AWS re:Invent

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

SEC207-R2

What's new with AWS threat detection services

Ryan Holland
Senior Manager GuardDuty Security Response
AWS

Himanshu Verma
Worldwide Security Specialist
AWS

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

Let’s raise the bar

Deployment at scale

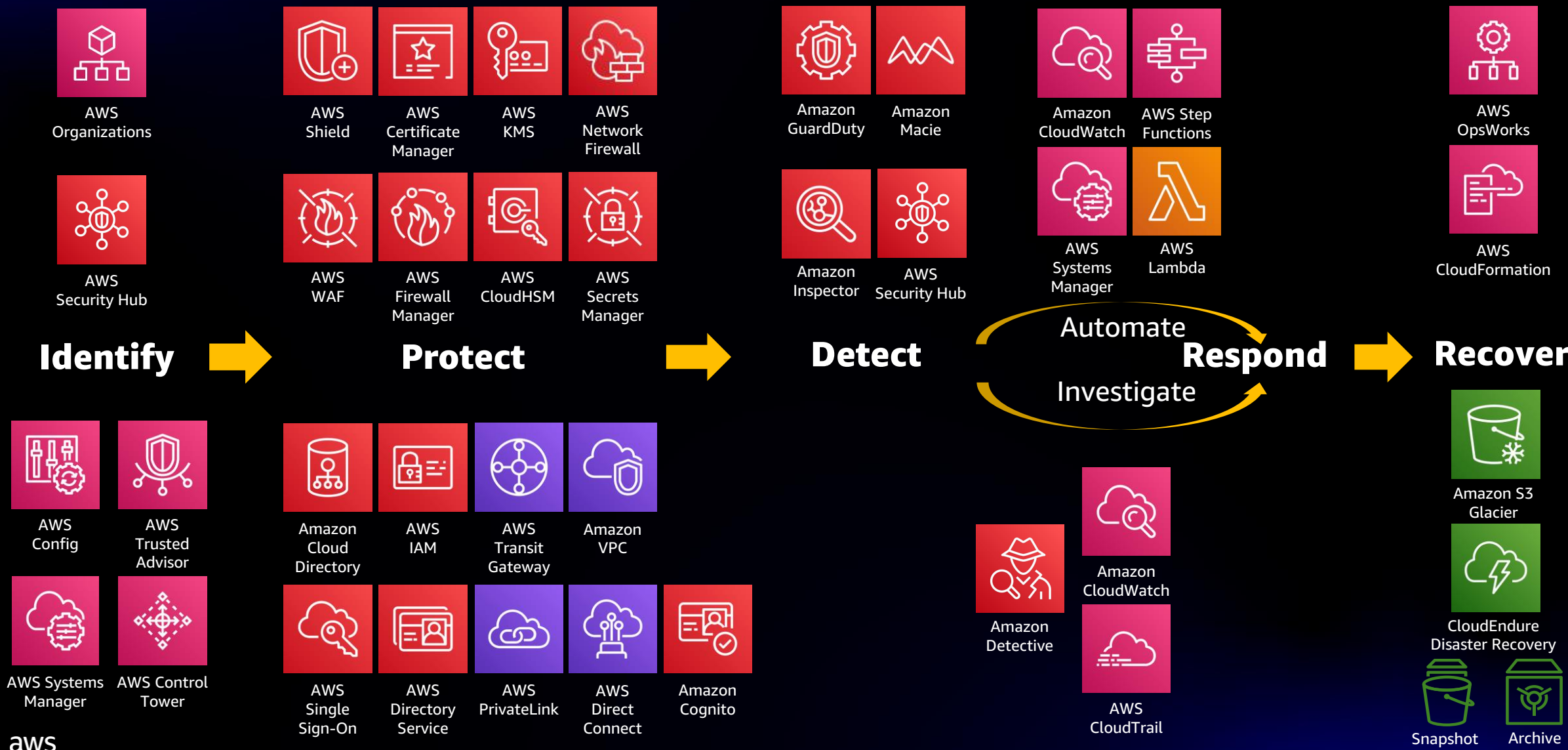
Best practices for continuous monitoring

Detection of threats, vulnerabilities, and suspicious events

How to automate response and remediation

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

AWS foundational and layered security services



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

Threat detection, monitoring, and response



Security monitoring and threat detection

Amazon EC2

AWS Identity and Access Management (IAM)

Amazon Simple Storage Service (S3)

Amazon GuardDuty

Detect threats and anomalous behavior

Amazon Macie

Discover sensitive data

Amazon Inspector

Detect vulnerabilities

AWS Security Hub

Centralized monitoring and security posture management

"Take Action"

Investigate events/findings

Amazon Detective

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

Deployment at scale

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

Scalable and centralized management

BUILT-IN INTEGRATION WITH AWS ORGANIZATIONS

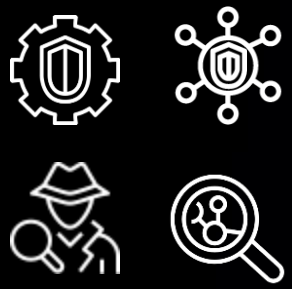
Administrator/member setup



- Designate a centralized delegated administrator



- Add all member accounts



- Auto-enable services on all member accounts

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

Visibility across AWS Regions

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

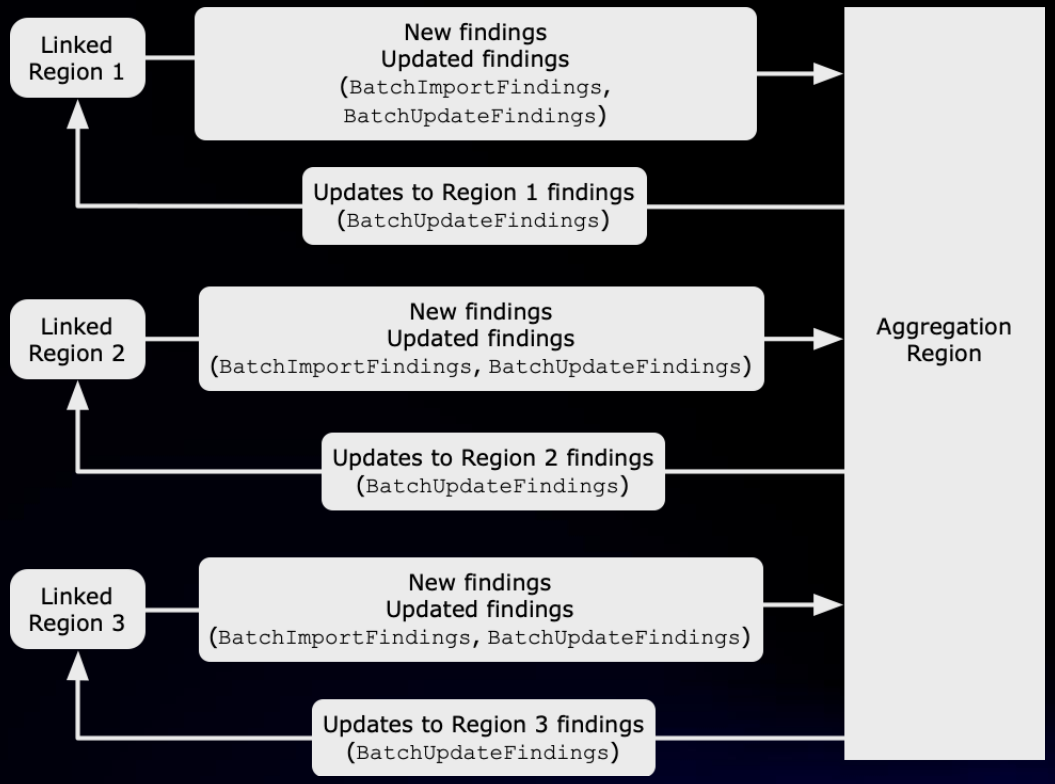
Cross-Region finding aggregation in AWS Security Hub

SIMPLIFY HOW YOU EVALUATE AND IMPROVE YOUR AWS SECURITY POSTURE

Requires
- Aggregation Region
- Linked Regions

New, updated findings replicate to aggregation Region

Updates replicated from aggregation Region to linked Regions



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

Acting on findings

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

Operationalize Amazon GuardDuty findings

Prioritizing GuardDuty operationalization

- Instance credential exfiltration
- Command and control
- Tor usage
- Domain reputation
- Cryptocurrency
- EMR port probe
- Denial of service
- Root credential usage

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

Operationalize anomaly findings

It’s possible that the activity is **unusual but benign**

Use Amazon Detective to dive deeper into user activity before and after the finding

Some possible automations

- Is the **country or ASN somewhere unexpected** for your users?
- Does the finding indicate **failed requests or access to sensitive APIs**?

Implement a workflow to **notify the user** impacted for verification

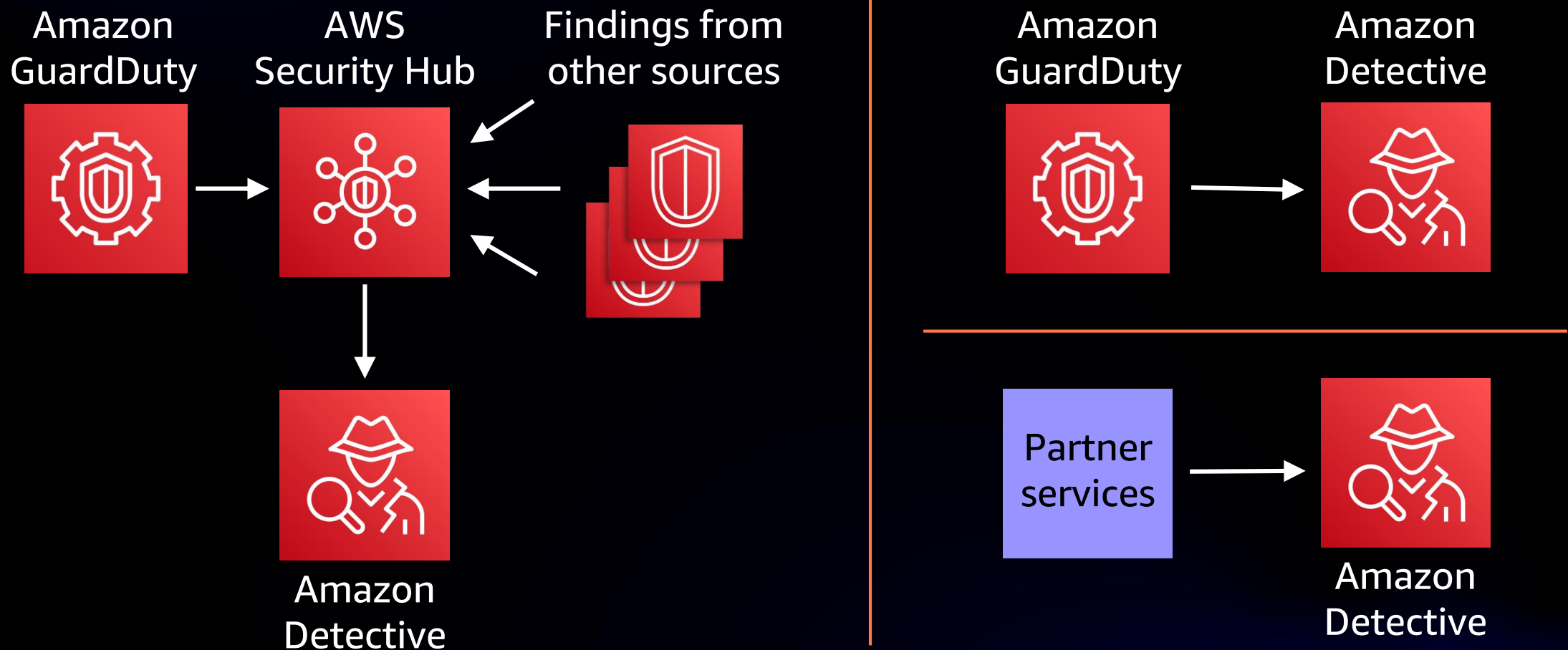
aws

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

Investigating events

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

Using Amazon Detective for investigation



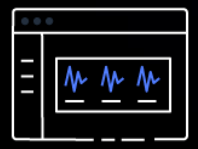
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Managing vulnerabilities

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

Amazon Inspector

Automated and continuous vulnerability management at scale



Gain centralized visibility

- Environment coverage
- High impact findings
- Resources by finding severity



One-click continuous monitoring

- Automatic discovery of resources
- Monitors throughout the resource life-cycle



Prioritize with contextualized scoring

- Inspector Risk score
- Security metrics
- Customized views



Centrally manage at scale

- AWS Organizations
- Package vulnerability, network reachability
- Environment coverage



Automate and take actions

- Management APIs
- Detailed findings in EventBridge
- Security hub integration

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

Automation for response and remediation

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

Security Hub – response and remediation



Enable **automated remediation** for high-severity configuration findings



Use **custom actions** to invoke runbooks for automated response



Use **partner integrations** to consolidate and normalize security findings



Integrate with **ticketing and workflow** tools

aws

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

Thank you!

Ryan Holland

Himanshu Verma

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