AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

STP301

Startup security: Techniques to stay secure while building quickly

J. Michael
Sr. Solutions Architect – Startups
AWS

Faisal Farooq
Solutions Architect – Startups
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Quick survey
- Overview of the workshop
- Modules 1–5: Execute the Attack
- Review AWS services
- Modules 6–8: Detect & Prevent the Attack
- Q&A

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

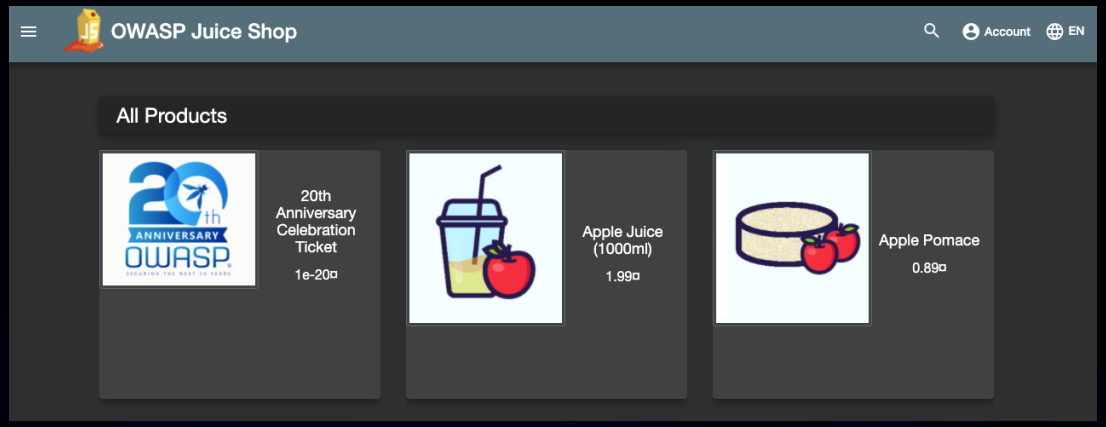
Quick survey

- Who works for a startup?
- Who is responsible for security as part of their job?
- Who has “security” in their job title?
- Who is familiar with every known web vulnerability that exists today?
- Who is confident their web applications have absolutely no vulnerabilities?
- Who is confident that they would know when a vulnerability in their application was being exploited?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop overview

- Exploit the OWASP Juice Shop
- Review threat detection finding
- Build preventions
- Watch them in action!



The OWASP® Word Mark and OWASP & Design™ Logo are registered or unregistered service marks of OWASP Foundation, Inc. in the United States and other countries. All rights reserved. Unauthorized use strictly prohibited.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Event Engine

https://dashboard.eventengine.run/

Enter your team hash: 198f-1ee5afbd84-5e

Email One-Time Password

Click “View Content Guide”

Click “AWS Console”

Click “Open AWS Console”

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Complete these modules

- Overview of the Environment
- Enable Threat Detection
- Execute the Attack



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OWASP: Web vulnerabilities

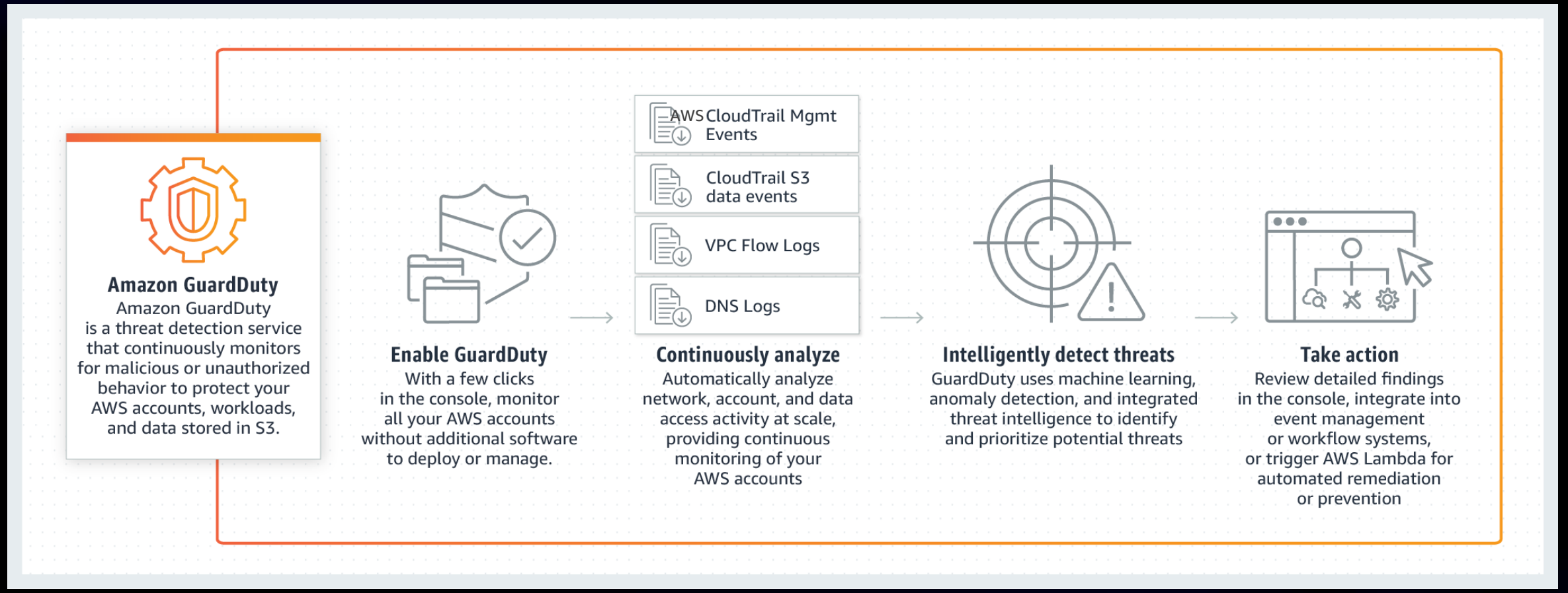
- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable & outdated components
- Identification & authentication failures
- Software and data integrity failures
- Security logging & monitoring failures
- Server-side request forgery (SSRF)



https://owasp.org/Top10/

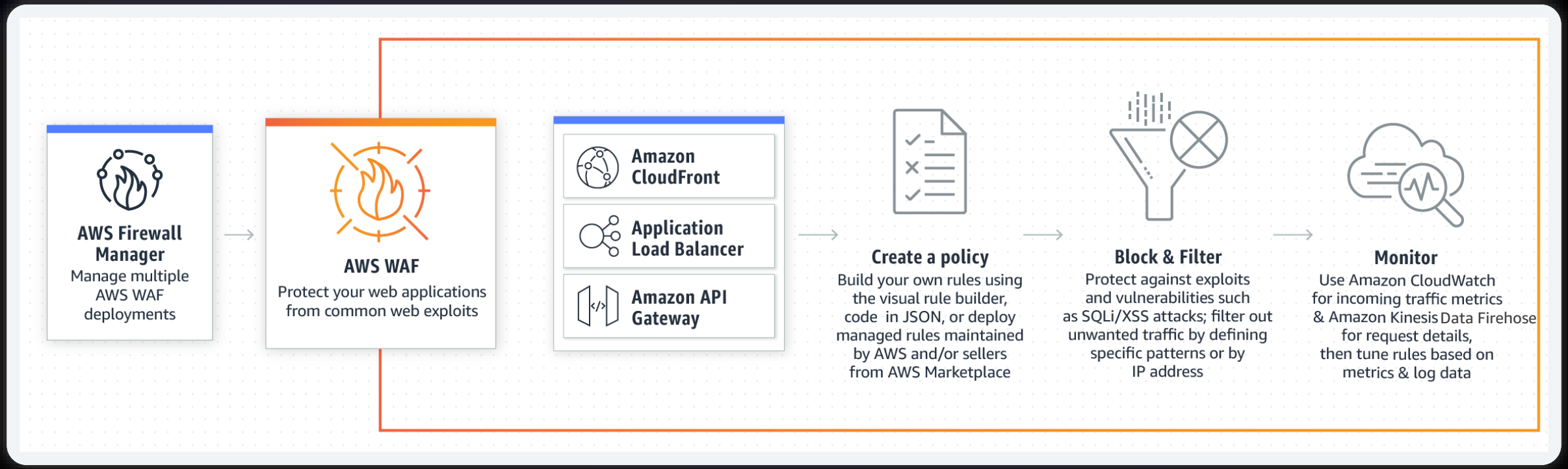
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Threat detection: Amazon GuardDuty



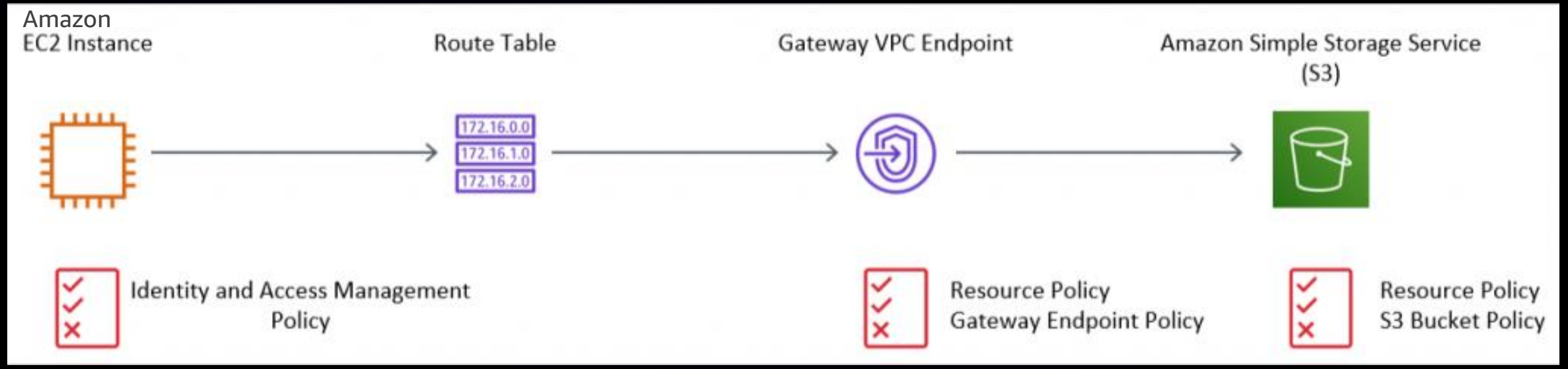
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Web Application Firewall (AWS WAF)



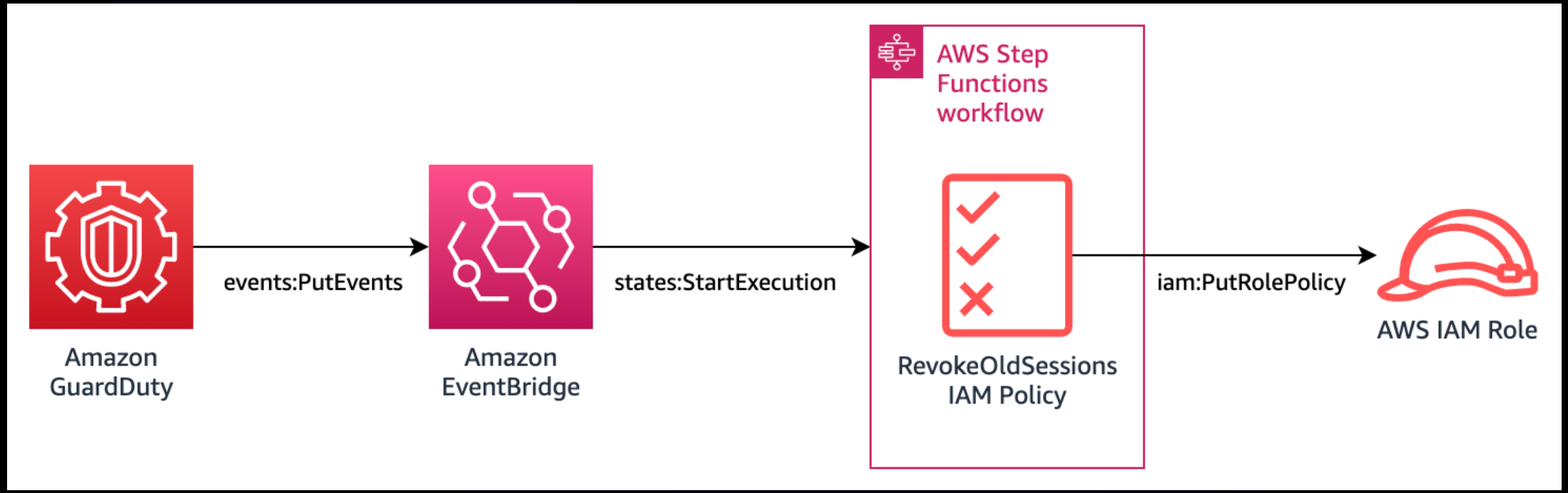
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC endpoint and Amazon S3 bucket policies



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EventBridge and AWS Step Functions



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Complete these modules

- Detect the Attack
- Prevent the Attack
- Retry the Attack



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary

- Amazon GuardDuty detects threats in your AWS account
- AWS Web Application Firewall can block threats at the perimeter using application-level rules
- Resource policies, such as for VPC endpoints and S3 buckets, define the conditions around which your resources can be accessed
- EventBridge and Step Functions can craft automated responses to threats

. . . all without having to change your application code!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Additional resources

- AWS Security Blog
  https://aws.amazon.com/blogs/security/
- AWS Security Incident Response Guide
  https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide
- AWS Well-Architected Framework: Security Pillar
  https://docs.aws.amazon.com/wellarchitected/latest/security-pillar
- Guidelines for Implementing AWS WAF
  https://d1.awsstatic.com/whitepapers/guidelines-implementing-aws-waf.pdf
- AWS WAF Security Automations Framework
  https://aws.amazon.com/solutions/implementations/aws-waf-security-automations/

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

J. Michael
jbako@amazon.com

Faisal Farooq
faifar@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.