STRIFEBOT

purple teaming Snowflake

James Henderson

hendo@reversec.com
hendo cloudsecurityforum slack

REVERSEC

1 Background

2 RED

- How to conduct simulated attacks

3 BLUE

- Defences and Detections

Wot is SnowFlake

- Saas Data Lake platform
  - AKA a database in the cloud

- Early 2024, Mandiant uncover campaign targeting Snowflake customers:
  - No vulns in snowflake exploited during attack
  - Stole credentials and accessed multiple tenants
  - Performed quick enumeration
  - Used legitimate features to exfil to external storage in cloud

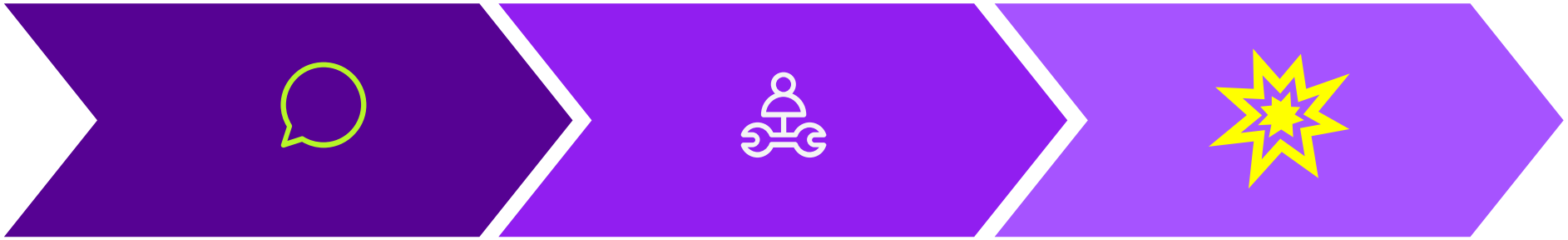
Threat Modelling

What does an attacker want to do?

Execution

Execute the attack

Analyse defences



Test Case Design

Build a plan of attack

Account(s)

Organisation

Database

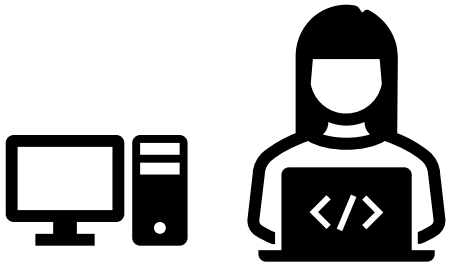
Table

- Users
- Functions
- Data
- Settings
- Integrations
- Logs

Table


snowflake®

CI/CD platforms

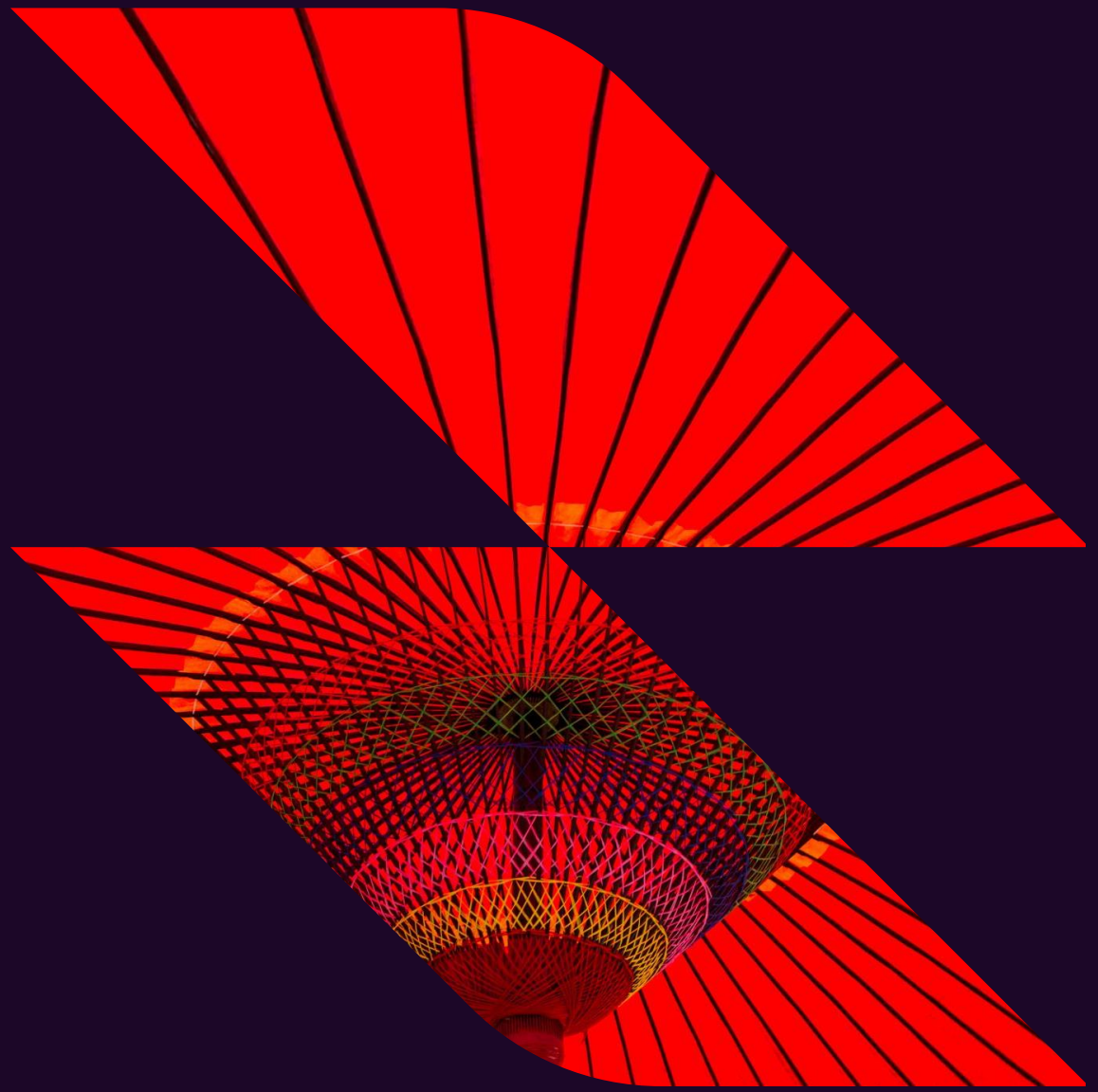


Administration platforms
- Dev workstations
- Credentials in config files

Connected Cloud environments

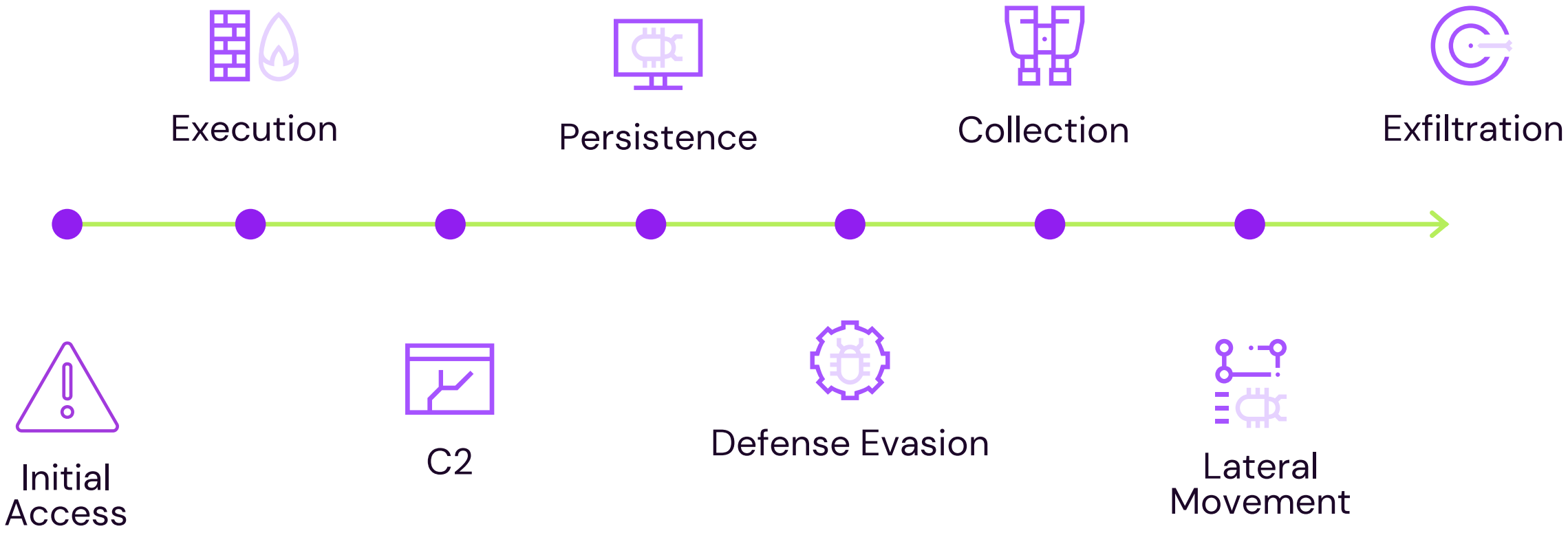
- Storage
- IAM roles / Service principals

Part 2: RED



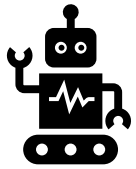
Simulating the attackers

Attack Lifecycle



Initial Access

Human Users

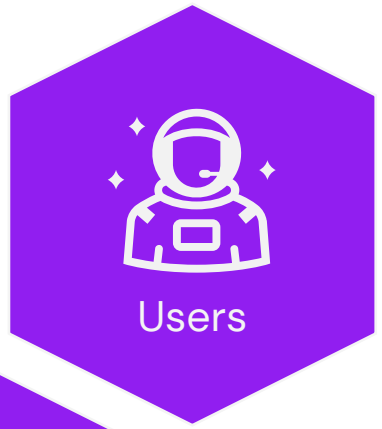


Service Account

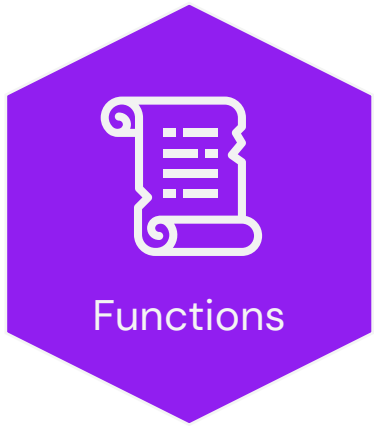
Passwords	• Password spraying • Brute forcing
Federated Access	• Compromise SSO • Cookie theft
Access tokens	• Steal from config files
RSA Key OAuth	• From files • Cloud env

Persistence

Will require high privileges



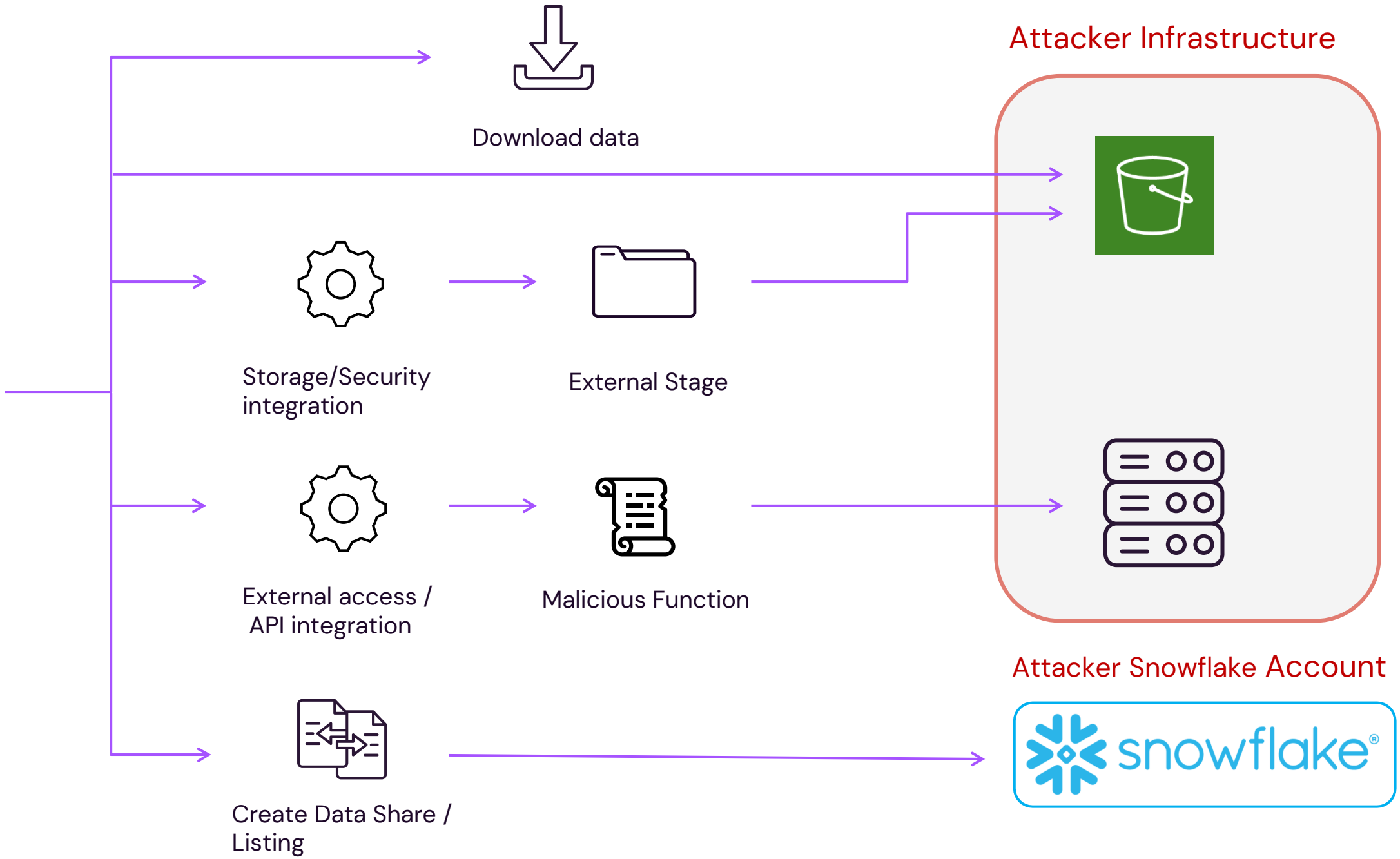
- Change password
- Add MFA method
- Add backdoor users



- Upload python/Java code
- Execute on a schedule

- Change network polices
- Disable defences

Exfiltration



STRIFEBOT

Repo of pre-written attack queries, Terraform templates, and guides to conduct purple teams against Snowflake accounts

```
├── playbooks
│   ├── blue
│   │   └── README.md
│   ├── README.md
│   ├── red
│   │   ├── 00_general.md
│   │   ├── 01_initial_access.md
│   │   ├── 02_discovery.md
│   │   ├── 03_persistence.md
│   │   ├── 04_privesc.md
│   │   ├── 05_defense_evasion.md
│   │   ├── 06_credential_access.md
│   │   ├── 07_collection.md
│   │   ├── 07_exfiltration.md
│   │   ├── 09_impact.md
│   │   ├── images
│   │   └── README.md
│   └── snowflake_for_beginners.md
```

https://github.com/reversecLabs/strifebot

Part 2: BLUE

Preventative vs Detective controls

Preventative: Stop attackers accomplishing objectives

- Ensuring IAM controls
- Strong passwords, secure credentials at rest, MFA
- Restrict egress
- Tokenise sensitive data

Detective: Catching attackers who do compromise the environment

- Ensure logs are being ingested and processed!
- Monitor login and authentication behaviour
- Create alerts for known attacker actions:
  - Persistence
  - Data exfil
  - . . .
- Use dashboards and visualisations to triage activity
- Behavioural Analysis (UBA): baseline typical user behaviour

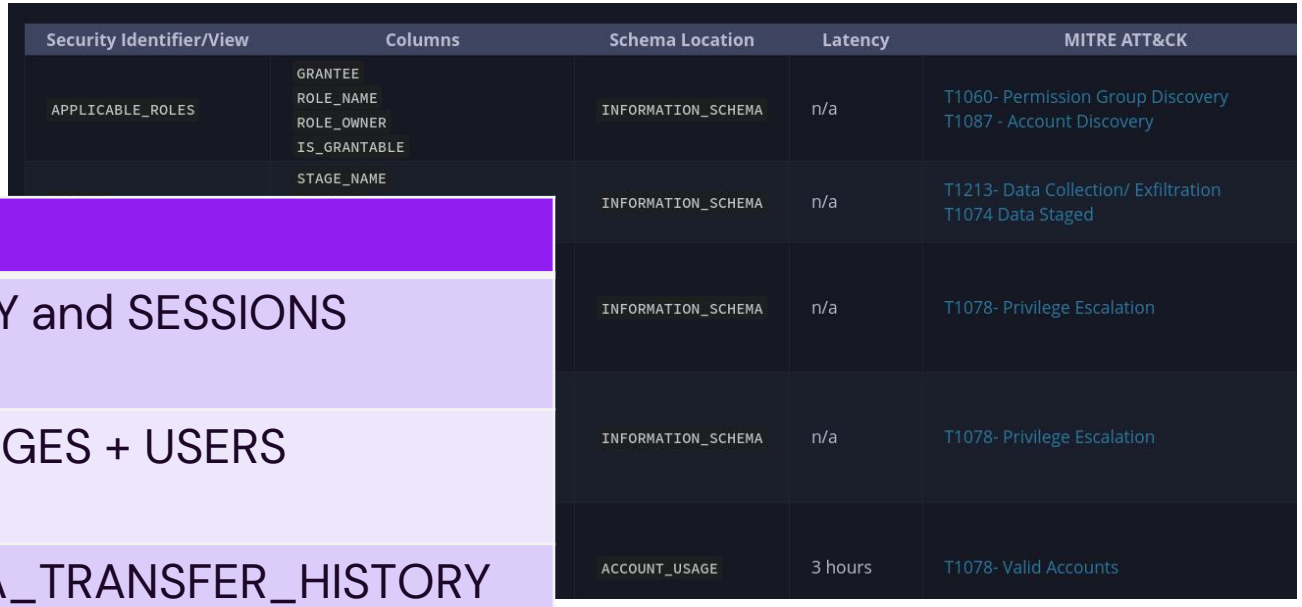
https://snowflake-labs.github.io/Sentry/reference/control-mapping.html

Log Sources

- https://snowflake-labs.gith
- https://quickstarts.snowflake.com/guide/security_dashboards_for_snowflake/index.html#0ub.io/Sentry/reference/log-sources.html

Key events

Attacker Technique	Log Tables
Initial Access	LOGIN_HISTORY and SESSIONS
Persistence / Privilege Escalation	USAGE_PRIVILEGES + USERS
Exfiltration	STAGES + DATA_TRANSFER_HISTORY
All	QUERY_HISTORY

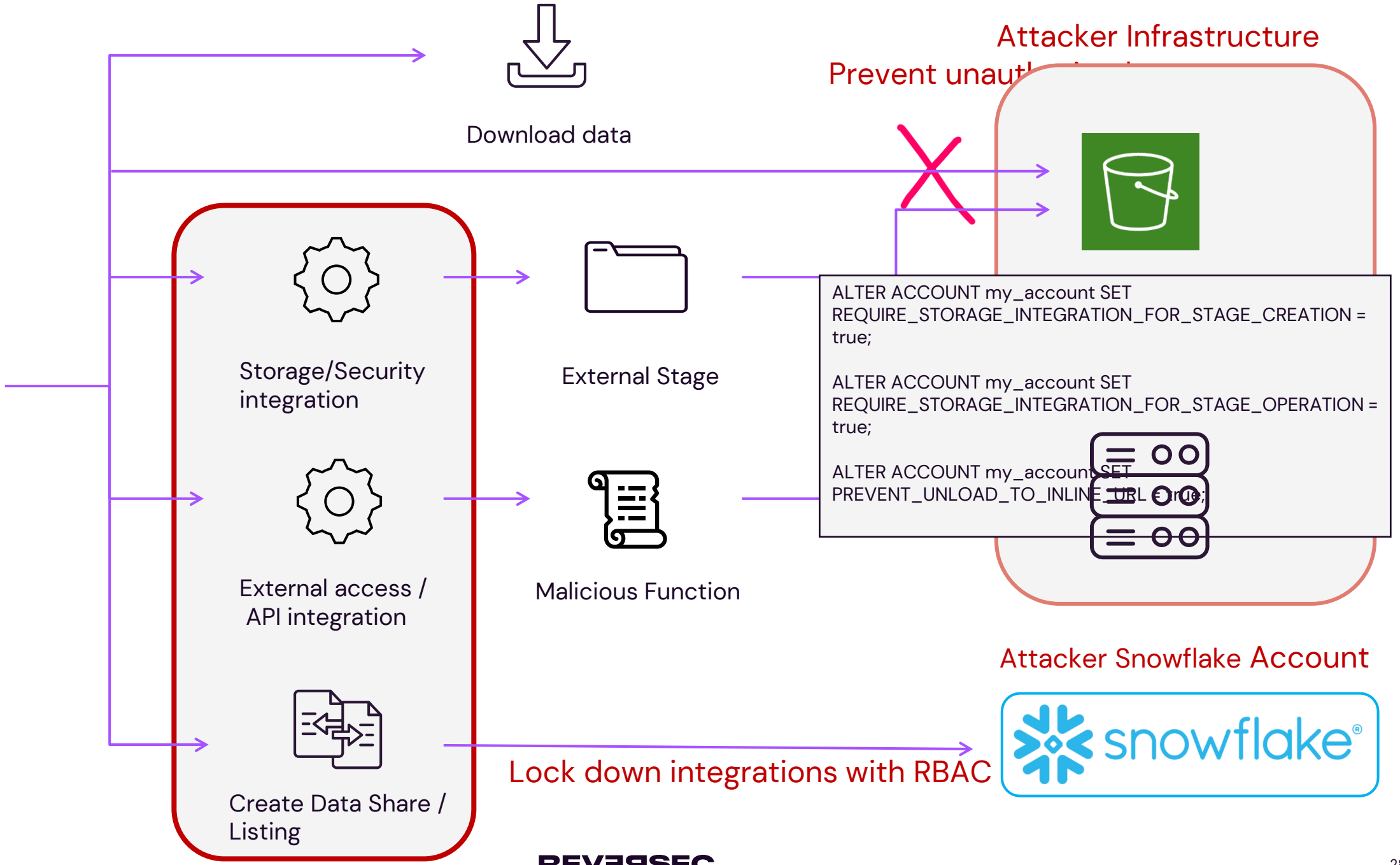


Security Identifier/View	Columns	Schema Location	Latency	MITRE ATT&CK
APPLICABLE_ROLES	GRANTEE ROLE_NAME ROLE_OWNER IS_GRANTABLE	INFORMATION_SCHEMA	n/a	T1060- Permission Group Discovery T1087 - Account Discovery
	STAGE_NAME	INFORMATION_SCHEMA	n/a	T1213- Data Collection/ Exfiltration T1074 Data Staged
		INFORMATION_SCHEMA	n/a	T1078- Privilege Escalation
		INFORMATION_SCHEMA	n/a	T1078- Privilege Escalation
		ACCOUNT_USAGE	3 hours	T1078- Valid Accounts

Initial Access

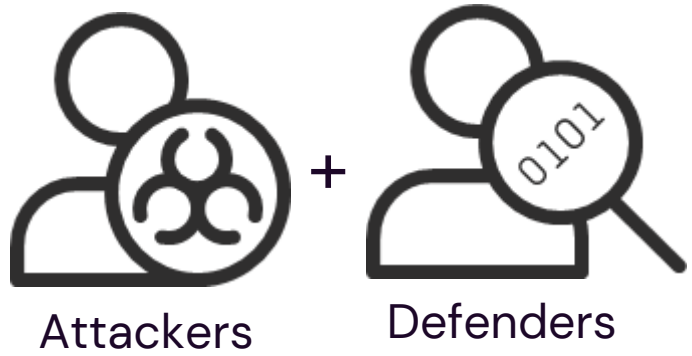
- Ensure admin workstations are protected, e.g from malware and credential harvesting
  - SACLs on config files to monitor reads
- Ensure CI/CD systems have protections to prevent IaC modification
- IP restrictions in snowflake
- Federated access
- Password policies + MFA for non-federated human accounts
- Protect static credentials
  - SP Ouath secrets

Exfiltration



Summary

- Datalakes such as Snowflake are becoming targets for attackers
- Conducting purple teams can allow you to stress test your defences
- For complex platforms, break up purple teams into phases:



- Construct an attack, execute against Snowflake environment
- Use findings to improve defences and detections

Thanks for listening!

References:

https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion/

https://snowflake-labs.github.io/Sentry/reference/queries.html

https://github.com/pushsecurity/saas-attacks/

https://www.snowflake.com/en/blog/how-to-configure-a-snowflake-account-to-prevent-data-exfiltration/

Slides

Questions? I can be contacted at
hendo@reversec.com

REVERSEC