Threat Response Scenarios using Amazon GuardDuty

Nathan Case, Security Geek
Amazon GuardDuty

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

Quick Intro – very quick, I promise...
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**
- 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 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 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

Enable GuardDuty
With a few clicks in the console, monitor all your AWS accounts without additional security software or infrastructure to deploy or manage.

Continuously analyze
Automatically analyze network and account activity at scale, providing broad, continuous monitoring of your AWS accounts.

Intelligently detect threats
GuardDuty combines managed rule-sets, threat intelligence from AWS Security and 3rd party intelligence partners, anomaly detection, and ML to intelligently detect malicious or unauthorized behavior.

Take action
Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention.
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...

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Understand Your Domains

- **Infrastructure**
  - VPC Resources
  - Connectivity
  - On-instance
  - ...

- **Application**
  - Patching
  - Coding hole
  - ...

- **Services**
  - IAM
  - S3 buckets
  - Billing
  - ...

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Incidents in the Service Domain

- Availability Zone A
  - VPC CIDR: 10.0.0.0/16
  - 10.0.0.0/19: Public subnet
  - 10.0.32.0/20: Private subnet
  - 10.0.48.0/21: Sensitive subnet
  - Availability Zone C
  - Availability Zone B

- AWS Services
  - Amazon S3
  - Amazon RDS
  - AWS Directory Service
  - AWS CloudHSM
  - IAM
  - AWS KMS
  - AWS Organizations
  - AWS KMS

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Understand Your Domains

Infrastructure
- VPC Resources
- Connectivity
- On-instance
- ...

Service
- IAM
- S3 buckets
- Billing
- ...

Application
- Patching
- Coding hole
- ...

Other?
## AWS security solutions

<table>
<thead>
<tr>
<th>Identity</th>
<th>Detective control</th>
<th>Infrastructure security</th>
<th>Data protection</th>
<th>Incident response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Identity &amp; Access Management (IAM)</td>
<td>AWS CloudTrail</td>
<td>AWS Systems Manager</td>
<td>AWS Key Management Service (KMS)</td>
<td>AWS Config Rules</td>
</tr>
<tr>
<td>AWS Directory Service</td>
<td>AWS Config</td>
<td>AWS Shield</td>
<td>AWS CloudHSM</td>
<td>AWS Lambda</td>
</tr>
<tr>
<td>AWS Organizations</td>
<td>Amazon CloudWatch</td>
<td>AWS WAF – Web application firewall</td>
<td>Amazon Macie</td>
<td></td>
</tr>
<tr>
<td>AWS Secrets Manager</td>
<td>AWS CloudWatch</td>
<td>AWS Firewall Manager</td>
<td>AWS Certificate Manager</td>
<td></td>
</tr>
<tr>
<td>AWS Single Sign-On</td>
<td>VPC Flow Logs</td>
<td>Amazon Inspector</td>
<td>Server-Side Encryption</td>
<td></td>
</tr>
<tr>
<td>Amazon Cognito</td>
<td>Amazon Virtual Private Cloud (VPC)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Responding to Findings: Remediation

- VPC Flow Logs
- AWS CloudTrail
- AWS WAF
- AWS Shield
- Amazon GuardDuty
- Amazon CloudWatch
- AWS Config
- Lambda function
- Amazon EC2 Systems Manager
- AWS Step functions
- AWS APIs
- Amazon EC2
- Team collaboration (Slack etc.)

Detection
Alerting
Remediation
Countermeasures
Forensics

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
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
Welcome to GuardDuty

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)
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 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, i.e. When does an incident equal forensics time to be spent.

4. What timed procedures are being run, i.e. 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?
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]
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]

Runbooks

– Example
"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]",
  "resource": {
    "resourceType": "Instance",
    "instanceDetails": {
      "instanceId": "i-99999999",
      "instanceType": "p2.xlarge",
      "launchTime": "2017-12-20T23:46:44Z",
      "platform": null,
      "productCodes": [
        {
          "productCodeId": "GeneratedFindingProductCodeId",
          "productCodeType": "GeneratedFindingProductCodeType"
        }
      ]
    }
  }
}]

Instance: [“instanceDetails”][“instanceId”] = “i-99999999”
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....
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....

Remediation - CryptoCurrency:EC2/BitcoinTool.B!DNS

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
**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 order:

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 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. ....
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. ...

Items to Code:

• AWS Labs - https://github.com/awslabs

Examples of Code:

"type": "UnauthorizedAccess:IAMUser/UnusualASNCaller",

An API was invoked from an IP address of an unusual network.
## 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?

### Triage Table

<table>
<thead>
<tr>
<th>Finding type</th>
<th>Resource</th>
<th>Last updated</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SAMPLE] Recon IAMUser/NetworkPermissions</td>
<td>GeneratedFindingUserName: GeneratedFindi...</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] Recon IAMUser/ResourcePermissions</td>
<td>GeneratedFindingUserName: GeneratedFindi...</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] UnauthorizedAccess EC2 RDPBruteForce</td>
<td>Instance: i-999999999</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] Trojan EC2 PhishingDomainRequest DNS</td>
<td>Instance: i-999999999</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] CryptoCurrency EC2 Bitcoin Tool BIDNS</td>
<td>Instance: i-999999999</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] Trojan EC2 DropPoint DNS</td>
<td>Instance: i-999999999</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] Persistence IAMUser UserPermissions</td>
<td>GeneratedFindingUserName: GeneratedFinding...</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] UnauthorizedAccess IAMUser InstanceCreation</td>
<td>GeneratedFindingUserName: GeneratedFinding...</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] Trojan EC2/BlackholeTraffic DNS</td>
<td>Instance: i-999999999</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] Recon IAMUser UserPermissions</td>
<td>GeneratedFindingUserName: GeneratedFinding...</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] UnauthorizedAccess IAMUser TorIPCaller</td>
<td>GeneratedFindingUserName: GeneratedFinding...</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] Resource Consumption IAMUser Compute</td>
<td>GeneratedFindingUserName: GeneratedFinding...</td>
<td>9 minutes</td>
<td>1</td>
</tr>
<tr>
<td>[SAMPLE] UnauthorizedAccess EC2 SSHBruteForce</td>
<td>Instance: i-999999999</td>
<td>9 minutes</td>
<td>1</td>
</tr>
</tbody>
</table>
Remediation

```
[  
  {  
    "schemaVersion": "2.0",  
    "accountId": "710582532708",  
    "region": "us-east-2",  
    "partition": "aws",  
    "id": "12b2c8c3d5aeec3406737c61d0935b322",  
    "arn": "arn:aws:guardduty:us-east-2:710582532708:detector/ceb20cc8177a06c5e775adac2e0606a7finding/12b2c8c3d5aeec3406737c61d0935b322",  
    "type": "UnauthorizedAccess:IAMUser/UnusualASNCaller",  
    "resource": {  
      "resourceType": "AccessKey",  
      "accessKeyDetails": {  
        "accessKeyId": "GeneratedFindingAccessKeyId",  
        "principalId": "GeneratedFindingPrincipalId",  
        "userType": "IAMUser",  
        "userName": "GeneratedFindingUserName"  
      }  
    },  
    "service": {  
      "serviceName": "guardduty",  
      "detectorId": "ceb20cc8177a06c5e775adac2e0606a7",  
      "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 order:
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 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 this order:
1. Someone, email and phone number
2. Someone Else, email phone number
3. Distribution List
4. ....
5. ....
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 order:
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.
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 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

- Compliance variance
- Service disruption
- Unauthorized resources
- Unauthorized access
- Privilege escalation
- Persistence
- Excessive permissions
- Information exposure
- Credentials exposure
Key GuardDuty Partners

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

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/