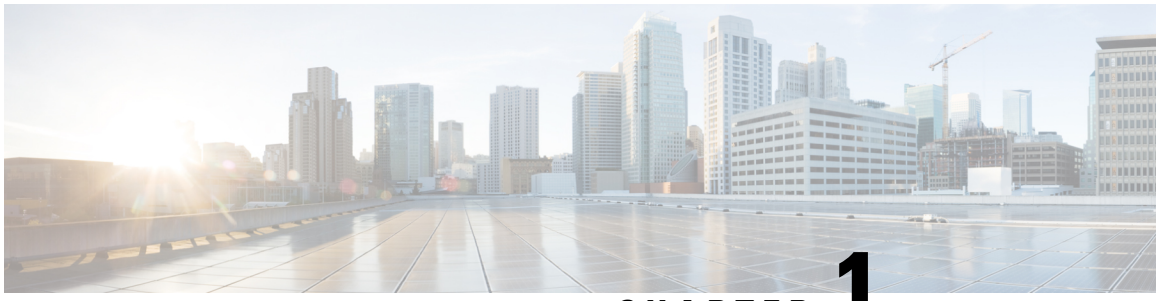
Cisco Secure Cloud Analytics Release Notes

First Published: 2021-01-12

Last Modified: 2023-03-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Cisco Secure Cloud Analytics New Features

New Features and Improvements

ANNOUNCEMENT

The Cisco Secure Cloud Analytics Release Notes are now available exclusively through the Cisco XDR Help Portal. Go here for both Cisco XDR and Cisco Secure Cloud Analytics Release Notes.

Note **Cisco Attack Surface Management**: Cisco Secure Cloud Insights is now Cisco Attack Surface Management. All related references within the Secure Cloud Analytics web portal have been updated. Visit Cisco Attack Surface Management, or refer to the Cisco Attack Surface Management (JupiterOne) Release Notes for more information.

MARCH 2024

Alerts and Observations Updates

Heartbeat Observation: This observation has been improved to detect suspicious activity from Azure infrastructure. Previously, Azure activity was considered trusted and excluded from Heartbeat observations.

FEBRUARY 2024

Announcements

Cisco Secure Email Threat Defense Integration: If you have transitioned to Cisco XDR, or are entitled with either the Cisco XDR Advantage or Premier licensing tier, the Cisco Secure Email Threat Defense offering is now available with Cisco XDR. Cisco Secure Email Threat Defense findings can generate and contribute to correlated incidents and workflows within Cisco XDR. Refer to Cisco XDR Third-Party Integrations for more information.

Cisco XDR Integration Listing/Deletion: If you have transitioned to Cisco XDR, you now have the option to list or delete the XDR organizations integrated within XDR Analytics. To view the XDR organizations, go to **Settings** >**Integrations** > **XDR**. Make sure you have the required XDR Analytics site manager permission required to list or delete a specific organization.

GCP Pub/Sub Flow Logs Collection Performance: We improved the process for retrieving and processing Google Cloud Platform (GCP) flows using Publishers (Pub) and Subscribers (Sub).

Alerts and Observations Updates

AWS AppStream Image Shared Alert: This new alert indicates that an Amazon Web Services (AWS) Appstream image was shared with another AWS account. This is a legitimate capability offered by AppStream, but Cisco Talos research has shown it also can be utilized for exfiltration or persistence.

Azure Anomalous RunCommand Alert: This new alert indicates that an Azure Virtual Machine has remotely executed a run command unexpectedly. Because this alert can signal an Advanced Persistent Threat (APT) 28 and/or APT 29, it should be investigated since it is atypical for your organization. You'll only see this alert for anomalies that have occurred within the last 7 days.

JANUARY 2024

Announcements

Cisco XDR Integration with Microsoft (MS) Defender for Endpoint: If you have transitioned to Cisco XDR, or are entitled with either the Cisco XDR Advantage or Premier licensing tier, the Cisco XDR Integration with MS Defender for Endpoint offering is now available. MS Defender findings can generate and contribute to correlated incidents and workflows within Cisco XDR. Refer to Cisco XDR Third-Party Integrations for more information.

Within Secure Cloud Analytics, MS Defender findings will be presented as suspicious endpoint alerts aligned to adversarial tactic categories. This includes the new Suspicious Endpoint Findings by MS Defender Proprietary Tactics alert.

For more details about endpoint-based alerts, go to **Settings** > **Alerts** and filter the **Telemetry** column by **Endpoint**.

Feature Updates

Email Management: Users with the **Site Manager** role now have the ability to enable and disable system email notification for all users. Go to **Settings** > **Account Management** > **User Management** and use the Email Notifications toggle to disable emails for a specific user account.

Meraki Tag: A new Meraki Netflow Collector profile tag has been added to properly account for Meraki devices which send Netflow on nonstandard ports. This new tag will contribute to the Netflow Exporter Role.

Session Traffic Pivot: When investigating Session Traffic records, you can now click **Event Viewer** to transition your query to the Event Viewer. Transitioning your query from Session Traffic to **Event Viewer** > **Session Traffic** allows you to search for records more than 7 days old.

Alerts and Observations Updates

- **Additional Endpoint-Based Detections**: If you have transitioned to Cisco XDR and are integrated with an endpoint solution, you'll see we've added three additional alerts that map to endpoint findings:
  - Suspicious Endpoint Findings by Reconnaissance
  - Suspicious Endpoint Findings by Resource Development
  - Suspicious Endpoint Findings without Tactics
- **Suspicious Endpoint Findings by MS Defender Proprietary Tactics Alert**: This new alert identifies behaviors detected on the endpoint that are mapped to MS Defender Proprietary tactics.
- **Suspicious Process Executed Alert**: The Metasploit Executed alert is now named Suspicious Process Executed alert.

DECEMBER 2023

Announcements

AWS CloudTrail Scaling: If integrated with AWS CloudTrail logs, you can now collect logs directly using AWS S3 storage. Using an S3 integration rather than an API integration will help to remediate the AWS API throttling experienced in large environments. Go to **Settings** > **Integrations** > **AWS** > **CloudTrail** to set up AWS CloudTrail log collection using S3.

Cisco XDR Transition: If looking to transition into Cisco XDR, you will now see references to Cisco XDR throughout your portal indicating integrations and workflows. To manage interconnectivity, go to **Integrations** > **Cisco XDR** and **Webhooks** > **Cisco XDR**. During your investigations, you can transition between SCA and Cisco XDR. From within a context menu, select **More with Cisco XDR** to switch to Cisco XDR. You can also go to **Alert** > **Post to Cisco XDR** or **Alert Priorities** > **Publish to XDR**.

Trusted External Networks: The Subnets VPN feature has been renamed **Trusted External Networks**. Configuring related subnets will allow your system to treat such trusted subnets as if they are part of your managed network.

NOVEMBER 2023

Announcements

Cisco XDR Integration with CloudStrike: If you have transitioned to Cisco XDR, or are entitled to with either the Cisco XDR Advantage or Premier licensing tier, you can now integrate the CrowdStrike Falcon Endpoint Detection and Response (EDR) offering with Cisco XDR. CloudStrike integration security events can generate and contribute to correlated incidents and workflows within Cisco XDR. Refer to Cisco XDR Third-Party Integrations for more information.

Alerts and Observations Updates

- **Heartbeat Connection Count Alert**: This existing alert has been modified to help eliminate noise typically found in service provider networks. The alert identifies devices having established new periodic connections with many remote devices. This behavior can indicate unauthorized P2P traffic or botnet activity.
- **Potential Database Exfiltration Alert**: This existing alert has passed through efficacy review and is now enabled by default. The alert evaluates traffic for statistically unusual amounts of data being transferred from a database server to a client. This behavior may indicate data exfiltration.
- **Suspicious Curl Behavior Alert**: When monitoring the Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM), this new alert looks for suspicious curl behavior that can indicate an exploitation of CVE-2023-38545. This alert is disabled by default.
- **Suspicious Endpoint Alerts**: Within Secure Cloud Analytics, CloudStrike integration security events will be presented as suspicious endpoint alerts aligned to adversarial tactic categories. For more details about these alerts, navigate to **Settings** > **Alerts** and filter the **Telemetry** column by **Endpoint**:
  - **Suspicious Endpoint Findings by Collection Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Collection MITRE tactic.
  - **Suspicious Endpoint Findings by Command and Control Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Command and Control MITRE tactic.
  - **Suspicious Endpoint Findings by Credential Access Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Credential Access MITRE tactic.

- **Suspicious Endpoint Findings by CrowdStrike Proprietary Tactics Alert**: Suspicious behaviors were detected on the endpoint that are not mapped to MITRE tactics.
- **Suspicious Endpoint Findings by Defense Evasion Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Defense Evasion MITRE tactic.
- **Suspicious Endpoint Findings by Discovery Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Discovery MITRE tactic.
- **Suspicious Endpoint Findings by Execution Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Execution MITRE tactic.
- **Suspicious Endpoint Findings by Exfiltration Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Exfiltration MITRE tactic.
- **Suspicious Endpoint Findings by Impact Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Impact MITRE tactic.
- **Suspicious Endpoint Findings by Initial Access Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Initial Access MITRE tactic.
- **Suspicious Endpoint Findings by Lateral Movement Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Lateral Movement MITRE tactic.
- **Suspicious Endpoint Findings by Persistence Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Persistence MITRE tactic.
- **Suspicious Endpoint Findings by Privilege Escalation Alert**: Suspicious behaviors were detected on the endpoint that are mapped to the Privilege Escalation MITRE tactic.
- **Suspicious Endpoint Security Finding Observation**: This is the observation related to all of the Suspicious Endpoint alerts listed above.

OCTOBER 2023

Announcements

Observation Type Filtering: You can now filter observation types based on the most relevant use cases. Go to **Monitor** > **Observations** > **Types**, then enter keywords to filter results in the Observation Name, Categories, or Telemetry columns. For example, to filter in the Observation Name column, you could use a keyword such as "endpoint."

User Time Preference: When investigating an alert, related observations will now reflect any new global time configuration you set up. To configure your default time preferences, go to **Settings** > **Account Management** > **Time**, then select the time zone you'd like to use.

Alerts and Observations Updates

Investigating ISE-Based Alerts: If you have the Cisco Identity Service Engine (ISE) integration and you're investigating alerts based on ISE, you can now pivot from the related user session summary to view additional ISE session details. For example, when viewing alert details for an alert such as New Internal Device, go to the **User Session** section to select the **View Sessions in Event Viewer** option in the **More Actions** column. A new browser tab opens displaying your session data filtered to include the related user and timeframe within the **Event Viewer** > **ISE** tab.

SEPTEMBER 2023

Announcements

Host Name from Cisco ISE: Once integrated with Cisco Identity Service Engine (ISE), ISE sessions will be used as an additional source of host name data. When a host name is present within the ISE user authentication session, that host name will be reflected throughout the UI.

Alerts and Observations Updates

Alert List Update: While triaging your list of alerts, you now have additional context to aid in your review. Go to to **Monitor** > **Alerts** to view and filter your list of alerts based on **Priority** or **MITRE ATT&CK Tactics**.

Suspicious Process Executed Alert: The existing endpoint-based Metasploit Executed alert has been renamed to better indicate suspicious process behavior. When monitoring the Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM), this alert currently signifies an endpoint has been discovered executing Metasploit. In the future, similarly suspicious process behavior will be included.

AUGUST 2023

Alerts and Observations Updates

- **AWS Domain Takeover Alert**: This existing alert has been adjusted to evaluate conditions more frequently. The activity identified can indicate attempts to take over a domain, which can then be used in future attacks or to hold the domain for ransom.
- **Azure Unusual Activity Alerts**: The following Azure activity-based alerts have been improved to alert only for activities that have been reported as successful:
    - Azure Firewall Deleted
    - Azure Key Vaults Deleted
    - Azure Network Security Group Deleted
    - Azure OAuth Bypass
    - Azure Resource Group Deleted
    - Azure Transfer Data To Cloud Account
- **GCP Cloud Function Invocation Spike Alert**: This exiting alert has been modified to aggregate instances of the same condition. The activity captured by this alert might indicate operational problems or a denial of service attack.

Feature Updates

Attack Chains Details Update: You can perform an in-depth investigation about attack chains by selecting the **Alert Breakdown** tab on the details page. You will find more details about the alerts along with an expandable list of related observations, particularly the observations that contributed to the alerting behavior.

NVM CMID Context: If you have transitioned to Cisco XDR and integrated with the Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM), you can view contextual endpoint information while investigating NVM records. For records returned using the **Investigate** > **Event Viewer** > **NVM Flow** tab, hover over the CMID value to view the host and device information for the related endpoint.

Post Attack Chains to Cisco XDR Update: If you have transitioned to Cisco XDR, attack chains that have been *closed* in SCA can now be promoted as Cisco XDR incidents. Click the **Post as Incident** button on the details page to promote an attack chain to Cisco XDR.

Menu and Page Updates

Dark Theme: The Secure Cloud Analytics (SCA) web portal allows you to toggle between a light view or dark view mode. Within the right section of your portal header, click the **Moon** icon to change the view.

Global Time Configuration: You can set the default time zone and time format for how you would like the time to display. Go to **Settings** > **Account Management** > **Time** to select the time format and preferred time zone.

JULY 2023

Announcements

Attack Chains: You can now use attack chains, which are built by correlating alerts that could be part of a larger threat. Attack chains reduce the time to investigate potential risks that could be early indications of an attack. We use extracted alert meta data to determine what the alerts have in common, which we refer to as common indicators. Common indicators include devices, IP addresses, host names, and user names.

We then follow the MITRE ATT&CK® framework to further identify the Tactics, Techniques, and Procedures (TTPs) to model the sequencing of actions and threat behaviors that can provide early indications of an intended attack. Depending on assessed threat levels, each attack chain is assigned a severity ranking based on the following:

- MITRE ATT&CK tactics identified
- subnet sensitivity of the devices involved
- alert priority (Low/Medium/High) of the alerts in the attack chain
- number of alerts in the attack chain

Also note that attack chains are ranked as Low/Medium/High, which allows you to prioritize which attack chains should be investigated immediately. Attack chains that are ranked High are automatically promoted as incidents to SecureX, if you have SecureX installed.

Go to **Monitor > Attack Chains** to access the attack chains that are found in your network. See the Attack Chain Guide at Cisco.com for more information.

Note When you transition to Cisco Extended Detection and Response (XDR), attack chains that are ranked High will be automatically promoted as incidents to XDR.

NVM Flow Tab: If you have transitioned to Cisco XDR, you can now access cloud data for the Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM) through the **NVM Flow** tab of Cisco Secure Cloud Analytics. You'll find the data is presented in a similar way as Event Viewer. NVM collects flow information from an endpoint whenever the AnyConnect VPN is connected back to your trusted network, which improves the visibility of remote devices. As there is an increase in users operating on unmanaged devices, administrators can have less visibility into what is going on inside and outside of the network. NVM provides visibility into network connected devices and user behaviors.

The advantages of using the **NVM Flow** tab include the following:

- storage of AnyConnect NVM fields
- visibility into end point fields such as OS version, OS name, Mac address, etc.
- existing policy violation rules to trigger from NVM flows

Alerts and Observations Updates

- **Alert List with Attack Chains**: The **Monitor > Alerts** list now includes related attack chains. When reviewing the list of alerts, any alert that's part of an attack chain displays in the **Attack Chain** column.
- **Alert Details with Attack Chains**: For any alerts included in an attack chain, the chain will be linked within the **Alert Types Details** section of the specific **Alert Details** page you are investigating.
- **Endpoint Based Alerts**: If you have transitioned to Cisco XDR and integrated with Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM), the following alerts are available:
  - **LDAP Connection from Suspicious Alert**: A device was detected running a non-standard LDAP process. This might indicate a credential theft attempt. This alert is disabled by default.
  - **Malicious Process Detected Alert**: A process running has a hash matching one in a list of known malicious hashes.
  - **Metasploit Executed Alert**: Execution of the offensive tool, Metasploit, has been detected in an endpoint through endpoint telemetry.
  - **Port 8888: Connections from Multiple Sources Alert**: 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.
  - **Potential Persistence Attempt Alert**: A 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.
  - **Potential System Process Impersonation Alert**: A process with a name that looks like a common process has been executed indicating a process impersonation.
  - **SMB|RDP: Connections to Multiple Destinations Alert**: The host has transferred files into multiple destination hosts using SMB and connected to those hosts using RDP.
  - **Suspicious Process Path Alert**: A process was executed on an endpoint from a directory that shouldn't have executables.
- **Invalid Mac Address Alert**: If you've integrated Cisco Identity Service Engine (ISE) with SCA, this new alert identifies the device has an Organizationally Unique Identifier (OUI) for an unregistered Mac address that's been detected using Cisco ISE telemetry. This indicates an attempt to bypass Mac Access Control (Mac filtering), conduct an Adversary-in-the-Middle technique, or impair other defensive capabilities. This alert is disabled by default.

Page and Menu Updates

Priorities Alerts/Watchlists Page Update: Go to **Settings > Alerts /Watchlists > Priorities** to access the **Priorities Alerts/Watchlists** page, which now includes a mapping of Alert Type to Observation Type. Use the **Observations Types** column to filter and view the dependencies.

Settings Menu Update: The portal account related menu names have been updated to clearly represent associated controls. **Settings > Account Management** (formerly **Account Settings**) contains pages related

to a specific user's individual account settings. For Site Admin users, **Settings > Account Management > User Management** (formerly **Account Management**) allows you to manage user access for your portal.

Other Updates

90-Day Report Extraction: When using **Investigate > Event Viewer**, you can now query any of your data types for results up to 90 days old. For more narrow queries, make sure to refine your search criteria and the time range for investigation.

Edit IP Scanner Rules: Existing IP Scanner rules can now be modified after initial creation. Go to **Settings > Alerts > Alerts/Watchlists > IP Scanner Rules** to edit an existing rule, then click the **Edit** (Pencil) icon for an IP Scanner rule you'd like to modify.

Session Connections Graph Device Context: An initial set of device information is now included when investigating IP connections using **Investigate > Session Traffic > Session Connections Graph**. To view the information in a context menu, click the IP address in the graph.

TCP Flag Reporting Update: When using **Investigate > Event Viewer** to investigate Session Traffic data, the **Manage Columns** menu provides access to the available TCP Flag information. The **TCP_Flags** and **TCP_Connected_Flags** columns show additional information about Session Traffic search results.

JUNE 2023

Alert and Observation Updates

- **AWS Logging Impairment Alert**: When monitoring **AWS CloudTrail** logs, this new alert indicates either **AWS CloudTrail** or **VPC Flow** logs have been deleted, or that collection has stopped. This could indicate an attempt of defense evasion within your environment.
- **Azure Firewall Deleted Alert**: This alert has been refined to focus on successfully deleted firewalls. The successful deletion of an Azure Firewall can indicate an attempt to impair network defenses.
- **New AWS Route53 Target Alert**: This CloudTrail alert has been refined to eliminate conditions that are not related to New Route53 associations. This alert indicates potential attempts to maliciously redirect traffic.
- **Additional Alerts Enabled By Default**: A number of additional alerts have passed through efficacy review and are now enabled by default. These are the updated alerts:
    - Azure Exposed Services Alert
    - Country Set Deviation Alert
    - Potential Data Exfiltration Alert
    - Static Device Deviation Alert
    - Unused AWS Resource Alert
- **Updated Trusted Company Alert/Observation Exceptions**: Secure Cloud Analytics maintains a list of companies considered, verified, and trusted as exclusions to specific alerts and observations. This exception list has been aligned as a global trusted company list and will modify behavior across the following alerts:
    - Country Set Deviation Alert
    - Exceptional Domain Controller Alert
    - Heartbeat Connection Count Alert

- ICMP Abuse Alert
- Persistent Remote Control Connections Alert
- Protocol Forgery Alert
- Protocol Violation (Geographic) Alert
- New External Connection Alert
- New Unusual DNS Resolver Alert
- New Long Session (Geographic) Alert
- Static Device Connection Deviation Alert
- Unusual External Server Alert
- Unusual File Extension from New External Server Alert

Custom Table Configuration: You can now adjust several configuration options for a selection of tables within your web portal. Use the **Cog** icon, which you'll find located at the bottom left of a table, to adjust the number of rows displayed, manage visible columns, or to abbreviate long byte counts into MB/GB.

Monthly Flows Report: The Monthly Flows Report, which is used for visibility into your daily effective flow counts, now includes a table to better visualize your data.

MAY 2023

Alert and Observation Updates

- **Azure Activity Log Watchlist Updates**: The Azure Activity Log Watchlist alerts have been improved by scrutinizing the log conditions that trigger the related detection. The updated alerts include:
  - Azure Firewall Deleted 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
- **Open Alert Count**: While navigating to the Alert list using the **Monitor** > **Alerts** page, you will no longer see a count of open alerts. To view the count of open alerts, hover over the **Bell** icon that displays at the top right of your screen.

APRIL 2023

Alert and Observation Updates

- **Drive By Download Observation**: This existing observation has been enhanced to focus more closely on connections with external hosts. The observation identifies any device that downloads a large amount of data from a remote host after an initial connection with the remote host. This may indicate an inadvertent download of a malicious payload.

AWS Visualization Reports Update: The AWS Visualization reports, which you can find by navigating to **Report** > **AWS Visualizations**, have been enhanced with usability improvements to provide a consistent look-and-feel. We have improved form input consistency and updated the relational graphs.

Observation Details Update: When investigating observations, you can now view all data elements captured by an observation. For any observation table within the **Alert Details** page or an observation page, such as the **Monitor** > **Observations** page, click any instance of an observation to expand the row for all contextual data.

Session Traffic Update: The **Investigate** > **Session Traffic** page, and the related sub-tabs, have been enhanced with usability improvements to provide a consistent look-and-feel. We have resolved existing bugs, improved form input consistency, and updated the relational graphs.

MARCH 2023

Alert and Observation Updates

- **AWS Domain Takeover Alert**: If you are monitoring **AWS CloudTrail** logs, this new alert signals that one of your AWS domains has been transferred to another account. This could indicate an attempt to hijack your domain or a violation of security policies.
- **AWS IAM User Takeover Alert**: If you are monitoring **AWS CloudTrail** logs, this new alert indicates a current 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.
- **AWS Snapshot Exfiltration Alert**: This existing **AWS CloudTrail** alert has been improved by filtering out additional common behaviors. This alert indicates an EC2 snapshot was modified to be accessible by another account. This can be a sign of an attacker attempting to exfiltrate data.
- **New Long Sessions (Geographic) Alert**: This existing alert indicates a device has established a long-lived connection with a host in your country watchlist. The alert has been improved by excluding additional trusted networks. It now allows for an established behavioral baseline of the internal device.

Copy Event Viewer Queries: During an investigation that takes you to Event Viewer reporting, you can now copy your current query, and all related active filters, for later use or for sharing with others on your team. When viewing or filtering results on the **Investigate** > **Event Viewer** page, use the **Copy** icon to copy the current date/time, inline, or query mode filters as a URL. You can then paste the URL directly into a browser.

First Direction Context: While analyzing Session Traffic records in the Event Viewer, use the **First Direction** field for context on the directionality of traffic at the time it was observed. Go to **Investigate** > **Event Viewer** > **Session Traffic**, and click the **Manage Columns** button to add the **First Direction Column** to your view.

Observation .CSV Exports: When downloading observation lists for offline investigation, the **.CSV** file now contains the IP or host name for the related internal device. Look for the **Source.name** within your file downloaded from an **Alert Details** page or any observation page such as **Monitor** > **Observations** > **Selected Observations**.

Top High Risk Countries Investigation: When reviewing the **Top High Risk Countries** map on the main dashboard, you can now continue your investigation to related observations for a country of interest. Click on a country highlighted with observations to be redirected to the Geographic Watchlist Observations for that selected country.

FEBRUARY 2023

Alert and Observation Updates

- **Abnormal ISE User Alert**: This existing alert has been improved by increasing the time window for related activity. If integrated with Cisco ISE, this alert indicates a user having authenticated on a device which is not typical and is associated with a different user. This may indicate compromised credentials or a rouge insider.
- **AWS ECS Credential Access Alert**: This existing **AWS CloudTrail** log-based alert has passed through efficacy review and is now enabled by default. This alert indicates an ECS Task Definition was registered with a container command to obtain credentials from the AWS Instance Metadata Service. This activity may indicate an attacker is attempting to obtain service credentials.
- **AWS IAM Anywhere Trust Anchor Created Alert**: This existing **AWS CloudTrail** log-based alert has passed through efficacy review and is now enabled by default. This alert indicates the creation of a new IAM Roles Anywhere trust anchor. The activity may be legitimate, but it could possibly indicate an adversary is attempting to establish persistent access to the account from outside AWS.
- **AWS Lambda Persistence Alert**: This existing **AWS CloudTrail** log-based alert has passed through efficacy review and is now enabled by default. This alert indicates a new AWS Lambda function has been created. This might indicate an attempt for persistence by adding a backdoor to newly created resources.
- **AWS Overlapping Subnet Alert**: The alert has been removed. This alert was used to indicate overlapping subnets in the same **AWS VPC**, which is no longer a possible configuration in AWS.
- **Drive by Download Observation**: This new observation indicates that a device has downloaded a large amount of data from a remote host after the external host's initial access. This may indicate the inadvertent download of a malicious payload.
- **Jailbroken Device Alert**: If integrated with Cisco ISE, you can now be alerted when Cisco ISE detects a device as "jailbroken." Such devices should be considered insecure as they can be more vulnerable to threats, which can increase organizational risk. This alert is disabled by default.
- **New AWS Lambda Invoke Permission Added Alert**: This existing **AWS CloudTrail** log-based alert has been improved by excluding additional valid AWS actions. This alert indicates the creation of a new invoke permission to take action from another AWS service, account, or organization. This behavior may indicate potential attempts to establish persistent access to the account from outside AWS.

Alert Priorities Download: The **Alert Priorities page** now includes an option to download valuable information about your Secure Cloud Analytics suite of detections. Go to **Settings** > **Alerts** > **Priorities** and click **CSV** to download a file containing the MITRE ATT&CK mappings, Dependent Observations, your current Alert configurations, and more. You can use this information for tasks such as integration planning and external review, or when creating playbooks.

ASN Description Context Update: Autonomous System Number (ASN) Descriptions are now available for all external IPs. This ASN Description reference uses a common Cisco dataset established by the Cisco Talos Threat Intelligence team. You may find this information during an investigation by using the left context menu for all external IP references. For a more complete classification of external IPs including ASN CIDR, Region, and DNS, continue to use the Cisco Umbrella Investigate integration found at **Settings** > **Integrations** > **Umbrella**.

Geographical Context Update: The geographical dataset used by Secure Cloud Analytics for mapping external IPs-to-country has been updated. This Geo IP reference now uses a common Cisco dataset established by the Cisco Talos Threat Intelligence team.

Session Details Update: If using Cisco Telemetry Broker as an on-premisis sensor, the display names for several **Session Details** fields within the **Investigate** > **Event Viewer** page have been improved or modified.

JANUARY 2023

Alert and Observation Updates:

- **Abnormal ISE User Alert**: If integrated with Cisco ISE, you can now be alerted when a user authenticates on a new device that is associated with a different user. This may indicate compromised credentials or a rouge insider. This alert is disabled by default.
- **Geographic Watchlist Observation Search**: 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 Obervations** within the **Observations** > **Selected Observation** page.
- **ISE Session Started Observation**: This new observation indicates that a new session was created. This observation requires integration with Cisco ISE.
- **ISE Suspicious Activity Observation**: This existing observation indicates when suspicious activity has been detected using Cisco ISE. This observation has been extended to look for devices reported by ISE as "jailbroken." Such devices should be considered insecure as they can be more vulnerable to threats.

AWS Integration Update: The **Settings** > **Integrations** >**AWS About** page has been updated with an improved performance and additional options to minimize your AWS S3 costs. If only storing VPC Flow Logs for integration with Secure Cloud Analytics, refer to the Amazon Web Services Integration Quick Start Guide for instructions about how to delete logs that are longer needed.

AWS Region Context: When investigating **AWS CloudTrail** based alerts, you can now find context of the specific AWS region for which the activity occurred. Within related **AWS CloudTrail** observations, or **Event Viewer** > **AWS CloudTrail** logs, you can expand a row of interest and look for the region exposed in the response element.

Additional Contextual Pivots: When investigating IP traffic using the **Investigate** > **by IP** page and external **IP Traffic** drill-downs, you can now more easily continue your investigation from summarized metrics down into related traffic. After identifying a row of data to drill into, use the **See Conversation in Event Viewer** pivot located in the table's last column. These contextual pivots will take you to **Event Viewer** > **Session Traffic** where you can view the corresponding results.

Alert Priorities Update: The **Settings** > **Alerts Priorities** and **Observation** > **Types** pages now indicate Cisco ISE as an additional telemetry type. Filter on this type to identify additional detections available when integrating. See **Settings** > **Integrations** > **ISE** for more information about integrating Cisco ISE with your portal.

Device Outline Update: The **Device Outline** > **Profiles** section had been optimized for improve performance of the **Alert Detail** pages and **Device** reporting. Use this section to get a 7-day summary of device activity matching known behaviors.

Open-Source Software: The open-source software provided by the Secure Cloud Analytics team has been relocated to a new repository. If you have links to any of our open-source tools, update your bookmarks to reflect https://github.com/obsrvbl-oss/.

Report Sidebar: In order to provide a consistent experience, a left navigation menu has been added to all reports within the **Report** menu section.

Visibility Assessment Update: The **Traffic to High-Risk Countries** section within **Report** > **Visibility Assessment** now includes additional detaills on how to use the information provided within the section. Use **Geographic Watchlist Observation Search** to continue your investigation.

DECEMBER 2022

Device Outline Update: The Device Outline panel found on both the **Alert Details** and **Device Report** pages has been updated to include Sensor and Exporter references. When the Sensor and Exporter data is available, it can be used to identify the portion of the network where the device is actively communicating.

Notifications Panel: You can now quickly view active System Warnings and What's New release notes from any page in your portal. Click the megaphone icon on the right side of your portal header to display the new Notifications panel.

Visibility Assessment Update: The Visibility Assessment report has been updated with additional functionality. Use the update descriptions for clarity on the insights being displayed. Then, continue your investigation using the incorporated device links. To access this report, go to **Report > Visibility Assessment**.

NOVEMBER 2022

Alert and Observation Updates:

- **AWS Repeated API Failures Alert**: If you are monitoring AWS CloudTrail logs, this new alert indicates when a user has performed multiple API calls, which in turn have resulted in failures due to insufficient privileges. This can indicate an adversary trying to obtain information about the environment, attempting enumeration, establishing persistence, or escalating privileges. This alert is disabled by default.
- **Azure Transfer Data to Cloud Account Alert**: This Azure Activity Log alert has been expanded to an additional Azure virtual hard drive exfiltration technique. In addition to snapshot exfiltration, we will now alert on URL-based exfiltration.
- **Emergent Profile Alert**: This existing alert has been improved by eliminating conditions where a client/server state can't be determined for specific profiles. This alert triggers when a device has traffic fitting a new profile and may indicate misconfiguration or compromise of the device.

Cisco Umbrella Investigations Update: If you have configured Umbrella Investigations, **Setting > Integrations > Umbrella**, your investigation pivot will now take you directly to the corresponding **Umbrella IP Results** page. The Cisco Umbrella Investigation can be found in the pivot menu of any external IP address. When integrated with SecureX, workflows for Cisco Umbrella and other tools can be added using Orchestrations through your SecureX portal.

Sensor Details Page: If you are using cloud configured on-prem sensors, you now have access to related telemetry stats. Go to **Settings > Sensors > Sensor Details** to see volume and general usage metrics for these sensors.

Sensor/Exporter Details: If available, Sensor and Exporter context is now included on the Device Outline for both the Alert Details and Device Report. Use this detail to provide context of where a given device was seen during your investigations.

Session Traffic Update: Session Traffic data now reflects Azure for Cloud Provider and Catalyst, a new sensor type, for on-prem sensor fields. If you have integrated these sensor types within your portal, this data can be found when making queries using **Investigate > Event Viewer > Session Traffic**.

Top High-Risk Countries Investigation: The Top High-Risk Countries widget on the Dashboard allows you to drill into country-specific Geographic Watchlist Observations. From the Dashboard, click anywhere on the inbound/outbound chart for a given country to continue your investigation.

OCTOBER 2022

Alert and Observation Updates:

- **AWS IAM Anywhere Trust Anchor Created Alert**: If you are monitoring AWS CloudTrail logs, this new alert will notify you of recently created IAM Roles Anywhere trust anchors. This may indicate an adversary attempting to establish persistent access to the account. This alert is disabled by default.
- **Heartbeat Observation**: This existing observation and the related alerts have been improved by adding Cisco (including openDNS) as a trusted company. This observation indicates devices that are maintaining a heartbeat with a remote host.
- **New AWS Lambda Invoke Permission Added Alert**: If you are monitoring AWS CloudTrail logs, this new alert indicates a new permission to invoke an AWS Lambda function from another AWS service, account, or organization has been added. This may indicate an attempt to establish persistent access to the account from outside AWS. This alert is disabled by default.
- **New High Throughput Connection Observation**: This existing observation has been improved by adding logic related to upload ratios and download ratios. This observation indicates a device has exchanged a large amount of inside-to-outside traffic with a new host.
- **Unusually Large EC2 Instance Alert**: If you are monitoring AWS CloudTrail logs, this new alert will notify you of the creation of unusually large EC2 instances. This may indicate an attacker has deployed an EC2 instance for resource hijacking. This alert is disabled by default.

Cloud Posture Watchlist Update: You can now manually trigger re-evaluation of GCP Frameworks by selecting the relevant **Re-Evaluate Cloud Posture** option on the **Settings > Alerts/Watchlists > Cloud Posture Watchlist** page.

Device Outline Update: The Device Outline panel found on both **Alert Details** and **Device Report** pages has been updated for improved usability. You may now use the **Copy** icon to copy specific device attributes, as indicated by the Notes icons next to certain elements. Both the Attendance and Observations sections have been relocated to better show they're overall device metrics (which are not specific to the current day).

Event Viewer Update: Sensor and Exporter detail columns are now included in the **Event Viewer > Session Traffic** table for Private Network Monitoring. These details provide context about where specific traffic is traversed on your network. You will need to click the **Manage Columns** icon to add these since they're not included as default table columns.

GCP Sensor Limit Status: If your GCP integration is beginning to hit GCP API limits, go to the **Settings > Sensors** page where you'll see an orange cloud icon for the particular GCP Sensor that's been impacted.

Integrations Page Update: The following **Settings > Integrations** pages have been updated for a more consistent experience:

- **Secure Cloud Insights**
- **Umbrella**
- **SecureX**

Site Navigation Update: The **Investigate** menu now includes a left-hand sub-navigation for quicker pivoting between pages. Note that we have not yet added this feature to the **Event Viewer** and **Session Traffic** pages.

Traffic Summary Page Update: Validations have been added to the **Report > Traffic Summary** page Date/Time selector, which clarifies that the report supports a max range of 8 days.

Alert Details Update: The **Alerts Details** page now includes specific time stamps that reflect various stages of alert activity. Within the Alert Rules Details section, you'll find timestamps for the following:

- **Detected At**

- **First Observation**
- **Latest Observation**

SEPTEMBER 2022

Alert and Observation Updates:

- **AWS EC2 Startup Script Modified Alert**: We've updated this alert to account for AWS reference changes, and we've added a check for stop instance events. These improvments quickly expose any atypical change behaviors that might indicate malicious activity. The alert is currently disabled by default for efficacy review.
- **Unusual EC2 Instance Observation**: A new CloudTrail-based observation indicating an unusually large EC2 instance has been deployed for a specific account.
- **AWS New User Action Observation**: This existing CloudTrail-based observation has been updated with a longer look-back period. The observation indicates CloudTrail has logged an AWS user doing an action for the first time. Resulting observations will now include **User** and **Remote IP** details for additional context.
- **MITRE ATT&CK Tactics and Techniques**: The following alert types have updated MITRE mappings:
  - **Discovery - Network Service Discovery**: New IP Scanner, New SNMP Sweep, NetBIOS Connection Spike, SMB Connection Spike, and LDAP Connection Spike.
  - **Reconnaissance - Active Scanning**: Outbound LDAP Connection Spike and Outbound SMB Connection Spike.

Alert Demos: We have the following new Alert demo videos available:

- AWS Detector Modified
- Azure OAuth Bypass
- New AWS Region
- Permissive AWS S3 Access Control List
- Permissive AWS Security Group Created

Public Cloud Integration Monitoring Update: When viewing the monitoring status of AWS or Azure, click the download CSV button if you'd like to have the data in a CSV file. To view a monitoring status, use the page specific to your integration service:

- **AWS - Settings > Integrations > AWS > VPC Flow Logs**
- **Azure - Settings > Integrations > Azure > Storage Access**

Sensor Page Update: You can now view the sensor IP for on-premises sensors on the **Settings > Sensor** page.

AUGUST 2022

Alert and Observation Updates:

- **Azure Oauth Bypass Alert**: This is an existing alert, which has passed through efficacy review and is now enabled by default. The alert indicates any action which is attempting to modify the kubeconfig file. If attackers were to get access to the kubeconfig file from a compromised client, they could use it to access the clusters.
- **ISE Session Started Observation**: If you have integrated Cisco Identity Services Engine (ISE), this new observation will look for newly established ISE user sessions.
- **Public IP Services Alert**: This alert has been removed. After improvements, this existing alert continued to report a low level of helpfulness as an actionable alert. The alert was designed to indicate when a device performed a DNS lookup of an IP service domain.

Dashboard Update: The Daily Traffic chart, which is located on the main dashboard, now distinguishes between internal and external traffic to allow for a better understanding of the traffic being monitored by Secure Cloud Analytics.

Device Report Update: The Device Report, which is accessible by pivoting from any device or device search, has been updated for increased context and usability. The report now includes additional metrics, highlights, and pivots. Also, you'll notice a new connections visualization is available within the Traffic Connections Visualization tab.

Encrypted Traffic Page Update: The **Investigate > Encrypted Traffic** page has been updated with a new Cisco look and feel.

Enhanced Network Telemetry: Cisco Telemetry Broker can now be used as a sensor for Secure Cloud Analytics. Once integrated, Cisco Telemetry Broker enables networking-based alerts. You can use your existing workflows to drill down through the **Investigate > Event Viewer** page to access the new Session Details tab, which provides additional forensic context for a more complete network record. For more information about Cisco Telemetry Broker and this integration, visit cs.co/telemetrybroker and refer to the Send On-Premises Flows to Secure Cloud Analytics Configuration Guide.

Entity Group Configuration Update: The workflow for creating Entity Groups has been streamlined for improved usability. You can now add context to your devices using the **Settings > Entity Group** page by creating and managing device groupings.

Observation Details Update: When investigating observations that provide additional context contained in JSON blobs, you'll now see an arrow icon located on the left side of the table. You can click the arrow icon to expand the observation and see the JSON context in a readable format. Expandable views can be found on alert detail pages and in observation specific reporting. To close a view you've expanded, click the down arrow icon.

Public Cloud Integration Monitoring Update: You can now use table-filtering to gain a more insightful view into your monitoring status for Azure, AWS, or GCP. To view a monitoring status, use the page specific to your integration service:

- **AWS - Settings > Integrations > AWS > VPC Flow Logs**
- **Azure - Settings > Integrations > Azure > Storage Access**
- **GCP - Settings > Integrations > GCP > Credentials**

Sensor Offline Notification Update: The threshold to trigger Sensor Offline notifications has been shortened from 8 hours to 4 hours of inactivity.

Sensor Page Update: You can now filter the **Settings > Sensor** page by sensor status to view specific sensors.

JULY 2022

Alert and Observation Updates:

- **New Remote Access Alert**: This is an existing alert that has been improved by expanding the look-back period. The alert indicates when a device has been accessed from a remote host for the first time in recent history. This may indicate that the device is compromised.
- **SMB Connection Outlier Alert**: This is an existing alert that has passed through efficacy review and is now enabled by default. The alert occurs when a device has exchanged an unusually large amount of SMB traffic with an unusually large set of SMB Peers. This may indicate reconnaissance activity.
- **Suspicious DNS over HTTPS Activity Alert**: This is an existing alert that has passed through efficacy review and is now enabled by default. The alert triggers when an internal server has been seen exchanging traffic with a known DNS over HTTPS server. This may indicate an attempt to evade DNS-based security.
- **Unusual External Server Alert**: This is an existing alert that has been improved by focusing the time period of related connections made to external servers. The alert indicates a device has communicated repeatedly with a new external server. This may indicate the presence of malware.

Alert Demos: We have two new Alert demo videos:

- Permissive AWS Security Group Created Alerts
- New Internal Device Alerts

Publish Alert Types to SecureX: When integrating with SecureX, use the **Alerts > Priorities** page to configure which alert types you would like automatically published as incidents to the SecureX Incident Manager. The **Talos Intelligence Watchlist Hits Alert** type is enabled by default. For more information, refer to the SecureX Integration Guide.

Role Page Update: The **Investigate > Active Roles** page is now the **Roles** page. This page includes additional information about how Active Roles are determined, a list of Inactive Roles types, and a description for each Role.

Secure Cloud Analytics Public IPs API: If you need to restrict access to your environment dynamically, you can now use the API endpoint `/api/v3/service/public-ips/` to access the list of public IPs required for Secure Cloud Analytics integrations.

SecureX Incident Manager Webhooks Update: You can now manage multiple SecureX Webhook integrations using the **Settings > Webhooks/Services > SecureX Incident Manager** page.

Sensor Page Update: You can now filter the **Settings > Sensors** page by Sensor Name and Sensor Type.

Subnet Sensitivity Updates: Subnet Sensitivity no longer includes an option of `None`. Use a setting of `Low`, `Medium`, or `High` to indicate device context and relative alert severity for each of your subnets.

JUNE 2022

Alert and Observation Updates:

- **Country Set Deviation Alert**: This existing alert's description has been modified to clarify it does not require configuration of the Country Watchlist. This behavioral alert indicates when a device is significantly deviating from any of the set of countries it usually communicates with. This may indicate a device is compromised.
- **S3 Bucket Lifecycle Configured Alert**: This existing alert has been improved by extending beyond noncurrent versions to all object types. The alert indicates a new S3 Bucket Lifecycle configuration has

been created that schedules the simultaneous permanent deletion of all files in the bucket. This may indicate a data destruction attempt.

Active Roles Page Update: The **Investigate > Active Roles** page now includes additional information describing how Active Roles are determined, as well as a description for each role type displayed.

Event Viewer Updates: The link for Event Viewer has been moved to the top of the Investigate menu in place of the legacy Session Traffic page link. Additionally, the Session Traffic table within Event Viewer now includes the following columns related to the cloud environment where the traffic was generated:

- Cloud_Account
- Cloud_Region
- Cloud_VPC

Use this data to pinpoint areas of concern or remediation when investigating an alert. To see the new columns, go to **Investigate > Event Viewer > Session Traffic**.

Mitel VoIP Client Role: A new role has been added identifying Mitel devices being used to make VoIP calls.

Subnet Sensitivity Updates: As an improvement to alert efficacy, the default sensitivity of subnets has been lowered to Normal/Medium. Additionally, the Subnet Sensitivity Matrix has been updated to clarify subnet sensitivity pertains to device specific alerts only. The configured sensitivity does not affect network type alerts. For more information on Subnet Sensitivity and configuration, go to **Settings > Subnets**.

Updated Trusted Company List: The trusted external IP logic now includes Cisco owned IP space and Mitel Cloud services. This excludes select alerts and observations, such as Unusual External Server and Outbound Traffic Spike, from triggering when interacting with these spaces. To include additional trusted 3rd parties, go to **Settings > Subnets > Virtual Private Networks** and configure additional VPN Subnets.

MAY 2022

Alert and Observation Updates:

- **Country Set Deviation Alert**: This existing alert has been adjusted to reduce observation to alert volumes for similar occurrences. The alert indicates when a device is seen having significantly deviated from the set of countries it usually communicates with. This may indicate a device is compromised.
- **NetBIOS Connection Spike Alert**: This existing alert has been adjusted to reduce the frequency of additional alerts for the same scanner. This alert indicates when a device has attempted to contact a large number of hosts using NetBIOS, which may be an indication of malware or abuse.
- **New File Extension Observation**: This existing observation has been improved to look for only suspicious extensions.
- **New SNMP Sweep Alert**: This existing alert has been improved by adjusting related thresholding for a higher efficacy. The alert indicates when a device has attempted to reach a large number of hosts using SNMP. This may be an indication of malware or abuse.
- **Public IP Services Alert**: This existing alert has been adjusted to reduce the number of additional alerts for the same source. The alert requires passive DNS data via your sensor or Security Analytics and Logging (SaaS) integration and indicates a device has performed a DNS lookup of an IP service domain.
- **Suspicious User Agent Alert**: If you have Security Analytics and Logging (SaaS) enabled, we will now alert for devices seen communicating with a device using a suspicious user agent string. The detection may indicate malware (e.g., Log4J exploitation) or abuse. This alert is disabled by default.

Nessus Scanner Role: Added a new role identifying Nessus Scanners.

Carbonite Profile Tag: Updated and expanded the existing Mozy profile tag to reflect Carbonite and additional matching behavior.

Alert Priorities Page:

- Includes additional alerts tagged with corresponding telemetry requirements.
- The **Reset All to Defaults** button now resets both Priority and Enabled states to their default settings.

Sensors Page:

- The **Settings > Sensors** page now reflects a sensor's hostname and status timestamps for each telemetry configured per sensor.
- GCP sensors will now notify by email when they go offline.

Metering Report: The **Report > Metering Reports** page now includes a trend line for EMF and the ability to filter the page by month and year. You can use this functionality to review historical endpoint and EMF trends.

Azure Integration Workflow: Updated the **Settings > Integrations > Azure > About** page to reflect updated language and steps required for Azure integration. This does not impact existing integrations. New integrations should take note of Azure's required application expiration requirement and registering the Insights Provider before enabling NSG Flow Logs.

Secure Cloud Analytics Public IPs: If you need to restrict access to your environments, you can access the list of public IPs required for Secure Cloud Analytics integrations. The list of IPs can be found on the following pages:

- AWS About (**Settings > Integrations > AWS > About**)
- Azure About (**Settings > Integrations > Azure > About**)
- GCP About (**Settings > Integrations > GCP > About**)
- Sensor Installation (**? (Help) icon > On-Prem Sensor Install**)

Entity Groups API: A REST API for Entity Groups is now available. Use Entity Groups to layer additional business context onto your devices. To configure and manage Entity Groups through the web portal, go to **Settings > Entity Groups**, or use the API `https://<portal name>/api/v3/entitygroups/entitygroups/`.

APRIL 2022

Alert and Observation Updates:

- **Azure Function Invocation Spike Alert**: This existing alert has passed through efficacy review and is now enabled by default. The alert indicates when the number of Azure function invocations is abnormally high. This may indicate operational problems or a denial of service attack.
- **LDAP Connection Spike Alert**: This existing alert has passed through efficacy review and is now enabled by default. The alert indicates when a device attempted to contact an unusually large number of internal LDAP servers. This may indicate malware or abuse.
- **Outbound LDAP Spike Alert**: This existing alert has passed through efficacy review and is now enabled by default. The alert indicates when a device is communicating with a large number of external hosts using an LDAP port. This may indicate a possible infected host or an internally-initiated port scan.

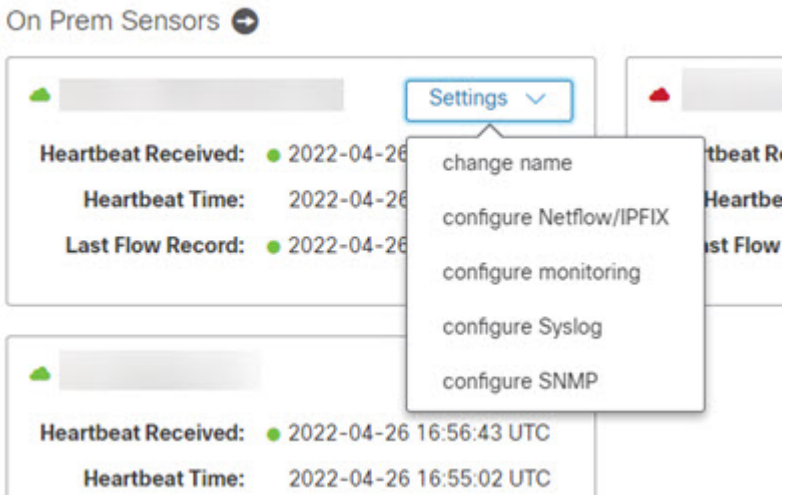
- **Unusual File Extension from New External Server Alert**: Added a new alert identifying when a new external server exchanges a new file extension with an internal device. This may indicate malware attempting to communicate with its command-and-control center. This alert requires both firewall and Netflow data. This alert is disabled by default.
- **Repeated Umbrella Sinkhole Communications Alert**: Added a new alert identifying when a device has established periodic connections with a known Cisco Umbrella sinkhole. This may indicate that the device is compromised. This alert is disabled by default.
- **Role Violation Alert**: This existing alert has passed through efficacy review and is now enabled by default. The alert notifies when a device identified with a particular role (e.g., Windows Workstation) was observed acting in a new role (e.g., SSH server). This alert may indicate the device is compromised.
- **Suspicious DNS over HTTPS Activity Alert**: Added a new alert for when an internal server was seen exchanging traffic with a DNS server over HTTPS. This may indicate an attempt to evade DNS-based security. This alert is disabled by default.
- **Umbrella Sinkhole Hit Observation**: Added a new observation identifying when a device communicates with a known Cisco Umbrella sinkhole. This observation is an indication that the device attempted to talk to a known bad domain.
- **Unusual File Extension from New External Server Alert**: Added a new alert identifying when a new external server exchanges a new file extension with an internal device. This may indicate malware attempting to communicate with its command-and-control center. This alert requires both firewall and Netflow data. This alert is disabled by default.

Updated Page Look and Feel: We updated the following pages under the Investigate menu to improve usability:

- External Services
- By IP Address
- User Activity

Updated Sensors Page: We updated the Sensors page to improve usability. You can now:

- View status time stamps for each sensor.
- Access Service Key and Service Hostname.
- Enable interface monitoring via SPAN/tap. To enable, go to **Settings > Sensors > Settings > Configure Monitoring**.



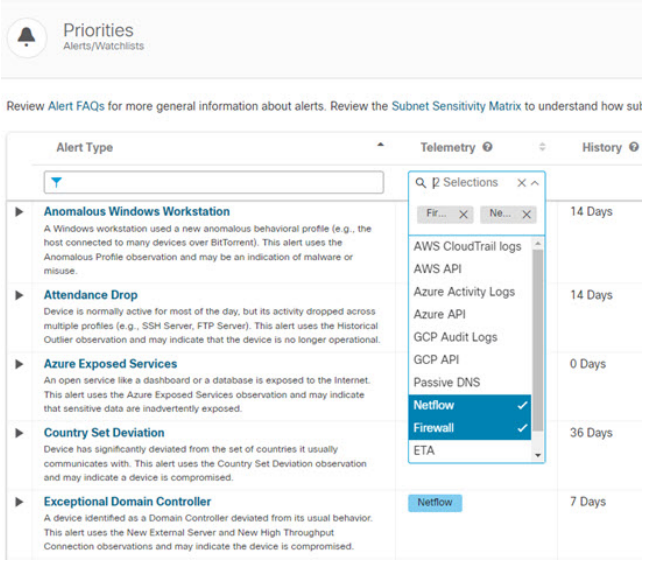
- Configure the sensor's public IP. To configure, go to **Settings** > **Sensors** > **Public IP**.
- Configure Netflow/IPFIX Probes for each on prem sensor. To configure, go to **Settings** > **Sensors** > **Selected Netflow/IPFIX**.

MARCH 2022

Alert and Observation Updates:

- **Azure Function Invocation Spike Alert**: Added a new alert for when the number of Azure function invocations is abnormally high. This may indicate operational problems or a denial of service attack. This alert is disabled by default.
- **Azure Transfer Data to Cloud Account Alert**: This existing alert has passed through efficacy review and is now enabled by default. The alert notifies when a publicly accessible snapshot has been created for a virtual machine. This may indicate an attempt to exfiltrate data.
- **ICMP Abuse Alert**: Added a new alert for identifying devices sending unusually large ICMP packets to a new external server. This may indicate an attacker is using the ICMP protocol as a covert communications channel to exfiltrate data. This alert is disabled by default.
- **Inbound Port Scanner Alert**: This existing network type alert will now ignore devices you have defined within low priority subnets. Subnet sensitivity can be adjusted by navigating to **Settings** > **Subnets**.
- **New File Extension Observation**: Added a new observation identifying when a device has exchanged a new file extension with an external IP. This behavior paired with other factors may indicate the presence of malware. This observation requires firewall data.
- **Suspected Remote Access Tool Heartbeat Alert**: Improved the ability to identify RevengeRAT signatures.
- **Talos Suspicious Activity Observation**: The existing observation has been updated to identify a broader range of remote access tools.
- **Unusual Packet Size Observation**: The existing observation has been expanded to identify unusual packet sizes in echo packets.

Alert Priorities Filtering by Telemetries: You can now filter the Alert Priorities page by one or more telemetry types. Filter this view to understand which alert types require which type of telemetry, as well as which additional alerts you may gain by integrating telemetry types into Secure Cloud Analytics.



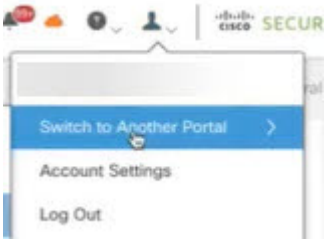
Azure Integration Update: The Azure `Network Contributor` role assignment is no longer required. This role has been removed from the Azure Integrations page and can safely be removed from your Azure instance.

Azure Log Analytics Webhook: You can now configure Azure Log Analytics as a supported webhook target, which can be used to post alerts into Azure and route them to Azure Sentinel. Go to **Settings > Webhooks/Services > Azure Log Analytics** for more information.

GCP Monitor Status: You can now use the GCP Credentials page to monitor the status of your GCP integration per projects and regions. Monitoring details can be found by navigating to **Settings > Integrations > GCP > Credentials**.

ISE Integration Guide: Improvements have been made to the ISE setup instructions. These instructions can be found at **Settings > Integrations > ISE**.

Portal Selection Menu: If you have access to more than one portal/tenant, you can now change your view without logging out. While logged in, click the user icon, and go to **Switch to Another Portal** to select the portal you wish to view.



Updated Sensor Package: A new version of the NetSA package is available for the sensor to support more Palo Alto firewalls. You can either update the sensor using the instructions in the Private Network Monitoring Advanced Configuration Guide or update the package separately using the following steps:

1. Enter the following commands:

```
curl -o netsa-pkg.deb --location
https://assets-production.obsrvbl.com/ona-packages/netsa/v0.1.27/netsa-pkg.deb
sudo apt-get install libsnappy1v5
sudo systemctl stop obsrvbl-ona.service
sudo dpkg -i netsa-pkg.deb
sudo systemctl start obsrvbl-ona.service
```

2. Wait a few minutes for the ona-service to start up.
3. Log into the portal web UI.
4. Select **Settings > Sensors**. Verify the sensor appears in the list.

FEBRUARY 2022

Alert and Observation Updates:

- **Anomalous User Agent Observation**: Added a new observation for when a device has an anomalous user agent string.
- **LDAP Connection Spike Alert**: Added a new alert for when a device attempts to contact an unusually large number of internal LDAP servers. This alert is disabled by default.
- **Outbound LDAP Connection Spike Alert**: Added a new alert for when a device is communicating with a large number of external hosts using an LDAP port. This alert is disabled by default.
- Mapped 39 additional Alerts to MITRE ATT&CK Tactics and Techniques. This provides additional context within an Alert's Details and the **Settings > Alerts > Priorities** page.

Bulk Delete IP Scanner Rules: You can now bulk delete IP Scanner Rules from the IP Scanner Allow List using the API endpoint `ip_scanner_allowlist/bulk/` and specifying specific Rule IDs or all.

New Roles: If you have Security Analytics and Logging (SaaS) enabled, Linux Device and Sony PlayStation are now identified in the Roles page.

New Profile Tags:

- **ShoreTel Profile Tag**: Added a new profile tag for identifying ShoreTel VoIP telephony appliances.
- **TikTok Profile Tag**: Added a new profile tag for identifying devices communicating with TikTok.

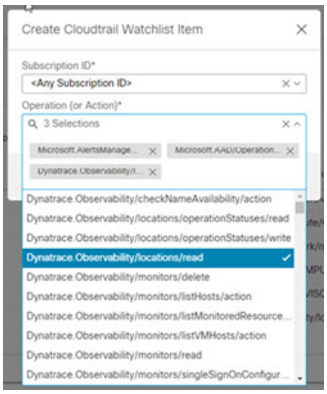
SecureX Integration Enhancment: The process to integrate your instance of SecureX is now more streamlined. For more information, refer to the SecureX Integration Guide.

JANUARY 2022

Improved AWS ECS Integration: Additional permissions added for AWS Integrations to improve modeling of containerized environments. You will need to update your IAM Role Policy Document(s) to add the new permissions requested. Go to **Settings > Integrations > AWS > About** for more information.

Azure Activity Log Watchlist Improvements: The Create Cloudtrail Watchlist Item menu now includes:

- a list of suggested Operation/Actions.
- the ability to create multiple Operations/Actions at the same time.



Alert Updates: Improved `Country Set Deviation` alert to prevent false positives for AWS Elastic Load Balancers.

DECEMBER 2021

Alert Updates: Improved the behavior and updated description of `Suspected Port Abuse (External)`.

Refreshed the set of peer IPs used by the `GitHub` profile tag.

NOVEMBER 2021

We have rebranded Cisco Stealthwatch Cloud products to Cisco Secure Cloud Analytics.

Integration with Cisco Secure Cloud Insights:

- Use the Secure Cloud Insights API to query your Secure Cloud Insights database for IP address and device information.
- In your portal, go to **Settings** > **Integrations** > **Cisco Secure Cloud Insights** for details.

AWS CloudTrail Watchlist Drop Down Selector: Improved selection across multiple accounts.

Alert updates: `Meterpreter Command and Control Success` published.

OCTOBER 2021

Enhancement to Detections in Kubernetes by monitoring by Controller for logical visiblity to application to service as a whole.

AWS VPC Cloud Coverage Report for Visibility to VPC monitoring status and gaps in coverage.

Updated searching and filtering of Scanner Rules for easier configuration.

Device Outline panel: Alert details page now shows additional device context in a separate panel.

Alert updates: Potential Data Exfiltration improved to prevent false positives for DNS and other trusted services.

SEPTEMBER 2021

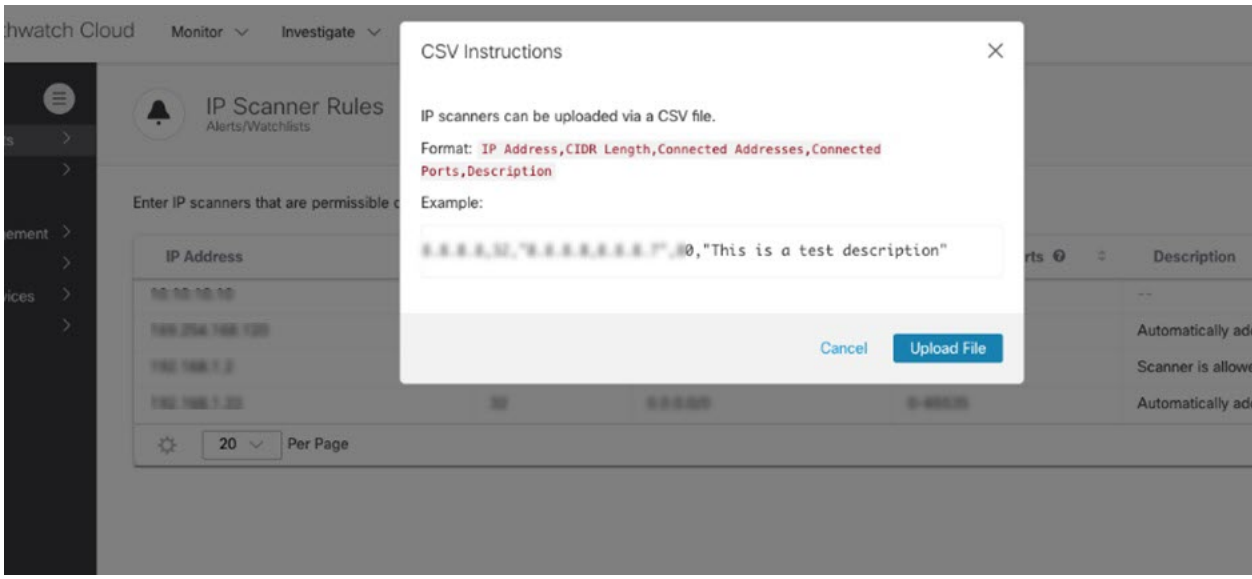
Customize Email Frequency by Alert Priority: Adjust email frequency based on the alert's priority by navigating to **Settings** > **Account Management** > **Email** and using the **Alert Updates** section.

AWS VPC Monitoring Status: We now display a table of all VPCs retrieved from AWS credentials provided and show their monitoring status. Go to **Account Settings > Integrations > AWS > VPC Flow Logs**.

AWS EC2 Startup Script Modified alert: An AWS EC2 instance startup script was modified. This alert uses the AWS CloudTrail Event observation and may indicate an attempt by a malicious actor to establish persistence or execute malicious code.

Worm Propagation alert: Previously scanned device started scanning the local IP network. This alert uses the Worm Propagation observation and may indicate that a worm is propagating itself inside the network. The alert is undergoing further research and refinement and currently disabled by default.

Added bulk import of IP scanners for configuring scanner rules.

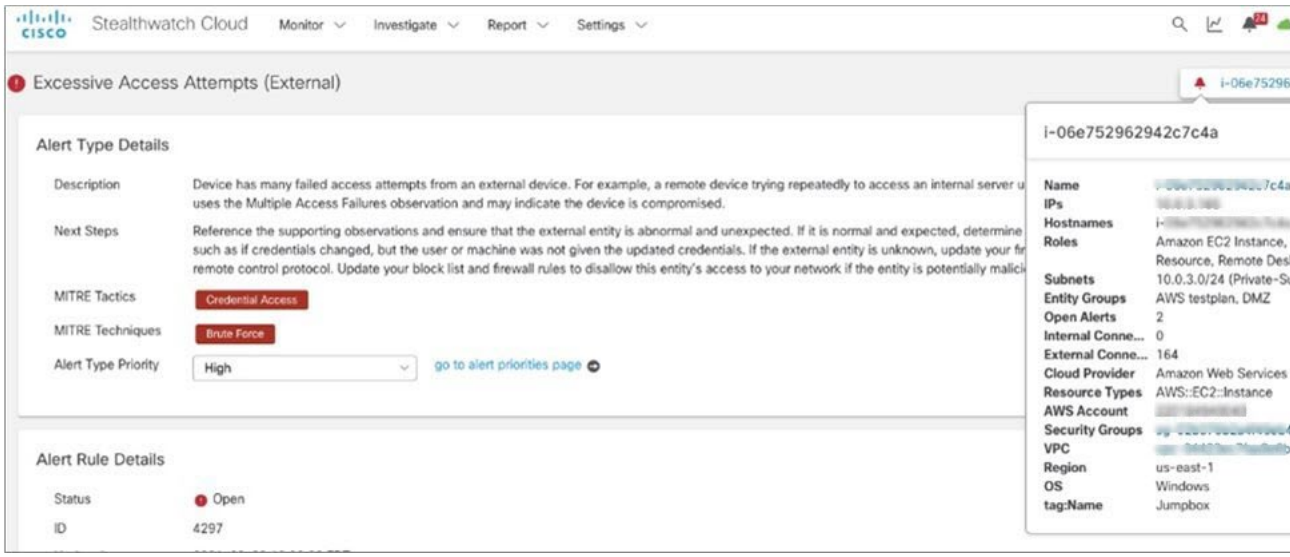


Added Device Outline section to alert details pages, making additional device context readily available during alert triage.

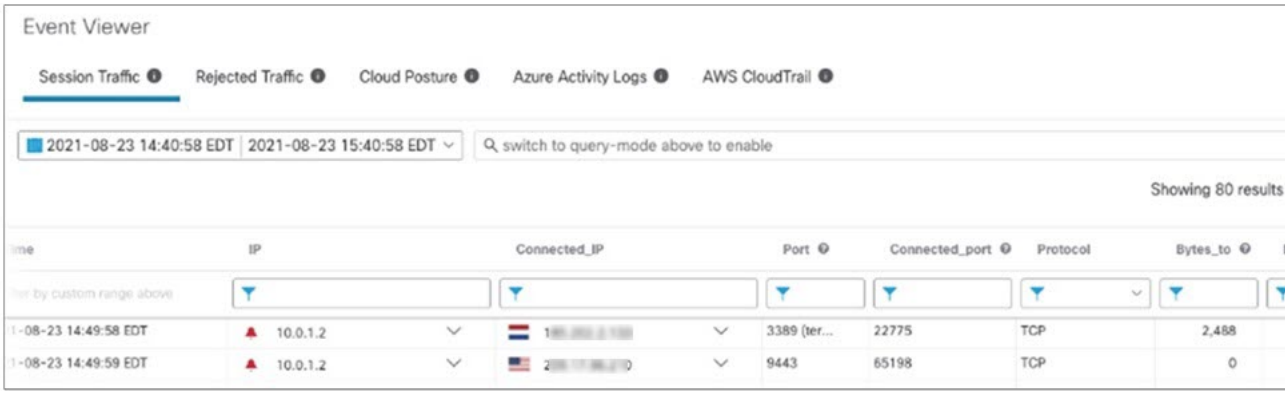
AUGUST 2021

Added ability to manage multiple API keys for key rotations.

AWS links added to Details for Device.



Added option to download all fields in the Event Viewer.



New Alerts (off by default):

- S3 Bucket Lifecycle Configured Alert added.

  A new S3 Bucket Lifecycle configuration has been created that schedules the simultaneous permanent deletion of all files in the bucket. This alert uses the AWS CloudTrail Event observation and may indicate a data destruction attempt.

- Meterpreter Command and Control Failure Alert added.

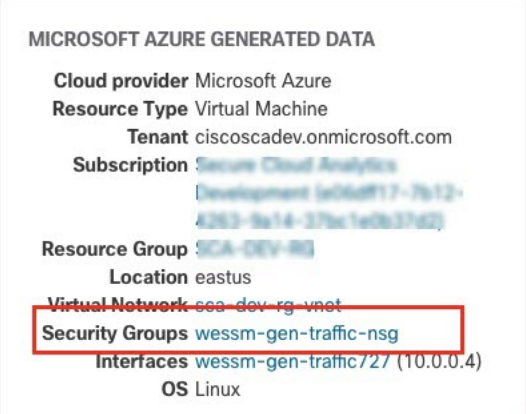
  Device has tried to establish new periodic connections that appear to be part of a Meterpreter Command and Control channel. This alert uses the Heartbeat observation and may indicate the device is compromised.

- Meterpreter Command and Control Success Alert added.

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

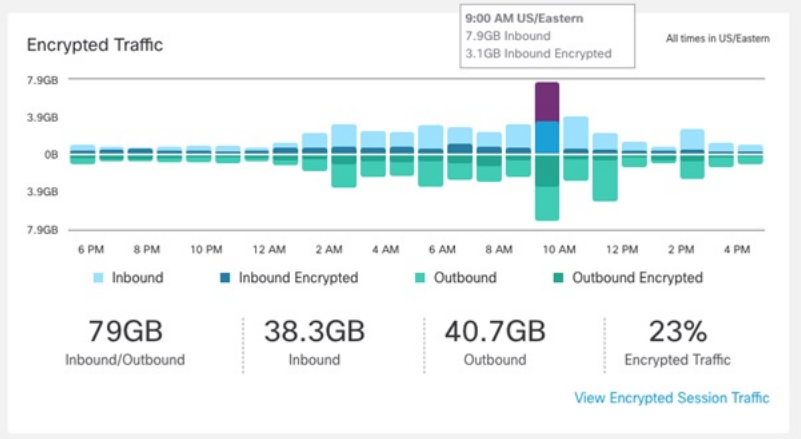
- AWS Lambda Persistence Alert added.

Azure device context update: Added Security Group on Alert List hover and Alert Details pages.

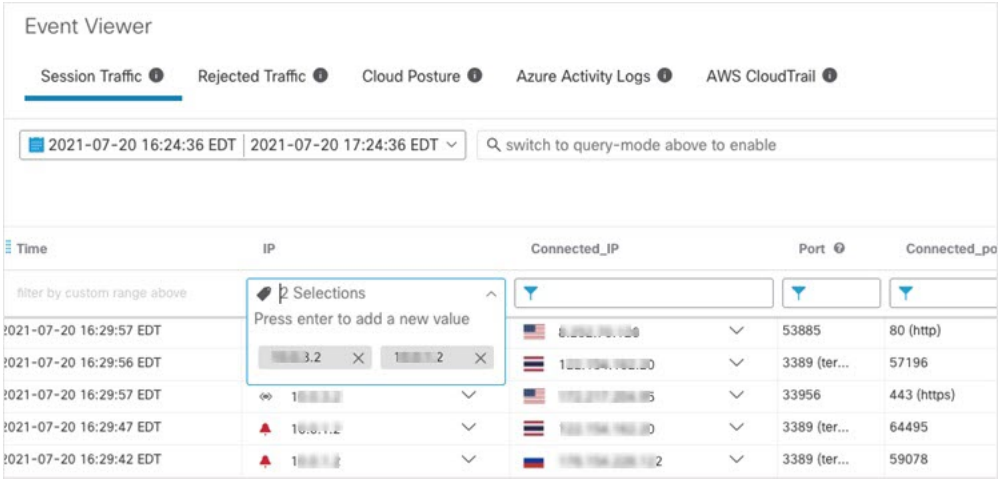


JULY 2021

Encrypted Traffic widget ability to click bar graph that links to filtered session traffic.



Added multiselect entry or bulk copy and paste insertion of IP and port in the Event Viewer.

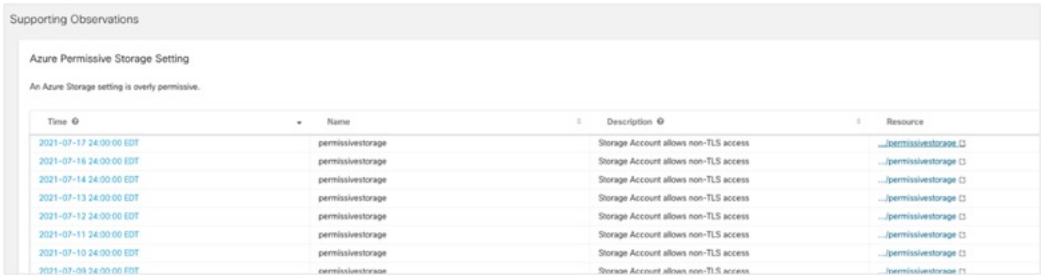


Added telemetry source to Observation types.

Persistent column resizing in the Event Viewer.

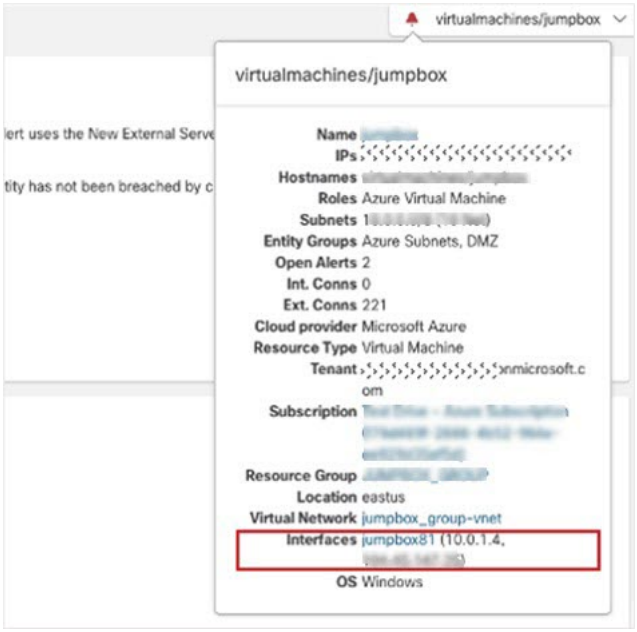
Supporting network session information for observations available in API.

Azure-based observations provide links to Azure portal for impacted resources.

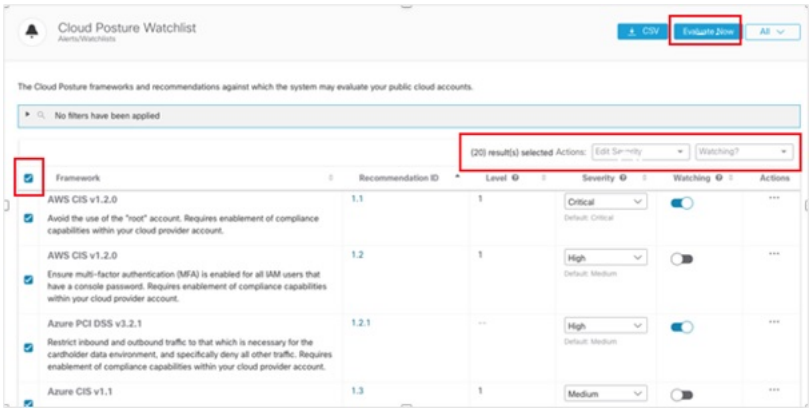


JUNE 2021

Azure network interfaces now available in Device Info.



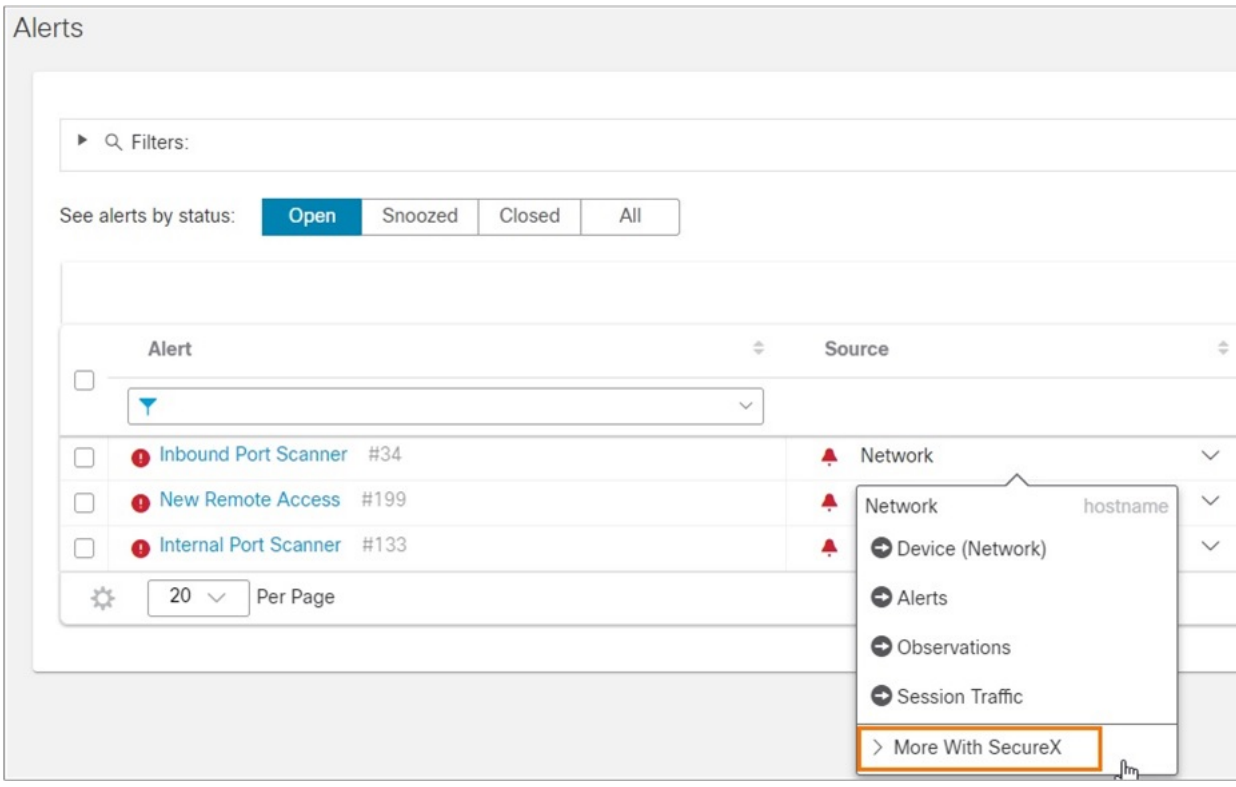
Cloud Posture on-demand watchlist checks and bulk watchlist editing.



In SecureX threat response, sightings from Secure Cloud Analytics now visible for external IP, including alerts and observations.

Updates to **Monitor > Alerts**:

- Ability to filter on Not Assigned.
- Source pivot menu now has a SecureX link.



MAY 2021

ISE Integration

- Easily configure ISE to send telemetry to Secure Cloud Analytics.
- View, query, and report on data in Event Viewer.
- Additional context from ISE telemetry will be made available in alert workflows (final release date pending beta results).

Azure

- Setup scripts for automated deployment are now available to site managers.
- Azure-related alerts or devices now provide direct links to the device in your Azure account.

Device Context

- Additional device context provided in the alert workflow, including the name of the virtual network, subscription name, and ID (for public cloud accounts).

DNA Center Integration

- Starting with DNA Center 2.2.2.0, a user can configure their catalyst devices to send flow telemetry directly to Secure Cloud Analytics at scale, without needed to configure manually at the switch command line.

APRIL 2021

Direct to cloud integration with Cisco Catalyst 9k series.

Sensor available as container on the switching platforms to enable easy configuration of telemetry from device to cloud without additional deployment or installation of sensors.

MARCH 2021

SecureX Enhancements:

- Incident Manager integration – publishes alerts to SecureX for deeper investigation.
- Five new orchestration workflows.

Device information now includes unique internal and external peers.

FEBRUARY 2021

Enhancements to alerts and observation pages:

- New look and feel.
- Additional context about related cloud accounts.
- Includes updated workflows for taking bulk actions with new filters available.

Cloud Data Store available in Tokyo region.

AWS CloudTrail and Azure activity logs now available in the Event Viewer.

JANUARY 2021

Cloud Posture Management

Secure Cloud Analytics now supports evaluating your AWS or Azure deployment against additional security and compliance best practices. Use the Cloud Posture tab in the Event Viewer for resulting recommendation verdicts related to your cloud assets. If you enable native compliance checking within AWS or Azure, Cloud Posture may display additional recommendations and recommendation verdicts from the cloud provider.

If you already integrated Secure Cloud Analytics with AWS, you must update your IAM policy permissions in AWS to enable the Cloud Posture report for AWS. The AWS About page in Secure Cloud Analytics lists the required permissions in the JSON object that starts with `"Sid": "CloudCompliance"`. If you do not want to grant these additional permissions, you will not be able to use the Cloud Posture Report.

If you already integrated Secure Cloud Analytics with Azure, you do not need to update permissions to enable the Cloud Posture report for Azure.

OCTOBER 2020

Entity Groups

Secure Cloud Analytics now supports Entity Groups, logical groups of entities that you can define, to better track subsets of entities within or outside your organization. You can define Entity Groups based on user-defined subnets within Secure Cloud Analytics, and CIDR blocks.

You can now configure the Internal Connection Watchlist to reference an Entity Group, in addition to adding CIDR blocks. Internal Connection Watchlist entries can either generate or not generate an alert when traffic between internal entities is detected, allowing you to better monitor communications within your network.

Alert Priorities

The Alert Priorities Settings page is updated and reorganized for more intuitive navigation.

This page now reflects mappings between alert types and any related MITRE ATT&CK tactics and techniques, allowing you to better understand alert types and assign an appropriate priority, based on your organization's needs.

Updated Site Navigation

The Secure Cloud Analytics high-level portal navigation is updated, based on user feedback, to better address common workflows. The menu options are:

- **Monitor** - Review the state of your network, and view the observations and alerts logged by Secure Cloud Analytics. Includes **Dashboard**, **Alerts**, and **Observations**.
- **Investigate** - Gather context and information on the state of your network, and investigate the possible root causes of alerts. Includes **Session Traffic**, **External Services**, **Device**, **IP or Domain**, **Encrypted Traffic**, **User Activity**, and **Active Roles**.
- **Report** - Generate reports that provide at-a-glance information about your network. Includes **AWS Visualizations**, **Metering Report**, **Monthly Flows Report**, **Subnet Report**, **Traffic Summary**, and **Visibility Assessment**.
- **Settings** - Configure and customize your Secure Cloud Analytics portal. Includes **Alerts**, **Integrations**, **Entity Groups**, **Account Management**, **Subnets**, **Webhooks/Services**, and **Sensors**.
- **Entity Search** field - Search for an entity.
- **Dashboard** icon - View the Dashboard.
- **Alerts** icon - View the Alerts Summary.
- **Secure Cloud Analytics sensors** icon - View the Sensors List.
- **Help** icon - Find documentation on how to configure and use Secure Cloud Analytics, and view information about open source licensing and data privacy. Includes **What's New?**, **FAQs**, **API Docs**, **Product Documentation**, **On-Prem Sensor Install**, **Open Source Licensing**, and **Privacy**.
- **User** icon - Review user settings for your account. Includes **Account Settings** and **Log Out**.