Cortex XDR Analytics Alert Reference by data source

1 | Cortex XDR Analytics Alert Reference

The Cortex XDR Analytics Alert Reference provides a description of every Cortex XDR Analytics Alert. Use this reference to understand what an alert means and what you should do about it.

The Analytics alerts that Cortex XDR can raise depend on the data sources you integrate with Cortex XDR. For example if the Cortex XDR agent is your only data source, the app raises only the alerts it can detect from agent endpoint data. Some alerts can also require a combination of data sources in order to raise the alert. Additionally, you can improve the accuracy of some Analytics alerts by adding additional data sources. For more information about the data sources you must configure to trigger alerts, see the Cortex XDR Administrator Guide or the Cortex XSIAM Administrator Guide

2 | Required Data Sources

Data Sources	Topics
AWS Audit Log	A Kubernetes Cronjob was created
	An AWS RDS Global Cluster Deletion
	Object versioning was disabled
	Suspicious usage of EC2 token
	Unusual secret management activity
	Kubernetes network policy modification
	Penetration testing tool activity
	Denied API call by a Kubernetes service account
	AWS CloudWatch log group deletion
	Kubernetes pod creation with host network
	IAM User added to an IAM group
	Unusual key management activity
	Cloud storage automatic backup disabled

Data Sources	Topics
	Cloud Trail Logging has been stopped/suspended
	Cloud snapshot of a database or storage instance was publicly shared
	A Command Line Interface (CLI) command was executed from an AWS serverless compute service
	An AWS EKS cluster was created or deleted
	A cloud function was created with an unusual runtime
	Kubernetes Pod created with host process ID (PID) namespace
	AWS config resource deletion
	A cloud identity had escalated its permissions
	AWS RDS cluster deletion
	A Kubernetes StatefulSet was created
	An AWS SAML provider was modified
	A Kubernetes service account executed an unusual API call

Data Sources	Topics
	An Email address was added to AWS SES
	Unusual Identity and Access Management (IAM) activity
	An AWS RDS instance was created from a snapshot
	An IAM group was created
	A Kubernetes node service account activity from external IP
	MFA device was removed/deactivated from an IAM user
	An AWS S3 bucket configuration was modified
	A Kubernetes deployment was created
	A Kubernetes service account was created or deleted
	An AWS ElastiCache security group was modified or deleted
	Unusual resource modification/creation
	Unusual certificate management activity
	A Kubernetes ephemeral container was created

Data Sources	Topics
	A Kubernetes secret was created or deleted
	A Kubernetes Pod was created with a sidecar container
	Cloud compute instance user data script modification
	A Kubernetes ReplicaSet was created
	AWS CloudWatch log stream deletion
	A Kubernetes Pod was deleted
	An AWS Lambda function was modified
	An AWS SES identity was deleted
	AWS user creation
	Cloud compute serial console access
	AWS network ACL rule creation
	Cloud impersonation attempt by unusual identity type
	A cloud identity created or modified a security group

Data Sources	Topics
	AWS Root account activity
	Kubernetes Pod Created with host Inter Process Communications (IPC) namespace
	Kubernetes Privileged Pod Creation
	Kubernetes pod creation from unknown container image registry
	A cloud snapshot was created or modified
	An identity attached an administrative policy to an IAM user/role
	AWS STS temporary credentials were generated
	An AWS Lambda Function was created
	A cloud identity invoked IAM related persistence operations
	An AWS EFS file-share was deleted
	AWS Flow Logs deletion
	Suspicious API call from a Tor exit node

Data Sources	Topics
	A Kubernetes service account has enumerated its permissions
	A Kubernetes namespace was created or deleted
	AWS Config Recorder stopped
	AWS Cloud Trail log trail modification
	Cloud storage delete protection disabled
	Cloud Trail logging deletion
	EC2 snapshot attribute has been modified
	AWS SecurityHub findings were modified
	A user logged in to the AWS console for the first time
	Kubernetes Pod Created With Sensitive Volume
	Disable encryption operations
	AWS network ACL rule deletion
	An AWS database service master user password was changed

Data Sources	Topics
	An AWS GuardDuty IP set was created
	AWS IAM resource group deletion
	Cloud unusual access key creation
	Unusual cloud identity impersonation
	Penetration testing tool attempt
	A Kubernetes cluster role binding was created or deleted
	An identity created or updated password for an IAM user
	Kubernetes vulnerability scanning tool usage
	Remote usage of an AWS service token
	Remote usage of AWS Lambda's token
	An AWS SES Email sending settings were modified
	A cloud instance was stopped
	Aurora DB cluster stopped

Data Sources	Topics
	A compute-attached identity executed API calls outside the instance's region
	An identity disabled bucket logging
	A Kubernetes API operation was successfully invoked by an anonymous user
	Network sniffing detected in Cloud environment
	A Kubernetes role binding was created or deleted
	An AWS EFS File-share mount was deleted
	Suspicious cloud compute instance ssh keys modification attempt
	Unusual IAM enumeration activity by a non-user Identity
	A Kubernetes cluster was created or deleted
	AWS Role Trusted Entity modification
	Kubernetes cluster events deletion
	Data encryption was disabled

Data Sources	Topics
	An operation was performed by an identity from a domain that was not seen in the organization
	Cloud Watch alarm deletion
	Kubernetes service account activity outside the cluster
	A Kubernetes service was created or deleted
	An identity started an AWS SSM session
	A Kubernetes ConfigMap was created or deleted
	A cloud storage configuration was modified
	AWS EC2 instance exported into S3
	AWS web ACL deletion
	Cloud email service activity
	An AWS ElastiCache security group was created
	Cloud identity reached a throttling API rate
	Kubernetes admission controller activity

Data Sources	Topics
	S3 configuration deletion
	Unusual AWS systems manager activity
	AWS SSM send command attempt
	A Kubernetes DaemonSet was created
	A container registry was created or deleted
	A cloud identity executed an API call from an unusual country
	Unusual cross projects activity
	Unusual exec into a Kubernetes Pod
	Unusual resource modification by newly seen IAM user
	An AWS Route 53 domain was transferred to another AWS account
	AWS Guard-Duty detector deletion
	Suspicious heavy allocation of compute resources - possible mining activity

Data Sources	Topics
	A Kubernetes dashboard service account was used outside the cluster
	Activity in a dormant region of a cloud project
	Billing admin role was removed
	Suspicious objects encryption in an AWS bucket
	Abnormal Allocation of compute resources in multiple regions
	An identity dumped multiple secrets from a project
	Storage enumeration activity
	Suspicious identity downloaded multiple objects from a bucket
	Cloud user performed multiple actions that were denied
	Kubernetes enumeration activity
	Allocation of multiple cloud compute resources
	IAM Enumeration sequence
	Multiple cloud snapshots export

Data Sources	Topics
	Multiple failed logins from a single IP
	An identity performed a suspicious download of multiple cloud storage objects
	Cloud infrastructure enumeration activity
	Deletion of multiple cloud resources
	Multi region enumeration activity
AWS Flow Log	Possible DCShadow attempt
	Unusual SSH activity that resembles SSH proxy
	An internal Cloud resource performed port scan on external networks
	SSH brute force attempt

Data Sources	Topics
AWS OCSF Flow Logs	Possible DCShadow attempt
	Unusual SSH activity that resembles SSH proxy
	An internal Cloud resource performed port scan on external networks
	SSH brute force attempt

Data Sources	Topics
Azure Audit Log	A Kubernetes Cronjob was created
	Object versioning was disabled
	Unusual secret management activity
	Azure Blob Container Access Level Modification
	Kubernetes network policy modification
	Penetration testing tool activity
	Denied API call by a Kubernetes service account
	Kubernetes pod creation with host network
	Azure user creation/deletion
	Azure mailbox rule creation
	Azure Key Vault modification
	An Azure Kubernetes Role or Cluster-Role was modified
	Unusual key management activity

Data Sources	Topics
	External user invitation to Azure tenant
	Cloud storage automatic backup disabled
	Kubernetes Pod created with host process ID (PID) namespace
	A cloud identity had escalated its permissions
	A Kubernetes StatefulSet was created
	A Kubernetes service account executed an unusual API call
	A Kubernetes node service account activity from external IP
	Credentials were added to Azure application
	Azure Network Watcher Deletion
	Azure Event Hub Deletion
	A Kubernetes deployment was created
	A Kubernetes service account was created or deleted
	Unusual resource modification/creation

Data Sources	Topics
	Unusual certificate management activity
	A Kubernetes ephemeral container was created
	Remote usage of an Azure Managed Identity token
	Azure Automation Webhook creation
	An Azure Kubernetes Cluster was created or deleted
	A Kubernetes secret was created or deleted
	A Kubernetes Pod was created with a sidecar container
	A Kubernetes ReplicaSet was created
	A Kubernetes Pod was deleted
	An Azure Network Security Group was modified
	An Azure virtual network was modified
	Azure diagnostic configuration deletion
	Cloud compute serial console access

Data Sources	Topics
	Azure Event Hub Authorization rule creation/modification
	A cloud identity created or modified a security group
	Azure group creation/deletion
	Kubernetes Pod Created with host Inter Process Communications (IPC) namespace
	An identity accessed Azure Kubernetes Secrets
	An Azure virtual network Device was modified
	An Azure Suppression Rule was created
	Kubernetes Privileged Pod Creation
	Kubernetes pod creation from unknown container image registry
	Azure device code authentication flow used
	OneDrive file download
	A cloud snapshot was created or modified
	Privileged role used by Azure application

Data Sources	Topics
	A cloud identity invoked IAM related persistence operations
	Suspicious API call from a Tor exit node
	An Azure Firewall Rule Collection was modified
	A Kubernetes service account has enumerated its permissions
	A Kubernetes namespace was created or deleted
	Azure conditional access policy creation or modification
	Azure Storage Account key generated
	An identity was granted permissions to manage user access to Azure resources
	Cloud storage delete protection disabled
	Azure Key Vault Secrets were modified
	Azure user password reset
	Azure Automation Runbook Creation/Modification
	An Azure Firewall policy deletion

Data Sources	Topics
	Kubernetes Pod Created With Sensitive Volume
	Modification or Deletion of an Azure Application Gateway Detected
	An Azure VPN Connection was modified
	OneDrive file upload
	An Azure firewall rule group was modified
	A Kubernetes cluster role binding was created or deleted
	Owner was added to Azure application
	Azure Service principal/Application creation
	Kubernetes vulnerability scanning tool usage
	Authentication method was added to Azure account
	PIM privilege member removal
	Azure permission delegation granted
	A cloud instance was stopped

Data Sources	Topics
	Unusual resource access by Azure application
	A Kubernetes API operation was successfully invoked by an anonymous user
	Azure Automation Account Creation
	Network sniffing detected in Cloud environment
	A Kubernetes role binding was created or deleted
	Suspicious cloud compute instance ssh keys modification attempt
	Azure virtual machine commands execution
	An Azure Key Vault key was modified
	Remote usage of an Azure Service Principal token
	A Kubernetes cluster was created or deleted
	Kubernetes cluster events deletion
	An Azure application reached a throttling API rate

Data Sources	Topics
	An Azure Kubernetes Role-Binding or Cluster-Role-Binding was modified or deleted
	An operation was performed by an identity from a domain that was not seen in the organization
	A Service Principal was created in Azure
	Kubernetes service account activity outside the cluster
	A Kubernetes service was created or deleted
	Azure application removed
	Soft delete of cloud storage configuration was disabled
	Attempted Azure application access from unknown tenant
	An Azure DNS Zone was modified
	An Azure Kubernetes Service Account was modified or deleted
	A Kubernetes ConfigMap was created or deleted
	A cloud storage configuration was modified
	Cloud email service activity

Data Sources	Topics
	Cloud identity reached a throttling API rate
	Azure Resource Group Deletion
	Kubernetes admission controller activity
	A Service Principal was removed from Azure
	An Azure Firewall was modified
	Removal of an Azure Owner from an Application or Service Principal
	An Azure Point-to-Site VPN was modified
	A Kubernetes DaemonSet was created
	Azure Kubernetes events were deleted
	A container registry was created or deleted
	Granting Access to an Account
	Azure Automation Runbook Deletion
	A cloud identity executed an API call from an unusual country

Data Sources	Topics
	Unusual cross projects activity
	OneDrive folder creation
	Unusual exec into a Kubernetes Pod
	Unusual resource modification by newly seen IAM user
	A New Server was Added to an Azure Active Directory Hybrid Health ADFS Environment
	An Azure Key Vault was modified
	Suspicious heavy allocation of compute resources - possible mining activity
	A Kubernetes dashboard service account was used outside the cluster
	Activity in a dormant region of a cloud project
	An Azure Cloud Shell was Created
	Billing admin role was removed
	Microsoft Teams enumeration activity

Data Sources	Topics
	Abnormal Allocation of compute resources in multiple regions
	An identity dumped multiple secrets from a project
	Storage enumeration activity
	Suspicious identity downloaded multiple objects from a bucket
	Cloud user performed multiple actions that were denied
	Mailbox enumeration activity by Azure application
	Kubernetes enumeration activity
	Allocation of multiple cloud compute resources
	Multiple cloud snapshots export
	Multiple failed logins from a single IP
	Azure high-volume data transfer
	Microsoft OneDrive enumeration activity
	An identity performed a suspicious download of multiple cloud storage objects

Data Sources	Topics
	An Azure identity performed multiple actions that were denied
	Deletion of multiple cloud resources
	Microsoft SharePoint enumeration activity
	Azure enumeration activity using Microsoft Graph API
	Multi region enumeration activity
Azure Flow Log	Possible DCShadow attempt
	Unusual SSH activity that resembles SSH proxy
	An internal Cloud resource performed port scan on external networks
	SSH brute force attempt

Data Sources	Topics
Azure SignIn Log	Suspicious SSO access from ASN
	SSO with abnormal user agent
	A user connected from a new country
	First SSO access from ASN in organization
	SSO authentication by a machine account
	First SSO access from ASN for user
	A user logged in at an unusual time via SSO
	User attempted to connect from a suspicious country
	First connection from a country in organization
	SSO authentication by a service account
	A disabled user attempted to authenticate via SSO
	First SSO Resource Access in the Organization
	SSO with new operating system

Data Sources	Topics
	A successful SSO sign-in from TOR
	A user accessed multiple unusual resources via SSO
	SSO Brute Force
	Impossible traveler - SSO
	SSO Password Spray
	Intense SSO failures

Data Sources	Topics
AzureAD	Suspicious SSO access from ASN
	SSO with abnormal user agent
	SSO authentication attempt by a honey user
	Suspicious authentication with Azure Password Hash Sync user
	A user connected from a new country
	First SSO access from ASN in organization
	SSO authentication by a machine account
	First SSO access from ASN for user
	A user logged in at an unusual time via SSO
	User attempted to connect from a suspicious country
	First connection from a country in organization
	SSO authentication by a service account
	A disabled user attempted to authenticate via SSO

Data Sources	Topics
	First SSO Resource Access in the Organization
	SSO with new operating system
	A successful SSO sign-in from TOR
	SSO with abnormal operating system
	Suspicious Azure AD interactive sign-in using PowerShell
	A user accessed multiple unusual resources via SSO
	SSO Brute Force
	Impossible traveler - SSO
	SSO Password Spray
	Intense SSO failures

Data Sources	Topics
AzureAD Audit Log	Authentication method added to an Azure account
	MFA was disabled for an Azure identity
	Device Registration Policy modification
	Azure application credentials added
	Azure AD PIM alert disabled
	BitLocker key retrieval
	Identity assigned an Azure AD Administrator Role
	Azure account deletion by a non-standard account
	Successful unusual guest user invitation
	Azure AD PIM role settings change
	Azure account creation by a non-standard account
	Azure domain federation settings modification attempt
	Azure AD PIM elevation request

Data Sources	Topics
	Conditional Access policy removed
	First Azure AD PowerShell operation for a user
	Azure application consent
	Unusual Conditional Access operation for an identity
	Owner added to Azure application
	Azure service principal assigned app role
	Azure application URI modification
	Azure Temporary Access Pass (TAP) registered to an account
	Unverified domain added to Azure AD
	Azure AD account unlock/password reset attempt
	Short-lived Azure AD user account
	Multiple Azure AD admin role removals

Data Sources	Topics
Box Audit Log	Suspicious SaaS API call from a Tor exit node
	Massive file downloads from SaaS service
	External SaaS file-sharing activity
	Massive upload to SaaS service
DropBox	Suspicious SaaS API call from a Tor exit node
	Massive file downloads from SaaS service
	External SaaS file-sharing activity
	Massive upload to SaaS service

Data Sources	Topics
Duo	Suspicious SSO access from ASN
	SSO with abnormal user agent
	A user connected from a new country
	First SSO access from ASN in organization
	SSO authentication by a machine account
	First SSO access from ASN for user
	A user logged in at an unusual time via SSO
	User attempted to connect from a suspicious country
	First connection from a country in organization
	SSO authentication by a service account
	A disabled user attempted to authenticate via SSO
	First SSO Resource Access in the Organization
	SSO with new operating system

Data Sources	Topics
	A successful SSO sign-in from TOR
	A user accessed multiple unusual resources via SSO
	SSO Brute Force
	Impossible traveler - SSO
	SSO Password Spray
	Intense SSO failures

Data Sources	Topics
Gcp Audit Log	A Kubernetes Cronjob was created
	GCP Virtual Private Cloud (VPC) Network Deletion
	Unusual secret management activity
	Remote usage of an App engine Service Account token
	Kubernetes network policy modification
	Penetration testing tool activity
	Denied API call by a Kubernetes service account
	Kubernetes pod creation with host network
	Unusual key management activity
	Cloud storage automatic backup disabled
	A cloud function was created with an unusual runtime
	Kubernetes Pod created with host process ID (PID) namespace
	A cloud identity had escalated its permissions

Data Sources	Topics
	A Kubernetes StatefulSet was created
	A Kubernetes service account executed an unusual API call
	Unusual Identity and Access Management (IAM) activity
	A Kubernetes node service account activity from external IP
	A Kubernetes deployment was created
	A Kubernetes service account was created or deleted
	GCP Pub/Sub Topic Deletion
	Unusual resource modification/creation
	Unusual certificate management activity
	A Kubernetes ephemeral container was created
	A Kubernetes secret was created or deleted
	A Kubernetes Pod was created with a sidecar container
	Cloud compute instance user data script modification

Data Sources	Topics
	A Kubernetes ReplicaSet was created
	A Kubernetes Pod was deleted
	GCP Storage Bucket Configuration Modification
	GCP Firewall Rule creation
	Cloud compute serial console access
	Cloud impersonation attempt by unusual identity type
	A cloud identity created or modified a security group
	GCP Pub/Sub Subscription Deletion
	GCP IAM Service Account Key Deletion
	Kubernetes Pod Created with host Inter Process Communications (IPC) namespace
	GCP Logging Bucket Deletion
	Kubernetes Privileged Pod Creation
	GCP Virtual Private Network Route Creation

Data Sources	Topics
	Kubernetes pod creation from unknown container image registry
	GCP Service Account key creation
	A cloud snapshot was created or modified
	A Command Line Interface (CLI) command was executed from a GCP serverless compute service
	A cloud identity invoked IAM related persistence operations
	Suspicious API call from a Tor exit node
	A Kubernetes service account has enumerated its permissions
	A Kubernetes namespace was created or deleted
	Cloud storage delete protection disabled
	GCP Virtual Private Network Route Deletion
	Kubernetes Pod Created With Sensitive Volume
	Cloud unusual access key creation
	Unusual cloud identity impersonation

Data Sources	Topics
	A Kubernetes cluster role binding was created or deleted
	Remote usage of VM Service Account token
	Kubernetes vulnerability scanning tool usage
	GCP Service Account Disable
	Cloud Organizational policy was created or modified
	GCP IAM Role Deletion
	A cloud instance was stopped
	GCP Firewall Rule Modification
	A Kubernetes API operation was successfully invoked by an anonymous user
	Network sniffing detected in Cloud environment
	A Kubernetes role binding was created or deleted
	Suspicious cloud compute instance ssh keys modification attempt
	Unusual IAM enumeration activity by a non-user Identity

Data Sources	Topics
	A Kubernetes cluster was created or deleted
	Kubernetes cluster events deletion
	GCP Service Account deletion
	GCP Storage Bucket deletion
	An operation was performed by an identity from a domain that was not seen in the organization
	Kubernetes service account activity outside the cluster
	A Kubernetes service was created or deleted
	A Kubernetes ConfigMap was created or deleted
	A cloud storage configuration was modified
	GCP Service Account creation
	Cloud identity reached a throttling API rate
	Kubernetes admission controller activity
	GCP IAM Custom Role Creation

Data Sources	Topics
	A Kubernetes DaemonSet was created
	A container registry was created or deleted
	GCP VPC Firewall Rule Deletion
	GCP Storage Bucket Permissions Modification
	GCP set IAM policy activity
	A cloud identity executed an API call from an unusual country
	Unusual cross projects activity
	Unusual exec into a Kubernetes Pod
	Unusual resource modification by newly seen IAM user
	Suspicious heavy allocation of compute resources - possible mining activity
	A Kubernetes dashboard service account was used outside the cluster
	Activity in a dormant region of a cloud project
	Billing admin role was removed

Data Sources	Topics
	GCP Logging Sink Deletion
	GCP Logging Sink Modification
	Abnormal Allocation of compute resources in multiple regions
	An identity dumped multiple secrets from a project
	Storage enumeration activity
	Suspicious identity downloaded multiple objects from a bucket
	Cloud user performed multiple actions that were denied
	Kubernetes enumeration activity
	Allocation of multiple cloud compute resources
	IAM Enumeration sequence
	Multiple cloud snapshots export
	Multiple failed logins from a single IP
	An identity performed a suspicious download of multiple cloud storage objects

Data Sources	Topics
	Cloud infrastructure enumeration activity
	Deletion of multiple cloud resources
	Multi region enumeration activity
Gcp Flow Log	Possible DCShadow attempt
	Unusual SSH activity that resembles SSH proxy
	An internal Cloud resource performed port scan on external networks
	SSH brute force attempt

Data Sources	Topics
Google Workspace Audit Logs	Gmail routing settings changed
	Data Sharing between GCP and Google Workspace was disabled
	External Sharing was turned on for Google Drive
	A Google Workspace service was configured as unrestricted
	A GCP service account was delegated domain-wide authority in Google Workspace
	User accessed SaaS resource via anonymous link
	A Google Workspace user was added to a group
	Admin privileges were granted to a Google Workspace user
	MFA Disabled for Google Workspace
	A third-party application's access to the Google Workspace domain's resources was revoked
	A Google Workspace identity used the security investigation tool
	Suspicious SaaS API call from a Tor exit node

Data Sources	Topics
	SaaS suspicious external domain user activity
	A Google Workspace identity created, assigned or modified a role
	A Google Workspace Role privilege was deleted
	An app was added to Google Marketplace
	Google Workspace organizational unit was modified
	A domain was added to the trusted domains list
	An app was removed from a blocked list in Google Workspace
	A Google Workspace user was removed from a group
	An app was added to the Google Workspace trusted OAuth apps list
	Google Workspace third-party application's security settings were changed
	A mail forwarding rule was configured in Google Workspace
	Google Marketplace restrictions were modified

Data Sources	Topics
	A Google Workspace identity performed an unusual admin console activity
	Gmail delegation was turned on for the organization
	A third-party application was authorized to access the Google Workspace APIs
	Massive file downloads from SaaS service
	External SaaS file-sharing activity
	Massive upload to SaaS service
Google Workspace Authentication	Suspicious SSO access from ASN
	First SSO access from ASN in organization
	First SSO access from ASN for user
	A user logged in at an unusual time via SSO

Data Sources	Topics
Health Monitoring Data	Collection error
	Parsing Rule Error
	Error in event forwarding
	Correlation rule error
	Logs were not collected from a data source for an abnormally long time

Data Sources	Topics
Office 365 Audit	Exchange user mailbox forwarding
	Exchange inbox forwarding rule configured
	Exchange email-hiding transport rule
	User accessed SaaS resource via anonymous link
	SharePoint Site Collection admin group addition
	Exchange audit log disabled
	Exchange Safe Link policy disabled or removed
	Exchange DKIM signing configuration disabled
	Penetration testing tool activity attempt
	Suspicious SaaS API call from a Tor exit node
	Exchange email-hiding inbox rule
	SaaS suspicious external domain user activity
	Exchange transport forwarding rule configured

Data Sources	Topics
	DLP sensitive data exposed to external users
	Exchange anti-phish policy disabled or removed
	Rare DLP rule match by user
	Exchange mailbox folder permission modification
	Exchange Safe Attachment policy disabled or removed
	Exchange malware filter policy removed
	Exchange compliance search created
	Exchange mailbox audit bypass
	Microsoft 365 DLP policy disabled or removed
	Massive file downloads from SaaS service
	External SaaS file-sharing activity
	User moved Exchange sent messages to deleted items
	Massive upload to SaaS service

Data Sources	Topics
	Sensitive Exchange mail sent to external users
	A user uploaded malware to SharePoint or OneDrive
	Exchange mailbox delegation permissions added
	User accessed multiple O365 AIP sensitive files

Data Sources	Topics
Okta	Suspicious SSO access from ASN
	SSO with abnormal user agent
	SSO authentication attempt by a honey user
	A user connected from a new country
	Suspicious SSO authentication
	First SSO access from ASN in organization
	SSO authentication by a machine account
	First SSO access from ASN for user
	A user logged in at an unusual time via SSO
	User attempted to connect from a suspicious country
	First connection from a country in organization
	SSO authentication by a service account
	A disabled user attempted to authenticate via SSO

Data Sources	Topics
	First SSO Resource Access in the Organization
	SSO with new operating system
	A successful SSO sign-in from TOR
	SSO with abnormal operating system
	A user accessed multiple unusual resources via SSO
	SSO Brute Force
	Impossible traveler - SSO
	A user rejected an SSO request from an unusual country
	SSO Password Spray
	Intense SSO failures
	Multiple SSO MFA attempts were rejected by a user

Data Sources	Topics
Okta Audit Log	Okta account unlock by admin
	Okta User Session Impersonation
	A user modified an Okta policy rule
	A user attempted to bypass Okta MFA
	A user modified an Okta network zone
	A user accessed Okta's admin application
	Potential Okta access limit breach
	User added a new device to Okta Verify instance
	Okta Reported Attack Suspected
	Okta API Token Created
	Okta admin privilege assignment
	A user observed and reported unusual activity in Okta
	Okta device assignment

Data Sources	Topics
	Okta account unlock
	Okta Reported Threat Detected

Data Sources	Topics
OneLogin	Suspicious SSO access from ASN
	SSO authentication attempt by a honey user
	A user connected from a new country
	First SSO access from ASN in organization
	SSO authentication by a machine account
	First SSO access from ASN for user
	A user logged in at an unusual time via SSO
	User attempted to connect from a suspicious country
	First connection from a country in organization
	SSO authentication by a service account
	A disabled user attempted to authenticate via SSO
	First SSO Resource Access in the Organization
	A successful SSO sign-in from TOR

Data Sources	Topics
	A user accessed multiple unusual resources via SSO
	SSO Brute Force
	Impossible traveler - SSO
	SSO Password Spray
	Intense SSO failures

Data Sources	Topics
Palo Alto Networks Global Protect	A disabled user attempted to log in to a VPN
	First VPN access attempt from a country in organization
	VPN login by a dormant user
	VPN login with a machine account
	A user connected to a VPN from a new country
	A user logged in at an unusual time via VPN
	First VPN access from ASN for user
	A Successful VPN connection from TOR
	VPN login by a service account
	VPN login attempt by a honey user
	First VPN access from ASN in organization
	VPN access with an abnormal operating system
	Impossible traveler - VPN

Data Sources	Topics
	VPN login Brute-Force attempt

Data Sources	Topics
Palo Alto Networks Platform Logs	Recurring access to rare IP
	Rare NTLM Usage by User
	Authentication Attempt From a Dormant Account
	Multiple uncommon SSH Servers with the same Server host key
	Failed Login For Locked-Out Account
	Rare SMB session to a remote host
	Abnormal Communication to a Rare IP
	A user accessed an uncommon AppID
	Suspicious Encrypting File System Remote call (EFSRPC) to domain controller
	FTP Connection Using an Anonymous Login or Default Credentials
	Recurring rare domain access to dynamic DNS domain
	Abnormal network communication through TOR using an uncommon port

Data Sources	Topics
	Weakly-Encrypted Kerberos Ticket Requested
	Unique client computer model was detected via MS-Update protocol
	Suspicious failed HTTP request - potential Spring4Shell exploit
	Weakly-Encrypted Kerberos TGT Response
	Rare RDP session to a remote host
	Possible DCShadow attempt
	Possible IPFS traffic was detected
	Bronze-Bit exploit
	Suspicious SSH Downgrade
	A rare FTP user has been detected on an existing FTP server
	Rare file transfer over SMB protocol
	Abnormal Communication to a Rare Domain
	A Torrent client was detected on a host

Data Sources	Topics
	Rare NTLM Access By User To Host
	Suspicious SMB connection from domain controller
	Possible path traversal via HTTP request
	Rare Scheduled Task RPC activity
	Failed Login For a Long Username With Special Characters
	Unusual SSH activity that resembles SSH proxy
	Unusual SSH activity that resembles SSH proxy
	Rare AppID usage to a rare destination
	Rare SMTP/S Session
	Possible Kerberoasting without SPNs
	Possible use of IPFS was detected
	Rare Windows Remote Management (WinRM) HTTP Activity
	New FTP Server

Data Sources	Topics
	Suspicious ICMP packet
	Uncommon SSH session was established
	Abnormal Recurring Communications to a Rare Domain
	Abnormal Recurring Communications to a Rare IP
	Rare MS-Update Server was detected
	A Possible crypto miner was detected on a host
	Multiple Weakly-Encrypted Kerberos Tickets Received
	Random-Looking Domain Names
	Download pattern that resembles Peer to Peer traffic
	Multiple Suspicious FTP Login Attempts
	NTLM Password Spray
	Kerberos Pre-Auth Failures by Host
	Subdomain Fuzzing

Data Sources	Topics
	NTLM Relay
	Large Upload (HTTPS)
	Spam Bot Traffic
	Massive upload to a rare storage or mail domain
	Large Upload (SMTP)
	Increase in Job-Related Site Visits
	NTLM Hash Harvesting
	SSH brute force attempt
	SSH brute force attempt
	Large Upload (FTP)
	Rare access to known advertising domains
	Kerberos Pre-Auth Failures by User and Host
	Large Upload (Generic)

Data Sources	Topics
	Upload pattern that resembles Peer to Peer traffic
	Port Scan
	Rare LDAP enumeration
	A user accessed multiple time-consuming websites
	New Administrative Behavior
	Failed DNS
	HTTP with suspicious characteristics
	Kerberos User Enumeration
	Failed Connections
	DNS Tunneling
	Suspicious DNS traffic

Data Sources	Topics
Palo Alto Networks Url Logs	Uncommon network tunnel creation
	Non-browser access to a pastebin-like site
	Rare connection to external IP address or host by an application using RMI-IIOP or LDAP protocol
	PowerShell Initiates a Network Connection to GitHub
	A non-browser process accessed a website UI

Data Sources	Topics
PingOne	Suspicious SSO access from ASN
	SSO with abnormal user agent
	SSO authentication attempt by a honey user
	A user connected from a new country
	First SSO access from ASN in organization
	SSO authentication by a machine account
	First SSO access from ASN for user
	A user logged in at an unusual time via SSO
	User attempted to connect from a suspicious country
	First connection from a country in organization
	SSO authentication by a service account
	A disabled user attempted to authenticate via SSO
	First SSO Resource Access in the Organization

Data Sources	Topics
	A successful SSO sign-in from TOR
	A user accessed multiple unusual resources via SSO
	SSO Brute Force
	Impossible traveler - SSO
	SSO Password Spray
	Intense SSO failures

Data Sources	Topics
Third-Party Firewalls	Recurring access to rare IP
	Rare SMB session to a remote host
	Recurring rare domain access to dynamic DNS domain
	Rare RDP session to a remote host
	Possible DCShadow attempt
	Abnormal Communication to a Rare Domain
	A Torrent client was detected on a host
	Suspicious SMB connection from domain controller
	Unusual SSH activity that resembles SSH proxy
	Rare AppID usage to a rare destination
	Rare SMTP/S Session
	Rare Windows Remote Management (WinRM) HTTP Activity
	New FTP Server

Data Sources	Topics
	Uncommon SSH session was established
	Abnormal Recurring Communications to a Rare Domain
	Large Upload (HTTPS)
	Spam Bot Traffic
	Large Upload (SMTP)
	SSH brute force attempt
	Upload pattern that resembles Peer to Peer traffic
	Port Scan
	New Administrative Behavior
	Failed Connections

Data Sources	Topics
Third-Party VPNs	A disabled user attempted to log in to a VPN
	First VPN access attempt from a country in organization
	VPN login by a dormant user
	VPN login with a machine account
	A user connected to a VPN from a new country
	A user logged in at an unusual time via VPN
	First VPN access from ASN for user
	A Successful VPN connection from TOR
	VPN login by a service account
	VPN login attempt by a honey user
	First VPN access from ASN in organization
	VPN access with an abnormal operating system
	Impossible traveler - VPN

Data Sources	Topics
	VPN login Brute-Force attempt

Data Sources	Topics
Windows Event Collector	Sensitive account password reset attempt
	A user certificate was issued with a mismatch
	Mailbox Client Access Setting (CAS) changed
	Service ticket request with a spoofed sAMAccountName
	PowerShell used to remove mailbox export request logs
	VM Detection attempt
	Possible Kerberos relay attack
	Unusual user account unlock
	User account delegation change
	Administrator groups enumerated via LDAP
	Rare machine account creation
	A machine certificate was issued with a mismatch
	A user was added to a Windows security group

Data Sources	Topics
	A user changed the Windows system time
	User added SID History to an account
	Masquerading as a default local account
	Security tools detection attempt
	Suspicious modification of the AdminSDHolder's ACL
	Member added to a Windows local security group
	A user account was modified to password never expires
	Machine account was added to a domain admins group
	Local user account creation
	Suspicious domain user account creation
	Suspicious hidden user created
	SPNs cleared from a machine account
	A user enabled a default local account

Data Sources	Topics
	Suspicious sAMAccountName change
	A computer account was promoted to DC
	TGT request with a spoofed sAMAccountName - Event log
	PowerShell used to export mailbox contents
	Multiple TGT requests for users without Kerberos pre-authentication
	Multiple user accounts were deleted
	Multiple suspicious user accounts were created
	A user printed an unusual number of files
	A user sent multiple TGT requests to irregular service
	A user received multiple weakly encrypted service tickets
	User added to a group and removed
	Excessive user account lockouts
	A new machine attempted Kerberos delegation

Data Sources	Topics
	Short-lived user account
	A user requested multiple service tickets

Data Sources	Topics
XDR Agent	Recurring access to rare IP
	Uncommon communication to an instant messaging server
	Scrcons.exe Rare Child Process
	Copy a process memory file
	Signed process performed an unpopular injection
	Delayed Deletion of Files
	Installation of a new System-V service
	Microsoft Office Process Spawning a Suspicious One-Liner
	Uncommon IP Configuration Listing via ipconfig.exe
	Rare NTLM Usage by User
	Local account discovery
	Uncommon Remote Monitoring and Management Tool
	Authentication Attempt From a Dormant Account

Data Sources	Topics
	Multiple uncommon SSH Servers with the same Server host key
	Globally uncommon injection from a signed process
	Wsmprovhost.exe Rare Child Process
	Fodhelper.exe UAC bypass
	Suspicious proxy environment variable setting
	Manipulation of netsh helper DLLs Registry keys
	Permission Groups discovery commands
	Remote service command execution from an uncommon source
	Kubernetes vulnerability scanner activity
	Execution of an uncommon process at an early startup stage by Windows system binary
	Failed Login For Locked-Out Account
	Suspicious container orchestration job
	Rare process execution in organization

Data Sources	Topics
	Rare process executed by an AppleScript
	Possible binary padding using dd
	Suspicious disablement of the Windows Firewall
	Kubernetes version disclosure
	Iptables configuration command was executed
	Suspicious setspn.exe execution
	Registration of Uncommon .NET Services and/or Assemblies
	Command running with COMSPEC in the command line argument
	Conhost.exe spawned a suspicious cmd process
	Encoded information using Windows certificate management tool
	Uncommon remote service start via sc.exe
	Possible collection of screen captures with Windows Problem Steps Recorder

Data Sources	Topics
	Globally uncommon root-domain port combination from a signed process
	Unpopular rsync process execution
	Rare SMB session to a remote host
	Remote DCOM command execution
	Abnormal Communication to a Rare IP
	Rare WinRM Session
	Possible DLL Hijack into a Microsoft process
	A user accessed an uncommon AppID
	Suspicious Encrypting File System Remote call (EFSRPC) to domain controller
	Globally uncommon process execution from a signed process
	Possible Kerberos relay attack
	Interactive login from a shared user account
	Rare process execution by user

Data Sources	Topics
	Recurring rare domain access to dynamic DNS domain
	Abnormal network communication through TOR using an uncommon port
	A compressed file was exfiltrated over SSH
	Discovery of host users via WMIC
	Weakly-Encrypted Kerberos Ticket Requested
	PsExec was executed with a suspicious command line
	Suspicious PowerShell Command Line
	Login by a dormant user
	Script file added to startup-related Registry keys
	System information discovery via psinfo.exe
	Suspicious sshpass command execution
	A contained executable was executed by an unusual process
	Suspicious docker image download from an unusual repository

Data Sources	Topics
	PowerShell suspicious flags
	Unusual Kubernetes dashboard communication from a pod
	Globally uncommon IP address connection from a signed process
	Suspicious failed HTTP request - potential Spring4Shell exploit
	Extracting credentials from Unix files
	A disabled user attempted to log in
	Weakly-Encrypted Kerberos TGT Response
	Compressing data using python
	Rare Remote Service (SVCCTL) RPC activity
	Rare RDP session to a remote host
	Reading bash command history file
	Network traffic to a crypto miner related domain detected
	Autorun.inf created in root C drive

Data Sources	Topics
	WmiPrvSe.exe Rare Child Command Line
	Contained process execution with a rare GitHub URL
	Msiexec execution of an executable from an uncommon remote location
	Kubernetes secret enumeration activity
	Possible DCShadow attempt
	Mimikatz command-line arguments
	Suspicious process executed with a high integrity level
	System shutdown or reboot
	Suspicious process accessed a site masquerading as Google
	Possible IPFS traffic was detected
	Bronze-Bit exploit
	Hidden Attribute was added to a file using attrib.exe
	Signed process performed an unpopular DLL injection

Data Sources	Topics
	Unusual AWS credentials creation
	Suspicious process execution from tmp folder
	Suspicious .NET process loads an MSBuild DLL
	Rundll32.exe executes a rare unsigned module
	TGT request with a spoofed sAMAccountName - Network
	Unprivileged process opened a registry hive
	Suspicious execution of ODBCConf
	Unsigned process injecting into a Windows system binary with no command line
	Run downloaded script using pipe
	Rare file transfer over SMB protocol
	Scripting engine connected to a rare external host
	Login attempt by a honey user
	Uncommon msiexec execution of an arbitrary file from a remote location

Data Sources	Topics
	Uncommon net localgroup execution
	Possible DCSync from a non domain controller
	Uncommon local scheduled task creation via schtasks.exe
	Abnormal Communication to a Rare Domain
	Uncommon DLL-sideloading from a logical CD-ROM (ISO) device
	Execution of an uncommon process at an early startup stage
	Remote code execution into Kubernetes Pod
	A Torrent client was detected on a host
	Possible compromised machine account
	Possible new DHCP server
	RDP Connection to localhost
	SMB Traffic from Non-Standard Process
	Possible Pass-the-Hash

Data Sources	Topics
	Office process creates a scheduled task via file access
	LOLBAS executable injects into another process
	Interactive at.exe privilege escalation method
	The Linux system firewall was disabled
	Rare NTLM Access By User To Host
	Suspicious SMB connection from domain controller
	Suspicious certutil command line
	AppleScript process executed with a rare command line
	Vulnerable driver loaded
	Kerberos Traffic from Non-Standard Process
	Linux network share discovery
	Attempt to execute a command on a remote host using PsExec.exe
	Possible path traversal via HTTP request

Data Sources	Topics
	Rare Scheduled Task RPC activity
	Suspicious process execution in a privileged container
	Globally uncommon root-domain port combination by a common process (sha256)
	Modification of PAM
	Failed Login For a Long Username With Special Characters
	Execution of dllhost.exe with an empty command line
	Unusual SSH activity that resembles SSH proxy
	Possible Email collection using Outlook RPC
	File transfer from unusual IP using known tools
	Ping to localhost from an uncommon, unsigned parent process
	Possible DLL Side-Loading
	Rare AppID usage to a rare destination
	Rare SMTP/S Session

Data Sources	Topics
	Possible Microsoft process masquerading
	Microsoft Office process spawns a commonly abused process
	Execution of renamed lolbin
	Possible Kerberoasting without SPNs
	Remote command execution via wmic.exe
	Possible use of IPFS was detected
	A user logged in from an abnormal country or ASN
	VM Detection attempt on Linux
	Netcat makes or gets connections
	Possible data obfuscation
	Unsigned process creates a scheduled task via file access
	LDAP traffic from non-standard process
	Rare Windows Remote Management (WinRM) HTTP Activity

Data Sources	Topics
	SUID/GUID permission discovery
	A suspicious process enrolled for a certificate
	Unusual Azure AD sync module load
	Reverse SSH tunnel to external domain/ip
	Injection into rundll32.exe
	Uncommon ARP cache listing via arp.exe
	Unusual DB process spawning a shell
	Unusual compressed file password protection
	Linux process execution with a rare GitHub URL
	New FTP Server
	Windows LOLBIN executable connected to a rare external host
	Svchost.exe loads a rare unsigned module
	Suspicious container runtime connection from within a Kubernetes Pod

Data Sources	Topics
	Executable moved to Windows system folder
	Phantom DLL Loading
	Suspicious ICMP packet
	Uncommon net group or localgroup execution
	Remote WMI process execution
	Uncommon DotNet module load relationship
	Office process spawned with suspicious command-line arguments
	Unicode RTL Override Character
	Suspicious data encryption
	A contained executable from a mounted share initiated a suspicious outbound network connection
	Suspicious usage of File Server Remote VSS Protocol (FSRVP)
	Suspicious RunOnce Parent Process
	Bitsadmin.exe persistence using command-line callback

Data Sources	Topics
	Indicator blocking
	A rare local administrator login
	Masquerading as the Linux crond process
	Rare signature signed executable executed in the network
	Uncommon cloud CLI tool usage
	Download a script using the python requests module
	Uncommon SSH session was established
	Windows Installer exploitation for local privilege escalation
	Possible network sniffing attempt via tcpdump or tshark
	Globally uncommon high entropy process was executed
	Command execution via wmiexec
	MSI accessed a web page running a server-side script
	Python HTTP server started

Data Sources	Topics
	Globally uncommon image load from a signed process
	Suspicious PowerShell Enumeration of Running Processes
	Recurring rare domain access from an unsigned process
	Suspicious Process Spawned by wininit.exe
	A LOLBIN was copied to a different location
	Service execution via sc.exe
	Indirect command execution using the Program Compatibility Assistant
	Wscript/Cscript loads .NET DLLs
	Procdump executed from an atypical directory
	Suspicious curl user agent
	Rare LOLBIN Process Execution by User
	MpCmdRun.exe was used to download files into the system
	Abnormal process connection to default Meterpreter port

Data Sources	Topics
	Rundll32.exe running with no command-line arguments
	Certutil pfx parsing
	Unusual process accessed the PowerShell history file
	Suspicious process loads a known PowerShell module
	Abnormal User Login to Domain Controller
	Memory dumping with comsvcs.dll
	An uncommon service was started
	Unusual weak authentication by user
	Execution of an uncommon process with a local/domain user SID at an early startup stage by Windows system binary
	Interactive login by a service account
	Unusual Kubernetes API server communication from a pod
	Execution of an uncommon process with a local/domain user SID at an early startup stage
	Suspicious print processor registered

Data Sources	Topics
	Possible DLL Search Order Hijacking
	Possible Search For Password Files
	A Successful login from TOR
	Setuid and Setgid file bit manipulation
	Command execution in a Kubernetes pod
	Wbadmin deleted files in quiet mode
	Windows Event Log was cleared using wevtutil.exe
	Suspicious SearchProtocolHost.exe parent process
	Remote service start from an uncommon source
	Unsigned and unpopular process performed a DLL injection
	LOLBIN process executed with a high integrity level
	Suspicious External RDP Login
	Mshta.exe launched with suspicious arguments

Data Sources	Topics
	Kubernetes nsenter container escape
	Possible network service discovery via command-line tool
	Rare communication over email ports to external email server by unsigned process
	Uncommon Service Create/Config
	Possible code downloading from a remote host by Regsvr32
	Rare security product signed executable executed in the network
	Suspicious runonce.exe parent process
	Unusual Lolbins Process Spawned by InstallUtil.exe
	Abnormal Recurring Communications to a Rare Domain
	A browser was opened in private mode
	Uncommon Managed Object Format (MOF) compiler usage
	New addition to Windows Defender exclusion list
	Keylogging using system commands

Data Sources	Topics
	Uncommon remote scheduled task creation
	Abnormal Recurring Communications to a Rare IP
	Suspicious process execution by scheduled task
	Globally uncommon high entropy module was loaded
	Interactive login by a machine account
	Rare DCOM RPC activity
	Suspicious Process Spawned by Adobe Reader
	Rundll32.exe spawns conhost.exe
	Rare SSH Session
	Unsigned and unpopular process performed an injection
	Suspicious time provider registered
	Rare process spawned by srvany.exe
	A process connected to a rare external host

Data Sources	Topics
	Unusual AWS user added to group
	Uncommon RDP connection
	Rare Unix process divided files by size
	Suspicious Certutil AD CS contact
	Copy a user's GnuPG directory with rsync
	Adding execution privileges
	Execution of the Hydra Linux password brute-force tool
	Suspicious dump of ntds.dit using Shadow Copy with ntdsutil/vssadmin
	Suspicious module load using direct syscall
	Globally uncommon root domain from a signed process
	Stored credentials exported using credwiz.exe
	A process was executed with a command line obfuscated by Unicode character substitution

Data Sources	Topics
	Possible malicious .NET compilation started by a commonly abused process
	Uncommon kernel module load
	Microsoft Office injects code into a process
	WebDAV drive mounted from net.exe over HTTPS
	Uncommon user management via net.exe
	Commonly abused process launched as a system service
	Screensaver process executed from Users or temporary folder
	Cloud Unusual Instance Metadata Service (IMDS) access
	Commonly abused AutoIT script connects to an external domain
	A TCP stream was created directly in a shell
	PowerShell runs suspicious base64-encoded commands
	Possible RDP session hijacking using tscon.exe
	Remote PsExec-like command execution

Data Sources	Topics
	Rare Unsigned Process Spawned by Office Process Under Suspicious Directory
	A service was disabled
	Globally uncommon IP address by a common process (sha256)
	Cached credentials discovery with cmdkey
	Tampering with Internet Explorer Protected Mode configuration
	Uncommon routing table listing via route.exe
	Suspicious authentication package registered
	The CA policy EditFlags was queried
	A Possible crypto miner was detected on a host
	Suspicious systemd timer activity
	NTLM Brute Force on a Service Account
	Possible TGT reuse from different hosts (pass the ticket)
	Multiple Weakly-Encrypted Kerberos Tickets Received

Data Sources	Topics
	Random-Looking Domain Names
	Download pattern that resembles Peer to Peer traffic
	Remote account enumeration
	Abnormal RDP connections to multiple hosts
	NTLM Password Spray
	Multiple Rare Process Executions in Organization
	Kerberos Pre-Auth Failures by Host
	Brute-force attempt on a local account
	Multiple discovery-like commands
	Suspicious ICMP traffic that resembles smurf attack
	External Login Password Spray
	Subdomain Fuzzing
	Interactive local account enumeration

Data Sources	Topics
	Abnormal SMB activity to multiple hosts
	NTLM Relay
	Multiple discovery commands on a Windows host by the same process
	Sudoedit Brute force attempt
	Multiple Rare LOLBIN Process Executions by User
	Multiple discovery commands on a Linux host by the same process
	Large Upload (HTTPS)
	Spam Bot Traffic
	A user authenticated with weak NTLM to multiple hosts
	Possible brute force or configuration change attempt on cytool
	Massive upload to a rare storage or mail domain
	Large Upload (SMTP)
	NTLM Hash Harvesting

Data Sources	Topics
	SSH brute force attempt
	Large Upload (FTP)
	A user logged on to multiple workstations via Schannel
	Possible brute force on sudo user
	Rare access to known advertising domains
	Kerberos Pre-Auth Failures by User and Host
	NTLM Brute Force
	Abnormal sensitive RPC traffic to multiple hosts
	Large Upload (Generic)
	Upload pattern that resembles Peer to Peer traffic
	Port Scan
	SSH authentication brute force attempts
	New Shared User Account

Data Sources	Topics
	Abnormal ICMP echo (PING) to multiple hosts
	Multiple users authenticated with weak NTLM to a host
	Internal Login Password Spray
	Possible external RDP Brute-Force
	New Administrative Behavior
	Account probing
	Failed DNS
	Multiple discovery commands
	Possible Brute-Force attempt
	HTTP with suspicious characteristics
	Kerberos User Enumeration
	Failed Connections
	DNS Tunneling

Data Sources	Topics
	Suspicious container reconnaissance activity in a Kubernetes pod
	Suspicious DNS traffic
	NTLM Brute Force on an Administrator Account

Data Sources	Topics
XDR Agent with eXtended Threat Hunting (XTH)	Space after filename
	Unusual Netsh PortProxy rule
	Uncommon SetWindowsHookEx API invocation of a possible keylogger
	Uncommon Security Support Provider (SSP) registered via a registry key
	Suspicious Print System Remote Protocol usage by a process
	Suspicious Udev driver rule execution manipulation
	A compiled HTML help file wrote a script file to the disk
	Potential SCCM credential harvesting using WMI detected
	A browser extension was installed or loaded in an uncommon way
	Unusual Encrypting File System Remote call (EFSRPC) to domain controller
	Unusual use of a 'SysInternals' tool
	System profiling WMI query execution

Data Sources	Topics
	Browser Extension Installed
	Sensitive account password reset attempt
	Uncommon jsp file write by a Java process
	Discovery of misconfigured certificate templates using LDAP
	A user certificate was issued with a mismatch
	Mailbox Client Access Setting (CAS) changed
	Service ticket request with a spoofed sAMAccountName
	PowerShell used to remove mailbox export request logs
	A user connected a USB storage device for the first time
	Uncommon NtWriteVirtualMemoryRemote API invocation with a PE header buffer
	Uncommon AT task-job creation by user
	DSC (Desired State Configuration) lateral movement using PowerShell
	Suspicious process modified RC script file

Data Sources	Topics
	Unusual process accessed a macOS notes DB file
	VM Detection attempt
	A user added a Windows firewall rule
	Office process accessed an unusual .LNK file
	Executable created to disk by lsass.exe
	Unusual process accessed a messaging app's files
	An uncommon file added to startup-related Registry keys
	Possible webshell file written by a web server process
	Suspicious AMSI decode attempt
	Windows event logs were cleared with PowerShell
	Scheduled Task hidden by registry modification
	An unpopular process accessed the microphone on the host
	A user queried AD CS objects via LDAP

Data Sources	Topics
	Known service display name with uncommon image-path
	Unusual user account unlock
	User account delegation change
	Creation or modification of the default command executed when opening an application
	New process created via a WMI call
	Uncommon GetClipboardData API function invocation of a possible information stealer
	Browser bookmark files accessed by a rare non-browser process
	An uncommon executable was remotely written over SMB to an uncommon destination
	Administrator groups enumerated via LDAP
	Suspicious access to shadow file
	Suspicious active setup registered
	Access to Kubernetes configuration file

Data Sources	Topics
	Rare machine account creation
	LSASS dump file written to disk
	A machine certificate was issued with a mismatch
	NTDS.dit file written by an uncommon executable
	Unusual Kubernetes service account file read
	A rare file path was added to the AppInit_DLLs registry value
	A user was added to a Windows security group
	A user changed the Windows system time
	User added SID History to an account
	Tampering with the Windows User Account Controls (UAC) configuration
	Commonly abused AutoIT script drops an executable file to disk
	Editing ld.so.preload for persistence and injection
	Masquerading as a default local account

Data Sources	Topics
	A user created a pfx file for the first time
	Security tools detection attempt
	Unusual process accessed web browser cookies
	Executable or Script file written by a web server process
	Sensitive browser credential files accessed by a rare non browser process
	Suspicious process accessed certificate files
	Suspicious modification of the AdminSDHolder's ACL
	Suspicious usage of Microsoft's Active Directory PowerShell module remote discovery cmdlet
	A remote service was created via RPC over SMB
	Unusual process accessed a crypto wallet's files
	Possible use of a networking driver for network sniffing
	An uncommon file was created in the startup folder
	LDAP search query from an unpopular and unsigned process

Data Sources	Topics
	A process queried the ADFS database decryption key via LDAP
	Uncommon browser extension loaded
	Possible Persistence via group policy Registry keys
	Member added to a Windows local security group
	A user account was modified to password never expires
	Rare service DLL was added to the registry
	Microsoft Office adds a value to autostart Registry key
	A user created an abnormal password-protected archive
	Possible LDAP Enumeration Tool Usage
	Machine account was added to a domain admins group
	Local user account creation
	Unusual access to the AD Sync credential files
	Suspicious domain user account creation

Data Sources	Topics
	Suspicious hidden user created
	An unusual archive file creation by a user
	A suspicious direct syscall was executed
	Possible SPN enumeration
	Elevation to SYSTEM via services
	A WMI subscriber was created
	A user connected a new USB storage device to a host
	SecureBoot was disabled
	RDP connections enabled remotely via Registry
	Possible GPO Enumeration
	Unusual process accessed a web browser history file
	SPNs cleared from a machine account
	Suspicious Kubernetes pod token access

Data Sources	Topics
	A user enabled a default local account
	Modification of NTLM restrictions in the Registry
	Rare process accessed a Keychain file
	User discovery via WMI query execution
	Known service name with an uncommon image-path
	Suspicious sAMAccountName change
	A computer account was promoted to DC
	User set insecure CA registry setting for global SANs
	A suspicious executable with multiple file extensions was created
	LOLBIN created a PSScriptPolicyTest PowerShell script file
	Unusual process accessed web browser credentials
	Suspicious PowerSploit's recon module (PowerView) used to search for exposed hosts

Data Sources	Topics
	Possible Distributed File System Namespace Management (DFSNM) abuse
	TGT request with a spoofed sAMAccountName - Event log
	Linux system firewall was modified
	Uncommon PowerShell commands used to create or alter scheduled task parameters
	Unusual ADConnect database file access
	Suspicious PowerSploit's recon module (PowerView) net function was executed
	Unusual process accessed FTP Client credentials
	Uncommon creation or access operation of sensitive shadow copy
	PowerShell used to export mailbox contents
	Change of sudo caching configuration
	A process modified an SSH authorized_keys file
	Suspicious LDAP search query executed

Data Sources	Topics
	A suspicious process queried AD CS objects via LDAP
	Suspicious disablement of the Windows Firewall using PowerShell commands
	PowerShell pfx certificate extraction
	Unusual access to the Windows Internal Database on an ADFS server
	Uncommon access to Microsoft Teams credential files
	Suspicious DotNet log file created
	Image file execution options (IFEO) registry key set
	Rare scheduled task created
	Massive file compression by user
	Possible data exfiltration over a USB storage device
	Multiple TGT requests for users without Kerberos pre-authentication
	Suspicious access to cloud credential files

Data Sources	Topics
	A user established an SMB connection to multiple hosts
	Multiple user accounts were deleted
	Multiple suspicious user accounts were created
	User collected remote shared files in an archive
	A user executed multiple LDAP enumeration queries
	Suspicious reconnaissance using LDAP
	Possible LDAP enumeration by unsigned process
	A user printed an unusual number of files
	A user performed suspiciously massive file activity
	User and Group Enumeration via SAMR
	A user took numerous screenshots
	A user sent multiple TGT requests to irregular service
	A user received multiple weakly encrypted service tickets

Data Sources	Topics
	Outlook files accessed by an unsigned process
	A user accessed an abnormal number of files on a remote shared folder
	User added to a group and removed
	A user connected a new USB storage device to multiple hosts
	A user accessed an abnormal number of remote shared folders
	Excessive user account lockouts
	Possible internal data exfiltration over a USB storage device
	A new machine attempted Kerberos delegation
	A contained process attempted to escape using the 'notify on release' feature
	Short-lived user account
	Massive file activity abnormal to process
	A user requested multiple service tickets

3 | AWS Audit Log

3.1 | A Kubernetes Cronjob was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job: Container Orchestration Job (T1053.007)
Severity	Informational

Description

A Kubernetes CronJob was created.

Attacker's Goals

- Maintain persistence by scheduling deployment of containers configured to execute malicious code.

Investigative actions

- Check which changes were made to the Kubernetes CronJob.

3.2 | An AWS RDS Global Cluster Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)

ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

An AWS RDS global cluster was deleted.

Attacker's Goals

Destruction of data.

Investigative actions

- Check for existing backups for the deleted cluster was.
- Check if a secondary cluster exists, which was detached before the global deletion.

3.3 | Object versioning was disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	Informational

Description

Object versioning of a cloud storage resource was disabled.

Attacker's Goals

Impair the ability of the cloud environment to recover in disaster scenarios.

Investigative actions

- Confirm that the identity intended to disable the resource versioning.
- Follow further actions done by the identity.
- Monitor this resource for other suspicious activities.

Variations

Object versioning was disabled by an unusual identity

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)

Severity	Informational

Description

Cloud storage versioning was disabled/suspended by an unusual identity.

Attacker's Goals

Impair the ability of the cloud environment to recover in disaster scenarios.

Investigative actions

- Confirm that the identity intended to disable the resource versioning.
- Follow further actions done by the identity.
- Monitor this resource for other suspicious activities.

3.4 | Suspicious usage of EC2 token

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Medium

Description

An AWS EC2 STS token was used externally from an EC2 instance.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the access key was generated by the attached instance.
- Check what actions were executed by the access-key.
- Check if the relevant instance is compromised.

Variations

Suspicious usage of EC2 token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	High

Description

An AWS EC2 STS token was used externally from an EC2 instance.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the access key was generated by the attached instance.
- Check what actions were executed by the access-key.
- Check if the relevant instance is compromised.

Suspicious usage of EC2 token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Low

Description

An AWS EC2 STS token was used externally from an EC2 instance.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the access key was generated by the attached instance.
- Check what actions were executed by the access-key.
- Check if the relevant instance is compromised.

3.5 | Unusual secret management activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Unsecured Credentials (T1552) • Credentials from Password Stores: Cloud Secrets Management Stores (T1555.006)
Severity	Informational

Description

A cloud Identity performed a secret management operation for the first time.

Attacker's Goals

Abuse exposed secrets to gain access to restricted cloud resources and applications.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive secret management operation that it shouldn't.

3.6 | Kubernetes network policy modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud

Detector Tags	Kubernetes - API
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Informational

Description

A change has been made to the network policies of a Kubernetes cluster.

Attacker's Goals

- Gain access to the network infrastructure.
- Gain access to sensitive data.
- Gain access to Kubernetes resources.

Investigative actions

- Investigate the Kubernetes Network Policy to identify the changes made.
- Verify whether the identity should be making this action.

3.7 | Penetration testing tool activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	7 Days
Required Data	- Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Medium

Description

A cloud API was successfully executed using a known penetration testing tool.

Attacker's Goals

Usage of known attack tools and frameworks.

Investigative actions

- Verify whether there is an ongoing PT test.

3.8 | Denied API call by a Kubernetes service account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A Kubernetes service account API call was denied.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Check whether the service account should be making this API call.
- Check service account's activity, including additional executed API calls.

Variations

Denied API call by Kubernetes service account for the first time in the cluster

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Low

Description

A Kubernetes service account API call was denied.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Check whether the service account should be making this API call.
- Check service account's activity, including additional executed API calls.

Suspicious denied API call by a Kubernetes service account

Synopsis

ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A Kubernetes service account API call was denied.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Check whether the service account should be making this API call.
- Check service account's activity, including additional executed API calls.

3.9 | AWS CloudWatch log group deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ○ AWS Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	• Impact (TA0040) • Defense Evasion (TA0005)
ATT&CK Technique	• Data Destruction (T1485) • Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Informational

Description

An AWS CloudWatch log group was deleted, this action permanently deletes all the archives associated with this group.

Attacker's Goals

An attacker may change the configuration of the affected resource to remain undetected.

Investigative actions

- Check why the identity deleted the log group.
- Check what resources were affected by this change.

3.10 | Kubernetes pod creation with host network

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	5 Days
Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	- Privilege Escalation (TA0004) - Execution (TA0002)
ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)
Severity	Informational

Description

An identity created a Kubernetes pod attached to the host network.
This may indicate an adversary attempting to access services bound to localhost, sniff traffic on any interface on the host, and potentially bypass the network policy.

Attacker's Goals

- Access services bound to localhost.
- Sniff traffic on any interface on the host.
- Bypass network policy.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any unusual access to localhost services.
- Inspect for any network sniffing tool being used inside the Kubernetes Pod.

Variations

Kubernetes pod creation with host network for the first time in the cluster

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Execution (TA0002)
ATT&CK Technique	Escape to Host (T1611) Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod attached to the host network.
This may indicate an adversary attempting to access services bound to localhost, sniff traffic on any interface on the host, and potentially bypass the network policy.

Attacker's Goals

- Access services bound to localhost.
- Sniff traffic on any interface on the host.
- Bypass network policy.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any unusual access to localhost services.
- Inspect for any network sniffing tool being used inside the Kubernetes Pod.

Kubernetes pod creation with host network for the first time in the namespace

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod attached to the host network.
This may indicate an adversary attempting to access services bound to localhost, sniff traffic on any interface on the host, and potentially bypass the network policy.

Attacker's Goals

- Access services bound to localhost.
- Sniff traffic on any interface on the host.
- Bypass network policy.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any unusual access to localhost services.
- Inspect for any network sniffing tool being used inside the Kubernetes Pod.

Kubernetes pod creation with host network for the first time by the identity

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)

Severity	Low

Description

An identity created a Kubernetes pod attached to the host network.
This may indicate an adversary attempting to access services bound to localhost, sniff traffic on any interface on the host, and potentially bypass the network policy.

Attacker's Goals

- Access services bound to localhost.
- Sniff traffic on any interface on the host.
- Bypass network policy.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any unusual access to localhost services.
- Inspect for any network sniffing tool being used inside the Kubernetes Pod.

3.11 | IAM User added to an IAM group

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Persistence (TA0003) • Privilege Escalation (TA0004)
ATT&CK Technique	• Account Manipulation (T1098) • Valid Accounts (T1078)
Severity	Informational

Description

An IAM user was added to a specified group.

Attacker's Goals

An attack may add a new/compromised user to a group to create persistence and elevate privileges in the account.

Investigative actions

- Check who is the identity which executed the API call.
- Check who is the IAM which was added to the group.
- Check the group's permissions and if they are relevant for the IAM user.

3.12 | Unusual key management activity

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials (T1552)
Severity	Informational

Description

A cloud Identity performed a key management operation for the first time.

Attacker's Goals

Abuse exposed cryptographic keys to decrypt sensitive information or create digital signatures to craft malicious messages.
Using the decrypted information, the attacker may perform additional activities in an evasive manner.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive KMS operation that it shouldn't.

3.13 | Cloud storage automatic backup disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)

Severity	Informational

Description

Automatic backup of a cloud storage resource was disabled.

Attacker's Goals

- Impair built-in protection of the cloud environment.
- This action may be a preliminary action before deleting the cloud resource itself.

Investigative actions

- Confirm that the identity intended to disable automatic backup on this resource.
- Follow further actions done by the identity.
- Monitor this resource for other suspicious activities.

Variations

Cloud storage automatic backup disabled from a CLI

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	Informational

Description

Automatic backup of a cloud storage resource was disabled from a CLI.

Attacker's Goals

- Impair built-in protection of the cloud environment.
- This action may be a preliminary action before deleting the cloud resource itself.

Investigative actions

- Confirm that the identity intended to disable automatic backup on this resource.
- Follow further actions done by the identity.
- Monitor this resource for other suspicious activities.

3.14 | Cloud Trail Logging has been stopped/suspended

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Informational

Description

A cloud trail logging has been stopped, which indicates that AWS API calls are not recorded in that trail.

Attacker's Goals

Hide an unwanted actor's actions.

Investigative actions

- Check if the Identity intended to stop the trail logging.
- Check if there are additional trails that are still recording.

3.15 | Cloud snapshot of a database or storage instance was publicly shared

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Transfer Data to Cloud Account (T1537)
Severity	Medium

Description

A cloud identity has publicly shared a snapshot of a database or storage instance.

Attacker's Goals

Exfiltrate sensitive data that resides on the snapshot.

Investigative actions

- Check if the identity intended to share the snapshot publicly.
- Check if the identity performed additional malicious operations within the cloud environment.

3.16 | A Command Line Interface (CLI) command was executed from an AWS serverless compute service

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	Cloud Serverless Function Credentials Theft Analytics
ATT&CK Tactic	- Initial Access (TA0001) - Credential Access (TA0006)
ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Steal Application Access Token (T1528) - Unsecured Credentials (T1552)
Severity	Low

Description

AWS serverless compute service token was used to execute a Command Line Interface (CLI) command. This may indicate token theft due to the nature of serverless compute.

Attacker's Goals

Exfiltrate serverless token and abuse it.

Investigative actions

- Verify whether the serverless-attached identity's credentials were intentionally used in CLI.
- Check what CLI commands were executed using the serverless attached token.
- Check if the suspected serverless function is compromised.

Variations

A Command Line Interface (AWS-CLI) command was executed from an AWS serverless compute service

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Credential Access (TA0006)
ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Steal Application Access Token (T1528) - Unsecured Credentials (T1552)
Severity	Informational

Description

AWS serverless compute service token was used to execute a Command Line Interface (CLI) command. This may indicate token theft due to the nature of serverless compute.

Attacker's Goals

Exfiltrate serverless token and abuse it.

Investigative actions

- Verify whether the serverless-attached identity's credentials were intentionally used in CLI.
- Check what CLI commands were executed using the serverless attached token.
- Check if the suspected serverless function is compromised.

Unusual Command Line Interface (CLI) command was executed from an AWS serverless compute service

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Credential Access (TA0006)
ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Steal Application Access Token (T1528) - Unsecured Credentials (T1552)

Severity	Low

Description

AWS serverless compute service token was used to execute a Command Line Interface (CLI) command. This may indicate token theft due to the nature of serverless compute.

Attacker's Goals

Exfiltrate serverless token and abuse it.

Investigative actions

- Verify whether the serverless-attached identity's credentials were intentionally used in CLI.
- Check what CLI commands were executed using the serverless attached token.
- Check if the suspected serverless function is compromised.

3.17 | An AWS EKS cluster was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Impact (TA0040)
ATT&CK Technique	• Data Destruction (T1485) • Valid Accounts (T1078)
Severity	Informational

Description

An AWS EKS cluster has been created or deleted.

Attacker's Goals

Gain access to the cluster and its resources.
Gain access to sensitive data stored in the cluster.

Investigative actions

Check whether the identity is authorized to perform changes to AWS EKS clusters.

3.18 | A cloud function was created with an unusual runtime

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Serverless Execution (T1648)
Severity	Low

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

- Examine the cloud function's code implementation and look for any unusual invocations.
- Check for any unusual activities within the same project.

Variations

A cloud function was created with an unusual runtime by a known cloud identity

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Serverless Execution (T1648)
Severity	Informational

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

- Examine the cloud function's code implementation and look for any unusual invocations.
- Check for any unusual activities within the same project.

A cloud function was created with a runtime that was not seen in the organization

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Serverless Execution (T1648)
Severity	Low

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

- Examine the cloud function's code implementation and look for any unusual invocations.
- Check for any unusual activities within the same project.

A cloud function was created with a custom runtime

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Serverless Execution (T1648)
Severity	Medium

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

- Examine the cloud function's code implementation and look for any unusual invocations.
- Check for any unusual activities within the same project.

3.19 | Kubernetes Pod created with host process ID (PID) namespace

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Informational

Description

An identity created a Kubernetes pod with the host process ID (PID) namespace.
This may indicate an adversary attempting to access processes running on the host, which could allow escalating privileges to root.

Attacker's Goals

- View processes on the host.
- View the environment variables for each pod on the host.
- View the file descriptors for each pod on the host.
- Kill processes on the node.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Variations

Kubernetes Pod created with host process ID (PID) namespace for the first time in the cluster

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Execution (TA0002)
ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with the host process ID (PID) namespace.
This may indicate an adversary attempting to access processes running on the host, which could allow escalating privileges to root.

Attacker's Goals

- View processes on the host.
- View the environment variables for each pod on the host.
- View the file descriptors for each pod on the host.
- Kill processes on the node.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Kubernetes Pod created with host process ID (PID) namespace for the first time in the namespace

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with the host process ID (PID) namespace.
This may indicate an adversary attempting to access processes running on the host, which could allow escalating privileges to root.

Attacker's Goals

- View processes on the host.
- View the environment variables for each pod on the host.
- View the file descriptors for each pod on the host.
- Kill processes on the node.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Kubernetes Pod created with host process ID (PID) namespace for the first time by the identity

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)

ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with the host process ID (PID) namespace.
This may indicate an adversary attempting to access processes running on the host, which could allow escalating privileges to root.

Attacker's Goals

- View processes on the host.
- View the environment variables for each pod on the host.
- View the file descriptors for each pod on the host.
- Kill processes on the node.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

3.20 | AWS config resource deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Informational

Description

An AWS config resource deletion this includes:
Config rule, organization rule, configuration recorder, remediation configuration, conformance pack, configuration aggregator, delivery channel, retention configuration.

Attacker's Goals

An attacker may modify Config configuration to evade detection.

Investigative actions

- Check why the identity deleted the configuration.
- Check what resources are relevant to the deleted config.

3.21 | A cloud identity had escalated its permissions

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A cloud identity had updated its permissions.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

Variations

A cloud identity with high administrative activity had escalated its permissions

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A cloud identity with high administrative activity had updated its permissions.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

A cloud compute service had escalated its permissions

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Medium

Description

A cloud compute service had updated its permissions.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

A cloud non-human identity had escalated its permissions

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A cloud non-human identity had updated its permissions.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

A cloud identity escalated its permissions to a high privilege role/policy

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)

Severity	Low

Description

A cloud identity escalated its permissions by adding itself to a high privileged policy/role/group.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

3.22 | AWS RDS cluster deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

A previously provisioned DB cluster (RDS) was deleted.
When a DB cluster is being deleted, all automated backups for that DB cluster are deleted and can't be recovered.

Attacker's Goals

Destruction of data.

Investigative actions

- Check which cluster was deleted.
- Check if there are any manual backups for that cluster (as they are not affected by this action).

3.23 | A Kubernetes StatefulSet was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Informational

Description

A Kubernetes StatefulSet was created.

Attacker's Goals

- Deploy a container into an environment to facilitate execution.

Investigative actions

- Check which changes were made to the Kubernetes StatefulSet.

3.24 | An AWS SAML provider was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Defense Evasion (TA0005)
ATT&CK Technique	• Trusted Relationship (T1199) • Modify Authentication Process (T1556)
Severity	Informational

Description

An AWS SAML provider was modified.

Attacker's Goals

- Gain privileged access to AWS accounts.

Investigative actions

- Check what changes were made to the SAML provider.

3.25 | A Kubernetes service account executed an unusual API call

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A Kubernetes service account executed an unusual API call.

Attacker's Goals

- Abuse a service account token to gain access to the Kubernetes cluster.

Investigative actions

- Verify whether the service account should be executing this API.
- Investigate other operations that were performed by the service account within the cluster.

Variations

A Kubernetes service account executed an API call on a first-seen resource

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Low

Description

A Kubernetes service account executed an API call on a first-seen resource.

Attacker's Goals

- Abuse a service account token to gain access to the Kubernetes cluster.

Investigative actions

- Verify whether the service account should be executing this API.
- Investigate other operations that were performed by the service account within the cluster.

A Kubernetes service account executed an API call on an unusual sensitive resource

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Low

Description

A Kubernetes service account executed an API call on an unusual sensitive resource.

Attacker's Goals

- Abuse a service account token to gain access to the Kubernetes cluster.

Investigative actions

- Verify whether the service account should be executing this API.
- Investigate other operations that were performed by the service account within the cluster.

A Kubernetes service account executed an unusual modification API call

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A Kubernetes service account executed an unusual modification API call.

Attacker's Goals

- Abuse a service account token to gain access to the Kubernetes cluster.

Investigative actions

- Verify whether the service account should be executing this API.
- Investigate other operations that were performed by the service account within the cluster.

A Kubernetes service account executed an API call on an unusual resource

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A Kubernetes service account executed an API call on an unusual resource.

Attacker's Goals

- Abuse a service account token to gain access to the Kubernetes cluster.

Investigative actions

- Verify whether the service account should be executing this API.
- Investigate other operations that were performed by the service account within the cluster.

3.26 | An Email address was added to AWS SES

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An Email address was added to AWS SES.

Attacker's Goals

- Gain access to SES account.
- Abuse the new identity as a spambot.

Investigative actions

- Check which identity was added to the service.

3.27 | Unusual Identity and Access Management (IAM) activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Account Manipulation: Additional Cloud Credentials (T1098.001) • Valid Accounts: Cloud Accounts (T1078.004)

Severity	Informational

Description

A cloud identity performed an unusual IAM operation.

Attacker's Goals

Manipulate IAM configuration to strengthen the foothold in the cloud environment of the organization, by creating new accounts, modifying credentials, and permissions.
Using the modified accounts, the attacker may perform additional activities in an evasive manner.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive IAM operation that it shouldn't.

Variations

Unusual Identity and Access Management (IAM) activity executed from a cloud Internet facing instance

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Account Manipulation: Additional Cloud Credentials (T1098.001) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Medium

Description

A cloud Internet facing instance performed an unusual IAM operation.

Attacker's Goals

Manipulate IAM configuration to strengthen the foothold in the cloud environment of the organization, by creating new accounts, modifying credentials, and permissions.

Using the modified accounts, the attacker may perform additional activities in an evasive manner.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive IAM operation that it shouldn't.

Unusual Identity and Access Management (IAM) activity

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Account Manipulation: Additional Cloud Credentials (T1098.001) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Low

Description

A cloud non-user identity performed an unusual IAM operation.

Attacker's Goals

Manipulate IAM configuration to strengthen the foothold in the cloud environment of the organization, by creating new accounts, modifying credentials, and permissions.
Using the modified accounts, the attacker may perform additional activities in an evasive manner.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive IAM operation that it shouldn't.

3.28 | An AWS RDS instance was created from a snapshot

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Transfer Data to Cloud Account (T1537)
Severity	Informational

Description

A new AWS RDS instance was created from a publicly available RDS snapshot.

Attacker's Goals

- Gain access to the RDS instance.
- Access confidential data stored in the RDS instance.

Investigative actions

- Check the RDS instance status in the AWS console.
- Verify if the instance is publicly accessible.

3.29 | An IAM group was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Create Account (T1136)
Severity	Informational

Description

IAM group creation.

Attacker's Goals

Gain persistence to account by IAM user which may be a member of the created group.

Investigative actions

- Check group's permissions.
- Check which users were added to the group.

3.30 | A Kubernetes node service account activity from external IP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud

Detector Tags	Kubernetes - API
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001)
Severity	Informational

Description

A Kubernetes node service account was seen operating from an external IP.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Determine which resources were accessed by the node service account.
- Investigate other actions made by the node service account.

Variations

A Kubernetes node service account was used outside the cluster

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001)
Severity	Low

Description

A Kubernetes node service account was seen operating from an external IP.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Determine which resources were accessed by the node service account.
- Investigate other actions made by the node service account.

3.31 | MFA device was removed/deactivated from an IAM user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)

Severity	Informational

Description

Deactivate an MFA device and disassociate it from an IAM user.

Attacker's Goals

This may allow an attacker to gain access to the IAM user.

Investigative actions

- Check if IAM requires MFA to be enabled.

3.32 | An AWS S3 bucket configuration was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	- Defense Evasion (TA0005) - Impact (TA0040)
ATT&CK Technique	- Impair Defenses (T1562) - Data Encrypted for Impact (T1486)
Severity	Informational

Description

An AWS S3 bucket configuration has been modified.

Attacker's Goals

- Modify storage configuration to detection or allow access to sensitive information.

Investigative actions

- Examine AWS S3 access to identify any suspicious activity.
- Check which S3 buckets were affected.

3.33 | A Kubernetes deployment was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Informational

Description

A Kubernetes deployment was created.

Attacker's Goals

- Deploy a container into an environment to facilitate execution.

Investigative actions

- Check which changes were made to the Kubernetes deployment.

3.34 | A Kubernetes service account was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A Kubernetes service account was created or deleted.

Attacker's Goals

- Maintain persistence using a valid service account.

Investigative actions

- Check which changes were made to the Kubernetes service account.

Variations

A Kubernetes service account was created or deleted in a default namespace

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A Kubernetes service account was created or deleted.

Attacker's Goals

- Maintain persistence using a valid service account.

Investigative actions

- Check which changes were made to the Kubernetes service account.

3.35 | An AWS ElastiCache security group was modified or

deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Informational

Description

An AWS ElastiCache security group was modified or deleted.

Attacker's Goals

- Gain access to sensitive data stored on AWS ElastiCache.

Investigative actions

- Verify what changes were made to the ElastiCache security group.

3.36 | Unusual resource modification/creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Impact (TA0040) • Persistence (TA0003)
ATT&CK Technique	• Data Destruction (T1485) • Account Manipulation (T1098)

Severity	Informational

Description

A cloud resource was modified/created by a newly seen user. The API call is unusual as it is normally executed by administrators or not popular within the organization.

Attacker's Goals

Evading detections, maintaining persistence and access to sensitive data.

Investigative actions

- Check which resources were manipulated and their severity.
- Check for abnormal activity by the executing identity before and after the manipulation.

Variations

Unusual resource modification/creation by an identity with high administrative activity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Persistence (TA0003)
ATT&CK Technique	• Data Destruction (T1485) • Account Manipulation (T1098)
Severity	Informational

Description

A cloud resource was modified/created by a newly seen user which has high administrative activity. The API call is unusual as it is normally executed by administrators or not popular within the organization.

Attacker's Goals

Evading detections, maintaining persistence and access to sensitive data.

Investigative actions

- Check which resources were manipulated and their severity.
- Check for abnormal activity by the executing identity before and after the manipulation.

Unusual resource modification/creation by newly seen user

Synopsis

ATT&CK Tactic	Impact (TA0040) Persistence (TA0003)
ATT&CK Technique	Data Destruction (T1485) Account Manipulation (T1098)
Severity	Low

Description

A cloud resource was modified/created by a newly seen user. The API call is unusual as it is normally executed by administrators or not popular within the organization.

Attacker's Goals

Evading detections, maintaining persistence and access to sensitive data.

Investigative actions

- Check which resources were manipulated and their severity.
- Check for abnormal activity by the executing identity before and after the manipulation.

3.37 | Unusual certificate management activity

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Private Keys (T1552.004)
Severity	Informational

Description

A cloud Identity performed a certificate management operation for the first time.

Attacker's Goals

Abuse certificate management functionalities to generate valid signed certificates, which enable to launch man-in-the-middle attacks against different services.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive certificate management operation that it shouldn't.

3.38 | A Kubernetes ephemeral container was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Informational

Description

A Kubernetes ephemeral container was created.

Attacker's Goals

- Deploy a container into an environment to facilitate execution.

Investigative actions

- Check which changes were made to the Kubernetes deployment.

3.39 | A Kubernetes secret was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Container API (T1552.007)
Severity	Informational

Description

A Kubernetes secret was created or deleted.

Attacker's Goals

- Obtain Kubernetes secrets to access restricted information.

Investigative actions

- Check which changes were made to the Kubernetes secret.

3.40 | A Kubernetes Pod was created with a sidecar container

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Informational

Description

A Kubernetes Pod was created with a sidecar container.

Attacker's Goals

- Deploy a container into an environment to facilitate execution.

Investigative actions

- Check which changes were made to the Kubernetes deployment.

3.41 | Cloud compute instance user data script modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Cloud Administration Command (T1651)
Severity	Informational

Description

The user data of a cloud compute instance was modified.

Attacker's Goals

Execute commands within virtual machines.

Investigative actions

- Verify whether this action is expected.
- Inspect the user data script for malicious content.

Variations

Unusual Cloud compute instance user data script modification

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Cloud Administration Command (T1651)
Severity	Low

Description

The user data of a cloud compute instance was modified.

Attacker's Goals

Execute commands within virtual machines.

Investigative actions

- Verify whether this action is expected.
- Inspect the user data script for malicious content.

3.42 | A Kubernetes ReplicaSet was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Informational

Description

A Kubernetes ReplicaSet was created.

Attacker's Goals

- Deploy a container into an environment to facilitate execution.

Investigative actions

- Check which changes were made to the Kubernetes ReplicaSet.

3.43 | AWS CloudWatch log stream deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Impact (TA0040) • Defense Evasion (TA0005)
ATT&CK Technique	• Data Destruction (T1485) • Impair Defenses: Disable or Modify Cloud Logs (T1562.008)

Severity	Informational

Description

An AWS CloudWatch log stream was deleted, this action permanently deletes all the archives associated with this stream.

Attacker's Goals

An attacker may change the configuration of the affected resource to remain undetected.

Investigative actions

- Check why the identity deleted the log stream.
- Check which resource is affected by this change.

3.44 | A Kubernetes Pod was deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log

Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

A Kubernetes Pod was deleted.

Attacker's Goals

- Destroy data to interrupt cluster services and availability.

Investigative actions

- Check which Kubernetes Pods were deleted.

3.45 | An AWS Lambda function was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	5 Days
Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Serverless Execution (T1648)
Severity	Informational

Description

An AWS Lambda function was modified.

Attacker's Goals

Modification of Lambda function may provide attack access to run code against the cloud environment.

Investigative actions

- Check what modifications were made to the AWS Lambda function.

3.46 | An AWS SES identity was deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

An AWS SES identity has been deleted.

Attacker's Goals

Gain access to confidential emails of an organization.

Investigative actions

- Check whether the identity that executed the API should be making this action.

3.47 | AWS user creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Create Account: Cloud Account (T1136.003)
Severity	Informational

Description

A new AWS user was created.

Attacker's Goals

Gain persistence into the account.

Investigative actions

- Check which User was created.

3.48 | Cloud compute serial console access

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Direct Cloud VM Connections (T1021.008)
Severity	Informational

Description

An identity connected to a compute instance using serial console access.
This may indicate an attacker attempting to move laterally between cloud instances.

Attacker's Goals

- Utilize direct access to virtual infrastructure to pivot through a cloud environment.

Investigative actions

- Verify whether the identity should be making this action.
- Investigate which actions were performed via serial console access.

Variations

Cloud compute serial console access by an identity with high administrative activity

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Direct Cloud VM Connections (T1021.008)
Severity	Informational

Description

An identity with high administrative activity connected to a compute instance using serial console access.
This may indicate an attacker attempting to move laterally between cloud instances.

Attacker's Goals

- Utilize direct access to virtual infrastructure to pivot through a cloud environment.

Investigative actions

- Verify whether the identity should be making this action.
- Investigate which actions were performed via serial console access.

Suspicious cloud compute serial console access in a project

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Direct Cloud VM Connections (T1021.008)
Severity	Low

Description

An identity connected to a compute instance using serial console access.
This may indicate an attacker attempting to move laterally between cloud instances.

Attacker's Goals

- Utilize direct access to virtual infrastructure to pivot through a cloud environment.

Investigative actions

- Verify whether the identity should be making this action.
- Investigate which actions were performed via serial console access.

3.49 | AWS network ACL rule creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Persistence (TA0003) • Exfiltration (TA0010)
ATT&CK Technique	• External Remote Services (T1133) • Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

An AWS network ACL rule was created with a specific rule number.

Attacker's Goals

This action may assist an attacker gain persistence for the cloud environment (in case of ingress rule).
Or in case of egress rule, this may allow an attacker to exfiltrate data.

Investigative actions

- Check the VPC behind affected by this change.
- Check the rule number (as they effect by order).
- Check if the rule is ingress/egress.

3.50 | Cloud impersonation attempt by unusual identity type

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A suspicious identity type has attempted to impersonate another identity.

Attacker's Goals

- Escalate privileges to bypass access controls
- Avoid detection throughout their compromise.

Investigative actions

- Check the identity's designation.
- Verify that the identity did not perform sensitive operation on behalf of the impersonated identity.

Variations

Successful cloud impersonation by an unusual identity type

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Medium

Description

A suspicious identity type has successfully impersonated another identity.

Attacker's Goals

- Escalate privileges to bypass access controls
- Avoid detection throughout their compromise.

Investigative actions

- Check the identity's designation.
- Verify that the identity did not perform sensitive operation on behalf of the impersonated identity.

3.51 | A cloud identity created or modified a security group

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Firewall (T1562.007)
Severity	Informational

Description

A cloud identity created or modified a security group.

Attacker's Goals

- Bypass network security controls to gain access to restricted cloud resources.

Investigative actions

- Check which security rules were added or modified.
- Check whether the identity that modified the security group rules is permitted to perform such action.
- Check which cloud resources can be affected by the security group.

Variations

A cloud identity opened a security group to the Internet

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Firewall (T1562.007)
Severity	Medium

Description

A cloud identity modified a security group to allow network access from the Internet.

Attacker's Goals

- Bypass network security controls to gain access to restricted cloud resources.

Investigative actions

- Check which security rules were added or modified.
- Check whether the identity that modified the security group rules is permitted to perform such action.
- Check which cloud resources can be affected by the security group.

A cloud identity opened a security group to an unknown IP

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Firewall (T1562.007)
Severity	Low

Description

A cloud identity modified a security group to allow network access from unknown IP.

Attacker's Goals

- Bypass network security controls to gain access to restricted cloud resources.

Investigative actions

- Check which security rules were added or modified.
- Check whether the identity that modified the security group rules is permitted to perform such action.
- Check which cloud resources can be affected by the security group.

3.52 | AWS Root account activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

The AWS Root account has successfully performed an operation in the project.

Attacker's Goals

Account hijackings.

Investigative actions

- Check that the Root user is not compromised.
- Check the need to modify the Root's credentials.

3.53 | Kubernetes Pod Created with host Inter Process Communications (IPC) namespace

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)

ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)
Severity	Informational

Description

An identity created a Kubernetes pod with the host Inter Process Communications (IPC) namespace.
This may indicate an adversary attempting to access data used by other pods that use the host's IPC namespace.

Attacker's Goals

Access data used by other pods that use the host's IPC namespace.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any files in the /dev/shm shared memory location.
- Inspect for any IPC facilities being used with /usr/bin/ipcs.

Variations

Kubernetes Pod Created with host Inter Process Communications (IPC) namespace for the first time in the cluster

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Execution (TA0002)
ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with the host Inter Process Communications (IPC) namespace.
This may indicate an adversary attempting to access data used by other pods that use the host's IPC namespace.

Attacker's Goals

Access data used by other pods that use the host's IPC namespace.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any files in the /dev/shm shared memory location.
- Inspect for any IPC facilities being used with /usr/bin/ipcs.

Kubernetes Pod Created with host Inter Process Communications (IPC) namespace for the first time in the namespace

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with the host Inter Process Communications (IPC) namespace.
This may indicate an adversary attempting to access data used by other pods that use the host's IPC namespace.

Attacker's Goals

Access data used by other pods that use the host's IPC namespace.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any files in the /dev/shm shared memory location.
- Inspect for any IPC facilities being used with /usr/bin/ipcs.

Kubernetes Pod Created with host Inter Process Communications (IPC) namespace for the first time by the identity

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with the host Inter Process Communications (IPC) namespace.
This may indicate an adversary attempting to access data used by other pods that use the host's IPC namespace.

Attacker's Goals

Access data used by other pods that use the host's IPC namespace.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any files in the /dev/shm shared memory location.
- Inspect for any IPC facilities being used with /usr/bin/ipcs.

3.54 | Kubernetes Privileged Pod Creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Informational

Description

An identity created a Kubernetes pod with a privileged container.
This may indicate an adversary attempting to access that host's filesystem or gain root access to the host.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Variations

Kubernetes Privileged Pod Creation for the first time in the cluster

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with a privileged container.
This may indicate an adversary attempting to access that host's filesystem or gain root access to the host.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Kubernetes Privileged Pod Creation for the first time in the namespace

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Execution (TA0002)
ATT&CK Technique	Escape to Host (T1611) Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with a privileged container.
This may indicate an adversary attempting to access that host's filesystem or gain root access to the host.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Kubernetes Privileged Pod Creation for the first time by the identity

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Execution (TA0002)

ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes pod with a privileged container.
This may indicate an adversary attempting to access that host's filesystem or gain root access to the host.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

3.55 | Kubernetes pod creation from unknown container image registry

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Low

Description

A Kubernetes pod was created with a container image from an unknown registry.

Attacker's Goals

Deploy container with a malicious image to facilitate execution.

Investigative actions

- Check the image registry designation in the organization.
- Scan the container image for any malicious components.

Variations

Kubernetes pod creation from unusual container image registry

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Low

Description

A Kubernetes pod was created with a container image from an unknown registry.

Attacker's Goals

Deploy container with a malicious image to facilitate execution.

Investigative actions

- Check the image registry designation in the organization.
- Scan the container image for any malicious components.

3.56 | A cloud snapshot was created or modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	- Exfiltration (TA0010) - Defense Evasion (TA0005)
ATT&CK Technique	- Transfer Data to Cloud Account (T1537) - Modify Cloud Compute Infrastructure (T1578)
Severity	Informational

Description

A cloud identity has created or modified a cloud snapshot.

Attacker's Goals

Exfiltrate sensitive data that resides on the snapshot.

Investigative actions

- Check if the identity intended to create or modify the snapshot.
- Check if the identity performed additional malicious operations within the cloud environment.

Variations

A cloud snapshot was publicly shared

Synopsis

ATT&CK Tactic	• Exfiltration (TA0010) • Defense Evasion (TA0005)
ATT&CK Technique	• Transfer Data to Cloud Account (T1537) • Modify Cloud Compute Infrastructure (T1578)
Severity	Low

Description

A cloud identity has created or modified a cloud snapshot.

Attacker's Goals

Exfiltrate sensitive data that resides on the snapshot.

Investigative actions

- Check if the identity intended to create or modify the snapshot.
- Check if the identity performed additional malicious operations within the cloud environment.

A cloud snapshot was shared with an unusual AWS account

Synopsis

ATT&CK Tactic	• Exfiltration (TA0010) • Defense Evasion (TA0005)
ATT&CK Technique	• Transfer Data to Cloud Account (T1537) • Modify Cloud Compute Infrastructure (T1578)
Severity	Low

Description

A cloud identity has created or modified a cloud snapshot.

Attacker's Goals

Exfiltrate sensitive data that resides on the snapshot.

Investigative actions

- Check if the identity intended to create or modify the snapshot.
- Check if the identity performed additional malicious operations within the cloud environment.
- Check which AWS accounts the snapshot was shared with.

3.57 | An identity attached an administrative policy to an IAM user/role

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

An identity attached a highly privileged policy to an IAM user/role.

Attacker's Goals

Escalate privileges in cloud environments.

Investigative actions

- Confirm whether this activity was intentional.
- Check for other API calls that were executed by the identity.
- Look for any suspicious behavior from the IAM user/role to whom the administrative policy was attached.

Variations

An identity with high administrative activity attached an administrative policy to an IAM user/role

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

An identity with high administrative activity attached a highly privileged policy to an IAM user/role.

Attacker's Goals

Escalate privileges in cloud environments.

Investigative actions

- Confirm whether this activity was intentional.
- Check for other API calls that were executed by the identity.
- Look for any suspicious behavior from the IAM user/role to whom the administrative policy was attached.

An identity attached an administrative policy to itself/role

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Low

Description

An identity attached a highly privileged policy to an IAM user/role.

Attacker's Goals

Escalate privileges in cloud environments.

Investigative actions

- Confirm whether this activity was intentional.
- Check for other API calls that were executed by the identity.
- Look for any suspicious behavior from the IAM user/role to whom the administrative policy was attached.

An identity failed to attach an administrative policy to an IAM user/role

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Medium

Description

An identity attached a highly privileged policy to an IAM user/role.

Attacker's Goals

Escalate privileges in cloud environments.

Investigative actions

- Confirm whether this activity was intentional.
- Check for other API calls that were executed by the identity.
- Look for any suspicious behavior from the IAM user/role to whom the administrative policy was attached.

A suspicious identity attached an administrative policy to an IAM user/role

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Medium

Description

An identity attached a highly privileged policy to an IAM user/role.

Attacker's Goals

Escalate privileges in cloud environments.

Investigative actions

- Confirm whether this activity was intentional.
- Check for other API calls that were executed by the identity.
- Look for any suspicious behavior from the IAM user/role to whom the administrative policy was attached.

3.58 | AWS STS temporary credentials were generated

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

AWS STS temporary credentials were generated for an AWS identity.

Attacker's Goals

- Gain access and persistence to AWS account.

Investigative actions

- Check which operation executed with the new credentials.

3.59 | An AWS Lambda Function was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	• Execution (TA0002) • Persistence (TA0003)
ATT&CK Technique	• Serverless Execution (T1648) • Scheduled Task/Job: Scheduled Task (T1053.005)
Severity	Informational

Description

An AWS Lambda Function was created.

Attacker's Goals

- Execute malicious code on AWS using Lambda functions.
- Maintain persistence on AWS Lambda by creating or invoking Lambda functions.

Investigative actions

- Identify the Lambda function that was created and analyze its code for any malicious activity.

3.60 | A cloud identity invoked IAM related persistence operations

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Account Manipulation (T1098) • Create Account (T1136) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

A cloud identity invoked IAM related persistence operations.

Attacker's Goals

Maintain persistence in cloud environments.

Investigative actions

- Check what API calls were executed by the identity.
- Check what cloud resources were affected.
- Look for signs that the identity is compromised.

Variations

A cloud identity invoked compute instance related persistence operations

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Event Triggered Execution (T1546) • Implant Internal Image (T1525)
Severity	Informational

Description

A cloud identity invoked compute instance related persistence operations.

Attacker's Goals

Maintain persistence in cloud environments.

Investigative actions

- Check what API calls were executed by the identity.
- Check what cloud resources were affected.
- Look for signs that the identity is compromised.

A cloud identity invoked compute function related persistence operations

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution (T1546)

Severity	Informational

Description

A cloud identity invoked compute function related persistence operations.

Attacker's Goals

Maintain persistence in cloud environments.

Investigative actions

- Check what API calls were executed by the identity.
- Check what cloud resources were affected.
- Look for signs that the identity is compromised.

3.61 | An AWS EFS file-share was deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

An AWS EFS File-share has been deleted.

Attacker's Goals

- Gain access to sensitive data stored on the AWS EFS File-share.

Investigative actions

Check the AWS EFS File-shares for any modifications or deletions.

3.62 | AWS Flow Logs deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Low

Description

A cloud identity has deleted one or more Flow Logs records.

Attacker's Goals

Exfiltrate information.

Investigative actions

- Check if the Identity intended to delete the Flow Logs record/s.
- Check what VPC is affected by this.

3.63 | Suspicious API call from a Tor exit node

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Multi-hop Proxy (T1090.003)
Severity	High

Description

A cloud API was called from a Tor exit node.

Attacker's Goals

Conceal information about malicious activities, such as location and network usage.

Investigative actions

Block all web traffic to and from public Tor entry and exit nodes.

Variations

Suspicious Kubernetes API call from a Tor exit node

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Multi-hop Proxy (T1090.003)
Severity	High

Description

A Kubernetes API was called from a Tor exit node.

Attacker's Goals

Conceal information about malicious activities, such as location and network usage.

Investigative actions

Block all web traffic to and from public Tor entry and exit nodes.

A Failed API call from a Tor exit node

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Multi-hop Proxy (T1090.003)
Severity	Informational

Description

A cloud API was called from a Tor exit node.

Attacker's Goals

Conceal information about malicious activities, such as location and network usage.

Investigative actions

Block all web traffic to and from public Tor entry and exit nodes.

3.64 | A Kubernetes service account has enumerated its permissions

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Container and Resource Discovery (T1613)
Severity	Informational

Description

A Kubernetes service account has enumerated its permissions using the self subject review API.

Attacker's Goals

Discover permissions to the Kubernetes cluster.

Investigative actions

- Determine the scope of the Kubernetes service account permissions.
- Review additional activity of the Kubernetes service account.

Variations

Suspicious permission enumeration by a Kubernetes service account

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Container and Resource Discovery (T1613)
Severity	Low

Description

A Kubernetes service account has enumerated its permissions using the self subject review API.

Attacker's Goals

Discover permissions to the Kubernetes cluster.

Investigative actions

- Determine the scope of the Kubernetes service account permissions.
- Review additional activity of the Kubernetes service account.

A Kubernetes service account attempted to enumerate its permissions

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Container and Resource Discovery (T1613)
Severity	Low

Description

A Kubernetes service account has attempted to enumerate its permissions using the self subject review API.

Attacker's Goals

Discover permissions to the Kubernetes cluster.

Investigative actions

- Determine the scope of the Kubernetes service account permissions.
- Review additional activity of the Kubernetes service account.

3.65 | A Kubernetes namespace was created or deleted

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading (T1036)
Severity	Informational

Description

A Kubernetes namespace was created or deleted.

Attacker's Goals

- Manipulating namespace name to make it appear legitimate or benign.

Investigative actions

- Check which changes were made to the Kubernetes namespace.

3.66 | AWS Config Recorder stopped

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Informational

Description

Configuration Recorder was stopped for a resource in AWS Config.

Attacker's Goals

An attacker may change the configuration of the affected resource to remain undetected.

Investigative actions

- Check the identity which stopped the configuration recording.
- Check what resources are affected by this change.

3.67 | AWS Cloud Trail log trail modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Impact (TA0040) • Defense Evasion (TA0005)
ATT&CK Technique	• Data Manipulation (T1565) • Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Informational

Description

Update trail's configuration, which controls what events are being logged, and how to handle log files.

Attacker's Goals

An attacker may change the configuration of the affected resource to remain undetected.

Investigative actions

- Check the identity which updated the trail's configuration.
- Check which resource is affected by this change.
- Check if there is a new destination for logs archiving.

3.68 | Cloud storage delete protection disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ○ AWS Audit Log OR ○ Azure Audit Log OR ○ Gcp Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	Informational

Description

Delete protection of a cloud storage resource was disabled.

Attacker's Goals

- Impair built-in protection of the cloud environment.
- This action may be a preliminary action before deleting the cloud resource itself.

Investigative actions

- Confirm that the identity intended to disable deletion protection on this resource.
- Follow further actions done by the identity.
- Monitor this resource for other suspicious activities.

Variations

Cloud storage delete protection disabled by an unusual identity

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	Informational

Description

Delete protection of a cloud storage resource was disabled by an unusual identity.

Attacker's Goals

- Impair built-in protection of the cloud environment.
- This action may be a preliminary action before deleting the cloud resource itself.

Investigative actions

- Confirm that the identity intended to disable deletion protection on this resource.
- Follow further actions done by the identity.
- Monitor this resource for other suspicious activities.

3.69 | Cloud Trail logging deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Low

Description

Cloud Trail logging deletion.

Attacker's Goals

An attacker may use this API to hide its actions.

Investigative actions

- Check if the identity intended to delete the trail.
- Check if another trail should be enabled.

Variations

Cloud Trail logging deletion by an identity with high administrative activity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Informational

Description

Cloud Trail logging deletion by an identity with high administrative activity.

Attacker's Goals

An attacker may use this API to hide its actions.

Investigative actions

- Check if the identity intended to delete the trail.
- Check if another trail should be enabled.

3.70 | EC2 snapshot attribute has been modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Transfer Data to Cloud Account (T1537)

Severity	Informational

Description

The snapshot's permissions were modified (added/removed).

Attacker's Goals

Exfiltrate backup/stored information.

Investigative actions

- Check if the snapshot is shared with an unwanted account/actor.

3.71 | AWS SecurityHub findings were modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ○ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Indicator Removal (T1070)
Severity	Informational

Description

AWS SecurityHub findings were modified.

Attacker's Goals

- Bypass security measures implemented by AWS SecurityHub.

Investigative actions

- Check the current AWS SecurityHub settings and verify they are configured properly.

3.72 | A user logged in to the AWS console for the first time

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	- Defense Evasion (TA0005) - Lateral Movement (TA0008)
ATT&CK Technique	- Use Alternate Authentication Material: Application Access Token (T1550.001) - Use Alternate Authentication Material: Application Access Token (T1550.001)
Severity	Informational

Description

A user logged in to the AWS console for the first time.

Attacker's Goals

- Evading detections by performing direct operations using the AWS console.
- Performing non-automatic operations easily.

Investigative actions

- Check if the identity is an AWS identity.
- Investigate which operations were performed by the identity.

Variations

A non-user identity logged in to the AWS console for the first time

Synopsis

ATT&CK Tactic	- Defense Evasion (TA0005) - Lateral Movement (TA0008)
ATT&CK Technique	- Use Alternate Authentication Material: Application Access Token (T1550.001) - Use Alternate Authentication Material: Application Access Token (T1550.001)
Severity	Medium

Description

A non-user identity logged in to the AWS console for the first time.

Attacker's Goals

- Evading detections by performing direct operations using the AWS console.
- Performing non-automatic operations easily.

Investigative actions

- Check if the identity is an AWS identity.
- Investigate which operations were performed by the identity.

3.73 | Kubernetes Pod Created With Sensitive Volume

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	• Privilege Escalation (TA0004) • Execution (TA0002)
ATT&CK Technique	• Escape to Host (T1611) • Deploy Container (T1610)
Severity	Informational

Description

An identity created a Kubernetes Pod with a sensitive volume, allowing the Pod to have read or write permissions on the host's filesystem
This could suggest an effort by an adversary to access sensitive files on the host and employ techniques for escalating privileges.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Variations

Kubernetes Pod Created With Sensitive Volume for the first time in the cluster

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Execution (TA0002)
ATT&CK Technique	Escape to Host (T1611) Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes Pod with a sensitive volume, allowing the Pod to have read or write permissions on the host's filesystem
This could suggest an effort by an adversary to access sensitive files on the host and employ techniques for escalating privileges.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Kubernetes Pod Created With Sensitive Volume for the first time in the namespace

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Execution (TA0002)
ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)
Severity	Low

Description

An identity created a Kubernetes Pod with a sensitive volume, allowing the Pod to have read or write permissions on the host's filesystem
This could suggest an effort by an adversary to access sensitive files on the host and employ techniques for escalating privileges.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Kubernetes Pod Created With Sensitive Volume for the first time by the identity

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Execution (TA0002)
ATT&CK Technique	- Escape to Host (T1611) - Deploy Container (T1610)

Severity	Low

Description

An identity created a Kubernetes Pod with a sensitive volume, allowing the Pod to have read or write permissions on the host's filesystem
This could suggest an effort by an adversary to access sensitive files on the host and employ techniques for escalating privileges.

Attacker's Goals

- Gain access to the host's filesystem.
- Gain root access to the host.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

3.74 | Disable encryption operations

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Manipulation (T1565)
Severity	Low

Description

Encryption was disabled on the servers that host EC2 instances, both for data-at-rest and data-in-transit.

Attacker's Goals

Decrypt sensitive data host on EC2 instance, this may be a step in a flow for data exfiltration.

Investigative actions

- Check if Identity intended to disable the encryption.

3.75 | AWS network ACL rule deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Low

Description

An AWS network ACL rule was deleted.

Attacker's Goals

This action may assist an attacker gain persistence for the cloud environment (in case of ingress rule).
Or in case of egress rule, this may allow an attacker to exfiltrate data.

Investigative actions

- Check which VPC is affected and the resources it contains.
- Check the rule number (as they effect by order).
- Check if the rule is ingress/egress.

3.76 | An AWS database service master user password was

changed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

An AWS database service master user password was changed.

Attacker's Goals

- Gain access and control of the database.

Investigative actions

- Confirm the identity intended to perform this action.
- Follow further actions done by the identity.
- Check what other changes were made to the AWS Database instance or cluster.

Variations

An AWS Database Service master user password was changed from an unusual country

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Low

Description

An AWS database service master user password was changed.

Attacker's Goals

- Gain access and control of the database.

Investigative actions

- Confirm the identity intended to perform this action.
- Follow further actions done by the identity.
- Check what other changes were made to the AWS Database instance or cluster.

An AWS Database Service master user password was changed by a non-DevOps identity

Synopsis

ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004)
Severity	Low

Description

An AWS database service master user password was changed.

Attacker's Goals

- Gain access and control of the database.

Investigative actions

- Confirm the identity intended to perform this action.
- Follow further actions done by the identity.
- Check what other changes were made to the AWS Database instance or cluster.

3.77 | An AWS GuardDuty IP set was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Informational

Description

An AWS GuardDuty IP set has been created.

Attacker's Goals

Evade detection.

Investigative actions

Check which IP set has been modified and confirm the changes.

3.78 | AWS IAM resource group deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

An AWS IAM resource group was deleted, this action may affect the permissions of the members of the deleted group.

Attacker's Goals

An attacker may interrupt the availability of an account, this may revoke access to the account.

Investigative actions

- Check what members were affected by this action.

3.79 | Cloud unusual access key creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Informational

Description

Cloud suspicious access key creation by a cloud identity.

Attacker's Goals

Persist in the environment.

Investigative actions

- investigate the identity who created the access token.
- Check the access token activity in the organization.

Variations

Cloud successful access key creation by an unusual identity

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Low

Description

Cloud suspicious access key creation by a cloud identity.

Attacker's Goals

Persist in the environment.

Investigative actions

- investigate the identity who created the access token.
- Check the access token activity in the organization.

Cloud unusual successful access key creation

Synopsis

ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Low

Description

Cloud suspicious access key creation by a cloud identity.

Attacker's Goals

Persist in the environment.

Investigative actions

- investigate the identity who created the access token.
- Check the access token activity in the organization.

3.80 | Unusual cloud identity impersonation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	- Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Gcp Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Privilege Escalation (TA0004) • Defense Evasion (TA0005)
ATT&CK Technique	• Valid Accounts: Cloud Accounts (T1078.004) • Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access (T1548.005)
Severity	Informational

Description

A cloud identity attempted to impersonate another identity for the first time.

Attacker's Goals

- Escalate privileges and bypass access controls
- Avoid detection throughout their compromise.

Investigative actions

- Check the identity's designation.
- Verify that the identity did not perform any sensitive operation on behalf of the impersonated identity.

Variations

Unusual cloud identity impersonation by an identity with high administrative activity

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Defense Evasion (TA0005)

ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access (T1548.005)
Severity	Informational

Description

A cloud identity with high administrative activity attempted to impersonate another identity for the first time.

Attacker's Goals

- Escalate privileges and bypass access controls
- Avoid detection throughout their compromise.

Investigative actions

- Check the identity's designation.
- Verify that the identity did not perform any sensitive operation on behalf of the impersonated identity.

Suspicious cloud identity impersonation was succeeded

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Defense Evasion (TA0005)
ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access (T1548.005)
Severity	Medium

Description

A cloud identity has impersonated another identity for the first time.

Attacker's Goals

- Escalate privileges and bypass access controls
- Avoid detection throughout their compromise.

Investigative actions

- Check the identity's designation.
- Verify that the identity did not perform any sensitive operation on behalf of the impersonated identity.

Suspicious cloud identity impersonation was failed

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Defense Evasion (TA0005)
ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access (T1548.005)
Severity	Informational

Description

A cloud identity has failed to impersonate another identity.

Attacker's Goals

- Escalate privileges and bypass access controls
- Avoid detection throughout their compromise.

Investigative actions

- Check the identity's designation.
- Verify that the identity did not perform any sensitive operation on behalf of the impersonated identity.

3.81 | Penetration testing tool attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A failed cloud API executed by a penetration testing tool.

Attacker's Goals

Usage of known tools and frameworks.

Investigative actions

- Check if there is an active PT test ongoing.

3.82 | A Kubernetes cluster role binding was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation: Additional Container Cluster Roles (T1098.006)

Severity	Informational

Description

A Kubernetes cluster role binding was created or deleted.

Attacker's Goals

- Escalate privileges to gain access to restricted resources in the Kubernetes cluster.

Investigative actions

- Check which changes were made to the Kubernetes cluster role binding.

3.83 | An identity created or updated password for an IAM user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	• Privilege Escalation (TA0004) • Persistence (TA0003)
ATT&CK Technique	• Valid Accounts: Cloud Accounts (T1078.004) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

An identity created or updated an AWS console password for an IAM user.

Attacker's Goals

Escalate privileges, maintain persistence in cloud environments.

Investigative actions

- Verify whether the identity should be making this action.
- Examine what additional API calls were made by the identity.

Variations

A suspicious identity created or updated password for an IAM user

Synopsis

ATT&CK Tactic	• Privilege Escalation (TA0004) • Persistence (TA0003)
ATT&CK Technique	• Valid Accounts: Cloud Accounts (T1078.004) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Low

Description

An identity created or updated an AWS console password for an IAM user.

Attacker's Goals

Escalate privileges, maintain persistence in cloud environments.

Investigative actions

- Verify whether the identity should be making this action.
- Examine what additional API calls were made by the identity.

3.84 | Kubernetes vulnerability scanning tool usage

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API

ATT&CK Tactic	- Execution (TA0002) - Discovery (TA0007)
ATT&CK Technique	- Deploy Container (T1610) - Container and Resource Discovery (T1613)
Severity	Medium

Description

A known vulnerability scanning tool was used within a Kubernetes cluster.

Attacker's Goals

Usage of known tools and frameworks to exploit Kubernetes clusters.

Investigative actions

- Check if this activity is expected (e.g. penetration testing).
- Determine which Kubernetes resources were affected.
- Review additional events for any suspicious activity within the cluster.

Variations

Kubernetes vulnerability scanning tool usage within a pod

Synopsis

ATT&CK Tactic	- Execution (TA0002) - Discovery (TA0007)
ATT&CK Technique	- Deploy Container (T1610) - Container and Resource Discovery (T1613)
Severity	Medium

Description

A known vulnerability scanning tool was used from a pod within a Kubernetes cluster.

Attacker's Goals

Usage of known tools and frameworks to exploit Kubernetes clusters.

Investigative actions

- Check if this activity is expected (e.g. penetration testing).
- Determine which Kubernetes resources were affected.
- Review additional events for any suspicious activity within the cluster.

External Kubernetes vulnerability scanning tool usage

Synopsis

ATT&CK Tactic	• Execution (TA0002) • Discovery (TA0007)
ATT&CK Technique	• Deploy Container (T1610) • Container and Resource Discovery (T1613)
Severity	Medium

Description

A known vulnerability scanning tool was used within a Kubernetes clusteroutside the cloud environment.

Attacker's Goals

Usage of known tools and frameworks to exploit Kubernetes clusters.

Investigative actions

- Check if this activity is expected (e.g. penetration testing).
- Determine which Kubernetes resources were affected.
- Review additional events for any suspicious activity within the cluster.

3.85 | Remote usage of an AWS service token

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Low

Description

An AWS service token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate a token and abuse it remotely.

Investigative actions

- Check what actions were executed by the service.
- Check if the IAM role was assumed by a different identity.
- Check which API calls were executed by the access-key.

Variations

Remote usage of an AWS EKS token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal Application Access Token (T1528) Unsecured Credentials (T1552)
Severity	High

Description

An AWS service token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate a token and abuse it remotely.

Investigative actions

- Check what actions were executed by the service.
- Check if the IAM role was assumed by a different identity.
- Check which API calls were executed by the access-key.

Suspicious usage of an AWS EKS token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Low

Description

An AWS service token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate a token and abuse it remotely.

Investigative actions

- Check what actions were executed by the service.
- Check if the IAM role was assumed by a different identity.
- Check which API calls were executed by the access-key.

Suspicious usage of an AWS ECS token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	High

Description

An AWS service token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate a token and abuse it remotely.

Investigative actions

- Check what actions were executed by the service.
- Check if the IAM role was assumed by a different identity.
- Check which API calls were executed by the access-key.

Remote usage of an AWS ECS token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Low

Description

An AWS service token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate a token and abuse it remotely.

Investigative actions

- Check what actions were executed by the service.
- Check if the IAM role was assumed by a different identity.
- Check which API calls were executed by the access-key.

Suspicious usage of AWS service token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)

Severity	High

Description

An AWS service token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate a token and abuse it remotely.

Investigative actions

- Check what actions were executed by the service.
- Check if the IAM role was assumed by a different identity.
- Check which API calls were executed by the access-key.

3.86 | Remote usage of AWS Lambda's token

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Informational

Description

An AWS Lambda's token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the role is attached to the Lambda.
- Check if the IAM role was assumed by a different identity.
- Check what API calls were executed by the access-key.

Variations

Remote command line usage of AWS Lambda's token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	High

Description

An AWS Lambda's token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the role is attached to the Lambda.
- Check if the IAM role was assumed by a different identity.
- Check what API calls were executed by the access-key.

Suspicious usage of AWS Lambda's role

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Medium

Description

An AWS Lambda's token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the role is attached to the Lambda.
- Check if the IAM role was assumed by a different identity.
- Check what API calls were executed by the access-key.

Suspicious usage of AWS Lambda's role

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Low

Description

An AWS Lambda's token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the role is attached to the Lambda.
- Check if the IAM role was assumed by a different identity.
- Check what API calls were executed by the access-key.

Suspicious usage of AWS Lambda's token

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	High

Description

An AWS Lambda's token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the role is attached to the Lambda.
- Check if the IAM role was assumed by a different identity.
- Check what API calls were executed by the access-key.

Usage of AWS Lambda's token from known ASN

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	• Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Informational

Description

An AWS Lambda's token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the role is attached to the Lambda.
- Check if the IAM role was assumed by a different identity.
- Check what API calls were executed by the access-key.

3.87 | An AWS SES Email sending settings were modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An AWS SES Email sending settings were modified.

Attacker's Goals

- Gain access to confidential emails of an organization.
- Compromise the organization's cloud Email infrastructure.

Investigative actions

- Check whether the SES Email sending setting modification was intentional.

3.88 | A cloud instance was stopped

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	System Shutdown/Reboot (T1529)

Severity	Informational

Description

A cloud compute instance was stopped.

Attacker's Goals

Interrupt business services.

Investigative actions

- Review recent activity related to the identity and the affected cloud instance.

3.89 | Aurora DB cluster stopped

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Service Stop (T1489)
Severity	Informational

Description

An Aurora DB cluster (RDS) was stopped.

Attacker's Goals

This may assist an attacker to exfiltrate sensitive information.

Investigative actions

- Check if the identity intended to stop the cluster.
- Check if this DB contains sensitive information.
- Check encryption for the DB cluster (at rest).

3.90 | A compute-attached identity executed API calls outside the instance's region

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires: - AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	- Initial Access (TA0001) - Credential Access (TA0006)
ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Steal Application Access Token (T1528) - Unsecured Credentials (T1552)
Severity	Informational

Description

A compute-attached identity performed actions outside the compute instance region.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Verify whether the compute-attached identity's credentials were intentionally used remotely.
- Check what API calls were executed using instance's attached role.
- Check if the suspected instance is compromised.

Variations

A compute-attached identity executed API calls outside the Lambda function's region

Synopsis

ATT&CK Tactic	• Initial Access (TA0001) • Credential Access (TA0006)
ATT&CK Technique	• Valid Accounts: Cloud Accounts (T1078.004) • Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Informational

Description

A compute-attached identity performed actions outside the Lambda function region.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Verify whether the compute-attached identity's credentials were intentionally used remotely.
- Check what API calls were executed using instance's attached role.
- Check if the suspected instance is compromised.

A compute-attached identity executed API calls outside the instance's region from an unusual geolocation and ASN

Synopsis

ATT&CK Tactic	• Initial Access (TA0001) • Credential Access (TA0006)
ATT&CK Technique	• Valid Accounts: Cloud Accounts (T1078.004) • Steal Application Access Token (T1528) • Unsecured Credentials (T1552)

Severity	High

Description

A compute-attached identity performed actions outside the compute instance region.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Verify whether the compute-attached identity's credentials were intentionally used remotely.
- Check what API calls were executed using instance's attached role.
- Check if the suspected instance is compromised.

A compute-attached identity executed API calls outside the instance's region from an unusual geolocation

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Credential Access (TA0006)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004) Steal Application Access Token (T1528) Unsecured Credentials (T1552)
Severity	Medium

Description

A compute-attached identity performed actions outside the compute instance region.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Verify whether the compute-attached identity's credentials were intentionally used remotely.
- Check what API calls were executed using instance's attached role.
- Check if the suspected instance is compromised.

A compute-attached identity executed API calls outside the instance's region from an unusual ASN

Synopsis

ATT&CK Tactic	• Initial Access (TA0001) • Credential Access (TA0006)
ATT&CK Technique	• Valid Accounts: Cloud Accounts (T1078.004) • Steal Application Access Token (T1528) • Unsecured Credentials (T1552)
Severity	Low

Description

A compute-attached identity performed actions outside the compute instance region.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Verify whether the compute-attached identity's credentials were intentionally used remotely.
- Check what API calls were executed using instance's attached role.
- Check if the suspected instance is compromised.

A compute-attached identity executed API calls outside the instance's region

Synopsis

ATT&CK Tactic	• Initial Access (TA0001) • Credential Access (TA0006)

ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Steal Application Access Token (T1528) - Unsecured Credentials (T1552)
Severity	Low

Description

A compute-attached identity performed actions outside the compute instance region.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Verify whether the compute-attached identity's credentials were intentionally used remotely.
- Check what API calls were executed using instance's attached role.
- Check if the suspected instance is compromised.

A compute-attached identity failed to execute API calls outside the instance's region

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Credential Access (TA0006)
ATT&CK Technique	- Valid Accounts: Cloud Accounts (T1078.004) - Steal Application Access Token (T1528) - Unsecured Credentials (T1552)
Severity	Informational

Description

A compute-attached identity performed actions outside the compute instance region.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Verify whether the compute-attached identity's credentials were intentionally used remotely.
- Check what API calls were executed using instance's attached role.
- Check if the suspected instance is compromised.

3.91 | An identity disabled bucket logging

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Logs (T1562.008)

Severity	Informational

Description

An identity disabled bucket logging.

Attacker's Goals

Avoid detection by disabling cloud logging capabilities.

Investigative actions

- Determine whether this activity was done on purpose.
- Examine additional API calls made by the identity.

3.92 | A Kubernetes API operation was successfully invoked by an anonymous user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log

Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001)
Severity	Medium

Description

An unauthenticated user successfully invoked API calls within the Kubernetes cluster.

Attacker's Goals

Gain initial access to a Kubernetes cluster.

Investigative actions

- Determine which resources were accessed anonymously.
- Verify whether the affected resource should be accessed by unauthenticated users.

Variations

A Kubernetes API operation was successfully invoked by an anonymous user outside the cluster

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001)
Severity	High

Description

An unauthenticated user successfully invoked API calls within the Kubernetes cluster.

Attacker's Goals

Gain initial access to a Kubernetes cluster.

Investigative actions

- Determine which resources were accessed anonymously.
- Verify whether the affected resource should be accessed by unauthenticated users.

3.93 | Network sniffing detected in Cloud environment

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	- Credential Access (TA0006) - Discovery (TA0007)
ATT&CK Technique	Network Sniffing (T1040)
Severity	Informational

Description

Network sniffing tool was used in cloud environment.

Attacker's Goals

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network.

Investigative actions

- Check the targeted resources and the sniffing policy.
- Check the cloud identity activity prior/after the network sniffing.

Variations

Unusual Network sniffing detected in Cloud environment

Synopsis

ATT&CK Tactic	- Credential Access (TA0006) - Discovery (TA0007)
ATT&CK Technique	Network Sniffing (T1040)
Severity	Low

Description

Network sniffing tool was used in cloud environment.

Attacker's Goals

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network.

Investigative actions

- Check the targeted resources and the sniffing policy.
- Check the cloud identity activity prior/after the network sniffing.

Successful Network sniffing detected in Cloud environment

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Discovery (TA0007)
ATT&CK Technique	Network Sniffing (T1040)
Severity	Informational

Description

Network sniffing tool was used in cloud environment.

Attacker's Goals

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network.

Investigative actions

- Check the targeted resources and the sniffing policy.
- Check the cloud identity activity prior/after the network sniffing.

3.94 | A Kubernetes role binding was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation: Additional Container Cluster Roles (T1098.006)
Severity	Informational

Description

A Kubernetes role binding was created or deleted.

Attacker's Goals

- Obtain Kubernetes secrets to access restricted information.

Investigative actions

- Check which changes were made to the Kubernetes secret.

3.95 | An AWS EFS File-share mount was deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)

Severity	Informational

Description

An AWS EFS File-share mount was deleted.

Attacker's Goals

- Modify or delete data stored in the EFS File-share.

Investigative actions

- Verify whether the identity that deleted the File-share should be making this action.

3.96 | Suspicious cloud compute instance ssh keys modification attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log

Detection Modules	Cloud
Detector Tags	Cloud Lateral Movement Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Informational

Description

An identity attempted to modify the SSH keys of a single compute instance.
This may indicate an attacker's attempt to maintain persistence on the cloud instance.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

Variations

Suspicious cloud compute instance ssh keys modification attempt by an identity with high administrative activity

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)

Severity	Informational

Description

An identity attempted to modify the SSH keys of a single compute instance.
The identity has high administrative activity
This may indicate an attacker's attempt to maintain persistence on the cloud instance.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

Instance SSH keys were modified for the first time in the cloud provider

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	High

Description

An identity has modified the SSH keys of an instance for the first time in the cloud provider.
This may indicate an attacker's attempt to maintain persistence on the cloud instance.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

Suspicious cloud compute instance SSH keys modification by a service account

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Medium

Description

A service account has modified the SSH keys of a single compute instance.
This may indicate an attacker's attempt to maintain persistence on the cloud instance.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

Suspicious cloud compute instance SSH keys modification

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Informational

Description

An identity has modified the SSH keys of a single compute instance.
This may indicate an attacker's attempt to maintain persistence on the cloud instance.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

Suspicious GCP project level metadata modification by a service account

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Low

Description

A service account has modified the metadata of the entire instances in the project.
This may indicate an attacker's attempt to perform lateral movement within the project.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

Suspicious GCP project level metadata modification

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Informational

Description

An identity account has modified the metadata of the entire instances in the project.
This may indicate an attacker's attempt to perform lateral movement within the project.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

Suspicious GCP project level metadata modification attempt

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Informational

Description

An identity account has modified the metadata of the entire instances in the project.
This may indicate an attacker's attempt to perform lateral movement within the project.

Attacker's Goals

- Maintain persistence on a compromised compute instance.
- Escalate local privileges to gain root on compute instance.

Investigative actions

- Investigate if SSH keys were modified or added at the instance or project level.
- Investigate which permissions were obtained as a result of the SSH keys modification.

3.97 | Unusual IAM enumeration activity by a non-user Identity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	- Account Discovery (T1087) - Permission Groups Discovery (T1069) - Cloud Service Discovery (T1526)
Severity	Informational

Description

An unusual command which may be related to an IAM recon enumeration was executed by a non-user identity.

Attacker's Goals

Gain information on the Cloud environment, specifically IAM information such as User, Group, Roles, Policies, etc.

Investigative actions

Check if the API call was made by the identity.
Check if there are additional unusual API calls from the identity.

3.98 | A Kubernetes cluster was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

A Kubernetes cluster was created or deleted.

Attacker's Goals

- Leverage access to manipulate the Kubernetes infrastructure.

Investigative actions

- Check which changes were made to the Kubernetes cluster and whether they are expected.

3.99 | AWS Role Trusted Entity modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

Role's trusted entity's has been updated, this grants cloud identities permission to assume that role.

Attacker's Goals

Modifying a Role's trusted entity's policy may allow an attacker to privilege his permissions.

Investigative actions

- Check which entities may assume the role after the policy modification.
- If the role allows cross account action, verify the role's policy and permissions.

3.100 | Kubernetes cluster events deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	- Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Tools (T1562.001)

Severity	Informational

Description

Kubernetes cluster events deletion.

Attacker's Goals

- Adversaries may delete Kubernetes events to avoid possible detection.

Investigative actions

- Check whether these changes are expected.

3.101 | Data encryption was disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	• Weaken Encryption (T1600) • Impair Defenses (T1562)
Severity	Informational

Description

A cloud identity has disabled data encryption.

Attacker's Goals

- Attacker is trying to access sensitive data in plaintext.
- Attacker might try to exfiltrate plaintext data to an endpoint controlled by the attacker and avoid detection.
- Attacker can re encrypt the data with a key that is available only to the attacker.

Investigative actions

- Check if the identity intended to disable data encryption.
- Check which cloud assets were affected by manipulating above-mentioned configuration file.
- Check if the identity performed additional suspicious actions to affected assets.

3.102 | An operation was performed by an identity from a domain that was not seen in the organization

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	External Remote Services (T1133)
Severity	Informational

Description

An operation was performed by an identity. This identity belongs to a domain that was not seen in the organization before.

Attacker's Goals

Gain their initial foothold within the organization and explore the environment to achieve their target.

Investigative actions

- investigate the external domain name.
- Check the cloud identity activity in the organization.

Variations

An operation was performed by an identity from a domain that was not seen in the tenant

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	External Remote Services (T1133)
Severity	Low

Description

An operation was performed by an identity. This identity belongs to a domain that was not seen in the organization before.

Attacker's Goals

Gain their initial foothold within the organization and explore the environment to achieve their target.

Investigative actions

- investigate the external domain name.
- Check the cloud identity activity in the organization.

3.103 | Cloud Watch alarm deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Informational

Description

A Cloud Watch alarm was deleted.

Attacker's Goals

Delete alarm to evade detection.

Investigative actions

- Check the identity that deleted the alarm.
- Check the which resource were related to the deleted alarm.

3.104 | Kubernetes service account activity outside the cluster

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001)
Severity	Informational

Description

A service account user successfully invoked API calls outside the Kubernetes cluster.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Determine which Kubernetes resources were accessed using the service account.
- Verify whether the service account token was exposed.

Variations

Unusual Kubernetes service account activity outside the cluster

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001)
Severity	Low

Description

A service account user successfully invoked API calls outside the Kubernetes cluster.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Determine which Kubernetes resources were accessed using the service account.
- Verify whether the service account token was exposed.

Kubernetes service account activity outside the cluster from non-cloud IP

Synopsis

ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001)
Severity	Low

Description

A service account user successfully invoked API calls outside the Kubernetes cluster.

Attacker's Goals

Gain access to the Kubernetes cluster.

Investigative actions

- Determine which Kubernetes resources were accessed using the service account.
- Verify whether the service account token was exposed.

3.105 | A Kubernetes service was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Informational

Description

A Kubernetes service was created or deleted.

Attacker's Goals

- Attackers may attempt to perform denial-of-service attacks to make services unavailable.

Investigative actions

- Check which changes were made to the Kubernetes service.

3.106 | An identity started an AWS SSM session

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	Cloud Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Direct Cloud VM Connections (T1021.008)
Severity	Informational

Description

AWS SSM interactive session.

Attacker's Goals

Gaining unauthorized access, executing unauthorized commands, or compromising sensitive information within the target system.

Investigative actions

- Examine the specifics of the SSM session, including the source IP address, identity, and timestamp.
- Validate the permissions and roles associated with the user initiating the SSM session to ensure they align with the expected level of access.
- Follow further actions taken by the identity or on the relevant instance.

Variations

An identity started an unusual AWS SSM session

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Direct Cloud VM Connections (T1021.008)
Severity	Medium

Description

AWS SSM interactive session.

Attacker's Goals

Gaining unauthorized access, executing unauthorized commands, or compromising sensitive information within the target system.

Investigative actions

- Examine the specifics of the SSM session, including the source IP address, identity, and timestamp.
- Validate the permissions and roles associated with the user initiating the SSM session to ensure they align with the expected level of access.
- Follow further actions taken by the identity or on the relevant instance.

An unusual identity started an AWS SSM session

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Direct Cloud VM Connections (T1021.008)
Severity	Low

Description

AWS SSM interactive session.

Attacker's Goals

Gaining unauthorized access, executing unauthorized commands, or compromising sensitive information within the target system.

Investigative actions

- Examine the specifics of the SSM session, including the source IP address, identity, and timestamp.
- Validate the permissions and roles associated with the user initiating the SSM session to ensure they align with the expected level of access.
- Follow further actions taken by the identity or on the relevant instance.

3.107 | A Kubernetes ConfigMap was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	5 Days
Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A Kubernetes ConfigMap was created or deleted.

Attacker's Goals

- Maintain persistence using valid credentials.

Investigative actions

- Check which changes were made to the Kubernetes ConfigMap.

3.108 | A cloud storage configuration was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Cloud Compute Infrastructure (T1578)
Severity	Informational

Description

A cloud storage configuration was modified.

Attacker's Goals

An attacker may use this API to grant storage access permission.

Investigative actions

- Check if the identity intended to modify the storage configuration.
- Check if the identity performed additional malicious operations in the cloud environment.

3.109 | AWS EC2 instance exported into S3

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Transfer Data to Cloud Account (T1537)

Severity	Informational

Description

A running or stopped instance was exported to an Amazon S3 bucket.

Attacker's Goals

An attack may exfiltrate data from an EC2 instance to an S3 bucket outside the account.

Investigative actions

- Check the identity which exported the instance.
- Check to which S3 bucket the EC2 was exported into.
- Check the S3 bucket permission and policy.

3.110 | AWS web ACL deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Low

Description

Web ACL defines a collection of rules to use to inspect and control web requests.
A Web ACL has been deleted.

Attacker's Goals

To impair defense, this may assist data exfiltration.

Investigative actions

- Verify if the Identity intended to delete the Web ACL.
- Check what resources are affected by the Web ACL deletion.

3.111 | Cloud email service activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Internal Spearphishing (T1534)
Severity	Informational

Description

A cloud Identity performed an email service operation.

Attacker's Goals

Abuse the cloud email service for sending phishing emails.

Investigative actions

- Check for any following actions related to this activity.
- Verify that the identity did not abuse the email service to send phishing emails to victims.

Variations

Unusual cloud email service activity

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Internal Spearphishing (T1534)
Severity	Low

Description

A cloud Identity performed an email service operation for the first time in the tenant.

Attacker's Goals

Abuse the cloud email service for sending phishing emails.

Investigative actions

- Check for any following actions related to this activity.
- Verify that the identity did not abuse the email service to send phishing emails to victims.

Cloud email service entity creation

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Internal Spearphishing (T1534)
Severity	Low

Description

A cloud Identity created a new cloud email identity.

Attacker's Goals

Abuse the cloud email service for sending phishing emails.

Investigative actions

- Check for any following actions related to this activity.
- Verify that the identity did not abuse the email service to send phishing emails to victims.

3.112 | An AWS ElastiCache security group was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Cloud Firewall (T1562.007)
Severity	Informational

Description

An AWS ElastiCache security group was created.

Attacker's Goals

- Gain access to sensitive data stored in AWS ElastiCache.

Investigative actions

- Check the security group and its rules to ensure they meet the security policies of the organization.

3.113 | Cloud identity reached a throttling API rate

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud

Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Informational

Description

A cloud identity has executed a high volume of API calls, causing a throttling error.

Attacker's Goals

Abuse cloud resource, such behavior is usually seen during a cryptocurrency attacks.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity.

Variations

Cloud identity reached a highly unusual throttling API rate

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Low

Description

A cloud identity has executed a high volume of API calls, causing a throttling error.
This indicates on a high volume of cloud instances allocation, such activity may be related to a cryptocurrency attack.

Attacker's Goals

Abuse cloud resource, such behavior is usually seen during a cryptocurrency attacks.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity.

Cloud identity reached an unusual throttling API rate in the cloud project

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Informational

Description

A cloud identity has executed a high volume of API calls, causing a throttling error.
This API rate is unusual on the project level.

Attacker's Goals

Abuse cloud resource, such behavior is usually seen during a cryptocurrency attacks.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity.

Cloud identity reached an unusual throttling API rate

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Informational

Description

A cloud identity has executed a high volume of API calls, causing a throttling error. This activity is unusual for the cloud identity, and was not seen in the last 30 days.

Attacker's Goals

Abuse cloud resource, such behavior is usually seen during a cryptocurrency attacks.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity.

3.114 | Kubernetes admission controller activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	- Persistence (TA0003) - Credential Access (TA0006)
ATT&CK Technique	- Valid Accounts (T1078) - Unsecured Credentials: Container API (T1552.007)
Severity	Informational

Description

A Kubernetes admission controller has been created or modified.

Attacker's Goals

- Intercept the requests to the Kubernetes API sever, records secrets, and other sensitive information.
- Modify requests to the Kubernetes API sever.

Investigative actions

- Verify whether the identity should use Kubernetes admission controllers.
- Examine the role of the Kubernetes admission controller and its intended function.
- Investigate other operations that were performed by the identity within the cluster.

Variations

Kubernetes validating admission controller was used in the organization for the first time

Synopsis

ATT&CK Tactic	• Persistence (TA0003) • Credential Access (TA0006)
ATT&CK Technique	• Valid Accounts (T1078) • Unsecured Credentials: Container API (T1552.007)
Severity	Low

Description

A validating Kubernetes admission controller has been created or modified.

Attacker's Goals

- Intercept the requests to the Kubernetes API sever, records secrets, and other sensitive information.
- Modify requests to the Kubernetes API sever.

Investigative actions

- Verify whether the identity should use Kubernetes admission controllers.
- Examine the role of the Kubernetes admission controller and its intended function.
- Investigate other operations that were performed by the identity within the cluster.

Kubernetes mutating admission controller was used in the organization for the first time

Synopsis

ATT&CK Tactic	• Persistence (TA0003) • Credential Access (TA0006)

ATT&CK Technique	• Valid Accounts (T1078) • Unsecured Credentials: Container API (T1552.007)
Severity	Medium

Description

A mutating Kubernetes admission controller has been created or modified.

Attacker's Goals

- Intercept the requests to the Kubernetes API sever, records secrets, and other sensitive information.
- Modify requests to the Kubernetes API sever.

Investigative actions

- Verify whether the identity should use Kubernetes admission controllers.
- Examine the role of the Kubernetes admission controller and its intended function.
- Investigate other operations that were performed by the identity within the cluster.

Kubernetes validating admission controller was used in the cluster for the first time

Synopsis

ATT&CK Tactic	• Persistence (TA0003) • Credential Access (TA0006)
ATT&CK Technique	• Valid Accounts (T1078) • Unsecured Credentials: Container API (T1552.007)
Severity	Low

Description

A validating Kubernetes admission controller has been created or modified.

Attacker's Goals

- Intercept the requests to the Kubernetes API sever, records secrets, and other sensitive information.
- Modify requests to the Kubernetes API sever.

Investigative actions

- Verify whether the identity should use Kubernetes admission controllers.
- Examine the role of the Kubernetes admission controller and its intended function.
- Investigate other operations that were performed by the identity within the cluster.

Kubernetes mutating admission controller was used in the cluster for the first time

Synopsis

ATT&CK Tactic	- Persistence (TA0003) - Credential Access (TA0006)
ATT&CK Technique	- Valid Accounts (T1078) - Unsecured Credentials: Container API (T1552.007)
Severity	Medium

Description

A mutating Kubernetes admission controller has been created or modified.

Attacker's Goals

- Intercept the requests to the Kubernetes API sever, records secrets, and other sensitive information.
- Modify requests to the Kubernetes API sever.

Investigative actions

- Verify whether the identity should use Kubernetes admission controllers.
- Examine the role of the Kubernetes admission controller and its intended function.
- Investigate other operations that were performed by the identity within the cluster.

3.115 | S3 configuration deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Encrypted for Impact (T1486)
Severity	Informational

Description

An S3 bucket configuration has been deleted.
This may affect the S3 access, and the objects it contains.

Attacker's Goals

Modify the S3 configuration and expose stored sensitive data.

Investigative actions

- Check what data is stored on the S3.
- Check which configuration change has been made.
- Verify this change did not make this S3 publicly available.

3.116 | Unusual AWS systems manager activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ∘ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Cloud Compute Infrastructure (T1578)
Severity	Informational

Description

A cloud Identity performed an SSM operation for the first time.

Attacker's Goals

Manipulate SSM operations to take control over EC2 instances and strengthen the foothold in the cloud environment of the organization, by running critical operating system commands, manipulating the parameters store, and patch management configuration.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive SSM operation that it shouldn't.

Variations

Unusual AWS systems manager activity by an identity with high administrative activity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Cloud Compute Infrastructure (T1578)
Severity	Informational

Description

A cloud identity with high administrative activity performed an SSM operation for the first time.

Attacker's Goals

Manipulate SSM operations to take control over EC2 instances and strengthen the foothold in the cloud environment of the organization, by running critical operating system commands, manipulating the parameters store, and patch management configuration.

Investigative actions

- Check the identity's role designation in the organization.
- Verify that the identity did not perform any sensitive SSM operation that it shouldn't.

3.117 | AWS SSM send command attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	Cloud Lateral Movement Analytics
ATT&CK Tactic	• Lateral Movement (TA0008) • Execution (TA0002)
ATT&CK Technique	• Remote Services: Direct Cloud VM Connections (T1021.008) • Cloud Administration Command (T1651)
Severity	Informational

Description

An identity executed an AWS SSM Document.

Attacker's Goals

Gaining unauthorized access, executing unauthorized commands, or compromising sensitive information within the target system.

Investigative actions

- Examine the code in the SSM document, and the target objects.
- Validate the permissions and roles associated with the user initiating the SSM session to ensure they align with the expected level of access.
- Follow further actions taken by the identity or on the relevant targets.

Variations

Unusual AWS SSM send command

Synopsis

ATT&CK Tactic	• Lateral Movement (TA0008) • Execution (TA0002)
ATT&CK Technique	• Remote Services: Direct Cloud VM Connections (T1021.008) • Cloud Administration Command (T1651)
Severity	Low

Description

An identity executed an AWS SSM Document.

Attacker's Goals

Gaining unauthorized access, executing unauthorized commands, or compromising sensitive information within the target system.

Investigative actions

- Examine the code in the SSM document, and the target objects.
- Validate the permissions and roles associated with the user initiating the SSM session to ensure they align with the expected level of access.
- Follow further actions taken by the identity or on the relevant targets.

3.118 | A Kubernetes DaemonSet was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Deploy Container (T1610)
Severity	Informational

Description

A Kubernetes DaemonSet was created.

Attacker's Goals

- Deploy a container into an environment to facilitate execution.

Investigative actions

- Check which changes were made to the Kubernetes DaemonSet.

3.119 | A container registry was created or deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

A container registry was created or deleted.

Attacker's Goals

- Gain access to sensitive data stored in the container registry.
- Modify or delete existing data in the container registry.

Investigative actions

- Check the activity logs to determine what was created or removed.

3.120 | A cloud identity executed an API call from an unusual country

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A cloud identity, that is usually connecting from a small set of countries, connected from a new country for the first time.

Attacker's Goals

Access sensitive resources and gain high privileges.

Investigative actions

Check if the identity routed their traffic via a VPN, or shared their credentials with a remote employee.

Variations

A Kubernetes identity executed an API call from a country that was not seen in the organization

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Medium

Description

A Kubernetes identity, that is usually connecting from a small set of countries, connected from a new country for the first time.

Attacker's Goals

Access sensitive resources and gain high privileges.

Investigative actions

Check if the identity routed their traffic via a VPN, or shared their credentials with a remote employee.

A cloud identity executed an API call from a country that was not seen in the organization

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Medium

Description

A cloud identity, that is usually connecting from a small set of countries, connected from a new country for the first time.

Attacker's Goals

Access sensitive resources and gain high privileges.

Investigative actions

Check if the identity routed their traffic via a VPN, or shared their credentials with a remote employee.

A cloud identity executed an API call from an unusual country

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A cloud identity, that is usually connecting from a small set of countries, connected from a new country for the first time.

Attacker's Goals

Access sensitive resources and gain high privileges.

Investigative actions

Check if the identity routed their traffic via a VPN, or shared their credentials with a remote employee.

A Kubernetes API call was executed from an unusual country

Synopsis

ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A Kubernetes identity, that is usually connecting from a small set of countries, connected from a new country for the first time.

Attacker's Goals

Access sensitive resources and gain high privileges.

Investigative actions

Check if the identity routed their traffic via a VPN, or shared their credentials with a remote employee.

A cloud API call was executed from an unusual country

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A cloud identity, that is usually connecting from a small set of countries, connected from a new country for the first time.

Attacker's Goals

Access sensitive resources and gain high privileges.

Investigative actions

Check if the identity routed their traffic via a VPN, or shared their credentials with a remote employee.

3.121 | Unusual cross projects activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ∘ AWS Audit Log OR ∘ Azure Audit Log OR ∘ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)

Severity	Low

Description

A suspicious activity between different cloud projects.

Attacker's Goals

Abuse an existing connection and pivot through multiple projects to find their target.

Investigative actions

- Check if the identity intended to perform actions on the project.
- Check the operations that were performed on the project {caller_project}.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Variations

Suspicious cross projects activity

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)
Severity	Medium

Description

A suspicious activity between different cloud projects.

Attacker's Goals

Abuse an existing connection and pivot through multiple projects to find their target.

Investigative actions

- Check if the identity intended to perform actions on the project.
- Check the operations that were performed on the project {caller_project}.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

3.122 | Unusual exec into a Kubernetes Pod

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Kubernetes - API
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)

Severity	Informational

Description

An identity initiated a shell session within a Kubernetes pod using the exec command.
The command allows an identity to establish a temporary shell session and execute commands in the pod.
This may indicate an attacker attempting to gain an interactive shell, which will allow access to the pod's data.

Attacker's Goals

- Execute commands within the Kubernetes Pod.
- Access any resource the Kubernetes Pod has access to.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Variations

First time execution into Kubernetes Pod at the cluster-level

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Medium

Description

An identity initiated a shell session within a Kubernetes pod using the exec command.
The command allows an identity to establish a temporary shell session and execute commands in the pod.
This may indicate an attacker attempting to gain an interactive shell, which will allow access to the pod's data.

Attacker's Goals

- Execute commands within the Kubernetes Pod.
- Access any resource the Kubernetes Pod has access to.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Identity executed into Kubernetes Pod for the first time

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Low

Description

An identity initiated a shell session within a Kubernetes pod using the exec command.
The command allows an identity to establish a temporary shell session and execute commands in the pod.
This may indicate an attacker attempting to gain an interactive shell, which will allow access to the pod's data.

Attacker's Goals

- Execute commands within the Kubernetes Pod.
- Access any resource the Kubernetes Pod has access to.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Identity executed into a Kubernetes namespace for the first time

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Low

Description

An identity initiated a shell session within a Kubernetes pod using the exec command.
The command allows an identity to establish a temporary shell session and execute commands in the pod.
This may indicate an attacker attempting to gain an interactive shell, which will allow access to the pod's data.

Attacker's Goals

- Execute commands within the Kubernetes Pod.
- Access any resource the Kubernetes Pod has access to.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

Identity executed into a Kubernetes Pod for the first time

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Low

Description

An identity initiated a shell session within a Kubernetes pod using the exec command.
The command allows an identity to establish a temporary shell session and execute commands in the pod.
This may indicate an attacker attempting to gain an interactive shell, which will allow access to the pod's data.

Attacker's Goals

- Execute commands within the Kubernetes Pod.
- Access any resource the Kubernetes Pod has access to.

Investigative actions

- Check the identity's role designation in the organization.
- Inspect for any additional suspicious activities inside the Kubernetes Pod.

3.123 | Unusual resource modification by newly seen IAM user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires one of the following data sources: ◦ AWS Audit Log OR ◦ Azure Audit Log OR ◦ Gcp Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Impact (TA0040)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004) Data Destruction (T1485)
Severity	Informational

Description

A cloud resource was modified by a newly seen IAM user.

Attacker's Goals

Leverage access to manipulate cloud infrastructure.

Investigative actions

- Examine which resources were affected and how.
- Investigate any unusual activity originating from the identity.

Variations

Unusual Kubernetes resource modification by newly seen IAM user

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Impact (TA0040)

ATT&CK Technique	• Valid Accounts: Cloud Accounts (T1078.004) • Data Destruction (T1485)
Severity	Informational

Description

A cloud resource was modified by a newly seen IAM user.

Attacker's Goals

Leverage access to manipulate cloud infrastructure.

Investigative actions

- Examine which resources were affected and how.
- Investigate any unusual activity originating from the identity.

Unusual IAM resource modification by newly seen IAM user

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Low

Description

A cloud resource was modified by a newly seen IAM user.

Attacker's Goals

Leverage access to manipulate cloud infrastructure.

Investigative actions

- Examine which resources were affected and how.
- Investigate any unusual activity originating from the identity.

Unusual resource modification by newly seen IAM user from an uncommon IP

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Impact (TA0040)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004) Data Destruction (T1485)
Severity	Low

Description

A cloud resource was modified by a newly seen IAM user.

Attacker's Goals

Leverage access to manipulate cloud infrastructure.

Investigative actions

- Examine which resources were affected and how.
- Investigate any unusual activity originating from the identity.

3.124 | An AWS Route 53 domain was transferred to another AWS account

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ AWS Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Resource Development (TA0042)
ATT&CK Technique	Acquire Infrastructure: Domains (T1583.001)
Severity	Informational

Description

An AWS Route 53 domain was transferred to another AWS account.

Attacker's Goals

- Gain access to DNS records and abuse them for malicious purposes.

Investigative actions

- Check if the domain transfer was done by an authorized user.