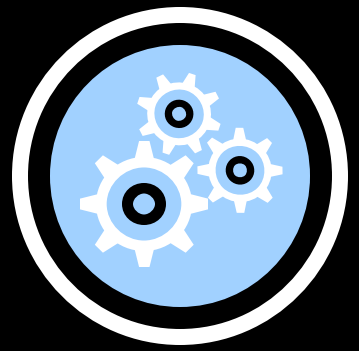
F-Secure | LABS

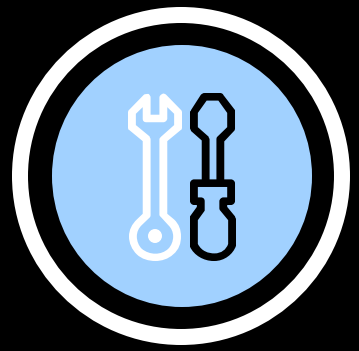
CLOUD-NATIVE ATTACK DETECTION AND SIMULATION

Nick Jones – DEF CON 28 Cloud Village

LABS

AGENDA

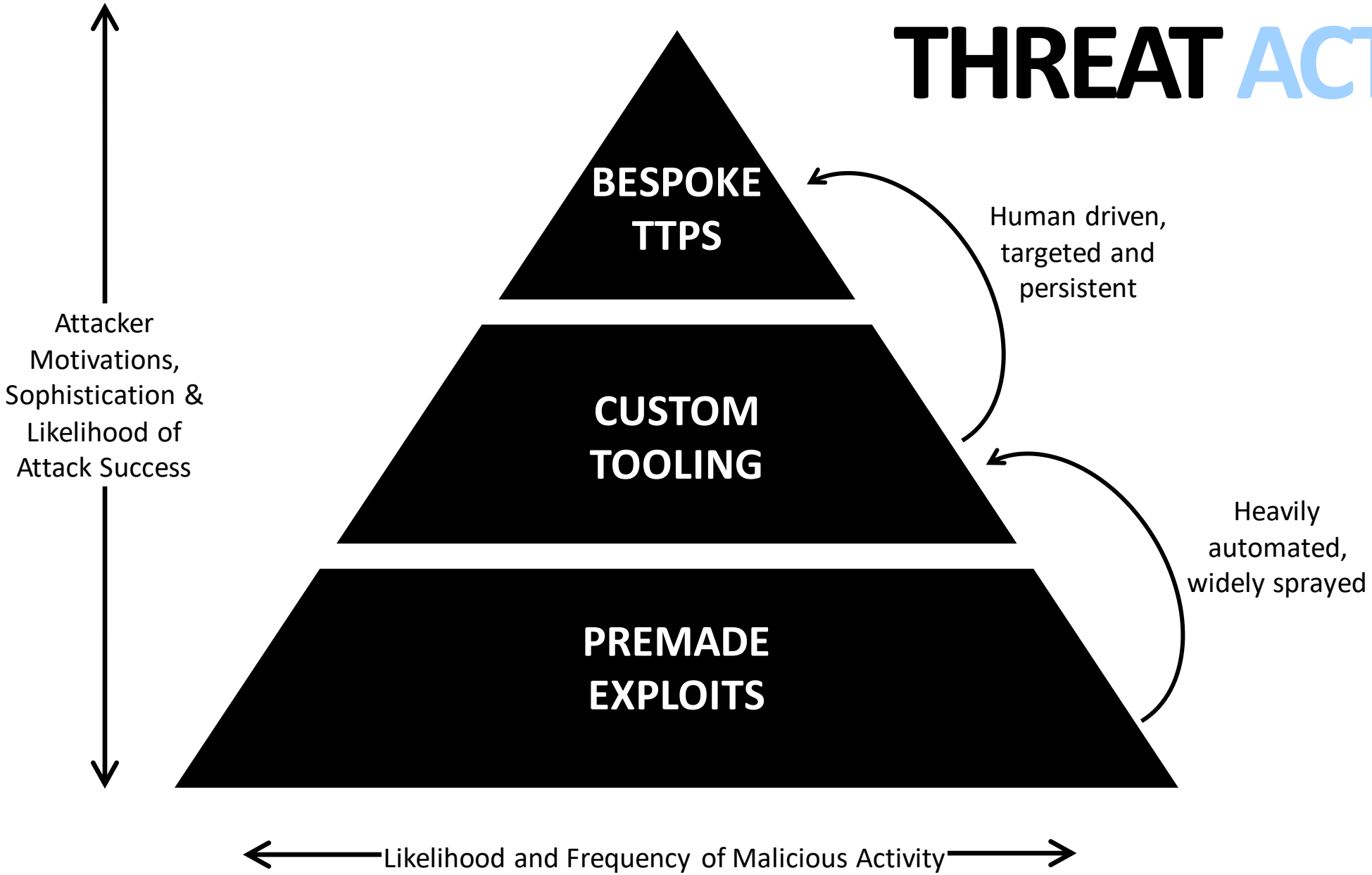




BRINGING DEVOPS TO DETECTION

LABS

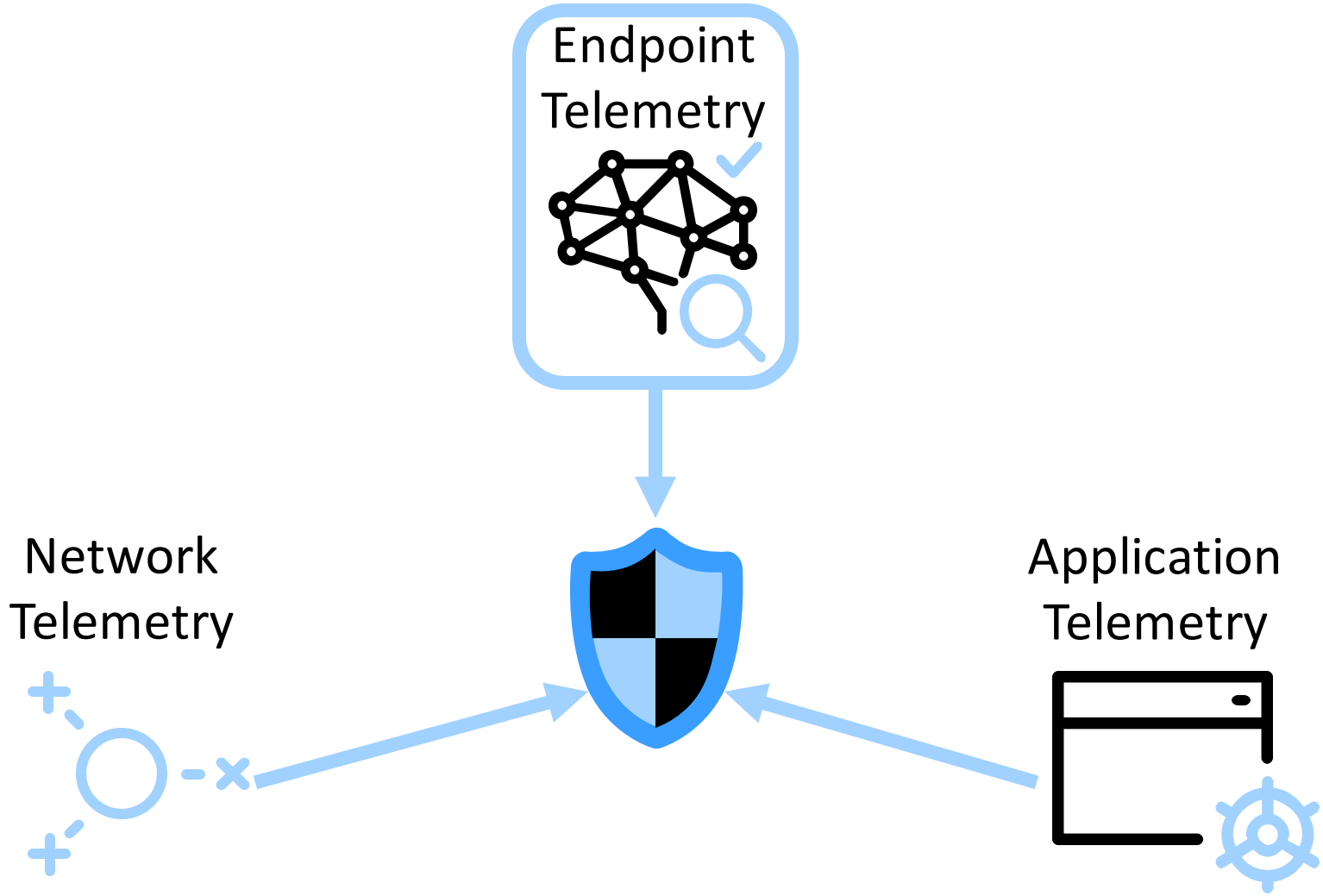
THREAT ACTORS



F-Secure | LABS

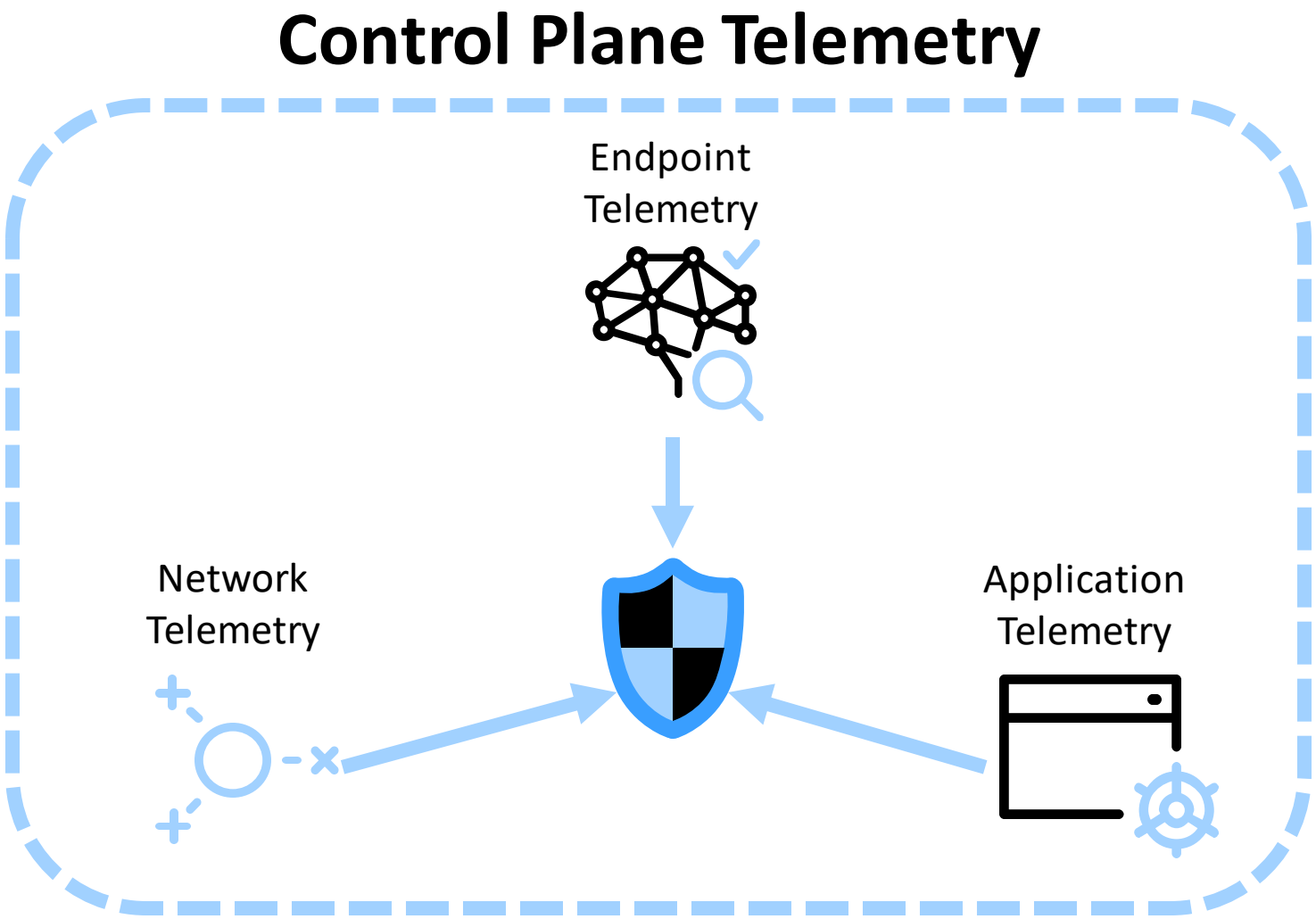
ON-PREMISE VS CLOUD

ON-PREMISE TELEMETRY



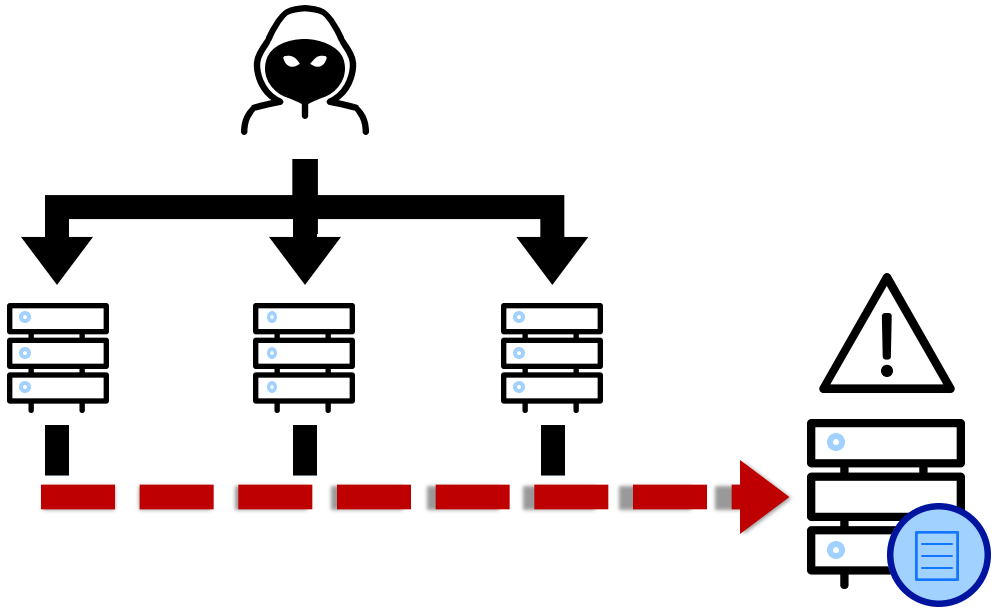
LABS

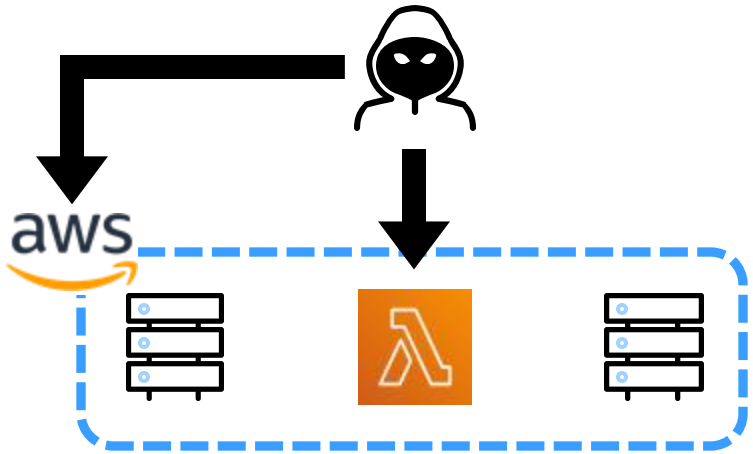
CLOUD TELEMETRY



LABS

ON-PREMISE VS CLOUD DETECTION





LABS

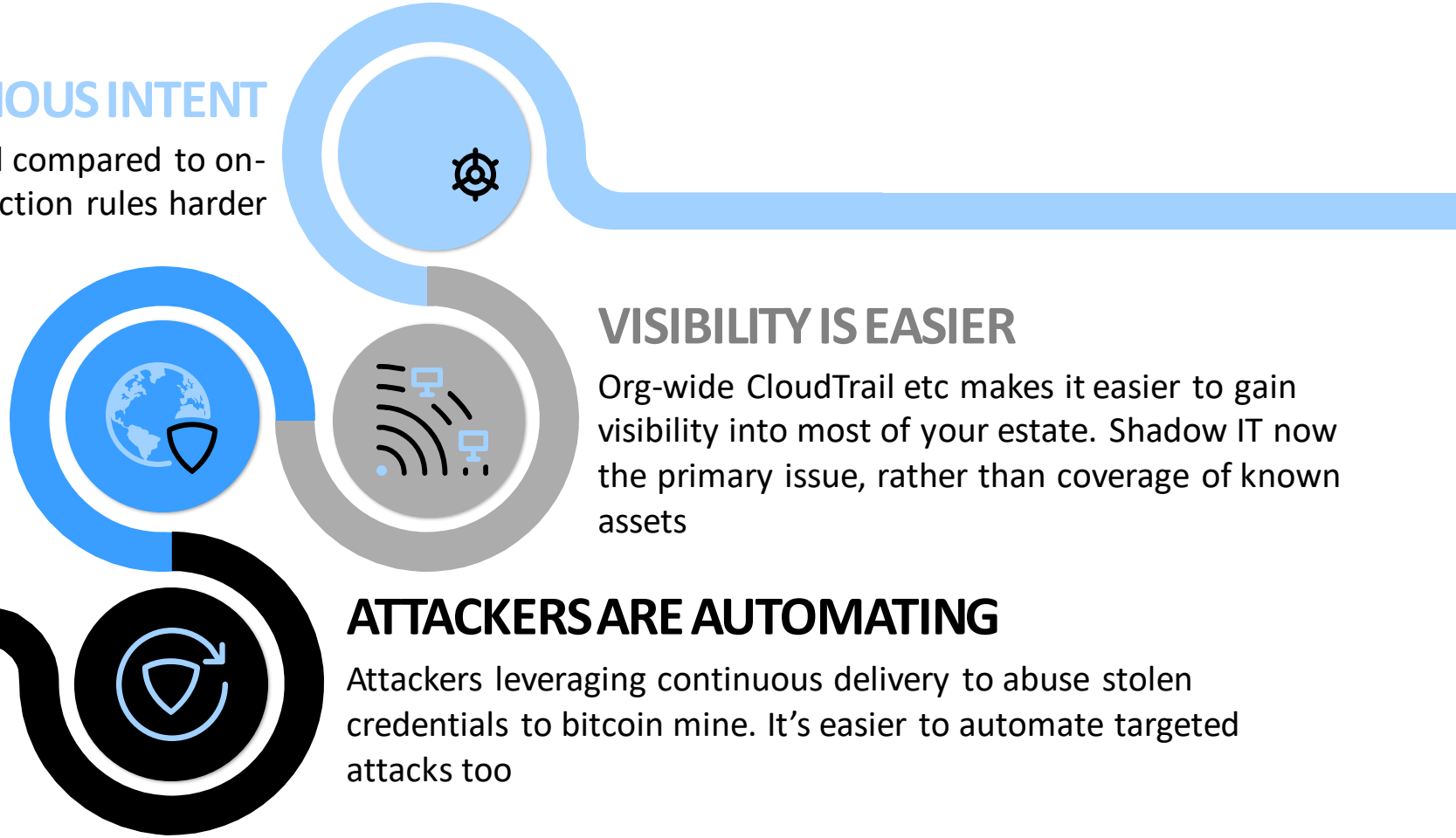
HOW CLOUD DETECTION DIFFERS

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 very important, but high end attackers will become context aware in time.



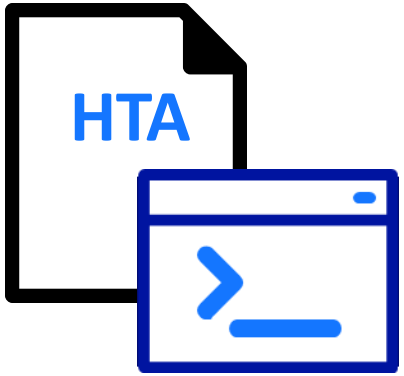
VISIBILITY IS EASIER

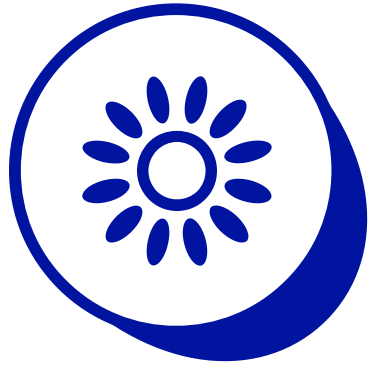
Org-wide CloudTrail etc makes it easier to gain visibility into most of your estate. Shadow IT now the primary issue, rather than coverage of known assets

ATTACKERS ARE AUTOMATING

Attackers leveraging continuous delivery to abuse stolen credentials to bitcoin mine. It's easier to automate targeted attacks too

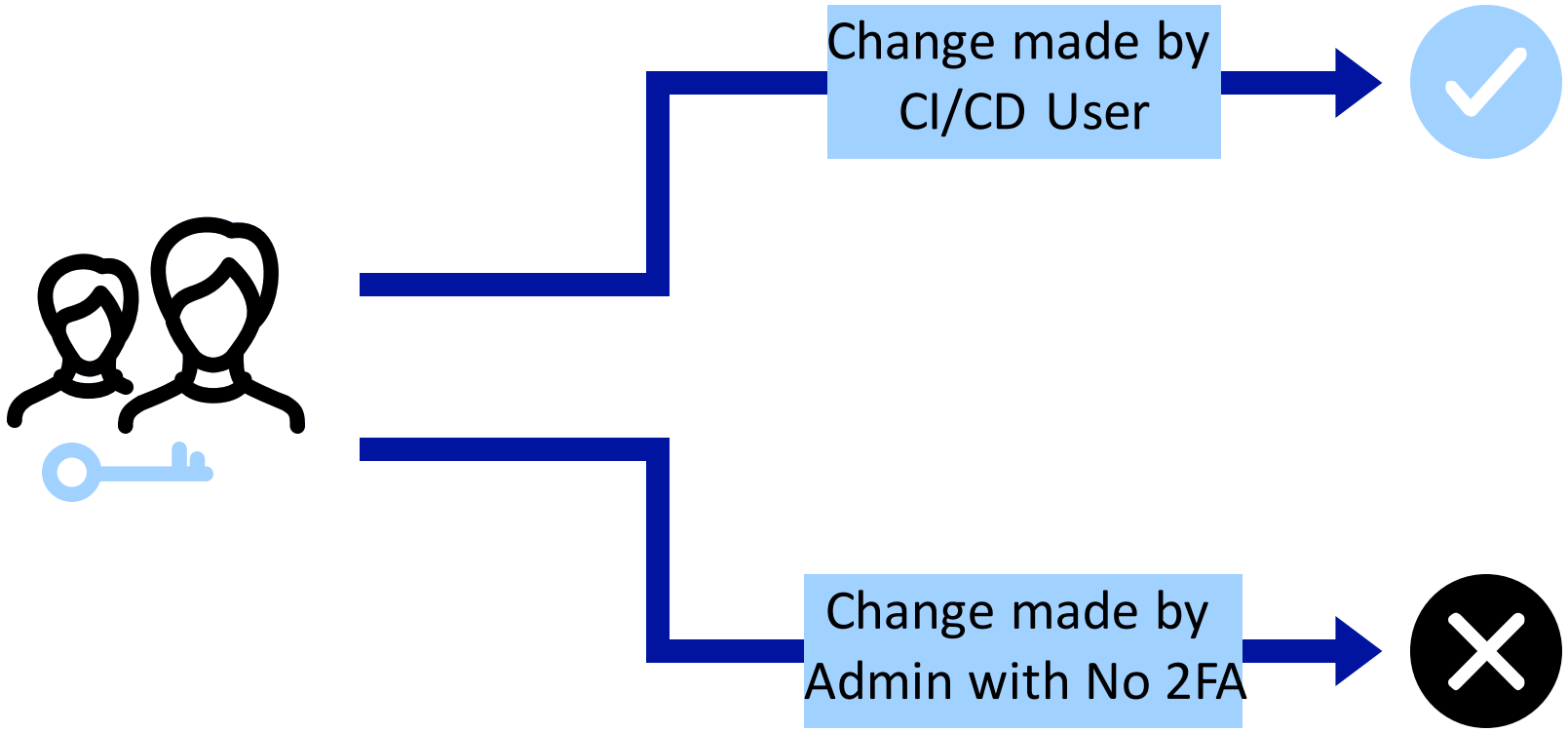
MINDSET SHIFT





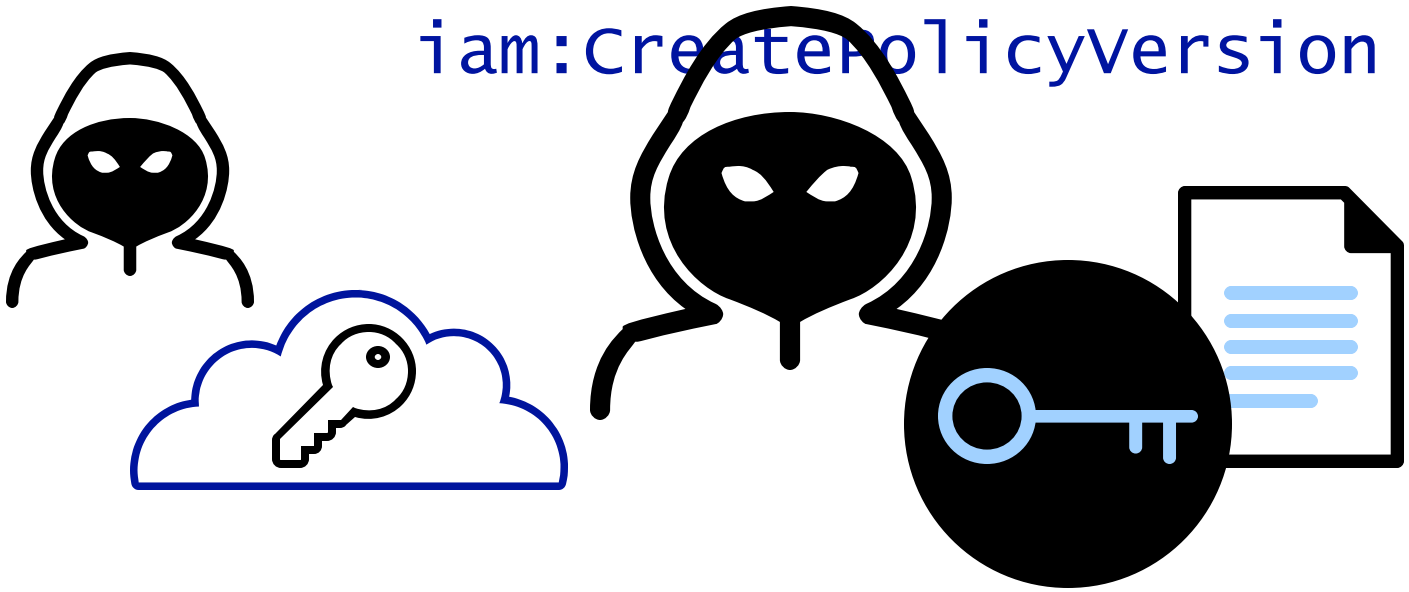
CERTAINTY OF MALICIOUS INTENT

CONTEXT IS KEY



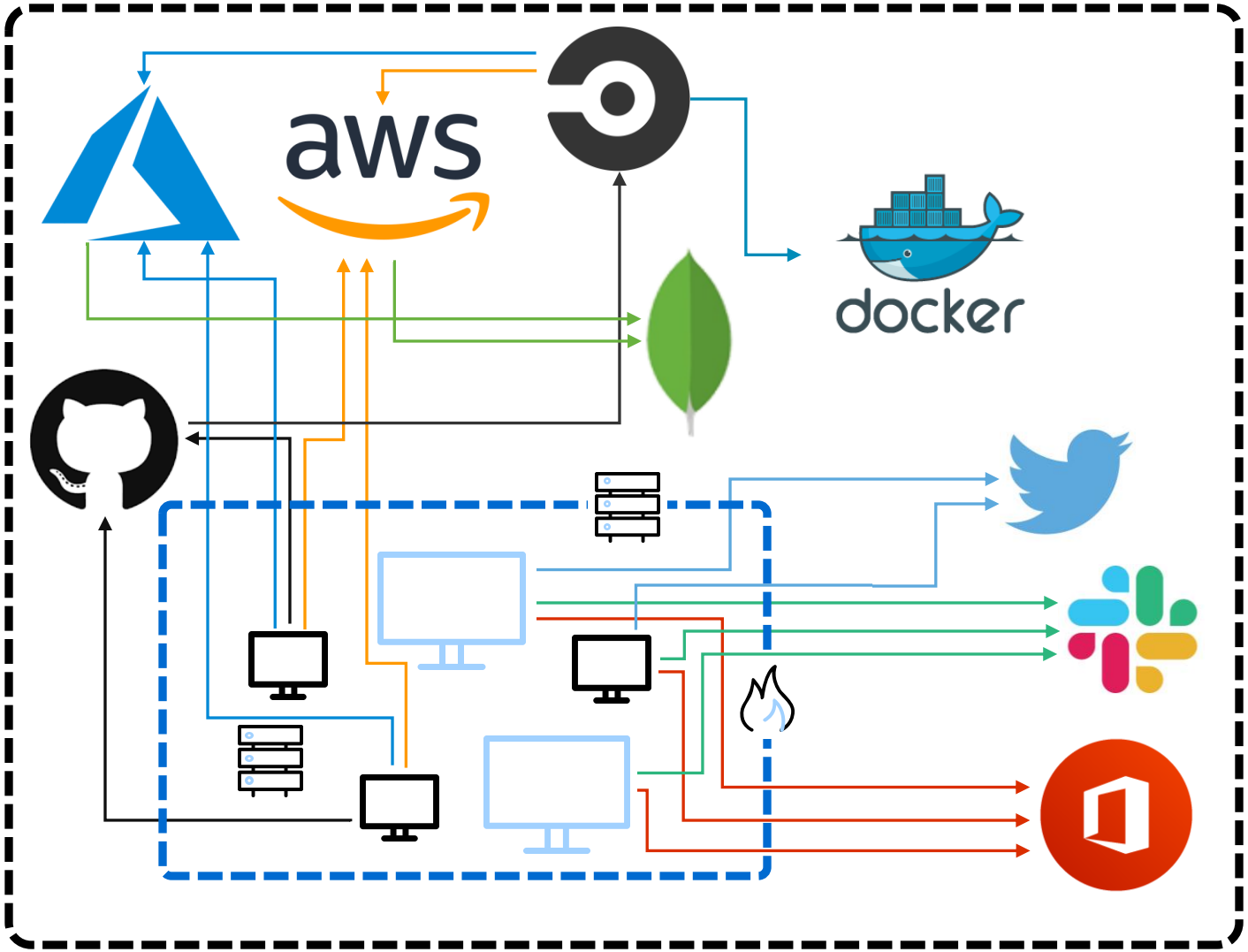
LABS

iam:CreatePolicyVersion



LABS

ENTERPRISE CLOUD ADOPTION

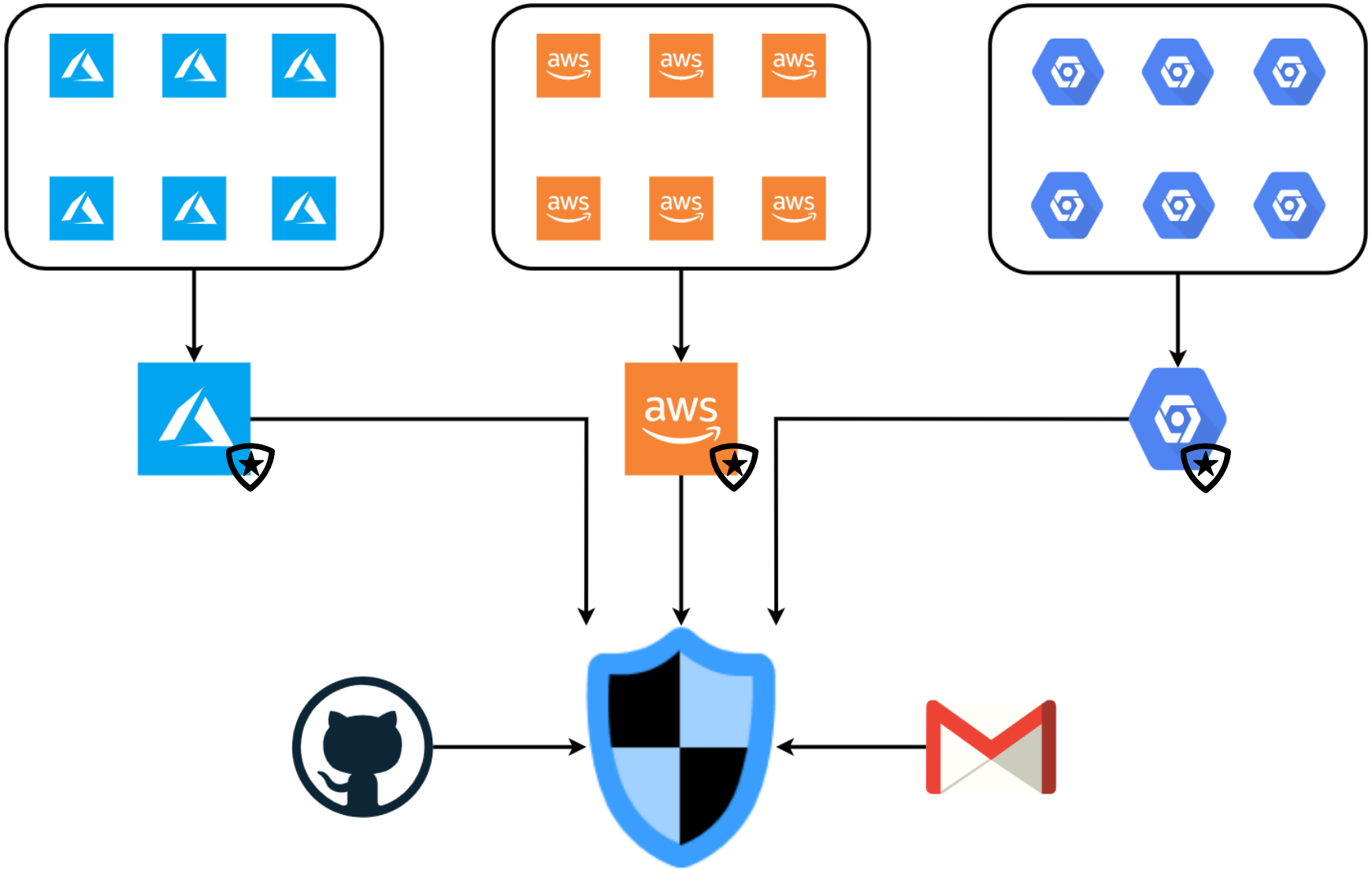


F-Secure | LABS

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

LABS

CONTROL PLANE AUDIT LOGS

Provider specifics

- AWS – CloudTrail
- Azure – Audit Log
- GCP – Audit Log
- Kubernetes – Audit Log

Why bother?

- The key data source for all cloud native exploitation
- Logs (almost) every control plane level event

Considerations

- “Data events” not always enabled
- For AWS, enable global events and multi-region logging

LABS

CLOUD-NATIVE DETECTION SERVICES

Provider Specifics

- AWS – GuardDuty
- Azure – Advanced Threat Protection
- GCP – Security Command Center

Why bother?

- Automatic detection of lower sophistication attacker activity
- Minimal integration effort compared to other sources
- Cost-effective way to detect low sophistication attacks

Considerations

- Typically signatures on known bad
- Some signatures of questionable value – Kali user agent detection in GuardDuty, for example

LABS

SERVICE-SPECIFIC TELEMETRY

Provider Specifics

- AWS – S3 access/object logs, Lambda executions, KMS key access
- Azure – Storage account access logs, function executions
- GCP – Storage Logs, Cloud Function Executions etc

Why bother?

- Can generate high fidelity telemetry on critical actions

Considerations

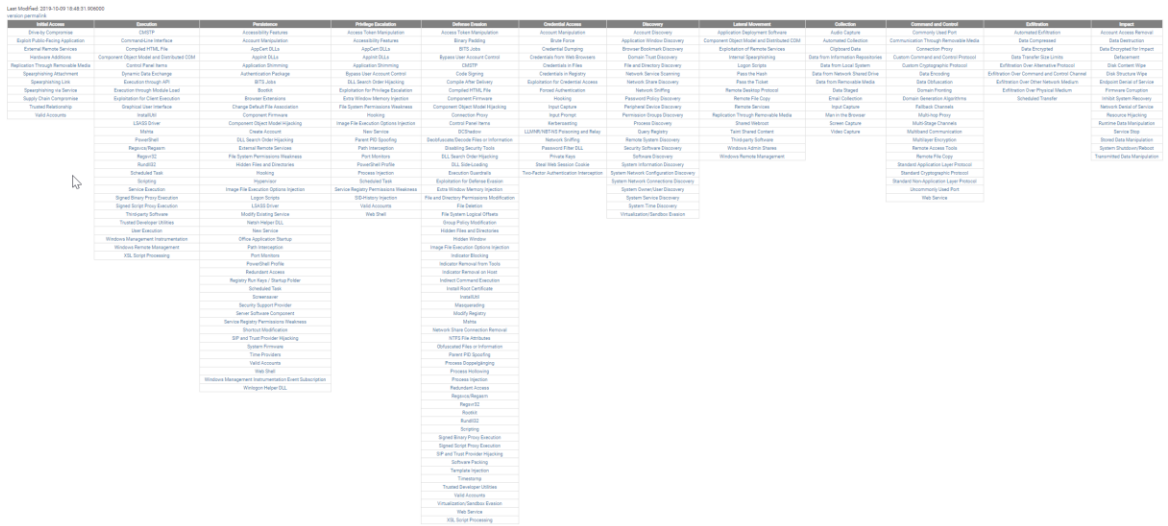
- Utility will vary by environment
- Requires that use cases and hunt queries are developed on a per environment basis
- Enable on a case by case basis

F-Secure | LABS

THE THREAT INTELLIGENCE PROBLEM

LABS

ON-PREMISE VS CLOUD ATT&CK



Last Modified: 2019-10-09 18:48:31.906000
version permalink

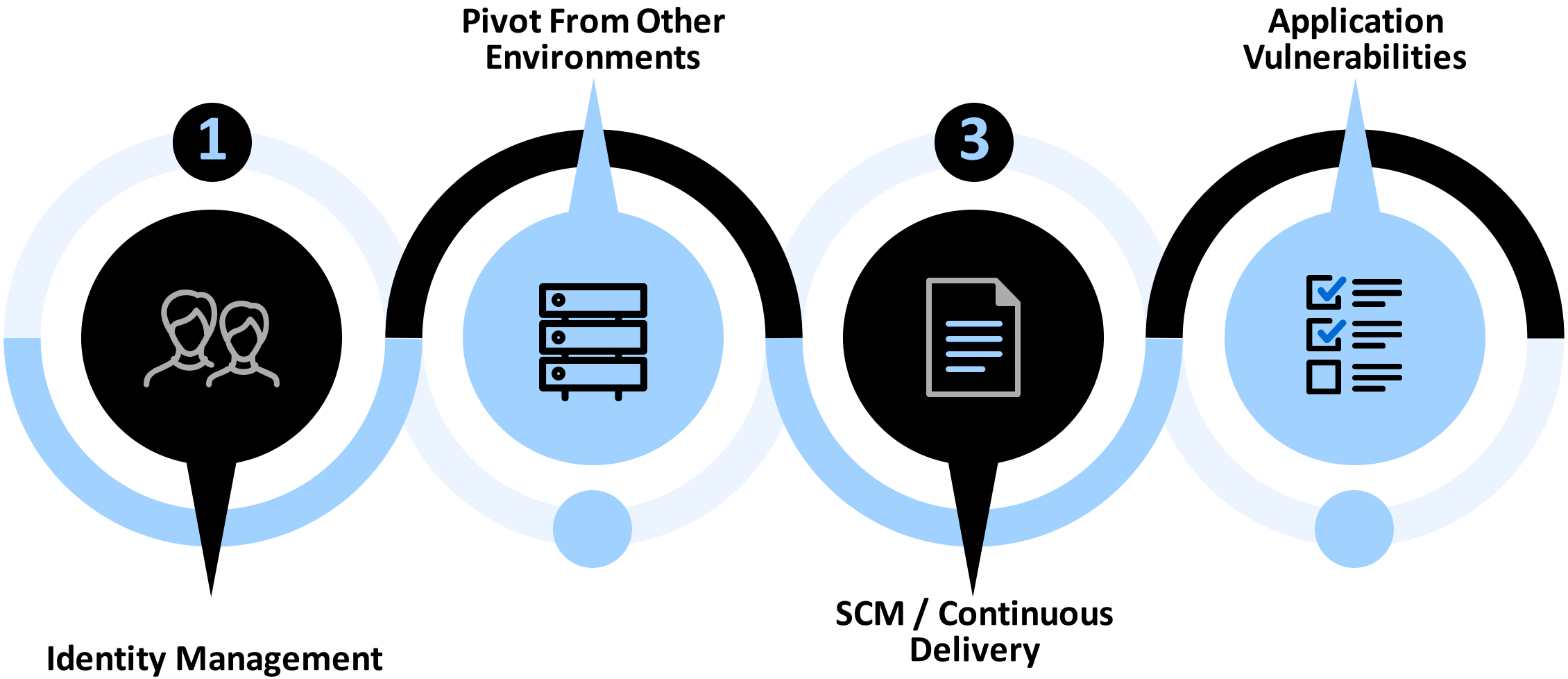
Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

DRAW INSPIRATION FROM...

F-Secure | LABS

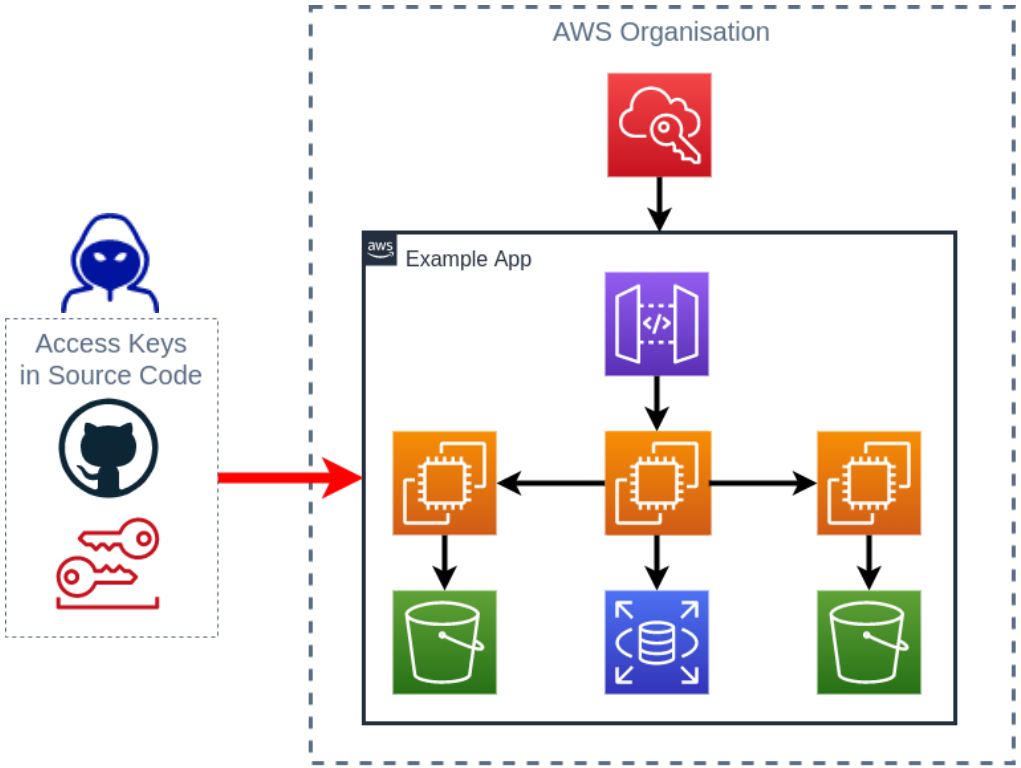
WHAT'S AN ATTACKER LIKELY TO DO?

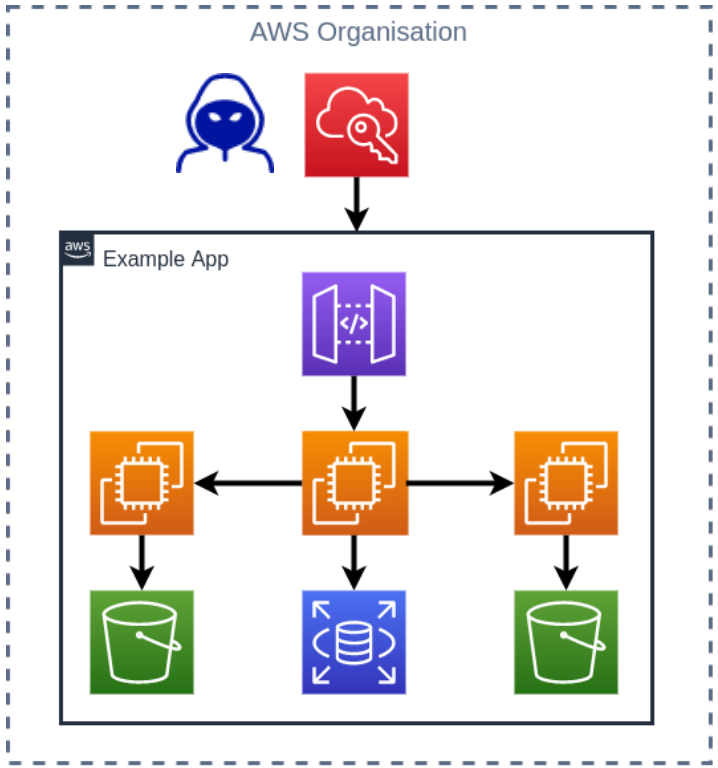
VECTORS WE'VE EXPLOITED



LABS

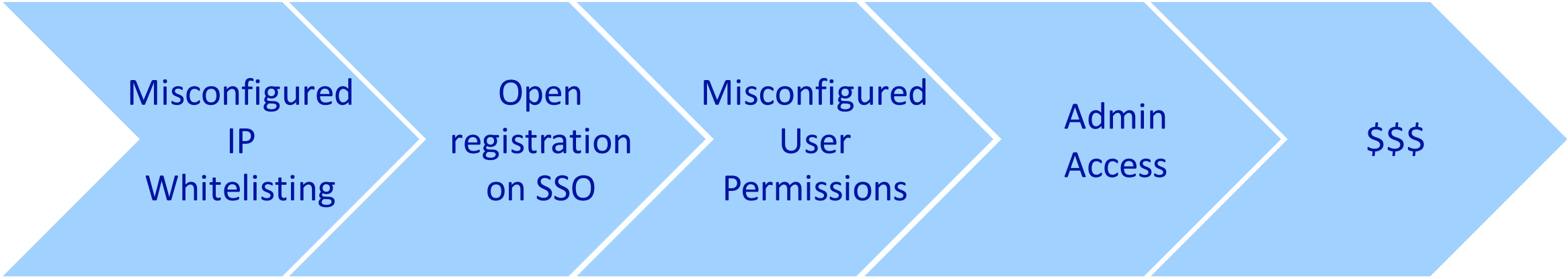
IDENTITY MANAGEMENT
EXPLOITATION





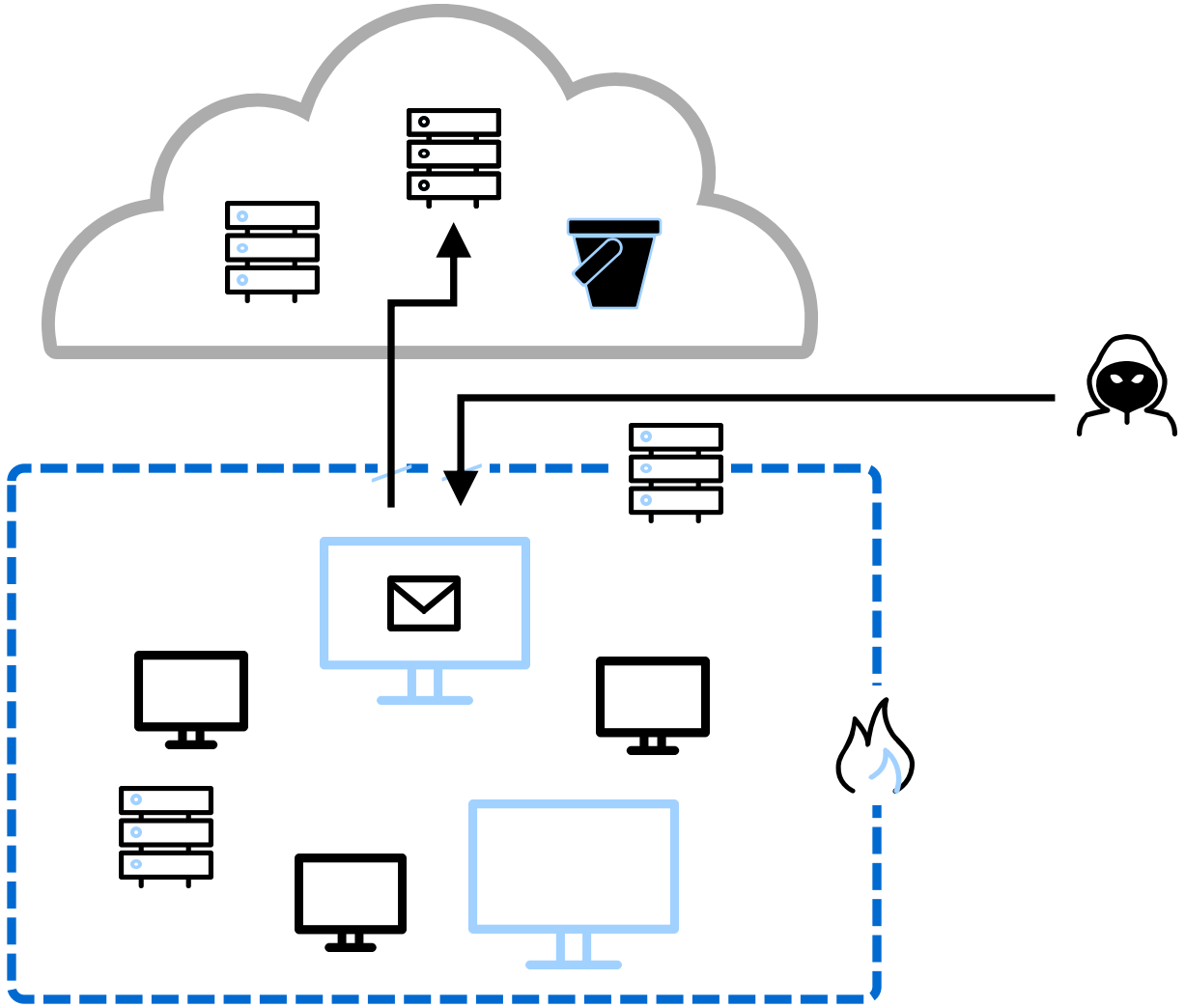
LABS

IDENTITY MANAGEMENT
ATTACK PATH



LABS

PIVOT FROM OTHER ENVIRONMENTS

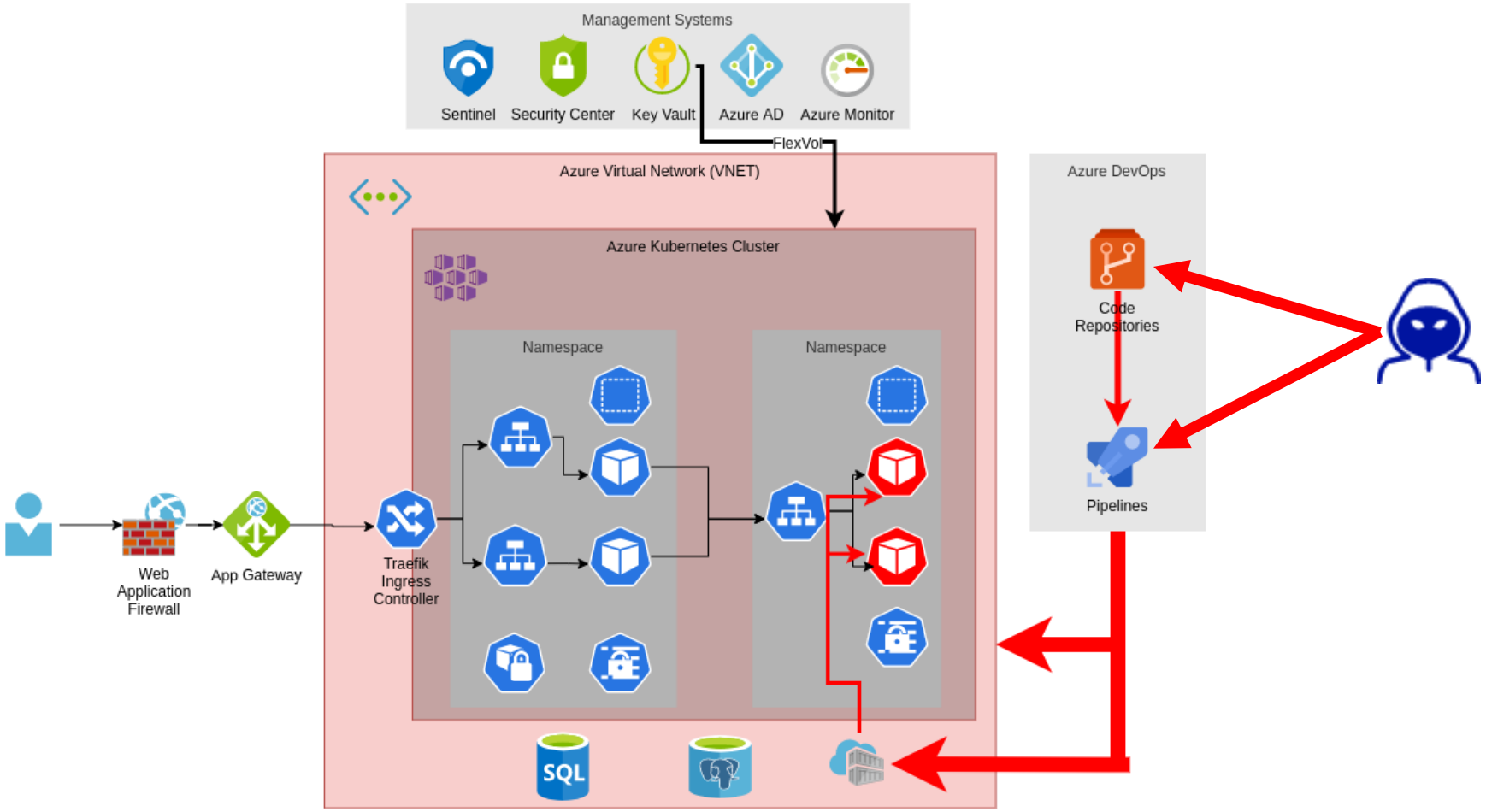


LABS

PIVOT ATTACK PATH

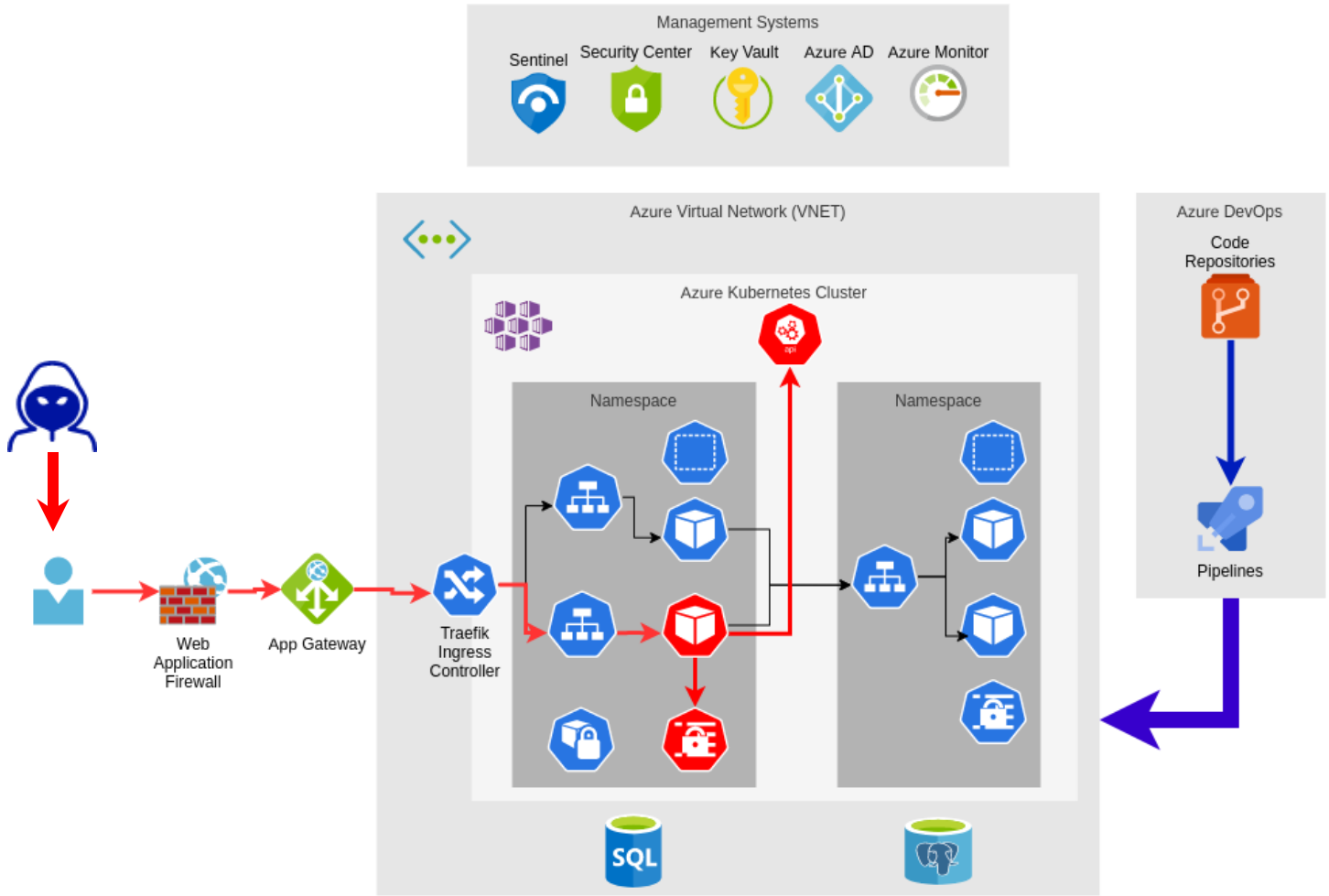
LABS

SCM & CONTINUOUS DELIVERY



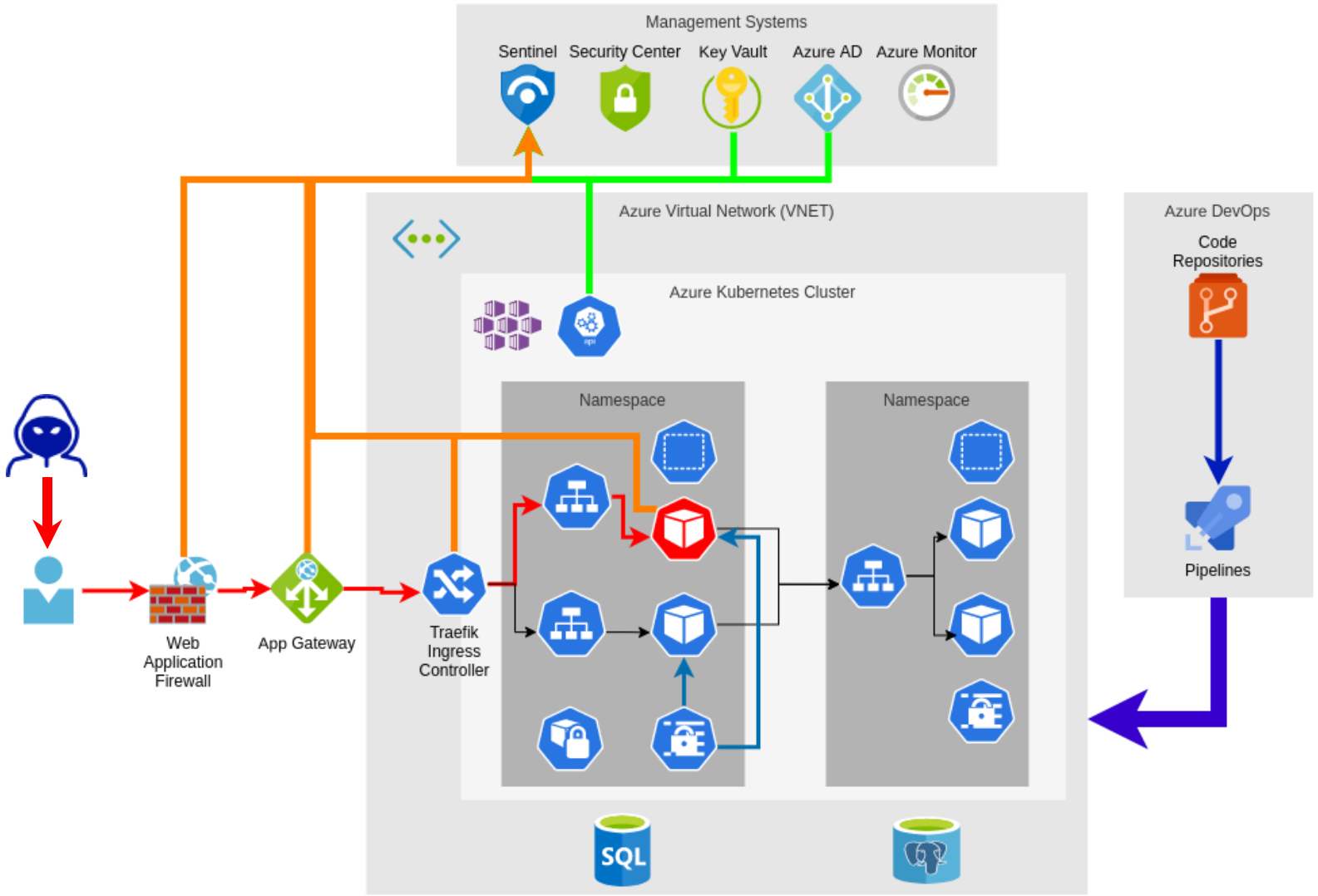
LABS

APPLICATION EXPLOITATION



LABS

DETECT APPLICATION EXPLOITATION



HOW DO I START?

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

02 Prioritise attack paths and actions

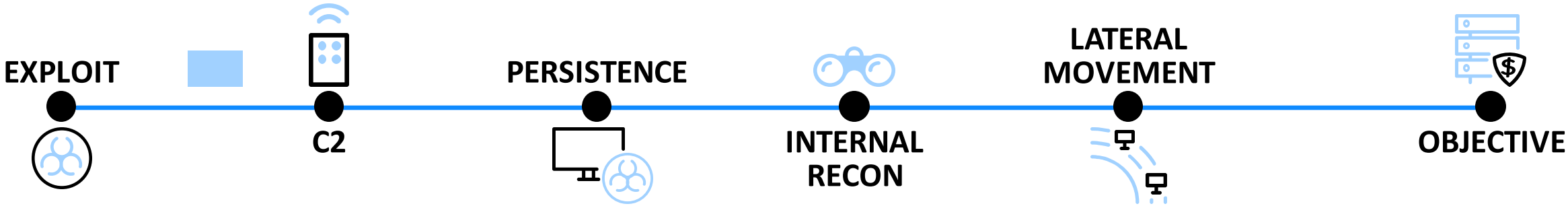
03 Pick the most important attack paths, codify them

04 Verify telemetry is available to defenders

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

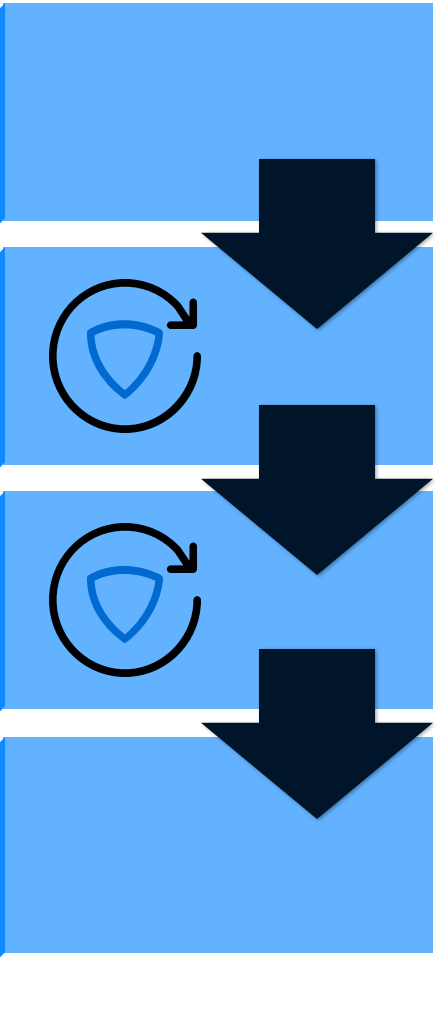
LABS

WHERE DO I START?



HOW DO WE VALIDATE?

- Identify likely attack paths
- Execute the identified attack paths
- Review telemetry/alerts, perform gap analysis versus attacks executed
- Identify missing telemetry and use cases, develop improvements



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

LEONIDAS

LABS

Leonidas 1.0

[Base URL: /dev]
https://nb2dfjx41h.execute-api.us-east-1.amazonaws.com/dev/swagger.json

An API for executing attacker actions within AWS

enumeration Enumeration

GET **/enumeration/enumerate_cloudtrails_for_all_regions** An adversary may attempt to enumerate the configured trails, to identify what actions will be logged and where they will be logged to

GET **/enumeration/enumerate_cloudtrails_for_current_region** An adversary may attempt to enumerate the configured trails, to identify what actions will be logged and where they will be logged to

defense_evasion Defense Evasion

GET **/defense_evasion/add_new_guardduty_ip_set** An adversary may attempt to add a new GuardDuty IP whitelist in order to whitelist systems they control and reduce the chance of malicious activity being detected

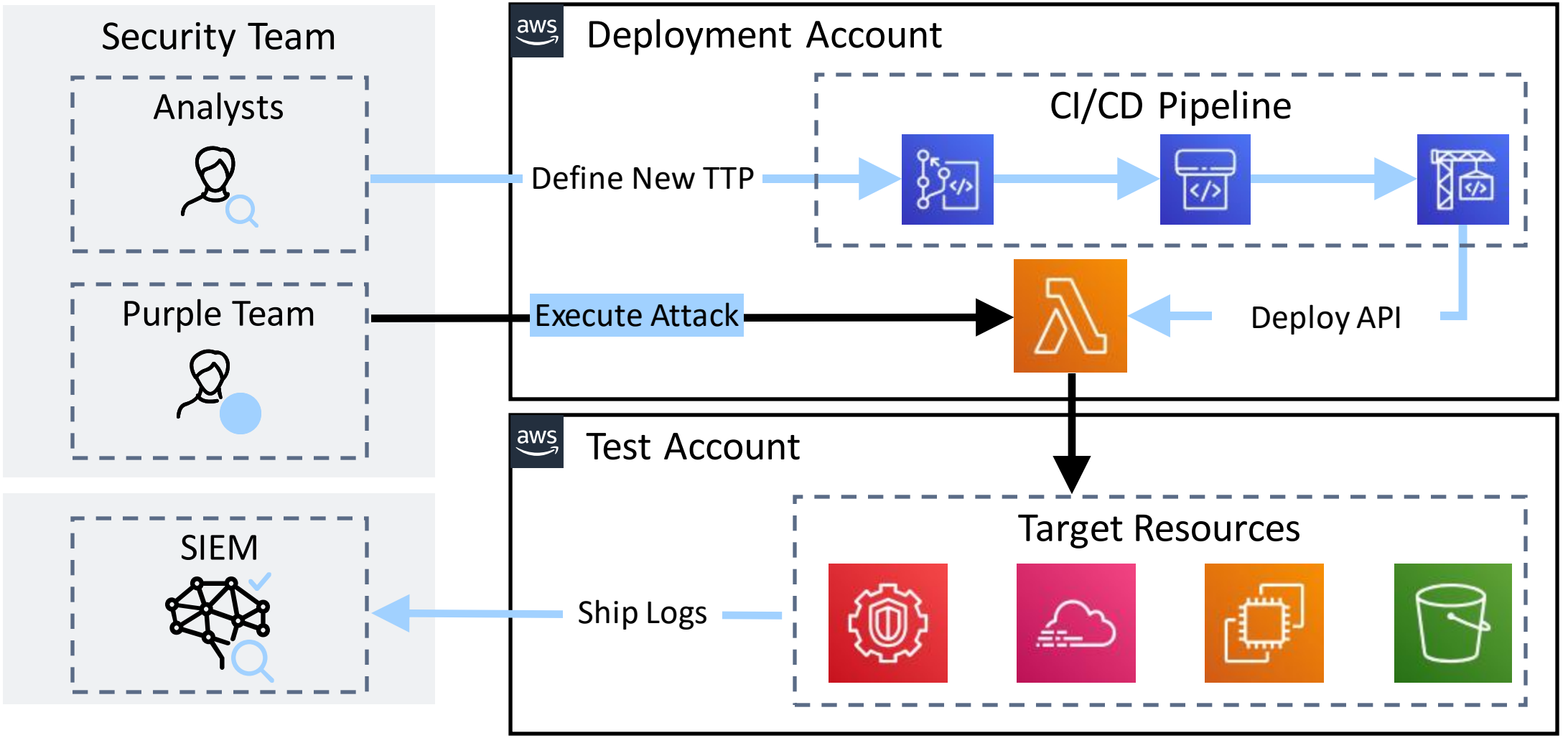
GET **/defense_evasion/update_guardduty_ip_set** An adversary may attempt to alter a configured GuardDuty IP whitelist in order to whitelist systems they control and reduce the chance of malicious activity being detected

Parameters Cancel

Name	Description
detectorid string *(query)*	ID of the guardduty detector associated with the IP set list detectorid - ID of the guardduty detector assc
ipsetid string *(query)*	ID of the IP set to be updated ipsetid - ID of the IP set to be updated
location string *(query)*	Location of the IP whitelist location - Location of the IP whitelist

LABS

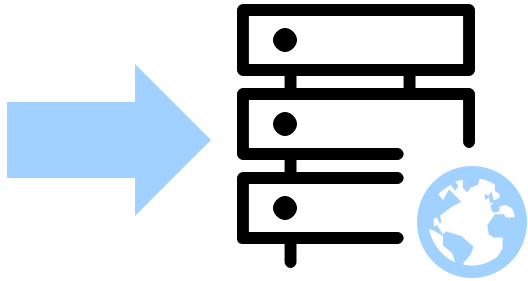
LEONIDAS



LABS

GENERATE ATTACK SIMULATION

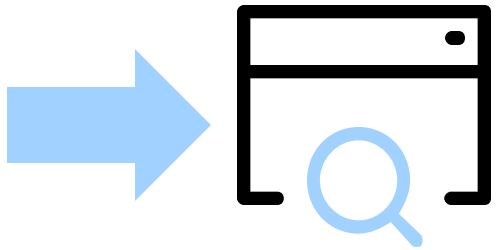
```
- name: Enumerate Cloudtrails for Current Region
  permissions:
  - cloudtrail:DescribeTrails
  input_arguments:
  executors:
    leonidas_aws:
      implemented: True
      clients:
        - cloudtrail
      code: |
        result = clients["cloudtrail"].describe_trails()
```



LABS

GENERATE DETECTION CASES

```
- name: Enumerate Cloudtrails for Current Region
  detection:
    sigma_id: 48653a63-085a-4a3b-88be-9680e9adb449
    status: experimental
    level: low
    sources:
      - name: "cloudtrail"
        attributes:
          eventName: "DescribeTrails"
          eventSource: "*.cloudtrail.amazonaws.com"
```



LABS

GENERATE ACCESS REQUIREMENTS

```
- name: Enumerate Cloudtrails for Current Region
  permissions:
  - cloudtrail:DescribeTrails
  input_arguments:
  executors:
    python:
      code: |
        client = boto3.client('cloudtrail')
        response = client.describe_trails()
        return response
```

LABS

Add new guardduty ip set

Author	Last Update
Nick Jones	2020-06-18

An adversary may attempt to add a new GuardDuty IP whitelist in order to whitelist systems they control and reduce the chance of malicious activity being detected.

MITRE IDs

- T1089

Required Permissions

- guardduty:CreateIPSet

Required Parameters

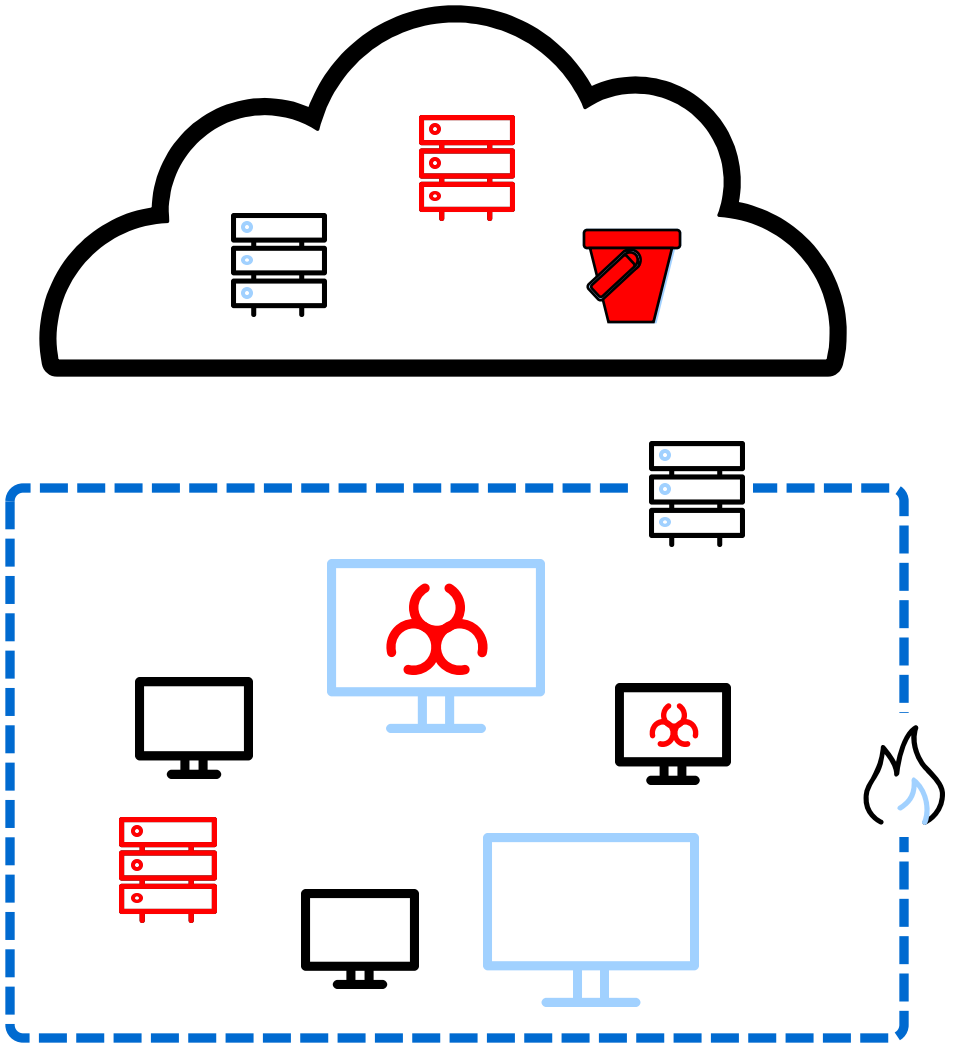
Name	Type	Description	Example Value
detectorid	str	ID of the guardduty detector associated with the IP set list	12345
format	str	Format of the new IP set list - choice of TXT, STIX, OTX_CSV, ALIEN_VAULT, PROOF_POINT, FIRE_EYE	TXT

GENERATE
DOCUMENTATION

F-Secure | LABS

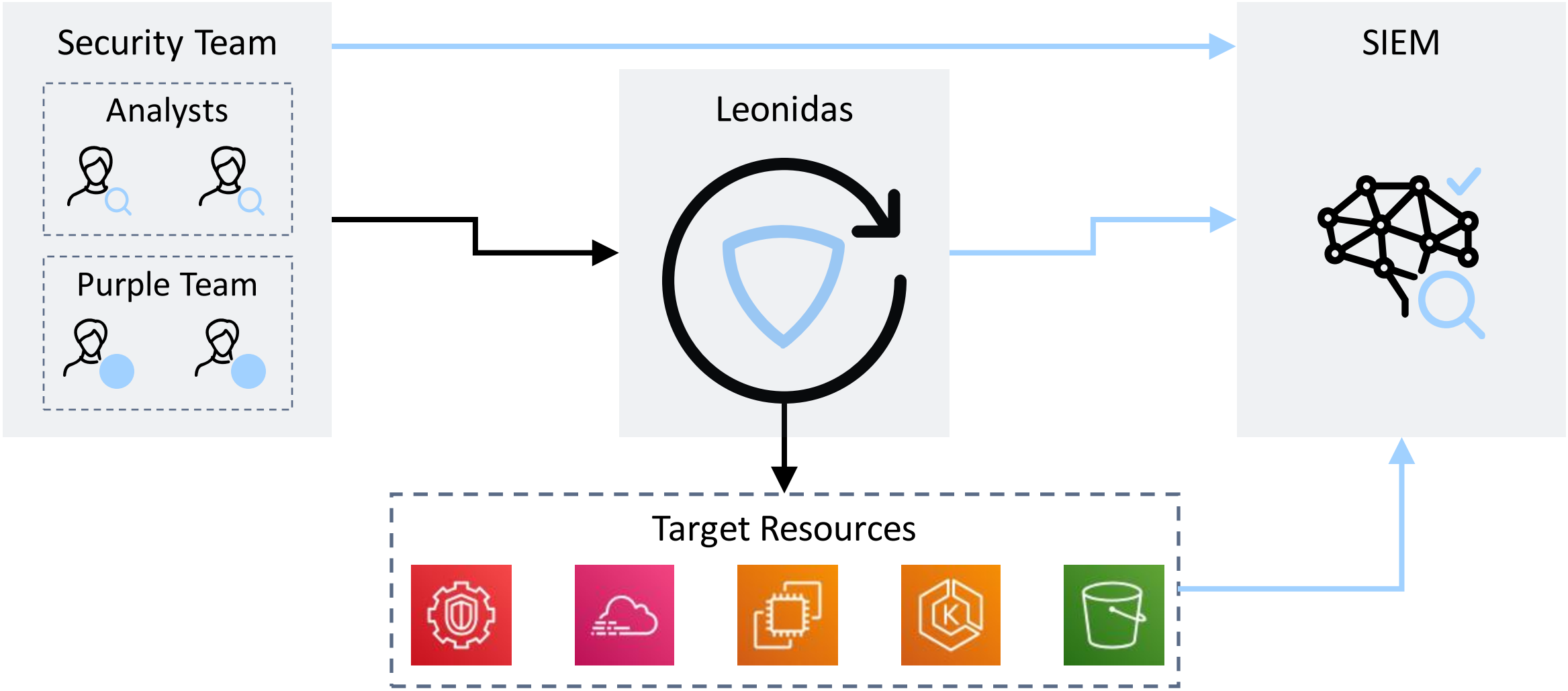
DEMO TIME!

CONTINUOUS TESTING



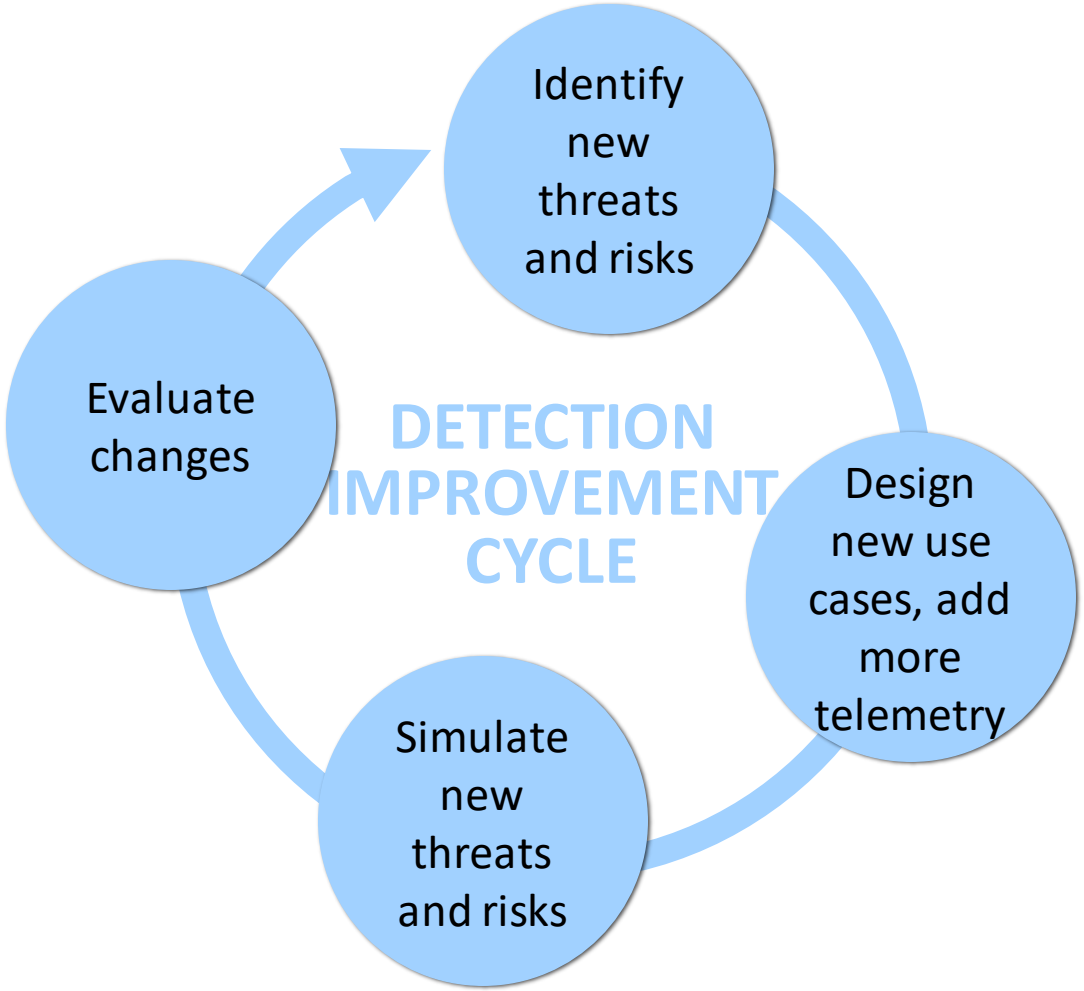
LABS

CONTINUOUS INTEGRATION



LABS

DETECTION IS A JOURNEY



Effective detection is a moving target

Treat it as an ongoing development project

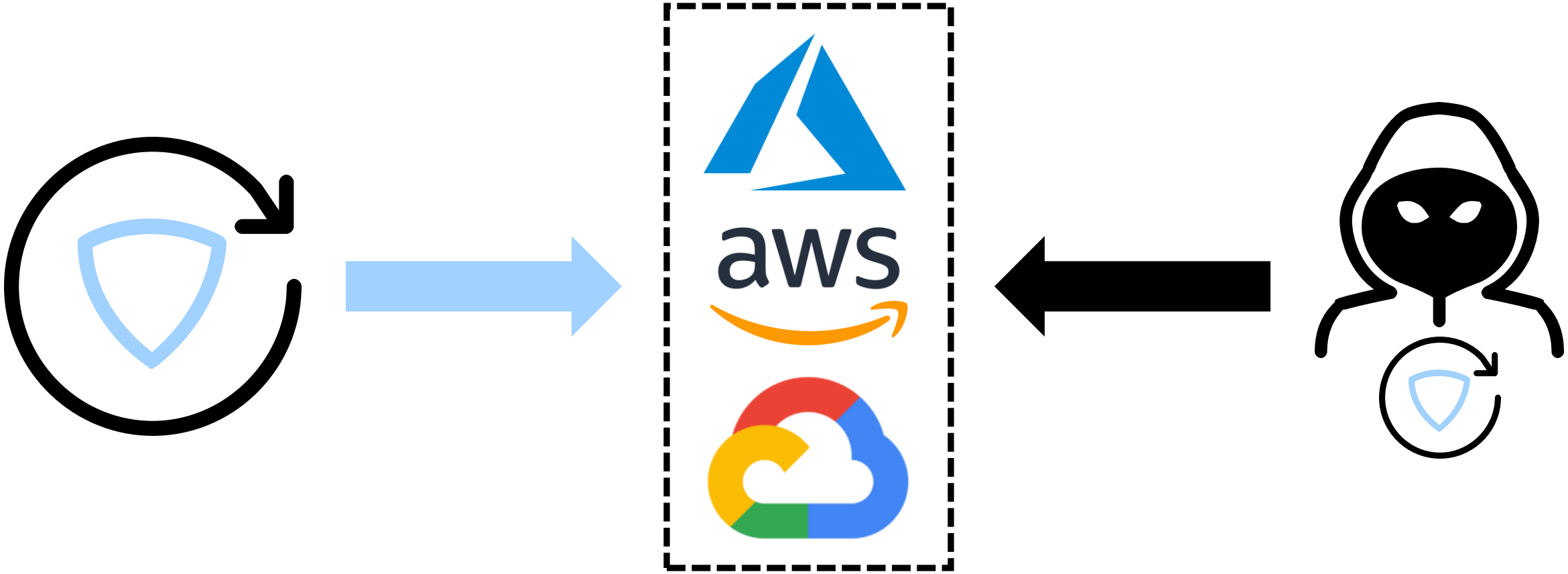
Agile/Scrum works for security too

F-Secure LABS

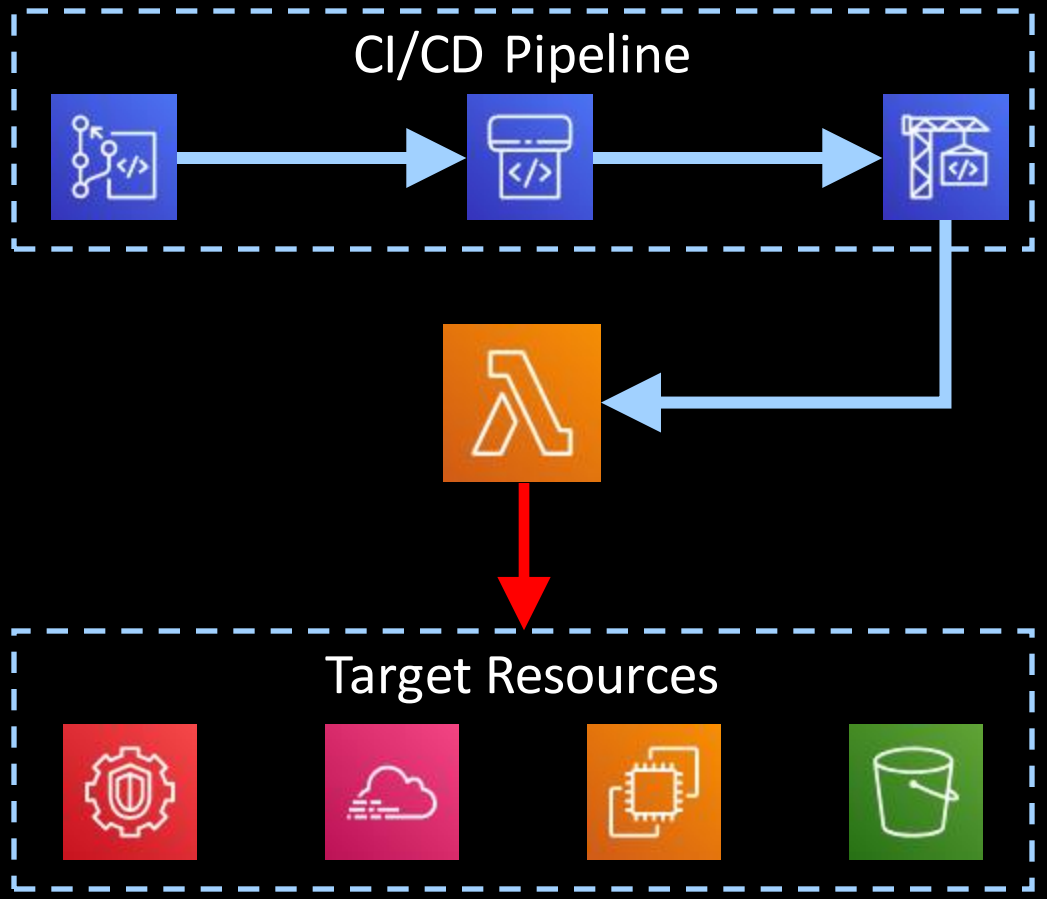
CONCLUSIONS

LABS

CONCLUSIONS



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