Evolving beyond heroics for threat detection and incident response

Ryan Holland
Senior Manager GD Security Response
AWS

Bill Shinn
Sr. Principal, Office of CISO
AWS
External security services

- Amazon GuardDuty
- Amazon Detective
- AWS Security Hub
- Amazon Inspector
- Amazon Macie
Reduce time to respond

Know your environment

• Know which accounts are production vs. non-production
• Document account ownership and its sensitivity

Use tagging consistently

• Useful for identifying the owner of an impacted resource
• Know instance purpose, data sensitivity, and availability requirements

Use delegated administrator and auto-enable feature
GuardDuty best practices

1 Identify and suppress expected or benign activity
Prioritize by severity but do not simply ignore low or medium findings
Operationalization is key
Use Security Hub or Amazon EventBridge for finding delivery
Define runbooks and response actions based on finding categories
Start small and expand your automation and response strategy
GuardDuty best practices

Use Amazon Detective for investigation
Prioritizing GuardDuty operationalization

- Instance credential exfiltration
- Command and control
- Tor usage
- Domain reputation
- Cryptocurrency
- EMR port probe
- Denial of service
- Root credential usage
Operationalizing 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
Often you can reduce the impact or severity of an event by implementing best practices.
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
Integrations with ticketing and workflow tools
AWS Security Operations teams

Bill Shinn
Sr. Principal, Office of CISO
A specialized AWS Customer Incident Response team that assists and advises customers during their active security events on the customer’s side of the AWS Shared Responsibility Model.

Who we are

Experienced team of AWS professional services and solutions architects in incident response

Assist and advise customers with active triage & recovery of their security event on AWS

Assist in root-cause analysis of a customer’s AWS service logs for the active security event

Provide advice to customers for long-term recovery from the active security event
Available escalations during an AWS customer’s active security event

Customer triage path

- AWS support case (all tiers)
  - AWS Account team
    - AWS Security
      - AWS Customer Incident Response team

AWS Customer Incident Response team

1. Validate AWS account ownership to customer(s) impacted
2. Assist with triage & recovery with customer and AWS teams
3. Investigate root cause(s) with customer for their event
4. Provide recommendations for next steps
Additional AWS customer responsibilities

- All activities that occur under your account – including unauthorized access
- Properly configuring and using an AWS service
- Keeping AWS account email current for notifications
- Taking appropriate action to secure, protect, and back up your account and your content
- Ensuring login credentials and access keys are not disclosed to unauthorized third parties
Common root causes for customer security events
Common root causes for customer security events

- Inaccurate AWS account information
- AWS resource configuration does not follow best practices
- Unintended disclosure of security credentials and secrets
- Inadvertent response to GuardDuty and Detective controls
- Lack of continuous vulnerability management
- Unmanaged application software security
Bill of materials

**Core AWS services**

- AWS Organizations
- AWS Identity and Access Management (IAM)
- Amazon GuardDuty
- AWS Security Hub
- AWS Config
- AWS Personal Health Dashboard
- AWS Secrets Manager
- AWS Backup

**AWS service tools**

- AWS IAM Access Advisor and Access Analyzer
- AWS IAM temporary security credential
- AWS IAM Policy Simulator
- Amazon VPC Reachability Analyzer
- AWS Well-Architected Tool
- Amazon CloudWatch
Security incident response simulation & security reference architecture

Scenario-driven guidance for common root causes of security events

- Grounded in **real-world** security events experienced by AWS customers
- **Prescriptive** guidance for how to prevent and detect by root cause

Reduce customer’s security risks to their AWS accounts and their resources

- Applicable to **all** AWS customers and their **existing** architectures
- Core AWS services to **start** your security journey and **iterate** beyond
- Prioritized to **critical** security practices **observed** to prevent and detect
Call to action – Top 10

1. Ensure you have a **defined** cloud security strategy and incident response plan, including people, processes, and technology for cloud

2. Use **business email distribution lists** for AWS account contact information to respond to AWS notifications

3. **Configure backups** with AWS Backup for **critical** resources and data, and periodically verify restores of backup and their priority of restore order

4. Ensure **enablement** of GuardDuty, AWS Config, Security Hub, CloudTrail, and audit logs for detection of security events

5. Assess risks **continuously** for **critical and high severities** for **common** AWS resource misconfigurations with AWS Foundational Security Best Practices
Call to action – Top 10

6. Assess **continuously** for least-privileged access with AWS IAM features

7. Replace **long-lived** credentials with **short-lived** credentials to reduce risks of security event impact and scope

8. Implement **OWASP Top 10** – especially input validation and rate limits – for your applications within your code and with AWS services (example: AWS WAF)

9. Routinely patch to **latest** security patches for your OS, applications, and dependencies

10. Routinely **train and simulate** for cloud security events to iterate and improve

Security is an **iterative** process, not a **one-time** project
Core references

1. Top 10 security items to improve in your AWS account
   aws.amazon.com/blogs/security/top-10-security-items-to-improve-in-your-aws-account

   docs.aws.amazon.com/wellarchitected/latest/security-pillar

3. AWS Security Reference Architecture (SRA)
   docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html

4. AWS Security Incident Response Guide
Leadership lessons learned

Enjoy the benefits of responding in the cloud, with the cloud

Teams of builders make the best teams of responders

Train how you respond

Create a culture of inspection (expect what you inspect)

Create a culture of escalation
Thank you!

Ryan Holland
ryanhlnd@amazon.com

Bill Shinn
billshin@amazon.com