Using RPA for a fast, reliable and repeatable Incident Response process

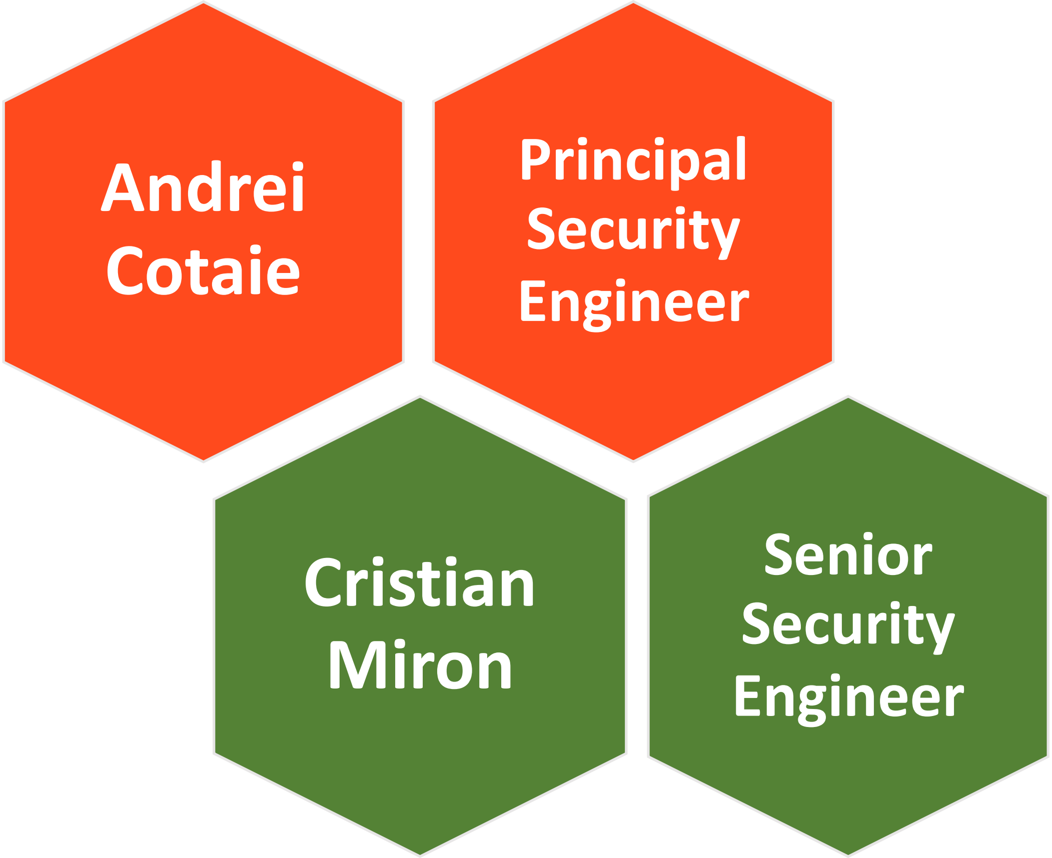
(or for whatever you want…)

UiPath The Foundation of Innovation™

whoami

UiPath

Security Operations / Incident Response Team



Andrei Cotaie

Principal Security Engineer

Cristian Miron

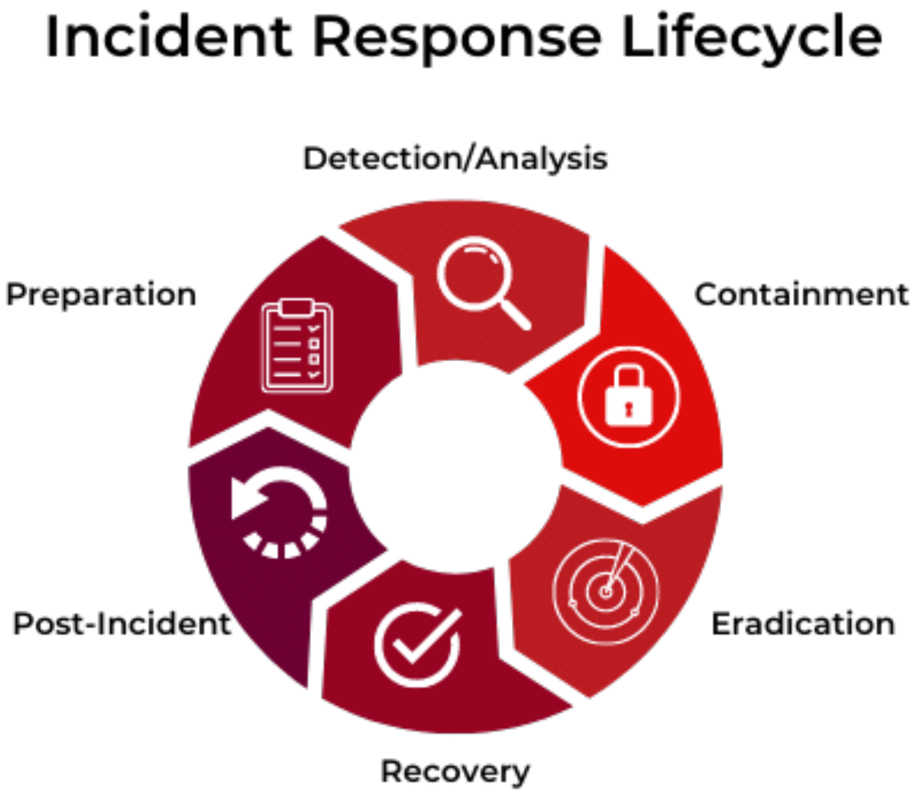
Senior Security Engineer

What is Incident Response?

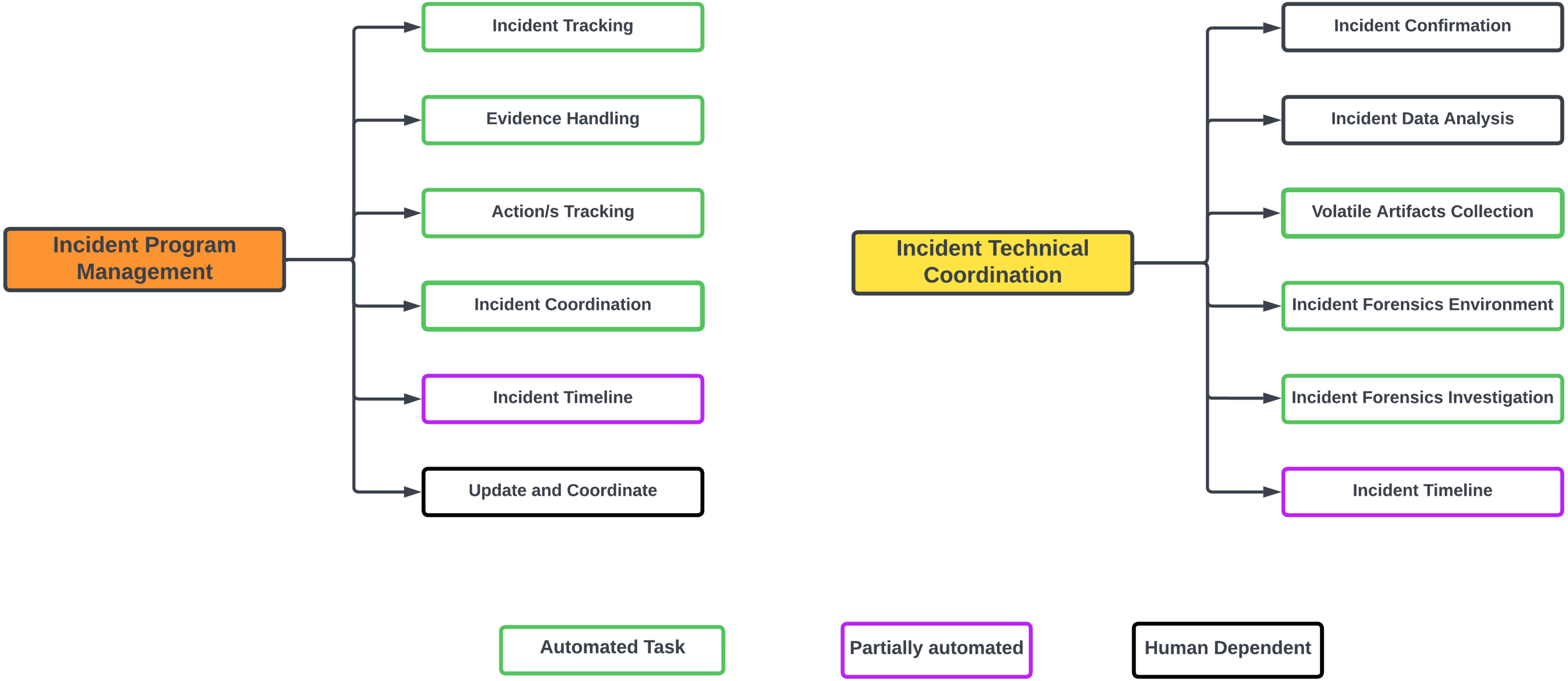
- It's the process used to respond to incidents... ha!

- Incident Response, officially, is the structured approach to managing and recovering from security incidents, with the ultimate aim of minimizing damage, reducing downtime, and improving overall cybersecurity posture. (so says ChatGPT);

- In other words:
  - Incidents happens when Security Fails
  - Incident Response is the Response to Failure



IR: Moment Zero



Incident Program Management

- Incident Tracking
- Evidence Handling
- Action/s Tracking
- Incident Coordination
- Incident Timeline
- Update and Coordinate

Incident Technical Coordination

- Incident Confirmation
- Incident Data Analysis
- Volatile Artifacts Collection
- Incident Forensics Environment
- Incident Forensics Investigation
- Incident Timeline

Automated Task

Partially automated

Human Dependent

Scripting *vs* RPA

Scripting

- Done locally;
- Requires environment with libraries downloaded;
- If going into more developed activities, it requires reading of documentation – I've heard 5 hours of debugging can save up to 5 minutes of reading documentation ;
- Needs integrations, formatting of data, compatibility issues when moved to another machine;
- Loves locally stored credentials

RPA

- Easy to develop;
- Built-in integrations with various tools;
- If you don't want to read documentation or install extra packages, you don't need to, click through the GUI and it will follow your instructions;
- Once developed it can run anywhere you need it to;
- Can integrate and execute code from various languages;
- Centralized credentials Vault in Orchestrator

RPA: Attended vs Unattended

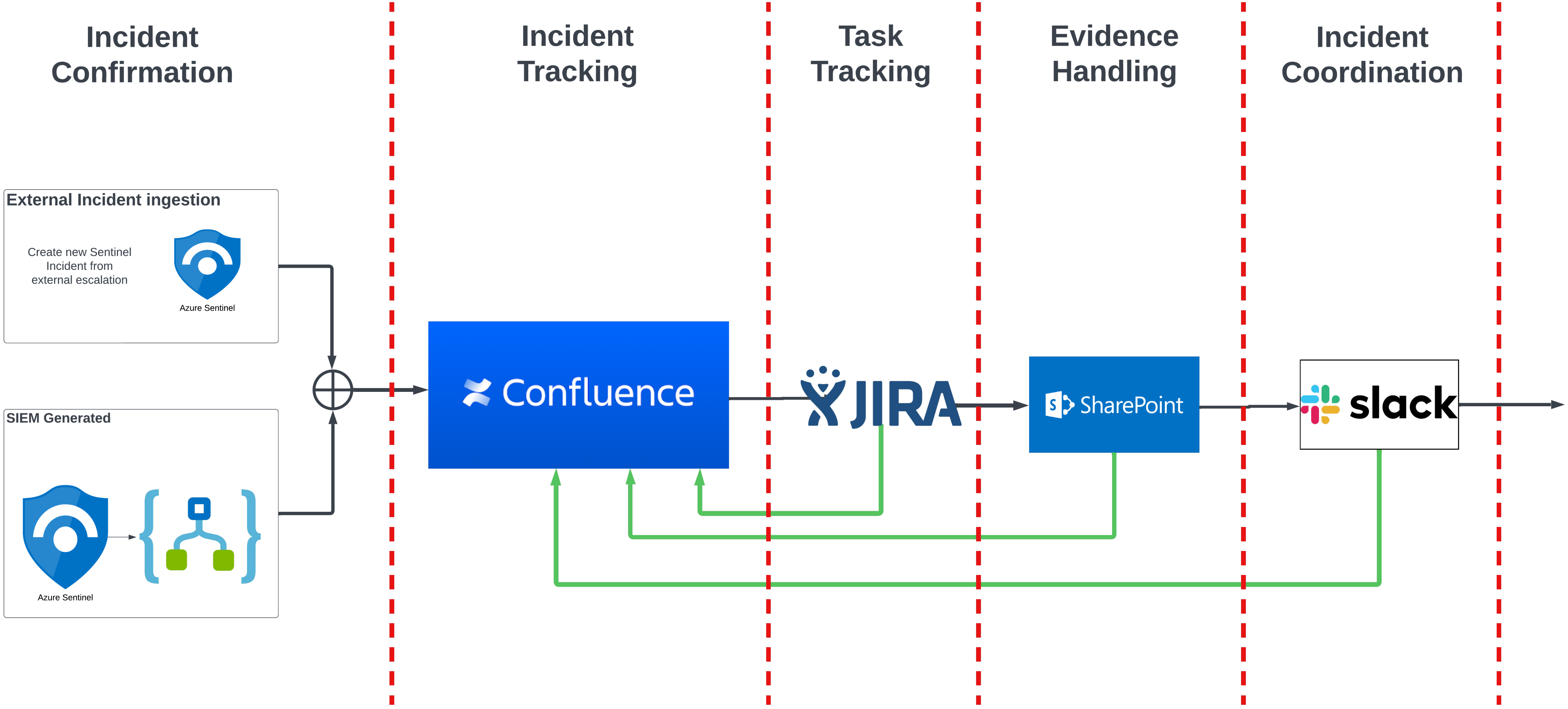
Attended

- Runs locally on the user's machine;
- Triggered by the user;
- Uses local credentials;
- It allows for interactions between the user and the robot;
- Need a person at the computer.

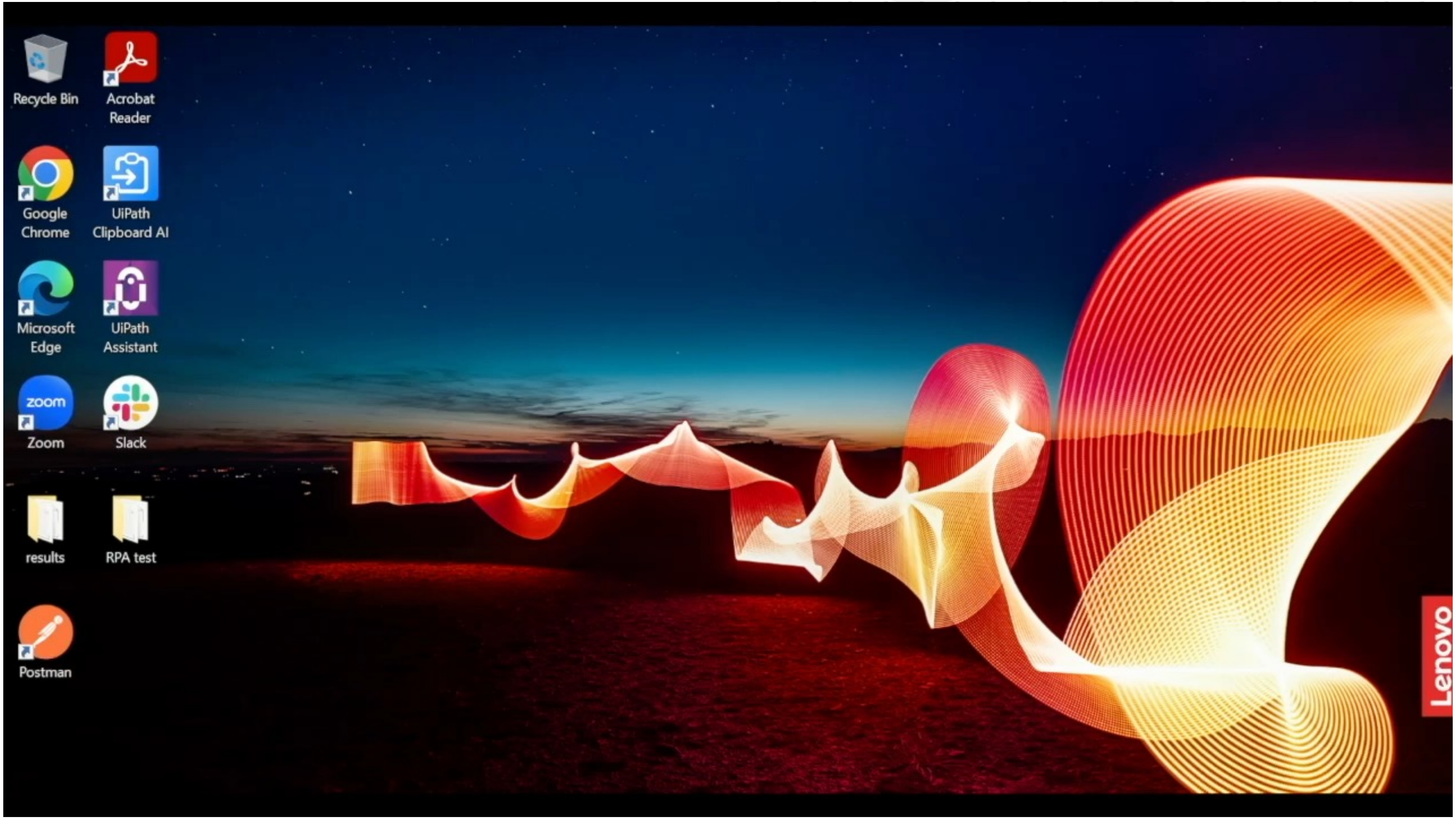
Unattended

- Runs on a dedicated VM used solely for that purpose;
- Can be scheduled trigger or queue;
- Uses credentials specific to the VM;
- Can notify the person watching the process of updates;

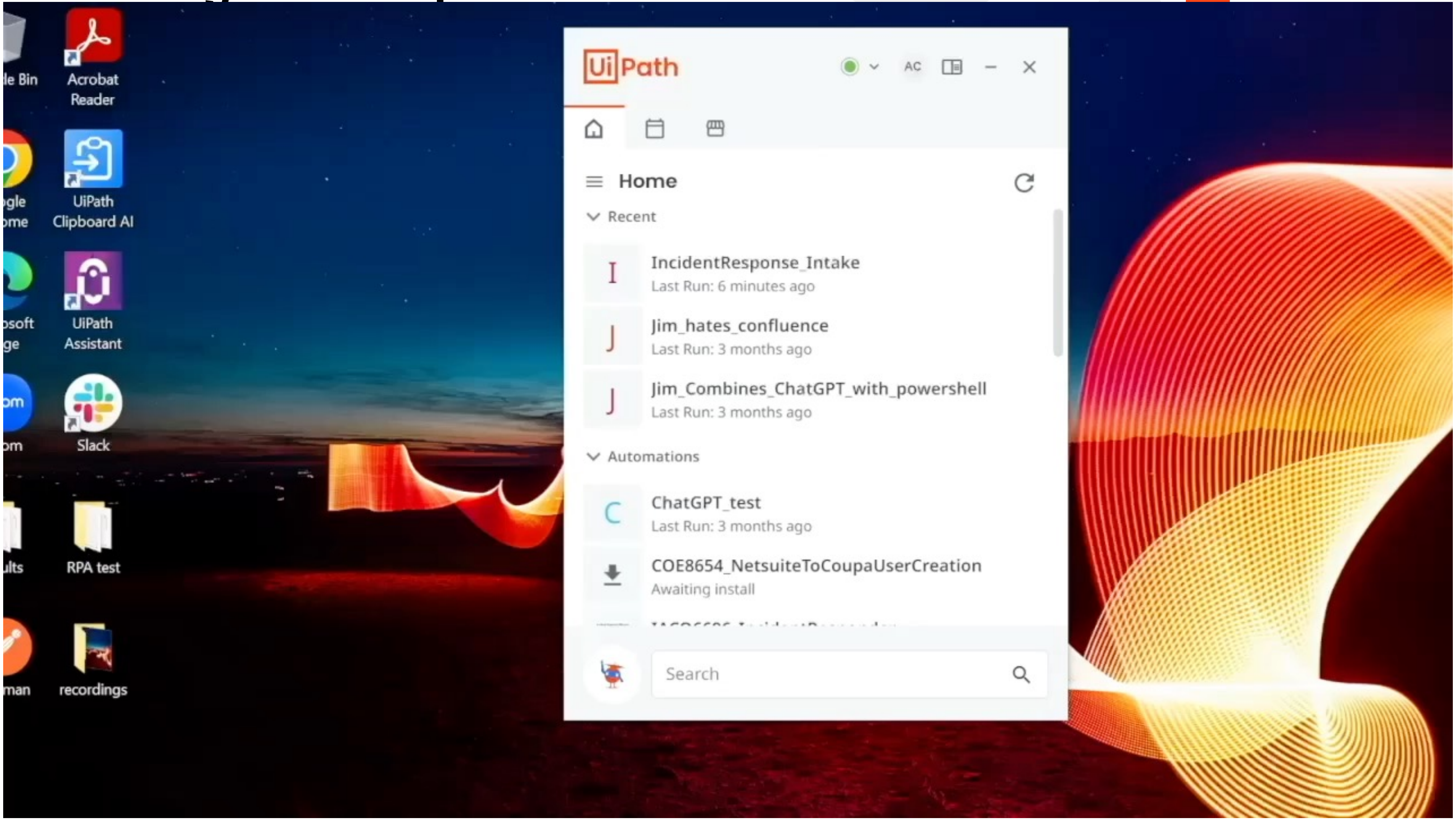
Incident Management



Incident Confirmation RPA (unattended)



Incident Management – quick PoC



Home

Recent

IncidentResponse_Intake
Last Run: 6 minutes ago

Jim_hates_confluence
Last Run: 3 months ago

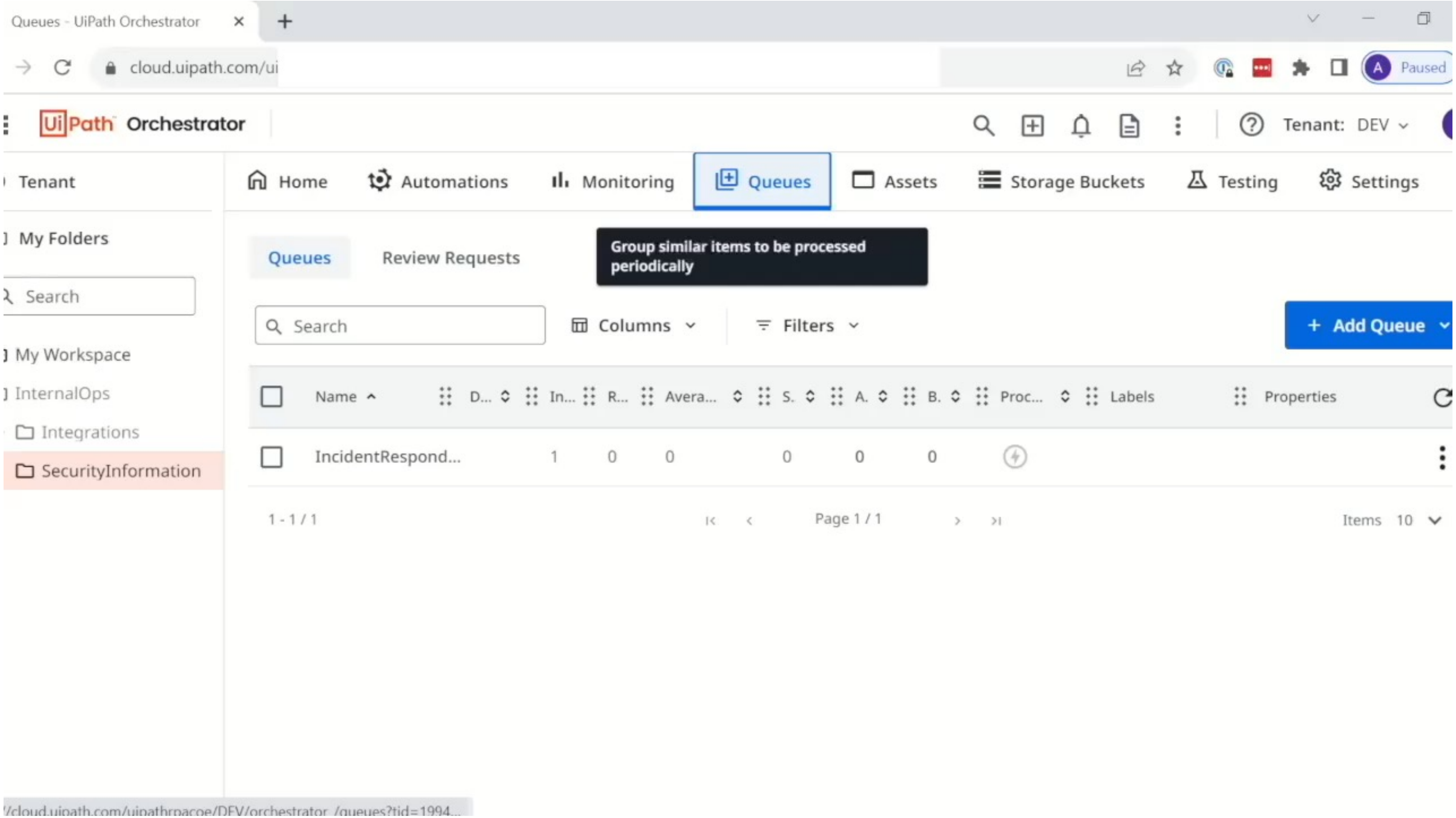
Jim_Combines_ChatGPT_with_powershell
Last Run: 3 months ago

Automations

ChatGPT_test
Last Run: 3 months ago

COE8654_NetsuiteToCoupaUserCreation
Awaiting install

Incident Tracking – automation tips and tricks



Group similar items to be processed periodically

	Name	D...	In...	R...	Avera...	S.	A.	B.	Proc...	Labels	Properties
□	IncidentRespond...		1	0	0	0	0	0			

1 - 1 / 1 Page 1 / 1 Items 10

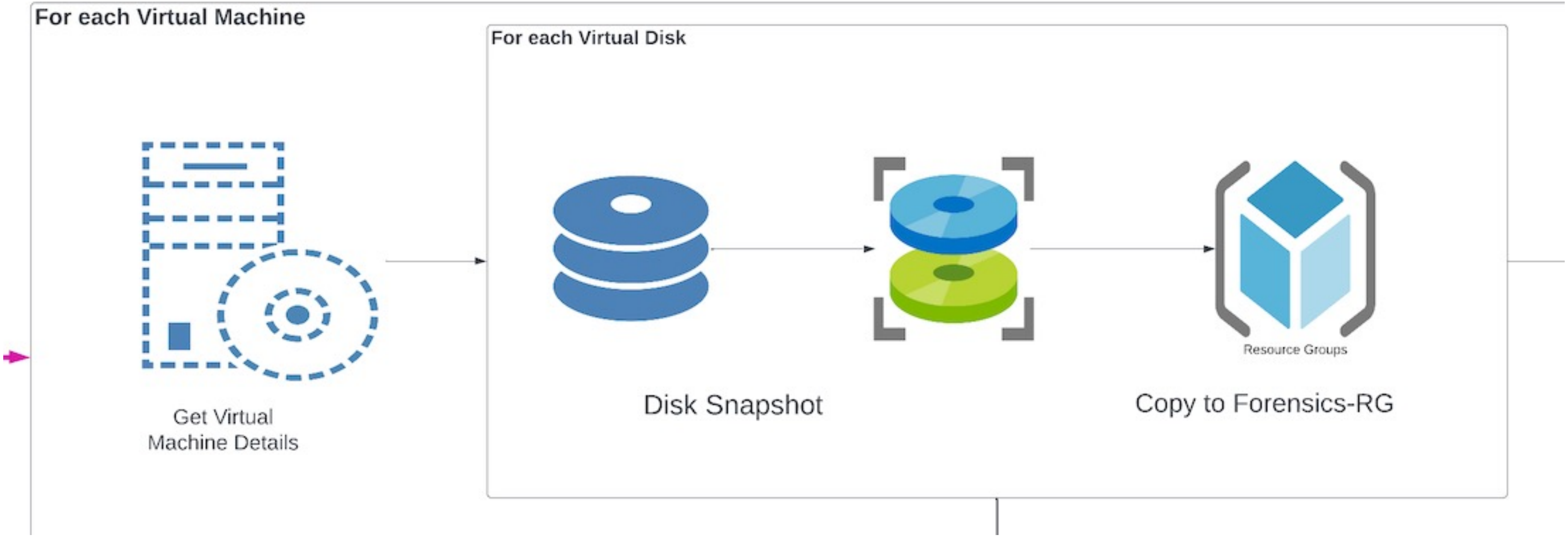
/cloud.uipath.com/uipathrpacoe/DEV/orchestrator_/queues?tid=1994...

The Cloud Forensic *DO NOT FORGET!*s

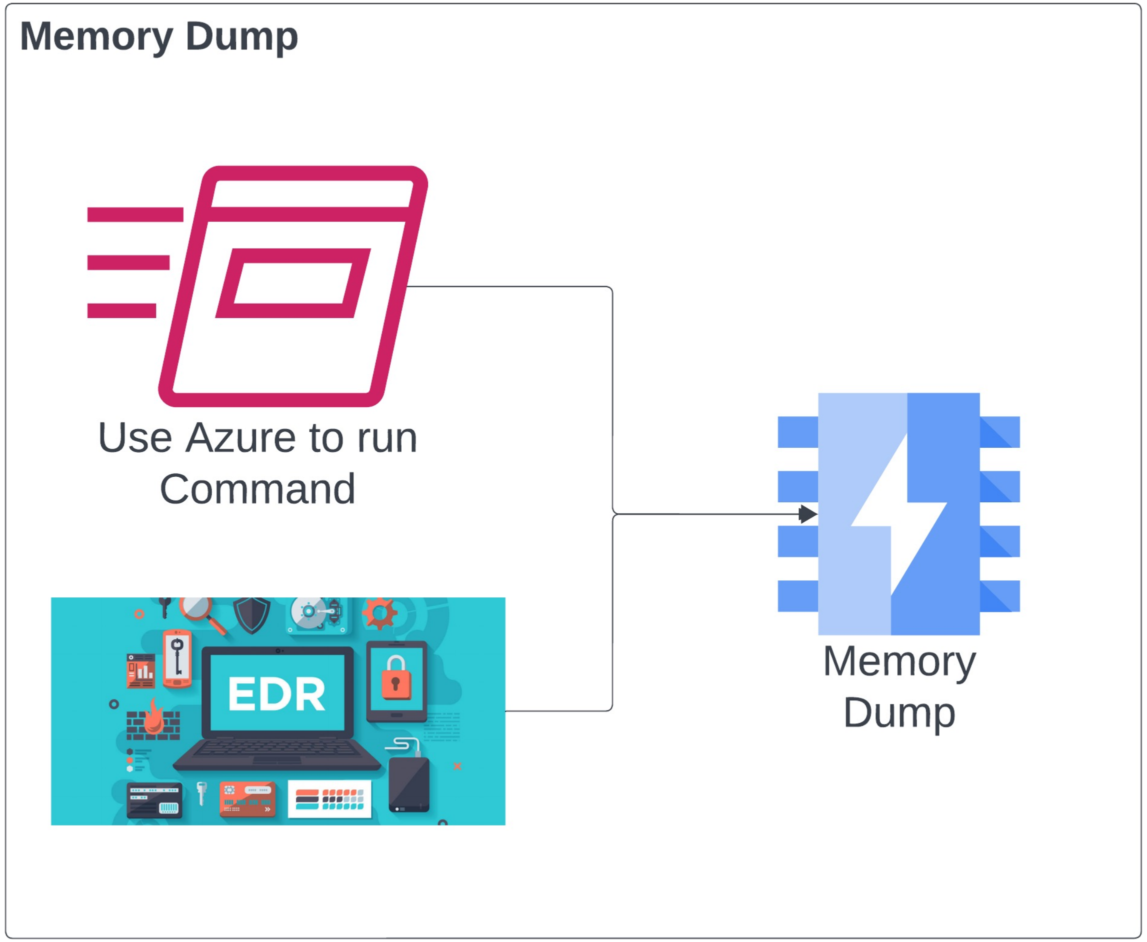
1. Snapshot
2. Memory dump
3. Snapshot

(yes, I said SNAPSHOT twice. Read the POSTER!)

Azure Snapshots



Memory Dump… in the world of cloud



Memory dump tools:
1. Windows – winpmem
2. Linux – avml

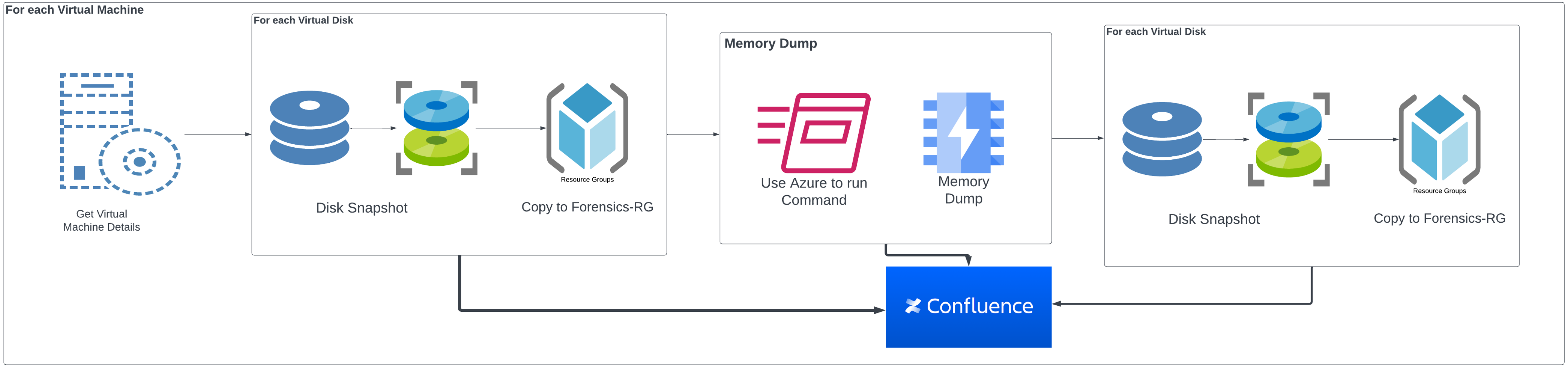
Dump Location:
1. Local disk
2. Will be acquired with secondary snapshot

Quick and Dirty memory dump

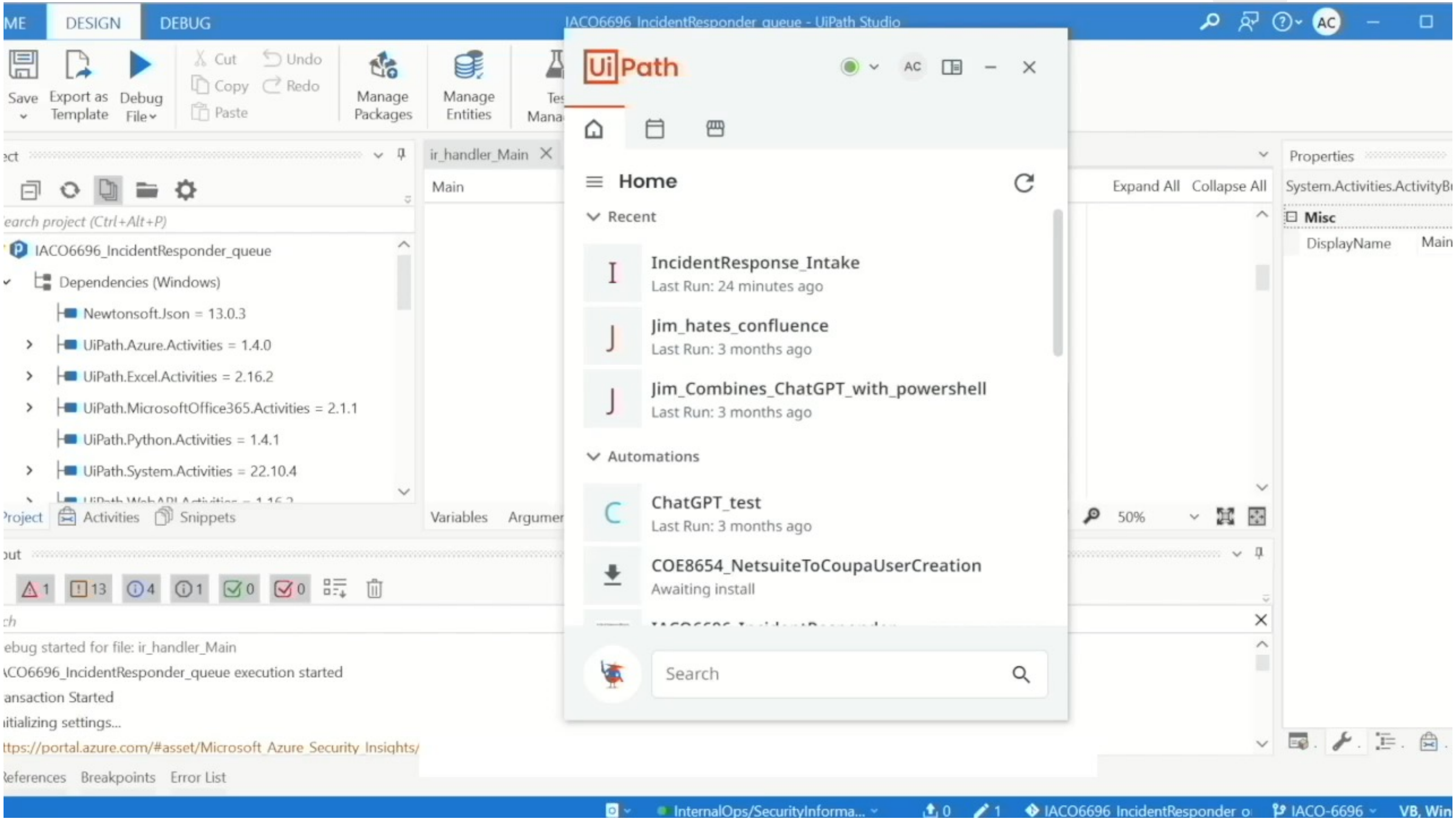
```
"cd /root; wget https://github.com/microsoft/avml/releases/download/v0.2.0/avml; chmod +x avml;output=$(./avml --compress output.lime.compressed);echo $output;"
```

```
"New-item –itemtype directory –path 'C:\memdump';Invoke-WebRequest -Uri 'https://github.com/Velocidex/WinPmem/releases/download/v4.0.rc1/winpmem_mini_x64_rc2.exe' -OutFile 'C:\memdump\winpmem_mini_x64_rc2.exe';Start-Sleep -s 5;cd C:\memdump\;C:\memdump\winpmem_mini_x64_rc2.exe C:\memdump\memory_dump.raw"
```

Incident Handling
Evidence Acquisition and Forensics



Forensics Acquisition PoC



IACO6696_IncidentResponder_queue - UiPath Studio

Home

Recent

IncidentResponse_Intake
Last Run: 24 minutes ago

Jim_hates_confluence
Last Run: 3 months ago

Jim_Combines_ChatGPT_with_powershell
Last Run: 3 months ago

Automations

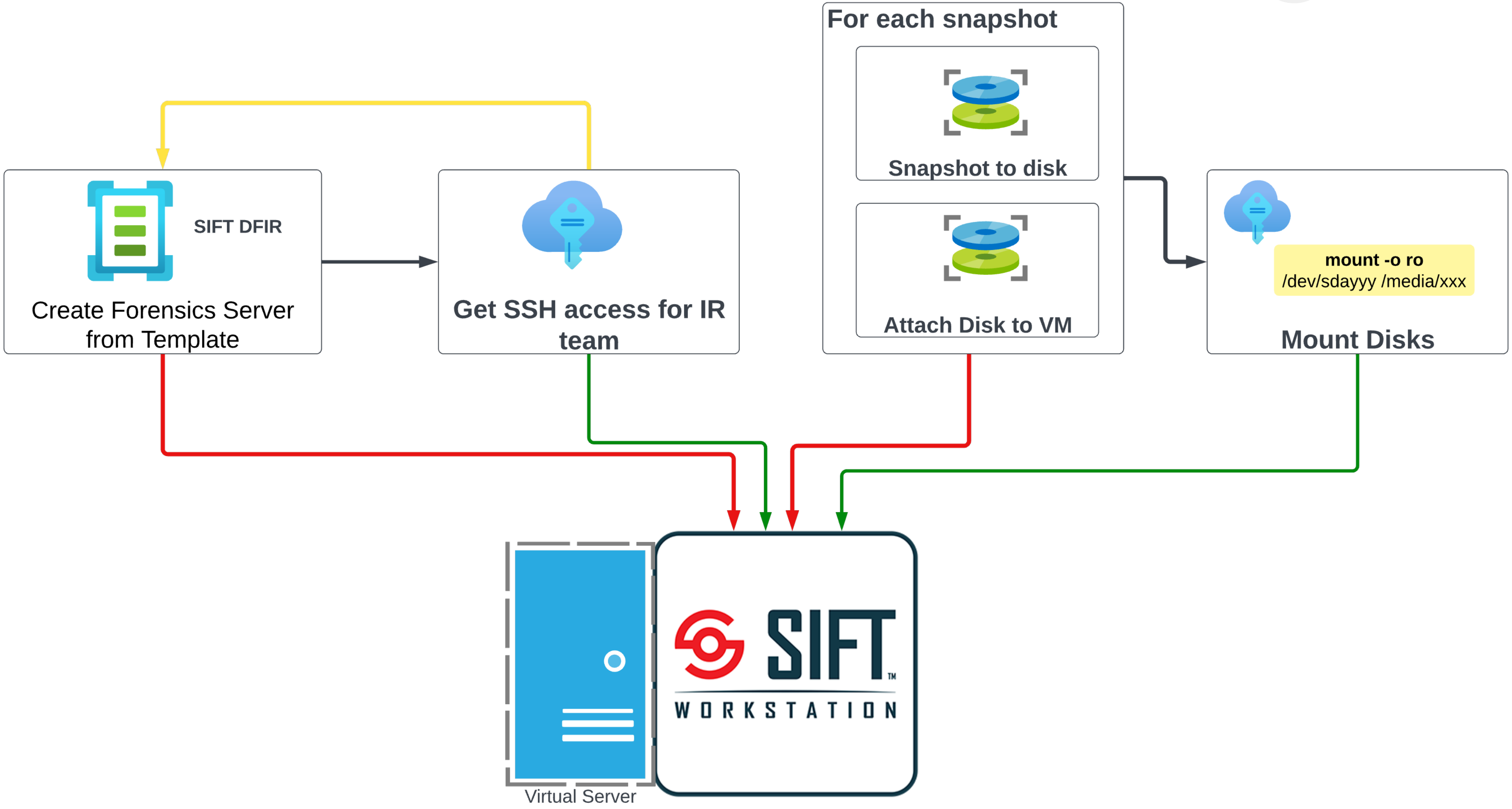
ChatGPT_test
Last Run: 3 months ago

COE8654_NetsuiteToCoupaUserCreation
Awaiting install

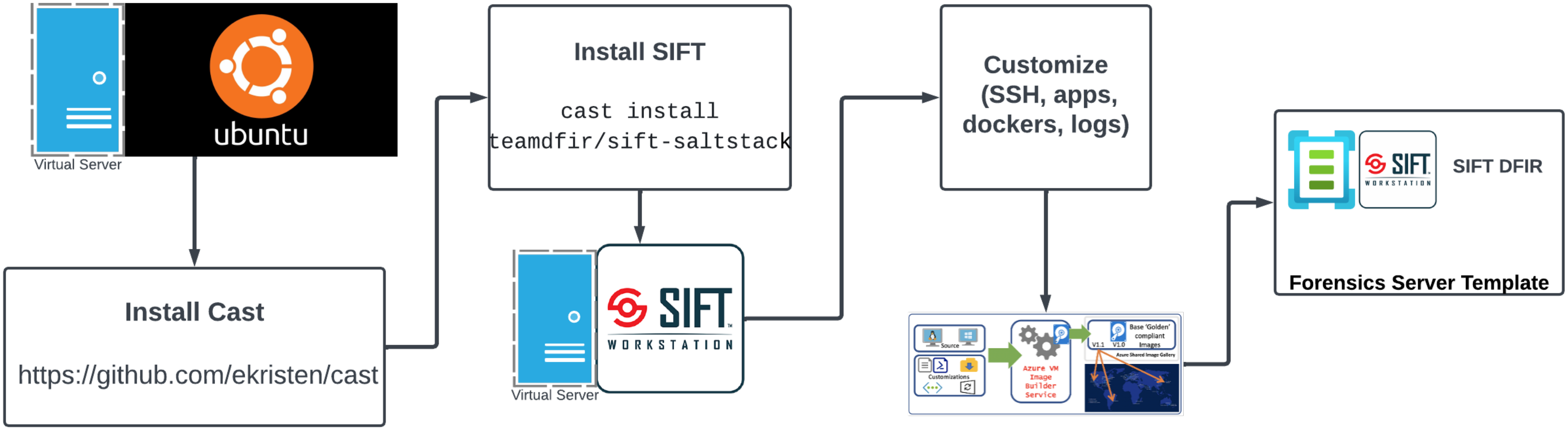
IACO6696_IncidentResponder_queue
Dependencies (Windows)
Newtonsoft.Json = 13.0.3
UiPath.Azure.Activities = 1.4.0
UiPath.Excel.Activities = 2.16.2
UiPath.MicrosoftOffice365.Activities = 2.1.1
UiPath.Python.Activities = 1.4.1
UiPath.System.Activities = 22.10.4

ebug started for file: ir_handler_Main
\CO6696_IncidentResponder_queue execution started
ansaction Started
iitializing settings...
ttps://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/

On the fly Forensics Environment!



Forensic Server (template) to the rescue



Install Cast

https://github.com/ekristen/cast

Install SIFT

```
cast install
teamdfir/sift-saltstack
```

Customize (SSH, apps, dockers, logs)

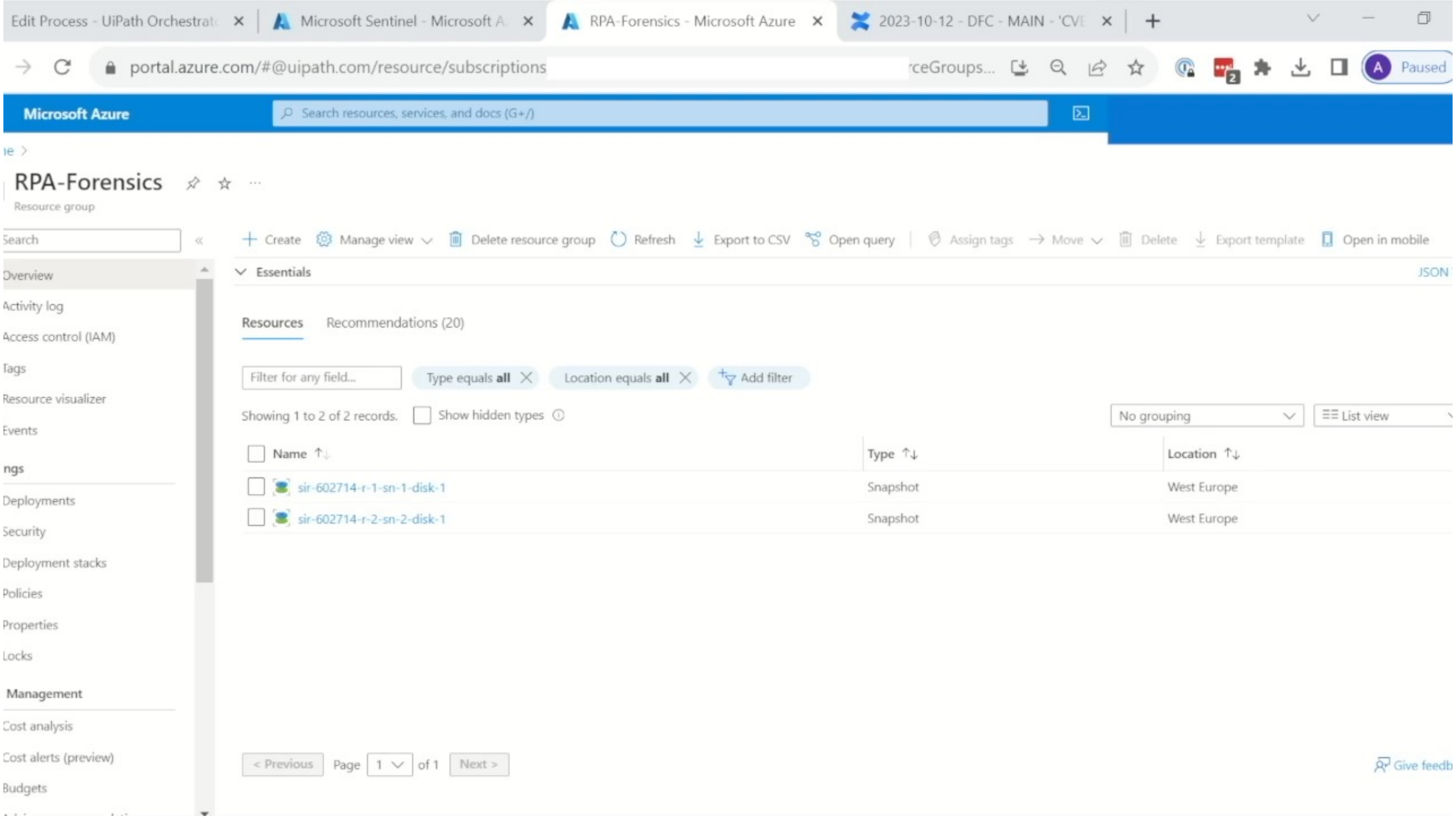
SIFT DFIR

Forensics Server Template

Forensics Lab PoC

1. Create forensics VM

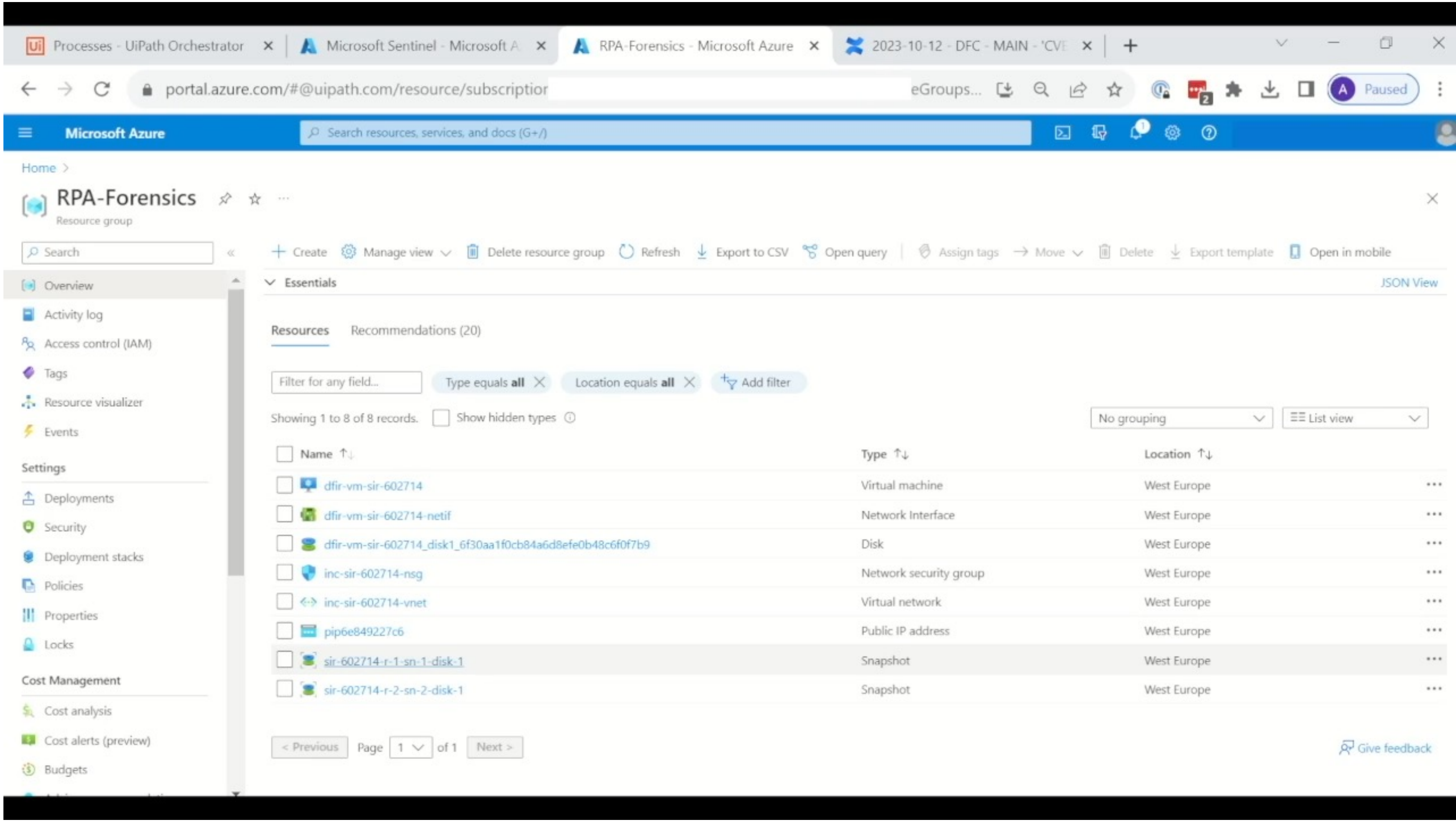
The Foundation of Innovation™



Name	Type	Location
sir-602714-r-1-sn-1-disk-1	Snapshot	West Europe
sir-602714-r-2-sn-2-disk-1	Snapshot	West Europe

Forensics Lab PoC

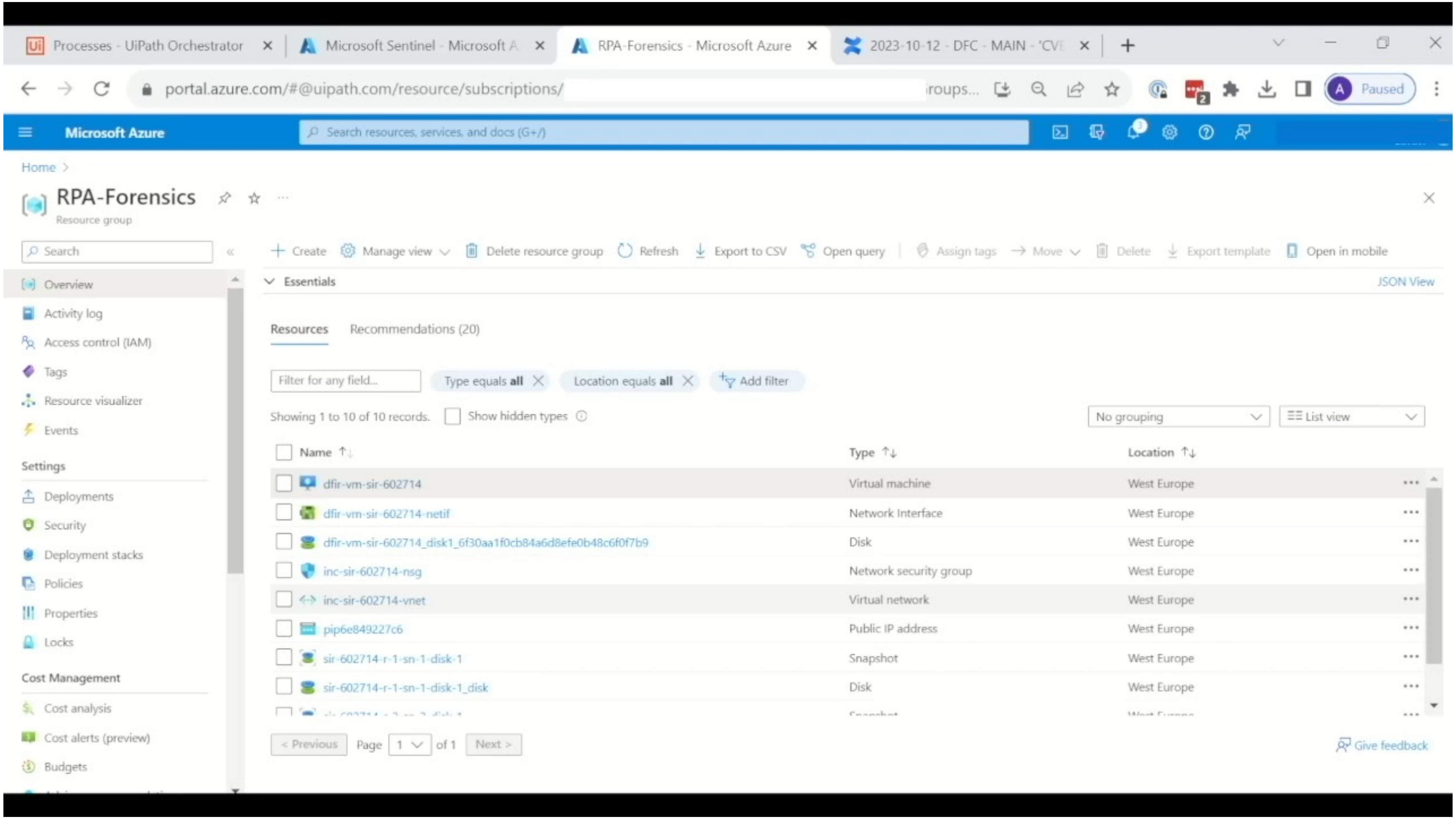
2. Snapshot to disk



Name	Type	Location
dfir-vm-sir-602714	Virtual machine	West Europe
dfir-vm-sir-602714-netif	Network Interface	West Europe
dfir-vm-sir-602714_disk1_6f30aa1f0cb84a6d8efe0b48c6f0f7b9	Disk	West Europe
inc-sir-602714-nsg	Network security group	West Europe
inc-sir-602714-vnet	Virtual network	West Europe
pip6e849227c6	Public IP address	West Europe
sir-602714-r-1-sn-1-disk-1	Snapshot	West Europe
sir-602714-r-2-sn-2-disk-1	Snapshot	West Europe

Forensics Lab PoC

3. Attach disk to VM



portal.azure.com/#@uipath.com/resource/subscriptions/ roups...

RPA-Forensics
Resource group

Type equals **all**   Location equals **all**

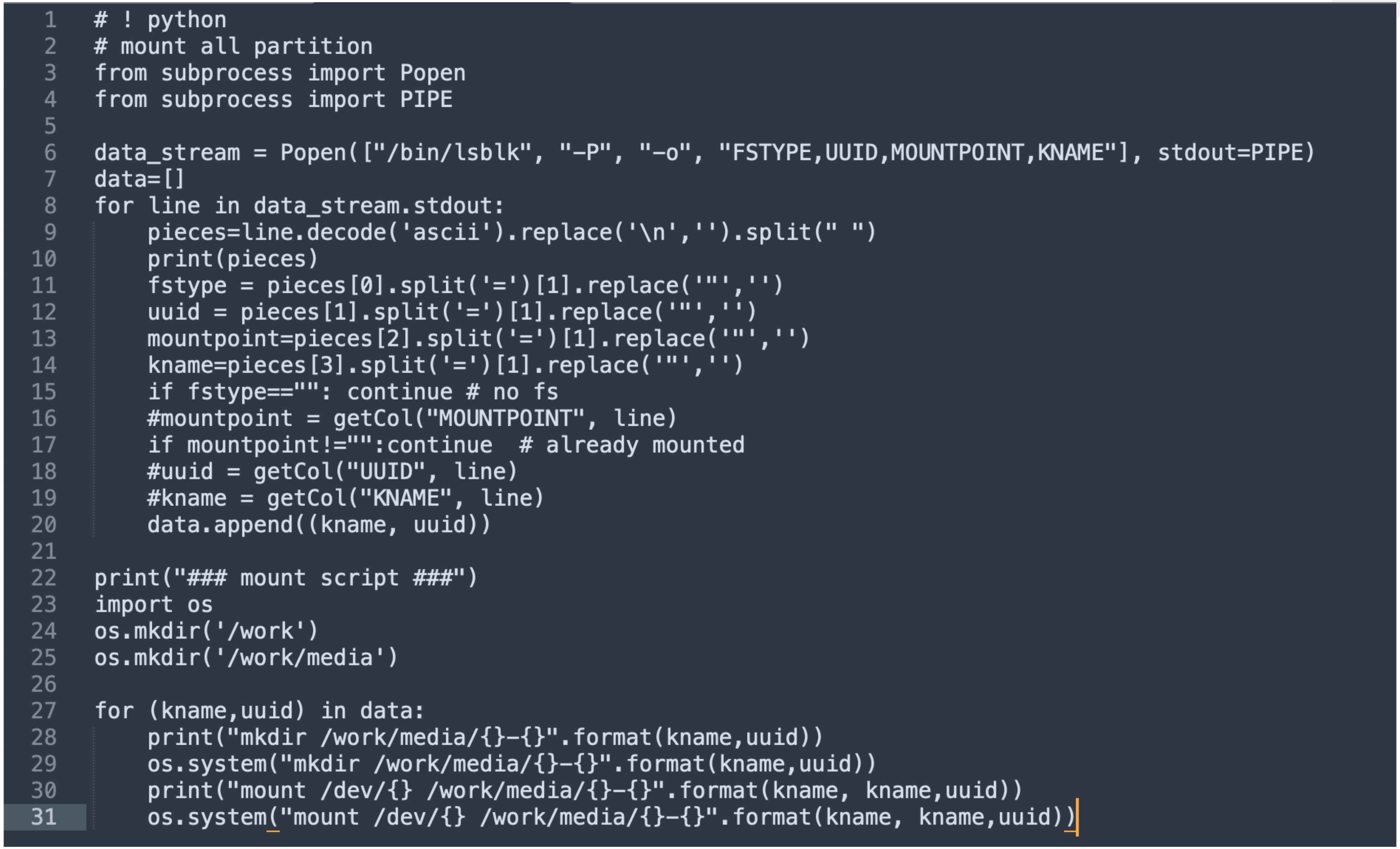
Showing 1 to 10 of 10 records. □ Show hidden types

No grouping   List view

Name	Type	Location
dfir-vm-sir-602714	Virtual machine	West Europe
dfir-vm-sir-602714-netif	Network Interface	West Europe
dfir-vm-sir-602714_disk1_6f30aa1f0cb84a6d8efe0b48c6f0f7b9	Disk	West Europe
inc-sir-602714-nsg	Network security group	West Europe
inc-sir-602714-vnet	Virtual network	West Europe
pip6e849227c6	Public IP address	West Europe
sir-602714-r-1-sn-1-disk-1	Snapshot	West Europe
sir-602714-r-1-sn-1-disk-1_disk	Disk	West Europe

< Previous   Page 1 of 1   Next >

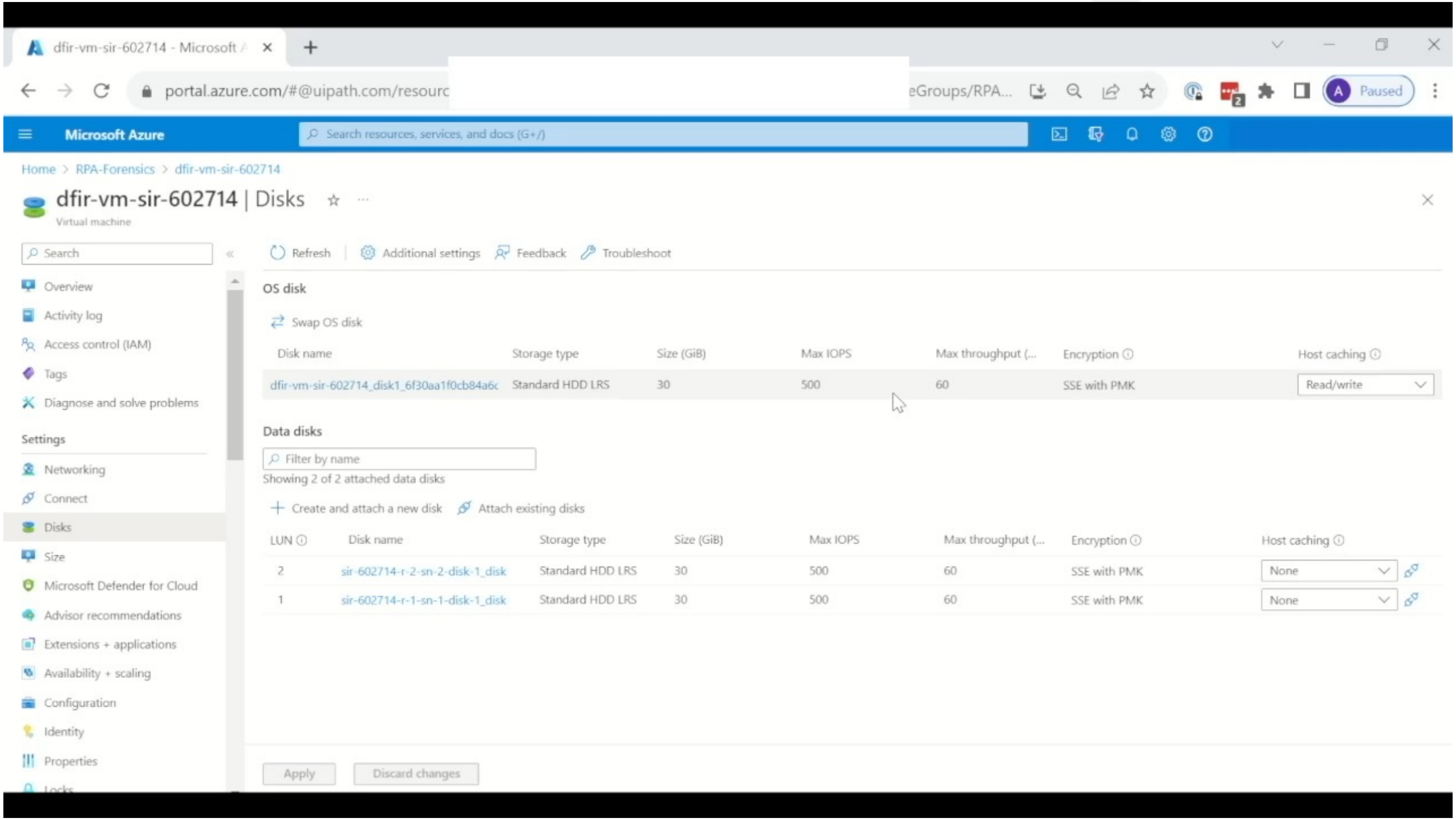
Quick and dirty volume mount



```python
# ! python
# mount all partition
from subprocess import Popen
from subprocess import PIPE

data_stream = Popen(["/bin/lsblk", "-P", "-o", "FSTYPE,UUID,MOUNTPOINT,KNAME"], stdout=PIPE)
data=[]
for line in data_stream.stdout:
    pieces=line.decode('ascii').replace('\n','').split(" ")
    print(pieces)
    fstype = pieces[0].split('=')[1].replace('"','')
    uuid = pieces[1].split('=')[1].replace('"','')
    mountpoint=pieces[2].split('=')[1].replace('"','')
    kname=pieces[3].split('=')[1].replace('"','')
    if fstype=="": continue # no fs
    #mountpoint = getCol("MOUNTPOINT", line)
    if mountpoint!="":continue  # already mounted
    #uuid = getCol("UUID", line)
    #kname = getCol("KNAME", line)
    data.append((kname, uuid))

print("### mount script ###")
import os
os.mkdir('/work')
os.mkdir('/work/media')

for (kname,uuid) in data:
    print("mkdir /work/media/{}-{}".format(kname,uuid))
    os.system("mkdir /work/media/{}-{}".format(kname,uuid))
    print("mount /dev/{} /work/media/{}-{}".format(kname, kname,uuid))
    os.system("mount /dev/{} /work/media/{}-{}".format(kname, kname,uuid))
```

Forensics Lab PoC

4. Mount volumes



dfir-vm-sir-602714 | Disks

OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ	Host caching ⓘ
dfir-vm-sir-602714_disk1_6f30aa1f0cb84a6c	Standard HDD LRS	30	500	60	SSE with PMK	Read/write

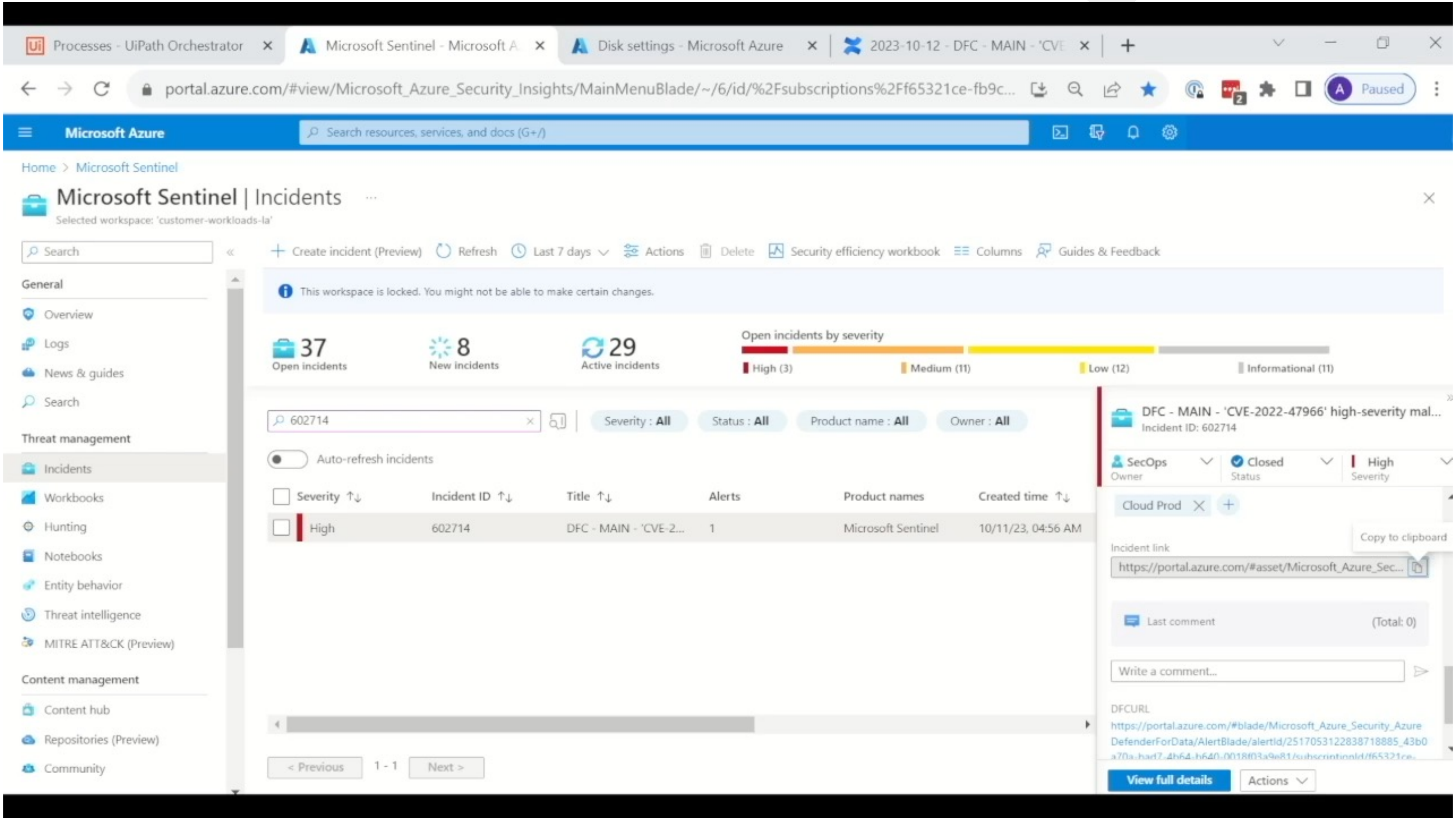
Data disks

Showing 2 of 2 attached data disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ	Host caching ⓘ
2	sir-602714-r-2-sn-2-disk-1_disk	Standard HDD LRS	30	500	60	SSE with PMK	None
1	sir-602714-r-1-sn-1-disk-1_disk	Standard HDD LRS	30	500	60	SSE with PMK	None

Forensics Lab PoC

5. check volumes via ssh



portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/6/id/%2Fsubscriptions%2Ff65321ce-fb9c...

Microsoft Sentinel | Incidents

Selected workspace: 'customer-workloads-la'

This workspace is locked. You might not be able to make certain changes.

37 Open incidents

8 New incidents

29 Active incidents

Open incidents by severity: High (3) Medium (11) Low (12) Informational (11)

Search: 602714

Severity	Incident ID	Title	Alerts	Product names	Created time
High	602714	DFC - MAIN - 'CVE-2...	1	Microsoft Sentinel	10/11/23, 04:56 AM

DFC - MAIN - 'CVE-2022-47966' high-severity mal...
Incident ID: 602714

Owner: SecOps
Status: Closed
Severity: High

Cloud Prod

Incident link: https://portal.azure.com/#asset/Microsoft_Azure_Sec...

Last comment (Total: 0)

Write a comment...

DFCURL
https://portal.azure.com/#blade/Microsoft_Azure_Security_Azure DefenderForData/AlertBlade/alertId/2517053122838718885_43b0a70a-bad7-4b64-b640-0018f03a9e81/subscriptionId/f65321ce-

Automating Forensics Activities via RPA

- Automate processes like:
  1. Disk timeline: Plaso – Log2TimeLine

  2. Memory Analysis:
     1. Volatility common commands: Network, processes, profile, cmds,
     2. Dump processes, handles, files from memory
     3. Memory elements timeline

  3. Automatic confluence Incident Timeline Update

Where to next

Conquering all clouds

In our case Memory dumps on **AWS** will depend on the EDR service we have present there.

And some of the logic of the forensics acquistion process will need minor updates.

Making flexible templates accessible to all clients

We are building a framework, something that can be easily imported and easily updated for ones needs. The beauty of RPA

Constant improvment and development of Forensics activities

This will be a never ending story. There are always new things you learned and things that ca be improved.

Empowering the Human

Conclusions

Incident Management is a necessary evil

- If it’s not writen, it never happened. If it never happened, we never learn

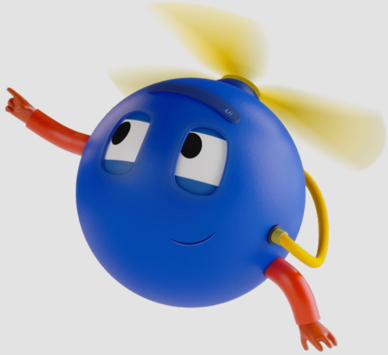
Work smarter, not more!

- You need to make you job a fun!
- You do that by automating stuff, so you can focus on what you love!

Make everything as repeatable and as less human dependable as possible

- We are prone to errors. Robot are not. They are just prone to failures

Q & A



UiPath The Foundation of Innovation™