
AWS
re:Invent

SEC313

A security operator's guide to practical AWS CloudTrail analysis

Brian Andrzejewski

Sr. Security Consultant, Customer Incident Response

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Review of AWS CloudTrail as security operators (SecOps)

Discuss the key anatomy of a CloudTrail event

Identify sources of data enrichment for a CloudTrail event

How to use CloudTrail events for analysis



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

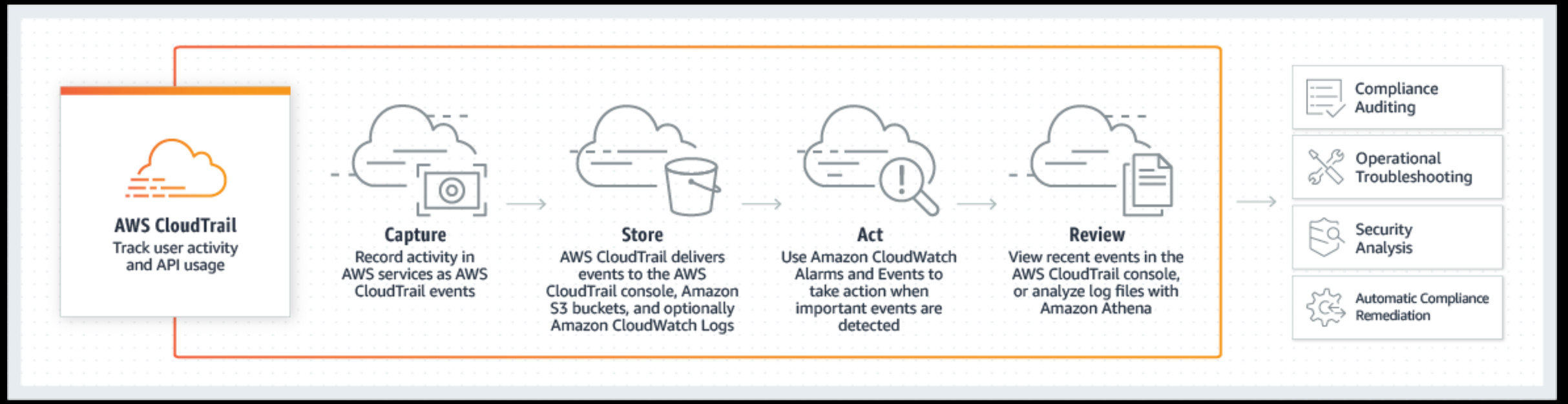
CloudTrail:
What it is and what it does



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudTrail provides audit logs for AWS



An audit log of an AWS account's
authenticated request to perform an action
with an AWS service and its resources

How CloudTrail can help Security Operations

- View, search, download, archive, analyze, and respond to account activity across your AWS services
- Gain detailed visibility into user, service, and resource activity
- Troubleshoot security and operational issues by tracking changes in your accounts
- Build detective security controls and automate their response around important CloudTrail event activity

How CloudTrail works for SecOps

- CloudTrail captures actions made directly by the user or on behalf of the user by an AWS service

- CloudTrail events are available to the AWS account within 15 minutes:
  - CloudTrail event history in AWS Management Console for 90 calendar days
  - CloudTrail trails as log data (if enabled and configured by customer)
  - Amazon EventBridge as events that can be filtered as a trigger for further action (if configured by customer)
  - Ingested independently by AWS security services if enabled (for example: Amazon GuardDuty, Amazon Detective)





CloudTrail event history and trails

WHAT IS THE DIFFERENCE?

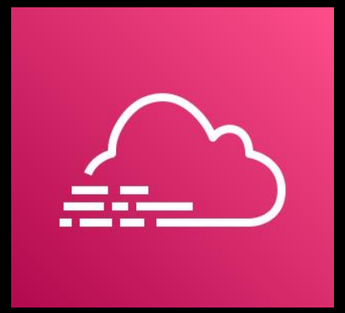
CloudTrail event history

- Enabled on creation of an AWS account
- Events are available for up to 90 days per Region, per account
- Available for limited search via the AWS Management Console or AWS CLI
- Can only search one Region at a time
- Events can be viewed or downloaded as CSV summary or JSON objects

CloudTrail trail

- Must be enabled by the customer in their AWS account
- Extends past 90 days after trail creation defaulted to multi-Region per account
- Search events via Amazon CloudWatch Logs insights, read from Amazon S3 into Amazon Athena for all fields, or load into third-party software
- Can be aggregated to search one-to-many AWS accounts and their Regions in Amazon S3 and third-party software

CloudTrail event search and analytics in AWS



CloudTrail event history

Always available to view and download the last 90 days of events per Region within AWS account

CloudTrail trail outputs



Amazon S3

Saves a CloudTrail trail event as a series of compressed logs in Amazon S3



CloudWatch Logs

Saves each CloudTrail event as a log event into a CloudWatch Logs

CloudTrail events search



Athena

Query and analyze your CloudTrail logs from your Amazon S3 bucket as SQL statements



CloudWatch insights

Search and analyze your CloudTrail events from their CloudWatch Logs group

20+ partner integrations for operational and security solutions

Anatomy of a CloudTrail event



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Critical CloudTrail event fields



Who

userIdentity.arn

sourceIPAddress

userAgent



What

accountId

eventSource

eventName

requestParameters



When

eventTime

awsRegion



How

eventType

userIdentity.type

userIdentity.accessKeyId

userIdentity.invokedBy



Result

eventID

errorCode

responseElements

sharedEventID

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html

CloudTrail event types

- Management events – enabled by default
  - Records of control plane operations that are performed on or within resources
- Data events – not enabled by default
  - Records of data plane operations that are performed on or within a **supported** AWS resource
  - Available for Amazon S3 objects events and Lambda execution at an additional cost
- Insights events – not enabled by default
  - Records unusual call volume of write management APIs in your AWS account up to 90 days

CloudTrail deep dive: userIdentity

KNOWING "USERIDENTITY"

- Type of AWS Identity and Access Management (IAM) identity that made the request (userIdentity.type, userIdentity.accessKeyId)
- Who used the credentials:
  - Principal who made the request (userIdentity.arn, userIdentity.principalId)
  - Friendly name for the identity (userIdentity.username)
  - AWS account made from (userIdentity.accountId)
- If temporary credentials were used:
  - How the credentials were obtained (userIdentity.sessionContext object AND userIdentity.sessionIssuer)
- If IAM identity was invoked by an AWS service (userIdentity.invokedBy)

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html

CloudTrail deep dive: IAM user examples

IAM user – Access Key

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn":
"arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "Alice"
}
```

IAM user – STS (console login)

```
"userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAIT6PBPQYAB2QOUEGW",
    "arn":
"arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "ASIASJ5PL7KYQZCMJFXQ",
    "userName": ”Alice",
    "sessionContext": {
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2019-01-
24T08:44:35Z"
        }
    }
}
```

CloudTrail deep dive: IAM role examples

IAM role – STS


```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
  "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
  "accountId": "123456789012",
  "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
  "sessionContext": {…}
}
```


IAM role – EC2


```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROAI3Z7EONDPA7LZ4RGM:i-0123456789abc0",
  "arn": "arn:aws:sts::123456789012:assumed-role/EC2InstanceRoleName/i-0123456789abc0",
  "accountId": "123456789012"
  "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
  "sessionContext": {…}
}
```

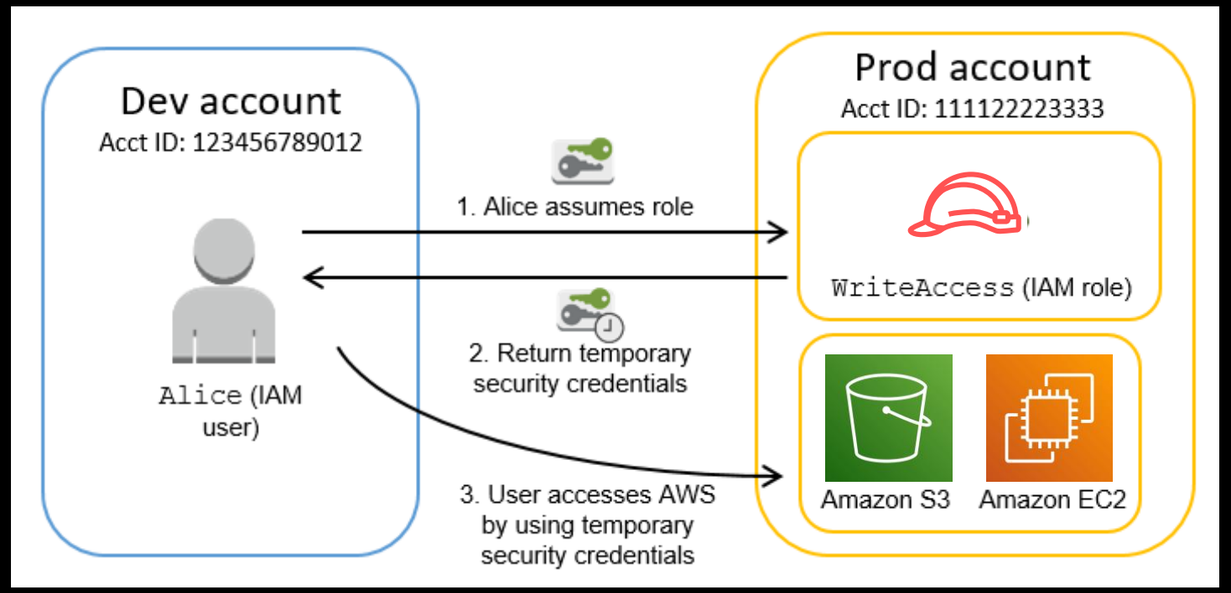
Advanced: Identifying cross-account access

Source account (S)

- Unique account requestID and eventID
- Same sharedEventID for both accounts
- userIdentity.account of source account
- recipientAccountId of source account

Destination account (D)

- Unique account requestID and eventID
- Same sharedEventID for both accounts
- userIdentity.account of source account
- recipientAccountId of destination account



Using CloudTrail events for analysis



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Our scenario

- DevOps team has identified unusual Amazon EC2s being seen in Region us-west-1 when the team operates in Region us-east-1
- Amazon GuardDuty detected the same EC2s in us-west-1 querying an IP address that is associated with cryptocurrency-related activity
- AWS Abuse has issued a notice that one of your IAM access keys has been compromised prior to the EC2s being seen by your DevOps team

Key enrichment sources for CloudTrail events



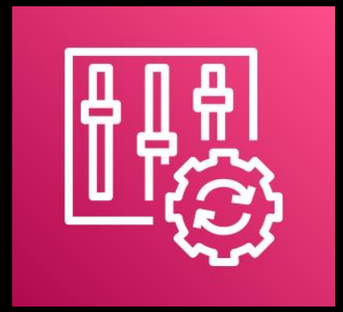
Geo IP attribution

Know your AWS account access sourceIpAddress to their ISPs and geographic IP network usage



Amazon GuardDuty

Context for detecting known threats with threat intelligence and unknown threats with anomaly detection



AWS Config Recorder

Work backward from resource configuration states to build your timeline analysis

SecOps “hunting” with CloudTrail

ESTABLISH YOUR HUNT

- Set your desired outcomes
  - Identify who and what executed EC2 launches outside of Region us-east-1
  - Explore why AWS Abuse provided a notice against an IAM access key
- Set a hypothesis to prove/disprove
- Work backward from the known events if interrelated
  - Investigate eventType:RunInstances for the unknown EC2 launches
  - Evaluate events using the userIdentity.accessKeyId provided by AWS Abuse notice

SecOps “hunting” with CloudTrail

BEHAVIOR PROFILE YOUR AWS ACCOUNT USAGE TO USERIDENTITY.ARN

- Review eventName from their eventSource
- Identify key userIdentity.arn of interest to profile their behavior
- Evaluate each userIdentity.arn of interest for both readonly types
  - Evaluate (sourceIPAddress + userAgent) changes over time to identity
  - Look for changes in behavior of AWS service usage across Regions for each userIdentity.arn
  - Look at the eventTime to produce a timeline of events for each userIdentity.arn

SecOps “hunting” with CloudTrail

DEEP DIVE ON ANOMALIES

- Establish key summary fields needed for your search across AWS service events

  .eventTime, .eventID, .userIdentity.arn, .userIdentity.accessKeyId, .readOnly, .eventType, .eventSource, .eventName, .sourceIPAddress, .userAgent, .sharedEventId, .errorCode, .errorMessage

- Review for GuardDuty findings by detectors in Region https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html

- Once finding an event “of interest,” begin to pivot and add fields:
  - requestParameters to evaluate what was sent in the request to the AWS service
  - responseElements to review the result of how the AWS service responded to the event

SecOps “hunting” with CloudTrail

APPLYING TO SCENARIO

- Evaluate for all Regions for readonly:false for 1 week
- Capture the userIdentity.arn for eventName:RunInstances starting November 1 for 1 week for all Regions
- Pivot search to userIdentity.arn for their prior activity to eventName
- Evaluate sourceIpAddress and userIdentity used for their actions
- Evaluate if other userIdentity.arn related to sourceIpAddress

Review



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Other re:Invent 2020 sessions of interest

- SEC301: Security investigations with Amazon Detective
- SEC306: Automated forensic artifact collection on AWS with Goldman Sachs
- SEC307: Use Amazon GuardDuty and AWS Security Hub to secure multiple accounts

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.