AWS re:Invent

SEC330

Protecting workloads on AWS from the instance to the edge

Cameron Worrell

Solutions Architect

Amazon Web Solutions

Jeff Levine

Security Solutions Architect

Amazon Web Solutions

About today’s workshop

Agenda:

- Overview of threat landscape
- AWS WAF intro and rule anatomy
- Intro to Amazon Inspector
- Intro to AWS Systems Manager
- Hands-on exercises

Workshop team

Milad

Fatima

Alejandro

Daniel

Alex

Louay

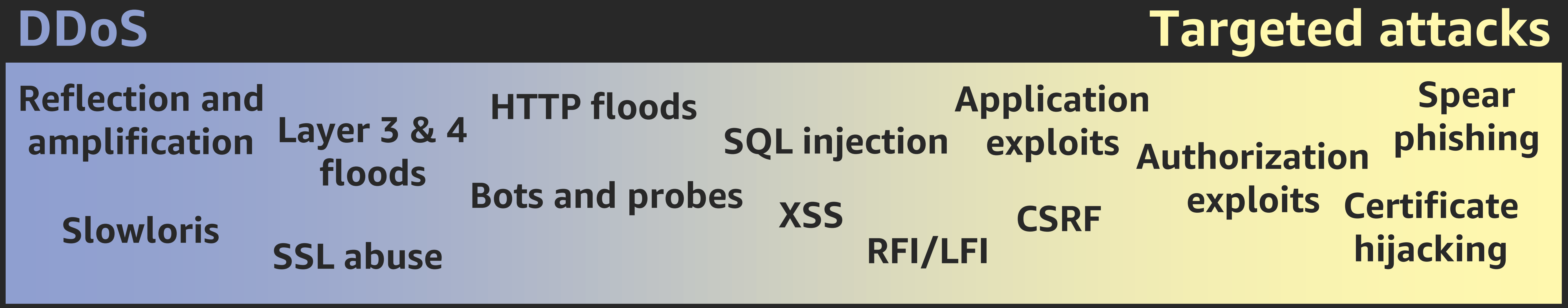
Edouard

Abhinav Krishna

Jeff

Cameron

Spectrum of attacks



DDoS

Targeted attacks

Reflection and amplification

Slowloris

Layer 3 & 4 floods

SSL abuse

HTTP floods

Bots and probes

SQL injection

XSS

RFI/LFI

Application exploits

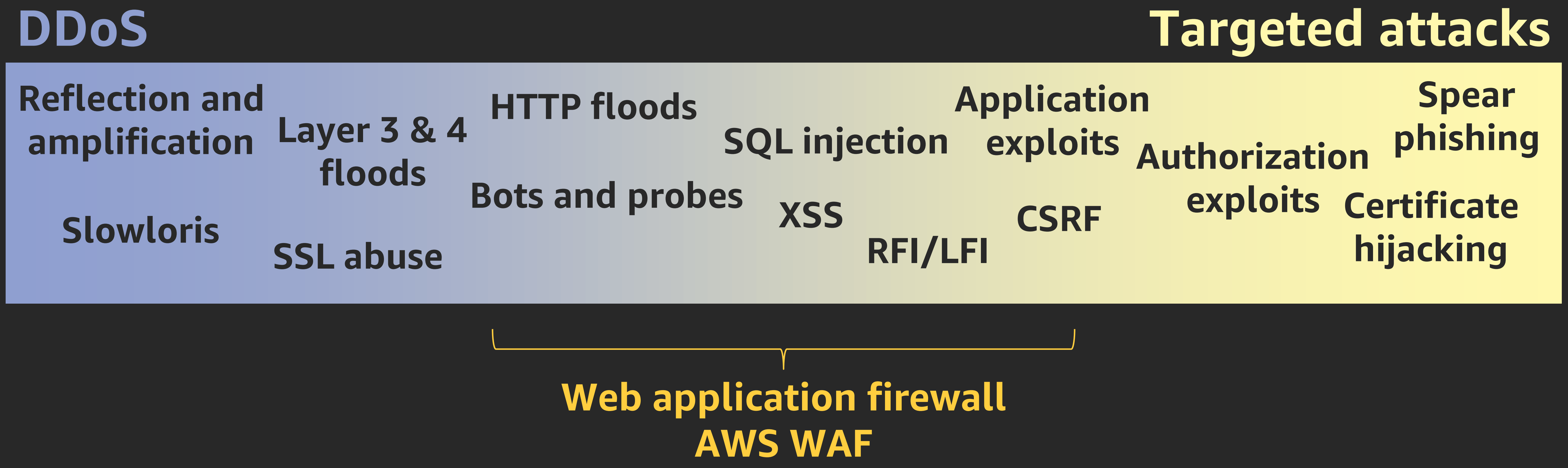
CSRF

Authorization exploits

Spear phishing

Certificate hijacking

Spectrum of attacks



DDoS

Targeted attacks

Reflection and amplification

Slowloris

Layer 3 & 4 floods

SSL abuse

HTTP floods

Bots and probes

SQL injection

XSS

RFI/LFI

Application exploits

CSRF

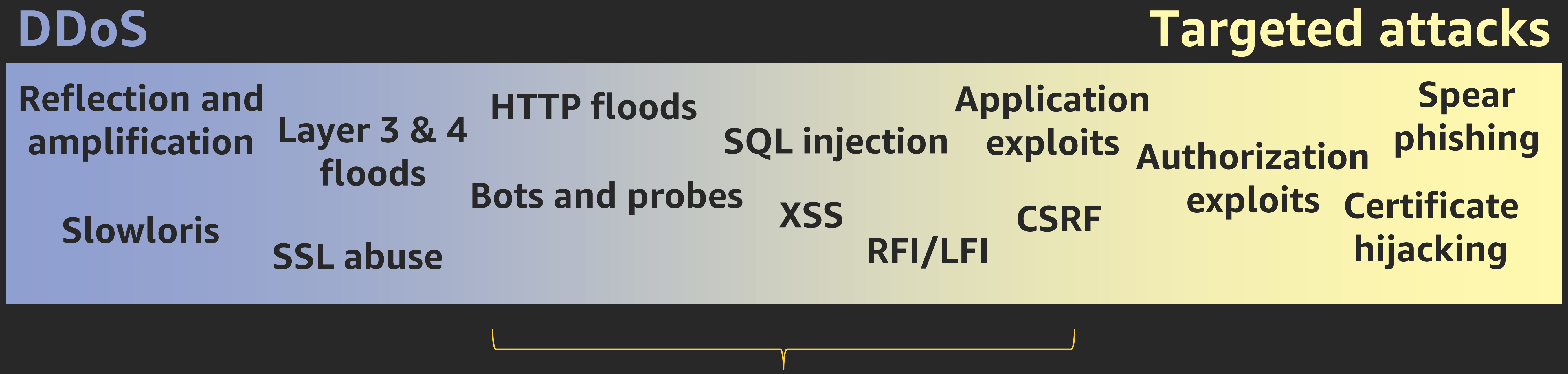
Authorization exploits

Spear phishing

Certificate hijacking

Web application firewall
AWS WAF

Spectrum of attacks



DDoS

Targeted attacks

Reflection and amplification

Slowloris

Layer 3 & 4 floods

SSL abuse

HTTP floods

Bots and probes

SQL injection

XSS

RFI/LFI

Application exploits

CSRF

Authorization exploits

Spear phishing

Certificate hijacking

- Amazon CloudFront
- Elastic Load Balancing
- AWS Shield Standard
- AWS Shield Advanced

Web application firewall
AWS WAF

- Amazon Inspector
- Amazon Macie
- Amazon Certificate Manager (ACM)
- AWS Marketplace: IDS/IPS, anti-malware

OWASP top 10 – 2017

Represents a broad consensus about the most critical web application security risks

A1
Injection

A2
Broken authentication

A3
Sensitive data exposure

A4
XML external entities (XXE)

A5
Broken access control

A6
Security misconfiguration

A7
Cross-site scripting (XSS)

A8
Insecure deserialization

A9
Using components with known vulnerabilities

A10
Insufficient logging and monitoring

Let’s start with the perimeter

Edge and perimeter

Virtual instance and OS

CloudFront

AWS Shield

AWS WAF

AWS Firewall Manager

AWS WAF

How AWS WAF can help you

AWS WAF

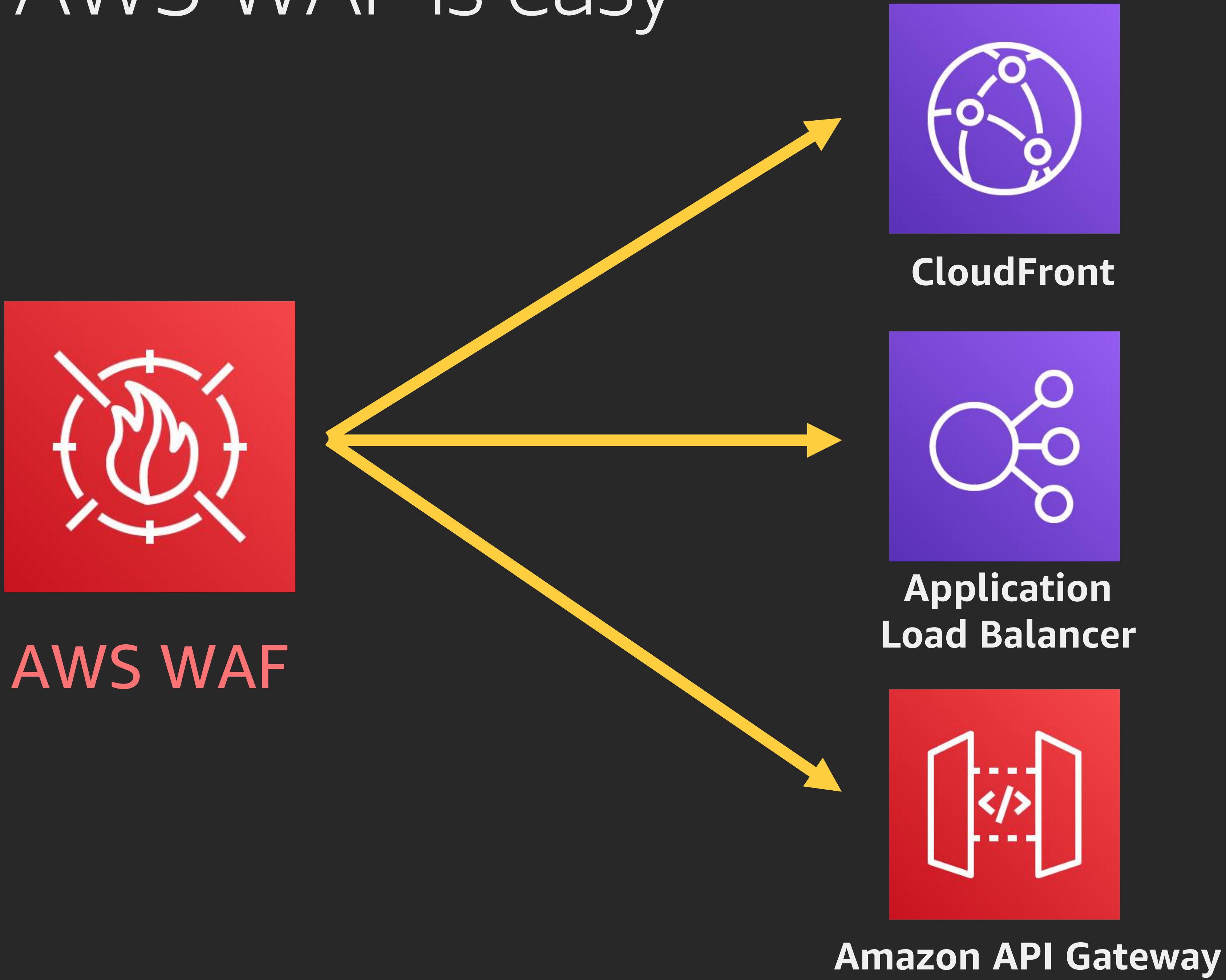
Customize security to your applications using custom rules

Utilize managed rules from the AWS Marketplace for hassle-free protection and deployment

Monitor using Amazon CloudWatch metrics or third-party log processors

Automate using AWS Lambda-based security automations

Deploying AWS WAF is easy



AWS WAF

CloudFront

Application
Load Balancer

Amazon API Gateway

Using AWS WAF to mitigate OWASP top 10

AWS WAF can mitigate application flaws in the OWASP top 10 categories

- A web application firewall does not fix the underlying flaws; it limits the ability to exploit them

- Ability to derive recognizable HTTP request pattern is key to effectiveness

- Ability to quickly change the rule configuration to keep up with changing attacks

What protection does AWS WAF provide?

Malicious traffic blocking

- SQL injection
- Cross-site scripting (XSS)
- IP blacklist

Web traffic filtering

- Rate-based rules
- IP match and geo-IP filters
- Regex and string match
- Size constraints

Active monitoring

- CloudWatch metrics/alarms
- Sampled logs
- Comprehensive logs

Strategies for building a web ACL

Blacklisting:

- **Block bad** patterns with rules; default action is: **ALLOW**
- More commonly used

Whitelisting:

- **Allow good** patterns with rules; default action is: **BLOCK**
- Works best for defined limited pattern sets

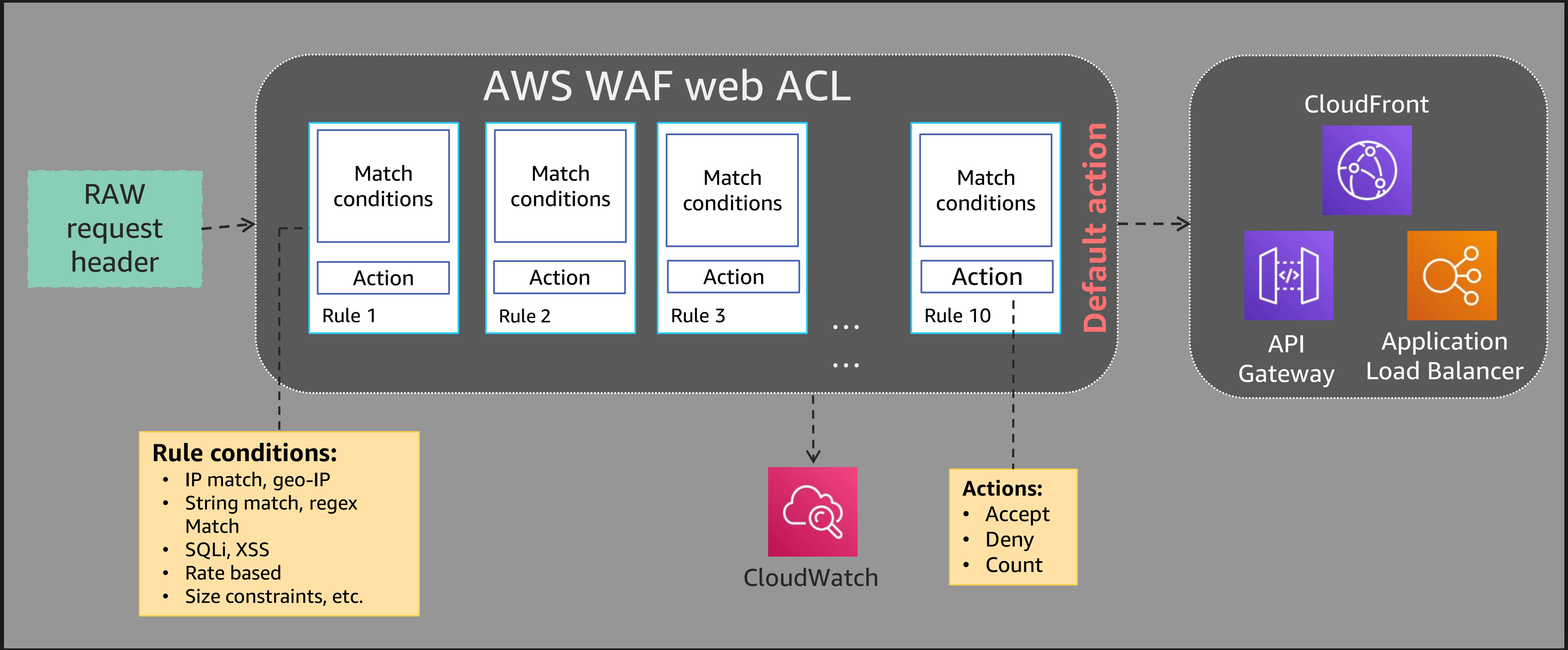
Mixed:

- Considerations: Rule ordering, bypass rules

Count effects:

- Test pattern effectiveness with **COUNT** rule action

How AWS WAF works



RAW request header

AWS WAF web ACL

Match conditions

Action

Rule 1

Match conditions

Action

Rule 2

Match conditions

Action

Rule 3

…

…

Match conditions

Action

Rule 10

Default action

CloudFront

API Gateway

Application Load Balancer

CloudWatch

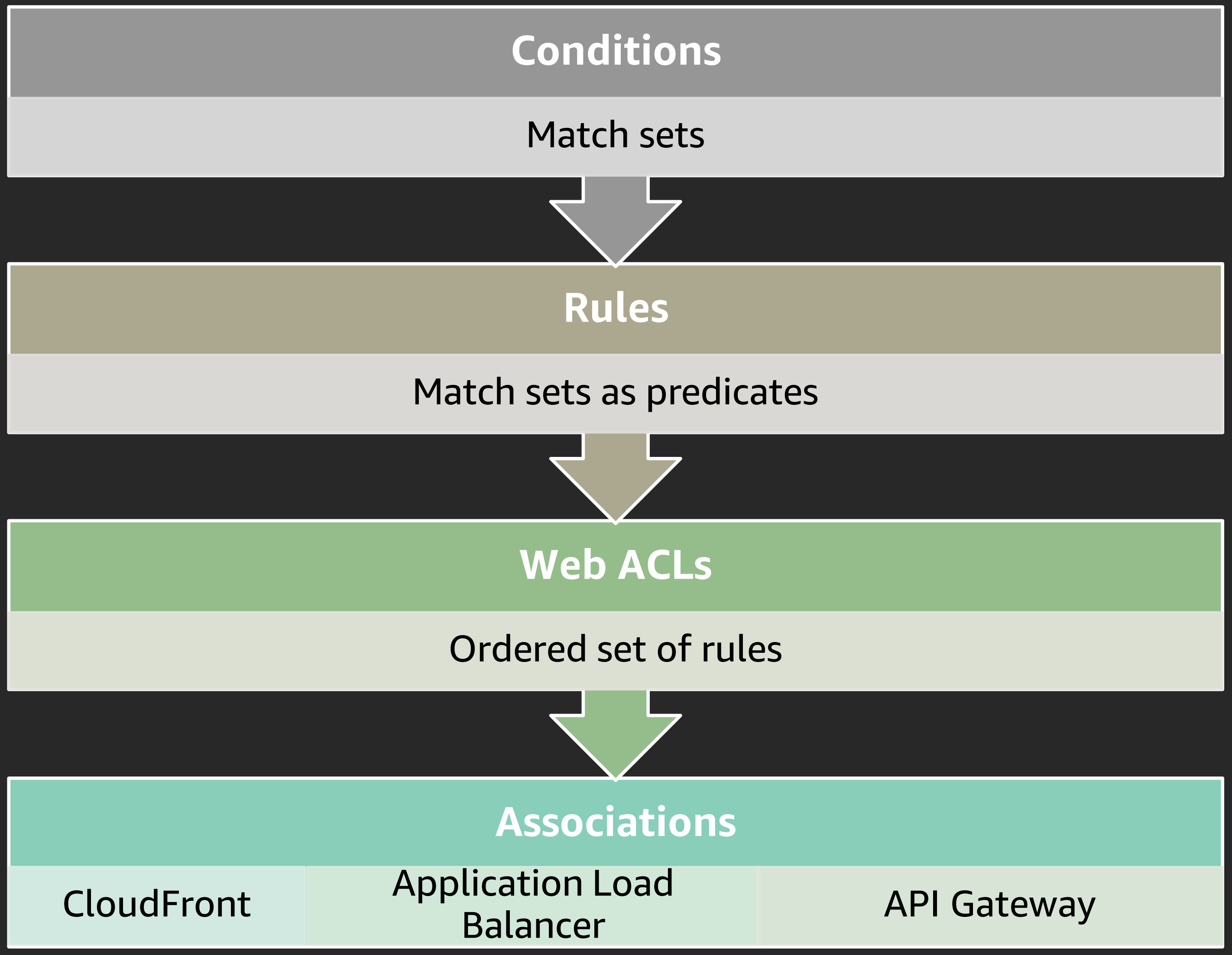
Rule conditions:

- IP match, geo-IP
- String match, regex Match
- SQLi, XSS
- Rate based
- Size constraints, etc.

Actions:

- Accept
- Deny
- Count

Implementing AWS WAF



Conditions

Match sets

Rules

Match sets as predicates

Web ACLs

Ordered set of rules

Associations

CloudFront

Application Load Balancer

API Gateway

- SQL injection
- Cross-site scripting (XSS)
- IP blacklisting/whitelisting
- Request hygiene/size constraints
- String and regex pattern filtering
- Geo matching

- Standard rules
- Rate-based rules (per 5-minute interval)

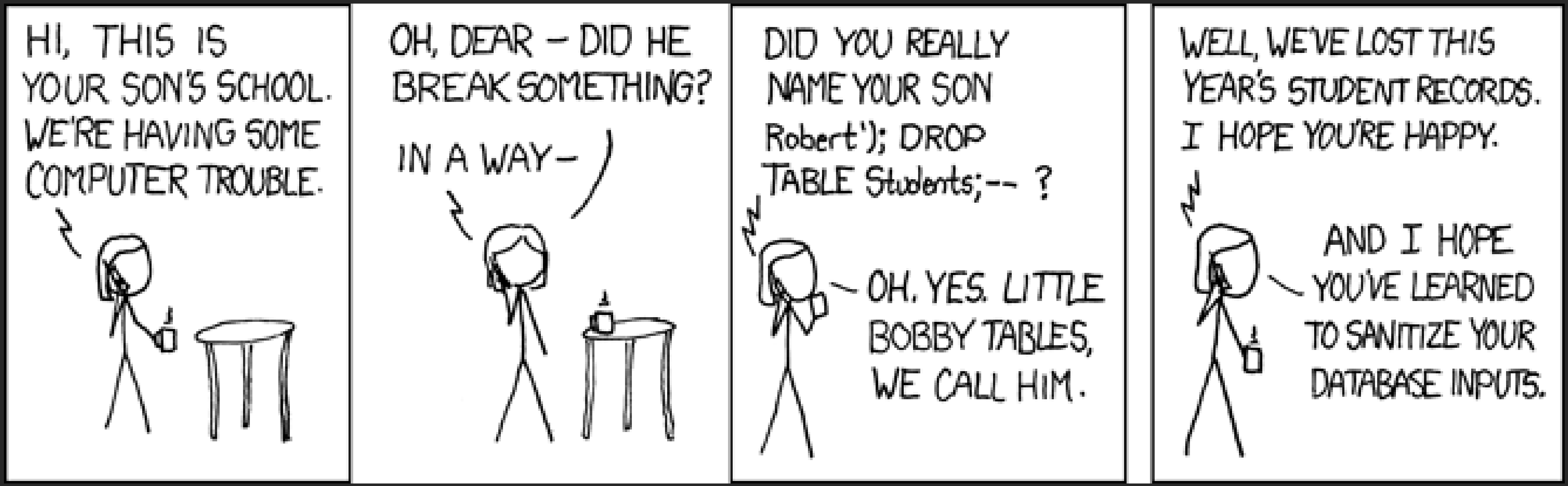
- Actions: Block, allow, count

- Perimeter protection

SQL injection

Injection flaw: application sends untrusted data to an interpreter, risk of altering original intent of request

Most well known are SQL injection flaws


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Credit: XKCD, "Exploits of a Mom"

Mitigate injection flaws

Mitigate using AWS WAF SQL injection match conditions

- What HTTP request components should you scan?
  - Query string, URI, body, cookie, and/or authorization header
- What transformations should you apply?
  - URL decode, decode HTML entities
- Considerations for false positives and other injection types

AWS WAF visibility and analytics

CloudWatch metrics

- Metrics on every rule
- Allowed | Blocked | Counted | Passed (No Action)
- Uses: Set alarms for notification

Sampled web requests

- *Sample* of requests with details about request (IP, header, etc.)
- Automatically available for every rule created
- Sample size up to 500 requests and time range within the previous three hours
- Uses: Quickly test rules before deployment
- Easy triaging on the console

Comprehensive logs (full logging)

- Detailed logs, of *all* requests (both matched and not matched)
- Optionally enabled for your WebACL
- Includes details about every request, along with all rules that match the request
- Uses: Security analytics, monitoring, automation, auditing and compliance

AWS WAF comprehensive logs

Key features

- ✓ Streaming logs available through Amazon Kinesis Data Firehose
- ✓ Available in JSON format
- ✓ Logs every request, contains all request headers, along with RuleIDs that matched
- ✓ Redact sensitive fields from logs (e.g., redact cookie or authentication header)
- ✓ Configure Kinesis Data Firehose for multiple destinations

Amazon S3

Amazon Redshift

Amazon Elasticsearch Service

Third-party solutions

What’s new in AWS WAF?

Write hundreds of rules: replaced multiple service limits with an easy to understand single limit (WCU), allows you to mix-and-match managed rules

Document-based rule writing in JSON: updating rules using single API calls and providing ability to version control rules

Streamlined console and API workflow: simplifying the console to be more intuitive and reducing API calls required to perform actions

New detection capabilities: adding support for OR logic between conditions, multiple chainable transform, and full CIDR range

AWS Managed Rules for AWS WAF: Curated and maintained by AWS Threat Research Team (TRT). Primarily influenced by OWASP Top 10.

Let’s talk about the instance layer

Edge and perimeter

Virtual instance and OS

Amazon Inspector

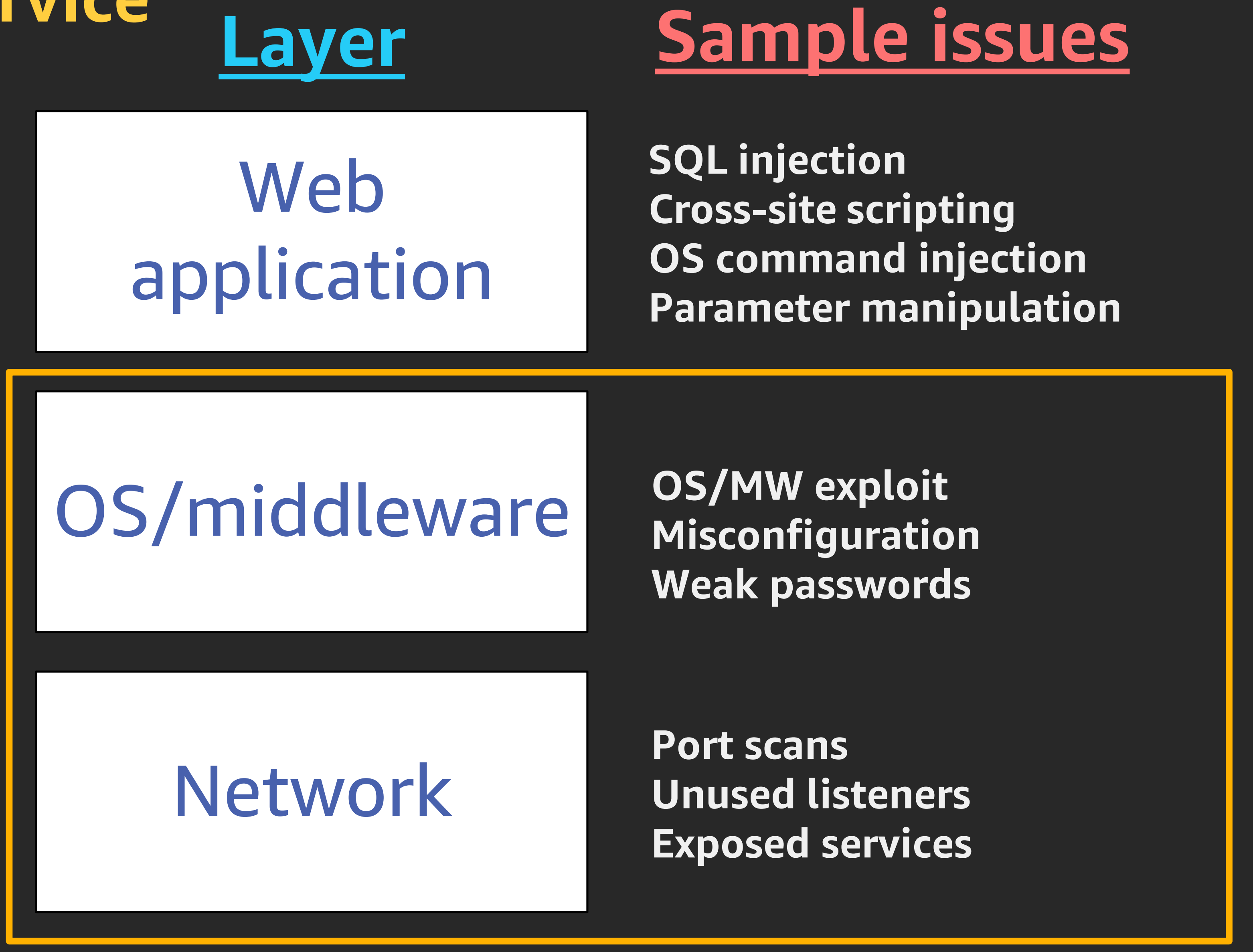
Systems Manager

Amazon Inspector

Amazon Inspector

Automated security assessment service

- Automatically assesses applications for vulnerabilities or deviations from best practices
- Produces a detailed list of security findings prioritized by level of severity
- Agent-based, API-driven, and delivered as a service



Layer	Sample issues
Web application	SQL injection Cross-site scripting OS command injection Parameter manipulation
OS/middleware	OS/MW exploit Misconfiguration Weak passwords
Network	Port scans Unused listeners Exposed services

Target scope for Amazon Inspector

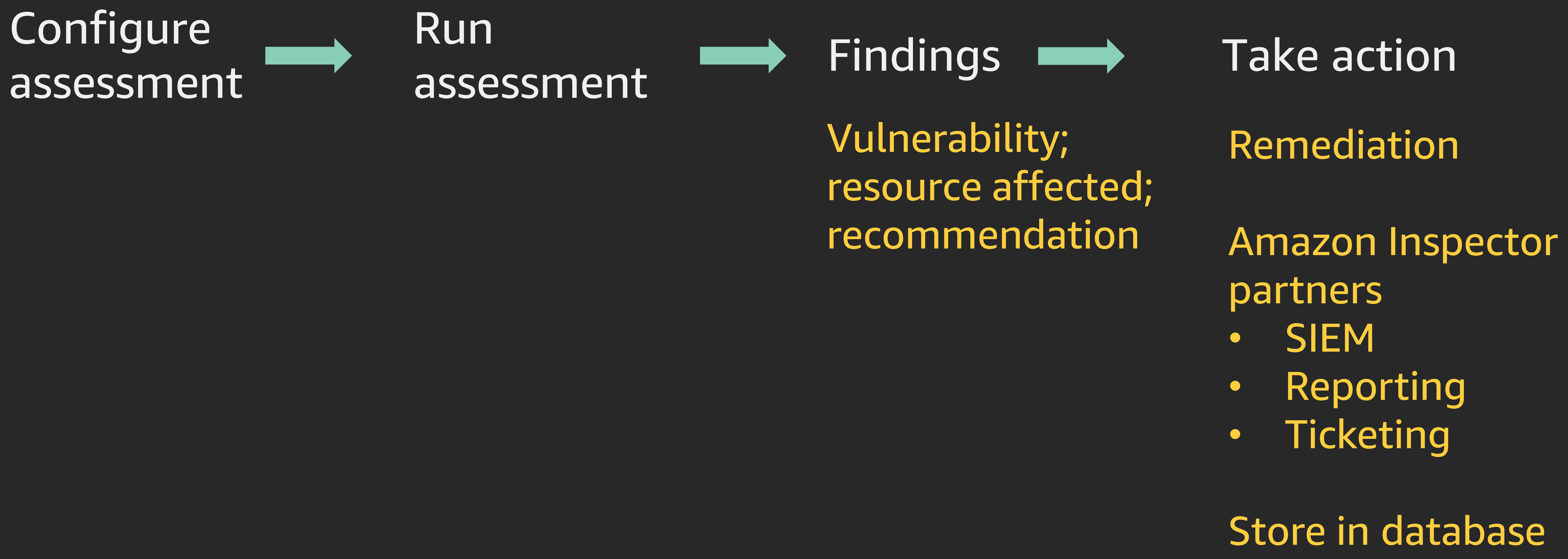
Amazon Inspector

Three kinds of rules packages

Severity levels for rules : High, medium, low, informational

- Common vulnerabilities and exposures (CVE)
- Center for Internet Security (CIS) benchmarks
- Security best practices

How to use Amazon Inspector?



Configure assessment → Run assessment → Findings → Take action

Findings:

Vulnerability; resource affected; recommendation

Take action:

Remediation

Amazon Inspector partners

- SIEM
- Reporting
- Ticketing

Store in database

Systems Manager

AWS Systems Manager capabilities

- Resource Groups
- Run Command
- Inventory
- Patch Manager
- Automation
- Parameter Store
- Distributor
- State Manager
- Maintenance Window
- Session Manager

Extensible

Hybrid

Works in hybrid and multi-cloud environments

Compliance

Use existing tools like Ansible, PowerShell DSC, and InSpec for configuration and compliance

Open source

SSM agent is open-sourced on GitHub

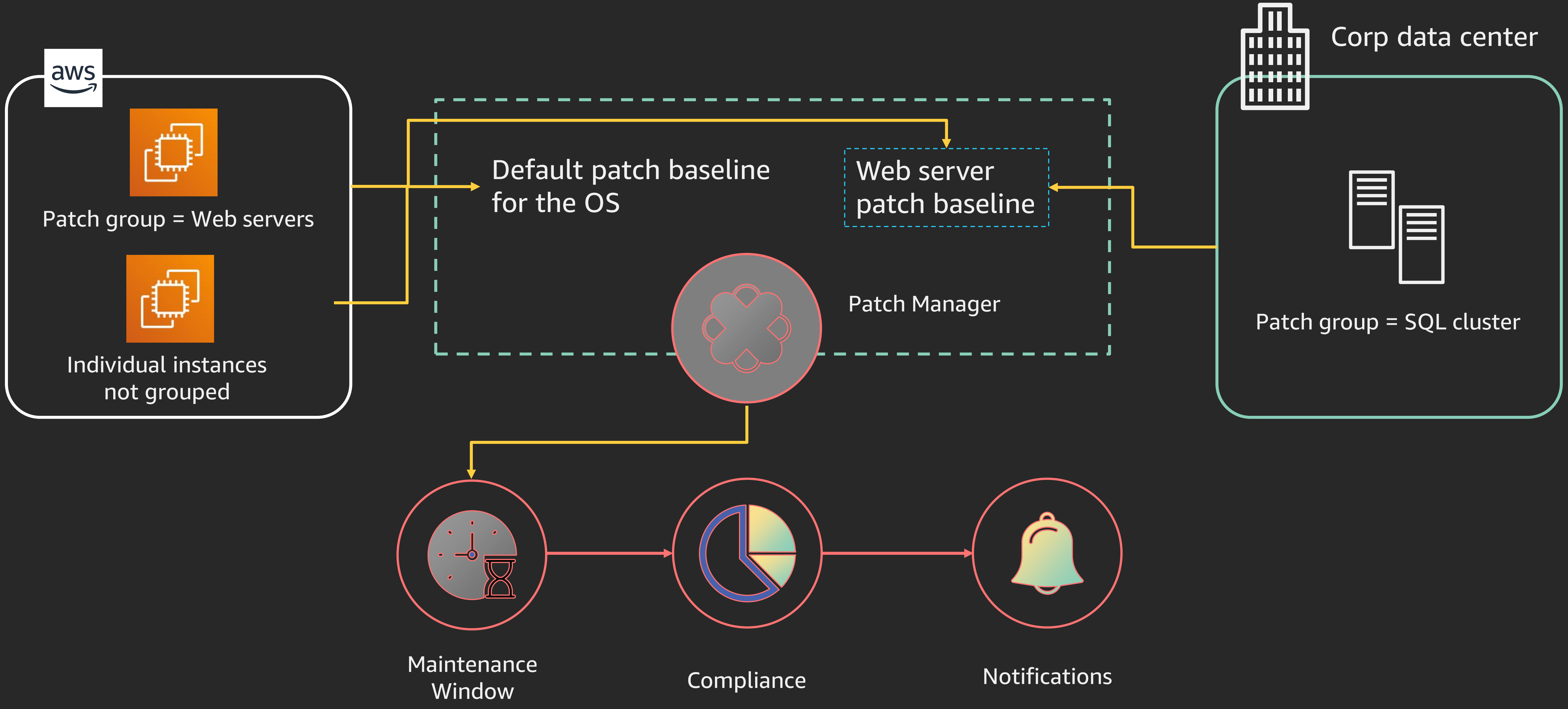
Cross-platform

Windows and Linux support

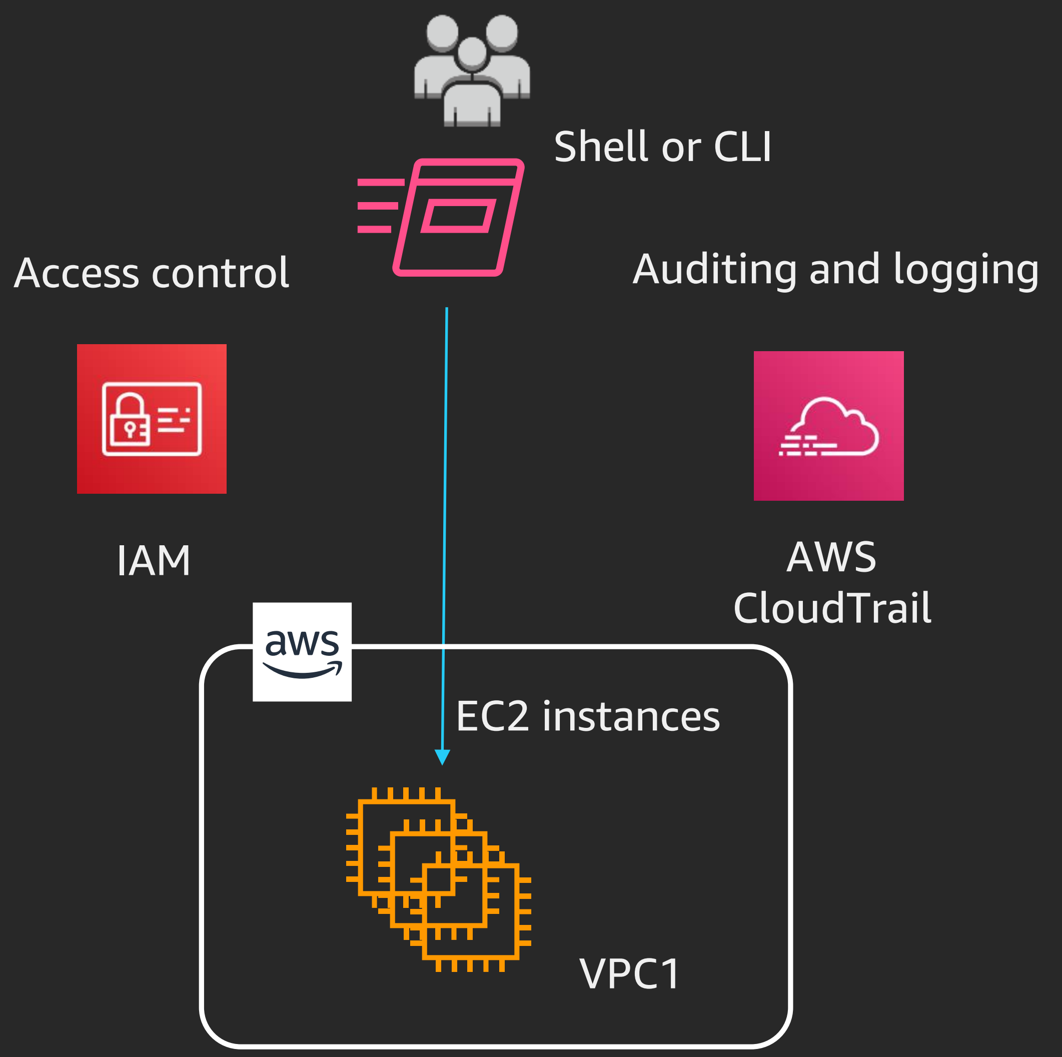
Extensible

Extensible capabilities to collect custom inventory from instances

Compliance with Patch Manager


aws
Patch group = Web servers
Individual instances not grouped
Default patch baseline for the OS
Web server patch baseline
Patch Manager
Corp data center
Patch group = SQL cluster
Maintenance Window
Compliance
Notifications

Interactive access to instances with Session Manager



- Interactive browser-based shell and CLI for EC2 instances
- No need to open inbound ports, manage SSH keys or certs
- Grant/revoke access from AWS Identity and Access Management (IAM)
- Session auditing and logging
- Support for AWS PrivateLink

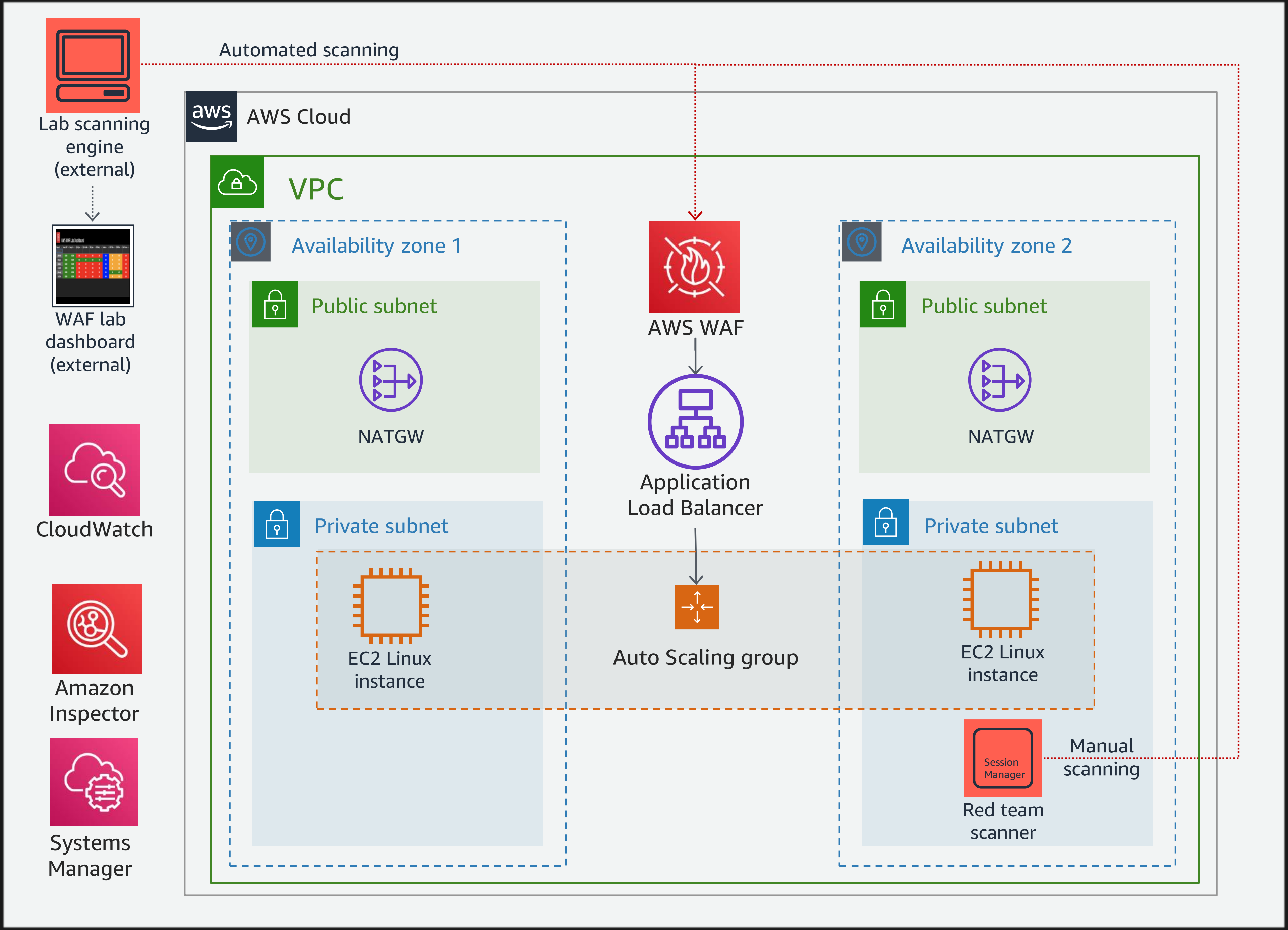
Hands-on exercises

Each participant has their own environment within Event Engine

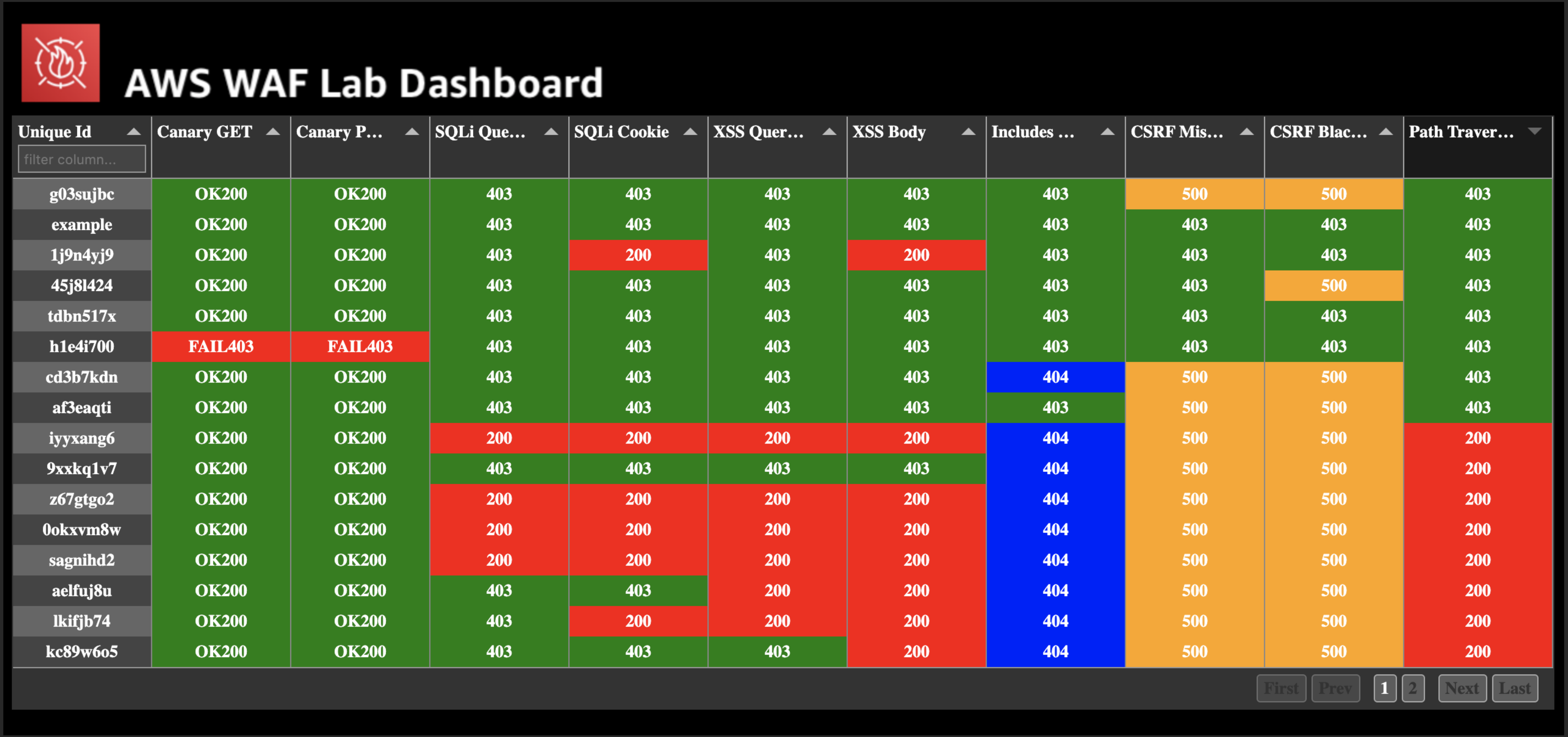
Mission:

- Build and test mitigating AWS WAF rule set
- Assess security posture of EC2 instances
- Remediate issues on EC2 instances
- Track AWS WAF mitigations on dashboard

Workshop architecture



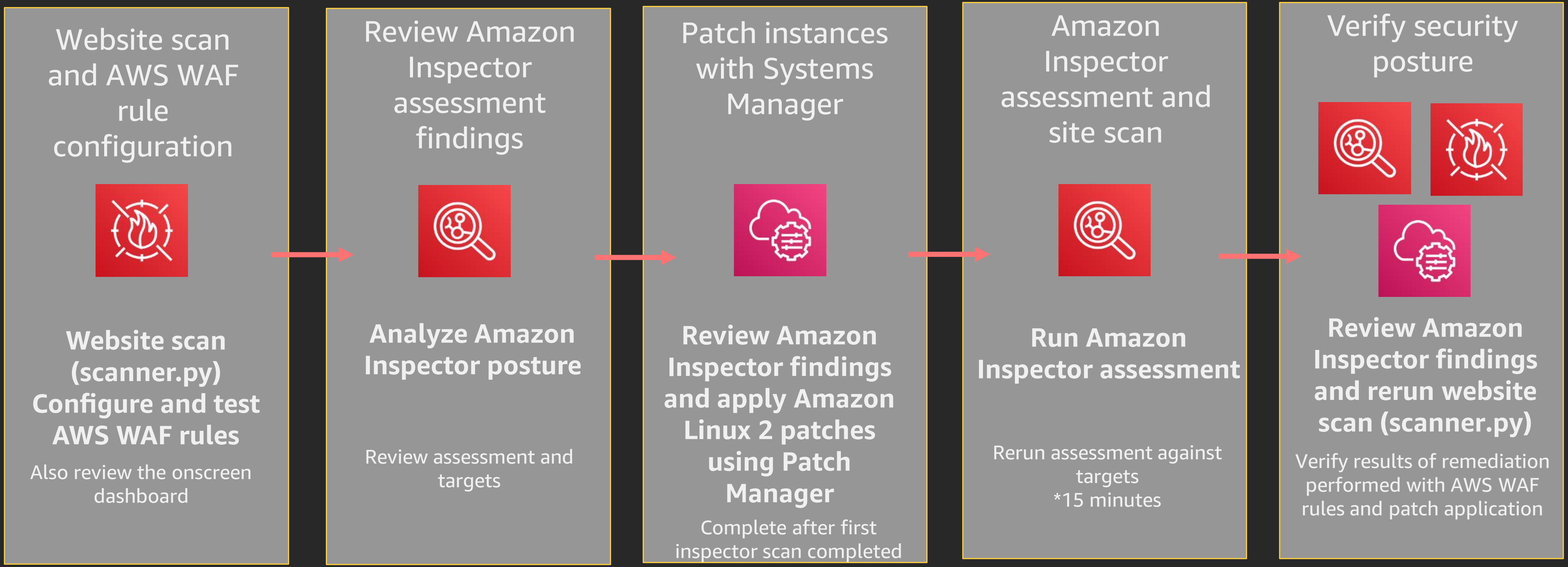
WAF mitigation dashboard



AWS WAF Lab Dashboard

Unique Id filter column...	Canary GET	Canary P…	SQLi Que…	SQLi Cookie	XSS Quer…	XSS Body	Includes …	CSRF Mis…	CSRF Blac…	Path Traver…
g03sujbc	OK200	OK200	403	403	403	403	403	500	500	403
example	OK200	OK200	403	403	403	403	403	403	403	403
1j9n4yj9	OK200	OK200	403	200	403	200	403	403	403	403
45j8l424	OK200	OK200	403	403	403	403	403	403	500	403
tdbn517x	OK200	OK200	403	403	403	403	403	403	403	403
h1e4i700	FAIL403	FAIL403	403	403	403	403	403	403	403	403
cd3b7kdn	OK200	OK200	403	403	403	403	404	500	500	403
af3eaqti	OK200	OK200	403	403	403	403	403	500	500	403
iyyxang6	OK200	OK200	200	200	200	200	404	500	500	200
9xxkq1v7	OK200	OK200	403	403	403	403	404	500	500	200
z67gtgo2	OK200	OK200	200	200	200	200	404	500	500	200
0okxvm8w	OK200	OK200	200	200	200	200	404	500	500	200
sagnihd2	OK200	OK200	200	200	200	200	404	500	500	200
aelfuj8u	OK200	OK200	403	403	200	200	404	500	500	200
lkifjb74	OK200	OK200	403	200	200	200	404	500	500	200
kc89w6o5	OK200	OK200	403	403	403	200	404	500	500	200

Hands-on workflow



Website scan and AWS WAF rule configuration

Website scan (scanner.py) Configure and test AWS WAF rules

Also review the onscreen dashboard

Review Amazon Inspector assessment findings

Analyze Amazon Inspector posture

Review assessment and targets

Patch instances with Systems Manager

Review Amazon Inspector findings and apply Amazon Linux 2 patches using Patch Manager

Complete after first inspector scan completed

Amazon Inspector assessment and site scan

Run Amazon Inspector assessment

Rerun assessment against targets
*15 minutes

Verify security posture

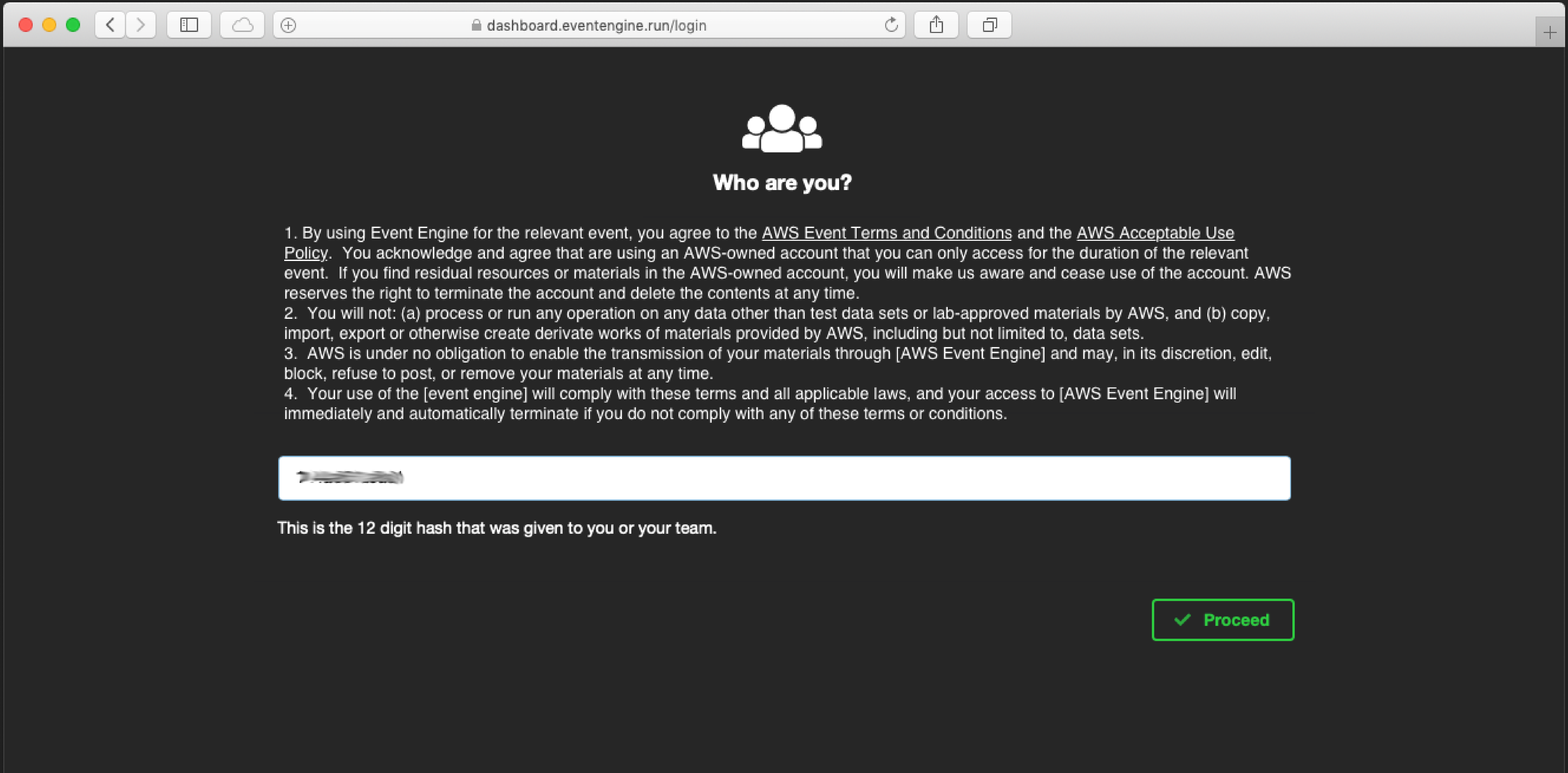
Review Amazon Inspector findings and rerun website scan (scanner.py)

Verify results of remediation performed with AWS WAF rules and patch application

Let’s get started

https://dashboard.eventengine.run

Enter your hash code



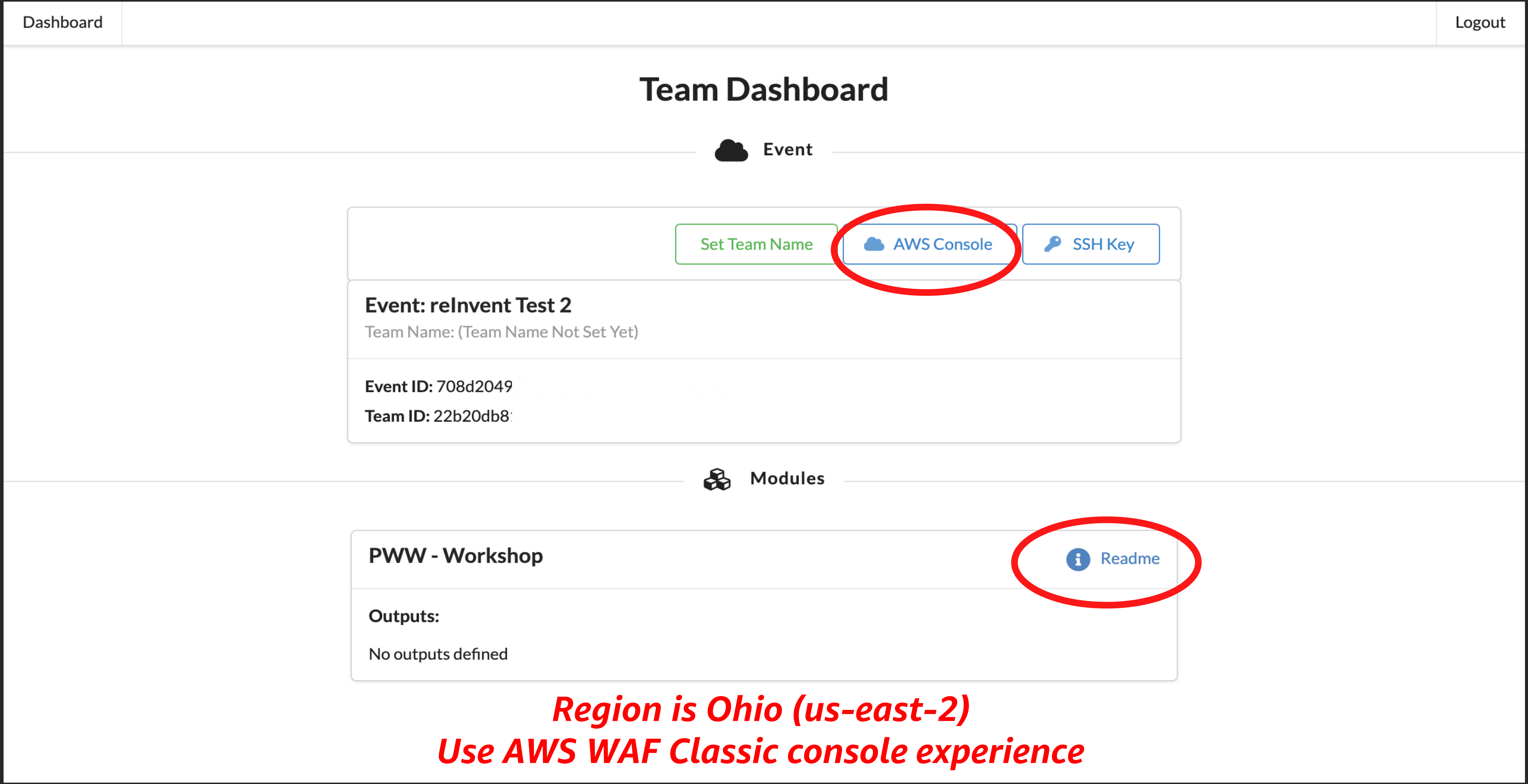
Who are you?

1. By using Event Engine for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.
2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivate works of materials provided by AWS, including but not limited to, data sets.
3. AWS is under no obligation to enable the transmission of your materials through [AWS Event Engine] and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.
4. Your use of the [event engine] will comply with these terms and all applicable laws, and your access to [AWS Event Engine] will immediately and automatically terminate if you do not comply with any of these terms or conditions.

[redacted]

This is the 12 digit hash that was given to you or your team.

Navigate the dashboard



Team Dashboard

Event

Event: reInvent Test 2

Team Name: (Team Name Not Set Yet)

Event ID: 708d2049

Team ID: 22b20db8

Modules

PWW - Workshop

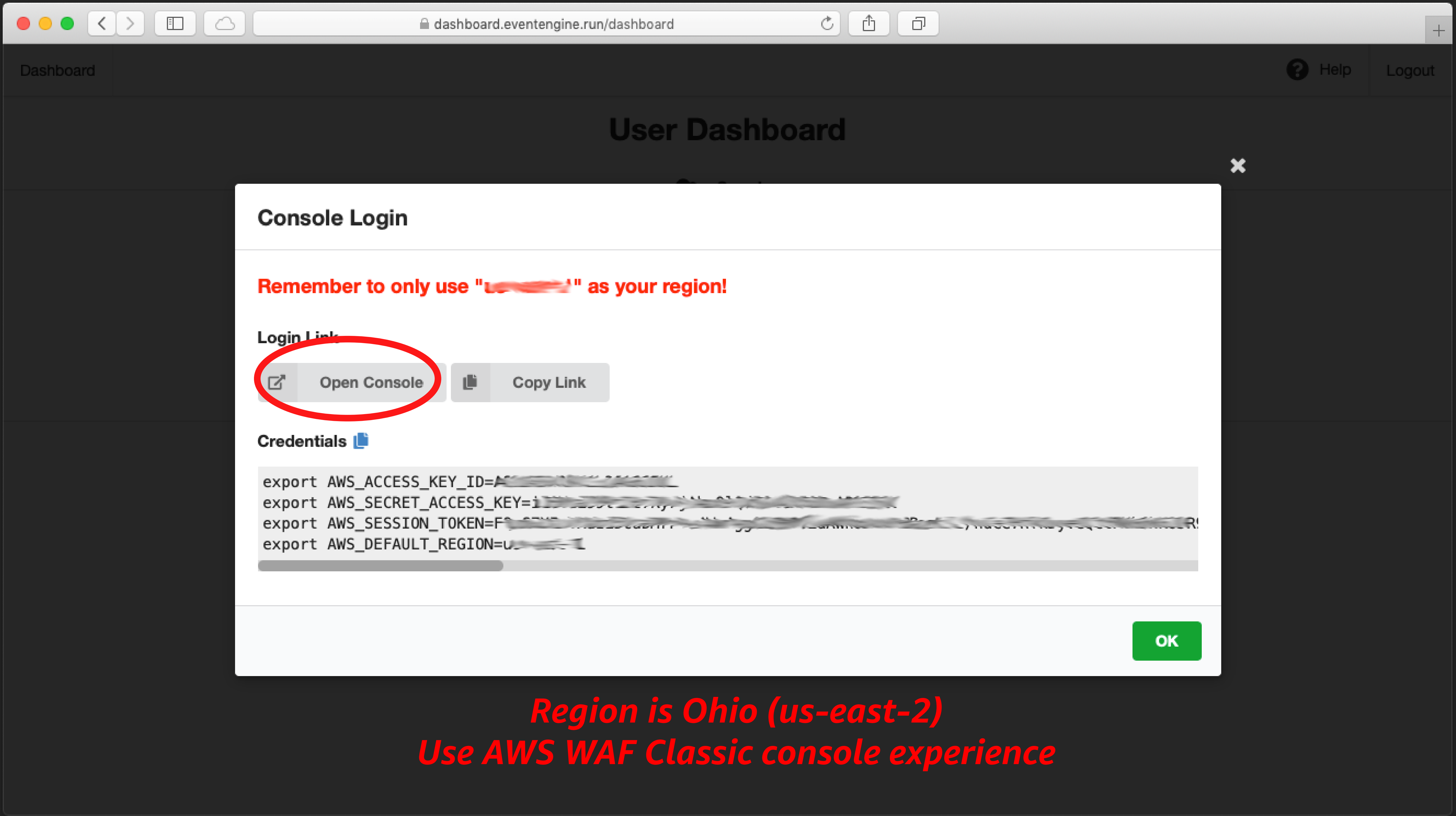
Outputs:

No outputs defined

Region is Ohio (us-east-2)

Use AWS WAF Classic console experience

Access the console



User Dashboard

Console Login

Remember to only use "[redacted]" as your region!

Login Link

Credentials

```
export AWS_ACCESS_KEY_ID=[redacted]
export AWS_SECRET_ACCESS_KEY=[redacted]
export AWS_SESSION_TOKEN=[redacted]
export AWS_DEFAULT_REGION=[redacted]
```

Region is Ohio (us-east-2)

Use AWS WAF Classic console experience

Before you start …

The AWS CloudFormation stack has already been deployed. Make sure you select the Event Engine options!

https://bit.ly/2uhcCIw

Workshop guide: **protecting-workloads.awssecworkshops.com**

Hash codes (use your assigned code)

Key takeaways

Internet-based attacks affect everyone, whether specifically targeted or not

You can no longer rely on just the application to thwart such attacks

Security controls should be implemented at the perimeter, network, and host layers

It's all about reducing the exposure footprint and risk

AWS WAF, Amazon Inspector, and Systems Manager can be used to help detect and mitigate attacks

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills

30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security

Classroom offerings, like AWS Security Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

aws training and certification

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.

AWS re:Invent

aws