Layering AWS security services to automate incident response

Igor Ivaniuk
Principal Solutions Architect, EMEA
AWS
Agenda

AWS layered security services portfolio

Enabling the threat detection and response services at scale

Adding automated response and remediation

Best practices to follow
Why is security traditionally challenging?

Lack of visibility

Low degree of automation
Before…

Move fast OR Stay secure
Now…

Move fast AND Stay secure
Scale with superior visibility and control

Control where your data is stored and who can access it

Fine-grain identity and access controls so users and groups have the right access to resources

Reduce risk via security automation and continuous monitoring

Integrate AWS services with your solutions to support existing workflows, streamline ops, and simplify compliance reporting
Highest standards for privacy and data security

Meet data residency requirements
Choose an AWS Region, and AWS will not replicate it elsewhere unless you choose to do so.

Encryption at scale
with keys managed by AWS Key Management Service or manage your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs.

Comply with local data privacy laws
by controlling who can access content, its lifecycle, and its disposal.

Access services and tools that enable you to build compliant infrastructure on top of AWS.
Automate and reduce risk with integrated services

- Comprehensive set of APIs and security tools
- Continuous monitoring and protection
- Threat remediation and response
- Operational efficiencies to focus on critical issues
- Securely deploy business critical applications
AWS security, identity, and compliance solutions

Identity and access management
- AWS Identity and Access Management (IAM)
- AWS IAM Identity Center
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager
- Amazon Verified Permissions

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

Infrastructure protection
- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF
- Amazon VPC
- AWS PrivateLink
- AWS Systems Manager
- AWS Verified Access

Data protection
- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Private CA
- AWS Secrets Manager
- AWS VPC
- AWS Verified Access
- Server-Side Encryption

Incident response
- Amazon Detective
- Amazon EventBridge
- AWS Security Hub
- AWS Elastic Disaster Recovery

Compliance
- AWS Artifact
- AWS Audit Manager
AWS foundational and layered security services

Identify
- AWS Organizations
- AWS Config
- AWS Systems Manager
- AWS Control Tower
- AWS Trusted Advisor

Protect
- AWS Security Hub
- AWS Certificate Manager (ACM)
- AWS KMS
- AWS Network Firewall
- AWS Firewall Manager
- AWS CloudHSM
- AWS Secrets Manager

Detect
- Amazon GuardDuty
- Amazon Inspector
- AWS Security Hub

Investigate
- Amazon CloudWatch
- Amazon Detective
- AWS Step Functions

Automate
- AWS Systems Manager
- AWS Lambda
- AWS CloudWatch

Respond
- Amazon Macie
- AWS Secrets Manager
- AWS Direct Connect

Recover
- Amazon S3 Glacier
- CloudEndure Disaster Recovery
- Amazon CloudTrail

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Threat detection, monitoring, and response

Security monitoring and threat detection

- Amazon EC2
- IAM
- Amazon S3

Amazon GuardDuty
Amazon Macie
Amazon Inspector

AWS Security Hub

Amazon Detective

“Take Action”
How do I enable threat detection at scale?
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
Amazon GuardDuty

FOUNDATIONAL THREAT DETECTION AND MONITORING LAYER

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 & unknown threats

Enterprise-wide consolidation & management
Amazon GuardDuty: How it works

Data sources:
- VPC flow logs
- DNS logs
- AWS CloudTrail events
- Amazon S3 data plane events

Finding types:
- Threat intelligence
- Bitcoin mining
- Command and control activity
- Anomaly detection (ML)

Finding types examples:
- Bitcoin mining
  - Command and control activity
- Anomaly detection (ML)
  - Unusual user behavior
    - Launch instance
    - Change network permissions
  - Unusual traffic patterns
    - Example: unusual ports and volume

Findings:
- High
- Medium
- Low

Action paths:
- Amazon Detective
- AWS Security Hub
- CloudWatch event
  - Alert
  - RemEDIATE
  - Partner solutions
  - Send to SIEM system

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

FOUNDATIONAL THREAT DETECTION AND MONITORING LAYER

**S3 Protection**
Identify potential security risks for data within your Amazon S3 buckets.

**EKS Protection**
Threat detection coverage to help you protect Amazon EKS clusters within your AWS environment.

**Malware Protection**
Identify your resources compromised by malware, or those resources that are at risk.

**RDS Protection**
Analyze and profiles RDS login activity for potential access threats to your Amazon Aurora databases.*

**Lambda Protection**
Continuously monitor network activity, starting with VPC Flow Logs, to detect threats to AWS Lambda functions.

*Amazon Aurora MySQL-Compatible Edition and Aurora PostgreSQL-Compatible Edition
GuardDuty use cases

- Improve security operations visibility
- Assist security analysts in investigations and automate remediation
- Identify files containing malware
- Detect and mitigate threats in your container environment
Amazon Detective

Quickly analyze, investigate, and identify the root cause of security issues

INVESTIGATIVE LAYER

Built-in data collection

Automated analysis

Visual insights
Amazon Detective usage flow

1. Amazon GuardDuty
2. AWS Security Hub
3. Findings from other sources
4. Amazon GuardDuty
5. Partner services
6. Amazon Detective
Multi-account telemetry collection

Administrator accounts

Amazon Detective security behavior graph

AWS CloudTrail

VPC network traffic

Amazon GuardDuty
Amazon Detective

- Allows multi-account enablement with no data sources to configure
- Decreases complexity and increases efficiency of your AWS security investigations
- Is graph based with purpose-built model
- Enables multiple personas on your security team to look back at findings for up to 1 year
- Records analytic baselines for common types of activity
- Is integrated tightly with GuardDuty to start deep investigations on findings with one click
How do I monitor and respond to threats at scale?
AWS Security Hub

CONTINUOUS SECURITY ASSESSMENT AND AUTOMATED RESPONSE LAYER

Centrally view and manage security alerts and automate security checks

- Save time with aggregated findings
- Improve security posture with automated checks
- Curated security best practices
- Seamless integration with standardized findings format
- Multi-account support
How AWS Security Hub works

- Better visibility into **security issues**; easier to stay in **compliance**

- **AWS Security Hub**
  - Aggregate and prioritize findings
  - Conduct automated security checks against benchmarks
  - Take action to investigate or respond and remediate

- **AWS Config**
- **Amazon GuardDuty**
- **Amazon Inspector**
- **IAM Access Analyzer**
- **Third-party integrations**
- **AWS Macie**
- **AWS Firewall Manager**
Automated security and compliance checks

- 150+ fully automated, nearly continuous checks evaluated against preconfigured rules
- Findings are displayed on main dashboard for quick access
- Best practices information is provided to help mitigate gaps and be in compliance
Security Hub as a central dashboard

- Centralize across accounts and prioritize findings without needing to normalize
- View security and compliance posture against key standards
- Take automated action on findings through Amazon CloudWatch Events
How do I automate response and remediation?
Acting on findings

Amazon GuardDuty → AWS Security Hub → Amazon CloudWatch

Selected findings and insights

CloudWatch Events

Detect → Aggregate → Report → Take action

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Automated detection and response

- Blocking traffic to and from suspicious remote hosts, for example to IP addresses associated with known command and control servers for botnets

- GuardDuty detection of unintended communication with remote hosts triggers a series of steps, including blocking of network traffic to those hosts by using Network Firewall, and notification of security operators
Use Security Hub custom actions to trigger automation

Security Hub custom action

Event

Rule

Lambda function

Security Hub custom action

Event

Rule

Amazon Kinesis Data Streams

Security Hub custom action

Event

Rule

Amazon SNS

Run command
AWS Security Hub Automated Response and Remediation solution architecture

Customizable response and remediation actions

1. All findings automatically send to CloudWatch Events, and
2. Security Hub user can select findings in the console and take a custom action on them; these findings are sent to CloudWatch decorated with a custom action ID
3. User creates Amazon CloudWatch Events rules to look for certain findings associated with a custom action ID or findings with specific characteristics
4. The rule defines a target, typically a Lambda function, Step Functions step, or automation document
5. The target could be things like a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook
Customizable response and remediation actions
Best practice – multi-account management

AWS threat detection and monitoring services can be configured and administered within AWS Organizations, so they can be managed across multiple accounts.

https://amzn.to/3wGlh4Y
Demo
Layered threat detection and response services

Security tools natively available in AWS

Reduce the burden for the security team

Centralized and scalable deployment with a click of a button
AWS Contacts for Kazakhstan

Almas Moldakanov
Territory Manager

almasmol@amazon.de

+49 152 09135498
(Mobile, Telegram, WhatsApp)
Please, help us do better!

Join User Group Kazakhstan
Thank you!

Igor Ivaniuk
iivaniuk@amazon.de