



From Snowflake to Snowstorm:

Cloud Breaches and Detections

www.mitiga.io

Roei Sherman

Field CTO | sherman@mitiga.io

NOVEMBER 2024 | CONFIDENTIAL

Roei Sherman

Field CTO at Mitiga



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



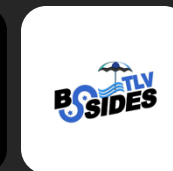
B.A - Information systems and Cybersecurity
M.A - Criminology



Co-organizer of BSidesTLV
Volunteer in Trace Labs



Amateur Homebrewer



The Snowflake Campaign - TL;DR

Threat Actor

UNC5537

Financially Motivated

Victims

165+ Organizations

 Santander

 ticketmaster

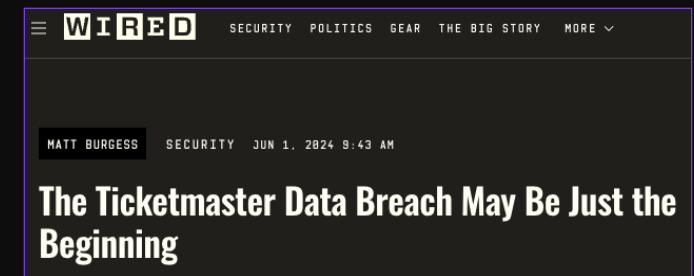
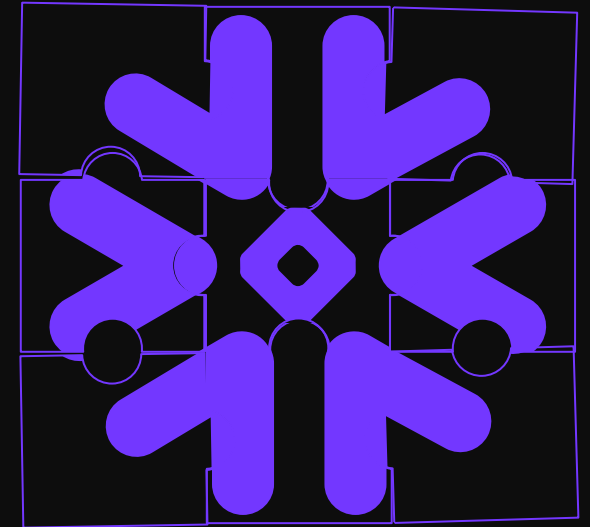
Time Frame

Few Months

Vulnerability

None

Combination of Misconfigurations



The Snowflake Campaign - ATT&CK

Resources Development

Tool to automate some/all exploitation

Way to identify instances owned by victims

Staging place for stolen data

Identify configuration gaps

Initial Access

Obtain creds from infostealer

Identify snowflake instance (Native tool)

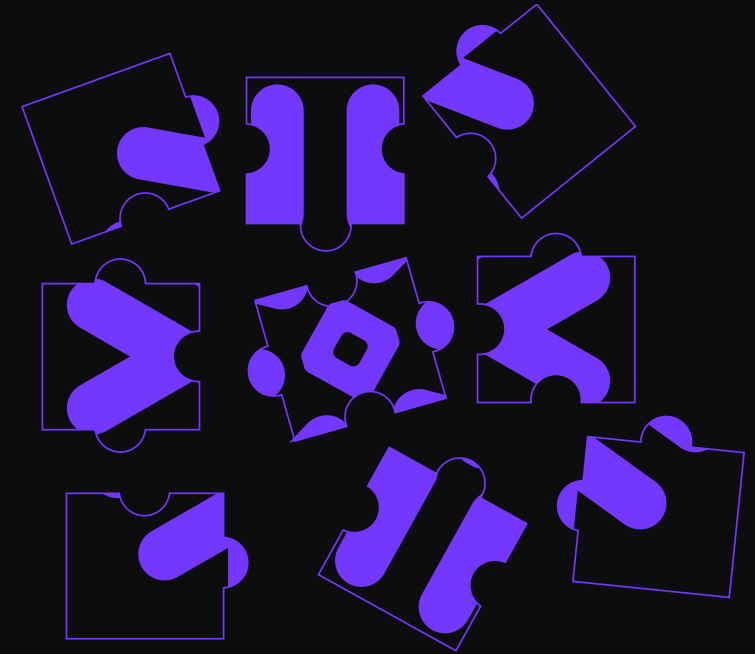
Login

Exfiltration

Exfiltrate data
outside of the
organization

Impact

Extortion



The Actual **Issues**

UNC5537 targets Snowflake customer databases for data theft and extortion, highlighting challenges in **securing cloud environments** against identity-based attacks.

UNC5537 has breached Snowflake instances using **credentials stolen via infostealer malware** — highlighting defenders' critical challenge against credential-based cloud attacks.

Attacks primarily hit **accounts lacking MFA** and proper network security, underscoring defenders' need for robust authentication and defenses.



The Actual **Issues**

The threat actors used
**built-in Snowflake features and
custom tools to exfiltrate data,**
which was then sold on cybercriminal forums or used for extortion.

We, Snowflake and Mandiant have provided guidance on detecting
and mitigating these threats by enforcing MFA,
monitoring for unusual activities,
and setting up network policies



Adversaries
aren't breaking in, **they**
log in. 



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



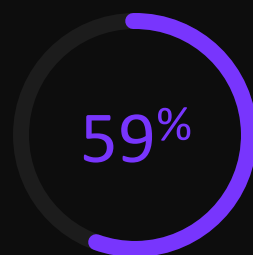
Availability



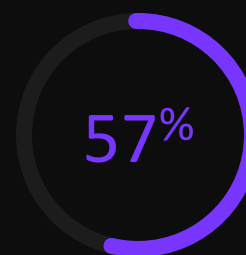
Scalability

Business' Top Cloud Initiatives in 2022

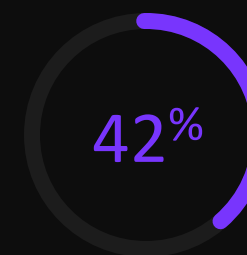
Source: Flexera 2022 Stat of the Cloud Report



Optimizing existing use of cloud



Migrate more workloads to cloud



Move from on-premise software to SaaS

Benefits

Source: Fortinet 2023 Cloud Security Report

53%

More Flexible Capacity/ Scalability

45%

Increased Agility

44%

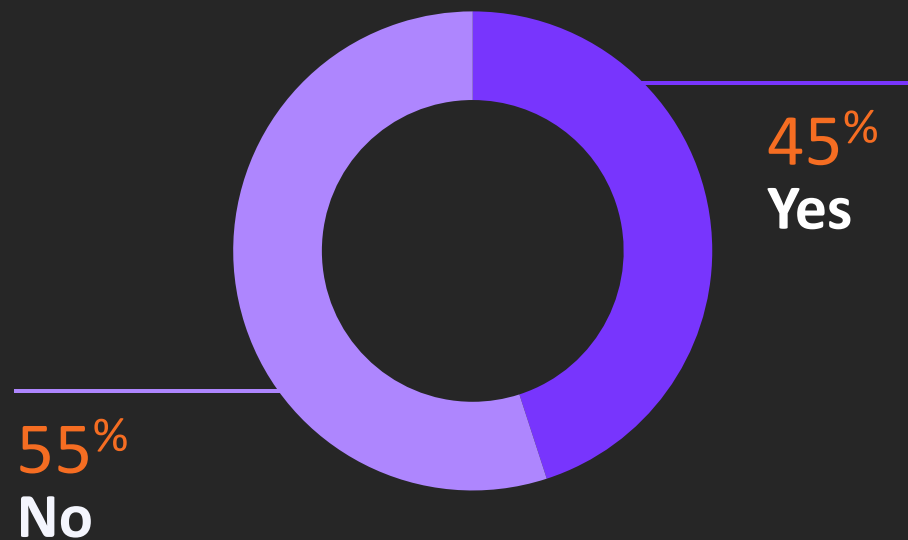
Improved Availability and Business Continuity

41%

Accelerated Deployment and Provisioning

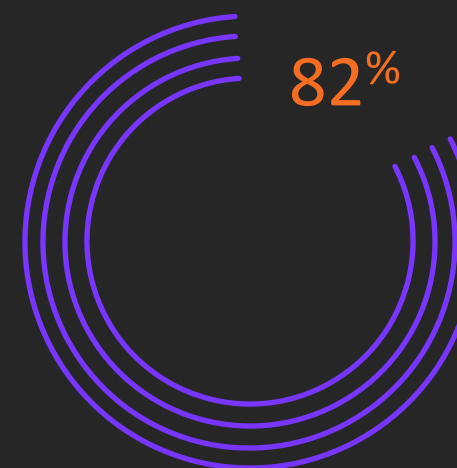
2022

Was data breached in the Cloud?



2023

Breaches that involved data stored in the Cloud



82% Share of breaches that involved data stored in cloud environments-public cloud, private cloud or across multiple environments

Case Study: Midnight Blizzard

Attacked November 2023

Disclosed January 2024



Threat actor is APT

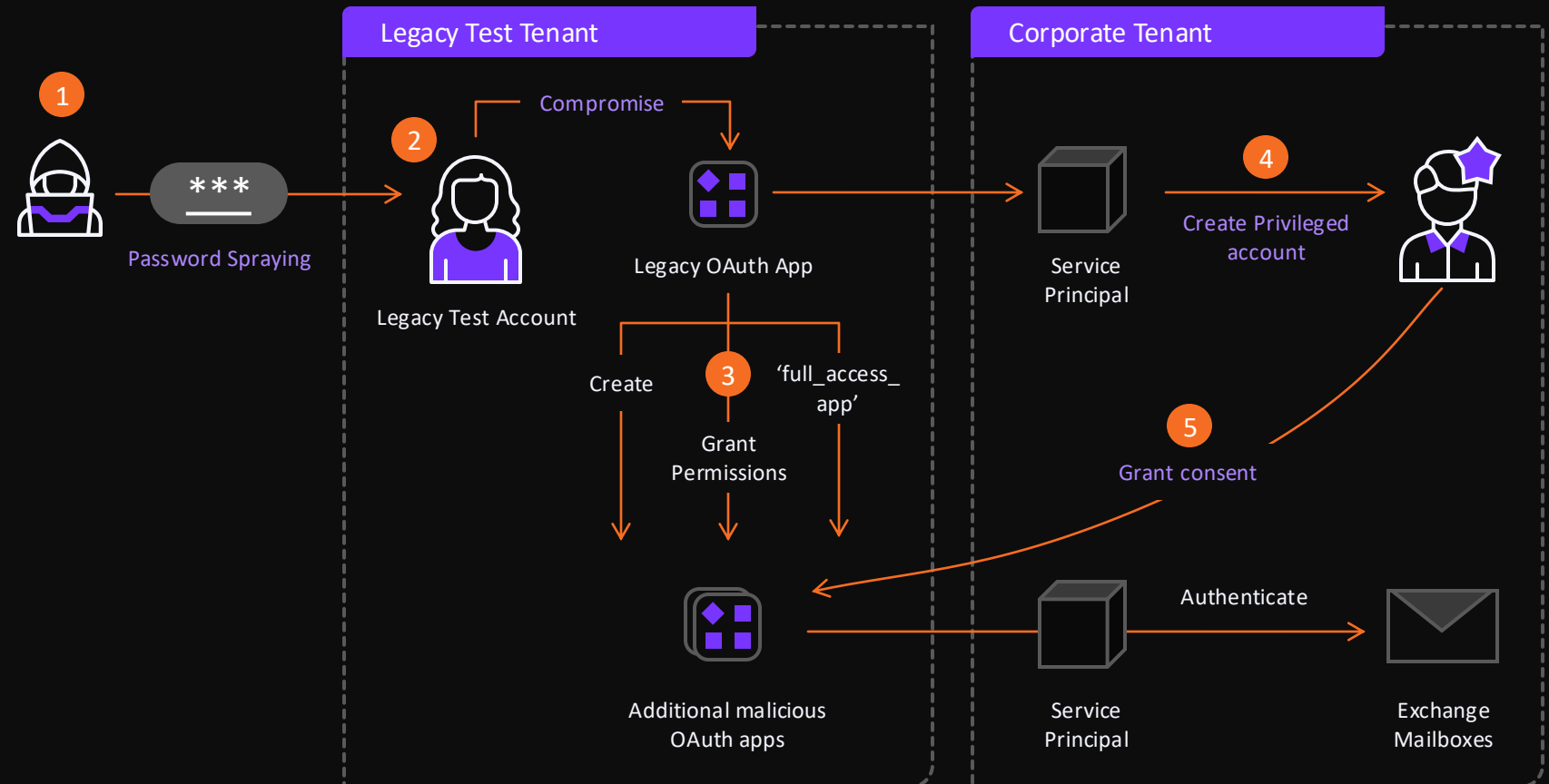


TTPs used are basic and common



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

Estimated Attack Flow



Context-Aware, Behavioral and Anomaly-based



Do we have a baseline
to compare against
actions?



When actions are
identical, we need to
detect intention.



Logic should be generic
to be applied across
the board.

Problem 1 : Visibility

CSP

- ! Turned off by default
- ! Retention time, regions
- ! Log types, log content

SaaS

- ! Doesn't always exist
- ! License tier
- ! Security logs vs. application logs

CSP

- ! Turned off by default
- ! Retention time, regions
- ! Log types, log content

SaaS

- ! Doesn't always exist
- ! License tier
- ! Security logs vs. application logs

Verify devops know
what to activate

CSP

- ! Turned off by default
- ! Retention time, regions
- ! Log types, log content

SaaS

- ! Doesn't always exist
- ! License tier
- ! Security logs vs. application logs

Verify devops know
where to activate

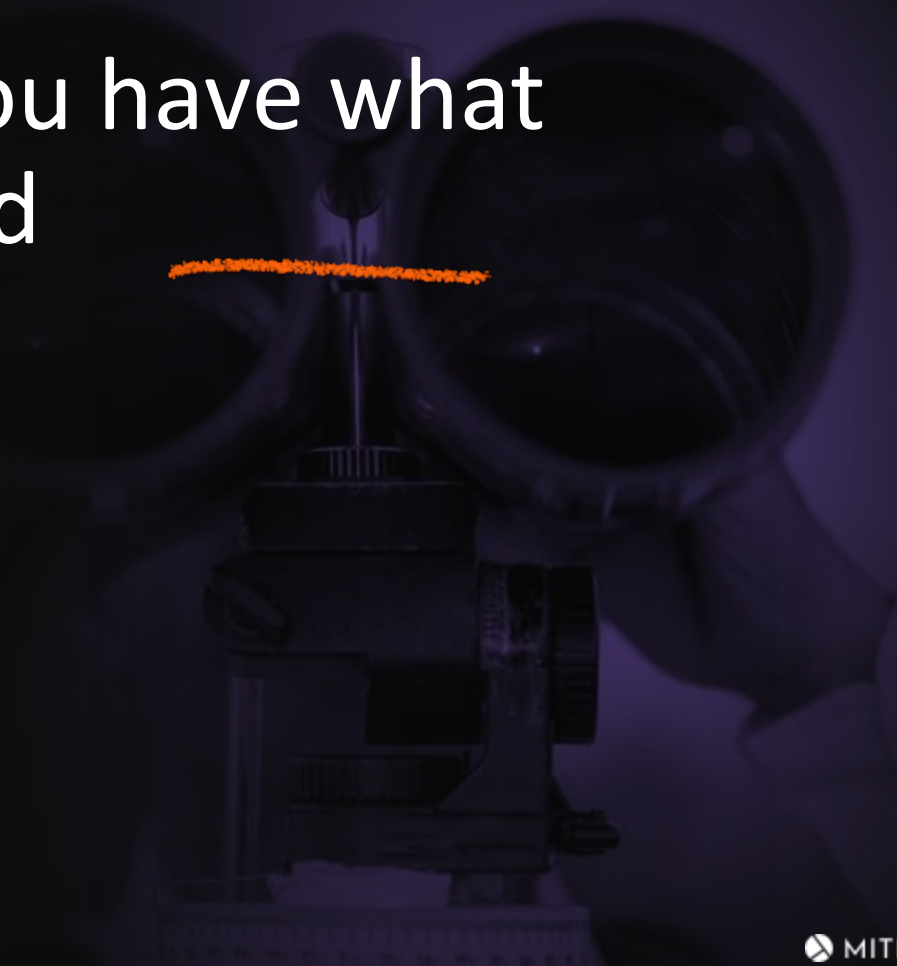
CSP

- ! Turned off by default
- ! Retention time, regions
- ! Log types, log content

SaaS

- ! Doesn't always exist
- ! License tier
- ! Security logs vs. application logs

Verify you have what
you need



CSP

- ! Turned off by default
- ! Retention time, regions
- ! Log types, log content

SaaS

- ! Doesn't always exist
- ! License tier
- ! Security logs vs. application logs

Simulate SaaS-focused
red team

CSP

- ! Turned off by default
- ! Retention time, regions
- ! Log types, log content

SaaS

- ! Doesn't always exist
- ! License tier
- ! Security logs vs. application logs

Contracts

CSP

- ! Turned off by default
- ! Retention time, regions
- ! Log types, log content

SaaS

- ! Doesn't always exist
- ! License tier
- ! Security logs vs. application logs

Send to SecOps

Problem 2 :

Identity Over Malware

- ! No need for 0-day/n-day
- ! You can't have hash for behavior
- ! InfoStealers are cheap and easy to use
- ! No more "Perimeter"



Solution 2 : Identity Over Malware

! No need for 0-day/n-day

! You can't have hash
for behavior

! InfoStealers are cheap
and easy to use

! No more "Perimeter"

MFA



Solution 2 : Identity Over Malware

- ! No need for 0-day/n-day
- ! You can't have hash for behavior
- ! InfoStealers are cheap and easy to use
- ! No more "Perimeter"

Characteristics



Solution 2 :

Identity Over Malware

- ! No need for 0-day/n-day
- ! You can't have hash for behavior
- ! InfoStealers are cheap and easy to use
- ! No more "Perimeter"

Proactive Threat Intelligence



Solution 2 : Identity Over Malware

- ! No need for 0-day/n-day
- ! You can't have hash for behavior
- ! InfoStealers are cheap and easy to use
- ! No more "Perimeter"

Automation



Solution 2 :

Identity Over Malware

- ! No need for 0-day/n-day
- ! You can't have hash for behavior
- ! InfoStealers are cheap and easy to use
- ! No more "Perimeter"

Follow-up events



Problem 3 :

Skillset

- ! Everything is over web and API
- ! How do you investigate a bucket “leak”?
- ! How to investigate HR SaaS after unauthorized login?
- ! No EDR for non-workload resources



Solution 3 :

Skillset

- ! Everything is over web and API
- ! How do you investigate a bucket “leak”?
- ! How to investigate HR SaaS after unauthorized login?
- ! No EDR for non-workload resources

Training



Solution 3 :

Skillset

- ! Everything is over web and API
- ! How do you investigate a bucket “leak”?
- ! How to investigate HR SaaS after unauthorized login?
- ! No EDR for non-workload resources

Hands-on drills (Purple\Red)



Solution 3 :

Skillset

- ! Everything is over web and API
- ! How do you investigate a bucket “leak”?
- ! How to investigate HR SaaS after unauthorized login?
- ! No EDR for non-workload resources

Ongoing internal Threat Hunting



Solution 3 :

Skillset

- ! Everything is over web and API
- ! How do you investigate a bucket “leak”?
- ! How to investigate HR SaaS after unauthorized login?
- ! No EDR for non-workload resources

Full monitoring
for non-workload
resources

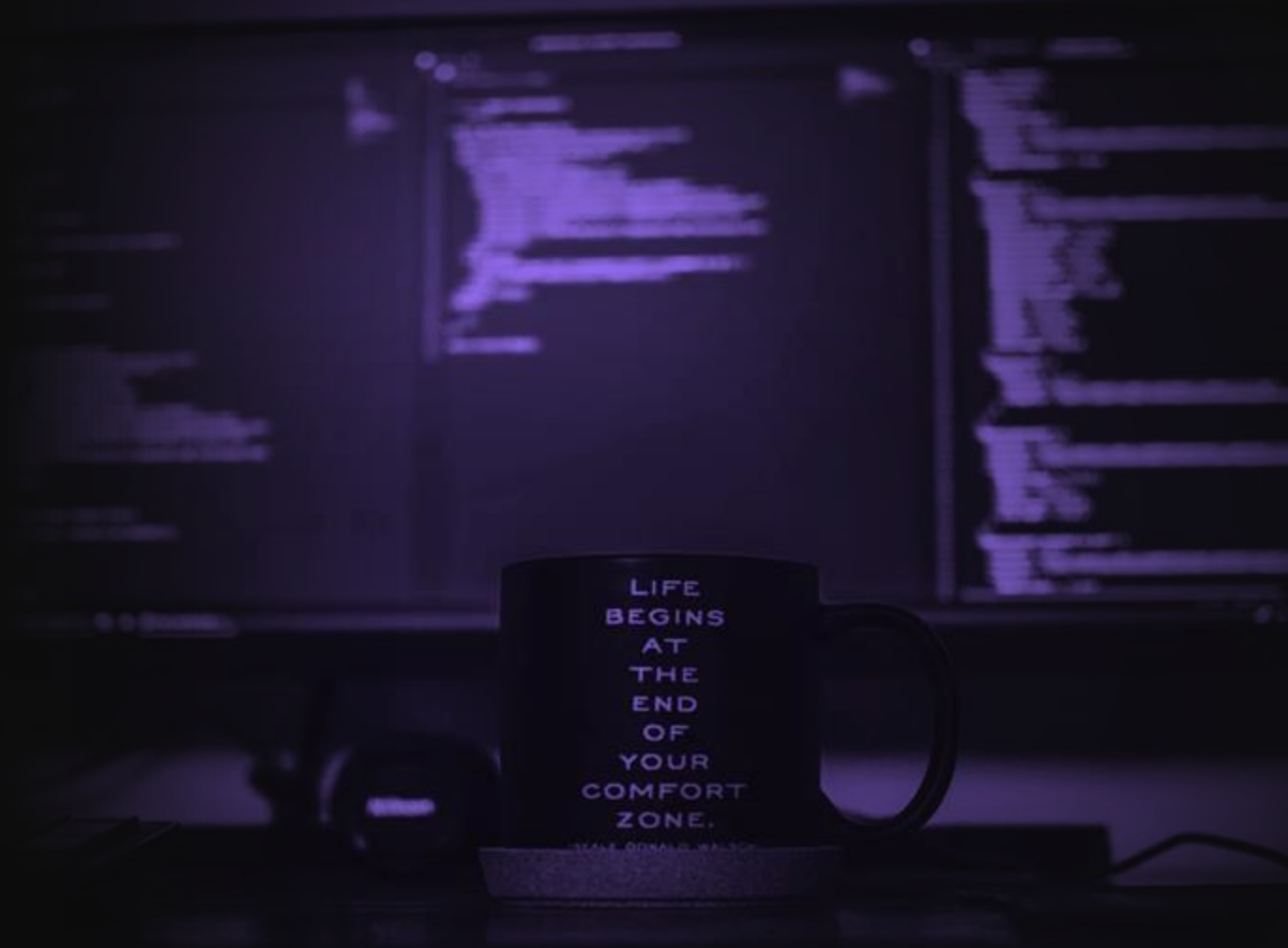


Problem 4 :

RACI

! Who owns Cloud Security/SaaS Security?

- Enabling logs?
- Using logs?
- Investigating?
- Mitigating?



Solution 4 :

RACI

! Who owns Cloud Security/SaaS Security?

- Enabling logs?
- Using logs?
- Investigating?
- Mitigating?

Clear definitions



Solution 4 :

RACI

! Who owns Cloud Security/SaaS Security?

- Enabling logs?
- Using logs?
- Investigating?
- Mitigating?

Security

“break glass” accounts



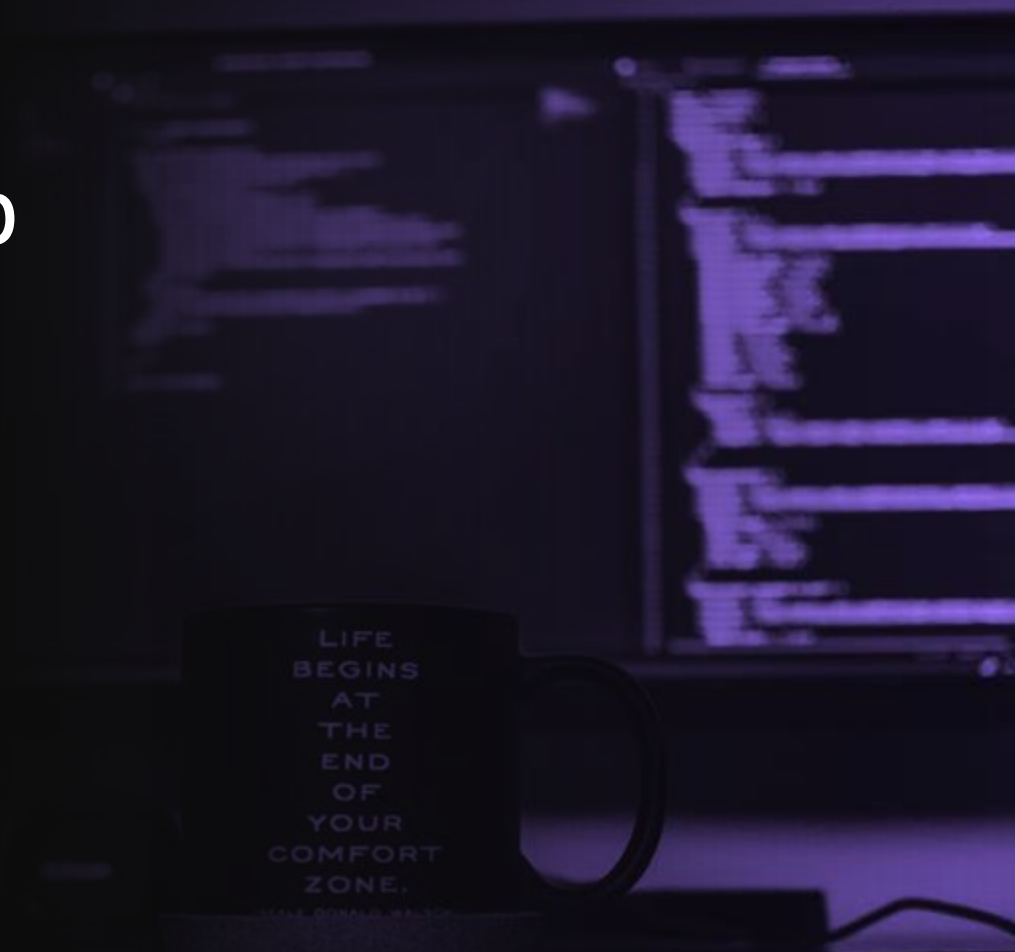
Solution 4 :

RACI

! Who owns Cloud Security/SaaS Security?

- Enabling logs?
- Using logs?
- Investigating?
- Mitigating?

Tabletop drills



Problem 5 : False-positives

- ! The age of Work from Anywhere
- ! Global companies
- ! Many SaaS
- ! Actions aren't malicious – the intent is



Solution 5 : False-positives

- ! The age of Work from Anywhere
- ! Global companies
- ! Many SaaS
- ! Actions aren't malicious – the intent is

How common are new thing?

- New actions
- New platform
- New regions

Solution 5 : False-positives

- ! The age of Work from Anywhere
- ! Global companies
- ! Many SaaS
- ! Actions aren't malicious – the intent is

Flow
detection

v/s

Atomic detection

Snowflake is a **Symptom**, not the problem

It will happen again

- Adversaries are no longer breaking in, they log in.
- Behavior beats tools, everywhere, every time.

Detection Engineering **Example**

Context-Aware, Behavioral and Anomaly-based

Where did they
authenticate
compared to usual?

Connection
metadata – user-
agent, OS, time

Is it a crown-jewel?

Do we have Threat
Intelligence?

And more...!

Behavioral Detection Engineering

Threat Intelligence

Event Metadata

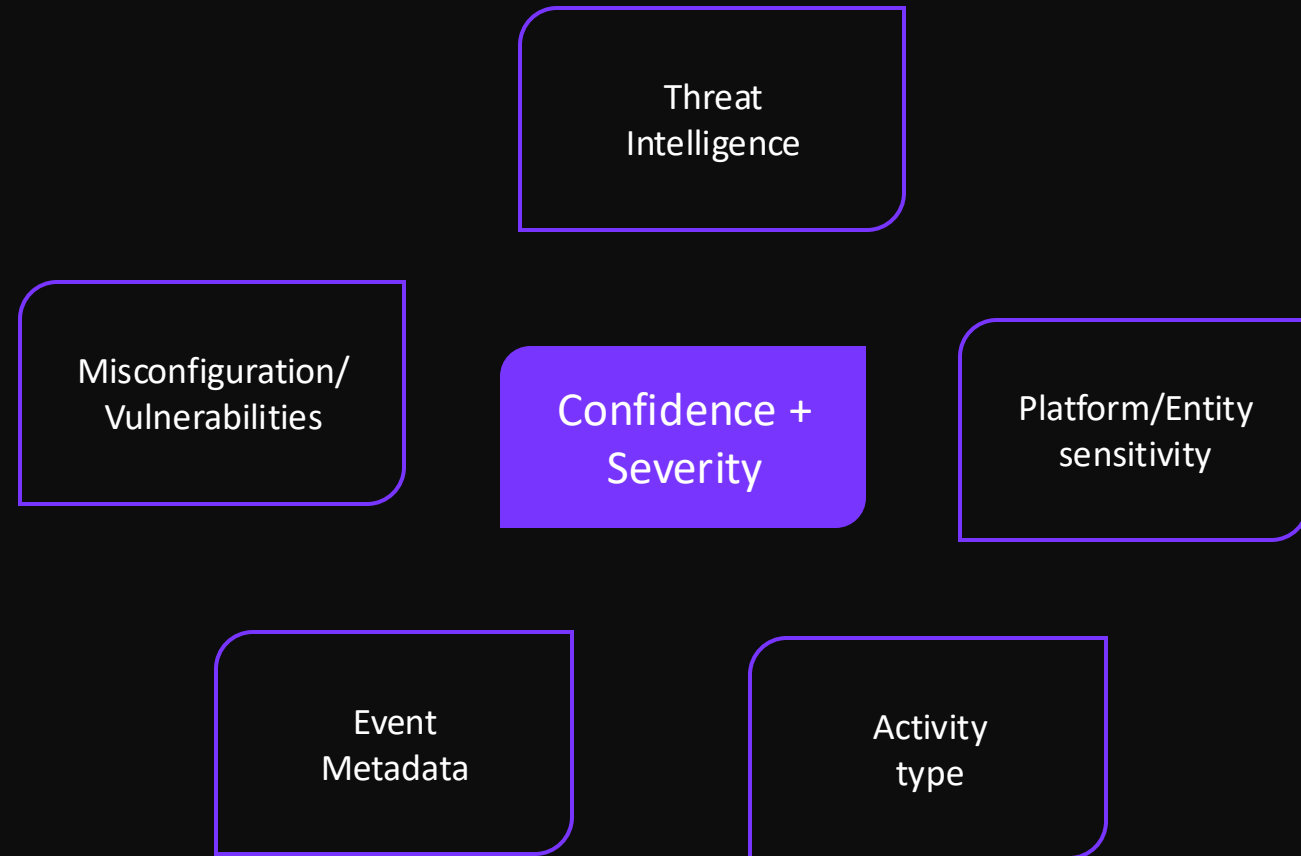
- Location, type (hosting, VPN, TOR)
 - Time, Browser, OS
 - Event-spike
-

Activity type

- Type of action
 - Platform and/or region
-

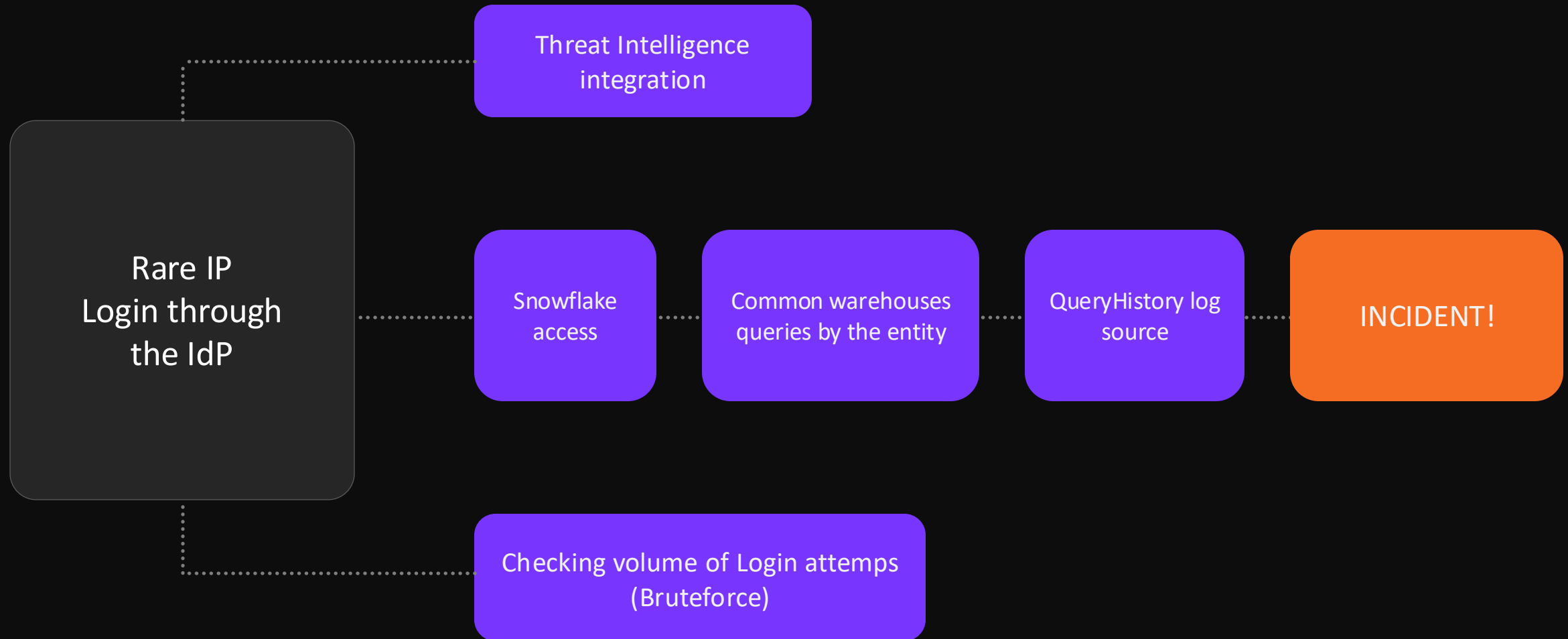
Platform/Entity sensitivity

Misconfiguration and/or vulnerabilities



Something is Going on

– Is it Malicious?



Apply What You Learned Today!



Next Week

Increase your cloud visibility

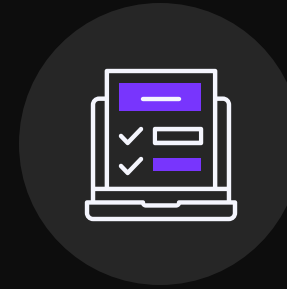
- Verify you have adequate logs from your CSPs.
- Verify you have logs from all SaaS platforms.



Next Month

Plan forward

- Develop behavioral detection strategy
- Establish clear RACI for cloud security
- Invest in ongoing upskilling and threat detection



And then...

Baselining

- Collect and analyze logs from all systems to establish a baseline of normal activity over time.
- Implement anomaly detection tools to compare current logs against the baseline and alert on deviations.



Thank you

Questions?

www.mitiga.io

Roei Sherman

Field CTO | sherman@mitiga.io

NOVEMBER 2024 | CONFIDENTIAL