# Demonstration of threat detection operationalization best practices

**Himanshu Verma**
Principal Worldwide Security Specialist

Modern applications need…

# Better visibility and security posture

Increase operational efficiency for your cloud-based workloads and applications

Improve visibility

Enhance security posture

Modern applications need…

# Continuously integrated security

Integrate AWS security services to achieve continuous threat detection, optimized route workflows, and minimal remediation time

Empower SecOps and DevOps teams to unify visibility and automate responses to help them achieve operational excellence in cloud security

# Best practices we will cover

1 Deployment at scale

2 Aggregated and continuous monitoring

3 Detection of threats, vulnerabilities, and suspicious events

4 Automated response and remediation

# Deployment at scale

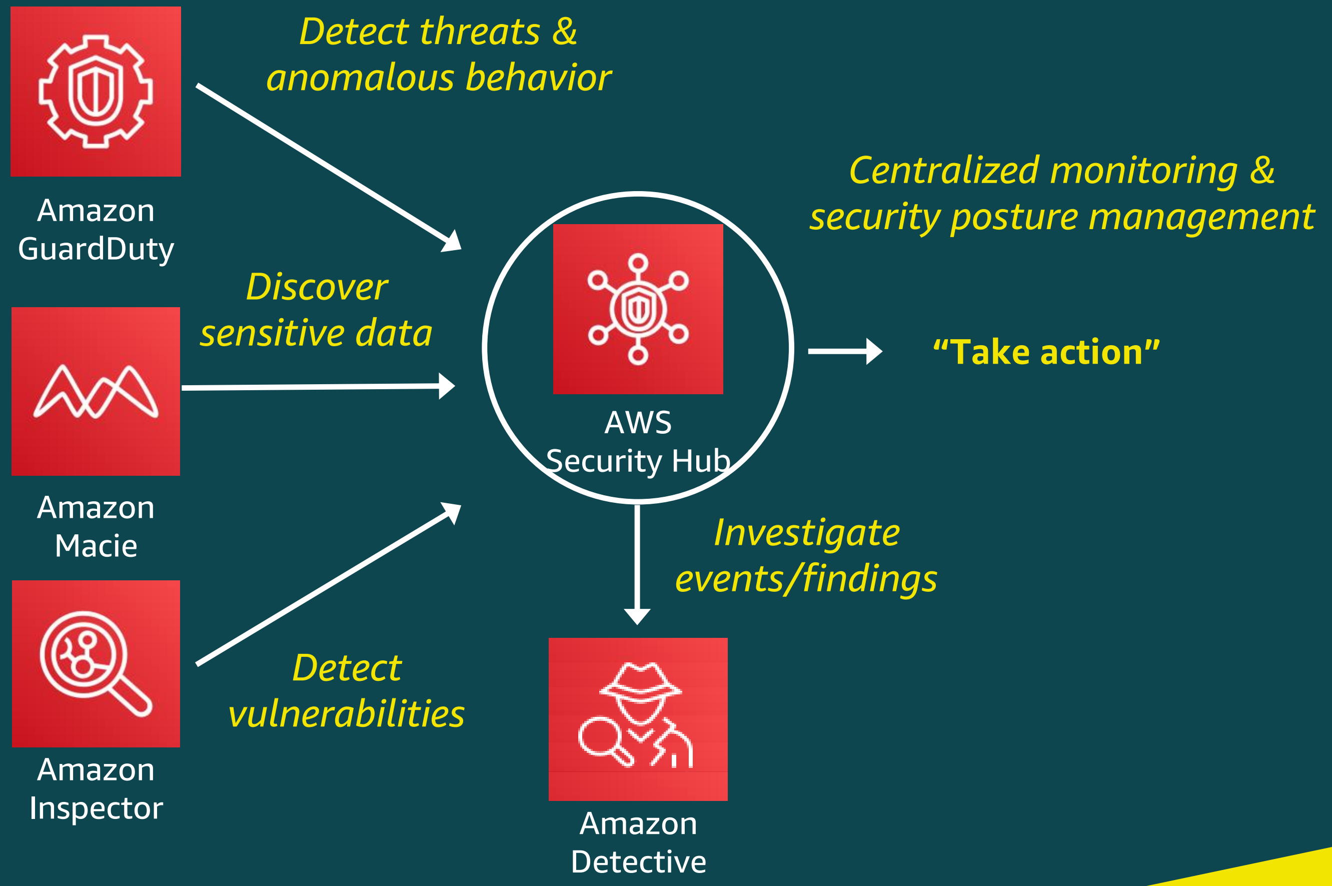
# Threat detection, monitoring, and response

## Security Monitoring and Threat Detection

Amazon EC2

AWS Identity and Access Management (IAM)

Amazon Simple Storage Service (S3)



Amazon GuardDuty

*Detect threats & anomalous behavior*

Amazon Macie

*Discover sensitive data*

Amazon Inspector

*Detect vulnerabilities*

AWS Security Hub

*Centralized monitoring & security posture management*

**"Take action"**

*Investigate events/findings*

Amazon Detective

# 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

# Detection of threats, vulnerabilities, and suspicious events

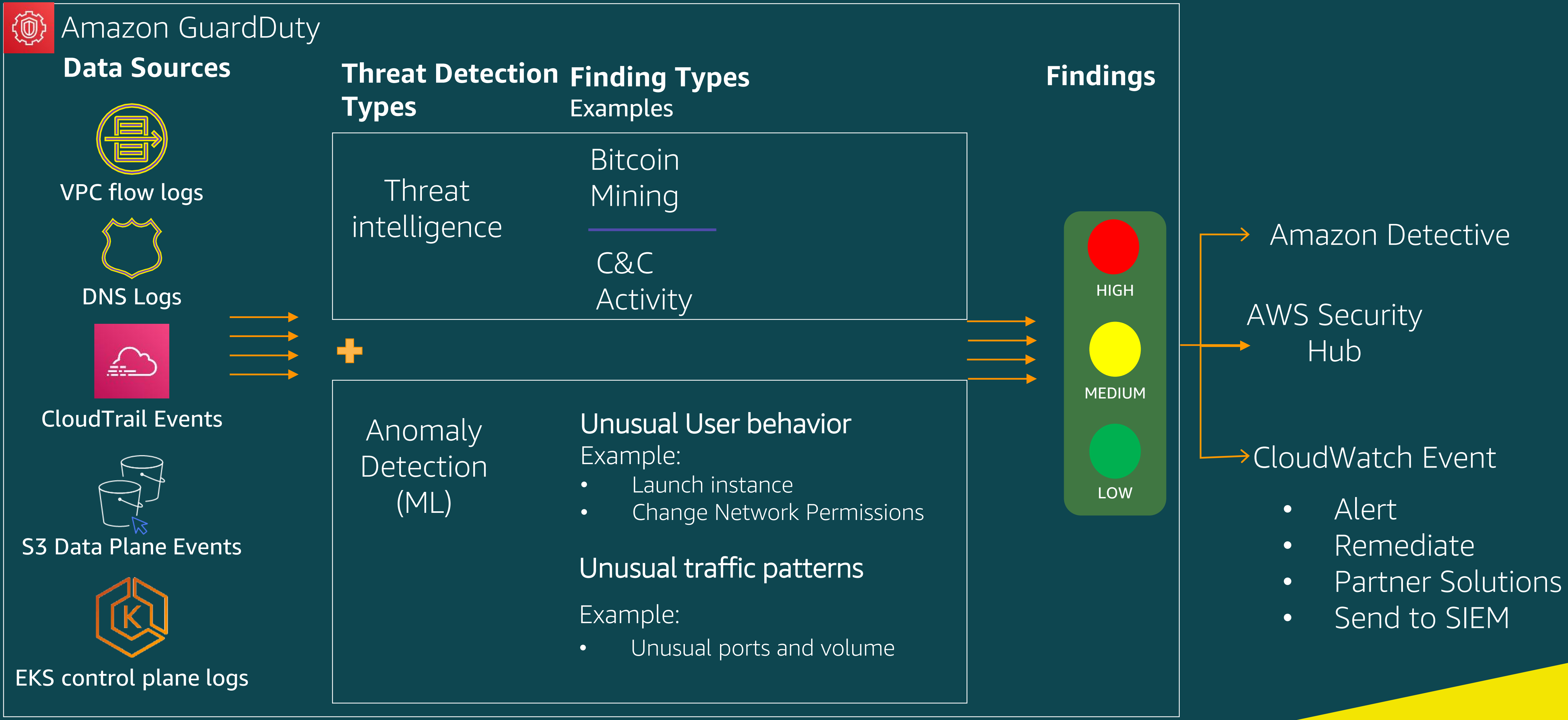
# Amazon GuardDuty

DETECT THREATS AND ABNORMAL ACTIVITY

## Protect your AWS accounts, workloads, and data with intelligent threat detection and continuous monitoring

- One-click activation with no performance impact
- Continuous monitoring of AWS accounts and resources
- Global coverage with regional results
- Detect known threats & unknown threats
- Enterprise-wide consolidation & management

# How Amazon GuardDuty works



Amazon GuardDuty

**Data Sources**

VPC flow logs

DNS Logs

CloudTrail Events

S3 Data Plane Events

EKS control plane logs

**Threat Detection Types**

**Finding Types**
Examples

Threat intelligence

Bitcoin Mining

C&C Activity

Anomaly Detection (ML)

Unusual User behavior
Example:
- Launch instance
- Change Network Permissions

Unusual traffic patterns

Example:
- Unusual ports and volume

**Findings**

HIGH

MEDIUM

LOW

Amazon Detective

AWS Security Hub

CloudWatch Event
- Alert
- Remediate
- Partner Solutions
- Send to SIEM

# Manage vulnerabilities

# 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

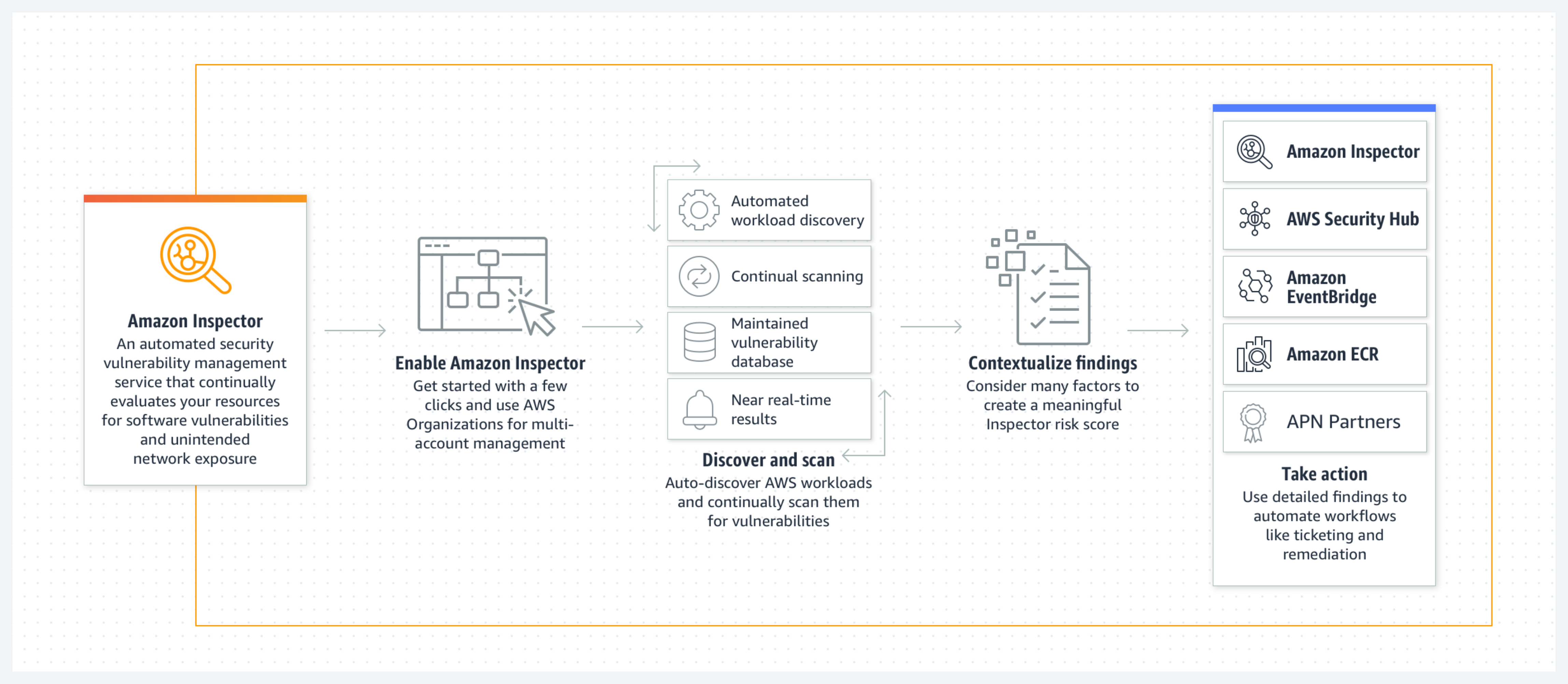
### Centrally manage at scale

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

### Automate and take actions

- Management APIs
- Detailed findings in Eventbridge
- Security Hub integration

# Amazon Inspector – How it works



**Amazon Inspector**
An automated security vulnerability management service that continually evaluates your resources for software vulnerabilities and unintended network exposure

**Enable Amazon Inspector**
Get started with a few clicks and use AWS Organizations for multi-account management

Automated workload discovery
Continual scanning
Maintained vulnerability database
Near real-time results

**Discover and scan**
Auto-discover AWS workloads and continually scan them for vulnerabilities

**Contextualize findings**
Consider many factors to create a meaningful Inspector risk score

**Take action**
Use detailed findings to automate workflows like ticketing and remediation

# Aggregated and continuous monitoring

# AWS Security Hub

CONTINUOUS SECURITY ASSESSMENT AND AUTOMATED RESPONSE

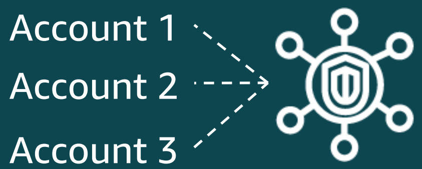
## Centrally view and manage security alerts and automate security checks across all AWS Accounts and Regions

Save time with aggregated findings

Improve security posture with automated checks

Curated security best practices

Seamless integration with standardized findings format



Multi-account support

# Using Security Hub to aggregate and prioritize

- View findings across multiple accounts and regions
- View findings for one resource from multiple sources
- Include findings from 3rd party products and your custom checks
- Security standards to help confirm best practice compliance

# Automated response & remediation

# Security Hub – response & 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

# Key takeaways

## ADVANCED THREAT DETECTION AND RESPONSE ON AWS

Security tools natively available in AWS

Reduce the burden for the security team

Centralized & scalable deployment with a click of a button

# Thank you!