MITIGA | x33fcon

# From Snowflake to Snowstorm:

## Cloud Breaches and Detections

www.mitiga.io

**Roei Sherman**
Sr. Director, Research | sherman@mitiga.io

June 2025

# Roei Sherman

Sr. Director, Research at Mitiga


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

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

Co-organizer of BSidesTLV
Defcon Goon
Volunteer in Trace Labs

Amateur Homebrewer

TRACE LABS

BSIDES TLV

ABInBev

DEFCON GROUPS 9723

MITIGA


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

# What is Snowflake

~~A fully managed, cloud-native data platform that decouples storage and compute for elastic scalability, high concurrency, and near-zero administration.~~

The chillest warehouse in the cloud:
Instantly scales, devours data mountains, and spits back results before you blink.

# The Snowflake Campaign - TL;DR

## Threat Actor

UNC5537

Financially Motivated

## Victims

**165+** Organizations

Santander

ticketmaster

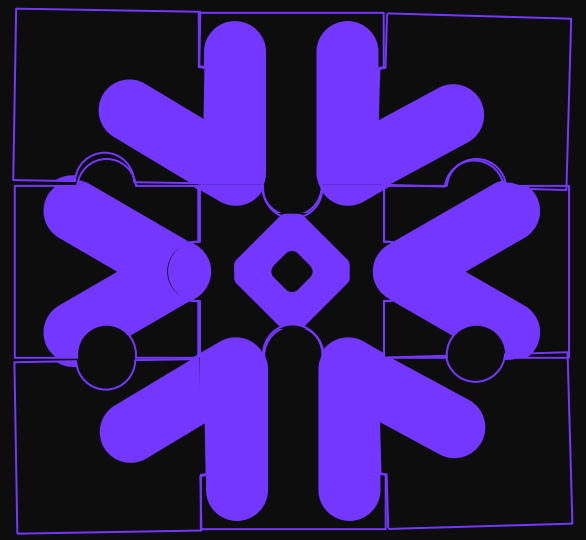
## Time Frame

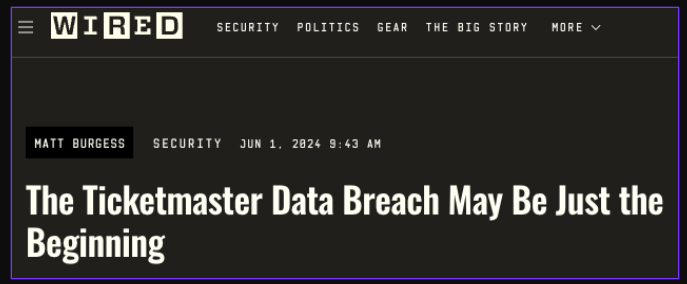
Few Months

## 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

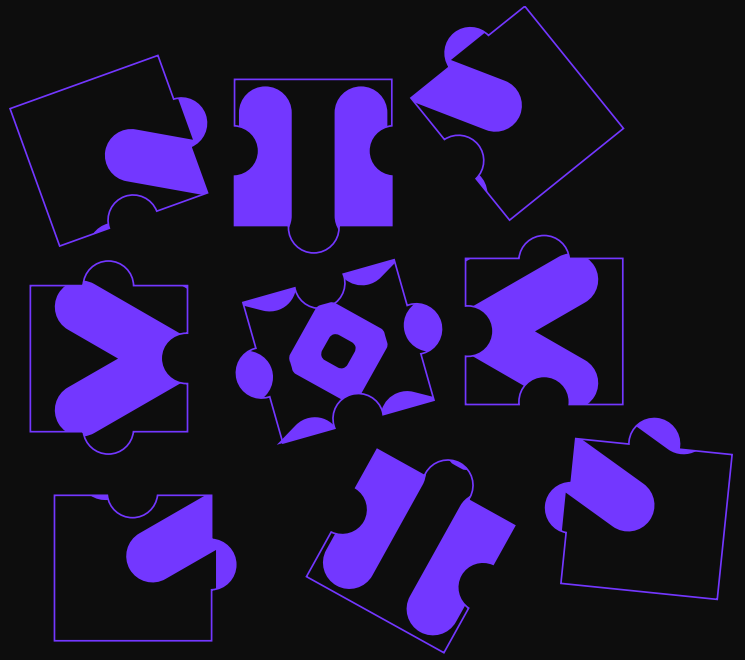
- Obtain creds from infostealer
- Identify snowflake instance (Native tool)
- Login

## Exfiltration

Exfiltrate data outside of the organization

## Impact

Extortion



# The Actual Issues

Challenges securing SaaS against identity attacks

Credentials stolen via infostealer

Accounts lacking MFA

MITIGA

# The Actual Issues

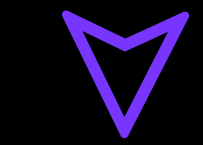
Built-in Snowflake features to exfiltrate data

Inability to Enforcing MFA and monitoring for unusual activities

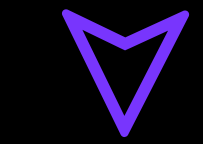
MITIGA

# Could Companies Detect This?

Does SaaS provide security logs?



Are you ingesting them?



Have you investigated them?

MITIGA

# We must remember,

# SaaS is Cloud.

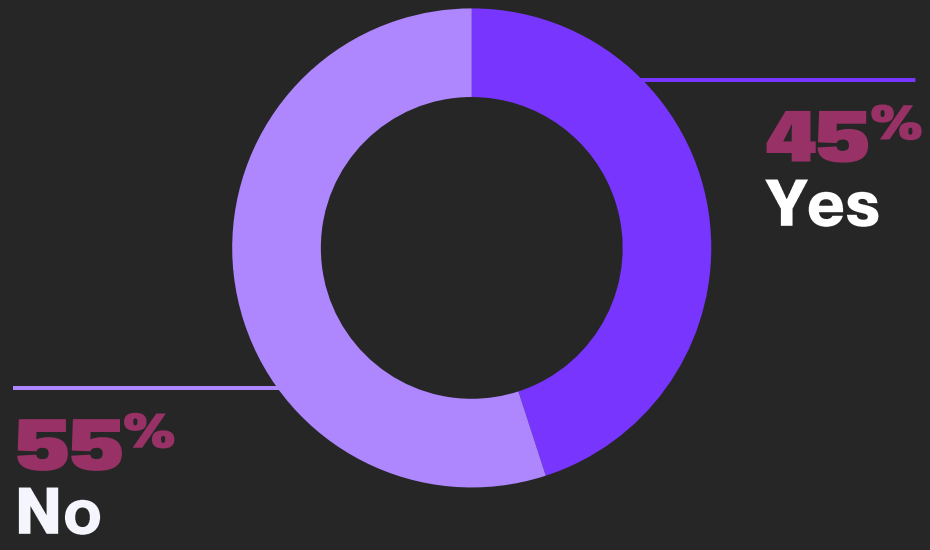

MITIGA

# Could Companies Detect This?

Do you have detection for inner-SaaS actions or just logins?

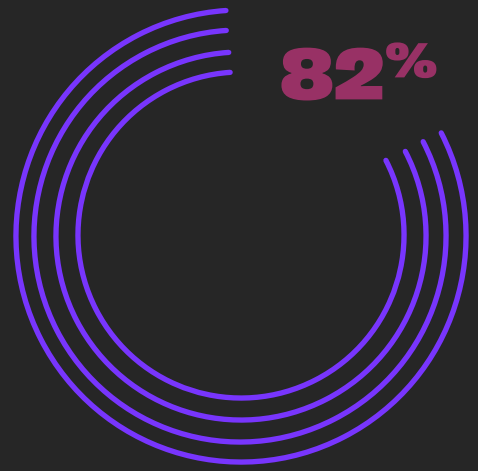
2022

## 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

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

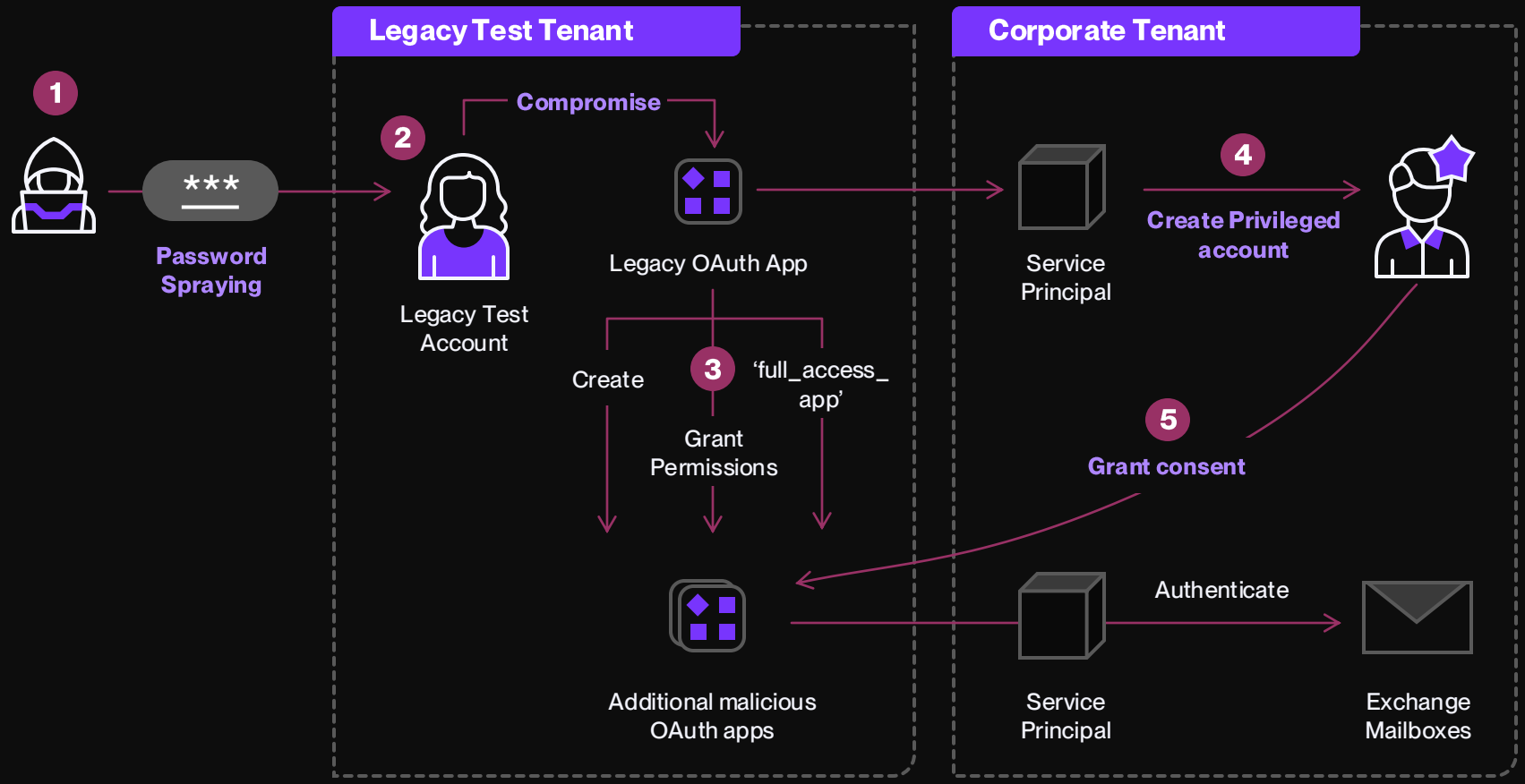
# Case Study:
# Midnight Blizzard

**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

# Cloud Detection Engineering is HARD

## 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.

# Behavioral Detection Engineering

Threat Intelligence

Event Metadata

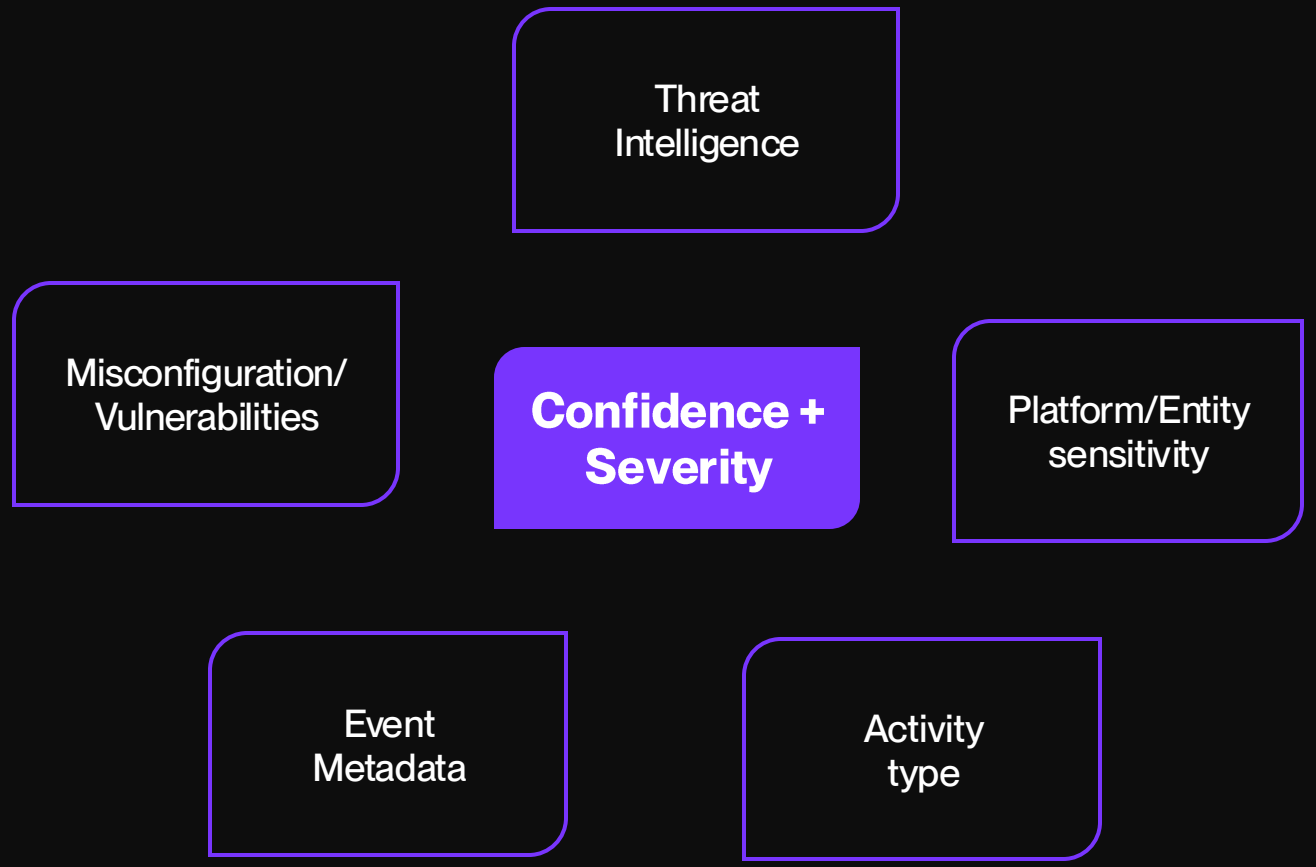
- Location, type (hosting, VPN, TOR)
- Time, Browser, OS
- Event-spike

Activity type

- Type of action
- Platform and/or region

Platform/Entity sensitivity

Misconfiguration and/or vulnerabilities

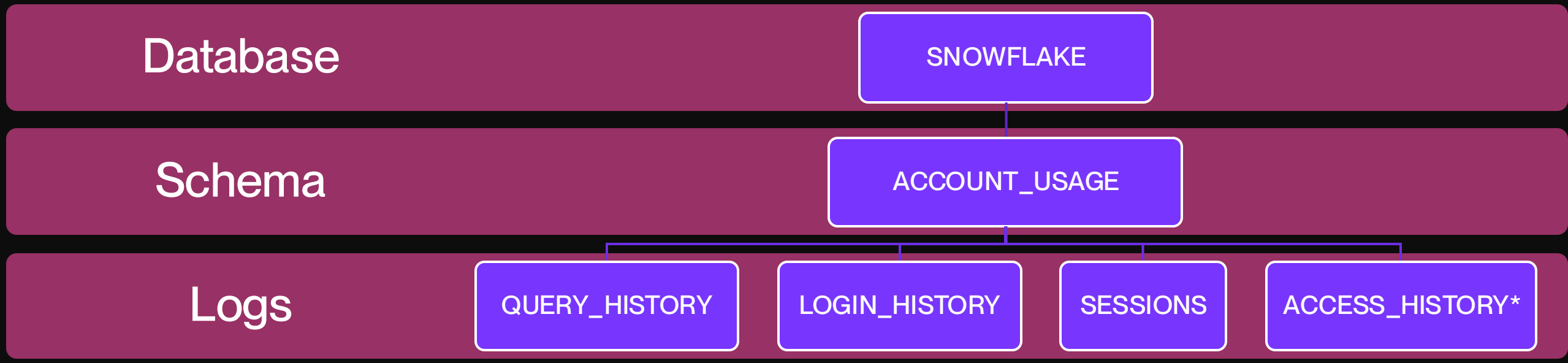


# Something is Going on
## – Is it Malicious?

# What is Snowflake

| | Databases | Snowflake |
|---|---|---|
| Logs | Audit logs written to local files or syslog | ACCESS_HISTORY & QUERY_HISTORY system views capture every auth, DML, DDL, etc. |
| Locations | On-prem and\on SIEM | Data lives in S3/ADLS/GCS object storage<br>Metadata & logs fully managed within Snowflake service |
| Integrations | Connect via ODBC/JDBC/CLI drivers<br>Must install & manage SIEM agents or log shippers (e.g. Beats) | Native connectors to Splunk, Datadog, etc.<br>- Snowpipe & event table streams for near-real-time SIEM ingest<br>- Rich partner ecosystem (Fivetran, StreamSets) |

# Practical Examples
# Snowflake log source



# Practical Examples
# Snowflake log source

QUERY_HISTORY

Latency for the view may be up to 45 minutes

- Logs all queries
- Example columns:
  - query_text
  - database_name
  - user_name
  - role_name
  - rows_produced
  - And more

# Practical Examples
# Snowflake log source

LOGIN_HISTORY

Latency for the view may be up to 120 minutes (2 hours)

- Logs login attempts
- Example columns:
  - EVENT_TIMESTAMP
  - USER_NAME
  - CLIENT_IP
  - IS_SUCCESS
  - SECOND_AUTHENTICATOR_FACTOR
  - And more

# Practical Examples
# Snowflake log source

SESSIONS

Latency for the view may be up to 180 minutes (3 hours)

- Details of sessions
- Example columns:
  - USER_NAME
  - AUTHENTICATION_METHOD
  - CLIENT_APPLICATION_ID
  - And more

# Practical Examples
# Snowflake log source

ACCESS_HISTORY

Enterprise edition ONLY
Latency for the view may be up to 180 minutes (3 hours).

- All user activity
- Example columns:
  - user_name
  - direct_object_accessed
  - objects_modified
  - And more

MITIGA

# Practical Examples
# Snowflake log source

## QUERY_HISTORY

Latency for the view may be up to 45 minutes

- Logs all queries
- Example columns:
  - query_text
  - database_name
  - user_name
  - role_name
  - rows_produced
  - And more

## LOGIN_HISTORY

Latency for the view may be up to 120 minutes (2 hours)

- Logs login attempts
- Example columns:
  - EVENT_TIMESTAMP
  - USER_NAME
  - CLIENT_IP
  - IS_SUCCESS
  - SECOND_AUTHENTICATOR_FACTOR
  - And more

## SESSIONS

Latency for the view may be up to 180 minutes (3 hours)

- Details of sessions
- Example columns:
  - USER_NAME
  - AUTHENTICATION_METHOD
  - CLIENT_APPLICATION_ID
  - And more

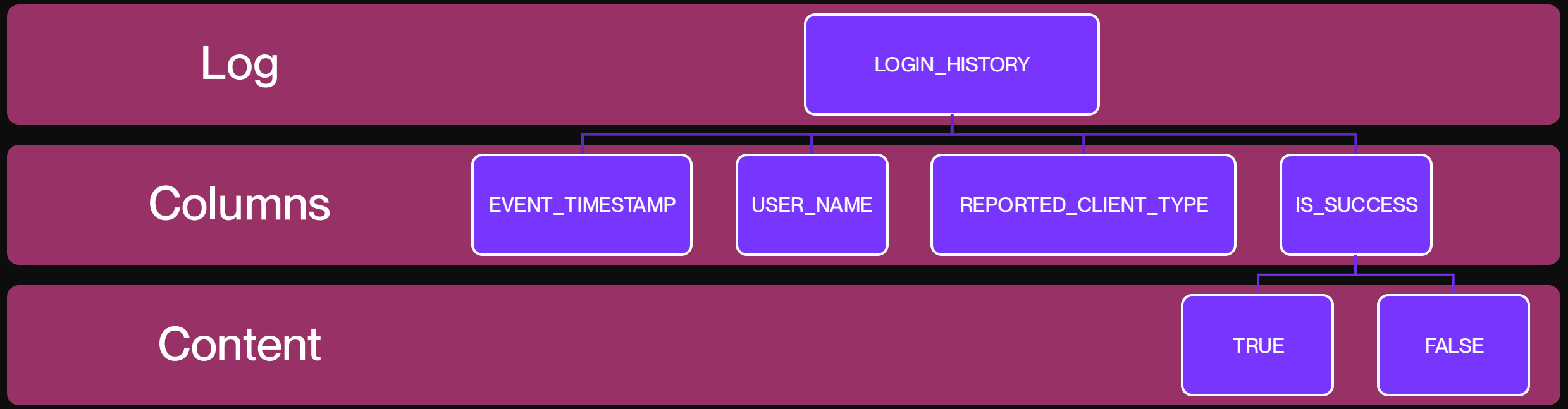
## ACCESS_HISTORY

Enterprise edition ONLY
Latency for the view may be up to 180 minutes (3 hours).

- All user activity
- Example columns:
  - user_name
  - direct_object_accessed
  - objects_modified
  - And more

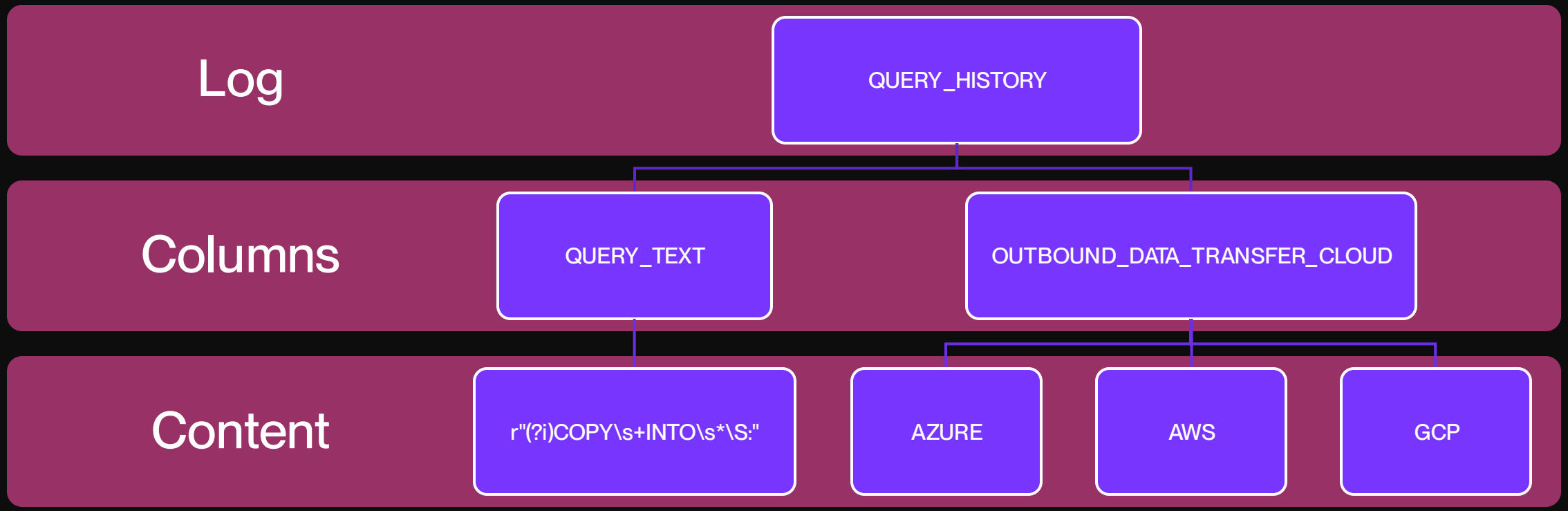
# Practical Examples
# Snowflake detections

## Password Spray



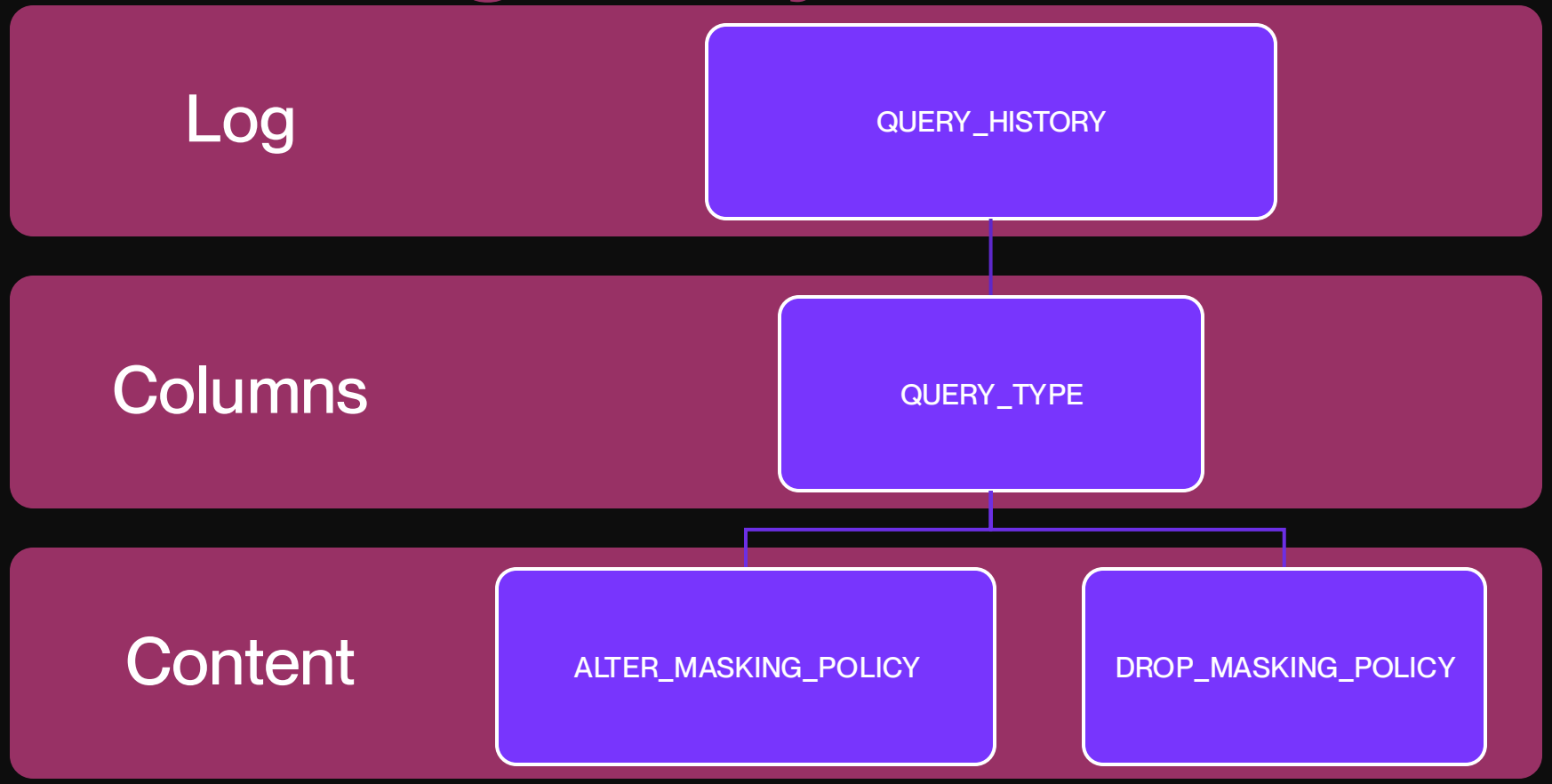
# Practical Examples
# Snowflake detections

## Exfiltration



# Practical Examples
# Snowflake detections

## Masking Policy Modification



# 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.

# What Has Changed

## MFA

Mandatory

## Shared Destiny

**“we've really pivoted from a shared-security model to more of a shared-destiny model with our customers”**

Snowflake’s CISO, Brad Jones

# Thank you

Questions?

www.mitiga.io

**Roei Sherman**
Sr. Director, Research | sherman@mitiga.io

MITIGA