AWS CloudTrail Cheat Sheet

This cheat sheet contains events names that are commonly used to search the CloudTrail logging for suspicious activity.

Contact us

info@invictus-ir.com

GitHub

https://github.com/invictus-ir/aws-cheatsheet

> Initial Access

Initial Access consists of techniques that use various entry vectors to gain their initial foothold in AWS.

- ConsoleLogin
- PasswordRecoveryRequested

> Execution

Execution consists of techniques that result in adversary-controlled code running on a local or remote system.

- SendCommand
- StartInstance
- StartInstances
- Invoke

> Persistence

Persistence consists of techniques that adversaries use to keep access to systems across restarts and other interruptions that could cut off their access.

- CreateAccessKey
- CreateUser
- CreateNetworkAclEntry
- CreateRoute
- CreateLoginProfile
- AuthorizeSecurityGroupEgress
- AuthorizeSecurityGroupIngress
- CreateVirtualMFADevice
- CreateConnection
- ApplySecurityGroupsToLoadBalancer
- SetSecurityGroups
- AuthorizeDBSecurityGroupIngress
- CreateDBSecurityGroup
- ChangePassword

> Privilege Escalation

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions in an AWS account.

- CreateGroup
- CreateRole
- UpdateAccessKey
- PutGroupPolicy
- PutRolePolicy
- PutUserPolicy
- AddRoleToInstanceProfile
- AddUserToGroup

> Defense Evasion

Defense Evasion consists of techniques that adversaries use to avoid detection or hinder response actions.

- StopLogging
- DeleteTrail
- UpdateTrail
- PutEventSelectors
- DeleteFlowLogs
- DeleteDetector
- DeleteMembers
- DeleteSnapshot
- DeactivateMFADevice
- DeleteCertificate
- DeleteConfigRule
- DeleteAccessKey
- LeaveOrganization
- DisassociateFromMasterAccount
- DisassociateMembers
- StopMonitoringMembers

> Credential Access

Credential Access consists of techniques for stealing credentials like access keys, certificates or passwords.

- GetSecretValue
- RequestCertificate
- UpdateAssumeRolePolicy
- GetPasswordData

> Lateral Movement

Lateral Movement consists of techniques that adversaries use to move around in an AWS environment.

- AssumeRole
- SwitchRole

> Discovery

Discovery consists of techniques an adversary may use to gain knowledge about the users, groups, roles and policies in an AWS account.

- ListUsers
- ListRoles
- ListIdentities
- ListAccessKeys
- ListServiceQuotas
- ListInstanceProfiles
- ListBuckets
- ListGroups
- GetCallerIdentity
- DescribeInstances
- GetBucketAcl
- GetBucketVersioning
- GetSendQuota
- GetAccountAuthorizationDetails

> Exfiltration

Exfiltration consists of techniques that adversaries may use to steal data from your AWS resources.

- CreateSnapShot
- ModifySnapshotAttributes
- ModifyImageAttribute
- SharedSnapshotCopyInitiated
- SharedSnapshotVolumeCreated
- ModifyDBSnapshotAttribute
- PutBucketPolicy
- PutBucketAcl

> Impact

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating AWS resources.

- PutBucketVersioning
- RunInstances
- DeleteAccountPublicAccessBlock

INVICTUS

INCIDENT RESPONSE