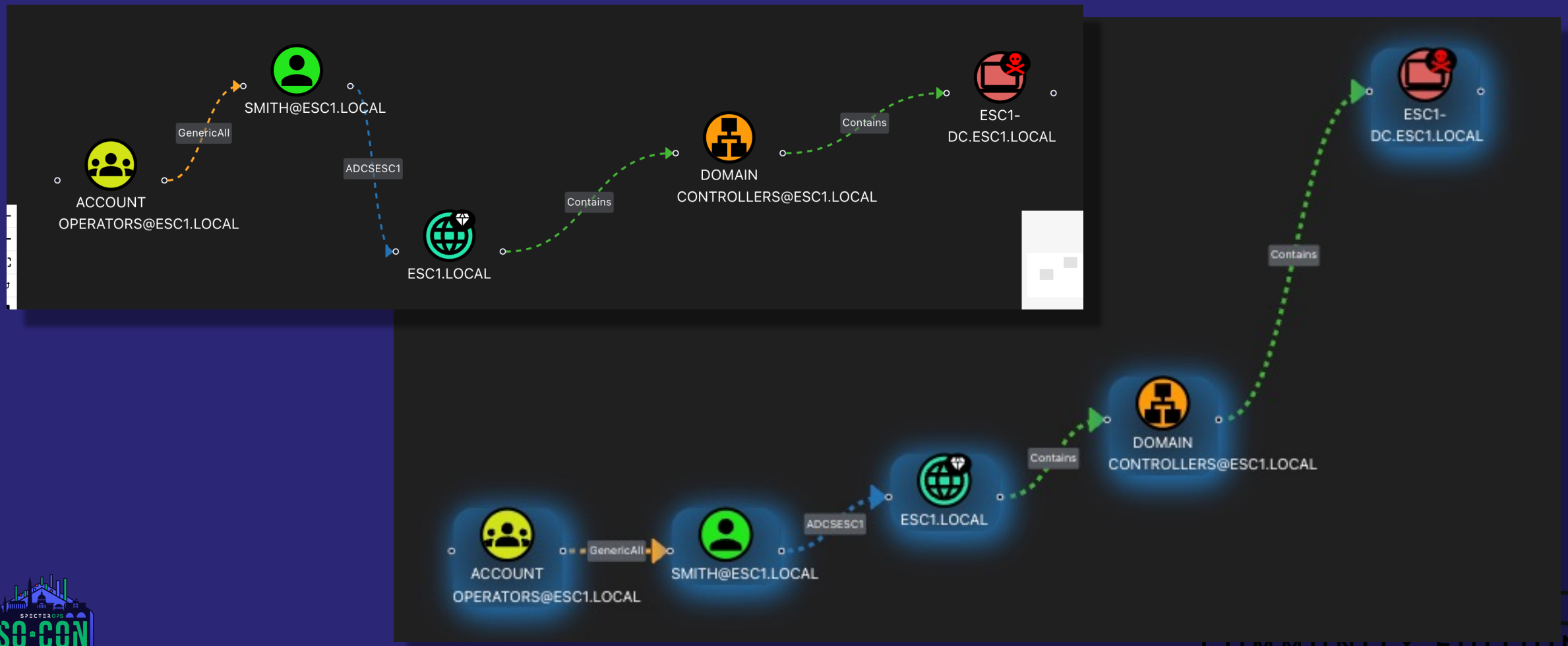


Bloodhound Agent: Graph Context Menus



Bloodhound Agent: Graph Pruning

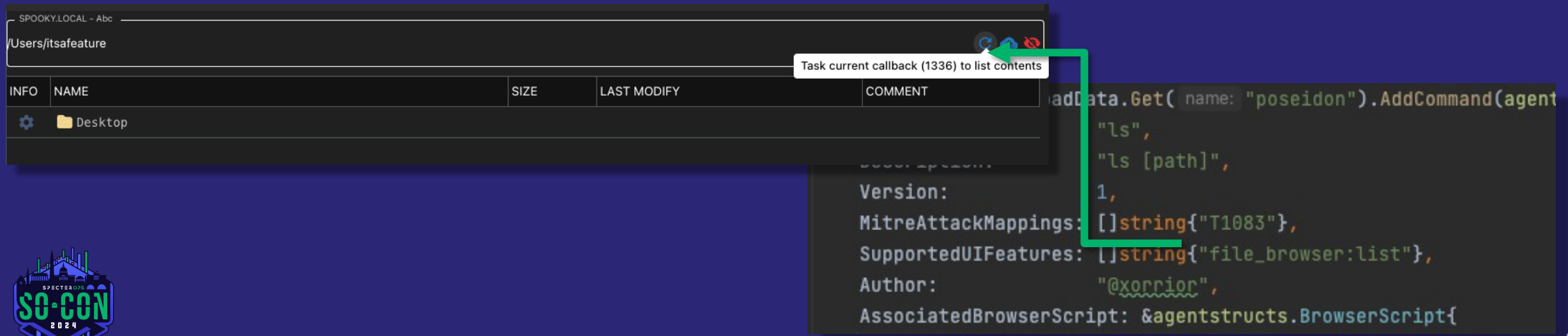
Show Only Selected



Bloodhound Agent: Leveraging Other Agents

Supported UI Features

- Mythic provides an option for “automatic” tasking via “UI Features”
  - Agents declare support for a “UI Feature” in commands
  - Browserscript buttons issue tasks via these features
  - ex: File Browser listing happens via loaded “file_browser:list” feature

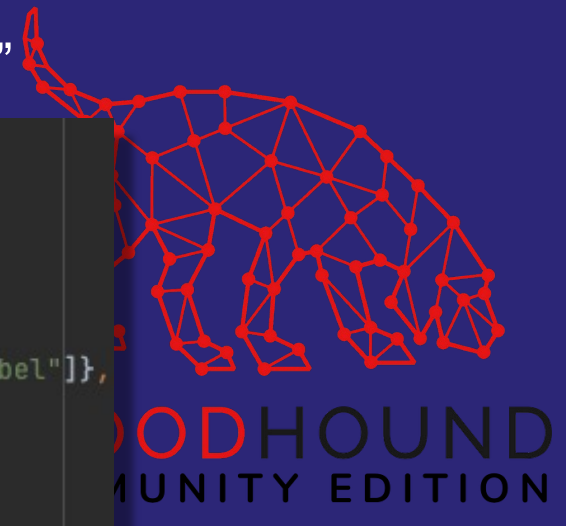


Bloodhound Agent: Leveraging Other Agents

Supported UI Features

- Some features are always present
  - callback_table:exit, file_browser:list, process_browser:list, etc
- Agents can define their own custom ones
  - Defaults to commands currently loaded within the same callback
  - Can request to task **OTHER** callbacks that support a “ui_feature”

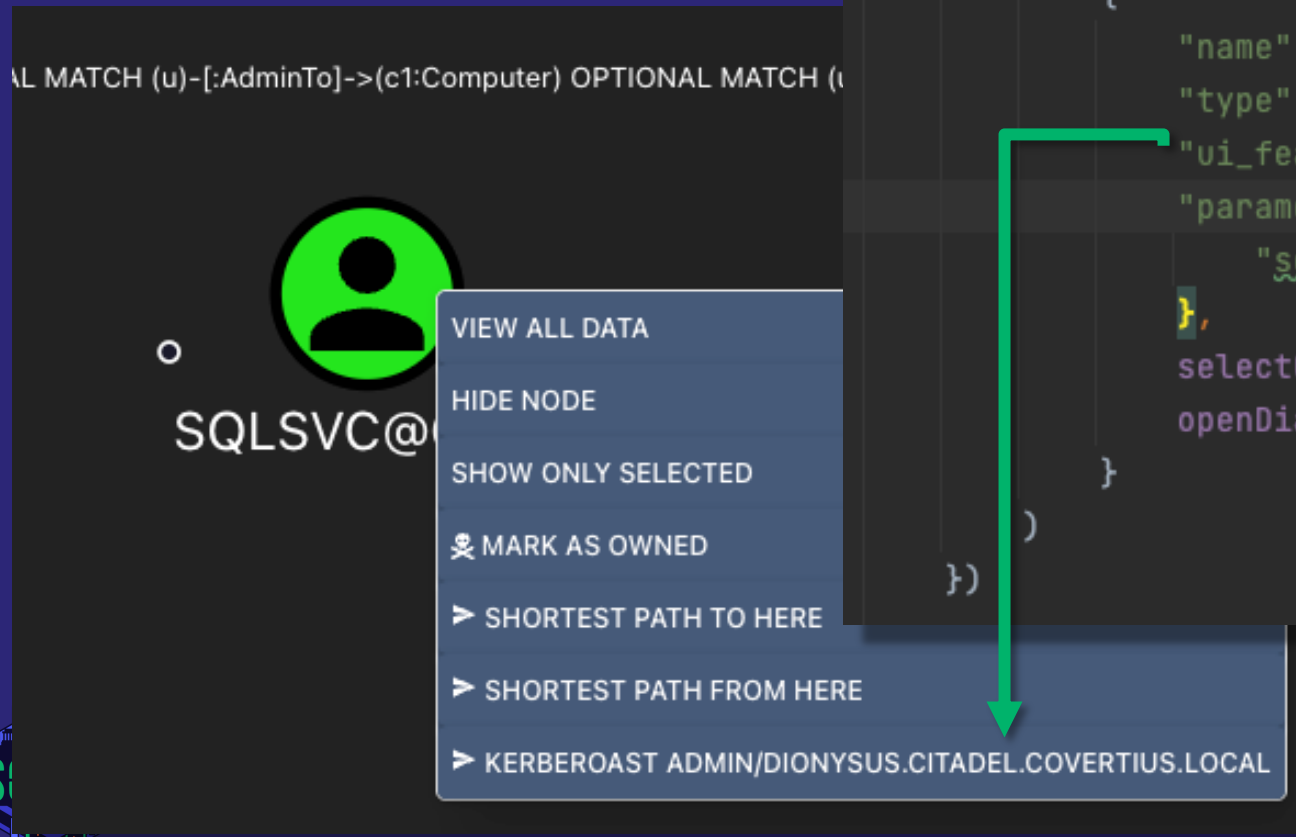
```
buttons: [
    {
        "name": "Abuse Edge",
        "type": "task",
        "ui_feature": `bloodhound:${e['kind']}`.toLowerCase(),
        "parameters": {"edge": e["kind"], "source": sData["label"], "destination": dData["label"]},
        "startIcon": "kill",
        selectCallback: true,
        openDialog: true,
```



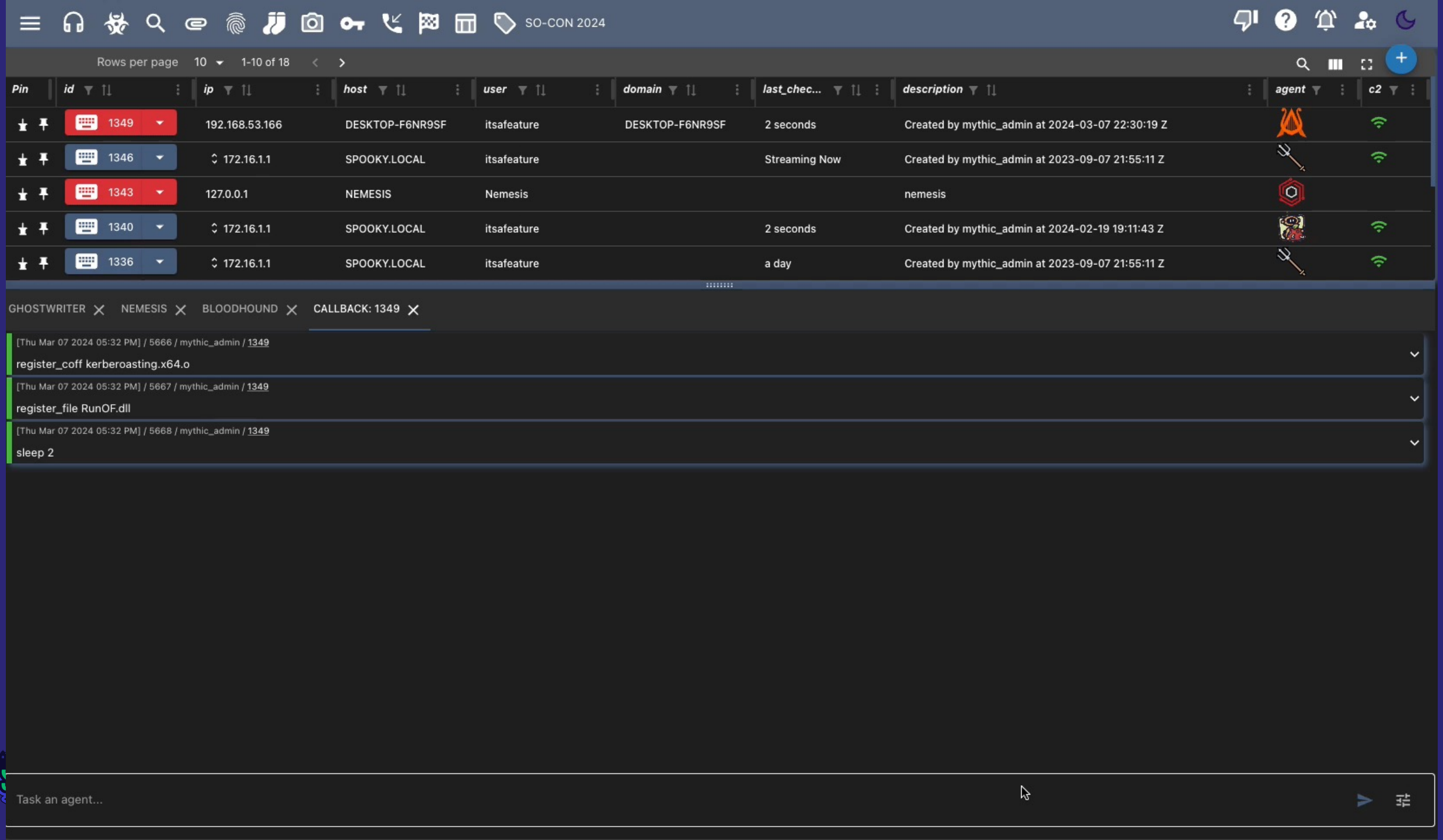
Bloodhound Agent: Leveraging Other Agents

Supported UI Features – Tasking Flow

```
if(val?.properties?.hasspn && val?.properties?.serviceprincipalnames?.length > 0){
    val?.properties?.serviceprincipalnames.forEach( (v) => {
        buttons.push(
            {
                "name": "Kerberoast " + v,
                "type": "task",
                "ui_feature": "bloodhound:kerberoast",
                "parameters": {
                    "serviceprincipalname": v,
                },
                selectCallback: true,
                openDialog: true,
            }
        )
    })
```



BLOODHOUND
COMMUNITY EDITION


SO-CON 2024
Rows per page 10 1-10 of 18
Pin id ip host user domain last_chec... description agent c2
1349 192.168.53.166 DESKTOP-F6NR9SF itsafeature DESKTOP-F6NR9SF 2 seconds Created by mythic_admin at 2024-03-07 22:30:19 Z
1346 172.16.1.1 SPOOKY.LOCAL itsafeature Streaming Now Created by mythic_admin at 2023-09-07 21:55:11 Z
1343 127.0.0.1 NEMESIS Nemesis nemesis
1340 172.16.1.1 SPOOKY.LOCAL itsafeature 2 seconds Created by mythic_admin at 2024-02-19 19:11:43 Z
1336 172.16.1.1 SPOOKY.LOCAL itsafeature a day Created by mythic_admin at 2023-09-07 21:55:11 Z
GHOSTWRITER NEMESIS BLOODHOUND CALLBACK: 1349
[Thu Mar 07 2024 05:32 PM] / 5666 / mythic_admin / 1349
register_coff kerberoasting.x64.o
[Thu Mar 07 2024 05:32 PM] / 5667 / mythic_admin / 1349
register_file RunOF.dll
[Thu Mar 07 2024 05:32 PM] / 5668 / mythic_admin / 1349
sleep 2
Task an agent...

Mythic 3rd Party - Nemesis

What **could help** on an op?

Mythic 3rd Party: Nemesis

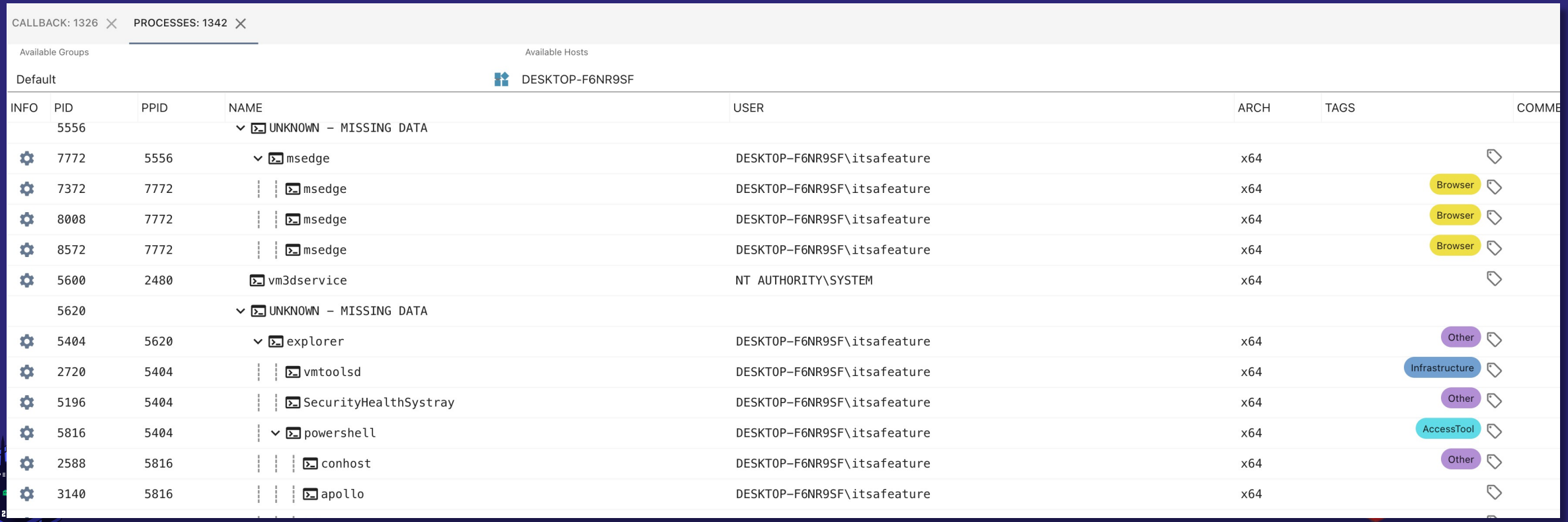
https://github.com/SpecterOps/Nemesis

- Nemesis is an offensive data enrichment pipeline and operator support system
  - Aggregates data across many “connectors”
- Automatically processes
  - Downloaded Files
  - Process Data
  - Certain Registry/Seatbelt Data

Mythic 3rd Party: Nemesis

https://github.com/SpecterOps/Nemesis

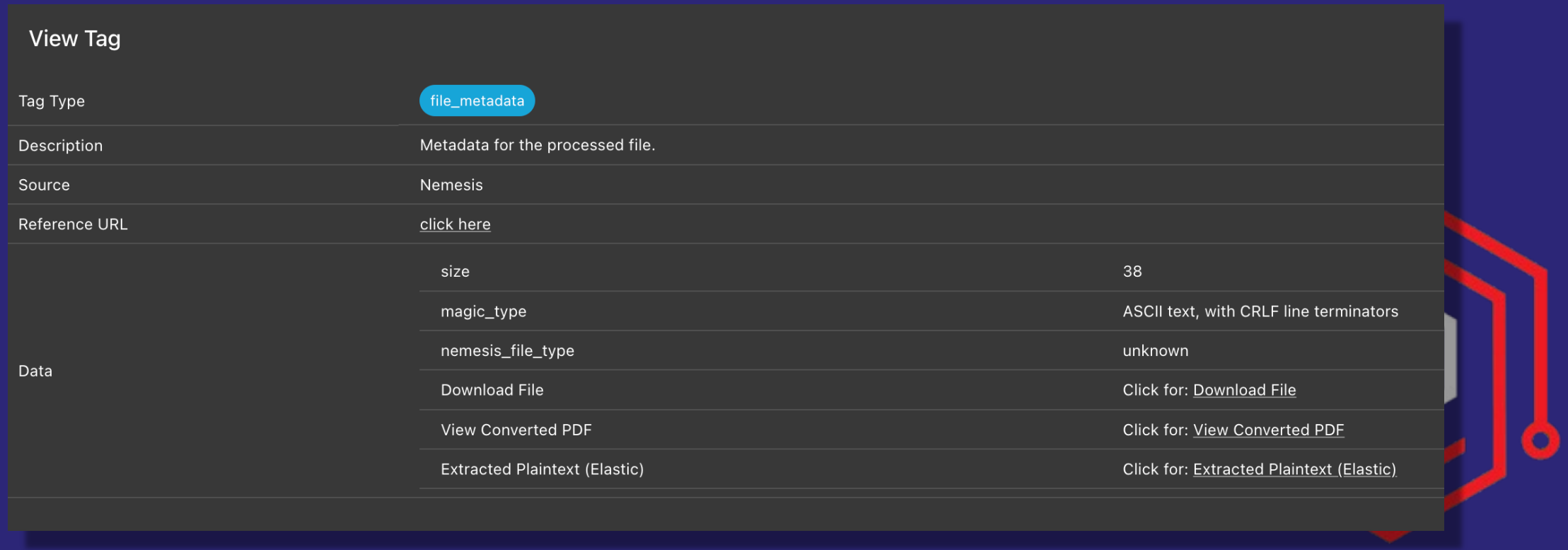
- Nemesis reports findings back to Mythic in the form of tags



Mythic 3rd Party: Nemesis

https://github.com/SpecterOps/Nemesis

- Clicking tags provides more context and links back to Nemesis



Mythic 3rd Party: Nemesis

https://github.com/SpecterOps/Nemesis

- Reducing the number of open tabs can help streamline workflows
- Fetching data from Nemesis directly can speed up collaboration
- Nemesis now includes an alpha version of a GraphQL (Hasura) API
- All a nemesis agent needs is:
  - URL location of nemesis
  - Username / Password for Basic Authentication

Mythic 3rd Party: Nemesis

https://github.com/SpecterOps/Nemesis

[Thu Mar 07 2024 03:10 PM] / 5636 / mythic_admin / 1343

chromium

Login Data

browser	decrypted	realm	user	username
chrome		https://www.example.com/	dpapiuser	harmj0y
chrome	This-Is-A-DPAPI-Protected-Value	https://test.local/	dpapiuser	harmj0y

History

browser	title	count	last	user
chrome	Download Microsoft Edge	3	2023-04-24T18:23:46.159Z	
chrome	Download Microsoft Edge	2	2023-04-24T18:23:45.733Z	
chrome	microsoft edge download - Google Search	2	2023-04-24T18:23:42.732Z	
chrome	Microsoft - Cloud, Computers, Apps & Gaming	1	2023-04-24T18:21:08.738Z	

Mythic 3rd Party: Nemesis

https://github.com/SpecterOps/Nemesis

[Wed Mar 06 2024 07:25 PM] / 5590 / mythic_admin / 1343

hashes

Collected Hashes

hash_type	hash_value	cracked
hash_dpapi_masterkey	$DPAPImk$1*2*S-1-5-21-937929760-3187473010-80948926-2115*de:	false
hash_dpapi_masterkey	$DPAPImk$1*3*S-1-5-21-937929760-3187473010-80948926-2115*de:	false
hash_pdf	pdf4*4*128*-12*1*16*562e567879655af5a69f601928067a99*32*b!	false
hash_pdf	pdf4*4*128*-1060*1*16*d660924040ec4846b61c034bd898c28c*32:	false
hash_ms_office	$office$*2013*100000*256*16*5737313473fee96e0bf6e5f0a31d09f!	false
hash_ms_office	$oldoffice$4*c7e570b71025429fe6c1ca66659e1db1*886ce474ec4b5(	false

Mythic 3rd Party: Nemesis

https://github.com/SpecterOps/Nemesis

upload's Parameters

Description
Upload a new file to Nemesis for processing

Requires Admin?
False

Parameter Group
Manually Upload New File

Parameter	Value
file Required	SELECT FILE
remote_path	

[Thu Mar 07 2024 03:23 PM] / 5627 / mythic_admin / 1343

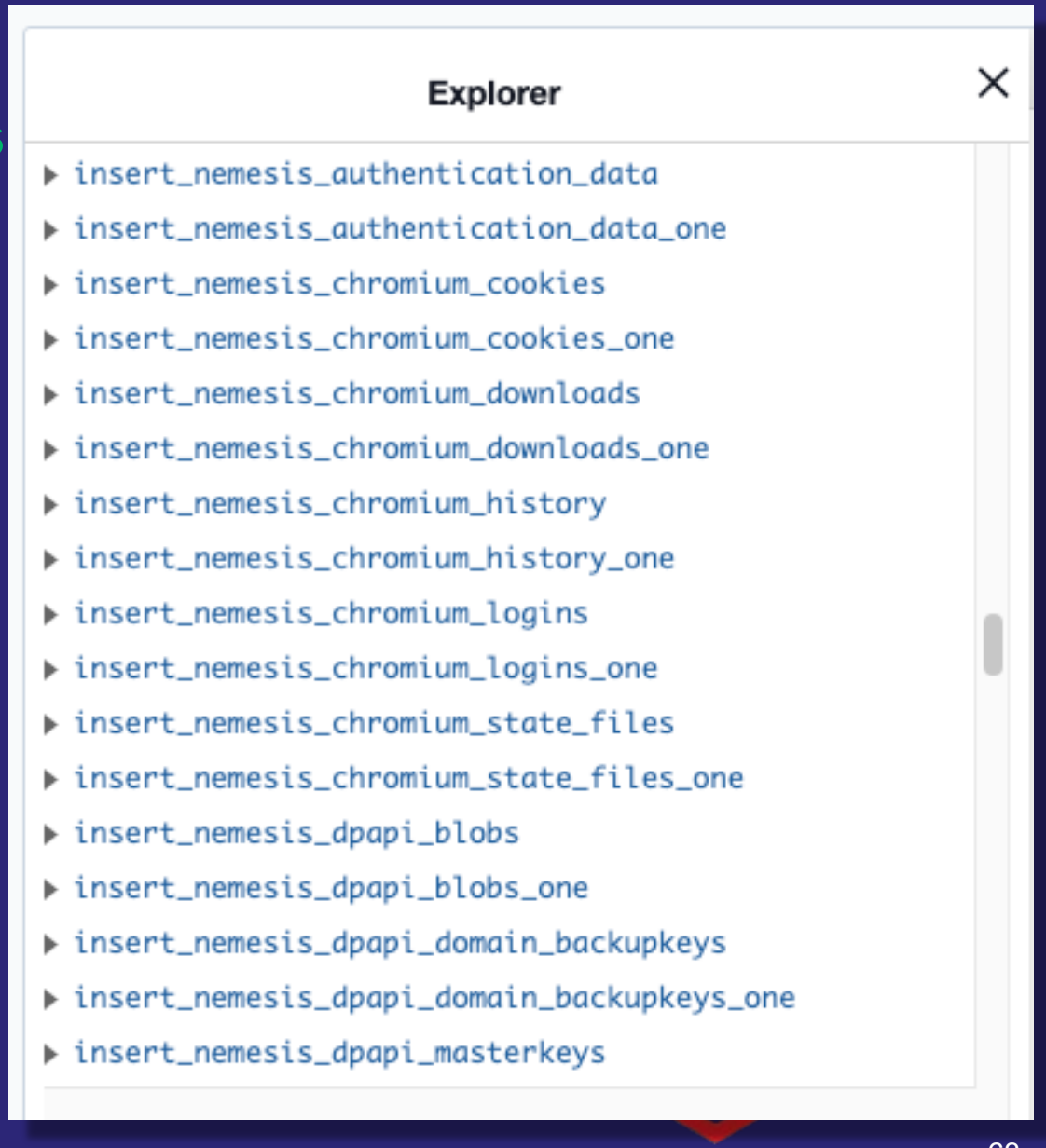
upload -remote_path C/Users/DPAPIUser/AppData/Roaming/Microsoft/Protect/S-1-5-21-937929760-3187473010-80948926-2115/ab998260-e99d-4871-8f4b-d922b2848ce6

```
{
    "file_id": "f56f102f-011e-451b-a17b-3a79278a6c07",
    "update_file": {
        "object_id": "454d18af-ae4e-49c7-8ab8-42e34046f6c9"
    }
}
```

Mythic 3rd Party: Nemesis

https://github.com/SpecterOps/Nemesis

- With Hasura API we can manipulate data too
- Update Nemesis directly with credentials collected from
  - screenshots
  - keylogs
- More features as Nemesis' API expands



Mythic 3rd Party - Wrap up

Mythic 3rd Party

Review

- Authenticate on a per-user basis to remote, 3rd party services
- Get API-level control but graphical representation of results
  - Browser Scripting
- Expose most user-needed functionality in familiar agent tasking interface
- Collaboration and API history provided by Mythic
- Open Source and open for PRs for more functionality!

SPECTEROPS

Thank you

https://github.com/its-a-feature/Mythic

https://mythicmeta.github.io/overview

https://github.com/MythicAgents/**nemesis**

https://github.com/MythicAgents/**ghostwriter**

https://github.com/MythicAgents/**bloodhound**

https://github.com/MythicAgents/**arachne**

Cody Thomas | cody@specterops.io