AUTOMATING ATTACK SIMULATIONS IN THE CLOUD

Nick Jones Fwd:CloudSec – 29th June 2019



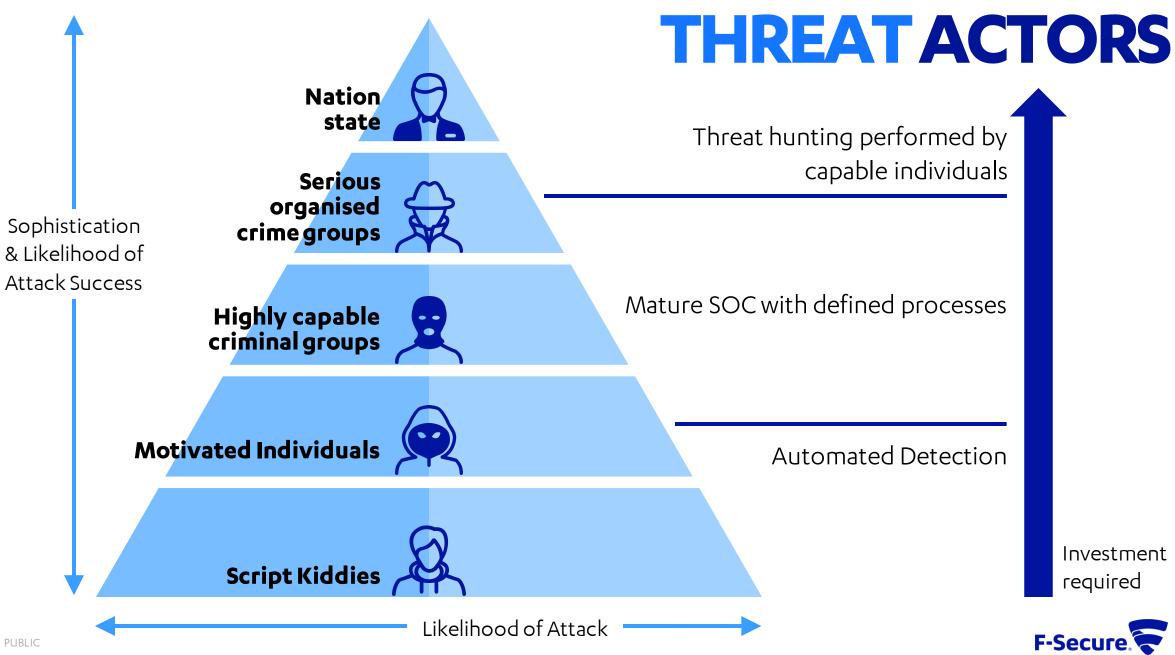
© F-SECURE CONSULTING

AGENDA

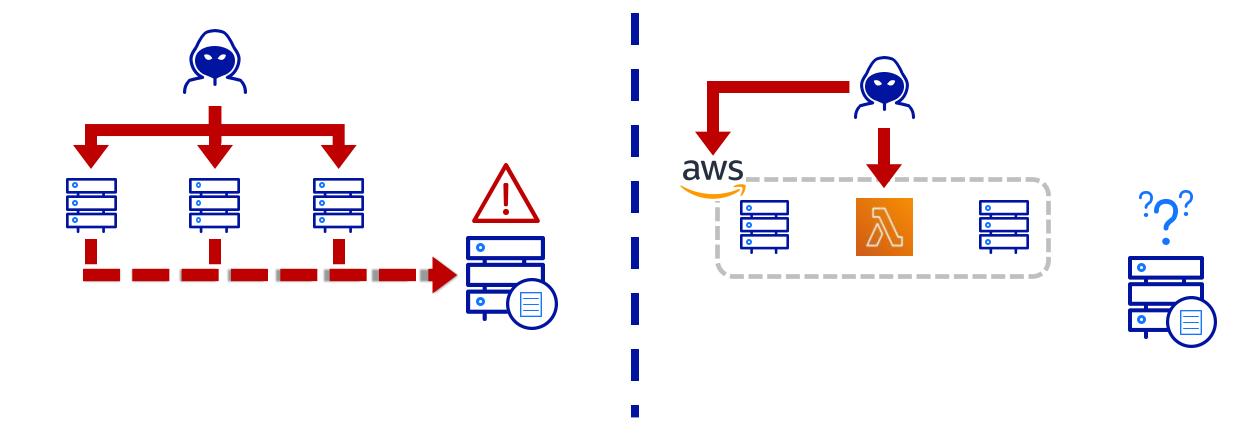


CHARLES CHARLE





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.



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

ATTACKERSARE AUTOMATING

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



ON-PREMISE VS CLOUD ATT&CK

Initial Access	Execution	Persistence		Defense Draskon			Lateral Movement				Impact	Last Modified: 2019-10-09	10/10/01/000000								
Drive-by Compromise alt Public-Facing Application	CMSTP Command-Line Interface	Accessibility Features Account Manipulation	Access Token Manipulation Access billty Features	Access Token Manipulation Binary Padding	Account Manipulation Brute Force	Account Discovery Application Window Discovery	Application Deployment Software Component Object Model and Distributed COM	Autio Capture Automated Collection	Commonly Used Port Communication Through Removable Media	Automated Exfiltration Data Compressed	Account Access Removal Data Destruction	version permalink									
temal Remote Services	Compled HTML File	AppCert DLLs	AppCettOLLa	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Outs Encrypted	Deta Encrypted for Impact	The second second		Privilege							
Hardware Additions	Component Object Model and Distributed COM	Appinit DLLs	Appinit DLLs	Rypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Outa Transfer Size Limits	Defacement	Initial Access	Persistence	Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impac
tion Through Removable Media (pearphishing Attachment	Control Panel Items Dynamic Data Exchange	Application Shimming Authentication Package	Application Shimming Bypess User Account Control	CMSTP Code Signing	Credentials in Files Credentials in Registry	File and Directory Discovery Network Service Scanning	Lagon Scripts Pass the Hash	Data from Local System Data from Network Shared Drive	Custom Cryptagraphic Protocol Data Encoding	Exfituation Over Alternative Protocol Exfituation Over Command and Control Char				Escalation							
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Gredential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuecation	Exfituation Over Other Network Medium	Endpoint Denial of Service	and the second	And the second second			And the second second		Application Access	Data from Cloud Storage	Transfer Data to Cloud	Resource
Spearphishing via Service	Execution through Module Load	Bookit	Exploitation for Privilege Excelution	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfittation Over Physical Medium	Ferrivare Comption	Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Token	Object	Account	Hijackir
Supply Chain Compromise Trusted Relationship	Exploitation for Client Execution Draphical User Interface	Browser Extensions Change Default File Association	Extra Window Memory Injection File System Permissions Weakness	Component Firmware Component Object Model Hijasking	Hooking Input Cepture	Password Policy Discovery Peripheral Device Discovery	Remote File Copy Remote Services	Eval Collection Input Capture	Domain Generation Algorithms Failback Channels	Scheduled Transfer	Inhibit System Recovery Network Denial of Service							(Onleri	object	riccount	- injustitut
Valid Accounts	InstallUbi	Component Firmware	Hooking	Connection Proxy	Input Prompt	Permission Droups Discovery	Replication Through Remonable Media	Man in the Browser	Multi-hop Proxy		Resource Hjacking	Exploit Public-Facing	Create Account	Redundant	Redundant Access	nt Access Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
	LSASS Driver Mahta	Component Object Model Hijacking Create Account	Image File Execution Options Injection New Service	Control Panel Items DCShedow	Kerbersetting LLMNP/NET/NS Palaoning and Balas	Process Discovery Duery Replatry	Shared Webroot Taint Shared Content	Screen Capture Video Capture	Multi-Stage Channels Multiband Communication		Purtine Data Manipulation Service Data	Application	Create Account		Redundant Access		Cibud Service Dashboard	internal openiprilaring			
	PoverDell	DLL Search Order Hijsching	Parent PID Spoofing	Deobfuscate Decode Files or Information	Network Sniffing	Remote System Discovery	Third party Software	Vide Captore	Multilayer Encryption	Browd Data Manipulation											
	Pagaron Registri	External Remote Services	Path Interception	Disabling Security Tools	Password Filter DLL	Security Software Discovery	Windows Admin Stares		Remote Access Tools		System Shutdown/Reboot	Spearphishing Link	Implant Container		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
	Regivit32 Rundi02	File System Permissions Weakness Hidden Files and Directories	Part Monitors PawerShell Prafile	BLL Search Order Hijacking DLL Side-Loading	Private Kays Steal Illeb Session Cookie	System Information Discovery	Windows Remote Management		Remote File Copy Standard Application Layer Protocol		Transmitted Data Manipulation	open prosting chin	Image								
	Scheduled Task	Hooking	Process Injection	Execution Quandhalla		System Network Configuration Discovery			Standard Cryptographic Protocol												
	Scripting	Hypervisor	Scheduled Task	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Non-Application Layer Protocol			Trusted Relationship	Office Application		Unused/Unsupported Cloud	Credentials in Files	Network Service Scanning		Data Staged		
	Senice Execution Signed Binary Proxy Execution	Image File Execution Options Injection Legon Scripts	Service Registry Permissions Weakness SD-History Injection	Extra Window Memory Injection File and Directory Permissions Modification		System Owner, User Discovery System Service Discovery			Uncommonly Used Port Web Service				Startup		Regions		the second se		a dia diagen		
	Signed Script Proxy Execution	LSASS Driver	Valid Accounts	File Deletion		System Time Discovery										Steel Application Accord					
	Third-party Software Trusted Developer Utilities	Modify Existing Service Netsh Helper DU,	Web Shell	File System Logical Offsets Onoug Palicy Modification		Virtualization/Sandbox Disasion					Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Network Share Disc	Network Share Discovery		Email Collection			
	Developer Utilities	Netsh Helper DLL. New Service		Holden Files and Directories												Token					
	Windows Management Instrumentation	Office Application Startup		Hidden Window									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									Valid Accounts		Web Session Gooke	Stear Web Session Gookle	Permission droups biscovery				
	Ast, sample Processing	PoverShell Profile		Indicator Blocking Indicator Removal from Tools													Remote System Discovery				
		Redundant Access		Indicator Removal on Host													Distance in Francisco Discourse				
		Registry Run Keyn / Startup Polder Scheduled Task		Indirect Command Execution Install Root Certificate													System Information Discovery				
		Screeneer		InstallUtil													System Network Connections				
		Security Support Provider		Masquerading							-						Discovery				
		Server Software Component Service Registry Permissions Weakness		Modify Registry Mahta							_	_					Discovery				
		Shortout Modification		Network Share Connection Removal																	
		SIP and Trust Provider Hijacking		NTES File Attributes																	
		System Firmware Time Providers		Obfuscated Files or Information Parent PID Spoafing																	
		Valid Accounts		Process Doppeiplinging																	
		Web Shell		Process Hollowing								-									
		Windows Management Instrumentation Event Subscription Winlopin Helper DLL		Process Injection Redundent Access							_										
		the age of the second sec		Regarda, Regas m																	
				Report22																	
				Rootit Rundit2																	
				Scripting																	
				Signed Binary Proxy Execution																	
				Signed Script Prory Execution SIP and Tryst Provider Hiacking																	
				Software Packing																	
				Template Injection																	
				Timestang Trusted Developer Utilities																	
				Valid Accounts																	
				Virtualization/Sandbox Evasion Web Service																	
				Web Service XB, Script Processing																	
				and the part of the state of the																	



DRAW INSPIRATION FROM...





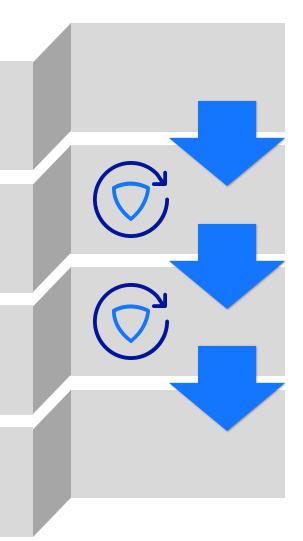
HOW DO WE VALIDATE?

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

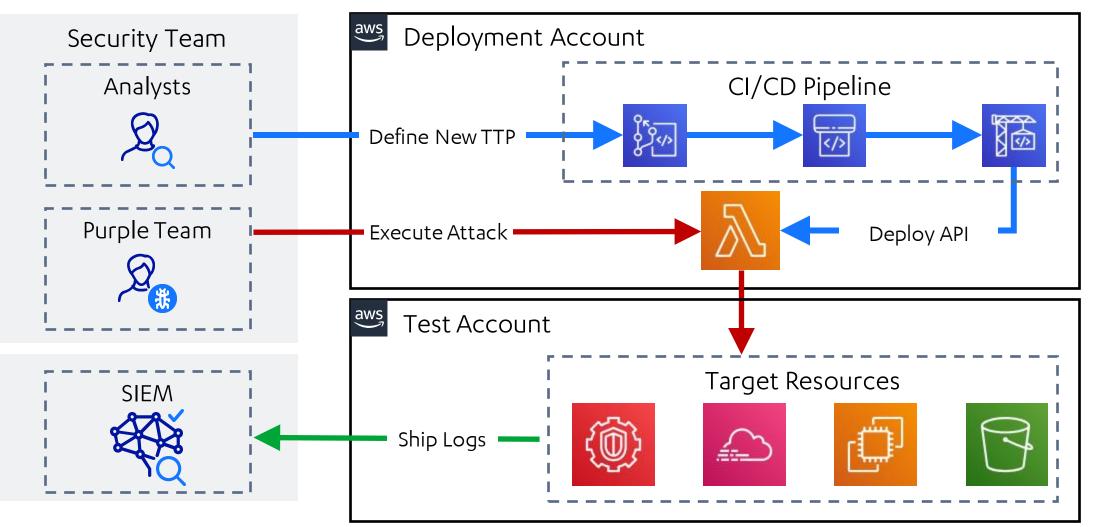


John Lambert – The Githubification of Infosec http://youtu.be/B3o-9z3Eitg https://medium.com/@johnlatwc/the-githubification-ofinfosec-afbdbfaad1d1



LEONIDAS

LEONIDAS





GENERATE ATTACK SIMULATION

- name: Enumerate Cloudtrails for Current Region

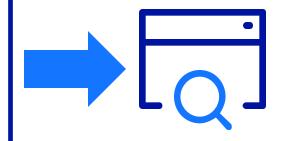
```
permissions:
- cloudtrail:DescribeTrails
input_arguments:
executors:
leonidas_aws:
    implemented: True
    clients:
        - cloudtrail
    code: |
        result = clients["cloudtrail"].describe_trails()
```



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"
```





>

 \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

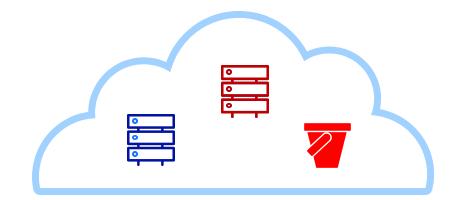
Detection Case

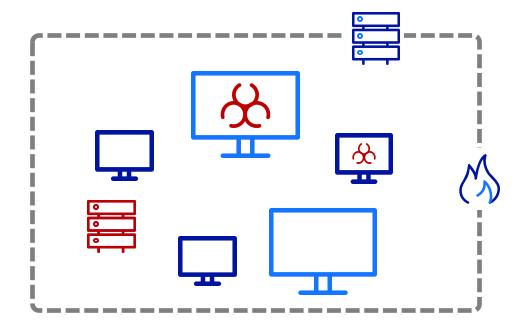
- ELK query
- Sigma Definition

GENERATE DOCUMENTATION



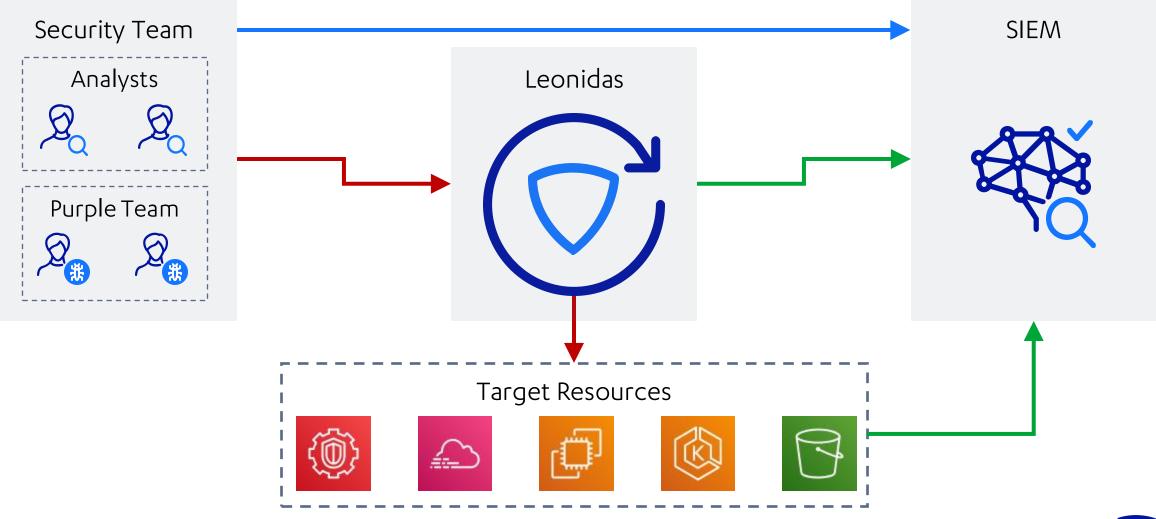
CONTINUOUS TESTING







CONTINUOUS INTEGRATION





HOW DO I START?



Prioritise attack paths and actions

04

Verify telemetry is available to defenders

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

Pick the most important attack paths, codify them

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

F-Secure

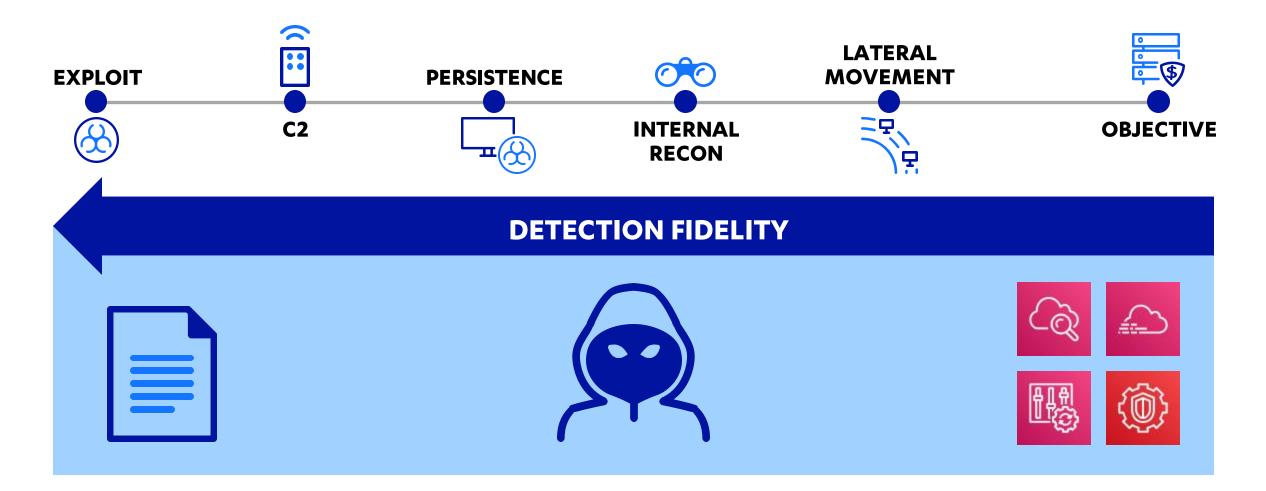
05

01

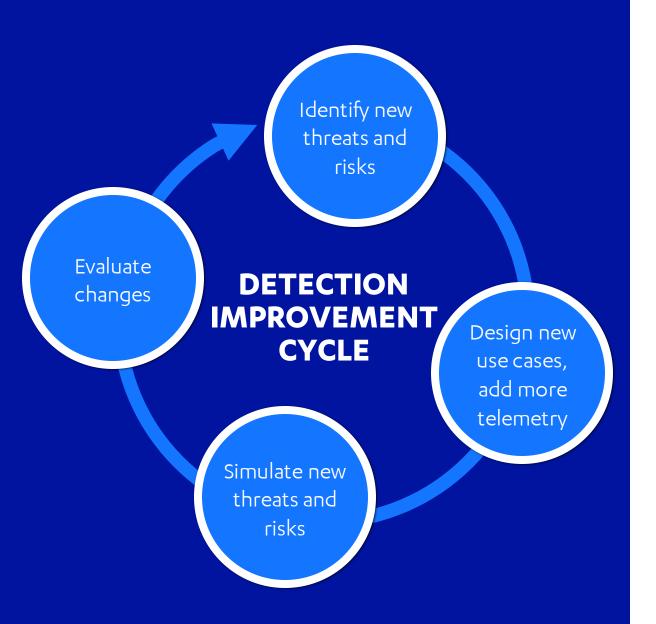


PUBLIC

WHERE DO I START?







DETECTION IS A JOURNEY

Ø

Effective detection is a moving target

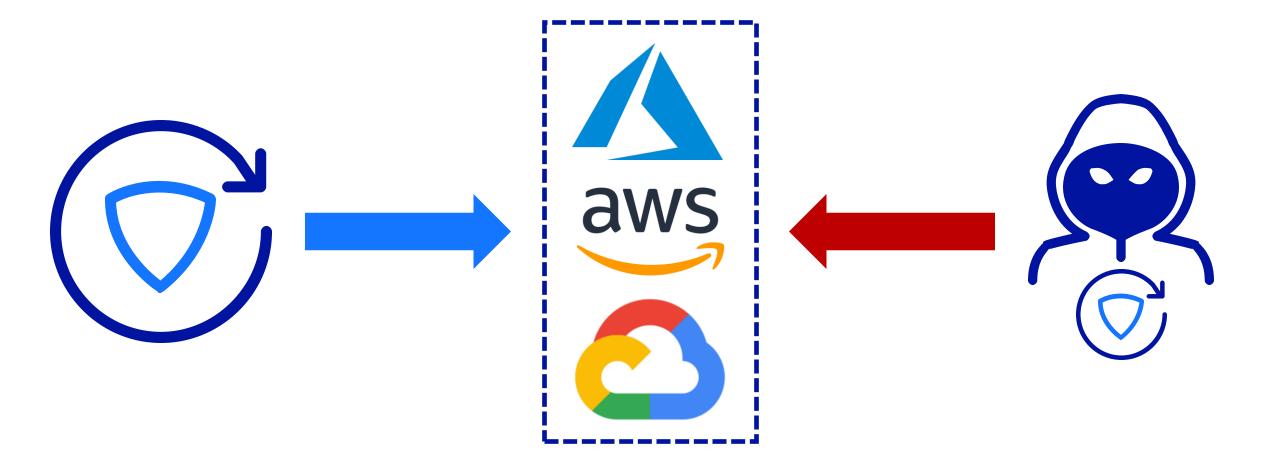


Treat it as an ongoing development project

Agile/Scrum works for security too

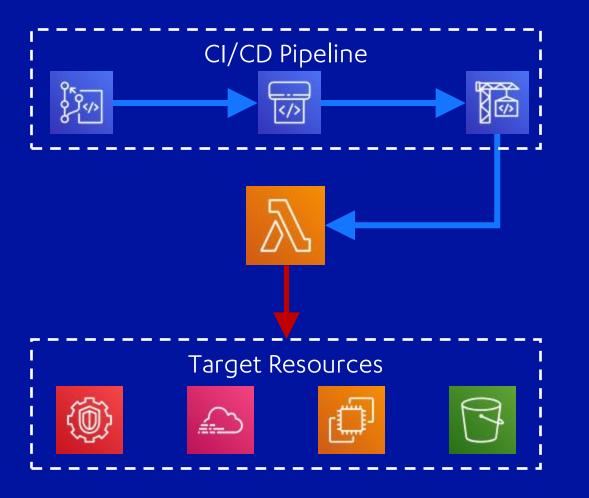


CONCLUSIONS





LEONIDAS





Automate attacker actions in the cloud



Both test and detection cases



AWS support now, Azure/GCP on the roadmap



34 test cases - more to come



https://github.com/fsecurelabs/leonidas





Feedback: <u>https://bit.ly/fwdcs-9</u>

© F-SECURE CONSULTING