



Cisco Secure Cloud Analytics

Alerts and Observations Reference Guide



Table of Contents

Alerts and Observations Reference Introduction	12
Alerts and Observations	12
Guide Overview	13
Alert Descriptions	14
Abnormal ISE User	14
Abnormal User	14
Amplification Attack	15
Anomalous AWS Workspace	16
Anomalous Azure Custom Script Extensions	16
Anomalous Domain Controller Activity	17
Anomalous Mac Workstation	18
Anomalous Windows Workstation	18
Attendance Drop	19
AWS Anomalous IAM Role Policy Update	20
AWS Anomalous RDS Password Reset	20
AWS Anomalous Secrets Manager Batch Retrieval	21
AWS API Call Using TOR IP	21
AWS API Watchlist IP Hit	22
AWS AppStream Image Shared	22
AWS CloudTrail Watchlist Hit	23
AWS Config Rule Violation	23
AWS Console Login Failures	24
AWS Detector Modified	24
AWS Domain Takeover	25
AWS EC2 Startup Script Modified	26
AWS ECS Credential Access	26
AWS High Volume of API GetPasswordData Call Failures	27
AWS IAM Anywhere Trust Anchor Created	27
AWS IAM User Takeover	28

AWS Inspector Finding	29
AWS Lambda Backdoor Function Created	29
AWS Lambda Invocation Spike	30
AWS Lambda Invoke Permission Added	31
AWS Logging Deleted	31
AWS Logging Impairment	32
AWS Multifactor Authentication Change	32
AWS Organization Exit Attempt	33
AWS Region Newly Utilized	34
AWS Repeated API Failures	34
AWS Resource Inactive	35
AWS Root Account Used	35
AWS Route 53 Hosted Zone Created	36
AWS Route53 Target Added	36
AWS S3 Bucket Lifecycle Configured	37
AWS Security Group Deleted	37
AWS Snapshot Exfiltration	38
AWS Stale Access Key	38
AWS Unusually Large EC2 Instance	39
Azure Activity Log IP Watchlist Hit	39
Azure Activity Log Watchlist Hit	40
Azure Advisor Watchlist	40
Azure Anomalous RunCommand	41
Azure Exposed Services	41
Azure Firewall Deleted	42
Azure Function Invocation Spike	42
Azure Key Vaults Deleted	43
Azure Network Security Group Deleted	44
Azure OAuth Bypass	44
Azure Permissive Security Group	45

Azure Permissive Storage Account	45
Azure Resource Group Deleted	46
Azure Transfer Data To Cloud Account	46
Azure Virtual Machine in Unused Location	47
Cloud Metadata Service Credential Access	47
Connection to TOR IP Address	48
Country Set Deviation	48
Country Watchlist: New Long Session	49
Country Watchlist: Protocol Violation	49
Country Watchlist: Remote Access	50
DC Sync Attack Behavior	51
DNS Abuse	51
Email Spam	52
Emergent Profile	53
Empire Command and Control	53
Endpoint Exfiltration of AWS Credentials	54
Excessive Access Attempts (External)	54
Excessive Connections to Network Printers	55
GCP API Call Using TOR IP	56
GCP Cloud Function Invocation Spike	56
GCP Operations Log Watchlist Hit	57
Geographically Unusual AWS API Usage	57
Geographically Unusual Azure API Usage	58
Geographically Unusual Remote Access	59
Heartbeat Connection Count	59
High Bandwidth Unidirectional Traffic	60
ICMP Abuse	60
IDS Emergent Profile	61
IDS Notice Spike	62
Inbound Port Scanner	62

Internal Connection Spike	63
Internal Connection Watchlist Hit	64
Internal Port Scanner	64
Invalid Mac Address	65
ISE Jailbroken Device	66
LDAP Connection from Anomalous Process	66
LDAP Connection Spike	67
Malicious Process Detected	67
Malware Spike	68
MFA Disabled for Azure	68
Microsoft Defender for Cloud Event	69
NetBIOS Connection Spike	69
Network Population Spike	70
Network Printer with Excessive Connections	70
New External Connection	71
New Internal Device	72
New IP Scanner	72
New Remote Access	73
New SNMP Sweep	73
New Unusual DNS Resolver	74
Non-Service Port Scanner	75
Outbound LDAP Connection Spike	75
Outbound Traffic Spike	76
Permissive Amazon Elastic Kubernetes Service Cluster Created	77
Permissive AWS S3 Access Control List	77
Permissive AWS Security Group Created	78
Persistent Remote Control Connections	78
Port 8888: Connections from Multiple Sources	79
Potential Database Exfiltration	79
Potential Data Exfiltration	80

Potential Gamaredon C2 Callout	80
Potential GhostPulse Malware C2	81
Potentially Harmful Hidden File Extension	81
Potentially Vulnerable Remote Control Protocol	82
Potential System Process Impersonation	83
Powershell RDP Connection	83
Powershell WinRM Connection	84
Protocol Forgery	84
Public Facing IP Watchlist Match	85
Repeated Umbrella Sinkhole Communications	85
Repeated Watchlist Communications	86
Role Violation	87
SMB Connection Outlier	87
SMB Connection Spike: Internal	88
SMB Connection Spike: Outbound	88
SMB RDP: Connection to Multiple Destinations	89
SMB Traffic Initiated From a Command Interpreter	89
Static Device Connection Deviation	90
Static Device Deviation	91
Suspected Botnet Interaction	91
Suspected Cryptocurrency Activity	92
Suspected Phishing Domain	92
Suspected Port Abuse: External	93
Suspected Remote Access Tool Heartbeat	94
Suspected Zerologon RPC Exploit Attempt	94
Suspicious Curl Behavior	95
Suspicious DNS over HTTPS Activity	95
Suspicious Domain Lookup Failures	96
Suspicious Email Findings by Initial Access	96
Suspicious Endpoint Findings by Collection	97

Suspicious Endpoint Findings by Command and Control	97
Suspicious Endpoint Findings by Credential Access	98
Suspicious Endpoint Findings by CrowdStrike Proprietary Tactics	98
Suspicious Endpoint Findings by Defense Evasion	99
Suspicious Endpoint Findings by Discovery	99
Suspicious Endpoint Findings by Execution	100
Suspicious Endpoint Findings by Exfiltration	100
Suspicious Endpoint Findings by Impact	101
Suspicious Endpoint Findings by Initial Access	101
Suspicious Endpoint Findings by Lateral Movement	102
Suspicious Endpoint Findings by MS Defender Proprietary Tactics	102
Suspicious Endpoint Findings by Persistence	103
Suspicious Endpoint Findings by Privilege Escalation	103
Suspicious Endpoint Findings by Reconnaissance	103
Suspicious Endpoint Findings by Resource Development	104
Suspicious Endpoint Findings without Tactics	104
Suspicious File Download Observed on Process Arguments	105
Suspicious MSHTA Activity	105
Suspicious Network Findings by Collection	106
Suspicious Network Findings by Command and Control	106
Suspicious Network Findings by Exfiltration	107
Suspicious Process Executed	107
Suspicious Process Path	108
Suspicious Request to Telegram	108
Suspicious SMB Activity	109
Suspicious User Agent	109
Suspicious User-Agent Activity	110
Talos Intelligence Watchlist Hits	110
TrickBot AnchorDNS Tunneling	111
Unusual DNS Connection	112

Unusual External Server	112
Unusual File Extension from New External Server	113
User Watchlist Hit	114
Vulnerable Transport Security Protocol	114
Watchlist Hit	115
Worm Propagation	116
Observation Descriptions	117
Amazon GuardDuty DNS Request Finding	117
Amazon GuardDuty Network Connection Finding	117
Amazon Inspector Finding	117
Anomalous Profile	117
Anomalous User Agent	118
AWS API Watchlist Access	118
AWS Architecture Compliance	118
AWS CloudTrail Event	118
AWS Config Compliance	120
AWS Config Update	120
AWS Lambda Metric Outlier	120
AWS Multifactor Authentication Change	120
AWS New User Action	121
AWS Root Account Used	121
Azure Advisor Recommendation	121
Azure Exposed Services	121
Azure Functions Metric Outlier	122
Azure Permissive Security Group	122
Azure Permissive Storage Setting	122
Azure Security Event	122
Azure Unusual Activity	122
Azure VM in Unused Location	123
Bad Protocol	123

Cluster Change	123
Compliance Verdict Summary	124
Confirmed Threat Indicator Match - Domain	124
Confirmed Threat Indicator Match - Hostname	124
Confirmed Threat Indicator Match - IP	124
Confirmed Threat Indicator Match - URL	125
Country Set Deviation	125
Domain Generation Algorithm	125
Domain Generation Algorithm Success	126
Drive By Download	126
Exceptional Domain Controller	126
Excessive Connections to Network Printers	126
External Mail Client Connections	126
External Port Scanner	127
GCP Cloud Function Metric Outlier	127
GCP Watchlist Activity	127
Geographic Watchlist	127
Heartbeat	128
Historical Outlier	128
Insecure Transport Protocol	128
Internal Connection Watchlist	129
Internal Port Scanner	129
Intrusion Detection System Notice	129
Invalid MAC Address	129
IP Scanner	130
ISE Session Started	130
ISE Suspicious Activity	130
Long Session	130
Malware Event	131
Multiple Access Failures	131

Multiple File Extensions	131
Network Printer with Excessive Connections	131
New Compliance Resource Failure	132
New External Connection	132
New External Server	132
New File Extension	132
New High Throughput Connection	133
New Internal Connection	133
New Internal Device	133
New Large Connection (External)	133
New Large Connection (Internal)	134
New Profile	134
Persistent External Server	134
Population Spike	134
Port Scanner	135
Potential Data Forwarding	135
Public Amazon Route 53 Hosted Zone Created	135
Public Facing IP Watchlist Match	135
Public IP Service	135
Rapid Logins	136
Record Metric Outlier	136
Record Profile Outlier	136
Remote Access	136
Role Violation	137
Scan Result	137
Session Closed	137
Session Opened	137
Static Connection Set Deviation	137
Static Port Set Deviation	138
Sumo Logic Log	138

Suspected Malicious URL	138
Suspected Phishing Domain	138
Suspicious Email Security Finding	139
Suspicious Endpoint Activity	139
Suspicious Endpoint Security Finding	140
Suspicious Firewall Activity	141
Suspicious Microsoft Entra ID Audit Logs Activity	141
Suspicious Network Activity	141
Suspicious Network Activity detected by EVE	141
Suspicious Network Security Finding	141
Suspicious SMB Activity	142
Traffic Amplification	142
TrickBot AnchorDNS Tunneling Activity	142
Umbrella Sinkhole Hit	142
Unused AWS Resource	143
Unusual DNS Resolver	143
Unusual Packet Size	143
Unusual EC2 Instance	143
Unusual Packet Size	143
Watchlist Interaction	144
Watchlist Lookup	144
Worm Propagation	144
Additional Resources	145
Contacting Support	146
Change History	147

Alerts and Observations Reference

Introduction

The following section provides an overview of the alert and observation types available in Cisco Secure Cloud Analytics.

Alerts and Observations

Secure Cloud Analytics uses dynamic entity modeling to track the state of your network. In the context of Secure Cloud Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network, or a Lambda function in your AWS deployment. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they perform on your network.

From this information, Secure Cloud Analytics identifies:

- roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Cloud Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, an interaction with an entity on a watchlist, or a remote access session established with another entity. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Based on the combination of roles, observations, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system.

When you open an alert in the Secure Cloud Analytics web portal UI, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted, and external threat intelligence if it is available.

Guide Overview

This guide lists the alert and observation types that Secure Cloud Analytics can generate.

Each alert in [Alert Descriptions](#) lists:

- the alert type
- associated observations
- any associated Mitre Att&ck Tactics
- any associated Mitre Att&ck Techniques
- a brief description, and why this may indicate malicious behavior

Each observation type in [Observation Descriptions](#) lists:

- the observation type
- any prerequisites for generation
- associated alerts
- a brief description

Alert Descriptions

Abnormal ISE User

Description	There is a user who is the only one who authenticated from the specific device in the past. Another user authenticated on the same device recently, but that user usually only authenticates from a different device.
Associated Observation	ISE Session Started Observations
History	36 days
Telemetry	This alert requires ISE integration for user data attribution.
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Persistence • Defense Evasion • Privilege Escalation • Initial Access
MITRE ATT&CK Techniques	Domain Accounts
Next Steps	Reference the supporting evidence to determine what user authenticated on the endpoint and at what time. Review the ISE session logs to verify the user and endpoint type. Contact the user and determine what they were doing. If their actions are not normal, perform additional investigation. If the user did not log in themselves, or the entity is not recognized, assume that the user credentials were compromised. Detected scenario is expected in environment with Virtual desktop infrastructure (VDI).

Abnormal User

Description	A user session was created on an endpoint that does not normally see sessions with this user.
Associated Observation	Session Opened Observations
History	36 days. Requires one of the following:

	<ul style="list-style-type: none"> • AWS integration • ISE integration for user data attribution • Sumo Logic
Telemetry	<ul style="list-style-type: none"> • AWS API • Active Directory
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Privilege Escalation • Defense Evasion • Initial Access • Persistence
MITRE ATT&CK Techniques	Domain Accounts
Next Steps	<p>Reference the supporting evidence to determine what user account logged into the entity and at what time. Contact the user and determine what they were doing. If their actions are not normal, perform additional investigation. If the user did not log in themselves, or the entity is not recognized or from an external network that you do not trust, update your blocklist and firewall rules to prevent the malicious actor from accessing your network. Determine what actions the user took on the entity, and remediate any negative effects, if possible. If the user exfiltrated data, determine what data was sent, and follow your organization's guidelines for data loss.</p>

Amplification Attack

Description	Device sent traffic with a profile that suggests participation in an amplification attack. This may indicate the device is part of a botnet.
Associated Observation	Traffic Amplification Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Impact

MITRE ATT&CK Techniques

Reflection Amplification

Next Steps

Reference the entity information and supporting evidence, and determine whether or not an external entity is responsible for spreading malware. If so, update your firewall rules to block traffic from the external entity, and any other entities if it is a distributed denial of service (DDoS) attack. If the entity sending the amplification attack is internal to your network, quarantine the entity from your network, and any other entities if it is a DDoS attack. Examine the entities for, and remove, malware.

Anomalous AWS Workspace

Description

An AWS Virtual Workspace used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This may be an indication of malware or misuse.

Associated Observation

[Anomalous Profile Observations](#)

History

14 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

Execution

MITRE ATT&CK Techniques

Cloud Administration Command

Next Steps

Reference the supporting evidence to determine the entity's roles and determine whether or not there is a legitimate business reason for the anomalous behavior. For example, if an entity used BitTorrent to connect to other entities, it may be a test entity or some type of possible testing of firewall rules or other security tests. If there is not a legitimate reason for the anomalous behavior, examine the entity and determine whether or not the entity is functioning as intended, and if it is free of malware.

Anomalous Azure Custom Script Extensions

Description

Azure Custom Script Extensions were utilized to execute

commands on an Azure Virtual Machine, and this behavior was anomalous for the account it was detected in. While Custom Script Extensions are a legitimate feature of Azure, they have been utilized by threat actors including Advanced Persistent Threat groups in the past.

Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	Execution
MITRE ATT&CK Techniques	Cloud Administration Command
Next Steps	Verify whether this behavior was performed legitimately. If not, investigate and potentially isolate the Virtual Machine and user account or Service Principal used to perform the action.

Anomalous Domain Controller Activity

Description	A device identified as a Domain Controller deviated from its usual behavior. This may indicate the device is compromised.
Associated Observation	<ul style="list-style-type: none"> • New External Server Observations • New High Throughput Connection Observations • New Profile Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Privilege Escalation • Credential Access • Lateral Movement • Persistence
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Abuse Elevation Control Mechanism • Domain Controller Authentication

Next Steps From the supporting evidence, view the entity's traffic profile and connections with other entities to determine what types of traffic it is sending, and if it is malicious in nature. Determine if data has been exfiltrated from your network, and if so, the types of data, and how best to remediate the situation.

Anomalous Mac Workstation

Description An Apple Mac Workstation used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This may be an indication of malware or misuse.

Associated Observation [Anomalous Profile Observations](#)

History 14 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics Execution

MITRE ATT&CK Techniques N/A

Next Steps Reference the supporting evidence to determine the entity's roles and determine whether or not there is a legitimate business reason for the anomalous behavior. For example, if an entity used BitTorrent to connect to other entities, it may be a test entity or some type of possible testing of firewall rules or other security tests. If there is not a legitimate reason for the anomalous behavior, examine the entity and determine whether or not the entity is functioning as intended, and if it is free of malware.

Anomalous Windows Workstation

Description A Windows workstation used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This may be an indication of malware or misuse.

Associated Observation [Anomalous Profile Observations](#)

History	14 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Execution
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting evidence to determine the entity's roles and determine whether or not there is a legitimate business reason for the anomalous behavior. For example, if an entity used BitTorrent to connect to other entities, it may be a test entity or some type of possible testing of firewall rules or other security tests. If there is not a legitimate reason for the anomalous behavior, examine the entity and determine whether or not the entity is functioning as intended, and if it is free of malware.

Attendance Drop

Description	Device is normally active for most of the day, but its activity dropped across multiple profiles (e.g., SSH Server, FTP Server). This may indicate that the device is no longer operational.
Associated Observation	Historical Outlier Observations
History	14 days
Telemetry	Netflow
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	Endpoint Denial of Service
Next Steps	Reference the supporting evidence to review the entity's roles and determine whether or not there is a legitimate business reason for the drop in activity. If there is not a legitimate reason for the drop in activity, examine the entity and determine whether or not someone shut it down, if the entity is functioning as intended, and if it is free of malware.

AWS Anomalous IAM Role Policy Update

Description	An update to an existing Identity and Access Management (IAM) role's AssumeRole policy, and this behavior is unusual in this AWS account. The AssumeRole feature of IAM can be used to establish persistence.
Associated Observation	AWS CloudTrail Event Observations
History	0 days
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	Additional Cloud Roles
Next Steps	Verify whether this was authorized activity. If not, review other CloudTrail events for the IAM principal that made the call and rotate credentials if applicable.

AWS Anomalous RDS Password Reset

Description	The main user password for a Relational Database Service instance was changed. This technique has been utilized by threat actors for Persistence and Impact.
Associated Observation	AWS CloudTrail Event
History	0 days
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> Impact Persistence
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> Additional Cloud Roles Account Access Removal
Next Steps	Verify whether this was authorized activity. If not, review other CloudTrail events for the IAM principal that made the call and rotate credentials if applicable.

AWS Anomalous Secrets Manager Batch Retrieval

Description	A batch retrieval of many secrets was made to AWS Secrets Manager by a principal that does not normally perform this action. Making one batch request for secrets can be a way of avoiding volumetric detection for secret retrieval.
Associated Observation	AWS CloudTrail Event
History	0 days
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Credential Access• Defense Evasion
MITRE ATT&CK Techniques	Cloud Secrets Management Stores
Next Steps	Verify whether this was authorized activity. If not, review other CloudTrail events for the IAM principal that made the call and rotate credentials if applicable.

AWS API Call Using TOR IP

Description	An AWS API call was made using an IP address believed to be a TOR Exit Node. While TOR has legitimate uses for individuals, it should not be allowed in an enterprise setting and this may indicate an attempt at defense evasion.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Command and Control• Defense Evasion
MITRE ATT&CK Techniques	Multi-hop Proxy
Next Steps	Verify whether this AWS API call made via TOR was authorized

activity. If not, review other CloudTrail events for the Identify Access Management (IAM) principal that made the call and rotate credentials if applicable.

AWS API Watchlist IP Hit

Description	An AWS API was accessed from an IP on a user-defined or integrated watchlist. This may indicate that user credentials are compromised.
Associated Observation	AWS API Watchlist Access Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	<ul style="list-style-type: none">• AWS CloudTrail logs• North-South
MITRE ATT&CK Tactics	Discovery
MITRE ATT&CK Techniques	Cloud Service Discovery
Next Steps	Research the entity that accessed the AWS API, and the API functions that the entity called. Determine if the access has caused malicious activity, if that malicious activity is ongoing, and remediate the activity. Review your AWS security settings and ensure that you have taken proper precautions to prevent unauthorized access. Update your firewall rules to block the entity if this access is malicious.

AWS AppStream Image Shared

Description	An AWS AppStream Image was shared with another AWS account. This is a legitimate capability offered by AppStream, but Cisco Talos research has shown it also can be utilized for exfiltration or persistence.
Associated Observation	AWS CloudTrail Event Observation
History	0 days
Telemetry	AWS CloudTrail logs

MITRE ATT&CK Tactics	Exfiltration
MITRE ATT&CK Techniques	Transfer Data to Cloud Account
Next Steps	Verify whether this activity was authorized and the secondary account ID is recognized. If not, review other CloudTrail events for the Identify Access Management (IAM) principal that shared the image to determine the scope of the incident and rotate credentials if needed.

AWS CloudTrail Watchlist Hit

Description	AWS CloudTrail reported an event on a user-supplied watchlist. This identifies known suspicious activity.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration, allowing Secure Cloud Analytics permission to read CloudTrail logs, and configuring the AWS CloudTrail Watchlist in the Secure Cloud Analytics web UI.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting evidence and determine if the behavior is malicious, and requires further investigation.

AWS Config Rule Violation

Description	An AWS Config rule was violated. This indicates that the resource is not compliant with configured AWS Config rules.
Associated Observation	AWS Config Compliance Observations
History	0 days. Requires AWS integration, AWS configuration to stream configuration changes to an SNS topic, and an SQS queue to send the configuration changes, and additional configuration in

	Secure Cloud Analytics to retrieve the messages.
Telemetry	AWS API
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	Account Manipulation
Next Steps	Reference the alert and supporting observations to determine which AWS resource is the source of the configuration change and Config rule violation. Examine whether the configuration change is expected and normal in the course of business, such as a necessary update without updating the AWS Config rule. If the change is unexpected, revert the change and review the logs to determine which user or session implemented the change.

AWS Console Login Failures

Description	This user tried and failed to log in to the AWS Console several times. This may indicate an unauthorized user is attempting to gain access.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read IAM logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK Techniques	Brute Force
Next Steps	Determine if this was a legitimate login attempt by the owner of the account in question. If not, investigate additional CloudTrail events for the account, and rotate the credentials associated with it.

AWS Detector Modified

Description	An AWS GuardDuty detector was deleted or disabled. This alert
--------------------	---

may indicate an attempt to avoid detection of malicious activity.

Associated Observation

[AWS CloudTrail Event Observations](#)

History

0 days. Requires AWS integration and GuardDuty enabled.

Telemetry

AWS CloudTrail logs

MITRE ATT&CK Tactics

Defense Evasion

MITRE ATT&CK Techniques

Disable or Modify Tools

Next Steps

Reenable the GuardDuty detector to reenable GuardDuty. Review your logs to determine how the GuardDuty detector was deleted or disabled. Update your firewall rules and security settings to prevent access if this was due to malicious behavior.

AWS Domain Takeover

Description

An attempt was made to transfer a domain registered with AWS Route53 to another AWS account. This may indicate an attempt to hijack this domain, which can then be used in future attacks, or to hold the domain for ransom.

Associated Observation

[AWS CloudTrail Event Observations](#)

History

0 days. Requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Telemetry

AWS CloudTrail logs

MITRE ATT&CK Tactics

- Resource Development
- Impact

MITRE ATT&CK Techniques

Domains

Next Steps

Ensure this action was undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk. If this does not appear to be legitimate domain transfer review CloudTrail logs for the role that transferred the domain and the account it was transferred to. You can also file a report to ICANN or AWS support to report the

unauthorized transfer of domain and attempt to recover your domain.

AWS EC2 Startup Script Modified

Description	An AWS EC2 instance was stopped and user data was modified. User data allows passing a script which runs after the instance starts. This may indicate an attempt by a malicious actor to establish persistence or execute malicious code.
Associated Observation	AWS CloudTrail Event Observations
History	1 day. Requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Defense Evasion• Persistence• Execution
MITRE ATT&CK Techniques	<ul style="list-style-type: none">• Boot or Logon Initialization Scripts• Cloud Administration Command
Next Steps	Confirm whether or not the startup script was modified by a legitimate user for a valid activity. If not, review the startup scripts and the actions they perform. Examine the other actions the IAM user performed and rotate the credentials for the user as they can be considered compromised.

AWS ECS Credential Access

Description	An ECS Task Definition was registered with a container command which will obtain credentials from the AWS Instance Metadata Service. This may indicate an attacker is attempting to obtain service credentials.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Privilege Escalation • Persistence
MITRE ATT&CK Techniques	Cloud Instance Metadata API
Next Steps	Ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk. If this does not appear to be legitimate access, review CloudTrail logs for the user or role whose credentials were accessed, and consider rotating the credentials used to make the request.

AWS High Volume of API GetPasswordData Call Failures

Description	A high volume of AWS GetPasswordData calls were made and failed. This may indicate an attempt by a threat actor to obtain the administrator password for a running Windows instance.
Associated Observation	AWS CloudTrail Event Observations
History	1 day. Requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK Techniques	Credentials from Password Stores
Next Steps	Verify the legitimacy of the GetPasswordData calls using the supporting evidence. If not legitimate, review CloudTrail logs for the user who made the calls, and the instance ID of the instance for which the password was requested. Verify when the instance was launched and by whom, and take necessary action to quarantine the user to prevent any further actions.

AWS IAM Anywhere Trust Anchor Created

Description	A new IAM Roles Anywhere trust anchor has been created. This
--------------------	--

can be legitimate activity, but it could also indicate an adversary attempting to establish persistent access to the account from outside AWS.

Associated Observation

[AWS CloudTrail Event Observations](#)

History

0 days. Requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Telemetry

AWS CloudTrail logs

MITRE ATT&CK Tactics

Persistence

MITRE ATT&CK Techniques

Additional Cloud Roles

Next Steps

Verify the legitimacy of the newly created trust anchor using the associated observations. If not legitimate, disable the new trust anchor and review CloudTrail logs for the user who created the trust anchor, to see if they performed other suspicious activity.

AWS IAM User Takeover

Description

An AWS access key was created for another user. This may indicate an attacker is attempting to establish persistence in the event their method of initial access is revoked. It can be a sign of malicious activity or a violation of security policies.

Associated Observation

[AWS CloudTrail Event Observations](#)

History

0 days. Requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Telemetry

AWS CloudTrail logs

MITRE ATT&CK Tactics

Persistence

MITRE ATT&CK Techniques

Account Manipulation

Next Steps

Ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk. If this does not appear to be legitimate

access key creation, review CloudTrail logs for the user or role who created the access key, and consider rotating the credentials used to make the request and also immediately disable the access key that was created.

AWS Inspector Finding

Description	AWS Inspector reported a high or critical-severity finding for the device. This indicates that the resource is not complying with best practices.
Associated Observation	Amazon Inspector Finding Observations
History	0 days. Requires AWS integration, and enabling Inspector.
Telemetry	AWS API
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	Account Manipulation
Next Steps	Examine the finding in AWS Inspector, and take necessary actions to remediate.

AWS Lambda Backdoor Function Created

Description	A new AWS Lambda function has been created and associated with a new CloudWatch event. This might indicate an attempt for persistence by adding a backdoor to newly created resources.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration, allowing Secure Cloud Analytics permission to read CloudTrail logs and at least one Lambda function in AWS.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Privilege Escalation • Credential Access • Persistence

	<ul style="list-style-type: none"> • Execution
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Additional Cloud Credentials • Serverless Execution
Next Steps	<p>Verify the actions triggering the Lambda function and the code executed. The event pattern triggering the Lambda can be found in the request of the PutRule event and the function name is included in the request of the CreateFunction event. Review the attached observations and ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk. If not, revert the action and verify that the credentials used are not compromised.</p>

AWS Lambda Invocation Spike

Description	An AWS Lambda function was invoked a record number of times. This may indicate operational problems or a denial of service attack.
Associated Observation	AWS Lambda Metric Outlier Observations
History	14 days. Requires AWS integration, and at least one Lambda function in AWS.
Telemetry	AWS API
MITRE ATT&CK Tactics	Impact, Execution
MITRE ATT&CK Techniques	Resource Hijacking
Next Steps	<p>If the number of Lambda function invocations causes problems for your network, temporarily disable the Lambda function, pending the results of your investigation. Review the criteria necessary to invoke the AWS Lambda function, and why the Lambda function was triggered multiple times. Correct the criteria to ensure this does not recur. If an external malicious entity caused the Lambda function to trigger, update your block list and firewall rules to disallow this entity from accessing your network. Update the Lambda function logic if this exposes a flaw in the Lambda function.</p>

AWS Lambda Invoke Permission Added

Description	A new permission to invoke an AWS Lambda function from another AWS service, account, or organization was added. Access from an external account or organization might be an attempt to implement a backdoor in your AWS environment. This can be legitimate activity, but it could also indicate an adversary attempting to establish persistent access to the account from outside AWS.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	<ul style="list-style-type: none">• Event Triggered Execution• Serverless Execution
Next Steps	Verify the legitimacy of the newly created Lambda resource-based policy using the associated observations. Review the response field of the CloudTrail event, which will list the new permissions. The principal field points to the AWS service or account allowed to invoke the function. If not legitimate, revoke them and review CloudTrail logs searching for the user who created these permissions, to see if they performed other suspicious activity.

AWS Logging Deleted

Description	An AWS VPC Flow Log or CloudTrail log was deleted. This alert may indicate an attempt to remove history of malicious activity.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and VPC flow logging or CloudTrail logging enabled.

Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Defense Evasion
MITRE ATT&CK Techniques	Impair Defenses
Next Steps	Confirm whether or not the logging was intentionally deleted. If needed, take action to reverse the AWS VPC Flow Logs or CloudTrail changes.

AWS Logging Impairment

Description	AWS CloudTrail, DNS or VPC Flow Log collection was impaired. Either the collection of new logs was stopped, existing logs were deleted or an S3 Bucket Lifecycle Policy to delete future logs very shortly after their creation and storage was put in place. This may indicate an attempt by a threat actor to conceal other malicious behavior.
Associated Observation	AWS CloudTrail Event Observations
History	0 days
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Defense Evasion
MITRE ATT&CK Techniques	Disable or Modify Cloud Logs
Next Steps	Confirm whether or not the detected activity was legitimate. If needed, take action to reverse the changes, rotate any long-lived credentials for the user who made the change, and investigate CloudTrail events for other activities they performed.

AWS Multifactor Authentication Change

Description	Multifactor authentication was removed from a user account. Removing multifactor authentication is a violation of security best practices.
Associated	AWS CloudTrail Event Observations

Observation

History 0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Telemetry AWS CloudTrail logs

MITRE ATT&CK Tactics

- Defense Evasion
- Persistence

MITRE ATT&CK Techniques Multi-Factor Authentication

Next Steps Depending on your organization's security requirements, disable the account as necessary. Determine who removed multifactor authentication, and why. If it was removed because a person lost one of their multifactor authentication devices, replace the device, and reset multifactor authentication. If a malicious actor removed multifactor authentication, disable the account and reset credentials. Update your block list and firewall rules to disallow this entity from accessing your network.

AWS Organization Exit Attempt

Description An attempt was made by a child account to leave an AWS Organization. Threat actors can perform this technique to impair defenses or monitoring.

Associated Observation [AWS CloudTrail Event](#)

History 0 days

Telemetry AWS CloudTrail logs

MITRE ATT&CK Tactics Defense Evasion

MITRE ATT&CK Techniques Impair Defenses

Next Steps Verify whether this was authorized activity. If not, review other CloudTrail events for the IAM principal that made the call and rotate credentials if applicable. Also consider implementing a Service Control Policy at the Organization level to prohibit this action.

AWS Region Newly Utilized

Description	An AWS resource was detected in a previously unused region. This may indicate unsanctioned use of AWS resources.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Defense Evasion• Impact
MITRE ATT&CK Techniques	Unused/Unsupported Cloud Regions
Next Steps	Locate the AWS resource and determine if it is expected on your AWS deployment or not. If the AWS resource is not expected, remediate it as necessary. Reference the supporting evidence to see more details about who created the resource and the configuration.

AWS Repeated API Failures

Description	A user has performed multiple API calls resulting in failures due to insufficient privileges. This can indicate an adversary attempting to discover/enumerate information about their environment, establish persistence or escalate privileges.
Associated Observation	AWS CloudTrail Event Observations
History	3 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Discovery• Reconnaissance
MITRE ATT&CK Techniques	Cloud Service Discovery

Next Steps	Inspect the associated CloudTrail observations for the users and API calls. If the calls were not the result of legitimate user actions, assume the user is compromised. Investigate recent activity by this user using CloudTrail logs and take necessary action to quarantine the user to prevent any further actions. Attempt to determine the method of initial access and review IAM principals for unnecessary privileges.
-------------------	--

AWS Resource Inactive

Description	No recent activity has been seen for this AWS resource. This may indicate an unexpected outage.
Associated Observation	Unused AWS Resource Observations
History	14 days
Telemetry	AWS API
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	Service Stop
Next Steps	Determine if you need this AWS resource, or if you can remove it. If it is supposed to be operating or otherwise exhibit activity, check the AWS resource and determine why it is inactive. Remediate as necessary.

AWS Root Account Used

Description	An action was performed using the AWS root account. This is a violation of AWS best practices.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Privilege Escalation• Execution

MITRE ATT&CK Techniques	Cloud Accounts
Next Steps	Determine if the user or role should have root-level permissions. If not, update your configuration to reduce exposure of the AWS root account.

AWS Route 53 Hosted Zone Created

Description	A public Amazon Route 53 hosted zone was created. This may indicate a malicious attempt to redirect users to an external resource.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Resource Development
MITRE ATT&CK Techniques	Domains
Next Steps	If you did not create the public hosted zone, this could be a malicious attempt to redirect users from your AWS-hosted resources to an unintended external resource. Check the AWS CloudTrail Event Observations to investigate the new zone.

AWS Route53 Target Added

Description	A new AWS Route53 resource record was assigned to a device that was not previously associated with a Route53 resource record. This may indicate an attempt to maliciously redirect traffic.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs

MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	Domains
Next Steps	Reference the alert and supporting observations to gather information about the entity, then determine if it is intended on your network. Review your logs in AWS to determine what behavior the entity is exhibiting. If this is an expected entity, update your configuration to allow the entity.

AWS S3 Bucket Lifecycle Configured

Description	A new S3 Bucket Lifecycle configuration has been created that schedules the simultaneous permanent deletion of all files in the bucket. This alert may indicate a data destruction attempt.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	Data Destruction
Next Steps	Review the attached observations and ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk. If not, revert the action and verify that the credentials used are not compromised.

AWS Security Group Deleted

Description	An AWS VPC Security Group or ElastiCache Security Group was deleted. This may indicate an attempt to impair legitimate functionality.
Associated Observation	AWS CloudTrail Event Observations

History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	Account Access Removal
Next Steps	Verify if this was legitimate behavior. If not, investigate history for this IAM principal for other unauthorized activity.

AWS Snapshot Exfiltration

Description	An EC2 snapshot was modified to be accessible by another account. This alert may indicate an attacker is attempting to exfiltrate data.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Exfiltration
MITRE ATT&CK Techniques	Transfer Data to Cloud Account
Next Steps	Ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk.

AWS Stale Access Key

Description	AWS IAM access key exceeded the configurable age. This indicates that this key violates AWS best practices.
Associated Observation	AWS Architecture Compliance Observations
History	30 days. Requires AWS integration.

Telemetry	AWS API
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Verify that the IAM user account should still have access. Adjust your IAM policy to ensure keys are rotated more regularly.

AWS Unusually Large EC2 Instance

Description	An unusually large EC2 instance has been created. This alert may indicate an attacker has deployed large EC2 instances for resource hijacking purposes.
Associated Observation	Unusual EC2 Instance Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	Resource Hijacking
Next Steps	Examine the new devices in question and determine whether they are legitimately deployed or not.

Azure Activity Log IP Watchlist Hit

Description	The Azure Activity Log reported an event that was initiated by an IP address that matched a user-defined or an integrated watchlist. This may indicate that an unauthorized user has gained access to Azure.
Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs

MITRE ATT&CK Tactics	Discovery
MITRE ATT&CK Techniques	Cloud Service Discovery
Next Steps	Verify that the watchlist entry is correct. Reference the supporting observations for the IP address and determine if the behavior is malicious. Remediate the activity if it is due to malicious behavior. Review your Azure security settings and ensure that you have taken proper precautions to prevent unauthorized access. Update your firewall rules to block the IP address if this access is malicious.

Azure Activity Log Watchlist Hit

Description	The Azure Activity Log reported an event on a user-supplied watchlist. This identifies known suspicious activity.
Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	Cloud Administration Command
Next Steps	Verify that the watchlist entry is correct. Reference the supporting observations for the entity's traffic profile and determine if the behavior is malicious. Remediate the activity if it is due to malicious behavior. Review your Azure security settings and ensure that you have taken proper precautions to prevent unauthorized access. Update your firewall rules to block the entity if this access is malicious.

Azure Advisor Watchlist

Description	An Azure Advisor Recommendation was detected for a recommendation type on the watchlist.
Associated	Azure Advisor Recommendation Observations

Observation**History** 0 days. Requires Azure integration and Azure Advisor.**Telemetry** AWS API**MITRE ATT&CK
Tactics** N/A**MITRE ATT&CK
Techniques** N/A**Next Steps** Follow instructions provided by Microsoft to resolve the recommendation.

Azure Anomalous RunCommand

Description Azure RunCommand was successfully utilized to remotely execute a command or commands on an Azure Virtual Machine, and this behavior was anomalous. Though potentially benign, adversaries (including Advanced Persistent Threats) are known to utilize this capability.**Associated
Observation** [Azure Unusual Activity Observations](#)**History** 0 days. Requires Azure integration and Azure Activity Logs.**Telemetry** Azure Activity Logs**MITRE ATT&CK
Tactics** Execution**MITRE ATT&CK
Techniques** Cloud Administration Command**Next Steps** Verify whether this behavior was performed legitimately. If not, investigate and potentially isolate the Virtual Machine and user account or Service Principal used to perform the action.

Azure Exposed Services

Description An open service like a dashboard or a database is exposed to the Internet. This alert may indicate that sensitive data are inadvertently exposed. This alert is enabled by default.**Associated
Observation** [Azure Exposed Services Observations](#)

History	0 days. Requires Azure integration.
Telemetry	<ul style="list-style-type: none">• Azure API• Netflow
MITRE ATT&CK Tactics	Reconnaissance
MITRE ATT&CK Techniques	Gather Victim Host Information
Next Steps	Examine the permissions of the service in Azure and restrict them only to authorized users, domains or IPs.

Azure Firewall Deleted

Description	An Azure Firewall was deleted. This alert may indicate an attacker is attempting to impair network defenses, focusing primarily on firewalls that have been successfully deleted. The successful deletion of an Azure Firewall and may indicate an attempt to impair network defenses.
Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Defense Evasion• Impact• Persistence• Execution
MITRE ATT&CK Techniques	Disable or Modify Cloud Firewall
Next Steps	Ensure this action was undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security vulnerability.

Azure Function Invocation Spike

Description	An Azure function was invoked a record number of times. This alert may indicate operational problems or a denial of service
--------------------	---

attack.

Associated Observation

[Azure Functions Metric Outlier Observations](#)

History

14 days

Telemetry

Azure API

MITRE ATT&CK Tactics

- Impact
- Execution

MITRE ATT&CK Techniques

- Resource Hijacking
- Event Triggered Execution
- Serverless Execution

Next Steps

If the number of Azure function invocations causes problems for your network, temporarily disable the Azure function, pending the results of your investigation. Review the criteria necessary to invoke the Azure function, and why the Azure function was triggered multiple times. Correct the criteria to ensure this does not recur. If an external malicious entity caused the Azure function to trigger, update your block list and firewall rules to disallow this entity from accessing your network. Update the Azure function logic if this exposes a flaw in the Azure function.

Azure Key Vaults Deleted

Description

A key vault was deleted. This alert may indicate an attempt to disrupt service availability by deleting keys.

Associated Observation

[Azure Unusual Activity Observations](#)

History

0 days. Requires Azure integration and Azure Activity Logs.

Telemetry

Azure Activity Logs

MITRE ATT&CK Tactics

Impact

MITRE ATT&CK Techniques

Account Access Removal

Next Steps

Ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did

not create a security risk.

Azure Network Security Group Deleted

Description	An Azure Network Security Group was deleted. This alert may indicate an attacker is attempting to impair network defenses.
Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Defense Evasion • Impact • Persistence • Execution
MITRE ATT&CK Techniques	Disable or Modify Cloud Firewall
Next Steps	Ensure this action was undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security vulnerability.

Azure OAuth Bypass

Description	An action modifying the kubeconfig file has been detected. The kubeconfig file, also used by kubectl, contains details about Kubernetes clusters including their location and credentials. Attackers can get access to this file from a compromised client, using the listClusterAdminCredential action. Then, they can use it for accessing the clusters.
Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Privilege Escalation • Lateral Movement
MITRE ATT&CK	Cloud Accounts

Techniques

Next Steps Examine the details of the action taken to determine if this was legitimate or malicious and remediate the issue, if needed.

Azure Permissive Security Group

Description Azure Network Security Group has an associated Rule that is excessively permissive (open to all IP addresses). This may indicate that this security group is overly permissive.

Associated Observation [Azure Permissive Security Group Observations](#)

History 0 days. Requires Azure integration and at least one Network Security Group.

Telemetry Azure API

MITRE ATT&CK Tactics

- Defense Evasion
- Persistence
- Execution

MITRE ATT&CK Techniques Disable or Modify Cloud Firewall

Next Steps Reference the supporting evidence and click the links on the affected resources that lead to the Azure portal, where excessively permissive configuration settings may be modified..

Azure Permissive Storage Account

Description Storage account settings were recently configured to allow public access or access via unencrypted transport protocol. This may indicate that sensitive data is inadvertently exposed.

Associated Observation [Azure Permissive Storage Setting Observations](#)

History 0 days. Requires Azure integration and at least one storage account.

Telemetry Azure API

MITRE ATT&CK Tactics

- Exfiltration
- Collection

MITRE ATT&CK Techniques	Data from Cloud Storage
Next Steps	Examine the storage account permissions in Azure, and restrict permissions only to authorized users or domains. Restrict port ranges as needed.

Azure Resource Group Deleted

Description	A resource group was deleted. This alert may indicate an attempt to destroy data.
Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Data Destruction • Service Stop
Next Steps	Ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk

Azure Transfer Data To Cloud Account

Description	A publicly accessible snapshot was created for a virtual machine. This alert may indicate an attempt to exfiltrate data.
Associated Observation	Azure Unusual Activity Observations
History	0 days. Requires Azure integration and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	Exfiltration
MITRE ATT&CK Techniques	Transfer Data to Cloud Account
Next Steps	Ensure this action is undertaken purposefully by authorized

personnel, in accordance with applicable procedures, and did not create a security risk.

Azure Virtual Machine in Unused Location

Description	An Azure Virtual Machine has been created in a location not used in the recent past.
Associated Observation	Azure VM in Unused Location Observations
History	0 days. Requires Azure integration and granting Secure Cloud Analytics the Monitoring Reader role permissions to review Azure Subscriptions.
Telemetry	Azure API
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	Resource Hijacking
Next Steps	Review the supporting evidence to identify the virtual machine and its location. If the virtual machine is potentially malicious, shut it down and remediate as needed.

Cloud Metadata Service Credential Access

Description	A request to one of the public cloud Instance Metadata Service endpoints was made for credentials. This is common adversary behavior.
Associated Observation	Suspicious Endpoint Activity Observations
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK Techniques	Cloud Instance Metadata API
Next Steps	Determine if this request was made for legitimate reasons. If not,

investigate both the identity principal whose credentials were accessed and the instance from which the request was made.

Connection to TOR IP Address

Description	Traffic to The Onion Router (TOR) IP address was detected. TOR has legitimate privacy preserving features when used on a personal device, but adversaries are known to leverage it for Command and Control traffic and defense evasion. Even if utilized by a legitimate user, it can circumvent some security controls.
Associated Observation	Suspicious Endpoint Activity
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Command and Control• Defense Evasion
MITRE ATT&CK Techniques	Multi-hop Proxy
Next Steps	Verify if this behavior was authorized. If not, investigate other evidence from both the device and user associated with the behavior. Consider rotating the users credentials or even quarantining the device, if required.

Country Set Deviation

Description	Device has significantly deviated from the set of countries it usually communicates with. This may indicate a device is compromised.
Associated Observation	Country Set Deviation Observations
History	36 days
Telemetry	<ul style="list-style-type: none">• Netflow• North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Exfiltration

- Command and Control
- Initial Access

MITRE ATT&CK Techniques

Valid Accounts

Next Steps

Reference the supporting evidence to find the entities to which the entity has established connections, and their geolocation. Determine why it established these connections, and remediate the issue if it was due to malicious behavior.

Country Watchlist: New Long Session

Description

A device has established a long-lived connection with a host in a watchlisted country. These connections may indicate malicious behavior by users in these countries.

Associated Observation

[Long Session Observations](#)

History

2 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

- Exfiltration
- Persistence

MITRE ATT&CK Techniques

Exfiltration Over Alternative Protocol

Next Steps

Reference the supporting observations to see the traffic flow details. Investigate the reputation for the external IP address by selecting **Talos Intelligence** and **AbuseIPDB** from the IP address menu. If the external IP appears malicious, investigate the host machine or block the traffic using security groups or firewall rules.

Country Watchlist: Protocol Violation

Description

Device tried to communicate with a host in a user-supplied watchlisted country on an illegal protocol / port combination (e.g., UDP on port 22). This may indicate the presence of a malicious covert communications channel.

Associated Observation	Bad Protocol Observations
History	0 days. You must configure the Country Watchlist with at least one country.
Telemetry	<ul style="list-style-type: none"> • ETA • Netflow • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Command and Control • Defense Evasion
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Non-Standard Port • Non-Application Layer Protocol
Next Steps	Reference the supporting observations to determine why the entity used the unusual protocol/port combination to communicate with the entity in the watchlisted country. Determine what was transferred in the communication. If deemed malicious, update your firewall and blocklist rules to prevent further access with this protocol/port combination, and with this geolocation, unless there is a business reason for allowing it.

Country Watchlist: Remote Access

Description	Device has been accessed from a remote host in a user-supplied watchlisted country. This may indicate a device is compromised.
Associated Observation	Remote Access Observations
History	0 days. This alert requires configuring the Country Watchlist with at least one country.
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Initial Access
MITRE ATT&CK Techniques	Valid Accounts

Next Steps	Reference the supporting observations to identify the external entity, and how the external entity interacted with your internal entity. Determine if the behavior was malicious, and if any data was exfiltrated, as well as what actions were taken on the internal entity. If needed, add additional firewall or security group rules to prevent future access.
-------------------	--

DC Sync Attack Behavior

Description	Suspicious behaviors were detected on the endpoint that are known to be part of the DC Sync attack.
Associated Observation	Suspicious Endpoint Activity
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK Techniques	DCSync
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

DNS Abuse

Description	Device has been sending unusually large DNS packets. This may indicate an attacker using the DNS protocol as a covert communications channel to exfiltrate data.
Associated Observation	Unusual Packet Size Observations
History	0 days
Telemetry	<ul style="list-style-type: none">• Netflow• North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Exfiltration• Impact

MITRE ATT&CK Techniques

- Exfiltration Over Alternative Protocol
- Reflection Amplification

Next Steps

Reference the supporting evidence to determine to which DNS server the entity is sending the DNS packets. If the DNS server is legitimate, add it to the VPN subnets in Subnet configuration. Perform further research on why the entity is sending large DNS packets. If the DNS server is not legitimate, review the entity's logs and determine why the entity is sending the DNS packets, and if it is malicious behavior. Remediate any malicious behavior. Update your firewall rules as necessary to prevent further malicious behavior.

Email Spam

Description

Device has had an anomalous increase in connections with external mail servers. This may indicate the device is compromised.

Associated Observation

- [External Mail Client Connections Observations](#)
- [Historical Outlier Observations](#)
- [New Profile Observations](#)

History

36 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

- Resource Development
- Initial Access

MITRE ATT&CK Techniques

Email Accounts

Next Steps

Reference the supporting observations and determine whether the external mail servers are expected and legitimate. If this is the case, determine why the entity has increased traffic with these servers. Otherwise, determine the cause of the malicious behavior. Quarantine the affected entity and remove malware. Ensure that other entities on your network are not similarly affected.

Emergent Profile

Description	A highly sensitive entity has traffic that fits a new profile. For example, an entity that starts accepting FTP connections may be exposing sensitive data.
Associated Observation	New Profile Observations
History	14 days
Telemetry	Netflow
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Lateral Movement• Command and Control• Initial Access
MITRE ATT&CK Techniques	<ul style="list-style-type: none">• Exfiltration Over Alternative Protocol• External Remote Services
Next Steps	Reference the entity's new traffic profile in the supporting observations, and whether it is expected, especially in light of the previous profile or role. For example, if an entity has been repurposed from an FTP server to a mail server, this shift in behavior is expected. If it is not expected, investigate why the entity's traffic has changed, and if it is malicious.

Empire Command and Control

Description	An entity has established new periodic connections that appear to be part of an Empire PowerShell Command and Control channel. This alert may indicate the device is compromised.
Associated Observation	Heartbeat Observations
History	1 day
Telemetry	<ul style="list-style-type: none">• Netflow• North-South
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK	Non-Application Layer Protocol

Techniques

Next Steps Review the entity's traffic in the supporting observations, identify the entity to which it is establishing the heartbeat connections, and determine if the traffic is anticipated or malicious. If malicious, determine if other entities on your network are similarly affected. Quarantine the entities and remove any malware. Update your block list and firewall rules to disallow the command and control servers' access to your network.

Endpoint Exfiltration of AWS Credentials

Description AWS credentials were accessed by a process that made a network connection. This can indicate exfiltration of these credentials

Associated Observation [Suspicious Endpoint Activity](#)

History 0 days

Telemetry Cisco NVM

MITRE ATT&CK Tactics Credential Access

MITRE ATT&CK Techniques Credentials In Files

Next Steps Verify if this behavior was legitimate. If not, investigate the endpoint in question further, review AWS CloudTrail logs for actions taken by any users in the credentials file on the endpoint, and rotate the AWS credentials.

Excessive Access Attempts (External)

Description Device has many failed access attempts from an external device. For example, a remote device trying repeatedly to access an internal server using SSH or Telnet. This may indicate the device is compromised.

Associated Observation

- [Multiple Access Failures Observations](#)
- [Remote Access Observations](#)

History 0 days

Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK Techniques	Brute Force
Next Steps	Reference the supporting evidence and ensure that the external entity is abnormal and unexpected. If it is normal and expected, determine why a user or machine keeps failing to login, such as if credentials changed, but the user or machine was not given the updated credentials. If the external entity is unknown, update your firewall or security group rules to limit access for the remote control protocol. Update your block list and firewall rules to disallow this entity's access to your network if the entity is potentially malicious.

Excessive Connections to Network Printers

Description	This entity initiates too many connections to network printers. This behavior may indicate a denial-of-service attack, or an attempt to exfiltrate data by printing documents.
Associated Observation	Excessive Connections to Network Printers Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • East-West • Netflow
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Credential Access • Impact • Discovery
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Endpoint Denial of Service • Brute Force • Peripheral Device Discovery
Next Steps	Reference the supporting observations and determine how the entity is communicating with the network printers. Quarantine

the entity and remove malware if the communications are malicious. Examine the printer job queues to determine what actions they are performing. Clear the queues if the printer is tasked to print confidential documents. Disconnect the printers' internet access if they are tasked to transmit confidential information to external entities. Remove any malware from the printers as necessary.

GCP API Call Using TOR IP

Description	An GCP API call was made using an IP address believed to be a TOR Exit Node. While TOR has legitimate uses for individuals, it should not be allowed in an enterprise setting and this may indicate an attempt at defense evasion.
Associated Observation	GCP Watchlist Activity
History	0 days
Telemetry	GCP Audit Logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Command and Control • Defense Evasion
MITRE ATT&CK Techniques	Multi-hop Proxy
Next Steps	Verify whether this GCP API call made via TOR was authorized activity. If not, review other GCP events for the Identify Access Management (IAM) principal that made the call and rotate credentials if applicable.

GCP Cloud Function Invocation Spike

Description	A GCP cloud function was invoked a record number of times. This may indicate operational problems or a denial of service attack.
Associated Observation	GCP Cloud Function Metric Outlier Observations
History	14 days
Telemetry	GCP API

MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Impact• Execution
MITRE ATT&CK Techniques	Resource Hijacking
Next Steps	Review the GCP cloud function and intended code. Determine if the function is corrupt or if an additional environmental factor caused the function to change behavior.

GCP Operations Log Watchlist Hit

Description	Google Cloud Platform (GCP) Stackdriver Logs reported an event on a user-supplied watchlist.
Associated Observation	GCP Watchlist Activity Observations
History	0 days
Telemetry	GCP Audit Logs
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Review the supporting observations to determine which watchlist entry generated the event. Remediate as necessary. Log in to GCP and update your watchlist as necessary.

Geographically Unusual AWS API Usage

Description	An AWS API has been accessed from a remote host in a country that doesn't normally access the API. For example, creating an IAM role from an unusual foreign IP. This may indicate that a user account is compromised.
Associated Observation	AWS CloudTrail Event Observations
History	14 days. Establish the normal geolocations for IP addresses that access the AWS API in your deployment. This alert also requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Execution • Discovery • Initial Access
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Cloud Service Discovery • Cloud Accounts • Cloud Administration Command
Next Steps	Reference the supporting observations and determine what action the entity took, and why it took the action. If the entity is expected, but is accessing the internet from another country than expected, confirm that the user identity was not compromised, then snooze the alert for that entity for the period of time they are traveling. If the user's identity was compromised, immediately disable that user account.

Geographically Unusual Azure API Usage

Description	The Azure API has been accessed from a remote host in a country that doesn't normally access the API. For example, creating an IAM role from an unusual foreign IP. This may indicate a user account is compromised.
Associated Observation	Azure Unusual Activity Observations
History	14 days
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Execution • Discovery • Initial Access
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Cloud Service Discovery • Cloud Accounts • Cloud Administration Command
Next Steps	Reference the supporting evidence and determine what action the entity took, and why it took the action. If the access is malicious, update your firewall or security group rules to prevent

further access and determine what actions were taken on the system. Remediate the action.

Geographically Unusual Remote Access

Description	Device has been accessed from a remote host in a country that doesn't normally access the local network. For example, a local server accepting an SSH connection from a foreign source. This may indicate misuse or a compromised device.
Associated Observation	Remote Access Observations
History	30 days
Telemetry	<ul style="list-style-type: none">• Netflow• North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Reconnaissance• Initial Access
MITRE ATT&CK Techniques	<ul style="list-style-type: none">• External Remote Services• Active Scanning
Next Steps	Reference the supporting evidence and determine what action the entity took, and why it took the action. If the entity is expected, but is accessing the internet from another country than expected, update your firewall settings to allow this traffic. Remediate the action, and update your blocklist and firewall rules to disallow the entity from accessing your network if this is malicious behavior.

Heartbeat Connection Count

Description	This entity has established new periodic connections with many remote entities, which might indicate unauthorized P2P traffic or botnet activity.
Associated Observation	Heartbeat Observations
History	8 day
Telemetry	<ul style="list-style-type: none">• Netflow• North-South

MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Non-Application Layer Protocol • Application Layer Protocol
Next Steps	<p>Reference the supporting observations and determine the entities to which the affected entity is establishing the heartbeat connections, and confirm that they are not expected.</p> <p>Understand the purpose for the periodic connections, and update your firewall and blocklist rules to prevent further access.</p>

High Bandwidth Unidirectional Traffic

Description	Device started sending large amounts of data to new remote hosts. For example, malware might cause an infected host to attack a website by directing a host to send lots of data to a vulnerable service. This may indicate the device is compromised.
Associated Observation	New High Throughput Connection Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Impact • Exfiltration
MITRE ATT&CK Techniques	Automated Exfiltration
Next Steps	<p>Reference the supporting observations for flow details, and determine why the entity is sending large amounts of traffic. If the traffic is permissible, snooze the alert for this host. If the traffic is not permissible, investigate what software on the host is responsible for the malicious traffic.</p>

ICMP Abuse

Description	Device has been sending unusually large ICMP packets to a new external server. This alert may indicate an attacker using the
--------------------	--

ICMP protocol as a covert communications channel to exfiltrate data.

Associated Observation

- [Unusual Packet Size Observations](#)
- [New External Server Observations](#)

History

0 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

Exfiltration

MITRE ATT&CK Techniques

- Exfiltration Over Alternative Protocol
- Network Denial of Service

Next Steps

Reference the supporting observations to determine to which external server the entity is sending the ICMP packets. Review the entity's logs and determine why the entity is sending the ICMP packets, and if it is malicious behavior. Remediate any malicious behavior. To prevent potential ICMP tunnel exfiltration attempts in the future, update your firewall rules to disallow external ICMP traffic.

IDS Emergent Profile

Description: This entity exhibits a new type of traffic at the same time it is flagged as suspicious by an IDS. This may indicate the device is compromised.

Associated Observation

- [Intrusion Detection System Notice Observations](#)
- [New Profile Observations](#)

History

14 days. This alert requires one of the following:

- Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator with a Secure Firewall appliance. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.
- Suricata IDS

Telemetry

- Firewall
- Netflow

MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the profile details in the supporting observations and determine if the new traffic profile is malicious. If malicious, quarantine the host and remove the offending software. If not, snooze the alert for this host.

IDS Notice Spike

Description	This entity triggered an abrupt rise in IDS observations.
Associated Observation	Intrusion Detection System Notice Observations
History	1 day. Requires one of the following: <ul style="list-style-type: none"> • Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator with a Secure Firewall appliance. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information. • Suricata IDS • Zeek IDS
Telemetry	Firewall
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting observations to identify the entity, then determine why it triggered multiple notices. Review and remediate the IDS notices. Determine if other entities may be affected. Update your firewall and blocklist rules as necessary.

Inbound Port Scanner

Description	Device belonging to a sensitive subnet was port-scanned by an external device. This may indicate an attacker is scanning for
--------------------	--

vulnerabilities.

Associated Observation

[External Port Scanner Observations](#)

History

1 day

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

- Discovery
- Reconnaissance

MITRE ATT&CK Techniques

- Network Service Discovery
- Gather Victim Network Information

Next Steps

Reference the supporting observations to identify the external entity that port scanned your internal entity. Determine if it is the result of planned penetration testing or other intended behavior, or if it is malicious. Update your IP scanner and allow list rules to allow the traffic if it is intended. Block the traffic if it is not intended. Update your firewall rules as necessary, including port access.

Internal Connection Spike

Description

A workstation had a sudden increase in internal connections. This may indicate internal scanning activity or attempted lateral movement.

Associated Observation

[Record Metric Outlier Observations](#)

History

0 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

- Lateral Movement
- Discovery

MITRE ATT&CK Techniques

- Network Service Discovery
- Remote Services

Next Steps

Reference the supporting observations to determine why the

entity is establishing multiple connections. Determine if it is performing scanning activity because of penetration testing or another allowed purpose, or if it is malicious behavior. Remediate the behavior as necessary.

Internal Connection Watchlist Hit

Description	Two IP addresses that shouldn't communicate were observed exchanging based on a user-supplied watchlist. This identifies known suspicious activity.
Associated Observation	Internal Connection Watchlist Observations
History	0 days
Telemetry	<ul style="list-style-type: none">• East-West• Netflow
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	Event Triggered Execution
Next Steps	<p>Reference the supporting observations to determine which watchlist rule matched and to analyze flow details. If this connection is permissible, update the watchlist rule to allow it.</p> <p>The system generates this alert only if a user enters a segmentation rule.</p>

Internal Port Scanner

Description	Device has started a port scan on a device internal to your network. This may indicate that an attacker is scanning for vulnerabilities.
Associated Observation	Internal Port Scanner Observations
History	7 days
Telemetry	<ul style="list-style-type: none">• East-West• Netflow• North-South

MITRE ATT&CK Tactics	Discovery
MITRE ATT&CK Techniques	Network Service Discovery
Next Steps	Reference the supporting observations to understand the type of scanning activity. Scanning activity is often associated with a compromised host that is searching for data or other hosts to infect. To gain more context, search for observations related to the entity that the system logged around the same time (such as watchlist interactions). This may provide additional information about the behavior.

Invalid Mac Address

Description	A device with an organizationally unique identifier (OUI) for an unregistered Mac address was detected using Cisco ISE telemetry. This is not always malicious, but it can indicate an attempt to bypass Mac Access Control (Mac filtering), conduct an Adversary-in-the-Middle technique, or impair other defensive capabilities.
Associated Observation	Invalid MAC Address
History	0 days
Telemetry	Cisco ISE
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Lateral Movement • Defense Evasion
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Masquerading • Impair Defenses
Next Steps	Verify the type of device, locate it and identify why the incorrect MAC address was set. If the MAC address change was not intentional, isolate the device and investigate further. If the MAC address change was intentional, set the correct (locally administered address) MAC address.

ISE Jailbroken Device

Description	A jailbroken device was detected. This does not necessarily indicate an active threat in isolation, but is a vulnerability that may increase organizational risk.
Associated Observation	ISE Suspicious Activity
History	0 Days. This alert requires integration with ISE.
Telemetry	Cisco ISE
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Privilege Escalation• Initial Access
MITRE ATT&CK Techniques	<ul style="list-style-type: none">• Drive-by Compromise• Device Administrator Permissions
Next Steps	Jailbroken devices can run malicious software from unauthorized sources other than official application stores. If the device is company owned, then isolate it from the corporate network and verify policy for the mobile devices. If the device is a private device, then verify the reason it is registered in the Mobile Device Management system and isolate it from the corporate network. Check with the owner of the device if the jailbreaking was intentional. If the owner was not aware of that, then it might point to a breach in the mobile device. Reinstalling the operating system on the mobile device is recommended.

LDAP Connection from Anomalous Process

Description	The device was detected running a non-standard LDAP process. This might indicate a credential theft attempt.
Associated Observation	Suspicious Endpoint Activity
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK	Domain Accounts

Techniques

Next Steps Investigate the processes executed and verify if their usage is justified by business needs.

LDAP Connection Spike

Description Device attempted to contact an unusually large number of internal LDAP servers. This alert may be an indication of malware or abuse.

Associated Observation [IP Scanner Observations](#)

History 9 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

- Credential Access
- Lateral Movement
- Discovery

MITRE ATT&CK Techniques

- Network Service Discovery
- Domain Account

Next Steps Reference the supporting observations and determine why the entity is establishing connections with multiple LDAP servers, what types of actions the entity is taking, and if this is malicious behavior. If data was exfiltrated, follow your organization's guidelines for dealing with data exfiltration. Quarantine the entity as necessary to remove malware.

Malicious Process Detected

Description A process running has a hash matching one in a list of known malicious hashes.

Associated Observation [Suspicious Endpoint Activity Observations](#)

History 0 days

Telemetry Cisco NVM

MITRE ATT&CK N/A

Tactics**MITRE ATT&CK
Techniques**

N/A

Next Steps

Isolate the endpoint and investigate to determine whether a malicious executable was run.

Malware Spike

Description

Device triggered an abrupt rise in malware events based on firewall logs.

**Associated
Observation**

[Malware Event Observations](#)

History

1 day. Requires integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator with a Secure Firewall appliance. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Telemetry

- Firewall
- North-South

**MITRE ATT&CK
Tactics**

N/A

**MITRE ATT&CK
Techniques**

N/A

Next Steps

Reference the supporting observations to identify the entity, then determine why it triggered multiple malware events. Review and remediate the malware events. Determine if other entities may be affected. Update your firewall and blocklist rules as necessary.

MFA Disabled for Azure

Description

MultiFactor Authentication has been disabled for a user in a Microsoft Azure environment, which makes unauthorized access easier and may indicate attempted persistence.

**Associated
Observation**

[Suspicious Microsoft Entra ID Audit Logs Activity](#)

History	0 Days
Telemetry	<ul style="list-style-type: none"> • Azure Audit Logs • North-South
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	Multi-Factor Authentication
Next Steps	Start by examining additional log events for the identity principal that disabled the MFA. Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Microsoft Defender for Cloud Event

Description	Microsoft Defender for Cloud reported a medium or high severity event.
Associated Observation	Azure Security Event Observations
History	0 days. Requires Azure integration, Microsoft Defender for Cloud - Standard tier, and Azure Activity Logs.
Telemetry	Azure Activity Logs
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Review the supporting evidence to identify the medium or high severity event. Log into Microsoft Defender for Cloud and review the event. Remediate as needed.

NetBIOS Connection Spike

Description	Source attempted to contact large number of hosts using NetBIOS. This can be an indication of malware or abuse.
Associated Observation	IP Scanner Observations

History	9 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Discovery
MITRE ATT&CK Techniques	Network Service Discovery
Next Steps	Reference the supporting evidence to determine the host and analyze the traffic flow details. NetBIOS is not a commonly used protocol, so any connection spike events would likely be malicious. If detected, review what applications are using NetBIOS and if that traffic is legitimate.

Network Population Spike

Description	A record number of IP addresses were observed communicating on the network. This may indicate spoofing of source addresses.
Associated Observation	Population Spike Observations
History	36 days
Telemetry	<ul style="list-style-type: none"> • East-West • Netflow
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Impact • Defense Evasion
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Network Denial of Service • Impair Defenses • Resource Hijacking
Next Steps	Reference the supporting observations associated with the alert and determine if the IP addresses are legitimate entities. If they are not legitimate, locate the source of the spoofed addresses, and remediate as necessary.

Network Printer with Excessive Connections

Description	This printer initiates too many connections. This may indicate
--------------------	--

that the device is compromised.

Associated Observation

[Network Printer with Excessive Connections Observations](#)

History

0 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

N/A

MITRE ATT&CK Techniques

N/A

Next Steps

Review the established connections, and the entities that established connections with the printer. Reference the supporting observations to see what type of connections were established by the printer. If the connections indicate the printer is compromised, quarantine the printer and consider removing and re-installing the operating systems.

New External Connection

Description

Device normally doesn't talk to external devices, but has recently. This may indicate that an internal device is unexpectedly exposed to the Internet.

Associated Observation

[New External Connection Observations](#)

History

35 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

N/A

MITRE ATT&CK Techniques

N/A

Next Steps

Reference the supporting observations and traffic flow details to determine if the traffic is legitimate or suspicious. Some very static entities occasionally call to an external IP (e.g., a printer checking for a software update). In this case, snooze the alert or

add that external IP range to the VPN Subnets.

New Internal Device

Description	A new device has appeared on a restricted subnet range after not being seen in the lookback period. This may indicate an unexpected device has joined the network.
Associated Observation	New Internal Device Observations
History	21 days. Requires selecting New Internal Device on the Subnet Configuration page.
Telemetry	<ul style="list-style-type: none"> • East-West • Netflow
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Persistence • Resource Development • Initial Access
MITRE ATT&CK Techniques	Hardware Additions
Next Steps	Reference the supporting evidence to determine if this entity is an expected entity, and is merely new to your network. If the entity is suspicious, determine the MAC address by accessing the local switch.

New IP Scanner

Description	Device started scanning the local IP network. This may indicate that an attacker is inside the network, scanning for vulnerabilities.
Associated Observation	IP Scanner Observations
History	9 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Discovery
MITRE ATT&CK	Network Service Discovery

Techniques**Next Steps**

Reference the supporting observations and investigate why the external entity is scanning the network. Determine if it is the result of penetration testing or other intended behavior, or if it is malicious. Update your IP scanner and firewall rules to allow the traffic if it is intended. If potentially malicious, search for associated observations for the entity or user who owns the machine to determine what software caused the scanning activity.

New Remote Access

Description

This entity has been accessed (e.g., via SSH) from a remote host for the first time in recent history. This may indicate that the device is compromised.

Associated Observation

[Remote Access Observations](#)

History

36 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

Initial Access

MITRE ATT&CK Techniques

- External Remote Services
- Valid Accounts

Next Steps

Reference the supporting observations to determine why the entity is being accessed by the external entity, and if it is a legitimate form of access. Also determine (based on the observations) if there were multiple access attempts to the source entity prior to this access, whether from this external entity or another external entity. Update your firewall and blocklist rules based on this information.

New SNMP Sweep

Description

Device attempted to reach a large number of hosts using SNMP. This can be an indication of malware or abuse.

Associated

[IP Scanner Observations](#)

Observation**History** 9 days**Telemetry**

- Netflow
- North-South

MITRE ATT&CK Tactics Discovery**MITRE ATT&CK Techniques** Network Service Discovery**Next Steps** Reference the supporting evidence to determine if the entity is intended to track network entities over SNMP, and if this behavior is malicious. If the activity is not part of planned penetration testing or otherwise intended behavior, quarantine the entity and remediate the issue. Determine if any of the entities have been affected, such as updated configuration or compromised security settings, and remediate any issues. If the entity is expected to perform SNMP sweeps, add the entity to the Scanner Watchlist.

New Unusual DNS Resolver

Description Device contacted a DNS resolver that it doesn't normally use. For example, an attacker could cause a DNS resolver to redirect a popular website to a domain that serves additional malware. This may indicate misconfiguration or the presence of malware.**Associated Observation** [Unusual DNS Resolver Observations](#)**History** 7 days**Telemetry**

- Netflow
- North-South
- Passive DNS

MITRE ATT&CK Tactics

- Resource Development
- Command and Control

MITRE ATT&CK Techniques

- Application Layer Protocol
- Compromise Infrastructure

Next Steps Verify the entity's configuration to ensure that it is configured with the proper DNS settings. If so, determine what software is making the DNS lookup. Block the external IP address if the traffic is deemed malicious.

Non-Service Port Scanner

Description Device started scanning the local network on a port not associated with a common service. This alert may indicate that an attacker is inside the network, scanning for vulnerabilities.

Associated Observation [IP Scanner Observations](#)

History 9 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics Discovery

MITRE ATT&CK Techniques Network Service Discovery

Next Steps Reference the supporting observations and investigate why the external entity is scanning the network. Determine if it is the result of penetration testing or other intended behavior, or if it is malicious. Update your IP scanner and firewall rules to allow the traffic if it is intended. If potentially malicious, search for associated observations for the entity or user who owns the machine to determine what software caused the scanning activity.

Outbound LDAP Connection Spike

Description Device is communicating with a large number of external hosts using an LDAP port. This alert may indicate a possible infected host or an internally initiated port scan.

Associated Observation [IP Scanner Observations](#)

History 0 days

Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Impact • Reconnaissance
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Active Scanning • Automated Exfiltration • Network Denial of Service
Next Steps	Reference the supporting observations and determine to which entities the source entity is sending traffic, what type of traffic, and if this is an update to the entity's roles or responsibilities, or if this is unintended. If this is unintended, remediate the issue. Update your firewall and blocklist rules to prevent this access.

Outbound Traffic Spike

Description	Device started sending a much larger amount of traffic to external destinations than before. This may indicate data exfiltration.
Associated Observation	<ul style="list-style-type: none"> • Record Metric Outlier Observations • Record Profile Outlier Observations • New Large Connection (External) Observations
History	14 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Impact • Exfiltration
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Automated Exfiltration • Network Denial of Service
Next Steps	Reference the supporting observations to determine the nature of the traffic and where it was sent (e.g., a large Dropbox upload). If the traffic is suspicious, contact the user or machine owner to determine why the traffic was moved externally. Block traffic as needed at the perimeter.

Permissive Amazon Elastic Kubernetes Service Cluster Created

Description	A new Amazon Elastic Kubernetes Service cluster has been created that allows access from any host. This alert may indicate that sensitive resources or data are at risk.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Execution
MITRE ATT&CK Techniques	<ul style="list-style-type: none">• Container and Resource Discovery• Cloud Administration Command
Next Steps	Examine the Amazon Elastic Kubernetes Service cluster settings and network security settings and restrict access as much as possible without impacting business needs.

Permissive AWS S3 Access Control List

Description	A new ACL has been created that allows permissive access to an S3 bucket. This may be a misconfiguration and might lead to unauthorized access to stored data.
Associated Observation	AWS CloudTrail Event Observations
History	0 days
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	Exfiltration
MITRE ATT&CK Techniques	Data from Cloud Storage
Next Steps	Examine the access control list and determine if the S3 bucket access permission is properly constrained. If it is misconfigured,

correct the entry.

Permissive AWS Security Group Created

Description	A new AWS security group has been created that allows access from any host on unsafe ports. This may indicate that sensitive data is at risk.
Associated Observation	AWS CloudTrail Event Observations
History	0 days. Requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.
Telemetry	AWS CloudTrail logs
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Persistence • Execution • Defense Evasion
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Account Manipulation • Disable or Modify Cloud Firewall
Next Steps	Examine the AWS security group settings either using the AWS console or the AWS visualizations page, and then restrict access as necessary.

Persistent Remote Control Connections

Description	Device is receiving persistent connections from a new host on a remote control protocol like Remote Desktop or SSH. This may indicate that a firewall rule or ACL is overly permissive.
Associated Observation	<ul style="list-style-type: none"> • New External Server Observations • Persistent External Server Observations
History	7 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Initial Access
MITRE ATT&CK	External Remote Services

Techniques**Next Steps**

Adjust firewall or security group rules to prevent malicious attempts to repeatedly access the entity. Confirm that the local entity has not been breached by checking [Remote Access Observations](#) or the entity.

Port 8888: Connections from Multiple Sources

Description

Multiple devices transferred files to a host serving on a lazy port. This might indicate an ex-filtration attempt.

This alert applies only when the devices and hosts are internal, primarily when multiple internal devices transfer files to an internal host serving on a lazy port. This might indicate an exfiltration attempt. This alert is disabled by default. Make sure to enable this alert, if needed.

Associated Observation

[Suspicious Endpoint Activity Observations](#)

History

0 Days

Telemetry

Cisco NVM

MITRE ATT&CK Tactics

Command and Control

MITRE ATT&CK Techniques

Automated Exfiltration

Next Steps:

Verify if the host serving on the port is a legitimate server.

Potential Database Exfiltration

Description

A statistically unusual amount of data was transferred from a database server to a client. This may indicate an unauthorized transfer of information, or other malicious behavior.

Associated Observation

[New High Throughput Connection Observations](#)

History

7 days

Telemetry

Netflow, North-South

MITRE ATT&CK Tactics

Exfiltration

MITRE ATT&CK Techniques

Exfiltration Over C2 Channel

Next Steps

Examine the client entity to determine if the behavior is expected in the normal course of business, such as a new scheduled backup. If it is malicious, determine what was transferred. Follow your organization's guidelines on data exfiltration.

Potential Data Exfiltration

Description

This entity downloaded a sizeable chunk of data from an internal entity that it doesn't communicate with regularly. Shortly after that, the entity uploaded a similar amount of data to an external entity. This may indicate an unauthorized transfer of information, or other malicious behavior. This alert is enabled by default.

Associated Observation[Potential Data Forwarding Observations](#)**History**

0 Days

Telemetry

- East-West
- Netflow
- North-South

MITRE ATT&CK Tactics

Exfiltration

MITRE ATT&CK Techniques

- Automated Exfiltration
- Exfiltration Over C2 Channel
- Exfiltration Over Alternative Protocol

Next Steps

Reference the supporting observation to determine the volume of traffic and the client entity to determine if the behavior is expected in the normal course of business, such as a new scheduled backup. If it is malicious, determine what was transferred. Follow your organization's guidelines on data exfiltration.

Potential Gamaredon C2 Callout

Description

A command line utility was used to contact a URL associated with the command-and-control servers of a threat actor known

as Gamaredon. Gamaredon (also known as Armageddon, Primitive Bear, and ACTINIUM) is an APT active since 2013 known to leverage spearphishing to infect victims with custom malware.

Associated Observation	Suspicious Endpoint Activity Observations
History	0 Days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Command and Scripting Interpreter
Next Steps	Determine if this was legitimate activity, and if not investigate and potentially quarantine the device that made the connection.

Potential GhostPulse Malware C2

Description	A device exhibited behavior similar to that of the GhostPulse malware family.
Associated Observation	Suspicious Endpoint Activity Observations
History	0 Days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Web Protocols
Next Steps	Investigate the processes executed and verify if their usage is justified by business needs.

Potentially Harmful Hidden File Extension

Description	Device has encountered a file with a potentially harmful hidden extension. This may indicate the device has downloaded malware.
--------------------	---

Associated Observation	Multiple File Extensions Observations
History	0 Days. Requires one or more of following: <ul style="list-style-type: none"> • Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator with a Firepower appliance. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information. • Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.
Telemetry	<ul style="list-style-type: none"> • ETA • Firewall
MITRE ATT&CK Tactics	Execution
MITRE ATT&CK Techniques	User Execution
Next Steps	Reference the supporting evidence to determine if the file is malware, or why it has the hidden extension. Understand where the file has been transferred on your network, and which entities are potentially infected by the malware. Quarantine affected entities and clear malware from them

Potentially Vulnerable Remote Control Protocol

Description	This entity was observed using an older version of a remote control application (e.g., OpenSSH). It may be at risk from known security vulnerabilities.
Associated Observation	Insecure Transport Protocol Observations
History	1 day. Requires Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.
Telemetry	<ul style="list-style-type: none"> • ETA • North-South

MITRE ATT&CK Tactics

- Execution
- Defense Evasion

MITRE ATT&CK Techniques

- Exploitation for Defense Evasion
- Weaken Encryption
- Downgrade Attack

Next Steps

Reference the supporting evidence to determine what application the entity is using, what connection it established, and to which entity. If the remote control application is otherwise allowed by your organization, update the application to the latest version, and update the entity's security settings to comply with your organization's use policy. If the remote control application is not allowed by your organization, determine if the installation was by an authorized or unauthorized individual, and remove the application.

Potential System Process Impersonation

Description

A process with a name that looks like a common process has been executed indicating a process impersonation.

Associated Observation

[Suspicious Endpoint Activity Observations](#)

History

0 days

Telemetry

Cisco NVM

MITRE ATT&CK Tactics

Defense Evasion

MITRE ATT&CK Techniques

Masquerade Task or Service

Next Steps:

Verify if it is a known legitimate process. If not isolate the endpoint and verify if a malicious executable has been run.

Powershell RDP Connection

Description

The system utility Powershell was seen making connections over the RDP port, which is indicative of RDP connections.

Associated Observation

[Suspicious Endpoint Activity](#)

History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Lateral Movement
MITRE ATT&CK Techniques	Remote Desktop Protocol
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Powershell WinRM Connection

Description	The system utility Powershell was seen making connections over the Windows Remote Management (WinRM) port, which is indicative of WinRM connections.
Associated Observation	Suspicious Endpoint Activity
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Lateral Movement
MITRE ATT&CK Techniques	Windows Remote Management
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Protocol Forgery

Description	This entity was observed running a potentially restricted service (such as SSH) on a non-standard port. This can indicate evasion of security controls.
Associated Observation	Bad Protocol Observation
History	1 day

Telemetry	<ul style="list-style-type: none"> • ETA • Netflow • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Defense Evasion • Command and Control
MITRE ATT&CK Techniques	Non-Standard Port
Next Steps	Reference the supporting observations to determine why the entity used the unusual protocol/port combination to communicate. Update your firewall and blocklist rules to prevent further access with this protocol/port combination, if deemed a security risk.

Public Facing IP Watchlist Match

Description	A public-facing IP in your network was discovered on a watchlist (either explicitly or implicitly via a domain name).
Associated Observation	Public Facing IP Watchlist Match Observations
History	0 days
Telemetry	Netflow
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting observations to examine the affected entity and log information. Determine what malware or activity resulted in the entity being added to a threat intelligence watchlist, and remediate the situation.

Repeated Umbrella Sinkhole Communications

Description	Device has established periodic connections with a Cisco Umbrella Sinkhole. This alert may indicate a device is compromised.
--------------------	--

Associated Observation	<ul style="list-style-type: none"> • Heartbeat Observations • Umbrella Sinkhole Hit Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Application Layer Protocol
Next Steps	Reference the supporting observations and examine the affected entity and log information. Determine why the entity is establishing periodic communications to the sinkhole, and remediate the situation.

Repeated Watchlist Communications

Description	This entity has established periodic connections with a watchlisted IP. This may indicate the presence of malware, or a compromised entity on your network.
Associated Observation	<ul style="list-style-type: none"> • Watchlist Interaction Observations • Heartbeat Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • ETA • Firewall • Netflow • North-South • Passive DNS
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting observations and examine the affected entity and log information. Determine why the entity is

establishing periodic communications, and remediate the situation. As necessary, contact the organization that maintains a given watchlist, either for advice to remediate the situation, or to verify that the entity is no longer infected with malware.

Role Violation

Description	This entity is identified with a particular role (e.g., User entity), but was observed acting in an atypical manner for that role (e.g., SSH server). If an entity changes roles, it may be an indication of malicious behavior, such as malware changing how an entity functions.
Associated Observation	Role Violation Observations
History	0 days
Telemetry	Netflow
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting observations and determine whether the new role behavior is intended and part of the normal course of business. If it is not, quarantine the entity. If it is intended, snooze the alert.

SMB Connection Outlier

Description	Device exchanged an unusually large amount of SMB traffic with an unusually large set of SMB peers. This alert may indicate network reconnaissance activity.
Associated Observation	Historical Outlier Observations
History	36 days
Telemetry	Netflow
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> Discovery Reconnaissance

MITRE ATT&CK Techniques

- Gather Victim Network Information
- Network Service Discovery
- System Network Connections Discovery

Next Steps

Reference the supporting observations and determine why the entity is establishing connections with multiple SMB servers, what types of actions the entity is taking, and if this is malicious behavior.

SMB Connection Spike: Internal

Description

Device attempted to contact an unusually large number of SMB servers. This can be an indication of malware or abuse.

Associated Observation

[IP Scanner Observations](#)

History

9 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics

Discovery

MITRE ATT&CK Techniques

- Active Scanning
- Network Denial of Service

Next Steps

Reference the supporting observations and determine why the entity is establishing connections with multiple SMB servers, what types of actions the entity is taking, and if this is malicious behavior. If data was exfiltrated, follow your organization's guidelines for dealing with data exfiltration. Quarantine the entity as necessary to remove malware.

SMB Connection Spike: Outbound

Description

This entity is communicating with a large number of external hosts using SMB ports. This can indicate a possible infected host, externally initiated abuse (e.g., a spoof attack), or an internally initiated port scan.

Associated Observation

[IP Scanner Observations](#)

History	0 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Impact • Reconnaissance
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Active Scanning • Automated Exfiltration • Network Denial of Service
Next Steps	Reference the supporting observations and determine to which entities the source entity is sending traffic, what type of traffic, and if this is an update to the entity's roles or responsibilities, or if this is unintended. If this is unintended, remediate the issue. Update your firewall and blocklist rules to prevent this access.

SMB|RDP: Connection to Multiple Destinations

Description	The host has transferred file(s) into multiple destination hosts using SMB and connected to those hosts using RDP. This could indicate lateral movement.
Associated Observation	Suspicious Endpoint Activity Observations
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Lateral Movement
MITRE ATT&CK Techniques	Remote Services
Next Steps	Verify if this type of internal connection is normal for these endpoints.

SMB Traffic Initiated From a Command Interpreter

Description	Detection of SMB traffic where the parent process is cmd, PowerShell, or Python (not executed by a system account) and where a significantly larger amount of data is sent than received.
--------------------	---

This is unusual activity, and may be indicative of the Petit Potam or DFSCoerce threat actor behaviors.

Associated Observation	Suspicious Endpoint Activity
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK Techniques	Forced Authentication
Next Steps	Verify if the activity was authorized. If not, investigate related actions by the user and device involved. Disable unnecessary SMB services, enforce robust authentication, and monitor for unusual network traffic to detect and prevent potential threats.

Static Device Connection Deviation

Description	Device is normally static on the network - it talks to the same devices, with a similar traffic pattern each. Recently this device has deviated from its norms including communicating with a new external host. This alert may indicate misuse or a compromise.
Associated Observation	<ul style="list-style-type: none"> • Historical Outlier Observations • Static Connection Set Deviation • New External Connection Observations
History	1 day
Telemetry	<ul style="list-style-type: none"> • East-West • Netflow • North-South
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting observations to understand the entity's normal communication. Determine if the deviation is benign or

malicious behavior. Remediate any malicious behavior.

Static Device Deviation

Description	Device is normally static on the network - it talks on the same ports, or to the same devices, with a similar traffic pattern each day. Recently this device has deviated from its norms. This may indicate misuse or a compromise.
Associated Observation	<ul style="list-style-type: none">• Historical Outlier Observations• Static Port Set Deviation Observations
History	35 days
Telemetry	Netflow
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting observations to understand the entity's normal communication. Determine if the deviation is benign or malicious behavior. Remediate any malicious behavior.

Suspected Botnet Interaction

Description	Device exchanged traffic with IP addresses associated with botnets or attempted to resolve domain names associated with botnets using an integrated watchlist. This may indicate a device is compromised.
Associated Observation	Watchlist Interaction Observations
History	1 day
Telemetry	<ul style="list-style-type: none">• ETA• Firewall• Netflow• North-South• Passive DNS
MITRE ATT&CK	Command and Control

Tactics**MITRE ATT&CK Techniques**

- Application Layer Protocol
- Non-Application Layer Protocol

Next Steps

Quarantine the entity, and remove all malware. Update your block list and firewall rules to disallow the botnet entities from accessing your network. Reference the supporting evidence and determine if any other entities on your network are also infected, based on communications that the entity may have established, and remediate as necessary.

Suspected Cryptocurrency Activity

Description

Device exchanged a significant amount of traffic with multiple addresses known to be operating cryptocurrency nodes.

Associated Observation

[Watchlist Interaction Observations](#)

History

0 days

Telemetry

- ETA
- Firewall
- Netflow
- North-South
- Passive DNS

MITRE ATT&CK Tactics

Impact

MITRE ATT&CK Techniques

Resource Hijacking

Next Steps

Quarantine the entity and remove all cryptocurrency mining software, whether it is malware or installed by a user.

Suspected Phishing Domain

Description

The entity performed a successful DNS lookup of a suspected phishing domain.

Associated Observation

[Suspected Phishing Domain Observations](#)

History	0 days. Requires one of the following: <ul style="list-style-type: none"> • Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator with a Firepower appliance. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information. • Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information. • DNS logs from a SPAN or mirror port.
Telemetry	<ul style="list-style-type: none"> • ETA • Firewall • North-South • Passive DNS
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	<p>Reference the supporting observations to determine the entity and the domain to which it connected. Determine if this was due to malware or otherwise malicious behavior, and remediate the issue. Update your firewall and blocklist rules as needed.</p> <p>Review the entity's activity, and determine if it is consistent with planned penetration testing, or malicious behavior. Determine the origin of the malicious behavior, and remediate the issue. Update your firewall and blocklist rules as needed.</p>

Suspected Port Abuse: External

Description	Device is communicating with an external host on unusual range of ports. This may indicate externally-initiated abuse (e.g., a TCP/IP spoof attack) or an internally-initiated port scan.
Associated Observation	External Port Scanner Observations
History	1 day

Telemetry	<ul style="list-style-type: none"> • Netflow • North-South
MITRE ATT&CK Tactics	Reconnaissance
MITRE ATT&CK Techniques	Active Scanning
Next Steps	Reference the supporting evidence to review the entity's activity, and determine if it is consistent with planned penetration testing, or malicious behavior. Determine the origin of the malicious behavior, and remediate the issue. Update your firewall and blocklist rules as needed.

Suspected Remote Access Tool Heartbeat

Description	Traffic with a signature matching Remote Access Tools (e.g., RevengeRAT) was seen on this device. This alert may indicate the device is compromised.
Associated Observation	Suspicious Network Activity Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South • Passive DNS
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Application Layer Protocol
Next Steps:	Ensure this device has the most recent security updates applied and investigate the device for signs of compromise.

Suspected Zerologon RPC Exploit Attempt

Description	Traffic with a signature matching the Zerologon RPC exploit was seen on this device. This may indicate the device is being targeted for
--------------------	---

	exploitation.
Associated Observation	Suspicious Network Activity Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • Netflow • North-South • Passive DNS
MITRE ATT&CK Tactics	Privilege Escalation
MITRE ATT&CK Techniques	Exploitation for Privilege Escalation
Next Steps	Ensure this device has the most recent security updates applied. Follow mitigation steps in reference to CVE-2020-1472 .

Suspicious Curl Behavior

Description	The system utility curl exhibited suspicious behavior that may be indicative of exploitation of CVE-2023-38545.
Associated Observation	Suspicious Endpoint Activity Observations
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Execution
MITRE ATT&CK Techniques	Exploitation for Client Execution
Next Steps	Isolate the endpoint, investigate recent utilization of the curl process and ensure curl is updated to version 8.4 or newer on all devices.

Suspicious DNS over HTTPS Activity

Description	An internal server was seen exchanging traffic with a known DNS over HTTPS server. This alert may indicate an attempt to evade DNS-based security.
--------------------	--

Associated Observation	Watchlist Lookup Observations
History	7 days
Telemetry	Passive DNS
MITRE ATT&CK Tactics	Defense Evasion
MITRE ATT&CK Techniques	Impair Defenses
Next Steps	Review the supporting observations to verify if DNS over HTTPS is used purposefully, and if it is malicious behavior. Remediate any malicious behavior.

Suspicious Domain Lookup Failures

Description	This entity tried to resolve multiple algorithmically generated domains (e.g., rgkte-hdvj.cc) to an IP address. This may indicate a malware infection or botnet activity.
Associated Observation	<ul style="list-style-type: none"> • Domain Generation Algorithm Observations • Domain Generation Algorithm Success Observations
History	0 days
Telemetry	Passive DNS
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Dynamic Resolution
Next Steps	Reference the supporting observations and determine if the entity is infected with malware, or the cause of the domain lookups. Remove offending software as needed. Check for other entities on your network which may be exhibiting similar behavior, and remediate it.

Suspicious Email Findings by Initial Access

Description	One or more suspicious behaviors or attributes was detected in an email that was mapped to the MITRE ATT&CK Tactic Initial Access.
--------------------	--

Associated Observation	Suspicious Email Security Finding Observations
History	0 days
Telemetry	Email
MITRE ATT&CK Tactics	Initial Access
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Collection

Description	Suspicious behaviors were detected on the endpoint that are mapped to the Collection MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	Collection
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Command and Control

Description	Suspicious behaviors were detected on the endpoint that are mapped to the Command and Control MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days

Telemetry	Endpoint
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Credential Access

Description	Suspicious behaviors were detected on the endpoint that are mapped to the Credential Access MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	Credential Access
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by CrowdStrike Propriety Tactics

Description	Suspicious behaviors were detected on the endpoint that are not mapped to MITRE tactics.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK	N/A

Tactics**MITRE ATT&CK
Techniques**

N/A

Next Steps

Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Defense Evasion

Description

Suspicious behaviors were detected on the endpoint that are mapped to the Defense Evasion MITRE tactic.

**Associated
Observation**

[Suspicious Endpoint Security Finding Observations](#)

History

0 days

Telemetry

Endpoint

**MITRE ATT&CK
Tactics**

Defense Evasion

**MITRE ATT&CK
Techniques**

N/A

Next Steps

Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Discovery

Description

Suspicious behaviors were detected on the endpoint that are mapped to the Discovery MITRE tactic.

**Associated
Observation**

[Suspicious Endpoint Security Finding Observations](#)

History

0 days

Telemetry

Endpoint

**MITRE ATT&CK
Tactics**

Discovery

**MITRE ATT&CK
Techniques**

N/A

Next Steps Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Execution

Description Suspicious behaviors were detected on the endpoint that are mapped to the Execution MITRE tactic.

Associated Observation [Suspicious Endpoint Security Finding Observations](#)

History 0 days

Telemetry Endpoint

MITRE ATT&CK Tactics Execution

MITRE ATT&CK Techniques N/A

Next Steps Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Exfiltration

Description Suspicious behaviors were detected on the endpoint that are mapped to the Exfiltration MITRE tactic.

Associated Observation [Suspicious Endpoint Security Finding Observations](#)

History 0 days

Telemetry Endpoint

MITRE ATT&CK Tactics Exfiltration

MITRE ATT&CK Techniques N/A

Next Steps Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Impact

Description	Suspicious behaviors were detected on the endpoint that are mapped to the Impact MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	Impact
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Initial Access

Description	One or more suspicious behaviors or attributes was detected in an email that was mapped to the MITRE ATT&CK Tactic Initial Access.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	Initial Access
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Lateral Movement

Description	Suspicious behaviors were detected on the endpoint that are mapped to the Lateral Movement MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	Lateral Movement
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by MS Defender Proprietary Tactics

Description	Suspicious behaviors were detected on the endpoint that are not mapped to MITRE tactics.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Persistence

Description	Suspicious behaviors were detected on the endpoint that are mapped to the Persistence MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	Persistence
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Privilege Escalation

Description	Suspicious behaviors were detected on the endpoint that are mapped to the Privilege Escalation MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	Privilege Escalation
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Reconnaissance

Description	Suspicious behaviors were detected on the endpoint that are
--------------------	---

mapped to the Reconnaissance MITRE tactic.

Associated Observation

[Suspicious Endpoint Security Finding Observations](#)

History

0 days

Telemetry

Endpoint

MITRE ATT&CK Tactics

Reconnaissance

MITRE ATT&CK Techniques

N/A

Next Steps

Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings by Resource Development

Description

Suspicious behaviors were detected on the endpoint that are mapped to the Resource Development MITRE tactic.

Associated Observation

[Suspicious Endpoint Security Finding Observations](#)

History

0 days

Telemetry

Endpoint

MITRE ATT&CK Tactics

Resource Development

MITRE ATT&CK Techniques

N/A

Next Steps

Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Endpoint Findings without Tactics

Description

Suspicious behaviors were detected on the endpoint that are not mapped to any tactics.

Associated Observation

[Suspicious Endpoint Security Finding Observations](#)

History	0 days
Telemetry	Endpoint
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious File Download Observed on Process Arguments

Description	A URL pattern indicating a file download was observed on a process command line. This activity has features that may be indicative of malicious payload delivery.
Associated Observation	Suspicious Endpoint Activity
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Ingress Tool Transfer
Next Steps	Verify if downloaded file is malicious. Also investigate other evidence from both the device and user associated with the behavior. Consider rotating the users credentials or even quarantining the device, if required.

Suspicious MSHTA Activity

Description	The built in Windows application MSHTA.exe was executed interactively by a non-system user and utilized to make a network connection. While typically legitimate when run automatically by the system, it is also known to be utilized by threat actors including Advanced Persistent Threats (APTs).
Associated	Suspicious Endpoint Activity

Observation**History** 0 days**Telemetry** Cisco NVM

MITRE ATT&CK Tactics

- Command and Control
- Defense Evasion

MITRE ATT&CK Techniques

- MSHTA
- Ingress Tool Transfer

Next Steps Verify if this behavior was legitimate. If not, investigate telemetry for the device and user that made the connection. If necessary, quarantine the device and rotate credentials for the user.

Suspicious Network Findings by Collection

Description Suspicious behaviors were detected on the network that are mapped to the Collection MITRE tactic

Associated Observation [Suspicious Endpoint Security Finding Observations](#)

History 0 days**Telemetry** Network

MITRE ATT&CK Tactics

Collection

MITRE ATT&CK Techniques

N/A

Next Steps Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Network Findings by Command and Control

Description Suspicious behaviors were detected on the network that are mapped to the Command and Control MITRE tactic.

Associated Observation [Suspicious Endpoint Security Finding Observations](#)

History 0 days

Telemetry	Network
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Network Findings by Exfiltration

Description	Suspicious behaviors were detected on the network that are mapped to the Exfiltration MITRE tactic.
Associated Observation	Suspicious Endpoint Security Finding Observations
History	0 days
Telemetry	Network
MITRE ATT&CK Tactics	Exfiltration
MITRE ATT&CK Techniques	N/A
Next Steps	Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

Suspicious Process Executed

Description	Execution of the offensive tool, Metasploit, has been detected in an endpoint through endpoint telemetry
Associated Observation	Suspicious Endpoint Activity Observations
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	Execution

MITRE ATT&CK Techniques	User Execution
Next Steps	Isolate the endpoint and investigate the exploits and payloads that got executed on the endpoint.

Suspicious Process Path

Description	A process was executed on an endpoint from a directory that shouldn't have executables.
Associated Observation	Suspicious Endpoint Activity Observations
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Execution• Defense Evasion
MITRE ATT&CK Techniques	Masquerading
Next Steps	Isolate the endpoint and investigate if executables were downloaded in non-standard directories and executed.

Suspicious Request to Telegram

Description	A suspicious attempt to communicate with the Telegram chat service or the Telegraph blog service using a tool other than the Telegram desktop application or a web browser. Adversaries have been known to use Telegram in this manner for C2 communications. Supports Windows and macOS
Associated Observation	Suspicious Endpoint Activity
History	0 days
Telemetry	Cisco NVM
MITRE ATT&CK Tactics	<ul style="list-style-type: none">• Execution• Defense Evasion
MITRE ATT&CK Techniques	Masquerading

Next Steps Determine if this was legitimate activity, and if not investigate and potentially quarantine the device that made the connection.

Suspicious SMB Activity

Description Multiple new SMB servers have communicated with common SMB peers. This can be an indication of malware or abuse.

Associated Observation [Suspicious SMB Activity Observations](#)

History 14 days

Telemetry

- Netflow
- North-South

MITRE ATT&CK Tactics Lateral Movement

MITRE ATT&CK Techniques

- Remote Services
- Network Service Discovery
- System Network Connections Discovery

Next Steps Reference the supporting evidence to examine the entity's traffic profile to determine if there is further evidence of botnet activity or other malicious behavior. Check for other entities on your network which may be exhibiting similar behavior, and remediate it.

Suspicious User Agent

Description Device seen communicating with a device using a suspicious user agent string. This alert may indicate malware (e.g., Log4J exploitation) or abuse.

Associated Observation [Anomalous User Agent Observations](#)

History 0 days. Requires User Agent data provided by firewalls via integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Telemetry	<ul style="list-style-type: none"> • Firewall • North-South
MITRE ATT&CK Tactics	Initial Access
MITRE ATT&CK Techniques	Exploit Public-Facing Application
Next Steps	Reference the supporting observations and determine if the user-agent string will impact the server (e.g., Log4J), what types of actions the entity is taking, and if this is malicious behavior. If data was exfiltrated, follow your organization's guidelines for dealing with data exfiltration. Quarantine the entity as necessary to remove malware.

Suspicious User-Agent Activity

Description	An unusual HTTP User-Agent header value was seen in Cisco Secure Firewall data. This user-agent matched a behavioral pattern exhibited by malware deployed by the Gamaredon Advanced Persistent Threat group.
Associated Observation	Suspicious Firewall Activity
History	0 days
Telemetry	<ul style="list-style-type: none"> • Firewall • North-South
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Web Protocols
Next Steps	Utilize Firewall events to determine the device that sent this unusual header value and investigate that device further, looking for unusual VBScript execution.

Talos Intelligence Watchlist Hits

Description	This entity exchanged a significant amount of traffic with multiple addresses on the Cisco Talos IP Blocklist.
--------------------	--

Associated Observation	Watchlist Interaction Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • ETA • Firewall • Netflow • North-South • Passive DNS
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Quarantine the entity and remove all malware. Investigate the external IP address by selecting Talos Intelligence from the menu to see what the traffic indicates and take appropriate remediation actions.

TrickBot AnchorDNS Tunneling

Description	Device looked up a domain matching the algorithm used by AnchorDNS, a tunneling method used by TrickBot malwares. This alert may indicate a malware infection or botnet activity.
Associated Observation	TrickBot AnchorDNS Tunneling Activity Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • North-South • Passive DNS
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	Application Layer Protocol
Next Steps	As AnchorDNS uses a specific algorithm for domain generation, this is probably a malicious behavior. Identify and examine the machine generating the lookup and determine whether or not the

entity is functioning as intended, and if it is free of malware. Review the evidence and determine if other entities are infected.

Unusual DNS Connection

Description	Device contacted an unusual DNS resolver and then established periodic connections with a remote device. This may indicate that the device is compromised.
Associated Observation	<ul style="list-style-type: none">• Unusual DNS Resolver Observations• Heartbeat Observations
History	1 day
Telemetry	<ul style="list-style-type: none">• Netflow• North-South• Passive DNS
MITRE ATT&CK Tactics	Command and Control
MITRE ATT&CK Techniques	DNS
Next Steps	Reference the supporting observations and determine if this behavior is malicious, and remove malware if it is present. Update your block list and firewall rules to disallow access.

Unusual External Server

Description	Device has repeatedly communicated with a new external server. This may indicate the presence of malware.
Associated Observation	<ul style="list-style-type: none">• New External Server Observations• Persistent External Server Observations• Watchlist Lookup Observations• Watchlist Interaction Observations
History	14 days
Telemetry	<ul style="list-style-type: none">• ETA• Firewall• Netflow

- North-South
- Passive DNS

**MITRE ATT&CK
Tactics**

N/A

**MITRE ATT&CK
Techniques**

N/A

Next Steps

Reference the supporting evidence to examine the entity's traffic profile to determine the nature of the traffic and if it is permitted. Quarantine the entity and remove offending software. Determine if other entities on your network exhibit similar behavior, and remediate that behavior.

Unusual File Extension from New External Server

Description

A new file extension, unseen in the recent past, was exchanged between the entity and a new external server. This may indicate a malware attempting to communicate with its command and control center.

**Associated
Observation**

- [New External Server Observations](#)
- [New File Extension Observations](#)

History

1 day. Requires URL data provided by firewalls via integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Telemetry

- Firewall
- Netflow
- North-South

**MITRE ATT&CK
Tactics**

Command and Control

**MITRE ATT&CK
Techniques**

- Application Layer Protocol
- User Execution
- Masquerading

Next Steps Reference the supporting observations to determine with which external server the file with this new extension was exchanged. Review the entity's logs and determine why the entity has exchanged this file, and if it is malicious behavior. Remediate any malicious behavior.

User Watchlist Hit

Description This entity exchanged traffic with an IP address on a user-supplied watchlist, or attempted to resolve a domain name on a user-supplied watchlist.

Associated Observation

- [Watchlist Lookup Observations](#)
- [Watchlist Interaction Observations](#)

History 0 days

Telemetry

- ETA
- Firewall
- Netflow
- North-South
- Passive DNS

MITRE ATT&CK Tactics N/A

MITRE ATT&CK Techniques N/A

Next Steps Reference the supporting evidence to examine the entity's traffic profile and determine if the behavior is malicious. Update your firewall and blocklist rules as necessary.

Vulnerable Transport Security Protocol

Description Device was observed using an insecure SSL/TLS protocol version. This indicates that the SSL communication is not sufficiently secure.

Associated Observation [Insecure Transport Protocol Observations](#)

History 1 day. Requires Enhanced NetFlow. See the [Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#) for more

	information.
Telemetry	<ul style="list-style-type: none"> • ETA • North-South
MITRE ATT&CK Tactics	<ul style="list-style-type: none"> • Execution • Defense Evasion
MITRE ATT&CK Techniques	<ul style="list-style-type: none"> • Exploitation for Defense Evasion • Weaken Encryption • Downgrade Attack
Next Steps	Reference the supporting observations and review the application that is using the insecure transport protocol. If it is a local application, update it to a secure version. If it is external to your network, determine if the application represents a security risk, and block access as needed using firewall rules.

Watchlist Hit

Description	Device exchanged traffic with an IP address on an integrated watchlist or attempted to resolve a domain name on that watchlist. This may indicate a device is compromised.
Associated Observation	<ul style="list-style-type: none"> • Watchlist Lookup Observations • Watchlist Interaction Observations
History	0 days
Telemetry	<ul style="list-style-type: none"> • ETA • Firewall • Netflow • North-South • Passive DNS
MITRE ATT&CK Tactics	N/A
MITRE ATT&CK Techniques	N/A
Next Steps	Reference the supporting observations to examine the entity's traffic profile and determine if the behavior is malicious. Update

your firewall and blocklist rules as necessary.

Worm Propagation

Description	Previously scanned device started scanning the local IP network. This alert may indicate that a worm is propagating itself inside the network.
Associated Observation	Worm Propagation Observations
History	9 days
Telemetry	<ul style="list-style-type: none">• East-West• Netflow
MITRE ATT&CK Tactics	Lateral Movement
MITRE ATT&CK Techniques	<ul style="list-style-type: none">• Exploitation of Remote Services• Valid Accounts
Next Steps	Reference the supporting observations and investigate why the internal entities are scanning the network. Determine if it is the result of penetration testing or other intended behavior, or if it is malicious. Update your IP scanner and firewall rules to allow the traffic if it is intended. If potentially malicious, search for associated observations for the entity or user who owns the machine to determine what software caused the scanning activity.

Observation Descriptions

Amazon GuardDuty DNS Request Finding

Description	Amazon GuardDuty reported a suspicious DNS request.
Prerequisites	This observation requires AWS integration and enabling GuardDuty.
Associated Alerts	None

Amazon GuardDuty Network Connection Finding

Description	Amazon GuardDuty reported a suspicious network connection.
Prerequisites	This observation requires AWS integration and enabling GuardDuty.
Associated Alerts	None

Amazon Inspector Finding

Description	A finding was reported for an AWS resource.
Prerequisites	This observation requires AWS integration and enabling Inspector.
Associated Alerts	AWS Inspector Finding Alerts

Anomalous Profile

Description	An entity or entities used a profile for the first time which differs from typical behaviors seen in the network (e.g., an abnormally high number of entities using the profile for the first time, sending anomalous traffic).
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Anomalous AWS Workspace Alerts• Anomalous Mac Workstation• Anomalous Windows Workstation Alerts

Anomalous User Agent

Description	Device was sent traffic with an anomalous user agent string. This may be an indicator of an attempted Log4J exploit or other malicious activity.
Prerequisites	This observation requires integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.
Associated Alerts	Suspicious User Agent Alerts

AWS API Watchlist Access

Description	AWS API was accessed from an IP on a watchlist. API access from an entity on a watchlist may need to be examined for the possibility of malicious behavior.
Prerequisites	This observation requires AWS integration and enabling CloudTrail.
Associated Alerts	AWS API Watchlist IP Hit Alerts

AWS Architecture Compliance

Description	Detected AWS resource that may violate AWS "Well-architected" guidelines.
Prerequisites	This observation requires AWS integration.
Associated Alerts	Stale AWS Access Key Alerts

AWS CloudTrail Event

Description	AWS CloudTrail event reported for the entity.
Prerequisites	This observation requires AWS integration and enabling CloudTrail.
Associated Alerts	<ul style="list-style-type: none">AWS Anomalous IAM Role Policy Update Alerts

- [AWS Anomalous RDS Password Reset Alerts](#)
- [AWS API Call Using TOR IP Alerts](#)
- [AWS AppStream Image Shared Alerts](#)
- [AWS CloudTrail Watchlist Hit Alerts](#)
- [AWS Console Login Failures Alerts](#)
- [AWS Detector Modified Alerts](#)
- [AWS Domain Takeover Alerts](#)
- [AWS EC2 Startup Script Modified Alerts](#)
- [AWS ECS Credential Access Alerts](#)
- [AWS High Volume of API GetPasswordData Call Failures Alerts](#)
- [AWS High Volume of GetPasswordData Failures Alerts](#)
- [AWS IAM Anywhere Trust Anchor Created Alerts](#)
- [AWS IAM User Takeover Alerts](#)
- [AWS Lambda Backdoor Function Created Alerts](#)
- [AWS Lambda Invoke Permission Added Alerts](#)
- [AWS Logging Deleted Alerts](#)
- [AWS Logging Impairment Alerts](#)
- [AWS Multifactor Authentication Change Alerts](#)
- [AWS Organization Exit Attempt Alerts](#)
- [AWS Region Newly Utilized Alerts](#)
- [AWS Repeated API Failures Alerts](#)
- [AWS Root Account Used Alerts](#)
- [AWS Route 53 Hosted Zone Created Alerts](#)
- [AWS Route53 Target Added Alerts](#)
- [AWS S3 Bucket Lifecycle Configured Alerts](#)
- [AWS Security Group Deleted Alerts](#)
- [AWS Snapshot Exfiltration Alerts](#)
- [Geographically Unusual AWS API Usage Alerts](#)
- [Permissive Amazon Elastic Kubernetes Service Cluster Created Alerts](#)

- [Permissive AWS S3 Access Control List Alerts](#)
- [Permissive AWS Security Group Created Alerts](#)

AWS Config Compliance

Description	Configuration compliance reported for an AWS resource.
Prerequisites	This observation requires AWS integration, AWS configuration to stream configuration changes to an SNS topic, and an SQS queue to send the configuration changes, and additional configuration in Secure Cloud Analytics to retrieve the messages.
Associated Alerts	AWS Config Rule Violation Alerts

AWS Config Update

Description	Updated configuration reported for an AWS resource
Prerequisites	This observation requires AWS integration, AWS configuration to stream configuration changes to an SNS topic, and an SQS queue to send the configuration changes, and additional configuration in Secure Cloud Analytics to retrieve the messages.
Associated Alerts	None

AWS Lambda Metric Outlier

Description	An AWS Lambda function had unusual activity on one of its metrics.
Prerequisites	None
Associated Alerts	AWS Lambda Invocation Spike

AWS Multifactor Authentication Change

Description	Multifactor authentication was removed from a user account.
Prerequisites	This observation requires AWS integration and enabling CloudTrail.

Associated Alerts None

AWS New User Action

Description CloudTrail logged an AWS user doing an action for the first time.

Prerequisites This observation requires AWS integration and enabling CloudTrail.

Associated Alerts None

AWS Root Account Used

Description An action was performed using the AWS root account.

Prerequisites This observation requires AWS integration and enabling CloudTrail.

Associated Alerts None

Azure Advisor Recommendation

Description Azure Advisor generated a recommendation for an Azure Resource Manager (ARM) resource.

Prerequisites This observation requires Azure integration and at least one Network Security Group or storage account.

Associated Alerts [Azure Advisor Watchlist Alerts](#)

Azure Exposed Services

Description The device has a publicly exposed service that could be used by an attacker to gather information on the infrastructure or gain access to the data.

Prerequisites This observation requires Azure integration.

Associated Alerts [Azure Exposed Services Alerts](#)

Azure Functions Metric Outlier

Description	An Azure Functions had unusual activity on one of its metrics.
Prerequisites	This observation requires Azure integration.
Associated Alerts	Azure Function Invocation Spike Alerts

Azure Permissive Security Group

Description	A Security Rule pertaining to a Network Security Group has been set with excessive permissions, allowing access to the whole internet, (e.g. *, 0.0.0.0, :0/0) rather than a more conservative explicit list of allowed IP addresses.
Prerequisites	This observation requires Azure integration and at least one Network Security Group.
Associated Alerts	Azure Permissive Security Group Alerts

Azure Permissive Storage Setting

Description	An Azure Storage setting is overly permissive.
Prerequisites	This observation requires Azure integration and at least one storage account.
Associated Alerts	Azure Permissive Storage Account Alerts

Azure Security Event

Description	An Azure Security Center alert was generated.
Prerequisites	This observation requires Azure integration, Azure Security Center, Standard tier, and Azure Activity Logs.
Associated Alerts	Microsoft Defender for Cloud Event

Azure Unusual Activity

Description	Unusual activity detected in Azure Activity Logs.
--------------------	---

Prerequisites	This observation requires Azure integration and Azure Activity Logs.
Associated Alerts	<ul style="list-style-type: none"> • Anomalous Azure Custom Script Extensions Alerts • Azure Activity Log IP Watchlist Hit Alerts • Azure Activity Log Watchlist Hit Alerts • Azure Anomalous RunCommand • Azure Firewall Deleted Alerts • Azure Key Vaults Deleted Alerts • Azure Network Security Group Deleted Alerts • Azure OAuth Bypass Alerts • Azure Resource Group Deleted Alerts • Azure Transfer Data To Cloud Account Alerts • Geographically Unusual Azure API Usage Alerts

Azure VM in Unused Location

Description	An Azure Security Center alert was generated.
Prerequisites	This observation requires Azure integration and granting Secure Cloud Analytics the Monitoring Reader role permissions to review Azure Subscriptions.
Associated Alerts	Azure Virtual Machine in Unused Location Alerts

Bad Protocol

Description	An entity used a non-standard protocol on a standard port (e.g., UDP on port 22).
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none"> • Country Watchlist: Protocol Violation • Protocol Forgery

Cluster Change

Description	The profile set for the entity is similar to the profile set of other entities with which the entity has not recently been associated.
--------------------	--

Prerequisites None

Associated Alerts None

Compliance Verdict Summary

Description Detected cloud resources that violate compliance framework recommendations.

Prerequisites This observation requires integration with a cloud provider for Cloud Posture Management.

Associated Alerts None

Confirmed Threat Indicator Match - Domain

Description An entity resolved a domain listed as an IOC for a known threat.

Prerequisites This observation requires integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Associated Alerts None

Confirmed Threat Indicator Match - Hostname

Description An entity interacted with a hostname listed as an IOC for a known threat. This observation uses information from Enhanced NetFlow.

Prerequisites This observation requires Enhanced NetFlow. See the [Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#) for more information.

Associated Alerts None

Confirmed Threat Indicator Match - IP

Description An entity communicated with an IP address listed as an IOC for a

	known threat.
Prerequisites	None
Associated Alerts	None

Confirmed Threat Indicator Match - URL

Description	An entity interacted with a URL listed as an IOC for a known threat. This observation uses information from Enhanced NetFlow.
Prerequisites	This observation requires one of the following: <ul style="list-style-type: none">• Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.• Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.
Associated Alerts	None

Country Set Deviation

Description	An entity communicated with a set of countries different from its usual one.
Prerequisites	None
Associated Alerts	Country Set Deviation Alerts

Domain Generation Algorithm

Description	An entity attempted to contact an algorithmically generated domain (e.g., qhjvd-hdvj.cc).
Prerequisites	None
Associated Alerts	Suspicious Domain Lookup Failures Alerts

Domain Generation Algorithm Success

Description	An entity succeeded in resolving an algorithmically generated domain (e.g., rgkte-hdvj.cc) to an IP address.
Prerequisites	None
Associated Alerts	Suspicious Domain Lookup Failures Alerts

Drive By Download

Description	An entity has downloaded a large amount of data from a remote host after the external host's initial access, which could indicate the inadvertent download of a malicious payload.
Prerequisites	None
Associated Alerts	None

Exceptional Domain Controller

Description	Domain Controller entity communicated with unusual external ports.
Prerequisites	None
Associated Alerts	None

Excessive Connections to Network Printers

Description	An entity initiated excessive connections to network printers.
Prerequisites	None
Associated Alerts	Excessive Connections to Network Printers Alerts

External Mail Client Connections

Description	An entity communicated with many external mail servers.
Prerequisites	None
Associated Alerts	Email Spam Alerts

Alerts

External Port Scanner

Description	An entity on the local network scanned (or was scanned by) a remote IP address.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Inbound Port Scanner Alerts• Suspected Port Abuse (External) Alerts

GCP Cloud Function Metric Outlier

Description	A GCP cloud function had unusual activity on one of its metrics.
Prerequisites	This observation requires integration with Google Cloud Platform (GCP).
Associated Alerts	GCP Cloud Function Invocation Spike Alerts

GCP Watchlist Activity

Description	Watchlist activity detected in GCP Stackdriver Logs.
Prerequisites	This observation requires integration with Google Cloud Platform (GCP), and Secure Cloud Analytics permission to access Stackdriver Logs.
Associated Alerts	<ul style="list-style-type: none">• GCP API Call Using TOR IP• GCP Operations Log Watchlist Hit

Geographic Watchlist

Description	An entity communicated with watchlisted geographic region. When investigating Geographic Watchlist Observations, you can now filter the list of observations by country name in addition to country code. Use this filter when drilling down after pivoting to, or directly investigating, Geographic Watchlist Observations within the Observations > Selected Observation page.
Prerequisites	None
Associated	None

Alerts

Heartbeat

Description	An entity maintained a heartbeat with a remote host.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Empire Command and Control Alert• Heartbeat Connection Count Alerts• Repeated Umbrella Sinkhole Communications Alerts• Repeated Watchlist Communications Alerts• Unusual DNS Connection Alerts

Historical Outlier

Description	One of the source's metrics deviated significantly from its historical baseline. This observation may be anticipated or intended, but could also indicate malicious behavior.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Attendance Drop Alerts• Email Spam Alerts• SMB Connection Outlier Alerts• Static Device Connection Deviation Alerts• Static Device Deviation Alerts

Insecure Transport Protocol

Description	Source was observed using an insecure transport protocol by a network resource with encrypted traffic analytics capabilities.
Prerequisites	This observation requires Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.
Associated Alerts	<ul style="list-style-type: none">• Potentially Vulnerable Remote Control Protocol Alerts• Vulnerable Transport Security Protocol Alerts

Internal Connection Watchlist

Description	Forbidden communications between two internal IP endpoints were detected.
Prerequisites	None
Associated Alerts	Internal Connection Watchlist Hit Alerts

Internal Port Scanner

Description	An entity scanned a large number of ports.
Prerequisites	None
Associated Alerts	Internal Port Scanner Alerts

Intrusion Detection System Notice

Description	An IDS saw traffic matching a suspicious signature.
Prerequisites	This observation requires one of the following: <ul style="list-style-type: none">• Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.• Suricata IDS• Zeek IDS
Associated Alerts	<ul style="list-style-type: none">• IDS Emergent Profile Alerts• IDS Notice Spike Alerts

Invalid MAC Address

Description	A device with unregistered MAC address was detected on Cisco telemetry.
Prerequisites	None
Associated Alerts	Invalid MAC Address

IP Scanner

Description	An entity scanned a large number of entities.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• LDAP Connection Spike Alerts• NetBIOS Connection Spike Alerts• New IP Scanner Alerts• New SNMP Sweep Alerts• Non-Service Port Scanner Alerts• Outbound LDAP Spike Alerts• SMB Connection Spike: Internal• SMB Connection Spike: Outbound

ISE Session Started

Description	A new user session was created on Cisco Identity Services Engine (ISE).
Prerequisites	This observation requires integration with Cisco Identity Services Engine (ISE).
Associated Alerts	Abnormal ISE User Alerts

ISE Suspicious Activity

Description	A suspicious activity was detected on Cisco ISE.
Prerequisites	This observation requires integration with Cisco Identity Services Engine (ISE).
Associated Alerts	ISE Jailbroken Device

Long Session

Description	An entity maintained a long-lived session with an external IP address.
Prerequisites	None

Associated Alerts [Country Watchlist: New Long Session](#)

Malware Event

Description Malware activity detected from the entity

Prerequisites This observation requires integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Associated Alerts [Malware Spike Alerts](#)

Multiple Access Failures

Description An entity had multiple failed application (e.g., FTP, SSH, RDP) access attempts.

Prerequisites None

Associated Alerts [Excessive Access Attempts \(External\) Alerts](#)

Multiple File Extensions

Description This entity has exchanged a file with multiple extensions.

Prerequisites This observation requires integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Associated Alerts [Potentially Harmful Hidden File Extension Alerts](#)

Network Printer with Excessive Connections

Description Network printer initiated excessive connections to other entities.

Prerequisites None

Associated Alerts [Network Printer with Excessive Connections Alerts](#)

Alerts

New Compliance Resource Failure

Description	Detected cloud resources that violate compliance framework recommendations when they were compliant the previous day.
Prerequisites	This observation requires integration with a cloud provider for Cloud Posture Management.
Associated Alerts	None

New External Connection

Description	A usually predictable local entity communicated with an external entity.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• New External Connection Alerts• Static Device Connection Deviation Alerts

New External Server

Description	An entity started communicating with an external server.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Anomalous Domain Controller Activity• ICMP Abuse Alerts• Persistent Remote Control Connections Alerts• Unusual External Server Alerts• Unusual File Extension from New External Server Alerts

New File Extension

Description	A new file extension was exchanged.
Prerequisites	This observation requires integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

Associated Alerts[Unusual File Extension from New External Server Alerts](#)

New High Throughput Connection

Description An entity has exchanged a large amount of traffic with a new host.

Prerequisites None

Associated Alerts

- [Anomalous Domain Controller Activity](#)
- [High Bandwidth Unidirectional Traffic Alerts](#)
- [Potential Database Exfiltration Alerts](#)

New Internal Connection

Description A usually predictable local entity communicated with a new internal entity.

Prerequisites None

Associated Alerts None

New Internal Device

Description After not being seen in the lookback period, a new entity emerges on the network.

Prerequisites None

Associated Alerts [New Internal Device Alerts](#)

New Large Connection (External)

Description An entity exchanged an unusually large amount of data with an external host.

Prerequisites None

Associated Alerts [Outbound Traffic Spike Alerts](#)

New Large Connection (Internal)

Description	An entity exchanged an unusually large amount of data with an internal host.
Prerequisites	None
Associated Alerts	None

New Profile

Description	An entity matches a profile tag (e.g., FTP server) that it hasn't matched recently.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Anomalous Domain Controller Activity Alerts• Email Spam Alerts• Emergent Profile Alerts• IDS Emergent Profile Alerts

Persistent External Server

Description	This entity has regularly communicated with the same external server (FTP, SSH, etc.).
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Persistent Remote Control Connections Alerts• Unusual External Server Alerts

Population Spike

Description	A record number of IP addresses were observed communicating on the local network.
Prerequisites	None
Associated Alerts	Network Population Spike Alerts

Port Scanner

Description	An entity scanned a large number of ports.
Prerequisites	None
Associated Alerts	None

Potential Data Forwarding

Description	A similarly sized, and closely timed, data transfer was detected between an internal data source to this entity (the "download"), and then from this entity to an external data sink (the "upload").
Prerequisites	None
Associated Alerts	Potential Data Exfiltration Alerts

Public Amazon Route 53 Hosted Zone Created

Description	A public Amazon Route 53 hosted zone was created.
Prerequisites	This observation requires integration with AWS and enabling CloudTrail.
Associated Alerts	None

Public Facing IP Watchlist Match

Description	A public-facing IP in your network was discovered on a watchlist (either explicitly or implicitly via a domain name).
Prerequisites	None
Associated Alerts	Public Facing IP Watchlist Match Alerts

Public IP Service

Description	The device used an IP service that could be used by a malware.
Prerequisites	This observation requires integration with Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_

[Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging](#) for more information.

Associated Alerts None

Rapid Logins

Description User logged in to many entities in a short period.

Prerequisites None

Associated Alerts None

Record Metric Outlier

Description An entity sent or received a record amount of traffic.

Prerequisites None

Associated Alerts

- [Internal Connection Spike Alerts](#)
- [Outbound Traffic Spike Alerts](#)

Record Profile Outlier

Description An entity sent or received a record amount of traffic that matched a known profile, such as being a Facebook client.

Prerequisites None

Associated Alerts [Outbound Traffic Spike Alerts](#)

Remote Access

Description An entity was accessed from a remote source.

Prerequisites None

Associated Alerts

- [Geographically Unusual Remote Access Alerts](#)
- [New Remote Access Alerts](#)
- [Remote Access \(Geographic\) Alerts](#)

Role Violation

Description	An entity has new traffic that doesn't fit its role (e.g., FTP server communicating on port 80).
Prerequisites	None
Associated Alerts	Role Violation Alerts

Scan Result

Description	An active scanner (e.g., nmap) discovered an entity behavior.
Prerequisites	None
Associated Alerts	None

Session Closed

Description	A user session was closed.
Prerequisites	This observation requires an OSSEC, Sumo Logic, or Active Directory deployment.
Associated Alerts	None

Session Opened

Description	A user session was opened
Prerequisites	None
Associated Alerts	Abnormal User Alerts

Static Connection Set Deviation

Description	An entity normally talks to a static set of (internal/external) entities, but has recently started/stopped talking to new/normal entities.
Prerequisites	None
Associated Alerts	Static Device Connection Deviation

Static Port Set Deviation

Description	An entity normally uses a static set of (local/connected) ports for (internal/external) communications, but has recently added/dropped ports.
Prerequisites	None
Associated Alerts	Static Device Deviation Alerts

Sumo Logic Log

Description	An entity may be contributing to logs hosted by Sumo Logic.
Prerequisites	This observation requires a Sumo Logic deployment.
Associated Alerts	None

Suspected Malicious URL

Description	The host communicated with a suspected malicious URL.
Prerequisites	This observation requires one of the following: <ul style="list-style-type: none">• Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.• Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.
Associated Alerts	None

Suspected Phishing Domain

Description	The host communicated with a suspected phishing domain.
Prerequisites	This observation requires one of the following: <ul style="list-style-type: none">• Security Analytics and Logging (SaaS) through Cisco Defense Orchestrator. See

https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging for more information.

- Enhanced NetFlow. See the [Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#) for more information.
- DNS logs from a SPAN or mirror port.

Associated Alerts

[Suspected Phishing Domain Alerts](#)

Suspicious Email Security Finding

Description One or more suspicious behaviors or attributes was detected in an email that was mapped to the MITRE ATT&CK Tactic Initial Access.

Prerequisites Email integration.

Associated Alerts

[Suspected Email Findings by Initial Access](#)

Suspicious Endpoint Activity

Description Suspicious endpoint activity was detected that is associated with known attacker tactics, techniques, and procedures.

Prerequisites Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM) integration.

Associated Alerts

- [Cloud Metadata Service Credential Access Alerts](#)
- [Connection to TOR IP Address Alerts](#)
- [DC Sync Attack Behavior Alerts](#)
- [Endpoint Exfiltration of AWS Credentials Alerts](#)
- [LDAP Connection from Anomalous Process Alerts](#)
- [Malicious Process Detected Alerts](#)
- [Port 8888: Connections from multiple sources Alerts](#)
- [Potential Gamaredon C2 Callout Alerts](#)
- [Potential GhostPulse Malware C2 Alerts](#)
- [Potential System Process Impersonation Alerts](#)

- [Powershell RDP Connection Alerts](#)
- [Powershell WinRM Connection Alerts](#)
- [SMB|RDP: Connection to multiple destinations Alerts](#)
- [Suspicious Curl Behavior Alerts](#)
- [Suspicious Process Executed Alerts](#)
- [Suspicious Process Path Alerts](#)
- [Suspicious Request to Telegram Alerts](#)

Suspicious Endpoint Security Finding

Description	Suspicious endpoint activity was detected that is associated with known attacker tactics, techniques, and procedures.
Prerequisites	Endpoint integration.
Associated Alerts	<ul style="list-style-type: none">• Suspicious Endpoint Findings by Collection• Suspicious Endpoint Findings by Command and Control• Suspicious Endpoint Findings by Credential Access• Suspicious Endpoint Findings by CrowdStrike Proprietary Tactics• Suspicious Endpoint Findings by Defense Evasion• Suspicious Endpoint Findings by Discovery• Suspicious Endpoint Findings by Execution• Suspicious Endpoint Findings by Exfiltration• Suspicious Endpoint Findings by Impact• Suspicious Endpoint Findings by Initial Access• Suspicious Endpoint Findings by Lateral Movement• Suspicious Endpoint Findings by MS Defender Proprietary Tactics• Suspicious Endpoint Findings by Persistence• Suspicious Endpoint Findings by Privilege Escalation• Suspicious Endpoint Findings by Reconnaissance• Suspicious Endpoint Findings by Resource Development• Suspicious Endpoint Findings without Tactics

Suspicious Firewall Activity

Description	Suspicious activity detected in firewall logs.
Prerequisites	None
Associated Alerts	Suspicious User-Agent Activity

Suspicious Microsoft Entra ID Audit Logs Activity

Description	Suspicious activity detected in Microsoft Entra ID Audit Logs
Prerequisites	None
Associated Alerts	MFA Disabled for Azure

Suspicious Network Activity

Description	Suspicious activity was detected that is associated with known attacker tactics, techniques, and procedures.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Suspected Remote Access Tool Heartbeat Alerts• Suspected Zerologon RPC Exploit Attempt Alerts

Suspicious Network Activity detected by EVE

Description	Encrypted Visibility Engine detected suspicious activity
Prerequisites	None
Associated Alerts	None

Suspicious Network Security Finding

Description	Suspicious behavior reported on the network
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Suspicious Network Findings by Collection• Suspicious Network Findings by Command and Control• Suspicious Network Findings by Exfiltration

Suspicious SMB Activity

Description	Multiple entities have performed anomalous activity using the SMB protocol for the first time.
Prerequisites	None
Associated Alerts	Suspicious SMB Activity Alerts

Traffic Amplification

Description	An entity's outbound and inbound traffic did not match the typical ratio associated with the profile it was using. This could indicate participation in an amplification attack. An amplification attack attempts to overwhelm a server with a massive amount of packets in response to a request, involving spoofed IP addresses or other identifying information. Participation in an amplification attack may also indicate that an entity has been infected with botnet malware, and it is sending these packets unintentionally.
Prerequisites	None
Associated Alerts	Amplification Attack Alerts

TrickBot AnchorDNS Tunneling Activity

Description	The device used the TrickBot Anchor_DNS tunneling method to communicate with a C&C server.
Prerequisites	None
Associated Alerts	TrickBot AnchorDNS Tunneling Alerts

Umbrella Sinkhole Hit

Description	The device communicated with a known Cisco Umbrella sinkhole.
Prerequisites	None
Associated Alerts	Repeated Umbrella Sinkhole Communications Alerts

Unused AWS Resource

Description	No recent activity seen for an AWS resource.
Prerequisites	This observation requires AWS integration.
Associated Alerts	AWS Resource Inactive

Unusual DNS Resolver

Description	An entity communicated with an unusual DNS resolver.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• New Unusual DNS Resolver Alerts• Unusual DNS Connection Alerts

Unusual Packet Size

Description	Device sent or received packets that are unusually sized for the given profile.
Prerequisites	None
Associated Alerts	None

Unusual EC2 Instance

Description	A new EC2 instance of unusual type and size has been created.
Prerequisites	This observation requires AWS integration and enabling CloudTrail.
Associated Alerts	Unusually Large EC2 Instance Alerts

Unusual Packet Size

Description	An entity sent or received packets that are unusually sized for the given profile.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• DNS Abuse Alerts

- [ICMP Abuse Alerts](#)

Watchlist Interaction

Description	An entity communicated with an IP address that is on a watchlist (either explicitly or implicitly via a domain name).
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Repeated Watchlist Communications Alerts• Suspected Botnet Interaction Alerts• Suspected Cryptocurrency Activity Alerts• Suspected DNS over HTTPS Activity Alerts• Talos Intelligence Watchlist Hits Alerts• Unusual External Server Alerts• User Watchlist Hit Alerts• Watchlist Hit Alerts

Watchlist Lookup

Description	An entity looked up a watchlisted domain.
Prerequisites	None
Associated Alerts	<ul style="list-style-type: none">• Suspicious DNS over HTTPS Activity• Unusual External Server• User Watchlist Hit Alerts• Watchlist Hit Alerts

Worm Propagation

Description	Previously scanned device started scanning the local IP network.
Prerequisites	None
Associated Alerts	Worm Propagation Alerts

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Revision	Revision Date	Description
1.0	April 3, 2020	Initial version.
1.1	September 4, 2020	<p>Added the following alerts and an observation:</p> <ul style="list-style-type: none"> • Anomalous AWS Workspace Alert • Anomalous Mac Workstation Alert • Empire Command and Control alert • Malware Spike Alert • Anomalous Profile Observation <p>Updated the following alert and observations:</p> <ul style="list-style-type: none"> • Email Spam Alert • Historical Outlier Observation • New Profile Observation <p>Also added additional information about Security Analytics and Logging (SaaS).</p>
2.0	October 25, 2021	<p>Rebranded and added the following alerts and observations:</p> <ul style="list-style-type: none"> • AWS Detector Modified Alert • AWS Logging Deleted Alert • AWS Temporary Token Persistence Alert • Azure Advisor Watchlist Alert • Non-Service Port Scanner Alert • Public IP Services Lookup Alert • Static Device Connection Deviation Alert • Suspected Zerologon RPC Exploit Attempt Alert • TrickBot AnchorDNS Tunneling Alert • A device used a public IP lookup service Observation

		<ul style="list-style-type: none"> • Azure Permissive Security Group Observation • Azure Permissive Storage Setting Observation • Compliance Verdict Summary Observation • New Compliance Resource Failure Observation • TrickBot AnchorDNS Tunneling Activity Observation
2.1	May 10, 2022	<p>Updated the MITRE ATT&CK tactics/techniques for alerts, and added the following alerts:</p> <ul style="list-style-type: none"> • AWS EC2 Startup Script Modified Alert • AWS ECS Credential Access Alert • AWS IMDS Produced Credentials Alert • AWS Lambda Persistence Alert • AWS Snapshot Exfiltration Alert • Azure Exposed Services Alert • Azure Firewall Deleted Alert • Azure Function Invocation Spike Alert • Azure Key Vaults Deleted Alert • Azure Network Security Group Deleted Alert • Azure OAuth Bypass Alert • Azure Resource Group Deleted Alert • Azure Transfer Data To Cloud Account Alert • Critical Severity Cloud Posture Watchlist Hit Alert • High Severity Cloud Posture Watchlist Hit Alert • ICMP Abuse Alert • LDAP Connection Spike Alert • Low Severity Cloud Posture Watchlist Hit Alert • Medium Severity Cloud Posture Watchlist Hit Alert • Meterpreter Command and Control Success

		<p>Alert</p> <ul style="list-style-type: none"> • Outbound LDAP Spike Alert • Permissive Amazon Elastic Kubernetes Service Cluster Created Alert • Repeated Umbrella Sinkhole Communications Alert • S3 Bucket Lifecycle Configured Alert • SMB Connection Outlier Alert • Suspected DNS Over HTTPS Activity Alert • Suspected Remote Access Tool Heartbeat Alert • Suspicious User Agent Alert • Unusual File Extension From New External Server Alert • Worm Propagation Alert <p>Added the following observations:</p> <ul style="list-style-type: none"> • Anomalous User Agent Observation • Azure Exposed Services Observation • Azure Functions Metric Outlier Observation • New File Extension Observation • Public IP Service Observation • Umbrella Sinkhole Hit Observation • Worm Propagation Observation <p>Removed the following alerts:</p> <ul style="list-style-type: none"> • AWS IMDS Produced Credentials Alert • Potential Ransomware Activity Alert • Rapid Logins Alert
2.2	August 2, 2022	Added Contacting Support.
2.3	September 14, 2022	Added the ISE Session Started Observation, and removed the Public IP Services Alert.

2.4	November 1, 2022	<p>Added the following alerts:</p> <ul style="list-style-type: none"> • AWS IAM Anywhere Trust Anchor Created Alert • New AWS Lambda Invoke Permission Added Alert • Unusually Large EC2 Instance Alert <p>Added the Unusual EC2 Instance Observation, and updated telemetry requirements for alerts and the MITRE ATT&CK tactics/techniques for alerts.</p>
2.5	January 17, 2023	Added the AWS Repeated API Failures Alert.
2.6	February 13, 2023	Added the Abnormal ISE User Alert and ISE Suspicious Activity Observation.
3.0	August 29, 2023	<p>Added the following alerts:</p> <ul style="list-style-type: none"> • AWS IAM User Takeover Alert • AWS Logging Impairment Alert • AWS Security Group Deleted Alert • Invalid Mac Address Alert • ISE Jailbroken Device Alert • LDAP Connection from Suspicious Process Alert • Malicious Process Detected Alert • Metasploit Executed Alert • Port 8888: Connects from Multiple Sources Alert • Potential Persistence Attempt Alert • Potential System Process Impersonation Alert • SMB RDP: Connection to Multiple Destinations Alert • Suspicious Process Path Alert <p>Updated the following alerts:</p> <ul style="list-style-type: none"> • Azure Exposed Services Alert

		<ul style="list-style-type: none">• Azure Firewall Deleted Alert• Potential Data Exfiltration Alert
3.1	February 9, 2024	<p>Added the following alerts:</p> <ul style="list-style-type: none">• Suspicious Curl Behavior Alert• Suspicious Email Findings by Initial Access Alert• Suspicious Endpoint Findings by Command and Control Alert• Suspicious Endpoint Findings by Credential Access Alert• Suspicious Endpoint Findings by CrowdStrike Proprietary Tactics Alert• Suspicious Endpoint Findings by Defense Evasion Alert• Suspicious Endpoint Findings by Discovery Alert• Suspicious Endpoint Findings by Execution Alert• Suspicious Endpoint Findings by Exfiltration Alert• Suspicious Endpoint Findings by Impact Alert• Suspicious Endpoint Findings by Initial Access Alert• Suspicious Endpoint Findings by MS Defender Proprietary Tactics Alert• Suspicious Endpoint Findings by Persistence Alert• Suspicious Endpoint Findings by Privilege Escalation Alert• Suspicious Endpoint Findings by Reconnaissance Alert• Suspicious Endpoint Findings by Resource Development Alert• Suspicious Endpoint Findings without Tactics

		<p>Alert</p> <ul style="list-style-type: none"> • Suspicious Process Executed Alert <p>Added the following observations:</p> <ul style="list-style-type: none"> • Suspicious Email Security Finding Observation • Suspicious Endpoint Security Finding Observation <p>Renamed the Metasploit Executed Alert to Suspicious Process Executed Alert.</p>
3.2	May 15, 2024	<p>Added the following alerts:</p> <ul style="list-style-type: none"> • AWS High Volume of API Get PasswordData Call Failures Alert • Potential Gamaredon C2 Callout Alert • Potential GhostPulse Malware C2 Alert • Suspicious Curl Request to Telegram Alert
3.3	June 14, 2024	<p>Added the Azure Anomalous RunCommand Alert.</p> <p>Renamed the following alerts:</p> <ul style="list-style-type: none"> • Azure Security Event to Microsoft Defender for Cloud Event • CloudTrail Watchlist Hit to AWS CloudTrail Watchlist Hit • Exceptional Domain Controller to Anomalous Domain Controller Activity • GCP Stackdriver Logging Watchlist Hit to GCP Operations Log Watchlist Hit • New AWS Lambda Invoke Permission Added to AWS Lambda Invoke Permission Added • New AWS Region to AWS Region Newly Utilized • New AWS Route53 Target to AWS Route53 Target Added

		<ul style="list-style-type: none"> • New Long Sessions (Geographic) to Country Watchlist: New Long Session • Outbound SMB Connection Spike to SMB Connection Spike: Outbound • Protocol Violation (Geographic) to Country Watchlist: Protocol Violation • Public Amazon Route53 Hosted Zone Created to AWS Route53 Hosted Zone Created • Remote Access (Geographic) to Country Watchlist: Remote Access • S3 Bucket Lifecycle Configured to AWS S3 Bucket Lifecycle Configured • SMB Connection Spike to SMB Connection Spike: Internal • Stale AWS Access Key to AWS Stale Access Key • Suspected Port Abuse (External) to Suspected Port Abuse: External • Unusually Large EC2 Instance to AWS Unusually Large EC2 Instance • Unused AWS Resource to AWS Resource Inactive • AWS Lambda Persistence to AWS Lambda Backdoor Function Created
3.4	July 17, 2024	Added the Anomalous Azure Custom Script Extensions alert.
4.0	September 24, 2024	<p>Updated the layout of both the Alerts section and the Observations section of the document. Moved the content for the alerts and observations descriptions from paragraph format to a table and multiple listings to unordered lists.</p> <p>Updated out-of-date descriptions and next steps for Alerts.</p>

Updated the **Alerts and Observations Introduction**.

Added the following **alerts** to the documentation:

- AWS Anomalous IAM Role Policy Update
- AWS Organization Exit Attempt
- Cloud Metadata Service Credential Access
- DC Sync Attack Behavior
- Suspicious Network Findings by Collection
- Suspicious Network Findings by Command and Control
- Suspicious Network Findings by Exfiltration

Removed the following *deprecated* **alerts** in the documentation:

- Confirmed Threat Watchlist Hit
- Domain Generation Algorithm Successful Lookup
- Meterpreter Command and Control Success
- Potential Persistence Attempt
- Suspected Malicious URL
- Suspicious Domain Lookup Failures

Alert Name Changes:

- **Suspicious Curl Request to Telegram** has been renamed to **Suspicious Request to Telegram**.

Added the following **observations** to the documentation:

- Invalid Mac Address
- Suspicious Firewall Activity
- Suspicious Microsoft Entra ID Audit Logs Activity
- Suspicious Network Activity detected by EVE

		<ul style="list-style-type: none">• Suspicious Network Security Finding
4.1	October 11, 2024	<p>Added the following alerts to the documentation:</p> <ul style="list-style-type: none">• Endpoint Exfiltration of AWS Credentials• Powershell RDP Connection• Powershell WinRM Connection• GCP API Call Using TOR IP• AWS Anomalous RDS Password Reset• MFA Disabled for Azure• SMB Traffic Tnitiated From a Command Interpreter• Suspicious MSHTA Activity• AWS Anomalous Secrets Manager Batch Retrieval• Suspicious File Download Observed on Process Arguments• Connection to TOR IP Address <p>Alert Name Changes:</p> <ul style="list-style-type: none">• LDAP Connection from Suspicious Process has been renamed to LDAP Connection from Anomalous Process

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

