Required Data	▪ Requires one of the following data sources: - AWS Audit Log OR - Azure Audit Log OR ▯ Gcp Audit Log
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	▪ Discovery (TA0007) Defense Evasion (TA0005)
ATT&CK Technique	▪ Cloud Infrastructure Discovery (T1580) Unused/Unsupported Cloud Regions (T1535) Cloud Service Discovery (T1526)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

15 | Gcp Flow Log

15.1 | Possible DCShadow attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▪ Requires one of the following data sources: - AWS Flow Log OR - AWS OCSF Flow Logs OR ▯ Azure Flow Log OR - Gcp Flow Log OR ▯ Palo Alto Networks Platform Logs OR - Third-Party Firewalls OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	▪ Credential Access (TA0006) ▪ Defense Evasion (TA0005)

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

Description

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

Attacker's Goals

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

Investigative actions

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

15.2 | Unusual SSH activity that resembles SSH proxy

Synopsis

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

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

Description

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

Attacker's Goals

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

Investigative actions

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

Variations

High Volume Unusual SSH activity that resembles SSH proxy

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

Suspicious SSH activity that resembles SSH proxy

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

Unusual SSH activity that resembles SSH proxy detected

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised.

Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

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

Synopsis

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

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

Description

An internal cloud resource attempted to connect to the same destination port of multiple external IP addresses.
This may be a result of the cloud resource being hijacked by an attacker.

Attackers perform port scans on a specific destination port for reconnaissance purposes, to detect known vulnerable services that accept connections in the specific port, and perform targeted attacks against them.

Attacker's Goals

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

Investigative actions

Check if similar activity was performed on additional cloud resources.

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

15.4 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources:
	  - AWS Flow Log
	  OR
	  - AWS OCSF Flow Logs
	  OR
	  - Azure Flow Log
	  OR
	  - Gcp Flow Log
	  OR
	  - Palo Alto Networks Platform Logs
	  OR
	  - Third-Party Firewalls
	Requires one of the following data sources:
	  - Palo Alto Networks Platform Logs
	  OR
	  - XDR Agent

Detection Modules	

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

Description

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

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

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

Variations

SSH brute force network detected from external source

Synopsis

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

Description

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

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

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

Rare SSH brute force attempt

Synopsis

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

Description

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

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

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

16 | Google Workspace Audit Logs

16.1 | Gmail routing settings changed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data Staged (T1074) Email Collection (T1114)
Severity	Informational

Description

Gmail routing settings were modified.

Attacker's Goals

Email Collection.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the new routing settings look suspicious.

  Investigate the IP address associated with the routing settings.
- Follow further actions done by the account.

Variations

Gmail routing settings changed by a non-administrative Google Workspace identity

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data Staged (T1074) Email Collection (T1114)
Severity	Low

Description

Gmail routing settings were modified.

Attacker's Goals

Email Collection.

Investigative actions

Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the new routing settings look suspicious.
- Investigate the IP address associated with the routing settings.
  Follow further actions done by the account.

16.2 | Data Sharing between GCP and Google Workspace was disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005) Impact (TA0040)
ATT&CK Technique	Indicator Removal (T1070) Impair Defenses (T1562) Data Manipulation (T1565) Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Informational

Description

An identity has modified data sharing settings between GCP and Google Workspace.

Attacker's Goals

Adversaries may stop audit log events from being sent to remove evidence of their presence or hinder defenses.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

check whether Google Workspace audit log events were configured to be sent to Google Cloud.

- Follow further actions done by the account.

Variations

Data Sharing between GCP and Google Workspace was disabled by a suspicious identity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Impact (TA0040)
ATT&CK Technique	Indicator Removal (T1070) Impair Defenses (T1562) Data Manipulation (T1565) Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Low

Description

An identity has modified data sharing settings between GCP and Google Workspace.

Attacker's Goals

Adversaries may stop audit log events from being sent to remove evidence of their presence or hinder defenses.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- check whether Google Workspace audit log events were configured to be sent to Google Cloud.
  Follow further actions done by the account.

Data Sharing between GCP and Google Workspace was disabled by a non Google Workspace administrative user

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) - Impact (TA0040)
ATT&CK Technique	Indicator Removal (T1070) - Impair Defenses (T1562) - Data Manipulation (T1565) Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Low

Description

An identity has modified data sharing settings between GCP and Google Workspace.

Attacker's Goals

Adversaries may stop audit log events from being sent to remove evidence of their presence or hinder defenses.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- check whether Google Workspace audit log events were configured to be sent to Google Cloud.
  Follow further actions done by the account.

Data Sharing between GCP and Google Workspace was disabled from an unusual ASN

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Impact (TA0040)
ATT&CK Technique	Indicator Removal (T1070) Impair Defenses (T1562) Data Manipulation (T1565) ▮ Impair Defenses: Disable or Modify Cloud Logs (T1562.008)
Severity	Low

Description

An identity has modified data sharing settings between GCP and Google Workspace.

Attacker's Goals

Adversaries may stop audit log events from being sent to remove evidence of their presence or hinder defenses.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  check whether Google Workspace audit log events were configured to be sent to Google Cloud.
- Follow further actions done by the account.

16.3 | External Sharing was turned on for Google Drive

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Transfer Data to Cloud Account (T1537)
Severity	Informational

Description

An identity has modified Google Drive sharing settings and allowed external sharing.

Attacker's Goals

Adversaries may exfiltrate data, such as sensitive documents.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  check the new setting details.
  Follow further actions done by the account.

Variations

External Sharing was turned on for Google Drive by a non Google Workspace administrative user from an unusual ASN

Synopsis

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

Description

An identity has modified Google Drive sharing settings and allowed external sharing.

Attacker's Goals

Adversaries may exfiltrate data, such as sensitive documents.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

check the new setting details.

- Follow further actions done by the account.

External Sharing was turned on for Google Drive by a non Google Workspace administrative user

Synopsis

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

Description

An identity has modified Google Drive sharing settings and allowed external sharing.

Attacker's Goals

Adversaries may exfiltrate data, such as sensitive documents.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
check the new setting details.

- Follow further actions done by the account.

External Sharing was turned on for Google Drive from an unusual ASN

Synopsis

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

Description

An identity has modified Google Drive sharing settings and allowed external sharing.

Attacker's Goals

Adversaries may exfiltrate data, such as sensitive documents.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- check the new setting details.
  Follow further actions done by the account.

16.4 | A Google Workspace service was configured as unrestricted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

An identity configured a Google Workspace service as unrestricted

- Apps configured with a trusted or limited access setting can access data for unrestricted services.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the new settings look suspicious.

  Follow further actions done by the account.

Variations

A Google Workspace service was configured as unrestricted by a suspicious identity

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

An identity configured a Google Workspace service as unrestricted
Apps configured with a trusted or limited access setting can access data for unrestricted services.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the new settings look suspicious.
- Follow further actions done by the account.

A Google Workspace service was configured as unrestricted from an unusual ASN

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

An identity configured a Google Workspace service as unrestricted

- Apps configured with a trusted or limited access setting can access data for unrestricted services.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the new settings look suspicious.
- Follow further actions done by the account.

A Google Workspace service was configured as unrestricted by a non-administrative identity

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

An identity configured a Google Workspace service as unrestricted
- Apps configured with a trusted or limited access setting can access data for unrestricted services.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Check if the new settings look suspicious.
- Follow further actions done by the account.

16.5 | A GCP service account was delegated domain-wide authority in Google Workspace

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

A Google Workspace admin has enabled domain-wide delegation to a GCP service account.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

  Check if the new settings look suspicious.
  Follow further actions done by the account.

Variations

A Google Workspace admin has enabled domain-wide delegation to a GCP service account and granted him access to a sensitive scope

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Medium

Description

A Google Workspace admin has enabled domain-wide delegation to a GCP service account.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

  Check if the new settings look suspicious.
  Follow further actions done by the account.

A Google Workspace admin has enabled domain-wide delegation to a globally uncommon Client ID

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Medium

Description

A Google Workspace admin has enabled domain-wide delegation to a GCP service account.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the new settings look suspicious.
  Follow further actions done by the account.

16.6 | User accessed SaaS resource via anonymous link

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: - 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 accessed a SaaS resource via an anonymous link.

Attacker's Goals

An attacker is attempting to collect sensitive data.

Investigative actions

- Check the IP address from which the access originated.
  Examine the file that was accessed for any sensitive indicators.
  Follow further actions taken, such as downloading files.

Variations

External user accessed a sensitive SaaS file via anonymous link

Synopsis

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

Description

An external user accessed a sensitive SaaS file via an anonymous link.

Attacker's Goals

An attacker is attempting to collect sensitive data.

Investigative actions

- Check the IP address from which the access originated.
- Examine the file that was accessed for any sensitive indicators.
  Follow further actions taken, such as downloading files.

User accessed a public Google Drive document

Synopsis

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

Description

A user accessed a Google Drive document that is public on the web.

Attacker's Goals

An attacker is attempting to collect sensitive data.

Investigative actions

- Check the IP address from which the access originated.
  Examine the file that was accessed for any sensitive indicators.
  Follow further actions taken, such as downloading files.

16.7 | A Google Workspace user was added to a group

Synopsis

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

Required Data	▮ Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

A user added another user to a Google Workspace group.

Attacker's Goals

Adversaries may manipulate accounts and groups to maintain access to victim systems.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the user was added to a sensitive group.
  Follow further actions done by the account.

16.8 | Admin privileges were granted to a Google Workspace

user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: • Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

Admin privileges were granted to a Google Workspace user. This user now has access to additional administrative functions and settings.

Attacker's Goals

Gain access to sensitive data stored in Google Workspace. Manipulate or delete data stored in Google Workspace. Gain access to privileged features in Google Workspace.

Investigative actions

- Check which Google Workspace user was granted the admin privileges.
  Check if the user is authorized to be granted such privileges.

  Review the audit logs to determine the actions taken by the user.

16.9 | MFA Disabled for Google Workspace

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	▪ Modify Authentication Process (T1556) ▪ Modify Authentication Process: Multi-Factor Authentication (T1556.006)
Severity	Low

Description

An administrator has disabled Multi-Factor Authentication for Google Workspace users.

Attacker's Goals

Gain access to Google Workspace accounts with disabled MFA. Exploit Google Workspace accounts with weaker security. Steal sensitive data from Google Workspace accounts.

Investigative actions

- Check the MFA settings for the Google Workspace users.
  Identify the users who have MFA disabled and investigate the reason for it.
  Check the security log to see if there have been any suspicious activities in the account.

Variations

MFA Disabled for Google Workspace from an unusual caller IP ASN

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	▪ Modify Authentication Process (T1556) Modify Authentication Process: Multi-Factor Authentication (T1556.006)
Severity	Low

Description

An administrator has disabled Multi-Factor Authentication for Google Workspace users.

Attacker's Goals

Gain access to Google Workspace accounts with disabled MFA. Exploit Google Workspace accounts with weaker security. Steal sensitive data from Google Workspace accounts.

Investigative actions

Check the MFA settings for the Google Workspace users.

Identify the users who have MFA disabled and investigate the reason for it.

Check the security log to see if there have been any suspicious activities in the account.

16.10 | A third-party application's access to the Google Workspace domain's resources was revoked

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Impact (TA0040)

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

Description

An identity removed a third-party application's access to Google Workspace domain's resources.

Attacker's Goals

An attacker might remove an application to impair the environment.

Investigative actions

Check the Google Workspace Application settings to determine which actions were triggered.

- Investigate the source of the request and the user associated with it.
- Review the access control policies to determine if the removal of the application is allowed.

16.11 | A Google Workspace identity used the security investigation tool

Synopsis

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

Required Data	▮ Requires: ▁ Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	▮ Data from Information Repositories (T1213) Email Collection (T1114)
Severity	Informational

Description

A Google Workspace identity used the security investigation tool

The Google Workspace security investigation tool can be abused to access sensitive data.

Attacker's Goals

Access sensitive data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Determine what data was accessed using the security investigation tool.

Variations

A suspicious Google Workspace identity used the security investigation tool

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213) Email Collection (T1114)
Severity	Low

Description

- A Google Workspace identity used the security investigation tool
- The Google Workspace security investigation tool can be abused to access sensitive data.

Attacker's Goals

Access sensitive data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Determine what data was accessed using the security investigation tool.

16.12 | 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.

16.13 | SaaS suspicious external domain user 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: - Google Workspace Audit Logs OR - Office 365 Audit
Detection Modules	Identity Threat Module
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 identity activity in the organization.

Variations

Suspicious external user activity detected from a domain first seen in the organization

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, both in cloud and SaaS environments.

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 identity activity in the organization.

16.14 | A Google Workspace identity created, assigned or modified a role

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	▮ Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A Google Workspace identity created, assigned or modified a delegated admin role.

Attacker's Goals

An adversary may create, assign or modify a role to elevate the permissions of other user accounts and persist in their target's environment.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
Check the identity's role designation in the organization.

- Follow further actions done by the account.

Variations

A non-administrative Google Workspace identity created, assigned or modified a role from an unusual ASN

Synopsis

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

Description

A Google Workspace identity created, assigned or modified a delegated admin role.

Attacker's Goals

An adversary may create, assign or modify a role to elevate the permissions of other user accounts and persist in their target's environment.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check the identity's role designation in the organization.
Follow further actions done by the account.

A non-administrative Google Workspace identity created, assigned or modified a role

Synopsis

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

Description

A Google Workspace identity created, assigned or modified a delegated admin role.

Attacker's Goals

An adversary may create, assign or modify a role to elevate the permissions of other user accounts and persist in their target's environment.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check the identity's role designation in the organization.
- Follow further actions done by the account.

A Google Workspace identity created, assigned or modified a role from an unusual ASN

Synopsis

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

Description

A Google Workspace identity created, assigned or modified a delegated admin role.

Attacker's Goals

An adversary may create, assign or modify a role to elevate the permissions of other user accounts and persist in their target's environment.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check the identity's role designation in the organization.
- Follow further actions done by the account.

16.15 | A Google Workspace Role privilege was deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	

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

Description

A privilege was removed from a Google Workspace Role, This could potentially affect the access to services and data in the organization.

Attacker's Goals

Gain access to sensitive data stored in the workspace. Gain elevated privileges in the workspace.

Investigative actions

Investigate who was assigned the deleted role privilege.
Verify if the role privilege was deleted intentionally.

16.16 | An app was added to Google Marketplace

Synopsis

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

Required Data	▪ Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Remote Access Software (T1219)
Severity	Informational

Description

An app was added to the Google Workspace Marketplace.

Attacker's Goals

An adversary may add a malicious application to an organization's Google Workspace domain to maintain a presence in their target's organization and steal data.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Investigate the new app that was added to Google workspace Marketplace.
  Follow further actions done by the account.

Variations

An app was added to Google Marketplace by a non-administrative identity

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Remote Access Software (T1219)
Severity	Informational

Description

An app was added to the Google Workspace Marketplace.

Attacker's Goals

An adversary may add a malicious application to an organization's Google Workspace domain to maintain a presence in their target's organization and steal data.

Investigative actions

Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

Investigate the new app that was added to Google workspace Marketplace.

- Follow further actions done by the account.

An app was added to Google Marketplace from an unusual ASN

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Remote Access Software (T1219)
Severity	Low

Description

An app was added to the Google Workspace Marketplace.

Attacker's Goals

An adversary may add a malicious application to an organization's Google Workspace domain to maintain a presence in their target's organization and steal data.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Investigate the new app that was added to Google workspace Marketplace.
- Follow further actions done by the account.

An unusual app was added to Google Marketplace

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Remote Access Software (T1219)
Severity	Low

Description

An app was added to the Google Workspace Marketplace.

Attacker's Goals

An adversary may add a malicious application to an organization's Google Workspace domain to maintain a presence in their target's organization and steal data.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Investigate the new app that was added to Google workspace Marketplace.
  Follow further actions done by the account.

16.17 | Google Workspace organizational unit was modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: • Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

A Google Workspace admin modified an organizational unit.

Attacker's Goals

Adversaries may change the organizational unit the user belongs to, so they could inherit permissions for applications and resources that were inaccessible before.

Investigative actions

Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Follow further actions done by the account.

16.18 | A domain was added to the trusted domains list

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562) Domain or Tenant Policy Modification: Trust Modification (T1484.002)

Severity	Low

Description

A domain was added to the Google Workspace trusted domains list.

Attacker's Goals

An adversary may add a trusted domain to collect and exfiltrate data from their target's organization with less restrictive security controls.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Investigate the new domain in the trusted domains list.
  Follow further actions done by the account.

Variations

A domain was added to the trusted domains list by a non Google Workspace administrative user

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	- Impair Defenses (T1562) Domain or Tenant Policy Modification: Trust Modification (T1484.002)
Severity	Low

Description

A domain was added to the Google Workspace trusted domains list.

Attacker's Goals

An adversary may add a trusted domain to collect and exfiltrate data from their target's organization with less restrictive security controls.

Investigative actions

Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Investigate the new domain in the trusted domains list.
- Follow further actions done by the account.

A domain was added to the trusted domains list from an unusual ASN

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	- Impair Defenses (T1562) - Domain or Tenant Policy Modification: Trust Modification (T1484.002)
Severity	Low

Description

A domain was added to the Google Workspace trusted domains list.

Attacker's Goals

An adversary may add a trusted domain to collect and exfiltrate data from their target's organization with less restrictive security controls.

Investigative actions

Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

Investigate the new domain in the trusted domains list.

- Follow further actions done by the account.

16.19 | An app was removed from a blocked list in Google Workspace

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Informational

Description

An identity removed an app from Google Workspace blocked OAuth or third-party apps list.

Attacker's Goals

Malicious OAuth Apps can be used to request elevated permissions or to impersonate another user.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Check if the app that was removed from the trusted apps list looks suspicious.
- Follow further actions done by the account.

Variations

An app was removed from a blocked list in Google Workspace by a suspicious identity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Low

Description

An identity removed an app from Google Workspace blocked OAuth or third-party apps list.

Attacker's Goals

Malicious OAuth Apps can be used to request elevated permissions or to impersonate another user.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Check if the app that was removed from the trusted apps list looks suspicious.
- Follow further actions done by the account.

An app was removed from a blocked list in Google Workspace by a non Google Workspace

administrative user

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Low

Description

An identity removed an app from Google Workspace blocked OAuth or third-party apps list.

Attacker's Goals

Malicious OAuth Apps can be used to request elevated permissions or to impersonate another user.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

  Check if the app that was removed from the trusted apps list looks suspicious.
  Follow further actions done by the account.

An app was removed from a blocked list in Google Workspace from an unusual ASN

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Low

Description

An identity removed an app from Google Workspace blocked OAuth or third-party apps list.

Attacker's Goals

Malicious OAuth Apps can be used to request elevated permissions or to impersonate another user.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Check if the app that was removed from the trusted apps list looks suspicious.
  Follow further actions done by the account.

16.20 | A Google Workspace user was removed from a group

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	- Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	

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

Description

A user removed another user from a Google Workspace group.

Attacker's Goals

Adversaries may interrupt the availability of services and resources by inhibiting access to users.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

Check if the user's work can be affected by this action.

Follow further actions done by the account.

16.21 | An app was added to the Google Workspace trusted OAuth apps list

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days

Required Data	▮ Requires: ▯ Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Informational

Description

An identity added an OAuth app to the Google Workspace trusted OAuth apps list.

Attacker's Goals

Malicious OAuth Apps can be used to request elevated permissions or to impersonate another user.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the app that was added to the trusted apps list looks suspicious.
  Follow further actions done by the account.

Variations

An unusual app was added to the Google Workspace trusted OAuth apps list

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Low

Description

An identity added an OAuth app to the Google Workspace trusted OAuth apps list.

Attacker's Goals

Malicious OAuth Apps can be used to request elevated permissions or to impersonate another user.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

Check if the app that was added to the trusted apps list looks suspicious.

- Follow further actions done by the account.

An app was added to the Google Workspace trusted OAuth apps list by a non-administrative identity

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Modify Authentication Process (T1556)
Severity	Low

Description

An identity added an OAuth app to the Google Workspace trusted OAuth apps list.

Attacker's Goals

Malicious OAuth Apps can be used to request elevated permissions or to impersonate another user.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the app that was added to the trusted apps list looks suspicious.
- Follow further actions done by the account.

16.22 | Google Workspace third-party application's security settings were changed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: Google Workspace Audit Logs
Detection Modules	Identity Threat Module

Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

An identity changed Google Workspace third-party application's security settings.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the new settings look suspicious.

  Follow further actions done by the account.

Variations

Google Workspace third-party application's security settings were changed by a suspicious identity

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

An identity changed Google Workspace third-party application's security settings.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the new settings look suspicious.
- Follow further actions done by the account.

Google Workspace third-party application's security settings were changed from an unusual ASN

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

An identity changed Google Workspace third-party application's security settings.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the new settings look suspicious.

Follow further actions done by the account.

Google Workspace third-party application's security settings were changed by a non Google Workspace administrative user

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

An identity changed Google Workspace third-party application's security settings.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the new settings look suspicious.

  Follow further actions done by the account.

16.23 | A mail forwarding rule was configured in Google Workspace

Synopsis

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

Deduplication Period	2 Days
Required Data	Requires: ▯ Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	▮ Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	▮ Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Medium

Description

A rule was set up to forward emails outside the Google Workspace domain.

Attacker's Goals

- Adversaries may abuse email forwarding rules to monitor the activities of a victim, steal information, and further gain intelligence on the victim or the victim's organization to use as part of further exploits or operations.
  Furthermore, email forwarding rules can allow adversaries to maintain persistent access to victim's emails even after compromised credentials are reset by administrators.

Investigative actions

Check if the identity intended to preform this action,
- and look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the forwarding domain is an unknown external domain and look up its reputation.
  Follow further actions done by the account.

Variations

A mail forwarding rule was configured in Google Workspace to an uncommon domain

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	High

Description

A rule was set up to forward emails outside the Google Workspace domain.

Attacker's Goals

Adversaries may abuse email forwarding rules to monitor the activities of a victim, steal information, and further gain intelligence on the victim or the victim's organization to use as part of further exploits or operations.
- Furthermore, email forwarding rules can allow adversaries to maintain persistent access to victim's emails even after compromised credentials are reset by administrators.

Investigative actions

Check if the identity intended to preform this action,
and look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
- Check if the forwarding domain is an unknown external domain and look up its reputation.
- Follow further actions done by the account.

16.24 | Google Marketplace restrictions were modified

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: • Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

An identity modified Google Marketplace Restrictions.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the new settings look suspicious.
  Follow further actions done by the account.

Variations

Google Marketplace restrictions were modified by a suspicious identity

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

An identity modified Google Marketplace Restrictions.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the new settings look suspicious.
  Follow further actions done by the account.

Google Marketplace restrictions were modified from an unusual ASN

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)

ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Low

Description

An identity modified Google Marketplace Restrictions.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

- Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the new settings look suspicious.
  Follow further actions done by the account.

Google Marketplace restrictions were modified by a non Google Workspace administrative user

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

An identity modified Google Marketplace Restrictions.

Attacker's Goals

Malicious Apps can be used to access the organization's Google data.

Investigative actions

Check if the identity intended to perform this action, or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Check if the new settings look suspicious.
  Follow further actions done by the account.

16.25 | A Google Workspace identity performed an unusual admin console activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	- Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A Google Workspace identity performed an admin console activity for the first time.

Attacker's Goals

To do.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if the changes that were made look suspicious.

  Follow further actions done by the account.

Variations

A non-administrative Google Workspace identity performed an unusual admin console activity

Synopsis

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

Description

A Google Workspace identity performed an admin console activity for the first time.

Attacker's Goals

To do.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

  Check if the changes that were made look suspicious.
  Follow further actions done by the account.

16.26 | Gmail delegation was turned on for the organization

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Domain or Tenant Policy Modification (T1484)
Severity	Informational

Description

A Google Workspace admin turned on Gmail delegation for all the organization's users.

Attacker's Goals

Email Collection.

Investigative actions

- Check if the identity intended to perform this action, Or look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check if any user in the organization granted other users access to their mail inbox.
  Follow further actions done by the account.

16.27 | A third-party application was authorized to access the Google Workspace APIs

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	- Requires: - Google Workspace Audit Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Privilege Escalation (TA0004)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A domain administrator authorized a third-party application to access the Google Workspace APIs. This allows the application to interact with the domain user's data within the authorized scope, as specified in the API call.

Attacker's Goals

Gain access to Google Workspace data and services. Collect confidential information from Google Workspace. Compromise user accounts and data.

Investigative actions

- Check which account was granted access to the Domain API.
  Identify the source IP address of the request.
  Verify the legitimacy of the request.

16.28 | 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.

16.29 | 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.

16.30 | 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.

17 | Google Workspace Authentication

17.1 | 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.

17.2 | 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.

17.3 | 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.

17.4 | 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.

18 | Health Monitoring Data

18.1 | Collection error

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Health Monitoring Data
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)

ATT&CK Technique	▮ Remote Services (T1021) ▮ System Services: Service Execution (T1569.002)
Severity	High

Description

A collection error was detected.

Attacker's Goals

N/A.

Investigative actions

N/A.

18.2 ▮ Parsing Rule Error

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	Requires: - Health Monitoring Data

Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) System Services: Service Execution (T1569.002)
Severity	Medium

Description

A Parsing Rule error was detected.

Attacker's Goals

N/A.

Investigative actions

N/A.

18.3 | Error in event forwarding

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	4 Hours
Required Data	Requires: - Health Monitoring Data
Detection Modules	
Detector Tags	
ATT&CK Tactic	▮ Lateral Movement (TA0008) ▮ Execution (TA0002)
ATT&CK Technique	▮ Remote Services (T1021) ▮ System Services: Service Execution (T1569.002)
Severity	Medium

Description

An error was detected in event forwarding.

Attacker's Goals

N/A.

Investigative actions

N/A.

18.4 | Correlation rule error

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	12 Hours
Required Data	Requires: - Health Monitoring Data
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	- Remote Services (T1021) System Services: Service Execution (T1569.002)
Severity	Medium

Description

An error was identified while running a correlation rule.

Attacker's Goals

N/A.

Investigative actions

N/A.

18.5 | Logs were not collected from a data source for an abnormally long time

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	6 Hours
Required Data	Requires: - Health Monitoring Data
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)

Severity	Low

Description

Logs were not collected from a data source for an abnormally long time.

Attacker's Goals

N/A.

Investigative actions

N/A.

19 | Office 365 Audit

19.1 | Exchange user mailbox forwarding

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: - Office 365 Audit
Detection Modules	Identity Threat Module

Detector Tags	
ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Low

Description

A user configured Exchange SMTP forwarding on a mailbox, which forwards all emails sent to that mailbox to a specified recipient.

Attacker's Goals

Leverage a compromised user account to modify a mailbox's settings to forward emails to an external recipient and collect sensitive information.

Investigative actions

- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the forwarding domain is an unknown external domain.
  Investigate the IP address associated with the rule.
- Follow further actions done by the account.

Variations

Exchange user mailbox forwarding by a delegate user

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)

ATT&CK Technique	▪ Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Informational

Description

A user configured Exchange SMTP forwarding on a mailbox, which forwards all emails sent to that mailbox to a specified recipient. The user who set the forwarding is a delegated user, who performed this action on behalf of another user.

Attacker's Goals

Leverage a compromised user account to modify a mailbox's settings to forward emails to an external recipient and collect sensitive information.

Investigative actions

- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the forwarding domain is an unknown external domain.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.

Suspicious Exchange user mailbox forwarding

Synopsis

ATT&CK Tactic	Collection (TA0009) ▪ Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) ▪ Automated Exfiltration (T1020) ▪ Email Collection (T1114)
Severity	Medium

Description

A user configured Exchange SMTP forwarding on a mailbox, which forwards all emails sent to that mailbox to a specified recipient.

Attacker's Goals

Leverage a compromised user account to modify a mailbox's settings to forward emails to an external recipient and collect sensitive information.

Investigative actions

- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the forwarding domain is an unknown external domain.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.

19.2 | Exchange inbox forwarding rule configured

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module

Detector Tags	
ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Informational

Description

A user configured an Exchange inbox forwarding rule, which forwards emails that meet specific conditions.

Attacker's Goals

Create an inbox rule using a compromised user account to automatically forward emails containing specific conditions to an external recipient.

Investigative actions

- Check what conditions are met in the inbox rule (e.g. specific keywords in the subject or body).
  Determine if any of the conditions and keywords look suspicious.

  Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
- Check if the forwarding domain is an unknown external domain and look up its reputation.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.

  Check for a possible phishing campaign on the organization.
- Look for emails sent to this recipient by other users.

Variations

Exchange inbox forwarding rule configured by a delegate user

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Informational

Description

A user configured an Exchange inbox forwarding rule, which forwards emails that meet specific conditions. The user who set the forwarding is a delegated user, who performed this action on behalf of another user.

Attacker's Goals

Create an inbox rule using a compromised user account to automatically forward emails containing specific conditions to an external recipient.

Investigative actions

Check what conditions are met in the inbox rule (e.g. specific keywords in the subject or body).

Determine if any of the conditions and keywords look suspicious.

- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the forwarding domain is an unknown external domain and look up its reputation.
  Investigate the IP address associated with the rule.

Follow further actions done by the account.

- Check for a possible phishing campaign on the organization.
- Look for emails sent to this recipient by other users.

Suspicious Exchange inbox forwarding rule configured

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)

Severity	Medium

Description

A user configured an Exchange inbox forwarding rule, which forwards emails that meet specific conditions.

Attacker's Goals

Create an inbox rule using a compromised user account to automatically forward emails containing specific conditions to an external recipient.

Investigative actions

- Check what conditions are met in the inbox rule (e.g. specific keywords in the subject or body).
  Determine if any of the conditions and keywords look suspicious.

  Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
- Check if the forwarding domain is an unknown external domain and look up its reputation.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.

  Check for a possible phishing campaign on the organization.
- Look for emails sent to this recipient by other users.

External Exchange inbox forwarding rule configured

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Low

Description

A user configured an Exchange inbox forwarding rule, which forwards emails that meet specific conditions. The rule forwards emails to a public domain, which may be a sign of compromise.

Attacker's Goals

Create an inbox rule using a compromised user account to automatically forward emails containing specific conditions to an external recipient.

Investigative actions

- Check what conditions are met in the inbox rule (e.g. specific keywords in the subject or body).
  Determine if any of the conditions and keywords look suspicious.

  Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
- Check if the forwarding domain is an unknown external domain and look up its reputation.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.

  Check for a possible phishing campaign on the organization.
- Look for emails sent to this recipient by other users.

19.3 | Exchange email-hiding transport rule

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: • Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Email Hiding Rules (T1564.008)
Severity	Informational

Description

A user configured an Exchange transport rule that may be used to hide emails in the organization.

Attacker's Goals

Prevent an organization from warning users that they've been compromised (e.g. an internal spear-phishing campaign).

Investigative actions

- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the rule contains keywords and if they look suspicious.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.
- Check for a possible phishing campaign on the organization.
- Look for multiple instances of email hiding, which may be an indication of a larger campaign.
  Check if the user regularly configures transport rules.

Variations

Suspicious Exchange email-hiding transport rule

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Email Hiding Rules (T1564.008)
Severity	Medium

Description

A user configured an Exchange transport rule that may be used to hide emails in the organization.

The rule hides emails that contain suspicious keywords, which may be a sign of a compromised account.

Attacker's Goals

Prevent an organization from warning users that they've been compromised (e.g. an internal spear-phishing campaign).

Investigative actions

Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

- Check if the rule contains keywords and if they look suspicious.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.

  Check for a possible phishing campaign on the organization.
- Look for multiple instances of email hiding, which may be an indication of a larger campaign.
  Check if the user regularly configures transport rules.

Exchange email-hiding transport rule based on message keywords

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Email Hiding Rules (T1564.008)
Severity	Low

Description

A user configured an Exchange transport rule that may be used to hide emails in the organization. The rule hides emails that contain certain keywords, which may be a sign of a compromised account.

Attacker's Goals

Prevent an organization from warning users that they've been compromised (e.g. an internal spear-phishing campaign).

Investigative actions

Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

- Check if the rule contains keywords and if they look suspicious.
- Investigate the IP address associated with the rule.
  Follow further actions done by the account.

  Check for a possible phishing campaign on the organization.
  Look for multiple instances of email hiding, which may be an indication of a larger campaign.
  Check if the user regularly configures transport rules.

19.4 | User accessed SaaS resource via anonymous link

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: - 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 accessed a SaaS resource via an anonymous link.

Attacker's Goals

An attacker is attempting to collect sensitive data.

Investigative actions

- Check the IP address from which the access originated.
- Examine the file that was accessed for any sensitive indicators. Follow further actions taken, such as downloading files.

Variations

External user accessed a sensitive SaaS file via anonymous link

Synopsis

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

Description

An external user accessed a sensitive SaaS file via an anonymous link.

Attacker's Goals

An attacker is attempting to collect sensitive data.

Investigative actions

- Check the IP address from which the access originated.
- Examine the file that was accessed for any sensitive indicators. Follow further actions taken, such as downloading files.

User accessed a public Google Drive document

Synopsis

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

Description

A user accessed a Google Drive document that is public on the web.

Attacker's Goals

An attacker is attempting to collect sensitive data.

Investigative actions

- Check the IP address from which the access originated.
  Examine the file that was accessed for any sensitive indicators.
  Follow further actions taken, such as downloading files.

19.5 | SharePoint Site Collection admin group addition

Synopsis

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

Required Data	▮ Requires: ▯ Office 365 Audit
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

A user made an addition to the site collection administrators group in SharePoint.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

Check the IP address from which the access originated.

- Verify the activity with the performing user.
- Follow further actions done by the account.

Variations

SharePoint site collection admin added to personal site

Synopsis

ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Account Manipulation: Additional Cloud Roles (T1098.003)
Severity	Informational

Description

A user was added as a site collection admin to a personal site, indicating that the user has accessed the SharePoint service for the first time.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

- Check the IP address from which the access originated.
  Verify the activity with the performing user.
  Follow further actions done by the account.

Abnormal SharePoint Site Collection admin group addition

Synopsis

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

Description

A user made an addition to the site collection administrators group in SharePoint. This user has not made any SharePoint site admin additions over the past 30 days.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

Check the IP address from which the access originated.
- Verify the activity with the performing user.
- Follow further actions done by the account.

19.6 | Exchange audit log disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
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 user disabled the Exchange audit log. This may indicate an attempt to evade detection.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Follow further actions done by the account.
  Verify that the configuration change was expected.
  Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

19.7 | Exchange Safe Link policy disabled or removed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	

ATT&CK Tactic	▮ Defense Evasion (TA0005) Initial Access (TA0001)
ATT&CK Technique	▮ Impair Defenses: Disable or Modify Tools (T1562.001) ▮ Phishing: Spearphishing Link (T1566.002)
Severity	Low

Description

A user disabled an Exchange Safe Link policy, which provides phishing protection to emails that contain hyperlinks.

Attacker's Goals

An attacker is attempting to bypass security measures associated with hyperlinks in email messages.

Investigative actions

- Follow further actions done by the account.
  Verify that the configuration change was expected.
  Look for email messages received with hyperlinks.
  Check for a possible phishing campaign on the organization.

19.8 | Exchange DKIM signing configuration disabled

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: ▯ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	▮ Defense Evasion (TA0005) Initial Access (TA0001)
ATT&CK Technique	▮ Impair Defenses: Disable or Modify Tools (T1562.001) Phishing (T1566)
Severity	Low

Description

A user disabled an Exchange DomainKeys Identified Mail (DKIM) signing configuration. DKIM helps ensure that emails are authorized and not spoofed.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Follow further actions done by the account.
  Verify that the configuration change was expected.
  Check for a possible phishing campaign on the organization.

Variations

A recently configured Exchange DKIM signing configuration was disabled

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Initial Access (TA0001)
ATT&CK Technique	Impair Defenses: Disable or Modify Tools (T1562.001) Phishing (T1566)
Severity	Informational

Description

A user disabled an Exchange DomainKeys Identified Mail (DKIM) signing configuration. DKIM helps ensure that emails are authorized and not spoofed.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

Follow further actions done by the account.

- Verify that the configuration change was expected.
- Check for a possible phishing campaign on the organization.

19.9 | Penetration testing tool activity attempt

Synopsis

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

Deduplication Period	2 Days
Required Data	Requires: ▯ Office 365 Audit
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Serverless Execution (T1648)
Severity	Informational

Description

A SaaS API was invoked by a penetration testing tool.

Attacker's Goals

Usage of known tools and frameworks.

Investigative actions

Check if there is an active PT test ongoing.

Variations

Penetration testing tool activity attempt

Synopsis

ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	Serverless Execution (T1648)
Severity	Medium

Description

A SaaS API was successfully invoked by a penetration testing tool.

Attacker's Goals

Usage of known tools and frameworks.

Investigative actions

Check if there is an active PT test ongoing.

19.10 | 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.

19.11 | Exchange email-hiding inbox rule

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: ▯ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Email Hiding Rules (T1564.008)
Severity	Informational

Description

A user configured an Exchange inbox rule that may be used to hide emails.

Attacker's Goals

Prevent an organization from warning users that they've been compromised (e.g. an internal spear-phishing campaign).

Investigative actions

Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

Check if the rule keywords look suspicious.

- Investigate the IP address associated with the rule.
- Follow further actions done by the account.
  Check for a possible phishing campaign on the organization.
  Look for multiple instances of email hiding, which may be an indication of a larger campaign.
- Check if the user regularly configures inbox rules.

Variations

Possible BEC Exchange email-hiding inbox rule

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Email Hiding Rules (T1564.008)
Severity	Medium

Description

A user configured an Exchange inbox rule that may be used to hide emails. The rule contains characteristics that resemble a business email compromise (BEC) attack.

Attacker's Goals

Prevent an organization from warning users that they've been compromised (e.g. an internal spear-phishing campaign).

Investigative actions

Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
Check if the rule keywords look suspicious.

- Investigate the IP address associated with the rule.
- Follow further actions done by the account.
  Check for a possible phishing campaign on the organization.

  Look for multiple instances of email hiding, which may be an indication of a larger campaign.
- Check if the user regularly configures inbox rules.

Suspicious Exchange email-hiding inbox rule

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Email Hiding Rules (T1564.008)
Severity	Medium

Description

A user configured an Exchange inbox rule that may be used to hide emails. The rule hides emails that contain suspicious keywords, which may be a sign of a compromised account.

Attacker's Goals

Prevent an organization from warning users that they've been compromised (e.g. an internal spear-phishing campaign).

Investigative actions

Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

- Check if the rule keywords look suspicious.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.

  Check for a possible phishing campaign on the organization.
- Look for multiple instances of email hiding, which may be an indication of a larger campaign.
  Check if the user regularly configures inbox rules.

19.12 | SaaS suspicious external domain user 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: - Google Workspace Audit Logs OR - Office 365 Audit
Detection Modules	Identity Threat Module
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 identity activity in the organization.

Variations

Suspicious external user activity detected from a domain first seen in the organization

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, both in cloud and SaaS environments.

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 identity activity in the organization.

19.13 | Exchange transport forwarding rule configured

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	- Collection (TA0009) Exfiltration (TA0010)

ATT&CK Technique	▪ Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Low

Description

A user configured an Exchange transport (mail flow) forwarding rule, which is applied to all emails that match certain conditions in the organization.

Attacker's Goals

Forward all emails in the organization that match specific criteria to an external recipient to collect sensitive information.

Investigative actions

Check what mailboxes are affected by the transport rule.
Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

- Check if the forwarding domain is an unknown external domain and look up its reputation.
- Investigate the IP address associated with the rule.
  Follow further actions done by the account.
  Check for a possible phishing campaign on the organization.

  Look for emails sent to this recipient by other users.

Variations

Exchange transport forwarding rule configured by a delegate user

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) ▪ Email Collection (T1114)

Severity	Informational

Description

A user configured an Exchange transport (mail flow) forwarding rule, which is applied to all emails that match certain conditions in the organization. The user who set the forwarding is a delegated user, who performed this action on behalf of another user.

Attacker's Goals

Forward all emails in the organization that match specific criteria to an external recipient to collect sensitive information.

Investigative actions

- Check what mailboxes are affected by the transport rule.
- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the forwarding domain is an unknown external domain and look up its reputation.
  Investigate the IP address associated with the rule.
  Follow further actions done by the account.
- Check for a possible phishing campaign on the organization.
- Look for emails sent to this recipient by other users.

Suspicious Exchange transport forwarding rule configured

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	- Email Collection: Email Forwarding Rule (T1114.003) Automated Exfiltration (T1020) Email Collection (T1114)
Severity	Medium

Description

A user configured an Exchange transport (mail flow) forwarding rule, which is applied to all emails that match certain conditions in the organization.

Attacker's Goals

Forward all emails in the organization that match specific criteria to an external recipient to collect sensitive information.

Investigative actions

- Check what mailboxes are affected by the transport rule.
- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Check if the forwarding domain is an unknown external domain and look up its reputation.
  Investigate the IP address associated with the rule.
- Follow further actions done by the account.
- Check for a possible phishing campaign on the organization.
- Look for emails sent to this recipient by other users.

19.14 | DLP sensitive data exposed to external users

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit

Detection Modules	Identity Threat Module
Detector Tags	O365 DLP Analytics
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Information Repositories: Sharepoint (T1213.002) Data from Information Repositories (T1213)
Severity	Informational

Description

A user triggered an O365 DLP rule match on data that is viewable by external users. This may indicate an attacker's attempt to access sensitive information.

Attacker's Goals

An attacker is attempting to access sensitive information.

Investigative actions

- Review the details of the triggered DLP rule match.
  Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

  Follow further actions done by the account.
- Communicate with the user to verify the legitimacy of the triggered event.

Variations

High-severity DLP sensitive data exposed to external users

Synopsis

ATT&CK Tactic	Collection (TA0009)

ATT&CK Technique	▮ Data from Information Repositories: Sharepoint (T1213.002) ▮ Data from Information Repositories (T1213)
Severity	Low

Description

A user triggered an O365 DLP rule match on data that is viewable by external users. This may indicate an attacker's attempt to access sensitive information.

Attacker's Goals

An attacker is attempting to access sensitive information.

Investigative actions

Review the details of the triggered DLP rule match.
Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

- Follow further actions done by the account.
- Communicate with the user to verify the legitimacy of the triggered event.

19.15 | Exchange anti-phish policy disabled or removed

Synopsis

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

Required Data	▮ Requires: ▁ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005) Initial Access (TA0001)
ATT&CK Technique	Impair Defenses: Disable or Modify Tools (T1562.001) Phishing (T1566)
Severity	Low

Description

A user disabled or removed an Exchange anti-phish policy, which may indicate evasion of a possible phishing campaign.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

Follow further actions done by the account.
Verify that the configuration change was expected.

Check for a possible phishing campaign on the organization.

Variations

Recently configured Exchange anti-phish policy disabled or removed

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Initial Access (TA0001)
ATT&CK Technique	Impair Defenses: Disable or Modify Tools (T1562.001) Phishing (T1566)
Severity	Informational

Description

A user disabled or removed an Exchange anti-phish policy, which may indicate evasion of a possible phishing campaign.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

Follow further actions done by the account.

- Verify that the configuration change was expected.
- Check for a possible phishing campaign on the organization.

19.16 | Rare DLP rule match by user

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: ▯ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	O365 DLP Analytics
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	▮ Data from Information Repositories: Sharepoint (T1213.002) ▮ Data from Information Repositories (T1213)
Severity	Informational

Description

A user triggered an O365 DLP rule match, which may indicate an attacker's attempt to access sensitive information.

Attacker's Goals

An attacker is attempting to access sensitive information.

Investigative actions

- Review the details of the triggered DLP rule match.
  Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Follow further actions done by the account.
  Communicate with the user to verify the legitimacy of the triggered event.

Variations

DLP rule match by user for the first time

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Information Repositories: Sharepoint (T1213.002) Data from Information Repositories (T1213)
Severity	Low

Description

A user triggered an O365 DLP rule match, which may indicate an attacker's attempt to access sensitive information.

Attacker's Goals

An attacker is attempting to access sensitive information.

Investigative actions

Review the details of the triggered DLP rule match.

Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

- Follow further actions done by the account.
  Communicate with the user to verify the legitimacy of the triggered event.

19.17 | Exchange mailbox folder permission modification

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Email Delegate Permissions (T1098.002)
Severity	Informational

Description

A user modified permissions to an Exchange mailbox folder.

Attacker's Goals

An attacker may add permissions to a mailbox folder for persistence reasons. For instance, an attacker may assign the Default or Anonymous user permissions. This will allow them to maintain persistent access to the mailbox folder, which may lead to exfiltration of the messages.

Investigative actions

Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).

- Investigate the IP address associated with the activity.
  Follow further actions done by the account.
  Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).

  Check for abnormal Azure AD non-interactive logins by the user.
- Monitor for changes that may indicate excessively broad permissions.

Variations

Exchange mailbox folder permission modification for a default user

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Email Delegate Permissions (T1098.002)
Severity	Low

Description

A user modified permissions to an Exchange mailbox folder. The user granted the permission is a default user, which effectively grants the permission to any user.

Attacker's Goals

An attacker may add permissions to a mailbox folder for persistence reasons. For instance, an attacker may assign the Default or Anonymous user permissions. This will allow them to maintain persistent access to the mailbox folder, which may lead to exfiltration of the messages.

Investigative actions

- Look for signs that the user account and mailbox are compromised (e.g. abnormal logins, unusual activity).
  Investigate the IP address associated with the activity.

  Follow further actions done by the account.
- Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).
- Check for abnormal Azure AD non-interactive logins by the user.
  Monitor for changes that may indicate excessively broad permissions.

19.18 | Exchange Safe Attachment policy disabled or removed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	❙ Defense Evasion (TA0005) ❙ Initial Access (TA0001)
ATT&CK Technique	❙ Impair Defenses: Disable or Modify Tools (T1562.001) ❙ Phishing: Spearphishing Attachment (T1566.001)
Severity	Low

Description

A user disabled an Exchange Safe Attachment policy, which provides phishing protection to email attachments.

Attacker's Goals

An attacker may attempt to disable the Safe Attachment policy to evade detection.

Investigative actions

Follow further actions done by the account.
Verify that the configuration change was expected.

Check for a possible phishing campaign on the organization.

19.19 | Exchange malware filter policy removed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562) Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Low

Description

A user removed an Exchange malware filter policy, which may prevent the detection of malware.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

Follow further actions done by the account.

Verify that the configuration change was expected.
Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
Investigate if any other security policies have been changed or removed.
Monitor for signs of malware in future messages.

19.20 | Exchange compliance search created

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: ▯ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Email Collection (T1114)
Severity	Informational

Description

A user created an Exchange compliance search. This feature enables Administrators to search mailboxes in an organization.

Attacker's Goals

An attacker is searching mailboxes to access sensitive information.

Investigative actions

Follow further actions done by the account.
Check to see if the search contained sensitive information.

- Check if any data was exfiltrated after the search.
- Look for suspicious search terms.

Variations

Suspicious Exchange compliance search created

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Email Collection (T1114)
Severity	Low

Description

A user created an Exchange compliance search. This feature enables Administrators to search mailboxes in an organization. The query contains potentially suspicious keywords, which could indicate an attempt of sensitive data collection.

Attacker's Goals

An attacker is searching mailboxes to access sensitive information.

Investigative actions

Follow further actions done by the account.

Check to see if the search contained sensitive information.

- Check if any data was exfiltrated after the search.
- Look for suspicious search terms.

Exchange compliance search created for the first time

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Email Collection (T1114)
Severity	Low

Description

A user created an Exchange compliance search. This feature enables Administrators to search mailboxes in an organization.

Attacker's Goals

An attacker is searching mailboxes to access sensitive information.

Investigative actions

Follow further actions done by the account.

- Check to see if the search contained sensitive information.
- Check if any data was exfiltrated after the search.
- Look for suspicious search terms.

19.21 | Exchange mailbox audit bypass

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562) Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Low

Description

A user added mailbox audit bypass for an account. This will allow the account to perform actions without being logged, and may indicate an attempt to evade detection.

Attacker's Goals

An attacker may abuse the audit bypass mechanism to conceal actions and evade detection.

Investigative actions

- Follow further actions done by the account.
- Verify that the configuration change was expected.

19.22 | Microsoft 365 DLP policy disabled or removed

Synopsis

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

Required Data	▮ Requires: ▮ Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	▮ Impair Defenses (T1562) Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Informational

Description

A user disabled or removed a Microsoft 365 data loss prevention (DLP) policy, which may indicate DLP monitoring evasion.

Attacker's Goals

An attacker is attempting to bypass Microsoft 365 Data Loss Prevention (DLP) policies.

Investigative actions

- Follow further actions done by the account.
  Verify that the configuration change was expected.
  Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Monitor the user's activity for any access to sensitive data or data exfiltration.
- Investigate if any other security policies have been changed or removed.

Variations

Rare Microsoft 365 DLP policy removal

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562) Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Low

Description

A user disabled or removed a Microsoft 365 data loss prevention (DLP) policy, which may indicate DLP monitoring evasion.

Attacker's Goals

An attacker is attempting to bypass Microsoft 365 Data Loss Prevention (DLP) policies.

Investigative actions

- Follow further actions done by the account.
- Verify that the configuration change was expected.
- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Monitor the user's activity for any access to sensitive data or data exfiltration.
- Investigate if any other security policies have been changed or removed.

19.23 | 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.

19.24 | 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.

19.25 | User moved Exchange sent messages to deleted items

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Indicator Removal: Clear Mailbox Data (T1070.008)
Severity	Informational

Description

A user moved sent messages to deleted items in Exchange.

Attacker's Goals

An attacker is attempting to hide newly sent email messages for evasion purposes.

Investigative actions

Look for signs that the user account and mailboxes are compromised (e.g. abnormal logins, unusual activity).

- Investigate the IP address associated with the activity.
  Follow further actions done by the account.
  Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).

  Examine the user's email activity history for suspicious behavior.

Variations

Sensitive Exchange sent messages moved to deleted items from unusual source

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Indicator Removal: Clear Mailbox Data (T1070.008)
Severity	Low

Description

A user moved sensitive sent messages to deleted items in Exchange.

Attacker's Goals

An attacker is attempting to hide newly sent email messages for evasion purposes.

Investigative actions

- Look for signs that the user account and mailboxes are compromised (e.g. abnormal logins, unusual activity).
  Investigate the IP address associated with the activity.

  Follow further actions done by the account.
- Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).
- Examine the user's email activity history for suspicious behavior.

19.26 | 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.

19.27 | Sensitive Exchange mail sent to external users

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module

Detector Tags	O365 DLP Analytics
ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection (T1114) Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

A user sent sensitive email messages to external users.

Attacker's Goals

An attacker is attempting to collect sensitive email information.

Investigative actions

Look for signs that the user account and mailboxes are compromised (e.g. abnormal logins, unusual activity).

- Follow further actions done by the account.
- Look for unusual email patterns from the affected mailbox (e.g. unusual email contents). Examine the user's email activity history for suspicious behavior.

Variations

Exchange mail to external account matching high severity DLP rules

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Email Collection (T1114) Exfiltration Over Alternative Protocol (T1048)

Severity	Low

Description

A user sent sensitive email messages to external users.

Attacker's Goals

An attacker is attempting to collect sensitive email information.

Investigative actions

- Look for signs that the user account and mailboxes are compromised (e.g. abnormal logins, unusual activity).
  Follow further actions done by the account.

  Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).
- Examine the user's email activity history for suspicious behavior.

Sensitive Exchange mail sent to an external user

Synopsis

ATT&CK Tactic	- Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	- Email Collection (T1114) - Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

A user sent sensitive email messages to external users.

Attacker's Goals

An attacker is attempting to collect sensitive email information.

Investigative actions

Look for signs that the user account and mailboxes are compromised (e.g. abnormal logins, unusual activity).

- Follow further actions done by the account.
  Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).
  Examine the user's email activity history for suspicious behavior.

19.28 | A user uploaded malware to SharePoint or OneDrive

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Hours
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	- Lateral Movement (TA0008) - Execution (TA0002)
ATT&CK Technique	- Taint Shared Content (T1080) - User Execution: Malicious File (T1204.002)

Severity	Low

Description

A user uploaded a file that was classified as malware to SharePoint or OneDrive.

Attacker's Goals

An attacker may upload malware to a shared location to gain execution and move laterally.

Investigative actions

- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Check the file that was uploaded for any malicious indicators.
- Follow further actions done by the account.

Variations

A user uploaded malware to SharePoint or OneDrive with suspicious characteristics

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Taint Shared Content (T1080) User Execution: Malicious File (T1204.002)
Severity	Medium

Description

A user uploaded a file that was classified as malware to SharePoint or OneDrive with some additional suspicious characteristics.

Attacker's Goals

An attacker may upload malware to a shared location to gain execution and move laterally.

Investigative actions

- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check the file that was uploaded for any malicious indicators.

  Follow further actions done by the account.

A user uploaded a malicious payload to SharePoint or OneDrive

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) - Execution (TA0002)
ATT&CK Technique	Taint Shared Content (T1080) - User Execution: Malicious File (T1204.002)
Severity	Informational

Description

A user uploaded a file that was classified as malware to SharePoint or OneDrive. The file was labelled as malicious by Microsoft's file scanning engine.

Attacker's Goals

An attacker may upload malware to a shared location to gain execution and move laterally.

Investigative actions

- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Check the file that was uploaded for any malicious indicators.
  Follow further actions done by the account.

19.29 | Exchange mailbox delegation permissions added

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	4 Hours
Deduplication Period	1 Day
Required Data	Requires: Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Email Delegate Permissions (T1098.002)
Severity	Informational

Description

A user added delegation permissions to an Exchange mailbox.

Attacker's Goals

Add delegation permissions to a mailbox for persistence reasons.

Investigative actions

- Look for signs that the user account and mailboxes are compromised (e.g. abnormal logins, unusual activity).
  Investigate the IP address associated with the activity.

  Follow further actions done by the account.
  Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).

Variations

Addition of Exchange mailbox delegation permissions with suspicious characteristics

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: Additional Email Delegate Permissions (T1098.002)
Severity	Low

Description

A user added delegation permissions to an Exchange mailbox.

Attacker's Goals

Add delegation permissions to a mailbox for persistence reasons.

Investigative actions

Look for signs that the user account and mailboxes are compromised (e.g. abnormal logins, unusual activity).

- Investigate the IP address associated with the activity.
- Follow further actions done by the account.
  Look for unusual email patterns from the affected mailbox (e.g. unusual email contents).

19.30 | User accessed multiple O365 AIP sensitive files

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - Office 365 Audit
Detection Modules	Identity Threat Module
Detector Tags	O365 DLP Analytics
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213) ▮ Data from Local System (T1005)
Severity	Informational

Description

A user accessed multiple O365 AIP sensitive files.

Attacker's Goals

An attacker is attempting to collect sensitive information.

Investigative actions

Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
Follow further actions done by the account.
Check what sensitivity labels are detected and how suspicious they are.

Examine the user's account history for suspicious behavior.

20 | Okta

20.1 | 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.

20.2 | 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 T 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.

20.3 | 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.

20.4 | 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) ı 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.

20.5 | Suspicious SSO authentication

Synopsis

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

Description

A suspicious SSO authentication was made by a user.

Attacker's Goals

Achieve initial access to a company's resources.

Investigative actions

See whether this was a legitimate action.

- Review the external IP/domain involved in the alert.
  Contact the user whose account is being accessed and verify that they are actually attempting to log in.

  Check if the login attempt is coming from an unfamiliar location or device.
- Look for unusual login patterns, such as login attempts at odd hours.
- Monitor the user's account for further unusual activity.

Variations

Successful SSO authentication with suspicious characteristics

Synopsis

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

Description

A user successfully accessed SSO with some suspicious characteristics that flagged this login attempt as a suspicious login.

Attacker's Goals

Achieve initial access to a company's resources.

Investigative actions

See whether this was a legitimate action.

- Review the external IP/domain involved in the alert.
- Contact the user whose account is being accessed and verify that they are actually attempting to log in.
  Check if the login attempt is coming from an unfamiliar location or device.

  Look for unusual login patterns, such as login attempts at odd hours.
- Monitor the user's account for further unusual activity.

SSO authentication attempt with suspicious characteristics

Synopsis

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

Description

A user accessed SSO with some suspicious characteristics that flagged this login attempt as a suspicious login.

Attacker's Goals

Achieve initial access to a company's resources.

Investigative actions

See whether this was a legitimate action.

Review the external IP/domain involved in the alert.
Contact the user whose account is being accessed and verify that they are actually attempting to log in.
Check if the login attempt is coming from an unfamiliar location or device.
Look for unusual login patterns, such as login attempts at odd hours.

Monitor the user's account for further unusual activity.

20.6 | 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.

20.7 | 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.

20.8 | 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.

20.9 | 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.

20.10 | 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.

20.11 | 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.

20.12 | 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.

20.13 | 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.

20.14 | 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.

20.15 | 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.

20.16 | 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.

20.17 | 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.

20.18 | 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.

20.19 | 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.

20.20 | 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.

20.21 | A user rejected an SSO request from an unusual country

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: ▯ Okta
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

A user rejected an SSO authentication request from an abnormal country.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- ! Verify the reject cause of the MFA attempts.
- ▮ Check to see if the user has successfully authenticated around the time of the alert, and confirm it's a legitimate login.
  Verify the authentication attempt from the rare country is benign.

20.22 | 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.

20.23 | 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.

20.24 | Multiple SSO MFA attempts were rejected by a user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: ▯ Okta
Detection Modules	Identity Analytics

Detector Tags	
ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Compromise Accounts (T1586) Multi-Factor Authentication Request Generation (T1621)
Severity	Informational

Description

Multiple SSO MFA attempts were rejected by a user. This may indicate an MFA request flooding attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

Verify the reasoning behind the MFA request rejections.
Follow further actions performed by the user.
Verify any successful authentication by the user.

Variations

User rejected numerous SSO MFA attempts

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Compromise Accounts (T1586) Multi-Factor Authentication Request Generation (T1621)

Severity	Medium

Description

A user rejected numerous SSO MFA attempts, which may indicate an MFA flooding attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Verify the reasoning behind the MFA request rejections.
  Follow further actions performed by the user.
  Verify any successful authentication by the user.

Multiple SSO MFA attempts were rejected by a user with suspicious characteristics

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Compromise Accounts (T1586) Multi-Factor Authentication Request Generation (T1621)
Severity	Low

Description

A user rejected multiple SSO MFA attempts with suspicious characteristics.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

Verify the reasoning behind the MFA request rejections.
Follow further actions performed by the user.
- Verify any successful authentication by the user.

21 | Okta Audit Log

21.1 | Okta account unlock by admin

Synopsis

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

Description

An administrative user unlocked an Okta account.

Attacker's Goals

The attacker's goal is to gain unauthorized access to sensitive information or resources and to gain control over the locked account.

Investigative actions

- Monitor the user account for indications of compromise, such as irregular login patterns or atypical activities.

  Investigate abnormal logins, reported suspicious activities, new processes run, and recent configuration changes for any indicators of potential compromise.
- Examine the user's actions preceding and following the activation of the alert.
- Initiate contact with the user to verify the authenticity of the account unlock action. Check account the user successfully authenticated after the event.

  Continue monitoring the account for any subsequent actions that may indicate suspicious behavior.

Variations

Suspicious Okta account unlock by admin

Synopsis

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

Description

An administrative user unlocked an Okta account.

Attacker's Goals

The attacker's goal is to gain unauthorized access to sensitive information or resources and to gain control over the locked account.

Investigative actions

Monitor the user account for indications of compromise, such as irregular login patterns or atypical activities.

- Investigate abnormal logins, reported suspicious activities, new processes run, and recent configuration changes for any indicators of potential compromise.
  Examine the user's actions preceding and following the activation of the alert.

  Initiate contact with the user to verify the authenticity of the account unlock action.
- Check account the user successfully authenticated after the event.
- Continue monitoring the account for any subsequent actions that may indicate suspicious behavior.

21.2 | Okta User Session Impersonation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)

Severity	Informational

Description

A user has initiated a session impersonation in Okta.

Attacker's Goals

An attacker's goal is to gain unauthorized access to sensitive information or perform malicious actions on behalf of the impersonated user.

Investigative actions

- Ensure the user is authorized to impersonate a user session.
- Review any activities that occurred during the impersonation session.
  Look for any activities related to the impersonated user's account during and after the impersonation event.

Variations

Okta User Session Impersonation with suspicious characteristics

Synopsis

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

Description

A user has initiated a session impersonation with suspicious characteristics in Okta.

Attacker's Goals

An attacker's goal is to gain unauthorized access to sensitive information or perform malicious actions on behalf of the impersonated user.

Investigative actions

- Ensure the user is authorized to impersonate a user session.
  Review any activities that occurred during the impersonation session.
  Look for any activities related to the impersonated user's account during and after the impersonation event.

21.3 | A user modified an Okta policy rule

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	- Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	- Impair Defenses (T1562) - Domain or Tenant Policy Modification (T1484) Modify Authentication Process (T1556)

Severity	Informational

Description

An Okta policy rule was modified by a user, suggesting a potential compromise of the account.

Attacker's Goals

An attacker may attempt to modify an Okta policy rule to weaken an organization's security controls.

Investigative actions

- Follow further actions done by the account.
- Verify that the configuration change was expected.
  Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

  Investigate if any other security policies have been changed or removed.

Variations

A user modified an Okta policy rule with suspicious characteristics

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	Impair Defenses (T1562) Domain or Tenant Policy Modification (T1484) Modify Authentication Process (T1556)
Severity	Low

Description

An Okta policy rule was modified by a suspicious user, suggesting a potential compromise of the account.

Attacker's Goals

An attacker may attempt to modify an Okta policy rule to weaken an organization's security controls.

Investigative actions

Follow further actions done by the account.
Verify that the configuration change was expected.

- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Investigate if any other security policies have been changed or removed.

21.4 | A user attempted to bypass Okta MFA

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	▪ Modify Authentication Process (T1556) Multi-Factor Authentication Request Generation (T1621)
Severity	Low

Description

A user may have attempted to bypass Okta MFA.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Contact the user who attempted to bypass MFA and ensure the request was legitimate.
- Check if the user successfully authenticated after the event.

Variations

A successful bypass of Okta MFA

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Modify Authentication Process (T1556) Multi-Factor Authentication Request Generation (T1621)
Severity	Low

Description

Suspicious MFA bypass attempt in Okta.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Contact the user who attempted to bypass MFA and ensure the request was legitimate. Check if the user successfully authenticated after the event.

21.5 | A user modified an Okta network zone

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	- Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses (T1562) Impair Defenses: Disable or Modify Cloud Firewall (T1562.007)
Severity	Informational

Description

An Okta network zone was modified by a user.

Attacker's Goals

An attacker may attempt to modify an Okta network zone to weaken an organization's security controls.

Investigative actions

Follow further actions done by the account.
Verify that the configuration change was expected.

Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Investigate if any other network zones have been changed or removed.

Variations

The user has made an unusual modification to the Okta Network zone

Synopsis

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

Description

An atypical modification to the Okta Network zone has been performed by the user.

Attacker's Goals

An attacker may attempt to modify an Okta network zone to weaken an organization's security controls.

Investigative actions

Follow further actions done by the account.
- Verify that the configuration change was expected.
- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Investigate if any other network zones have been changed or removed.

A user modified an Okta network zone with suspicious characteristics

Synopsis

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

Description

An Okta network zone was modified by a user with suspicious characteristics.

Attacker's Goals

An attacker may attempt to modify an Okta network zone to weaken an organization's security controls.

Investigative actions

Follow further actions done by the account.
- Verify that the configuration change was expected.
- Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
  Investigate if any other network zones have been changed or removed.

21.6 | A user accessed Okta's admin application

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: • Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	• Initial Access (TA0001) Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Domain or Tenant Policy Modification (T1484) Valid Accounts (T1078)
Severity	Informational

Description

An attempt to access Okta's admin management application.

Attacker's Goals

Adversaries are attempting to infiltrate Okta's administrative application, a breach that could lead to the manipulation of authentication procedures, creation of persistent user accounts, and various activities aiding in the compromise of additional assets.

Investigative actions

Reach out to the user responsible for the alert to confirm the legitimacy of the activity. Examine the user's actions preceding and following the activation of the alert.

- Assess the reputation of the IP address along with that of the Autonomous System Number (ASN).

Variations

Suspicious Okta Admin App Access Attempt

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	- Account Manipulation (T1098) - Domain or Tenant Policy Modification (T1484) Valid Accounts (T1078)
Severity	Low

Description

A user attempted to access the Okta Admin Application in a suspicious way.

Attacker's Goals

Adversaries are attempting to infiltrate Okta's administrative application, a breach that could lead to the manipulation of authentication procedures, creation of persistent user accounts, and various activities aiding in the compromise of additional assets.

Investigative actions

Reach out to the user responsible for the alert to confirm the legitimacy of the activity.
- Examine the user's actions preceding and following the activation of the alert.
- Assess the reputation of the IP address along with that of the Autonomous System Number (ASN).

21.7 | Potential Okta access limit breach

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Collection (TA0009) - Initial Access (TA0001)
ATT&CK Technique	Automated Collection (T1119) - Valid Accounts (T1078)
Severity	Informational

Description

A user surpassed Okta's rate limit, leading to an access limit violation. This could suggest a potential account takeover attempt.

Attacker's Goals

An adversary may attempt to use a compromised account in an unusual way to harvest as much data as possible, which could result in exceeding the access limit policy.

Investigative actions

Reach out to the user responsible for the alert to confirm the legitimacy of the activity.

- Examine the user's actions preceding and following the activation of the alert.
  Investigate abnormal logins, reported suspicious activities, new processes run, and recent configuration changes for any indicators of potential compromise.
  Assess the reputation of the IP address along with that of the Autonomous System Number (ASN).

Variations

A breach in access limits within Okta, accompanied by suspicious characteristics

Synopsis

ATT&CK Tactic	Collection (TA0009) Initial Access (TA0001)
ATT&CK Technique	Automated Collection (T1119) Valid Accounts (T1078)
Severity	Low

Description

The user exceeded the access threshold in Okta, triggering a violation alert.

Attacker's Goals

An adversary may attempt to use a compromised account in an unusual way to harvest as much data as possible, which could result in exceeding the access limit policy.

Investigative actions

- Reach out to the user responsible for the alert to confirm the legitimacy of the activity.
- Examine the user's actions preceding and following the activation of the alert. Investigate abnormal logins, reported suspicious activities, new processes run, and recent configuration changes for any indicators of potential compromise.
- Assess the reputation of the IP address along with that of the Autonomous System Number (ASN).

21.8 | User added a new device to Okta Verify instance

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)

Severity	Informational

Description

The user has successfully registered a new device with the Okta Verify application.

Attacker's Goals

Attackers may exploit the device registration process in Okta by registering unauthorized devices, thereby gaining access to sensitive resources and user accounts within an organization.

Investigative actions

- Reach out to the user responsible for the device registration to confirm its legitimacy.
- Examine the user's actions preceding and following the activation of the alert.
  Assess the reputation of the IP address along with that of the Autonomous System Number (ASN).

  Make sure the IP address is not showing any abnormal activity.
- Monitor the activity from the new registered device and ensure that it matches the user's normal activity.

Variations

Suspicious device enrollment to Okta

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098) - Valid Accounts (T1078)
Severity	Low

Description

A new device was registered on Okta with suspicious characteristics, which increased the alert severity.

Attacker's Goals

Attackers may exploit the device registration process in Okta by registering unauthorized devices, thereby gaining access to sensitive resources and user accounts within an organization.

Investigative actions

Reach out to the user responsible for the device registration to confirm its legitimacy.

Examine the user's actions preceding and following the activation of the alert.

- Assess the reputation of the IP address along with that of the Autonomous System Number (ASN).
Make sure the IP address is not showing any abnormal activity.
Monitor the activity from the new registered device and ensure that it matches the user's normal activity.

21.9 | Okta Reported Attack Suspected

Synopsis

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

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

Description

Okta Threat Insight Reported Attack Suspected.

Attacker's Goals

An attacker might attempt to compromise Okta accounts to gain access to sensitive assets or data.

Investigative actions

Examine Okta alerts and search for signs of compromise to evaluate the potential risk.

21.10 | Okta API Token Created

Synopsis

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

Required Data	▪ Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Privilege Escalation (TA0004) Execution (TA0002) Persistence (TA0003)
ATT&CK Technique	Access Token Manipulation: Make and Impersonate Token (T1134.003) ▪ Command and Scripting Interpreter: Cloud API (T1059.009) ▪ Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Informational

Description

A user created a new API token in Okta.

Attacker's Goals

An attacker's goal is to gain unauthorized access, compromise user accounts, and perform malicious actions within an organization's systems, potentially leading to data breaches, account takeovers, and the escalation of privileges.

Investigative actions

- Review the actions taken by the user that created the token.
  Follow the operations made using this API token by the ID token.
  Contact the user who created the API token and ensure that the API token is needed.

Variations

An Okta API token was generated with suspicious characteristics

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Execution (TA0002) Persistence (TA0003)
ATT&CK Technique	Access Token Manipulation: Make and Impersonate Token (T1134.003) Command and Scripting Interpreter: Cloud API (T1059.009) Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Low

Description

A user created a new API token in Okta with suspicious conditions.

Attacker's Goals

An attacker's goal is to gain unauthorized access, compromise user accounts, and perform malicious actions within an organization's systems, potentially leading to data breaches, account takeovers, and the escalation of privileges.

Investigative actions

Review the actions taken by the user that created the token.

Follow the operations made using this API token by the ID token.

- Contact the user who created the API token and ensure that the API token is needed.

21.11 | Okta admin privilege assignment

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Informational

Description

A user assigned admin privileges to a new user or group.

Attacker's Goals

An attacker is attempting to gain access to sensitive information or systems, while privilege escalation involves their attempt to increase control and access within the system or network.

Investigative actions

- Reach out to the user responsible for the alert to confirm the legitimacy of the activity.
  Examine the user's actions preceding and following the activation of the alert.
  Analyze the actions carried out by the user responsible for granting permission.

Variations

Abnormal Okta admin privilege assignment with suspicious characteristics

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Low

Description

A suspicious user assignment of admin privileges to a new user or group.

Attacker's Goals

An attacker is attempting to gain access to sensitive information or systems, while privilege escalation involves their attempt to increase control and access within the system or network.

Investigative actions

Reach out to the user responsible for the alert to confirm the legitimacy of the activity. Examine the user's actions preceding and following the activation of the alert.

Analyze the actions carried out by the user responsible for granting permission.

21.12 | A user observed and reported unusual activity in Okta

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user observed and reported unusual activity in Okta.

Attacker's Goals

An attacker tries infiltrating an Okta account to gain unauthorized access to valuable resources.

Investigative actions

- Investigate the original event that was reported as suspicious.
  Contact the user and understand why he reported the activity as suspicious.
  Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Follow further actions done by the account.

Variations

Multiple users have reported the same suspicious activity

Synopsis

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

Description

Unusual activity in Okta reported about an IP not linked to an EDR agent, the operation is rare and flagged by multiple users.

Attacker's Goals

An attacker tries infiltrating an Okta account to gain unauthorized access to valuable resources.

Investigative actions

Investigate the original event that was reported as suspicious.
Contact the user and understand why he reported the activity as suspicious.

Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).

- Follow further actions done by the account.

Unusual activity in Okta was reported by a user along with suspicious characteristics

Synopsis

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

Severity	Low

Description

A user observed and reported unusual activity in Okta.

Attacker's Goals

An attacker tries infiltrating an Okta account to gain unauthorized access to valuable resources.

Investigative actions

- Investigate the original event that was reported as suspicious.
  Contact the user and understand why he reported the activity as suspicious.
  Look for signs that the user account is compromised (e.g. abnormal logins, unusual activity).
- Follow further actions done by the account.

21.13 | Okta device assignment

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	6 Hours
Deduplication Period	1 Day
Required Data	- Requires: - Okta Audit Log
Detection Modules	Identity Threat Module

Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A device was assigned as an Okta MFA device to a user.

Attacker's Goals

For purposes of maintaining persistence, an attacker could potentially register his device with various accounts that have been compromised.

Investigative actions

Confirm that the device assignments were intentionally made by the users and are legitimate.
Examine the IP address and assess its reputation.
- Continue monitoring the accounts for any subsequent actions that may indicate suspicious behavior.

Variations

A suspicious assignment of a mobile device to multiple users

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	Valid Accounts (T1078)

Severity	Low

Description

A single device is being used as an Okta MFA device by multiple users.

Attacker's Goals

For purposes of maintaining persistence, an attacker could potentially register his device with various accounts that have been compromised.

Investigative actions

Confirm that the device assignments were intentionally made by the users and are legitimate.

Examine the IP address and assess its reputation.

- Continue monitoring the accounts for any subsequent actions that may indicate suspicious behavior.

21.14 | Okta account unlock

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	3 Hours
Required Data	- Requires: - Okta Audit Log

Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

Okta user account was unlocked.

Attacker's Goals

The attacker's goal is to gain unauthorized access to sensitive information or resources and to gain control over the locked account.

Investigative actions

- Monitor the user account for indications of compromise, such as irregular login patterns or atypical activities.
  Examine the user's actions preceding and following the activation of the alert.
  Initiate contact with the user to verify the authenticity of the account unlock action.

  Check account the user successfully authenticated after the event.
- Continue monitoring the account for any subsequent actions that may indicate suspicious behavior.

Variations

Okta account unlock with suspicious characteristics

Synopsis

ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

Okta user account was unlocked.

Attacker's Goals

The attacker's goal is to gain unauthorized access to sensitive information or resources and to gain control over the locked account.

Investigative actions

- Monitor the user account for indications of compromise, such as irregular login patterns or atypical activities.
  Examine the user's actions preceding and following the activation of the alert.
  Initiate contact with the user to verify the authenticity of the account unlock action.
- Check account the user successfully authenticated after the event.
- Continue monitoring the account for any subsequent actions that may indicate suspicious behavior.

21.15 | Okta Reported Threat Detected

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Hours
Deduplication Period	1 Day

Required Data	▮ Requires: _ Okta Audit Log
Detection Modules	Identity Threat Module
Detector Tags	Okta Audit Analytics
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

Okta Threat Insight Reported Threat Detected.

Attacker's Goals

An attacker tries infiltrating an Okta account to gain unauthorized access to valuable resources.

Investigative actions

Investigate the original events that were reported as suspicious.
Investigate additional alerts that are activated based on the IP address.

- Follow further actions done by the ip.

Variations

Okta detected multiple threats from the same IP along with other suspicious characteristics

Synopsis

ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

Okta Threat Insight Reported Threat Detected.

Attacker's Goals

An attacker tries infiltrating an Okta account to gain unauthorized access to valuable resources.

Investigative actions

- Investigate the original events that were reported as suspicious.
- Investigate additional alerts that are activated based on the IP address.
- Follow further actions done by the ip.

22 | OneLogin

22.1 | 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.

22.2 | 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.

22.3 | 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.

22.4 | 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.

22.5 | 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.

22.6 | 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.

22.7 | 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 T 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.

22.8 | 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.

22.9 | 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.

22.10 | 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.

22.11 | 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 T 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.

22.12 | 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.

22.13 | 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.

22.14 | 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.

22.15 | 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.

22.16 | 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.

22.17 | 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.

22.18 | 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.

23 | Palo Alto Networks Global Protect

23.1 | A disabled user attempted to log in to a VPN

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: - Palo Alto Networks Global Protect OR - Third-Party VPNs

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 disabled user attempted to log in suspiciously to a VPN.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.

- Confirm that the activity is benign (e.g. a contractor user).
- Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

Variations

Possible VPN login attempt by disabled user

Synopsis

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

Severity	Informational

Description

A disabled user attempted to log in suspiciously to a VPN.

Attacker's Goals

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

Investigative actions

- See whether the service authentication was successful.
  Confirm that the activity is benign (e.g. a contractor user).
  Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

23.2 | First VPN access attempt 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs

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 attempted to connect from an unusual country that no one from this organization has connected from before. This may indicate the account was compromised.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.
Confirm that the activity is benign (e.g. the user has switched locations and providers).

Verify if the country is an approved country to connect from.

- Follow further actions done by the user.

Variations

First successful VPN access 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	Low

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

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

Investigative actions

- See whether the service authentication was successful.
- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the country is an approved country to connect from.
- Follow further actions done by the user.

23.3 | VPN login by a dormant 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A dormant user logged on to a VPN service after having been unused for a month or longer. This may indicate the account is misused by an attacker.

Attacker's Goals

Use a compromised user account which has not been used for a long while, and therefore is less likely to be noticed.

Investigative actions

Confirm that the activity is benign (e.g. the user returned from a long leave of absence).

See whether there are other abnormal actions done by the user (e.g. files\commands\other logins).

- Check if the user initiated other logins aside from a VPN login.
  Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

23.4 | VPN login with 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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 machine account successfully logged in to a VPN service.

Attacker's Goals

Use an account that was possibly compromised in the past to gain access to the network and access privileged resources.

Investigative actions

See whether the service login was successful.
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 VPN login with a machine account

Synopsis

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

Description

A machine account successfully logged in to a VPN service.

Attacker's Goals

Use an account that was possibly compromised in the past to gain access to the network and access privileged resources.

Investigative actions

- See whether the service login was successful.
  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.

23.5 | A user connected to a VPN 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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 a VPN from an unusual country that the user has not connected from before. This may indicate the account was compromised.

Attacker's Goals

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

Investigative actions

- See whether the service authentication was successful.
  Confirm that the activity is benign (e.g. the user has switched locations and providers).
  Verify if the country is an approved country to connect from.

  Follow further actions done by the user.

Variations

A user connected to a VPN 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 connected to a VPN service from an unusual country. This may indicate the account was compromised.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.
Confirm that the activity is benign (e.g. the user has switched locations and providers).

- Verify if the country is an approved country to connect from.
- Follow further actions done by the user.

23.6 | A user logged in at an unusual time via VPN

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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user connected to a VPN on a day and hour, which 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 amount of traffic and how long it continues.
  Follow further actions done by the user.

23.7 | First VPN 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:
	  - Palo Alto Networks Global Protect
	  OR
	  - Third-Party VPNs

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 logged in to a VPN 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

Unusual VPN access from ASN

Synopsis

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

Description

An unusual VPN login 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.

23.8 | A Successful VPN connection 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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 VPN connection 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 VPN connection 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 VPN connection 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.

23.9 | VPN login 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:
	  - Palo Alto Networks Global Protect
	  OR
	  - Third-Party VPNs

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 attempted to log in to a VPN service.

Attacker's Goals

Use an account that was possibly compromised in the past to gain access to the network and access privileged resources.

Investigative actions

See whether the service authentication was successful.
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 VPN login by an administrative service account

Synopsis

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

Description

An administrative service account attempted to log in to a VPN service.

Attacker's Goals

Use an account that was possibly compromised in the past to gain access to the network and access privileged resources.

Investigative actions

See whether the service authentication was successful.
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.

23.10 | VPN login 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
Detection Modules	Identity Analytics
Detector Tags	Honey User Analytics
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A VPN login 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 VPN login by a honey user

Synopsis

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

Description

A VPN login 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.

23.11 | First VPN 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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 VPN connection was attempted from a new ASN.

Attacker's Goals

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

Investigative actions

- See whether the connection was successful.
  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.

23.12 | VPN access with an 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: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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 accessed a VPN with an abnormal operating system.

Attacker's Goals

Use a legitimate user and connect to a VPN service to gain access to the network.

Investigative actions

- See whether the service authentication was successful.
- 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.

Variations

VPN access with a suspicious operating system

Synopsis

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

Description

A user accessed a VPN with an abnormal operating system.

Attacker's Goals

Use a legitimate user and connect to a VPN service to gain access to the network.

Investigative actions

See whether the service authentication was successful.

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.

VPN access from an abnormal operating system with suspicious characteristics

Synopsis

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

Description

A user accessed a VPN from an abnormal operating system with some more suspicious characteristics that flagged this login attempt as a suspicious login.

Attacker's Goals

Use a legitimate user and connect to a VPN service to gain access to the network.

Investigative actions

- See whether the service authentication was successful.
- 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.

23.13 | Impossible traveler - VPN

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Hours
Deduplication Period	7 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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

A user connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.

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 proxy, or shared their credentials with a remote employee.

Variations

Possible Impossible traveler via VPN

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 connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.
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 proxy, or shared their credentials with a remote employee.

VPN 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

A user connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.
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 proxy, or shared their credentials with a remote employee.

VPN impossible traveler with an unusual parameter

Synopsis

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

Description

A user connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.
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 proxy, or shared their credentials with a remote employee.

23.14 | VPN login Brute-Force attempt

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: ▯ Palo Alto Networks Global Protect OR - Third-Party VPNs
Detection Modules	Identity Analytics
Detector Tags	

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

Description

A user account failed to log in to a VPN service multiple times in a short time period. This may indicate a brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

Verify any successful connections by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

Variations

VPN Login Brute Force

Synopsis

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

Description

A user account failed to log in to a VPN service multiple times in a short time period. This may indicate a brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

Verify any successful connections by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

24 | Palo Alto Networks Platform Logs

24.1 | Recurring access to rare IP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	21 Days
Required Data	▌ Requires one of the following data sources: ▯ Palo Alto Networks Platform Logs OR ▁ XDR Agent OR ▯ Third-Party Firewalls
Detection Modules	
Detector Tags	

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

The endpoint is periodically accessing an external fixed-IP address that its peers rarely use. Access to this external IP address has occurred repeatedly over many days.
This connection pattern is consistent with malware connecting to its command and control server for updates and operating instructions.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the IP address belongs to a reputable organization or an asset used in a public cloud.

Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
View all related traffic generated by the suspicious process to understand the purpose.

Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process to look for potential artifacts on infected endpoints.

24.2 | Rare NTLM Usage by 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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material (T1550)
Severity	Informational

Description

Rare authentication by user account to host via NTLM.
The user has not authenticated with NTLM in the past 30 days.
This may be indicative of downgrade attacks from Kerberos to NTLM.

Attacker's Goals

The attacker is attempting to move laterally within a compromised network.

Investigative actions

Verify any successful authentication for the user account referenced by the alert, as these can indicate the attacker managed to use the stolen credentials.

24.3 | Authentication Attempt From a Dormant Account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	31 Days
Required Data	Requires one of the following data sources: Palo Alto Networks Platform Logs OR XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A dormant user account tried to authenticate to a service using a TGS, after having been unused for a year or more. This may indicate the account is misused by an attacker.

Attacker's Goals

Use a compromised user account which has not been used in a long time, and therefore less likely to be noticed.

Investigative actions

- See whether the service authentication was successful.
- 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.

Variations

Authentication Attempt From a Dormant Account to a sensitive server

Synopsis

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

Description

A dormant user account tried to authenticate to a service using a TGS, after having been unused for a year or more. This may indicate the account is misused by an attacker on a sensitive server.

Attacker's Goals

Use a compromised user account which has not been used in a long time, and therefore less likely to be noticed.

Investigative actions

See whether the service authentication was successful.
- 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.

24.4 | Multiple uncommon SSH Servers with the same Server host key

Synopsis

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

Required Data	- Requires:
	  - Palo Alto Networks Platform Logs
	Requires:
	  - XDR Agent

Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Adversary-in-the-Middle (T1557)

Severity	Low

Description

Multiple uncommon SSH Servers with the same Server host key.

Attacker's Goals

Attackers may attempt to move laterally within the network by exploiting and relaying stolen client credentials to another SSH server.

Investigative actions

- Audit the authentication attempts to SSH server using the same key.
- Look for unusual or repeated connections from the same or unexpected hosts.
  Audit Client Credentials, check for any signs of compromised client credentials being used on different SSH servers.

24.5 | Failed Login For Locked-Out 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: - Palo Alto Networks Platform Logs OR - XDR Agent

Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A locked-out user account (event ID 4725 or 4740) was used in a Kerberos TGT pre-authentication attempt.

Attacker's Goals

Authenticate using the principal in the TGT, not knowing that it has been revoked.

Investigative actions

- Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.
  Check whether the attempt to use the principals (user accounts) specified in the alert are legitimate. For example, a user or a script that was not updated that the account has been revoked.
- The lockout can be temporary, for example, in the case of too many login attempts, and may not be visible after the account was released.
  Search for Windows Event Log 4740 to ascertain whether the account was locked out during the time of the alert.

24.6 | Rare SMB session to a remote host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

The endpoint performed a rare SMB activity to a remote host.

Attacker's Goals

Attackers may use the SMB protocol in an attempt to move laterally in the network, and expand their foothold in the organization.

Investigative actions

Check whether the username used in the SMB connection is legitimate.
Verify that this isn't IT activity.

Variations

Rare SMB session to a remote host

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Informational

Description

The endpoint performed a rare SMB activity to a remote host.

Attacker's Goals

Attackers may use the SMB protocol in an attempt to move laterally in the network, and expand their foothold in the organization.

Investigative actions

- Check whether the username used in the SMB connection is legitimate.
  Verify that this isn't IT activity.

24.7 | Abnormal Communication to a Rare IP

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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	NDR C2 Detection
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare external address.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.

View all related traffic generated by the suspicious process to understand the purpose.

- Look for other endpoints on your network that are also contacting the suspicious IP address.
- Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Variations

Abnormal Communication to a Rare IP With a Port Commonly Used by Attack Platforms

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare external address.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

- Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.
  Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
  View all related traffic generated by the suspicious process to understand the purpose.
  Look for other endpoints on your network that are also contacting the suspicious IP address.

  Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Communication to a Rare IP With a NetBIOS Port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare external address.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.
- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Communication to a Rare IP Using a Peer to Peer Protocol

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare external address.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.
- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Communication to a Rare IP Using a Gaming Protocol

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare external address.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.
- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Communication to a Rare IP Using a Video and Audio Conversation Protocol

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare external address.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Communication to a Rare IP From an Unmanaged Host

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare external address.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

24.8 | A user accessed an uncommon AppID

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs - Requires: - XDR Agent
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)

ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon AppID that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon AppID that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

Variations

A user accessed an uncommon external peer-to-peer service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon external peer-to-peer service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon external peer-to-peer service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

A user accessed an uncommon external file-sharing service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon external file-sharing service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon external file-sharing service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

A user accessed an uncommon peer-to-peer service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)

ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon peer-to-peer service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon peer-to-peer service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

A user accessed an uncommon file-sharing service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon file-sharing service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon file-sharing service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

A user accessed an uncommon VPN service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user connected to an unusual VPN service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to hide their online activity.

Attacker's Goals

A user connected to an unusual VPN service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to hide their online activity.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

24.9 | Suspicious Encrypting File System Remote call (EFSRPC) to domain controller

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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material: Pass the Hash (T1550.002)
Severity	Medium

Description

An Encrypting File System Remote call (EFSRPC) was made to a domain controller.

Attacker's Goals

An attacker is attempting to steal credentials and move laterally within a network.

Investigative actions

Check for suspicious processes on the host.
Check if the source host is a vulnerability scanner.

Look for following suspicious connections using the DC machine account.

24.10 | FTP Connection Using an Anonymous Login or Default Credentials

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110) Valid Accounts (T1078)
Severity	Low

Description

An FTP connection using an anonymous login was detected.

Attacker's Goals

Attackers may seek access to FTP accounts and use them to exfiltrate data, stage attack tools, or create command and control channels through trusted services.

Investigative actions

Examine the legitimacy of the application that produced this FTP.
Examine the parent process of this application.
Verify that the connection attempts were not performed from an illegitimate source.

24.11 | Recurring rare domain access to dynamic DNS domain

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	14 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Low

Description

The endpoint is periodically connecting to an external domain that it and its peers rarely use. Access to this domain has occurred repeatedly over multiple days.
This connection pattern is consistent with malware connecting to its command and control server for updates and operating instructions.

Attacker's Goals

Communicate with malware running on your network to control malware activities, perform software updates on the malware, or to take inventory of infected machines.

Investigative actions

- Identify the process/user contacting the remote domain and determine whether the traffic is malicious.
  Look for other endpoints on your network that are also periodically contacting the suspicious domain.

24.12 | Abnormal network communication through TOR using an uncommon port

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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	- Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

Suspicious connection from a known TOR IP to an uncommon port.

Attacker's Goals

Attackers might use TOR IP combined with random ports.to hide C2 inbound communication from inside a host.

Investigative actions

Investigate the network configuration related to the participating port.
Investigate processes that were listening to that port.

Variations

Abnormal network communication through TOR using an uncommon port and App-id

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

Suspicious connection from a known TOR IP to an uncommon port and App-id.

Attacker's Goals

Attackers might use TOR IP combined with random ports.to hide C2 inbound communication from inside a host.

Investigative actions

Investigate the network configuration related to the participating port.

Investigate processes that were listening to that port.

Abnormal network communication through TOR using a suspicious port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	▮ Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

Suspicious connection from a known TOR IP to an uncommon potential C2 communication port.

Attacker's Goals

Attackers might use TOR IP combined with random ports.to hide C2 inbound communication from inside a host.

Investigative actions

Investigate the network configuration related to the participating port.
Investigate processes that were listening to that port.

24.13 | Weakly-Encrypted Kerberos Ticket Requested

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: Palo Alto Networks Platform Logs OR XDR Agent
Detection Modules	
Detector Tags	

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Low

Description

A user specifically requested weak and deprecated encryption in a Kerberos TGS request. This provides easy-to-crack hashes, and is typically a sign of a Kerberoasting attack.

Attacker's Goals

Crack account credentials by obtaining an easy-to-crack Kerberos ticket.

Investigative actions

Check who used the host at the time of the alert, to rule out a benign service or tool requesting weak Kerberos encryption.

Variations

Weakly-Encrypted Kerberos Ticket Requested on a sensitive server

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Medium

Description

A user specifically requested weak and deprecated encryption in a Kerberos TGS request. This provides easy-to-crack hashes, and is typically a sign of a Kerberoasting attack. This action occurred on a sensitive server, which may indicate a malicious activity.

Attacker's Goals

Crack account credentials by obtaining an easy-to-crack Kerberos ticket.

Investigative actions

Check who used the host at the time of the alert, to rule out a benign service or tool requesting weak Kerberos encryption.

24.14 | Unique client computer model was detected via MS-Update protocol

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	▮ Requires: - Palo Alto Networks Platform Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Hardware Additions (T1200)

Severity	Informational

Description

A unique client computer model was detected via MS-Update protocol.

Attacker's Goals

The Windows Server Update Services enables machines to discover and download

software updates from a dedicated update server while providing the necessary client characteristics to install the suitable client version and build.
characteristics may consist of computer model, bios version and architecture.
A unique computer model in the network may indicate on an unauthorized and unmanaged

connection to the internal network.

Investigative actions

Inspect the legitimacy of the host and its hardware components.

- Verify that this host is not a newly deployed end-point or virtual machine as part of a legitimate IT activity.

24.15 | Suspicious failed HTTP request - potential Spring4Shell exploit

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: ▮ Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Exploit Public-Facing Application (T1190)
Severity	Low

Description

A potentially malicious failed HTTP request was received, possibly as part of a Spring4Shell exploitation attempt.

Attacker's Goals

Gain the ability to execute code remotely or drop malware.

Investigative actions

- Check if suspicious process executions occurred after the request.
  Consider limiting access to the vulnerable serve.

Variations

Suspicious HTTP request - potential Spring4Shell exploit

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Exploit Public-Facing Application (T1190)
Severity	Medium

Description

A potentially malicious HTTP request was received, possibly as part of a Spring4Shell exploitation attempt.

Attacker's Goals

Gain the ability to execute code remotely or drop malware.

Investigative actions

Check if suspicious process executions occurred after the request.
Consider limiting access to the vulnerable serve.

24.16 | Weakly-Encrypted Kerberos TGT Response

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: ▯ Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006) ❙ Defense Evasion (TA0005) ❙ Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process: Domain Controller Authentication (T1556.001)
Severity	Informational

Description

A weakly encrypted TGT was issued by a DC. The encryption type is abnormal to the DC and provides an easy-to-crack TGT. This might indicate a Skeleton Key attack.

Attacker's Goals

To patch the DC's authentication process, bypass standard authentication, and gain access to hosts and resources in single-factor authentication environments.

Investigative actions

Checked the user or entity that accessed the host during the alert-triggering timeframe, to eliminate the possibility of a benign service or application requesting weak Kerberos encryption.
Checking if the DC is patched for Skeleton key attack (CVE-2016-1567).

Variations

Abnormal Weakly-Encrypted Kerberos TGT Response

Synopsis

ATT&CK Tactic	▮ Credential Access (TA0006) Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process: Domain Controller Authentication (T1556.001)
Severity	Low

Description

A weakly encrypted TGT was issued by a DC. The encryption type is abnormal to the DC and provides an easy-to-crack TGT. This might indicate a Skeleton Key attack.

Attacker's Goals

To patch the DC's authentication process, bypass standard authentication, and gain access to hosts and resources in single-factor authentication environments.

Investigative actions

Checked the user or entity that accessed the host during the alert-triggering timeframe, to eliminate the possibility of a benign service or application requesting weak Kerberos encryption.
Checking if the DC is patched for Skeleton key attack (CVE-2016-1567).

24.17 | Rare RDP session to a remote host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Low

Description

The endpoint performed a rare RDP session to a remote host.

Attacker's Goals

- Attackers may attempt to move laterally over the network by using compromised accounts or machines to connect to remote hosts using the RDP protocol.

Investigative actions

Inspect the legitimacy of the user which the RDP made the connection with.
Verify that this isn't IT activity.

Variations

Rare RDP session to a remote host

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Informational

Description

The endpoint performed a rare RDP session to a remote host.

Attacker's Goals

Attackers may attempt to move laterally over the network by using compromised accounts or machines to connect to remote hosts using the RDP protocol.

Investigative actions

- Inspect the legitimacy of the user which the RDP made the connection with.
  Verify that this isn't IT activity.

24.18 | Possible DCShadow attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AWS Flow Log OR - AWS OCSF Flow Logs OR - Azure Flow Log OR - Gcp Flow Log OR - Palo Alto Networks Platform Logs OR - Third-Party Firewalls OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006) Defense Evasion (TA0005)

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

Description

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

Attacker's Goals

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

Investigative actions

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

24.19 | Possible IPFS traffic was detected

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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010) ▪ Initial Access (TA0001)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048) ▪ Phishing (T1566)
Severity	Informational

Description

The host attempted to access other nodes in an IPFS manner.

Attacker's Goals

IPFS access may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Investigative actions

1. Check the host for IPFS client software.
2. Examine the client's network traffic for uploaded or downloaded file hashes.

24.20 | Bronze-Bit exploit

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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	High

Description

A forwardable Kerberos ticket for delegation of a Protected User was observed.

Attacker's Goals

Gain a special user's Kerberos ticket to move laterally.

Investigative actions

- Check the initiating service account delegation privileges.
  Check the delegated account credentials and if it has high privileges.
  Check the ticket destination to verify whether it is a sensitive asset.

24.21 | Suspicious SSH Downgrade

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008) Defense Evasion (TA0005)

ATT&CK Technique	▮ Remote Services (T1021) Impair Defenses: Downgrade Attack (T1562.010)
Severity	Low

Description

The endpoint asked for an ssh downgrade, ssh downgrade may enable attackers to perform attacks such as data decryption, man in the middle, session hijack, replay attack and more.

Attacker's Goals

Attackers may attempt to move laterally over the network by exploiting problems in a lower version of ssh.

Investigative actions

Audit the authentication attempts in the SSH server from the alerted host.
If the source host authenticated to the SSH server, it may indicate that the attacker managed to connect to the remote host maliciously.

Variations

A Host Performed an SSH Downgrade For The First Time In The Last 30 Days

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Defense Evasion (TA0005)
ATT&CK Technique	Remote Services (T1021) Impair Defenses: Downgrade Attack (T1562.010)
Severity	Low

Description

The endpoint asked for an ssh downgrade, ssh downgrade may enable attackers to perform attacks such as data decryption, man in the middle, session hijack, replay attack and more. With a lower version than the source host used in the past.

Attacker's Goals

Attackers may attempt to move laterally over the network by exploiting problems in a lower version of ssh.

Investigative actions

Audit the authentication attempts in the SSH server from the alerted host.
If the source host authenticated to the SSH server, it may indicate that the attacker managed to connect to the remote host maliciously.

A Target Server Performed an SSH Downgrade For The First Time In The Last 30 Days

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Defense Evasion (TA0005)
ATT&CK Technique	Remote Services (T1021) Impair Defenses: Downgrade Attack (T1562.010)
Severity	Low

Description

The endpoint asked for an ssh downgrade, ssh downgrade may enable attackers to perform attacks such as data decryption, man in the middle, session hijack, replay attack and more. With a lower version than the remote host used in the past.

Attacker's Goals

Attackers may attempt to move laterally over the network by exploiting problems in a lower version of ssh.

Investigative actions

Audit the authentication attempts in the SSH server from the alerted host.
If the source host authenticated to the SSH server, it may indicate that the attacker managed to connect to the remote host maliciously.

24.22 | A rare FTP user has been detected on an existing FTP server

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: - Palo Alto Networks Platform Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213) Valid Accounts (T1078)

Severity	Low

Description

A rare or new FTP user has been detected on an existing FTP server.

Attacker's Goals

Attackers may seek to access FTP resources to exfiltrate data, stage attack tools or create a command and control channel through a trusted service.

Investigative actions

- Verify that the new username is legitimate.
- Examine the legitimacy of the application that produced this uncommon FTP.
  Examine the parent process of this application.
  Check the logs on the FTP server for a new user creation.

Variations

Possible FTP User Scanning Detected

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213) Valid Accounts (T1078)
Severity	Low

Description

A rare or new FTP user has been detected on an existing FTP server.

Attacker's Goals

Attackers may seek to access FTP resources to exfiltrate data, stage attack tools or create a command and control channel through a trusted service.

Investigative actions

- Verify that the new username is legitimate.
  Examine the legitimacy of the application that produced this uncommon FTP.
  Examine the parent process of this application.

  Check the logs on the FTP server for a new user creation.

24.23 | Rare file transfer over SMB protocol

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: - Palo Alto Networks Platform Logs - Requires: - XDR Agent
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)

ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

The endpoint performed an abnormal file transfer over SMB to a remote host.

Attacker's Goals

Attackers may attempt to gain persistence or move laterally over the network by dropping executable files and scripts on remote hosts using the SMB protocol.

Investigative actions

Inspect the file that was transferred to the remote host.

- Verify that this isn't IT activity.

24.24 | Abnormal Communication to a Rare Domain

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: ▯ Palo Alto Networks Platform Logs OR ▁ XDR Agent OR ▯ Third-Party Firewalls
Detection Modules	
Detector Tags	NDR C2 Detection
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare domain.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious domain name.
  Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Variations

Abnormal Communication to a Rare Domain With a Port Commonly Used by Attack Platforms

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

An abnormal communication was seen from an internal entity to a rare domain.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious domain name.
  Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Communication to a Rare Domain to a Suspicious Autonomous System (AS)

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

An abnormal communication was seen from an internal entity to a rare domain.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious domain name.
  Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Communication to a Rare Domain With a Less Common Port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

An abnormal communication was seen from an internal entity to a rare domain.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious domain name.
  Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

24.25 | A Torrent client was detected on a host

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: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	

ATT&CK Tactic	▮ Exfiltration (TA0010) Initial Access (TA0001)
ATT&CK Technique	▮ Exfiltration Over Alternative Protocol (T1048) ▮ Phishing (T1566)
Severity	Informational

Description

The host produced traffic consistent with the BitTorrent protocol.
Torrents may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Attacker's Goals

Exfiltrate data or as a phishing entry point.

Investigative actions

- Check the host for torrent client software.
- Look at the download's folder for foreign files or Torrent files.
  Examine the client's network traffic for uploaded or downloaded file hashes.

Variations

A Torrent client was detected on a host

Synopsis

ATT&CK Tactic	Exfiltration (TA0010) Initial Access (TA0001)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048) Phishing (T1566)
Severity	Informational

Description

The host produced traffic consistent with the BitTorrent protocol.
Torrents may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Attacker's Goals

Exfiltrate data or as a phishing entry point.

Investigative actions

- Check the host for torrent client software.
- Look at the download's folder for foreign files or Torrent files.
- Examine the client's network traffic for uploaded or downloaded file hashes.

24.26 | Rare NTLM Access By User To Host

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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	Identity Analytics

Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material (T1550)
Severity	Informational

Description

An unusual NTLM authentication attempt by a user to host
This may be indicative of using stolen credentials or access tokens to access restricted hosts.

Attacker's Goals

The attacker is attempting to move laterally within a compromised network.

Investigative actions

Verify any successful authentication for the user account referenced by the alert, as these can indicate the attacker managed to use the stolen credentials.

24.27 | Suspicious SMB connection from domain controller

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: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material: Pass the Hash (T1550.002)
Severity	Low

Description

A domain controller has initiated an SMB connection to another host. The domain controllers usually communicate over SMB only with other domain controllers. An attacker can abuse such sessions for relay attacks.

Attacker's Goals

An attacker is attempting to steal credentials and move laterally within a network.

Investigative actions

- Check if the destination is domain controller, if it is, exclude it.
- Look for earlier connections to the DC which may cause it to initiate the session.

24.28 | Possible path traversal via HTTP request

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Low

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

Inspect the legitimacy of the URI path.
Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

Variations

Possible sensitive path traversal via HTTP request

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Medium

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

- Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

Inspect the legitimacy of the URI path.

Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

Possible path traversal via HTTP request from a TOR exit node

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Medium

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

- Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

Inspect the legitimacy of the URI path.

Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

Possible credential path traversal via HTTP request

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Medium

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

- Inspect the legitimacy of the URI path.
- Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

24.29 | Rare Scheduled Task RPC 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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	

Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008) Persistence (TA0003)
ATT&CK Technique	Remote Services (T1021) Scheduled Task/Job (T1053)
Severity	Informational

Description

The endpoint performed abnormal Scheduled Task RPC activity to a remote host.

Attacker's Goals

- Attackers may attempt to gain persistence or move laterally over the network by executing code on remote hosts using scheduled tasks.

  The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

- Review the action of the created scheduled task on the remote host.
  Correlate the RPC call from the source host and understand which software initiated it.
  Verify that this isn't IT activity.

Variations

Rare remote task registration and creation via Scheduled Task RPC interface

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Persistence (TA0003)

ATT&CK Technique	▮ Remote Services (T1021) Scheduled Task/Job (T1053)
Severity	Medium

Description

The endpoint performed abnormal task registration and creation via Scheduled Task RPC interface to a remote host.

Attacker's Goals

- Attackers may attempt to gain persistence or move laterally over the network by executing code on remote hosts using scheduled tasks.
  The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

- Review the action of the created scheduled task on the remote host.
- Correlate the RPC call from the source host and understand which software initiated it.
- Verify that this isn't IT activity.

Rare remote task creation via Scheduled Task RPC interface

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Persistence (TA0003)
ATT&CK Technique	Remote Services (T1021) Scheduled Task/Job (T1053)
Severity	Medium

Description

The endpoint performed abnormal task registration or creation via Scheduled Task RPC interface to a remote host.

Attacker's Goals

- Attackers may attempt to gain persistence or move laterally over the network by executing code on remote hosts using scheduled tasks.
  The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

Review the action of the created scheduled task on the remote host.

- Correlate the RPC call from the source host and understand which software initiated it. Verify that this isn't IT activity.

Rare Scheduled Task RPC activity

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Persistence (TA0003)
ATT&CK Technique	Remote Services (T1021) Scheduled Task/Job (T1053)
Severity	Low

Description

The endpoint performed abnormal Scheduled Task RPC activity to a remote host.

Attacker's Goals

- Attackers may attempt to gain persistence or move laterally over the network by executing code on remote hosts using scheduled tasks.
  The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

- Review the action of the created scheduled task on the remote host.
- Correlate the RPC call from the source host and understand which software initiated it. Verify that this isn't IT activity.

24.30 | Failed Login For a Long Username With Special Characters

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: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Exploit Public-Facing Application (T1190)
Severity	Informational

Description

A long username containing special characters failed to log in to the domain.

Attacker's Goals

An attacker is trying to get code execution on internet-facing assets through command injection.

Investigative actions

- Is the host running internet-facing services?
- Are we looking at sanction vulnerability scanning?

24.31 | Unusual SSH activity that resembles SSH proxy

Synopsis

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

Required Data	- Requires one of the following data sources:
	  - AWS Flow Log
	  OR
	  - AWS OCSF Flow Logs
	  OR
	  - Azure Flow Log
	  OR
	  - Gcp Flow Log
	  OR
	  - Palo Alto Networks Platform Logs
	  OR
	  - Third-Party Firewalls
	Requires one of the following data sources:
	  - Palo Alto Networks Platform Logs
	  OR
	  - XDR Agent

Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

Variations

High Volume Unusual SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

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

Attacker's Goals

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

Investigative actions

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

Suspicious SSH activity that resembles SSH proxy

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate

the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Unusual SSH activity that resembles SSH proxy detected

Synopsis

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

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.

This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

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

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate

the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

24.32 | Unusual SSH activity that resembles SSH proxy

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AWS Flow Log OR - AWS OCSF Flow Logs OR - Azure Flow Log OR - Gcp Flow Log OR - Palo Alto Networks Platform Logs OR - Third-Party Firewalls - Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Informational

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.

This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

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

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised.

Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Variations

High Volume Unusual SSH activity that resembles SSH proxy

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

Suspicious SSH activity that resembles SSH proxy

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

Unusual SSH activity that resembles SSH proxy detected

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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