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	Low

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.

8.19 | Intense SSO failures

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	10 Minutes
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) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

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 whether a successful login was made after unsuccessful attempts.

Variations

Intense SSO failures with suspicious characteristics

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001)
Severity	Low

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

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 whether a successful login was made after unsuccessful attempts.

9 | AzureAD

9.1 | 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.

9.2 | 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.

9.3 | SSO authentication attempt by a honey user

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 ◦ Okta OR ◦ OneLogin OR ◦ PingOne
Detection Modules	Identity Analytics
Detector Tags	Honey User Analytics

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

Description

An SSO authentication attempt was made by a honey user, a decoy account created specifically to detect unauthorized access. This may indicate potential attacker activity.

Attacker's Goals

An attacker is attempting to gain unauthorized access by exploiting valid or stolen credentials.

Investigative actions

- Confirm that the alert was triggered by a honey user account.
- Check for other login attempts on different accounts from the same source IP.
- Analyze any subsequent actions performed by the user after the login attempt.
- Follow further actions performed by the user.

Variations

Abnormal SSO authentication by a honey user

Synopsis

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

Description

An SSO authentication attempt was made by a honey user, a decoy account created specifically to detect unauthorized access. This may indicate potential attacker activity.

Attacker's Goals

An attacker is attempting to gain unauthorized access by exploiting valid or stolen credentials.

Investigative actions

- Confirm that the alert was triggered by a honey user account.
- Check for other login attempts on different accounts from the same source IP.
- Analyze any subsequent actions performed by the user after the login attempt.
- Follow further actions performed by the user.

9.4 | Suspicious authentication with Azure Password Hash Sync user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD
Detection Modules	Identity Analytics

Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Defense Evasion (TA0005)
ATT&CK Technique	• Valid Accounts (T1078) • Modify Authentication Process: Hybrid Identity (T1556.007)
Severity	Medium

Description

Authentication to an unusual authentication target was performed by the Azure AD Password Hash Sync user.

Attacker's Goals

- The attacker may be attempting to exploit a PHS user, the attacker wants to escalate and abuse this user, to get access to all the user's hashes.

Investigative actions

- Follow further actions done by the account.

9.5 | 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.

9.6 | 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.

9.7 | 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.

9.8 | 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.

9.9 | 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.

9.10 | 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.

9.11 | 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.

9.12 | 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.

9.13 | 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.

9.14 | 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.

9.15 | 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.

9.16 | 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.

9.17 | SSO with abnormal 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: ◦ AzureAD OR ◦ Okta
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 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.

9.18 | Suspicious Azure AD interactive sign-in using PowerShell

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)

Severity	Informational

Description

A user interactively logged in to Azure AD via PowerShell.

Attacker's Goals

The attacker attempts to gain access to the organization's resources.

Investigative actions

- Analyze the actions taken by the user during the session and verify that this is a legitimate session.
- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

Variations

Unusual Azure AD interactive sign-in using PowerShell

Synopsis

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

Description

A user interactively logged in to Azure AD via PowerShell from an unusual geolocation or ASN.

Attacker's Goals

The attacker attempts to gain access to the organization's resources.

Investigative actions

- Analyze the actions taken by the user during the session and verify that this is a legitimate session.
- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

9.19 | 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.

9.20 | 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.

9.21 | 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.

9.22 | 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

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	Low

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.

9.23 | Intense SSO failures

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	10 Minutes
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) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

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 whether a successful login was made after unsuccessful attempts.

Variations

Intense SSO failures with suspicious characteristics

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001)
Severity	Low

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

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 whether a successful login was made after unsuccessful attempts.

10 | AzureAD Audit Log

10.1 | Authentication method added to an Azure account

Synopsis

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

Description

An identity attempted to add an Azure authentication method.

Attacker's Goals

- An attacker can add an authentication method to an account, so they can have later access to the tenant and resources.

Investigative actions

- Check if the authentication method is legitimate in the organization.
- Check whether the identity is permitted to perform such actions.
- Follow the account for possible suspicious or unusual logins.

Variations

Suspicious authentication method addition to Azure account

Synopsis

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

Description

An identity added an Azure authentication method.

Attacker's Goals

- An attacker can add an authentication method to an account, so they can have later access to the tenant and resources.

Investigative actions

- Check if the authentication method is legitimate in the organization.
- Check whether the identity is permitted to perform such actions.
- Follow the account for possible suspicious or unusual logins.

10.2 | MFA was disabled for an Azure identity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	• Credential Access (TA0006) • Defense Evasion (TA0005) • Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Low

Description

MFA was disabled for the user.

Attacker's Goals

This allows the attacker to connect using this account without the need for the additional layer of authentication.

Investigative actions

- Follow further actions by the initiator.
- Check the login activity from this account.
- Follow further actions done by this account.

Variations

MFA was disabled for an Azure identity from a new country

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Defense Evasion (TA0005) • Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Medium

Description

MFA was disabled for the user from a new country.

Attacker's Goals

This allows the attacker to connect using this account without the need for the additional layer of authentication.

Investigative actions

- Follow further actions by the initiator.
- Check the login activity from this account.
- Follow further actions done by this account.

MFA was disabled for an Azure identity regularly by the user

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Defense Evasion (TA0005) • Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Informational

Description

MFA was disabled for the user.

Attacker's Goals

This allows the attacker to connect using this account without the need for the additional layer of authentication.

Investigative actions

- Follow further actions by the initiator.
- Check the login activity from this account.
- Follow further actions done by this account.

10.3 | Device Registration Policy modification

Synopsis

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

Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Informational

Description

An identity changed the Device Registration policy.

Attacker's Goals

- An attacker attempts to change Active Directory configuration for persistence or defense evasion.
- With a modified Device Registration policy, an attacker might be able to access the tenant without possible blockage for later access.

Investigative actions

- Check what policy has been changed.
- Check whether the user changing the configuration is permitted to perform such actions.

Variations

A user modified the Device Registration Policy for the first time

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Low

Description

An identity changed the Device Registration policy.

Attacker's Goals

- An attacker attempts to change Active Directory configuration for persistence or defense evasion.
- With a modified Device Registration policy, an attacker might be able to access the tenant without possible blockage for later access.

Investigative actions

- Check what policy has been changed.
- Check whether the user changing the configuration is permitted to perform such actions.

10.4 | Azure application credentials added

Synopsis

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

Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
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 identity added credentials to an Azure application.

Attacker's Goals

- An attacker may add certificates or modify authentication methods of an application to authenticate as the application.

Investigative actions

- Check if the modified application is new to the organization.
- Check whether the account that modified the credentials is supposed to perform such actions.
- Check for possible logins from the application modified.
- Follow further actions done by the application.

Variations

Suspicious credential operation on an Azure application

Synopsis

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

Description

An identity added a certificate to an Azure application in a suspicious way.

Attacker's Goals

- An attacker may add certificates or modify authentication methods of an application to authenticate as the application.

Investigative actions

- Check if the modified application is new to the organization.
- Check whether the account that modified the credentials is supposed to perform such actions.
- Check for possible logins from the application modified.
- Follow further actions done by the application.

Unusual certificate operation on an Azure application

Synopsis

ATT&CK Tactic	• Defense Evasion (TA0005) • Persistence (TA0003)

ATT&CK Technique	• Account Manipulation (T1098) • Use Alternate Authentication Material (T1550)
Severity	Low

Description

An identity added a certificate to an Azure application with some unusual parameters.

Attacker's Goals

- An attacker may add certificates or modify authentication methods of an application to authenticate as the application.

Investigative actions

- Check if the modified application is new to the organization.
- Check whether the account that modified the credentials is supposed to perform such actions.
- Check for possible logins from the application modified.
- Follow further actions done by the application.

10.5 | Azure AD PIM alert disabled

Synopsis

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

Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Medium

Description

An identity disabled an Azure AD PIM alert.

Attacker's Goals

- An attacker might want to disable alerts associated with authentication requirements for privileged access.
- This may allow malicious activities to go unnoticed.

Investigative actions

- Check what alert was disabled.
- Check whether the user that disabled the alert is permitted to perform such actions.

10.6 | BitLocker key retrieval

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Informational

Description

An identity retrieved a BitLocker Key.

Attacker's Goals

- BitLocker keys are used for mitigating unauthorized data access on lost or stolen computers by encrypting all user files and system files on the operating system drive.
- An attacker that retrieves this key, can potentially access the data that should be encrypted.

Investigative actions

- Check what key was retrieved.
- Check for a possible compromised device.
- Check whether the user is permitted to perform such actions.

10.7 | Identity assigned an Azure AD Administrator Role

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Cloud Roles (T1098.003)
Severity	Informational

Description

An identity was assigned an Azure AD Administrator role.

Attacker's Goals

- An attacker may add additional roles or permissions to an attacker controlled cloud account to maintain persistent access to a tenant.

Investigative actions

- Check if the added account is new to the organization.
- Check whether the account that added the account to the role is permitted to perform such actions.
- Check what can be affected by the assigned role
- Follow further actions done by the account that was added to the role.

Variations

Identity assigned an Azure AD Administrator Role by an Application

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Cloud Roles (T1098.003)
Severity	Medium

Description

An identity was assigned an Azure AD Administrator role by an application.

Attacker's Goals

- An attacker may add additional roles or permissions to an attacker controlled cloud account to maintain persistent access to a tenant.

Investigative actions

- Check if the added account is new to the organization.
- Check whether the account that added the account to the role is permitted to perform such actions.
- Check what can be affected by the assigned role
- Follow further actions done by the account that was added to the role.

Suspicious Azure AD Administrator Role assignment

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Cloud Roles (T1098.003)
Severity	Low

Description

An identity was assigned an Azure AD Administrator role.

Attacker's Goals

- An attacker may add additional roles or permissions to an attacker controlled cloud account to maintain persistent access to a tenant.

Investigative actions

- Check if the added account is new to the organization.
- Check whether the account that added the account to the role is permitted to perform such actions.
- Check what can be affected by the assigned role
- Follow further actions done by the account that was added to the role.

10.8 | Azure account deletion by a non-standard account

Synopsis

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

Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Low

Description

An Azure AD account deletion was performed by a user that doesn't typically delete users.

Attacker's Goals

Interrupt availability and access to Azure by deleting access accounts.

Investigative actions

- Follow further actions by the initiator.
- Check what services, groups and applications are affected by the deleted user being removed.
- Check if the deleted user had a privileged role.

Variations

Azure account deletion by a non-standard account with high administrative activity

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

An Azure AD account deletion was performed by an identity with high administrative activity that doesn't typically delete users.

Attacker's Goals

Interrupt availability and access to Azure by deleting access accounts.

Investigative actions

- Follow further actions by the initiator.
- Check what services, groups and applications are affected by the deleted user being removed.
- Check if the deleted user had a privileged role.

A suspicious Azure account deletion by a non-standard account

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Medium

Description

An Azure AD account deletion was performed by a user that doesn't typically delete users in a suspicious manner.

Attacker's Goals

Interrupt availability and access to Azure by deleting access accounts.

Investigative actions

- Follow further actions by the initiator.
- Check what services, groups and applications are affected by the deleted user being removed.
- Check if the deleted user had a privileged role.

10.9 | Successful unusual guest user invitation

Synopsis

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

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

Description

An identity successfully invited a guest user to the tenant with unusual characteristics.

Attacker's Goals

An attacker can invite users to for evasion.

Investigative actions

- Check who is the invited guest user.
- Check whether the inviter is permitted to perform such actions.
- Check if the domain of the invited guest is allowed for invitations in the organization.

Variations

Rare successful guest invitation in the organization

Synopsis

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

Description

An identity successfully invited a suspicious guest user to the tenant.

Attacker's Goals

An attacker can invite users to for evasion.

Investigative actions

- Check who is the invited guest user.
- Check whether the inviter is permitted to perform such actions.
- Check if the domain of the invited guest is allowed for invitations in the organization.

10.10 | Azure AD PIM role settings change

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	• Defense Evasion (TA0005) • Privilege Escalation (TA0004)

ATT&CK Technique	• Abuse Elevation Control Mechanism (T1548) • Valid Accounts (T1078)
Severity	Low

Description

An identity changed the PIM role settings.

Attacker's Goals

- An attacker can modify the PIM role settings to make it easier to acquire a privileged account.

Investigative actions

- Check what role settings have been updated.
- Check whether the user changing the settings is permitted to perform such actions.

10.11 | Azure account creation by a non-standard account

Synopsis

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

Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	• Account Manipulation (T1098) • Create Account (T1136)
Severity	Informational

Description

An Azure AD account creation was performed by a user that doesn't typically create users.

Attacker's Goals

Create a backdoor account for later access to Azure AD or Azure resources, or delete evidence of such an account.

Investigative actions

- Follow further actions by the initiator.
- Check for new resource creations by the new user.
- Check if the new user was added to a privileged role.
- Follow further actions done by the new user.

Variations

Unusual Azure account creation by a non-standard account

Synopsis

ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	• Account Manipulation (T1098) • Create Account (T1136)
Severity	Low

Description

An Azure AD account creation was performed by a user that doesn't typically create users.

Attacker's Goals

Create a backdoor account for later access to Azure AD or Azure resources, or delete evidence of such an account.

Investigative actions

- Follow further actions by the initiator.
- Check for new resource creations by the new user.
- Check if the new user was added to a privileged role.
- Follow further actions done by the new user.

10.12 | Azure domain federation settings modification attempt

Synopsis

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

Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	• Persistence (TA0003) • Privilege Escalation (TA0004)
ATT&CK Technique	• Account Manipulation: Additional Cloud Credentials (T1098.001) • Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

A user or application attempted to modify the federation settings of the domain.

Attacker's Goals

An attacker attempts to change Active Directory configuration for persistence or defense evasion.

Investigative actions

- Check what configuration has been changed.
- Check whether the user changing the configuration is permitted.

Variations

A successful Azure domain federation settings modification

Synopsis

ATT&CK Tactic	• Persistence (TA0003) • Privilege Escalation (TA0004)
ATT&CK Technique	• Account Manipulation: Additional Cloud Credentials (T1098.001) • Domain or Tenant Policy Modification (T1484)
Severity	Medium

Description

A user or application successfully modified the federation settings of the domain.

Attacker's Goals

An attacker attempts to change Active Directory configuration for persistence or defense evasion.

Investigative actions

- Check what configuration has been changed.
- Check whether the user changing the configuration is permitted.

10.13 | Azure AD PIM elevation request

Synopsis

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

Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An Azure AD PIM elevation request was denied/approved.

Attacker's Goals

Getting elevated permissions to perform malicious actions.

Investigative actions

- Check if the elevation is authorized.
- Follow further actions or suspicious logins from the elevated account.

10.14 | Conditional Access policy removed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Low

Description

An identity removed a Conditional Access policy.

Attacker's Goals

- An attacker attempts to change Active Directory configuration for persistence or defense evasion.
- Without a Conditional Access policy, an attacker would be able to access the tenant without possible blockage for later access.

Investigative actions

- Check implications of the policy being removed.
- Check whether the user changing the configuration is permitted to perform such actions.

10.15 | First Azure AD PowerShell operation for a user

Synopsis

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

Severity	Low

Description

A user performed an Azure AD operation using a PowerShell user-agent for the first time.

Attacker's Goals

Achieve initial access to a company's resources.

Investigative actions

- Follow the actions the user performed using PowerShell.
- Confirm with the user that the action was intended.

10.16 | Azure application consent

Synopsis

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

Detector Tags	
ATT&CK Tactic	• Initial Access (TA0001) • Credential Access (TA0006)
ATT&CK Technique	• Phishing (T1566) • Phishing: Spearphishing Link (T1566.002) • Steal Application Access Token (T1528) • Trusted Relationship (T1199)
Severity	Informational

Description

An identity consented permissions to an application.

Attacker's Goals

Get access to credentials, data or an organization via applications with sufficient permissions.

Investigative actions

- Follow further actions by the consenting user.
- Check for new resource creations by the new user.
- Check how the consenting user got to the application.
- Verify the application creators.
- Check what permissions the application requested.
- Check for possible phishing in the organization.

Variations

First seen Azure admin consent to an application

Synopsis

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

ATT&CK Technique	• Phishing (T1566) • Phishing: Spearphishing Link (T1566.002) • Steal Application Access Token (T1528) • Trusted Relationship (T1199)
Severity	Low

Description

An administrative identity consented permissions to an application.

Attacker's Goals

Get access to credentials, data or an organization via applications with sufficient permissions.

Investigative actions

- Follow further actions by the consenting user.
- Check for new resource creations by the new user.
- Check how the consenting user got to the application.
- Verify the application creators.
- Check what permissions the application requested.
- Check for possible phishing in the organization.

10.17 | Unusual Conditional Access operation for an identity

Synopsis

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

Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Informational

Description

An identity attempted to add or update an Azure AD Conditional Access policy.

Attacker's Goals

- An attacker attempts to change Active Directory configuration for persistence or defense evasion.
- With a modified Conditional Access policy, an attacker might be able to access the tenant without possible blockage for later access.

Investigative actions

- Check implications of the updated policy.
- Check whether the user changing the configuration is permitted to perform such actions.

Variations

Suspicious Conditional Access operation for an identity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Low

Description

An identity that doesn't usually modify Azure AD Conditional Access policies successfully modified a policy.

Attacker's Goals

- An attacker attempts to change Active Directory configuration for persistence or defense evasion.
- With a modified Conditional Access policy, an attacker might be able to access the tenant without possible blockage for later access.

Investigative actions

- Check implications of the updated policy.
- Check whether the user changing the configuration is permitted to perform such actions.

10.18 | Owner added to Azure application

Synopsis

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

Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal Application Access Token (T1528)
Severity	Informational

Description

An identity was added as an owner to an Azure application.

Attacker's Goals

- An attacker may add owners to an application to authenticate as the application later on and access resources.

Investigative actions

- Check if the added account is new to the organization.
- Check whether the account that added the new owner is supposed to perform such actions.
- Check for possible logins from the application modified.
- Follow further actions done by the application.

10.19 | Azure service principal assigned app role

Synopsis

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

Description

An identity assigned an app role (permissions) to a service principal.

Attacker's Goals

- An attacker may add roles to service principals that will allow them to access sensitive information and perform other actions.

Investigative actions

- Check if the added service principle is new to the organization.
- Check whether the account that added the app role is supposed to perform such actions.
- Check for possible logins and actions from the service principle with the role.
- Follow further actions done by the application and the assigner.

10.20 | Azure application URI modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
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 identity added or updated an Azure application's URI.

Attacker's Goals

- An attacker may add certificates or modify authentication methods of an application to authenticate as the application.

Investigative actions

- Check whether the account that modified the URI is supposed to perform such actions.
- Check for possible logins from the application modified.
- Check for possible account consents or credential changes regarding the application.
- Follow further actions done by the application.

Variations

Suspicious Azure application URI modification

Synopsis

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

Description

An identity added or updated an Azure application's URI.

Attacker's Goals

- An attacker may add certificates or modify authentication methods of an application to authenticate as the application.

Investigative actions

- Check whether the account that modified the URI is supposed to perform such actions.
- Check for possible logins from the application modified.
- Check for possible account consents or credential changes regarding the application.
- Follow further actions done by the application.

10.21 | Azure Temporary Access Pass (TAP) registered to an account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	• Defense Evasion (TA0005) • Privilege Escalation (TA0004)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An identity registered an Azure Temporary Access Pass (TAP) to an account.

Attacker's Goals

- A TAP can allow setting of other authentication methods and can be used as an initial replacement of a multifactor authentication.

Investigative actions

- Check if the account that got the TAP should get it.
- Check whether the account that registered the TAP is supposed to perform such actions.
- Check if the TAP was registered to a privileged account.
- Follow further actions done by the initiator and the account with the TAP.

Variations

Abnormal Azure Temporary Access Pass (TAP) account registration

Synopsis

ATT&CK Tactic	• Defense Evasion (TA0005) • Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

An identity registered an Azure Temporary Access Pass (TAP) to an account.

Attacker's Goals

- A TAP can allow setting of other authentication methods and can be used as an initial replacement of a multifactor authentication.

Investigative actions

- Check if the account that got the TAP should get it.
- Check whether the account that registered the TAP is supposed to perform such actions.
- Check if the TAP was registered to a privileged account.
- Follow further actions done by the initiator and the account with the TAP.

10.22 | Unverified domain added to Azure AD

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

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

Description

A new unverified domain was added to Azure AD.

Attacker's Goals

An attacker attempts to change Active Directory configuration for persistence or defense evasion.

Investigative actions

- Check if the new domain is known for the organization.
- Check whether the user changing the configuration is permitted.
- Monitor network activity to and from the added domain.

Variations

Rare unverified domain addition to Azure AD

Synopsis

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

Description

A new unverified domain was added to Azure AD.

Attacker's Goals

An attacker attempts to change Active Directory configuration for persistence or defense evasion.

Investigative actions

- Check if the new domain is known for the organization.
- Check whether the user changing the configuration is permitted.
- Monitor network activity to and from the added domain.

10.23 | Azure AD account unlock/password reset attempt

Synopsis

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

Description

An identity attempted to unlock their account or reset their Azure AD password.

Attacker's Goals

- An attacker may switch a valid account's password for persistence.

Investigative actions

- Check if the password reset is authorized.
- Check whether the user who reset the password is permitted to perform such actions.
- Check if the account is in the password reset group or is acting out of scope.
- Check whether the user has not completed the password reset, and cancelled before successfully passing authentication methods.
- Follow further actions or suspicious logins from the account.

Variations

Azure AD account unlock/successful password reset

Synopsis

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

Description

An identity successfully reset or changed Azure AD password.

Attacker's Goals

- An attacker may switch a valid account's password for persistence.

Investigative actions

- Check if the password reset is authorized.
- Check whether the user who reset the password is permitted to perform such actions.
- Check if the account is in the password reset group or is acting out of scope.
- Check whether the user has not completed the password reset, and cancelled before successfully passing authentication methods.
- Follow further actions or suspicious logins from the account.

10.24 | Short-lived Azure AD user account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

An Azure AD user was created and deleted within a short period of time.

Attacker's Goals

Evasion using a valid account.

Investigative actions

- Check the user who created the account and verify the activity.
- Confirm that the account creation was not accidental.

Variations

Abnormal Short-lived Azure AD user account

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

An Azure AD user was created and deleted within a short period of time. by an identity does not regularly create and delete accounts.

Attacker's Goals

Evasion using a valid account.

Investigative actions

- Check the user who created the account and verify the activity.
- Confirm that the account creation was not accidental.

10.25 | Multiple Azure AD admin role removals

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Hours
Deduplication Period	1 Day
Required Data	• Requires: ◦ AzureAD Audit Log
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Low

Description

An Azure AD identity removed multiple administrators from their roles.

Attacker's Goals

An attacker may want to lock out an organization and retain sole access.

Investigative actions

- Check if the identity performing the actions was authorized to perform them.
- Check what roles the users were removed from.
- Check whether the identity is a newly added admin.
- Check if the identity is operating in its usual matter (location, time, operations)
- Check if the identity performed additional operations in the cloud environment that might be malicious.

11 | Box Audit Log

11.1 | Suspicious SaaS 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: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	

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

Description

A SaaS 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

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 SaaS 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.

Suspicious SaaS API call from a Tor exit node via Mobile Device

Synopsis

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

Description

A SaaS 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.

11.2 | Massive file downloads from SaaS service

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: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Informational

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

Variations

Massive code file downloads from SaaS service

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Informational

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

Suspicious SaaS service file downloads

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Low

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior. The user connected from an unknown IP and displayed suspicious characteristics.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

Massive file downloads from SaaS service by terminated user

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Low

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

11.3 | External SaaS file-sharing activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day

Required Data	• Requires one of the following data sources: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Informational

Description

A user shared files from within a SaaS service to an external domain.

Attacker's Goals

An attacker may share files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Determine if the files are shared with users outside the organization and if the recipients are familiar.
- Review the files that were shared to determine if they contain sensitive data.
- Analyze the file types that were shared.
- Monitor the account for any further suspicious actions.

Variations

SaaS external file sharing to an abnormal domain

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Low

Description

A user shared files to an external domain, which the organization does not typically share files with.

Attacker's Goals

An attacker may share files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Determine if the files are shared with users outside the organization and if the recipients are familiar.
- Review the files that were shared to determine if they contain sensitive data.
- Analyze the file types that were shared.
- Monitor the account for any further suspicious actions.

11.4 | Massive upload to SaaS service

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	3 Hours
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	• Exfiltration (TA0010) • Collection (TA0009)
ATT&CK Technique	• Exfiltration Over Web Service (T1567) • Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002) • Data Staged: Remote Data Staging (T1074.002)
Severity	Informational

Description

A user uploaded a large amount of data to an organizational cloud storage. This behavior may indicate that the data is being exfiltrated or staged.

Attacker's Goals

An attacker may upload files to a SaaS service to stage and exfiltrate data from the organization.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were uploaded to determine if they contain sensitive data.
- Verify if the user account that uploaded the files is authorized to access them.
- Analyze the file types that were uploaded.
- Monitor the account for any further suspicious actions.

Variations

Massive upload to SaaS service by suspicious user

Synopsis

ATT&CK Tactic	• Exfiltration (TA0010) • Collection (TA0009)
ATT&CK Technique	• Exfiltration Over Web Service (T1567) • Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002) • Data Staged: Remote Data Staging (T1074.002)
Severity	Low

Description

A suspicious user uploaded a large amount of data to an organizational cloud storage. This behavior may indicate that the data is being exfiltrated or staged.

Attacker's Goals

An attacker may upload files to a SaaS service to stage and exfiltrate data from the organization.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were uploaded to determine if they contain sensitive data.
- Verify if the user account that uploaded the files is authorized to access them.
- Analyze the file types that were uploaded.
- Monitor the account for any further suspicious actions.

12 | DropBox

12.1 | Suspicious SaaS 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: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	

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

Description

A SaaS 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

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 SaaS 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.

Suspicious SaaS API call from a Tor exit node via Mobile Device

Synopsis

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

Description

A SaaS 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.

12.2 | Massive file downloads from SaaS service

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: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Informational

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

Variations

Massive code file downloads from SaaS service

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Informational

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

Suspicious SaaS service file downloads

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Low

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior. The user connected from an unknown IP and displayed suspicious characteristics.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

Massive file downloads from SaaS service by terminated user

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Low

Description

A user downloaded a large volume of files from an organizational SaaS service, either exceeding the normal file count or size for the user's typical behavior.

Attacker's Goals

An attacker may download files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were downloaded to determine if they contain sensitive data.
- Verify if the user account that downloaded the files is authorized to access them.
- Analyze the file types that were downloaded.
- Monitor the account for any further suspicious actions.

12.3 | External SaaS file-sharing activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day

Required Data	• Requires one of the following data sources: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Informational

Description

A user shared files from within a SaaS service to an external domain.

Attacker's Goals

An attacker may share files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Determine if the files are shared with users outside the organization and if the recipients are familiar.
- Review the files that were shared to determine if they contain sensitive data.
- Analyze the file types that were shared.
- Monitor the account for any further suspicious actions.

Variations

SaaS external file sharing to an abnormal domain

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Cloud Storage (T1530)
Severity	Low

Description

A user shared files to an external domain, which the organization does not typically share files with.

Attacker's Goals

An attacker may share files from a SaaS service to exfiltrate sensitive data.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Determine if the files are shared with users outside the organization and if the recipients are familiar.
- Review the files that were shared to determine if they contain sensitive data.
- Analyze the file types that were shared.
- Monitor the account for any further suspicious actions.

12.4 | Massive upload to SaaS service

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	3 Hours
Deduplication Period	1 Day
Required Data	• Requires one of the following data sources: ◦ Box Audit Log OR ◦ DropBox OR ◦ Google Workspace Audit Logs OR ◦ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	• Exfiltration (TA0010) • Collection (TA0009)
ATT&CK Technique	• Exfiltration Over Web Service (T1567) • Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002) • Data Staged: Remote Data Staging (T1074.002)
Severity	Informational

Description

A user uploaded a large amount of data to an organizational cloud storage. This behavior may indicate that the data is being exfiltrated or staged.

Attacker's Goals

An attacker may upload files to a SaaS service to stage and exfiltrate data from the organization.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were uploaded to determine if they contain sensitive data.
- Verify if the user account that uploaded the files is authorized to access them.
- Analyze the file types that were uploaded.
- Monitor the account for any further suspicious actions.

Variations

Massive upload to SaaS service by suspicious user

Synopsis

ATT&CK Tactic	• Exfiltration (TA0010) • Collection (TA0009)
ATT&CK Technique	• Exfiltration Over Web Service (T1567) • Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002) • Data Staged: Remote Data Staging (T1074.002)
Severity	Low

Description

A suspicious user uploaded a large amount of data to an organizational cloud storage. This behavior may indicate that the data is being exfiltrated or staged.

Attacker's Goals

An attacker may upload files to a SaaS service to stage and exfiltrate data from the organization.

Investigative actions

- Check for signs of account compromise, such as abnormal login activity or unusual behavior.
- Review the files that were uploaded to determine if they contain sensitive data.
- Verify if the user account that uploaded the files is authorized to access them.
- Analyze the file types that were uploaded.
- Monitor the account for any further suspicious actions.

13 | Duo

13.1 | 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.

13.2 | 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.

13.3 | 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.

13.4 | 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.

13.5 | 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.

13.6 | 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.

13.7 | 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.

13.8 | 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.

13.9 | 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.

13.10 | 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.

13.11 | 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.

13.12 | 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.

13.13 | 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.

13.14 | 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.

13.15 | 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.

13.16 | 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.

13.17 | 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.

13.18 | 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

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	Low

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.

13.19 | Intense SSO failures

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	10 Minutes
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) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

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 whether a successful login was made after unsuccessful attempts.

Variations

Intense SSO failures with suspicious characteristics

Synopsis

ATT&CK Tactic	• Credential Access (TA0006) • Initial Access (TA0001)
ATT&CK Technique	• Valid Accounts (T1078) • Brute Force: Password Spraying (T1110.003) • Brute Force: Password Guessing (T1110.001)
Severity	Low

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

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 whether a successful login was made after unsuccessful attempts.

14 | Gcp Audit Log

14.1 | 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.

14.2 | GCP Virtual Private Cloud (VPC) Network Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	• Requires: ◦ 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 GCP VPC network was deleted. An attacker might use this technique to interrupt business resources and workflows.

Attacker's Goals

Block the availability of targeted resources to users/services.

Investigative actions

- Check which services were affected by the VPC deletion.
- Check the cloud identity activity prior/after the VPC network deletion.

14.3 | 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.

14.4 | Remote usage of an App engine Service Account token

Synopsis

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

Description

A GCP Service Account token, which is attached to an app engine, was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the Service Account was attached to a specific app engine.
- Check if the Service Account was used by a user.
- Check if the relevant app engine is compromised.

Variations

Suspicious usage of App engine Service Account token

Synopsis

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

Description

A GCP Service Account token, which is attached to an app engine, was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the Service Account was attached to a specific app engine.
- Check if the Service Account was used by a user.
- Check if the relevant app engine is compromised.

14.5 | 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.

14.6 | 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.

14.7 | 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.

14.8 | 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.

14.9 | 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.

14.10 | 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.

14.11 | A cloud function was created with an unusual runtime

Synopsis

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

ATT&CK Technique	Serverless Execution (T1648)
Severity	Low

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

Examine the cloud function's code implementation and look for any unusual invocations.

Check for any unusual activities within the same project.

Variations

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

Synopsis

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

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

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

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

Synopsis

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

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

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

A cloud function was created with a custom runtime

Synopsis

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

Description

A cloud function was created with an unusual runtime.

Attacker's Goals

Execute arbitrary code in cloud environments.

Investigative actions

Examine the cloud function's code implementation and look for any unusual invocations.

Check for any unusual activities within the same project.

14.12 | 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.

14.13 | 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.

14.14 | 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.

14.15 | 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.

14.16 | Unusual Identity and Access Management (IAM) activity

Synopsis

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

Deduplication Period	5 Days
Required Data	▪ Requires one of the following data sources: ▫ AWS Audit Log OR ▫ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001) ▪ Valid Accounts: Cloud Accounts (T1078.004)
Severity	Informational

Description

A cloud identity performed an unusual IAM operation.

Attacker's Goals

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

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

Investigative actions

Check the identity's role designation in the organization.

- Verify that the identity did not perform any sensitive IAM operation that it shouldn't.

Variations

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

Synopsis

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

Description

A cloud Internet facing instance performed an unusual IAM operation.

Attacker's Goals

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

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

Investigative actions

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

Unusual Identity and Access Management (IAM) activity

Synopsis

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

Severity	Low

Description

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

Attacker's Goals

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

Investigative actions

Check the identity's role designation in the organization.

Verify that the identity did not perform any sensitive IAM operation that it shouldn't.

14.17 | 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.

14.18 | 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.

14.19 | 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.

14.20 | GCP Pub/Sub Topic Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Service Stop (T1489)
Severity	Informational

Description

A GCP Pub/Sub topic was deleted, might affect workflows due to interrupts within the Pub/Sub pipeline.

Attacker's Goals

Interrupt business services.

Investigative actions

Check which services were affected due to the Pub/Sub topic deletion.
- Check the cloud identity activity prior/after the topic deletion.

14.21 | 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.

14.22 | 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.

14.23 | 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.

14.24 | 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.

14.25 | 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.

14.26 | Cloud compute instance user data script modification

Synopsis

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

Description

The user data of a cloud compute instance was modified.

Attacker's Goals

Execute commands within virtual machines.

Investigative actions

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

Variations

Unusual Cloud compute instance user data script modification

Synopsis

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

Description

The user data of a cloud compute instance was modified.

Attacker's Goals

Execute commands within virtual machines.

Investigative actions

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

14.27 | 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.

14.28 | 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.

14.29 | GCP Storage Bucket Configuration Modification

Synopsis

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

Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Manipulation: Stored Data Manipulation (T1565.001)
Severity	Informational

Description

A GCP storage bucket configuration has been modified.

Attacker's Goals

Manipulate stored data.

Investigative actions

- Check if there were any services/procedures affected by the modification.
- Check what other actions were taken by the identity that modified the configuration.

14.30 | GCP Firewall Rule creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours

Required Data	▮ Requires: ▮ 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 GCP VPN firewall rule was created. An attacker might use this technique to block or open access to/from restricted areas.

Attacker's Goals

Access restricted resources.

Investigative actions

- Check if there were any network attempts that fit the created rule.
- Check the cloud identity activity prior/after to the rule creation.

14.31 | 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.

14.32 | Cloud impersonation attempt by unusual identity type

Synopsis

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

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

Description

A suspicious identity type has attempted to impersonate another identity.

Attacker's Goals

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

Investigative actions

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

Variations

Successful cloud impersonation by an unusual identity type

Synopsis

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

Description

A suspicious identity type has successfully impersonated another identity.

Attacker's Goals

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

Investigative actions

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

14.33 | 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.

14.34 | GCP Pub/Sub Subscription Deletion

Synopsis

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

Description

A GCP Pub/Sub subscription was deleted. An attacker might use this technique to affect business workflows.

Attacker's Goals

Interrupt business services.

Investigative actions

- Check which services were affected due to the Pub/Sub deletion.
- Check the cloud identity activity prior/after the subscription deletion.

14.35 | GCP IAM Service Account Key Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

A GCP IAM service account key was deleted. An attacker might use this technique to interrupt business operations.

Attacker's Goals

Account access removal.

Investigative actions

Check which operations were corrupted after the deletion.

14.36 | 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.

14.37 | GCP Logging Bucket Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: - Gcp 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

A GCP logging bucket was deleted. An attacker might delete the bucket to evade detection.

Attacker's Goals

Evade detection.

Investigative actions

- Check which logs were affected by the bucket deletion.
  Check the cloud identity activity prior/after to the bucket deletion.

14.38 | 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.

14.39 | GCP Virtual Private Network Route Creation

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - 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 GCP VPC route was created. An attacker might use this technique to impact business workflows.

Attacker's Goals

Block the availability of targeted resources to users/services.

Investigative actions

- Check which services were affected by the route creation.
  Check the cloud identity activity prior/after the route creation.

14.40 | 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.

14.41 | GCP Service Account key creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Informational

Description

A GCP service account key was created. An attacker might use this technique to evade detection.

Attacker's Goals

Persistence using the created key.

Investigative actions

- Check what actions were taken using the newly created service account key.
- Check what other actions were taken by the identity that created the key.

14.42 | 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.

14.43 | A Command Line Interface (CLI) command was executed from a GCP serverless compute service

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	Cloud Serverless Function Credentials Theft Analytics
ATT&CK Tactic	Initial Access (TA0001) Credential Access (TA0006)
ATT&CK Technique	Valid Accounts: Cloud Accounts (T1078.004) Steal Application Access Token (T1528) Unsecured Credentials (T1552)
Severity	Low

Description

A GCP serverless compute service token was used to execute a Command Line Interface (CLI) command.

Attacker's Goals

Exfiltrate serverless token and abuse it.

Investigative actions

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

Variations

Suspicious Command Line Interface (CLI) command was executed from a GCP serverless compute service

Synopsis

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

Description

A GCP serverless compute service token was used to execute a Command Line Interface (CLI) command.

Attacker's Goals

Exfiltrate serverless token and abuse it.

Investigative actions

Verify whether the serverless-attached identity's credentials were intentionally used in CLI.

Check what CLI commands were executed using the serverless attached token.
- Check if the suspected serverless function is compromised.

Unusual Command Line Interface (CLI) command was executed from a GCP serverless compute service

Synopsis

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

Description

A GCP serverless compute service token was used to execute a Command Line Interface (CLI) command.

Attacker's Goals

Exfiltrate serverless token and abuse it.

Investigative actions

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

14.44 | 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.

14.45 | 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.

14.46 | 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.

14.47 | 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.

14.48 | 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.

14.49 | GCP Virtual Private Network Route Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - 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 GCP VPC route was deleted. An attacker might use this technique to impact business workflows.

Attacker's Goals

Block the availability of targeted resources to users/services.

Investigative actions

Check which services were affected by the route deletion.
- Check the cloud identity activity prior/after the route deletion.

14.50 | 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.

14.51 | Cloud unusual access key creation

Synopsis

Activation Period	14 Days
Training Period	30 Days

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

Description

Cloud suspicious access key creation by a cloud identity.

Attacker's Goals

Persist in the environment.

Investigative actions

investigate the identity who created the access token.

Check the access token activity in the organization.

Variations

Cloud successful access key creation by an unusual identity

Synopsis

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

Description

Cloud suspicious access key creation by a cloud identity.

Attacker's Goals

Persist in the environment.

Investigative actions

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

Cloud unusual successful access key creation

Synopsis

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

Description

Cloud suspicious access key creation by a cloud identity.

Attacker's Goals

Persist in the environment.

Investigative actions

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

14.52 | Unusual cloud identity impersonation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires one of the following data sources: - AWS Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	- Privilege Escalation (TA0004) Defense Evasion (TA0005)

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

Description

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

Attacker's Goals

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

Investigative actions

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

Variations

Unusual cloud identity impersonation by an identity with high administrative activity

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

Suspicious cloud identity impersonation was succeeded

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

Check the identity's designation.

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

Suspicious cloud identity impersonation was failed

Synopsis

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

Description

A cloud identity has failed to impersonate another identity.

Attacker's Goals

Escalate privileges and bypass access controls

- Avoid detection throughout their compromise.

Investigative actions

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

14.53 | 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.

14.54 | Remote usage of VM Service Account token

Synopsis

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

Description

A GCP Service Account token, which is attached to a VM, was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

- Check if the Service Account was attached to a specific VM.
- Check if the Service Account was used by a user.
  Check if the relevant VM is compromised.

Variations

Suspicious usage of VM Service Account token

Synopsis

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

Description

A GCP Service Account token, which is attached to a VM, was used externally of the cloud environment.

Attacker's Goals

Exfiltrate token and abuse it remotely.

Investigative actions

Check if the Service Account was attached to a specific VM.
Check if the Service Account was used by a user.
Check if the relevant VM is compromised.

14.55 | 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.

14.56 | GCP Service Account Disable

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

A GCP service account was disabled. An attacker might use this technique to interrupt business procedures and workflows.

Attacker's Goals

Account access removal.

Investigative actions

Check if there were any services/procedures affected by the disable operation.

14.57 | Cloud Organizational policy was created or modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562) Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

Cloud organizational policy was created or modified.

Attacker's Goals

Gain elevated privileges, disable security measures, misuse resources or cause disruption.

Investigative actions

- Check which services were affected by the policy creation.
- Check the cloud identity activity prior/after the policy creation.

Variations

Cloud Organizational policy was created or modified

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562) - Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

Cloud organizational policy was created or modified.

Attacker's Goals

Gain elevated privileges, disable security measures, misuse resources or cause disruption.

Investigative actions

Check which services were affected by the policy creation.
- Check the cloud identity activity prior/after the policy creation.

14.58 | GCP IAM Role Deletion

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

A GCP IAM role was created. An attacker might use this technique to interrupt users' actions.

Attacker's Goals

Inhibit users from accessing resources.

Investigative actions

- Check which users were affected by the role deletion.
- Check what other actions were taken by the identity that deleted the role.

14.59 | 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.

14.60 | GCP Firewall Rule Modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: 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 GCP firewall rule was modified. An attacker might use this technique to access restricted resources.

Attacker's Goals

Access restricted resources.

Investigative actions

- Check if there were any network attempts that fit the deleted rule.
- Check the cloud identity activity prior/after to the rule deletion.

14.61 | 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.

14.62 | 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.

14.63 | 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.

14.64 | 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.

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

Synopsis

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

Required Data	▮ Requires one of the following data sources: - AWS Audit Log OR - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087) Permission Groups Discovery (T1069) ▮ Cloud Service Discovery (T1526)
Severity	Informational

Description

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

Attacker's Goals

Gain information on the Cloud environment, specifically IAM information such as User, Group,

Roles, Policies, etc.

Investigative actions

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

14.66 | 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.

14.67 | 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.

14.68 | GCP Service Account deletion

Synopsis

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

Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

A GCP service account was deleted. An attacker might use this technique to remove access to valid accounts.

Attacker's Goals

Account access removal.

Investigative actions

Check which operations were corrupted after the deletion.

14.69 | GCP Storage Bucket deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours

Required Data	▮ Requires: - Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Data Destruction (T1485)
Severity	Informational

Description

A GCP bucket was deleted. An attacker might use this technique to destroy business data and its workflows.

Attacker's Goals

Data destruction.

Investigative actions

Check which data was deleted from the bucket.

14.70 | 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.

14.71 | 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.

14.72 | 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.

14.73 | 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.

14.74 | 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.

14.75 | GCP Service Account creation

Synopsis

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

Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Create Account (T1136)
Severity	Informational

Description

A GCP service account was created. An attacker might use this technique to evade detection.

Attacker's Goals

Persistence with service account.

Investigative actions

Check the identity that created the account and its actions.

14.76 | 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.

14.77 | 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.

14.78 | GCP IAM Custom Role Creation

Synopsis

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

Severity	Informational

Description

A GCP IAM custom role was created. An attacker might use this technique to gain persistence.

Attacker's Goals

Persistence with privileged account.

Investigative actions

Check the identity that created the role and its actions.

14.79 | 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.

14.80 | 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.

14.81 | GCP VPC Firewall Rule Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: - 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 GCP VPC firewall rule was deleted. An attacker might use this technique to access restricted resources.

Attacker's Goals

Access restricted resources.

Investigative actions

- Check if there were any network attempts that fit the deleted rule.
- Check the cloud identity activity prior/after to the rule deletion.

14.82 | GCP Storage Bucket Permissions Modification

Synopsis

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

A GCP storage bucket's IAM permissions were modified. An attacker might use this technique to exposure sensitive data or data loss.

Attacker's Goals

Exfiltrate information.

Investigative actions

Check which data exists in the modified bucket and its classification.
Look for events that involve actions for the bucket data.

14.83 | GCP set IAM policy activity

Synopsis

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

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

A cloud identity had modified a resource policy bindings.

Attacker's Goals

Escalate privileges.

Investigative actions

Verify which permissions were granted to the identity.

Variations

GCP set IAM policy activity by an identity with high administrative activity

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

A cloud identity with high administrative activity had modified a resource policy binding.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

GCP IAM add sensitive role

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Medium

Description

A cloud identity added an IAM sensitive role to itself.

Attacker's Goals

Escalate privileges.

Investigative actions

Verify which permissions were granted to the identity.

GCP storage add sensitive role

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Medium

Description

A cloud identity added a storage sensitive role to itself.

Attacker's Goals

Escalate privileges.

Investigative actions

Verify which permissions were granted to the identity.

GCP compute add sensitive role

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Medium

Description

A cloud identity added a compute sensitive role to itself.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

GCP secret manager add sensitive role

Synopsis

ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Account Manipulation (T1098)
Severity	Medium

Description

A cloud identity added a secret manager sensitive role to itself.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

GCP cloud run add sensitive role

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Medium

Description

A cloud identity added a cloud run sensitive role to itself.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

GCP function add sensitive role

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Medium

Description

A cloud identity added a function sensitive role to itself.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

GCP deployment manager add sensitive role

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Medium

Description

A cloud identity added a deployment manager sensitive role to itself.

Attacker's Goals

Escalate privileges.

Investigative actions

- Verify which permissions were granted to the identity.

14.84 | 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.

14.85 | 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.

14.86 | 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.

14.87 | 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.

14.88 | 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.

14.89 | 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.

14.90 | 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.

14.91 | 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.

14.92 | GCP Logging Sink Deletion

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	- Requires: - Gcp 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

A GCP logging sink entity was deleted. Logs that match the logging sink rule will not arrive at their destination.

An attacker might use this technique to evade detection.

Attacker's Goals

Evade detection.

Investigative actions

- Check which logs were affected by the deletion.
  Check the cloud identity activity prior/after to the entity deletion.

14.93 | GCP Logging Sink Modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	- Requires: - Gcp 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

A GCP logging sink entity was modified. Logs that match the logging sink rule will not arrive at their destination. An attacker might use this technique to evade detection.

Attacker's Goals

Evade detection.

Investigative actions

Check which logs were affected by the modification.

Check the cloud identity activity prior/after to the entity modification.

14.94 | 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

1. Check the identity created resources and its legitimacy.
2. 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.

14.95 | 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.

14.96 | 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.

14.97 | 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.

14.98 | 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.

14.99 | 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.

14.100 | 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.

14.101 | 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.

14.102 | 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.

14.103 | 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.

14.104 | 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.

14.105 | 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.

14.106 | 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.

14.107 | Multi region enumeration activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
Deduplication Period	5 Days