RSAConference2021

May 17 – 20 | Virtual Experience

SESSION ID: **AIR-T14**

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

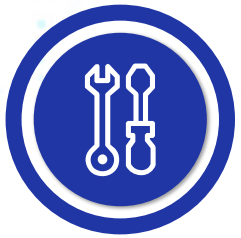
Alfie Champion

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

RSAConference2021

On-Premise vs Cloud

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 are important here, so is developing environment-specific alerting.

GAINING VISIBILITY IS EASIER

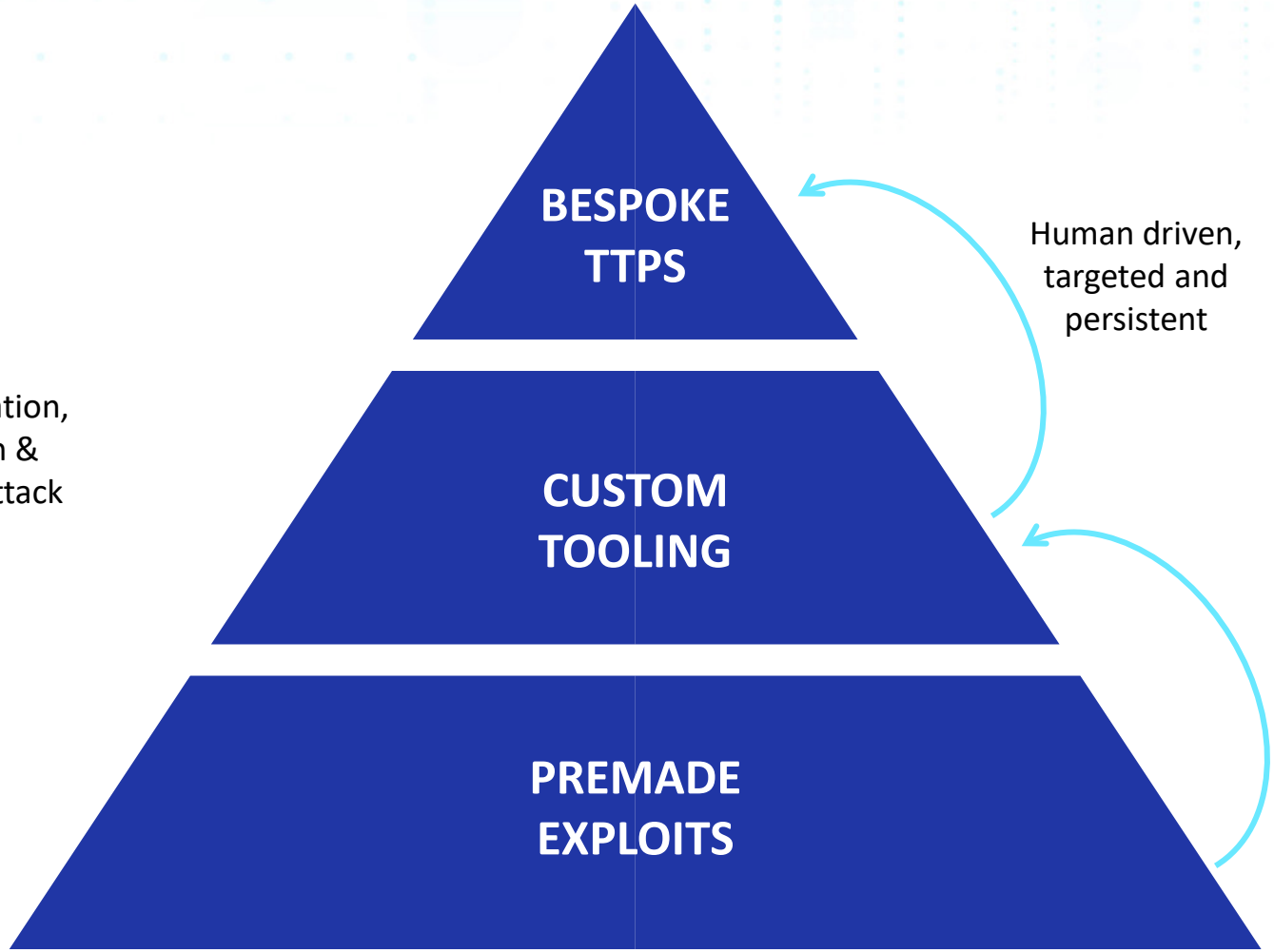
Org-wide CloudTrail, etc. makes it easier to gain visibility into much of your estate. Shadow IT now the primary issue, rather than coverage of known assets.

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.

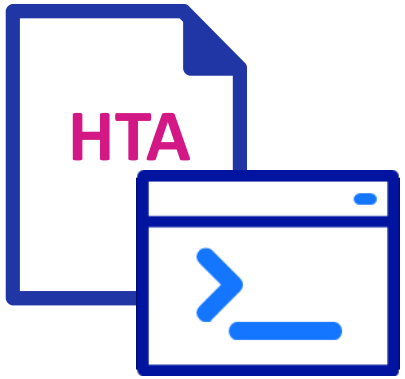
Threat Actors

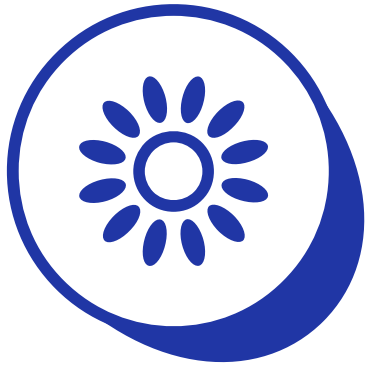
Attacker Motivation, Sophistication & Likelihood of Attack Success



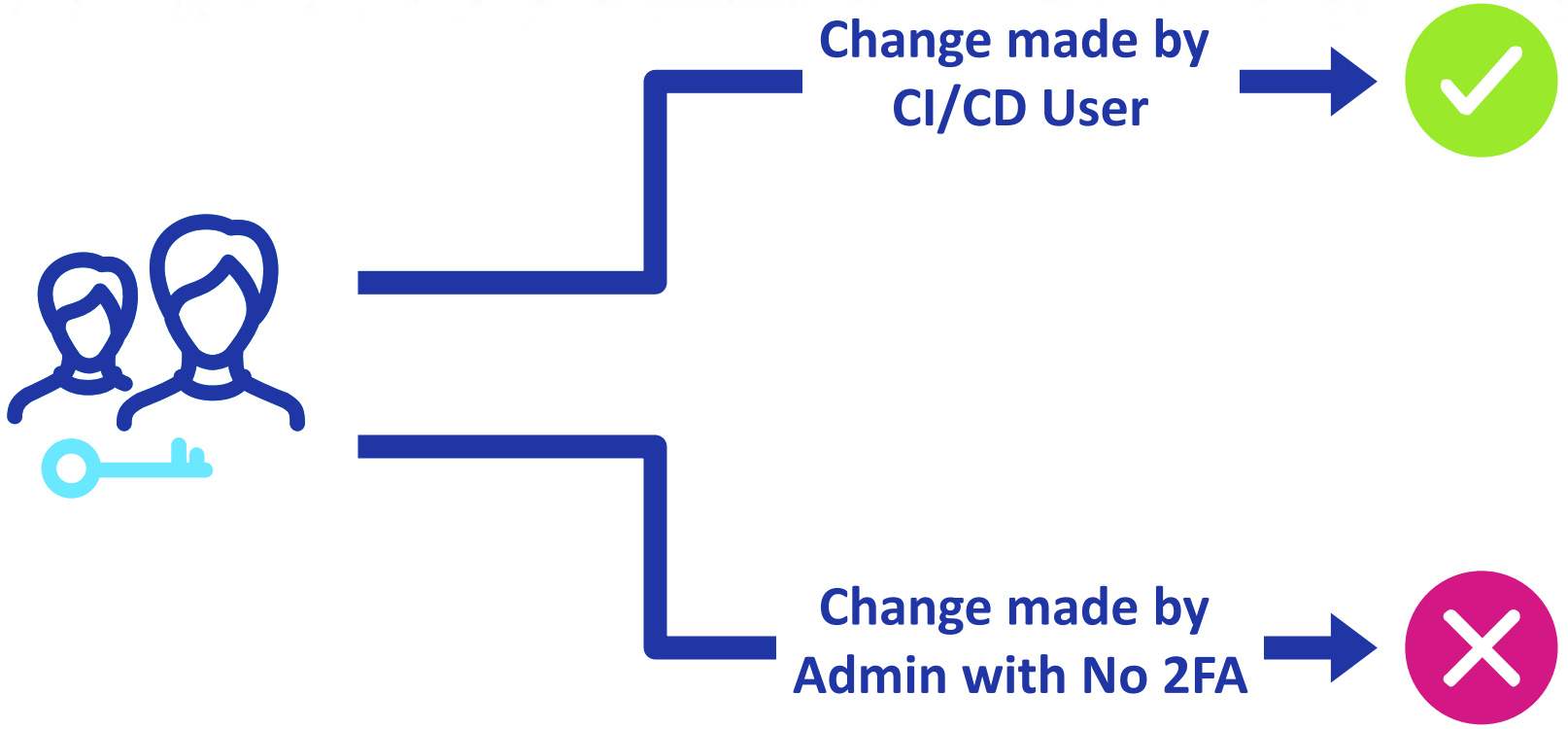
Likelihood and Frequency of Malicious Activity

Mindset Shift

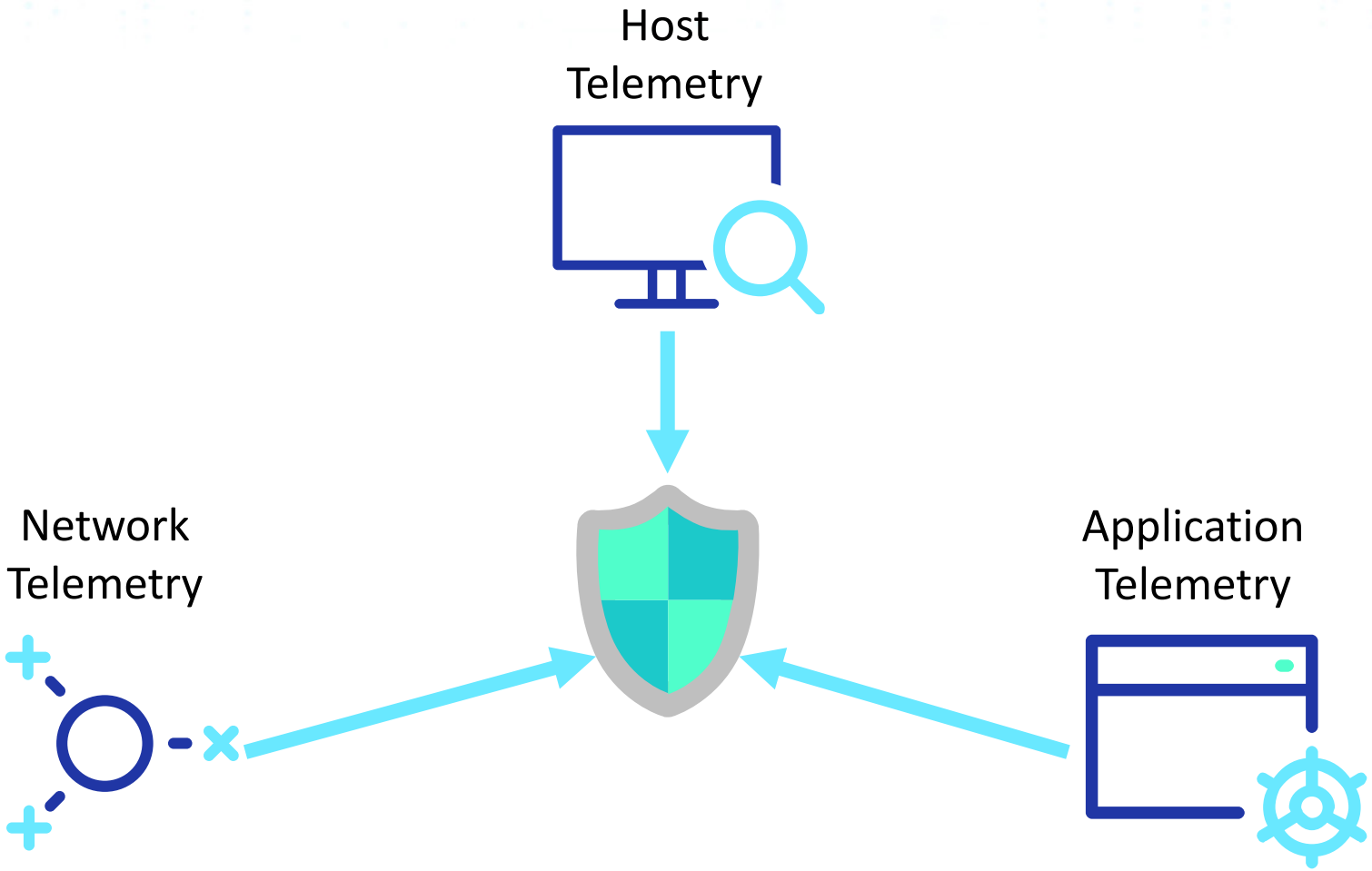




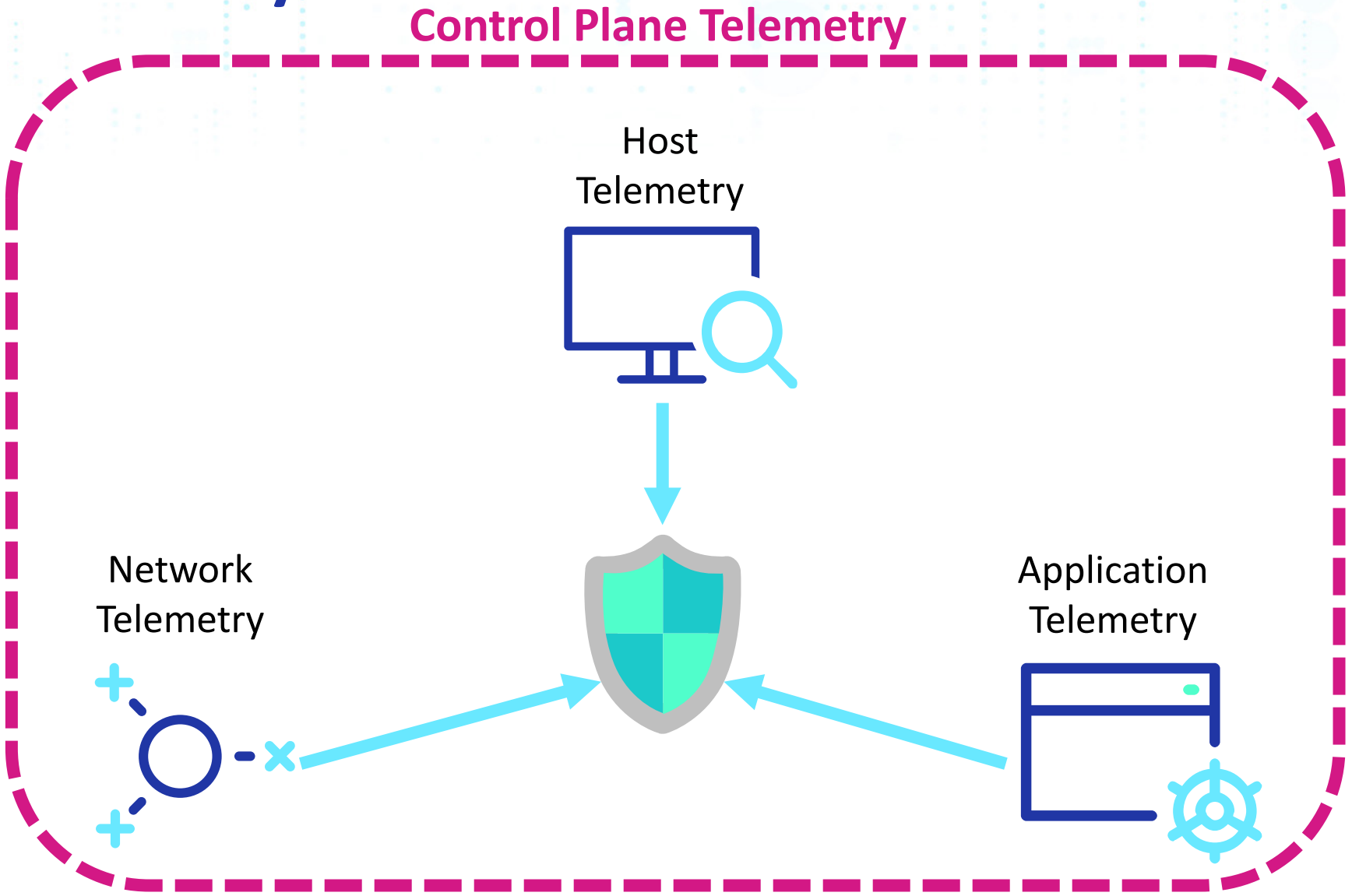
Context is key



On-Premise Telemetry



Cloud 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

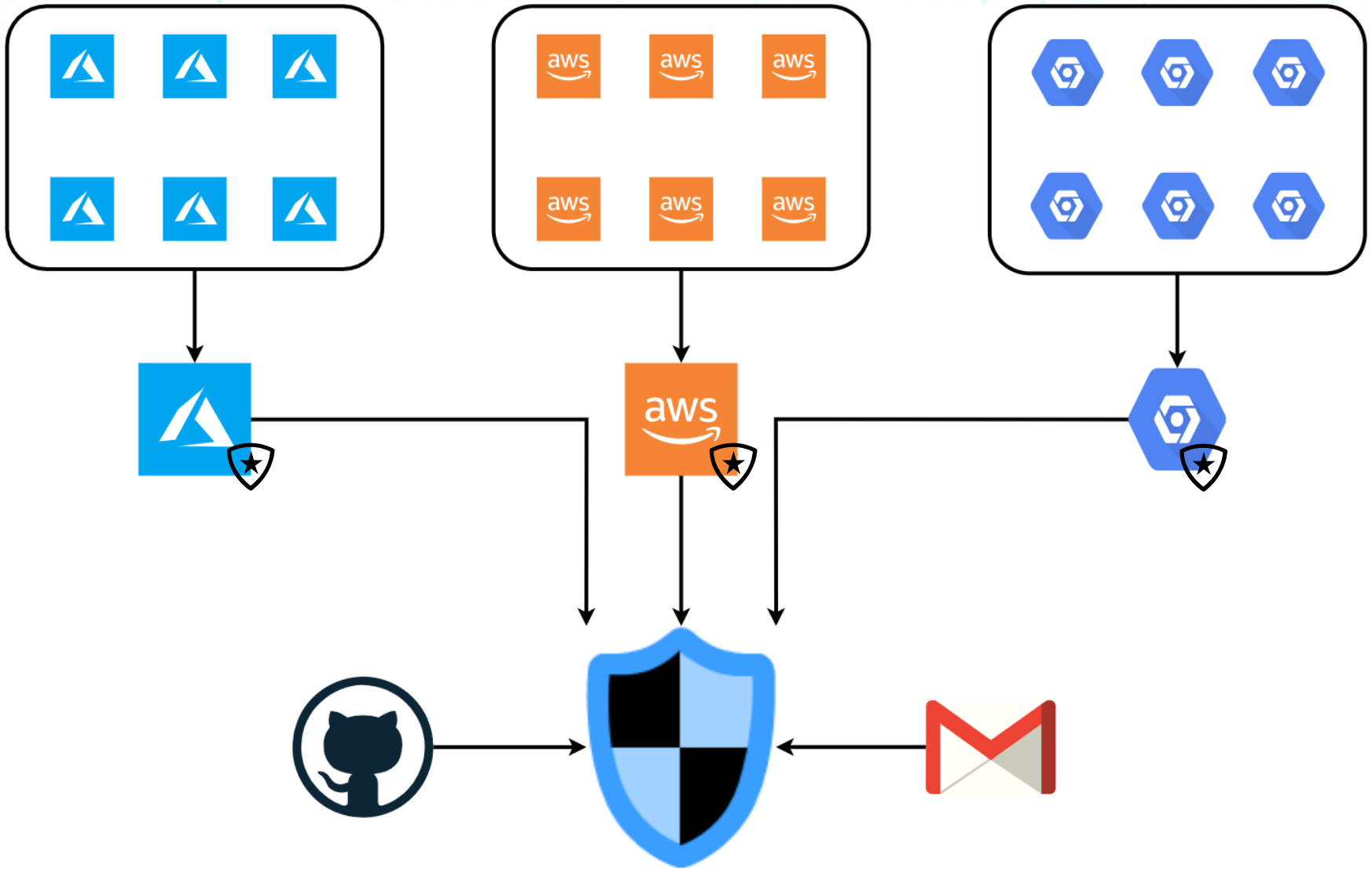
- Build the context from the architectural stage.
  - What should the environment do?
  - What shouldn't it do?
- Sharing the above with analysts gives them the insight into what things should be doing?

- BONUS: Exercising this with analysts gets them used to investigation in cloud.

RSAConference2021

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

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

Prioritising Telemetry and Use Cases

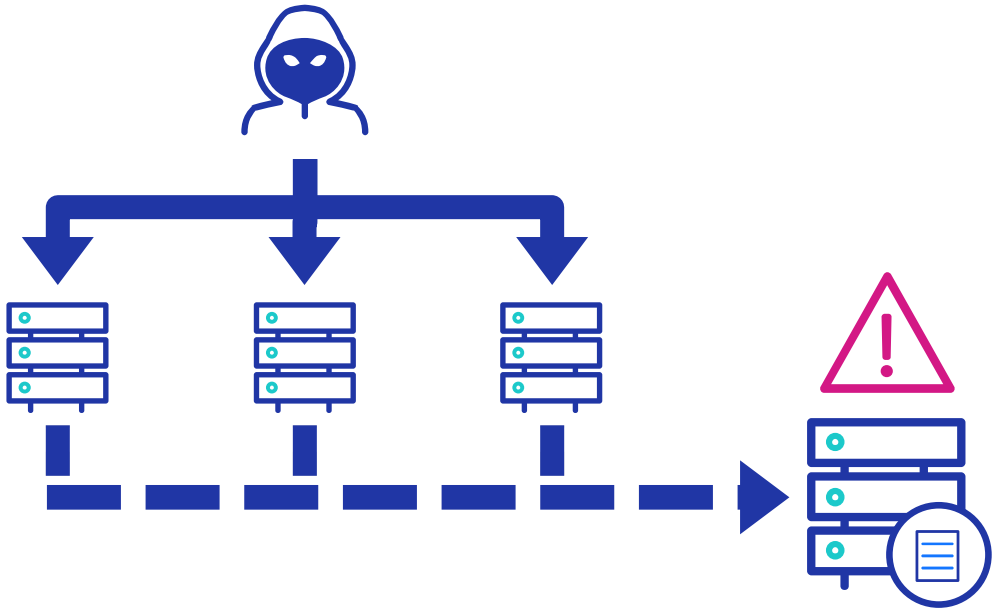
- Gather telemetry for the services you're using.

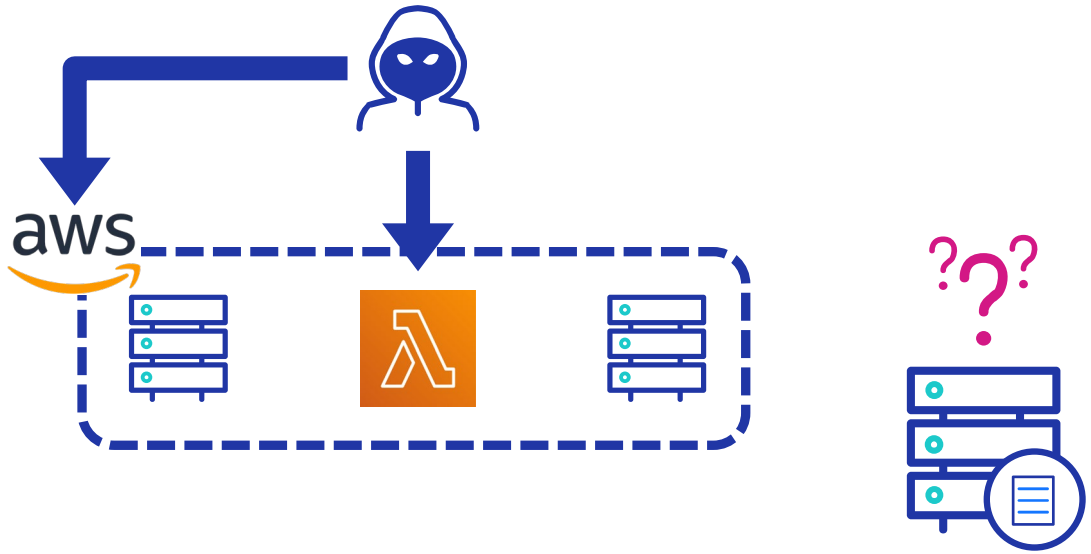
- Where are the areas of critical activity?
  - What detections can/should you build?
  - Does a given log source provide actionable insight?
  - Use cases should be prioritized based on threat modelling outputs.

RSAConference2021

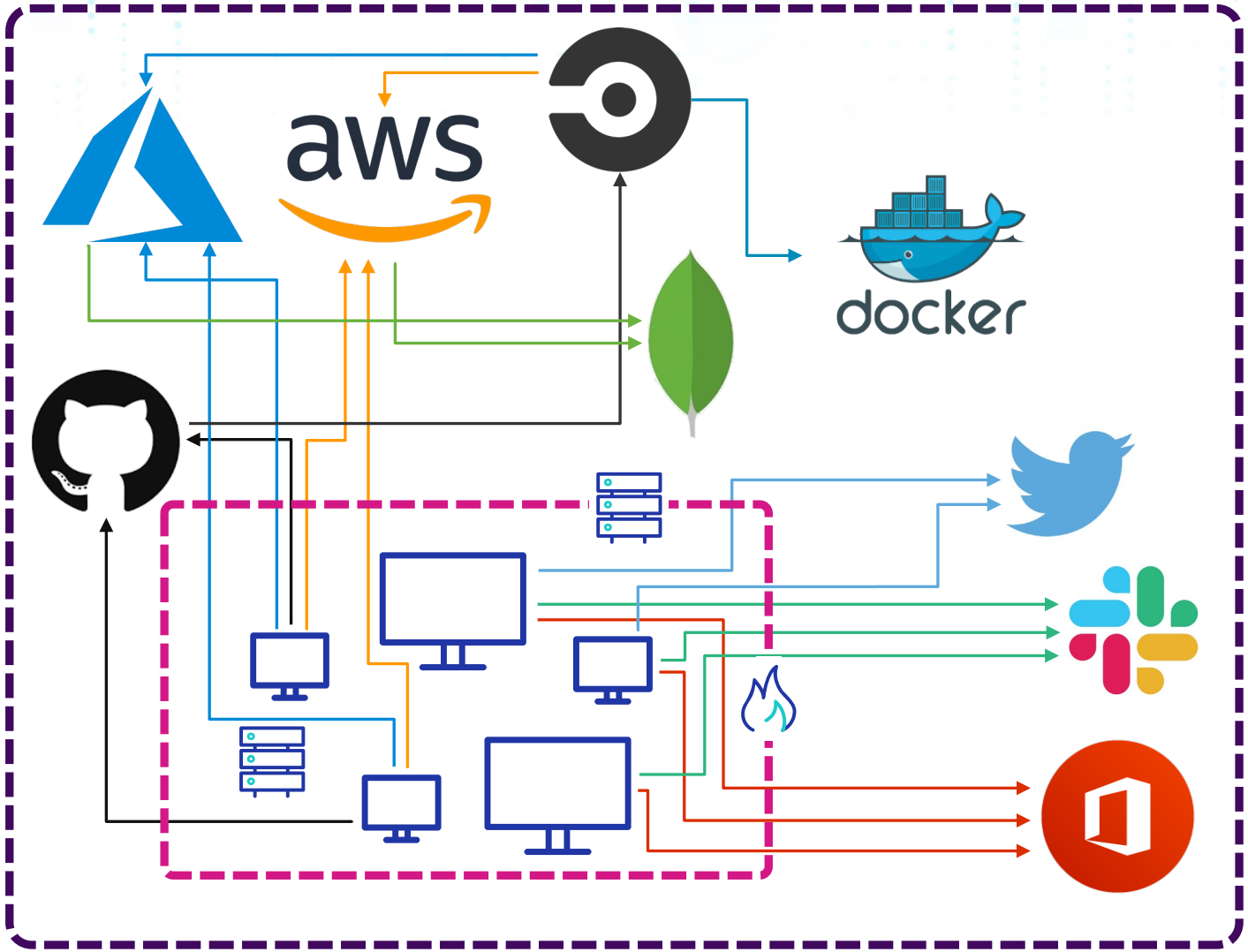
Likely Attacker Activity

On-Premise vs Cloud Detection

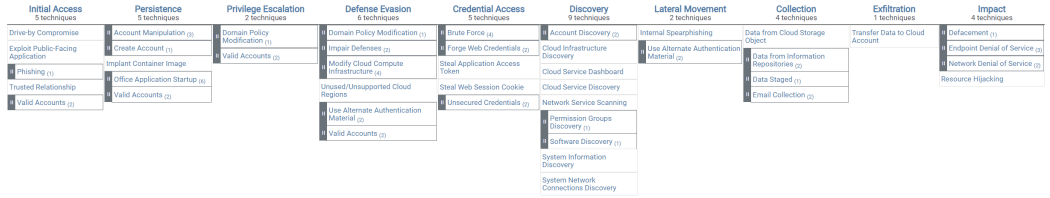




Enterprise Cloud Adoption



Enterprise vs Cloud ATT&CK



MITRE ATT&CK™

What's an attacker likely to do?

Vectors We've Exploited

Identity Management

- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials

Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.

Application Vulnerabilities

- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

Vectors We've Exploited

Identity Management

- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials

Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.

Application Vulnerabilities

- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

Vectors We've Exploited

Identity Management

- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials

Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.

Application Vulnerabilities

- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

Vectors We've Exploited

Identity Management

- Exposed credentials in source code repositories
- Single Sign-On with compromised or reused credentials

Pivot From Other Environments

- On-premise host compromise leading to privileged cloud access.
- Similarly, access tied to on-premise Active Directory

SCM and CI/CD

- Infrastructure-as-code repositories compromised.
- Adding users, misconfigurations or network access.

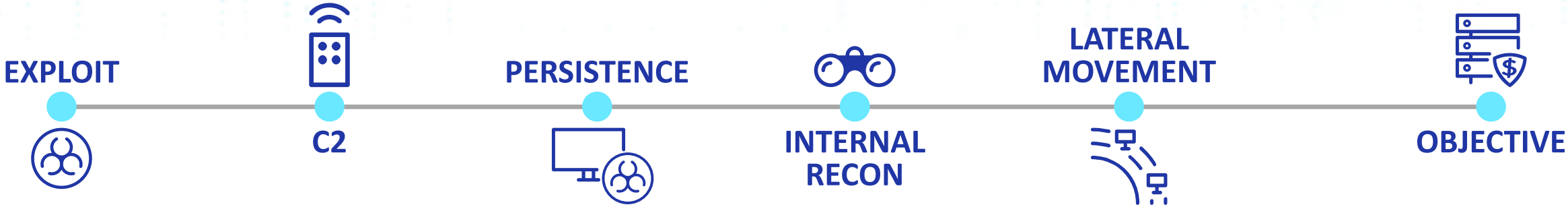
Application Vulnerabilities

- RCE vulnerabilities on cloud-hosted assets to provide initial foothold.
- Misconfiguration to pivot to control plane.

How do I start?

1. Threat model your environment, identify attack paths
2. Prioritise attack paths
3. Understand the TTPs the attack paths consist of
4. Verify telemetry available to defenders
5. Execute attacker actions as kill chains, verify detection cases work as expected.

Where do I start?



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

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

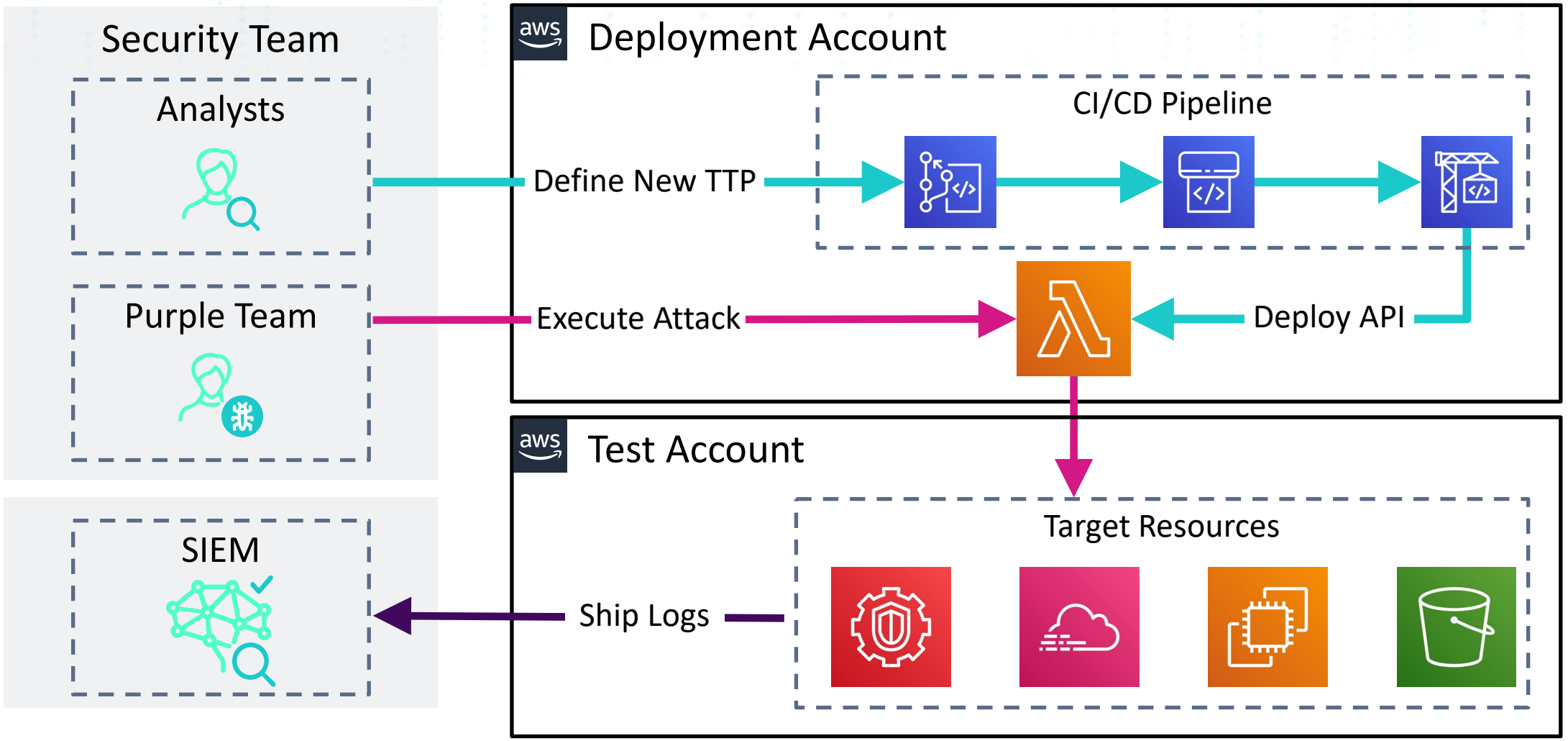
Framework automatically generates…

- Executor – serverless function
- Sigma detection rules
- Documentation

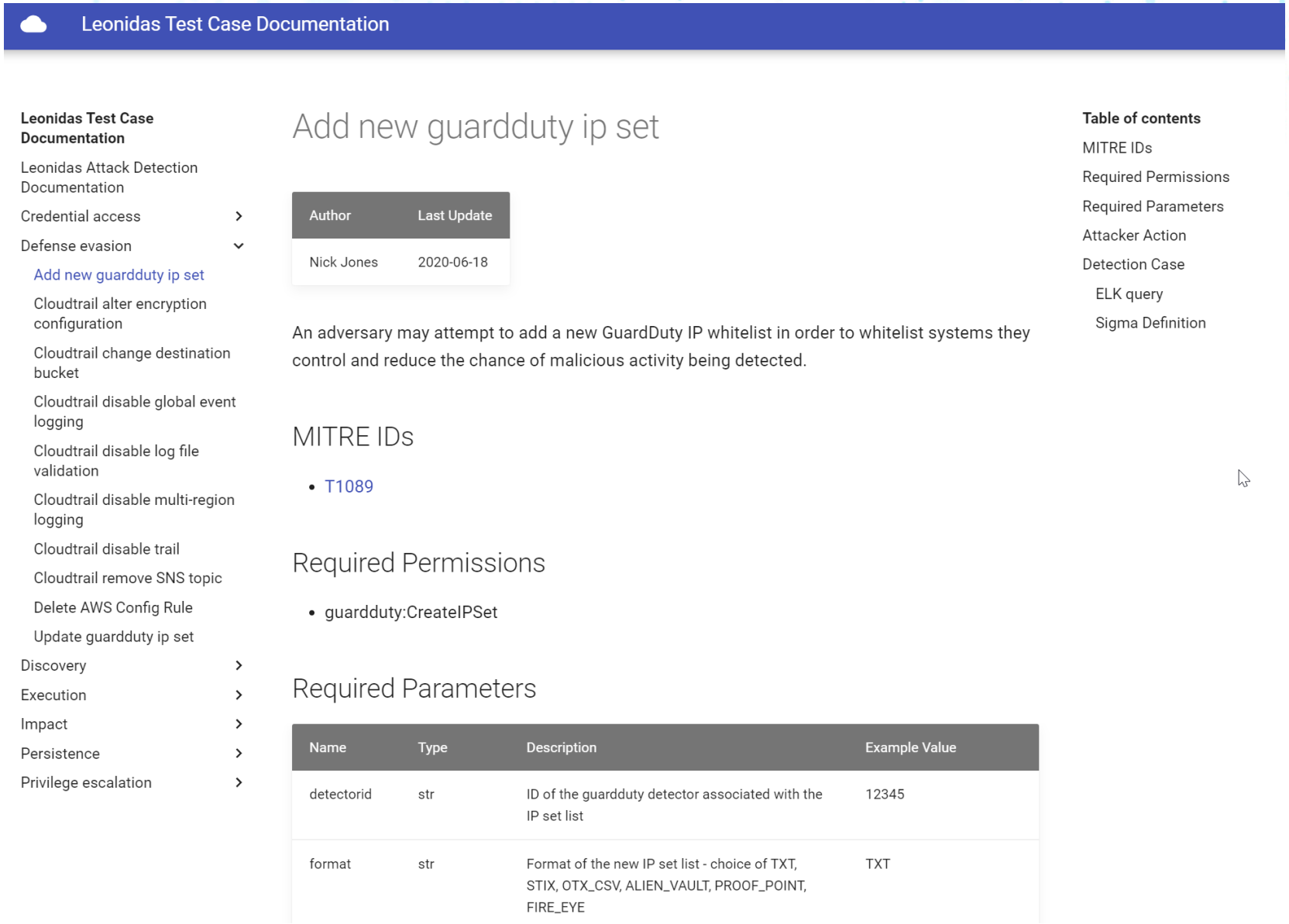
Executor

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

Leonidas

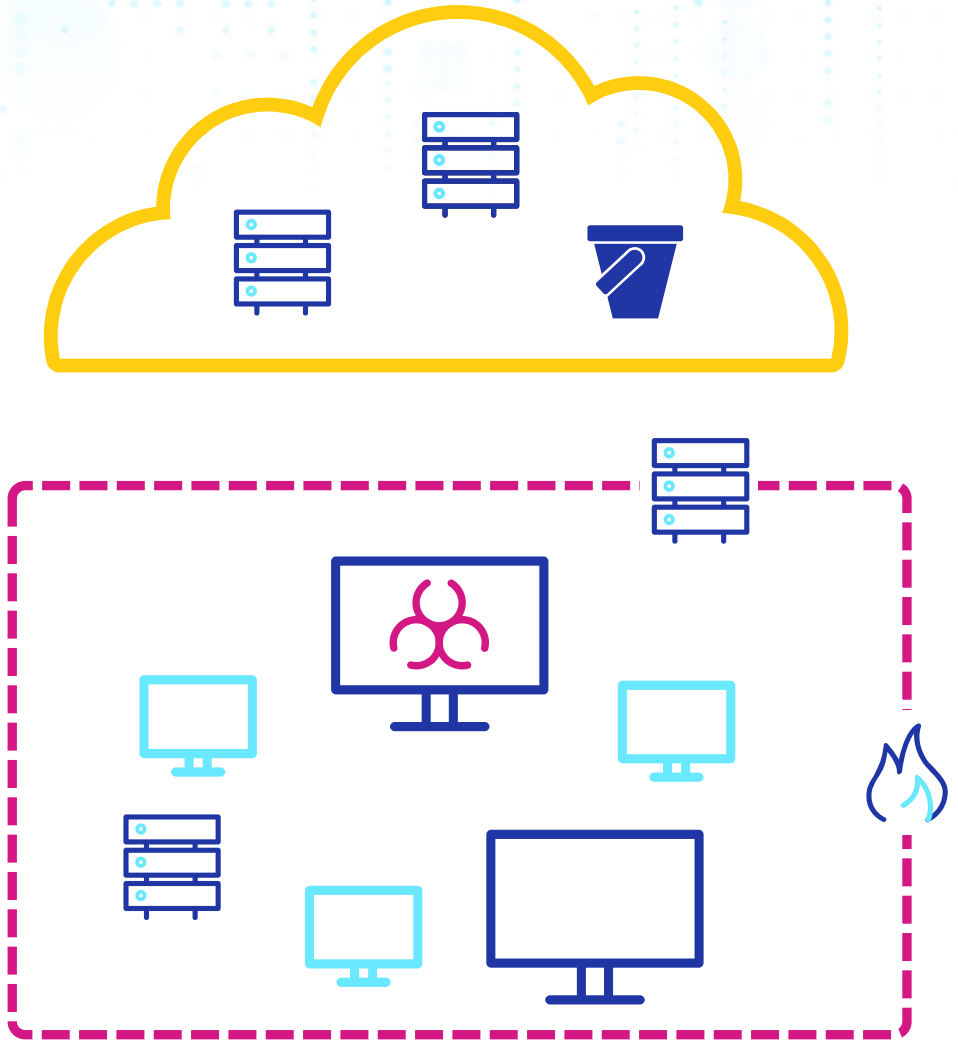

Security Team
Analysts
Purple Team
SIEM
aws
Deployment Account
CI/CD Pipeline
Define New TTP
Execute Attack
Deploy API
aws
Test Account
Target Resources
Ship Logs

Generate Documentation

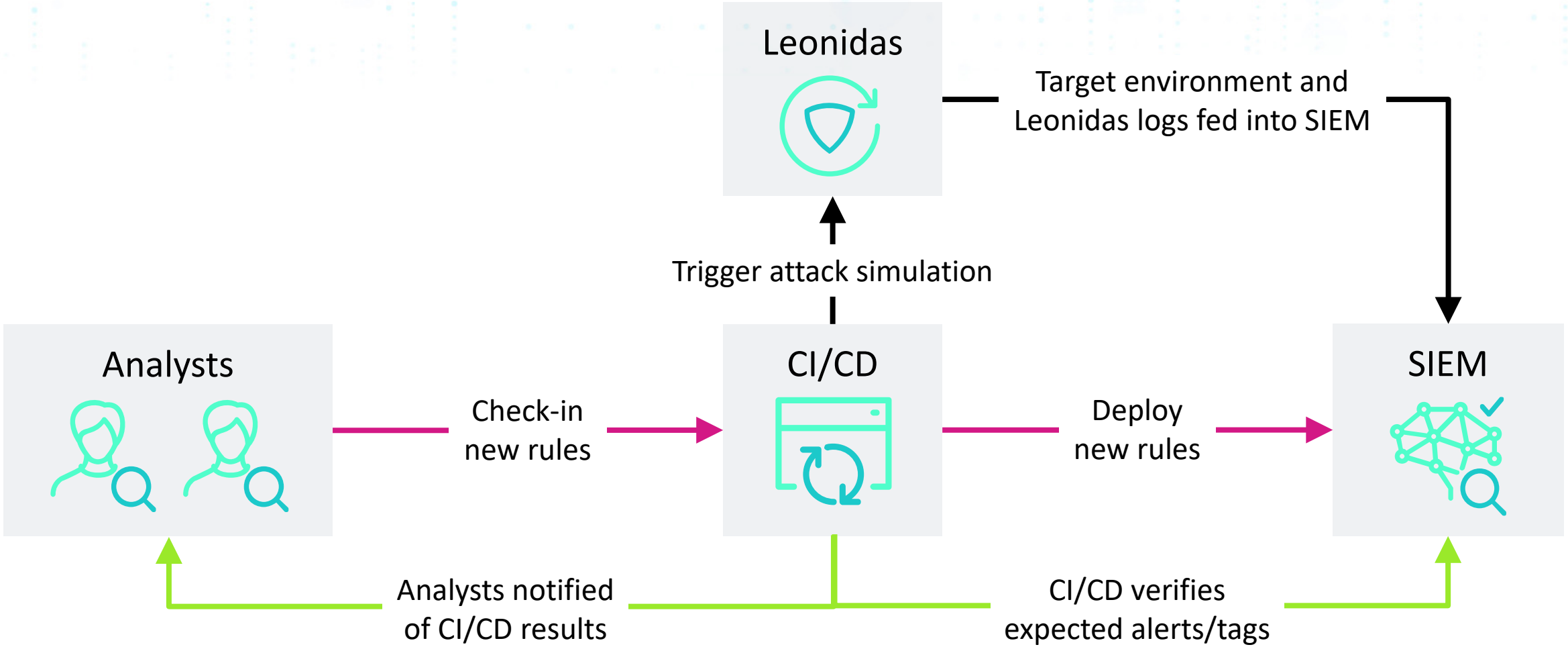


Demo

Continuous
Cross-Environment
Testing



Continuous Detection Validation



RSAConference2021

Conclusions

Detection is a journey

Cloud environments change, your detection will too

Context is key, use it to your advantage

Codify and share use cases (and attacks!) to aid knowledge sharing

Applying What You Have Learned Today

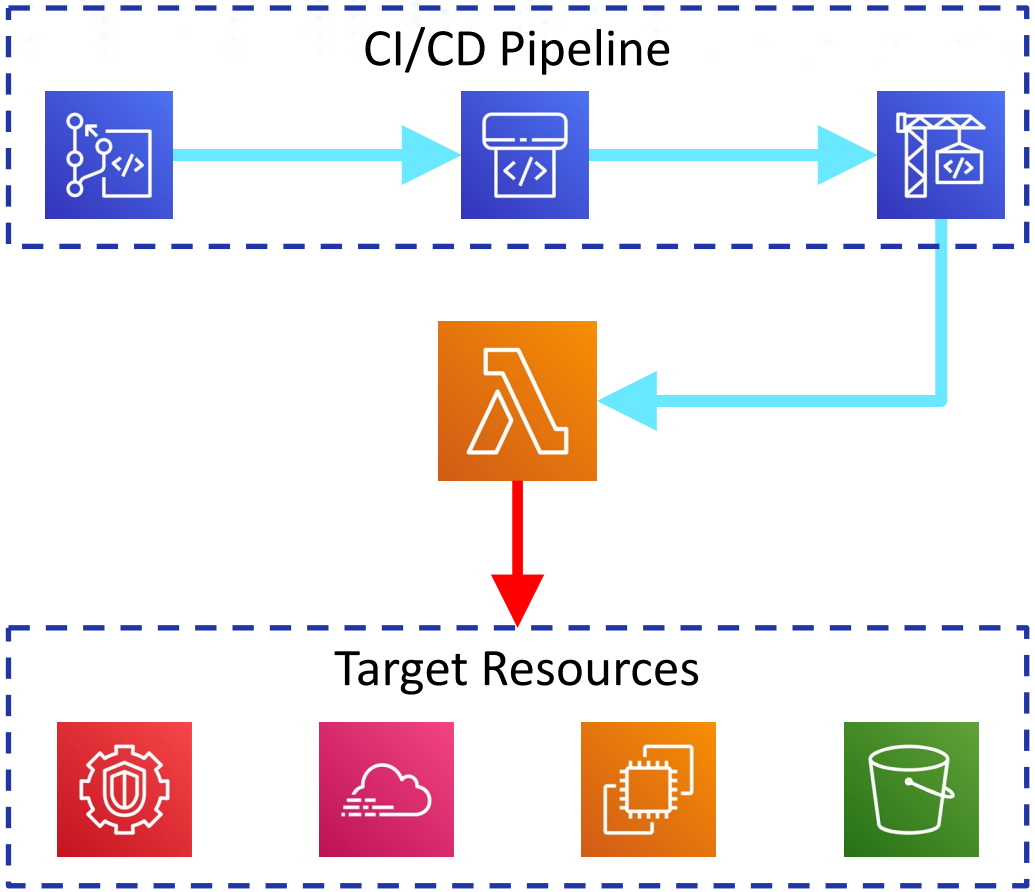
- Next week you should:
  - Identify existing org policies for logging and confirm aggregation.
  - Where possible, ensure quick-wins e.g. Guard Duty are configured.

- 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



- Automate attacker actions in the cloud
- Both test and detection cases
- 55 test cases - more to come
- https://github.com/fsecurelabs/leonidas