Cisco Secure Cloud Analytics New Features

- New Features, on page 1

New Features

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.

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

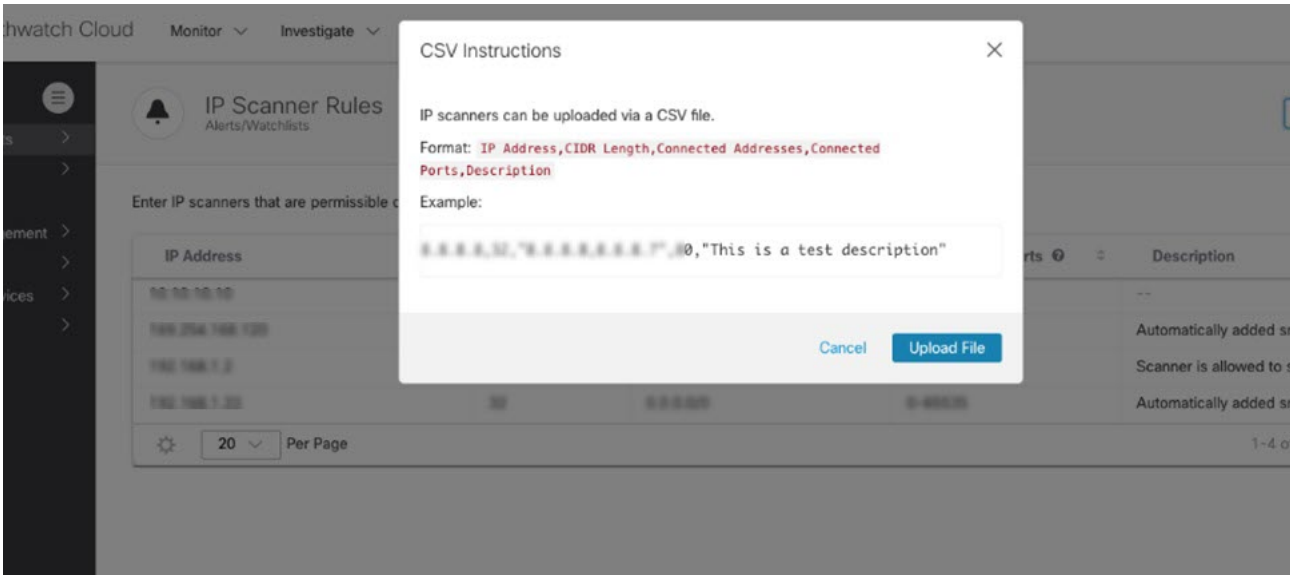
Customize Email Frequency by Alert Priority: Adjust email frequency based on the alert's priority by navigating to **Account Settings > Account Management > Email**.

AWS VPC Monitoring Status: We now display a table of all VPCs retrieved from AWS credentials provided and show their monitoring status. Navigate 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.

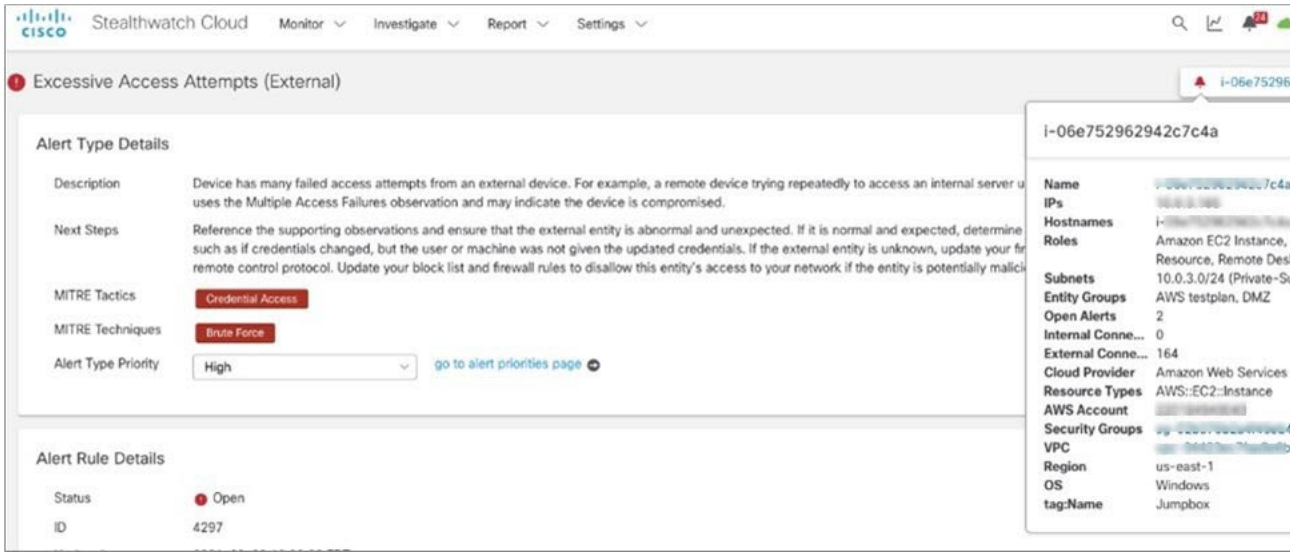


Added Device Outline section to alert details pages, making additional device context readily available during alert triage.

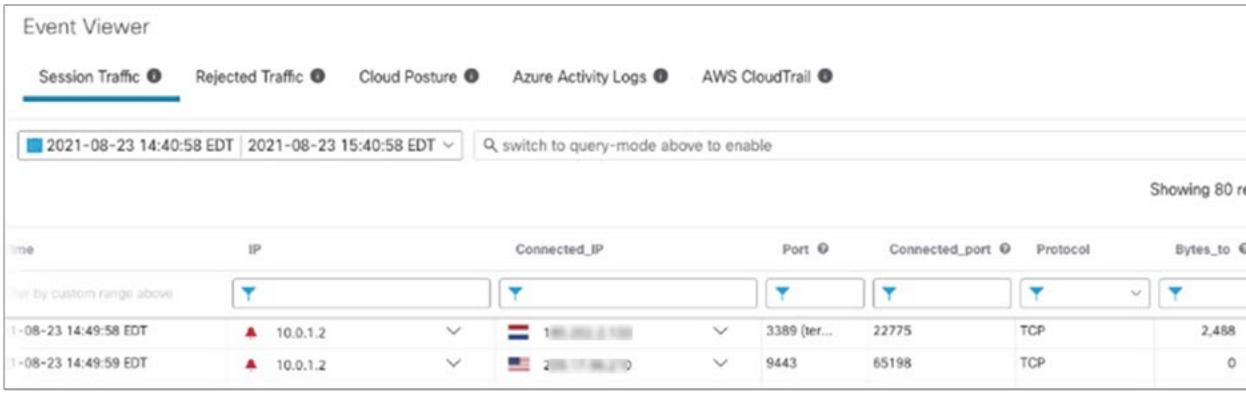
August 2021

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.

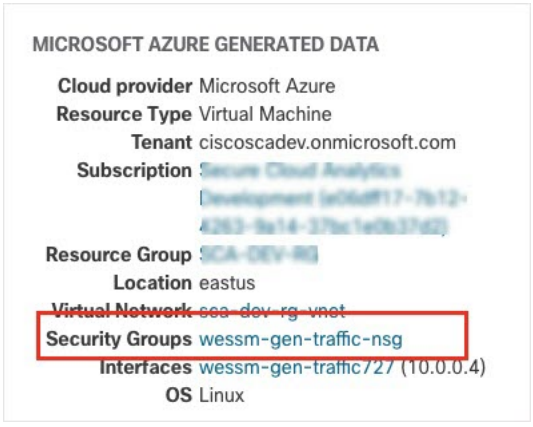
  Device has tried to establish new periodic connections that appear to be part of a Meterpreter Command and Control channel. This alert uses the Heartbeat observation and may indicate the device is compromised.

- 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.

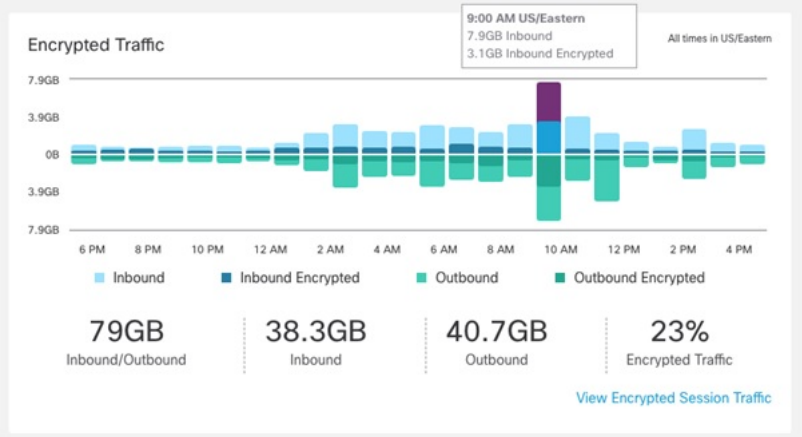
- AWS Lambda Persistence Alert added.

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

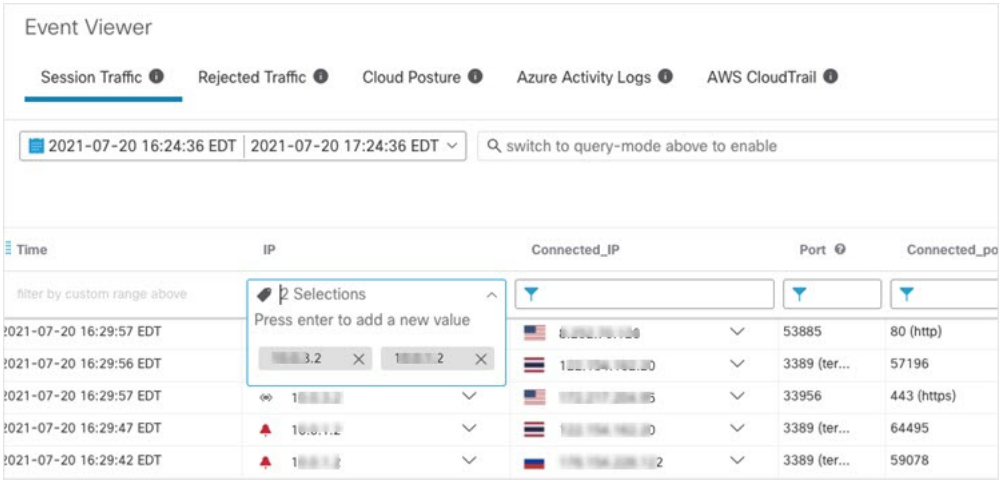


July 2021

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.

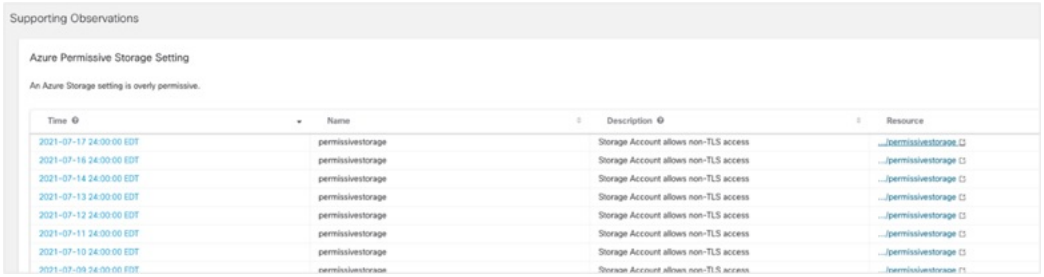


Added telemetry source to Observation types.

Persistent column resizing in the Event Viewer.

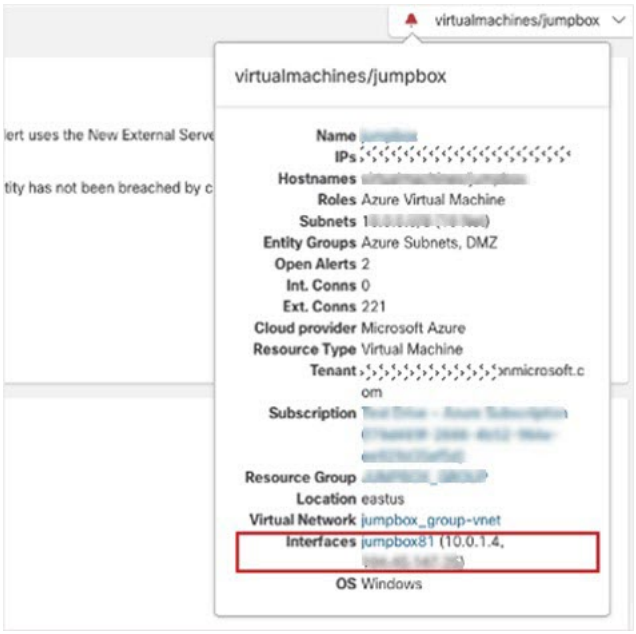
Supporting network session information for observations available in API.

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

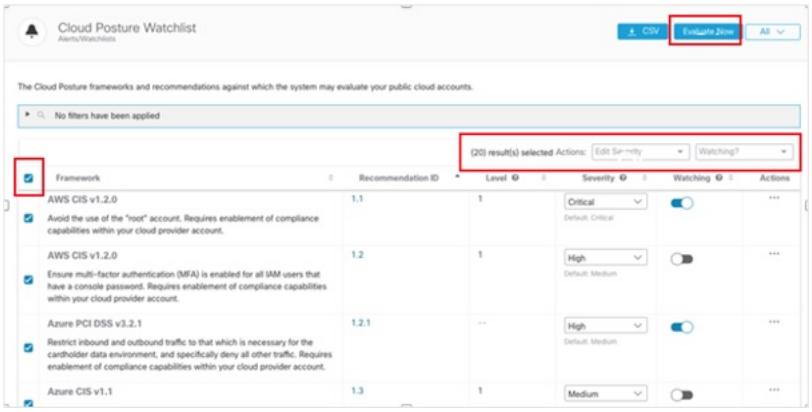


June 2021

Azure network interfaces now available in Device Info.



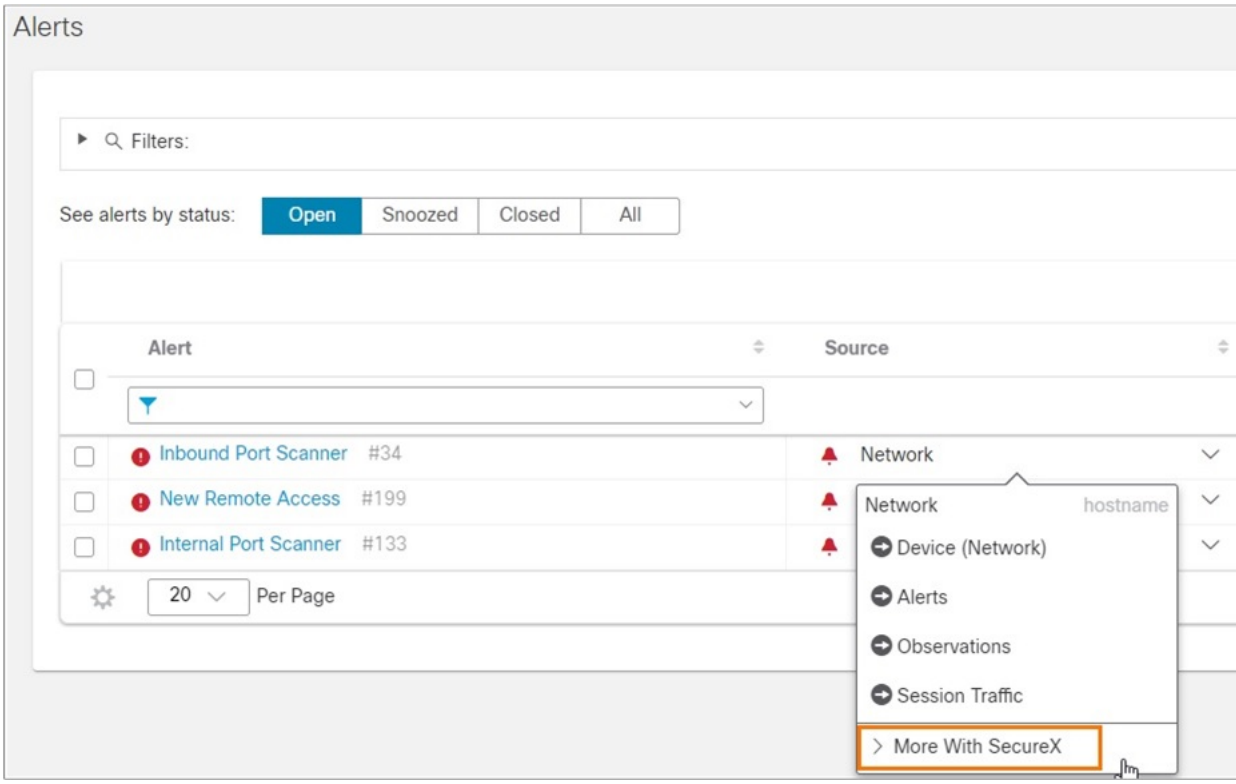
Cloud Posture on-demand watchlist checks and bulk watchlist editing.



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.

Cisco Secure Cloud Analytics sensor (formerly Stealthwatch Cloud 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**.