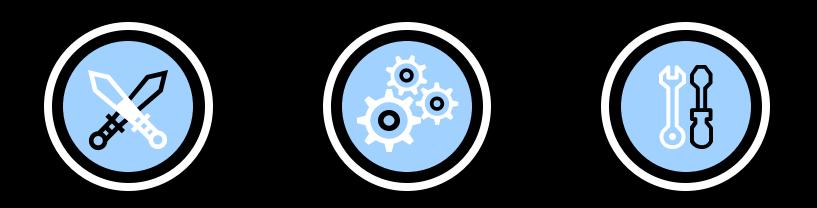


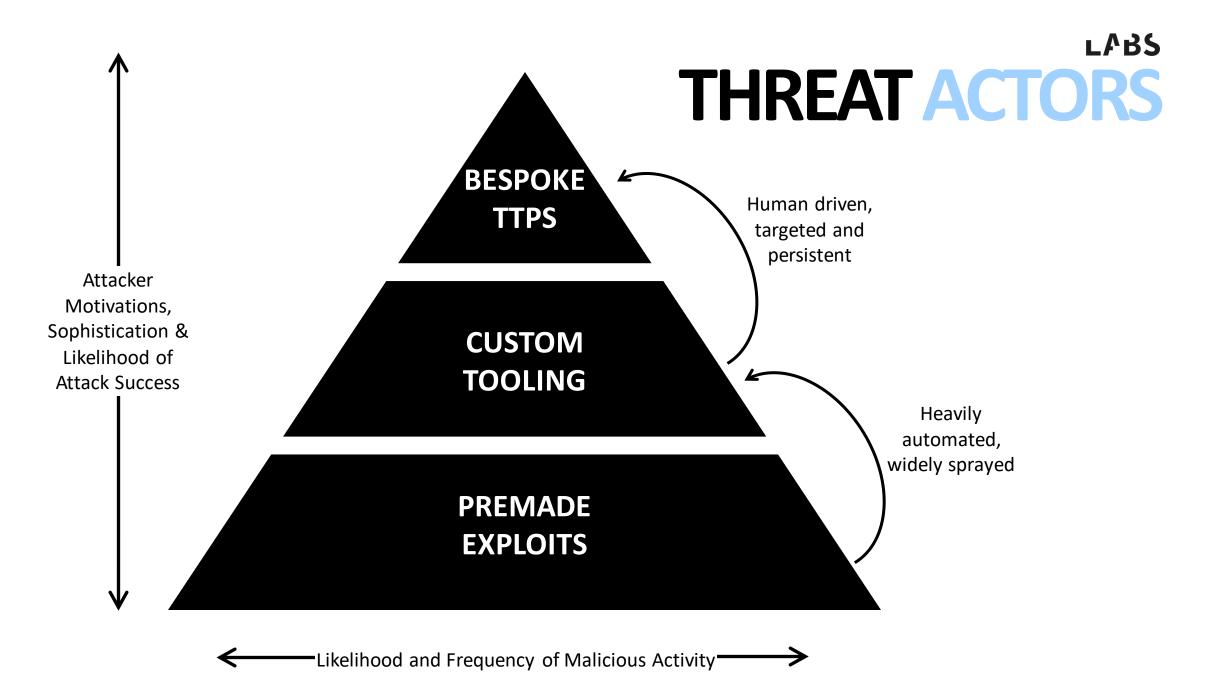
CLOUD-NATIVE DETECTION ANDSIMULATION

Nick Jones – DEF CON 28 Cloud Village

AGENDA



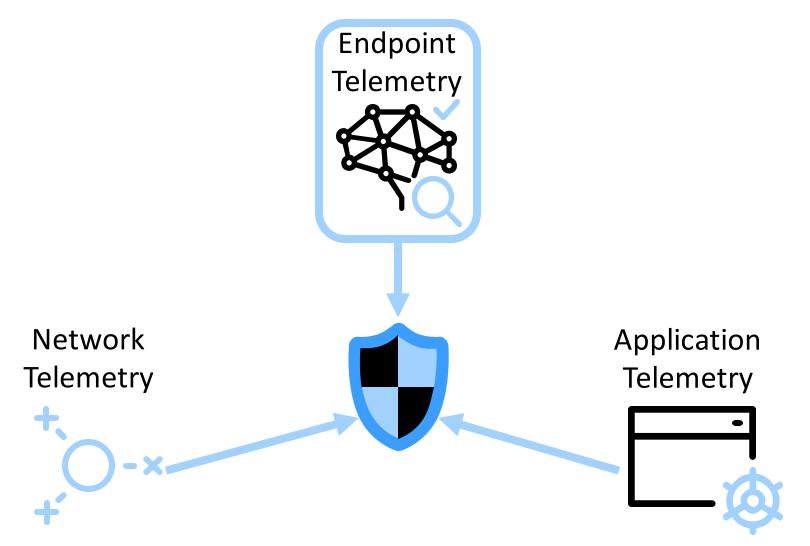
BRIRKINSBRVALKSRODDER EGTON





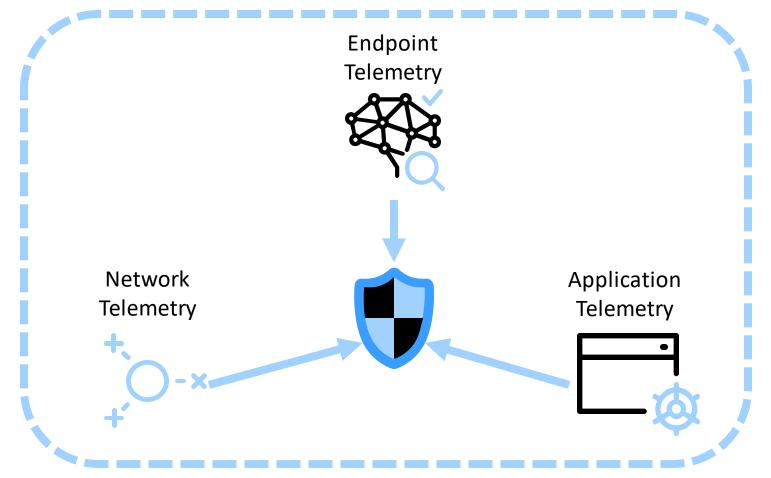
ON-PREMISE VS CLOUD

ON-PREMISE TELEMETRY

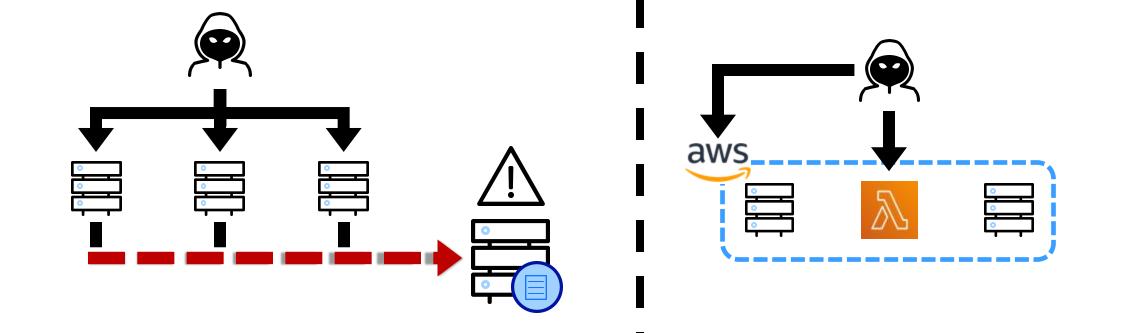


CLOUD TELEMETRY

Control Plane Telemetry



ON-PREMISE VS CLOUD DETECTION





HOW CLOUD DETECTION DIFFERS

UNCERTAINTY OF MALICIOUS INTENT

Fewer actions in the cloud are obviously bad compared to onpremise, 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.



Ø

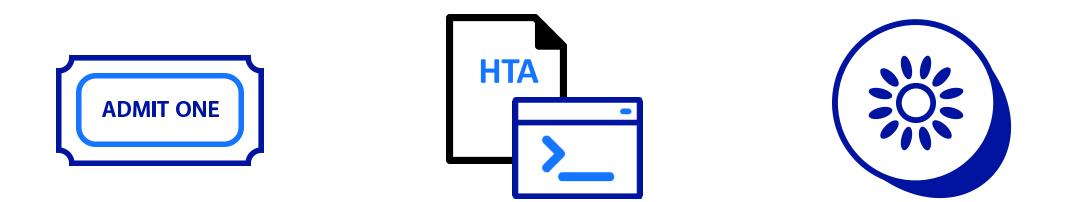
VISIBILITY IS EASIER

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

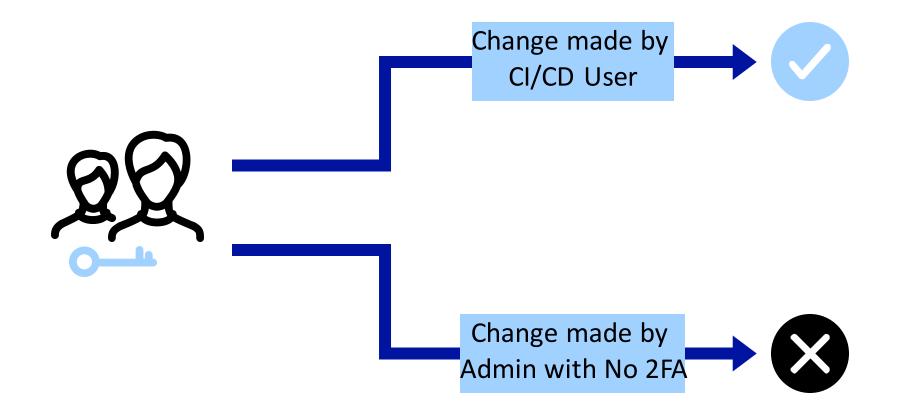
Attackers leveraging continuous delivery to abuse stolen credentials to bitcoin mine. It's easier to automate targeted attacks too

MINDSET SHIFT

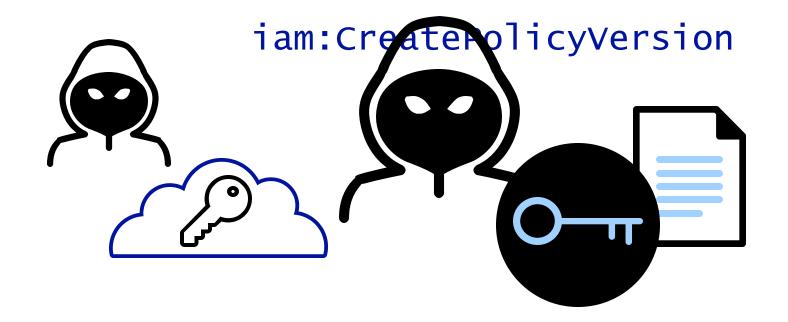


CERTAINTY OF MALICIOUS INTENT

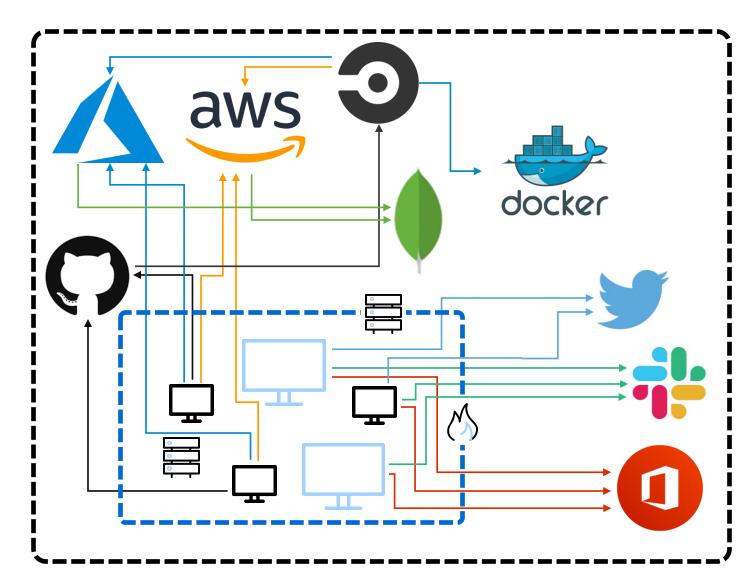
CONTEXT IS KEY



LABS



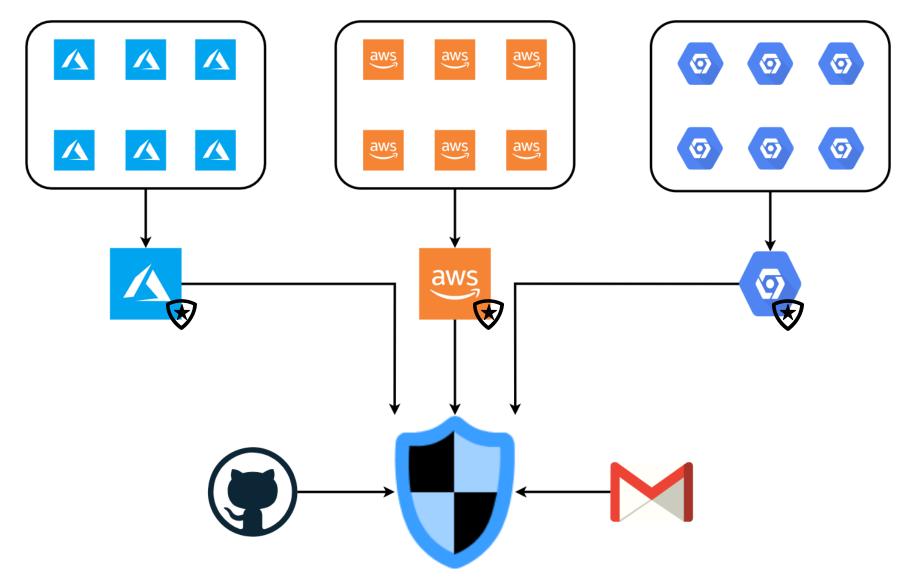
ENTERPRISE CLOUD ADOPTION





DESIGNING YOUR CLOUD DETECTION STACK

CENTRALISE EVERYTHING



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

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

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



THE THREAT INTELLIGENCE PROBLEM

ON-PREMISE VS CLOUD ATT&CK

Initial Access	Emoution	Penistence	Phylinge Escalation	Defense Deuton	Credential Access	Discovery	Lateral Movement				Impet	Last Modified: 2019-10-09	10,40.31.900000								
tive by Compromise Public-Facing Application	CMSTP Command-Line Interface	Accessibility Features Account Manipulation	Access Token Manipulation Accessibility Features	Access Token Manipulation Binary Padding	Account Manipulation Brute Force	Account Discovery Application Window Discovery	Application Deployment Software Component Object Model and Distributed COM	Audio Capture Automated Collection	Commonly Used Port Communication Through Removable Media	Automated Exfibration Data Compressed	Account Access Removal Data Destruction	version permalink									
i Remote Services	Compiled HTML File	AppCert DLLs	AppCentOLLa	BITS Jobs	Oredential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Owter Encrypted	Data Encrypted for Impact		Persistence	Privilege Escalation	Defense Evasion	Credential Access			Collection	Exfiltration	110000000
re Additions O uph Removable Media	reponent Object Model and Distributed COM Control Panel Items	Applinit DLLs Application Shimming	Applisit DLLs Application Shimming	Bypass User Account Control CMSTP	Credentials from Web Browsers Credentials in Files	Domain Trust Discovery File and Directory Discovery	Internal Spearphishing Logon Scripts	Data from Information Repositorie Data from Local System	Custom Command and Control Protocol Custom Cryptographic Protocol	Data Transfer Size Linits Exfittation Over Attenuative Protocol	Defacement Diak Content Wipe	Initial Access	Persistence	Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exhitration	Impact
ishing Attachment	Dynamic Data Exchange	Authentication Package	Bypess User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Oata Encoding	Exfiltration Over Command and Control Charm	el Disk Structure Wipe			Autoritative in the local of							
phishing Link shing via Service	Execution through API Execution through Module Load	BITS Jobs Bootkit	ELL Search Order Hijacking Exploitation for Privilege Escalation	Compile After Delivery Compiled HTML He	Exploitation for Oredential Access Forced Authentication	Network Share Discovery Network Sniffing	Pass the Ticket Remote Desktop Protocol	Data from Removable Media Data Staged	Data Obfuscation Domain Pronting	Exfination Over Other Network Medium Exfittetion Over Physical Medium	Endpoint Denial of Service Pirmware Comption	Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access	Data from Cloud Storage	Transfer Data to Cloud	Resourc
Drain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery	arrie by comprehinad	recourt manparation		- opposite of the second former	Processing triangle and the	riscourt biscorery	Token	Object	Account	Hijacking
d Relationship	Graphical User Interface InstallUSI	Change Default File Association Component Firmware	File System Permissions Weakness	Component Object Model Hijecking Connection Proxy	Input Cepture Input Prompt	Peripheral Device Discovery Permission Broups Discovery	Familie Services Replication Through Removable Media	Input Capture Man in the Browser	Falbeck Channels Multi-hop Proxy		Network Denial of Service Resource Hijacking	Exploit Public-Facing							Data from Information		
d Accounts	LSASS Driver	Component Ditject Model Hijacking	Hooking Image File Execution Options Injection	Control Panel Items	Ketersating	Permasion crocps bacevery Process Discovery	Shared Webrott	Screet Capture	Muti-Stage Channels		Runtime Data Manipulation		Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing			
	Mahta	Create Account	New Service	DCSwdow	LUMNER/NETINS Palaoning and Balay	Query Registry	Taint Shared Contant	Video Capture	Multiband Communication		Service Drop	Application							Repositories		
	PowerShell Registrics (Registrin	DLL Search Order Hijacking External Remote Services	Parent PID Spoofing Path Interception	Deobfuscate: Decode Files or Information Disabiling Security Tools	Network Snilling Password Filter DLL	Remote System Discovery Security Software Discovery	Third party Software Windows Admin Shares		Multilayer Encryption Remote Access Tools		Browd Data Manipulation System Shutdown/Reboot		Implant Container		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
	Report 32	File System Permissions Weakness	Port Monitors	BLL Search Order Hijacking	Privata Kayo	Selfman Discovery	Windows Remote Management,		Remote File Copy		Transmitted Data Manipulation	Spearphishing Link	Image								
	Rundil02 Scheduled Task	Hidden Files and Directories Wooking	PowerShell Profile Process Injection	DLL Side-Loading Execution Quantitatia	Steal Web Session Coakie	System Information Discovery System Network Configuration Discovery			Standard Application Layer Protocol Standard Cryptographic Protocol				unage								
	Series	Hapenvisor	Scheduled Task	Exploitation for Defense Evasion	Internet of the second second second	System Network Connections Discovery			Standard Non-Application Layer Protocol		_	Trusted Relationship	Office Application		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
P.G.	Senice Execution Signed Binary Proce Execution	Image File Execution Options Injection Legon Scripts	Service Registry Permissions Vesiness SD-History Injection	Extra Window Memory Injection File and Directory Permissions Modification		System Owner, User Discovery System Service Discovery			Uncommonly Used Port		-		Startup						Data Staged		
	Signed Briegt Proxy Execution Signed Script Proxy Execution	Linger Scripts	SID-Hatory Injection Valid Accounts	File and Directory Permissions Modification File Deletion		System Service Discovery System Time Discovery			Web Service							- 11 H - 1					
	Third-party Software	Modify Existing Service	Web Shell	File System Logical Offsets		Virtualization/Sandbox Evasion						Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access	Network Share Discovery		Email Collection		
	Trusted Developer Utilities User Execution	Netsh Helper DLL Nets Service		Group Palicy Modification Hidden Files and Directories								Tuna Hoodanto				Token	Herror on are brootery		Citian Concondit		
	Windows Management Instrumentation	Office Application Startup		Hidden Window								1	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
	Windows Remote Management XSL Script Processing	Path Interception Port Manitore		Image File Execution Options Injection Indicator Blocking									Valia Accounts		Web Session Gookle	Stedi Web Session Gookie	Permission droups biscovery				
	Ast, single Processing	PowerShell Profile		Indicator Removal from Tools													Remote System Discovery				
		Redundant Access		Indicator Removal on Host													System Information Discovery				
		Registry Run Keys / Startup Polder Scheduled Task		Indirect Command Execution Install Root Certificate													System mornation biscovery				
		Screensaver		InstallUti													System Network Connections				
		Security Support Provider Server Software Component		Masquerating Modify Registry							_						Discovery				
		Service Registry Permissions Weakness		Mahta							-										
		Shortost Modification SIP and Trust Provider Hjacking		Network Share Connection Removal NTES File Attributes																	
		System Firmware		Obfuscated Files or Information																	
		Time Providers		Parent PID Speeling																	
		Velid Accounts Teats Shell		Process Doppelginging Process Holowing																	
		Windows Management Instrumentation Event Subscription		Process Injection																	
		Winleger Helper DLL		Redundent Access Regards, Regarm																	
				Region 32																	
				Rootik Rundit2																	
				Scripting																	
				Signed Binary Proxy Execution Signed Script Proxy Execution																	
				Signed Script Provider Hiscking																	
				Software Packing																	
				Templata Injection Timestamp																	
				Trusted Developer Utilities																	
				Valid Accounts Virtualization/Sandbax Evasion																	
				Web Service							_	_									
				XB, Soript Processing																	

LABS

DRAW INSPIRATION FROM...

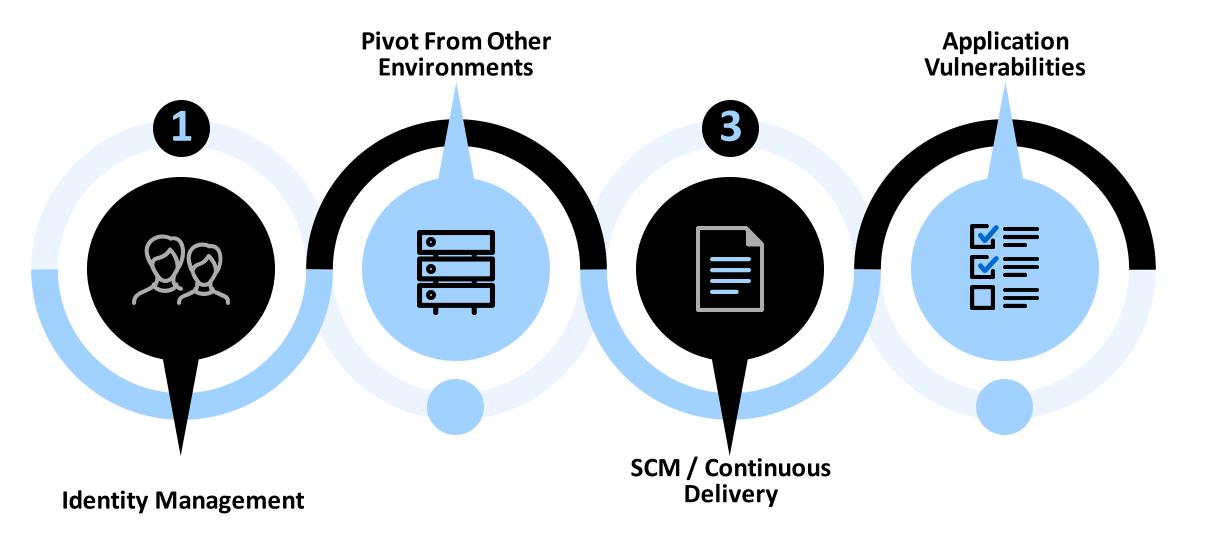


LFBS

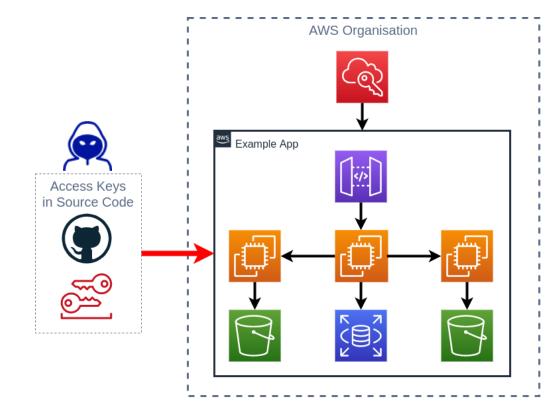


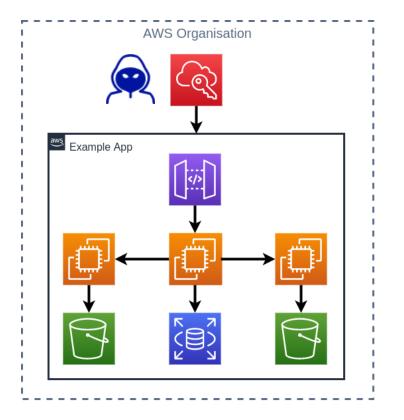
WHAT'S AN ATTACKER LIKELY TO DO?

VECTORS WE'VE EXPLOITED



IDENTITY MANAGEMENT



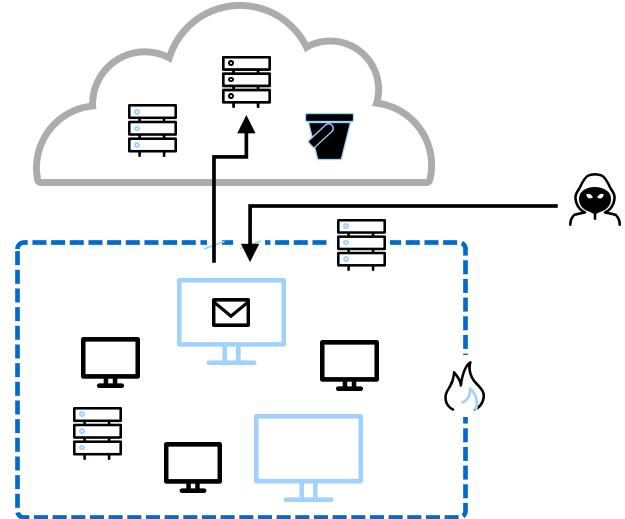


LABS

IDENTITY MANAGEMENT



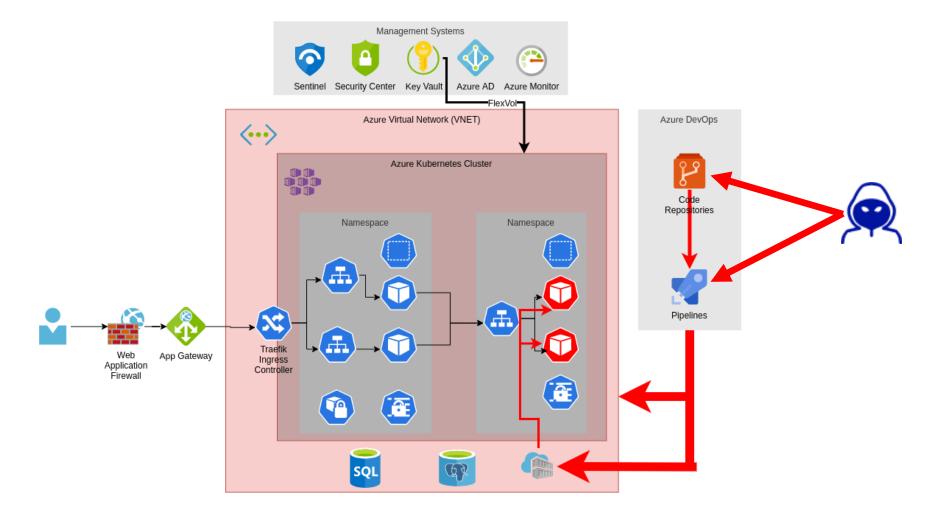
PIVOT FROM OTHER ENVIRONMENTS



PIVOT ATTACK PATH

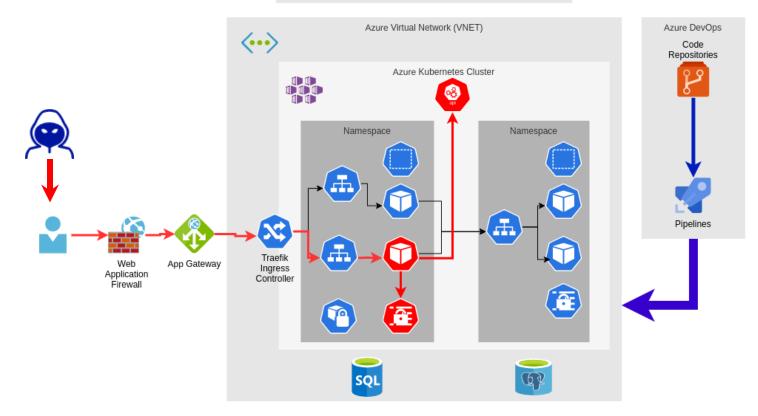


SCM & CONTINUOUS DELIVERY

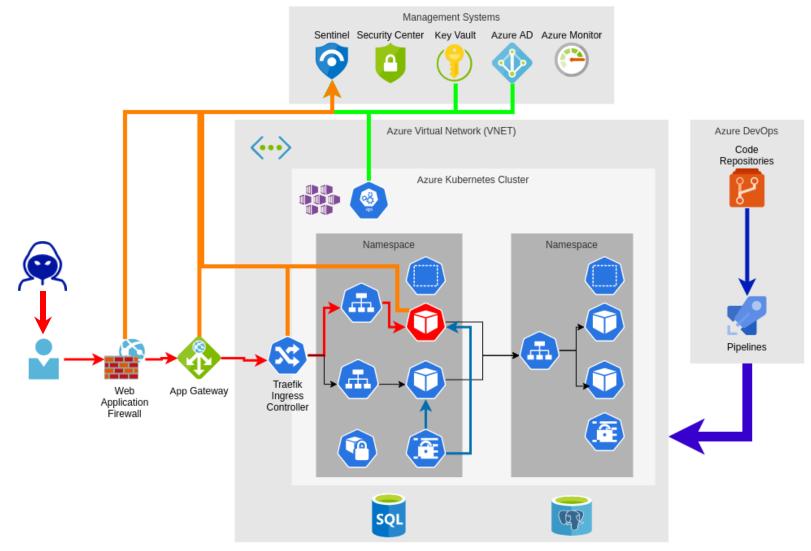


APPLICATION EXPLOITATION





DETECT APPLICATION EXPLOITATION



LYBS

01

05

HOW DO I START?

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

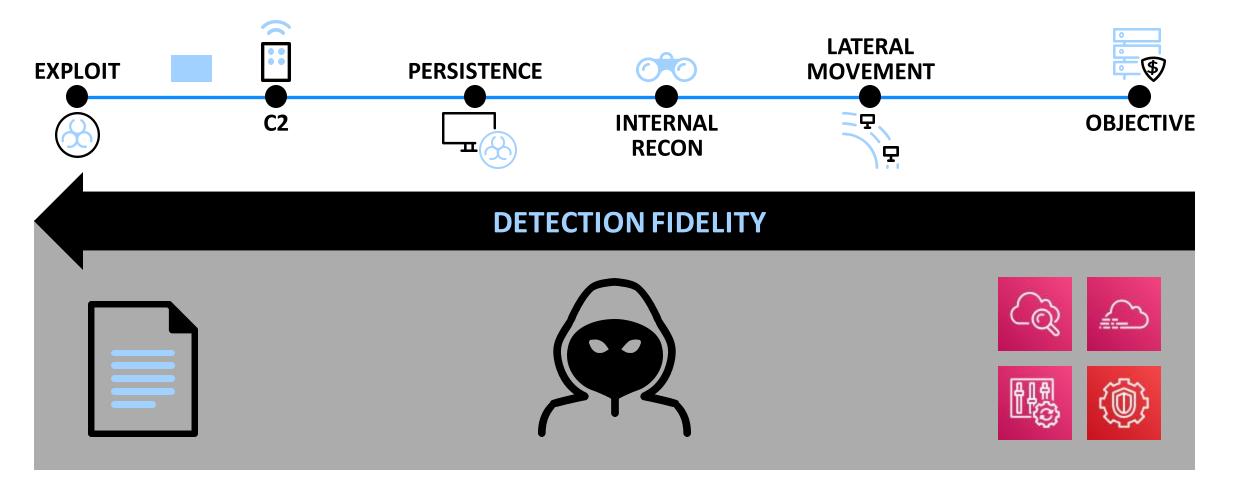
Prioritise attack paths and actions

Pick the most important attack paths, codify them

Verify telemetry is available to defenders

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

WHERE DO I START?



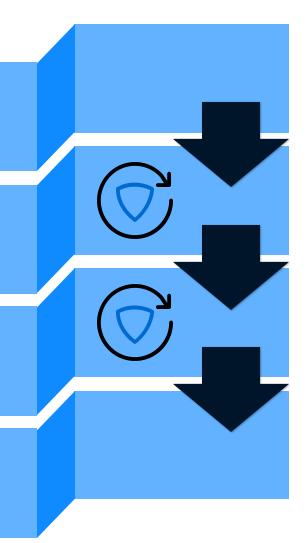
HOW DO WE VALIDATE?

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-jupyternotebooks-part-1-your-first-notebook-9a99a781fde7



John Lambert – The Githubification of Infosec

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

https://medium.com/@johnlatwc/the-githubification-of-infosecafbdbfaad1d1



LEONIDAS

LEONIDAS

Leonidas [®]

[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

/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

/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

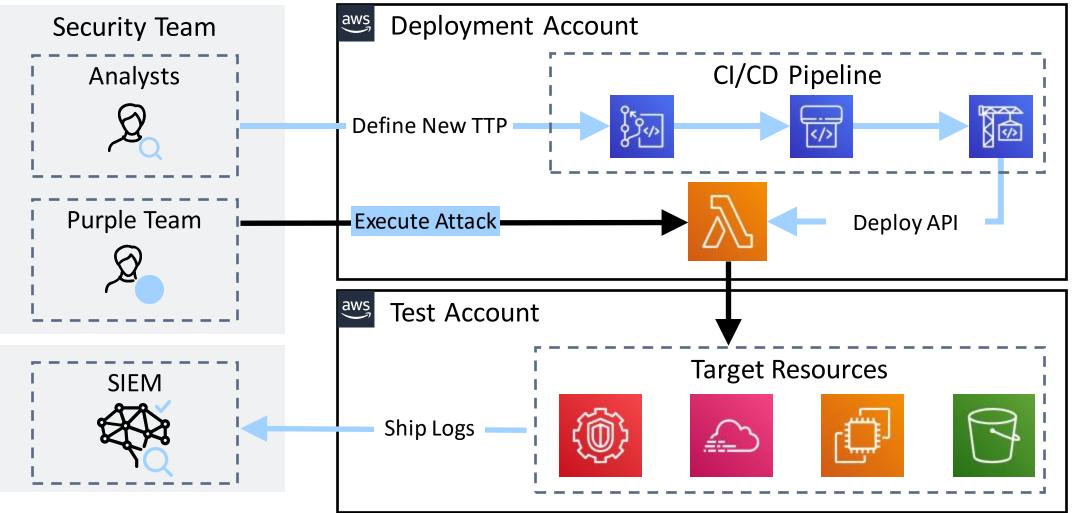
defense_evasion Defense Evasion

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

 \sim

 \sim

LEONIDAS



GENERATE ATTACK SIMULATION

- name: Enumerate Cloudtrails for Current Region

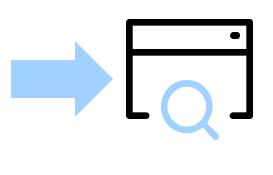
```
permissions:
- cloudtrail:DescribeTrails
input_arguments:
executors:
   leonidas_aws:
    implemented: True
    clients:
        - cloudtrail
        code: |
        result = clients["cloudtrail"].describe trails()
```



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 ACCESS REQUIREMENTS



>

 \mathbf{v}

>

>

>

>

>

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	Туре	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	ТХТ

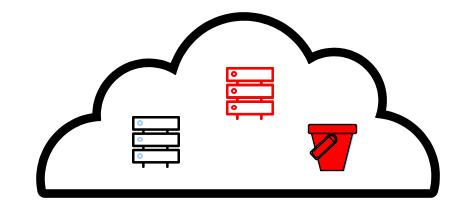
Table of contents MITRE IDs Required Permissions Required Parameters Attacker Action Detection Case ELK query Sigma Definition

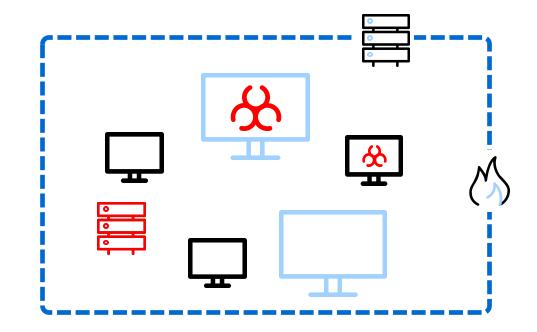
GENERATE DOCUMENTATION



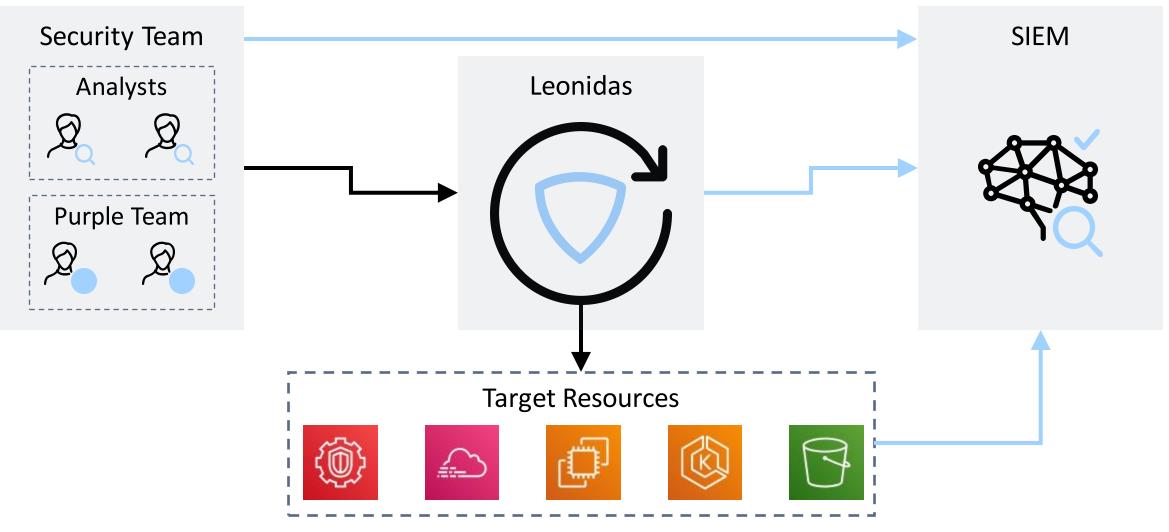
DEMOTIME!

CONTINUOUS TESTING

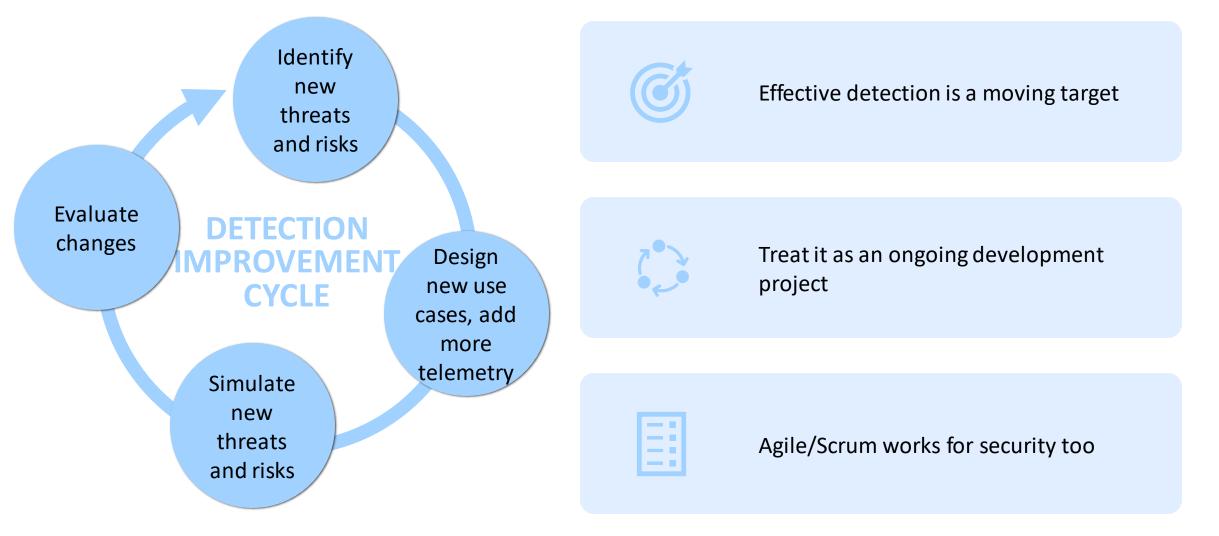




CONTINUOUS INTEGRATION



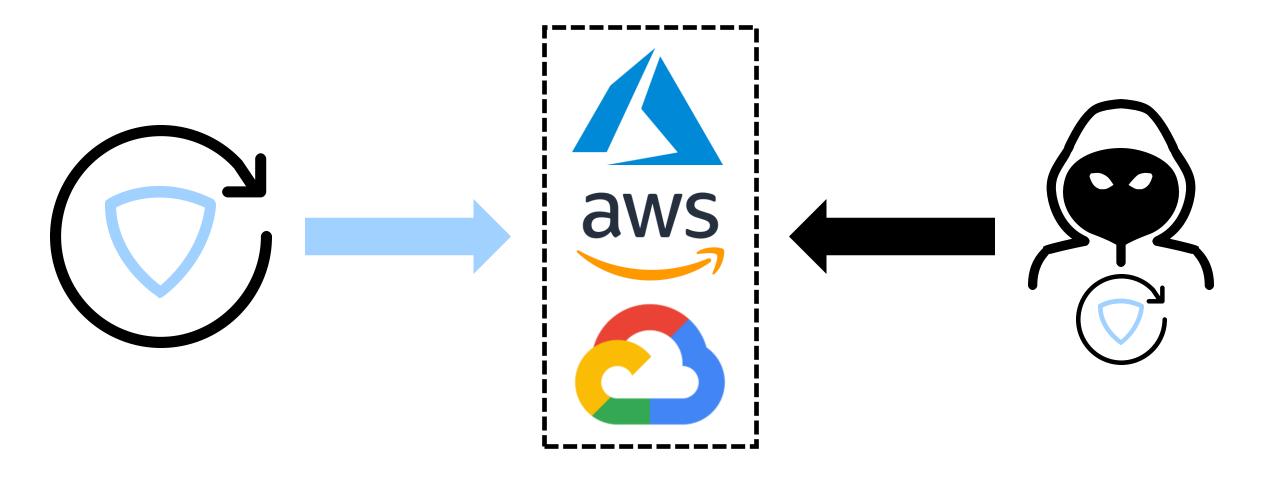
DETECTION IS A JOURNEY



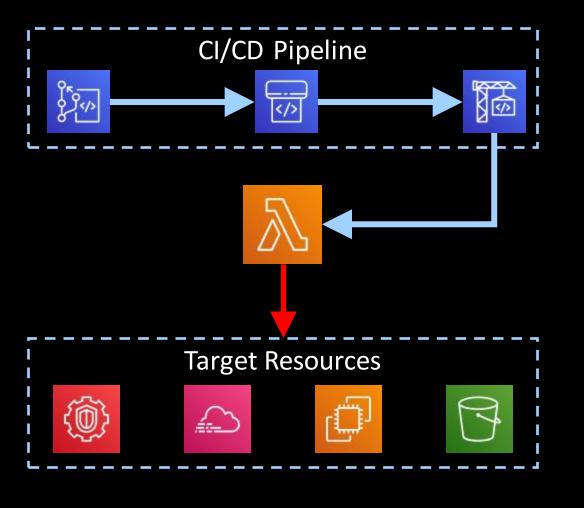


CONCLUSIONS

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