aws RE:INFORCE

DEV08

Threat Hunting In Cloudtrail & Guardduty

Chris Farris
Cloud Security Lead
WARNERMEDIA

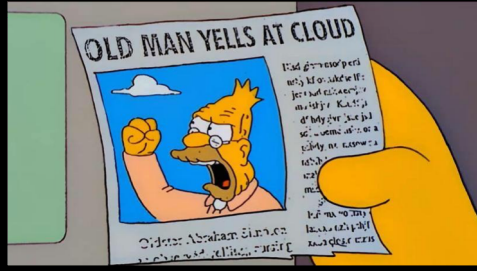
What do we say to the God of account compromise?

Goals

- Getting data into Splunk
- Splunk Queries
  - CloudTrail
  - GuardDuty
  - Resource Inventory
- What to do about with what you discover

https://www.chrisfarris.com/post/reinforce-threat-hunting/

Who Am I?



Cloud Security Architect for Turner (now WarnerMedia)

My job is to keep the Russians off cnn.com and my friends from downloading Rick & Morty

Tools

- Centralized CloudTrail
- Centralized GuardDuty
- Antiope
- Splunk

Scale

- 275 AWS Accounts
- 5m CT Events per hour
- 13% are Management Events
- 7% AssumeRole
- 2% Decrypt

Centralized Cloudtrail

- CloudTrail deployed via CFT in all accounts
- Events written to one bucket per payer
- Dedicated Logging account
- Splunk Ingests the CT Events

CloudTrail Primer


```
{
  "awsRegion": "us-east-1",
  "eventName": "CreateBucket",
  "eventSource": "s3.amazonaws.com",
  "eventTime": "2019-06-09T15:37:18Z",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012",
  "requestParameters": {},
  "responseElements": null,
  "sourceIPAddress": "192.168.357.420",
  "userAgent": "[S3Console/0.4, aws-internal/3 aws-sdk-java/1.11.56 blah]",
  "userIdentity": {
    "accessKeyId": "ASIATFNORDFNORDAZQ",
    "accountId": "123456789012",
    "arn": "arn:aws:sts::123456789012:assumed-role/rolename/email@company.com",
    "type": "AssumedRole"
  }
}
```

Root Login Detection

index=cloudtrail "userIdentity.type"=Root AND eventName=ConsoleLogin


```
{
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home?blah",
    "MFAUsed": "No",
    "MobileVersion": "No"
  },
  "eventName": "ConsoleLogin",
  "eventSource": "signin.amazonaws.com",
  "eventType": "AwsConsoleSignIn",
  "responseElements": {"ConsoleLogin": "Success"},
  "sourceIPAddress": "192.168.357.420",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac) AppleWebKit/537.36 blah",
  "userIdentity": {
    "accessKeyId": "",
    "accountId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "principalId": "123456789012",
    "type": "Root"
  }
}
```

IAM Login with no MFA

```
index=cloudtrail ConsoleLogin
"additionalEventData.MFAUsed"!=Yes
"userIdentity.type"=IAMUser
| dedup userIdentity.arn
  sourceIPAddress
| table "userIdentity.accountId"
  "userIdentity.arn"
  sourceIPAddress
  "responseElements.ConsoleLogin"
```

IAM Login Locations!

```
| iplocation sourceIPAddress
| search Country!="United States"
| table "userIdentity.accountId"
  "userIdentity.arn"
  sourceIPAddress, City, Country
  "responseElements.ConsoleLogin"
```

Expensive Ec2 Detection

```
index=cloudtrail eventName=RunInstances
| regex "requestParameters.instanceType"
=\d{2}xlarge
| dedup userIdentity.arn
| table "userIdentity.accountId"
  "userIdentity.arn"
  sourceIPAddress
  "requestParameters.instanceType"
```

Wall Of Shame


```
index=cloudtrail
eventName = AuthorizeSecurityGroupIngress
"requestParameters.ipPermissions.items{}.ipRanges.items{
}.cidrIp"="0.0.0.0/0"
"requestParameters.ipPermissions.items{}.fromPort"=22
OR
"requestParameters.ipPermissions.items{}.fromPort"=3389
| stats count by userIdentity.arn
```

User Creation Detection

```
index=cloudtrail
eventName="CreateUser"
sourceIPAddress!="357.420.*"
sourceIPAddress!="*.amazonaws.com"
| iplocation sourceIPAddress
| stats count by Country
```

User Creation - Deeper

Country	count
Argentina	20
Brazil	7
Hong Kong	4
Ireland	2
United Kingdom	4
United States	165

```
index=cloudtrail eventName="CreateUser"
sourceIPAddress!="*.amazonaws.com"
| iplocation sourceIPAddress
| search Country="Hong Kong"
```

Event Names to Care about

- `CreateClientVpnEndpoint`
- `DeleteDetector`
- `DeleteMembers`
- `DisassociateFromMasterAccount`
- `DisassociateMembers`
- `StopMonitoringMembers`
- `DeleteTrail`
- `StopLogging`
- `UpdateTrail`
- `AuthorizeSecurityGroupEgress`
- `AttachInternetGateway`

GUARDDUTY

Night’s Watch - Game of Thrones (HBO)

Centralized Guardduty

- All GuardDuty fed to centralized account
- CloudWatch Events triggers a push to Splunk to Splunk HTTP Event Collector (HEC)
- Must be done in all regions

https://github.com/turnerlabs/aws-guardduty-enterprise

How does it work?

AWS GuardDuty

- Baselines accounts
- 30 day learning period
- Leverages AWS Internal "threat lists"
- You can add your own set of trusted and bad actor IPs.

GuardDuty Findings

```
  "id": "d5b0fccf-THIS-IS-UNIQUE-PER-FINDING",
  "account": "987654321098", <-- SECURITY ACCOUNT
  "time": "2019-06-14T14:07:29Z",
  "region": "us-east-1",
  "detail": {
    "schemaVersion": "2.0",
    "accountId": "123456789012", <-- MONITORED ACCOUNT
    "region": "us-east-1",
    "partition": "aws",
    "type": "Recon:EC2/PortProbeUnprotectedPort", <-- AWS CLASSIFICATION
    "severity": 2,
    "resource": {}, <-- either AccessKey or Instance
    "service": {},
    "createdAt": "2019-02-27T23:41:19.160Z",
    "updatedAt": "2019-06-14T13:59:41.042Z",
    "title": "Unprotected port on EC2 instance i-fnord is being probed.",
    "description": "EC2 instance has an unprotected port which is being probed
by a known malicious host."
```

GuardDuty Findings - Service


```
"service": {
  "action": {
    "actionType": "PORT_PROBE",
    "portProbeAction": {
      "portProbeDetails": [
        {
          "localPortDetails": {"port": 22, "portName": "SSH"},
          "remoteIpDetails": {
            "ipAddressV4": "116.112.202.89",
            "organization": {"org": "China Unicom Neimeng"},
            "country": {"countryName": "China"},
            "city": {"cityName": "Ordos"},
            "geoLocation": {"lat": 39.6, "lon": 109.7833 }
      "blocked": false
  "resourceRole": "TARGET",
  "additionalInfo": {"threatName": "Scanner", "threatListName": "ProofPoint"},
},
```

What events are you seeing?

```
index=guardduty
| dedup id
| stats count by detail.type
```

- 66% are PortProbeUnprotectedPort
- 3% are Unusual IAM Recon Activity
- 2.5% are Logins from unusual IP addresses

Logins From New IP Addresses

```
index=guardduty
"detail.type"="UnauthorizedAccess:IAMUser/ConsoleLogin"
"detail.service....remoteIpDetails.organization.org"!="MYORG"
| dedup "detail....awsApiCallAction.remoteIpDetails.ipAddressV4"
| rename "detail.service....remoteIpDetails.country.countryName" as
Country
| rename "detail.service....remoteIpDetails.city.cityName" as City
| rename "detail.service....remoteIpDetails.organization.org" as Org
| rename "detail.resource.accessKeyDetails.userName" as UserName
| rename "detail.resource.accessKeyDetails.userType" as LoginType
| rename "detail.service....remoteIpDetails.ipAddressV4" as IPAddr
| table UserName City Country IPAddr Org LoginType
```

Logins From New IP Addrs

UserName	City	Country	IPAddr	Org	LoginType
	Atlanta	United States		AT&T U-verse	AssumedRole
	Atlanta	United States		AT&T U-verse	AssumedRole
	Los Angeles	United States		Spectrum	IAMUser
	Canton	United States		Windstream Communications	AssumedRole
	Seattle	United States		T-Mobile USA	AssumedRole
	Atlanta	United States		Cyber Wurx LLC	AssumedRole
	Bengaluru	India		Jio	AssumedRole
	Atlanta	United States		AT&T U-verse	AssumedRole
	Bengaluru	India		Bharti Airtel	AssumedRole
	Jersey City	United States			AssumedRole
	Marietta	United States		AT&T U-verse	AssumedRole
	Accra	Ghana		MTN Ghana	IAMUser
	Chicago	United States		Gogo Inflight Internet	AssumedRole
	Newark	United States		Cogent Communications	IAMUser
	Lod	Israel		INTERWISE Ltd	IAMUser
	Lawrenceville	United States		Kennesaw State University	IAMUser

RDP Brute Force Report

```
index=guardduty
"detail.type"="UnauthorizedAccess:EC2/RDPBruteForce"
| dedup id
| rename "detail.service.....remoteIpDetails.country.countryName" as
Country
| rename "detail.service.....remoteIpDetails.city.cityName" as City
| rename "detail.service.....remoteIpDetails.organization.org" as Org
| rename "detail.service.....localPortDetails.port" as Port
| rename "detail.service.....remoteIpDetails.ipAddressV4" as IPAddr
| rename "detail.resource.instanceDetails.instanceId" as Target
| dedup Target
| table City Country Org IPAddr Port Target
```

RDP Brute Force Report

City	Country	Org	IPAddr	Port	instar
	Panama	NFOrce Entertainment B.V.	45.227.255.20	3389	i-0f8
	Panama	NFOrce Entertainment B.V.	45.227.255.20	3389	i-036
	Russia	Arturas Zavaliauskas	185.254.120.21	3389	i-079
	Moldova	RM Engineering LLC	185.153.196.40	3389	i-095

This is the difference between
"you have a vulnerability"
and
"you are under attack"

Antiope

https://github.com/turnerlabs/antiope

- Lots of accounts and lots of regions makes for a big haystack
- Enterprise tools are ridiculously expensive
- AWS Config service doesn't support all AWS services at Turner
- Requirement to track (and identify) foreign AWS accounts
- Search engine to help find BGSHs
- Opensource
- Azure & GCP are in progress
- An-Tie-Oh-Pee

Robin Wright as Antiope
Wonder Woman 1984 (Warner Bros. Pictures)

Support Cases

```
index=antiope  resourceType="AWS::Support::Case"
| dedup resourceId
| table awsAccountName configuration.serviceCode
  configuration.categoryCode
  configuration.status configuration.subject
```

```
index=antiope  resourceType="AWS::Support::Case"
"configuration.serviceCode"="customer-account"
| dedup resourceId
```

Public ElasticSearch

```
index=antiope resourceType="AWS::ElasticSearch::Domain"
NOT configuration.VPCOptions.VPCId=*
NOT ".AccessPolicies.Statement{}.Condition.IpAddress.aws:SourceIp{}"=*
NOT ".AccessPolicies.Statement{}.Condition.IpAddress.aws:SourceIp"=*
NOT ".AccessPolicies.Statement{}.Condition.StringEquals.aws:SourceVpc"=*
| regex ".AccessPolicies.Statement{}.Principal.AWS"="\*"
| dedup resourceId
| table configuration.Endpoint resourceName awsAccountName
```

Taking Action

- This isn't a vendor plug, but….
- Splunk queries -> Demisto
- Demisto playbooks take automated actions
- What isn't resolved is queued for Analysts

DEMISTO

A PALO ALTO NETWORKS® COMPANY

PSA: Set Your Security Contact!

- My new goal is to find account compromise before AWS does
- But if I don't - AWS Abuse will be reaching out
- Make sure to set the account security contact if your IR team isn't on the root email list for every account

https://www.chrisfarris.com/post/reinforce-threat-hunting/

- @jcfarris
- https://github.com/jchrisfarris
- https://www.linkedin.com/in/jcfarris
- http://www.chrisfarris.com
- https://github.com/turnerlabs/antiope