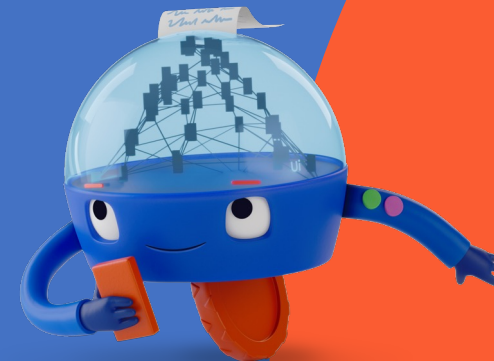


# Using **RPA** for a fast, reliable and repeatable **Incident Response** process

(or for whatever you want...)



# whoami

**UiPath**

**Security**

**Operations / Incident  
Response**

**Team**

**Andrei  
Cotaie**

**Principal  
Security  
Engineer**

**Cristian  
Miron**

**Senior  
Security  
Engineer**

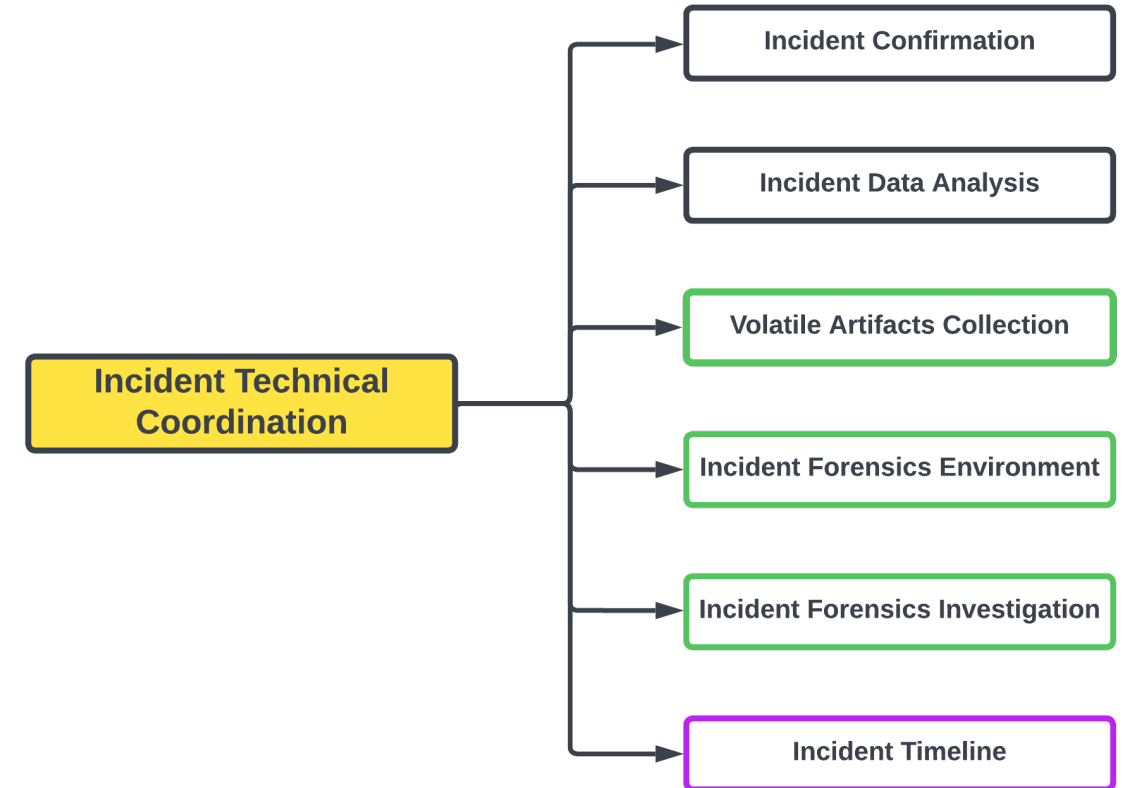
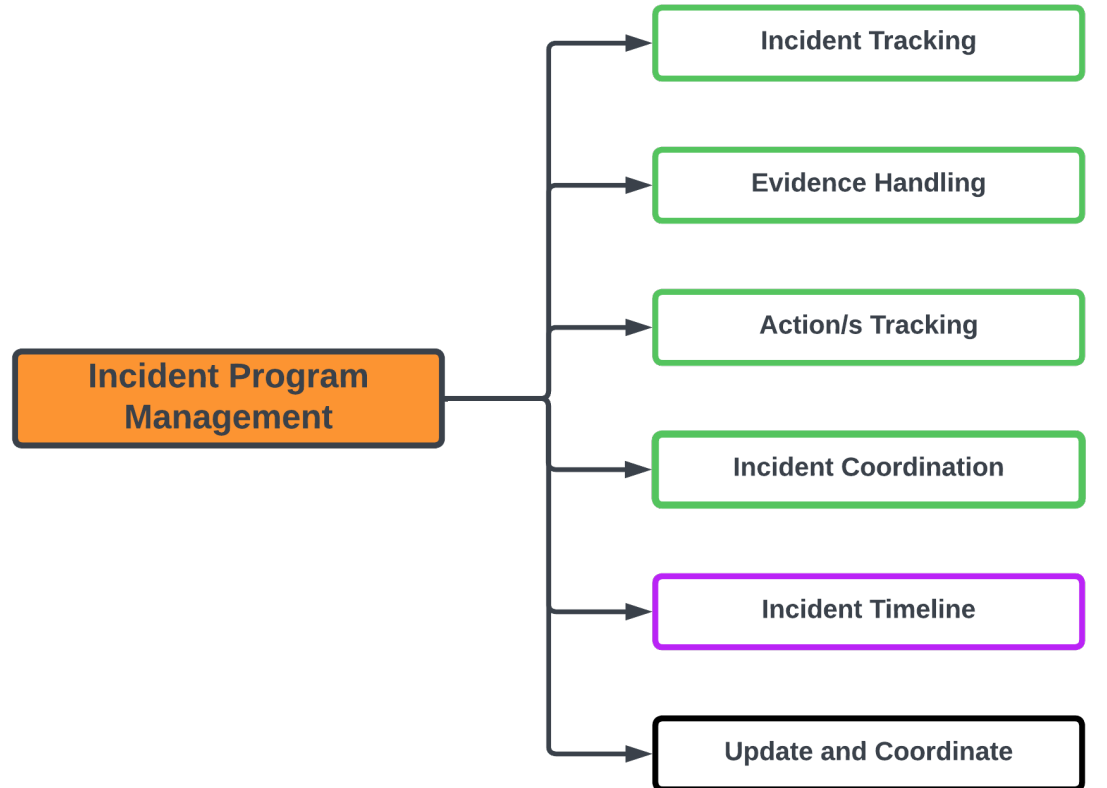
# What is Incident Response?

- 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

## Incident Response Lifecycle



# IR: Moment Zero



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**

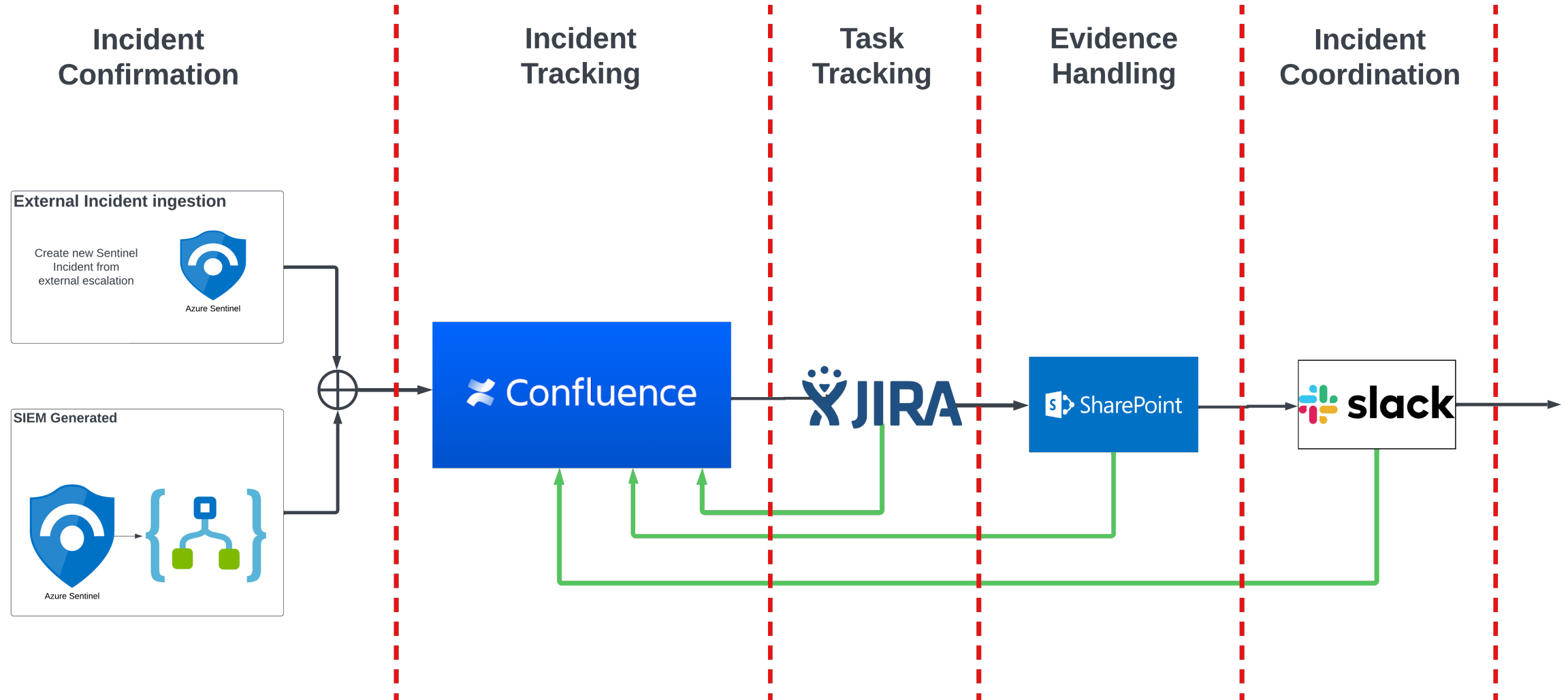
## **Attended**

- 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.

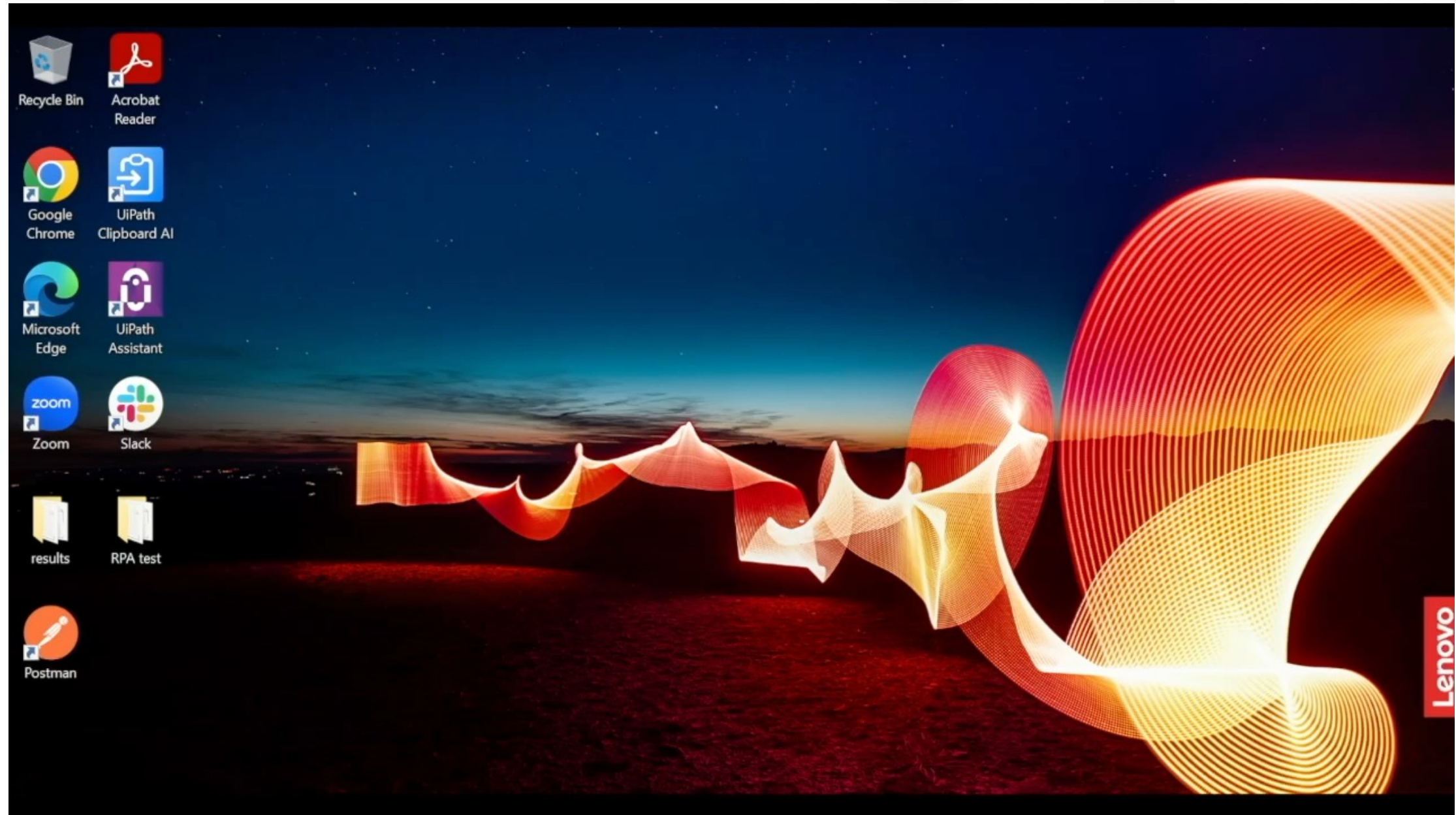
## **Unattended**

- 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

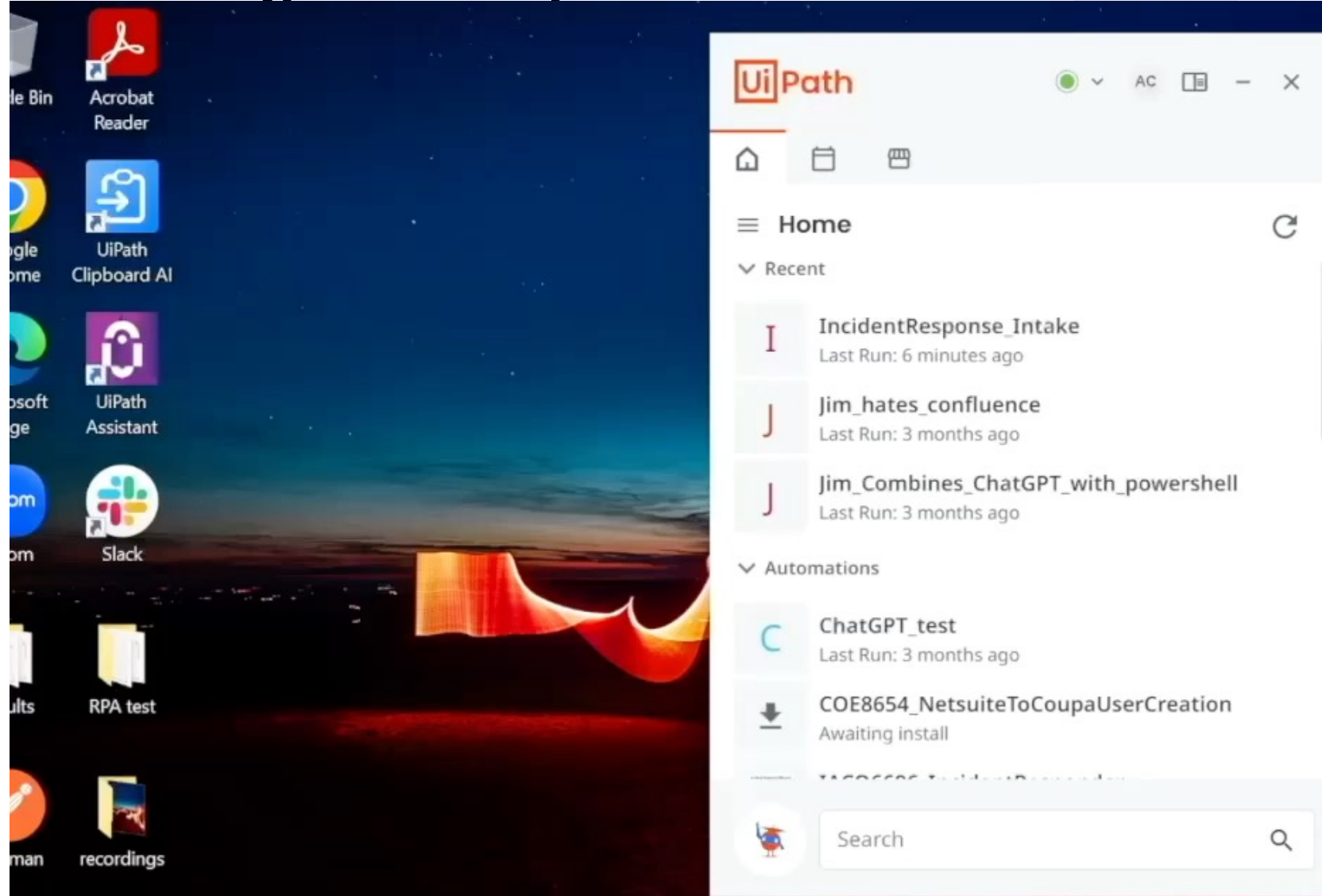


# Incident Confirmation RPA (unattended)





# Incident Management – quick PoC



# Incident Tracking – automation tips and tricks

Queues - UiPath Orchestrator

cloud.uipath.com/ui

UiPath Orchestrator

Tenant: DEV

Home Automations Monitoring **Queues** Assets Storage Buckets Testing Settings

Queues Review Requests

Group similar items to be processed periodically

Search Columns Filters + Add Queue

<input type="checkbox"/>	Name ^	D...	In...	R...	Avera...	S.	A.	B.	Proc...	Labels	Properties
<input type="checkbox"/>	IncidentRespond...	1	0	0	0	0	0	0			

1 - 1 / 1 Page 1 / 1 Items 10

/cloud.uipath.com/uipathrocoe/DEV/orchestrator/queues?tid=1994...

# The Cloud Forensic **DO NOT FORGET!**s



1. Snapshot

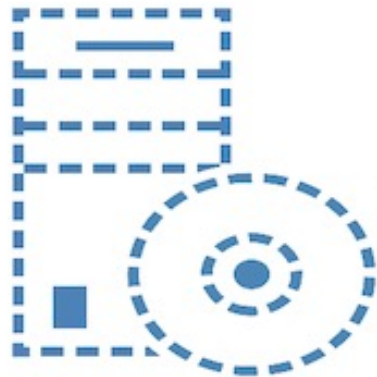
2. Memory dump

3. Snapshot

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

# Azure Snapshots

For each Virtual Machine

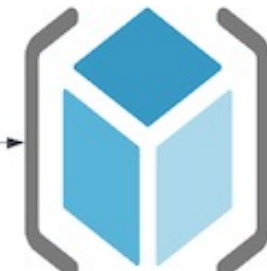
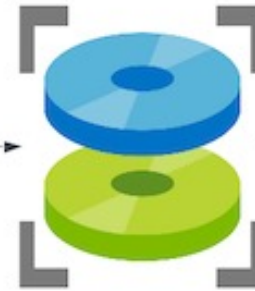


Get Virtual  
Machine Details

For each Virtual Disk



Disk Snapshot



Resource Groups

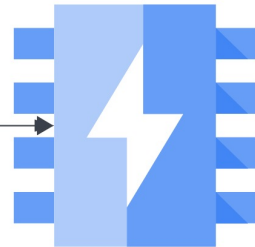
Copy to Forensics-RG

# Memory Dump... in the world of cloud

## Memory Dump



Use Azure to run  
Command



Memory  
Dump

## 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

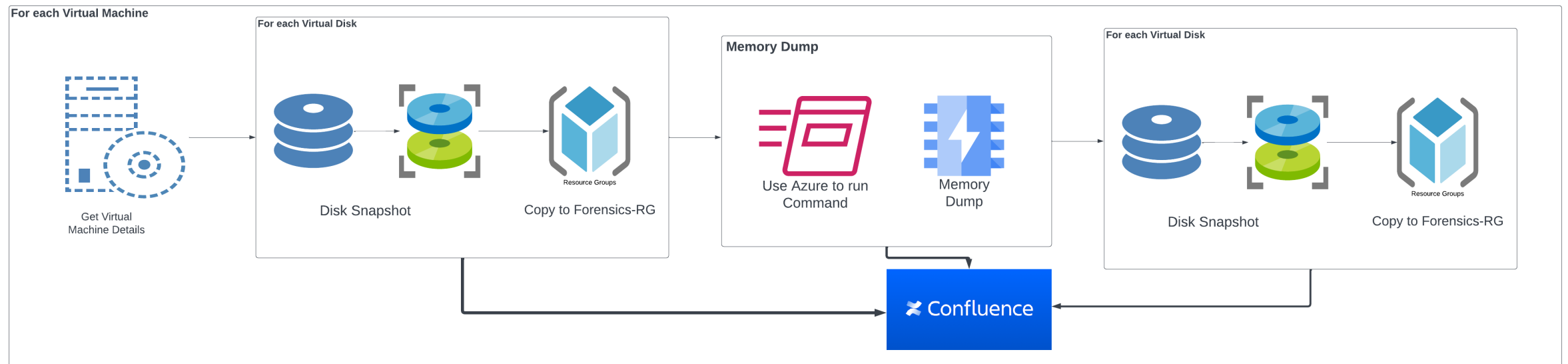
```
"cd /root; wget  
https://github.com/microsoft/avml  
/releases/download/v0.2.0/avml;  
chmod +x avml; output=$(./avml -  
-compress  
output.lime.compressed); echo  
$output;"
```

```
"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

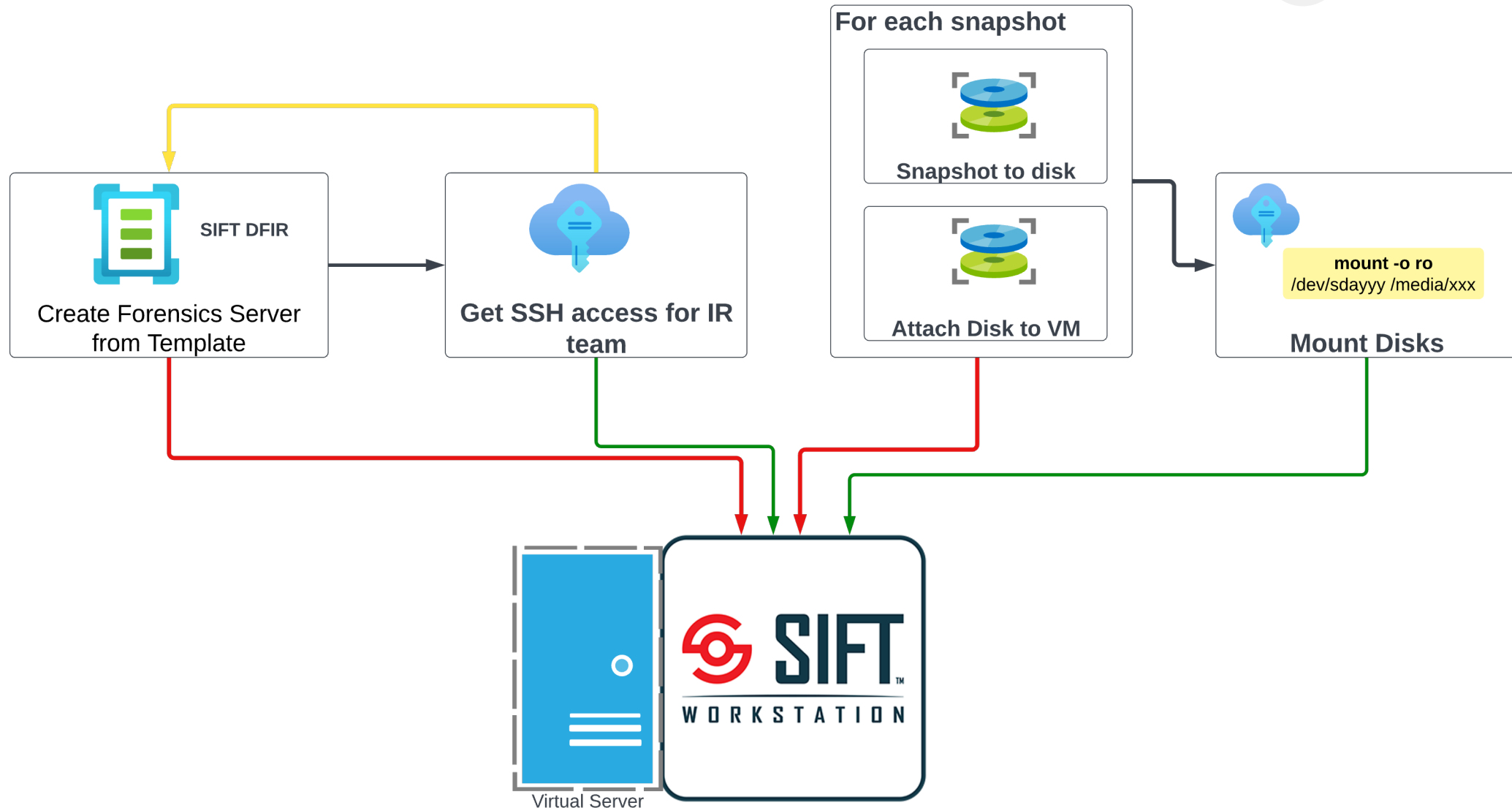


# Forensics Acquisition PoC

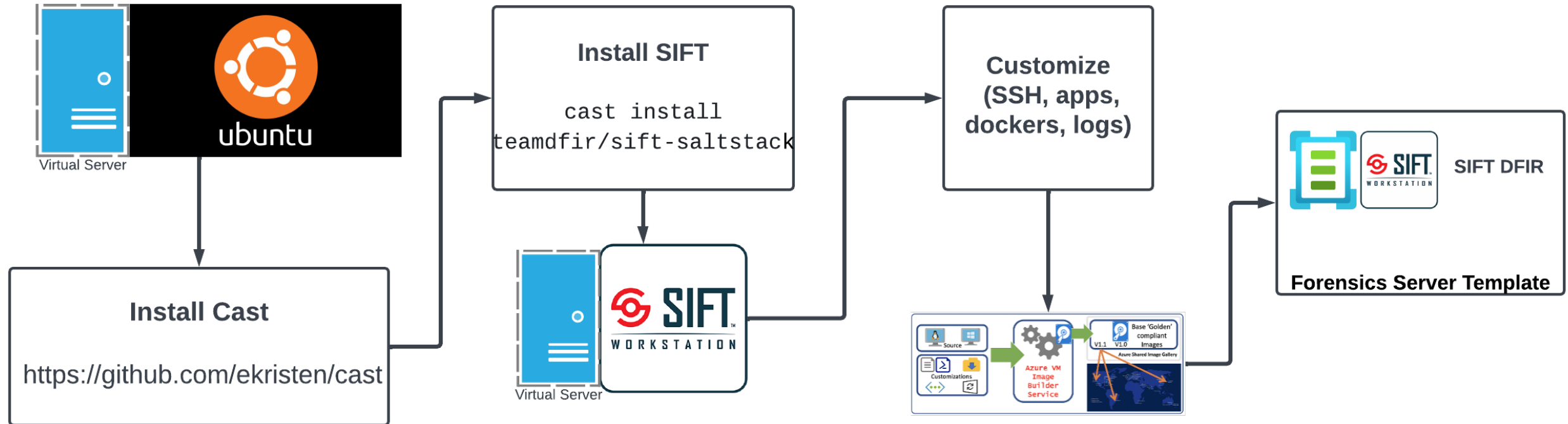
The screenshot displays the UiPath Studio environment. The main workspace shows a project named 'IACO6696\_IncidentResponder\_queue' with a dependency tree including packages like 'Newtonsoft.Json', 'UiPath.Azure.Activities', 'UiPath.Excel.Activities', 'UiPath.MicrosoftOffice365.Activities', 'UiPath.Python.Activities', 'UiPath.System.Activities', and 'UiPath.WebAPI.Activities'. The 'Properties' pane on the right shows the 'Misc' section with 'DisplayName' set to 'Main'. The 'Output' pane at the bottom shows the execution log for the 'ir\_handler\_Main' file, indicating that the 'IACO6696\_IncidentResponder\_queue' execution started and is initializing settings. A 'UiPath' window is overlaid in the center, displaying a 'Home' view with a 'Recent' section listing three automations: 'IncidentResponse\_Intake' (Last Run: 24 minutes ago), 'Jim\_hates\_confluence' (Last Run: 3 months ago), and 'Jim\_Combines\_ChatGPT\_with\_powershell' (Last Run: 3 months ago). The 'Automations' section lists 'ChatGPT\_test' (Last Run: 3 months ago) and 'COE8654\_NetsuiteToCoupaUserCreation' (Awaiting install). A search bar is visible at the bottom of the 'UiPath' window.



# On the fly Forensics Environment!



# Forensic Server (template) to the rescue



# Forensics Lab PoC

## 1. Create forensics VM

The screenshot shows the Microsoft Azure portal interface. The browser tabs at the top include 'Edit Process - UiPath Orchestrator', 'Microsoft Sentinel - Microsoft A...', 'RPA-Forensics - Microsoft Azure', and '2023-10-12 - DFC - MAIN - 'CVE''. The address bar shows 'portal.azure.com/#@uipath.com/resource/subscriptions'. The main header is 'Microsoft Azure' with a search bar. The left sidebar shows the navigation menu with 'RPA-Forensics' selected. The main content area shows the 'Essentials' view for the 'RPA-Forensics' resource group. It includes a 'Resources' tab and a table of resources. The table has columns for 'Name', 'Type', and 'Location'. Two resources are listed: 'sir-602714-r-1-sn-1-disk-1' and 'sir-602714-r-2-sn-2-disk-1', both of type 'Snapshot' and located in 'West Europe'. The page also shows a 'Filter for any field...' input, filter buttons for 'Type equals all' and 'Location equals all', and a 'Show hidden types' checkbox. The bottom of the page shows pagination: '< Previous', 'Page 1 of 1', and 'Next >'. A 'Give feedback' link is in the bottom right corner.

Search resources, services, and docs (G+/f)

RPA-Forensics

Resource group

Search

« + Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

ngs

Deployments

Security

Deployment stacks

Policies

Properties

Locks

Management

Cost analysis

Cost alerts (preview)

Budgets

Essentials

Resources Recommendations (20)

Filter for any field...

Type equals all

Location equals all

Add filter

Showing 1 to 2 of 2 records. Show hidden types

No grouping

List view

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

< Previous Page 1 of 1 Next >

Give feedback

# Forensics Lab PoC

## 2. Snapshot to disk

The screenshot shows the Microsoft Azure portal interface for the 'RPA-Forensics' resource group. The 'Resources' tab is selected, showing a list of 8 resources. The resource 'sir-602714-r-1-sn-1-disk-1' is highlighted, indicating it is a Snapshot located in West Europe.

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
<b>sir-602714-r-1-sn-1-disk-1</b>	<b>Snapshot</b>	<b>West Europe</b>
sir-602714-r-2-sn-2-disk-1	Snapshot	West Europe

# Forensics Lab PoC

## 3. Attach disk to VM

The screenshot shows the Microsoft Azure portal interface for the 'RPA-Forensics' resource group. The 'Resources' tab is selected, showing a list of 10 resources. The first resource is 'dfir-vm-sir-602714', a Virtual machine located in West Europe. The interface includes a left sidebar with navigation options like Overview, Activity log, and Settings, and a top navigation bar with search and action buttons.

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
...	...	...

# Quick and dirty volume mount

```
1  # ! python
2  # mount all partition
3  from subprocess import Popen
4  from subprocess import PIPE
5
6  data_stream = Popen(["/bin/lsblk", "-P", "-o", "FSTYPE,UUID,MOUNTPOINT,KNAME"], stdout=PIPE)
7  data=[]
8  for line in data_stream.stdout:
9      pieces=line.decode('ascii').replace('\n','').split(" ")
10     print(pieces)
11     fstype = pieces[0].split('=')[1].replace('"','')
12     uuid = pieces[1].split('=')[1].replace('"','')
13     mountpoint=pieces[2].split('=')[1].replace('"','')
14     kname=pieces[3].split('=')[1].replace('"','')
15     if fstype=="": continue # no fs
16     #mountpoint = getCol("MOUNTPOINT", line)
17     if mountpoint!="":continue # already mounted
18     #uuid = getCol("UUID", line)
19     #kname = getCol("KNAME", line)
20     data.append((kname, uuid))
21
22  print("### mount script ###")
23  import os
24  os.mkdir('/work')
25  os.mkdir('/work/media')
26
27  for (kname,uuid) in data:
28      print("mkdir /work/media/{0}-{1}".format(kname,uuid))
29      os.system("mkdir /work/media/{0}-{1}".format(kname,uuid))
30      print("mount /dev/{0} /work/media/{0}-{1}".format(kname, kname,uuid))
31      os.system("mount /dev/{0} /work/media/{0}-{1}".format(kname, kname,uuid))
```

# Forensics Lab PoC

## 4. Mount volumes

dfir-vm-sir-602714 - Microsoft Azure

portal.azure.com/#@uipath.com/resourceGroups/RPA...

Microsoft Azure

Search resources, services, and docs (G+)

Home > RPA-Forensics > dfir-vm-sir-602714

dfir-vm-sir-602714 | Disks

Virtual machine

Search

Refresh Additional settings Feedback Troubleshoot

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Availability + scaling

Configuration

Identity

Properties

Locks

OS disk

Swap 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

Filter by name

Showing 2 of 2 attached data disks

Create and attach a new disk Attach existing 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

Apply Discard changes

# Forensics Lab PoC

## 5. check volumes via ssh

Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'customer-workloads-la'

Search

Create incident (Preview) Refresh Last 7 days Actions Delete Security efficiency workbook Columns Guides & Feedback

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)

602714

Severity: All Status: All Product name: All Owner: All

Auto-refresh incidents

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

SecOps Owner Closed Status High Severity

Cloud Prod

Incident link  
[https://portal.azure.com/#asset/Microsoft\\_Azure\\_Sec...](https://portal.azure.com/#asset/Microsoft_Azure_Sec...)

Last comment (Total: 0)

Write a comment...

DFCURL  
[https://portal.azure.com/#blade/Microsoft\\_Azure\\_Security\\_AzureDefenderForData/AlertBlade/alertId/2517053122838718885\\_43b0a70a-had7-4h64-h640-001803a9e81/subscripionId/65321ce...](https://portal.azure.com/#blade/Microsoft_Azure_Security_AzureDefenderForData/AlertBlade/alertId/2517053122838718885_43b0a70a-had7-4h64-h640-001803a9e81/subscripionId/65321ce...)

View full details Actions



# Automating Forensics Activities via RPA

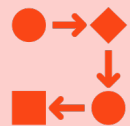
- Automate processes like:
  1. Disk timeline: Plaso – Log2TimeLine
  2. Memory Analysis:
    1. Volatility common commands: Network, processes, profile, cmds,
    2. Dump processes, handles, files from memory
    3. Memory elements timeline
  3. Automatic confluence Incident Timeline Update

# 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 acquisition 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 written, it never happened. If it never happened, we never learn

Work smarter, not more!

- You need to make your 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. Robots are not. They are just prone to failures

# Q & A

