F-Secure | LABS

BUILDING EFFECTIVE ATTACK DETECTION IN THE CLOUD

Alfie Champion & Nick Jones

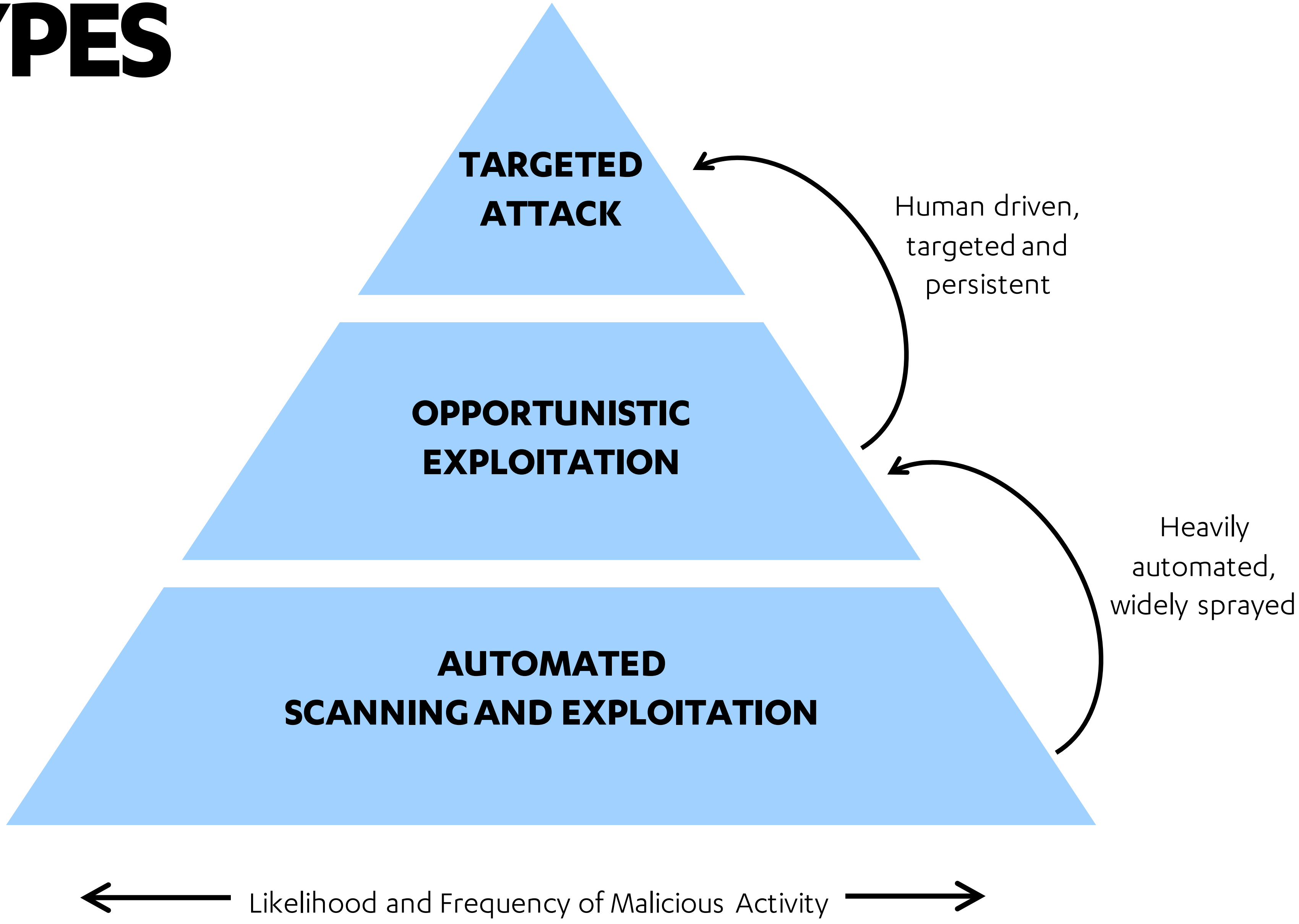
LABS

AGENDA

[illegible] DEVOPS [illegible]

ON-PREMISE VS CLOUD

ATTACK TYPES



TARGETED ATTACK

OPPORTUNISTIC EXPLOITATION

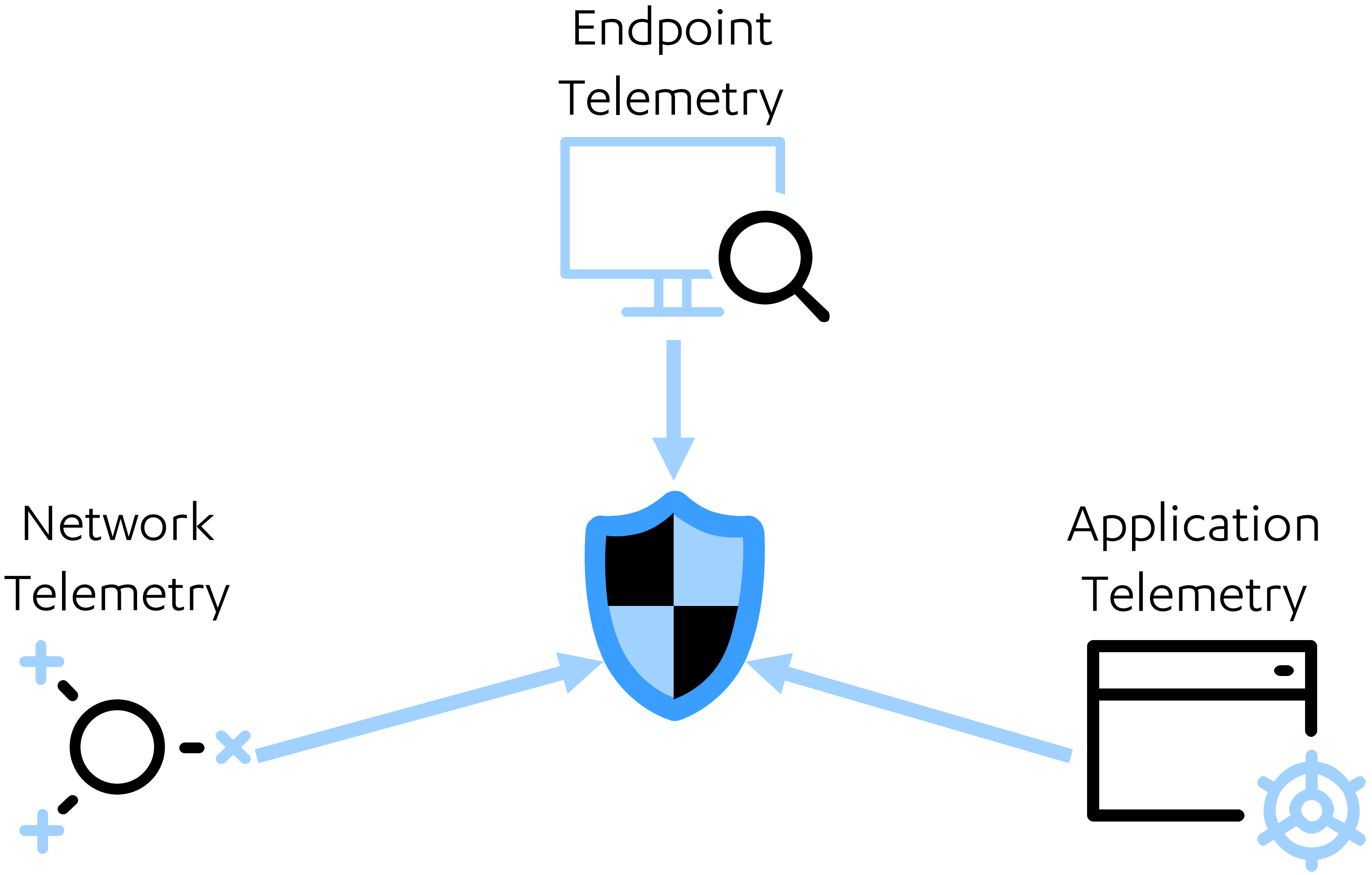
AUTOMATED SCANNING AND EXPLOITATION

Human driven, targeted and persistent

Heavily automated, widely sprayed

Likelihood and Frequency of Malicious Activity

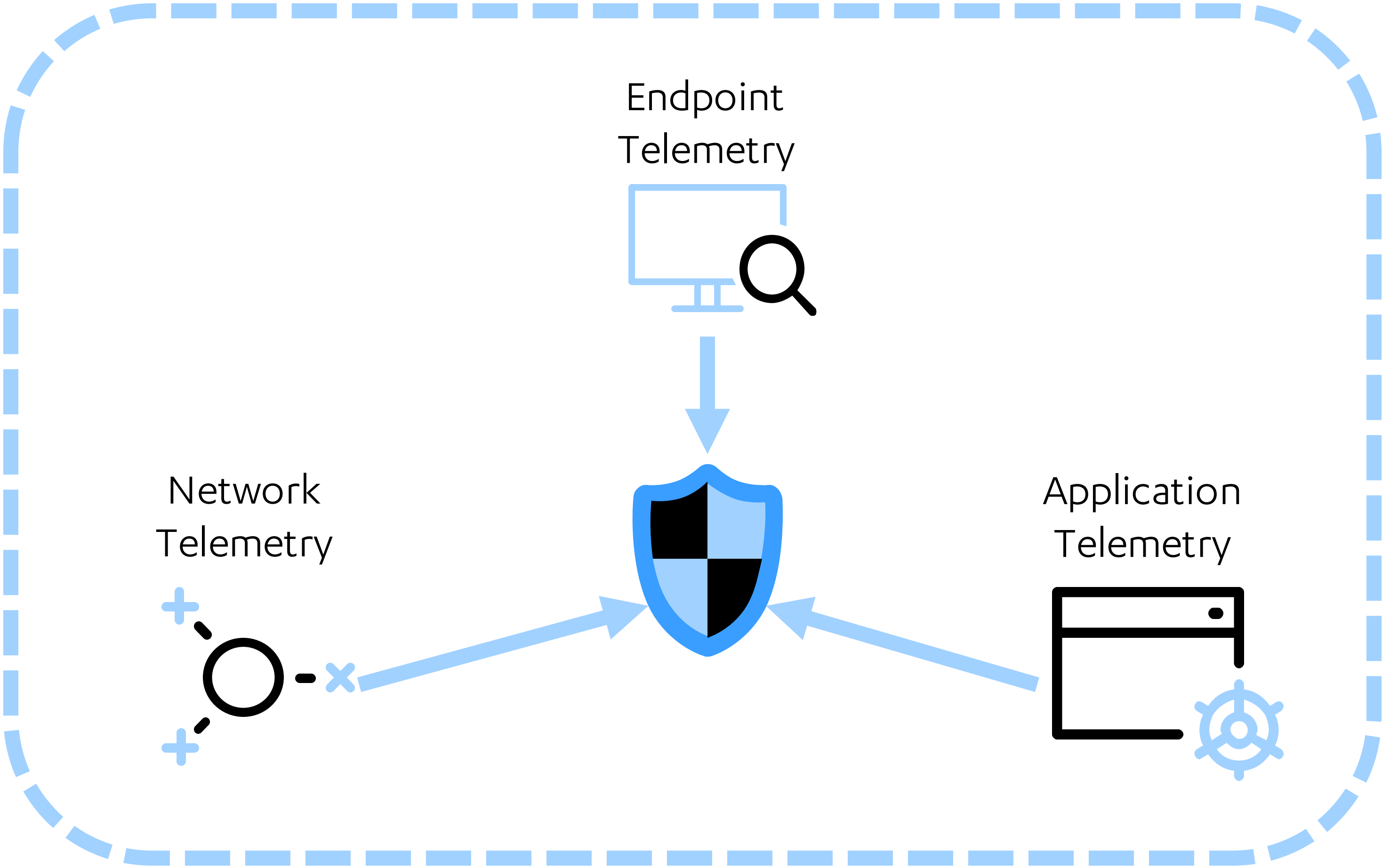
ON-PREMISE TELEMETRY



LABS

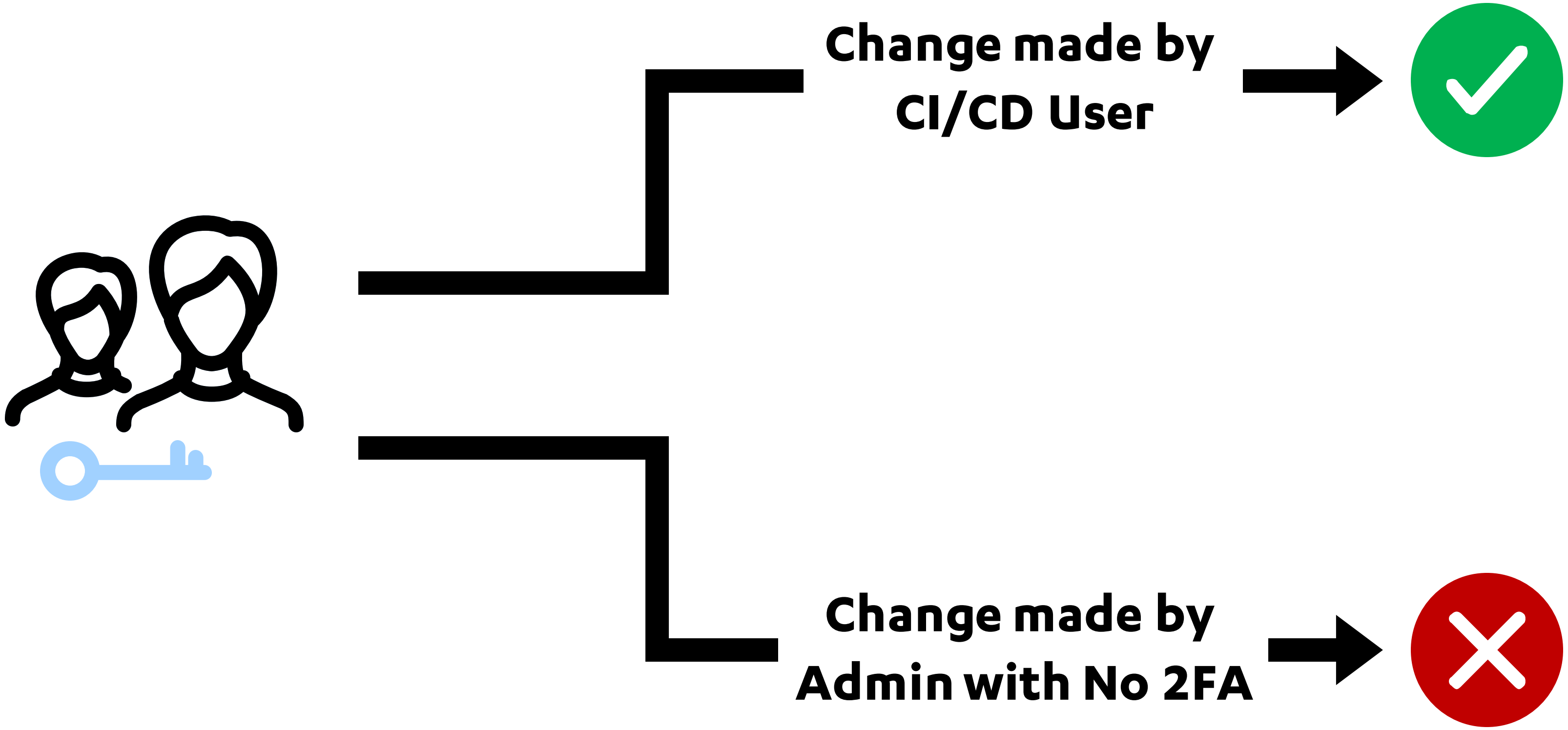
CLOUD TELEMETRY

Control Plane Telemetry



LABS

CONTEXT IS KEY

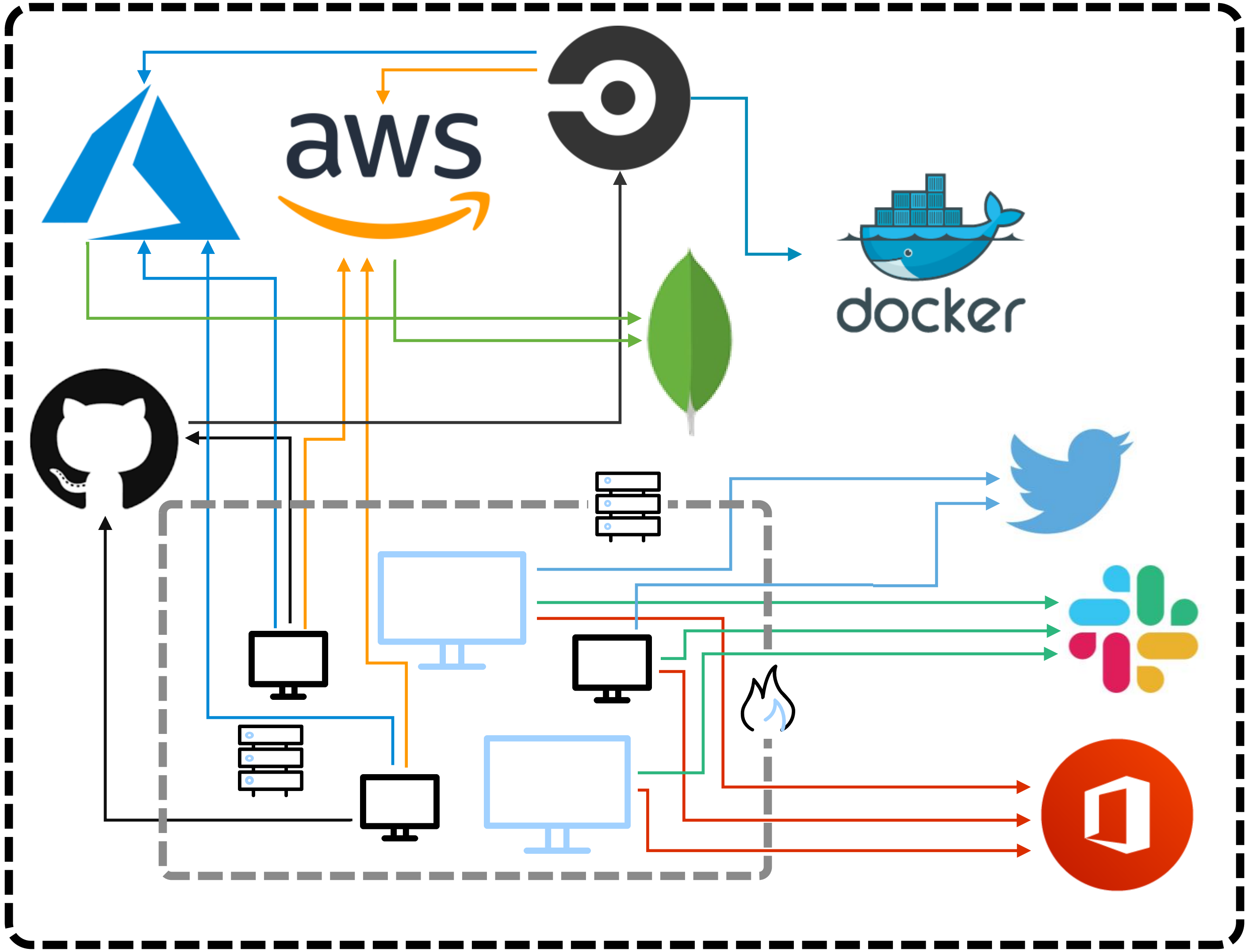


Change made by CI/CD User → ✓

Change made by Admin with No 2FA → ✗

LABS

ENTERPRISE CLOUD ADOPTION

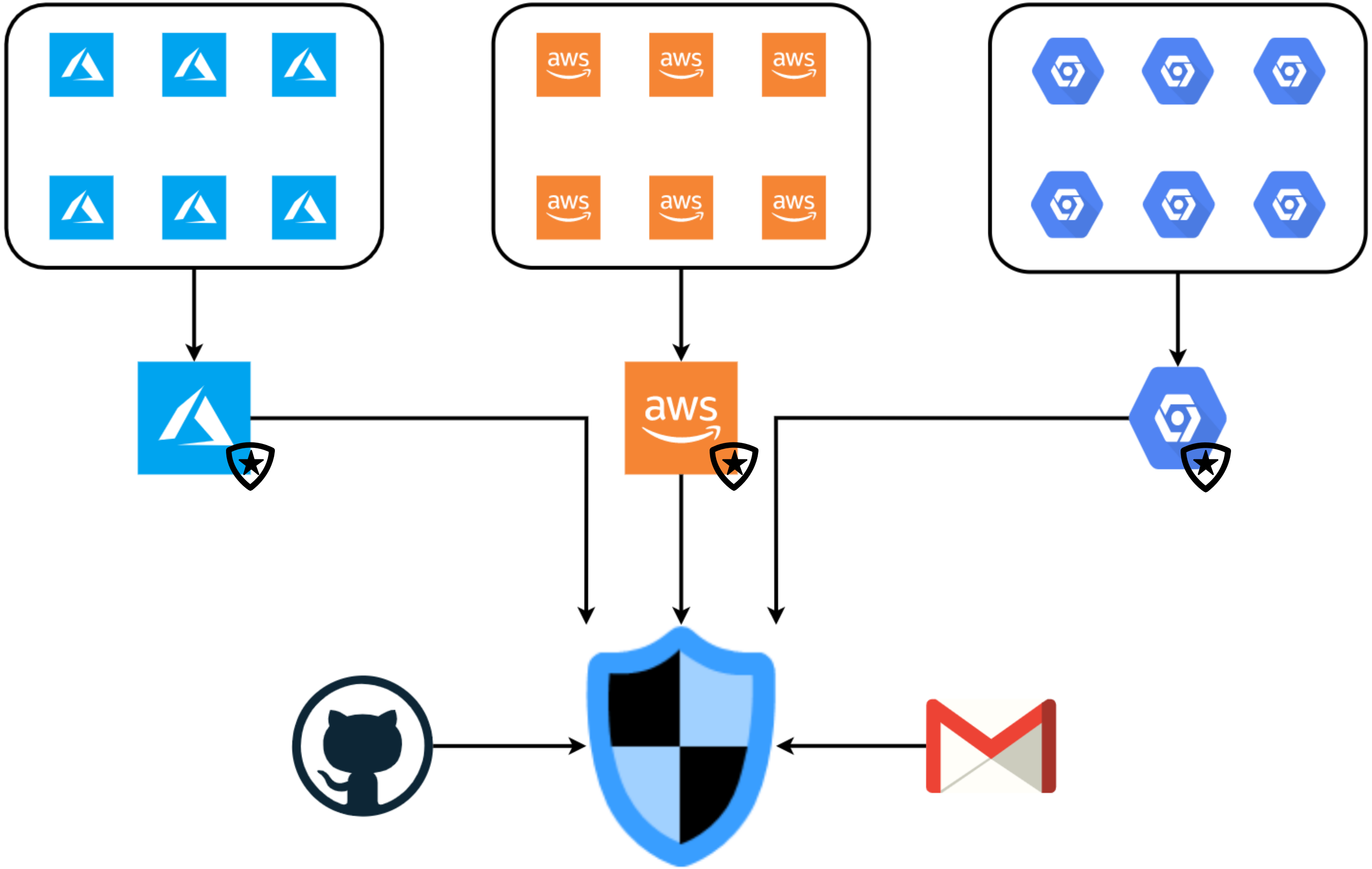


F-Secure | LABS

DESIGNING YOUR CLOUD DETECTION STACK

LABS

CENTRALISE EVERYTHING



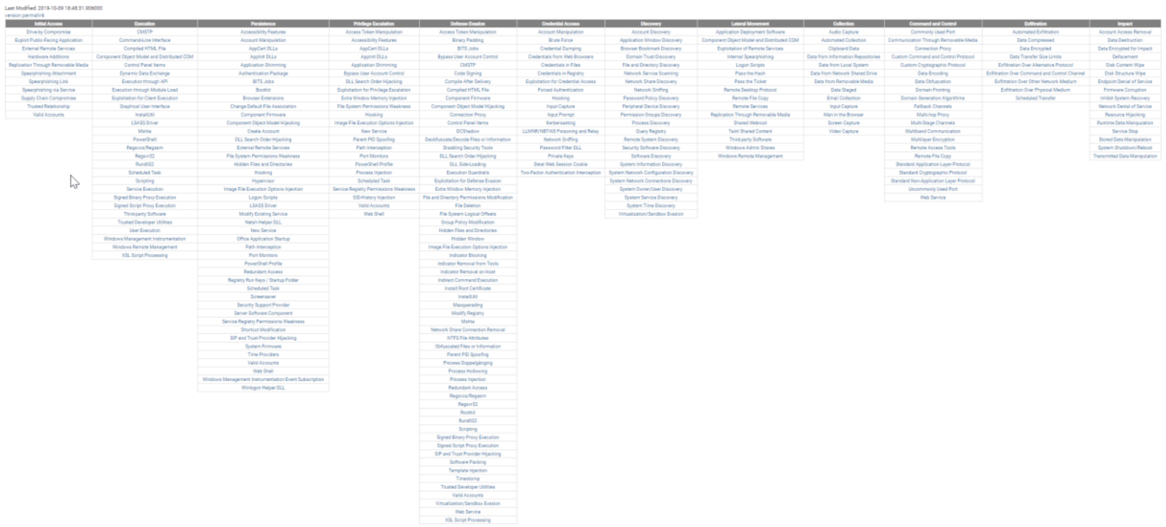
DATA SOURCES

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

F-Secure | LABS

THE THREAT INTELLIGENCE PROBLEM

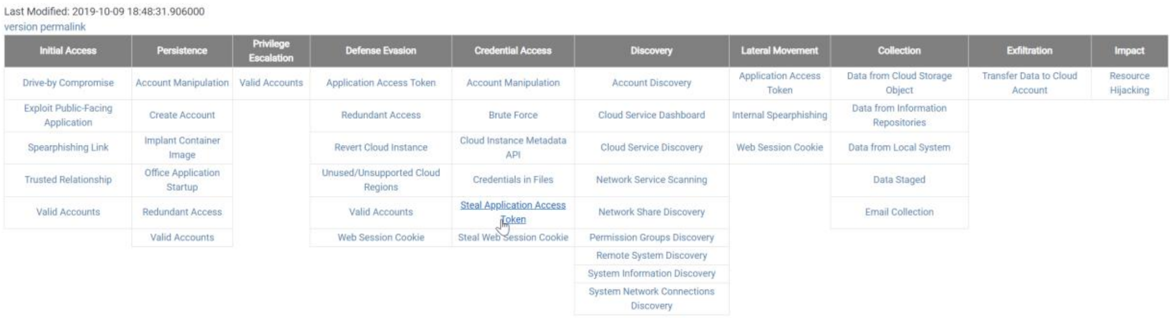
ON-PREMISE VS CLOUD ATT&CK



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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture
Valid Accounts	InstallUtil	Component Firmware	Hooking	Connection Proxy	Input Prompt
	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	Control Panel Items	Kerberoasting
	Mshta	Create Account	New Service	DCShadow	LLMNR/NBT-NS Poisoning and Relay
	PowerShell	DLL Search Order Hijacking	Parent PID Spoofing	Deobfuscate/Decode Files or Information	Network Sniffing
	Regsvcs/Regasm	External Remote Services	Path Interception	Disabling Security Tools	Password Filter DLL
	Regsvr32	File System Permissions Weakness	Port Monitors	DLL Search Order Hijacking	Private Keys
	Rundll32	Hidden Files and Directories	PowerShell Profile	DLL Side-Loading	Steal Web Session Cookie
	Scheduled Task	Hooking	Process Injection	Execution Guardrails	Two-Factor Authentication Interception
	Scripting	Hypervisor	Scheduled Task	Exploitation for Defense Evasion	
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Extra Window Memory Injection	
	Signed Binary Proxy Execution	Logon Scripts	SID-History Injection	File and Directory Permissions Modification	
	Signed Script Proxy Execution	LSASS Driver	Valid Accounts	File Deletion	
	Third-party Software	Modify Existing Service	Web Shell	File System Logical Offsets	
	Trusted Developer Utilities	Netsh Helper DLL		Group Policy Modification	
	User Execution	New Service		Hidden Files and Directories	
	Windows Management Instrumentation	Office Application Startup		Hidden Window	
	Windows Remote Management	Path Interception		Image File Execution Options Injection	
	XSL Script Processing	Port Monitors		Indicator Blocking	
		PowerShell Profile		Indicator Removal from Tools	
		Redundant Access		Indicator Removal on Host	
		Registry Run Keys / Startup Folder		Indirect Command Execution	
		Scheduled Task		Install Root Certificate	
		Screensaver		InstallUtil	
		Security Support Provider		Masquerading	
		Server Software Component		Modify Registry	
		Service Registry Permissions Weakness		Mshta	
		Shortcut Modification		Network Share Connection Removal	
		SIP and Trust Provider Hijacking		NTFS File Attributes	
		System Firmware		Obfuscated Files or Information	
		Time Providers		Parent PID Spoofing	
		Valid Accounts		Process Doppelgänging	
		Web Shell		Process Hollowing	
		Windows Management Instrumentation Event Subscription		Process Injection	
		Winlogon Helper DLL		Redundant Access	
				Regsvcs/Regasm	
				Regsvr32	
				Rootkit	
				Rundll32	
				Scripting	
				Signed Binary Proxy Execution	
				Signed Script Proxy Execution	
				SIP and Trust Provider Hijacking	
				Software Packing	
				Template Injection	
				Timestomp	
				Trusted Developer Utilities	
				Valid Accounts	
				Virtualization/Sandbox Evasion	
				Web Service	
				XSL Script Processing	

Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Network Denial of Service
Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Resource Hijacking
Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
Query Registry	Taint Shared Content	Video Capture	Multiband Communication		Service Stop
Remote System Discovery	Third-party Software		Multilayer Encryption		Stored Data Manipulation
Security Software Discovery	Windows Admin Shares		Remote Access Tools		System Shutdown/Reboot
Software Discovery	Windows Remote Management		Remote File Copy		Transmitted Data Manipulation
System Information Discovery			Standard Application Layer Protocol		
System Network Configuration Discovery			Standard Cryptographic Protocol		
System Network Connections Discovery			Standard Non-Application Layer Protocol		
System Owner/User Discovery			Uncommonly Used Port		
System Service Discovery			Web Service		
System Time Discovery					
Virtualization/Sandbox Evasion					

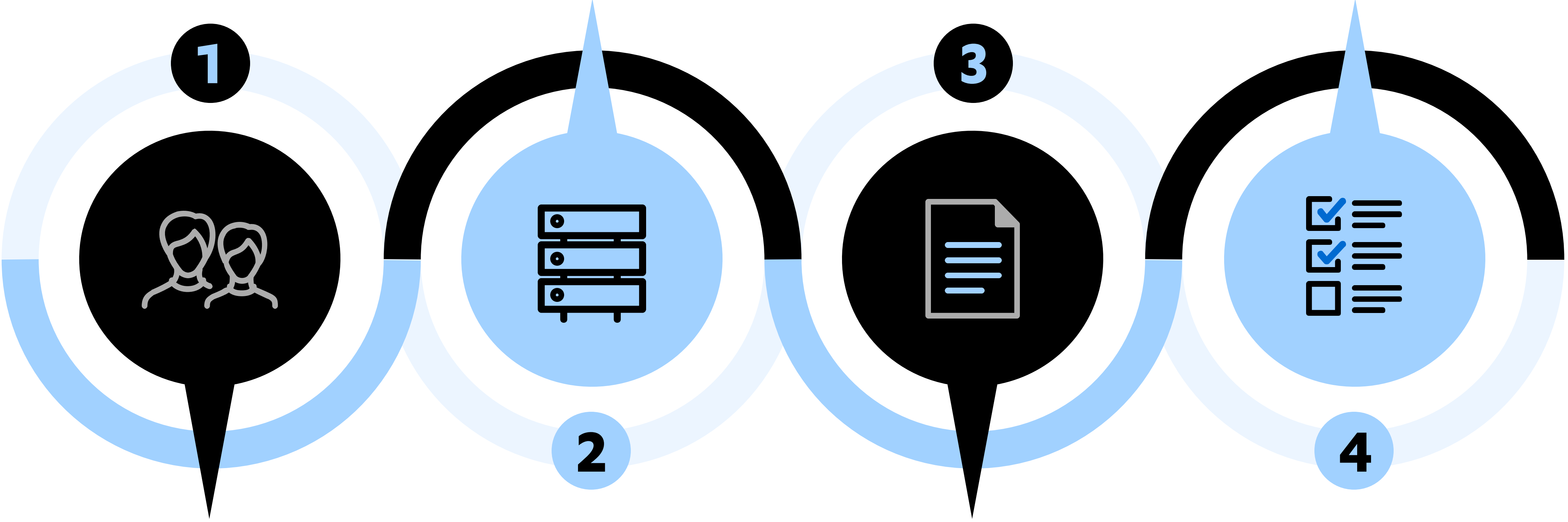


Last Modified: 2019-10-09 18:48:31.906000
version permalink

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				

WHAT'S AN ATTACKER LIKELY TO DO?

VECTORS WE'VE EXPLOITED



1

Identity Management

2

Pivot From Other Environments

3

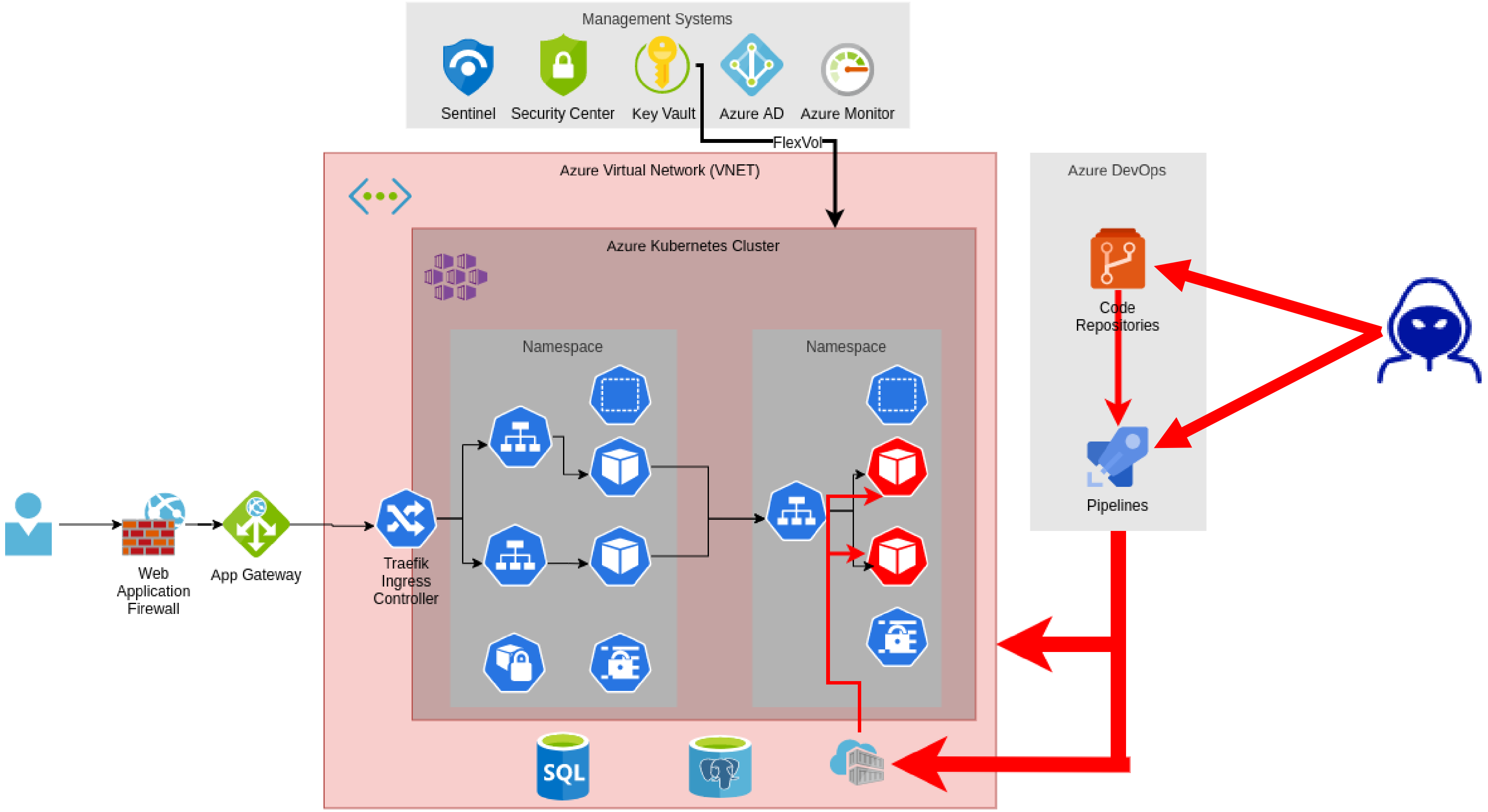
SCM / Continuous Delivery

4

Application Vulnerabilities

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.

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

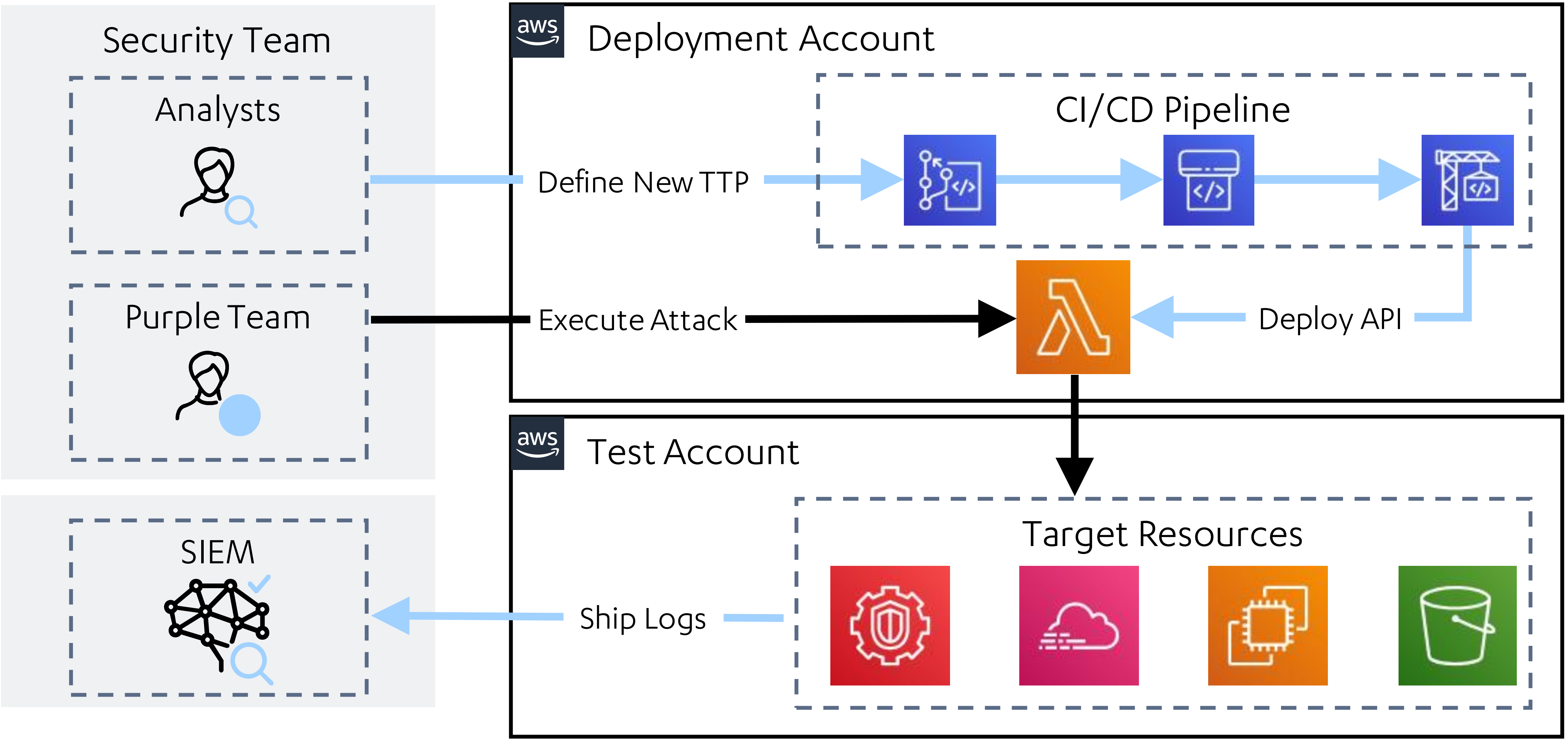
John Lambert – The Githubification of Infosec

http://youtu.be/B3o-9z3Eitg

https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1

LEONIDAS

LEONIDAS


Security Team
Analysts
Purple Team
SIEM
aws
Deployment Account
CI/CD Pipeline
Define New TTP
Execute Attack
Deploy API
aws
Test Account
Target Resources
Ship Logs

GENERATE ATTACK SIMULATION

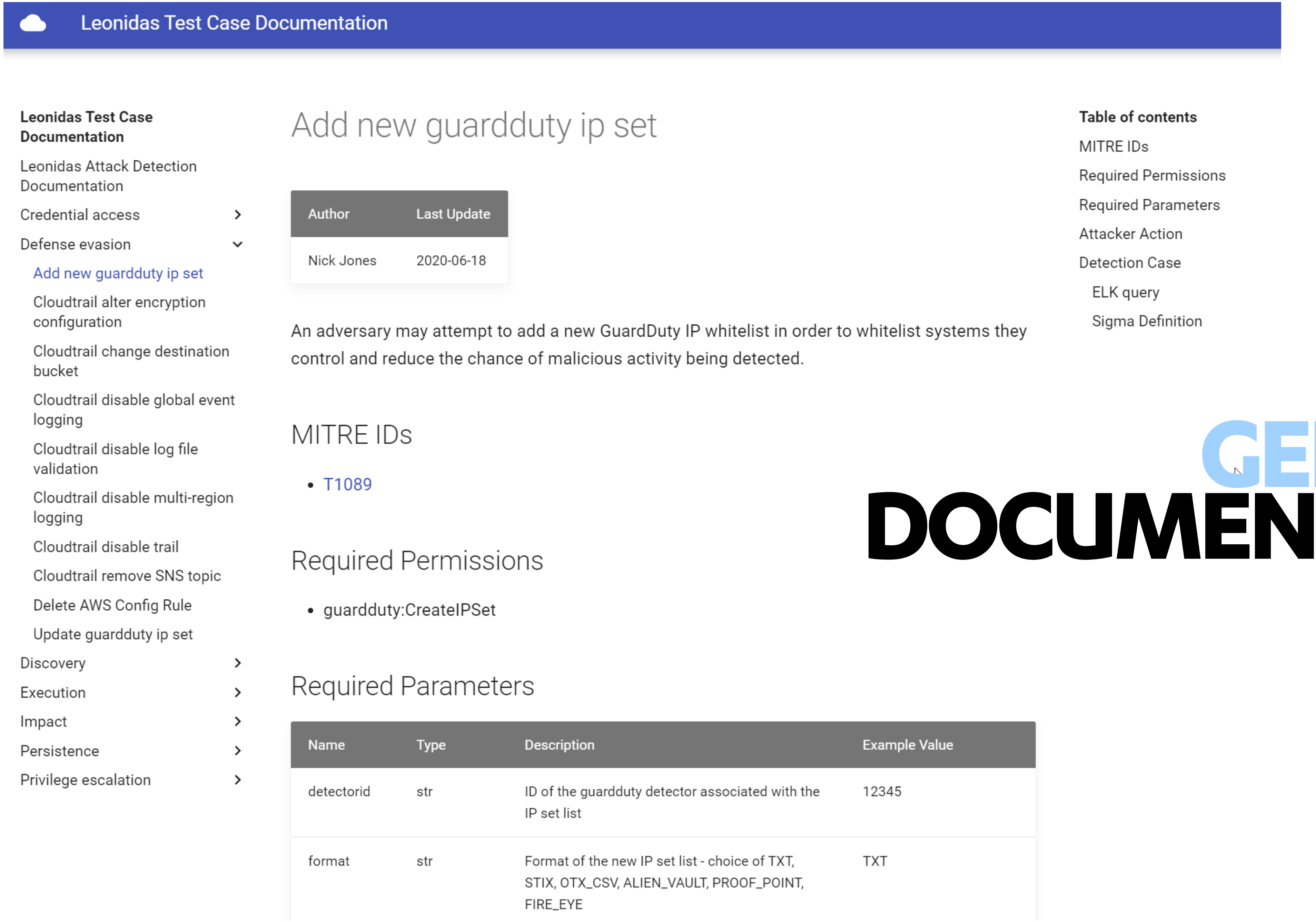
```
- name: Enumerate Cloudtrails for Current Region
  permissions:
  - cloudtrail:DescribeTrails
  input_arguments:
  executors:
    leonidas_aws:
      implemented: True
      clients:
        - cloudtrail
      code: |
        result = clients["cloudtrail"].describe_trails()
```

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"
```

LABS

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

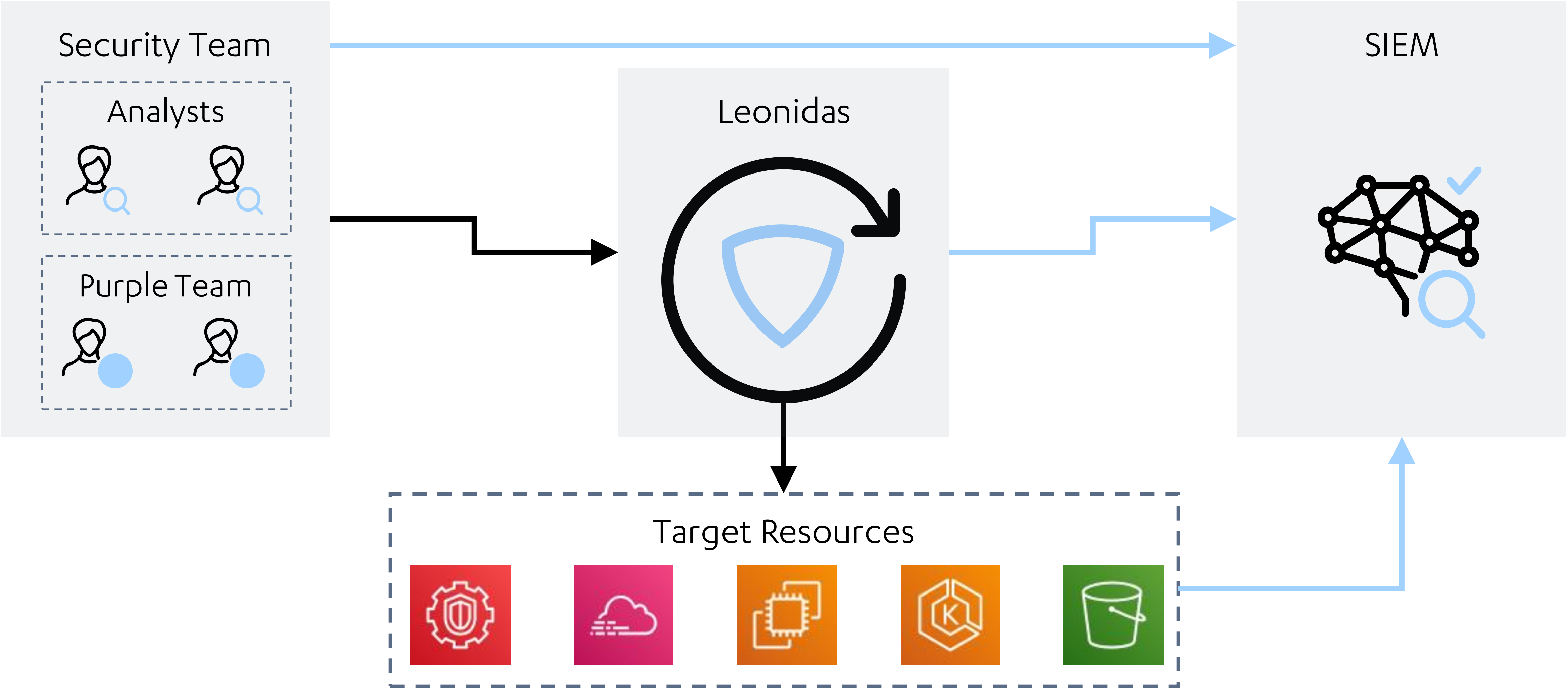
Required Parameters

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

Table of contents

DEMO TIME!

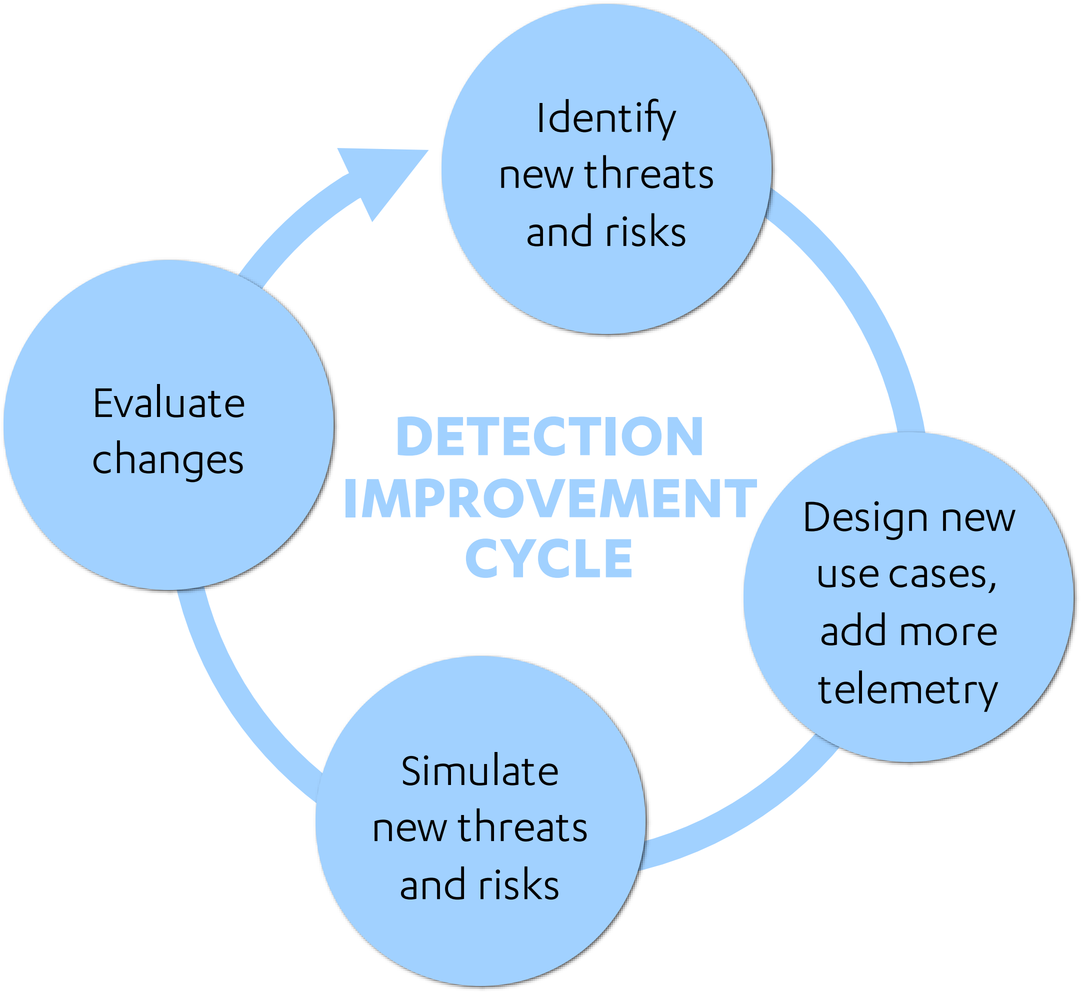
CONTINUOUS INTEGRATION



CONCLUSIONS

LABS

DETECTION IS A JOURNEY

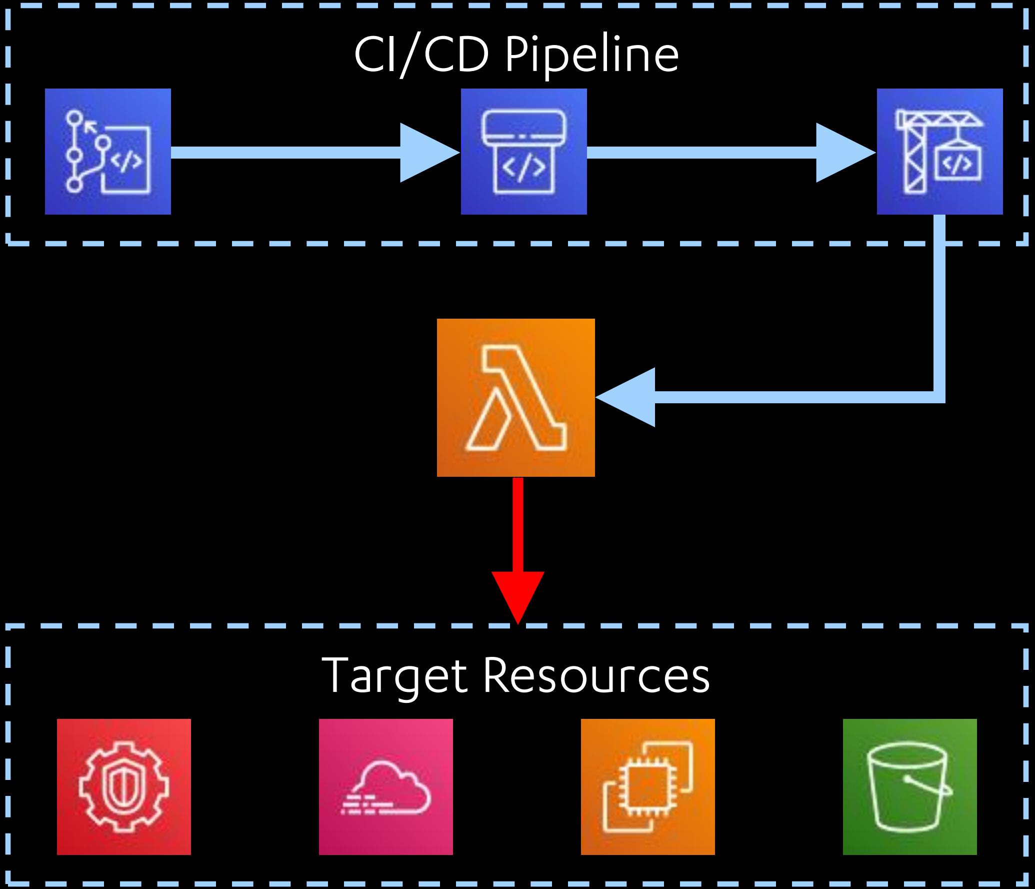

Identify new threats and risks
Design new use cases, add more telemetry
Simulate new threats and risks
Evaluate changes
DETECTION IMPROVEMENT CYCLE

Context is key, use it to your advantage

Cloud environments change, your detection will to

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 on the roadmap
- 45 test cases - more to come
- https://github.com/fsecurelabs/leonidas