RSA®Conference2021

May 17 – 20 | Virtual Experience

SESSION ID: AIR-T14



Beyond Public Buckets: Lessons Learned on Attack Detection in the Cloud

Alfie Champion

Senior Consultant / Global Attack Detection Lead F-Secure Consulting @ajpc500

Nick Jones

Senior Consultant / Global Cloud Lead F-Secure Consulting @nojonesuk

Agenda



On-Premise Vs Cloud Detection

Designing Your Cloud Detection Stack



Likely Attacker Activity



Bringing DevOps To Detection



#RSAC

RS∧[°]Conference2021

RSAConference2021

On-Premise vs Cloud

How Cloud Detection differs

CONTEXT IS KEY

#RSAC

Anomalies will vary by environment. Behavioral analytics are important here, so is developing environment-specific alerting.

UNCERTAINTY OF MALICIOUS INTENT

Fewer actions in the cloud are obviously bad compared to on-premise, making generic detection rules harder

GAINING VISIBILITY IS EASIER

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





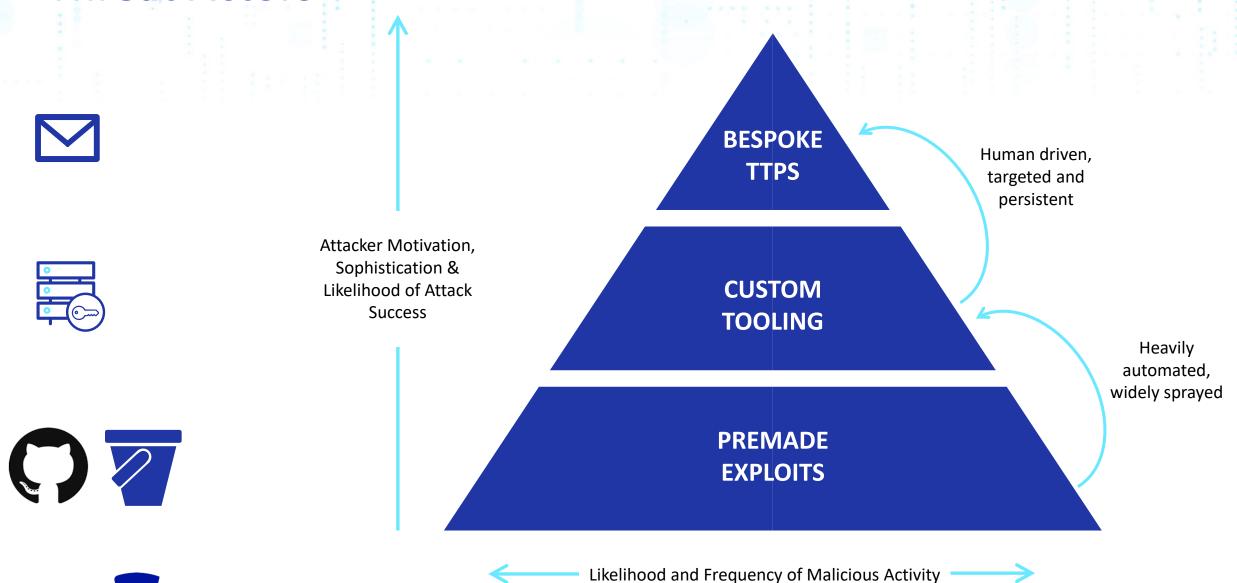
ATTACKERS ARE AUTOMATING

Attackers leveraging scripted attacks to abuse stolen credentials for cryptocurrency mining. With an API-driven attack surface by-design, it's easier to automate targeted attacks too.









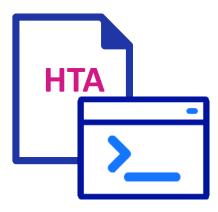
5

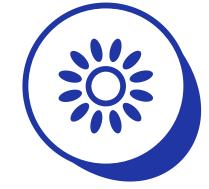
#RSAC



Mindset Shift





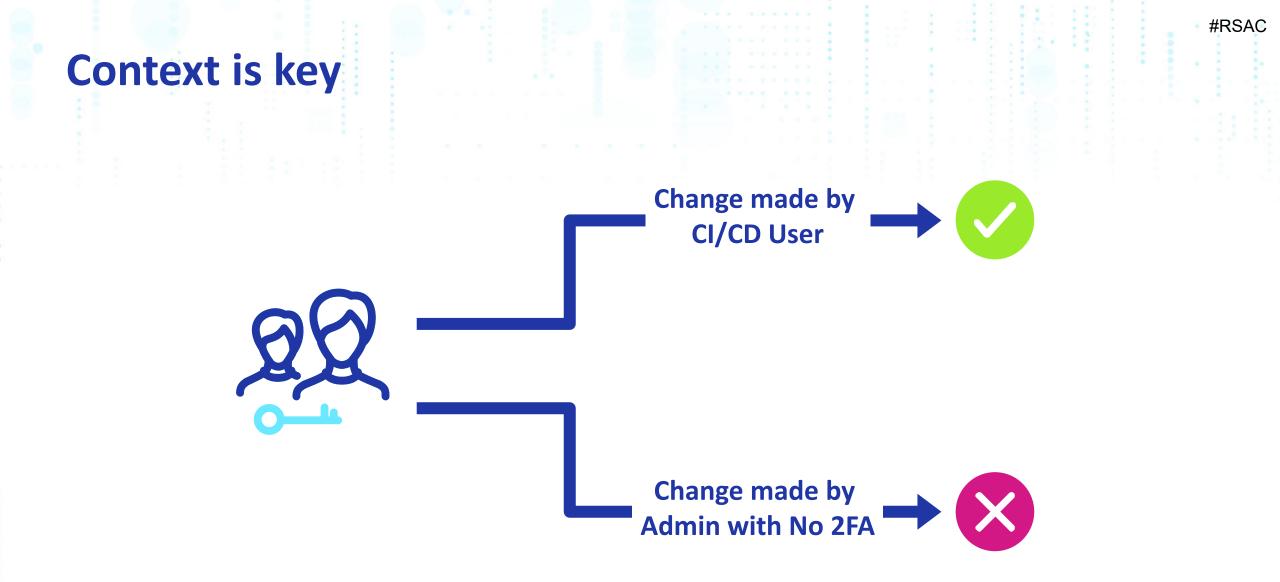


CERTAINTY OF MALICIOUS INTENT



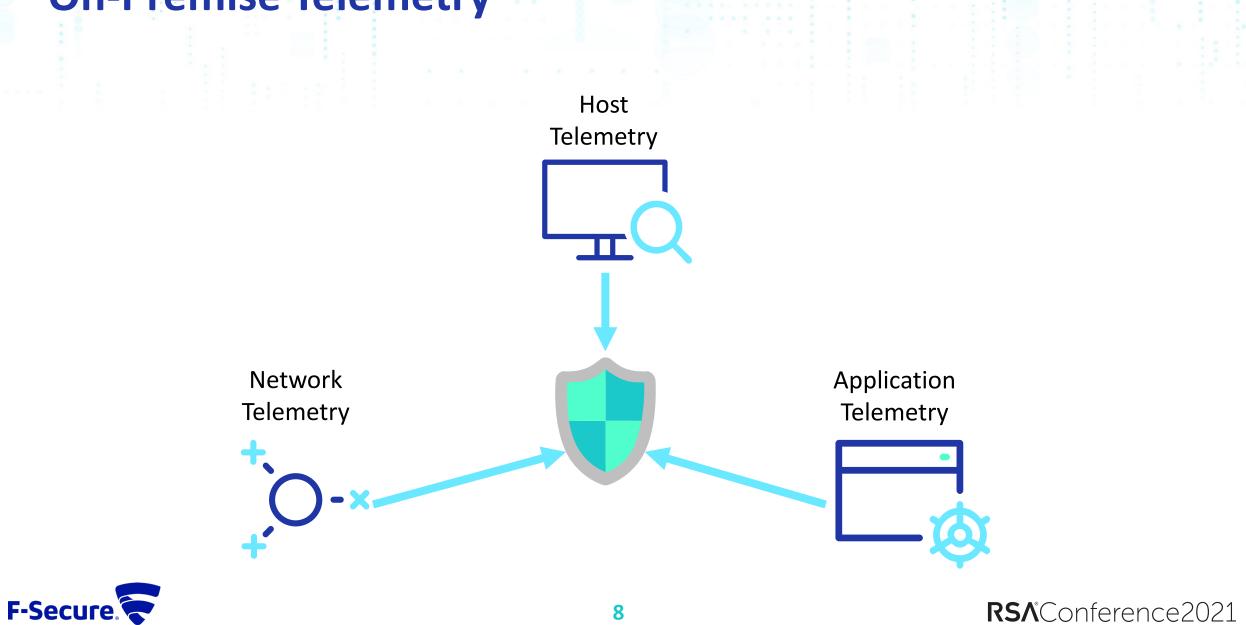


RSAConference2021



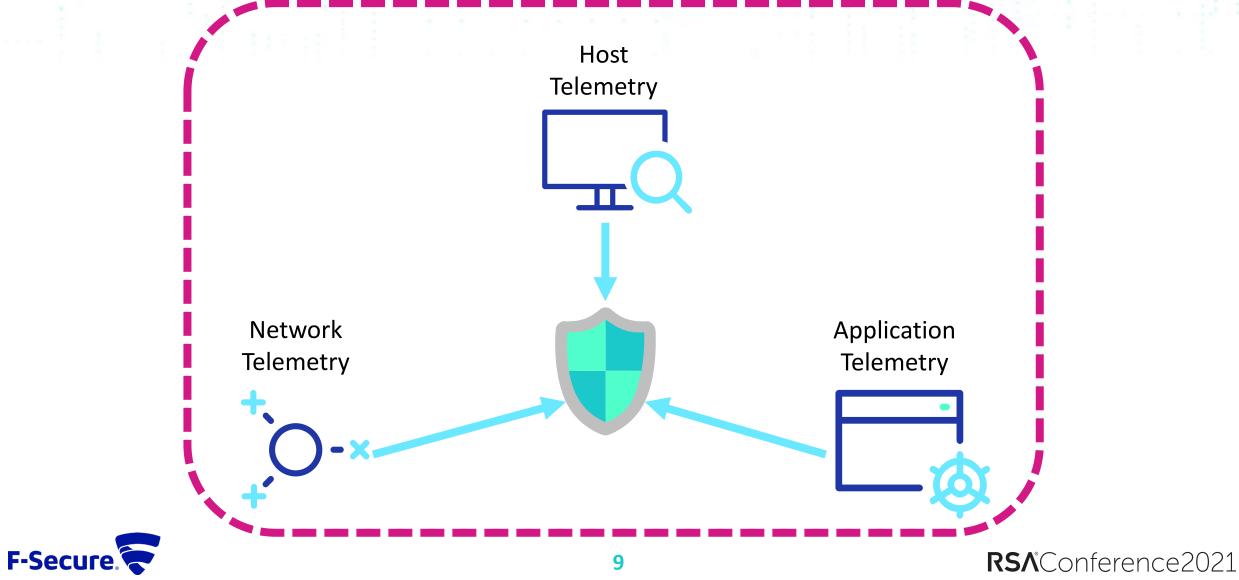






Cloud Telemetry

Control Plane Telemetry



Common Mistakes and Pitfalls

- Telemetry aggregated with no provided (or available) context.
 - **Bad** in one account, **Good** in another.
- Commonly overlooking authentication logs.
 - Interfaces between On-premise/Cloud, management interfaces, etc.
- Never too early to threat model and test some offensive scenarios.



Common Mistakes and Pitfalls

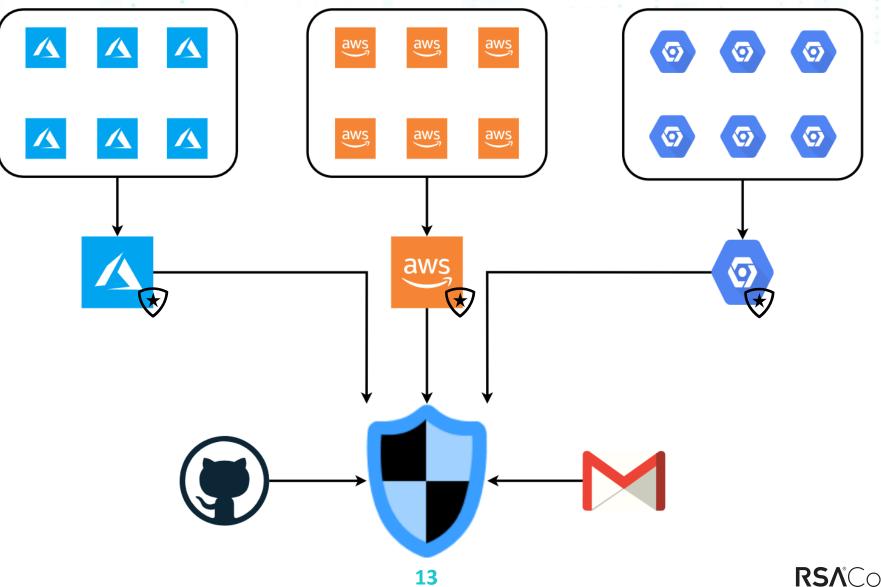
- Build the context from the architectural stage.
 - What should the environment do?
 - What shouldn't it do?
- Sharing the above with analysts gives them the insight into what things should be doing?
- BONUS: Exercising this with analysts gets them used to investigation in cloud.



RSA Conference 2021

Designing Your Cloud Detection Stack

Centralize 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





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



#RSAC

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



#RSAC

Prioritising Telemetry and Use Cases

Gather telemetry for the services you're using.

- Where are the areas of critical activity?
 - What detections can/should you build?
 - Does a given log source provide actionable insight?
 - Use cases should be prioritized based on threat modelling outputs.

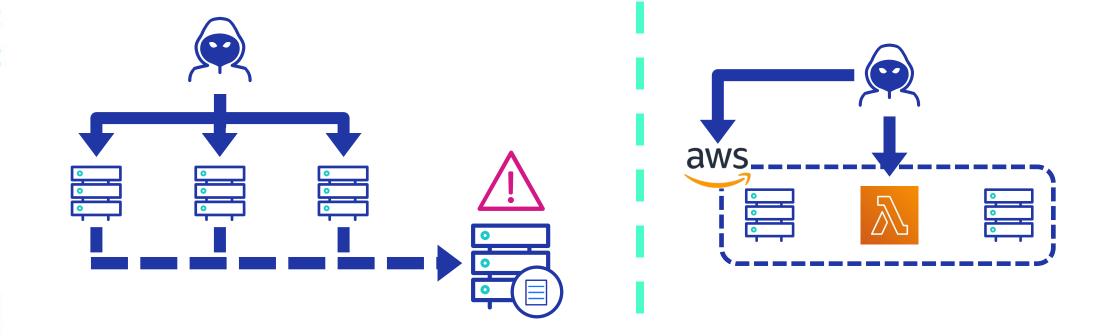
#RSAC



RS∧[°]Conference2021

Likely Attacker Activity

On-Premise vs Cloud Detection

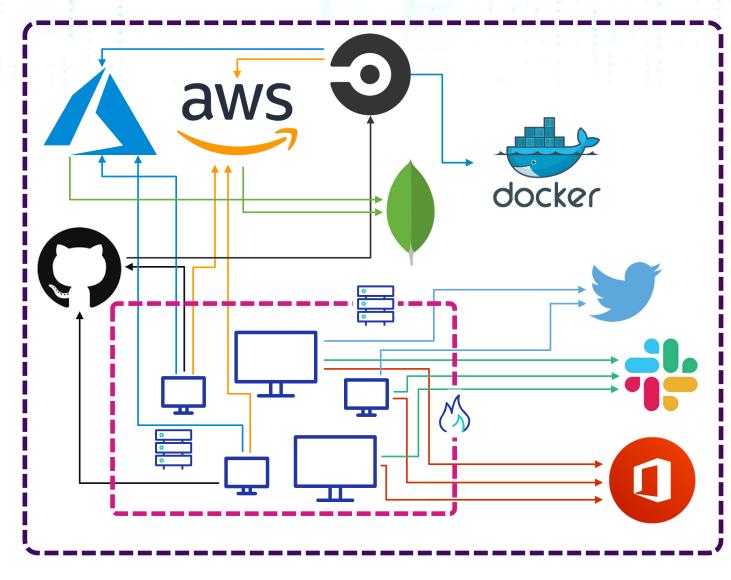




#RSAC



Enterprise Cloud Adoption







Enterprise vs Cloud ATT&CK

Reconnaissance	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation	Defense Evasion	Credential Access	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire	Drive-by	Command and	Account	Abuse Elevation	Abuse Elevation Control	Brute Force (4)	Account Discovery (4)	Exploitation of	Archive	Application	Automated	Account Access
Gather Victim Host	Compromise	Compromise Exploit Public-	Scripting Interpreter (8)	Manipulation (4)	Control Mechanism (4)	Mechanism (4)	Credentials from Password	Application Window	Remote Services	Collected Data (3)	II Layer Protocol (4)	Exfiltration (1)	Removal Data Destruction
Gather Victim Identity	Accounts (2)	Facing Application	Exploitation for Client Execution	Boot or Logon	Access Token Manipulation (5)	Manipulation (5)	Stores (3)	Discovery Browser Bookmark	Spearphishing	Audio Capture	Communication	Size Limits	Data Destruction
Information (3)	Compromise	External Remote Services	Inter-Process	Autostart Execution (12)	Boot or Logon	BITS Jobs	Exploitation for Credential Access	Discovery	Lateral Tool Transfer	Automated Collection	Removable Media	Exfiltration	Impact
Gather Victim Network Information (6)	Develop	Hardware Additions	Communication (2)	Boot or Logon	Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced	Cloud Infrastructure Discovery	Remote Service	Clipboard Data	II Data Encoding (2)	Alternative Protocol (3)	II Data Manipulation (3)
Gather Victim Org	Capabilities (4) Establish	II Phishing (3)	Native API	Initialization Scripts (5)	Boot or Logon	Direct Volume Access	Authentication	Cloud Service Dashboard	Session Hijacking (2)	Data from Cloud	Data	Exfiltration Over C2 Channel	II Defacement (2)
Phishing for	Accounts (2)	Replication	Task/Job (6)	Browser Extensions	Scripts (5)	Domain Policy Modification (2)	Credentials (2)	Cloud Service Discovery	B Remote Services (6)	Storage Object	Obfuscation (3)	Exfiltration	0 Disk Wipe (2)
Information (8)	Obtain Capabilities (6)	Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System	Execution Guardrails (1)	II Input Capture (4)	Domain Trust Discovery	Replication	Configuration Repository (2)	Resolution (3)	II Over Other Network	II Endpoint Denial of Service (4)
II Search Closed Sources (2)		Bupply Chain Compromise (3)	Software Deployment Tools	Create	Process (4)	Exploitation for Defense	II Man-in-the- Middle (2)	File and Directory Discovery	Through Removable Media	Data from	II Encrypted Channel (2)	Medium (1)	Firmware
Bearch Open Technical Databases //o		Trusted Relationship	System Services (2)	Create or Modify	Domain Policy Modification (2)	Evasion	Modify Authentication	Network Service Scanning	Software	Information Repositories (2)	Fallback Channels	Exfiltration Over Physical	Corruption
Search Open		Valid	User Execution (2)	System Process (a)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Process (4)	Network Share Discovery	Deployment Tools	Data from Local System	Ingress Tool Transfer	Medium (1) Exfiltration	Inhibit System Recovery
Websites/Domains (2)		Accounts (4)	Windows Management	Event Triggered	Exploitation for	Hide Artifacts (7)	Network Sniffing	Network Sniffing	Content	Data from Network	Multi-Stage	Over Web Service (2)	II Network Denial of Service (2)
Search Victim-Owned Websites			Instrumentation	Execution (15)	Privilege Escalation	Hijack Execution	II OS Credential Dumping (8)	Password Policy Discovery	Use Alternate Authentication	Shared Drive	Channels	Scheduled	Resource Hijacking
				External Remote Services	II Hijack Execution Flow (11)	Flow (11)	Steal Application	Peripheral Device Discovery	Material (4)	Data from Removable Media	Non-Application Layer Protocol	Transfer	Service Stop
				Hijack Execution	Process Injection (11)	Impair Defenses (7) Indicator Removal on	Access Token Steal or Forge	Permission Groups		II Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Account	System Shutdown/Reboot
				Flow (11) Implant Container	Scheduled	Host (6)	Kerberos Tickets (4)	Discovery (3)		Email Collection (2)	Protocol Tunneling		Shutdown/Reboot
				Image	Task/Job (6)	Indirect Command Execution	Steal Web Session			II Input Capture (4)	II Proxy (4)		
				Office Application Startup (6)	U Valid Accounts (4)	II Masquerading (6)	Cookie Two-Factor	Remote System Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot (5)		Modify Authentication Process (d)	Authentication Interception	II Software Discovery (1)		II Man-in-the- Middle (2)	Traffic Signaling (1)		
				II Scheduled Task/Job (6)		Modify Cloud Compute	Unsecured	System Information Discovery		Screen Capture	Web Service (2)		
				Server Software		Infrastructure (4)	Credentials (6)	System Network		Video Capture			
				Component (3)		Modify Registry		Configuration Discovery					
				II Traffic Signaling (1)		 Modify System Image (2) Network Boundary 		System Network Connections Discovery					
				II Valid Accounts (4)		Bridging (1)		System Owner/User Discovery					
						Diffuscated Files or Information (S)		System Service Discovery					
						Pre-OS Boot (5)		System Time Discovery					
						Process Injection (11)		Wirtualization/Sandbox					
						Rogue Domain Controller		Evasion (3)					
						Rootkit							
						Bigned Binary Proxy Execution (11)							
						Signed Script Proxy							
						Execution (1) Subvert Trust							
						Controls (4)							
						Template Injection							
						Traffic Signaling (1)							
						Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

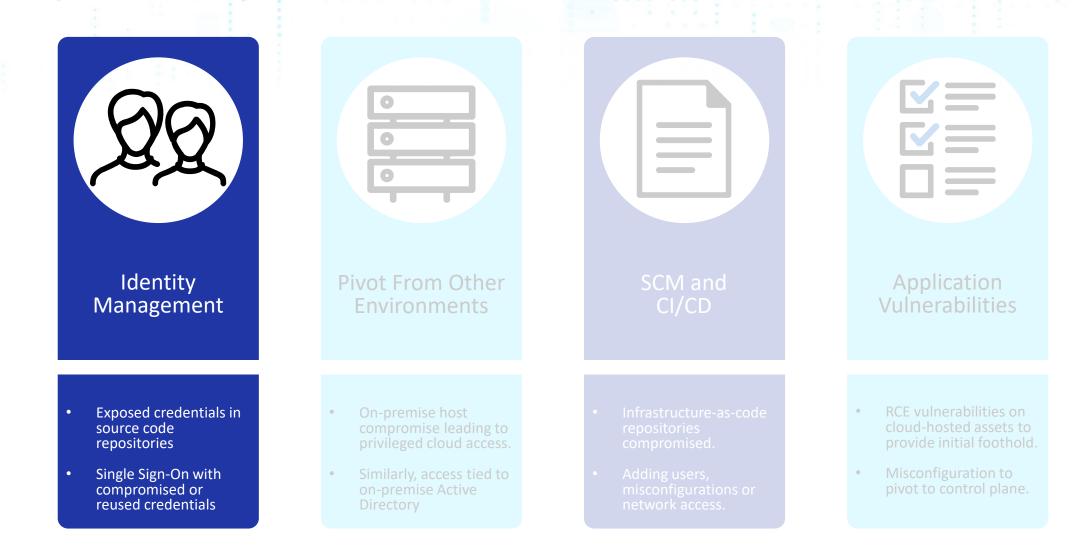
Initial Access 5 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Defense Evasion 6 techniques	Credential Access 5 techniques	Discovery 9 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 4 techniques
Drive-by Compromise	Account Manipulation (8)	Domain Policy Modification on	B Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)		Object	Account	Defacement (1)
Exploit Public-Facing Application	Create Account (1)	Valid Accounts (2)	II Impair Defenses (2)	Forge Web Credentials (2)	Cloud Infrastructure Discovery	Use Alternate Authentication Material (2)			Endpoint Denial of Service (3)
	Implant Container Image	valid Accounts (2)		Steal Application Access					Network Denial of Service (2)
Phishing (1)	U Office Application Startup (6)		Infrastructure (4)	Token	Cloud Service Dashboard		Data Staged (1)		Resource Hijacking
Trusted Relationship	Valid Accounts (2)		Regions	Steal Web Session Cookie	Cloud Service Discovery		II Email Collection (2)		
Valid Accounts (2)			Use Alternate Authentication	Unsecured Credentials (2)	Network Service Scanning				
			Material (2)		Permission Groups				
			II Valid Accounts (2)		Discovery (1)				





What's an attacker likely to do?



















How do I start?

Threat model your environment, identify attack paths

Prioritise attack paths

consist of

Verify telemetry available to defenders

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

Understand the TTPs the attack paths



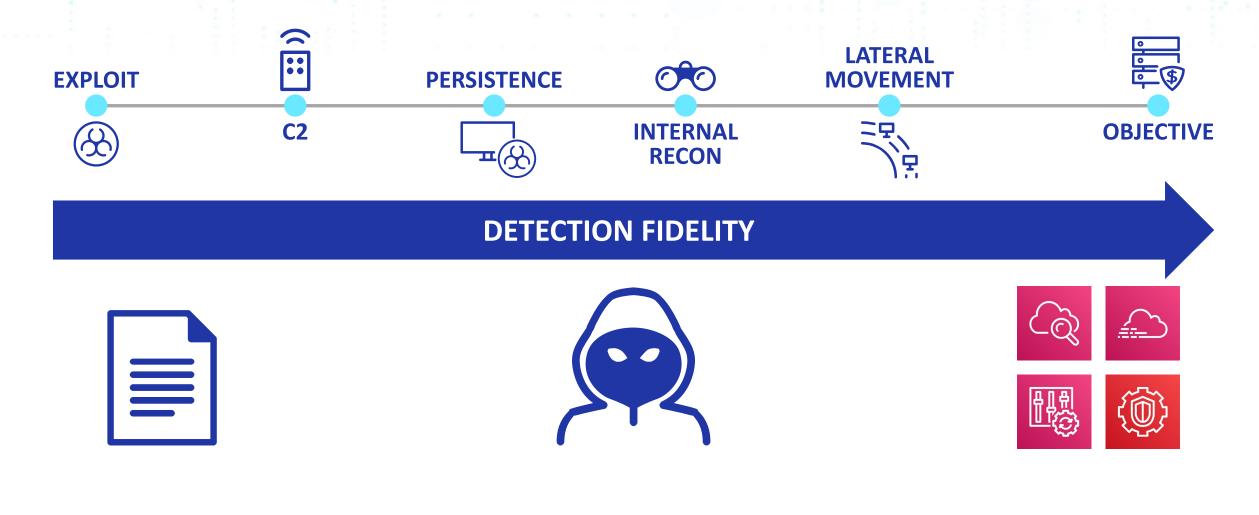




3

5

Where do I start?



#RSAC



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

Ø

Jupyter Notebooks

https://posts.specterops.io/threat-hunting-with-jupyternotebooks-part-1-your-first-notebook-9a99a781fde7

#RSAC



John Lambert – The Githubification of Infosec

http://youtu.be/B3o-9z3Eitg https://medium.com/@johnlatwc/the-githubification-ofinfosec-afbdbfaad1d1



RSAConference2021

Bringing DevOps To Detection

Leonidas

Automated Attack Simulation

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

Framework automatically generates...

- Executor serverless function
- Sigma detection rules
- Documentation

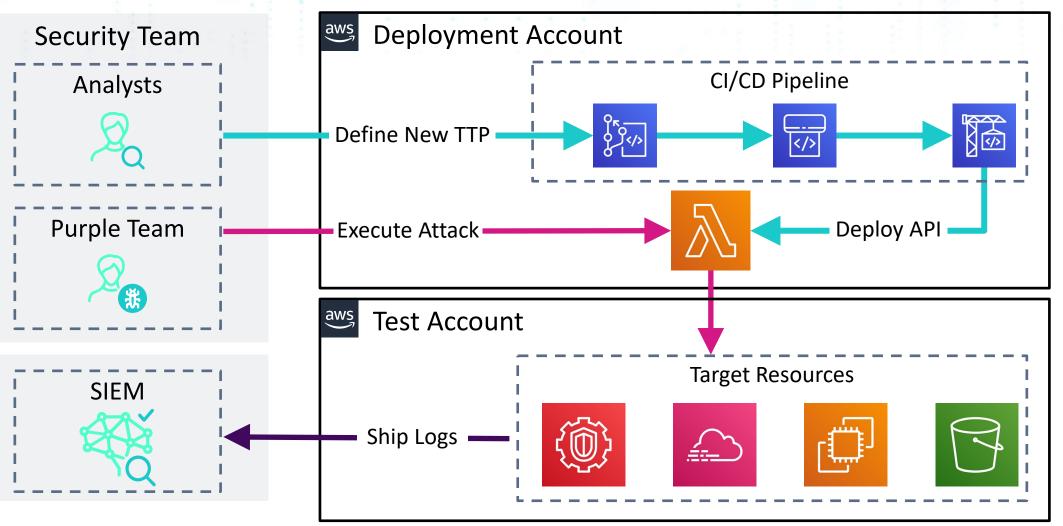
Executor

- Multi-cloud support in a single instance
- User/role/service account impersonation



#RSAC

Leonidas







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

control and reduce the chance of malicious activity being detected.

Author	Last Update
Nick Jones	2020-06-18

Required Permissions Required Parameters Attacker Action **Detection Case** ELK query Sigma Definition An adversary may attempt to add a new GuardDuty IP whitelist in order to whitelist systems they

Table of contents

MITRE IDs

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



Generate

Documentation





2

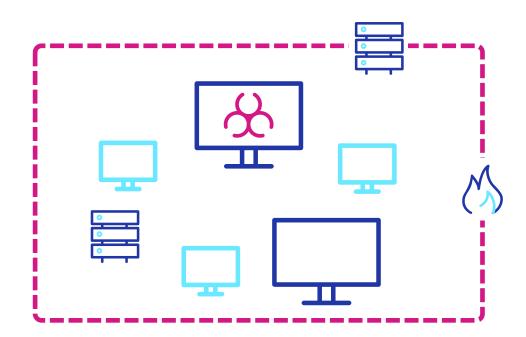




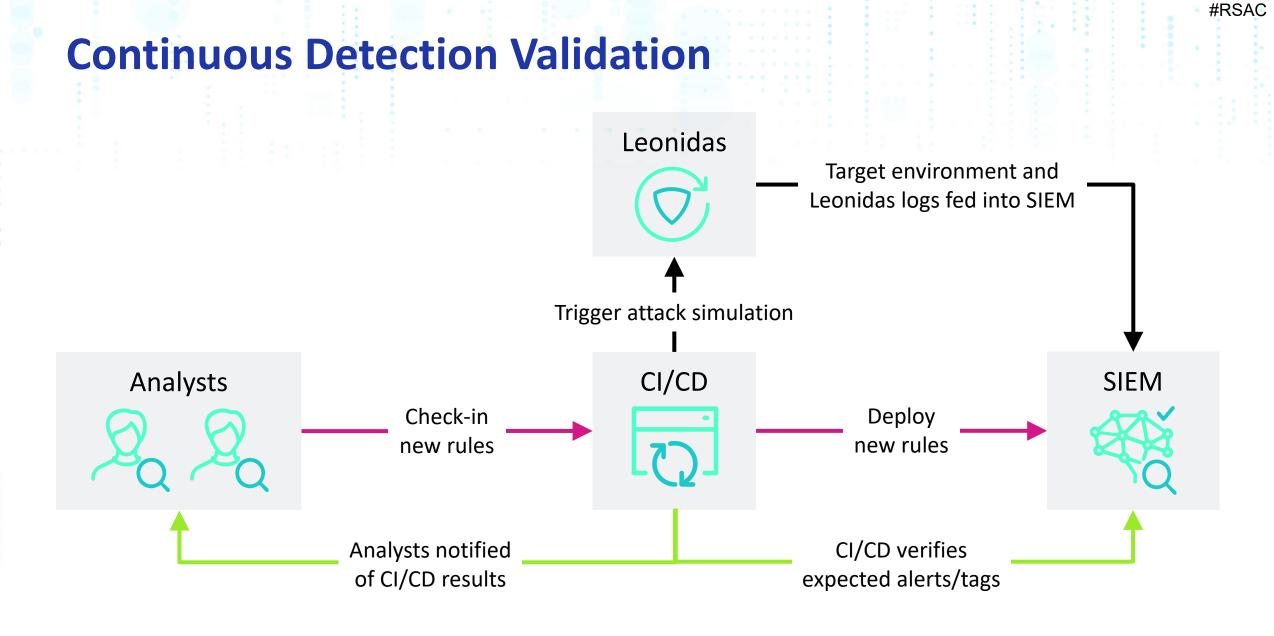




Continuous Cross-Environment Testing





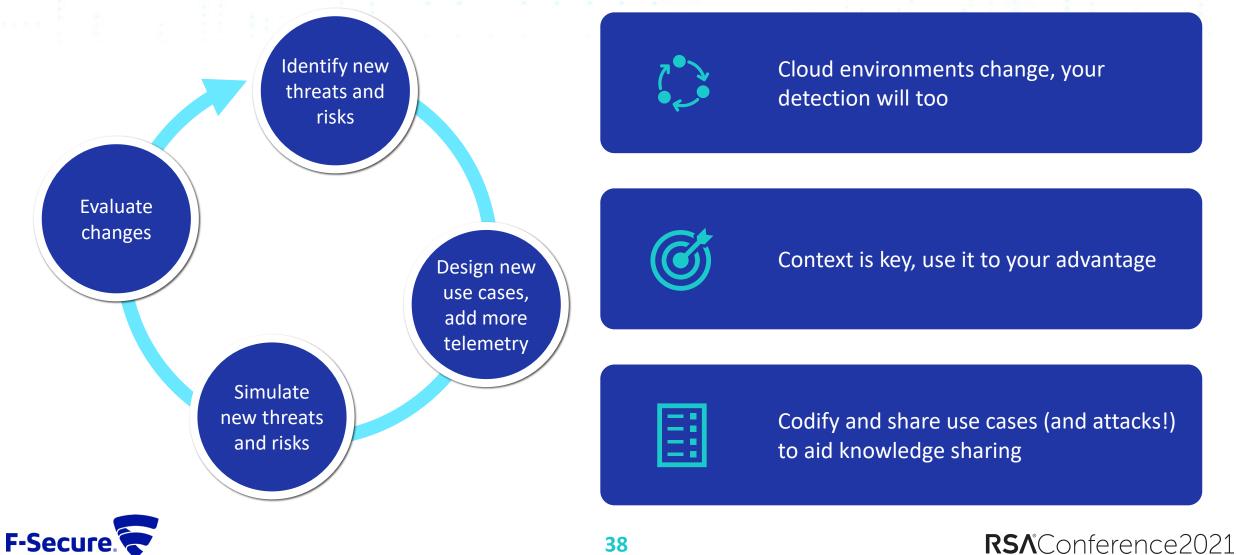




RS∧°Conference2021

Conclusions

Detection is a journey



Applying What You Have Learned Today

• Next week you should:

- Identify existing org policies for logging and confirm aggregation.
- Where possible, ensure quick-wins e.g. Guard Duty are configured.

- In the first three months you should:
 - Document org's cloud workloads.
 - Take example workload and perform threat modelling exercise.
 - Execute test cases and confirm efficacy of detection capability.



Applying What You Have Learned Today

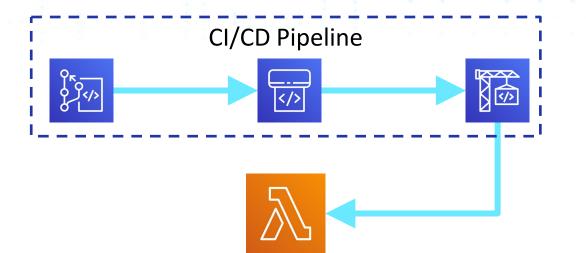
• Within six months you should:

- Ensure defenders have access and familiarity with cloud attacks and subsequent triage.
- Ensure these activities form part of your development lifecycle.
- Devise continuous threat modeling and detection engineering process.
- Evangelize this approach across your teams!



Leonidas





Target Resources



Automate attacker actions in the cloud



Both test and detection cases



55 test cases - more to come



https://github.com/fsecurelabs/leonidas



