Secure the cloud
and
Save the day

Anderson@CYBERSEC2021

Whois

I am Anderson Lin

MaiCoin 幣 Cybersecurity Engineer
AWS Certified All-5 + Sec specialty

4ndersonLin

Agenda

→ Cloud and cloud security

→ Prevent, detect, and respond

→ Summary

Cloud and cloud security

Cloud

$$$ ↓

Speed↑

Cloud security (?)

The good, the bad and the ugly

Good

Chance

- → Compliance ready
- → Availability
- → Anti DDoS
- → Automation & Reviewable infrastructure

Bad

Reality

- → Responsibility
- → Lower visibility
- → Misconfiguration/ Lack of security expertise
- → Lack of access control

Ugly

👻

- → Data breach
- → Vulnerability
- → Compromised credential
- → Old protection/strategy not works here

Prevent

Detect

respond

Prevent

Secure by design

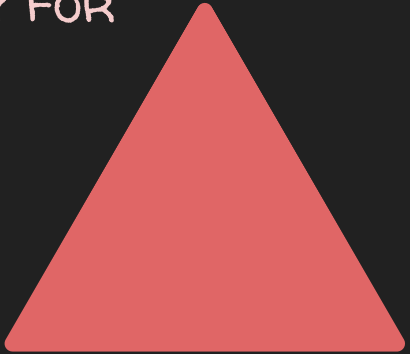
Reduce the surfaces

Vulnerability

Prevent

Secure by design

- Guideline from provider
- New security strategy for PaaS and SaaS



Vulnerability

- Patch: responsibility model
- Patch: automation
- Review resource which has the default setting

Reduce the surfaces

- least privilege access
- Use the strong 2FA

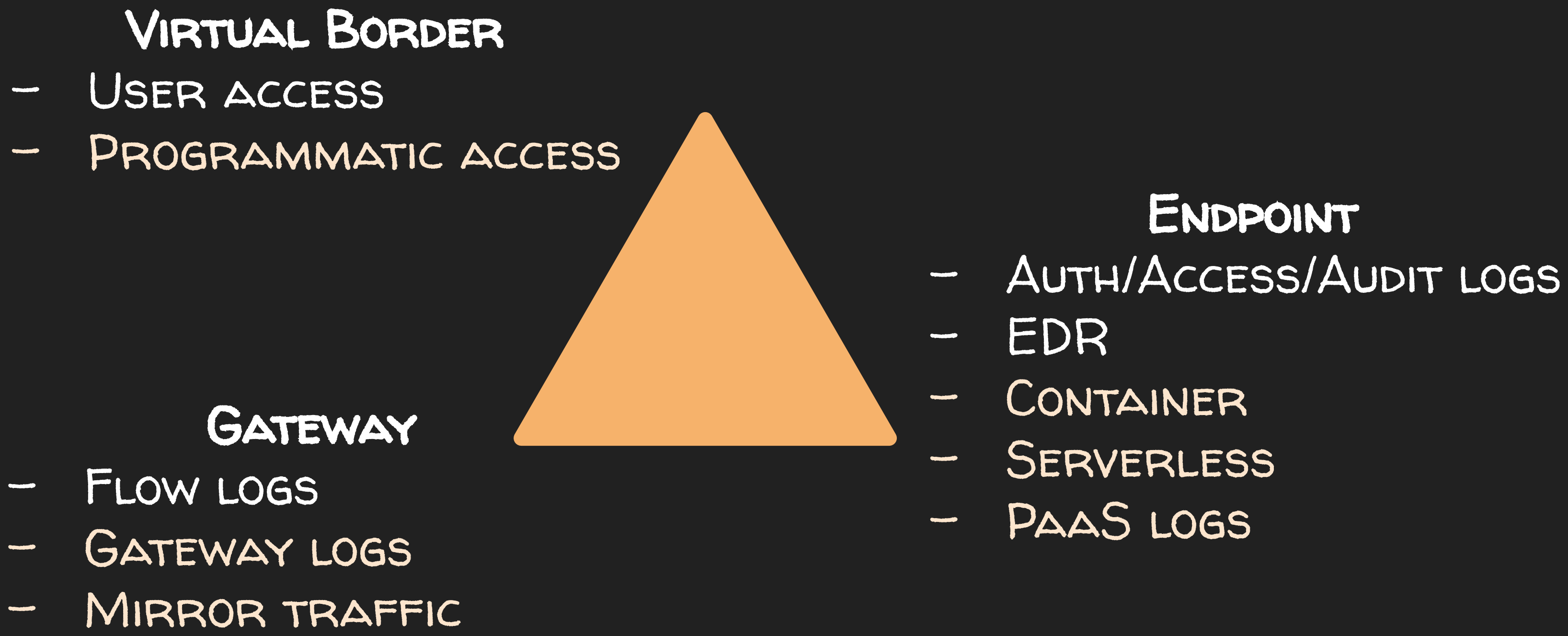
Detect

Virtual Border

Gateway

Endpoint

Detect



Virtual Border

- User access
- Programmatic access

Endpoint

- Auth/Access/Audit logs
- EDR
- Container
- Serverless
- PaaS logs

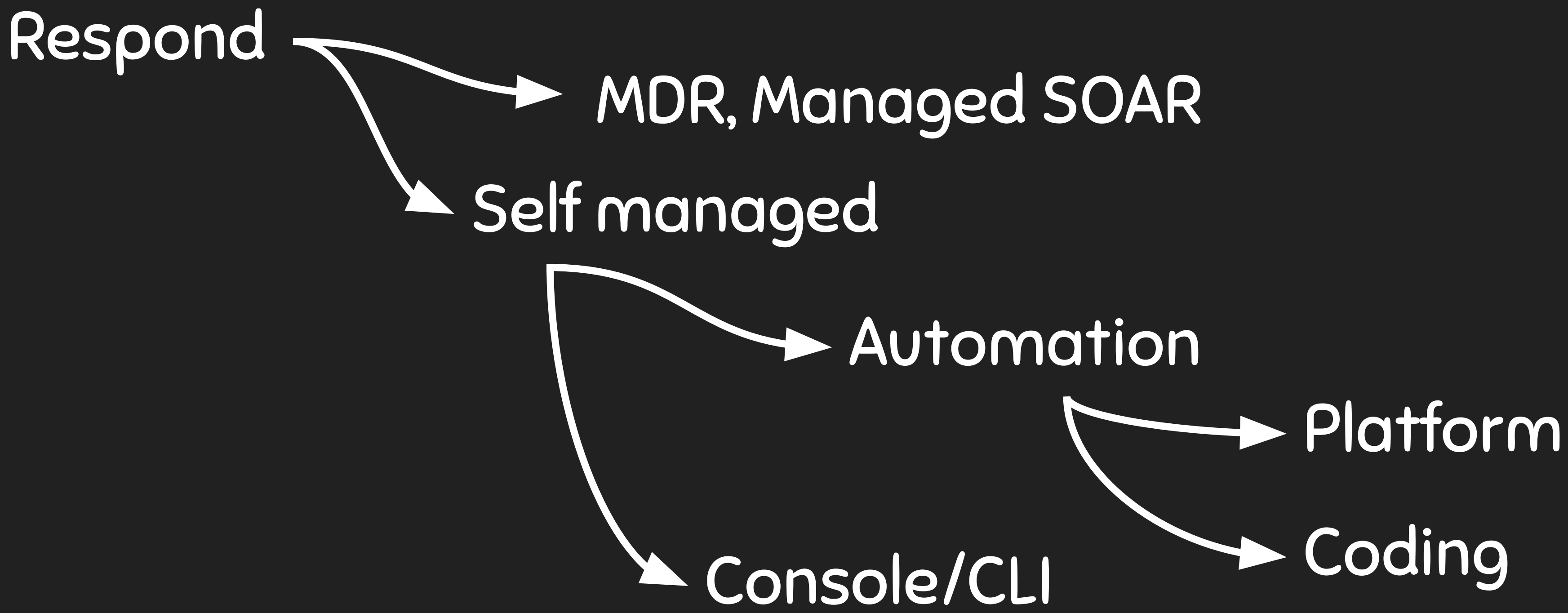
Gateway

- Flow logs
- Gateway logs
- Mirror traffic

Respond

~~Manual~~
Automation

Decision of respond



Respond

MDR, Managed SOAR

Self managed

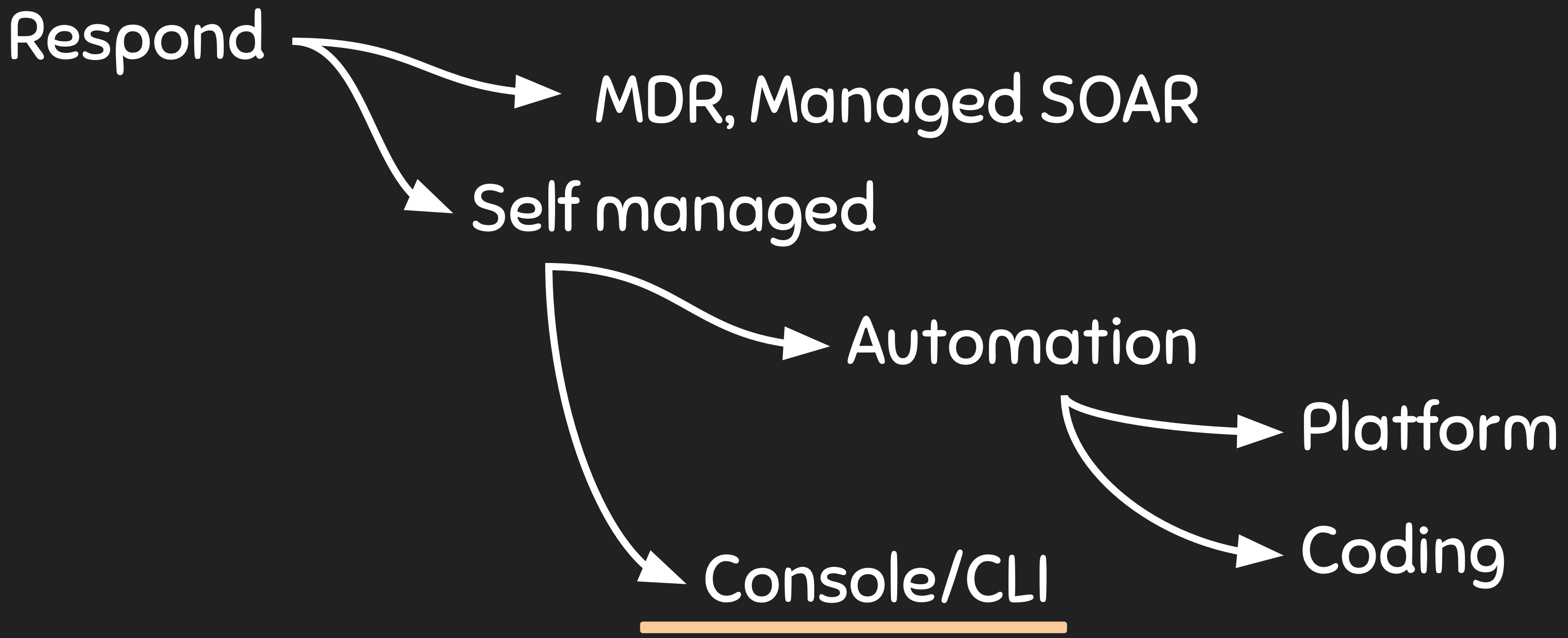
Automation

Platform

Coding

Console/CLI

Decision of respond



Respond

MDR, Managed SOAR

Self managed

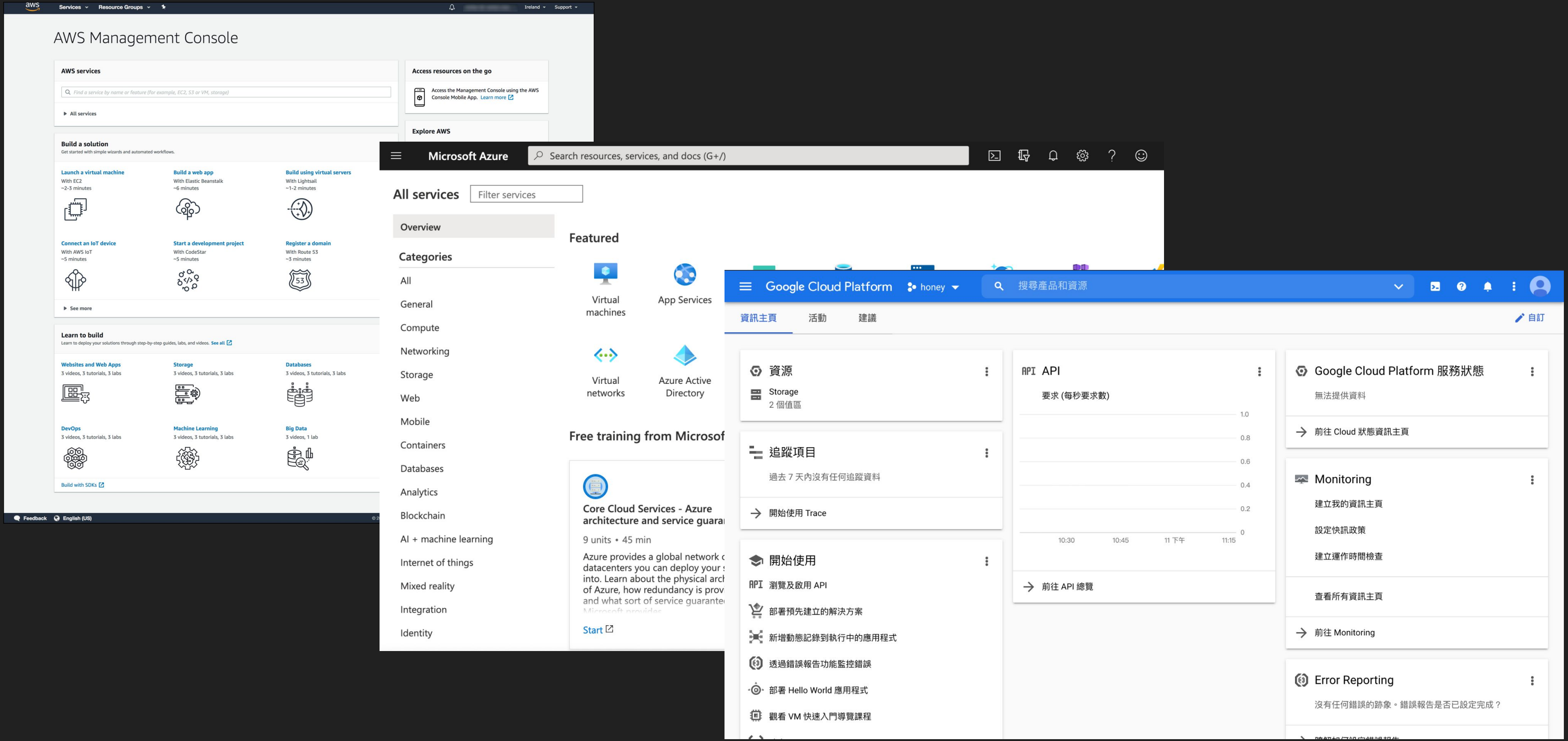
Automation

Platform

Coding

Console/CLI

Go console and click



AWS Management Console

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage)

▶ All services

Access resources on the go

Access the Management Console using the AWS Console Mobile App. Learn more

Explore AWS

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
~2-3 minutes

Build a web app
With Elastic Beanstalk
~6 minutes

Build using virtual servers
With Lightsail
~1-2 minutes

Connect an IoT device
With AWS IoT
~5 minutes

Start a development project
With CodeStar
~5 minutes

Register a domain
With Route 53
~3 minutes

▶ See more

Learn to build

Learn to deploy your solutions through step-by-step guides, labs, and videos. See all

Websites and Web Apps
3 videos, 3 tutorials, 3 labs

Storage
3 videos, 3 tutorials, 3 labs

Databases
3 videos, 3 tutorials, 3 labs

DevOps
3 videos, 3 tutorials, 3 labs

Machine Learning
3 videos, 3 tutorials, 3 labs

Big Data
3 videos, 1 lab

Build with SDKs

All services

Featured

Free training from Microsof

Core Cloud Services - Azure architecture and service guara

9 units • 45 min

Azure provides a global network c datacenters you can deploy your s into. Learn about the physical arch of Azure, how redundancy is prov and what sort of service guarante

Start

資源

Storage
2 個值區

追蹤項目

過去 7 天內沒有任何追蹤資料

→ 開始使用 Trace

開始使用

- 瀏覽及啟用 API
- 部署預先建立的解決方案
- 新增動態記錄到執行中的應用程式
- 透過錯誤報告功能監控錯誤
- 部署 Hello World 應用程式
- 觀看 VM 快速入門導覽課程

API

要求 (每秒要求數)

→ 前往 API 總覽

Google Cloud Platform 服務狀態

無法提供資料

→ 前往 Cloud 狀態資訊主頁

Monitoring

建立我的資訊主頁

設定快訊政策

建立運作時間檢查

查看所有資訊主頁

→ 前往 Monitoring

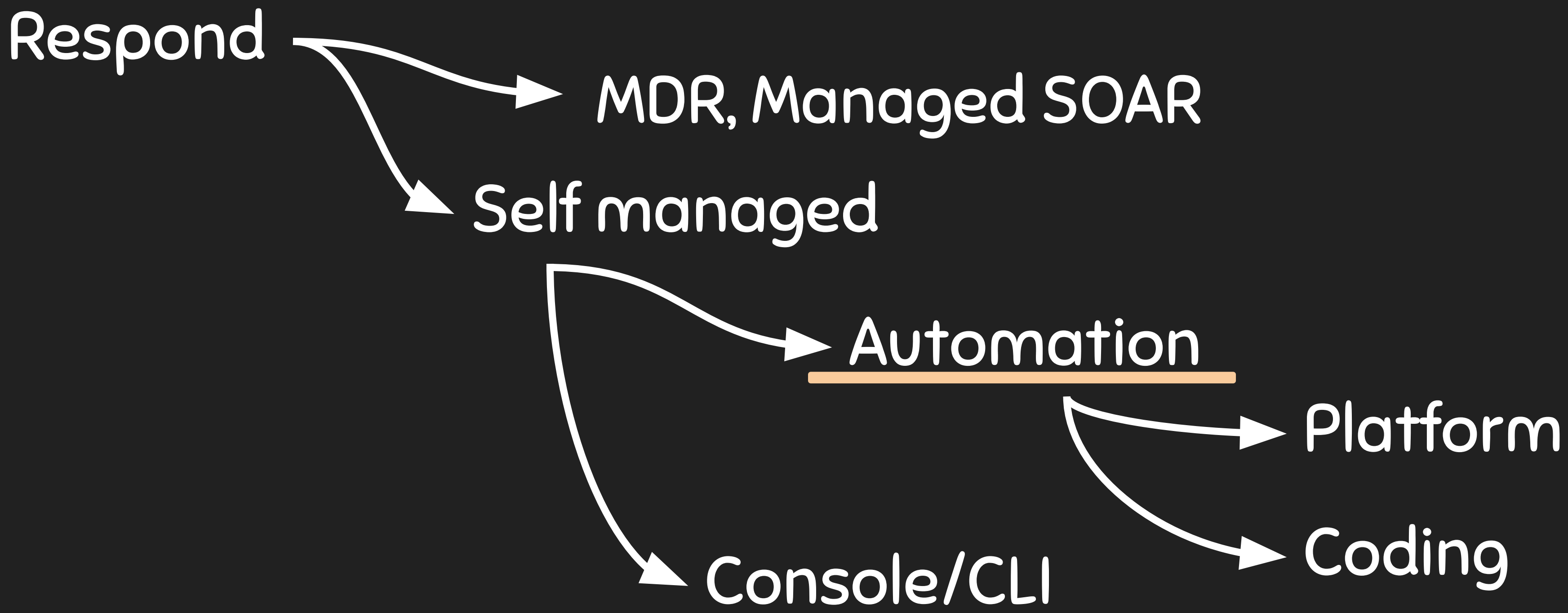
Error Reporting

沒有任何錯誤的跡象。錯誤報告是否已設定完成？

Demo : Google/cloud-forensics-utils

Demo :
ThreatResponse/aws_ir

Decision of respond



Respond

MDR, Managed SOAR

Self managed

Automation

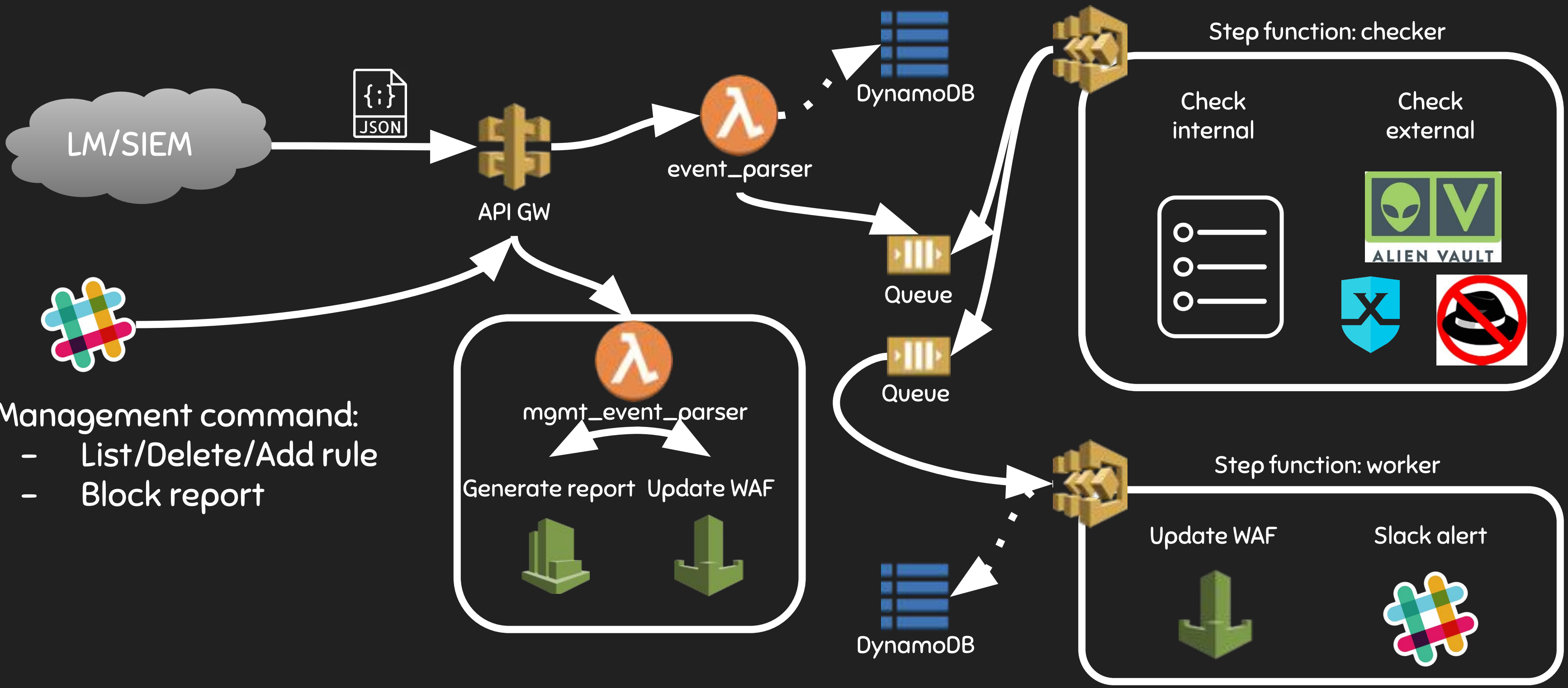
Platform

Coding

Console/CLI

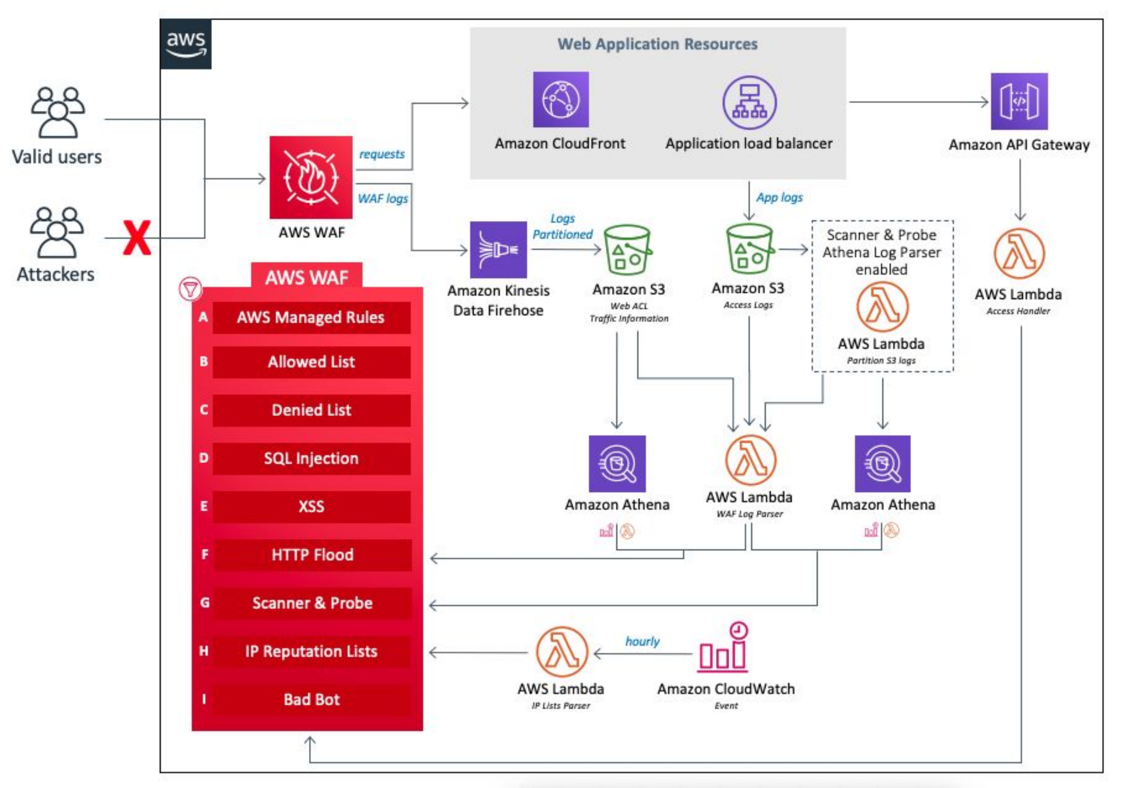
Demo : Tines

Design and coding by your team

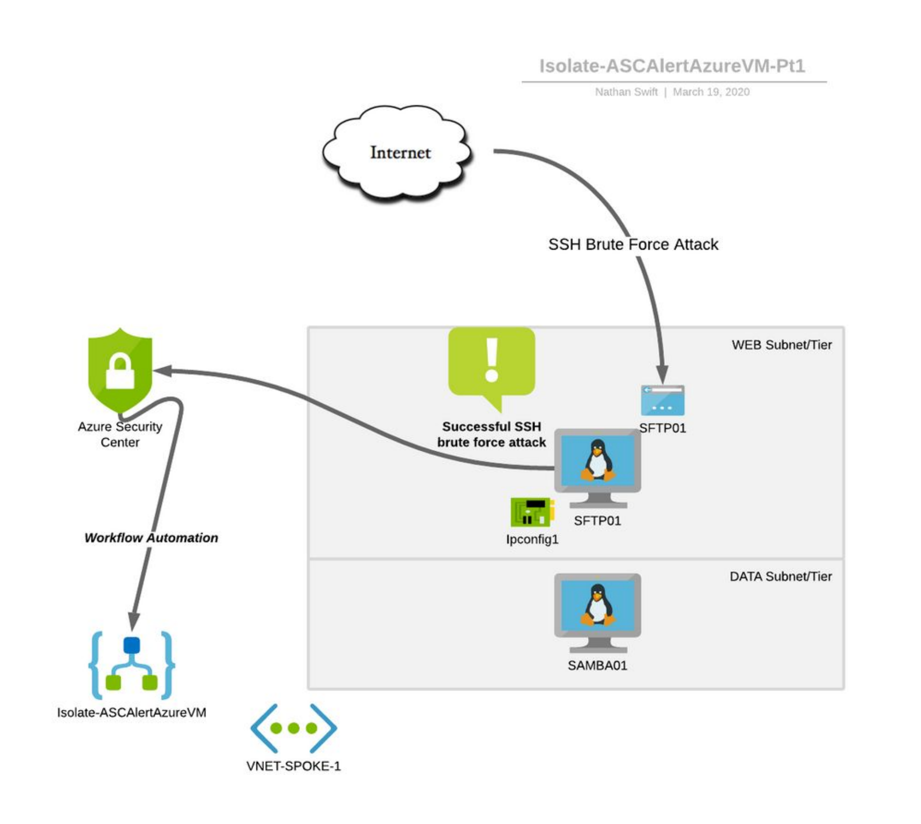


Management command:

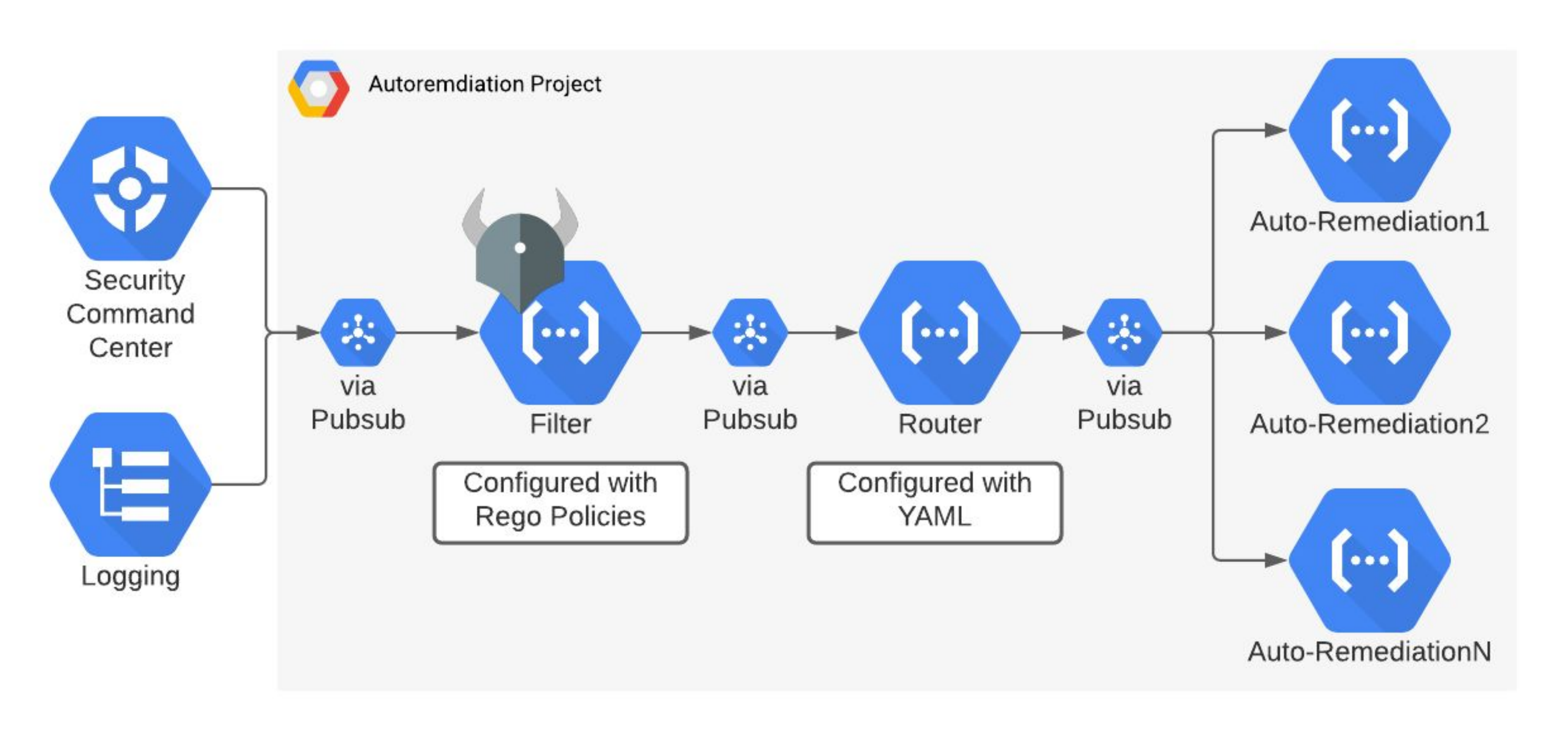
- List/Delete/Add rule
- Block report



Reference:
https://docs.aws.amazon.com/solutions/latest/aws-waf3-security-automations



Reference:https://techcommunity.microsoft.com/t5/azure-security-center/how-to-isolate-an-azure-vm-using-azure-security-center-s/ba-p/1250985

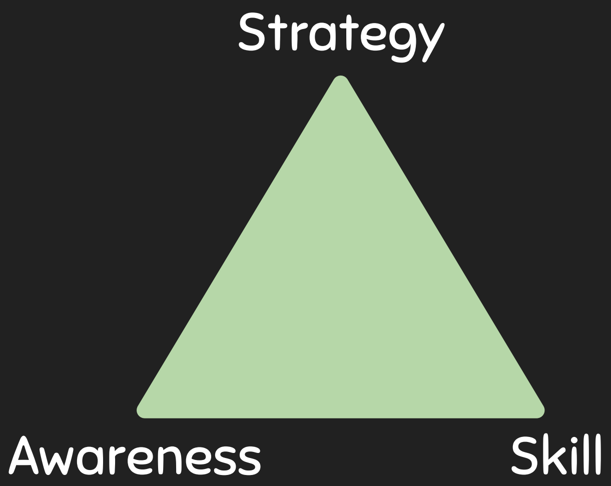


Reference:
https://github.com/GoogleCloudPlatform/security-response-automation

Summary

Summary

Always up to date



Strategy

Awareness

Skill

Embrace automation

Take away

Tools

- Tines.io
- https://docs.aws.amazon.com/solutions/latest/aws-waf3-security-automations
- https://techcommunity.microsoft.com/t5/azure-security-center/how-to-isolate-an-azure-vm-using-azure-security-center-s/ba-p/1250985
- https://github.com/GoogleCloudPlatform/security-response-automation
- https://github.com/google/cloud-forensics-utils
- https://github.com/ThreatResponse/aws_ir

Collection

- https://github.com/4ndersonLin/awesome-cloud-security

We Are Hiring

AMIS

https://github.com/MaiAmis/Careers

Thanks!

Mailto: 4nderson.lin@pm.me