



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 visibility 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

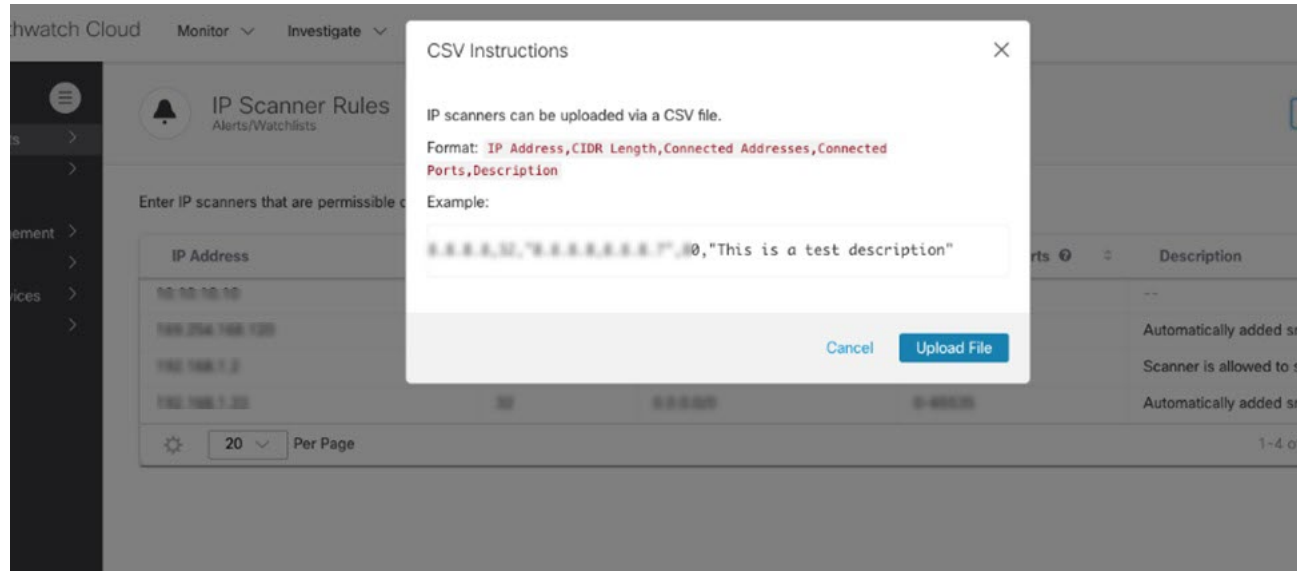
Customize Email Frequency by Alert Priority: Adjust email frequency based on the alert's priority by navigating to **Account Settings > Account Management > Email**.

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.

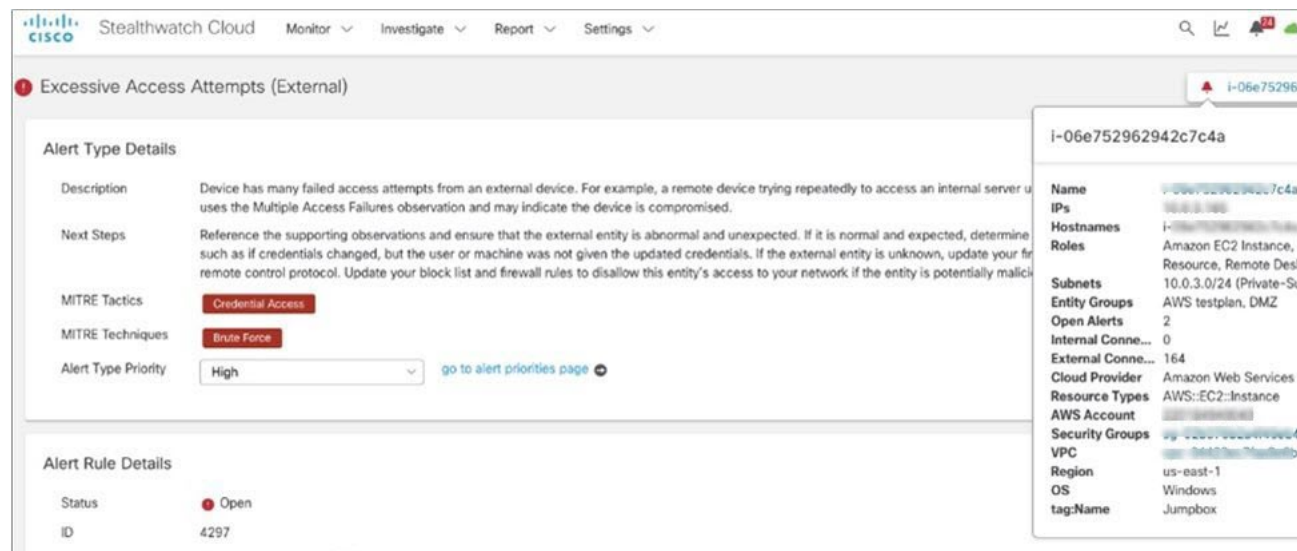


Added Device Outline section to alert details pages, making additional device context readily available during alert triage.

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.

Event Viewer

Session Traffic ● Rejected Traffic ● Cloud Posture ● Azure Activity Logs ● AWS CloudTrail ●

2021-08-23 14:40:58 EDT 2021-08-23 15:40:58 EDT

Showing 80 records

Time	IP	Connected_IP	Port	Connected_port	Protocol	Bytes_to
2021-08-23 14:49:58 EDT	10.0.1.2	10.0.0.1	3389 (ter...)	22775	TCP	2,488
2021-08-23 14:49:59 EDT	10.0.1.2	20.177.186.210	9443	65198	TCP	0

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.

MICROSOFT AZURE GENERATED DATA

Cloud provider Microsoft Azure

Resource Type Virtual Machine

Tenant ciscoscadev.onmicrosoft.com

Subscription Secure Cloud Analytics
[Development (a06d917-7b12-4263-9a14-37bc1a9b3742)]

Resource Group SCA-DEV-001

Location eastus

Virtual Network sea-dev-rg-vnet

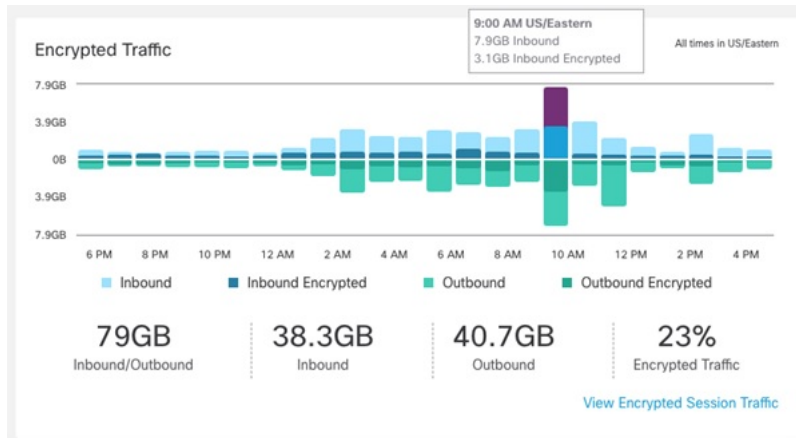
Security Groups wessm-gen-traffic-nsg

Interfaces wessm-gen-traffic/27 (10.0.0.4)

OS Linux

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.

Event Viewer

Session Traffic **1** Rejected Traffic **1** Cloud Posture **1** Azure Activity Logs **1** AWS CloudTrail **1**

2021-07-20 16:24:36 EDT | 2021-07-20 17:24:36 EDT |

Time	IP	Connected_IP	Port	Connected_po
2021-07-20 16:29:57 EDT	10.0.3.2	8.200.30.100	53885	80 (http)
2021-07-20 16:29:56 EDT	10.0.1.2	100.100.100.20	3389 (ter...)	57196
2021-07-20 16:29:57 EDT	10.0.3.2	100.217.200.95	33956	443 (https)
2021-07-20 16:29:47 EDT	10.0.1.2	100.100.100.20	3389 (ter...)	64495
2021-07-20 16:29:42 EDT	10.0.1.2	100.100.200.102	3389 (ter...)	59078

Added telemetry source to Observation types.

Observations

Highlights
Types
By Device
Selected Observations

Anomalous Profile Observation (6)
Device(s) used a profile for the first time which differs from typical behaviors seen in the network (e.g., an abnormally high number of devices using the profile for the first time, sending anomalous traffic).
Telemetry: [Follow](#)

AWS API Watchlist Access Observation (2)
AWS API was accessed from an IP on a watchlist.
Categories: [Powered by Teles](#)

AWS Architecture Compliance Observation (3/7)
Detected AWS resource that may violate AWS "Well-architected" guidelines.
Telemetry: [AWS API](#)

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.

Supporting Observations

Azure Permissive Storage Setting

An Azure Storage setting is overly permissive.

Time @	Name	Description @	Resource
2021-07-17 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage
2021-07-16 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage
2021-07-14 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage
2021-07-13 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage
2021-07-12 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage
2021-07-11 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage
2021-07-10 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage
2021-07-09 24:00:00 EDT	permissivestorage	Storage Account allows non-TLS access	...permissivestorage

June 2021

Azure network interfaces now available in Device Info.

virtualmachines/jumpbox

virtualmachines/jumpbox

Name jumpbox

IPs 10.0.0.10, 10.0.0.11, 10.0.0.12, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.16, 10.0.0.17, 10.0.0.18, 10.0.0.19, 10.0.0.20, 10.0.0.21, 10.0.0.22, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.29, 10.0.0.30, 10.0.0.31, 10.0.0.32, 10.0.0.33, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.37, 10.0.0.38, 10.0.0.39, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.43, 10.0.0.44, 10.0.0.45, 10.0.0.46, 10.0.0.47, 10.0.0.48, 10.0.0.49, 10.0.0.50, 10.0.0.51, 10.0.0.52, 10.0.0.53, 10.0.0.54, 10.0.0.55, 10.0.0.56, 10.0.0.57, 10.0.0.58, 10.0.0.59, 10.0.0.60, 10.0.0.61, 10.0.0.62, 10.0.0.63, 10.0.0.64, 10.0.0.65, 10.0.0.66, 10.0.0.67, 10.0.0.68, 10.0.0.69, 10.0.0.70, 10.0.0.71, 10.0.0.72, 10.0.0.73, 10.0.0.74, 10.0.0.75, 10.0.0.76, 10.0.0.77, 10.0.0.78, 10.0.0.79, 10.0.0.80, 10.0.0.81, 10.0.0.82, 10.0.0.83, 10.0.0.84, 10.0.0.85, 10.0.0.86, 10.0.0.87, 10.0.0.88, 10.0.0.89, 10.0.0.90, 10.0.0.91, 10.0.0.92, 10.0.0.93, 10.0.0.94, 10.0.0.95, 10.0.0.96, 10.0.0.97, 10.0.0.98, 10.0.0.99, 10.0.0.100

Hostnames 10.0.0.10, 10.0.0.11, 10.0.0.12, 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.16, 10.0.0.17, 10.0.0.18, 10.0.0.19, 10.0.0.20, 10.0.0.21, 10.0.0.22, 10.0.0.23, 10.0.0.24, 10.0.0.25, 10.0.0.26, 10.0.0.27, 10.0.0.28, 10.0.0.29, 10.0.0.30, 10.0.0.31, 10.0.0.32, 10.0.0.33, 10.0.0.34, 10.0.0.35, 10.0.0.36, 10.0.0.37, 10.0.0.38, 10.0.0.39, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.43, 10.0.0.44, 10.0.0.45, 10.0.0.46, 10.0.0.47, 10.0.0.48, 10.0.0.49, 10.0.0.50, 10.0.0.51, 10.0.0.52, 10.0.0.53, 10.0.0.54, 10.0.0.55, 10.0.0.56, 10.0.0.57, 10.0.0.58, 10.0.0.59, 10.0.0.60, 10.0.0.61, 10.0.0.62, 10.0.0.63, 10.0.0.64, 10.0.0.65, 10.0.0.66, 10.0.0.67, 10.0.0.68, 10.0.0.69, 10.0.0.70, 10.0.0.71, 10.0.0.72, 10.0.0.73, 10.0.0.74, 10.0.0.75, 10.0.0.76, 10.0.0.77, 10.0.0.78, 10.0.0.79, 10.0.0.80, 10.0.0.81, 10.0.0.82, 10.0.0.83, 10.0.0.84, 10.0.0.85, 10.0.0.86, 10.0.0.87, 10.0.0.88, 10.0.0.89, 10.0.0.90, 10.0.0.91, 10.0.0.92, 10.0.0.93, 10.0.0.94, 10.0.0.95, 10.0.0.96, 10.0.0.97, 10.0.0.98, 10.0.0.99, 10.0.0.100

Roles Azure Virtual Machine

Subnets 10.0.0.0/24 (10.0.0.0)

Entity Groups Azure Subnets, DMZ

Open Alerts 2

Int. Conns 0

Ext. Conns 221

Cloud provider Microsoft Azure

Resource Type Virtual Machine

Tenant 72f988bf-86f1-41af-91ab-2d7cd011db47@microsoft.com

Subscription Test Drive - Azure Subscription (10000000-0000-0000-0000-000000000000)

Resource Group jumpbox_group

Location eastus

Virtual Network jumpbox_group-vnet

Interfaces jumpbox81 (10.0.1.4, 10.0.0.10)

OS Windows

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

Cloud Posture Watchlist

3 CSV Evaluate Now All

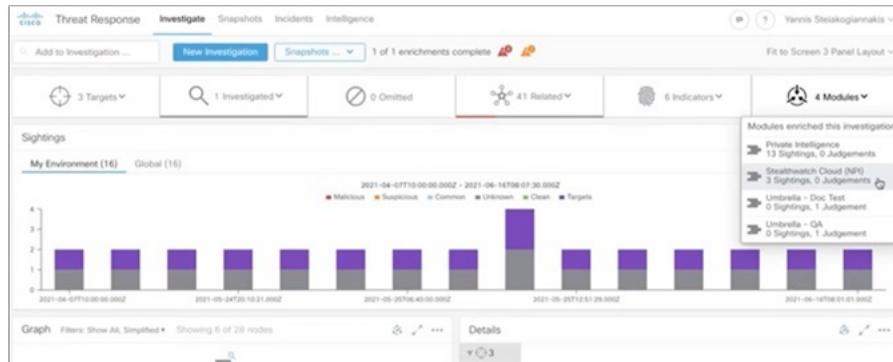
The Cloud Posture frameworks and recommendations against which the system may evaluate your public cloud accounts.

No filters have been applied

(20) result(s) selected Actions: Edit Severity Watching?

Framework	Recommendation ID	Level	Severity	Watching	Actions
<input checked="" type="checkbox"/> AWS CIS v1.2.0	1.1	1	Critical	<input checked="" type="checkbox"/>	...
<input checked="" type="checkbox"/> Avoid the use of the "root" account. Requires enablement of compliance capabilities within your cloud provider account.			Default: Critical		
<input checked="" type="checkbox"/> AWS CIS v1.2.0	1.2	1	High	<input type="checkbox"/>	...
<input checked="" type="checkbox"/> Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password. Requires enablement of compliance capabilities within your cloud provider account.			Default: Medium		
<input checked="" type="checkbox"/> Azure PCI DSS v3.2.1	1.2.1	---	High	<input checked="" type="checkbox"/>	...
<input checked="" type="checkbox"/> Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. Requires enablement of compliance capabilities within your cloud provider account.			Default: Medium		
<input checked="" type="checkbox"/> Azure CIS v1.1	1.3	1	Medium	<input type="checkbox"/>	...

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.

Alert	Source
<input type="checkbox"/> Inbound Port Scanner #34	Network
<input type="checkbox"/> New Remote Access #199	Network
<input type="checkbox"/> Internal Port Scanner #133	Network

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**.

