F-Secure | LABS

LESSONS LEARNED ON ATTACK DETECTION IN THE CLOUD

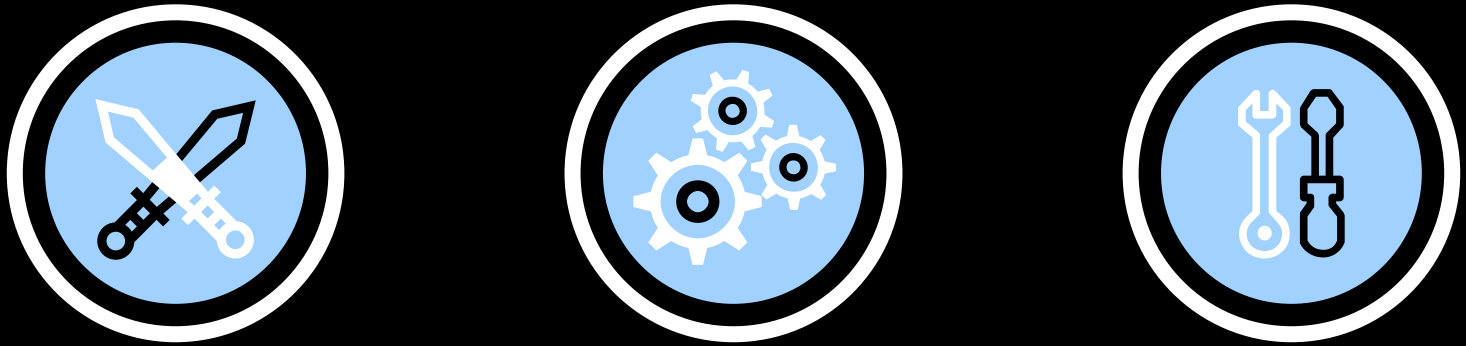
Nick Jones – ISF Denmark – September 2021

WHO AM I?

Nick Jones

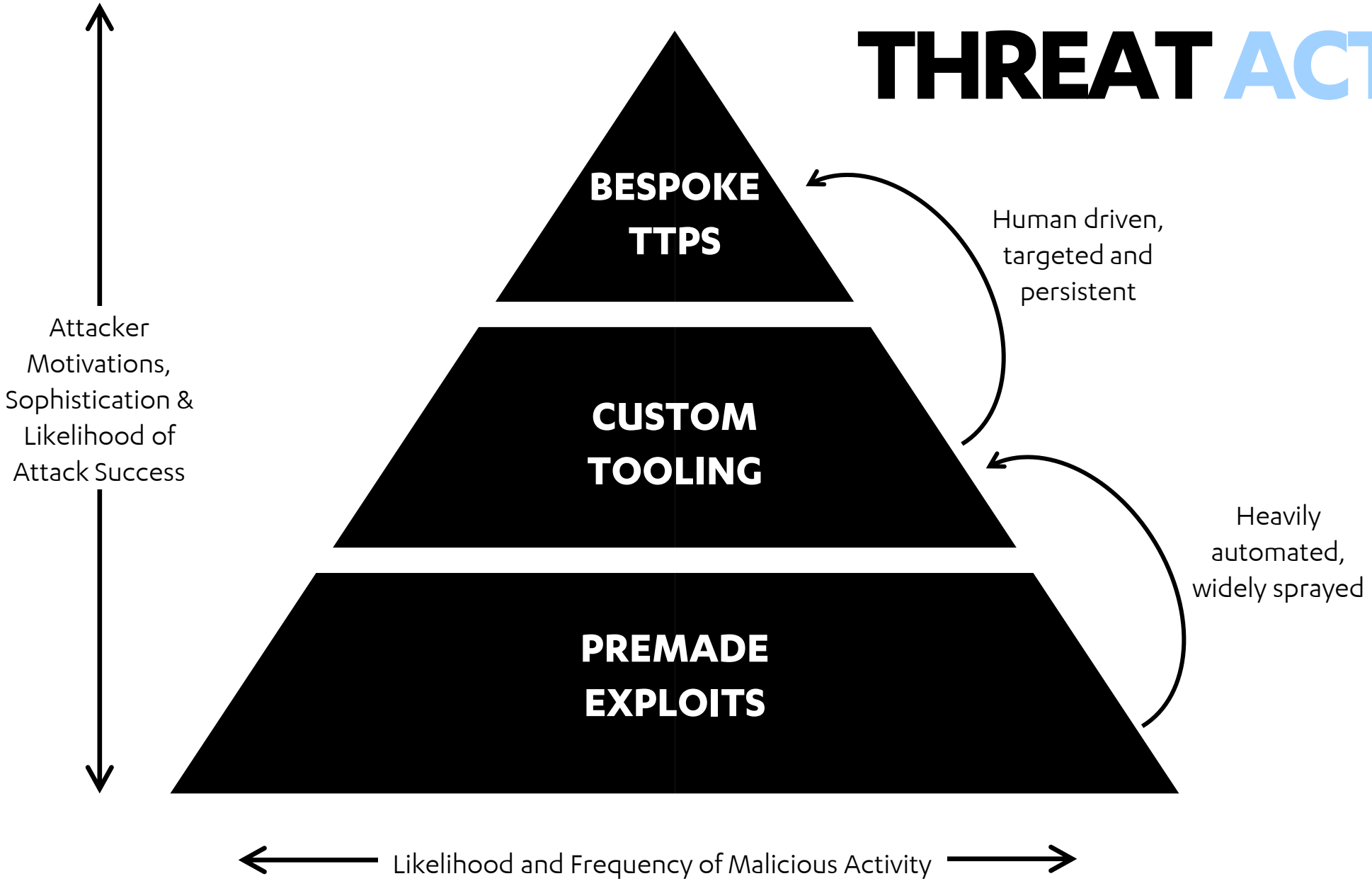
- Senior Security Consultant @ F-Secure
- Global cloud security lead
- Working on:
  - Attack Detection
  - Cloud security at scale
  - DevSecOps & security automation

AGENDA



LABS

THREAT ACTORS



F-Secure | LABS

ON-PREMISE VS CLOUD

HOW CLOUD DETECTION DIFFERS

UNCERTAINTY OF MALICIOUS INTENT

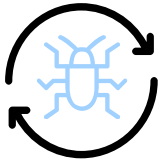
Fewer actions in the cloud are obviously bad compared to on-premise, making generic detection rules harder

CONTEXT IS KEY

Anomalies will vary by environment. Behavioral analytics are important here, so is developing environment-specific alerting.

GAINING VISIBILITY IS EASIER

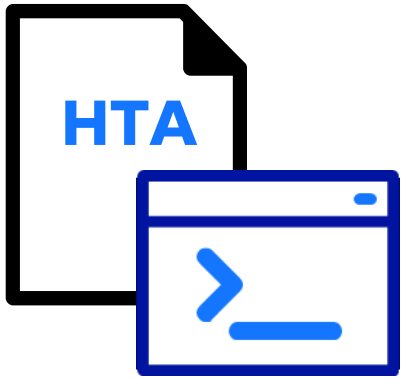
Org-wide CloudTrail, etc. makes it easier to gain visibility into much of your estate. Shadow IT now the primary issue, rather than coverage of known assets.

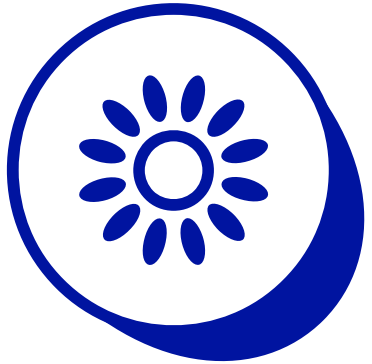


ATTACKERS ARE AUTOMATING

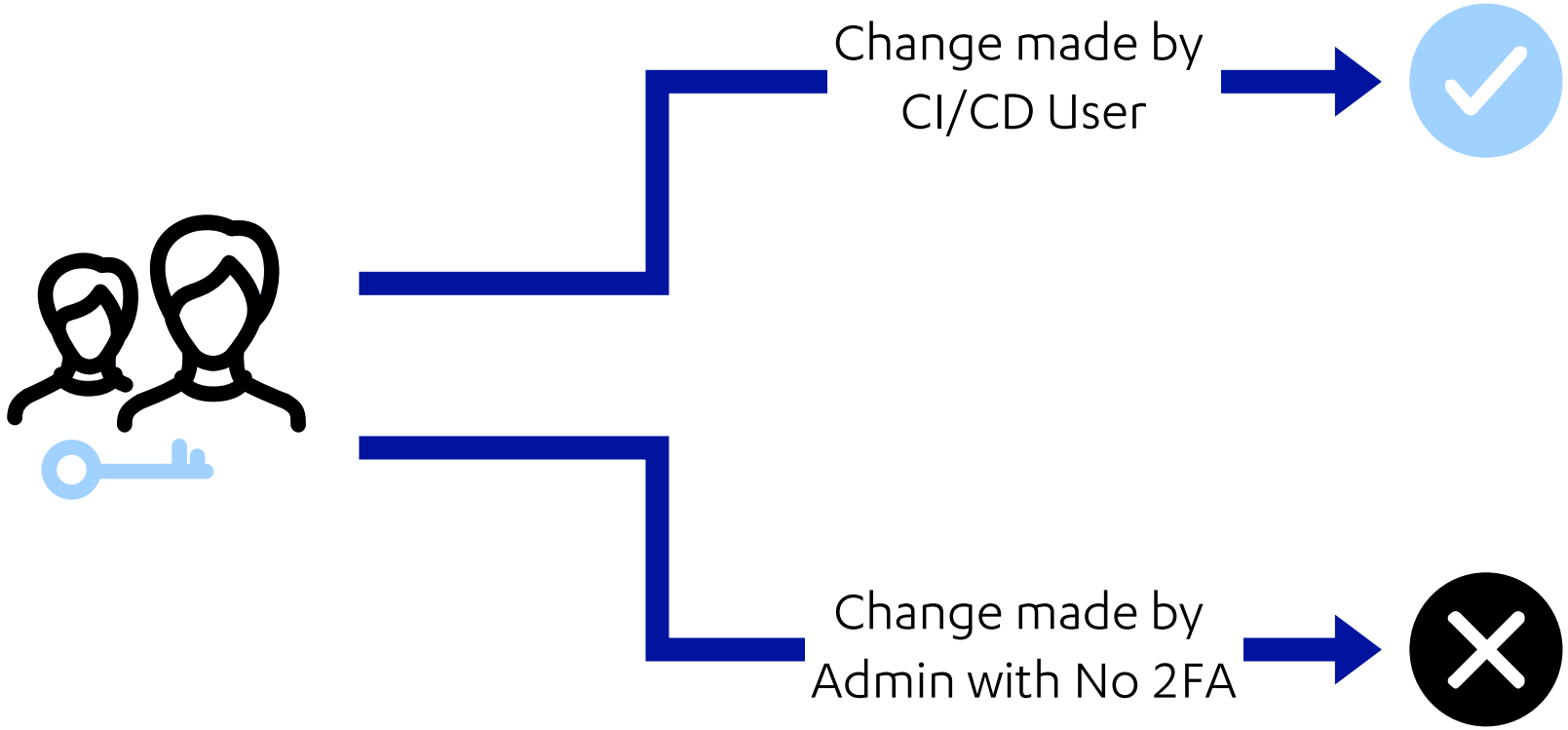
Attackers leveraging scripted attacks to abuse stolen credentials for cryptocurrency mining. With an API-driven attack surface by-design, it's easier to automate targeted attacks too.

MINDSET SHIFT



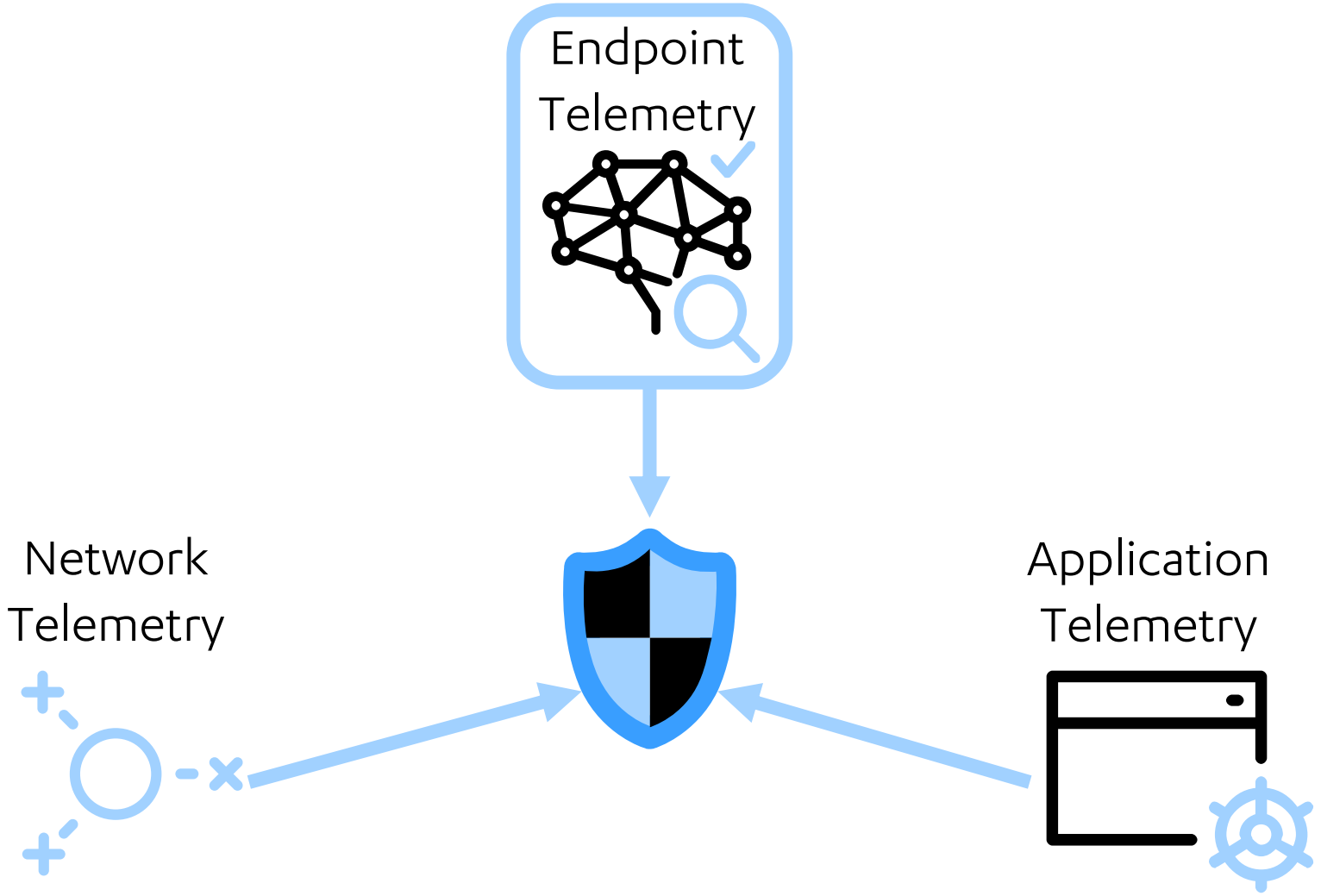


CONTEXT IS KEY



LABS

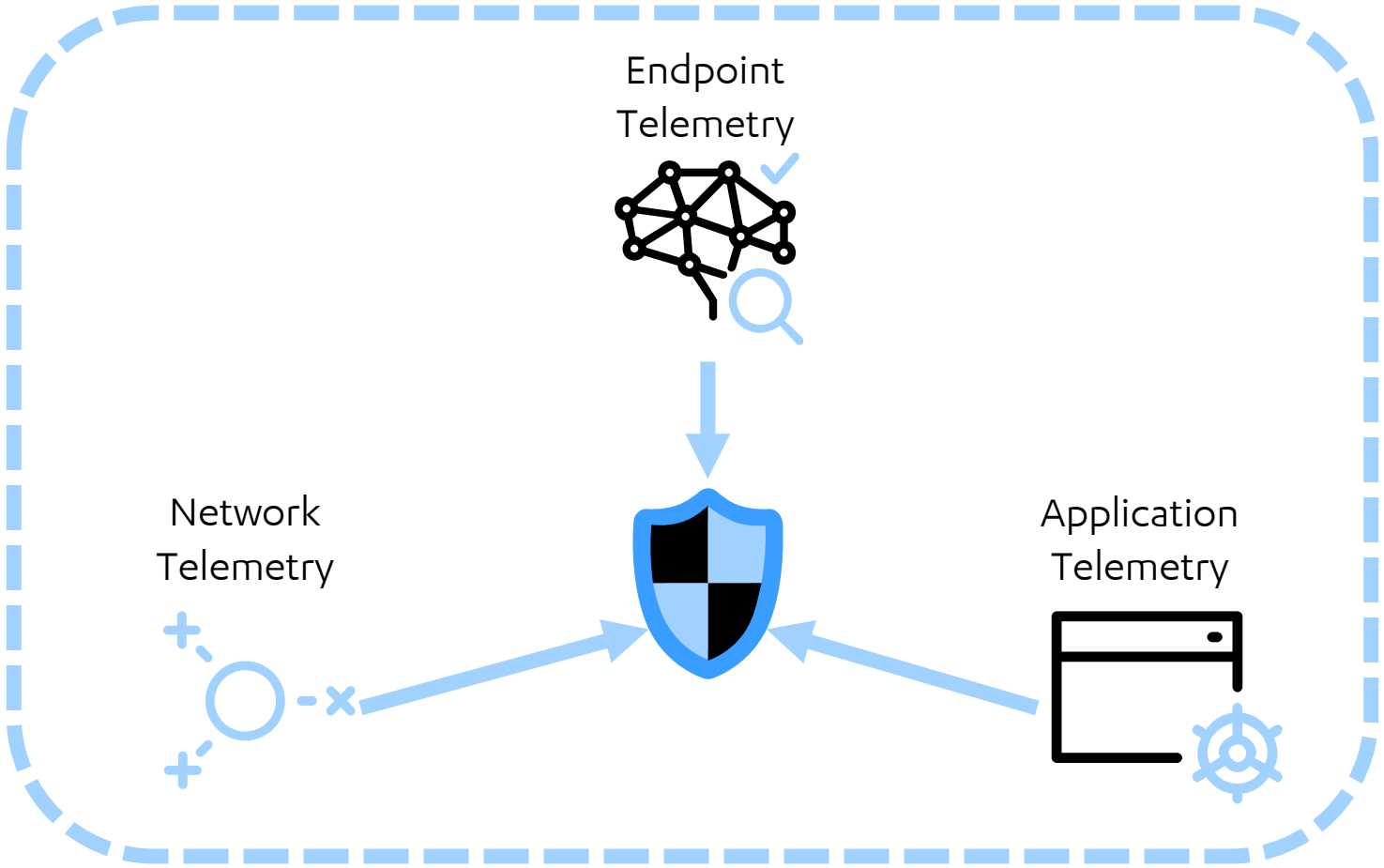
ON-PREMISE TELEMETRY



LABS

CLOUD TELEMETRY

Control Plane Telemetry

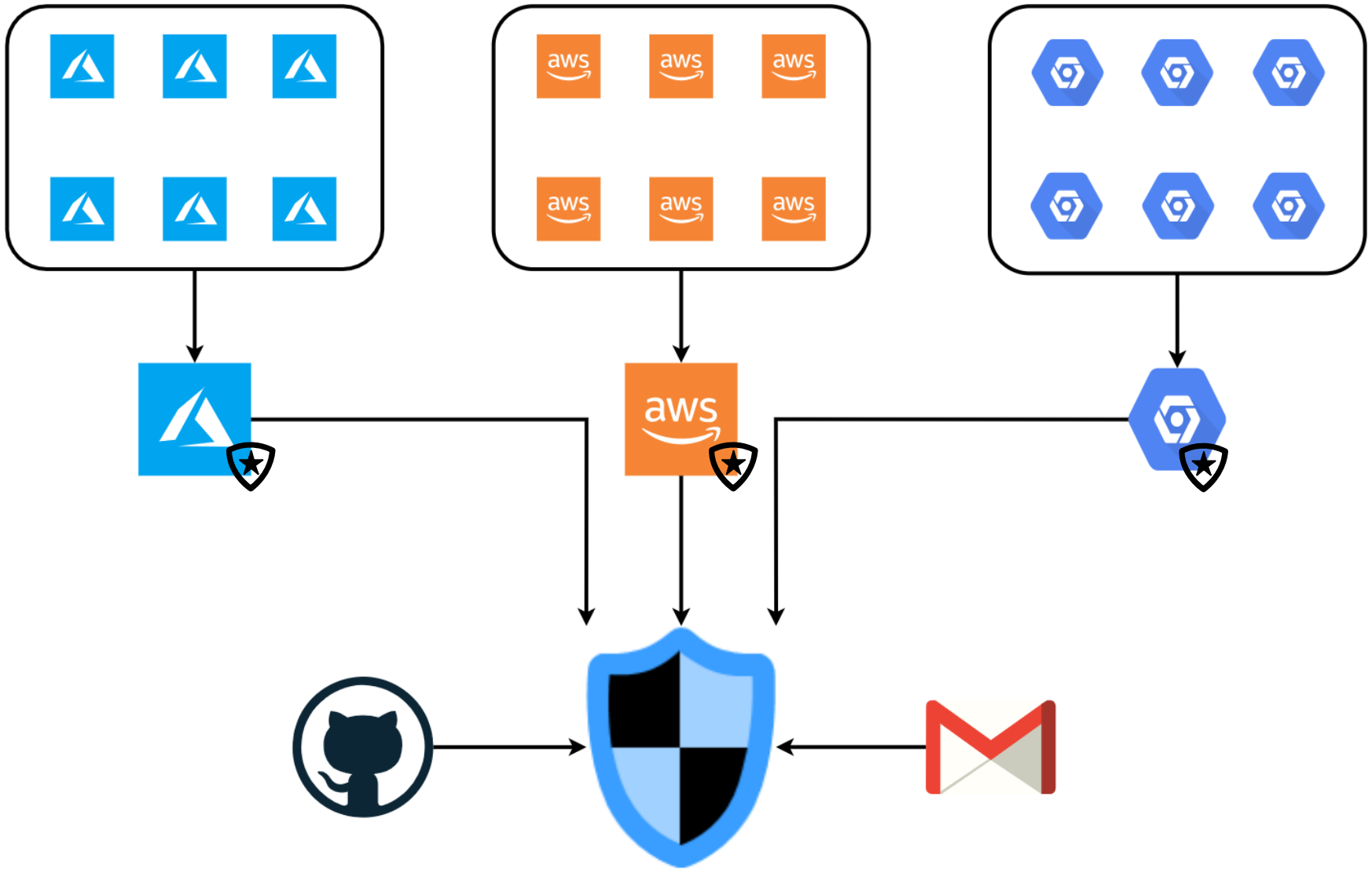


F-Secure | LABS

DESIGNING YOUR CLOUD DETECTION STACK

LABS

CENTRALISE EVERYTHING



LABS

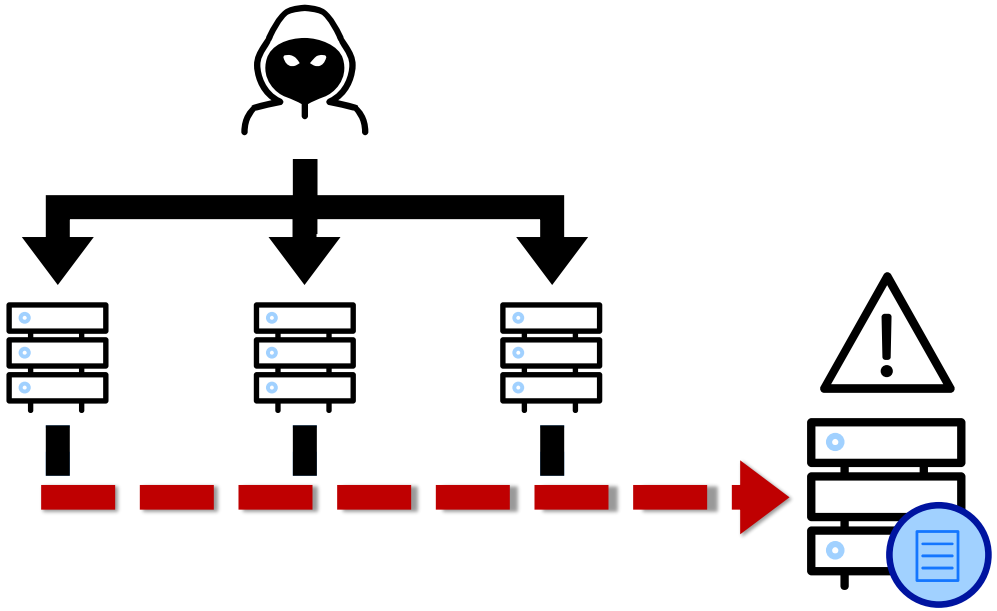
DATA SOURCES

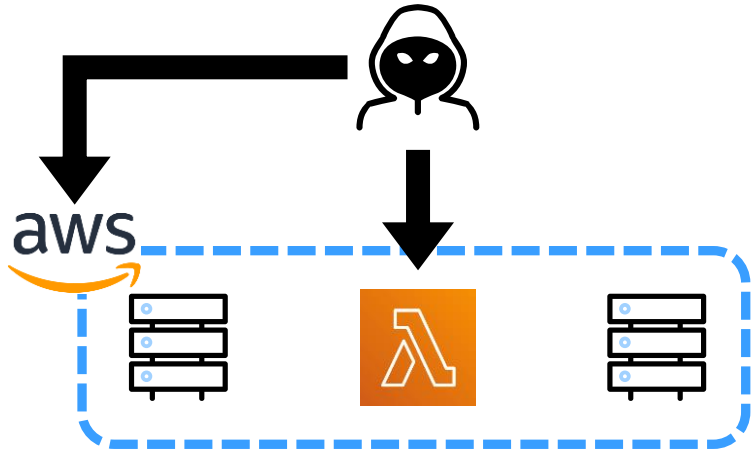
SOURCE	BENEFIT
Control Plane audit logs (CloudTrail, Audit Log etc)	**Visibility of all administrative actions**
Cloud-native detection services	Detection of known bad activity
API Gateway/WAF Logs	Identify malicious requests to applications
Network flow logs	Identify anomalous traffic by source and destination, volumes etc
System logs from any VMs	Grants OS-level visibility of potential attacker activity
Endpoint Detection and Response agents in VMs	Detects malicious activity within VMs as with on premise estates
Application logs	Provides app-specific contextual information
Service Specific Logs (storage access logs, function executions, KMS key access etc)	Shows access and usage of specific resources and services, which may help to track lateral movement or actions on objective

F-Secure | LABS

THE THREAT INTELLIGENCE PROBLEM

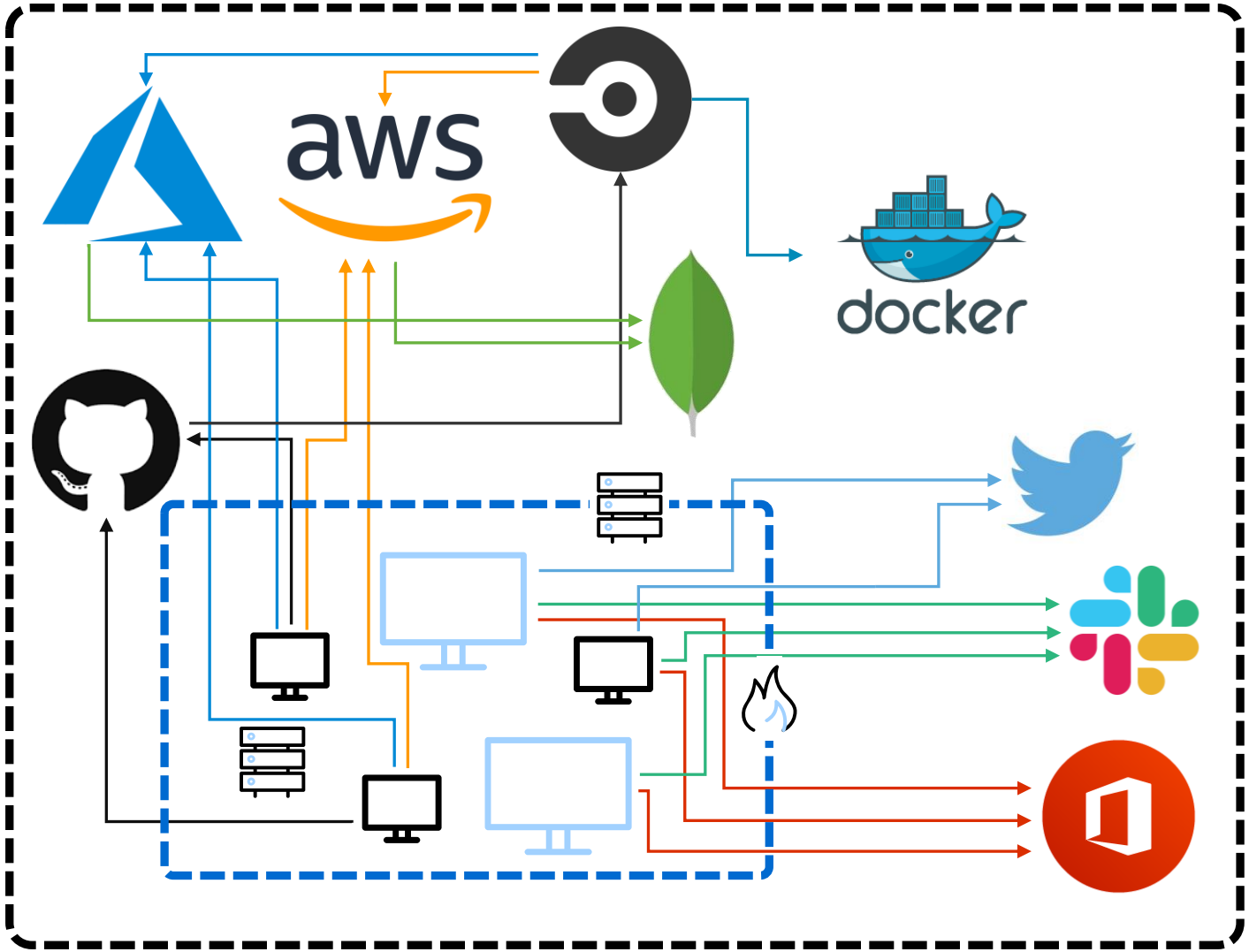
ON-PREMISE VS CLOUD DETECTION





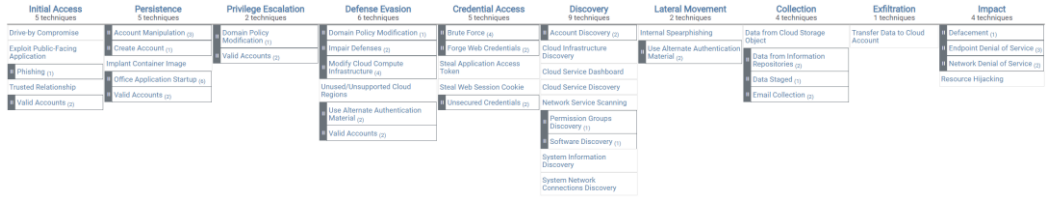
LABS

ENTERPRISE CLOUD ADOPTION



LABS

ENTERPRISE VS CLOUD ATT&CK



MITRE ATT&CK™

Retrieved 11th February 2020

F-Secure | LABS

WHAT'S AN ATTACKER LIKELY TO DO?

LABS

VECTORS WE'VE EXPLOITED

Identity Management

- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials

Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.

Application Vulnerabilities

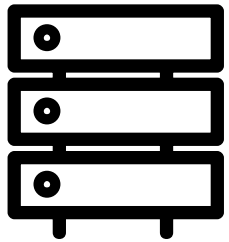
- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

LABS

VECTORS WE'VE EXPLOITED

Identity Management

- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials



Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.

Application Vulnerabilities

- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

LABS

VECTORS WE'VE EXPLOITED

Identity Management

- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials

Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.

Application Vulnerabilities

- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

LABS

VECTORS WE'VE EXPLOITED

Identity Management

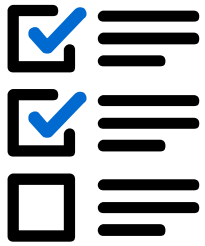
- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials

Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.



Application Vulnerabilities

- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

HOW DO I START?

01 Threat model your environment, identify attack paths and likely attacker actions

02 Prioritise attack paths and actions

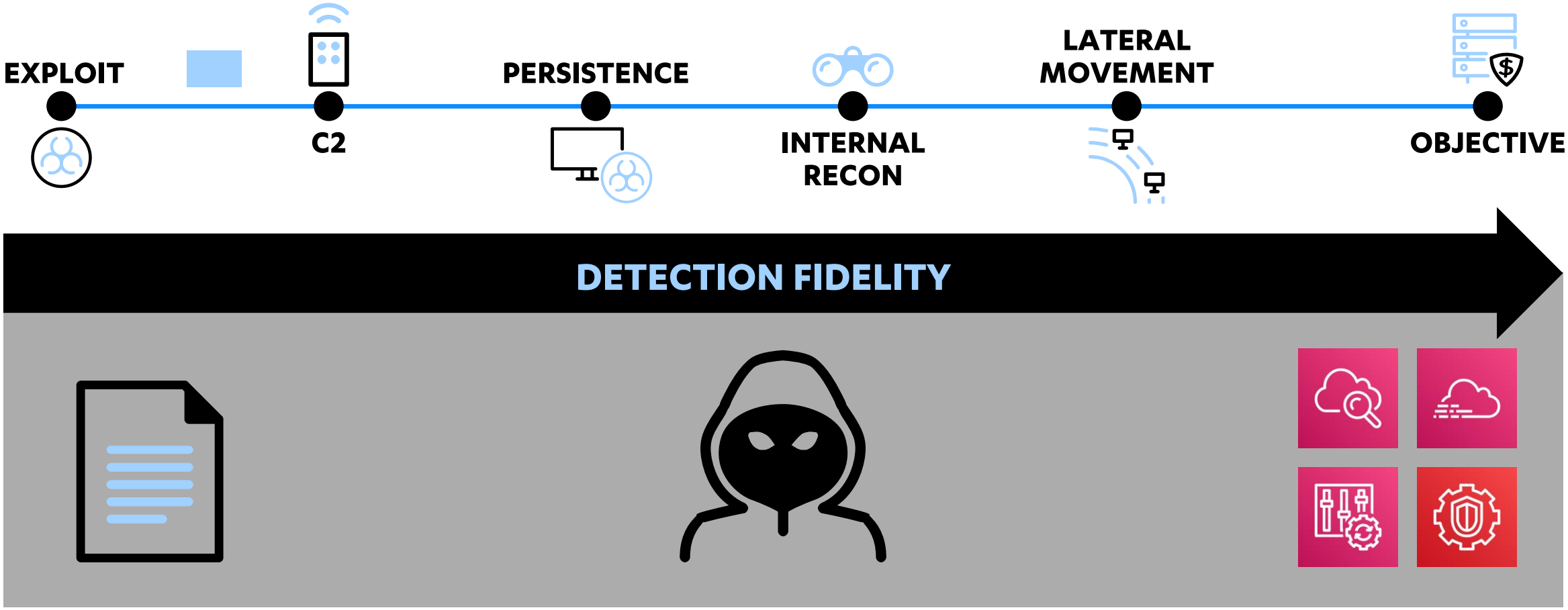
03 Pick the most important attack paths, codify them

04 Verify telemetry is available to defenders

05 Execute attacker actions as kill chains, verify detection cases work as expected.

LABS

WHERE DO I START?



LEARN FROM DEVOPS:
TREAT EVERYTHING AS CODE

Detection as code makes internal and external knowledge sharing easier

SIGMA (SIEM-agnostic rules) https://github.com/Neo23x0/sigma

Jupyter Notebooks https://posts.specterops.io/threat-hunting-with-jupyter-notebooks-part-1-your-first-notebook-9a99a781fde7

John Lambert – The Githubification of Infosec http://youtu.be/B3o-9z3Eitg https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1

F-Secure | LABS

LEONIDAS

LABS

LEONIDAS

Automated Attack Simulation

- Framework for defining, executing and detecting attacker TTPs in the cloud
- Execution and detection all defined as code
- TTPs linked to MITRE ATT&CK for easy correlation with TI/existing tooling

Framework automatically generates…

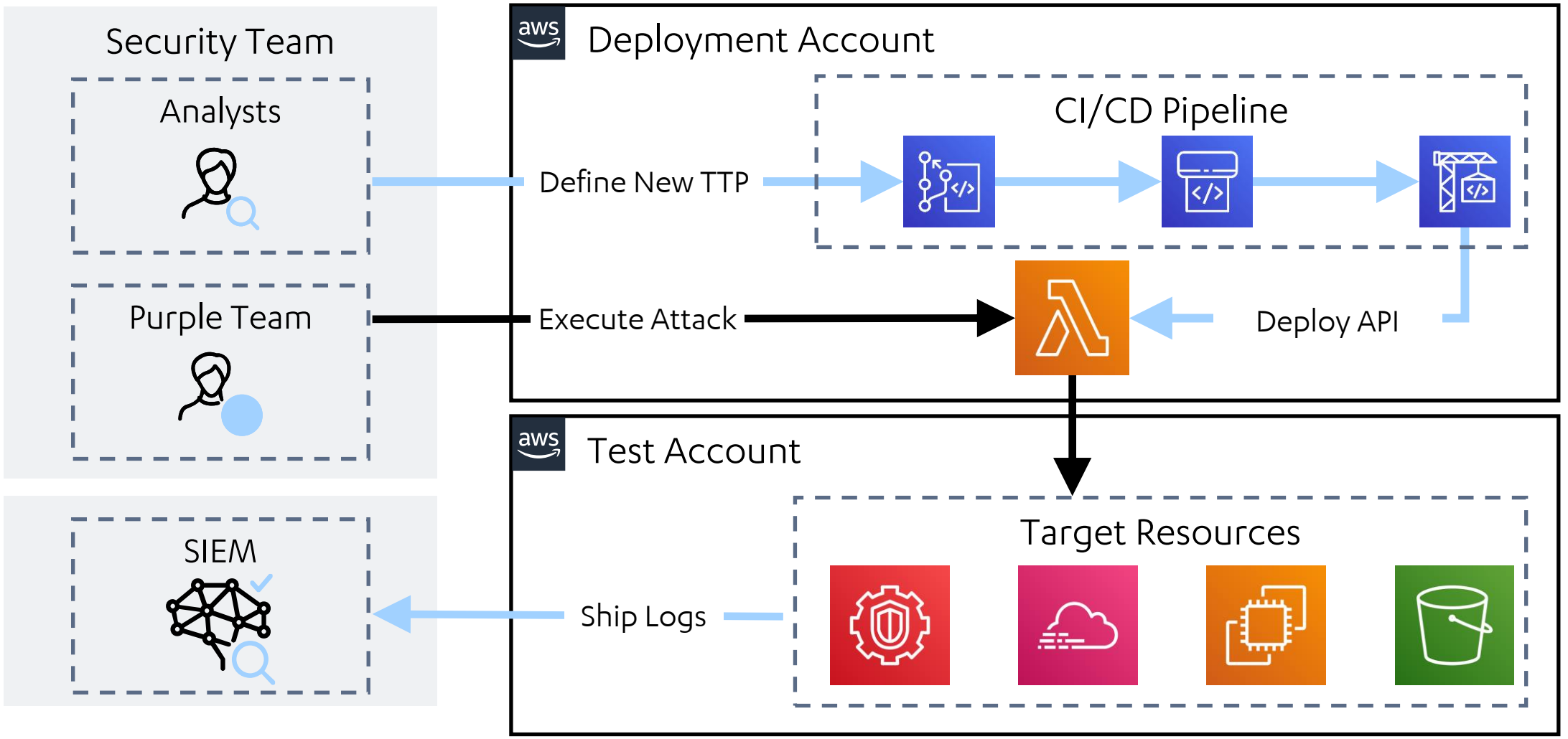
- Executor – serverless function
- Sigma detection rules
- Documentation

Executor

- Multi-cloud support in a single instance
- User/role/service account impersonation

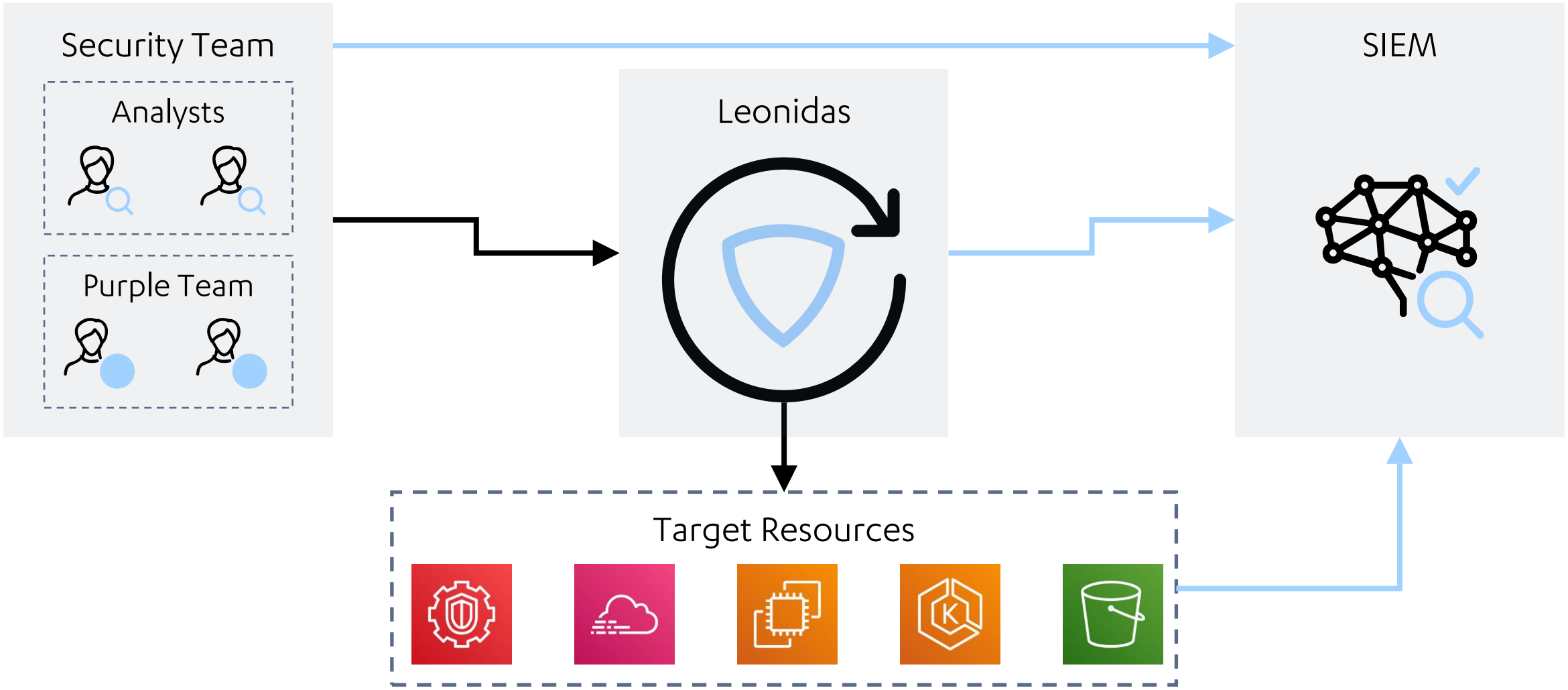
LABS

LEONIDAS



LABS

CONTINUOUS INTEGRATION

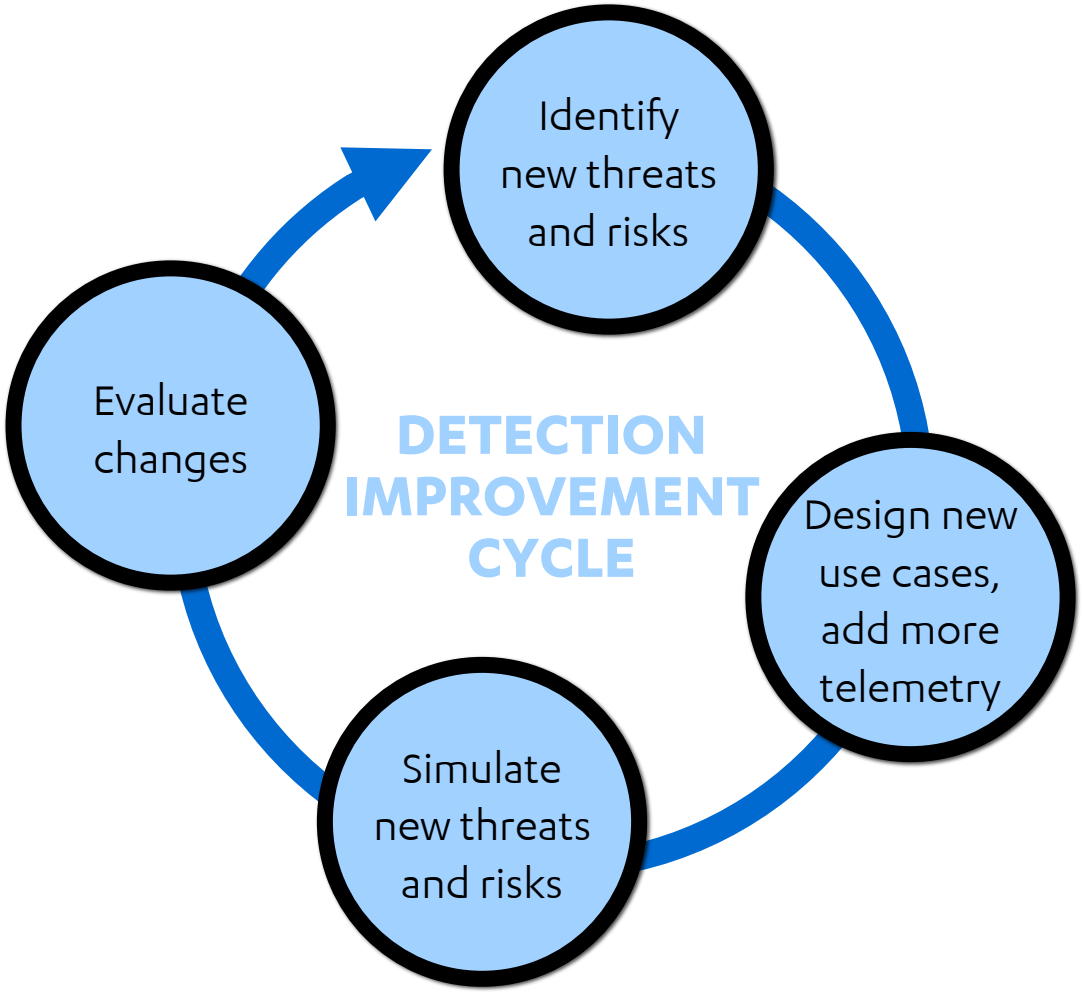


F-Secure | LABS

CONCLUSIONS

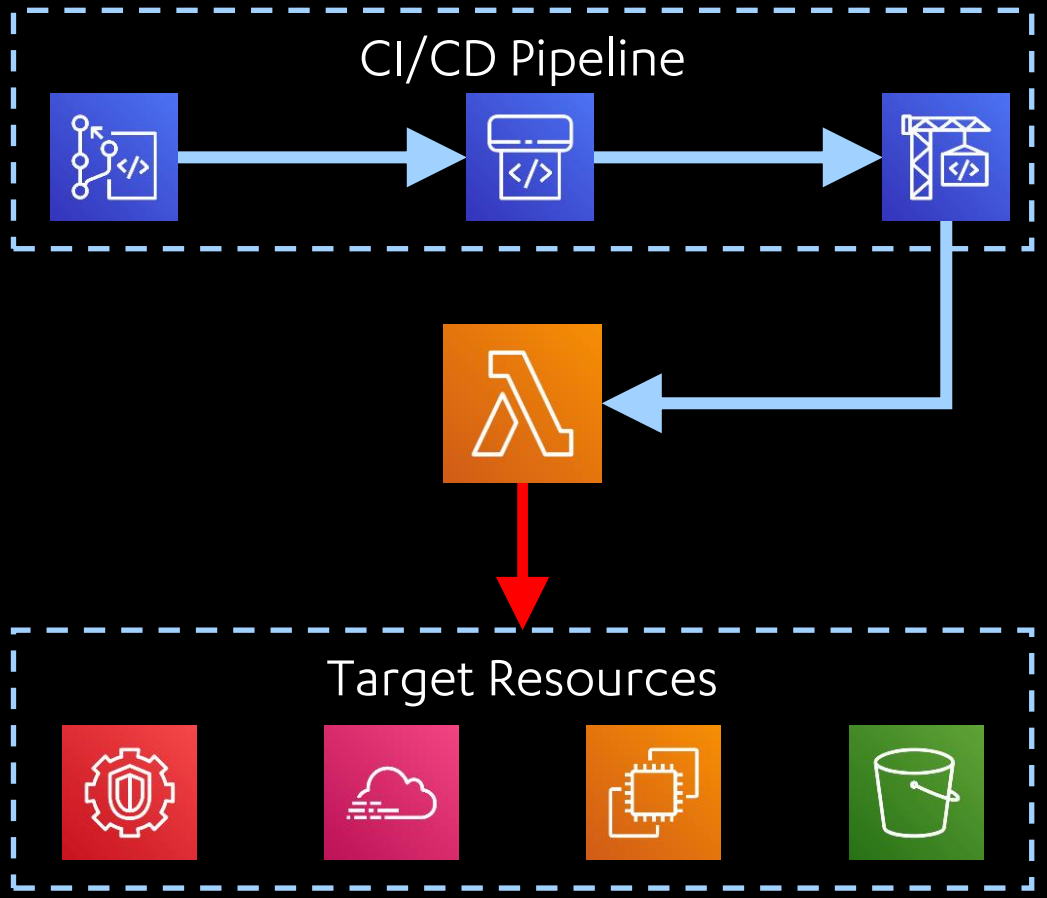
LABS

DETECTION IS A JOURNEY



- Context is key, use it to your advantage
- Cloud environments change, your detection will too
- Codify use cases (and attacks) to aid knowledge sharing

LEONIDAS



- Automate attacker actions in the cloud
- Both test and detection cases
- AWS support now, Azure/GCP on the roadmap
- 41 test cases - more to come
- https://github.com/fsecurelabs/leonidas