

Threat Response Scenarios using Amazon GuardDuty

Nathan Case,
Security Geek



Amazon GuardDuty

- GuardDuty, overview
- Threat Detection
- Response to a given threat.



Amazon GuardDuty

Amazon GuardDuty

Quick Intro – very quick, I promise...



Amazon GuardDuty

Find the Needle, Skip the Haystack



GuardDuty helps security professionals quickly find the threats (needle) to their environments in the sea of log data (haystack) so they can focus on hardening their AWS environments and responding quickly to malicious or suspicious behavior.



Amazon GuardDuty:
All Signal, No Noise

GuardDuty Data Sources



VPC Flow Logs



VPC flow logs

- Flow Logs for VPCs Do Not Need to Be Turned On to Generate Findings, data is consumed through independent duplicate stream.
- Suggested Turning On VPC Flow Logs to Augment Data Analysis (charges apply).

DNS Logs



DNS Logs

- DNS Logs are based on queries made from EC2 instances to known questionable domains.
- DNS Logs are in addition to Route 53 query logs. Route 53 is not required for GuardDuty to generate DNS based findings.

CloudTrail Events

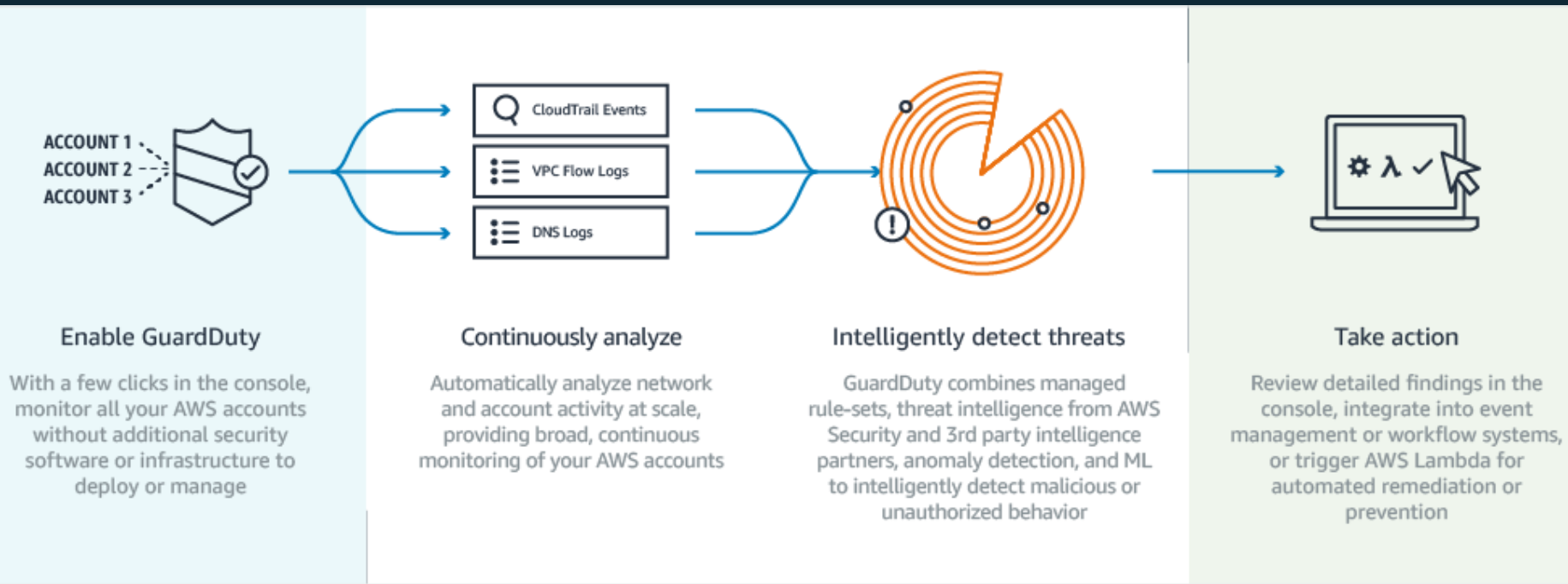


CloudTrail Events

- CloudTrail history of AWS API calls used to access the Management Console, SDKs , CLI, etc. presented by GuardDuty.
- Identification of user and account activity including source IP address used to make the calls.

Capture and save all event data via CWE or API Call for long term retention. Additional charges apply.

GuardDuty Threat Detection and Notification



GuardDuty Findings: Threat Purpose Details



Describes the primary purpose of the threat. Available at launch, more coming!

- **Backdoor:** resource compromised and capable of contacting source home
- **Behavior:** activity that differs from established baseline
- **Crypto Currency:** detected software associated with Crypto currencies
- **Pentest:** activity detected similar to that generated by known pen testing tools
- **Recon:** attack scoping vulnerabilities by probing ports, listening, database tables, etc
- **Stealth:** attack trying to hide actions / tracks
- **Trojan:** program detected carrying out suspicious activity
- **Unauthorized Access:** suspicious activity / pattern by unauthorized user

Understand Your Domains

Infrastructure

VPC Resources

Connectivity

On-instance

...

Application

Patching Issue

Code Insecurity

...

The diagram illustrates a multi-availability zone AWS VPC architecture. At the top, an **AWS** logo is shown. Below it, an **Internet Gateway** is connected to a **VPC** (Virtual Private Cloud) with a **VPC CIDR: 10.0.0.0/16**. The VPC is divided into three subnets: a **Public subnet** (10.0.0.0/19), a **Private subnet** (10.0.32.0/20), and another **Private subnet** (10.0.48.0/21). The Public subnet contains a **Route table** icon. The Private subnet contains a **Security groups** icon. The third Private subnet contains a **Instance compromise** icon. A **NACLs** (Network Access Control Lists) icon is also shown. The VPC is spread across three **Availability Zones** (AZs), labeled **Availability Zone A**, **Availability Zone B**, and **Availability Zone C**. On the left side, various AWS services are listed: **Amazon S3**, **Amazon RDS**, **AWS Directory Service**, **AWS CloudHSM**, **IAM**, **AWS KMS**, and **AWS Organization**.

Understand Your Domains

Infrastructure

VPC Resources

Connectivity

On-instance

...

Application

Patching

Coding hole

...

Services

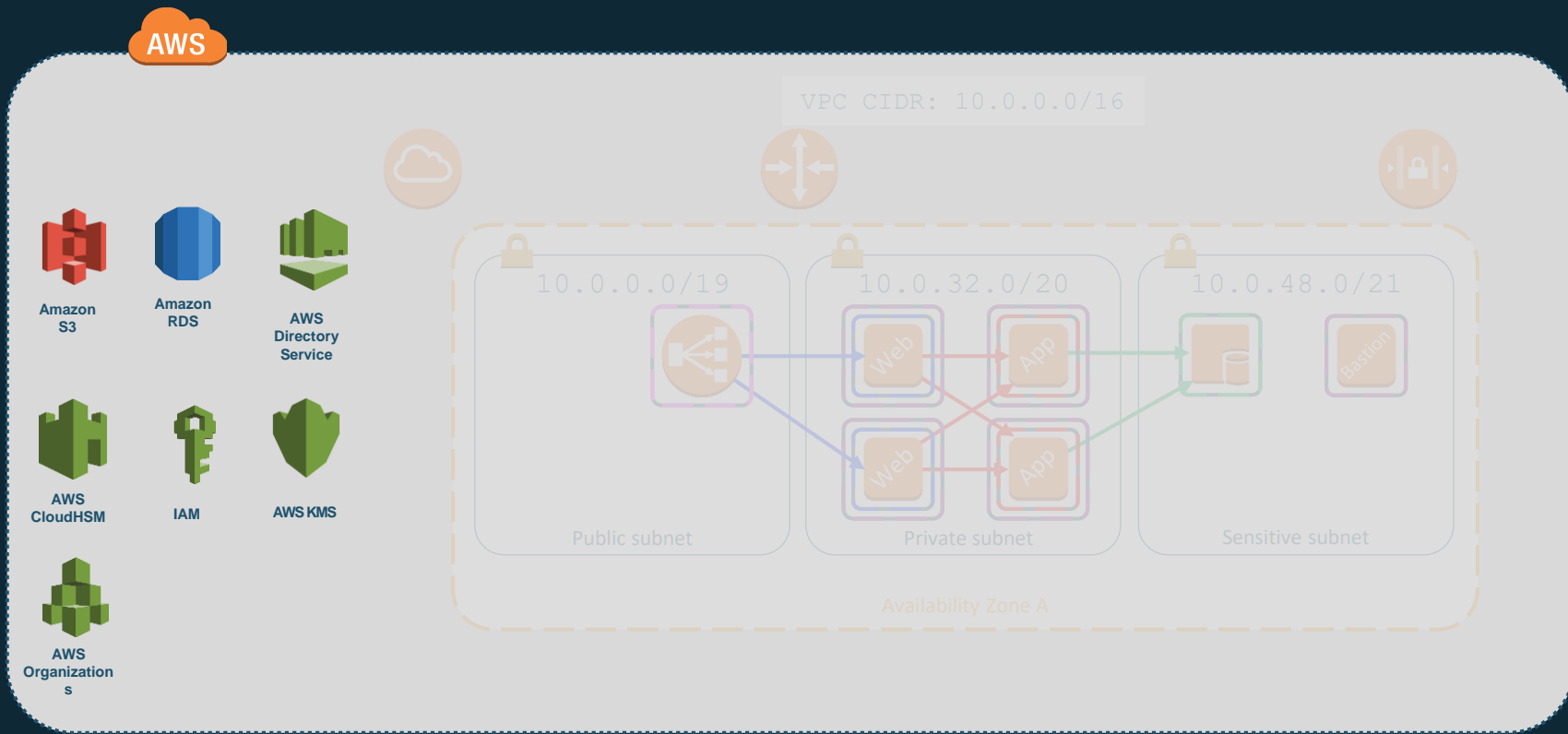
IAM

S3 buckets

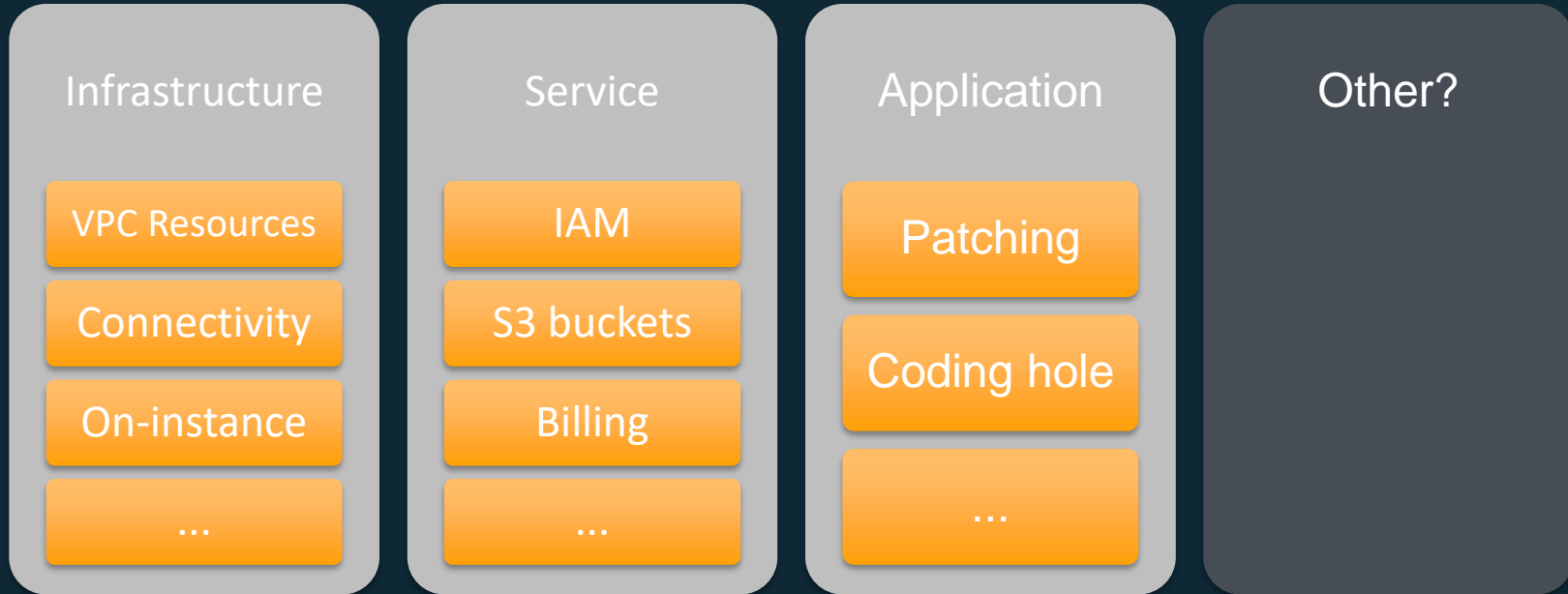
Billing

...

Incidents in the Service Domain



Understand Your Domains



AWS security solutions



Identity

AWS Identity & Access Management (IAM)
AWS Directory Service
AWS Organizations
AWS Secrets Manager
AWS Single Sign-On
Amazon Cognito



Detective control

AWS CloudTrail
AWS Config
Amazon CloudWatch
Amazon GuardDuty
VPC Flow Logs



Infrastructure security

AWS Systems Manager
AWS Shield
AWS WAF – Web application firewall
AWS Firewall Manager
Amazon Inspector
Amazon Virtual Private Cloud (VPC)



Data protection

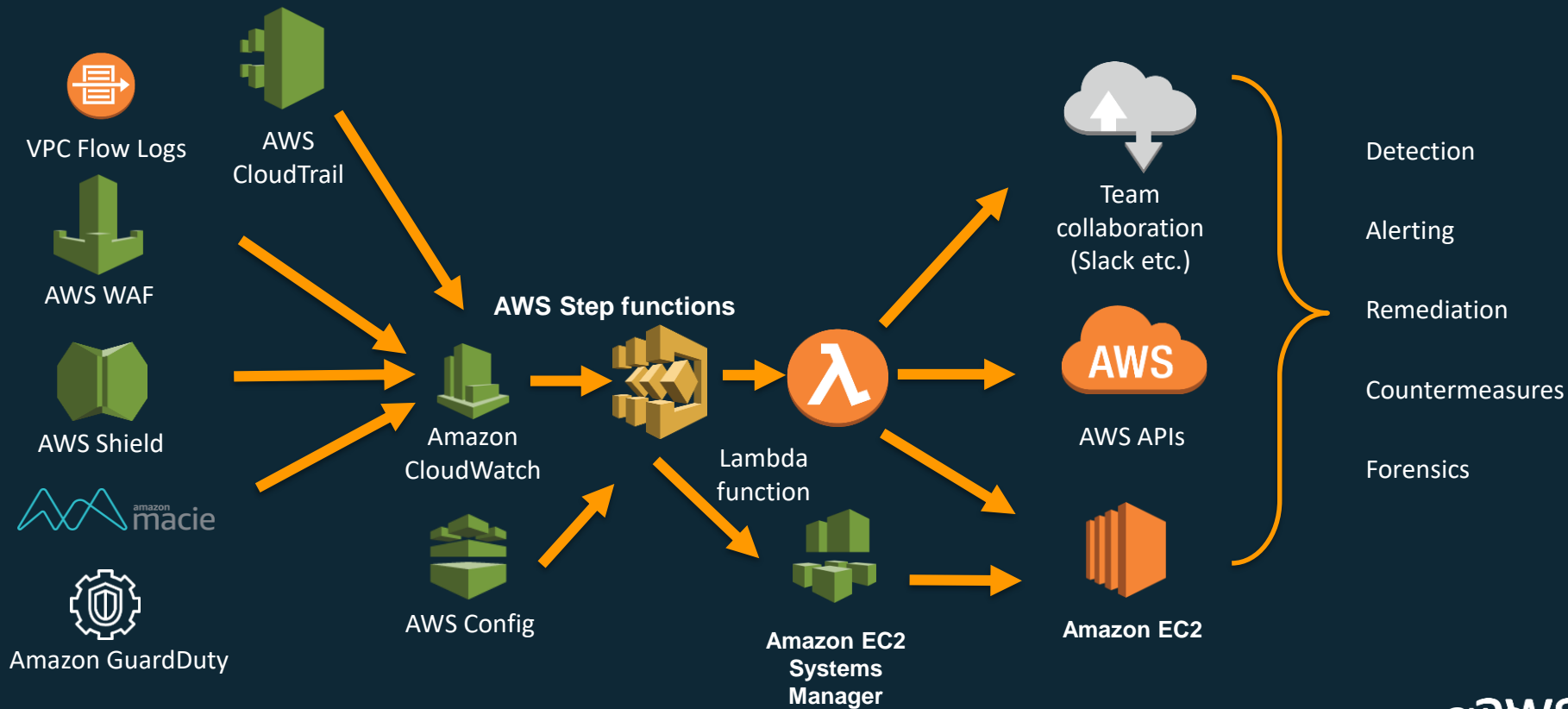
AWS Key Management Service (KMS)
AWS CloudHSM
Amazon Macie
AWS Certificate Manager
Server-Side Encryption



Incident response

AWS Config Rules
AWS Lambda

Responding to Findings: Remediation



Responding to Findings: Automation Example



- Lambda Function:
 - Removes instance from current Security Group(s) and adds to one with all ingress and egress blocked
 - Snapshots EBS volume(s)
 - Alerts Security Team
- SSM Document:
 - Forensics can begin
 - Network Capture
 - Memory Dump
 - Process review
 - Internal Tools



GuardDuty Management Console

Secure | <https://eu-west-2.console.aws.amazon.com/guardduty/home?region=eu-west-2#/onboard>

aws Services Resource Groups

Michael Fuller London Support

GuardDuty

Enable GuardDuty

Partners

Welcome to GuardDuty

30 day free trial

Service permissions

When you enable GuardDuty, you grant GuardDuty permissions to analyze AWS CloudTrail logs, VPC Flow Logs, and DNS query logs to generate security findings. [Learn more](#)

[View service role permissions](#)

Note: GuardDuty doesn't manage AWS CloudTrail logs, VPC Flow Logs, and DNS query logs or make their events and logs available to you. You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable GuardDuty at any time to stop it from processing and analyzing events and logs. [Learn more](#)

When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day [GuardDuty free trial](#). Learn more about [GuardDuty pricing](#).

[Enable GuardDuty](#)



Click here

Crypto Currency (Account Breach)

GuardDuty

Findings

Settings

Lists

Accounts

What's New

Usage

Partners

Findings

Showing 3 of 3

021

Actions

Saved filters / Auto-archive

No saved filters

Add filter criteria

	Finding type	Resource	La...	...
<input type="checkbox"/>	Backdoor:EC2/C&CActivity.BIDNS	Instance: i-08bca12eea0feb0ca	4 hour...	2
<input type="checkbox"/>	CryptoCurrency:EC2/BitcoinTool.BI...	Instance: i-08bca12eea0feb0ca	4 hour...	4
<input type="checkbox"/>	UnauthorizedAccess:IAMUser/Unus...	DeepLens: ASIAIMFJJY5JHHBE	a mont...	4

Useful?

Close

CryptoCurrency:EC2/BitcoinTool.BIDNS

Finding ID: 2ab29c8fbaa5d5be8e0f063524c4ef7d1

EC2 instance i-08bca12eea0feb0ca is querying a domain name that is associated with Bitcoin-related activity.

Severity	Region	Count
Medium	us-east-1	4
Account ID	Resource ID	Threat list name
215879485286	i-08bca12eea0feb...	ProofPoint
Created at	Updated at	
08-14-2018 11:48:...	08-14-2018 12:31:...	

Resource affected

Resource role	Resource type
TARGET	Instance
Instance ID	Instance type
i-08bca12eea0feb0ca	t2.micro
Instance state	Availability zone
running	us-east-1b
Image ID	Image description
ami-97785bed	Amazon Linux AMI 2017.09.12...
Launch time	
02-23-2018 00:44:30	
Instance profile	
Arn: arn:aws:iam::215879485286:instance-profile/test-lab3-rinstanceProfile-1814TYCLUGE6X	
ID: AIPACFVSNZJVU4CV3JVO	
Tags	
aws:cloudformation:stack-id: arn:aws:cloudformation:us-east-1:215879485286:stack/test-lab3/1d2fcd50-185c-11e8-b123-50fae9826c35	
aws:cloudformation:logical-id: rinstance1	
Name: Lab 3	
aws:cloudformation:stack-name: test-lab3	

Auto Remediation !

- 1. Lambda Remediation of Crypto Mining
 1. Account Password Rest
 2. Instance Removal
 - And
 - And
 - And
 - And your internal management/legal department is not happy.
- Lets make sure we take a moment to plan correctly.

Runbooks!

Working Definition :

- A way to have an employee actively and succinctly remediate an issue in an enterprise's infrastructure, application and/or service layer.

Wikipedia:

- In a [computer system](#) or [network](#), a **runbook** is a compilation of routine procedures and operations that the system administrator or operator carries out. [System administrators](#) in [IT](#) departments and [NOCs](#) use runbooks as a reference. Runbooks can be in either electronic or in physical book form. Typically, a runbook contains procedures to begin, stop, supervise, and debug the system. It may also describe procedures for handling special requests and contingencies. An effective runbook allows other operators, with prerequisite expertise, to effectively manage and troubleshoot a system. Through runbook automation, these processes can be carried out using software tools in a predetermined manner.

Runbooks – Things to consider

1. Attribution – Catching or at least knowing who caused the incident.
 - Legal Counsel - This is a not legal guidance. It is a suggestion to speak to your legal counsel and follow their suggestion for your business and the needs that it may have.
 - What steps can you take to ensure chain of custody
2. Review if a third party will need to control the information surrounding the incident.
3. Review if your enterprise wants to do forensics
 - List of tools
 - List of data
 - Reasons for use case, ie When does an incident equal forensics time to be spent.
4. What timed procedures are being run, ie end of month book close
5. Review the ground rules that you have found, Build these as your guard rails.

Runbooks – Example

Problem description

[Your Enterprise Here] is under a [Attack Type]

[Attack Description]

Data to gather for troubleshooting

[Evaluation of current data.]

Steps to troubleshoot and fix

- 1.Log in to AWS
- 2.Do stuff
- 3.Correct Issue
- 4.Jump to forensics environment?

Urgency category

[Critical, Important, moderate, informational]

Escalation path:

Unable to fix, escalate to these individuals or groups in this order:

- 1.Someone, email and phone number
- 2.Someone Else, email phone number
- 3.Distribution List/Slack?
- 4.CTO/CISO?
- 5.CEO?

Runbooks – Exam

Problem description

[Your Enterprise Here] is und

[Attack Description]

Data to gather for troublesh

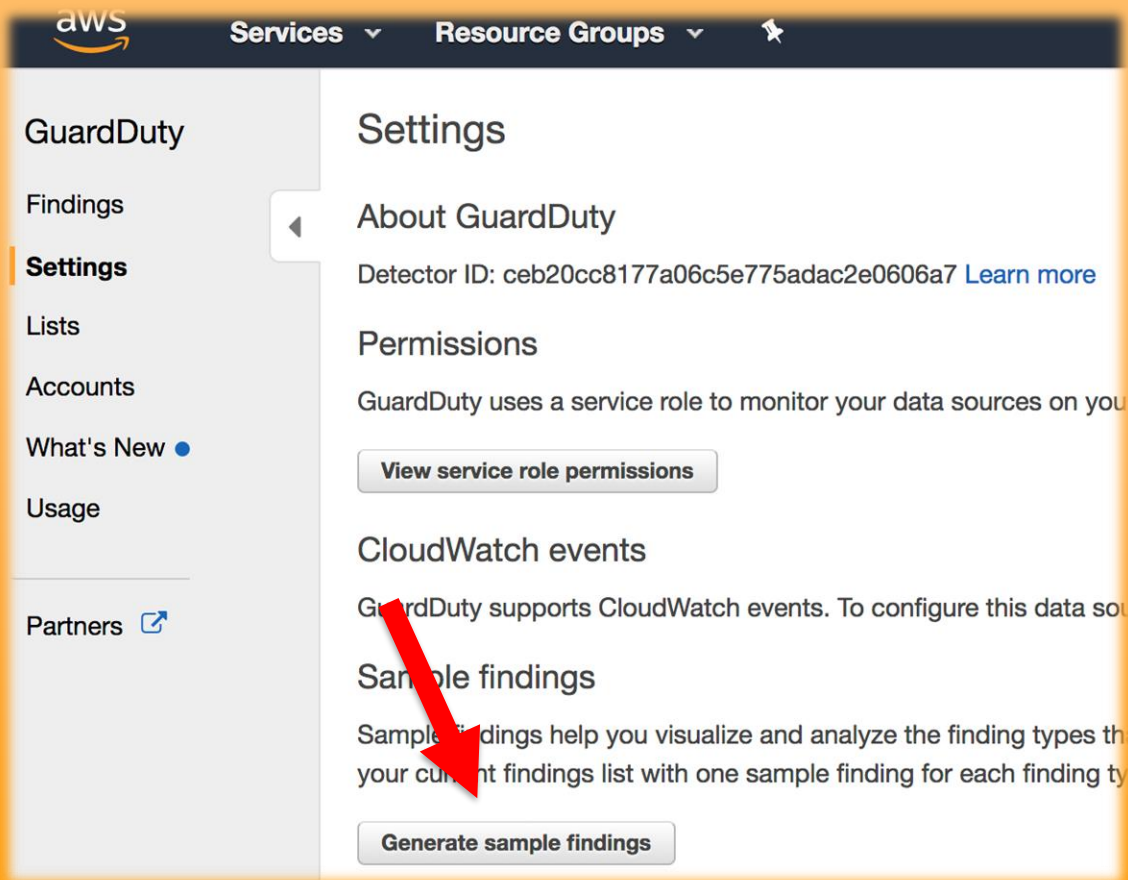
[Evaluation of current data.]

Steps to troubleshoot and fi

- 1.Log in to AWS
- 2.Do stuff
- 3.Correct Issue
- 4.Jump to forensics environm

Urgency category

[Critical, Important, moderat



Runbook

Problem description

[Your Enterprise]

[Attack Description]

Data to gather

[Evaluation of findings]

Steps to troubleshoot

1. Log in to AWS IAM console

2. Do stuff














3. Correct Issues

4. Jump to forensics

Urgency category

[Critical, Important]

 Add filter criteria

<input type="checkbox"/>		Finding type	Resource	Last s...	C...
<input type="checkbox"/>		[SAMPLE] Recon:IAMUser/NetworkPermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Recon:IAMUser/ResourcePermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Trojan:EC2/PhishingDomainRequest!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Trojan:EC2/DropPoint!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Persistence:IAMUser/UserPermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:IAMUser/InstanceCre...	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Trojan:EC2/BlackholeTraffic!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Recon:IAMUser/UserPermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:IAMUser/TorIPCaller	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] ResourceConsumption:IAMUser/Compute...	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-999999999	9 minutes ...	1

"type": "CryptoCurrency:EC2/BitcoinTool.B!DNS"
EC2 instance is communicating with Bitcoin mining pools.

Remediation - CryptoCurrency:EC2/BitcoinTool.B!DNS

```
[
{
  "schemaVersion": "2.0",
  "accountId": "0123456789",
  "region": "us-west-2",
  "partition": "aws",
  "id": "[GUID]",
  "arn": "arn:aws:guardduty:us-west-2:01234567890:detector/[GUID]/finding/[Finding GUID]",
  "type": "CryptoCurrency:EC2/BitcoinTool.B!DNS",
  "resource": {
    "resourceType": "Instance",
    "instanceDetails": {
      "instanceId": "i-999999999"
      "instanceType": "p2.xlarge"
      "launchTime": "2017-12-20"
      "platform": null,
      "productCodes": [
        {
          "productCodeId": "GeneratedFindingProductCodeId",
          "productCodeType": "GeneratedFindingProductCodeType"
        }
      ]
    }
  }
}
```

Finding: ["type"] = "CryptoCurrency:EC2/BitcoinTool.B!DNS"
Instance: ["instanceDetails"]["instanceId"] = "i-999999999"

Remediation - CryptoCurrency:EC2/BitcoinTool.B!DNS

Problem description

CryptoCurrency:EC2/BitcoinTool.B!DNS has been found in GuardDuty under this mean that we have an account or machine that has been compromised.

This finding informs you that an EC2 instance in your AWS environment is querying a domain name that is associated with Bitcoin-related activity. Bitcoin is a worldwide cryptocurrency and digital payment system. Besides being created as a reward for Bitcoin mining, bitcoin can be exchanged for other currencies, products, and services. Unless you use this EC2 instance to mine or manage cryptocurrency or your EC2 instance is involved in blockchain activity, your EC2 instance might be compromised.

Data to gather for troubleshooting

Account User ID, Role or Profile that was accessed

Instance ID , Subnet ID, VPC ID

Connectivity to other systems

Review of CloudTrail and VPC Flows to and around the specified instance.

Steps to troubleshoot and fix

- 1.Notify IR Team On call.
- 2.Run Automate instance quarantine
- 3.Role credentials associated with the above identity
- 4.Snapshot instance and VPC Flow logs to forensics account
- 5.Validate that new ASG created instance is working correctly

Urgency category

Critical

Escalation path:

Unable to fix, escalate to these individuals or groups in the organization

- 1.Someone, email and phone number
- 2.Someone Else, email phone number
- 3.Distribution List
- 4....
- 5....

Finding: [{"type"}]= "**CryptoCurrency:EC2/BitcoinTool.B!DNS**"
Instance: [{"instanceDetails"}][{"instanceId"}] = "i-999999999"

Remediation - CryptoCurrency:EC2/BitcoinTool.B!DNS

Problem description

CryptoCurrency:EC2/BitcoinTool.B!DNS has been found in GuardDuty under this mean that we have an account or machine that has been compromised.

This finding informs you that an EC2 instance in your AWS environment is querying a domain name that is associated with Bitcoin-related activity. Bitcoin is a worldwide cryptocurrency and digital payment system. Besides being created as a reward for Bitcoin mining, bitcoin can be exchanged for other currencies, products, and services. Unless you use this EC2 instance to mine or manage cryptocurrency or your EC2 instance is involved in blockchain activity, your EC2 instance might be compromised.

Data to gather for troubleshooting

Account User ID, Role or Profile that was accessed

Instance ID , Subnet ID, VPC ID

Connectivity to other systems

Review of CloudTrail and VPC Flows to and around the specified instance.

Steps to troubleshoot and fix

- 1.Notify IR Team On call.
- 2.Run Automate instance quarantine
- 3.Role credentials associated with the above identity
- 4.Snapshot instance and VPC Flow logs to forensics account
- 5.Validate that new ASG created instance is working correctly

Urgency category

Critical

Escalation path:

Unable to fix, escalate to these individuals or groups in this order

- 1.Someone, email and phone number
- 2.Someone Else, email phone number
- 3.Distribution List
- 4....
- 5....

Steps to troubleshoot and fix

- 1.Notify IR Team On call.
- 2.Run Automate instance quarantine
- 3.Role credentials associated with the above identity
- 4.Snapshot instance and VPC Flow logs to forensics account
- 5.Validate that new ASG created instance is working correctly

Remediation - CryptoCurrency:EC2/BitcoinTool.B!DNS

Problem description

CryptoCurrency:EC2/BitcoinTool.B!DNS has been found in GuardDuty under this mean that we have an account or machine that has been compromised.

This finding informs you that an EC2 instance in your AWS environment is querying a domain name that is associated with Bitcoin-related activity. Bitcoin is a worldwide cryptocurrency and digital payment system. Besides being created as a reward for Bitcoin mining, bitcoin can be exchanged for other currencies, products, and services. Unless you use this EC2 instance to mine or manage cryptocurrency or your EC2 instance is involved in blockchain activity, your EC2 instance might be compromised.

Data to gather for troubleshooting

Account User ID, Role or Profile that was accessed

Instance ID , Subnet ID, VPC ID

Connectivity to other systems

Review of CloudTrail and VPC Flows to and around the sp

Steps to troubleshoot and fix

1.Notify IR Team On call.

2.Run Automate Instance quarantine

3.Role credentials associated with the above identity

4.Snapshot instance and VPC Flow logs to forensics accou

5.Validate that new ASG created instance is working corre

Urgency category

Critical

Escalation path:

Unable to fix, escalate to these individuals or groups in th

1.Someone, email and phone number

2.Someone Else, email phone number

3.Distribution List

4....

5....

Items to Code:

1. Cloud Watch Filter to trap a finding from GuardDuty, with:
[“type”]= “**CryptoCurrency:EC2/BitcoinTool.B!DNS**”
2. Step Functions Start
 - a. SNS Fires to notify Ops of an issue
 - b. Lambda Function is fired to run SSM
 - i. Finished and a Lambda Function is fired to quarantine the instance
 - c. Lambda Function is fired to Snap Shot the instance
 - d. Step Function checks responses
3. Lambda is fired to Stop and destroy the instance.

Remediation - CryptoCurrency:EC2/BitcoinTool.B!DNS

Problem description

CryptoCurrency:EC2/BitcoinTool.B!DNS has been found in GuardDuty under this mean that we have an account or machine that has been compromised.

This finding informs you that an EC2 instance in your AWS environment is querying a domain name that is associated with Bitcoin-related activity. Bitcoin is a worldwide cryptocurrency and digital payment system. Besides being created as a reward for Bitcoin mining, bitcoin can be exchanged for other currencies, products, and services. Unless you use this EC2 instance to mine or manage cryptocurrency or your EC2 instance is involved in blockchain activity, your EC2 instance might be compromised.

Data to gather for troubleshooting

Account User ID, Role or Profile that was accessed

Instance ID , Subnet ID, VPC ID

Connectivity to other systems

Review of CloudTrail and VPC Flows to and around the specified instance.

Steps to troubleshoot and fix

- 1.Notify IR Team On call.
- 2.Run Automate instance quarantine
- 3.Role credentials associated with the above identity
- 4.Snapshot instance and VPC Flow logs to forensics a
- 5.Validate that new ASG created instance is working

Urgency category

Critical

Escalation path:

Unable to fix, escalate to these individuals or groups

- 1.Someone, email and phone number
- 2.Someone Else, email phone number
- 3.Distribution List
- 4....
- 5....

Escalation path:

Unable to fix, escalate to these individuals or groups in this order:

- 1.Someone, email and phone number
- 2.Someone Else, email phone number
- 3.Distribution List
- 4....
- 5....

Remediation - CryptoCurrency:EC2/BitcoinTool.B!DNS

Problem description

CryptoCurrency:EC2/BitcoinTool.B!DNS has been found in GuardDuty under this mean that we have an account or machine that has been compromised.

This finding informs you that an EC2 instance in your AWS environment is querying a domain name that is associated with Bitcoin-related activity. Bitcoin is a worldwide cryptocurrency and digital payment system. Besides being created as a reward for Bitcoin mining, bitcoin can be exchanged for other currencies, products, and services. Unless you use this EC2 instance to mine or manage cryptocurrency or your EC2 instance is involved in blockchain activity, your EC2 instance might be compromised.

Data to gather for troubleshooting

Account User ID, Role or Profile that was accessed

Instance ID , Subnet ID, VPC ID

Connectivity to other systems

Review of CloudTrail and VPC Flows to and around the specified instance.

Steps to troubleshoot and fix

- 1.Notify IR Team On call.
- 2.Run Automate Instance quarantine
- 3.Role credentials associated with the above identity
- 4.Snapshot instance and VPC Flow logs to forensics account
- 5.Validate that new ASG created

Urgency category

Critical

Escalation path:

Unable to fix, escalate to:

- 1.Someone, email and phone
- 2.Someone Else, email and phone
- 3.Distribution List
- 4....
- 5....

Items to Code:

- **AWS Labs** - <https://github.com/aws-labs>

Examples of Code:

- **Security Automation** - <https://github.com/aws-labs/aws-security-automation>

"type": "UnauthorizedAccess:IAMUser/UnusualASNCaller",
An API was invoked from an IP address of an unusual network.

Unauth

Problem description

[Your Enterprise Here] is

[Attack Description]

Data to gather for troubleshooting

[Evaluation of current data]

Steps to troubleshoot and fix

1. Log in to AWS
2. Do stuff
3. Correct Issue
4. Jump to forensics enviro














Urgency category

[Critical, Important, mode

Escalation path:

- Unable to fix, escalate to
1. Someone, email and ph
 2. Someone Else, email ph
 3. Distribution List/Slack?
 4. CTO/CISO?
 5. CEO?

 Add filter criteria

<input type="checkbox"/>		Finding type	Resource	Last s...	C...
<input type="checkbox"/>		[SAMPLE] Recon:IAMUser/NetworkPermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Recon:IAMUser/ResourcePermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Trojan:EC2/PhishingDomainRequest!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Trojan:EC2/DropPoint!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Persistence:IAMUser/UserPermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:IAMUser/InstanceCre...	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Trojan:EC2/BlackholeTraffic!DNS	Instance: i-999999999	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] Recon:IAMUser/UserPermissions	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:IAMUser/TorIPCaller	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] ResourceConsumption:IAMUser/Compute...	GeneratedFindingUserName: GeneratedFinding	9 minutes ...	1
<input type="checkbox"/>		[SAMPLE] UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-999999999	9 minutes ...	1

Remediation

```
[
  {
    "schemaVersion": "2.0",
    "accountId": "710582532708",
    "region": "us-east-2",
    "partition": "aws",
    "id": "12b2c8c3d5aec3406737c61d0935b322",
    "arn": "arn:aws:guardduty:us-east-2:710582532708:detector/ceb20cc8177a06c5e775adac2e0606a7/finding/12b2c8c3d5aec3406737c61d0935b322",
    "type": "UnauthorizedAccess:IAMUser/UnusualASNCaller",
    "resource": {
      "resourceType": "AccessKey",
      "accessKeyDetails": {
        "accessKeyId": "GeneratedFindingAccessKeyId",
        "principalId": "GeneratedFindingPrincipalId",
        "userType": "IAMUser",
        "userName": "GeneratedFindingUserName"
      }
    },
    "service": {
      "serviceName": "guardduty",
      "detectorId": "ceb20cc8177a06c5e7",
      "action": {
        "actionType": "AWS_API_CALL",
        "awsApiCallAction": {
```

Finding: ["type"]= "UnauthorizedAccess:IAMUser/UnusualASNCaller"
["username"]: "GeneratedFindingUserName"

Runbooks – UnauthorizedAccess:IAMUser/UnusualASNCaller

Problem description

UnauthorizedAccess:IAMUser/UnusualASNCaller. An API was invoked from an IP address of an unusual network.

This finding informs you that certain activity was invoked from an IP address of an unusual network. This network was never observed throughout the AWS usage history of the described user. This activity can include a console login, an attempt to launch an EC2 instance, create a new IAM user, modify your AWS privileges, etc. This can indicate unauthorized access to your AWS resources.

Data to gather for troubleshooting

Account User Name, Role or Profile that was used

Connectivity to other systems

Review of CloudTrail for specified around actions taken from user.

Steps to troubleshoot and fix

1. Notify IR Team On call.
2. Rotate User Credentials, terminate active sessions
3. Role credentials associated with the above identity
4. Review Cloud Trail in Splunk or SumoLogic
5. Redeploy active account, remove any non-sanctioned constructs from the account. Or deploy to a new account, burning the compromised account

Urgency category

Critical

Escalation path:

Unable to fix, escalate to these individuals or groups in the organization

1. Someone, email and phone number
2. Someone Else, email phone number
3. Distribution List
- 4....
- 5....

Finding: `[“type”]= “UnauthorizedAccess:IAMUser/UnusualASNCaller”
[“username”]: “GeneratedFindingUserName”`

Runbooks – UnauthorizedAccess:IAMUser/UnusualASNCaller

Problem description

UnauthorizedAccess:IAMUser/UnusualASNCaller. An API was invoked from an IP address of an unusual network.

This finding informs you that certain activity was invoked from an IP address of an unusual network. This network was never observed throughout the AWS usage history of the described user. This activity can include a console login, an attempt to launch an EC2 instance, create a new IAM user, modify your AWS privileges, etc. This can indicate unauthorized access to your AWS resources.

Data to gather for troubleshooting

Account User Name, Role or Profile that was used
Connectivity to other systems
Review of CloudTrail for specified around actions taken from

Steps to troubleshoot and fix

1. Notify IR Team On call.
2. Rotate User Credentials, terminate active sessions
3. Role credentials associated with the above identity
4. Review Cloud Trail in Splunk or SumoLogic
5. Redeploy active account, remove any non-sanctioned constructs

Urgency category

Critical

Escalation path:

- Unable to fix, escalate to these individuals or groups in the organization
1. Someone, email and phone number
 2. Someone Else, email phone number
 3. Distribution List
 - 4....
 - 5....

Steps to troubleshoot and fix

1. Notify IR Team On call.
2. Rotate User Credentials, terminate active sessions
3. Role credentials associated with the above identity
4. Review Cloud Trail in Splunk or SumoLogic
5. Redeploy active account, remove any non-sanctioned constructs from the account. Or deploy to a new account, burning the compromised account

Runbooks – UnauthorizedAccess:IAMUser/UnusualASNCaller

Problem description

UnauthorizedAccess:IAMUser/UnusualASNCaller. An API was invoked from an IP address of an unusual network.

This finding informs you that certain activity was invoked from an IP address of an unusual network. This network was never observed throughout the AWS usage history of the described user. This activity can include a console login, an attempt to launch an EC2 instance, create a new IAM user, modify your AWS privileges, etc. This can indicate unauthorized access to your AWS resources.

Data to gather for troubleshooting

Account User Name, Role or Profile that was used
Connectivity to other systems
Review of CloudTrail for specified around actions taken from

Steps to troubleshoot and fix

1. Notify IR Team On call.
2. Rotate User Credentials, terminate active sessions
3. Role credentials associated with the above identity
4. Review Cloud Trail in Splunk or SumoLogic
5. Redeploy active account, remove any non-sanctioned c

Urgency category

Critical

Escalation path:

- Unable to fix, escalate to these individuals or groups in the
1. Someone, email and phone number
 2. Someone Else, email phone number
 3. Distribution List
 - 4....
 - 5....

Items to Code:

1. Cloud Watch Filter to trap a finding from GuardDuty, with:
[“type”]=
“UnauthorizedAccess:IAMUser/UnusualASNCaller”
2. Step Functions Start
 - a. SNS Fires to notify Ops of an issue
 - b. Lambda Function is fired to:
 - i. Rotate Keys, User Passwords
 - ii. Revoke sessions
 - c. Lambda to list actions taken by User
 - a. Remediate any that can be and Messaged items that can't be.

Runbooks – UnauthorizedAccess:IAMUser/UnusualASNCaller

Problem description

UnauthorizedAccess:IAMUser/UnusualASNCaller. An API was invoked from an IP address of an unusual network.

This finding informs you that certain activity was invoked from an IP address of an unusual network. This network was never observed throughout the AWS usage history of the described user. This activity can include a console login, an attempt to launch an EC2 instance, create a new IAM user, modify your AWS privileges, etc. This can indicate unauthorized access to your AWS resources.

Data to gather for troubleshooting

Account User Name, Role or Profile that was used

Connectivity to other systems

Review of CloudTrail for specified around actions taken from user.

Steps to troubleshoot and fix

1. Notify IR Team On call.
2. Rotate User Credentials, terminate active sessions
3. Role credentials associated with the above identity
4. Review Cloud Trail in Splunk or SumoLogic
5. Redeploy active account, remove any non-sanctioned

Urgency category

Critical

Escalation path:

Unable to fix, escalate to these individuals or groups

1. Someone, email and phone number
2. Someone Else, email phone number
3. Distribution List
- 4....
- 5....

Escalation path:

Unable to fix, escalate to these individuals or groups in this order:

1. Someone, email and phone number
2. Someone Else, email phone number
3. Distribution List
- 4....
- 5....

Final Thoughts
Making sure we see all the failures in each bad day.

Prevention verse Reaction

**Compliance
variance**

**Service
disruption**

**Unauthorized
resources**

**Unauthorized
access**

**Privilege
escalation**

Persistence

**Excessive
permissions**

**Information
exposure**

**Credentials
exposure**

Prevention verse Reaction



Key GuardDuty Partners

Partners Are Here to Help Providing Consulting, Data Analysis, Threat Detection, and Managed Security Operations all with Amazon GuardDuty.



evident.io



Find all GuardDuty Partners at: <https://aws.amazon.com/guardduty/resources/partners/>

Close the Loop

Reviewing the issues that occurred, and harden the application, infrastructure or procedures, so that the event can't happen again.

- Git-Secrets - <https://github.com/awslabs/git-secrets>
- ECS-Secrets - <https://github.com/awslabs/ecs-secrets>
- AWSScout2 - <https://github.com/nccgroup/Scout2>



Prevention verse Reaction

Least permissions

- Profiles
 - Lambda Functions
 - Containers
 - EC2
- Roles
- Users
- Everything!

Dev Sec Ops!

- Keep Humans away from the data
- Production is set apart, cleaner patterns means better threat detection.
- The Pipeline is a no human zone, more so than production.



GuardDuty + Planning (Run books * SIRS) * Partners = More Sleep

- This pattern holds regardless of product
- GuardDuty's importance is multiplied with CloudWatch, Config or custom Lambdas
- Notification and remediations allow you, the administrator to better meet uptime and DR goals
- Run books help with knowledge and training, but also to feel in control of a situation. Both as a coordinator and as an engineer.



Amazon GuardDuty Call to Action

Enable GuardDuty - monitor the cost and findings during the 30 day free period – assess after 30 days where GuardDuty will sit in your overall security strategy.

Plan out how GuardDuty will be used in your originations. Write runbooks. Test them and remediate GuardDuty findings.

<https://aws.amazon.com/guardduty/>

