SPOTTING THE STORM: ATTACK DETECTION IN THE CLOUD

Nick Jones

AGENDA

[illegible] DEVOPS [illegible]

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

F-Secure | LABS

ON-PREMISE VS CLOUD

THE PENTESTER'S VIEW OF CLOUD

LABS

THE AVERAGE SOC'S VIEW OF CLOUD

OUR EDR WILL PROTECT YOUR AWS ACCOUNTS TOO
WE HAVE NO VIRTUAL MACHINES

A LOT HAS CHANGED

Container-as-a-Service/Function-as-a-Service means no direct OS access

Networking now custom SDNs, often no network logging for PaaS/SaaS

Some app vulnerabilities are now much more important (SSRF)

RAPID DEPLOYMENT CYCLES

Mature orgs deploy frequently

- Netflix – hundreds/thousands of times a day
- Amazon – every ***11.7 seconds*** on average

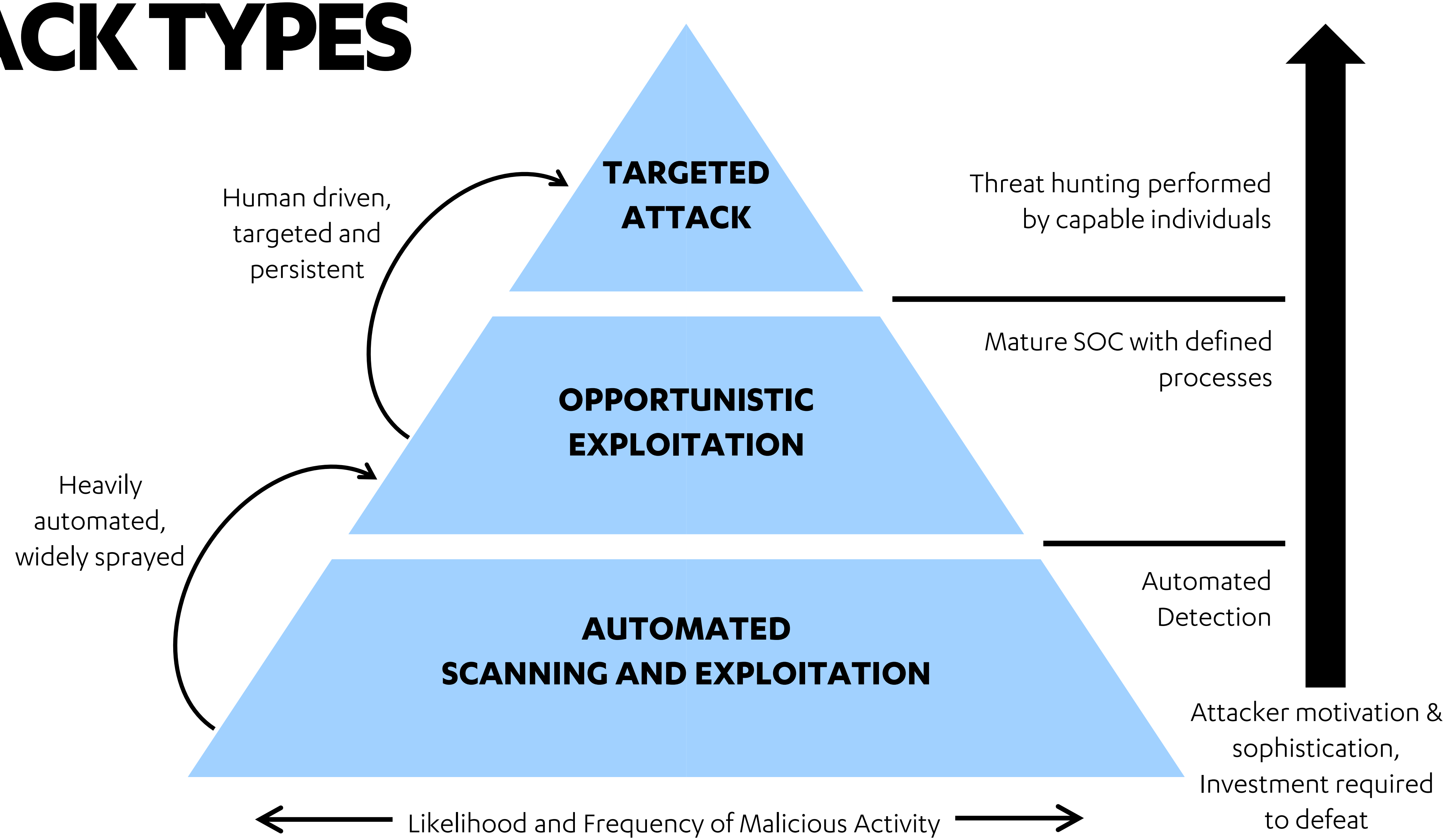
How does an attacker persist?

- Serverless microvm/container lifetime measured in minutes
- Control plane level persistence more common

Old D&R approaches no longer work

- Does your EDR, support Kubernetes, Lambda etc?
- How do you do IR on systems that no longer exist?

ATTACK TYPES



TARGETED ATTACK

OPPORTUNISTIC EXPLOITATION

AUTOMATED SCANNING AND EXPLOITATION

Human driven, targeted and persistent

Heavily automated, widely sprayed

Threat hunting performed by capable individuals

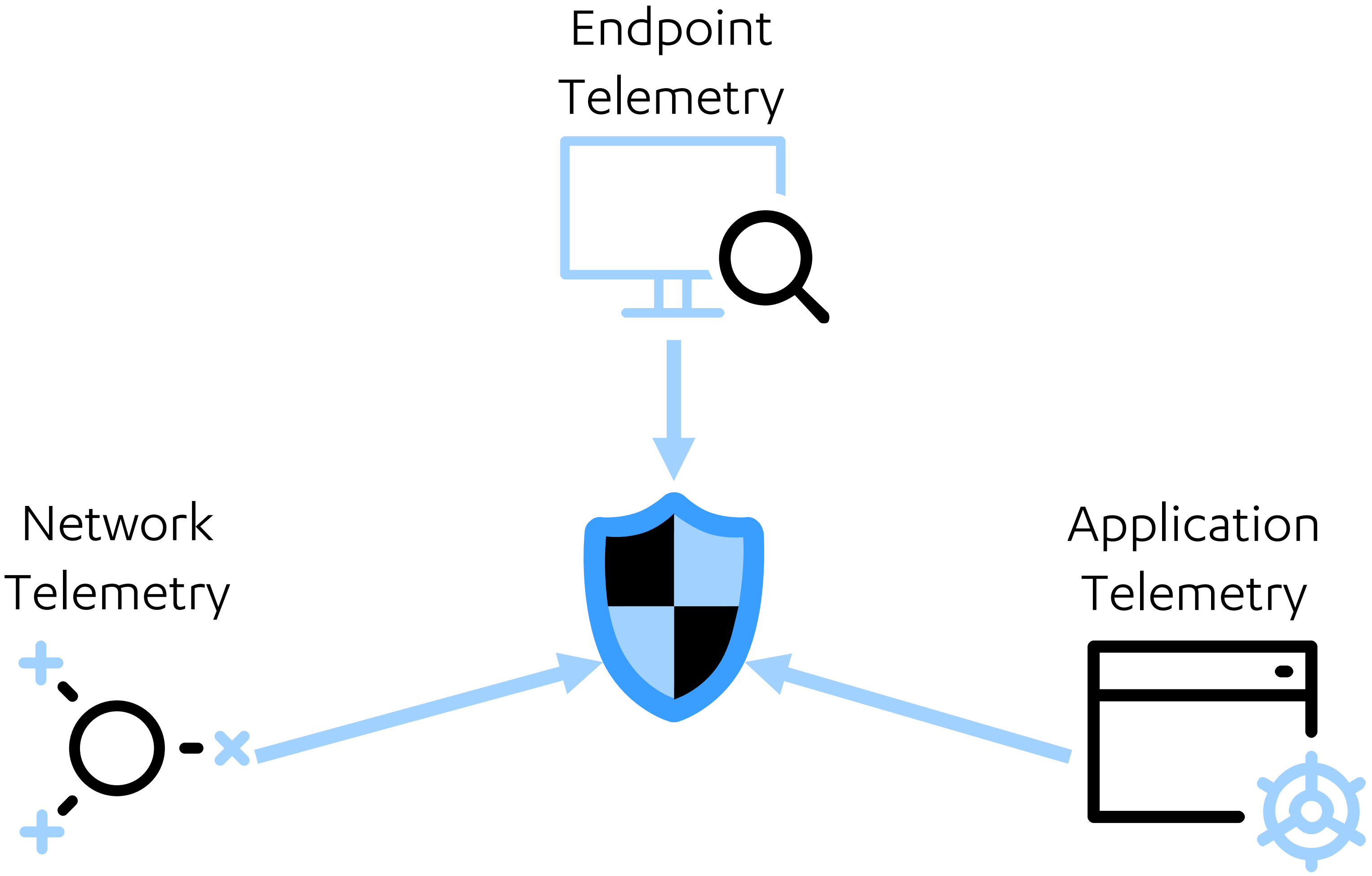
Mature SOC with defined processes

Automated Detection

Attacker motivation & sophistication, Investment required to defeat

Likelihood and Frequency of Malicious Activity

ON-PREMISE TELEMETRY



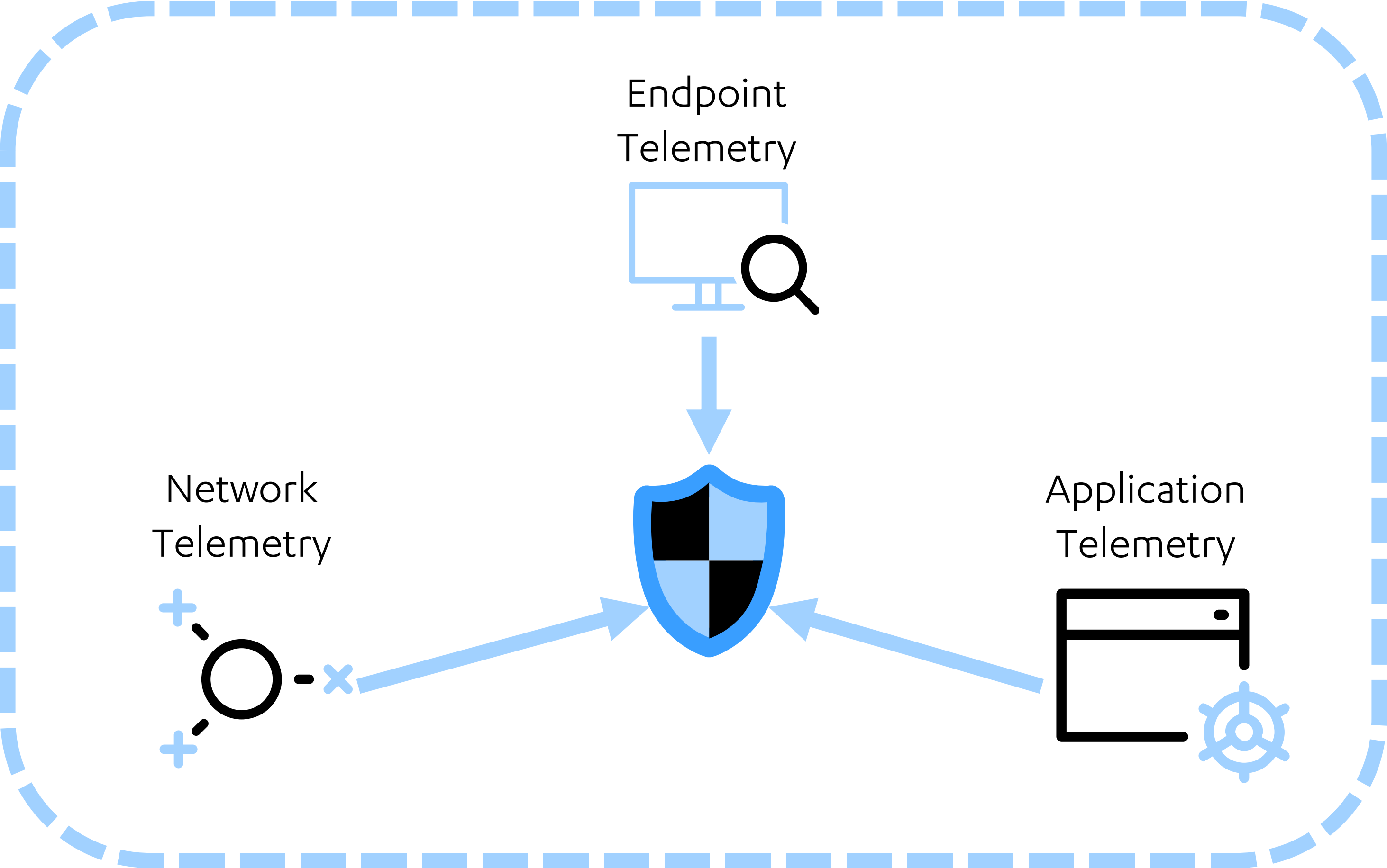
Endpoint Telemetry

Network Telemetry

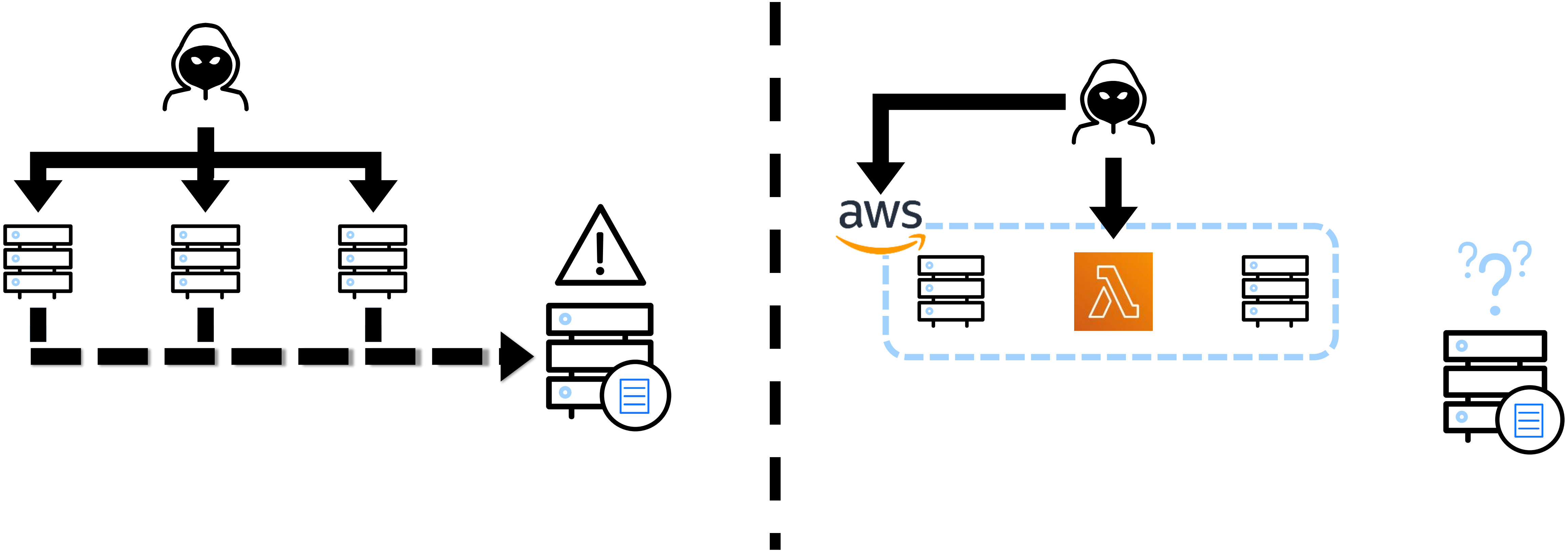
Application Telemetry

CLOUD TELEMETRY

Control Plane Telemetry

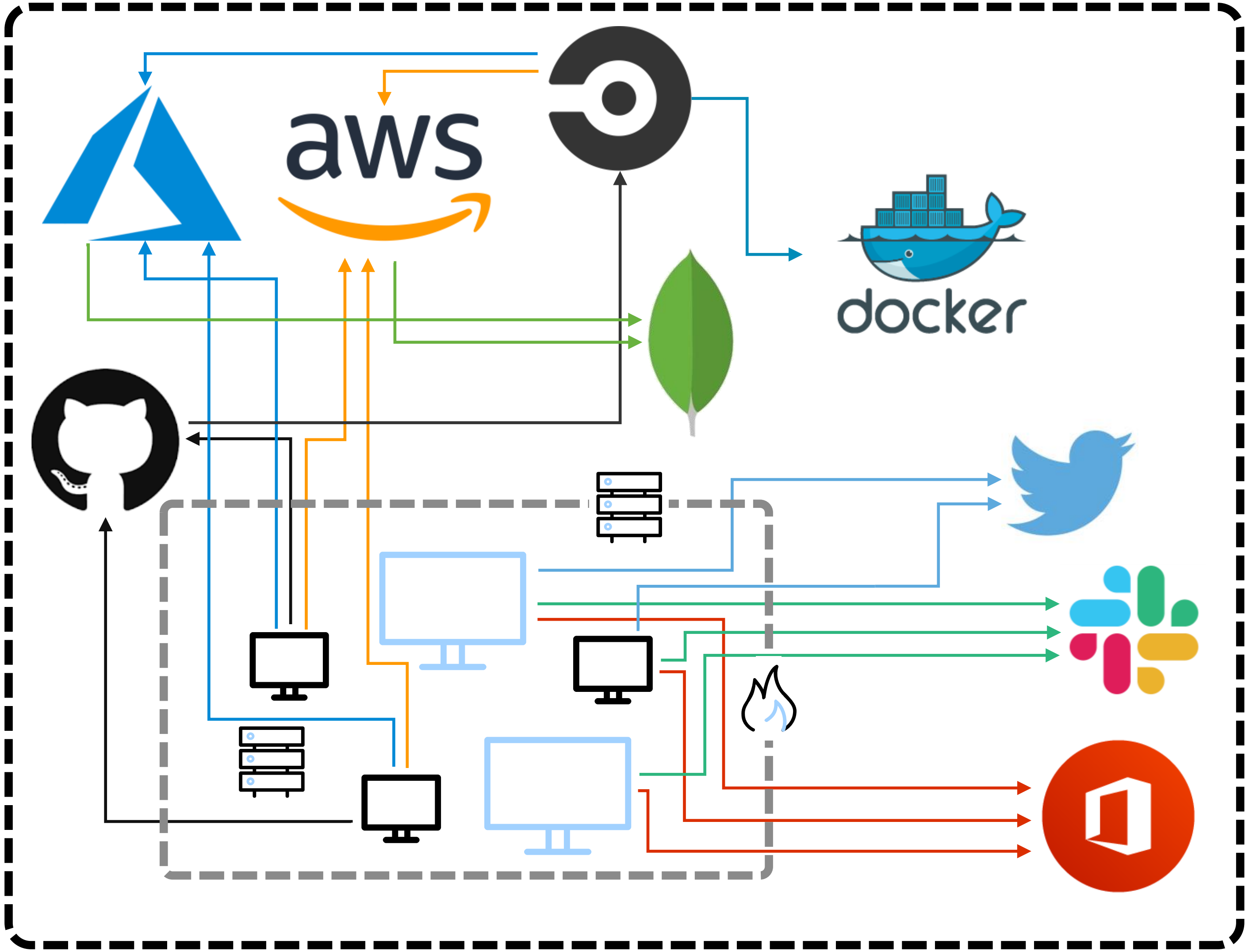


ON-PREMISE VS CLOUD DETECTION



LABS

ENTERPRISE CLOUD ADOPTION

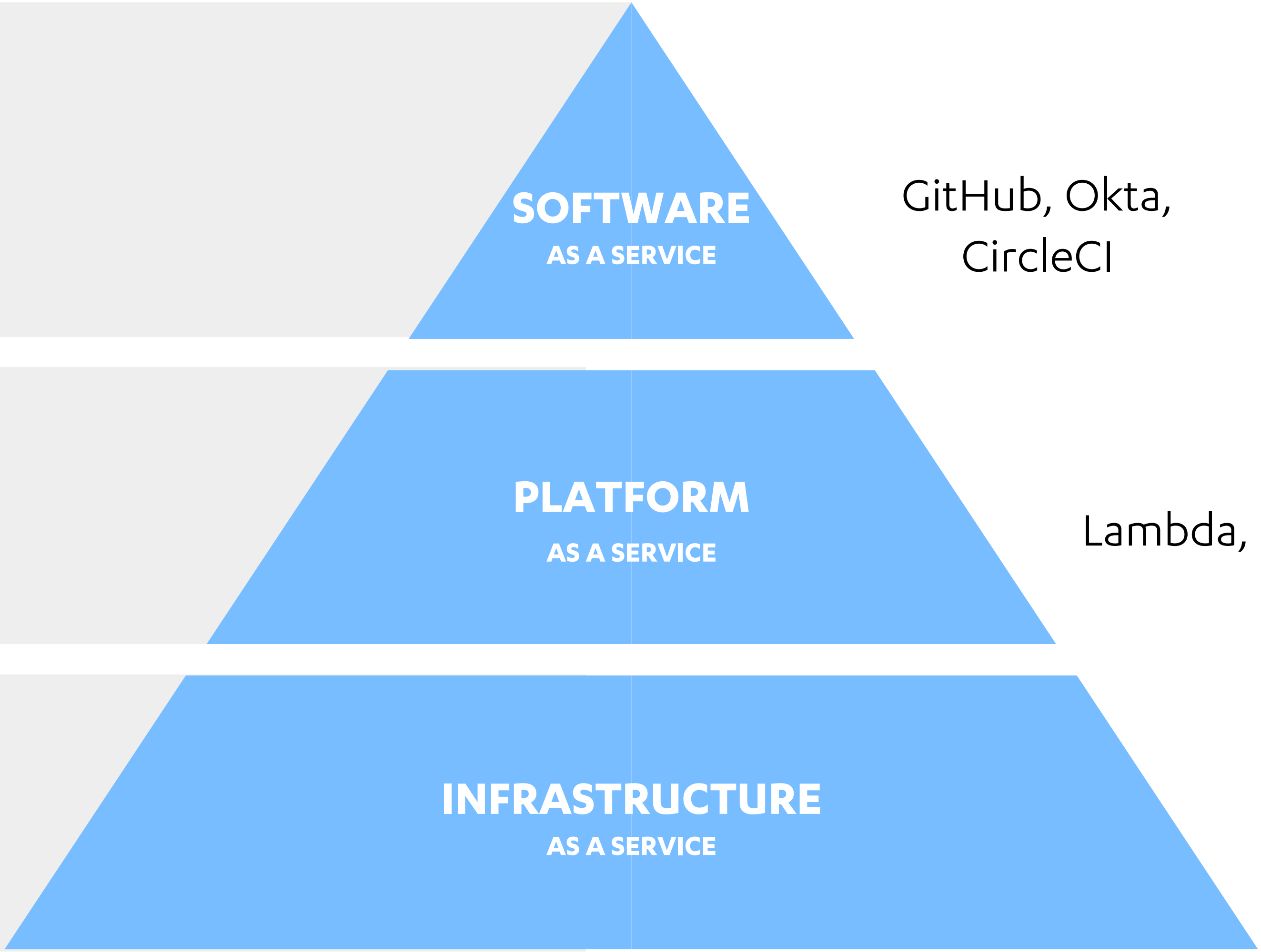


CLOUD SERVICES

🤷

- CloudTrail + Object-level Data Events
- Logging into CloudWatch

- EDR / VPC / CloudTrail
- App Logs



GitHub, Okta, CircleCI

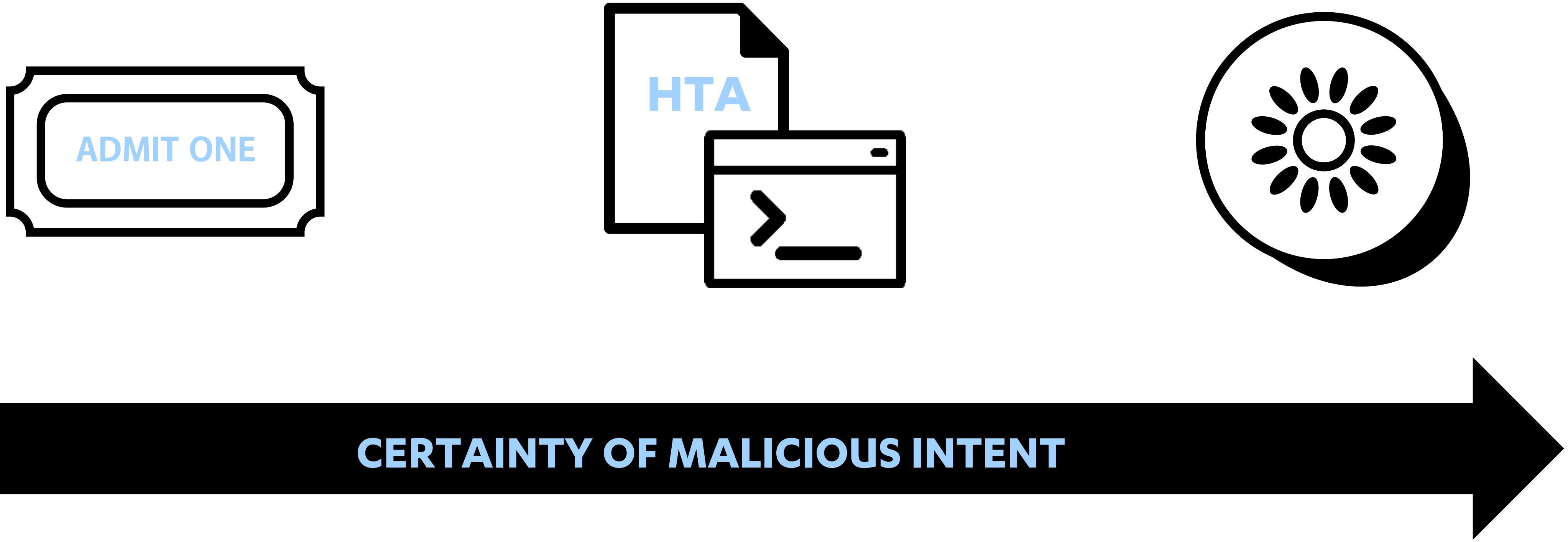
Lambda, S3

EC2

← Administrative Requirements of the Customer →

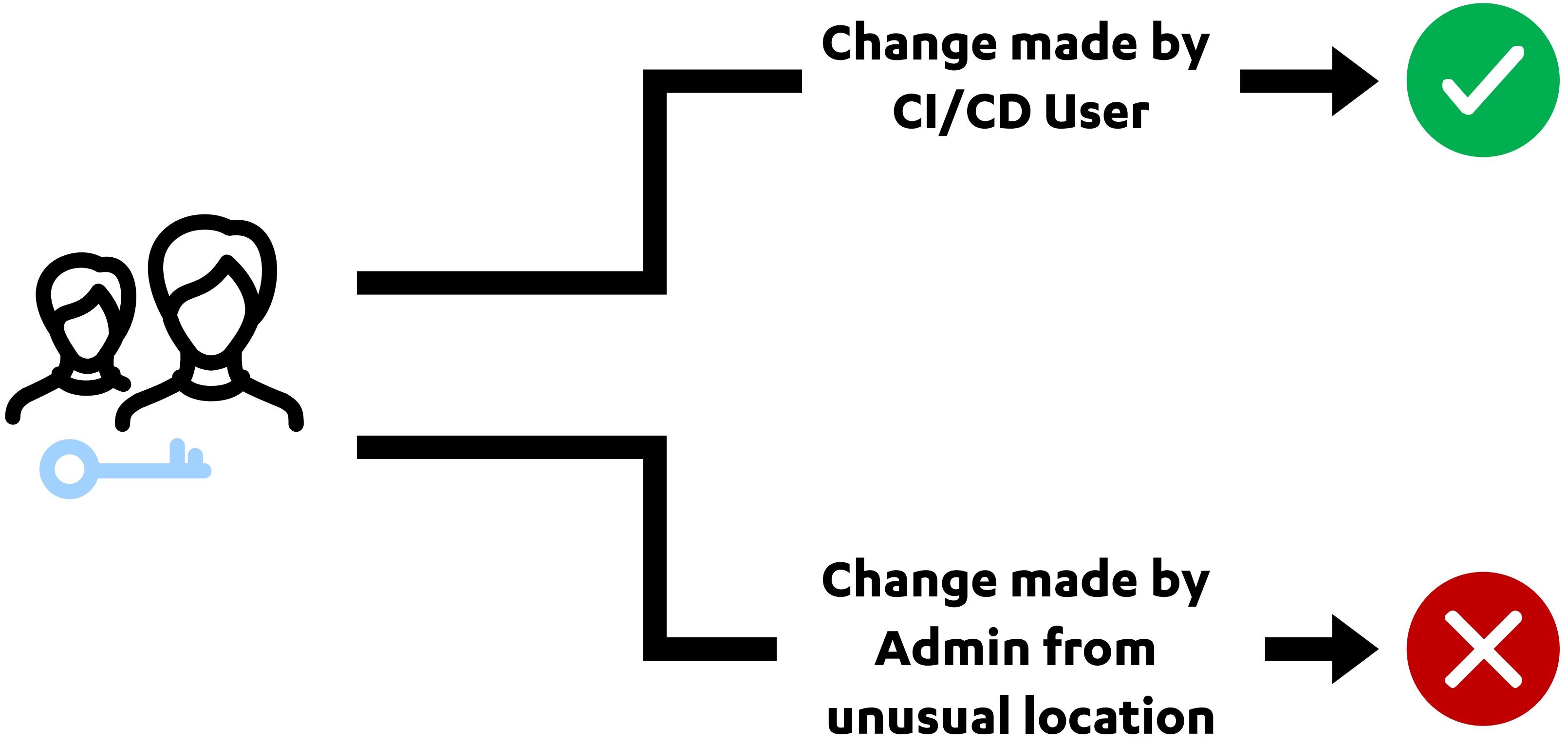
https://circleci.com/docs/2.0/security/#audit-logs

MINDSET SHIFT



CERTAINTY OF MALICIOUS INTENT

CONTEXT IS KEY

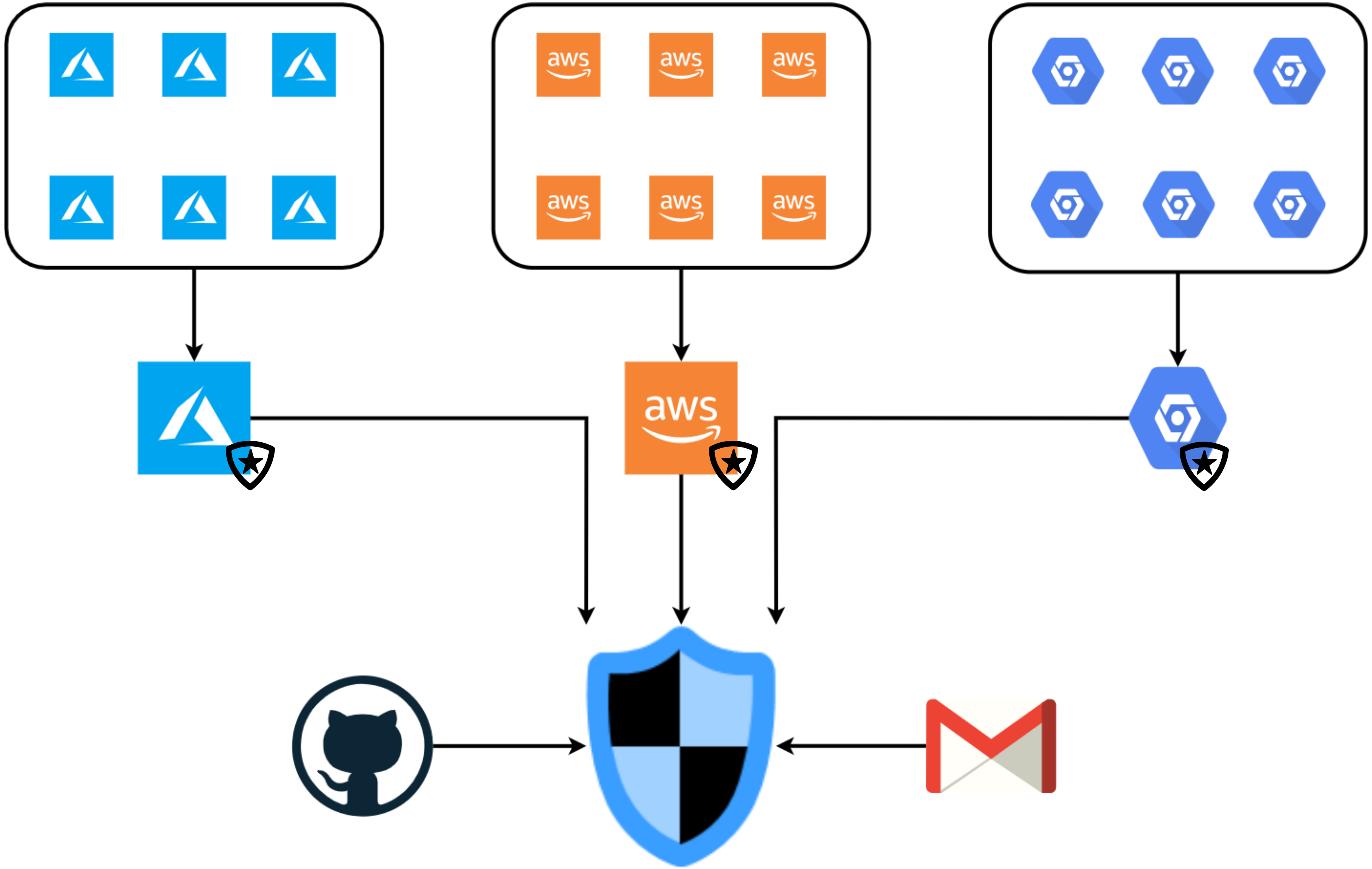


Change made by CI/CD User → ✓

Change made by Admin from unusual location → ✗

DESIGNING YOUR CLOUD DETECTION STACK

CENTRALISE EVERYTHING



LABS

DATA SOURCES

SOURCE	BENEFIT
Control Plane audit logs (CloudTrail, Audit Log etc)	**Visibility of all administrative actions**
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**
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

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

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

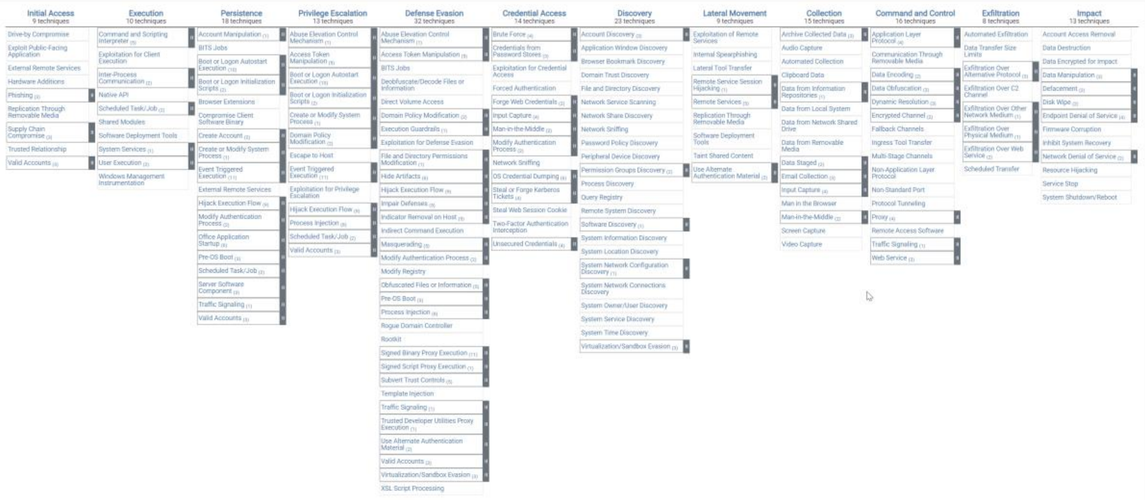
- Utility will vary by environment
- Requires that use cases and hunt queries are developed on a per environment basis
- Enable on a case by case basis

F-Secure | LABS

THE THREAT INTELLIGENCE PROBLEM

LABS

ON-PREMISES VS CLOUD ATT&CK



Initial Access
9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (3)

Execution
10 techniques
- Command and Scripting Interpreter (5)
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (2)
- Shared Modules
- Software Deployment Tools
- System Services (1)
- User Execution (2)
- Windows Management Instrumentation

Persistence
18 techniques
- Account Manipulation (1)
- BITS Jobs
- Boot or Logon Autostart Execution (10)
- Boot or Logon Initialization Scripts (2)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (2)
- Create or Modify System Process (1)
- Event Triggered Execution (11)
- External Remote Services
- Hijack Execution Flow (9)
- Modify Authentication Process (3)
- Office Application Startup (6)
- Pre-OS Boot (3)
- Scheduled Task/Job (2)
- Server Software Component (3)
- Traffic Signaling (1)
- Valid Accounts (3)

Privilege Escalation
13 techniques
- Abuse Elevation Control Mechanism (1)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (10)
- Boot or Logon Initialization Scripts (2)
- Create or Modify System Process (1)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (11)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (9)
- Process Injection (8)
- Scheduled Task/Job (2)
- Valid Accounts (3)

Defense Evasion
32 techniques
- Abuse Elevation Control Mechanism (1)
- Access Token Manipulation (5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (1)
- Hide Artifacts (6)
- Hijack Execution Flow (9)
- Impair Defenses (5)
- Indicator Removal on Host (5)
- Indirect Command Execution
- Masquerading (5)
- Modify Authentication Process (3)
- Modify Registry
- Obfuscated Files or Information (5)
- Pre-OS Boot (3)
- Process Injection (8)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11)
- Signed Script Proxy Execution (1)
- Subvert Trust Controls (5)
- Template Injection
- Traffic Signaling (1)
- Trusted Developer Utilities Proxy Execution (1)
- Use Alternate Authentication Material (2)
- Valid Accounts (3)
- Virtualization/Sandbox Evasion (3)
- XSL Script Processing

Credential Access
14 techniques
- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Man-in-the-Middle (2)
- Modify Authentication Process (3)
- Network Sniffing
- OS Credential Dumping (6)
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (4)

Discovery
23 techniques
- Account Discovery (3)
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (2)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

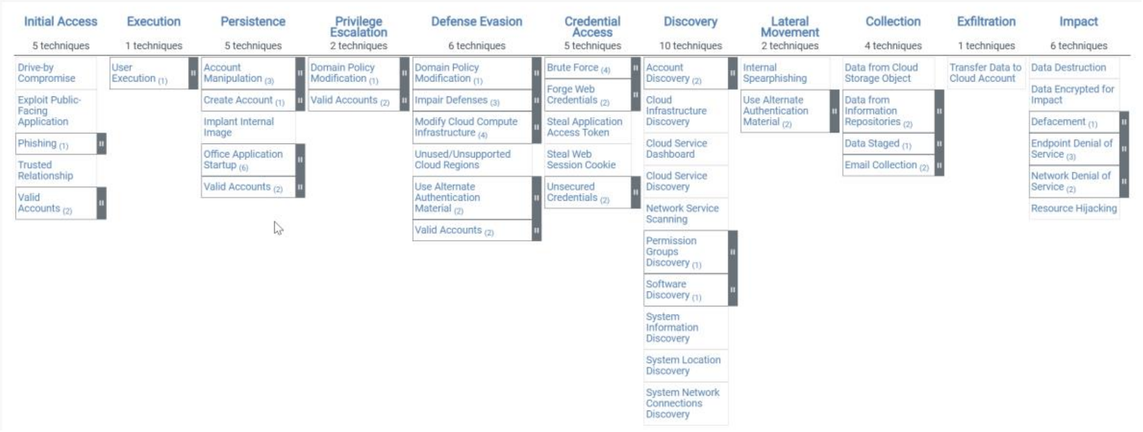
Lateral Movement
9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (1)
- Remote Services (5)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2)

Collection
15 techniques
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories (1)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Man in the Browser
- Man-in-the-Middle (2)
- Screen Capture
- Video Capture

Command and Control
16 techniques
- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

Exfiltration
8 techniques
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer

Impact
13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot



Initial Access
5 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- Phishing (1)
- Trusted Relationship
- Valid Accounts (2)

Execution
1 techniques
- User Execution (1)

Persistence
5 techniques
- Account Manipulation (3)
- Create Account (1)
- Implant Internal Image
- Office Application Startup (6)
- Valid Accounts (2)

Privilege Escalation
2 techniques
- Domain Policy Modification (1)
- Valid Accounts (2)

Defense Evasion
6 techniques
- Domain Policy Modification (1)
- Impair Defenses (3)
- Modify Cloud Compute Infrastructure (4)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (2)
- Valid Accounts (2)

Credential Access
5 techniques
- Brute Force (4)
- Forge Web Credentials (2)
- Steal Application Access Token
- Steal Web Session Cookie
- Unsecured Credentials (2)

Discovery
10 techniques
- Account Discovery (2)
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Network Service Scanning
- Permission Groups Discovery (1)
- Software Discovery (1)
- System Information Discovery
- System Location Discovery
- System Network Connections Discovery

Lateral Movement
2 techniques
- Internal Spearphishing
- Use Alternate Authentication Material (2)

Collection
4 techniques
- Data from Cloud Storage Object
- Data from Information Repositories (2)
- Data Staged (1)
- Email Collection (2)

Exfiltration
1 techniques
- Transfer Data to Cloud Account

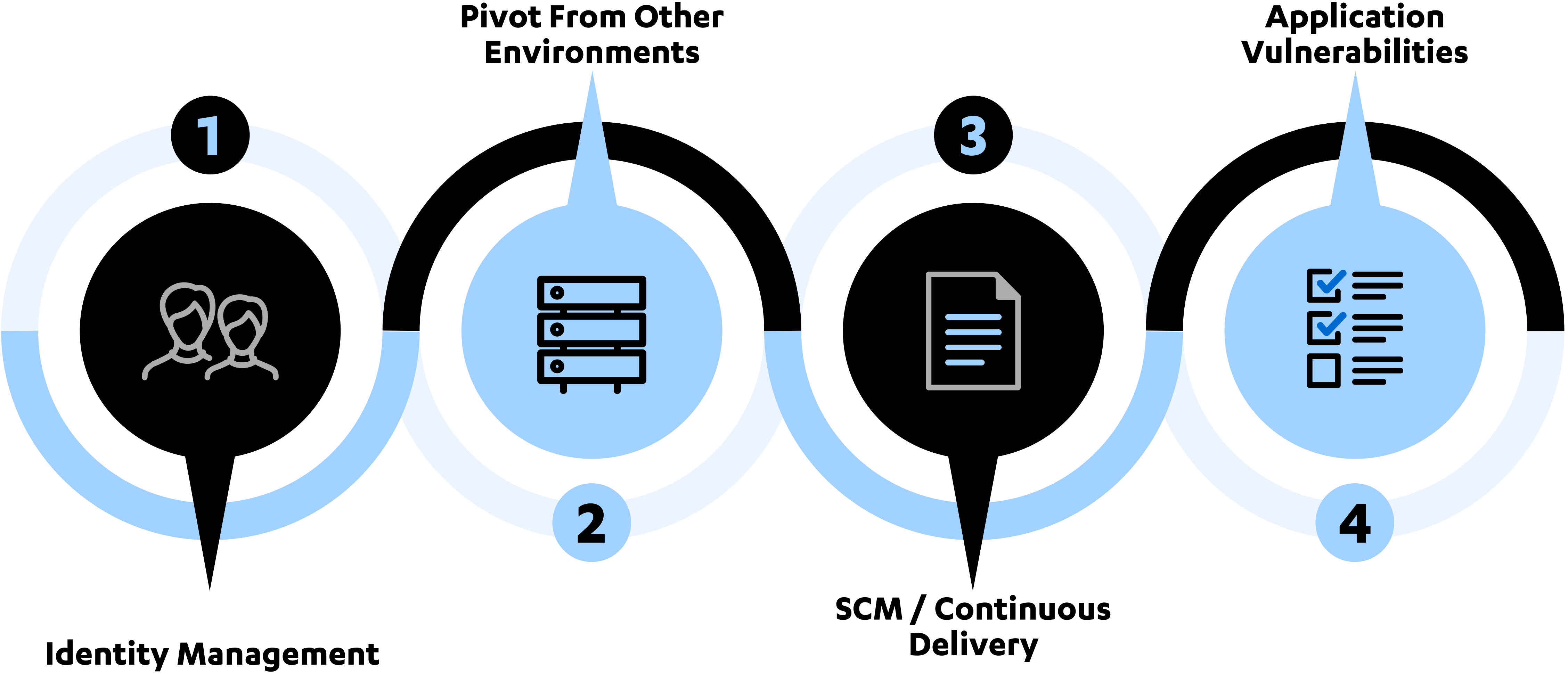
Impact
6 techniques
- Data Destruction
- Data Encrypted for Impact
- Defacement (1)
- Endpoint Denial of Service (3)
- Network Denial of Service (2)
- Resource Hijacking

MITRE ATT&CK™

Retrieved 15th May 2021

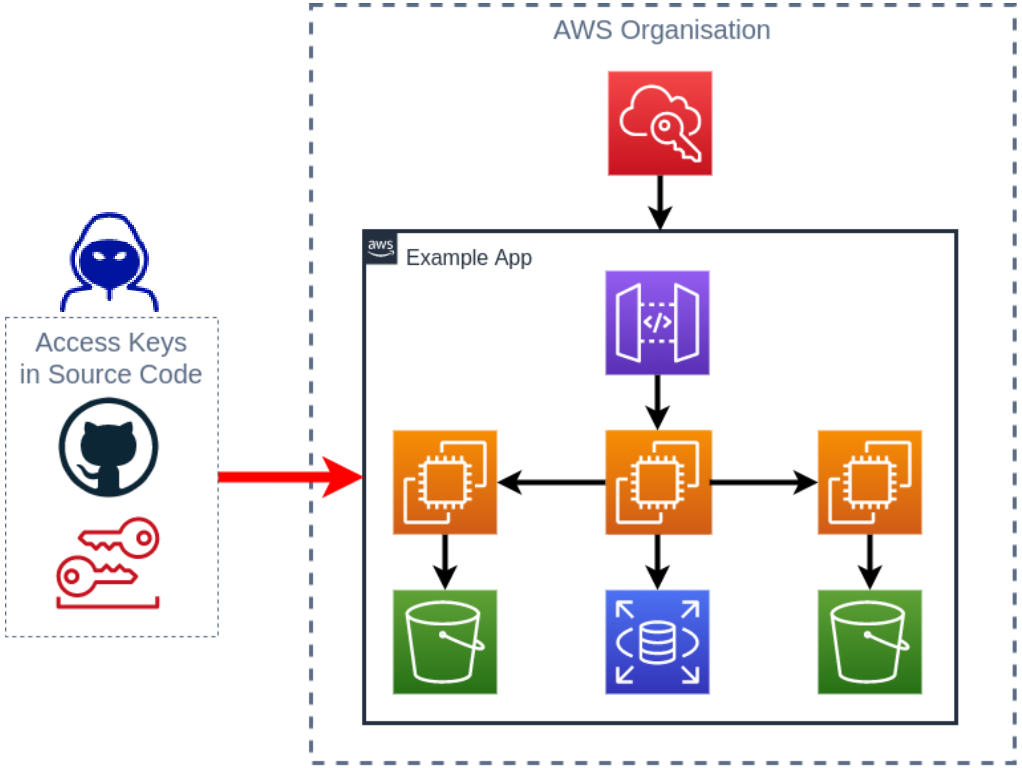
WHAT'S AN ATTACKER LIKELY TO DO?

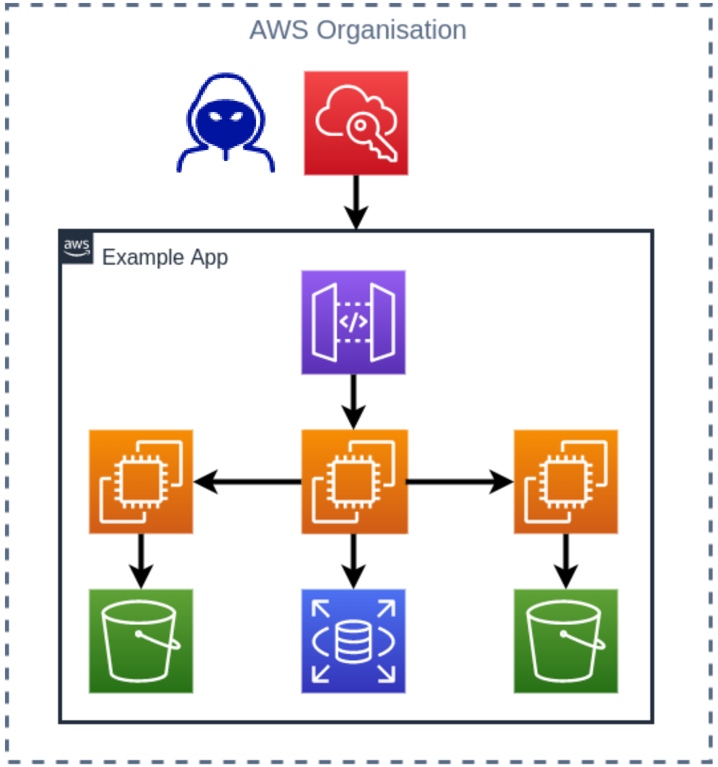
VECTORS WE'VE EXPLOITED



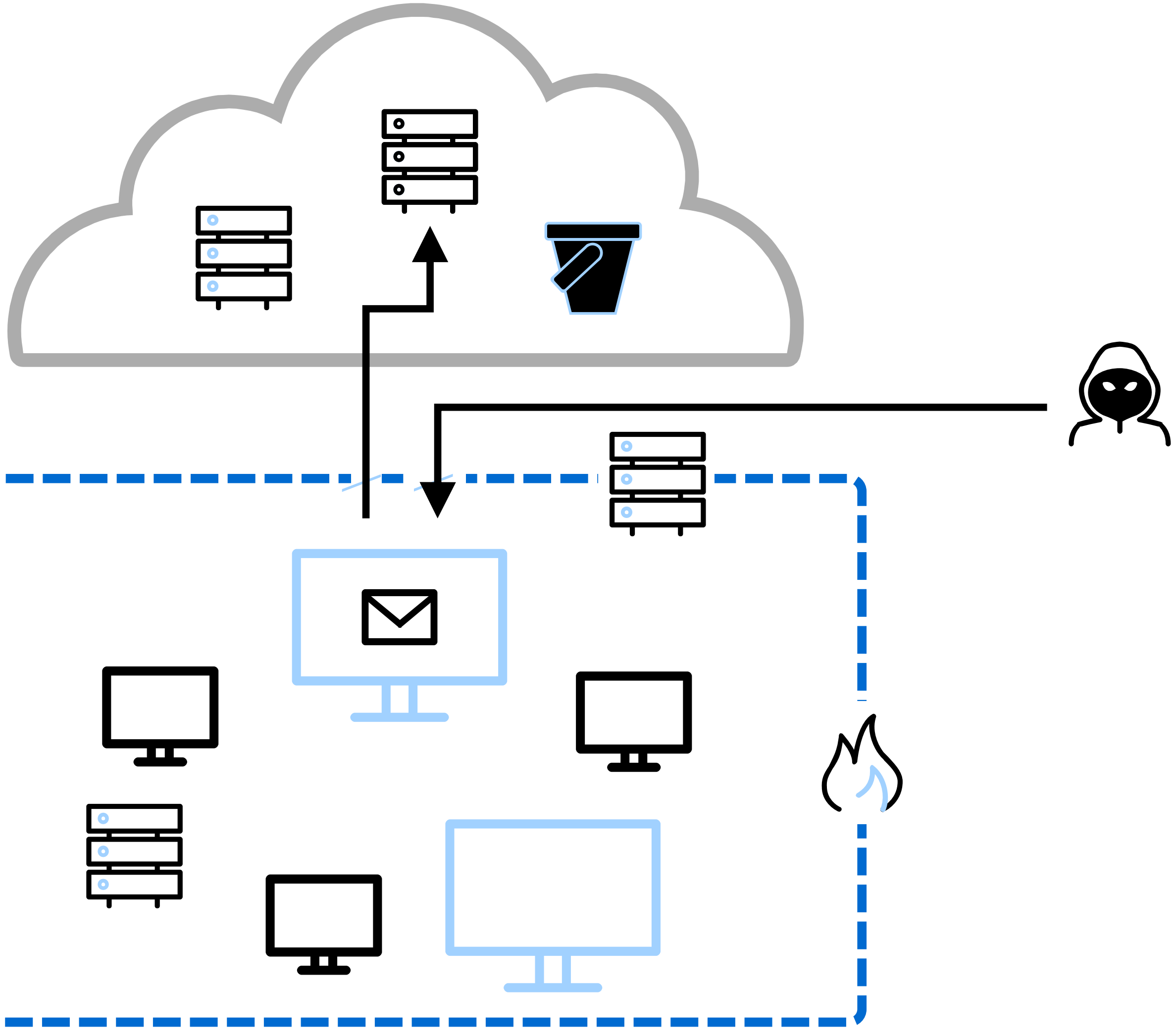
Pivot From Other Environments
Application Vulnerabilities
1
3
2
4
Identity Management
SCM / Continuous Delivery

IDENTITY MANAGEMENT EXPLOITATION



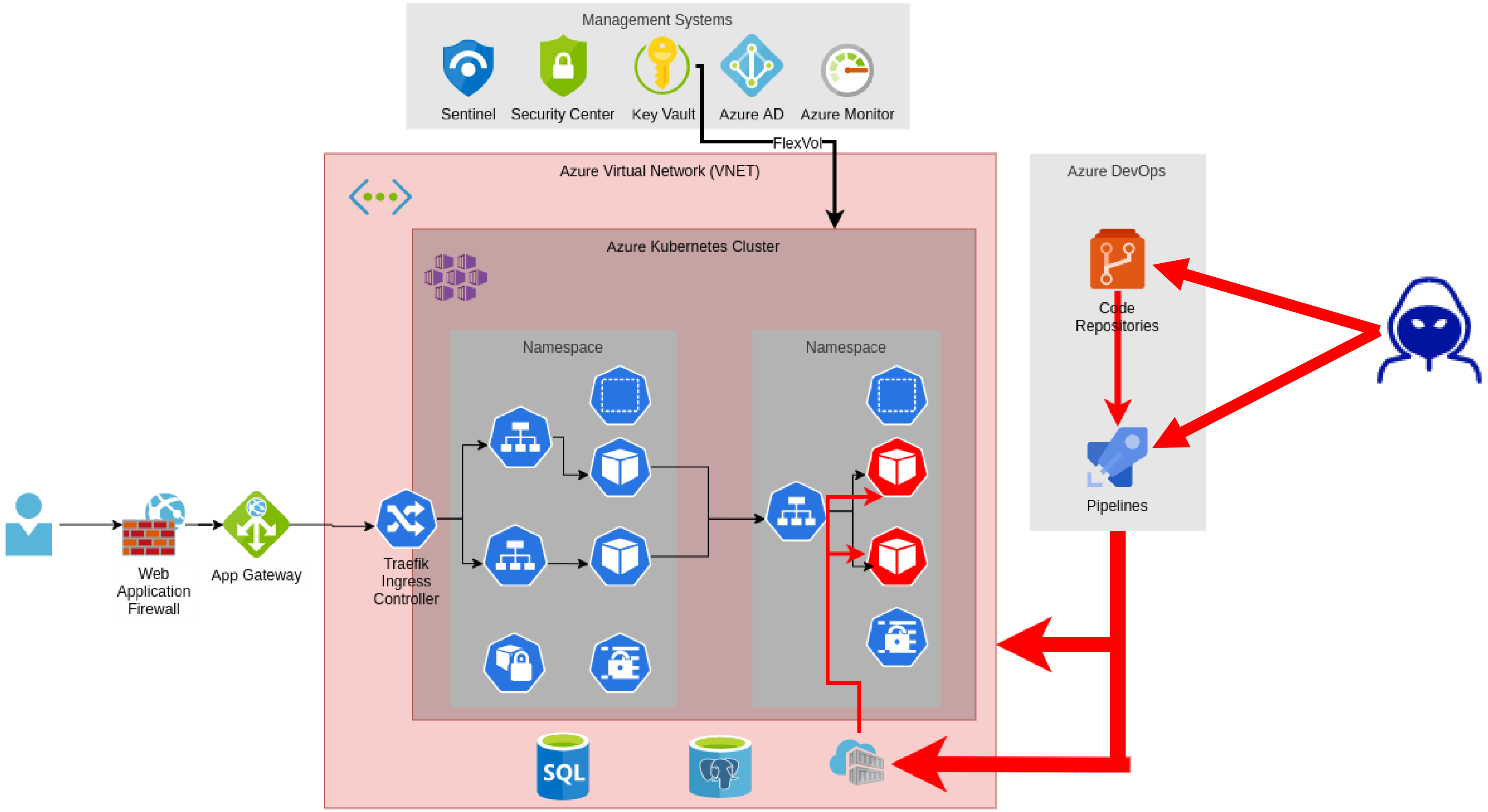


PIVOT FROM OTHER ENVIRONMENTS



LABS

SCM & CONTINUOUS DELIVERY



HOW DO I START?

01 Threat model your environment, identify attack paths

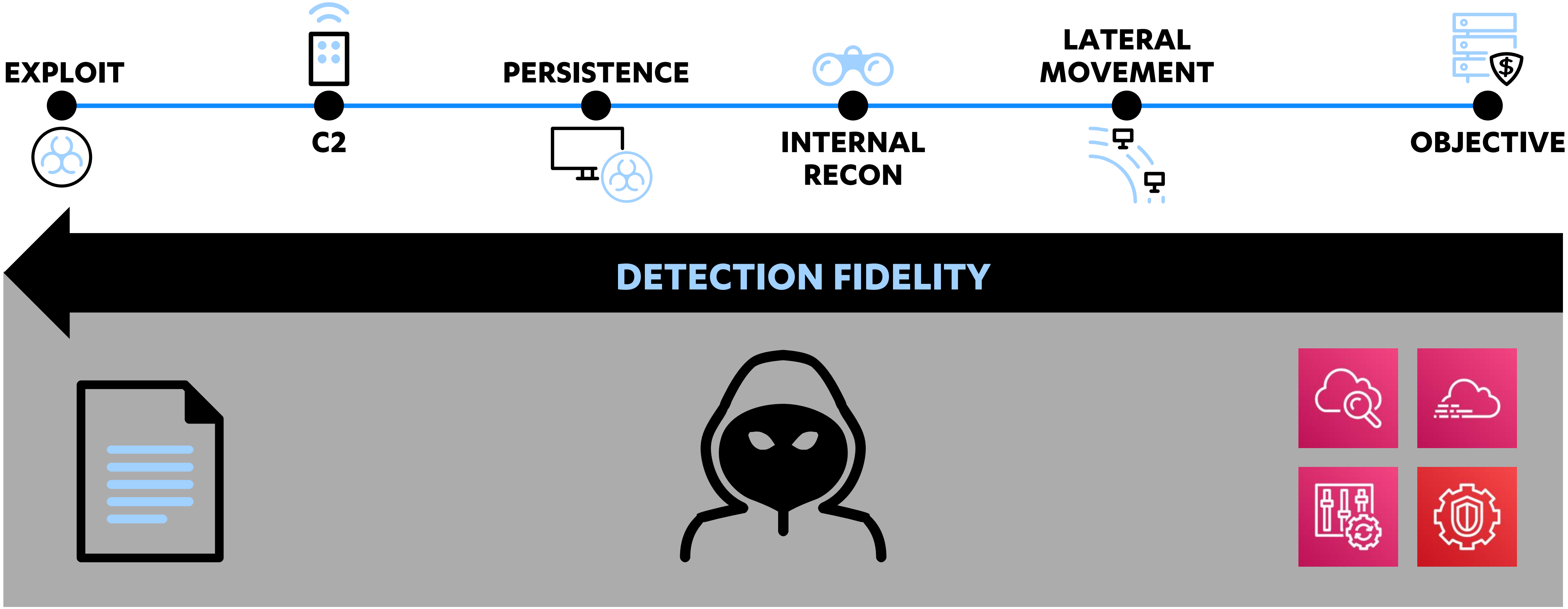
02 Prioritise attack paths

03 Understand the TTPs the attack paths consist of

04 Verify telemetry is available to defenders

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

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

LEONIDAS

LEONIDAS

Automated Attack Simulation

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

Framework automatically generates…

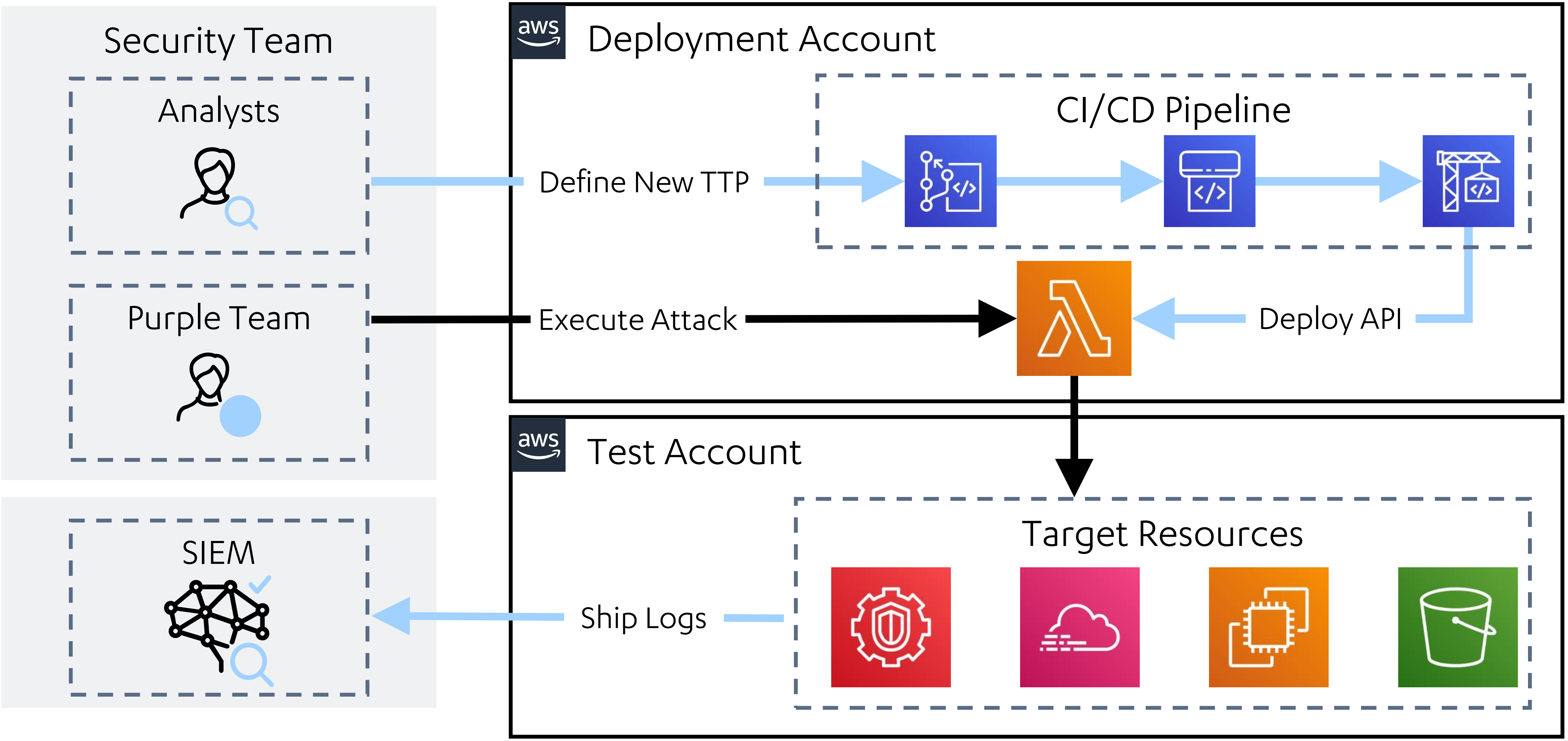
- Executor – serverless function
- Sigma detection rules
- Documentation

Executor

- User/role/service account impersonation
- Abstracts details away from analysts

LABS

LEONIDAS



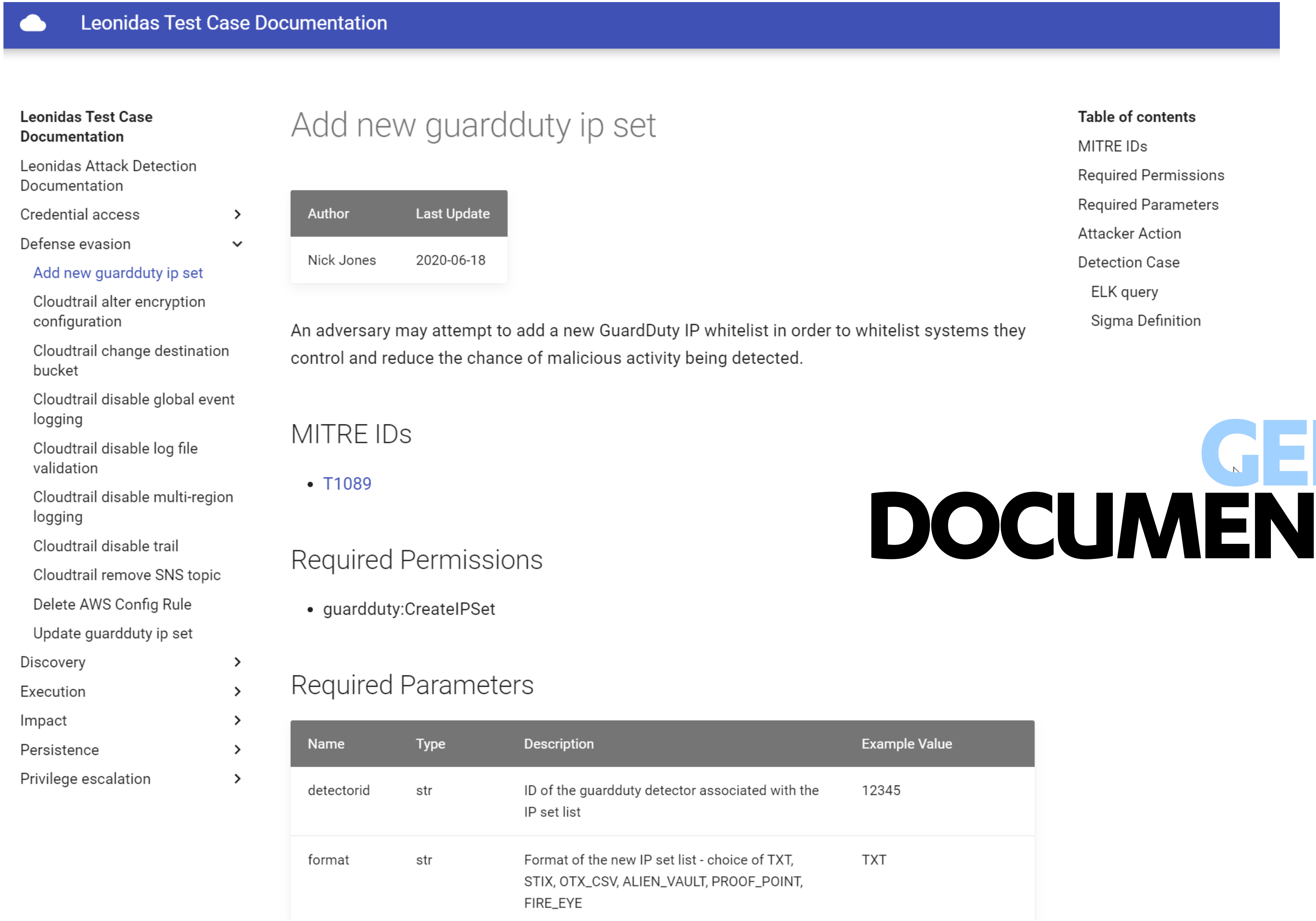
GENERATE ATTACK SIMULATION

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

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"
```

GENERATE DOCUMENTATION



Leonidas Test Case Documentation

Leonidas Test Case Documentation

Leonidas Attack Detection Documentation

- Credential access
- Defense evasion
  - Add new guardduty ip set
  - Cloudtrail alter encryption configuration
  - Cloudtrail change destination bucket
  - Cloudtrail disable global event logging
  - Cloudtrail disable log file validation
  - Cloudtrail disable multi-region logging
  - Cloudtrail disable trail
  - Cloudtrail remove SNS topic
  - Delete AWS Config Rule
  - Update guardduty ip set
- Discovery
- Execution
- Impact
- Persistence
- Privilege escalation

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

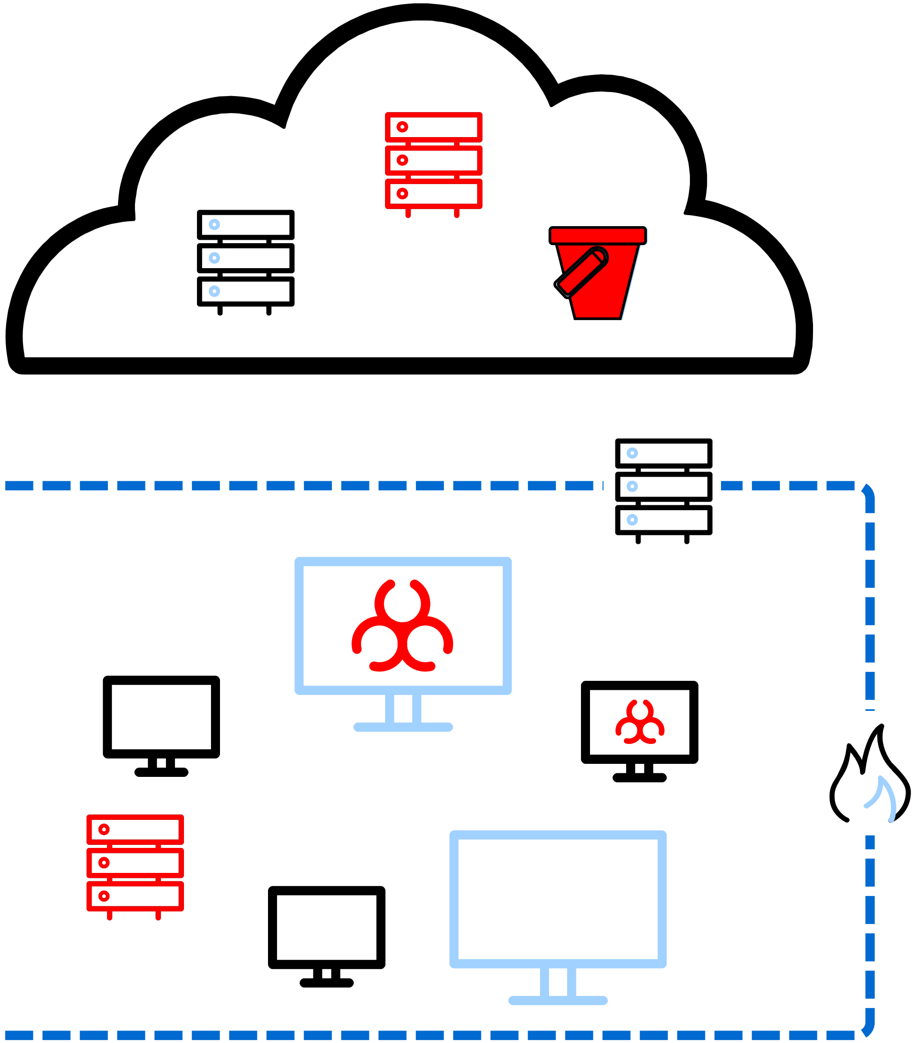
Required Permissions

- guardduty:CreateIPSet

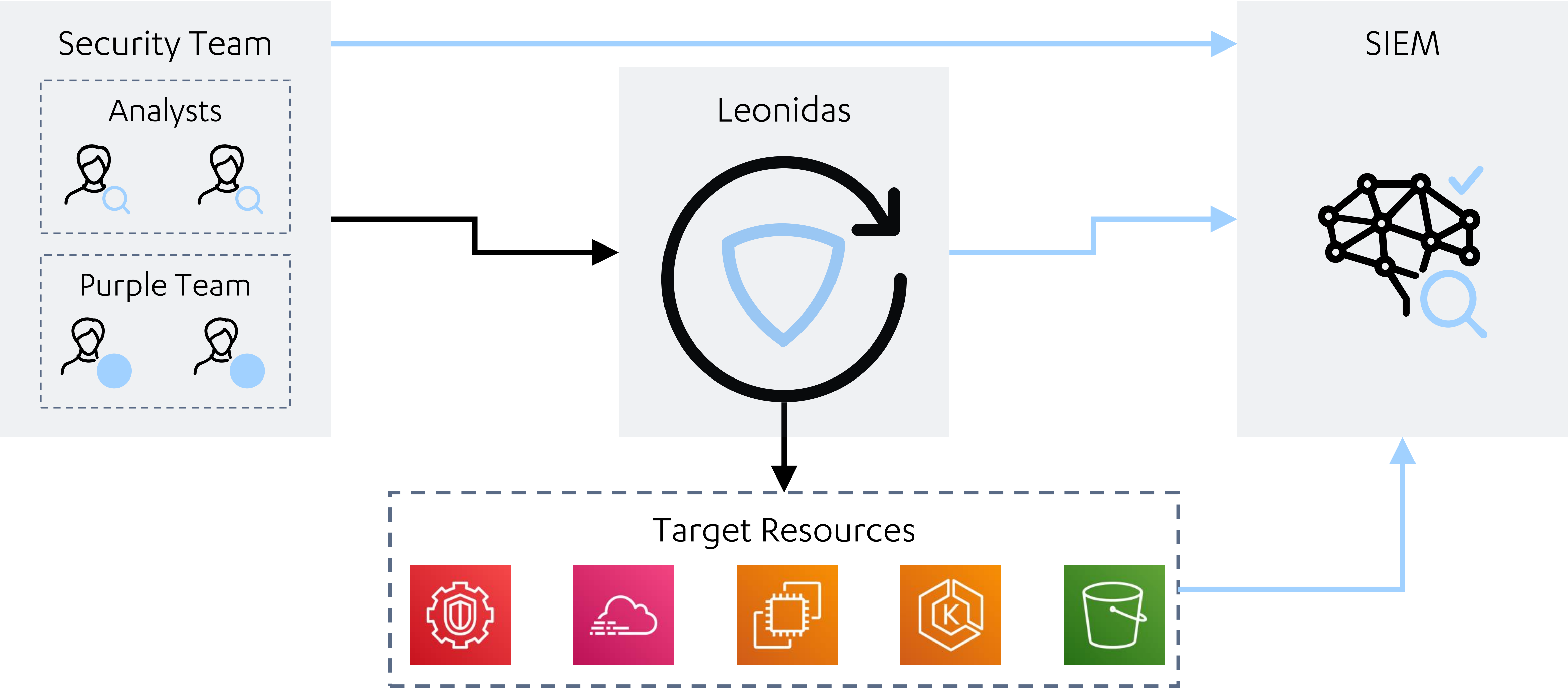
Required Parameters

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

CONTINUOUS TESTING



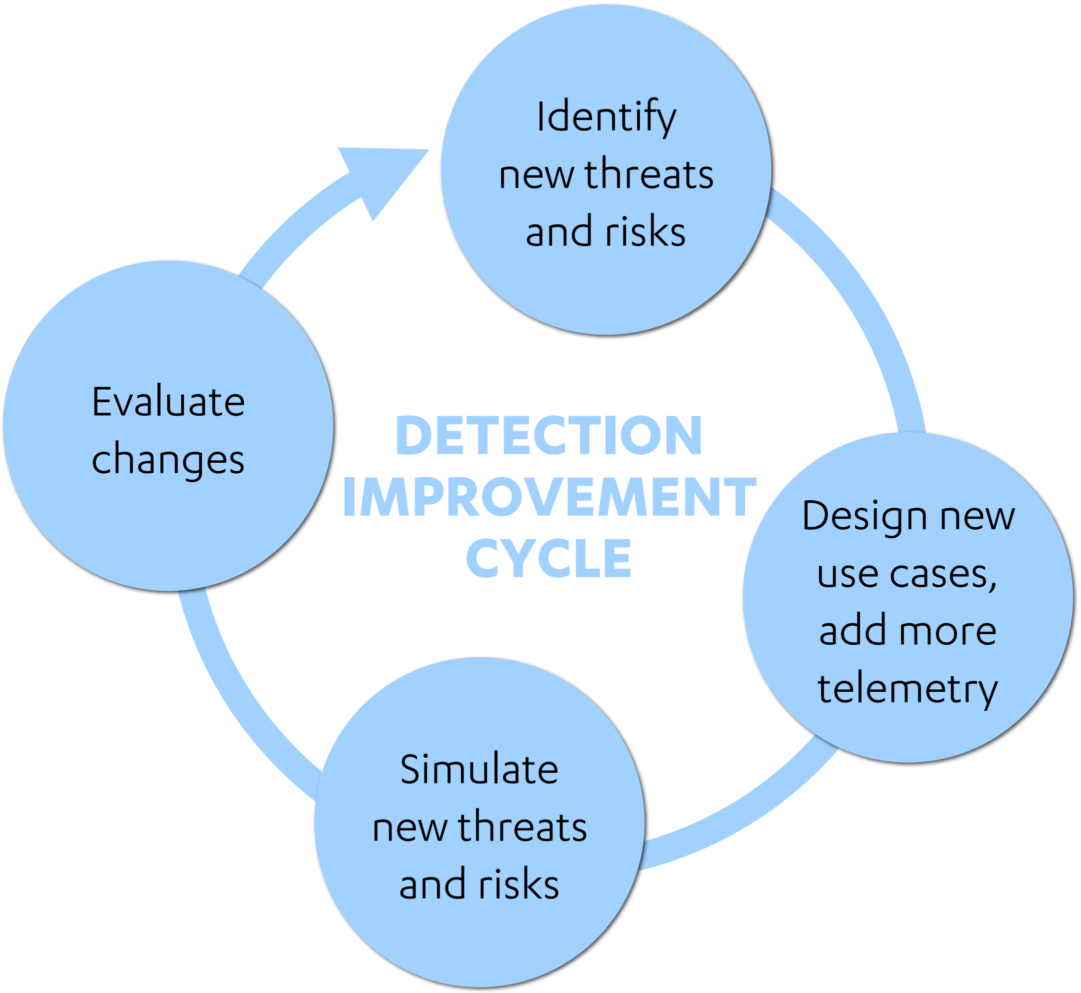
CONTINUOUS INTEGRATION



CONCLUSIONS

LABS

DETECTION IS A JOURNEY

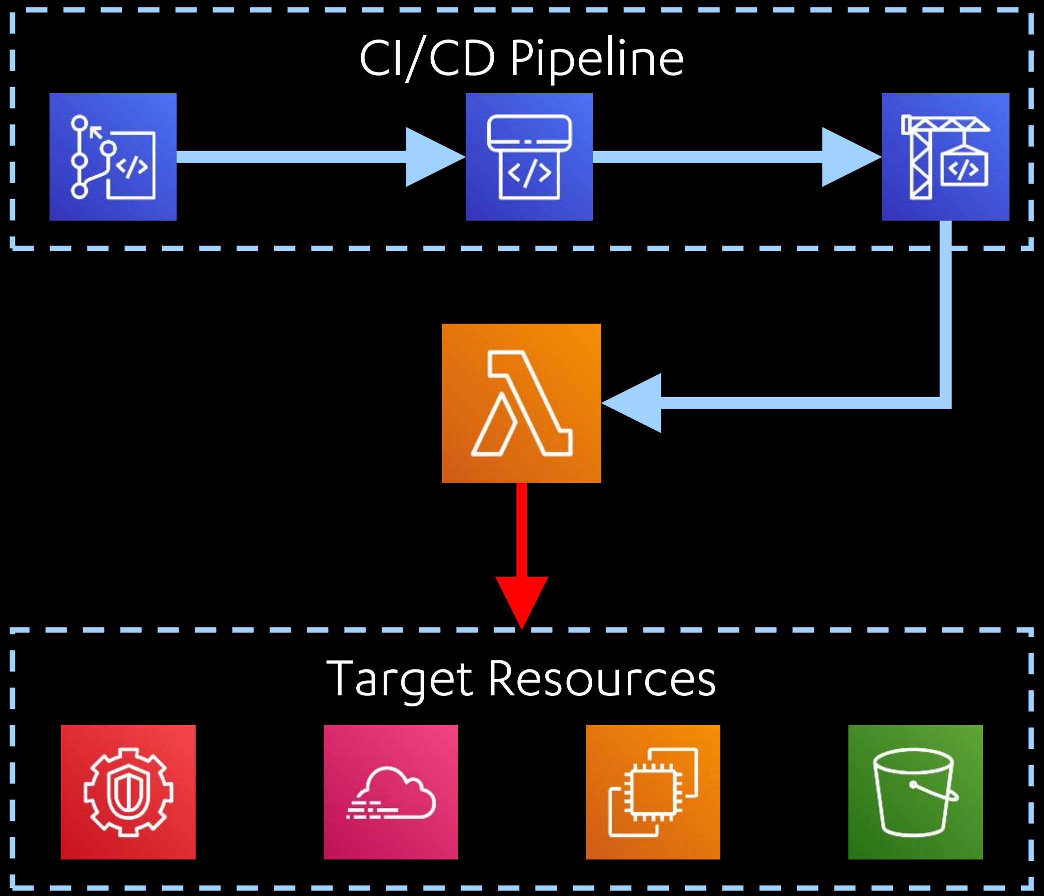

Identify new threats and risks
Design new use cases, add more telemetry
Simulate new threats and risks
Evaluate changes
DETECTION IMPROVEMENT CYCLE

Context is key, use it to your advantage

Cloud environments change, your detection will too

Codify and share 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 soonTM
- 45 test cases - more to come
- https://github.com/fsecurelabs/leonidas