aws INNOVATE2018 ONLINE CONFERENCE

Self-Defending Borders: A Developer's Approach to Security (Level 300)

Shane Baldacchino, Solution Architect

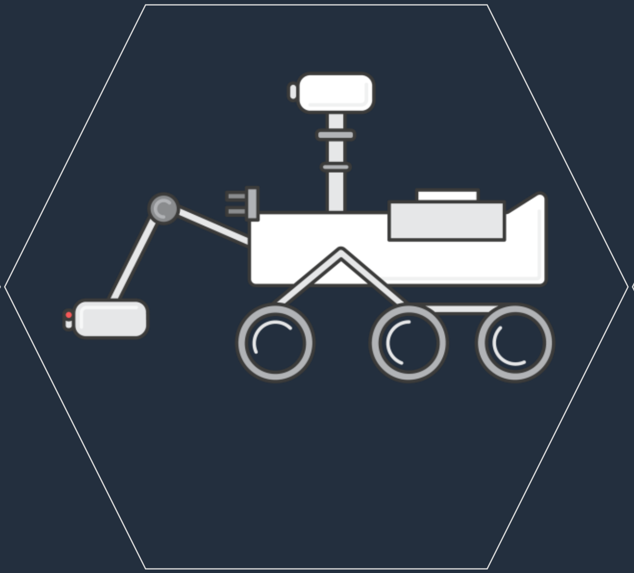
What To Expect From This Session

Together, we will:

- Dive right in!
- Explore a use case of edge transformation using AWS Development Services in conjunction with AWS secuirty services.
- Walk through a demo of how a self defending AWS architecture will increase your security posture.
- Take a deep dive into the architecture behind the demonstration.

Modern Business Challenges

Increased Frequency



Low Capital Investment

Rules and Regulations

Disparate

Non Connected System

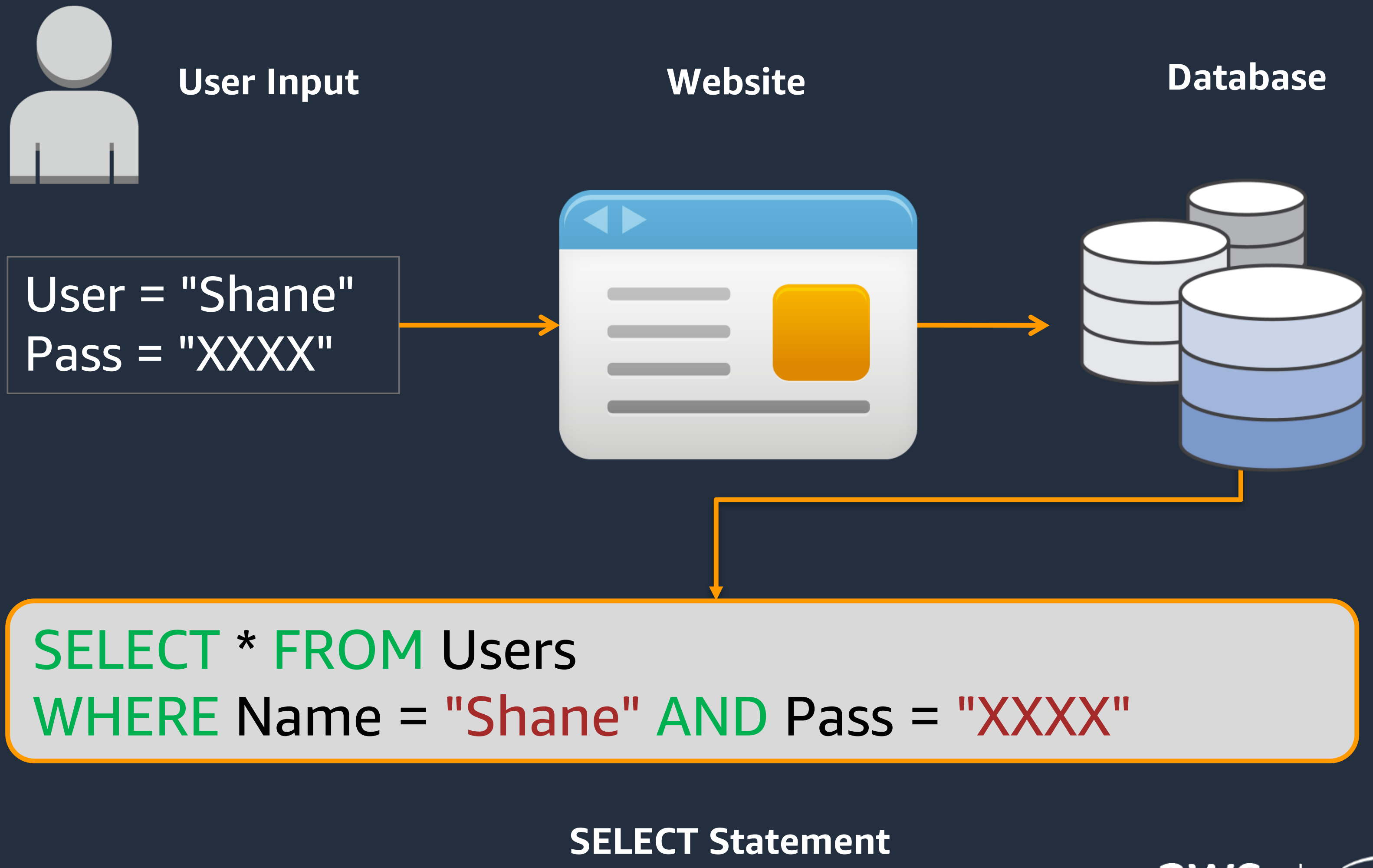
Threats facing online assets?

Threats facing online assets?
There Are Many

OWASP Style Attacks

Critical Web Application Security Risks

OWASP Injection



User Input

Website

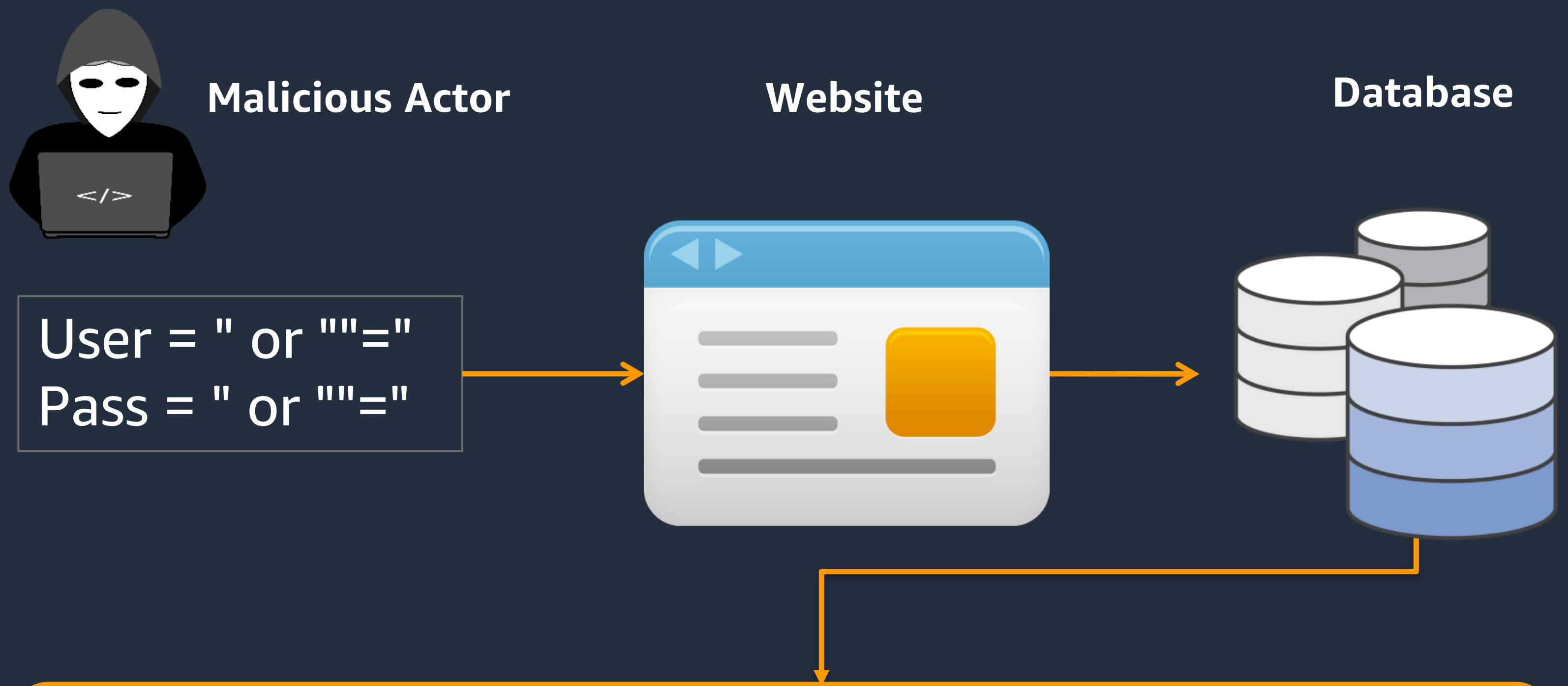
Database

```
User = "Shane"
Pass = "XXXX"
```

```
SELECT * FROM Users
WHERE Name = "Shane" AND Pass = "XXXX"
```

SELECT Statement

OWASP Injection



User = " or ""="
Pass = " or ""="

```
SELECT * FROM Users
WHERE Name ="" or ""="" AND Pass ="" or ""=""
```

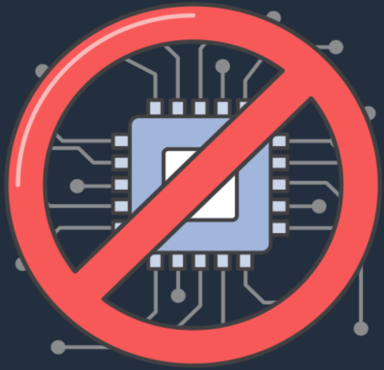
SELECT Statement

How are we fighting these threats today?

How are we fighting these threats today?
We Use Controls

Expensive

CAPEX Heavy
Over Provisioning
License Locked



Lack Automation

Integration Challenges
With DevSecOps
Models

False Positives

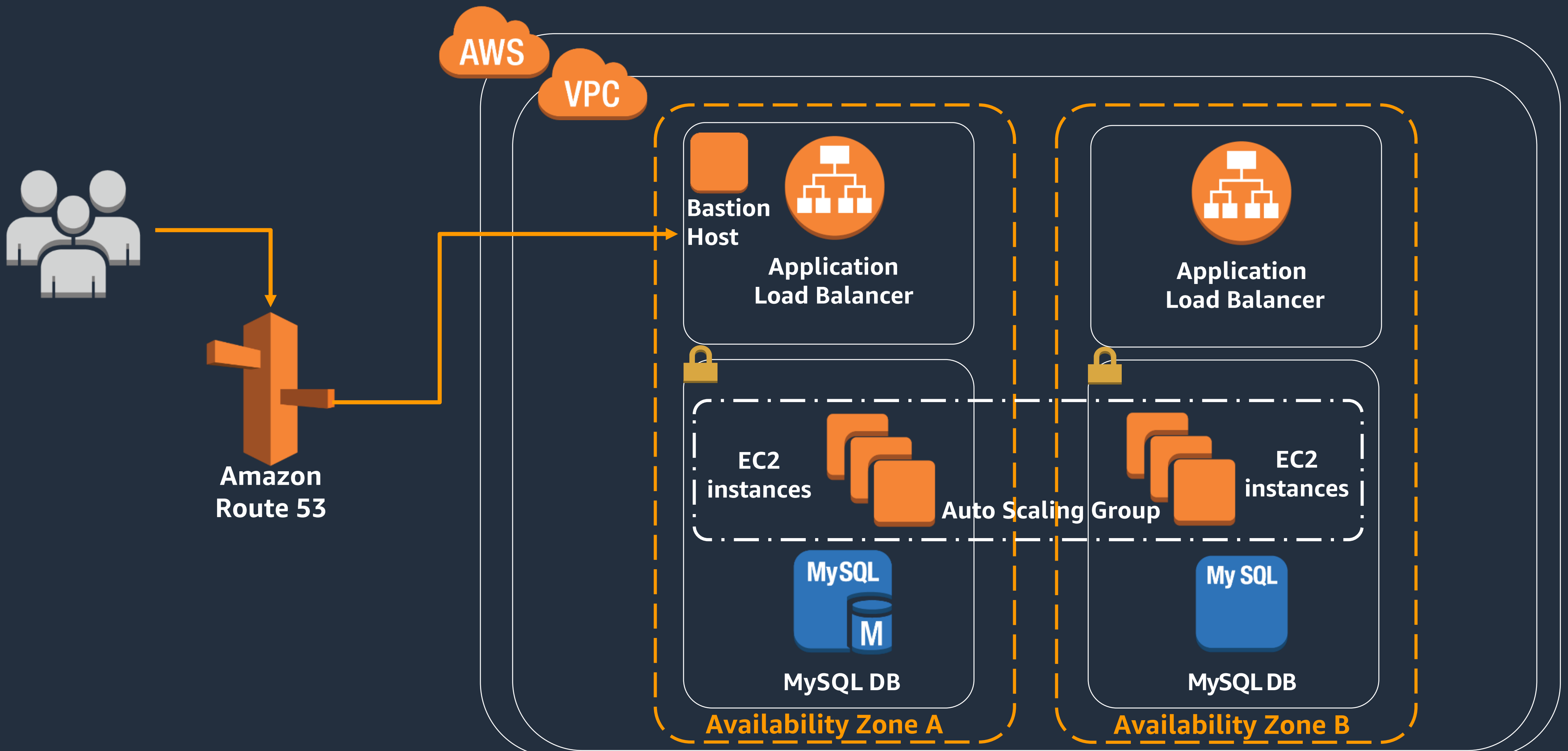
Content Changes
Often Require New
Rules

Let’s make this real.

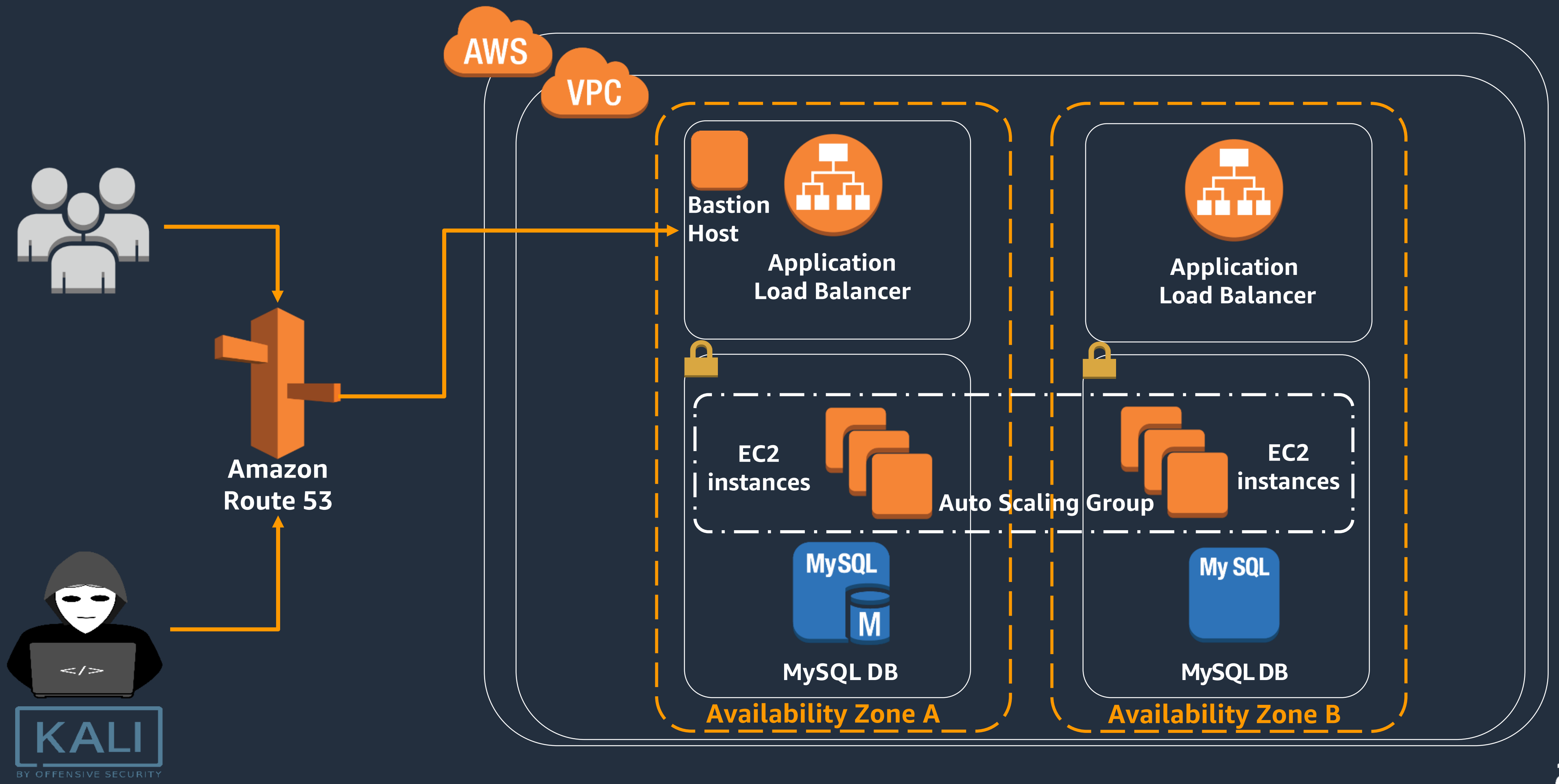
The Snowy Unicorn Elevator Company

- N-Tier Architecture
- ERP and CRM Integration
- Quickly Growing
- Limited IT resources

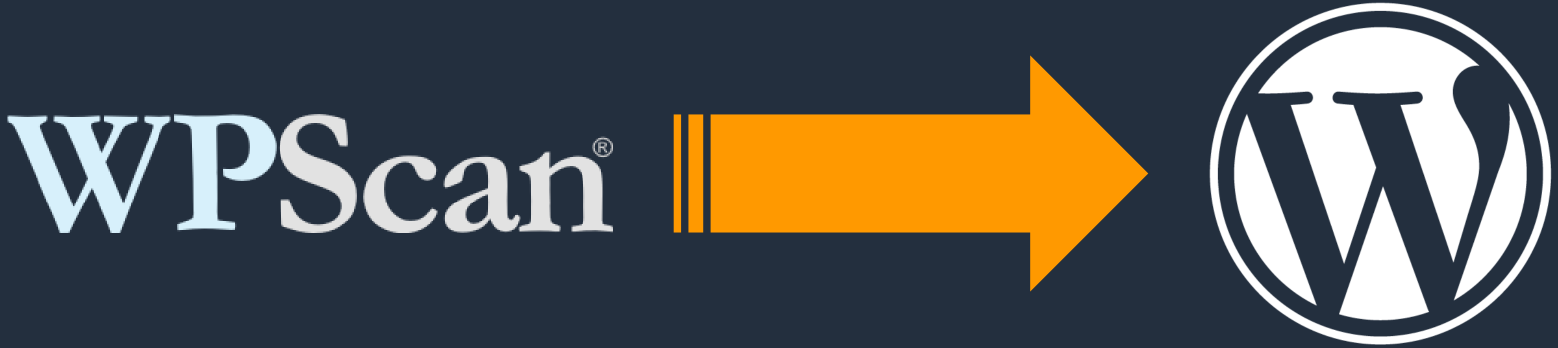
Online Architecture



Online Architecture

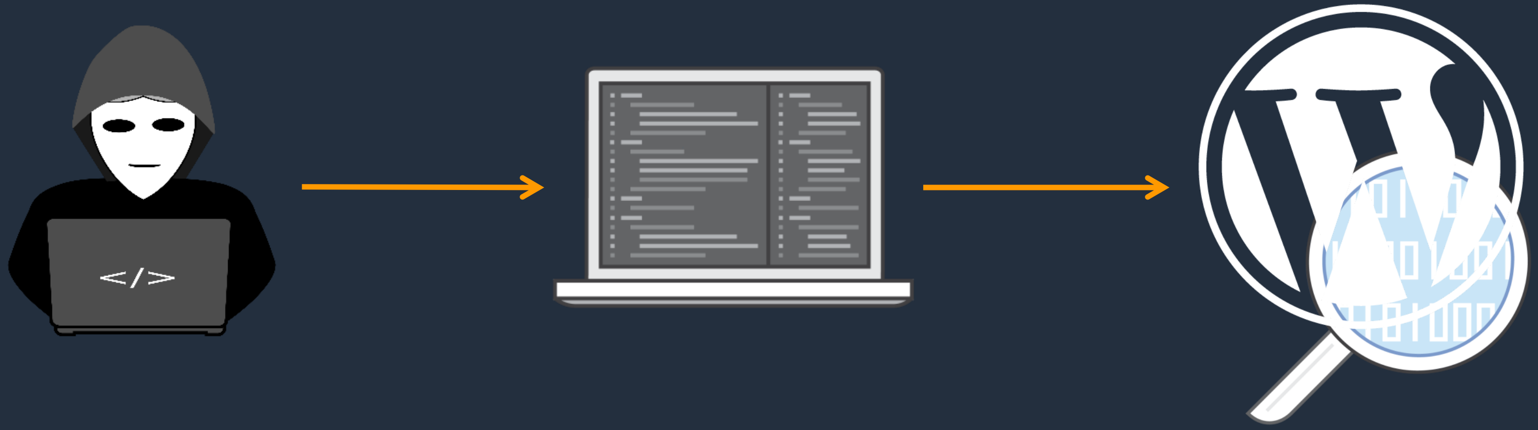


Kali Linux

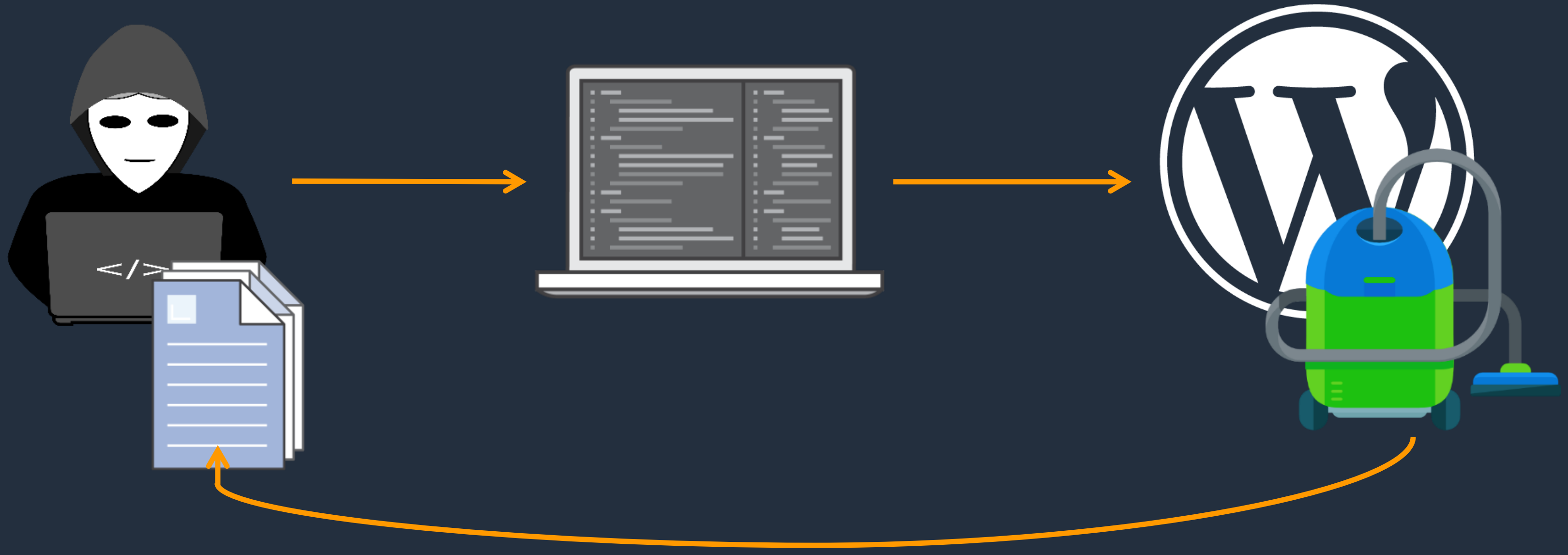


- Designed For **Penetration** Testing and Security **Auditing**
- Contains **Several Hundred** Tools
- Available in **AWS Marketplace**

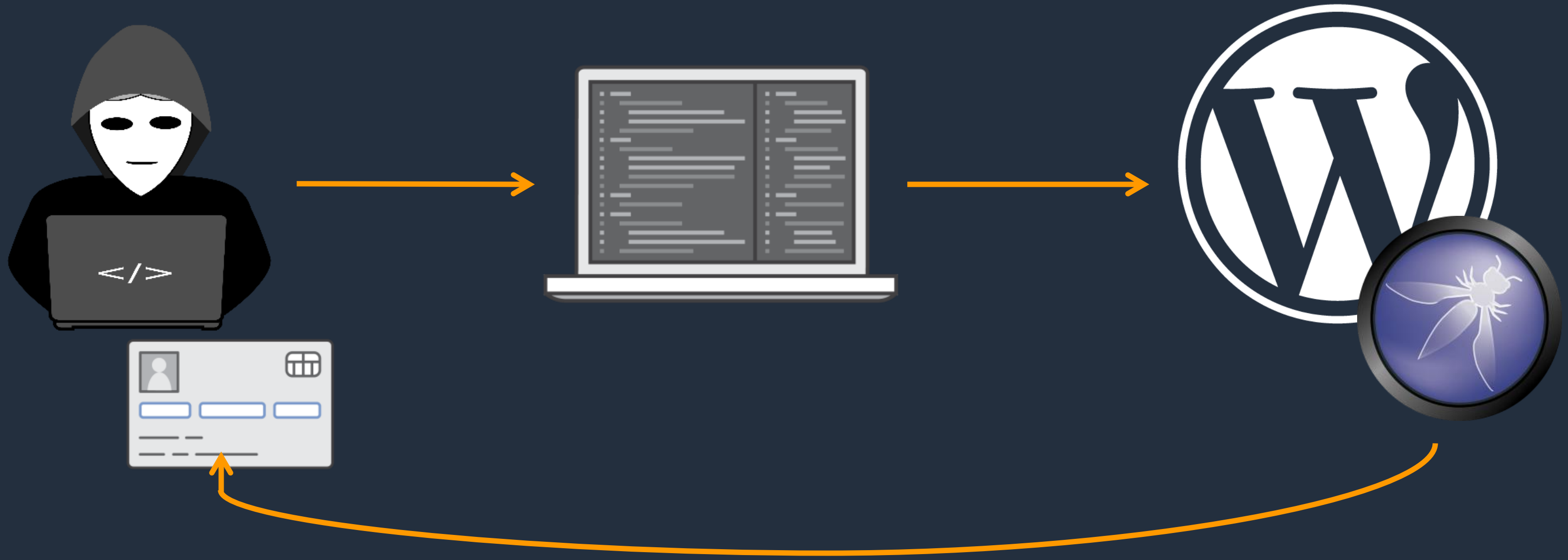
Architecture Of Attacks - Discovery



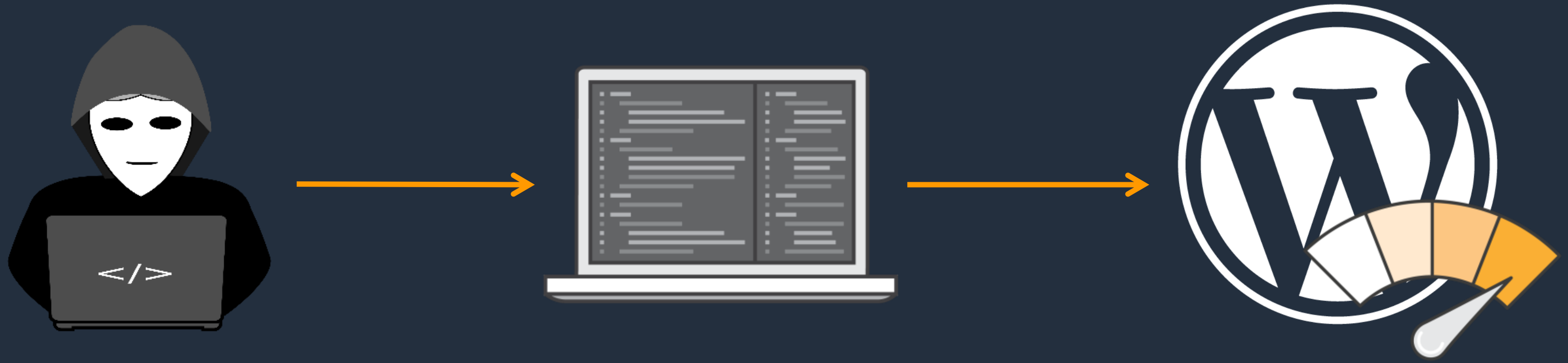
Architecture Of Attacks - Crawl



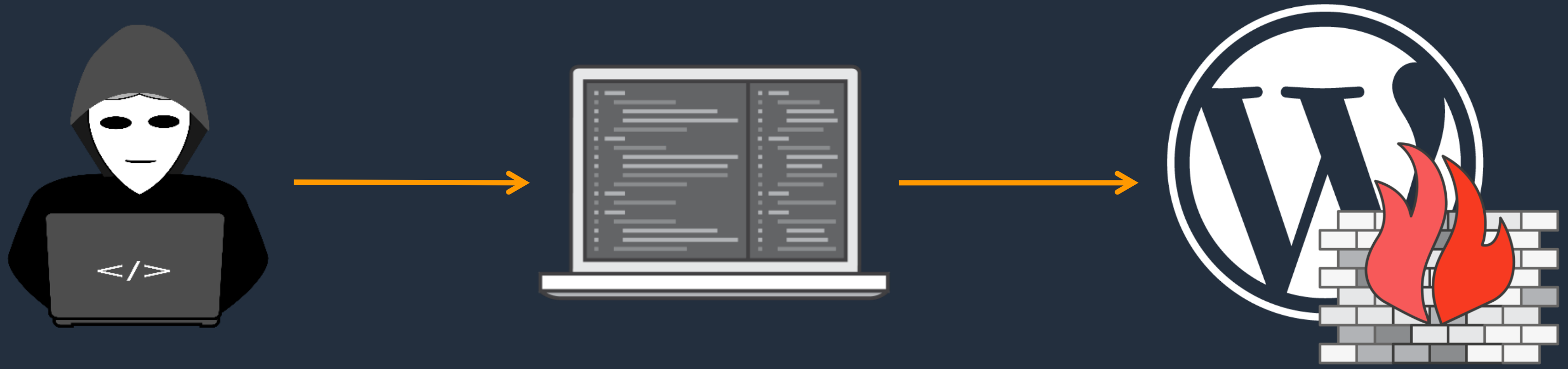
Architecture Of Attacks - OWASP



Architecture Of Attacks - DOS



Architecture Of Attacks - Brute Force



Demo

The Snowy Unicorn Elevator Company

What’s Wrong With Our Architecture?

L7 Attacks

Traditional security control were ineffective

Scale, Cost & Reputation

ASG Elasticity

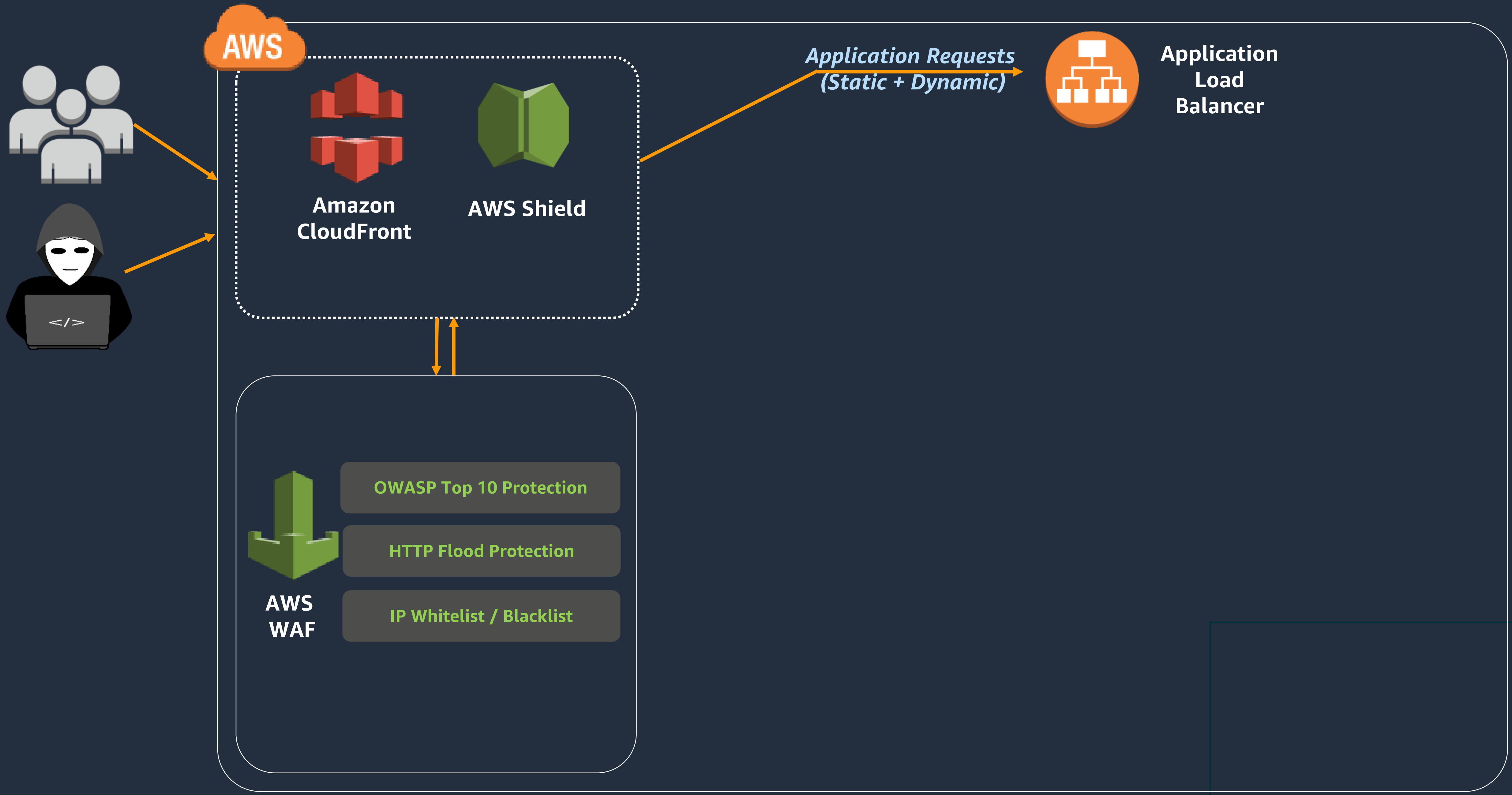
Network Bandwidth

Visibility

Flew under the radar

Self Defending Borders

Putting the ‘Dev’ in Security (DevSecOps)



AWS

Amazon CloudFront

AWS Shield

Application Requests (Static + Dynamic)

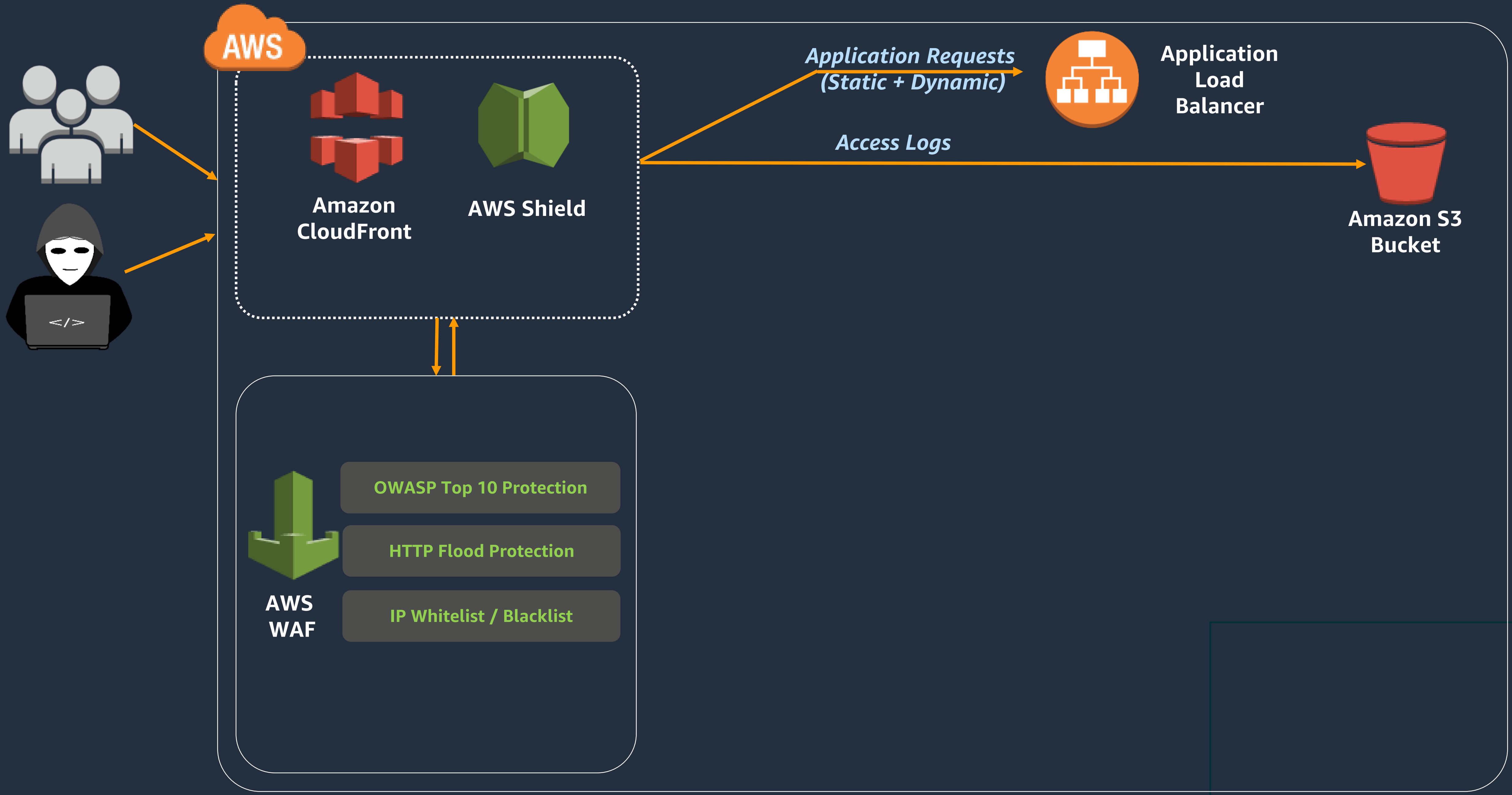
Application Load Balancer

AWS WAF

OWASP Top 10 Protection

HTTP Flood Protection

IP Whitelist / Blacklist



AWS

Amazon CloudFront

AWS Shield

Application Requests (Static + Dynamic)

Application Load Balancer

Access Logs

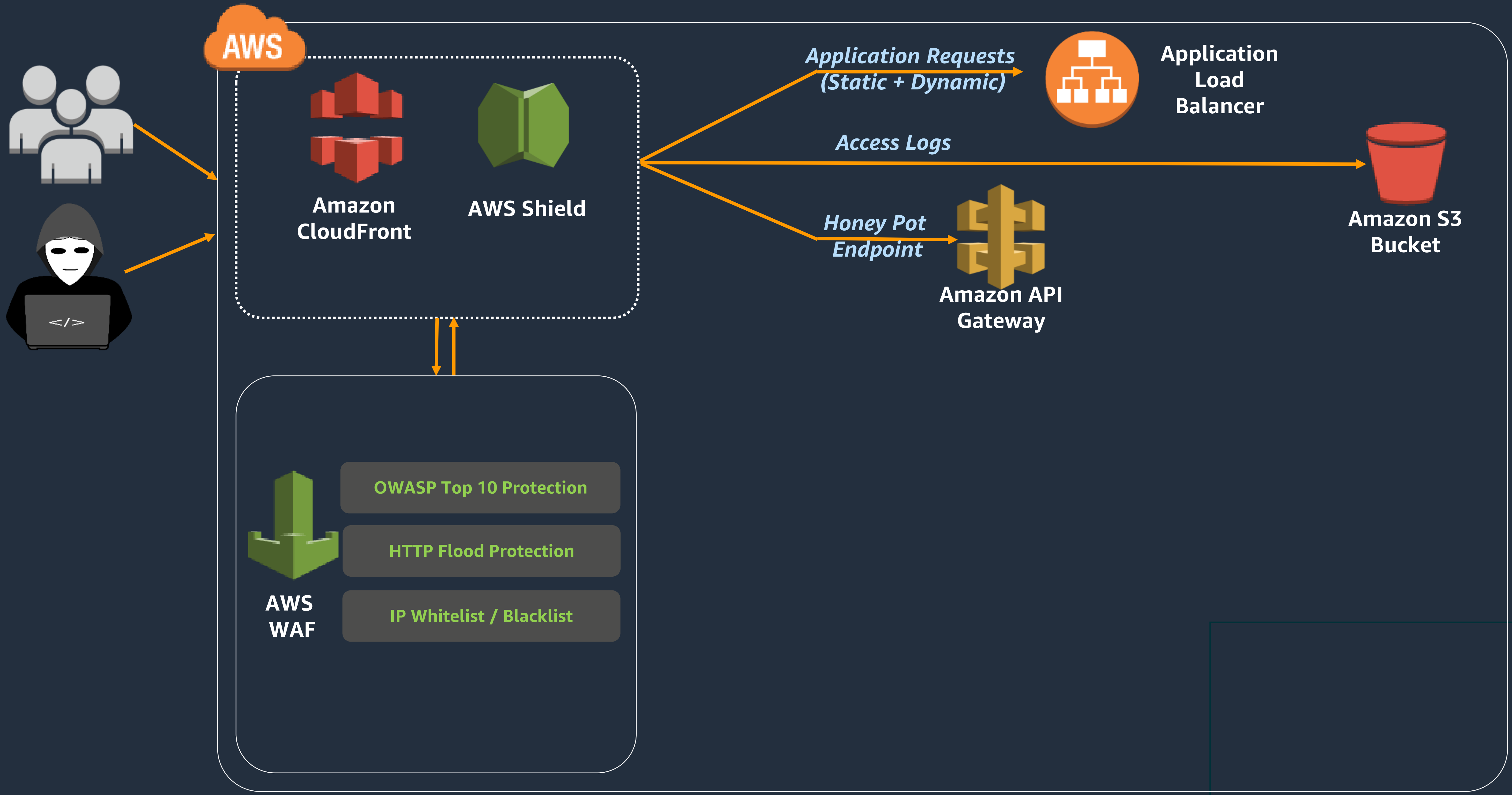
Amazon S3 Bucket

AWS WAF

OWASP Top 10 Protection

HTTP Flood Protection

IP Whitelist / Blacklist


AWS
Amazon CloudFront
AWS Shield
Application Requests (Static + Dynamic)
Application Load Balancer
Access Logs
Amazon S3 Bucket
Honey Pot Endpoint
Amazon API Gateway
&lt;/&gt;
AWS WAF
OWASP Top 10 Protection
HTTP Flood Protection
IP Whitelist / Blacklist

Demo

The Snowy Unicorn Elevator Company

AWS WAF

AWS Shield

Tightknit API Driven Platform

Amazon SQS

Fully managed message queue

Amazon CloudWatch

Monitoring for cloud resources

AWS Step Functions

Build distributed applications

Amazon SNS

Highly scalable push messaging

Amazon DynamoDB

NoSQL data store

Amazon ElasticSearch

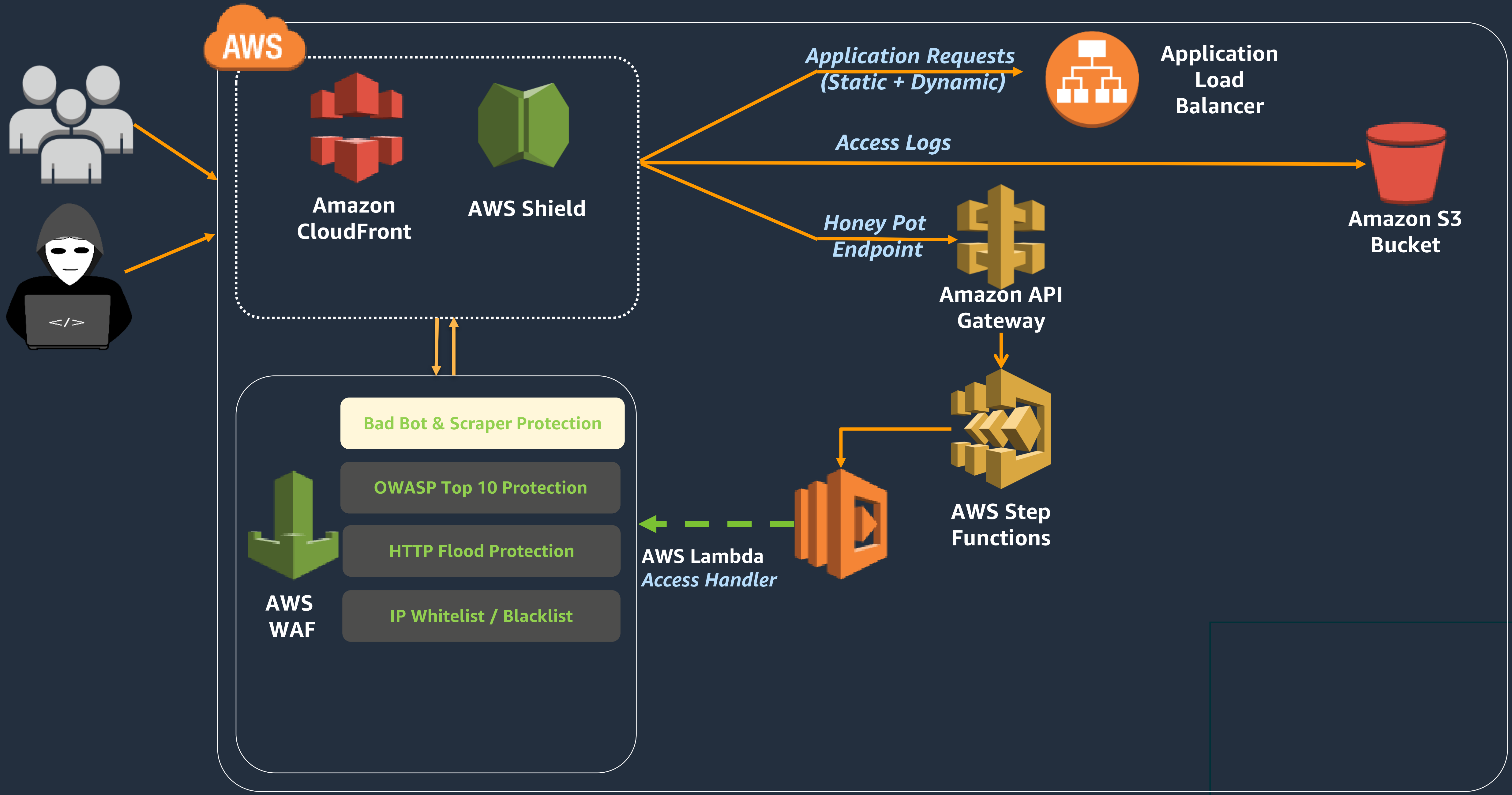
Scalable ElasticSearch

Amazon S3

Simple, durable object store

AWS Lambda

Run code without servers


AWS
Amazon CloudFront
AWS Shield
Application Requests (Static + Dynamic)
Application Load Balancer
Access Logs
Amazon S3 Bucket
Honey Pot Endpoint
Amazon API Gateway
AWS Step Functions
AWS Lambda
Access Handler
Bad Bot & Scraper Protection
OWASP Top 10 Protection
HTTP Flood Protection
IP Whitelist / Blacklist
AWS WAF
</>

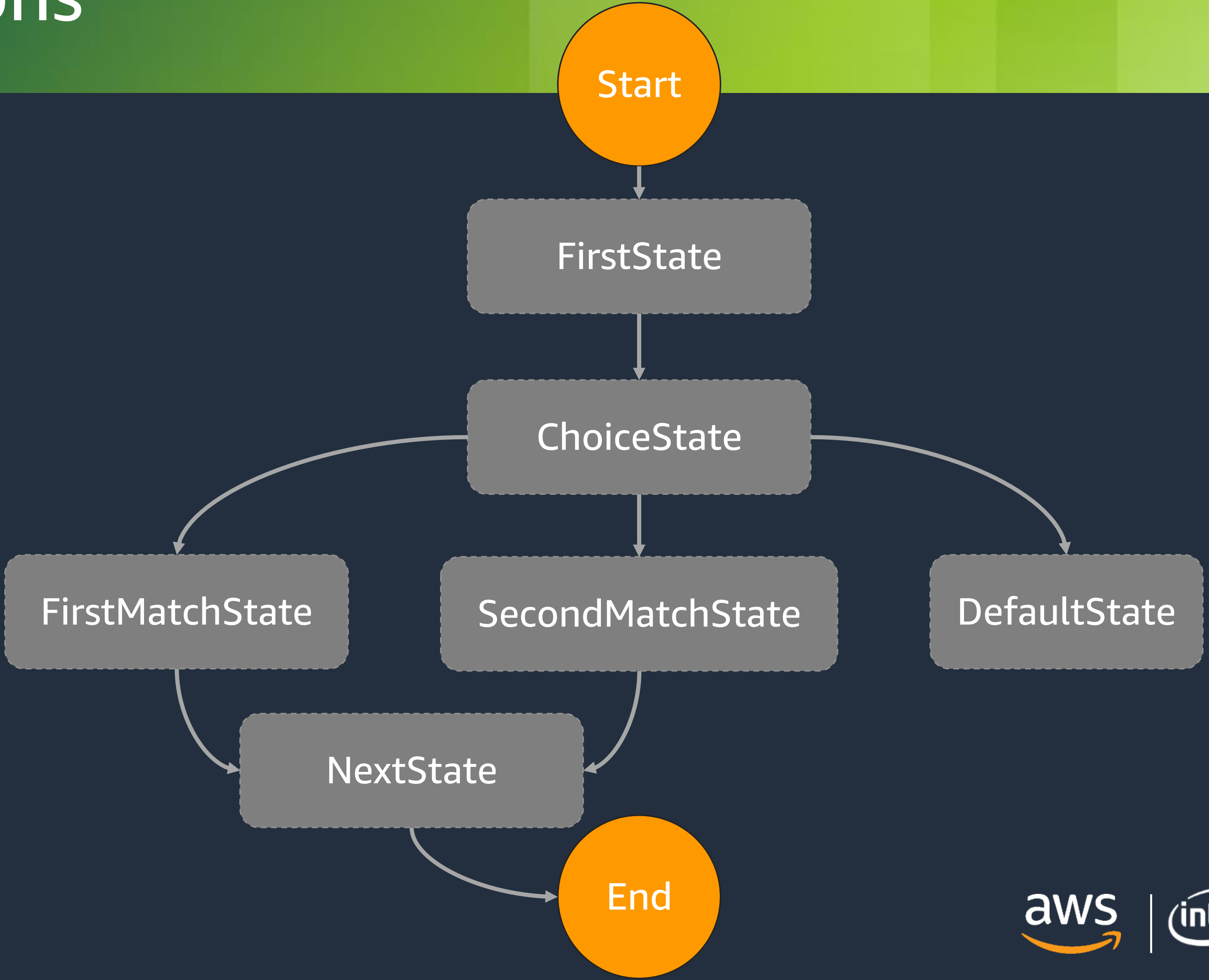
AWS Lambda

Build and run applications without thinking about servers

Availability and scalability is managed by AWS

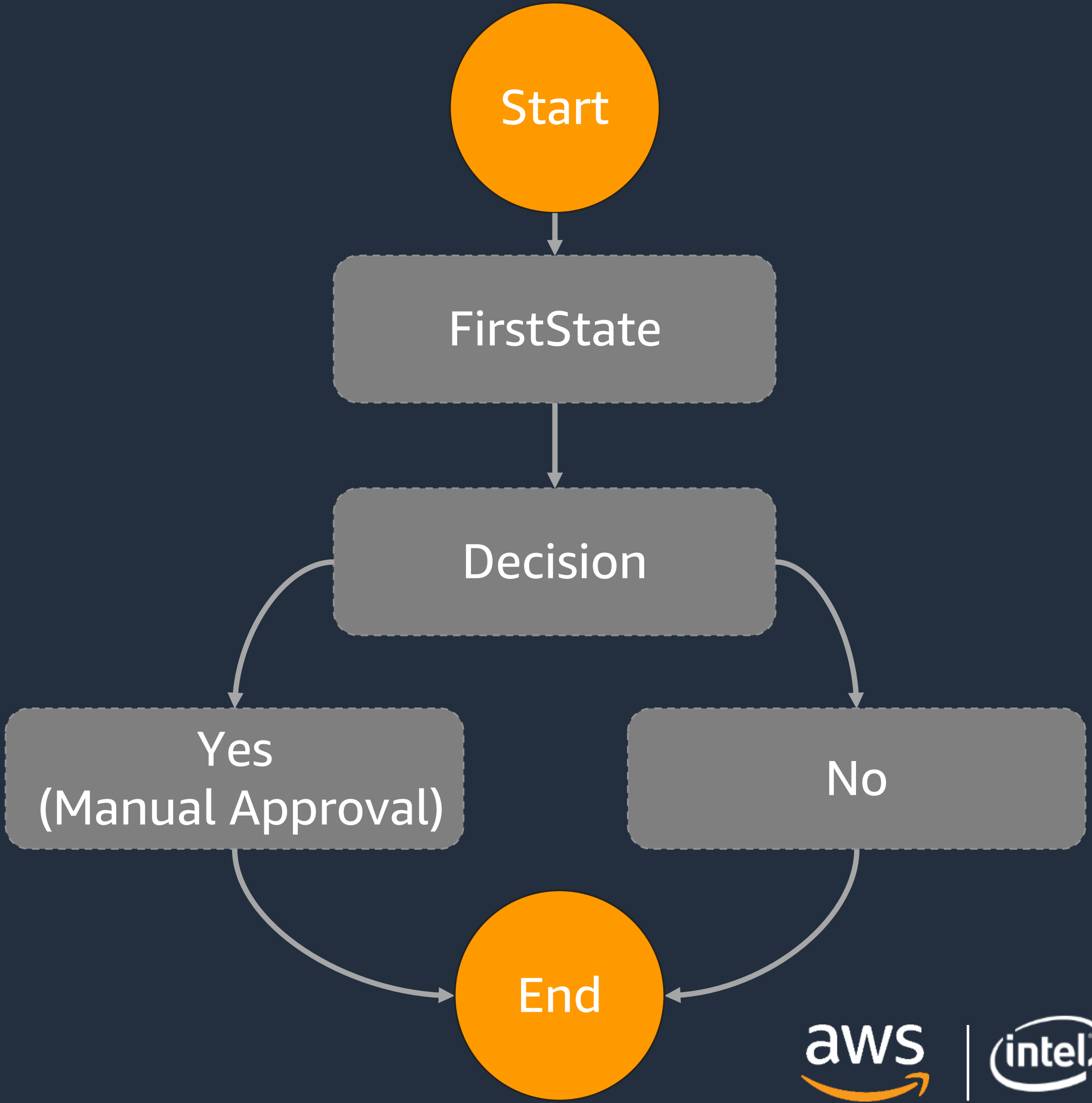
Not paying for idle time

AWS Step Functions

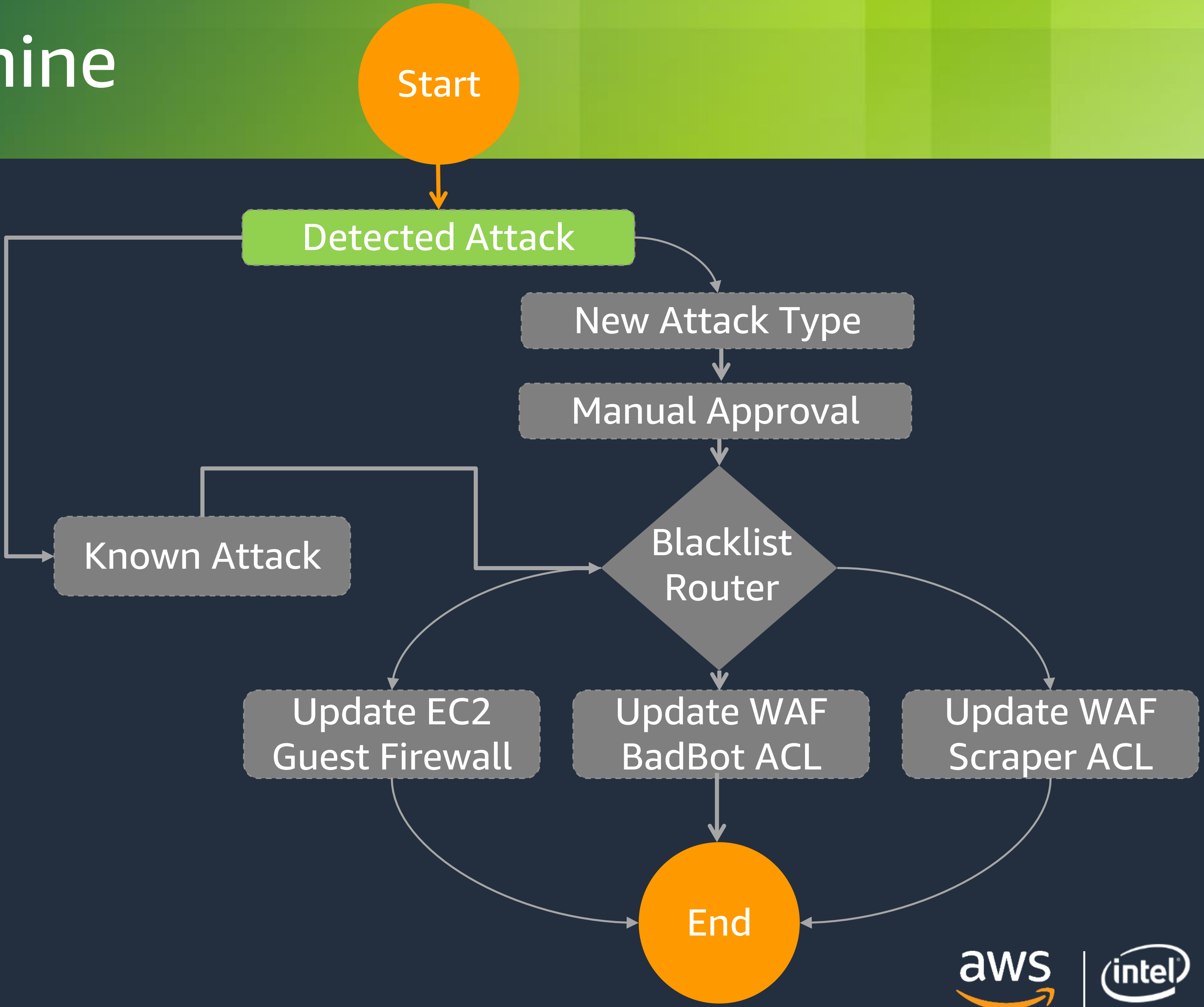


Define in JSON, Visualise In The Console

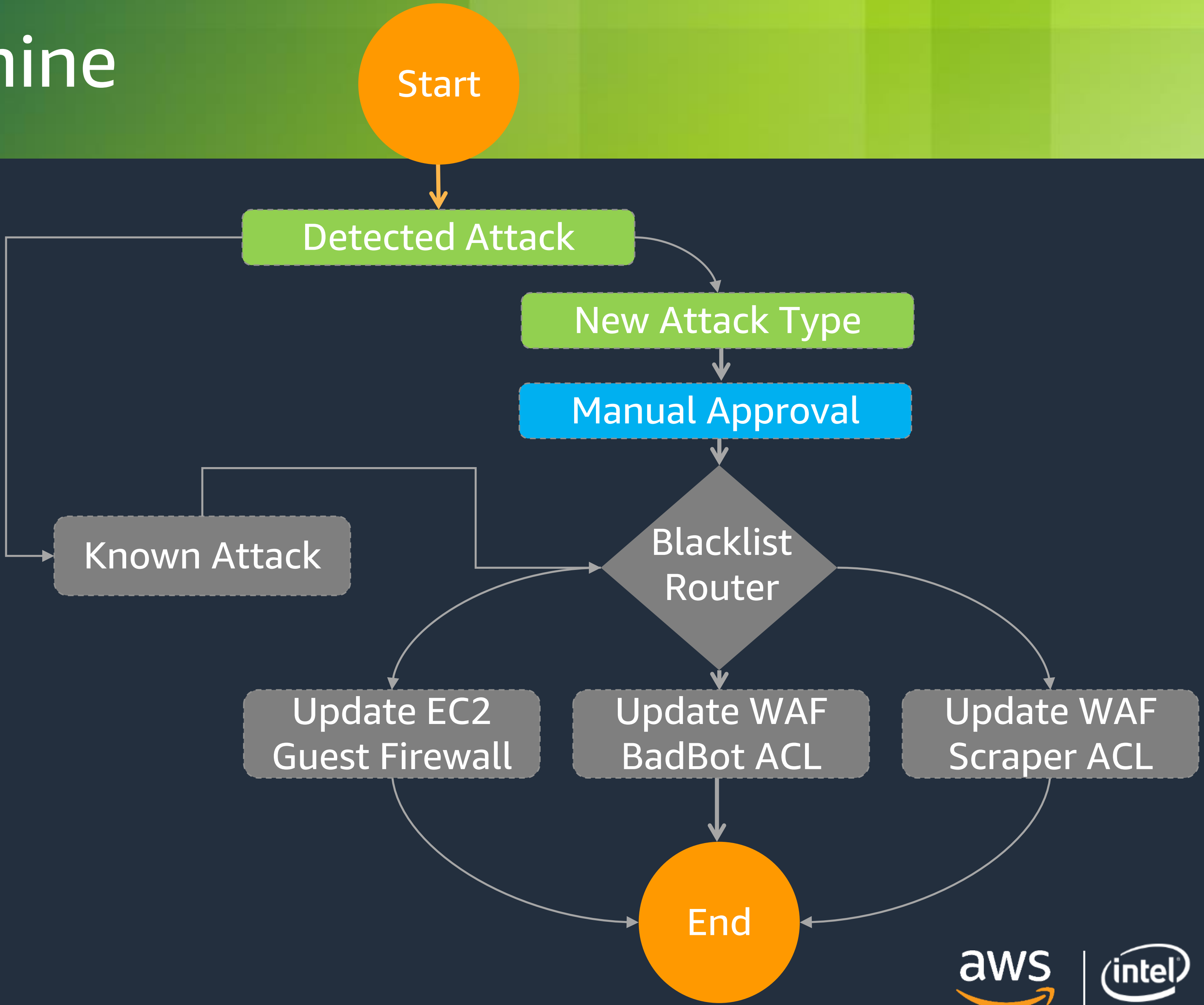
```
{
"StartAt": "FirstState",
"States":
 {
          "ManualApproval": {
          "Type": "Task",
          "Resource": "arn:aws:states:aws-region:xxxxxxxxxxx:activity:ManualStep",
          "Next": ”Log_Ticket_InfoSec"
          },
          ”Decision": {
          "Type" : "Choice",
          "Choices": [
          {
                   "Variable": "$.user_agent",
                   "NumericEquals": 1,
                   "Next": "Yes"
                   },
                   {
                   "Variable": "$.user_agent",
                   "NumericEquals": 0,
                   "Next": "No"
                   }
          ]
},
”Update_AWS_WAF": {
"Type": ”Task",
"Resource": "arn:aws:states:aws-region:xxxxxxxxxxx:activity:UpdateWAF"
"End": true
}
```



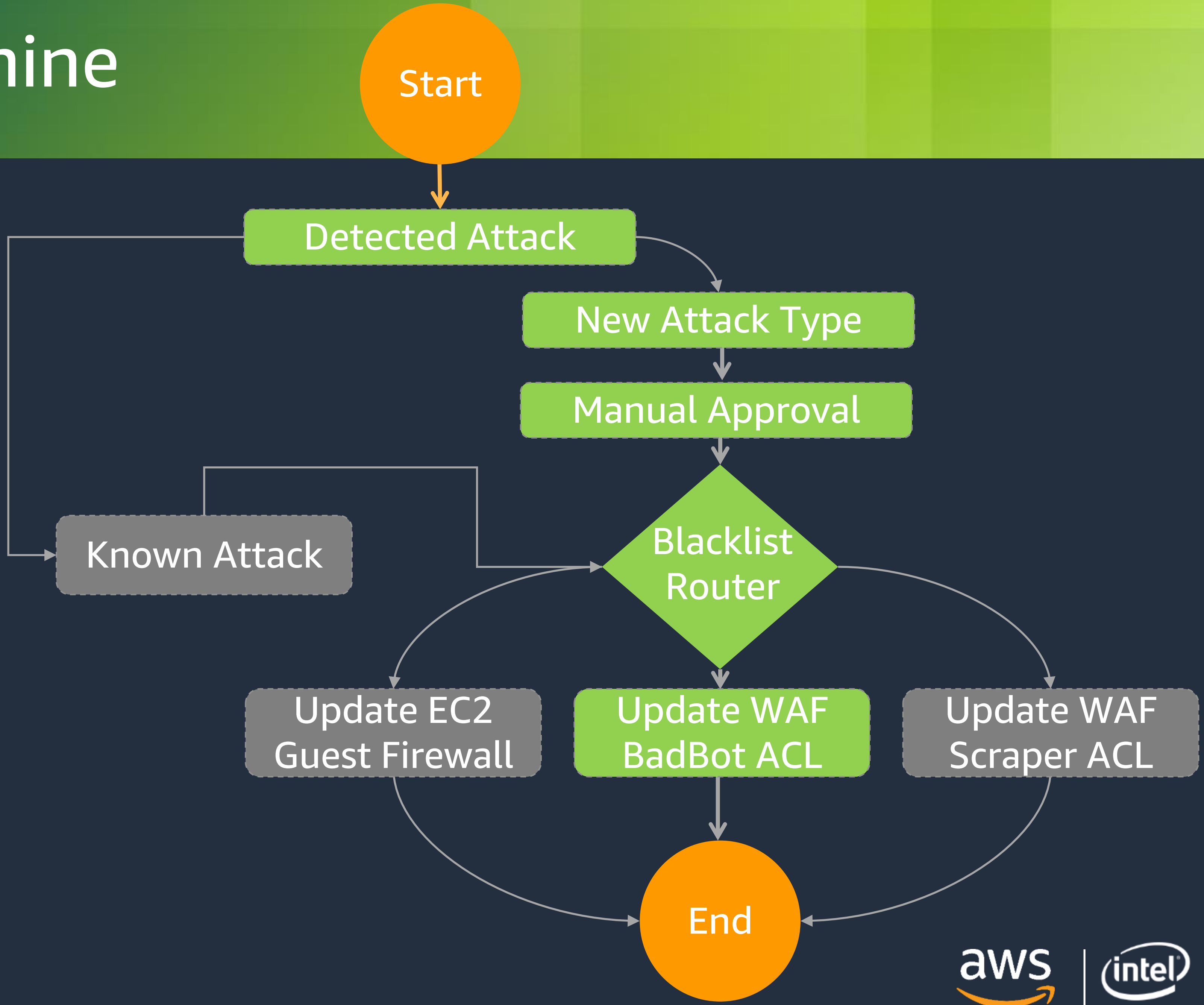
Security State Machine



Security State Machine



Security State Machine



Start

Detected Attack

New Attack Type

Manual Approval

Known Attack

Blacklist Router

Update EC2 Guest Firewall

Update WAF BadBot ACL

Update WAF Scraper ACL

End

Amazon SNS

Message Delivery Over Multiple Transports

Simple API Integration

Proven Reliability Multi AZ Architecture

Demo

The Snowy Unicorn Elevator Company

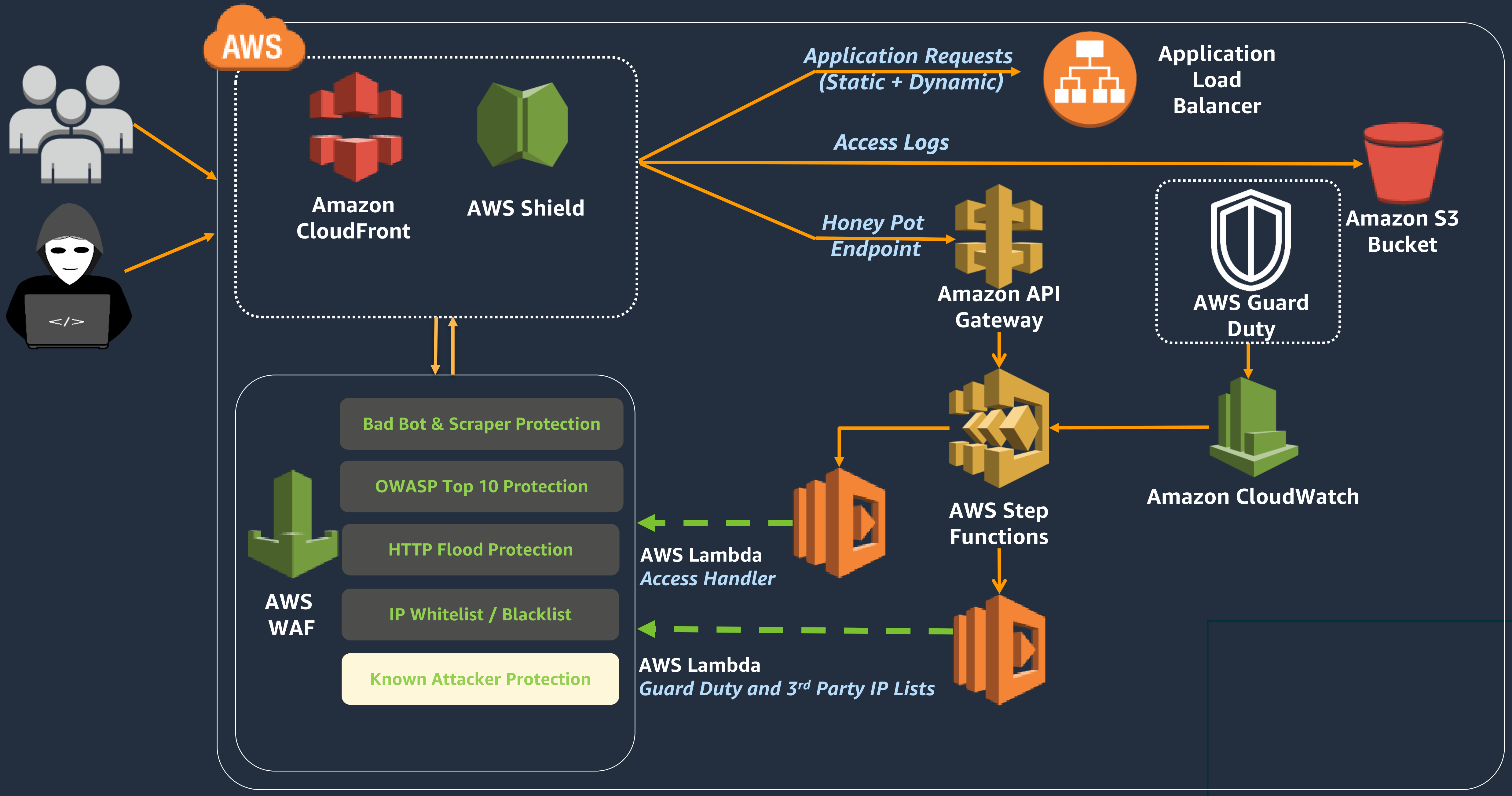
AWS WAF

AWS Lambda

Amazon API Gateway

AWS Step Functions

AWS Shield


AWS
Amazon CloudFront
AWS Shield
Application Requests (Static + Dynamic)
Application Load Balancer
Access Logs
Amazon S3 Bucket
Honey Pot Endpoint
Amazon API Gateway
AWS Guard Duty
AWS Step Functions
Amazon CloudWatch
Bad Bot & Scraper Protection
OWASP Top 10 Protection
HTTP Flood Protection
IP Whitelist / Blacklist
Known Attacker Protection
AWS WAF
AWS Lambda
Access Handler
AWS Lambda
Guard Duty and 3rd Party IP Lists
</>

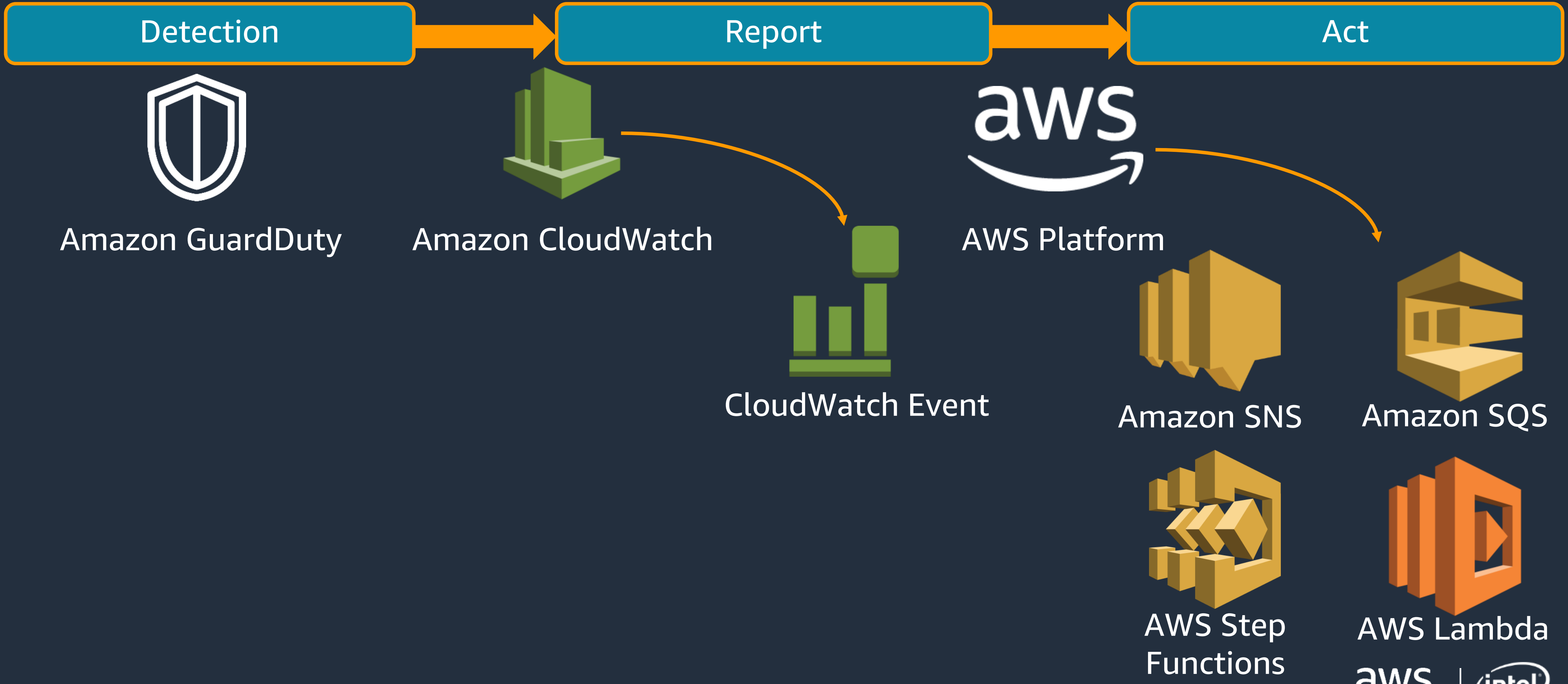
AWS Guard Duty

Generate findings through VPC Log Stream

Queries to questionable domains

AWS CloudTrail history of AWS calls and user activity

Automating Remediation



Detection

Report

Act

Amazon GuardDuty

Amazon CloudWatch

CloudWatch Event

AWS Platform

Amazon SNS

Amazon SQS

AWS Step Functions

AWS Lambda

Demo

The Snowy Unicorn Elevator Company

AWS WAF

Amazon API Gateway

AWS Lambda

AWS Guard Duty

AWS Step Functions

AWS Shield

Our Security ToolBox

AWS WAF

Amazon API Gateway

AWS Lambda

AWS Guard Duty

AWS Step Functions

AWS Shield

Can I Afford This?

Can I Afford This? Let’s Do The Math

All This For Under $20

FEDERAL RESERVE NOTE
20
THE UNITED STATES OF AMERICA
JB 99955579 A
B2
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES 2009
Secretary of the Treasury.
TWENTY DOLLARS
JACKSON

All This For Under $20

$16

AWS WAF

Web ACL and Rules	$5 per month per WebACL + $1 per month per rule
Request Charge	$0.60 per million requests

All This For Under $20

$16

$0.05

Amazon API Gateway

$3.50 per million API calls

All This For Under $20

$16

$0.05

$0.02

AWS Lambda

$0.20 per million requests

All This For Under $20

$16

$0.05

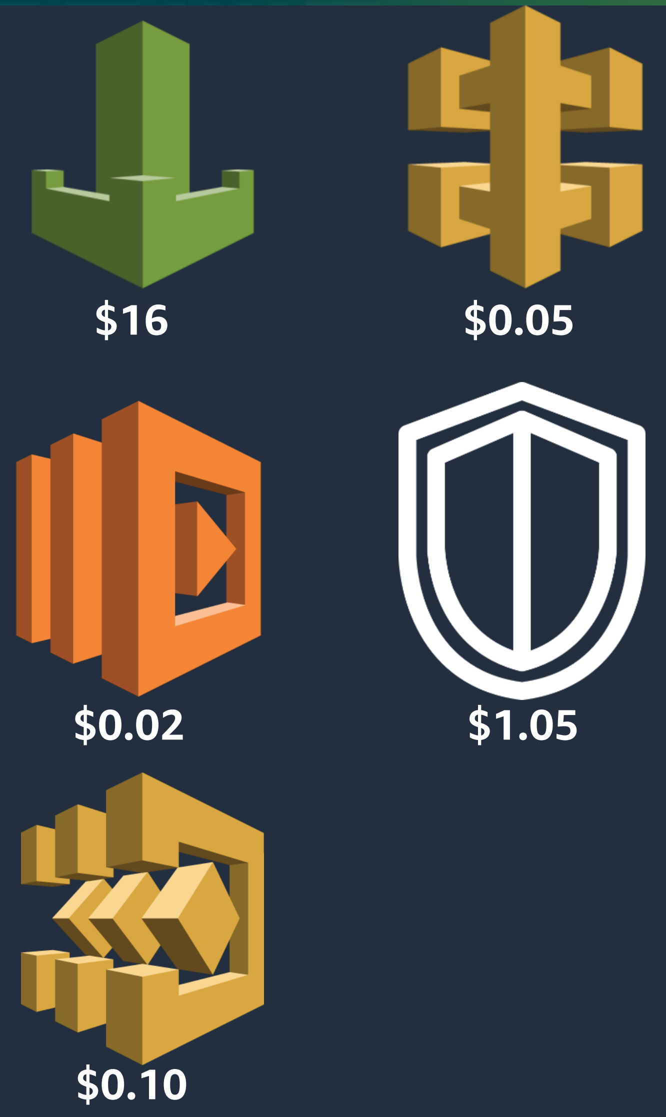
$0.02

$1.05

AWS GuardDuty

VPC Flow Log and DNS Log Analysis	First 500GB $1.10 per GB
CloudTrail Event Analysis	$4.40 per 1 million requests

All This For Under $20



AWS Step Functions

$0.025 per 100 state transitions

All This For Under $20

$16
$0.05
$0.02
$1.05
$0.10
$0.00

AWS Shield - Standard

$0.00

Session Recap

Build Dynamic Security Architectures

Leverage AWS development services to provide visibility and drive maturity in to your InfoSec practice

Session Recap

Build Dynamic Security Architectures

Leverage AWS development services to provide visibility and drive maturity in to your InfoSec practice

Comprehensive Security Portfolio

Security at AWS is the highest priority. Benefit from security architecture for the most security-sensitive organisations

Session Recap

Build Dynamic Security Architectures

Leverage AWS development services to provide visibility and drive maturity in to your InfoSec practice

Comprehensive Security Portfolio

Security at AWS is the highest priority. Benefit from security architecture for the most security-sensitive organisations

Cost Optimised Security

Drive the cost of performing security down whilst providing full stack automation with the AWS platform

How To Get Started

AWS Lambda

Product Details -
https://aws.amazon.com/lambda/
Tutorial - https://amzn.to/2IJn4Bm

AWS Automation

WAF / Lambda Automation - http://amzn.to/2gblvOz
Step Functions Approval Workflow -
http://amzn.to/2hkPOUF

AWS Step Functions

Product Details -
https://aws.amazon.com/stepfunctions/
Tutorial - https://amzn.to/2rESkIf

Learn from AWS experts. Advance your skills and knowledge. Build your future in the AWS Cloud.

Digital Training

Free, self-paced online courses built by AWS experts

Classroom Training

Classes taught by accredited AWS instructors

AWS Certification

Exams to validate expertise with an industry-recognized credential

Ready to begin building your cloud skills?
Get started at: https://www.aws.training/

aws | intel

With deep expertise on AWS, APN Partners can help your organization at any stage of your Cloud Adoption Journey.

aws msp

AWS Managed Service Providers

APN Consulting Partners who are skilled at cloud infrastructure and application migration, and offer proactive management of their customer's environment.

aws competency

AWS Competency Partners

APN Partners who have demonstrated technical proficiency and proven customer success in specialized solution areas.

aws marketplace

AWS Marketplace

A digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS.

aws service delivery

AWS Service Delivery Partners

APN Partners with a track record of delivering specific AWS services to customers.

Ready to get started with an APN Partner?

Find a partner: https://aws.amazon.com/partners/find/

Learn more at the AWS Partner Network Booth

aws | intel

Thank You for Attending AWS Innovate

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.

- aws-apac-marketing@amazon.com
- twitter.com/AWSCloud
- facebook.com/AmazonWebServices
- youtube.com/user/AmazonWebServices
- slideshare.net/AmazonWebServices
- twitch.tv/aws