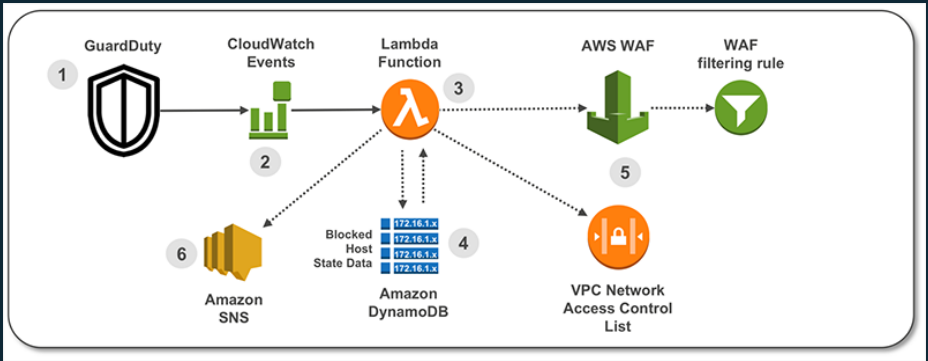
Automate Threat Mitigation Using AWS WAF and Amazon GuardDuty



Alex Tomic, AWS Solutions Architect
Cameron Worrell, AWS Solutions Architect

Agenda

- Intro to AWS Security Services
- AWS Web Application Firewall (WAF)
- Amazon GuardDuty
- Response Automation Patterns
- Demo
- Next Steps and Resources

In AWS:

Move fast **AND** Stay secure

with automation

AWS security solutions

Identity

AWS Identity & Access Management (IAM)

AWS Organizations

AWS Cognito

AWS Directory Service

AWS Single Sign-On

Detective control

AWS CloudTrail

AWS Config

Amazon CloudWatch

Amazon GuardDuty

VPC Flow Logs

Infrastructure security

Amazon EC2 Systems Manager

AWS Shield

AWS Web Application Firewall (WAF)

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

Data protection

AWS Key Management Service (KMS)

AWS CloudHSM

Amazon Macie

Certificate Manager

Server Side Encryption

Incident response

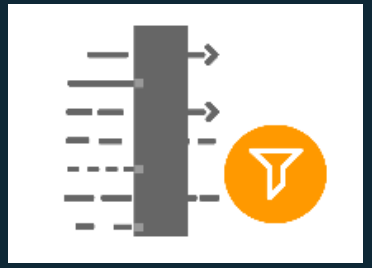
AWS Config Rules

AWS Lambda

aws

aws

What is AWS WAF?



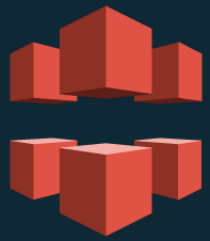
Web traffic filtering with custom rules

Malicious request blocking

Active monitoring and tuning

aws

AWS WAF available on



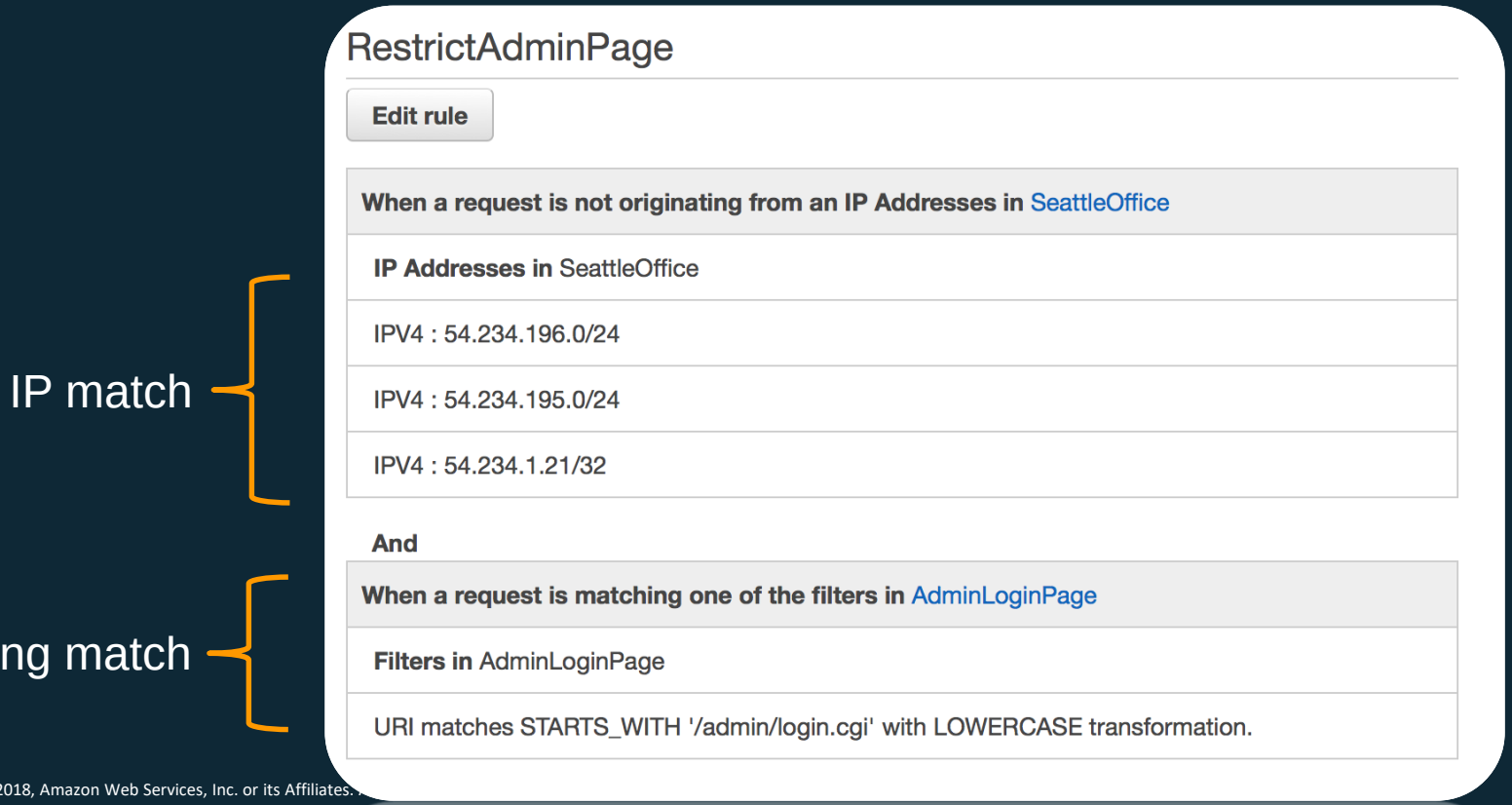
Amazon CloudFront
(Amazon's CDN)

Application Load Balancer
(ALB)

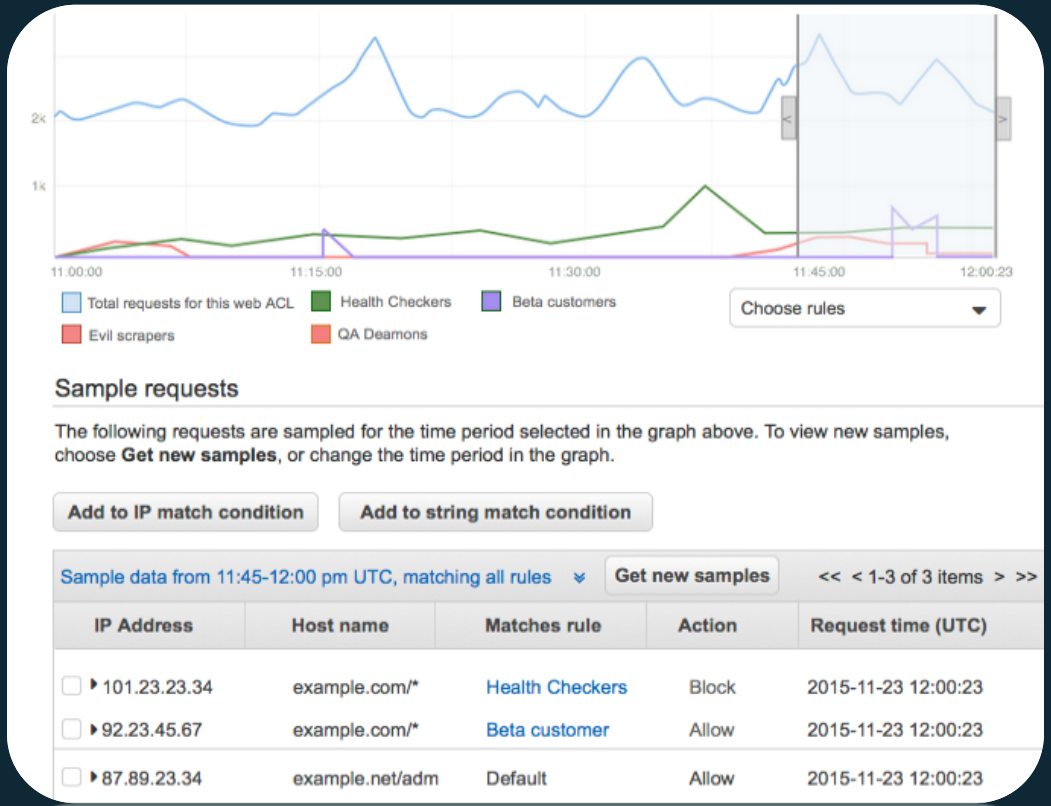
aws

Flexible Rule Language (Combine conditions)

Restrict a rule to specific URIs, such as the login page.



AWS WAF - Dashboard



aws

Introducing Amazon GuardDuty
Threat Detection and Notification

Enable GuardDuty

With a few clicks in the console, monitor your AWS accounts without additional security software or infrastructure to deploy or manage

Continuously analyze

Automatically analyze network and account activity at scale providing broad, continuous monitoring of your AWS accounts and workloads

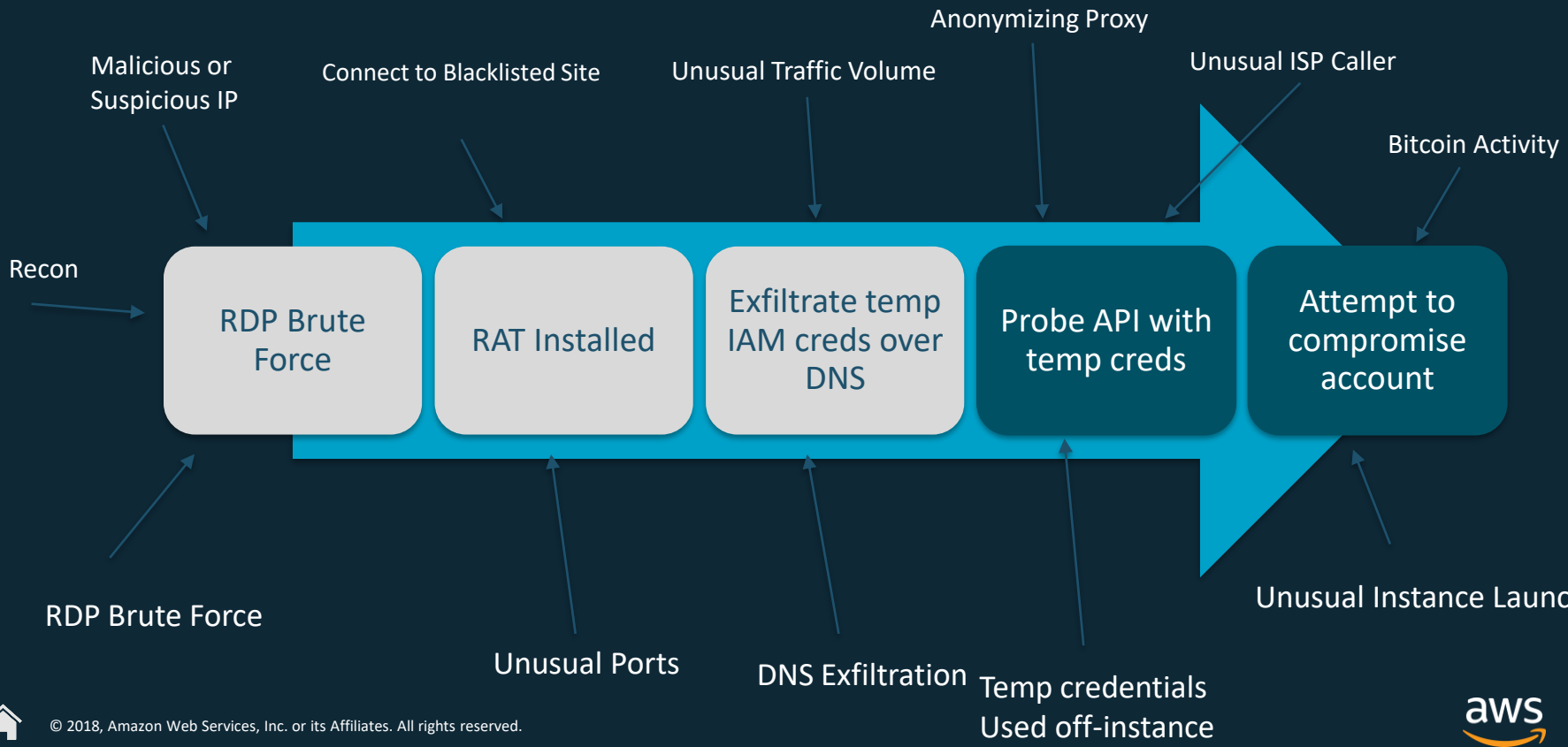
Intelligently detect threats

Utilize managed rule-sets, integrated threat intelligence, anomaly detection, and machine learning to intelligently detect malicious or unauthorized behavior

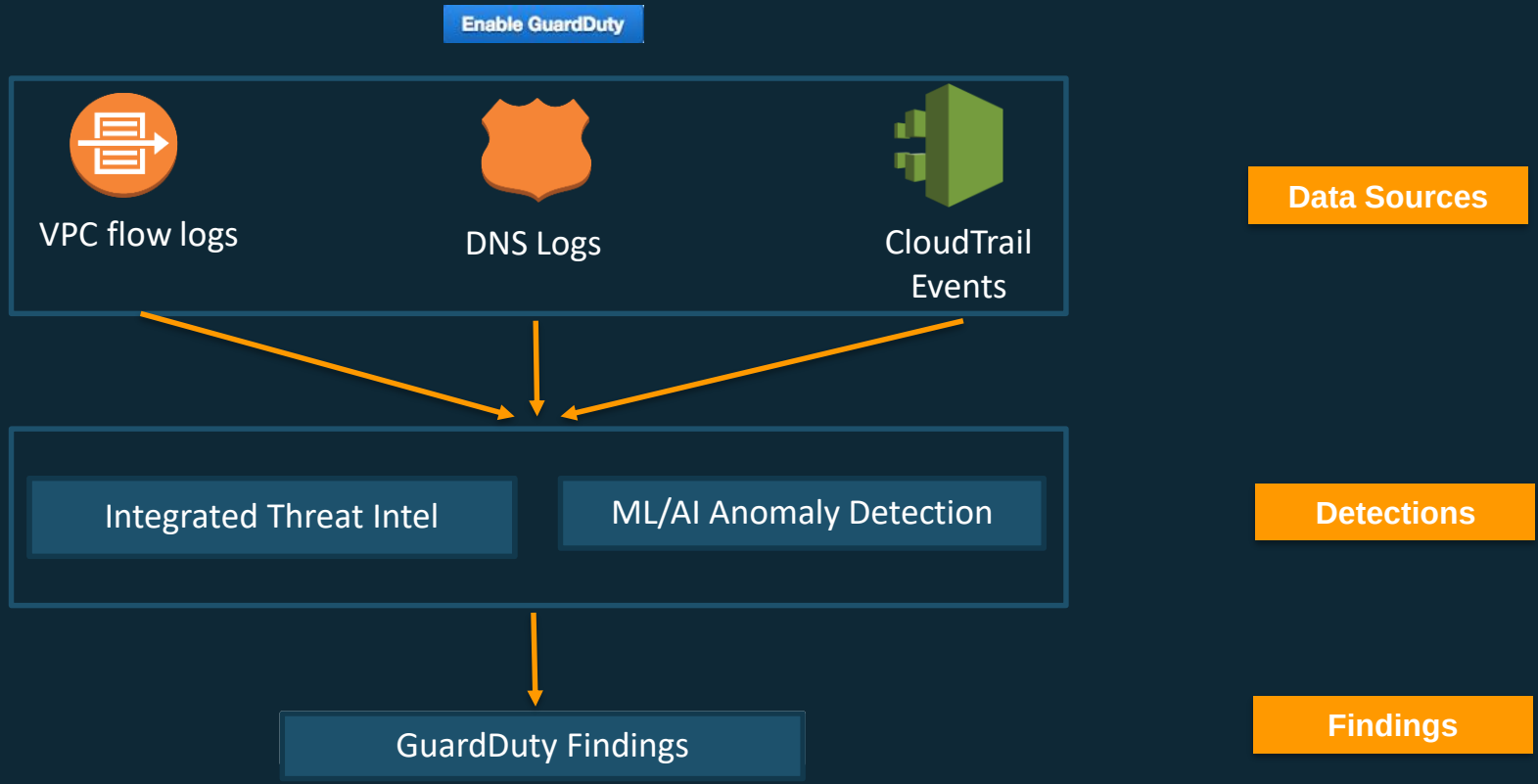
Leverage actionable alerts

Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

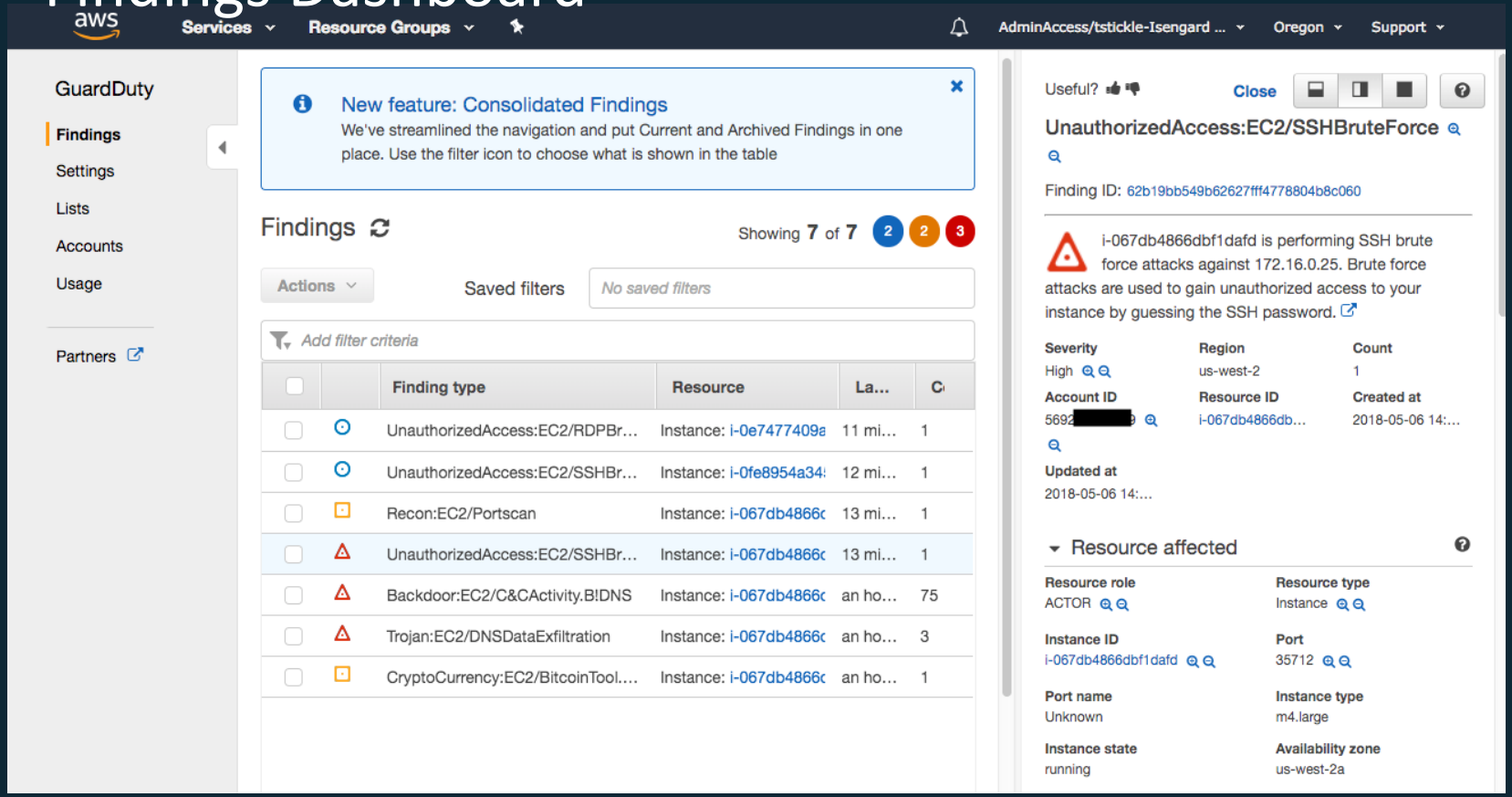
Covering the Attackers Kill Chain



How Does Amazon GuardDuty Work?

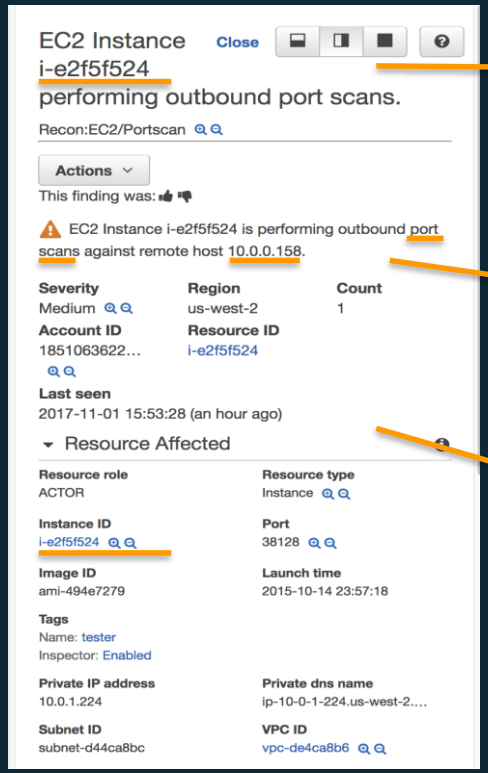


Findings Dashboard

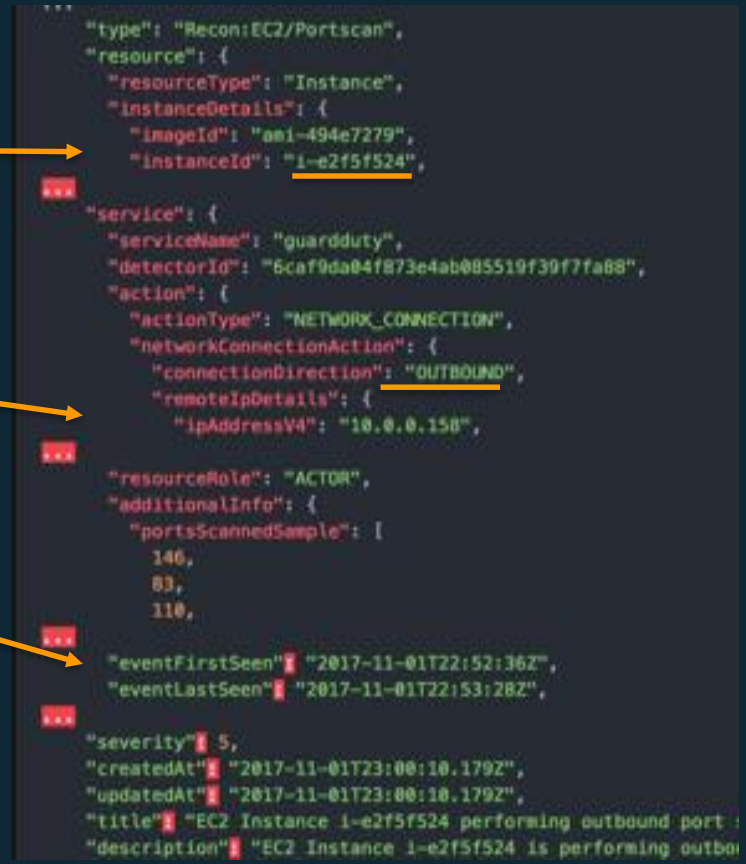


Findings Formats

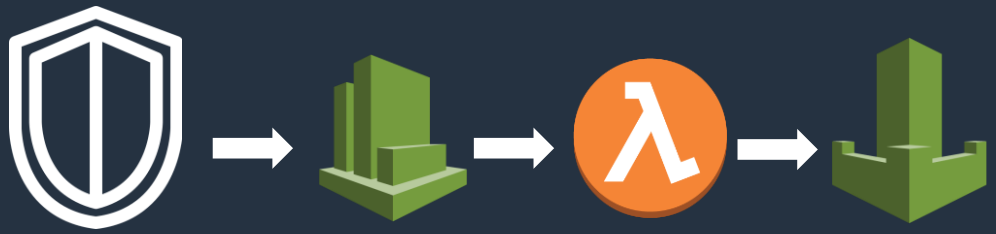
AWS Management Console



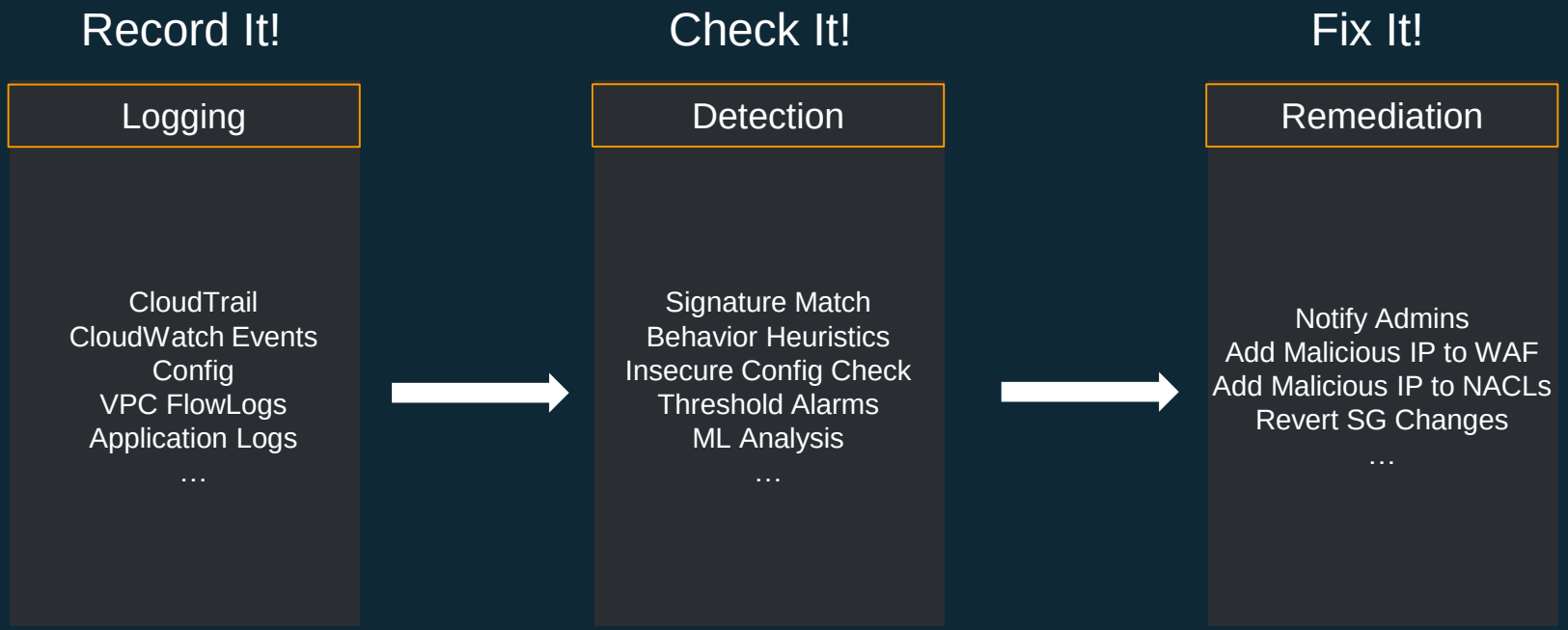
API / JSON Format



Response Automation Patterns



Automated Response Pattern



Automated Response Pattern

Record It!

Logging

GuardDuty Findings are recorded in CloudWatch Events

Check It!

Detection

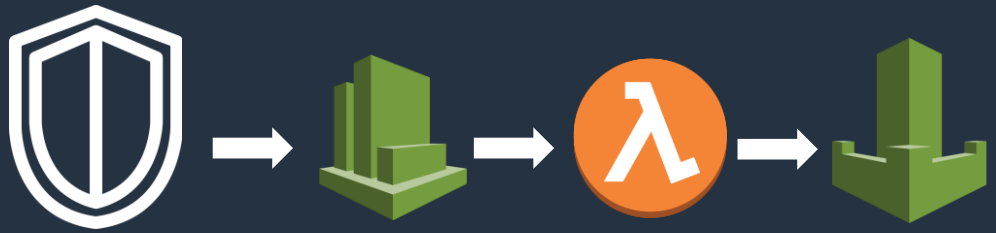
CloudWatch Event Rule routes GD findings to a Lambda function

Fix It!

Remediation

Lambda updates WAF ACL, VPC NACL and emails via SES

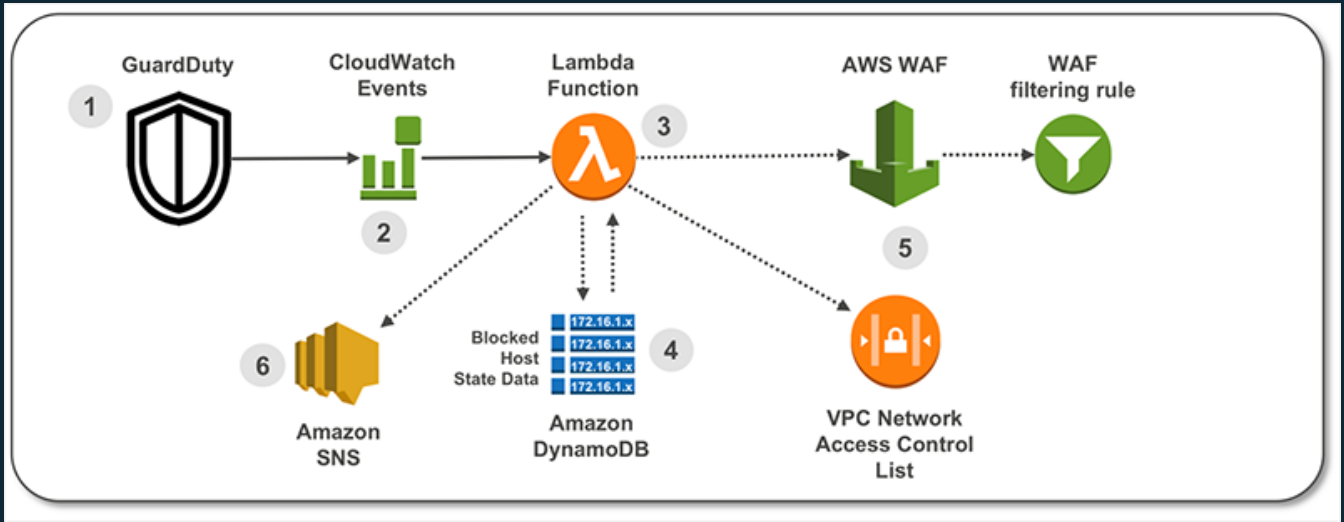
Demo Time!



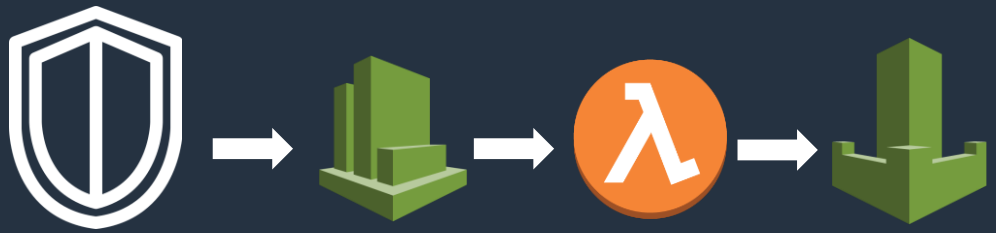
aws

Automated Response Pattern

Based on Blog Post: “How to use Amazon GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts”



Next Steps and Resources



WAF for Web App Protection

1. Easy to deploy

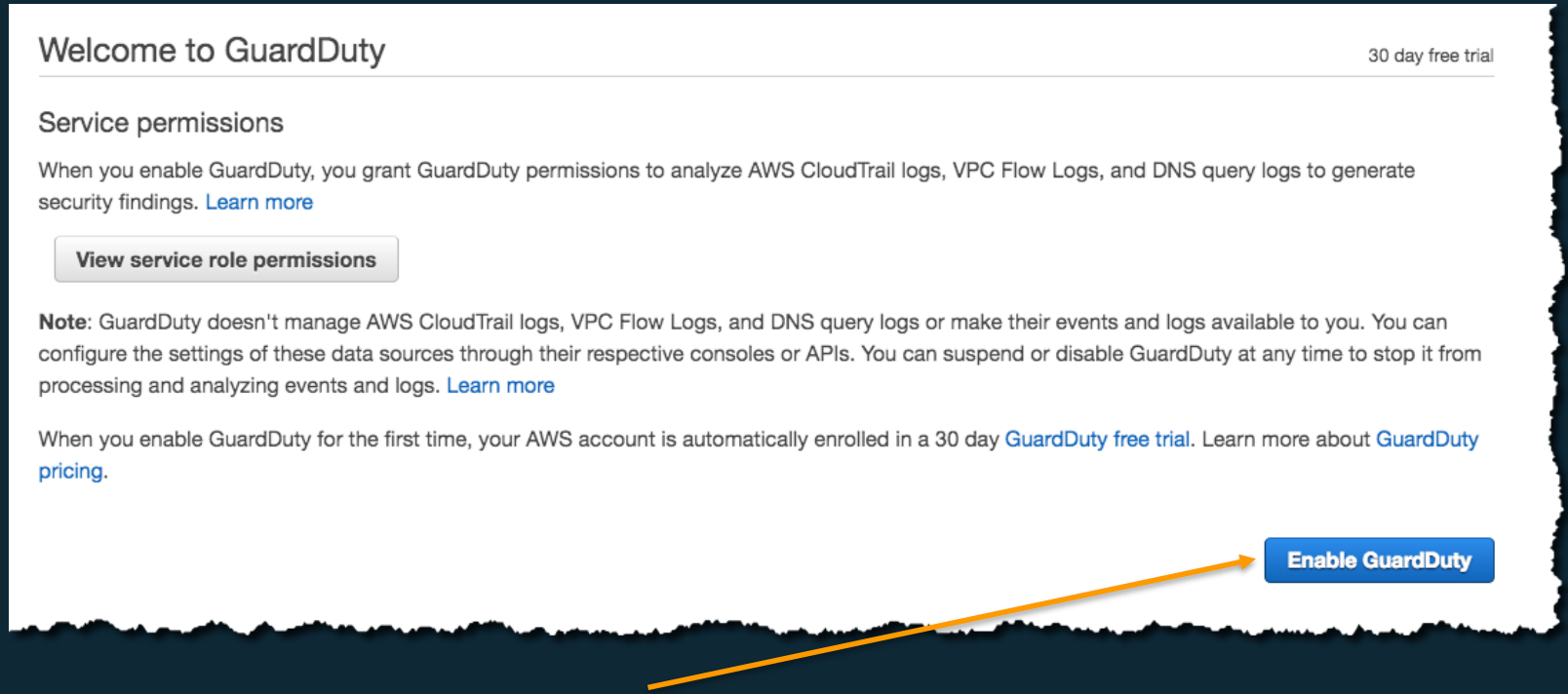
2. Fast Incident Response

3. Affordable

4. Full API Support

5. Managed Service

Turn On GuardDuty!



Review the Blog Post

AWS Security Blog

How to use Amazon GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts

by Cameron Worrell, Alex Tomic, and Sundar Jayashekar | on 03 AUG 2018 | in Amazon GuardDuty, AWS WAF, Security, Identity, & Compliance | Permalink | Comments | Share

When you're implementing security measures across your AWS resources, you should use a holistic approach that incorporates controls across multiple areas. In the Cloud Adoption Framework (CAF) Security perspective whitepaper, we define these controls across four categories.

- **Directive controls**. Establish the governance, risk, and compliance models the environment will operate within.
- **Preventive controls**. Protect your workloads and mitigate threats and vulnerabilities.
- **Detective controls**. Provide full visibility and transparency over the operation of your deployments in AWS.
- **Responsive controls**. Drive remediation of potential deviations from your security baselines.

aws

Links to More Resources:

- How to use Amazon GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts: https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/
- GitHub repo: https://github.com/aws-samples/amazon-guardduty-waf-acl

- AWS WAF Documentation: https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html
- AWS GuardDuty Documentation: https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

Thank You!