Adversaries Also Lift & Shift

Cloud Threats Through the Eyes of an Adversary

www.mitiga.io

Roei Sherman
Field CTO | sherman@mitiga.io

NOVEMBER 2024

Nice to meet you!

Roei Sherman

Field CTO at Mitiga

Ex-Global Director, Offensive Services
AB InBev | Independent IR

B.A - Information systems and Cybersecurity
M.A - Criminology

Co-organizer of BSidesTLV
Volunteer in Trace Labs

Amateur Homebrewer

We must remember,

SaaS is Cloud.

Everyone is
Moving to the Cloud.

30,000

SaaS companies
worldwide

Companies: As of 2023, there are approximately 30,000 SaaS companies worldwide. (Spendesk)

$678.8 B

End-user spending
in 2024

Spending: Gartner forecasts that worldwide end-user spending on public cloud services will grow 20.4% to reach $678.8 billion in 2024, up from $563.6 billion in 2023

$908.21 B

Cloud market
by 2023

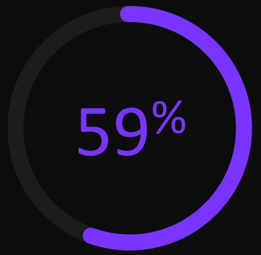
Growth: The market is projected to reach $908.21 billion by 2030, growing at a compound annual growth rate (CAGR) of 18.7% during this period (Forbes)

It’s Huge for Good Reason.

- Cost reduction
- Maintenance
- Digital transformation
- Availability
- Scalability

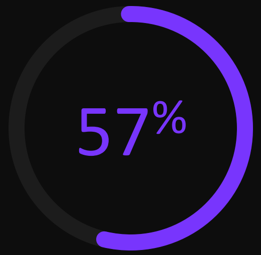
Business’ Top Cloud Initiatives in 2022

Source: Flexera 2022 Stat of the Cloud Report



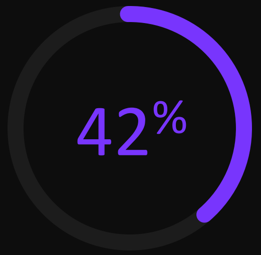
59%

Optimizing existing use of cloud



57%

Migrate more workloads to cloud



42%

Move from on-premise software to SaaS

Benefits

Source: Fortinet 2023 Cloud Security Report

53%
More Flexible Capacity/ Scalability

45%
Increased Agility

44%
Improved Availability and Business Continuity

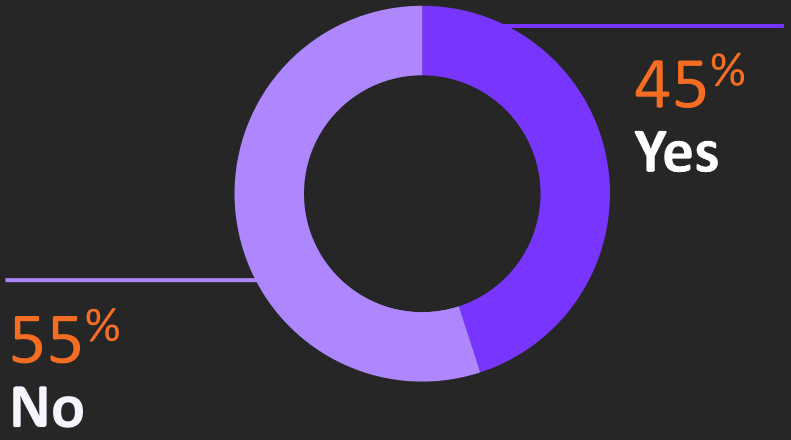
41%
Accelerated Deployment and Provisioning

Attackers have moved to the Cloud too

In one year, cloud breaches doubled

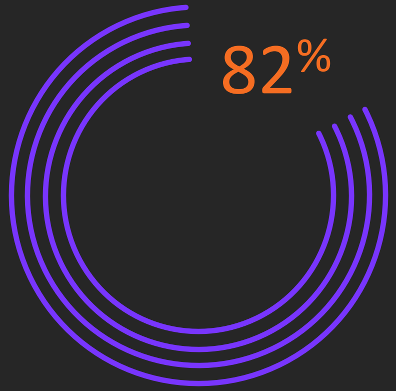
2022

Was data breached in the Cloud?



2023

Breaches that involved data stored in the Cloud



share of breaches that involved data stored in cloud environments- public cloud, private cloud or across multiple environments

Source: Cost of Data Breach Report 2022, 2023, IBM

Adversaries will choose the path of least

Resistance.

Case Study:
Midnight Blizzard

Attacked November 2023

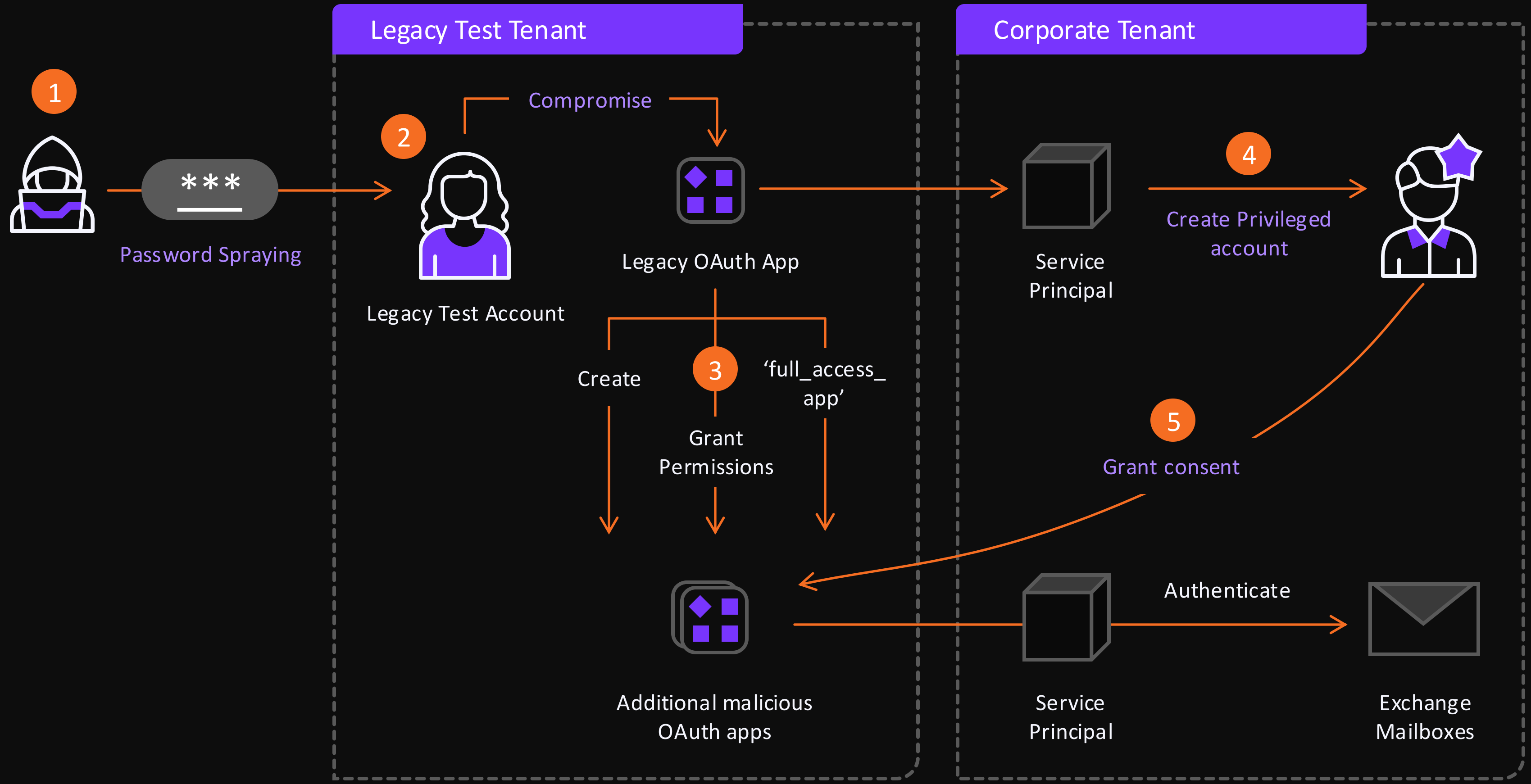
Disclosed January 2024

Threat actor is APT

TTPs used are basic and common

Target was Microsoft – owner and builder of Azure – one of the main Cloud Service Providers

Estimated Attack Flow



MITIGA

Attacking
On-Prem vs Cloud

	On-Premises		Cloud	
	Attackers	Defenders	Attackers	Defenders
Required Skillset	High	Moderate	Low	High
Availability of Tools	Abundant	High	High	Limited
Knowledge about the Organization	Detailed understanding needed	Detailed understanding needed	Minimal understanding needed	Detailed understanding needed
Perimeter Difference	Well-defined perimeter (network based)	Well-defined perimeter	Expansive, often unclear perimeter (identity based)	Expansive, often unclear perimeter
Ability to Respond Effectively	-	Controlled, Centralized	-	Challenged by complex permissions

Attackers POV »

Attackers POV

Skillset required

Old-school hacking meets the cloud revolution

On-Premises

V/S

- ✓ Basic computer knowledge
- ✓ Protocols
- ✓ Compile and run exploits
- ✓ Bypassing EDR
- ✓ Everything has OS

Cloud

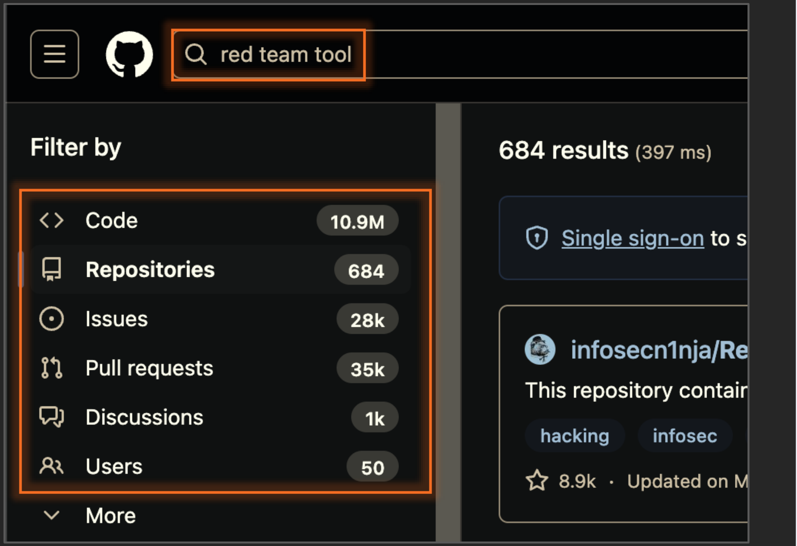
- ✓ Everything has a UI
- ✓ Everything available over web and API
- ✓ Plenty of usage documentation
- ✓ Widely known misconfigurations

Attackers POV

Tools of the Trade

Red Teamers:

Collecting tools like Pokemons



red team tool

Filter by

Code	10.9M
Repositories	684
Issues	28k
Pull requests	35k
Discussions	1k
Users	50

More

684 results (397 ms)

Single sign-on to s

infosecn1nja/Re

This repository contair

hacking infosec

8.9k · Updated on M

On-Premises

V/S

- ✓ Tools are getting “burned” by defense
- ✓ C2 frameworks costs
- ✓ Mimikatz, n-day exploits
- ✓ Metasploit

Cloud

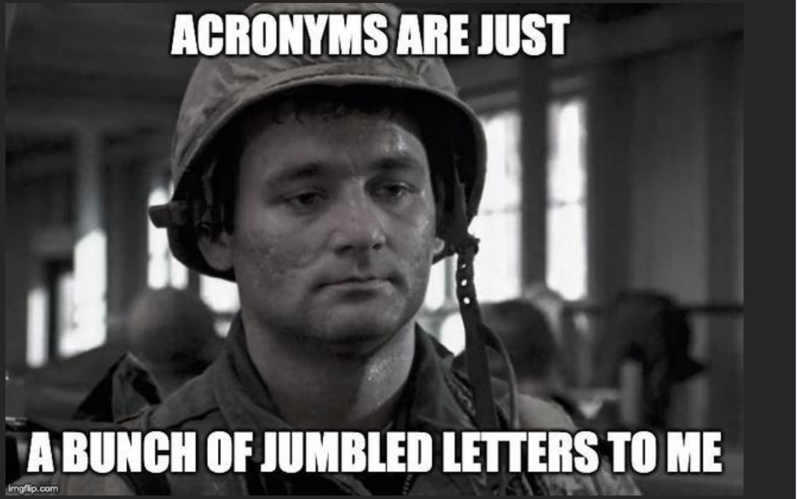
- ✓ You can’t have hash for behaviour
- ✓ No need for 0-day\n-day
- ✓ “exploits” are for configuration\design

Attackers POV

Security tech-stack

Acronyms:

making hackers feel important since ever



On-Premises

V/S

- ✓ EDR - endpoints
- ✓ IPS\IDS - network
- ✓ NAC - physical
- ✓ Internal FW - segmentation

Cloud

- ✓ CSPM – Cloud Security Posture Management
- ✓ CASB - Cloud Access Security Broker
- ✓ SSPM – SaaS Security Posture Management
- ✓ TDIR\CDR – Threat Detection Incident Response\Cloud Detection Response

Attackers POV

The “PeRiMeTer”

'The New Perimeter’

As effective as the old one.

ATTACKERS DON’T BREAK IN; THEY LOG IN.

On-Premises

V/S

- ✓ Malware on host
- ✓ VPN
- ✓ Vulnerability in edge device
- ✓ Physical access

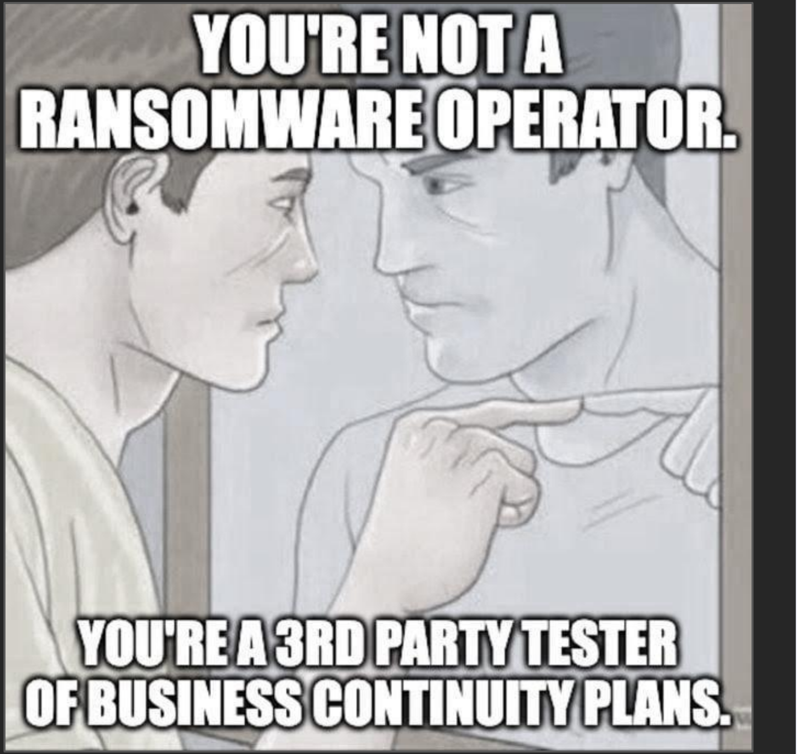
Cloud

- ✓ Identity (yeah, that’s it)

Attackers POV

I am the admin now

Malicious tool vs. malicious intent


YOU'RE NOT A RANSOMWARE OPERATOR.
YOU'RE A 3RD PARTY TESTER OF BUSINESS CONTINUITY PLANS.

On-Premises

- ✓ Interacting with LSASS is suspicious
- ✓ Tool signatures
- ✓ NT(LM)
- ✓ Exploit running
- ✓ DNS exfiltration

V/S

Cloud

- ✓ Bucket\ Storage replication
- ✓ App added to EntraID
- ✓ App added to GitHub\Gitlab
- ✓ Creating a GPU VM
- ✓ Creating API\ Access keys

Defenders POV

Defenders POV

New Tech, New Skills

On-Premises

V/S

- ✓ Tech is (mostly) same
- ✓ We know the architecture
- ✓ AD lateral movement and privilege escalation
- ✓ Common Event IDs
- ✓ Common SIEM queries\playbooks

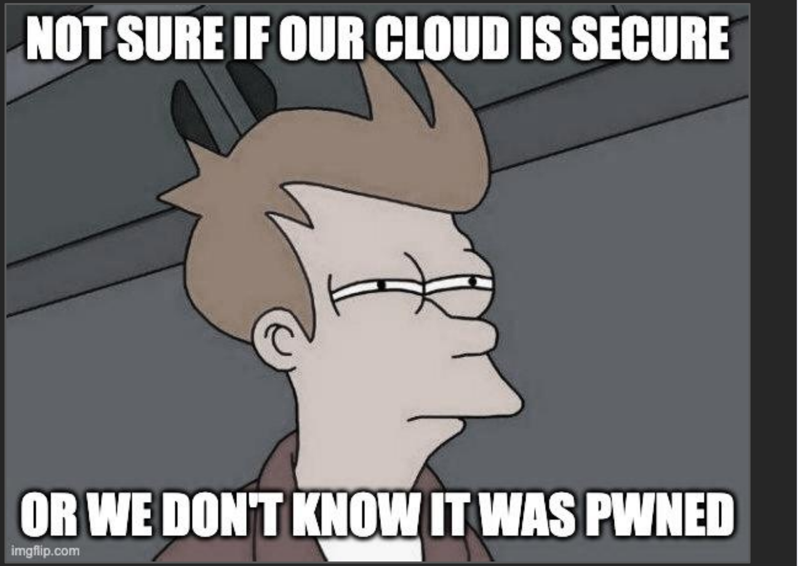
Cloud

- ✓ How do you investigate a bucket “leak”?
- ✓ What is the “architecture” between the serverless, containers and storage?
- ✓ How to investigate HR SaaS after unauthorized login?
- ✓ Do we have a playbook that fits 3 different CSPs?

Defenders POV

We've Got Security Covered

Just ignore those daily breaches


NOT SURE IF OUR CLOUD IS SECURE
OR WE DON'T KNOW IT WAS PWNED
imgflip.com

On-Premises

V/S

- ✓ IOCs, hashes, signatures
- ✓ SIGMA, YARA, Snort rules
- ✓ Isolation via EDR
- ✓ Able to patch vulnerabilities

Cloud

- ✓ IPs & Domains
- ✓ IOAs
- ✓ Can't isolate a bucket
- ✓ Can't patch (Shared Responsibility)

Defenders POV

Security tech-stack

So many tools, so little security

CISO BUYING ANOTHER SECURITY PLATFORM
SECOPS GET ANOTHER SECURITY PLATFORM
imgflip.com
GENILDO

On-Premises

V/S

- ✓ EDR\XDR
- ✓ SIEM
- ✓ SOAR\XSOAR
- ✓ IDS\IPS
- ✓ FW
- ✓ Network Analysis

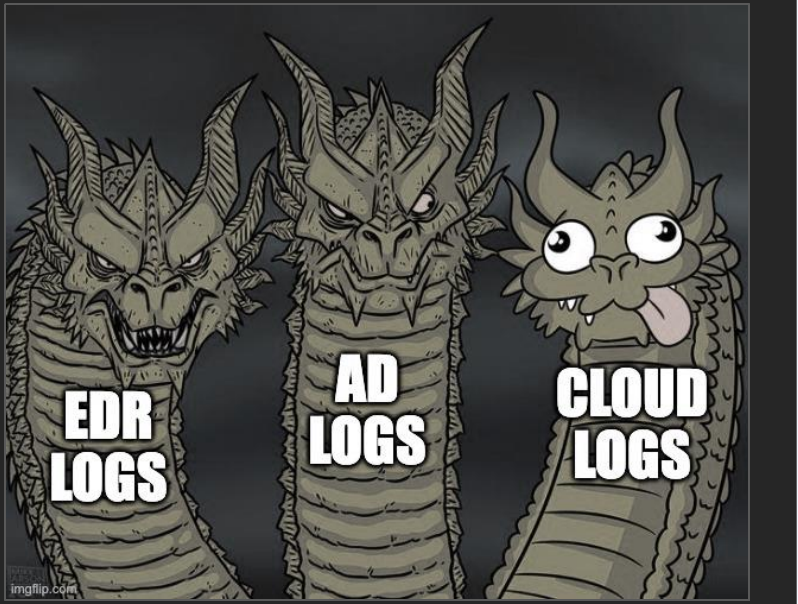
Cloud

- ✓ SIEM?
- ✓ Logs?

Defenders POV

Visibility

It's like finding a needle in a haystack. Blind. Hands tied behind your back. In the dark.



On-Premises

V/S

Cloud

On-Premises:

- ✓ Enable using policy
- ✓ Same structure
- ✓ Common types – Syslog, Network flow, Powershell logging, Event logs, App logs, AD logs, Linux logs…

Cloud:

- ✓ Turned off by default
- ✓ Need to turn on in each region
- ✓ Different type\content\structure
- ✓ SaaS sometimes don’t have them (and when they do it is blocked by license tiers)

Defenders POV

RACI

Structured Chaos vs. Complete Anarchy

On-Premises

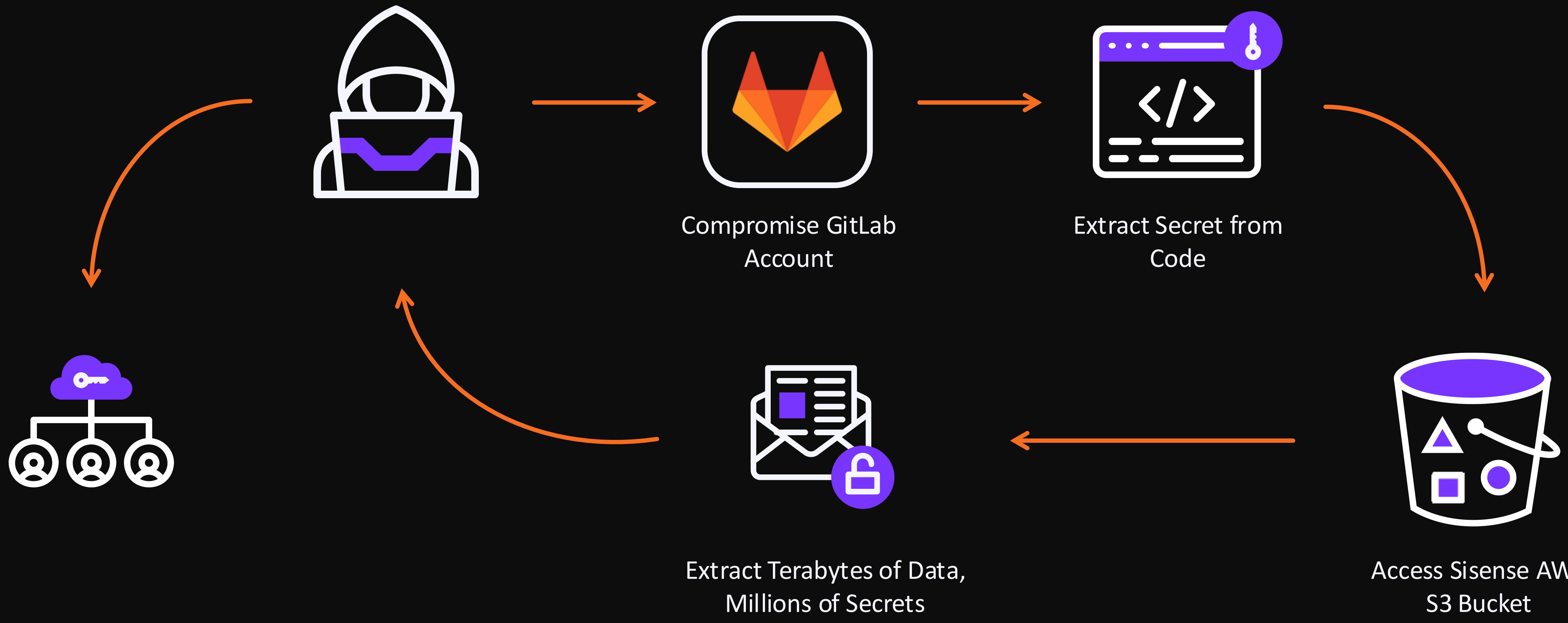
V/S

- ✓ Existing RACI
- ✓ IT\Cyber Security
- ✓ SOC\SecOps
- ✓ Have administrative access
- ✓ Security policy for new resources
- ✓ Patch\update cycles

Cloud

- ✓ Dev\DevOps\DevSecOps
- ✓ Soc\SecOps
- ✓ No administrative access
- ✓ Don’t manage the cloud
- ✓ Zero control over cloud\saas vulnerabilities

Sisense - Attack Flow



Compromise GitLab Account

Extract Secret from Code

Access Sisense AWS S3 Bucket

Extract Terabytes of Data, Millions of Secrets

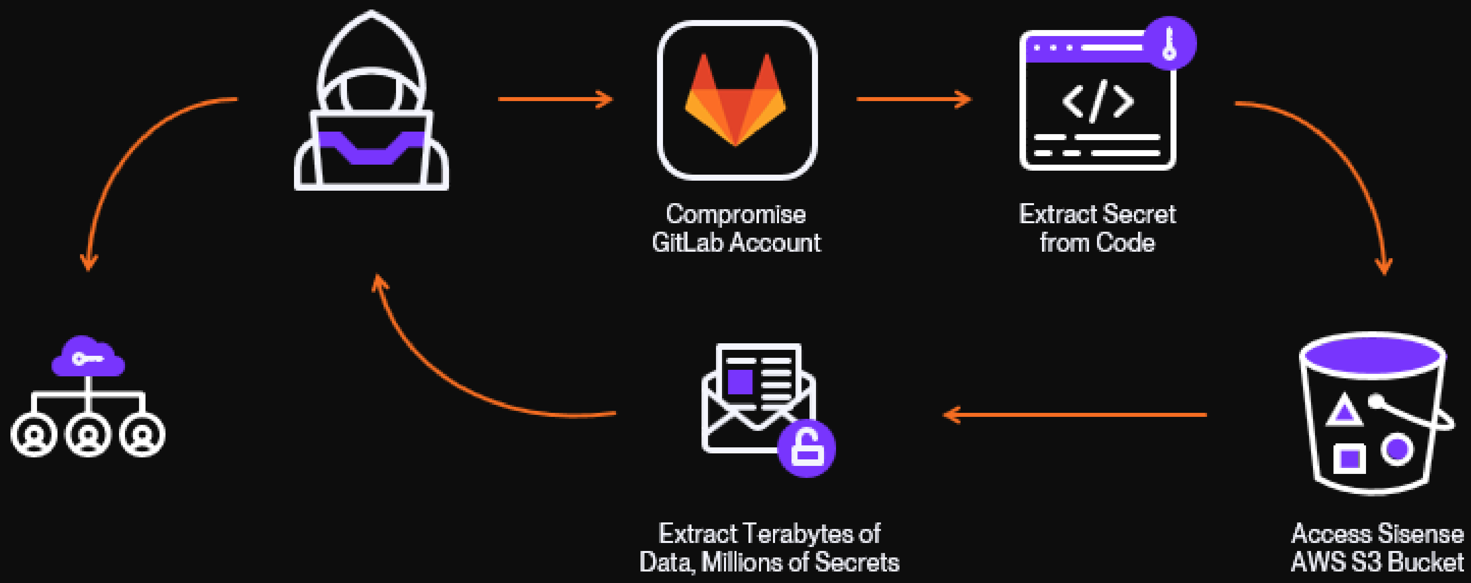
Case Study

Sisense - Attack Flow

April 2024

Sisense's GitLab code repository was breached, leading to data exfiltration from its Amazon S3 accounts.

- Exposed credentials and tokens potentially compromised Sisense and third-party services like Salesforce, AWS, and Google.
- CISA urged Sisense customers to reset credentials and investigate suspicious activity.
- Sisense's CISO recommended rotating credentials and provided mitigation actions.
- Attackers accessed Sisense’s GitLab and used credentials to download data from AWS.


Compromise GitLab Account
Extract Secret from Code
Access Sisense AWS S3 Bucket
Extract Terabytes of Data, Millions of Secrets

Apply What You Learned Today!

Next Week

Increase your cloud visibility

- Verify you have adequate logs from your CSPs.
- Verify you have logs from all SaaS platforms.

Next Month

Use what they give you

Make sure you enable all security tooling offered by the platforms:

- AWS offers GuardDuty
- Azure offers Security Center / Microsoft Defender for Cloud
- GCP offers Google Cloud Security Command Center (SCC)

And then...

Don’t Stop There! Become Proactive!

- Perform red team and threat hunting on cloud and SaaS, like any other system.
- Start building anomaly and behavioral detections for your cloud footprint.

Thank you

Questions?

www.mitiga.io

Roei Sherman
Field CTO | sherman@mitiga.io

NOVEMBER 2024