3.125 | AWS Guard-Duty detector 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

AWS Guard-Duty detector was deleted.

Attacker's Goals

This action may assist an attacker to evade detection.

Investigative actions

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

3.126 | Suspicious heavy allocation of compute resources - possible mining 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	• Impact (TA0040) • Initial Access (TA0001)

ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity.
Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Variations

Suspicious heavy allocation of compute resources - possible mining activity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity.
Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Suspicious heavy allocation of compute resources - possible mining activity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity.
Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Suspicious heavy allocation of compute resources - possible mining activity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity.
Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

3.127 | A Kubernetes dashboard service account was used 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	External Remote Services (T1133)
Severity	Medium

Description

A Kubernetes dashboard service account was successfully used externally of the Kubernetes environment, which may indicate that the dashboard is exposed to the internet and does not require authentication.

Attacker's Goals

Gain initial access to the Kubernetes cluster.

Investigative actions

- Determine which Kubernetes resources were accessed through the dashboard.
- Check whether any changes were made to the Kubernetes cluster.

Variations

A Kubernetes dashboard service account was unsuccessfully used outside the cluster

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	External Remote Services (T1133)
Severity	Low

Description

A Kubernetes dashboard service account was successfully used externally of the Kubernetes environment, which may indicate that the dashboard is exposed to the internet and does not require authentication.
The operation was unsuccessful.

Attacker's Goals

Gain initial access to the Kubernetes cluster.

Investigative actions

- Determine which Kubernetes resources were accessed through the dashboard.
- Check whether any changes were made to the Kubernetes cluster.

3.128 | Activity in a dormant region of a cloud project

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	Defense Evasion (TA0005)
ATT&CK Technique	Unused/Unsupported Cloud Regions (T1535)
Severity	Informational

Description

A cloud project had unusual activity in a previously dormant region.

Attacker's Goals

Abuse services in unused geographic regions to evade detection.
Attackers can take advantage of unmonitored regions to avoid detection of their activities. These activities may include various malicious activities, including attacks against internal cloud resources, lateral movement within the environment, mining cryptocurrency through resource hijacking, and more.

Investigative actions

- Check if the detected region is required.
- Delete any resource that was created in the unused region.
- Disable all unused regions.

Variations

Activity in a dormant region of a cloud project by an identity with high administrative activity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Unused/Unsupported Cloud Regions (T1535)
Severity	Informational

Description

A cloud project had unusual activity in a previously dormant region made by an identity with high administrative activity.

Attacker's Goals

Abuse services in unused geographic regions to evade detection.
Attackers can take advantage of unmonitored regions to avoid detection of their activities. These activities may include various malicious activities, including attacks against internal cloud resources, lateral movement within the environment, mining cryptocurrency through resource hijacking, and more.

Investigative actions

- Check if the detected region is required.
- Delete any resource that was created in the unused region.
- Disable all unused regions.

A cloud compute instance was created in a dormant region

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Unused/Unsupported Cloud Regions (T1535)
Severity	Medium

Description

A cloud project had unusual activity in a previously dormant region.

Attacker's Goals

Abuse services in unused geographic regions to evade detection.
Attackers can take advantage of unmonitored regions to avoid detection of their activities. These activities may include various malicious activities, including attacks against internal cloud resources, lateral movement within the environment, mining cryptocurrency through resource hijacking, and more.

Investigative actions

- Check if the detected region is required.
- Delete any resource that was created in the unused region.
- Disable all unused regions.

3.129 | Billing admin role was removed

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	Account Access Removal (T1531)
Severity	Low

Description

Sensitive Action - Billing admin role was removed.

Attacker's Goals

Prevent billing notifications from being sent to the billing admin.

Investigative actions

- Check if the identity intended to remove the billing admin.
- Check if the identity performed additional malicious operations in the cloud environment.

3.130 | Suspicious objects encryption in an AWS bucket

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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	High

Description

An AWS KMS key from a non-organization owned account was used to encrypt multiple objects in the bucket for the first time.
This may indicate an attacker's attempt to perform a ransomware attack against the organization's cloud environment.

Attacker's Goals

- Gain monetary compensation in exchange for decryption or the decryption key.
- Permanently deny access to important storage objects.

Investigative actions

- Check if the external KMS service is a legit encryption service.
- Check if the identity performed enumeration activity to detect insecure s3 buckets, which are configured without the versioning and MFA Delete mechanisms.
- Detect additional buckets that were encrypted using the same external KMS service.
- Disable the identity from which the external service was configured.
- Enable versioning on every critical bucket.
- Enable MFA Delete on every critical bucket.

3.131 | Abnormal Allocation of compute resources in multiple regions

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes

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) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Informational

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Variations

Abnormal Unusual allocation of compute resources in multiple regions

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Abnormal Suspicious allocation of compute resources in multiple regions

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)

Severity	High

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Abnormal Allocation of compute resources in a high number of regions

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Abnormal Allocation of compute resources in multiple regions by an unusual identity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

3.132 | An identity dumped multiple secrets from a project

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	1 Hour
Deduplication Period	6 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) • Collection (TA0009)
ATT&CK Technique	• Unsecured Credentials (T1552) • Data from Cloud Storage (T1530)
Severity	Low

Description

An identity dumped multiple secrets from the project, considerably more than usual.
This may indicate an attacker's attempt to dump sensitive information from the cloud environment.

Attacker's Goals

Collect secrets from the cloud environment.

Investigative actions

- Check the accessed secrets' designation.
- Verify that the identity did not dump any sensitive information that it shouldn't.

Variations

An administrative identity dumped multiple secrets from a project

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Collection (TA0009)
ATT&CK Technique	• Unsecured Credentials (T1552) • Data from Cloud Storage (T1530)
Severity	Informational

Description

An identity dumped multiple secrets from the project, considerably more than usual.
This may indicate an attacker's attempt to dump sensitive information from the cloud environment.

Attacker's Goals

Collect secrets from the cloud environment.

Investigative actions

- Check the accessed secrets' designation.
- Verify that the identity did not dump any sensitive information that it shouldn't.

3.133 | Storage enumeration activity

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	10 Minutes
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	• Discovery (TA0007) • Collection (TA0009)
ATT&CK Technique	• Cloud Storage Object Discovery (T1619) • Data from Cloud Storage (T1530) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity attempted to discover cloud objects within storage buckets.
This might be an attempt by an adversary to find sensitive data stored in cloud storage, which could lead to data theft.

Attacker's Goals

Access sensitive data stored in cloud infrastructure.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which storage buckets were enumerated and whether they contained sensitive information.

Variations

Storage enumeration activity by an identity with high administrative activity

Synopsis

ATT&CK Tactic	• Discovery (TA0007) • Collection (TA0009)
ATT&CK Technique	• Cloud Storage Object Discovery (T1619) • Data from Cloud Storage (T1530) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity with high administrative activity attempted to discover cloud objects within storage buckets.
This might be an attempt by an adversary to find sensitive data stored in cloud storage, which could lead to data theft.

Attacker's Goals

Access sensitive data stored in cloud infrastructure.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which storage buckets were enumerated and whether they contained sensitive information.

3.134 | Suspicious identity downloaded multiple objects from a bucket

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)

Severity	Low

Description

An identity downloaded multiple objects from a bucket, considerably more than usual.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

Variations

Suspicious identity with DevOps behavior downloaded multiple objects from a bucket

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Informational

Description

An identity with DevOps behavior downloaded multiple objects from a bucket, considerably more than usual.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

Suspicious identity downloaded multiple objects from a backup storage bucket

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Medium

Description

An identity downloaded multiple objects from a bucket, considerably more than usual.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

3.135 | Cloud user performed multiple actions that were denied

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
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	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Informational

Description

An Identity performed multiple actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute a verity of commands to explore the cloud environment.

Investigative actions

Check if the API calls were made by the identity.
Check if there are additional calls executed by the identity.

Variations

Cloud non-user identity performed multiple actions that were denied

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Low

Description

An Identity performed multiple actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute a verity of commands to explore the cloud environment.

Investigative actions

Check if the API calls were made by the identity.
Check if there are additional calls executed by the identity.

3.136 | Kubernetes enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
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	Kubernetes - API
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Container and Resource Discovery (T1613) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity attempted to discover available resources within a cluster.
This may indicate an adversary attempting to map the Kubernetes environment and discover resources that may assist to perform additional attacks within the environment.

Attacker's Goals

Map the cluster environment and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

Variations

Suspicious Kubernetes enumeration activity

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Container and Resource Discovery (T1613) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity attempted to discover available resources within a cluster.
This may indicate an adversary attempting to map the Kubernetes environment and discover resources that may assist to perform additional attacks within the environment.

Attacker's Goals

Map the cluster environment and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

3.137 | Allocation of multiple cloud compute resources

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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) • Initial Access (TA0001)

ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Informational

Description

An identity allocated multiple compute resources.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Variations

Unusual allocation of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated multiple compute resources.
This activity is highly unusual, such volume of compute allocation was not seen across all the projects during the past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Unusual allocation of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated multiple compute resources.
This activity is highly unusual, such volume of compute allocation was not seen at in this project during the past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Unusual allocation of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated multiple compute resources.
The allocated instances contains GPU accelerators, such pattern is related to a crypto mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Allocation of multiple cloud compute resources with accelerator gear

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity allocated multiple compute resources.
his activity is unusual for this identity in past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Unusual allocation attempt of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity attempted to allocate multiple compute resources.
This activity is highly unusual, such volume of compute allocation was not seen at in this project during the past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

3.138 | IAM Enumeration sequence

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	7 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	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An Identity has executed a sequence of events which may be related to an IAM recon enumeration.

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 calls were made by the identity.
Check if there are additional calls executed by the identity.

Variations

IAM Enumeration sequence executed from a cloud Internet facing instance

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069) • Cloud Service Discovery (T1526)
Severity	Low

Description

A cloud Internet facing instance performed an unusual IAM enumeration.

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 calls were made by the identity.
Check if there are additional calls executed by the identity.

3.139 | Multiple cloud snapshots export

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
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	Exfiltration (TA0010)
ATT&CK Technique	Transfer Data to Cloud Account (T1537)

Severity	Informational

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots locally.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Variations

Multiple cloud snapshots export

Synopsis

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

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots from an external IP address.
This action was unusual based on the cloud project history.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Multiple cloud snapshots export

Synopsis

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

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots from an external IP address.
This action was unusual based on the cloud identity history.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Multiple cloud snapshots export

Synopsis

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

Severity	Low

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots locally.
This action was unusual based on the unsuccessful attempts rate.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Multiple cloud snapshots export

Synopsis

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

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots locally.
This action was unusual based on the cloud project or identity history.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

3.140 | Multiple failed logins from a single IP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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	Informational

Description

Multiple failed logins were observed in a short period of time from a single external IP.
The IP is not a known identity provider.

Attacker's Goals

Gain initial access to the cloud console.

Investigative actions

- Check if the IP is a known IP.
- Check if a successful login from the same IP occurred after the failed login attempts.

Variations

Multiple failed logins from an unknown IP

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)
Severity	Medium

Description

Multiple failed logins were observed in a short period of time from a single external IP.
The IP is not a known identity provider.
The IP is not a known IP in the organization.
This could indicate on an active brute force attempt.

Attacker's Goals

Gain initial access to the cloud console.

Investigative actions

- Check if the IP is a known IP.
- Check if a successful login from the same IP occurred after the failed login attempts.

3.141 | An identity performed a suspicious download of multiple cloud storage objects

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)

Severity	Informational

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

Variations

An identity performed a suspicious download of multiple cloud storage objects from an internal IP

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Informational

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

An identity performed a suspicious download of multiple cloud storage objects

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	High

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.
This large volume of downloaded cloud storage objects had not been seen across all projects for the last 30 days.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

An identity performed a suspicious download of multiple cloud storage objects

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Medium

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.
This large volume of downloaded cloud storage objects had not been seen in this project for the last 30 days.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

An identity performed a suspicious download of multiple cloud storage objects from multiple buckets

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)

Severity	Medium

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.
This large volume of downloaded cloud storage objects from several buckets had not been seen for the last 30 days.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

3.142 | Cloud infrastructure enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
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	Discovery (TA0007)
ATT&CK Technique	• Cloud Infrastructure Discovery (T1580) • Cloud Service Discovery (T1526)
Severity	Informational

Description

A cloud identity attempted to discover available resources within the cloud environment.
This may indicate an adversary attempting to map the organization's cloud environment and discover cloud resources that may assist to perform additional attacks within the environment.

Attacker's Goals

Map the cloud environment and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

Variations

Suspicious cloud infrastructure enumeration activity

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	• Cloud Infrastructure Discovery (T1580) • Cloud Service Discovery (T1526)
Severity	Low

Description

A cloud identity attempted to discover available resources within the cloud environment.
This may indicate an adversary attempting to map the organization's cloud environment and discover cloud resources that may assist to perform additional attacks within the environment.

Attacker's Goals

Map the cloud environment and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

3.143 | Deletion of multiple cloud resources

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
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) • Initial Access (TA0001)
ATT&CK Technique	• Data Destruction (T1485) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

An identity deleted multiple cloud resources.

Attacker's Goals

Leverage access to the cloud to delete resources and cause damage to an organization's infrastructure.

Investigative actions

- Confirm the legitimacy of the suspected identity and what cloud resources have been deleted by the identity.
- Look for any unusual activity associated with the suspected identity and determine whether they are compromised.

Variations

Deletion of multiple cloud resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Data Destruction (T1485) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Medium

Description

An identity deleted multiple cloud resources.
This large volume of deleted cloud resources had not been seen across all projects for the last 30 days.

Attacker's Goals

Leverage access to the cloud to delete resources and cause damage to an organization's infrastructure.

Investigative actions

- Confirm the legitimacy of the suspected identity and what cloud resources have been deleted by the identity.
- Look for any unusual activity associated with the suspected identity and determine whether they are compromised.

Deletion of multiple cloud resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)

ATT&CK Technique	• Data Destruction (T1485) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Low

Description

An identity deleted multiple cloud resources.
This large volume of deleted cloud resources had not been seen in this project for the last 30 days.

Attacker's Goals

Leverage access to the cloud to delete resources and cause damage to an organization's infrastructure.

Investigative actions

- Confirm the legitimacy of the suspected identity and what cloud resources have been deleted by the identity.
- Look for any unusual activity associated with the suspected identity and determine whether they are compromised.

3.144 | Multi region enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
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	• Discovery (TA0007) • Defense Evasion (TA0005)
ATT&CK Technique	• Cloud Infrastructure Discovery (T1580) • Unused/Unsupported Cloud Regions (T1535) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An internal identity performed an operation on multiple regions, considerably more than usual. This may indicate an attacker's attempt to identify all available resources in the cloud environment.

Attacker's Goals

- Discover cloud resources that are available within the environment and leverage them to perform additional attacks against the organization.
- Detect unused geographic regions and leverage them to evade detection of malicious operations.

Investigative actions

- Check the identity designation.
- Verify that the identity did not perform any operation in a region that it shouldn't.

4 | AWS Flow Log

4.1 | Possible DCShadow attempt

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 Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls OR ◦ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Defense Evasion (TA0005)

ATT&CK Technique	• OS Credential Dumping (T1003) • Rogue Domain Controller (T1207)
Severity	High

Description

Attackers may register a compromised host as a new DC to get other DCs to replicate data to it, and then push their malicious AD changes to all DCs.

Attacker's Goals

Retrieve Active Directory data, to later be able to push out malicious Active Directory changes.

Investigative actions

Check whether the destination is a new domain controller or a host that syncs with ADFS or Azure AD.

4.2 | Unusual SSH activity that resembles SSH proxy

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 Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls • Requires one of the following data sources: ◦ Palo Alto Networks Platform Logs OR ◦ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Informational

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Variations

High Volume Unusual SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Suspicious SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Unusual SSH activity that resembles SSH proxy detected

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

4.3 | An internal Cloud resource performed port scan on external networks

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	5 Days

Required Data	• Requires one of the following data sources: ◦ AWS Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Discovery (TA0007) • Impact (TA0040)
ATT&CK Technique	• Network Service Discovery (T1046) • Resource Hijacking (T1496) • Cloud Service Discovery (T1526)
Severity	Medium

Description

An internal cloud resource attempted to connect to the same destination port of multiple external IP addresses.
This may be a result of the cloud resource being hijacked by an attacker.
Attackers perform port scans on a specific destination port for reconnaissance purposes, to detect known vulnerable services that accept connections in the specific port, and perform targeted attacks against them.

Attacker's Goals

Detect vulnerable services, which listen on known ports and are opened to the Internet.

Investigative actions

- Check if similar activity was performed on additional cloud resources.
- Check if similar activity was performed against additional ports and external ip addresses from the same cloud resource.
- Check which process triggered the port scanning activity and for what purpose.

4.4 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls • Requires one of the following data sources: ◦ Palo Alto Networks Platform Logs OR ◦ XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Variations

SSH brute force network detected from external source

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Rare SSH brute force attempt

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

5 | AWS OCSF Flow Logs

5.1 | Possible DCShadow attempt

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 Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls OR ◦ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Defense Evasion (TA0005)

ATT&CK Technique	• OS Credential Dumping (T1003) • Rogue Domain Controller (T1207)
Severity	High

Description

Attackers may register a compromised host as a new DC to get other DCs to replicate data to it, and then push their malicious AD changes to all DCs.

Attacker's Goals

Retrieve Active Directory data, to later be able to push out malicious Active Directory changes.

Investigative actions

Check whether the destination is a new domain controller or a host that syncs with ADFS or Azure AD.

5.2 | Unusual SSH activity that resembles SSH proxy

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 Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls • Requires one of the following data sources: ◦ Palo Alto Networks Platform Logs OR ◦ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Informational

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Variations

High Volume Unusual SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Suspicious SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Unusual SSH activity that resembles SSH proxy detected

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

5.3 | An internal Cloud resource performed port scan on external networks

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	5 Days

Required Data	• Requires one of the following data sources: ◦ AWS Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Discovery (TA0007) • Impact (TA0040)
ATT&CK Technique	• Network Service Discovery (T1046) • Resource Hijacking (T1496) • Cloud Service Discovery (T1526)
Severity	Medium

Description

An internal cloud resource attempted to connect to the same destination port of multiple external IP addresses.
This may be a result of the cloud resource being hijacked by an attacker.
Attackers perform port scans on a specific destination port for reconnaissance purposes, to detect known vulnerable services that accept connections in the specific port, and perform targeted attacks against them.

Attacker's Goals

Detect vulnerable services, which listen on known ports and are opened to the Internet.

Investigative actions

- Check if similar activity was performed on additional cloud resources.
- Check if similar activity was performed against additional ports and external ip addresses from the same cloud resource.
- Check which process triggered the port scanning activity and for what purpose.

5.4 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls • Requires one of the following data sources: ◦ Palo Alto Networks Platform Logs OR ◦ XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Variations

SSH brute force network detected from external source

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Rare SSH brute force attempt

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

6 | Azure Audit Log

6.1 | 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.

6.2 | 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.

6.3 | 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.

6.4 | Azure Blob Container Access Level Modification

Synopsis

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

Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	File and Directory Permissions Modification (T1222)
Severity	Informational

Description

Access level modification for a blob container, this action might be dangerous as sensitive data can be exposed.

Attacker's Goals

Access restricted data.

Investigative actions

- Check if and which data was exposed after the access level modification.

6.5 | 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.

6.6 | 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.

6.7 | 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.

6.8 | 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.

6.9 | Azure user creation/deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Valid Accounts (T1078) • Account Manipulation (T1098)
Severity	Informational

Description

A user in Azure was created or deleted.

Attacker's Goals

Gain persistence into the account.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.10 | Azure mailbox rule creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Collection (TA0009) • Defense Evasion (TA0005)
ATT&CK Technique	• Email Collection: Email Forwarding Rule (T1114.003) • Indicator Removal: Clear Mailbox Data (T1070.008)
Severity	Informational

Description

A Mailbox rule in Azure was created.

Attacker's Goals

Intercept or exfiltrate sensitive information.

Investigative actions

- Investigate the rule's details and confirm its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

Variations

Unusual Azure mailbox rule creation

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Defense Evasion (TA0005)
ATT&CK Technique	• Email Collection: Email Forwarding Rule (T1114.003) • Indicator Removal: Clear Mailbox Data (T1070.008)
Severity	Low

Description

A Mailbox rule in Azure was created.

Attacker's Goals

Intercept or exfiltrate sensitive information.

Investigative actions

- Investigate the rule's details and confirm its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.11 | Azure Key Vault modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials (T1552)
Severity	Informational

Description

Azure Key Vault modifications can be crucial as it stores secrets e.g. encryption keys, certifications, etc.

Attacker's Goals

Exfiltrate information, persistence on existing users or damage critical accounts.

Investigative actions

- Check the identity actions prior/after the Key Vault modification.
- Find which credentials were modified and their usage.

6.12 | An Azure Kubernetes Role or Cluster-Role was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An Azure Kubernetes Role or Cluster-Role was modified or deleted. This could indicate malicious activity and should be investigated.

Attacker's Goals

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

Investigative actions

- Investigate which actions were made by the identity and identify any suspicious activity.

6.13 | 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.

6.14 | External user invitation to Azure tenant

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Persistence (TA0003) • Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

An external user was invited to Azure tenant.

Attacker's Goals

Gain unauthorized access to the tenant.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.15 | 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.

6.16 | 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.

6.17 | 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.

6.18 | 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.

6.19 | 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.

6.20 | 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.

6.21 | Credentials were added to Azure application

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Persistence (TA0003) • Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001)

Severity	Informational

Description

Credentials were added to an Azure application.

Attacker's Goals

An attacker can establish a backdoor in the application by adding additional credentials to it, such as secrets or certificates.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.22 | Azure Network Watcher Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud

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

Description

Network Watchers are used for monitoring and diagnosing for Azure resources. An attacker might use this technique to avoid security mitigations.

Attacker's Goals

Avoid security mitigations and detections.

Investigative actions

- Check which devices are monitored by the deleted Network Watcher.

6.23 | Azure Event Hub Deletion

Synopsis

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

Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	• Impair Defenses (T1562) • Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Low

Description

An Azure event hub was deleted. An attacker might use this technique to evade detection.

Attacker's Goals

Evade detection.

Investigative actions

- Check what actions were taken by the identity that deleted the event hub.

6.24 | 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.

6.25 | 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.

6.26 | 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.

6.27 | 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.

6.28 | 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.

6.29 | Remote usage of an Azure Managed Identity token

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	Cloud Serverless Function Credentials Theft Analytics
ATT&CK Tactic	Credential Access (TA0006)

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

Description

An Azure Managed Identity token, which is attached to a compute service, was used externally of the cloud environment.

Attacker's Goals

Exfiltrate valid token and abuse it remotely.

Investigative actions

- Verify whether the Managed Identity should be used remotely.
- Check what API calls were executed by the Managed Identity.
- Check if the relevant compute service is compromised.

Variations

Remote usage of an Azure Managed Identity token from an unusual ASN

Synopsis

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

Description

An Azure Managed Identity token, which is attached to a compute service, was used externally of the cloud environment.

Attacker's Goals

Exfiltrate valid token and abuse it remotely.

Investigative actions

- Verify whether the Managed Identity should be used remotely.
- Check what API calls were executed by the Managed Identity.
- Check if the relevant compute service is compromised.

Remote usage of an Azure Managed Identity token from an unusual IP

Synopsis

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

Description

An Azure Managed Identity token, which is attached to a compute service, was used externally of the cloud environment.

Attacker's Goals

Exfiltrate valid token and abuse it remotely.

Investigative actions

- Verify whether the Managed Identity should be used remotely.
- Check what API calls were executed by the Managed Identity.
- Check if the relevant compute service is compromised.

6.30 | Azure Automation Webhook creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

Azure Automation Webhook can be used to pass a payload with specific attributes to run a malicious Runbook.

Attacker's Goals

Persistence using a valid account.

Investigative actions

- Check the identity actions prior/after the webhook creation.
- Find which Runbook was executed using the webhook.

6.31 | An Azure 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: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

An Azure Kubernetes Cluster was created or deleted.

Attacker's Goals

- Leverage access to Azure Kubernetes to damage organization's infrastructure.

Investigative actions

- Verify whether the identity should be making this action.
- Look for any suspicious activity initiated by the identity.

6.32 | 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.

6.33 | 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.

6.34 | 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.

6.35 | 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.

6.36 | An Azure Network Security Group was modified

Synopsis

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

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

Description

An Azure Network Security Group was modified or deleted. This could indicate malicious activity or a misconfiguration.

Attacker's Goals

- Bypass security measures to gain access to cloud resources.

Investigative actions

- Check the network security settings of the Azure account to identify any recent changes.

6.37 | An Azure virtual network was modified

Synopsis

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

Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Informational

Description

An Azure virtual network has been modified or deleted.

Attacker's Goals

- Manipulate, interrupt, or destroy data.

Investigative actions

- Verify whether the identity should be making this action.
- Check the audit logs for any suspicious activity related to the virtual network.

6.38 | Azure diagnostic configuration deletion

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	• Impair Defenses (T1562) • Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Informational

Description

An attacker might delete the Azure diagnostic settings to evade detection.

Attacker's Goals

Evade detection.

Investigative actions

- Check the identity and its actions after the deletion action.

6.39 | 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.

6.40 | Azure Event Hub Authorization rule creation/modification

Synopsis

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

Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	External Remote Services (T1133)
Severity	Informational

Description

An authorization rule is bound with specific rights, once created within a namespace, which has management permissions.

Attacker's Goals

Persistence using the created/updated rule.

Investigative actions

- Check the identity that created/updated the authorization rule.
- What actions were taken using the rule.

6.41 | 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.

6.42 | Azure group creation/deletion

Synopsis

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

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

Description

A group in Azure was created or deleted.

Attacker's Goals

Gain persistence to the environment.

Investigative actions

- Check group's assigned roles.
- Check which members were added to the group.

6.43 | 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.

6.44 | An identity accessed Azure Kubernetes Secrets

Synopsis

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

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

An identity has accessed or attempted to access Azure Kubernetes secrets or Config Objects.

Attacker's Goals

- Extract Kubernetes secrets to gain access to restricted resources in the cluster.

Investigative actions

- Verify whether the identity should be making this action.
- Check for any suspicious activity initiated by the identity.

6.45 | An Azure virtual network Device was modified

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Network Denial of Service (T1498)
Severity	Informational

Description

An Azure virtual network Device was modified or deleted.

Attacker's Goals

- Gain access to resources within the virtual network.
- Gain access to sensitive data stored on the virtual network.

Investigative actions

- Investigate the Azure portal for the relevant virtual network device and review the changes made to it.
- Review the Azure Activity Log for any suspicious activities related to the virtual network device.

6.46 | An Azure Suppression Rule was created

Synopsis

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

Description

An Azure Suppression Rule was created.

Attacker's Goals

- Bypass security measures.

Investigative actions

- Investigate the user's activity to determine the cause of the alert.

6.47 | 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.

6.48 | 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.

6.49 | Azure device code authentication flow used

Synopsis

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

Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Defense Evasion (TA0005) • Persistence (TA0003)
ATT&CK Technique	• Account Manipulation (T1098) • Use Alternate Authentication Material (T1550)
Severity	Informational

Description

An Azure AD login was performed with Device code flow.

Attacker's Goals

- An attacker may use a device to access resources in the tenant using an access token from device code authentication flows.

Investigative actions

- Check what devices are listed with the logged-in user.
- Check if the account is authorized to use such devices to access resources.
- Check for possible logins from the device.
- Follow further actions done by the account and device.

Variations

Suspicious Azure device code authentication flow used

Synopsis

ATT&CK Tactic	• Defense Evasion (TA0005) • Persistence (TA0003)
ATT&CK Technique	• Account Manipulation (T1098) • Use Alternate Authentication Material (T1550)
Severity	Low

Description

An Azure AD login was performed with Device code flow.

Attacker's Goals

- An attacker may use a device to access resources in the tenant using an access token from device code authentication flows.

Investigative actions

- Check what devices are listed with the logged-in user.
- Check if the account is authorized to use such devices to access resources.
- Check for possible logins from the device.
- Follow further actions done by the account and device.

6.50 | OneDrive file download

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213)
Severity	Informational

Description

A file was downloaded from OneDrive using Microsoft Graph API.

Attacker's Goals

Exfiltrate sensitive data by downloading files from OneDrive.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.51 | 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.

6.52 | Privileged role used by Azure application

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation: Additional Cloud Roles (T1098.003)
Severity	Informational

Description

An Azure application with high-level API permissions invoked a request to the Microsoft Graph API.

Attacker's Goals

Leverage high-level permissions to gain persistence and access to sensitive information.

Investigative actions

- Check the application's role designation in the organization.
- Look for any unusual behavior originated from the suspected application.

Variations

First-time privileged role is used by Azure application

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation: Additional Cloud Roles (T1098.003)
Severity	Low

Description

An Azure application with high-level API permissions invoked a request to the Microsoft Graph API.

Attacker's Goals

Leverage high-level permissions to gain persistence and access to sensitive information.

Investigative actions

- Check the application's role designation in the organization.
- Look for any unusual behavior originated from the suspected application.

6.53 | 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.

6.54 | 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.

6.55 | An Azure Firewall Rule Collection was modified

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure 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 Azure Firewall Rule Collection was modified. This could indicate a malicious actor attempting to bypass security measures.

Attacker's Goals

- Bypass security measures to gain access to cloud resources.

Investigative actions

- Check the Azure Firewall Rule Collection to identify the modified or deleted rule.

6.56 | 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.

6.57 | 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.

6.58 | Azure conditional access policy creation or modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

An Azure conditional access policy was created or modified.

Attacker's Goals

Bypass authentication controls.

Investigative actions

- Investigate the rule's details and confirm its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.59 | Azure Storage Account key generated

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal Application Access Token (T1528)
Severity	Informational

Description

Azure storage access keys rotation, might affect services/applications depended on the key set.

Attacker's Goals

Exfiltrate information or damage critical services.

Investigative actions

- Check what actions were made by the users a few hours prior/after to the generation operation.
- Which actions were taken using the newly generated access keys.

6.60 | An identity was granted permissions to manage user access to Azure resources

Synopsis

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

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Informational

Description

An identity was granted the User Access Administrator permission at the tenant scope.

Attacker's Goals

- Elevate permission to gain access to all Azure Subscriptions.

Investigative actions

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

6.61 | 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.

6.62 | Azure Key Vault Secrets were modified

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

Azure key vault secrets were modified. A change or deletion of secrets in Azure Key Vault has been detected.

Attacker's Goals

- Gain access to confidential data stored in the Azure Key Vault.

Investigative actions

- Investigate what Azure Key Vault Secrets were modified or deleted.
- Check for any suspicious activity initiated by the identity.

6.63 | Azure user password reset

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Valid Accounts (T1078) • Account Manipulation (T1098)
Severity	Informational

Description

The password of an Azure AD user was reset.

Attacker's Goals

An attacker may attempt to gain access to the account.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.64 | Azure Automation Runbook Creation/Modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An Azure Automation Runbook was being modified or created.

Attacker's Goals

Persistence using a valid account.

Investigative actions

- Check the identity and its actions after the modify/create action.

6.65 | An Azure Firewall policy deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	Impair Defenses (T1562)
Severity	Low

Description

An Azure Firewall policy was deleted. An attacker might use this technique to disable network defenses.

Attacker's Goals

Exfiltrate information, network persistence of a service/resource.

Investigative actions

- Check which subnets or specific IP addresses were affected by the change.
- Check which services were being leveraged after the changes by used protocols/traffic.

6.66 | 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.

6.67 | Modification or Deletion of an Azure Application Gateway Detected

Synopsis

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

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	External Remote Services (T1133)
Severity	Informational

Description

Modification or Deletion of an Azure Application Gateway Detected. A change has been detected in an Azure Application Gateway. This may indicate unauthorized access or malicious activity.

Attacker's Goals

- Gain access to the resources behind the Azure Application Gateway.

Investigative actions

- Check the Azure Application Gateway to identify the changes made.
- Verify whether the identity should be making this action.

6.68 | An Azure VPN Connection was modified

Synopsis

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

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

Description

Modification or removal of an Azure VPN connection was detected. This alert indicates a change to an existing VPN connection, or the deletion of an existing connection.

Attacker's Goals

- Bypass security measures.

Investigative actions

- Check how Azure VPN Connection was modified.
- Verify whether the identity should be making this action.

6.69 | OneDrive file upload

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Resource Development (TA0042)
ATT&CK Technique	• Stage Capabilities (T1608) • Stage Capabilities: Upload Malware (T1608.001)
Severity	Informational

Description

A file was uploaded to OneDrive using Microsoft Graph API.

Attacker's Goals

Establish persistence by uploading files to OneDrive, potentially using it as a staging area for further malicious activities.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.70 | An Azure firewall rule group was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure 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 Azure firewall rule group was modified or deleted.

Attacker's Goals

- Bypass security controls to gain access to restricted resources within the Azure cloud environment.

Investigative actions

- Check the Azure Firewall rule configuration to identify the changes made.
- Verify whether the identity should be making this action.

6.71 | 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.

6.72 | Owner was added to Azure application

Synopsis

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

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

Description

An Owner was added to an Azure application.

Attacker's Goals

Gain administrative control and manipulate the application's permissions and settings.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.73 | Azure Service principal/Application creation

Synopsis

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

Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

An Azure Service principal/Application was created.

Attacker's Goals

To gain persistent access and elevate privileges within the environment.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.74 | 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.

6.75 | Authentication method was added to Azure account

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Informational

Description

A new authentication method was added to an Azure AD user.

Attacker's Goals

Establish a backdoor for persistent access.

Investigative actions

- Review recent authentication attempts and access logs to detect any unauthorized activities or potential misuse of the newly added authentication method.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.76 | PIM privilege member removal

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

An identity with an assigned role from PIM was removed from the membership.

Attacker's Goals

- Revoke access from other temporary privileged accounts.
- Gain sole access to more systems.

Investigative actions

- Investigate the user who initiated the removal.
- Identify the privileged accounts that were affected.
- Review the current access rights of the privileged accounts.

6.77 | Azure permission delegation granted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

An identity delegated permissions to access a certain resource or application.

Attacker's Goals

- Gain control over user accounts.

Investigative actions

- Check the user access logs for any suspicious activity.
- Review the permissions granted and the scope of the permissions.

6.78 | 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.

6.79 | Unusual resource access by Azure application

Synopsis

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

Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

An Azure application had interacted with an unusual resource using the Microsoft Graph API.

Attacker's Goals

Abuse applications to gain access to the Azure tenant.

Investigative actions

- Verify whether the application is intended to use the resource in question.
- Investigate any unusual activity originating from the application.

Variations

Suspicious resource access by Azure application

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Low

Description

An Azure application had interacted with an unusual resource using the Microsoft Graph API.

Attacker's Goals

Abuse applications to gain access to the Azure tenant.

Investigative actions

- Verify whether the application is intended to use the resource in question.
- Investigate any unusual activity originating from the application.

6.80 | 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.

6.81 | Azure Automation Account Creation

Synopsis

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

Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

Azure Automation account was created. An attacker might create an account for persistence.

Attacker's Goals

Persistence using a valid account.

Investigative actions

- Check the identity that created the account and verify its activity.

6.82 | 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.

6.83 | 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.

6.84 | 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.

6.85 | Azure virtual machine commands execution

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	• Requires: ◦ Azure Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter (T1059)
Severity	Informational

Description

An Azure virtual machine executed PowerShell commands with System privileges.

Attacker's Goals

Executing malicious commands for discovery, privilege escalation, etc.

Investigative actions

- Check the VM that executed the commands and their results.

6.86 | An Azure Key Vault key was modified

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

An Azure Key Vault key was modified.

Attacker's Goals

- Gain access to sensitive data stored in the Azure Key Vault.

Investigative actions

- Check the Azure Key Vault configuration to identify what changes were made.

6.87 | Remote usage of an Azure Service Principal token

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure 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 Azure Service Principal token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate valid token and abuse it remotely.

Investigative actions

- Verify whether the Service Principal should be used remotely.
- Check what API calls were executed by the Service Principal.
- Determine whether the Service Principal is compromised.

Variations

Remote usage of an Azure Service Principal token from an unusual ASN

Synopsis

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

Description

An Azure Service Principal token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate valid token and abuse it remotely.

Investigative actions

- Verify whether the Service Principal should be used remotely.
- Check what API calls were executed by the Service Principal.
- Determine whether the Service Principal is compromised.

Remote usage of an Azure Service Principal token from an unusual IP

Synopsis

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

Description

An Azure Service Principal token was used externally of the cloud environment.

Attacker's Goals

Exfiltrate valid token and abuse it remotely.

Investigative actions

- Verify whether the Service Principal should be used remotely.
- Check what API calls were executed by the Service Principal.
- Determine whether the Service Principal is compromised.

6.88 | 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.

6.89 | 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.

6.90 | An Azure application 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: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

An Azure application has executed a high volume of Microsoft Graph API calls, causing a throttling error.

Attacker's Goals

Enumerate cloud services in an Azure tenant.

Investigative actions

- Check the application's role designation in the organization.
- Look for any unusual behavior originated from the suspected application.

Variations

An Azure application reached an unusual throttling API rate

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Low

Description

An Azure application has executed a high volume of Microsoft Graph API calls, causing a throttling error.

Attacker's Goals

Enumerate cloud services in an Azure tenant.

Investigative actions

- Check the application's role designation in the organization.
- Look for any unusual behavior originated from the suspected application.

6.91 | An Azure Kubernetes Role-Binding or Cluster-Role-Binding

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: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An Azure Kubernetes Role-Binding or Cluster-Role-Binding was modified or deleted. This could indicate a security breach or malicious activity.

Attacker's Goals

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

Investigative actions

- Investigate which actions were made by the identity and identify any suspicious activity.
- Review the Kubernetes configuration to identify any other changes.

6.92 | 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.

6.93 | A Service Principal was created in Azure

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A Service Principal was created in Azure. This could indicate a malicious actor attempting to gain access to a resource.

Attacker's Goals

- Access user data.
- Gain control of the Azure environment.

Investigative actions

- Check the Service Principal to ensure it has the correct access rights.
- Review the Azure Activity Log to determine the source of the Service Principal creation.

6.94 | 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.

6.95 | 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.

6.96 | Azure application removed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts (T1564)
Severity	Informational

Description

An Azure application has been deleted.

Attacker's Goals

- Delete apps used for malicious activities.
- Delete evidence of activity.

Investigative actions

- Check the Azure Portal for any changes in applications.
- Review the activities performed by the application.

6.97 | Soft delete of cloud storage configuration was disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	Informational

Description

A Soft Delete configuration was disabled on a cloud storage account.
Soft delete allows a deletion of a blob or a container to be restored.
Disabling it will impair the ability of the cloud environment to recover in disaster scenarios.

Attacker's Goals

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

Investigative actions

- Check if the identity intended to disable soft delete for this storage account.
- Check if the identity performed additional malicious operations in the cloud environment.

6.98 | Attempted Azure application access from unknown tenant

Synopsis

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

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)
Severity	Informational

Description

A Microsoft Graph API was unsuccessfully executed by an Azure application from an unknown tenant.

Attacker's Goals

Abuse serverless services to execute code in cloud environments.

Investigative actions

- Validate the legitimacy of the tenant in question.
- Investigate any unusual activity originating from the application.

Variations

Attempted Azure application access from an unusual tenant

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)
Severity	Medium

Description

A Microsoft Graph API was unsuccessfully executed by an Azure application from an unknown tenant.

Attacker's Goals

Abuse serverless services to execute code in cloud environments.

Investigative actions

- Validate the legitimacy of the tenant in question.
- Investigate any unusual activity originating from the application.

Azure application access from unknown tenant

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)
Severity	Low

Description

A Microsoft Graph API was executed by an Azure application from an unknown tenant.

Attacker's Goals

Abuse serverless services to execute code in cloud environments.

Investigative actions

- Validate the legitimacy of the tenant in question.
- Investigate any unusual activity originating from the application.

6.99 | An Azure DNS Zone was modified

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol: DNS (T1071.004)
Severity	Informational

Description

An Azure DNS zone has been changed or removed, which may indicate malicious activity or a misconfiguration.

Attacker's Goals

- Take control of DNS zones to redirect traffic to malicious websites.

Investigative actions

- Verify whether the identity should be making this action.
- Check what Azure DNS zones were changed or removed.

6.100 | An Azure Kubernetes Service Account 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: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

An Azure Kubernetes Service Account was modified or deleted.

Attacker's Goals

- Gain access to privileged resources using Kubernetes Service Account.

Investigative actions

- Verify whether the identity should be making this action.
- Check the Kubernetes cluster for any suspicious activity initiated by the identity.
- Check if any other service accounts have been modified or deleted.

6.101 | 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.

6.102 | 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.

6.103 | 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.

6.104 | 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.

6.105 | Azure Resource Group Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	

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

Description

Resource group deletion permanently deletes all resources within the group, An attacker might use this technique to avoid detection or destroy procedures/data.

Attacker's Goals

Evade detection.

Investigative actions

- Check which resource group was deleted.

6.106 | 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.

6.107 | A Service Principal was removed from Azure

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Cloud Compute Infrastructure: Delete Cloud Instance (T1578.003)
Severity	Informational

Description

A Service Principal was removed from Azure. This indicates a change in access permissions and may indicate malicious activity.

Attacker's Goals

- Evade defensive measures by deleting a possibly malicious service principal.

Investigative actions

- Check the Azure Active Directory audit logs for the details of the removed service principal.
- Check the Azure role assignments to identify which resources were impacted by the removal of the service principal.

6.108 | An Azure Firewall was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure 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 Azure Firewall was modified or deleted. This may indicate a security risk.

Attacker's Goals

- Bypass security measures.

Investigative actions

- Verify whether the identity should be making this action.
- Check what changes were made to Azure Firewall.

6.109 | Removal of an Azure Owner from an Application or Service Principal

Synopsis

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

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

Description

An Azure Owner was removed from an application or service principal. This may indicate malicious activity or unauthorized access to the application or service.

Attacker's Goals

- Remove owners from applications for full control of the application or service principal.
- Manipulate or delete data stored in the Azure environment.

Investigative actions

- Check the Azure Activity Log to identify which user removed the Azure Owner.
- Check the Azure Role Assignments to identify the current Azure Owners.
- Check the Application or Service Principal to identify if any changes have been made.

6.110 | An Azure Point-to-Site VPN was modified

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562)
Severity	Informational

Description

Modification or Deletion of an Azure Point-to-Site VPN.

Attacker's Goals

- Bypass security controls.

Investigative actions

- Check how the Azure Point-to-Site VPN was modified.
- Verify whether the identity should be making this action.

6.111 | 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.

6.112 | Azure Kubernetes events were deleted

Synopsis

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

Severity	Informational

Description

Events have been deleted in Azure Kubernetes. This could indicate malicious activity.

Attacker's Goals

- Remove evidence or hinder defenses.

Investigative actions

- Look for any suspicious activity initiated by the identity.

6.113 | 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.

6.114 | Granting Access to an Account

Synopsis

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

Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Credential Access (TA0006)
ATT&CK Technique	• Valid Accounts (T1078) • Unsecured Credentials (T1552) • Modify Authentication Process (T1556) • OS Credential Dumping (T1003) • Brute Force (T1110) • Forge Web Credentials (T1606)
Severity	Informational

Description

Azure access has been granted to an account.

Attacker's Goals

- Gain unauthorized access to an account.
- Gain access to sensitive data.

Investigative actions

- Check the account access logs to determine the source of the access.
- Check the account activity logs to determine the purpose of the access.

6.115 | Azure Automation Runbook Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Defense Evasion (TA0005) • Impact (TA0040)
ATT&CK Technique	• Impair Defenses (T1562) • Service Stop (T1489)
Severity	Informational

Description

Azure Automation Runbook deletion damage cause on business automated procedures or a remove malicious Runbook that was part of an attack.

Attacker's Goals

Stop business services.

Investigative actions

- Check which Runbook was deleted and whether it is malicious or valid.

6.116 | 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.

6.117 | 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.

6.118 | OneDrive folder creation

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data Staged: Remote Data Staging (T1074.002)
Severity	Informational

Description

A folder was created in OneDrive using Microsoft Graph API.

Attacker's Goals

Establish persistence or prepare for data exfiltration by creating a storage location in OneDrive via the Microsoft Graph API, enabling them to later upload or manipulate files undetected.

Investigative actions

- Look for any unusual behavior originated from the suspected identity, and check if they're compromised.

6.119 | 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.

6.120 | 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.

6.121 | A New Server was Added to an Azure Active Directory Hybrid Health ADFS Environment

Synopsis

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

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Informational

Description

A new server has been added to an Azure Active Directory Hybrid Health AD FS Environment.

Attacker's Goals

- Gain access to sensitive data stored in the new server.
- Gain access to other servers in the Azure Active Directory Hybrid Health AD FS Environment.
- Gain access to user accounts in the Azure Active Directory Hybrid Health AD FS Environment.

Investigative actions

- Check the Azure Active Directory Hybrid Health Monitor to identify the new server.
- Verify that the new server is correctly configured for ADFS.
- Check the logs for any errors related to the new server.

6.122 | An Azure Key Vault was modified

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

Azure Key Vault has been modified or deleted by an Identity. This could be an indication of unauthorized access or malicious activity.

Attacker's Goals

-
- Gain access to sensitive data stored in the Azure Key Vault.

Investigative actions

- Check the Azure Key Vault configuration to identify what changes were made.

6.123 | Suspicious heavy allocation of compute resources - possible mining 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	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity. Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Variations

Suspicious heavy allocation of compute resources - possible mining activity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity. Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Suspicious heavy allocation of compute resources - possible mining activity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity.
Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Suspicious heavy allocation of compute resources - possible mining activity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)

ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated an unusual heavy compute resource, suspected as mining activity. Heavy machines normally have a high amount of CPU cores or attached with GPU, which are targeted by adversaries to mine Cryptocurrency.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

6.124 | A Kubernetes dashboard service account was used 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	External Remote Services (T1133)
Severity	Medium

Description

A Kubernetes dashboard service account was successfully used externally of the Kubernetes environment, which may indicate that the dashboard is exposed to the internet and does not require authentication.

Attacker's Goals

Gain initial access to the Kubernetes cluster.

Investigative actions

- Determine which Kubernetes resources were accessed through the dashboard.
- Check whether any changes were made to the Kubernetes cluster.

Variations

A Kubernetes dashboard service account was unsuccessfully used outside the cluster

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	External Remote Services (T1133)
Severity	Low

Description

A Kubernetes dashboard service account was successfully used externally of the Kubernetes environment, which may indicate that the dashboard is exposed to the internet and does not require authentication.
The operation was unsuccessful.

Attacker's Goals

Gain initial access to the Kubernetes cluster.

Investigative actions

- Determine which Kubernetes resources were accessed through the dashboard.
- Check whether any changes were made to the Kubernetes cluster.

6.125 | Activity in a dormant region of a cloud project

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	Defense Evasion (TA0005)
ATT&CK Technique	Unused/Unsupported Cloud Regions (T1535)
Severity	Informational

Description

A cloud project had unusual activity in a previously dormant region.

Attacker's Goals

Abuse services in unused geographic regions to evade detection.
Attackers can take advantage of unmonitored regions to avoid detection of their activities. These activities may include various malicious activities, including attacks against internal cloud resources, lateral movement within the environment, mining cryptocurrency through resource hijacking, and more.

Investigative actions

- Check if the detected region is required.
- Delete any resource that was created in the unused region.
- Disable all unused regions.

Variations

Activity in a dormant region of a cloud project by an identity with high administrative activity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Unused/Unsupported Cloud Regions (T1535)
Severity	Informational

Description

A cloud project had unusual activity in a previously dormant region made by an identity with high administrative activity.

Attacker's Goals

Abuse services in unused geographic regions to evade detection.
Attackers can take advantage of unmonitored regions to avoid detection of their activities. These activities may include various malicious activities, including attacks against internal cloud resources, lateral movement within the environment, mining cryptocurrency through resource hijacking, and more.

Investigative actions

- Check if the detected region is required.
- Delete any resource that was created in the unused region.
- Disable all unused regions.

A cloud compute instance was created in a dormant region

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Unused/Unsupported Cloud Regions (T1535)

Severity	Medium

Description

A cloud project had unusual activity in a previously dormant region.

Attacker's Goals

Abuse services in unused geographic regions to evade detection.
Attackers can take advantage of unmonitored regions to avoid detection of their activities. These activities may include various malicious activities, including attacks against internal cloud resources, lateral movement within the environment, mining cryptocurrency through resource hijacking, and more.

Investigative actions

- Check if the detected region is required.
- Delete any resource that was created in the unused region.
- Disable all unused regions.

6.126 | An Azure Cloud Shell was Created

Synopsis

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

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter (T1059)
Severity	Informational

Description

A new Cloud Shell was created in Azure. This indicates that a new virtual environment is available for use.

Attacker's Goals

- Execute malicious commands, scripts, or binaries using newly created cloud shell environment.

Investigative actions

- Check for any suspicious activity initiated by the identity.
- Check if the cloud shell was created by a legitimate user.
- Check if any malicious code was added to the cloud shell.

6.127 | Billing admin role was removed

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	Account Access Removal (T1531)
Severity	Low

Description

Sensitive Action - Billing admin role was removed.

Attacker's Goals

Prevent billing notifications from being sent to the billing admin.

Investigative actions

- Check if the identity intended to remove the billing admin.
- Check if the identity performed additional malicious operations in the cloud environment.

6.128 | Microsoft Teams enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

The Microsoft Graph API was used to enumerate Microsoft Teams channels in an Azure tenant.

Attacker's Goals

To extract sensitive information stored in Microsoft Teams.

Investigative actions

- Determine which Teams channels were enumerated and whether they contained any sensitive information.
- Investigate the identity following actions.

6.129 | Abnormal Allocation of compute resources in multiple regions

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
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) • Initial Access (TA0001)

ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Informational

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Variations

Abnormal Unusual allocation of compute resources in multiple regions

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Abnormal Suspicious allocation of compute resources in multiple regions

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Abnormal Allocation of compute resources in a high number of regions

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Abnormal Allocation of compute resources in multiple regions by an unusual identity

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity allocated an unusual compute resource pool, suspected as mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

6.130 | An identity dumped multiple secrets from a project

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	6 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) • Collection (TA0009)
ATT&CK Technique	• Unsecured Credentials (T1552) • Data from Cloud Storage (T1530)
Severity	Low

Description

An identity dumped multiple secrets from the project, considerably more than usual.
This may indicate an attacker's attempt to dump sensitive information from the cloud environment.

Attacker's Goals

Collect secrets from the cloud environment.

Investigative actions

- Check the accessed secrets' designation.
- Verify that the identity did not dump any sensitive information that it shouldn't.

Variations

An administrative identity dumped multiple secrets from a project

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Collection (TA0009)
ATT&CK Technique	• Unsecured Credentials (T1552) • Data from Cloud Storage (T1530)

Severity	Informational

Description

An identity dumped multiple secrets from the project, considerably more than usual.
This may indicate an attacker's attempt to dump sensitive information from the cloud environment.

Attacker's Goals

Collect secrets from the cloud environment.

Investigative actions

- Check the accessed secrets' designation.
- Verify that the identity did not dump any sensitive information that it shouldn't.

6.131 | Storage enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
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	• Discovery (TA0007) • Collection (TA0009)
ATT&CK Technique	• Cloud Storage Object Discovery (T1619) • Data from Cloud Storage (T1530) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity attempted to discover cloud objects within storage buckets.
This might be an attempt by an adversary to find sensitive data stored in cloud storage, which could lead to data theft.

Attacker's Goals

Access sensitive data stored in cloud infrastructure.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which storage buckets were enumerated and whether they contained sensitive information.

Variations

Storage enumeration activity by an identity with high administrative activity

Synopsis

ATT&CK Tactic	• Discovery (TA0007) • Collection (TA0009)

ATT&CK Technique	• Cloud Storage Object Discovery (T1619) • Data from Cloud Storage (T1530) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity with high administrative activity attempted to discover cloud objects within storage buckets.
This might be an attempt by an adversary to find sensitive data stored in cloud storage, which could lead to data theft.

Attacker's Goals

Access sensitive data stored in cloud infrastructure.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which storage buckets were enumerated and whether they contained sensitive information.

6.132 | Suspicious identity downloaded multiple objects from a bucket

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Low

Description

An identity downloaded multiple objects from a bucket, considerably more than usual.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

Variations

Suspicious identity with DevOps behavior downloaded multiple objects from a bucket

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Informational

Description

An identity with DevOps behavior downloaded multiple objects from a bucket, considerably more than usual.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

Suspicious identity downloaded multiple objects from a backup storage bucket

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Medium

Description

An identity downloaded multiple objects from a bucket, considerably more than usual.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

6.133 | Cloud user performed multiple actions that were denied

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
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	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Informational

Description

An Identity performed multiple actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute a verity of commands to explore the cloud environment.

Investigative actions

Check if the API calls were made by the identity.
Check if there are additional calls executed by the identity.

Variations

Cloud non-user identity performed multiple actions that were denied

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Low

Description

An Identity performed multiple actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute a verity of commands to explore the cloud environment.

Investigative actions

Check if the API calls were made by the identity.
Check if there are additional calls executed by the identity.

6.134 | Mailbox enumeration activity by Azure application

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

Microsoft Graph API was used to enumerate mailboxes in Azure tenant.

Attacker's Goals

To extract sensitive information stored in mailboxes.

Investigative actions

- Determine which mailboxes were enumerated and whether they contained any sensitive information.
- Investigate the identity following actions.

Variations

Mailbox enumeration activity by Azure user

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

Microsoft Graph API was used by a user to enumerate mailboxes.

Attacker's Goals

To extract sensitive information stored in mailboxes.

Investigative actions

- Determine which mailboxes were enumerated and whether they contained any sensitive information.
- Investigate the identity following actions.

6.135 | Kubernetes enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
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	Kubernetes - API
ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	• Container and Resource Discovery (T1613) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity attempted to discover available resources within a cluster.
This may indicate an adversary attempting to map the Kubernetes environment and discover resources that may assist to perform additional attacks within the environment.

Attacker's Goals

Map the cluster environment and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

Variations

Suspicious Kubernetes enumeration activity

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Container and Resource Discovery (T1613) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An identity attempted to discover available resources within a cluster.
This may indicate an adversary attempting to map the Kubernetes environment and discover resources that may assist to perform additional attacks within the environment.

Attacker's Goals

Map the cluster environment and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

6.136 | Allocation of multiple cloud compute resources

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Informational

Description

An identity allocated multiple compute resources.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Variations

Unusual allocation of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)

ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	High

Description

An identity allocated multiple compute resources.
This activity is highly unusual, such volume of compute allocation was not seen across all the projects during the past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Unusual allocation of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated multiple compute resources.
This activity is highly unusual, such volume of compute allocation was not seen at in this project during the past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Unusual allocation of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Medium

Description

An identity allocated multiple compute resources.
The allocated instances contains GPU accelerators, such pattern is related to a crypto mining activity.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Allocation of multiple cloud compute resources with accelerator gear

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity allocated multiple compute resources.
his activity is unusual for this identity in past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

Unusual allocation attempt of multiple cloud compute resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Resource Hijacking (T1496) • Valid Accounts (T1078)
Severity	Low

Description

An identity attempted to allocate multiple compute resources.
This activity is highly unusual, such volume of compute allocation was not seen at in this project during the past 30 days.

Attacker's Goals

Leverage cloud compute resources to earn virtual currency.

Investigative actions

- Check the identity created resources and its legitimacy.
- Look for any unusual behavior originated from the suspected identity, and check if they're compromised, e.g. Access key, Service account, etc.

6.137 | Multiple cloud snapshots export

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
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	Exfiltration (TA0010)
ATT&CK Technique	Transfer Data to Cloud Account (T1537)
Severity	Informational

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots locally.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Variations

Multiple cloud snapshots export

Synopsis

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

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots from an external IP address.
This action was unusual based on the cloud project history.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Multiple cloud snapshots export

Synopsis

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

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots from an external IP address.
This action was unusual based on the cloud identity history.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Multiple cloud snapshots export

Synopsis

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

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots locally.
This action was unusual based on the unsuccessful attempts rate.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

Multiple cloud snapshots export

Synopsis

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

Description

A cloud identity has downloaded multiple virtual machines or DB snapshots locally.
This action was unusual based on the cloud project or identity history.

Attacker's Goals

Exfiltrate sensitive data that resides on the disk.

Investigative actions

- Check if the identity intended to export the virtual machines or DB snapshots.
- Check if the identity performed additional operations in the cloud environment that might be malicious.

6.138 | Multiple failed logins from a single IP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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	Informational

Description

Multiple failed logins were observed in a short period of time from a single external IP.
The IP is not a known identity provider.

Attacker's Goals

Gain initial access to the cloud console.

Investigative actions

- Check if the IP is a known IP.
- Check if a successful login from the same IP occurred after the failed login attempts.

Variations

Multiple failed logins from an unknown IP

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)
Severity	Medium

Description

Multiple failed logins were observed in a short period of time from a single external IP.
The IP is not a known identity provider.
The IP is not a known IP in the organization.
This could indicate on an active brute force attempt.

Attacker's Goals

Gain initial access to the cloud console.

Investigative actions

- Check if the IP is a known IP.
- Check if a successful login from the same IP occurred after the failed login attempts.

6.139 | Azure high-volume data transfer

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

An Identity performed multiple Microsoft Graph actions, resulting in a high volume of data transfer.

Attacker's Goals

Exfiltrate data over Microsoft Graph API.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

Variations

Unusual Azure high-volume data transfer

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Medium

Description

An Identity performed multiple Microsoft Graph actions, resulting in a high volume of data transfer.

Attacker's Goals

Exfiltrate data over Microsoft Graph API.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

Suspicious Azure high-volume data transfer by identity

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Medium

Description

An Identity performed multiple Microsoft Graph actions, resulting in a high volume of data transfer.

Attacker's Goals

Exfiltrate data over Microsoft Graph API.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

Unusual high-volume data transfer from multiple Azure tenants

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)

Severity	Low

Description

An Identity performed multiple Microsoft Graph actions, resulting in a high volume of data transfer.

Attacker's Goals

Exfiltrate data over Microsoft Graph API.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

6.140 | Microsoft OneDrive enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

Microsoft Graph API was used to enumerate Microsoft OneDrive items.

Attacker's Goals

To extract sensitive information stored in Microsoft OneDrive.

Investigative actions

- Determine which OneDrive files were enumerated and whether they contained any sensitive information.
- Investigate the identity following actions.

6.141 | An identity performed a suspicious download of multiple cloud storage objects

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
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	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Informational

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

Variations

An identity performed a suspicious download of multiple cloud storage objects from an internal IP

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Informational

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

An identity performed a suspicious download of multiple cloud storage objects

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	High

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.
This large volume of downloaded cloud storage objects had not been seen across all projects for the last 30 days.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

An identity performed a suspicious download of multiple cloud storage objects

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Medium

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.
This large volume of downloaded cloud storage objects had not been seen in this project for the last 30 days.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

An identity performed a suspicious download of multiple cloud storage objects from multiple buckets

Synopsis

ATT&CK Tactic	• Collection (TA0009) • Exfiltration (TA0010)
ATT&CK Technique	• Data from Cloud Storage (T1530) • Automated Exfiltration (T1020)
Severity	Medium

Description

An identity downloaded multiple objects from cloud storage.
This may indicate an attacker's attempt to download sensitive data from a bucket in the cloud environment.
This large volume of downloaded cloud storage objects from several buckets had not been seen for the last 30 days.

Attacker's Goals

Exfiltrate sensitive data from the cloud environment.

Investigative actions

- Check the accessed bucket and objects designation.
- Verify that the identity did not download any sensitive information that it shouldn't.

6.142 | An Azure identity performed multiple actions that were

denied

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Informational

Description

An Identity performed multiple Microsoft Graph actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute various of commands to explore the cloud environment.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

Variations

An Azure application attempted multiple actions on resources that were denied

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Medium

Description

An Identity performed multiple Microsoft Graph actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute various of commands to explore the cloud environment.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

An Azure identity attempted multiple actions on resources that were denied

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Low

Description

An Identity performed multiple Microsoft Graph actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute various of commands to explore the cloud environment.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

An Azure application performed multiple actions that were denied

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) • Permission Groups Discovery (T1069)
Severity	Low

Description

An Identity performed multiple Microsoft Graph actions that were denied, which may indicate it is being misused.

Attacker's Goals

Execute various of commands to explore the cloud environment.

Investigative actions

Check the identity's role designation in the organization.
Check if there are additional calls executed by the identity.

6.143 | Deletion of multiple cloud resources

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
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) • Initial Access (TA0001)
ATT&CK Technique	• Data Destruction (T1485) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

An identity deleted multiple cloud resources.

Attacker's Goals

Leverage access to the cloud to delete resources and cause damage to an organization's infrastructure.

Investigative actions

- Confirm the legitimacy of the suspected identity and what cloud resources have been deleted by the identity.
- Look for any unusual activity associated with the suspected identity and determine whether they are compromised.

Variations

Deletion of multiple cloud resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Data Destruction (T1485) • Valid Accounts: Cloud Accounts (T1078.004)

Severity	Medium

Description

An identity deleted multiple cloud resources.
This large volume of deleted cloud resources had not been seen across all projects for the last 30 days.

Attacker's Goals

Leverage access to the cloud to delete resources and cause damage to an organization's infrastructure.

Investigative actions

- Confirm the legitimacy of the suspected identity and what cloud resources have been deleted by the identity.
- Look for any unusual activity associated with the suspected identity and determine whether they are compromised.

Deletion of multiple cloud resources

Synopsis

ATT&CK Tactic	• Impact (TA0040) • Initial Access (TA0001)
ATT&CK Technique	• Data Destruction (T1485) • Valid Accounts: Cloud Accounts (T1078.004)
Severity	Low

Description

An identity deleted multiple cloud resources.
This large volume of deleted cloud resources had not been seen in this project for the last 30 days.

Attacker's Goals

Leverage access to the cloud to delete resources and cause damage to an organization's infrastructure.

Investigative actions

- Confirm the legitimacy of the suspected identity and what cloud resources have been deleted by the identity.
- Look for any unusual activity associated with the suspected identity and determine whether they are compromised.

6.144 | Microsoft SharePoint enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

The Microsoft Graph API was used to enumerate Microsoft SharePoint sites in an Azure tenant.

Attacker's Goals

To extract sensitive information stored in Microsoft SharePoint.

Investigative actions

- Determine which SharePoint sites were enumerated and whether they contained any sensitive information.
- Investigate the identity following actions.

6.145 | Azure enumeration activity using Microsoft Graph API

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	5 Days
Required Data	• Requires: ◦ Azure Audit Log

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)
Severity	Informational

Description

The Microsoft Graph API was used to enumerate an Azure tenant.

Attacker's Goals

Map the Azure tenant and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

Variations

Azure sensitive resources enumeration activity using Microsoft Graph API

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Cloud Service Discovery (T1526)

Severity	Informational

Description

Microsoft Graph API was used to enumerate sensitive resources in Azure tenant.

Attacker's Goals

Map the Azure tenant and detect potential resources to abuse.

Investigative actions

- Check the identity's role designation in the organization.
- Identify which available resources were discovered.
- Investigate if the discovered resources were used to extract sensitive information or perform other attacks in the cloud environment.

6.146 | Multi region enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
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	• Discovery (TA0007) • Defense Evasion (TA0005)
ATT&CK Technique	• Cloud Infrastructure Discovery (T1580) • Unused/Unsupported Cloud Regions (T1535) • Cloud Service Discovery (T1526)
Severity	Informational

Description

An internal identity performed an operation on multiple regions, considerably more than usual. This may indicate an attacker's attempt to identify all available resources in the cloud environment.

Attacker's Goals

- Discover cloud resources that are available within the environment and leverage them to perform additional attacks against the organization.
- Detect unused geographic regions and leverage them to evade detection of malicious operations.

Investigative actions

- Check the identity designation.
- Verify that the identity did not perform any operation in a region that it shouldn't.

7 | Azure Flow Log

7.1 | Possible DCShadow attempt

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 Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls OR ◦ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Defense Evasion (TA0005)

ATT&CK Technique	• OS Credential Dumping (T1003) • Rogue Domain Controller (T1207)
Severity	High

Description

Attackers may register a compromised host as a new DC to get other DCs to replicate data to it, and then push their malicious AD changes to all DCs.

Attacker's Goals

Retrieve Active Directory data, to later be able to push out malicious Active Directory changes.

Investigative actions

Check whether the destination is a new domain controller or a host that syncs with ADFS or Azure AD.

7.2 | Unusual SSH activity that resembles SSH proxy

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 Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls • Requires one of the following data sources: ◦ Palo Alto Networks Platform Logs OR ◦ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Informational

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Variations

High Volume Unusual SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Suspicious SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Unusual SSH activity that resembles SSH proxy detected

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

7.3 | An internal Cloud resource performed port scan on external networks

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	5 Days

Required Data	• Requires one of the following data sources: ◦ AWS Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	• Discovery (TA0007) • Impact (TA0040)
ATT&CK Technique	• Network Service Discovery (T1046) • Resource Hijacking (T1496) • Cloud Service Discovery (T1526)
Severity	Medium

Description

An internal cloud resource attempted to connect to the same destination port of multiple external IP addresses.
This may be a result of the cloud resource being hijacked by an attacker.
Attackers perform port scans on a specific destination port for reconnaissance purposes, to detect known vulnerable services that accept connections in the specific port, and perform targeted attacks against them.

Attacker's Goals

Detect vulnerable services, which listen on known ports and are opened to the Internet.

Investigative actions

- Check if similar activity was performed on additional cloud resources.
- Check if similar activity was performed against additional ports and external ip addresses from the same cloud resource.
- Check which process triggered the port scanning activity and for what purpose.

7.4 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AWS Flow Log OR ◦ AWS OCSF Flow Logs OR ◦ Azure Flow Log OR ◦ Gcp Flow Log OR ◦ Palo Alto Networks Platform Logs OR ◦ Third-Party Firewalls • Requires one of the following data sources: ◦ Palo Alto Networks Platform Logs OR ◦ XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Variations

SSH brute force network detected from external source

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Rare SSH brute force attempt

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

8 | Azure SignIn Log

8.1 | Suspicious SSO access from ASN

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Google Workspace Authentication OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A suspicious SSO authentication was made by a user.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Variations

Google Workspace - Suspicious SSO access from ASN

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A suspicious SSO authentication was made by a user.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

8.2 | SSO with abnormal user agent

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: ◦ Okta OR ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A user successfully authenticated via SSO with an abnormal user agent.

Attacker's Goals

Use a legitimate user and authenticate via an SSO service to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has really moved to a new user agent app).
- Follow actions and suspicious activities regarding the user.

Variations

SSO with an offensive user agent

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Low

Description

A user successfully authenticated via SSO with an offensive user agent.

Attacker's Goals

Use a legitimate user and authenticate via an SSO service to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has really moved to a new user agent app).
- Follow actions and suspicious activities regarding the user.

8.3 | A user connected from a new country

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	30 Days
Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics

Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

A user connected from an unusual country that the user has not connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

Variations

A user connected from a new country using an anonymized proxy

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)

Severity	Low

Description

A user connected from an unusual country that the user has not connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

8.4 | First SSO access from ASN in organization

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Google Workspace Authentication OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

An SSO authentication was made with a new ASN.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the provider or location is allowed or a new user).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Variations

First successful SSO access from ASN in the organization

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Low

Description

An SSO authentication was made with a new ASN.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the provider or location is allowed or a new user).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Google Workspace - First SSO access from ASN in organization

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

An SSO authentication was made with a new ASN.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the provider or location is allowed or a new user).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

8.5 | SSO authentication by a machine account

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Low

Description

A machine account successfully authenticated via SSO.

Attacker's Goals

Use an account that has access to resources to move laterally in the network and access privileged resources.

Investigative actions

- Check whether the account has done any administrative actions it should not usually do.
- Look for more logins and authentications by the account throughout the network.

8.6 | First SSO access from ASN for user

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Google Workspace Authentication OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)

Severity	Informational

Description

A user successfully authenticated via SSO with a new ASN.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Variations

First SSO access from ASN for user using an anonymized proxy

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Low

Description

A user successfully authenticated via SSO with a new ASN. using an anonymized proxy.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Google Workspace - First SSO access from ASN for user

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A user successfully authenticated via SSO with a new ASN.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

8.7 | A user logged in at an unusual time via SSO

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Google Workspace Authentication OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user connected via SSO on a day and hour that is unusual for this user. This may indicate that the account was compromised.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Check the login of the user.
- Check further actions done by the account (e.g. creating files in suspicious locations, creating users, elevating permissions, etc.).
- Check if the user accessing remote resources or connecting to other services.
- Check if the user is logging in from an unusual time zone while traveling.
- Check if the user usually logs in from this country.

Variations

Google Workspace - A user logged in at an unusual time via SSO

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user connected via SSO on a day and hour that is unusual for this user. This may indicate that the account was compromised.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Check the login of the user.
- Check further actions done by the account (e.g. creating files in suspicious locations, creating users, elevating permissions, etc.).
- Check if the user accessing remote resources or connecting to other services.
- Check if the user is logging in from an unusual time zone while traveling.
- Check if the user usually logs in from this country.

8.8 | User attempted to connect from a suspicious country

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	30 Days
Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics

Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

A user connected from an unusual country. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

Variations

User successfully connected from a suspicious country

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)

Severity	Low

Description

A user successfully connected from an unusual country. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

8.9 | First connection from a country in organization

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

A user connected to an SSO service from an unusual country that no one from this organization has connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

Variations

First successful SSO connection from a country in organization

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

A user successfully connected from an unusual country that no one from this organization has connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

8.10 | SSO authentication by a service account

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Low

Description

A service account successfully authenticated via SSO.

Attacker's Goals

Use an account that has access to resources to move laterally in the network and access privileged resources.

Investigative actions

- Check whether the account has done any administrative actions it should not usually do.
- Look for more logins and authentications by the account throughout the network.

Variations

Rare non-interactive SSO authentication by a service account

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A service account successfully authenticated via SSO.

Attacker's Goals

Use an account that has access to resources to move laterally in the network and access privileged resources.

Investigative actions

- Check whether the account has done any administrative actions it should not usually do.
- Look for more logins and authentications by the account throughout the network.

First time SSO authentication by a service account

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)

Severity	Medium

Description

A service account successfully authenticated via SSO.

Attacker's Goals

Use an account that has access to resources to move laterally in the network and access privileged resources.

Investigative actions

- Check whether the account has done any administrative actions it should not usually do.
- Look for more logins and authentications by the account throughout the network.

8.11 | A disabled user attempted to authenticate via SSO

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A disabled user attempted to authenticate via SSO.

Attacker's Goals

Use an account that was possibly compromised in the past to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user returned from a long leave of absence).
- Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

8.12 | First SSO Resource Access in the Organization

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: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Discovery (TA0007)
ATT&CK Technique	• Valid Accounts: Domain Accounts (T1078.002) • Cloud Service Discovery (T1526)

Severity	Informational

Description

A resource was accessed for the first time via SSO.

Attacker's Goals

Use a possibly compromised account to access privileged resources.

Investigative actions

- Confirm that the activity is benign (e.g. this is a newly approved resource).
- Follow further actions done by the user that attempted to access the resource.

Variations

Abnormal first access to a resource via SSO in the organization

Synopsis

ATT&CK Tactic	• Initial Access (TA0001) • Discovery (TA0007)
ATT&CK Technique	• Valid Accounts: Domain Accounts (T1078.002) • Cloud Service Discovery (T1526)
Severity	Low

Description

A resource was accessed for the first time via SSO with suspicious characteristics.

Attacker's Goals

Use a possibly compromised account to access privileged resources.

Investigative actions

- Confirm that the activity is benign (e.g. this is a newly approved resource).
- Follow further actions done by the user that attempted to access the resource.

8.13 | SSO with new operating system

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: ◦ Okta OR ◦ Azure SignIn Log OR ◦ AzureAD OR ◦ Duo
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)

Severity	Informational

Description

A user successfully authenticated via SSO with a new operating system.

Attacker's Goals

Use a legitimate user and authenticate via an SSO service to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has really moved to a new operating system).
- Follow actions and suspicious activities regarding the user.

8.14 | A successful SSO sign-in from TOR

Synopsis

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

Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Command and Control (TA0011)
ATT&CK Technique	• Proxy: Multi-hop Proxy (T1090.003) • Valid Accounts (T1078)
Severity	High

Description

A successful sign-in from a TOR exit node.

Attacker's Goals

Gain initial access to organization and hiding itself.

Investigative actions

- Block all web traffic to and from public Tor entry and exit nodes.
- Search for additional logins from the same user around the alert timestamp.

Variations

A successful SSO sign-in from TOR via Mobile Device

Synopsis

ATT&CK Tactic	• Initial Access (TA0001) • Command and Control (TA0011)
ATT&CK Technique	• Proxy: Multi-hop Proxy (T1090.003) • Valid Accounts (T1078)
Severity	Medium

Description

A successful sign-in from a TOR exit node.

Attacker's Goals

Gain initial access to organization and hiding itself.

Investigative actions

- Block all web traffic to and from public Tor entry and exit nodes.
- Search for additional logins from the same user around the alert timestamp.

8.15 | A user accessed multiple unusual resources via SSO

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	1 Hour
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Discovery (TA0007) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Cloud Service Dashboard (T1538) • Cloud Service Discovery (T1526)
Severity	Informational

Description

A user accessed multiple resources via SSO that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual resources may be accessed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

Investigate the resources that were accessed to determine if they were used for legitimate purposes or malicious activity.

Variations

A user accessed multiple resources via SSO using an anonymized proxy

Synopsis

ATT&CK Tactic	• Discovery (TA0007) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Cloud Service Dashboard (T1538) • Cloud Service Discovery (T1526)
Severity	Medium

Description

A user accessed multiple resources via SSO, using an anonymized proxy, that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual resources may be accessed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

Investigate the resources that were accessed to determine if they were used for legitimate purposes or malicious activity.

Suspicious user access to multiple resources via SSO

Synopsis

ATT&CK Tactic	• Discovery (TA0007) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Cloud Service Dashboard (T1538) • Cloud Service Discovery (T1526)
Severity	Low

Description

A user accessed multiple resources via SSO that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual resources may be accessed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

Investigate the resources that were accessed to determine if they were used for legitimate purposes or malicious activity.

8.16 | SSO Brute Force

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	1 Hour
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Brute Force (T1110) • Brute Force: Password Guessing (T1110.001) • Compromise Accounts (T1586)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a brute-force attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Check the legitimacy of this activity and determine whether it is malicious or not.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

Variations

SSO Brute Force Threat Detected

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Brute Force (T1110) • Brute Force: Password Guessing (T1110.001) • Compromise Accounts (T1586)
Severity	Medium

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a brute-force attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Check the legitimacy of this activity and determine whether it is malicious or not.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

SSO Brute Force Activity Observed

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Brute Force (T1110) • Brute Force: Password Guessing (T1110.001) • Compromise Accounts (T1586)
Severity	Low

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a brute-force attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Check the legitimacy of this activity and determine whether it is malicious or not.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

8.17 | Impossible traveler - SSO

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	6 Hours
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Low

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.

This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

Variations

Impossible traveler - non-interactive SSO authentication

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

Possible Impossible traveler via SSO

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

SSO impossible traveler from a VPN or proxy

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Compromise Accounts (T1586) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

8.18 | SSO Password Spray

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Hour

Required Data	• Requires one of the following data sources: ◦ AzureAD OR ◦ Azure SignIn Log OR ◦ Duo OR ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001) • Compromise Accounts (T1586)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a login password spray attack.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

- See whether this was a legitimate action.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

Variations

SSO Password Spray Threat Detected

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Resource Development (TA0042)
ATT&CK Technique	• Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001) • Compromise Accounts (T1586)
Severity	Medium

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a login password spray attack.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

- See whether this was a legitimate action.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

SSO Password Spray Activity Observed