Building a comprehensive security solution with AWS Security services

Michael Leighty

Sr. Solutions Architect- Edge Services
Amazon Web Services

Mun Hossain

Principal - Network & Application Security
Amazon Web Services

© 2023, Amazon Web Services, Inc. or its affiliates.

Agenda

- Benefits of Integrating Security Services
- Use Cases
- Automation techniques
- Call to Action

AWS Security Services

Identity and access management

- AWS Identity and Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager

Detective controls

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender

Infrastructure protection

Network Edge Protection

- AWS Network Firewall
- AWS Shield
- AWS WAF

- Amazon VPC
- AWS PrivateLink
- AWS Systems Manager

Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident response

- Amazon Detective
- Amazon EventBridge
- AWS Backup
- AWS Security Hub
- AWS Elastic Disaster Recovery

Compliance

- AWS Artifact
- AWS Audit Manager

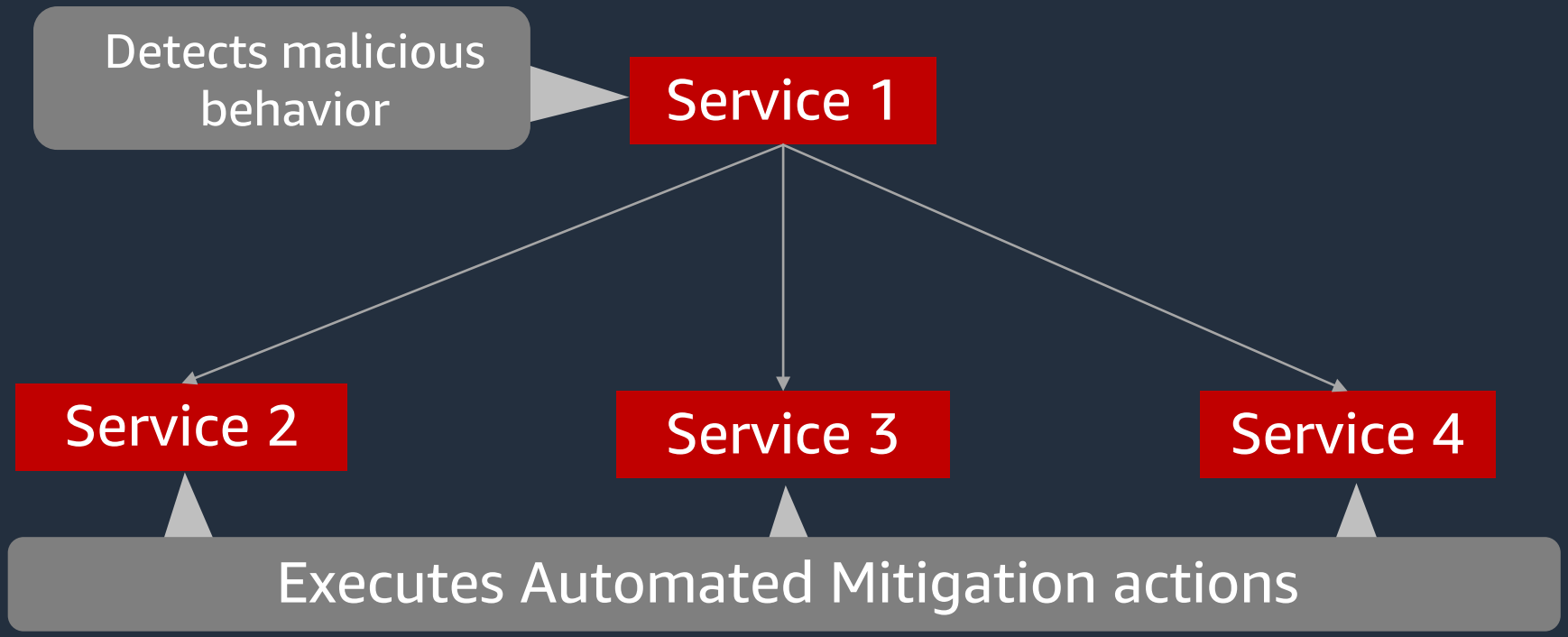
© 2023, Amazon Web Services, Inc. or its affiliates.

Benefits of Integrating AWS Security Services

© 2023, Amazon Web Services, Inc. or its affiliates.

Benefits of Integrating AWS Security Services

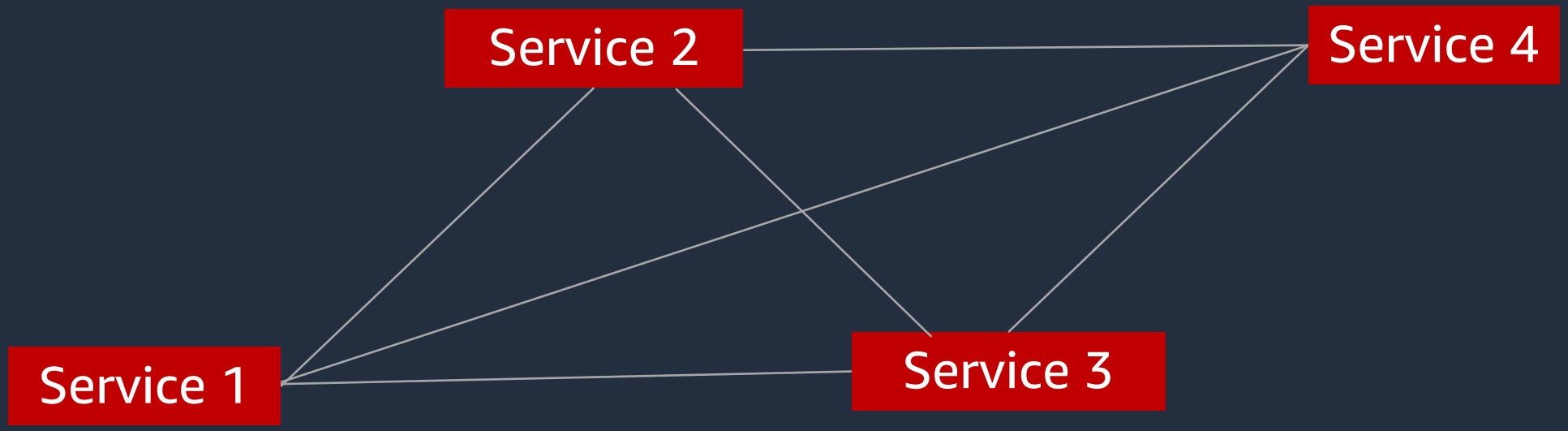
Distributed Mitigation Actions



aws
© 2023, Amazon Web Services, Inc. or its affiliates.

Benefits of Integrating AWS Security Services

Sharing of Threat Intel

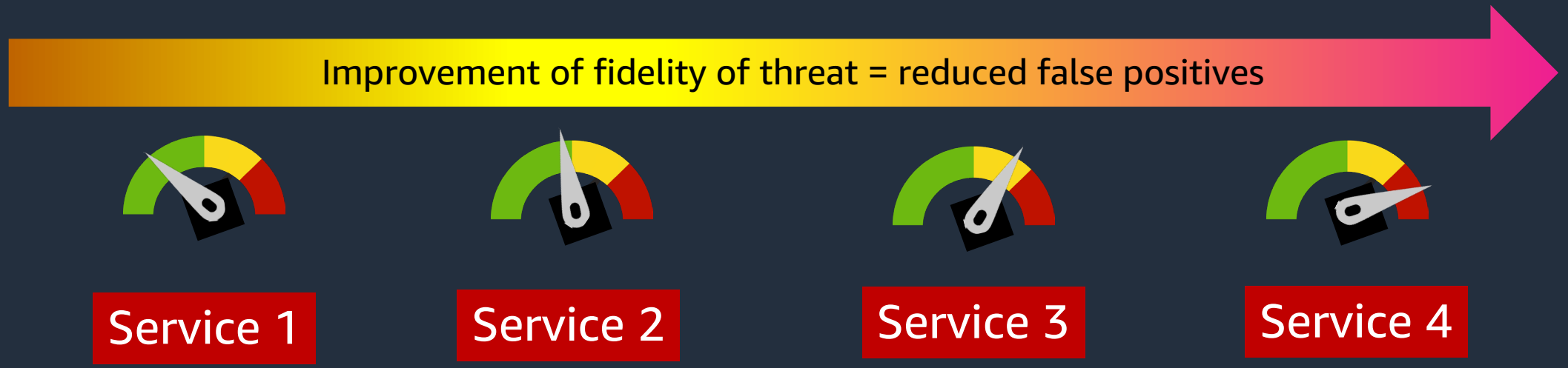


Sharing threat intel improves visibility

aws
© 2023, Amazon Web Services, Inc. or its affiliates.

Benefits of Integrating AWS Security Services

Correlation of Threat Intel

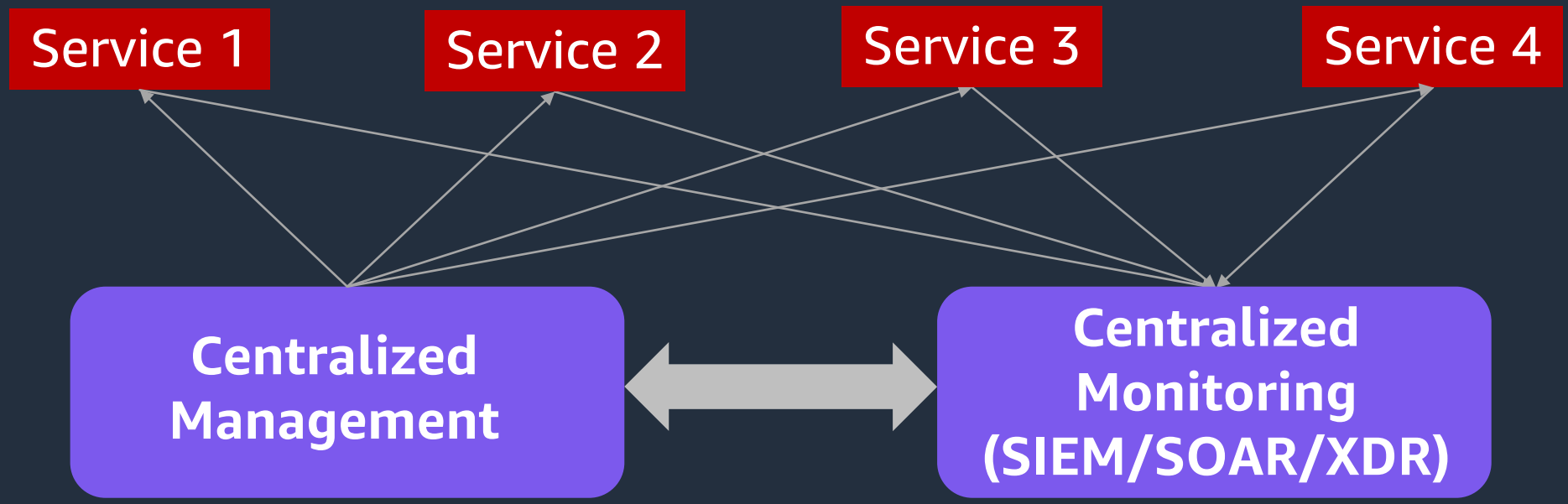


Alerts of same malicious activity detected by multiple services increases the fidelity of the event – reduces false positives

aws
© 2023, Amazon Web Services, Inc. or its affiliates.

Benefits of Integrating AWS Security Services

Centralized Management/Monitoring



Centralized management delivers consistent and scalable config options

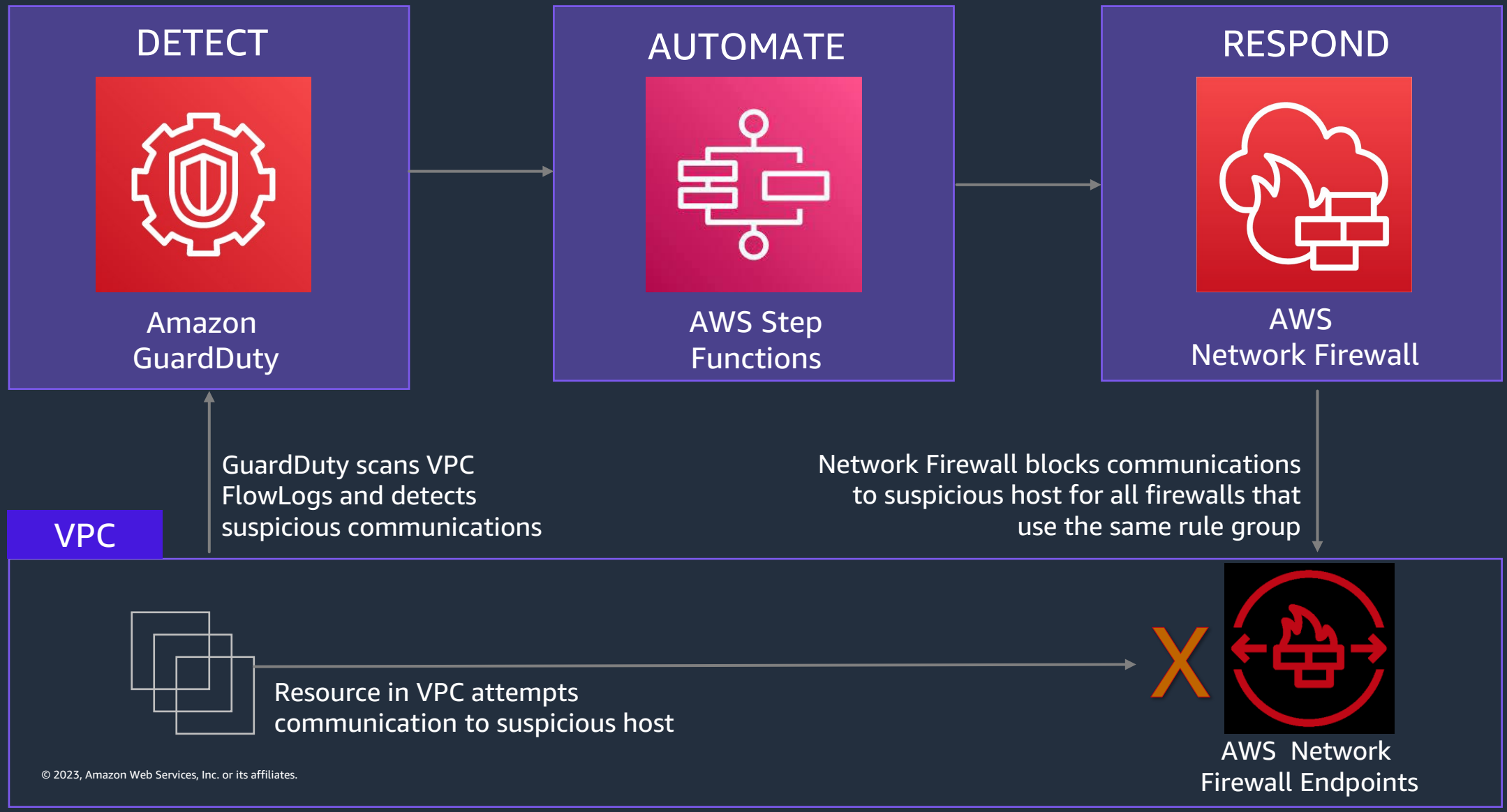
aws
© 2023, Amazon Web Services, Inc. or its affiliates.

Integrating AWS Security Services through automation techniques

© 2023, Amazon Web Services, Inc. or its affiliates.

Distributed Mitigation Actions via Shared Intel

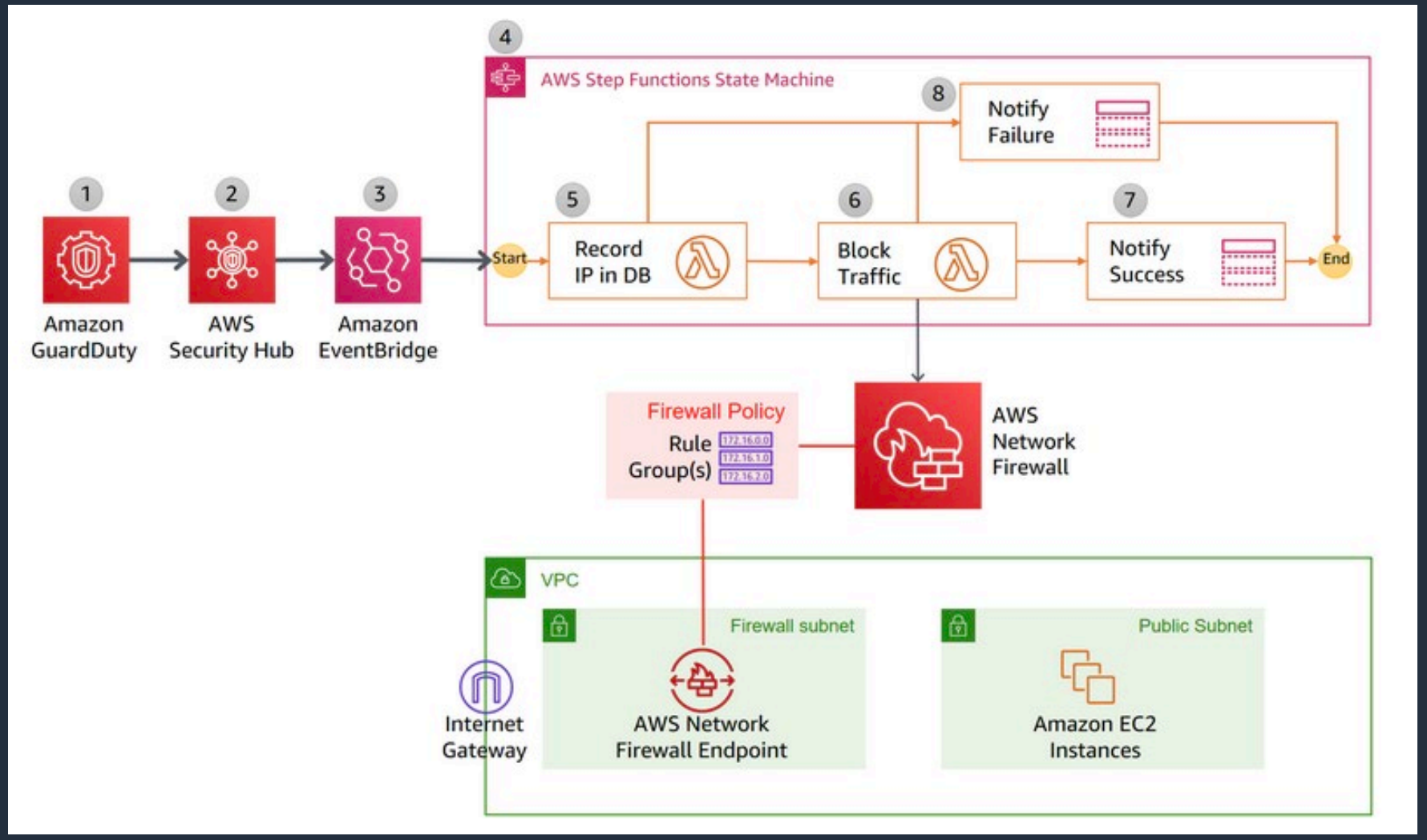
AWS Network Firewall + Amazon GuardDuty



© 2023, Amazon Web Services, Inc. or its affiliates.

Distributed Mitigation Actions via Shared Intel

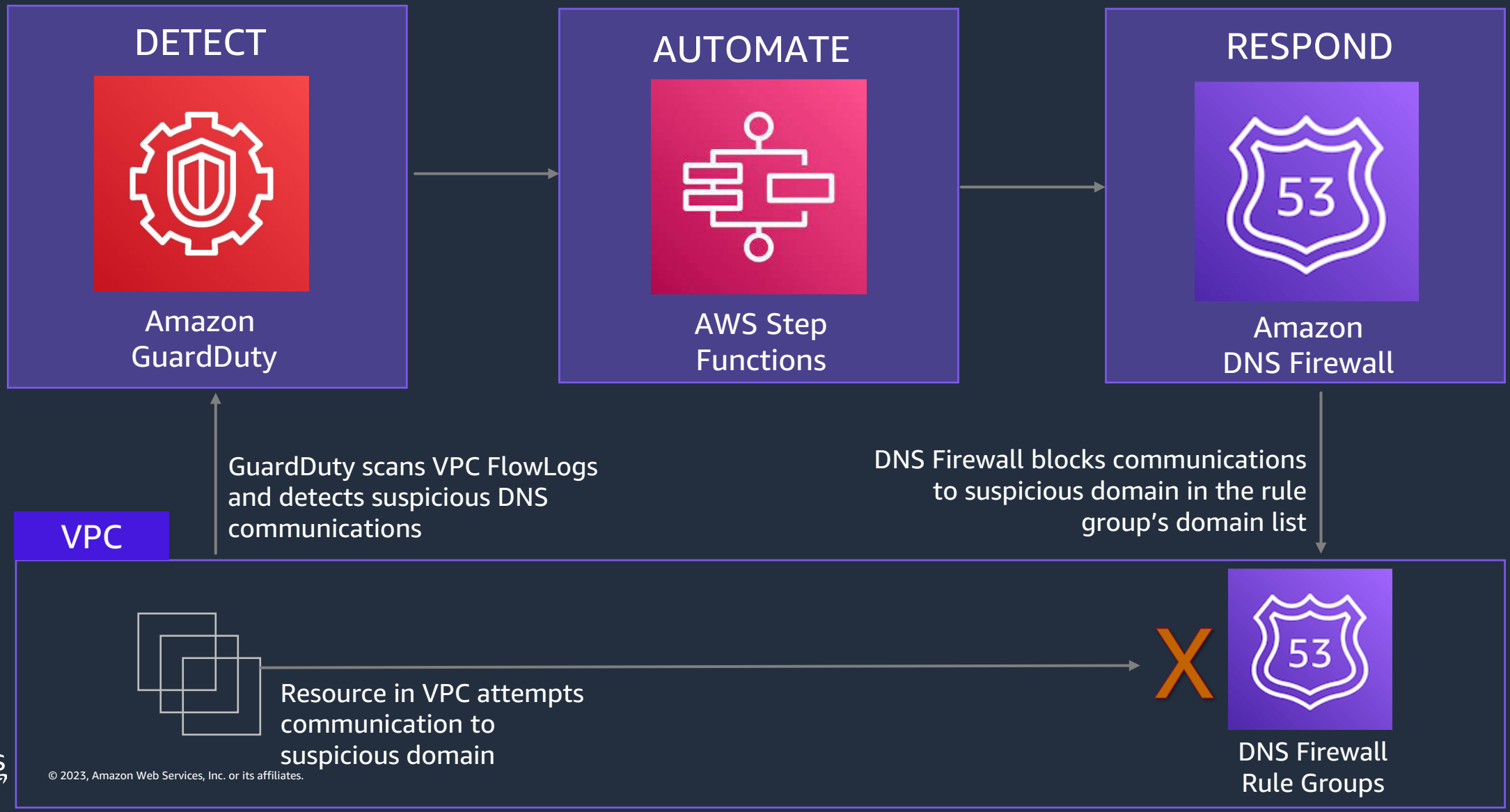
AWS Network Firewall + Amazon GuardDuty



© 2023, Amazon Web Services, Inc. or its affiliates.

Distributed Mitigation Actions via Shared Intel

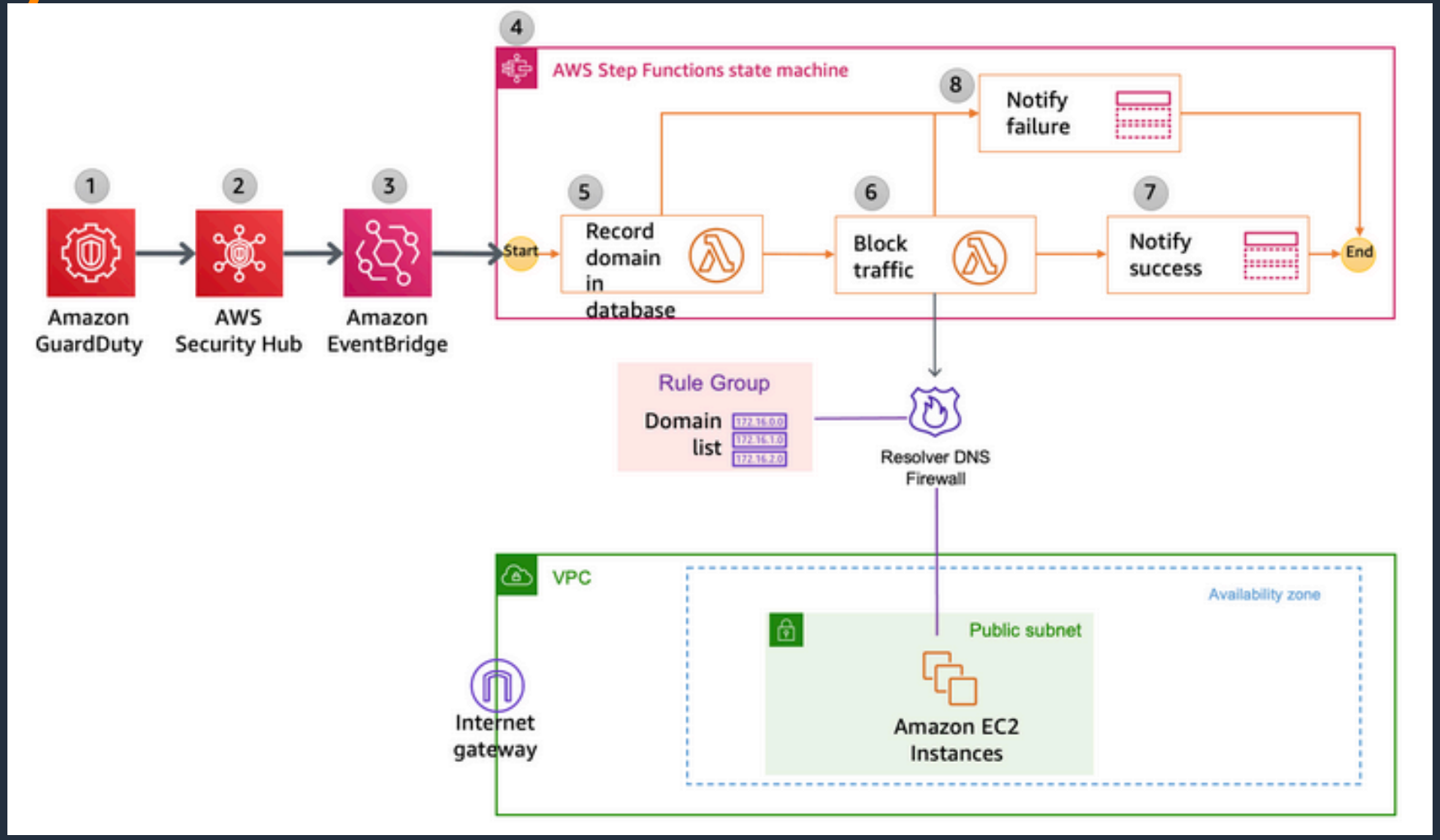
Amazon Route 53 Resolver DNS Firewall + Amazon GuardDuty



© 2023, Amazon Web Services, Inc. or its affiliates.

Distributed Mitigation Actions via Shared Intel

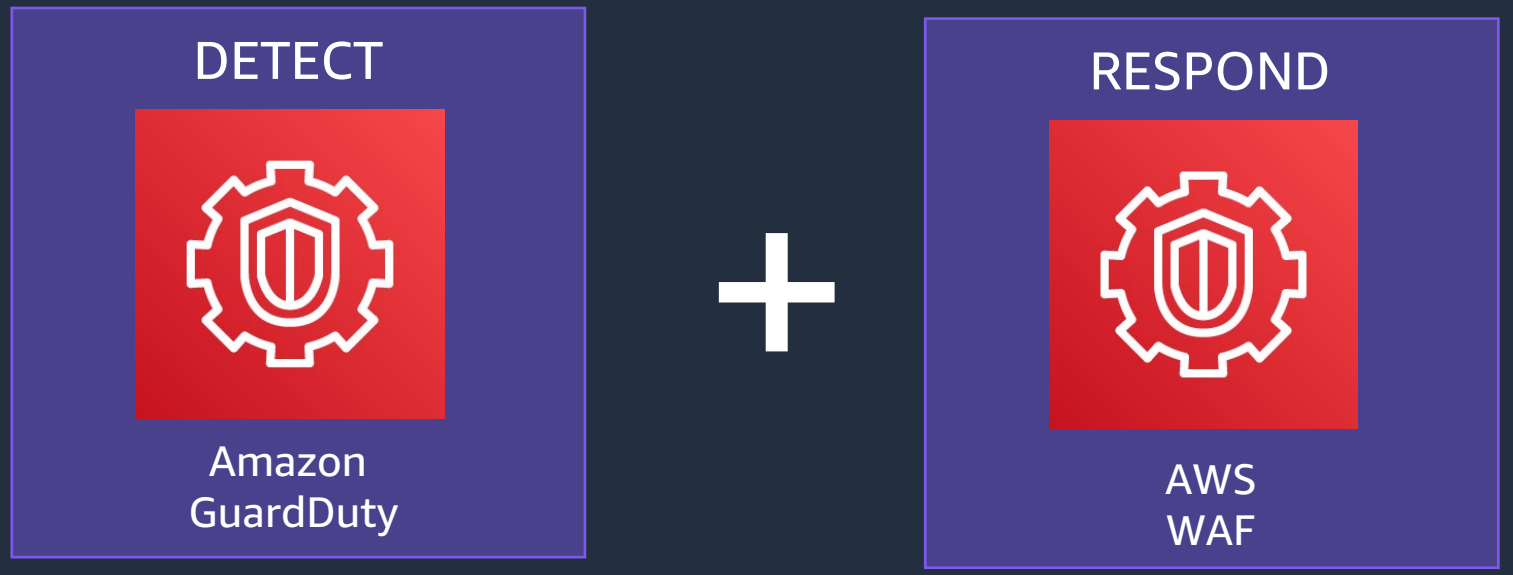
Amazon Route 53 Resolver DNS Firewall + Amazon GuardDuty



© 2023, Amazon Web Services, Inc. or its affiliates.

Distributed Mitigation Actions via Shared Intel

AWS WAF + Amazon GuardDuty

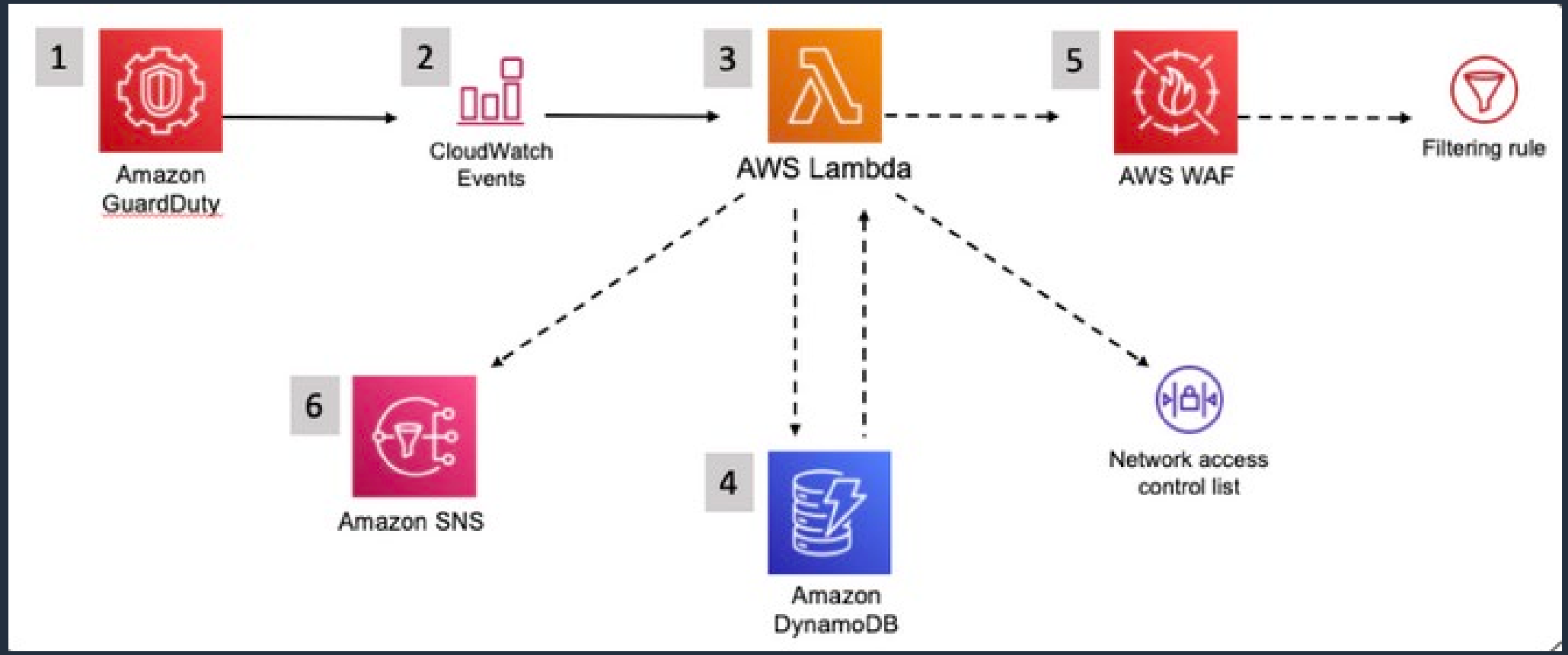


- Protection from L7 attacks destined to web applications using AWS WAF
- Inferences from Guard Duty influence triggers on Lambda
- Lambda functions are used to create Web ACL in AWS WAF and updates subnet network ACL
- AWS WAF rules actions can block, allow, rate limit, or instantiate CAPTCHA challenges upon detection of suspicious activity

aws
© 2023, Amazon Web Services, Inc. or its affiliates.

Distributed Mitigation Actions via Shared Intel

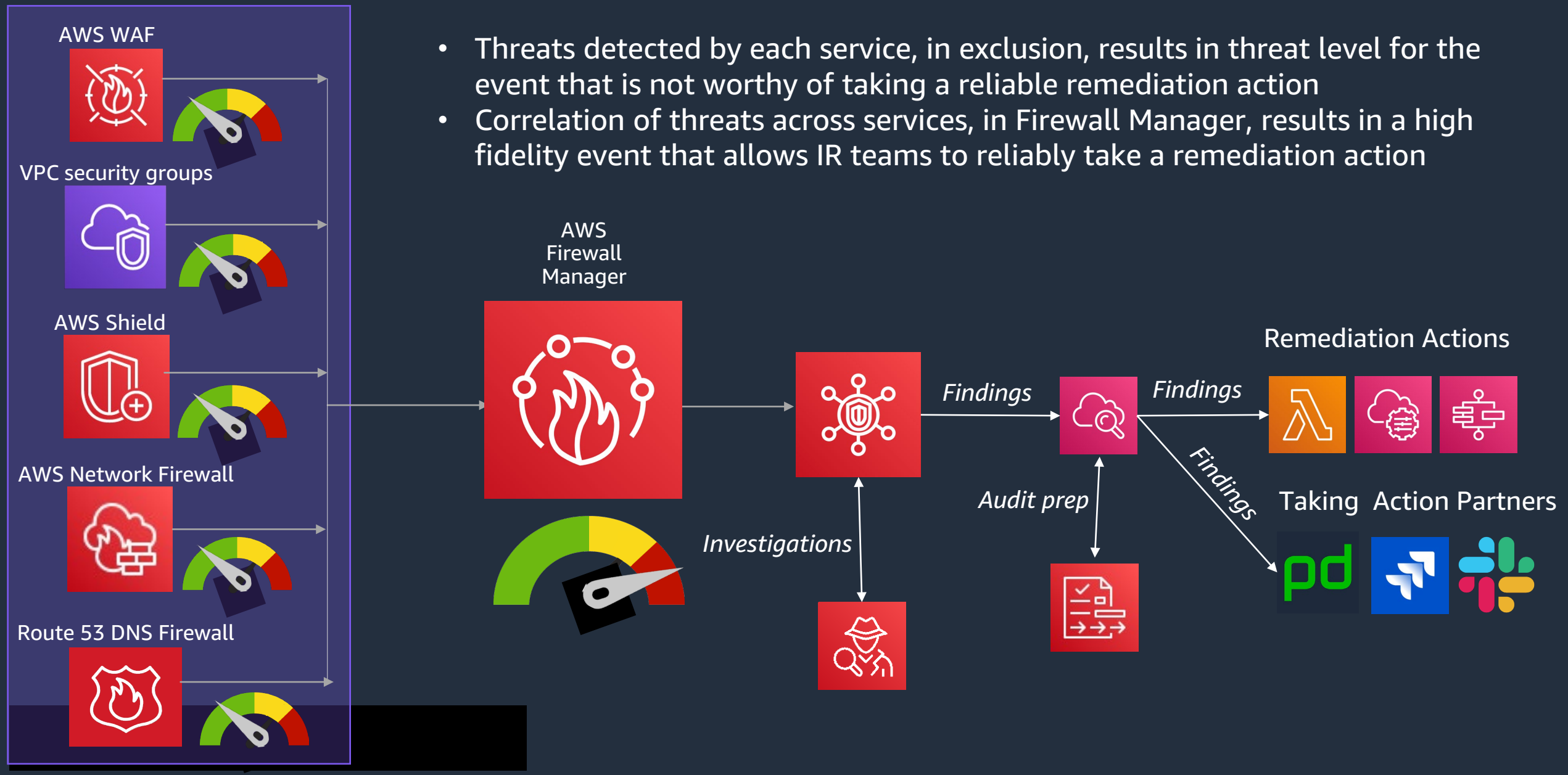
AWS WAF + Amazon GuardDuty



© 2023, Amazon Web Services, Inc. or its affiliates.

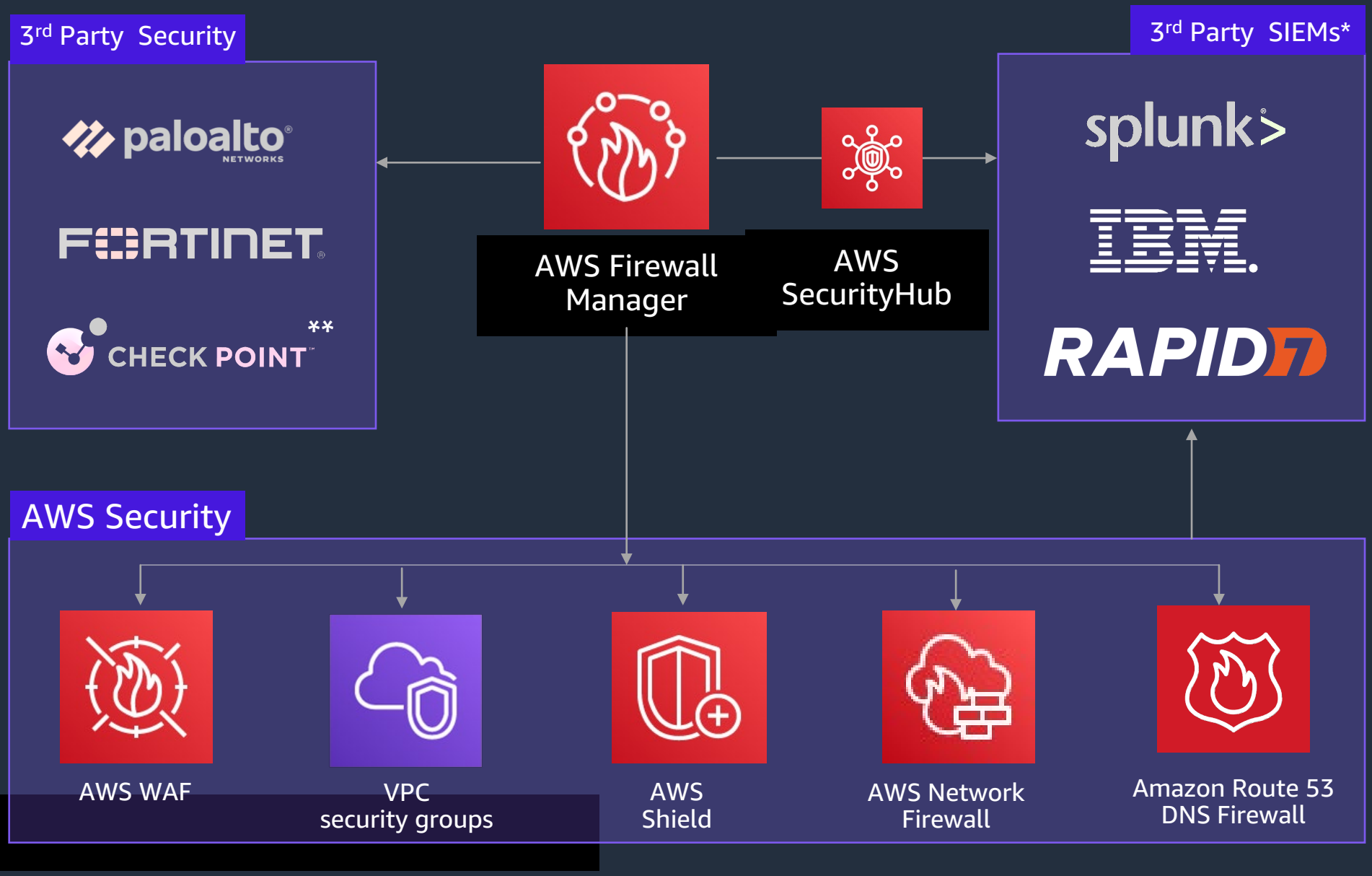
Correlation of Threat Intel

- Threats detected by each service, in exclusion, results in threat level for the event that is not worthy of taking a reliable remediation action
- Correlation of threats across services, in Firewall Manager, results in a high fidelity event that allows IR teams to reliably take a remediation action



Centralized Management and Monitoring

Integration of AWS Firewall Manager with AWS Security & 3rd Parties



- Centrally enable baseline security using AWS WAF, Shield, and VPC security groups across your organization
- Consistently enforce the protections, even as new applications are created
- View perimeter protection posture centrally across your AWS accounts
- Expand deployments to include 3rd party security solutions

Call to action

1. BLOG: Automatically block suspicious traffic with AWS Network Firewall and Amazon GuardDuty
2. BLOG: Automatically block suspicious DNS activity with Amazon GuardDuty and Route 53 Resolver DNS Firewall
3. BLOG: How to use Amazon GuardDuty and AWS WAF v2 to automatically block suspicious hosts
4. AWS Firewall Manager | https://aws.amazon.com/firewall-manager/

© 2023, Amazon Web Services, Inc. or its affiliates.

Thank you!

Michael Leighty
mleighty@amazon.com

Mun Hossain
munahoss@amazon.com

© 2023, Amazon Web Services, Inc. or its affiliates.