Cisco Secure Cloud Analytics

Alerts and Observations Reference Guide

Table of Contents

Alerts and Observations Reference Introduction

The following provides an overview of the alert and observation types available in Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud).

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.

The Alert Prerequisites provide tables of the alerts sorted by their baseline requirement, with basic generation prerequisites.

Each alert in Alert Descriptions lists:

- the alert type
- any prerequisites for generation
- associated observations
- 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 Prerequisites and MITRE ATT&CK Mapping

The following table provides an overview of how much history is required to generate a given alert type, whether it can be generated through Cisco Secure Cloud Analytics private network monitoring (formerly Stealthwatch Cloud Private Network Monitoring) or Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring), and if there are any additional limitations or prerequisites for generation (such as requiring AWS integration). It also lists any MITRE ATT&CK tactics or techniques associated with an alert type.

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Abnormal ISE User	requires Cisco Identity Services Engine (ISE)	requires Cisco Identity Services Engine (ISE)	36 days	Initial Access	Valid Accounts
Abnormal User	yes	yes	36 days	Persistence	Valid Accounts
Amplification Attack	yes	yes	0 days	Impact	Network Denial of Service
Anomalous AWS Workspace	no	AWS-only	14 days		
Anomalous Mac Workstation	yes	yes	14 days		
Anomalous Windows Workstation	yes	yes	14 days		
Attendance Drop	yes	yes	14 days	Impact	Endpoint Denial of Service
AWS API Call Using TOR IP	no	AWS-only	0 days	Defense Evasion	Proxy
AWS API Watchlist IP Hit	no	AWS-only	0 days	Discovery	Cloud Service Discovery
AWS Config Rule Violation	no	AWS-only	0 days	Persistence	Account Manipulation
AWS Console Login Failures	no	AWS-only	0 days	Credential Access	Brute Force
AWS Detector Modified	no	AWS-only	0 days	Defense Evasion	Impair Defenses

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
AWS Domain Takeover	no	AWS-only	0 days	Resource Development	Compromise Infrastructure
AWS EC2 Startup Script Modified	no	AWS-only	0 days	Persistence	Boot or Logon Initialization Scripts
AWS ECS Credential Access	no	AWS-only	0 days	Persistence	Implant Internal Image
AWS IAM Anywhere Trust Anchor Created	no	AWS-only	0 days	Persistence	Account Manipulation
AWS IAM User Takeover	no	AWS-only	0 days	Persistence	Account Manipulation
AWS Inspector Finding	no	AWS-only	0 days	Persistence	Account Manipulation
AWS Lambda Invocation Spike	no	AWS-only	14 days	Impact	Resource Hijacking
AWS Lambda Persistence	no	AWS-only	0 days	Persistence	Event Triggered Execution
AWS Logging Deleted	no	AWS-only	0 days	Defense Evasion	Impair Defenses
AWS Logging Impairment	no	AWS-only	0 days	Defense Evasion	Impair Defenses
AWS Multifactor Authentication Change	no	AWS-only	0 days	Persistence	Account Manipulation
AWS Repeated API Failures	no	AWS-only	3 days	Discovery	Cloud Service Discovery
AWS Root Account Used	no	AWS-only	0 days	Persistence	Valid Accounts
AWS Security Group Deleted	no	AWS-only	0 days	Impact	Account Access Removed
AWS Snapshot Exfiltration	no	AWS-only	0 days	Exfiltration	Transfer Data to Cloud Account
Azure Activity Log IP Watchlist Hit	no	Azure-only	0 days	Discovery	Cloud Service Discovery
Azure Activity Log Watchlist Hit	no	Azure-only	0 days	Persistence	Event Triggered Execution

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Azure Advisor Watchlist	no	Azure-only	0 days	Persistence	Event Triggered Execution
Azure Exposed Services	no	Azure-only	0 days	Reconnaissance	Gather Victim Host Information
Azure Firewall Deleted	no	Azure-only	0 days	Defense Evasion	Impair Defenses
Azure Function Invocation Spike	no	Azure-only	14 days	Impact	Resource Hijacking
Azure Key Vaults Deleted	no	Azure-only	0 days	Impact	Account Access Removal
Azure Network Security Group Deleted	no	Azure-only	0 days	Defense Evasion	Impair Defenses
Azure OAuth Bypass	no	Azure-only	0 days	Initial Access	Valid Accounts
Azure Permissive Security Group	no	Azure-only	0 days	Initial Access	External Remote Services
Azure Permissive Storage Account	no	Azure-only	0 days	Persistence	Account Manipulation
Azure Resource Group Deleted	no	Azure-only	0 days	Impact	Data Destruction
Azure Security Event	no	Azure-only	0 days	Persistence	Event Triggered Execution
Azure Transfer Data To Cloud Account	no	Azure-only	0 days	Exfiltration	Exfiltration Over Web Services
Azure Virtual Machine in Unused Location	no	Azure-only	0 days	Impact	Resource Hijacking
CloudTrail Watchlist Hit	no	AWS-only	0 days	Persistence	Event Triggered Execution
Confirmed Threat Watchlist Hit	requires Security Analytics and Logging (SaaS), or Enhanced NetFlow , or DNS logs	requires Security Analytics and Logging (SaaS), or Enhanced NetFlow , or DNS logs	0 days	Command And Control	Application Layer Protocol
Country Set Deviation	yes	yes	36 days	Initial Access	Valid Accounts

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Critical Severity Cloud Posture Watchlist Hit	no	yes	0 days		
DNS Abuse	yes	yes	0 days	Exfiltration	Exfiltration Over Alternative Protocol
Domain Generation Algorithm Successful Lookup	requires DNS logs	no	0 days	Command And Control	Dynamic Resolution
Email Spam	yes	yes	36 days	Exfiltration	Exfiltration Over Alternative Protocol
Emergent Profile	yes	yes	14 days	Exfiltration	Exfiltration Over Alternative Protocol
Empire Command and Control	yes	yes	1 day	Command And Control	Non-Application Layer Protocol
Exceptional Domain Controller	yes	yes	7 days	Privilege Escalation	Abuse Elevation Control Mechanism
Excessive Access Attempts (External)	yes	yes	0 days	Credential Access	Brute Force
Excessive Connections to Network Printers	yes	yes	0 days	Impact	Endpoint Denial of Service
GCP Cloud Function Invocation Spike	no	GCP-only	14 days	Impact	Resource Hijacking
GCP Stackdriver Logging Watchlist Hit	no	GCP-only	0 days	Persistence	Event Triggered Execution
Geographically Unusual AWS API Usage	no	AWS-only	14 days	Discovery	Cloud Service Discovery
Geographically Unusual Azure API Usage	no	Azure-only	14 days	Discovery	Cloud Service Discovery
Geographically Unusual Remote Access	yes	yes	14 days	Initial Access	External Remote Services
Heartbeat Connection Count	yes	yes	1 day	Command And Control	Non-Application Layer Protocol
High Bandwidth	yes	yes	0 days	Exfiltration	Automated Exfiltration

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Unidirectional Traffic					
High Severity Cloud Posture Watchlist Hit	no	yes	0 days		
ICMP Abuse	yes	yes	0 days	Exfiltration	Exfiltration Over Alternative Protocol
IDS Emergent Profile	requires Cisco Security Analytics and Logging (SaaS) or IDS	requires Security Analytics and Logging (SaaS) or IDS	14 days	Impact	Endpoint Denial of Service
IDS Notice Spike	requires Security Analytics and Logging (SaaS) or IDS	requires Security Analytics and Logging (SaaS) or IDS	1 day	Impact	Endpoint Denial of Service
Inbound Port Scanner	yes	yes	1 day	Discovery	Network Service Scanning
Internal Connection Spike	yes	yes	0 days	Discovery	Network Service Scanning
Internal Connection Watchlist Hit	yes	yes	0 days	Persistence	Event Triggered Execution
Internal Port Scanner	yes	yes	7 days	Discovery	Network Service Scanning
Invalid Mac Address	requires Cisco Identity Services Engine (ISE)	requires Cisco Identity Services Engine (ISE)	0 days	Lateral Movement	Masquerading
ISE Jailbroken Device	requires Cisco Identity Services Engine (ISE)	requires Cisco Identity Services Engine (ISE)	0 days	Initial Access	Drive-by Compromise
LDAP Connection from Suspicious Process	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module	0 days	Credential Access	Valid Accounts

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
	(NVM)	(NVM)			
LDAP Connection Spike	yes	yes	9 days	Discovery	Network Service Scanning
Low Severity Cloud Posture Watchlist Hit	no	yes	0 days		
Malicious Process Detected	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	0 days	Execution	Masquerading
Malware Spike	requires Security Analytics and Logging (SaaS)	requires Security Analytics and Logging (SaaS)	1 day	Execution	User Execution
Medium Severity Cloud Posture Watchlist Hit	no	yes	0 days		
Meterpreter Command and Control Success	yes	yes	1 day	Command And Control	Non-Application Layer Protocol
Missing Sumo Logic Log	requires Sumo Logic	no	0 days	Impact	Data Manipulation
NetBIOS Connection Spike	yes	yes	7 days	Discovery	Network Service Discovery
Network Population Spike	yes	yes	36 days	Impact	Network Denial of Service
Network Printer with	yes	yes	0 days	Command And Control	Web Service

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Excessive Connections					
New AWS Lambda Invoke Permission Added	no	AWS-only	0 days	Persistence	Event Triggered Execution
New AWS Region	no	AWS-only	0 days	Defense Evasion	Unused/ Unsupported Cloud Regions
New AWS Route53 Target	no	AWS-only	0 days	Persistence	Account Manipulation
New External Connection	yes	yes	35 days	Collection	Automated Collection
New Internal Device	yes	yes	21 days	Initial Access	Hardware Additions
New IP Scanner	yes	yes	7 days	Discovery	Network Service Discovery
New Long Sessions (Geographic)	yes	yes	2 days	Exfiltration	Exfiltration Over Alternative Protocol
New Remote Access	yes	yes	36 days	Initial Access	External Remote Services
New SNMP Sweep	yes	yes	7 days	Discovery	Network Service Discovery
New Unusual DNS Resolver	yes	yes	7 days	Command And Control	Application Layer Protocol
Non-Service Port Scanner	yes	yes	9 days	Discovery	Network Service Scanning
Outbound LDAP Connection Spike	yes	yes	0 days	Reconnaissance	Active Scanning
Outbound SMB Connection Spike	yes	yes	0 days	Reconnaissance	Active Scanning
Outbound Traffic Spike	yes	yes	14 days	Exfiltration	Automated Exfiltration
Permissive Amazon Elastic Kubernetes Service Cluster Created	no	AWS-only	0 days	Discovery	Container and Resource Discovery
Permissive AWS S3 Access Control List	no	AWS-only	0 days	Collection	Data from Cloud Storage Object
Permissive AWS Security Group	no	AWS-only	0 days	Persistence	Account Manipulation

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Created					
Persistent Remote Control Connections	yes	yes	7 days	Initial Access	External Remote Services
Port 8888: Connections from Multiple Sources	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	0 days	Command and Control	Automated Exfiltration
Potential Data Exfiltration	yes	yes	0 days	Exfiltration	Automated Exfiltration
Potential Database Exfiltration	yes	yes	7 days	Exfiltration	Exfiltration Over Alternative Protocol
Potential Persistence Attempt	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	0 days	Persistence	Event Triggered Execution
Potential System Process Impersonation	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	0 days	Defense Evasion	Masquerading
Potentially Harmful	requires	requires	0 days	Execution	User Execution

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Hidden File Extension	Security Analytics and Logging (SaaS) or Enhanced NetFlow	Security Analytics and Logging (SaaS) or Enhanced NetFlow			
Potentially Vulnerable Remote Control Protocol	requires Enhanced NetFlow	requires Enhanced NetFlow	1 day	Defense Evasion	Exploitation for Defense Evasion
Protocol Forgery	yes	yes	1 day	Command And Control	Non-Standard Port
Protocol Violation (Geographic)	yes	yes	0 days	Command And Control	Application Layer Protocol
Public Amazon Route 53 Hosted Zone Created	no	AWS-only	0 days	Resource Development	Establish accounts
Public Facing IP Watchlist Match	yes	yes	0 days	Reconnaissance	Gather Victim Network Information
Remote Access (Geographic)	yes	yes	0 days	Initial Access	Valid Accounts
Repeated Umbrella Sinkhole Communications	yes	yes	0 days	Command And Control	Application Layer Protocol
Repeated Watchlist Communications	yes	yes	0 days	Command And Control	Application Layer Protocol
Role Violation	yes	yes	0 days	Persistence	Create or Modify System Process
S3 Bucket Lifecycle Configured	no	AWS-only	0 days	Impact	Data Destruction
SMB Connection Outlier	yes	yes	36 days	Reconnaissance	Gather Victim Network Information
SMB Connection Spike	yes	yes	7 days	Discovery	Network Service Discovery
SMB|RDP: Connection to Multiple Destinations	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility	1 day	Lateral Movement	Remote Services

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
	Client Network Visibility Module (NVM)	Client Network Visibility Module (NVM)			
Stale AWS Access Key	no	AWS-only	30 days	Collection	Data from Cloud Storage Object
Static Device Connection Deviation	yes	yes	1 day	Initial Access	External Remote Services
Static Device Deviation	yes	yes	35 days	Impact	Resource Hijacking
Suspected Botnet Interaction	yes	yes	1 day	Command And Control	Application Layer Protocol
Suspected Cryptocurrency Activity	yes	yes	0 days	Impact	Resource Hijacking
Suspected Malicious URL	requires Security Analytics and Logging (SaaS) or Enhanced NetFlow	requires Security Analytics and Logging (SaaS) or Enhanced NetFlow	0 days	Initial Access	Drive-by Compromise
Suspected Phishing Domain	requires Security Analytics and Logging (SaaS), Enhanced NetFlow, or DNS logs	requires Security Analytics and Logging (SaaS), Enhanced NetFlow, or DNS logs	0 days	Initial Access	Drive-by Compromise
Suspected Port Abuse (External)	yes	yes	1 day	Discovery	Network Service Scanning
Suspected Remote Access Tool Heartbeat	yes	yes	0 days	Command And Control	Non-Application Layer Protocol
Suspicious Curl Behavior	requires transitioning to Cisco XDR and Cisco AnyConnect	requires transitioning to Cisco XDR and Cisco AnyConnect	0 days	Execution	Exploitation for Client Execution

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
	Secure Mobility Client Network Visibility Module (NVM)	Secure Mobility Client Network Visibility Module (NVM)			
Suspicious DNS Over HTTPS Activity	yes	yes	7 days	Defense Evasion	Impair Defenses
Suspicious DNS Over HTTPS Activity	yes	yes	7 days	Defense Evasion	Impair Defenses
Suspicious Domain Lookup Failures	requires DNS logs	no	0 days	Command And Control	Dynamic Resolution
Suspicious Email Findings by Initial Access	requires transitioning to Cisco XDR and require transitioning to Cisco XDR and Cisco ETD (Email Threat Defense)	requires transitioning to Cisco XDR and require transitioning to Cisco XDR and Cisco ETD (Email Threat Defense)	0 days	Initial Access	
Suspicious Endpoint Findings by Collection	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Collection	
Suspicious Endpoint Findings by Command and Control	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike	0 days	Command and Control	

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
	and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	and/or Cisco Secure Endpoint and/or MS Defender for Endpoint			
Suspicious Endpoint Findings by Credential Access	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Credential Access	
Suspicious Endpoint Findings by CrowdStrike Propriety Tactics	requires transitioning to Cisco XDR and CrowdStrike integration	requires transitioning to Cisco XDR and CrowdStrike integration	0 days		
Suspicious Endpoint Findings by Defense Evasion	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Defense Evasion	
Suspicious Endpoint Findings by Discovery	requires transitioning to Cisco XDR and an Endpoint integration such as	requires transitioning to Cisco XDR and an Endpoint integration such as	0 days	Discovery	

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
	CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint			
Suspicious Endpoint Findings by Execution	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Execution	
Suspicious Endpoint Findings by Exfilitration	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Exfiltration	
Suspicious Endpoint Findings by Impact	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for	0 days	Impact	

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
	Endpoint	Endpoint			
Suspicious Endpoint Findings by Initial Access	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Initial Access	
Suspicious Endpoint Findings by Lateral Movement	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	User Execution	
Suspicious Endpoint Findings by MS Defender Proprietary Tactics	requires transitioning to Cisco XDR and MS Defender for Endpoint integration	requires transitioning to Cisco XDR and MS Defender for Endpoint integration	0 days		
Suspicious Endpoint Findings by Persistence	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint	0 days	Persistence	

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
	and/or MS Defender for Endpoint	and/or MS Defender for Endpoint			
Suspicious Endpoint Findings by Privilege Escalation	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Privilege Escalation	
Suspicious Endpoint Findings by Reconnaissance	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Reconnaissance	
Suspicious Endpoint Findings by Resource Development	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	requires transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	0 days	Resource Development	
Suspicious Endpoint Findings without	requires	requires	0 days		

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Tactics	transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint	transitioning to Cisco XDR and an Endpoint integration such as CrowdStrike and/or Cisco Secure Endpoint and/or MS Defender for Endpoint			
Suspicious Process Executed	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	0 days	Execution	User Execution
Suspicious Process Path	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	requires transitioning to Cisco XDR and Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM)	0 days	Defense Evasion	Masquerading
Suspicious SMB Activity	yes	yes	14 days	Lateral Movement	Remote Services
Suspicious User Agent	requires Security Analytics and Logging (SaaS)	requires Security Analytics and Logging (SaaS)	0 days	Initial Access	Exploit Public-Facing Application
Talos Intelligence Watchlist Hits	yes	yes	0 days	Command And Control	Application Layer Protocol

Alert	Private Network Monitoring	Public Cloud Monitoring	History	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
TrickBot AnchorDNS Tunneling	no	AWS-only	14 days	Command And Control	Application Layer Protocol
Unused AWS Resource	no	AWS-only	14 days	Impact	Service Stop
Unusual DNS Connection	yes	yes	1 day	Command And Control	Application Layer Protocol
Unusual External Server	yes	yes	14 days	Command And Control	Application Layer Protocol
Unusual File Extension From New External Server	requires Security Analytics and Logging (SaaS)	requires Security Analytics and Logging (SaaS)	1 days	Command and Control	Application Layer Protocol
Unusually Large EC2 Instance	no	AWS-only	0 days	Impact	Resource Hijacking
User Watchlist Hit	yes	yes	0 days	Command And Control	Web Service
Vulnerable Transport Security Protocol	requires Enhanced NetFlow	requires Enhanced NetFlow	1 day	Defense Evasion	Exploitation for Defense Evasion
Watchlist Hit	yes	yes	0 days	Command And Control	Web Service
Worm Propagation	yes	yes	9 days	Lateral Movement	Exploitation of Remote Services

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. This alert is disabled by default. Make sure to enable this alert, if needed.

Prerequisites: This alert requires 36 days of history to establish the generally expected users that establish sessions with an entity. This alert requires ISE integration for user data attribution.

Associated Observations: ISE Session Started Observations

Next Steps: Reference the supporting observations associated with this alert to determine what user authenticated on the endpoint and at what time. Review the ISE session logs to verify the user and endpoint type correlated with the observations. 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 entity that does not normally see sessions with this user. New user sessions may indicate malicious activity, or expected users that have not yet established regular, repeated sessions.

Prerequisites: This alert requires 36 days of history to establish the generally expected users that establish sessions with an entity. This alert requires one of the following:

- AWS integration.
- ISE integration for user data attribution.
- Sumo Logic

Associated Observations: Session Opened Observations

Next Steps: Reference the supporting observations associated with this alert 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.

Amplification Attack

Description: This entity sent traffic with a profile that suggests participation in an amplification attack. An amplification attack attempts to overwhelm a server with a massive amount of packets in response to a request, usually involving spoofed IP addresses to allow multiple entities to send traffic in response to a request. Participation in an amplification attack may indicate that an entity has been infected with botnet malware, and it is sending these packets unintentionally.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Traffic Amplification Observations

Next Steps: Reference the entity information in the alert and supporting observations, and then 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 entities over BitTorrent). This may be an indication of malware or misuse.

Prerequisite: This alert requires 14 days of history to establish an entity's normal activity level.

Associated Observations: Anomalous Profile Observations

Next Steps: Reference the supporting observations 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 Mac Workstation

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

Prerequisite: This alert requires 14 days of history to establish an entity's normal activity level.

Associated Observations: Anomalous Profile Observations

Next Steps: Reference the supporting observations 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 entities over BitTorrent). This alert may be an indication of malware or misuse.

Prerequisite: This alert requires 14 days of history to establish an entity's normal activity level.

Associated Observations: Anomalous Profile Observations

Next Steps: Reference the supporting observations 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: This entity is normally active for most of the day, but its activity dropped across multiple profiles (e.g., SSH Server, FTP Server). Such behavior may indicate planned downtime or maintenance for the entity, but may also indicate malware that affects the entity's capacity to function, or other malicious behavior that has somehow affected the entity.

Prerequisite: This alert requires 14 days of history to establish an entity's normal activity level.

Associated Observations: Historical Outlier Observations

Next Steps: Reference the supporting observations 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 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.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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: AWS API was accessed from an IP on a watchlist. If an entity on a Secure Cloud Analytics watchlist accessed an API in your AWS deployment, it could indicate an attempt to maliciously access resources, and should be investigated further.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS API Watchlist Access Observations

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 Config Rule Violation

Description: An AWS Config rule was violated. If a configuration change violates your AWS configuration rules, you should examine the change and update the configuration for compliance with the configuration rules.

Prerequisites: This alert requires 0 days of history. This alert 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 Observations: AWS Config Compliance Observations

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: A user tried and failed to log in to the AWS Console several times. If a user repeatedly fails to log into the AWS console, it may indicate an unauthorized user attempting to gain access, or a user that has forgotten their credentials.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read IAM logs.

Associated Observations: AWS CloudTrail Event Observations

Next Steps: Identify the user account associated with the failed logins. Reference the supporting observations to determine whether the logins occurred from a recognized entity on your network. If the logins came from an entity you do not recognize, perform further research on whether or not this is a malicious entity, and reset or lock the user's credentials pending the results of your investigation. Update your block list and firewall rules to disallow this malicious entity from accessing your network.

If you recognize the entity that submitted the login requests, contact the user and determine whether or not they forgot their credentials. If they forgot their credentials, reset them. If they did not forget their credentials, and someone else is attempting to log in as that person, reset or lock the user's credentials, and try to identify the malicious actor on your network. Disconnect the entity's connections to the network and determine if it is infected with malware, or if a malicious actor gained remote access through malware.

AWS Detector Modified

Description: An AWS GuardDuty detector was deleted or disabled. This alert may indicate an attempt to avoid detection of malicious activity.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and GuardDuty enabled.

Associated Observations: AWS CloudTrail Event Observations

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. The may indicate an attempt to hijack the domain, which can then be used in future attacks or to hold the domain for ransom.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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 EC2 Startup Script Modified

Description: An AWS EC2 instance startup script was modified. This alert may indicate an attempt by a malicious actor to establish persistence or execute malicious code.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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 alert may indicate an attacker is attempting to obtain service credentials.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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 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.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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: If you are monitoring AWS CloudTrail logs, this alert indicates a user has created credentials for a different user. This may indicate an attacker is attempting to establish additional persistence in the environment. This alert is disabled by default. Make sure to enable this alert, if needed.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

Next Steps: Verify the legitimacy of the newly created user credentials using the associated observations. If not legitimate, disable the new user, then review CloudTrail logs for the user who created the credentials to see if they performed other suspicious activity.

AWS Inspector Finding

Description: AWS Inspector reported a high-severity finding for the entity. High-severity inspector findings indicate an important security and compliance finding that you should remediate as soon as possible.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, and enabling Inspector.

Associated Observations: Amazon Inspector Finding Observations

Next Steps: Examine the finding in AWS Inspector and take necessary actions to remediate the finding.

AWS Lambda Invocation Spike

Description: A Lambda function was invoked a record number of times. This spike in Lambda function activity could be due to non-malicious behavior, such as Lambda misconfiguration. It could also be due to malicious behavior, such as a malicious actor invoking the function repeatedly in order to tie up resources.

Prerequisites: This alert requires 14 days of history to establish metrics for how often Lambda functions run. This alert also requires AWS integration, and at least one Lambda function in AWS.

Associated Observations: AWS Lambda Metric Outlier Observations

Next Steps: 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.

AWS Lambda Persistence

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.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, allowing Secure Cloud Analytics permission to read CloudTrail logs and at least one Lambda function in AWS.

Associated Observations: AWS Lambda Metric Outlier Observations

Next Steps: 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.

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.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and VPC flow logging or CloudTrail logging enabled.

Associated Observations: AWS CloudTrail Event Observations

Next Steps: Determine what user or process deleted the log information, and identify any other actions that user or process may have taken around the time of the log deletion. Update your firewall rules and security setting to prevent further access if this is the result of malicious behavior.

AWS Logging Impairment

Description: An AWS CloudTrail 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 the attempt by a threat actor to conceal other malicious behavior and utilizes the AWS CloudTrail Event observation.

Associated Observations: AWS CloudTrail Event Observations

Next Steps: Determine whether the detected activity was legitimate. If needed, take action to reverse the AWS VPC Flow Logs, CloudTrail, S3 lifecycle, or event selector changes.

AWS Multifactor Authentication Change

Description: Multifactor authentication was removed from a user account. Removing multifactor authentication is a violation of security best practices.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations, AWS Multifactor Authentication Change Observations

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 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.

Prerequisites: This alert requires 3 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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 Root Account Used

Description: An action was performed using the AWS root account. AWS recommended best practice is to delegate only those permissions required to perform tasks to a user-created account, and to not use the root account if unnecessary.

Prerequisite: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations, AWS Root Account Used Observations

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 Security Group Deleted

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.

Prerequisite: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration, and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

Next Steps: Ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk.

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observations

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. If an entity on a Secure Cloud Analytics watchlist accessed your Azure deployment, it could indicate an attempt to maliciously access resources, and should be investigated further.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Advisor.

Associated Observations: Azure Advisor Recommendation Observations

Next Steps: Review the associated Azure Advisor Recommendation, and take action based on the recommendation.

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration.

Associated Observations: Azure Exposed Services Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observation

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.

Prerequisites: This alert requires 14 days of history. This alert requires Azure integration.

Associated Observations: Azure Functions Metric Outlier Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observations

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: Network Security Groups are identified by Azure Security Center as being too permissive. This can occur if inbound rules allow access from "Any" or "Internet" ranges, or if allowed port ranges are overly permissive. Hardening these rules can help prevent attackers from easily targeting your resources.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and at least one Network Security Group.

Associated Observations: Azure Permissive Security Group Observations

Next Steps: Examine the Network Security Group permissions in Azure, and restrict permissions only to authorized users or domains. Restrict port ranges as needed.

Azure Permissive Storage Account

Description: Storage accounts are identified by Azure Security Center as having unrestricted firewall settings. This could lead to unauthorized access of stored data. It is recommended to configure network rules so only applications from allowed networks or IP address ranges can access the storage account.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and at least one storage account.

Associated Observations: Azure Permissive Storage Setting Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observations

Next Steps: Ensure this action is undertaken purposefully by authorized personnel, in accordance with applicable procedures, and did not create a security risk.

Azure Security Event

Description: Azure Security Center reported a medium or high severity event.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration, Azure Security Center, Standard tier, and Azure Activity Logs.

Associated Observations: Azure Security Event Observations

Next Steps: Review the supporting observations to identify the medium or high severity event. Log into Azure Security Center and review the event. Remediate as needed.

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.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and Azure Activity Logs.

Associated Observations: Azure Unusual Activity Observations

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 previously unused location.

Prerequisites: This alert requires 0 days of history. This alert requires Azure integration and granting Secure Cloud Analytics the Monitoring Reader role permissions to review Azure Subscriptions.

Associated Observations: Azure VM in Unused Location Observations

Next Steps: Review the supporting observations to identify the virtual machine and its location. If the virtual machine creation is possibly malicious, shut down the virtual machine. Remediate as needed.

CloudTrail Watchlist Hit

Description: AWS CloudTrail reported an event on a user-supplied watchlist. You can customize the CloudTrail watchlist to focus on events for your AWS accounts and perform additional research if the system generates these alerts.

Prerequisites: This alert 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.

Associated Observations: AWS CloudTrail Event Observations

Next Steps: Reference the reported event and the alert's supporting observations. Determine if the behavior is malicious, and requires further investigation.

Confirmed Threat Watchlist Hit

Description: This entity interacted with an external resource that is associated with a known threat. This alert is part of encrypted traffic analytics capabilities. Using threat intelligence based on Enhanced NetFlow can provide additional insight into threats to your network.

Prerequisites: This alert requires 0 days of history. The supporting Confirmed Threat Indicator Match – Domain Observations, Confirmed Threat Indicator Match – Hostname Observation, and Confirmed Threat Indicator Match – URL Observations require one or more 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.
- Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.
- DNS logs from a SPAN or mirror port.

Associated Observations: Confirmed Threat Indicator Match – Hostname Observation, Confirmed Threat Indicator Match – IP Observations, Confirmed Threat Indicator Match – Domain Observations, Confirmed Threat Indicator Match – URL Observations

Next Steps: Reference the alert and supporting observations for the type of known threat (domain name, hostname, IP address, or malicious URL). Based on the known threat, remediate as necessary. Update your firewall rules to prevent access to or from the known threat.

Country Set Deviation

Description: This entity has significantly deviated from the set of countries it usually communicates with. This alert is enabled by default.

Prerequisite: This alert requires 36 days of history to establish the normal set of countries an entity communicates with.

Associated Observations: Country Set Deviation Observations

Next Steps: Reference the supporting observations 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. Update your Country Watchlist as necessary to include any countries involved with malicious behavior.

Critical Severity Cloud Posture Watchlist Hit

Description: One or more critical severity compliance failures on the Cloud Posture Watchlist were identified in cloud environments monitored by Secure Cloud Analytics. This alert may indicate the environment is not compliant with best practices.

Prerequisites: This alert requires 0 days of history. This alert requires AWS or Azure integration.

Associated Observations: Compliance Verdict Summary Observations, New Compliance Resource Failure Observations

Next Steps: Click on the ID of the observations in the alert for more information about the compliance failure and remediation next steps to address the failure.

DNS Abuse

Description: This entity has been sending unusually large DNS packets. This could be an attempt to disguise data transfers as DNS traffic. For example, malware could cause an entity to send sensitive information to a remote server under an attacker's control.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Unusual Packet Size Observations

Next Steps: Reference the supporting observations 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 to reduce the number of false positive alerts. 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.

Domain Generation Algorithm Successful Lookup

Description: This entity succeeded in resolving an algorithmically generated domain (e.g., rgkte-hdvj.cc) to an IP address. This can indicate a malware infection or an attempt to create a botnet using command and control servers at the generated domain, or other botnet activity.

Prerequisite: This alert requires 0 days of history. This alert requires DNS logs from a SPAN or mirror port.

Associated Observations: Domain Generation Algorithm Success Observations

Next Steps: Reference the domains listed in the supporting observation, and determine if the domain lookups are benign or malicious. If malicious, identify the software generating

the lookups. Review the Domain Generation Algorithm Success Observations and determine if other entities are making suspicious calls.

Email Spam

Description: This entity has had an anomalous increase in connections with external mail servers. This may indicate malicious behavior, such as botnet malware or an attempt to exfiltrate data, malware that sends and receives spam email, or some other type of compromise.

Prerequisite: This alert requires 36 days of history to establish entity models and expected traffic profiles.

Associated Observations: External Mail Client Connections Observations, Historical Outlier Observations, New Profile Observations

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.

Prerequisite: This alert requires 14 days of history to establish entity models and determine expected traffic profiles.

Associated Observations: New Profile Observations

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.

Prerequisite: This alert requires 1 day of history to establish entity models and determine expected traffic profiles.

Associated Observations: Heartbeat Observations

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.

Exceptional Domain Controller

Description: This entity identified as a Domain Controller deviated from its usual behavior. This may indicate abuse. For example, if the entity is establishing many outbound connections, it may be a sign of data exfiltration, botnet malware, or possibly malicious DNS request redirects.

Prerequisite: This alert requires 7 days of history to establish normal entity traffic profiles.

Associated Observations: Exceptional Domain Controller Observations, New External Server Observations, New High Throughput Connection Observations, New Profile Observations

Next Steps: From the alert and supporting observations, 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.

Excessive Access Attempts (External)

Description: This entity has many failed access attempts from an external entity. For example, a remote entity trying repeatedly to access an internal server using SSH or Telnet would trigger this alert.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Multiple Access Failures Observations

Next Steps: Reference the supporting observations and ensure that the external entity is abnormal and unexpected. If it is normal and expected, determine why a user or machine login 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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Excessive Connections to Network Printers Observations

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 Cloud Function Invocation Spike

Description: A GCP cloud function was invoked a record number of times.

Prerequisites: This alert requires 14 days of history to determine how often functions are invoked. This alert requires integration with GCP.

Associated Observations: GCP Cloud Function Metric Outlier Observations

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. If the invocation spike is benign, Cisco recommends snoozing the alert.

GCP Stackdriver Logging Watchlist Hit

Description: Google Cloud Platform (GCP) Stackdriver Logs reported an event on a user-supplied watchlist.

Prerequisites: This alert requires 0 days of history. This alert also requires integration with GCP and granting Secure Cloud Analytics permission to access Stackdriver Logs.

Associated Observations: GCP Watchlist Activity Observations

Next Steps: Review the supporting observations to determine which watchlist entry generated the event. Remediate as necessary. Log into GCP and update your watchlist as necessary.

Geographically Unusual AWS API Usage

Description: The AWS API has been accessed from a remote host in a country that doesn't normally access the API. For example, accessing your cloud console from an unusual foreign IP would trigger this alert. Users from unexpected geographical locations that access the AWS API could indicate malicious behavior.

Prerequisites: This alert requires 14 days of history to 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.

Associated Observations: AWS CloudTrail Event Observations

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 would trigger this alert. Users from unexpected geographical locations that access the Azure API could indicate malicious behavior.

Prerequisites: This alert requires 14 days of history to establish the normal geolocations for IP addresses that access the Azure API in your deployment. This alert requires Azure integration.

Associated Observations: Azure Unusual Activity Observations

Next Steps: Reference the supporting observations and determine what action the entity took, and why it took the action. If the entity is expected, close the alert if this is a one-time access, or snooze the alert if the unusual access is expected for a period of time. 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: This entity 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 would trigger this alert. Remote access from an unusual geolocation could be an indication of malicious access.

Prerequisite: This alert requires 14 days of history to establish sufficient traffic history, and determine normal traffic based on geolocation.

Associated Observations: Remote Access Observations

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, 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.

Prerequisite: This alert requires 1 day of history to establish traffic models.

Associated Observations: Heartbeat Observations

Next Steps: 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. Understand the purpose for the periodic connections, and update your firewall and blocklist rules to prevent further access.

High Bandwidth Unidirectional Traffic

Description: This entity started sending large amounts of data to new remote hosts. This can indicate misuse or misconfiguration. 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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: New High Throughput Connection Observations

Next Steps: 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.

High Severity Cloud Posture Watchlist Hit

Description: One or more high severity compliance failures on the Cloud Posture Watchlist were identified in cloud environments monitored by Secure Cloud Analytics. This alert may indicate the environment is not compliant with best practices.

Prerequisites: This alert requires 0 days of history. This alert requires AWS or Azure integration.

Associated Observations: Compliance Verdict Summary Observations, New Compliance Resource Failure Observations

Next Steps: Click on the ID of the observations in the alert for more information about the compliance failure and remediation next steps to address the failure.

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.

Prerequisites: This alert requires 0 days of history.

Associated Observations: Unusual Packet Size Observations, New External Server Observations

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.

Prerequisites: This alert requires 14 days of history to establish entity models sufficient to determine when entities start transmitting different traffic types. 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

Associated Observations: Intrusion Detection System Notice Observations, New Profile Observations

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.

Prerequisites: This alert requires 1 day of history to establish normal IDS reporting behavior. This alert also 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
- Zeek IDS

Associated Observations: Intrusion Detection System Notice Observations

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: This entity was port scanned by an external entity. If an external entity is scanning entities internal to your network, it may be scanning for unpatched vulnerabilities or other ways to infiltrate entities on your network.

Prerequisite: This alert requires 1 day of history to establish entity models and determine normal behavior.

Associated Observations: External Port Scanner Observations

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: This entity had a sudden increase in internal connections, which is suggestive of scanning activity.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Record Metric Outlier Observations

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 data.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Internal Connection Watchlist Observations

Next Steps: 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.

The system generates this alert only if a user enters a segmentation rule.

Internal Port Scanner

Description: This entity has started a port scan on an entity internal to your network. If an internal entity is scanning entities internal to your network, it may be a penetration test by your network security team, or it may be malicious behavior from an entity on your network.

Prerequisite: This alert requires 7 days of history to establish entity models and normal entity behavior.

Associated Observations: Internal Port Scanner Observations, Port Scanner Observations

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.

Prerequisite: This alert requires 0 days of history to establish entity models and normal entity behavior.

Associated Observations: ISE Session Started Observations

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.

ISE Jailbroken Device

Description: Cisco Identity Services Engine (ISE) detected a device that has been jailbroken. Such devices should be considered insecure because they're more vulnerable to threats. This does not necessarily indicate an active threat in isolation, but is a vulnerability that may increase organizational risk. This alert is disabled by default. Make sure to enable this alert, if needed.

Prerequisite: This alert requires integration with ISE. This alert requires 0 days of history.

Associated Observations: ISE Session Started Observations

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 Suspicious Process

Description: Device was detected running a non-standard LDAP process. This might indicate a credential theft attempt. This alert is disabled by default. Make sure to enable this alert, if needed.

Prerequisite: This alert requires integration with NVM. This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

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.

Prerequisite: This alert requires 9 days of history to establish normal behavior.

Associated Observations: IP Scanner Observations

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.

Low Severity Cloud Posture Watchlist Hit

Description: One or more low severity compliance failures on the Cloud Posture Watchlist were identified in cloud environments monitored by Secure Cloud Analytics. This alert may indicate the environment is not compliant with best practices.

Prerequisites: This alert requires 0 days of history. This alert requires AWS or Azure integration.

Associated Observations: Compliance Verdict Summary Observations, New Compliance Resource Failure Observations

Next Steps: Click on the ID of the observations in the alert for more information about the compliance failure and remediation next steps to address the failure.

Malicious Process Detected

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

Prerequisite: This alert requires integration with NVM. This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

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

Malware Spike

Description: This entity triggered an abrupt rise in IDS observations.

Prerequisites: This alert requires 1 day of history to establish normal IDS reporting behavior. This alert also 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.

Associated Observations: Malware Event Observations

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.

Medium Severity Cloud Posture Watchlist Hit

Description: One or more medium severity compliance failures on the Cloud Posture Watchlist were identified in cloud environments monitored by Secure Cloud Analytics. This alert may indicate the environment is not compliant with best practices.

Prerequisites: This alert requires 0 days of history. This alert requires AWS or Azure integration.

Associated Observations: Compliance Verdict Summary Observations, New Compliance Resource Failure Observations

Next Steps: Click on the ID of the observations in the alert for more information about the compliance failure and remediation next steps to address the failure.

Meterpreter Command and Control Success

Description: Device has established new periodic connections that appear to be part of a Meterpreter Command and Control channel. This alert may indicate the device is compromised.

Prerequisites: This alert requires 1 day of history to establish normal behavior.

Associated Observations: Heartbeat Observations

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.

Missing Sumo Logic Log

Description: One or more logs, expected for entities with this role, were not found in your Sumo Logic database. This may mean that one of your Sumo Logic collectors is misconfigured or missing.

Prerequisites: This alert requires 0 days of history. This alert requires a Sumo Logic integration.

Associated Observations: Sumo Logic Log Observations

Next Steps: Examine your Sumo Logic collectors and check their configuration. If one of your Sumo Logic collectors cannot be detected from the network, redeploy it or verify its connection.

NetBIOS Connection Spike

Description: Source attempted to contact large number of hosts using NetBIOS. This can be an indication of malware or abuse.

Prerequisite: This alert requires 7 days of history to establish entity traffic models and determine normal traffic behavior.

Associated Observations: IP Scanner Observations

Next Steps: Reference the supporting observations 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. If so, snooze this alert for the host.

Network Population Spike

Description: A record number of IP addresses were observed communicating on the network. This might indicate spoofing of source addresses or scanning activity.

Prerequisite: This alert requires 36 days of history to establish a sufficient amount of days to count the total number of entities communicating on the network.

Associated Observations: Population Spike Observations

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 malicious behavior, such as botnet malware infection.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Network Printer with Excessive Connections Observations

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 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.

Prerequisite: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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.

New AWS Region

Description: An AWS resource was detected in a previously unused region.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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 AWS CloudTrail Event Observations to see more details about who created the resource and the configuration.

New AWS Route53 Target

Description: A new AWS Route53 resource record was assigned to an entity that was not previously associated with a Route53 resource record. This alert requires 0 days of history. A new Route53 resource record may indicate an attempt to maliciously redirect traffic for the entity.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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.

New External Connection

Description: During the baseline period, the entity never communicated bidirectionally outside the organization, then did so for the first time, which is a behavior deviation.

Prerequisite: This alert requires 35 days of history to establish traffic models and determine expected traffic behavior.

Associated Observations: New External Connection Observations

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 entity has appeared on a restricted subnet range after not being seen in the look-back period.

Prerequisite: This alert requires 21 days of history to learn which entities are normally seen on the network. This alert also requires selecting **New Internal Device** on the Subnet Configuration page.

Associated Observations: New Internal Device Observations

Next Steps: Reference the supporting observations to determine if this is an expected entity that is new to your network. If the entity is expected and not malicious, close the alert; future new entities will continue to generate alerts. If the entity is suspicious, determine the Mac address by accessing the local switch.

New IP Scanner

Description: This entity started scanning the local IP network. This could indicate, for example, reconnaissance by an attacker.

Prerequisite: This alert requires 7 days of history to establish entity traffic models and determine normal traffic behavior.

Associated Observations: IP Scanner Observations

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 Long Sessions (Geographic)

Description: This entity has established a long-lived connection with a host in a watchlisted country. These connections may indicate malicious behavior by users in these countries.

Prerequisite: This alert requires 2 days of history to establish which connections have been established for an extended period of time. You can configure the countries added to the Country Watchlist in the Secure Cloud Analytics web portal UI.

Associated Observations: Long Session Observations

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.

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 remote access may indicate malicious behavior, especially if the entity is not expected to accept connections from external entities.

Prerequisite: This alert requires 36 days of history to establish sufficient traffic history and entity models.

Associated Observations: Remote Access Observations

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: This entity attempted to reach a large number of hosts using SNMP. This can be an indication of network reconnaissance cause by malicious software. An SNMP sweep, when performed by a malicious actor, could result in gathering information about your network, or malicious entity configuration updates.

Prerequisite: This alert requires 7 days of history to establish entity traffic models and determine normal traffic behavior.

Associated Observations: IP Scanner Observations

Next Steps: Reference the supporting observations 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, or snooze the alert.

New Unusual DNS Resolver

Description: This entity contacted a DNS resolver that it doesn't normally use. This can indicate misconfiguration or the presence of malware. For example, an attacker could cause a DNS resolver to redirect a popular website to a domain that serves additional malware.

Prerequisite: This alert requires 7 days of history to establish entity roles and model normal traffic.

Associated Observations: Unusual DNS Resolver Observations

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, and snooze the alert if traffic is expected.

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.

Prerequisite: This alert requires 9 days of history to establish entity models and determine normal behavior.

Associated Observations: IP Scanner Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: IP Scanner Observations

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 SMB Connection Spike

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: IP Scanner Observations

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: Source started sending a much larger amount of traffic to external destinations than before. Large traffic spikes that have not been seen before could indicate malicious behavior, such as data exfiltration. Even if this behavior is non-malicious, it may still need to be investigated.

Prerequisite: This alert requires 14 days of history to establish an entity model with enough information to show the normal levels of traffic that this entity sends.

Associated Observations: Historical Outlier Observations, Record Metric Outlier Observations, Record Profile Outlier Observations, New Large Connection (External) Observations

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.

Prerequisite: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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. A VPC security group with unsafe ports unsecured constitutes a security issue, and those ports should be secured.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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: This entity 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.

Prerequisite: This alert requires 7 days of history to establish traffic models and determine normal traffic behavior.

Associated Observations: New External Server Observations, Persistent External Server Observations

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.

Prerequisite: This alert requires integration with NVM. This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

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

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Potential Data Forwarding Observations

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 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.

Prerequisite: This alert requires 7 days of history to establish which entities normally serve as databases, and what their normal traffic profiles are.

Associated Observations: New High Throughput Connection Observations

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 Persistence Attempt

Description: Device was detected applying known persistence mechanisms like establishing background processes used for network access or running applications from network shares. This alert is disabled by default. Make sure to enable this alert, if needed.

Prerequisite: This alert requires integration with NVM. This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

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

Potential System Process Impersonation

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

Prerequisite: This alert requires integration with NVM. This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

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

Potentially Harmful Hidden File Extension

Description: This entity has encountered a file with a potentially harmful hidden extension. Files with hidden, potentially harmful extensions may constitute malware.

Prerequisites: This alert requires 0 days of history. This alert requires one or more of following:

- 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.

Associated Observations: Multiple File Extension Observations

Next Steps: Reference the supporting observations 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.

Prerequisites: This alert requires 1 day of history to establish which entities use remote control applications. This alert requires Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.

Associated Observations: Insecure Transport Protocol Observations

Next Steps: Reference the supporting observations 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.

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.

Prerequisite: This alert requires 1 day of history to establish entity models and see which entities use potentially restricted services.

Associated Observations: Insecure Transport Protocol Observations

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.

Protocol Violation (Geographic)

Description: This entity tried to communicate with a host in a watchlisted country on an illegal protocol / port combination (e.g., UDP on port 22).

Prerequisites: This alert requires 0 days of history. You must configure the Country Watchlist with at least one country.

Associated Observations: Bad Protocol Observations

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.

Public Amazon Route 53 Hosted Zone Created

Description: A public Amazon Route 53 hosted zone was created.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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.

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).

Prerequisite: This alert requires 0 days of history.

Associated Observations: Public Facing IP Watchlist Match Observations

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.

Remote Access (Geographic)

Description: This entity has been accessed from a remote host in a watchlisted country.

Prerequisite: This alert requires 0 days of history. This alert requires configuring the Country Watchlist with at least one country.

Associated Observations: Remote Access Observations

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.

Repeated Umbrella Sinkhole Communications

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

Prerequisite: This alert requires 0 days of history.

Associated Observations: Heartbeat Observations, Umbrella Sinkhole Hit Observations,

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Watchlist Interaction Observations, Heartbeat Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Role Violation Observations

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.

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.

Prerequisites: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: AWS CloudTrail Event Observations

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.

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.

Prerequisite: This alert requires 36 days of history to establish entity traffic models and determine normal traffic behavior.

Associated Observations: Historical Outlier Observations

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

Description: This entity attempted to contact an unusually large number of SMB servers. This can be an indication of malware or abuse. As SMB is used primarily for file sharing, but can also be used for accessing network printers or browsing other hosts on a network, this could indicate data exfiltration or network resource misuse.

Prerequisite: This alert requires 9 days of history to establish entity traffic models and determine normal traffic behavior.

Associated Observations: IP Scanner Observations

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|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.

Prerequisite: This alert requires integration with NVM. This alert requires 1 day of history.

Associated Observations: Suspicious Endpoint Activity Observations

Next Steps: Verify if this type of internal connection is normal for these endpoints.

Stale AWS Access Key

Description: AWS IAM access key exceeded the configurable age. This violates best practices.

Prerequisites: This alert requires 30 days of history. This alert also requires AWS integration.

Associated Observations: AWS Architecture Compliance Observations

Next Steps: Verify that the IAM user account should still have access. Adjust your IAM policy to ensure keys are rotated more regularly.

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.

Prerequisite: This alert requires 1 day of history to establish entity models and determine normal traffic and behavior.

Associated Observations: Historical Outlier Observations and New External Connection Observations

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: This entity is normally static on the network, communicating on the same ports or to the same entities, with a similar traffic pattern each day. This entity has recently deviated from its norms, which may be a sign of misuse. This alert is enabled by default.

Prerequisite: This alert requires 35 days of history to establish entity models and determine normal traffic and behavior.

Associated Observations: Historical Outlier Observations, Static Connection Set Deviation Observations, Static Port Set Deviation Observations

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: This entity exchanged traffic with IP addresses associated with botnets, or attempted to resolve domain names associated with botnets.

Prerequisite: This alert requires 1 day of history to establish entity models.

Associated Observations: Watchlist Interaction Observations

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 observations 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: Source exchanged a significant amount of traffic with multiple addresses known to be operating cryptocurrency nodes, based on Talos intelligence, and other sources. This behavior may indicate that an entity is being used to mine cryptocurrency.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Watchlist Interaction Observations

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

Suspected Malicious URL

Description: The entity communicated with a suspected malicious URL. This may indicate malicious access or compromise of an entity.

Prerequisites: This alert requires 0 days of history. This alert requires one of the following:

- 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.

Associated Observations: Suspected Malicious URL Observations

Next Steps: Reference the supporting observations to determine what URL the entity accessed. Determine if the entity is compromised, and remove malware from the entity if it is infected. Update your block list and firewall rules to prevent access to the URL.

Suspected Phishing Domain

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

Prerequisites: This alert requires 0 days of history. This alert requires one of the following:

- 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.

Associated Observations: Suspected Phishing Domain Observations

Next Steps: 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.

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 Port Abuse (External)

Description: This entity is communicating with an external host on unusual range of ports. This can indicate externally initiated abuse (e.g., a spoof attack) or an internally initiated port scan.

Prerequisite: This alert requires 1 day of history to establish entity models.

Associated Observations: Port Scanner Observations, External Port Scanner Observations

Next Steps: Reference the supporting observations 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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Network Activity Observations

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 alert uses the Suspicious Network Activity observation and may indicate the device is being targeted for exploitation.

Prerequisites: This alert requires 0 days of history.

Associated Observations: Suspicious Network Activity Observations

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.

Prerequisite: This alert requires integration with NVM. This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

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.

Prerequisite: This alert requires 7 days of history.

Associated Observations: Watchlist Interaction Observations

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 can indicate a malware infection or an attempt to create a botnet using command and control servers at the generated domain.

Prerequisite: This alert requires 0 days of history. This alert requires DNS logs from a SPAN or mirror port.

Associated Observations: Domain Generation Algorithm Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Email Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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: Execution of the offensive tool, Metasploit, has been detected in an endpoint through endpoint telemetry.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Security Finding Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Suspicious Endpoint Activity Observations

Next Steps: Isolate the endpoint and investigate if executables were downloaded in non-standard directories and executed.

Suspicious SMB Activity

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

Prerequisite: This alert requires 14 days of history.

Associated Observations: Suspicious SMB Activity Observations

Next Steps: Reference the supporting observations 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.

Prerequisite: This alert requires 0 days of history. This alert 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.

Associated Observations: Anomalous User Agent Observations

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.

Talos Intelligence Watchlist Hits

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

Prerequisite: This alert requires 0 days of history.

Associated Observations: Watchlist Interaction Observations

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.

Prerequisites: This alert requires 0 days of history. This alert requires DNS logs from a SPAN or mirror port.

Associated Observations: TrickBot AnchorDNS Tunneling Activity Observations

Next Steps: Quarantine the entity and remove all malware. Update your block list and firewall rules to disallow any botnet entities from accessing your network. Reference the supporting observations 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.

Unused AWS Resource

Description: No recent activity has been seen for this AWS resource. This may be expected behavior, as a resource is no longer relevant.

Prerequisites: This alert requires 0 days of history.

Associated Observations: Unused AWS Resource Observations

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.

Unusual DNS Connection

Description: This entity contacted an unusual DNS resolver and then established periodic connections with a remote entity. This behavior may indicate a malicious redirect of traffic, or a malware infection on an entity.

Prerequisite: This alert requires 1 day of history to establish entity models.

Associated Observations: Unusual DNS Resolver Observations, Heartbeat Observations

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: This entity has repeatedly communicated with a new external server with suspicious traffic profiles. This could indicate, for example, a new piece of software that is acting as a server to an external entity, such as syslog or TeamViewer.

Prerequisite: This alert requires 14 days of history to establish normal traffic patterns, and determine expected external entity traffic.

Associated Observations: New External Server Observations, Persistent External Server Observations

Next Steps: Reference the supporting observations 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.

Prerequisite: This alert requires 1 day of history to establish entity models. This alert 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.

Associated Observations: New External Server Observations, New File Extension Observations

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.

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.

Prerequisite: This alert requires 0 days of history. This alert requires AWS integration and allowing Secure Cloud Analytics permission to read CloudTrail logs.

Associated Observations: Unusual EC2 Instance Observations

Next Steps: Examine the new devices in question and determine whether they are legitimately deployed or not.

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.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Watchlist Lookup Observations, Watchlist Interaction Observations

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.

Vulnerable Transport Security Protocol

Description: This entity was observed using an insecure SSL/TLS protocol version.

Prerequisite: This alert requires 1 day of history to establish entity models. This alert requires Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.

Associated Observations: Insecure Transport Protocol Observations

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: This entity exchanged traffic with an IP address on a watchlist, or attempted to resolve a domain name on a watchlist. The Secure Cloud Analytics engine includes

several built-in watchlists.

Prerequisite: This alert requires 0 days of history.

Associated Observations: Watchlist Lookup Observations, Watchlist Interaction Observations

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.

Prerequisite: This alert requires 9 days of history to establish normal behavior.

Associated Observations: Worm Propagation Observations

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 Observation

Description: Amazon GuardDuty reported a suspicious DNS request.

Prerequisites: This observation requires AWS integration and enabling GuardDuty.

Amazon GuardDuty Network Connection Finding Observation

Description: Amazon GuardDuty reported a suspicious network connection.

Prerequisites: This observation requires AWS integration and enabling GuardDuty.

Amazon Inspector Finding Observation

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 Observation

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).

Prerequisite: None.

Associated Alerts: Anomalous AWS Workspace Alerts, Anomalous Mac Workstation, Anomalous Windows Workstation Alerts

Anomalous User Agent Observation

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 Observation

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 Observation

Description: Detected AWS resource that may violate AWS "Well-architectured" guidelines.

Prerequisite: This observation requires AWS integration.

Associated Alerts: Stale AWS Access Key Alerts

AWS CloudTrail Event Observation

Description: AWS CloudTrail event reported for the entity.

Prerequisites: This observation requires AWS integration and enabling CloudTrail.

Associated Alerts: AWS Console Login Failures Alerts, AWS Detector Modified Alerts, AWS EC2 Startup Script Modified Alerts, AWS ECS Credential Access Alerts, AWS IAM Anywhere Trust Anchor Created Alerts, AWS Logging Deleted Alerts, AWS Repeated API Failures Alerts, AWS Root Account Used Alerts, AWS Snapshot Exfiltration Alerts, AWS Temporary Token Persistence Alerts, Geographically Unusual AWS API Usage Alerts, New AWS Lambda Invoke Permission Added Alerts, New AWS Region Alerts, New AWS Route53 Target Alerts, Permissive Amazon Elastic Kubernetes Service Cluster Created Alerts, Permissive AWS S3 Access Control List Alerts, Permissive AWS Security Group Created Alerts, Public Amazon Route 53 Hosted Zone Created Alerts, S3 Bucket Lifecycle Configured Alerts

AWS Config Compliance Observation

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 Observation

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: AWS Config Rule Violation Alerts

AWS Lambda Metric Outlier Observation

Description: An AWS Lambda function had unusual activity on one of its metrics, such as number of times invoked.

Prerequisites: This observation requires AWS integration and at least one Lambda function.

Associated Alerts: AWS Lambda Invocation Spike Alerts, AWS Lambda Persistence Alerts

AWS Multifactor Authentication Change Observation

Description: Multifactor authentication was removed from a user account.

Prerequisites: This observation requires AWS integration and enabling CloudTrail.

Associated Alerts: AWS Multifactor Authentication Change Alerts

AWS New User Action Observation

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

Prerequisites: This observation requires AWS integration and enabling CloudTrail.

AWS Root Account Used Observation

Description: An action was performed using the AWS root account.

Prerequisites: This observation requires AWS integration and enabling CloudTrail.

Associated Alerts: AWS Root Account Used Alerts

Azure Advisor Recommendation Observation

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 Observation

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 Observation

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 Observation

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 Observation

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 Observation

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: Azure Security Event Alerts

Azure Unusual Activity Observation

Description: Unusual activity detected in Azure Activity Logs.

Prerequisites: This observation requires Azure integration and Azure Activity Logs.

Associated Alerts: Azure Activity Log IP Watchlist Hit, Azure Activity Log Watchlist Hit Alerts, 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 Observation

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 Observation

Description: An entity used a non-standard protocol on a standard port (e.g., UDP on port 22).

Prerequisite: None

Associated Alerts: Protocol Violation (Geographic) Alerts

Cluster Change Observation

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.

Prerequisite: None.

Compliance Verdict Summary Observation

Description: Detected cloud resources that violate compliance framework recommendations.

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

Associated Alerts: Critical Severity Cloud Posture Watchlist Hit Alerts, High Severity Cloud Posture Watchlist Hit Alerts, Low Severity Cloud Posture Watchlist Hit Alerts, Medium Severity Cloud Posture Watchlist Hit Alerts

Confirmed Threat Indicator Match - Domain Observation

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

Prerequisite: 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: Confirmed Threat Watchlist Hit Alerts

Confirmed Threat Indicator Match - Hostname Observation

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

Prerequisite: This observation requires Enhanced NetFlow. See the Secure Cloud Analytics Configuration Guide for Enhanced NetFlow for more information.

Associated Alerts: Confirmed Threat Watchlist Hit Alerts

Confirmed Threat Indicator Match - IP Observation

Description: An entity communicated with an IP address listed as an IOC for a known threat.

Prerequisite: None.

Associated Alerts: Confirmed Threat Watchlist Hit Alerts

Confirmed Threat Indicator Match - URL Observation

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

Prerequisite: This observation requires one of the following:

- 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: Confirmed Threat Watchlist Hit Alerts

Country Set Deviation Observation

Description: An entity communicated with a set of countries different from its usual one.

Prerequisite: None.

Associated Alerts: Country Set Deviation Alerts

Domain Generation Algorithm Observation

Description: An entity attempted to contact an algorithmically generated domain (e.g., qhjvd-hdvj.cc).

Prerequisite: None.

Associated Alerts: Suspicious Domain Lookup Failures Alerts

Domain Generation Algorithm Success Observation

Description: An entity succeeded in resolving an algorithmically generated domain (e.g., rgkte-hdvj.cc) to an IP address.

Prerequisite: None.

Associated Alerts: Domain Generation Algorithm Successful Lookup Alerts

Drive By Download Observation

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.

Prerequisite: None.

Associated Alerts: None.

Exceptional Domain Controller Observation

Description: Domain Controller entity communicated with unusual external ports.

Prerequisite: None.

Associated Alerts: Exceptional Domain Controller Alerts

Excessive Connections to Network Printers Observation

Description: An entity initiated excessive connections to network printers.

Prerequisite: None.

Associated Alerts: Excessive Connections to Network Printers Alerts

External Mail Client Connections Observation

Description: An entity communicated with many external mail servers.

Prerequisite: None.

Associated Alerts: Email Spam Alerts

External Port Scanner Observation

Description: An entity on the local network scanned (or was scanned by) a remote IP address.

Prerequisite: None.

Associated Alerts: Inbound Port Scanner Alerts, Suspected Port Abuse (External) Alerts

GCP Cloud Function Metric Outlier Observation

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 Observation

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: GCP Stackdriver Logging Watchlist Hit Alerts

Geographic Watchlist Observation

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.

Prerequisite: None.

Heartbeat Observation

Description: An entity maintained a heartbeat with a remote host.

Prerequisite: None.

Associated Alerts: Empire Command and Control Alert, Heartbeat Connection Count Alerts, Meterpreter Command and Control Success Alerts, Repeated Umbrella Sinkhole Communications Alerts, Repeated Watchlist Communications Alerts, Unusual DNS Connection Alerts

Historical Outlier Observation

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.

Prerequisite: None.

Associated Alerts: Attendance Drop Alerts, Email Spam Alerts, Outbound Traffic Spike Alerts, SMB Connection Outlier Alerts, Static Device Connection Deviation Alerts, Static Device Deviation Alerts

Insecure Transport Protocol Observation

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: Potentially Vulnerable Remote Control Protocol Alerts, Protocol Forgery Alerts, Vulnerable Transport Security Protocol Alerts

Internal Connection Watchlist Observation

Description: Forbidden communications between two internal IP endpoints were detected.

Prerequisite: None.

Associated Alerts: Internal Connection Watchlist Alerts

Internal Port Scanner Observation

Description: An entity scanned a large number of ports.

Prerequisite: None.

Associated Alerts: Internal Port Scanner Alerts

Intrusion Detection System Notice Observation

Description: An IDS saw traffic matching a suspicious signature.

Prerequisites: This observation requires one of the following:

- 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: IDS Emergent Profile Alerts, IDS Notice Spike Alerts

IP Scanner Observation

Description: An entity scanned a large number of entities.

Prerequisite: None.

Associated Alerts: 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, Outbound SMB Spike Alerts, SMB Connection Spike Alerts

ISE Session Started Observation

Description: A new user session was created on Cisco Identity Services Engine (ISE).

Prerequisite: This observation requires integration with Cisco Identity Services Engine (ISE).

Associated Alerts: Abnormal ISE User Alerts

ISE Suspicious Activity Observation

Description: A suspicious activity was detected on Cisco ISE.

Prerequisite: This observation requires integration with Cisco Identity Services Engine (ISE).

Long Session Observation

Description: An entity maintained a long-lived session with an external IP address.

Prerequisite: None.

Associated Alerts: New Long Sessions (Geographic) Alerts

Malware Event Observation

Description: Malware activity detected from the entity

Prerequisite: 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 Observation

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

Prerequisite: None.

Associated Alerts: Excessive Access Attempts (External) Alerts

Multiple File Extensions Observation

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 Observation

Description: Network printer initiated excessive connections to other entities.

Prerequisite: None.

Associated Alerts: Network Printer with Excessive Connections Alerts

New Compliance Resource Failure Observation

Description: Detected cloud resources that violate compliance framework recommendations when they were compliant the previous day.

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

Associated Alerts: Critical Severity Cloud Posture Watchlist Hit Alerts, High Severity Cloud Posture Watchlist Hit Alerts, Low Severity Cloud Posture Watchlist Hit Alerts, Medium Severity Cloud Posture Watchlist Hit Alerts

New External Connection Observation

Description: A usually predictable local entity communicated with an external entity.

Prerequisite: None.

Associated Alerts: New External Connection Alerts, Static Device Connection Deviation Alerts

New External Server Observation

Description: An entity started communicating with an external server.

Prerequisite: None.

Associated Alerts: Exceptional Domain Controller Alerts, ICMP Abuse Alerts, Persistent Remote Control Connections Alerts, Unusual External Server Alerts, Unusual File Extension from New External Server Alerts

New File Extension Observation

Description: A new file extension was exchanged.

Prerequisite: 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, Unusual File Extension from New External Server Alerts

New High Throughput Connection Observation

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

Prerequisite: None.

Associated Alerts: Exceptional Domain Controller Alerts, High Bandwidth Unidirectional Traffic Alerts, Potential Database Exfiltration Alerts

New Internal Connection Observation

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

Prerequisite: None.

New Internal Device Observation

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

Prerequisite: None.

Associated Alerts: New Internal Device Alerts

New Large Connection (External) Observation

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

Prerequisite: None.

Associated Alerts: Outbound Traffic Spike Alerts

New Large Connection (Internal) Observation

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

Prerequisite: None.

New Profile Observation

Description: An entity matches a profile tag (e.g., FTP server) that it hasn't matched recently.

Prerequisite: None.

Associated Alerts: Email Spam Alerts, Emergent Profile Alerts, Exceptional Domain Controller Alerts

Persistent External Server Observation

Description: This entity has regularly communicated with the same external server (FTP, SSH, etc.).

Prerequisite: None.

Associated Alerts: Persistent Remote Control Connections Alerts, Unusual External Server Alerts

Population Spike Observation

Description: A record number of IP addresses were observed communicating on the local network.

Prerequisite: None.

Associated Alerts: Network Population Spike Alerts

Port Scanner Observation

Description: An entity scanned a large number of ports.

Prerequisite: None.

Associated Alerts: Internal Port Scanner Alerts, Suspected Port Abuse (External) Alerts

Potential Data Forwarding Observation

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").

Prerequisite: None.

Associated Alerts: Potential Data Exfiltration Alerts

Public Amazon Route 53 Hosted Zone Created Observation

Description: A public Amazon Route 53 hosted zone was created.

Prerequisite: This observation requires integration with AWS and enabling CloudTrail.

Public Facing IP Watchlist Match Observation

Description: A public-facing IP in your network was discovered on a watchlist (either explicitly or implicitly via a domain name).

Prerequisite: None.

Associated Alerts: Public Facing IP Watchlist Match Alerts

Public IP Service Observation

Description: The device used an IP service that could be used by a malware.

Prerequisite: 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: Public IP Services Alerts

Rapid Logins Observation

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

Prerequisite: None.

Record Metric Outlier Observation

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

Prerequisite: None.

Associated Alerts: Internal Connection Spike Alerts, Outbound Traffic Spike Alerts

Record Profile Outlier Observation

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

Prerequisite: None.

Associated Alerts: Outbound Traffic Spike Alerts

Remote Access Observation

Description: An entity was accessed from a remote source.

Prerequisite: None.

Associated Alerts: Geographically Unusual Remote Access Alerts, New Remote Access Alerts, Remote Access (Geographic) Alerts

Role Violation Observation

Description: An entity has new traffic that doesn't fit its role (e.g., FTP server communicating on port 80).

Prerequisite: None.

Associated Alerts: Role Violation Alerts

Scan Result Observation

Description: An active scanner (e.g., nmap) discovered an entity behavior.

Prerequisite: None.

Session Closed Observation

Description: A user session was closed.

Prerequisites: This observation requires an OSSEC, Sumo Logic, or Active Directory deployment.

Session Opened Observation

Description: A user session was opened.

Prerequisite: None.

Associated Alerts: Abnormal User Alerts

Static Connection Set Deviation Observation

Description: An entity normally talks to a static set of (internal/external) entities, but has recently started/stopped talking to new/normal entities.

Prerequisite: None.

Associated Alerts: Static Device Deviation Alerts

Static Port Set Deviation Observation

Description: An entity normally uses a static set of (local/connected) ports for (internal/external) communications, but has recently added/dropped ports.

Prerequisite: None.

Associated Alerts: Static Device Deviation Alerts

Sumo Logic Log Observation

Description: An entity may be contributing to logs hosted by Sumo Logic.

Prerequisite: This observation requires a Sumo Logic deployment.

Associated Alerts: Missing Sumo Logic Log Alerts

Suspected Malicious URL Observation

Description: The host communicated with a suspected malicious URL.

Prerequisite: This observation requires one of the following:

- 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: Suspected Malicious URL Alerts

Suspected Phishing Domain Observation

Description: The host communicated with a suspected phishing domain.

Prerequisites: This observation requires one of the following:

- 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 Observation

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

Prerequisite: Email integration.

Associated Alerts: Suspected Email Findings by Initial Access

Suspicious Endpoint Activity Observation

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

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

Associated Alerts: LDAP Connection from Suspicious Process Alerts, Malicious Process Detected Alerts, Port 8888: Connects from Multiple Sources Alerts, Potential Persistence Attempt Alerts, Potential System Process Impersonation Alerts, SMB|RDP: Connection to Multiple Destinations Alerts, Suspicious Curl Behavior, Suspicious Process Executed, and Suspicious Process Path Alerts

Suspicious Endpoint Security Finding Observation

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

Prerequisite: Endpoint integration.

Associated Alerts: Suspicious Endpoint Findings by Collection, Suspicious Endpoint Findings by Command and Control, Suspicious Endpoint Findings by Credential Access, Suspicious Endpoint Findings by CrowdStrike Propriety Tactics, Suspicious Endpoint Findings by Defense Evasion, Suspicious Endpoint Findings by Discovery, Suspicious Endpoint Findings by Execution, Suspicious Endpoint Findings by Exfilitration, 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, and Suspicious Endpoint Findings without Tactics

Suspicious Network Activity Observation

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

Prerequisite: None.

Associated Alerts: Suspected Remote Access Tool Heartbeat Alerts, Suspected Zerologon RPC Exploit Attempt Alerts

Suspicious SMB Activity Observation

Description: Multiple entities have performed anomalous activity using the SMB protocol for the first time.

Prerequisite: None.

Associated Alerts: Suspicious SMB Activity Alerts

Traffic Amplification Observation

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.

Prerequisite: None.

Associated Alerts: Amplification Attack Alerts

TrickBot AnchorDNS Tunneling Activity Observation

Description: The device used the TrickBot Anchor_DNS tunneling method to communicate with a C&C server.

Prerequisite: None.

Associated Alerts: TrickBot AnchorDNS Tunneling Alerts

Umbrella Sinkhole Hit Observation

Description: The device communicated with a known Cisco Umbrella sinkhole.

Prerequisite: None.

Associated Alerts: Repeated Umbrella Sinkhole Communications Alerts

Unused AWS Resource Observation

Description: No recent activity seen for an AWS resource.

Prerequisite: This observation requires AWS integration.

Associated Alerts: Unused AWS Resource Alerts

Unusual DNS Resolver Observation

Description: An entity communicated with an unusual DNS resolver.

Prerequisite: None.

Associated Alerts: New Unusual DNS Resolver Alerts, Unusual DNS Connection Alerts

Unusual EC2 Instance Observation

Description: A new EC2 instance of unusual type and size has been created.

Prerequisite: This observation requires AWS integration and enabling CloudTrail.

Associated Alerts: Unusually Large EC2 Instance Alerts

Unusual Packet Size Observation

Description: An entity sent or received packets that are unusually sized for the given profile.

Prerequisite: None.

Associated Alerts: DNS Abuse Alerts, ICMP Abuse Alerts

Watchlist Interaction Observation

Description: An entity communicated with an IP address that is on a watchlist (either explicitly or implicitly via a domain name).

Prerequisite: None.

Associated Alerts: 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 Observation

Description: An entity looked up a watchlisted domain.

Prerequisite: None.

Associated Alerts: User Watchlist Hit Alerts, Watchlist Hit Alerts

Worm Propagation Observation

Description: Previously scanned device started scanning the local IP network.

Prerequisite: 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	Added the following alerts and an observation: • Anomalous AWS Workspace Alert • Anomalous Mac Workstation Alert • Empire Command and Control alert • Malware Spike Alert • Anomalous Profile Observation Updated the following alert and observations: • Email Spam Alert • Historical Outlier Observation • New Profile Observation Also added additional information about Security Analytics and Logging (SaaS).
2.0	October 25, 2021	Rebranded, and added the following alerts and observations: • 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

		• 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	Updated the MITRE ATT&CK tactics/techniques for alerts, and added the following alerts: • 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 Alert • 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 Added the following observations: • 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 Removed the following alerts: • 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	Added the following alerts: • AWS IAM Anywhere Trust Anchor Created Alert • New AWS Lambda Invoke Permission Added Alert

		• Unusually Large EC2 Instance Alert Added the Unusual EC2 Instance Observation, and updated telemetry requirements for alerts and the MITRE ATT&CK tactics/techniques for alerts.
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	Added the following alerts: • 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 Updated the following alerts: • Azure Exposed Services Alert • Azure Firewall Deleted Alert • Potential Data Exfiltration Alert
3.1	February 9, 2024	Added the following alerts: • 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 Alert • Suspicious Process Executed Alert Added the following observations: • Suspicious Email Security Finding Observation • Suspicious Endpoint Security Finding Observation Renamed the Metaploit Executed Alert to Suspicious Process Executed Alert.

Copyright Information