AUTOMATING ATTACK SIMULATIONS IN THE CLOUD

Nick Jones

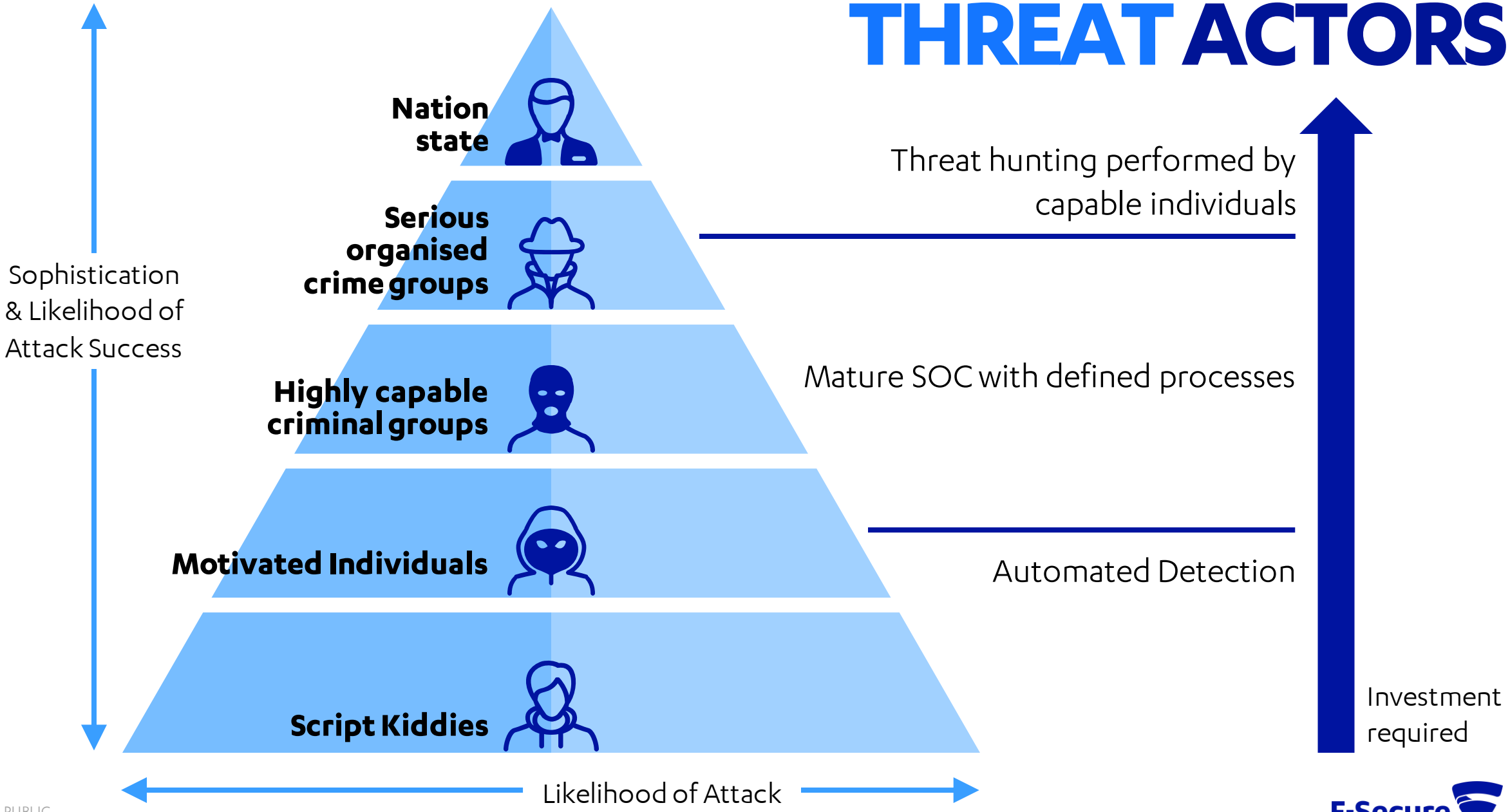
Fwd:CloudSec – 29th June 2019

F-Secure

AGENDA

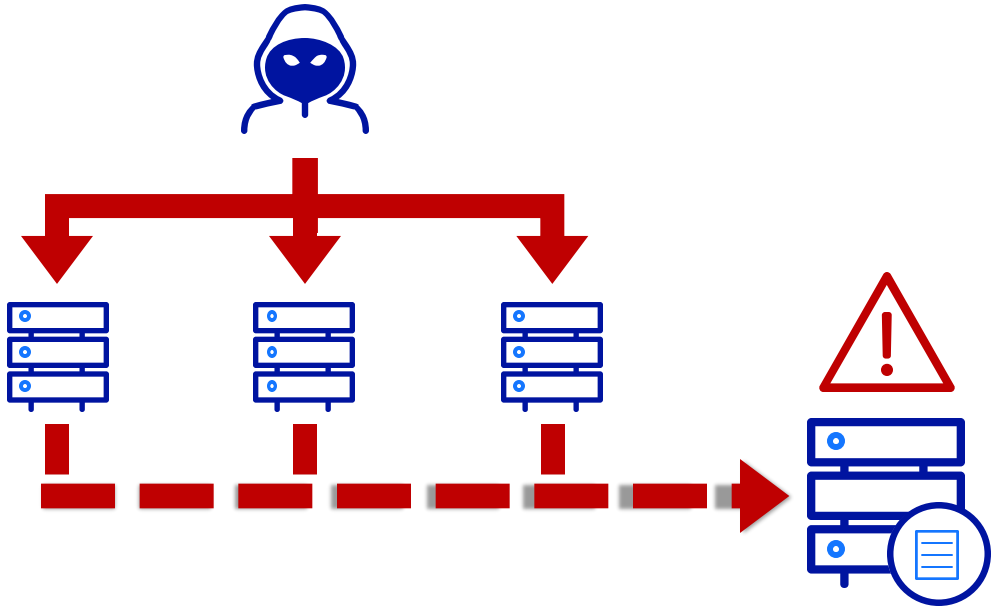
CHALLENGES IN C# AUTOMATION

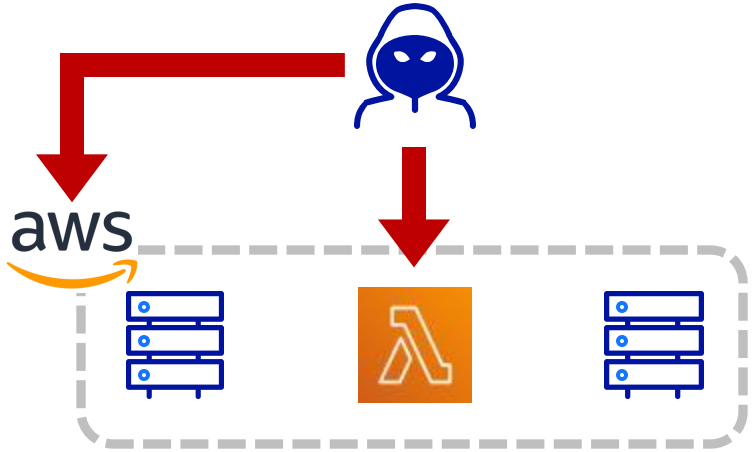
THREAT ACTORS



F-Secure

ON-PREMISE VS CLOUD DETECTION





HOW CLOUD DETECTION DIFFERS

UNCERTAINTY OF MALICIOUS INTENT

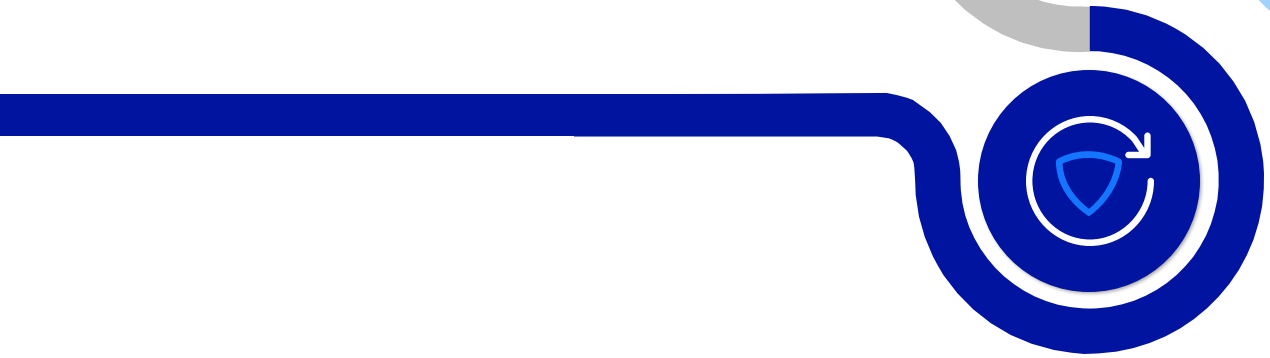
Fewer actions in the cloud are obviously bad compared to on-premise, making generic detection rules harder

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

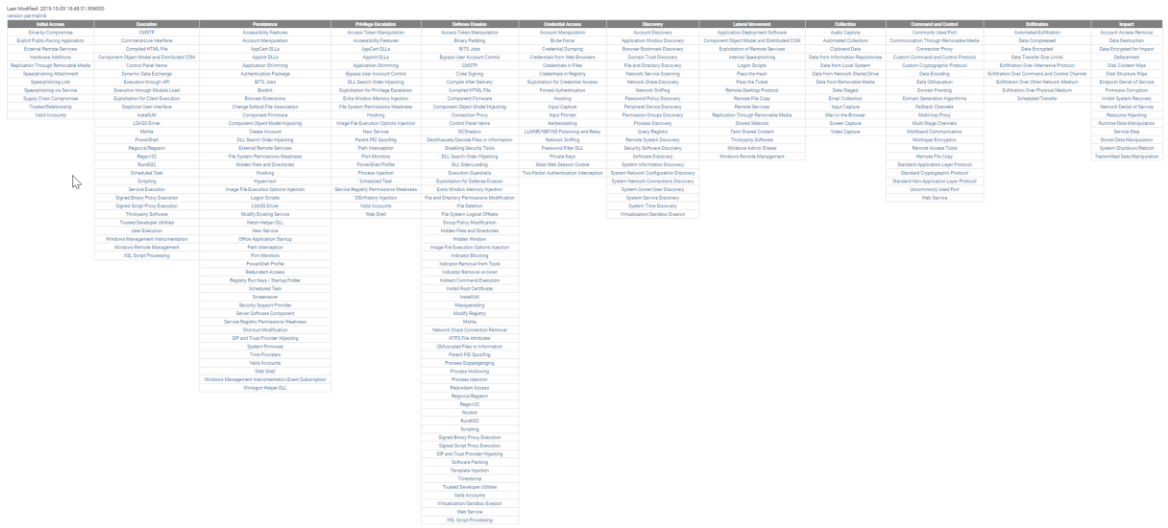
Org-wide CloudTrail etc makes it easier to gain visibility into most of your estate. Shadow IT now the primary issue, rather than coverage of known assets



ATTACKERS ARE 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



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				

F-Secure

DRAW INSPIRATION FROM...

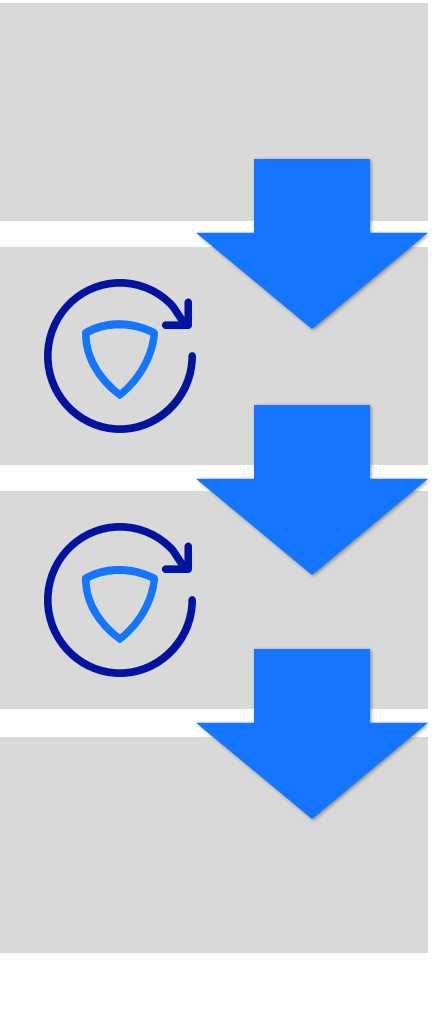
HOW DO WE VALIDATE?

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

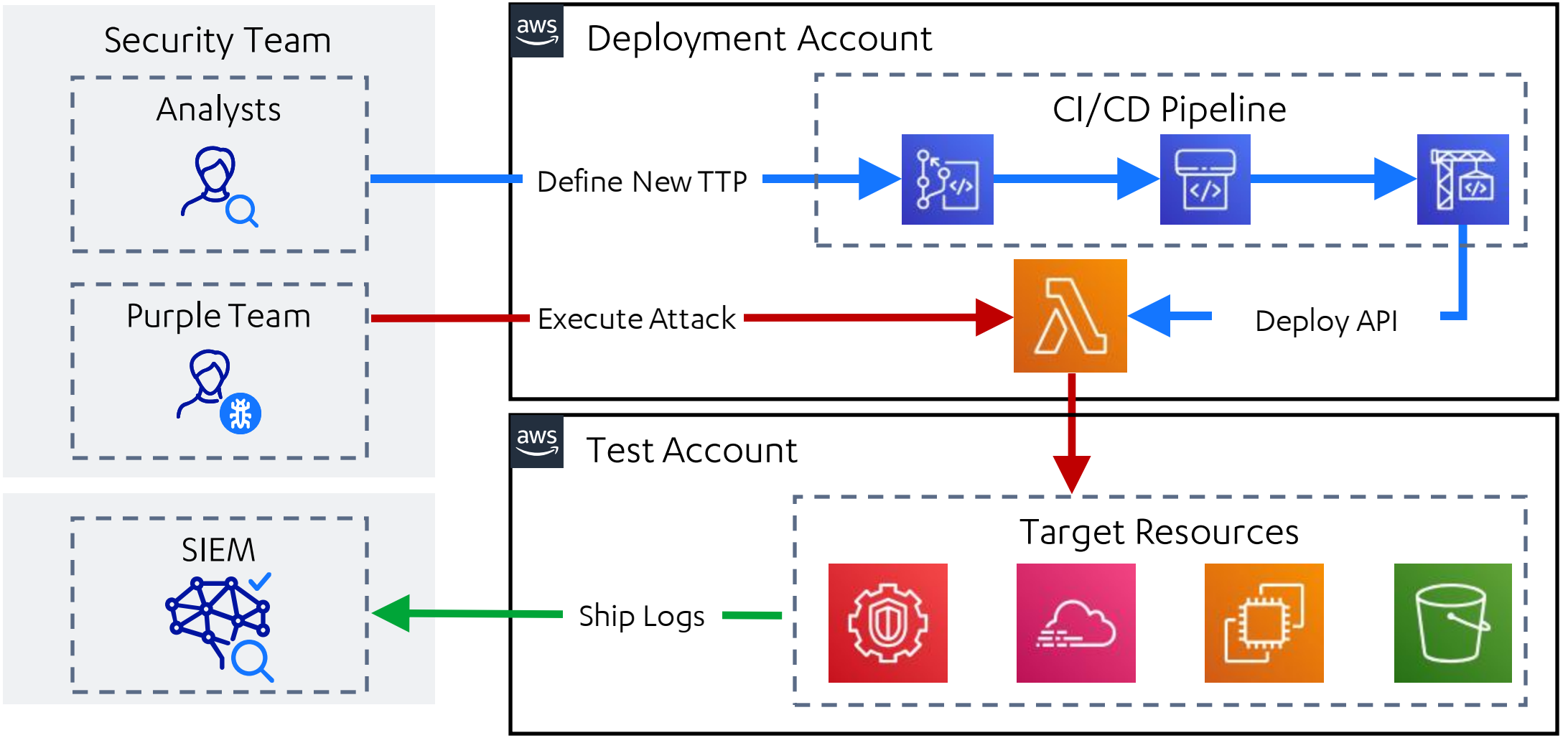
https://posts.specterops.io/threat-hunting-with-jupyter-notebooks-part-1-your-first-notebook-9a99a781fde7

John Lambert – The Githubification of Infosec

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

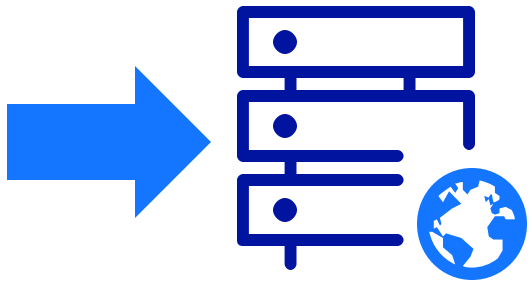
https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1

LEONIDAS



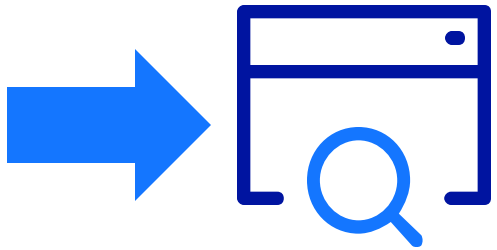
GENERATE ATTACK SIMULATION

```
- 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

```yaml
- 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"
```



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

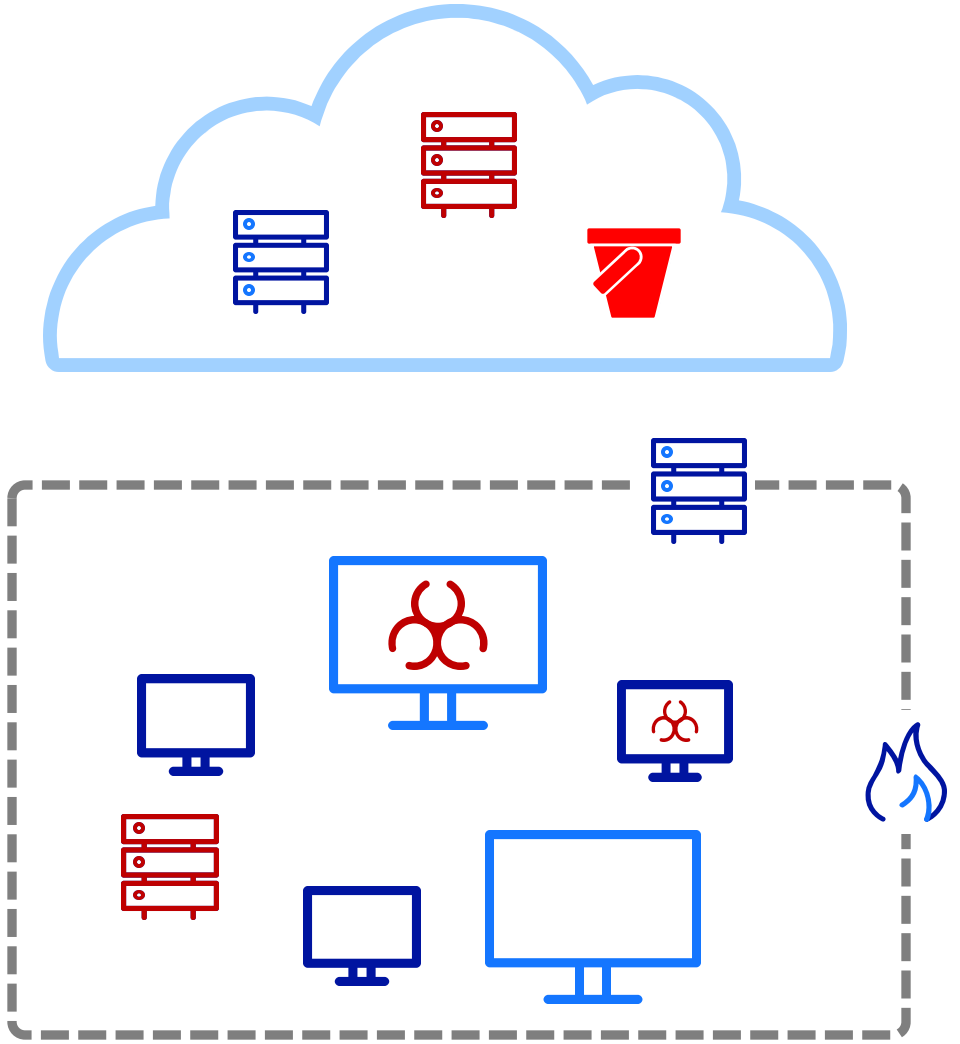
Required Parameters

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

GENERATE DOCUMENTATION

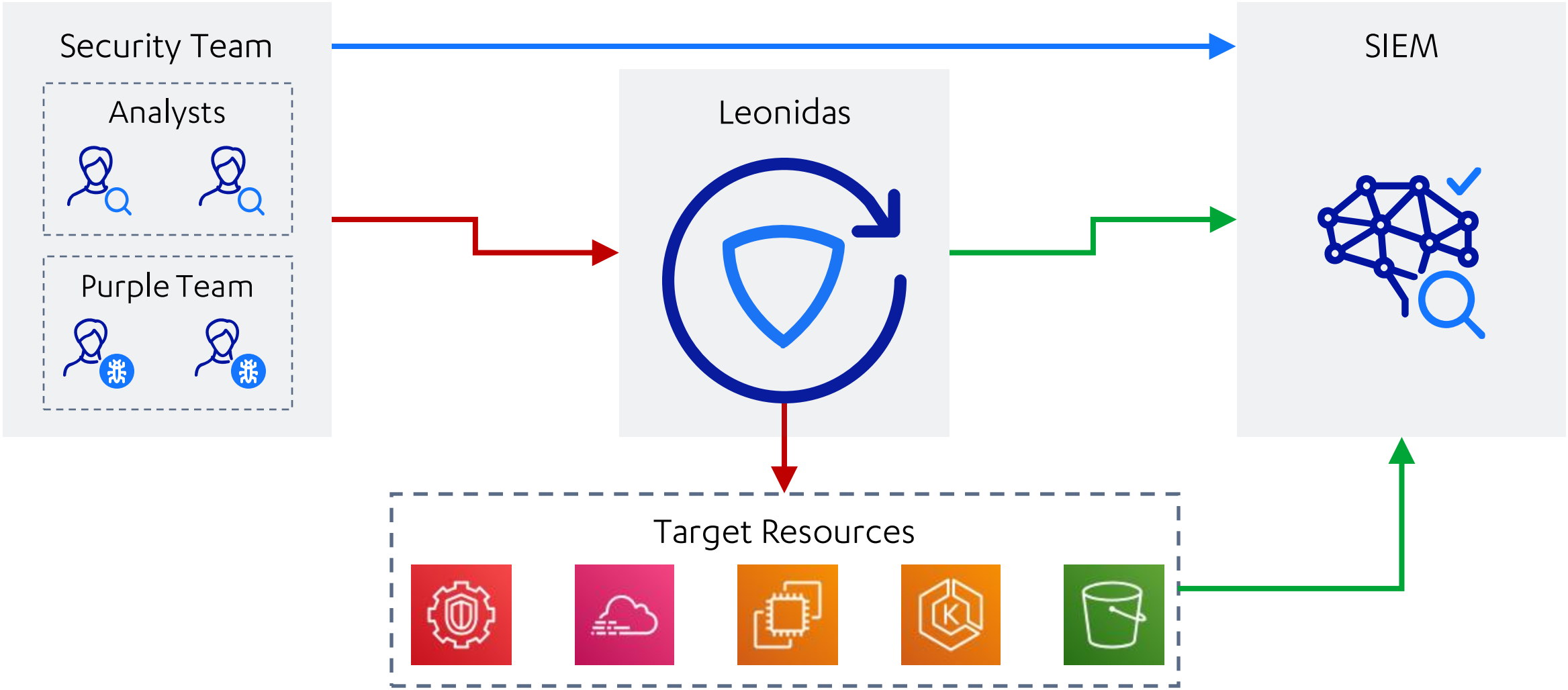
F-Secure

CONTINUOUS TESTING



F-Secure

CONTINUOUS INTEGRATION



HOW DO I START?

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

02 Prioritise attack paths and actions

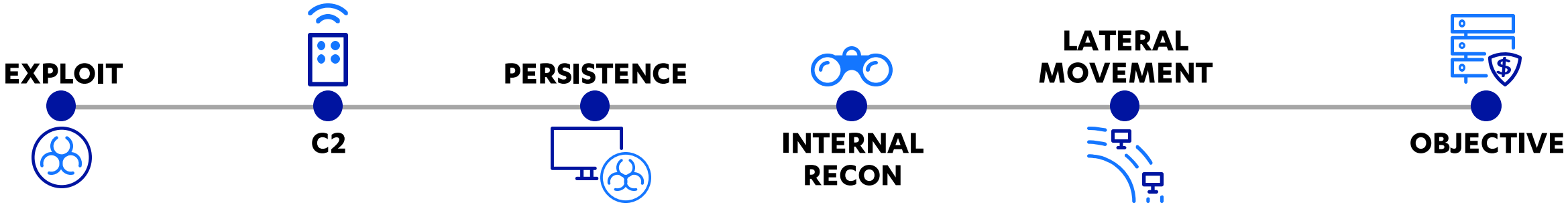
03 Pick the most important attack paths, codify them

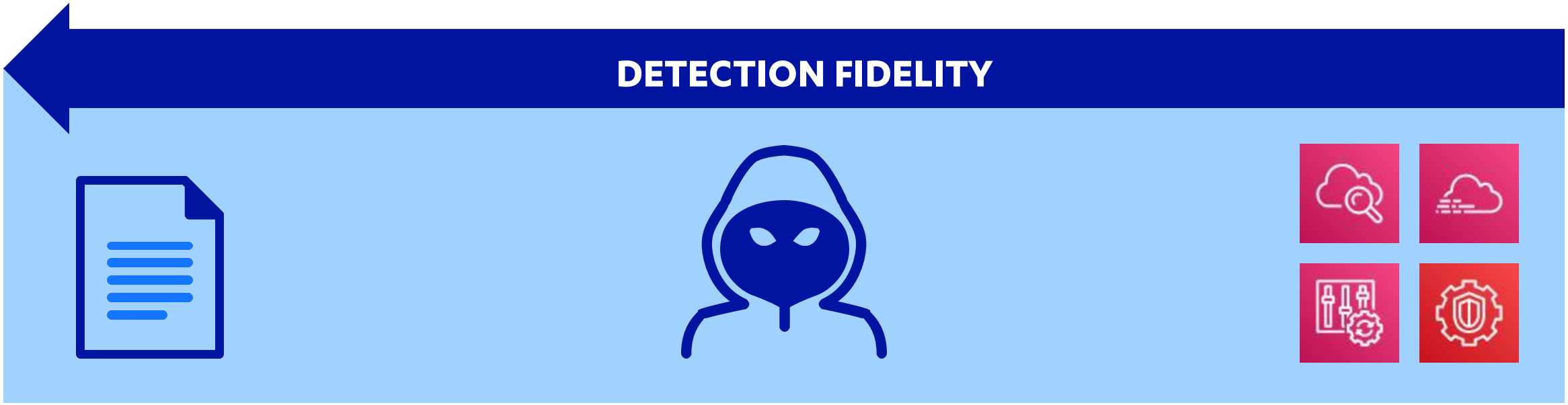
04 Verify telemetry is available to defenders

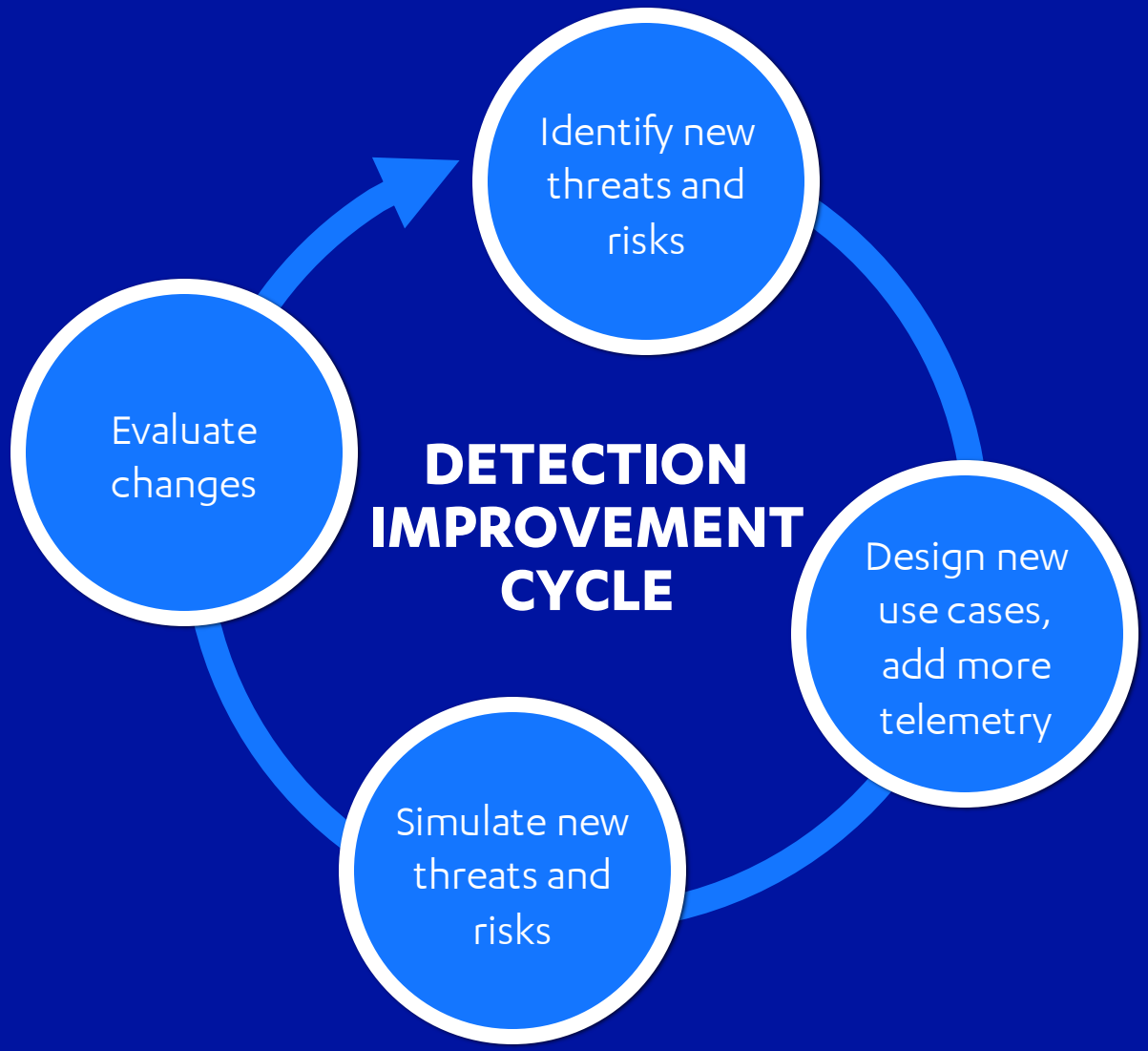
05 Execute attacker actions as kill chains, verify detection cases work as expected.

F-Secure

WHERE DO I START?





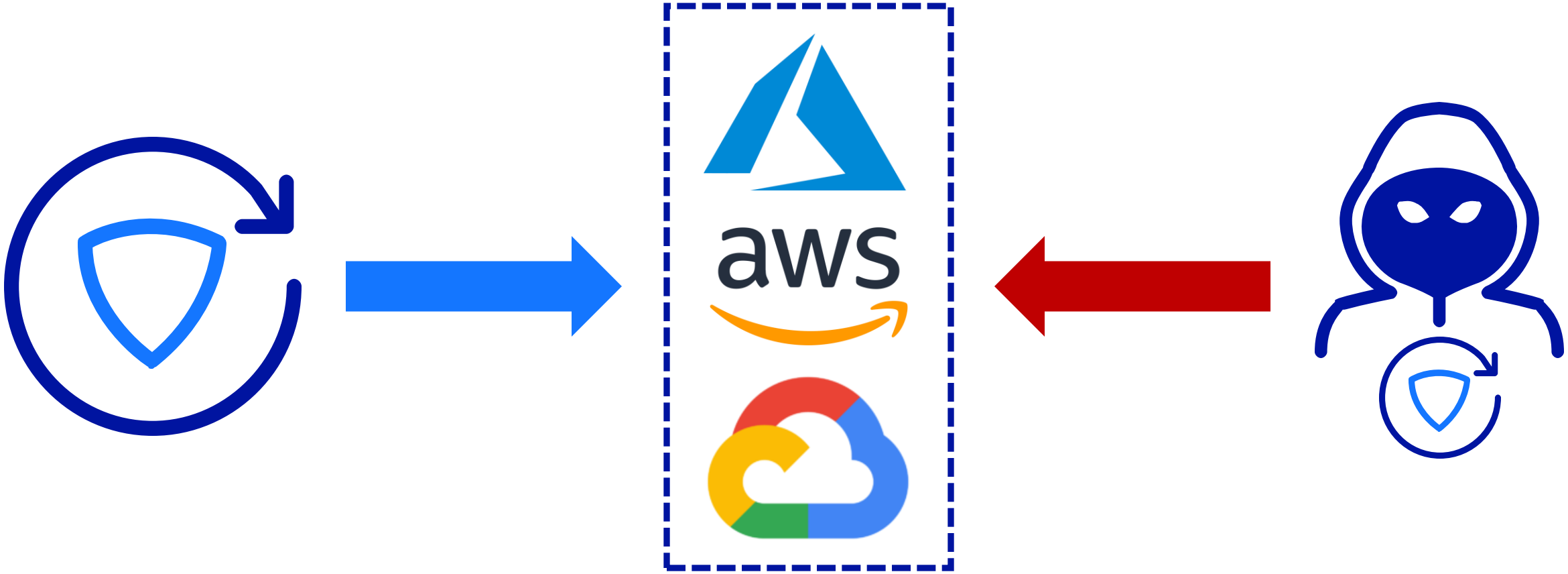


DETECTION IS A JOURNEY

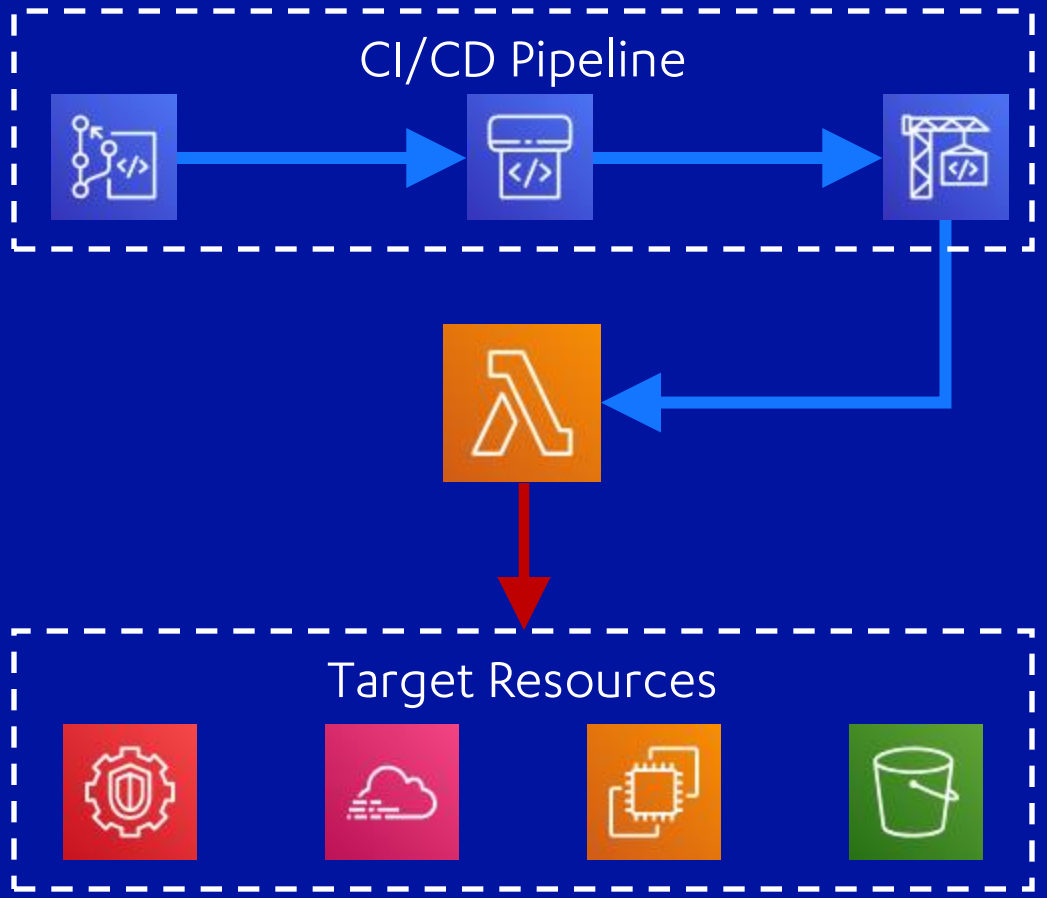
- Effective detection is a moving target
- Treat it as an ongoing development project
- Agile/Scrum works for security too

F-Secure

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

F-Secure

F-Secure®

Feedback: https://bit.ly/fwdcs-9