

Automated response, easier management, and enhanced security analytics

What's new in Cisco Stealthwatch Release 7.3.0

A lot of things have fundamentally changed how users work today. Applications, data, and user identities have moved to the cloud, branch offices connect directly to the internet, and many users work off-premises. Although this has given users an unprecedented ability to access, create, and share information online, it has also increased the likelihood of them exposing sensitive information. Couple that with today's evolving threats, and it comes as no surprise that security breaches continue to proliferate. You need comprehensive visibility into all network behavior both on and off premises to be able to detect any suspicious behavior. This is where a network detection and response (NDR) solution like Cisco Stealthwatch can help.

Stealthwatch collects telemetry from network traffic, applies behavioral based modeling analytics and machine learning, and incorporates threat intelligence from Cisco Talos to derive a baseline of what normal network behavior looks like to identify suspicious and anomalous behavior in your organization, alert you to its presence, and facilitate response efforts.

Stealthwatch release 7.3.0, introduces automated response capabilities to Stealthwatch, giving you new methods to share and respond to alarms, both through improvements to the Response Management module, and through SecureX integration enhancements. In addition to that, we are announcing other exciting updates to the web UI to increase ease of use, and security analytics updates that offer more threat detection advancements.



New Features

- Modernized response management module now in the web UI with customizable settings to facilitate automated data sharing and remediation
- Configurable rules and actions to offer numerous possibilities on how to share or respond to alarms
- SecureX platform integration enhancements
- Optimized installation process through full configuration in the web UI
- Flow Sensor deployment configuration and visibility improvements
- Enhanced security analytics

Automated Response updates

New methods for sharing and responding to alarms

With release 7.3.0, Stealthwatch's response management module has been moved to the web-based UI and modernized to facilitate data-sharing with 3rd party event gathering and ticketing systems. It now offers numerous ways to share and respond to alarms through a range of customizable action and rule options to aid in streamlining remediation operations and accelerating containment. You can also reduce noise and accelerate incident investigations with flexible rule configurations that allow you to specify which alarms from Stealthwatch are shared with SecureX threat response and improve operational efficiency by automating responses with pre-built workflows through the SecureX platform's orchestration capabilities.

Figure 1: The response management module allows you to automate response and alert sharing in a variety of ways through configurable rules and actions.

1. Automate remediation by limiting the compromised device's network access when detections occur, through automated and customizable quarantine policies that leverage Identity Services Engine (ISE) and Adaptive Network Control (ANC)
2. Webhooks to enhance data-sharing with third-party tools add unparalleled flexibility in response management and save time
3. Streamline and accelerate incident investigation and remediation efforts by specifying which malware detections to send to SecureX threat response as well as associated response actions

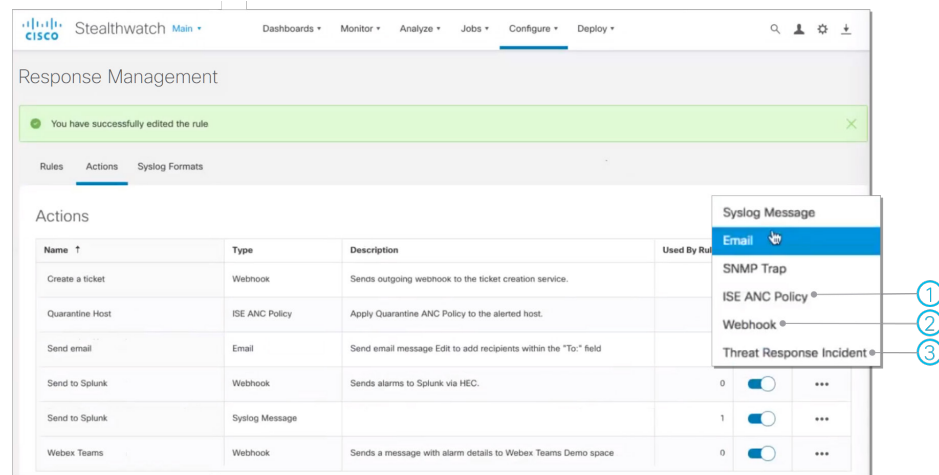


Figure 2: Configure numerous possibilities on how to share or respond to alarms from Cisco Stealthwatch: the following is a specific example of a rule and action combination in the response management module that triggers a specified response if an employee device connected either locally or remotely triggers a remote access breach alarm or a botnet infected host alarm. The response includes isolating the device with Cisco ISE, sending an incident notification to SecureX, and opening a ticket by using webhooks.

1. Set up rules to trigger when an alarm fires
2. Configure specific actions or responses that will take place once the above rule is triggered

The screenshot shows the 'Response Management' interface with a rule named 'Rules | Host Alarm'. The rule is currently disabled. The configuration for the rule is as follows:

Rule is triggered if:

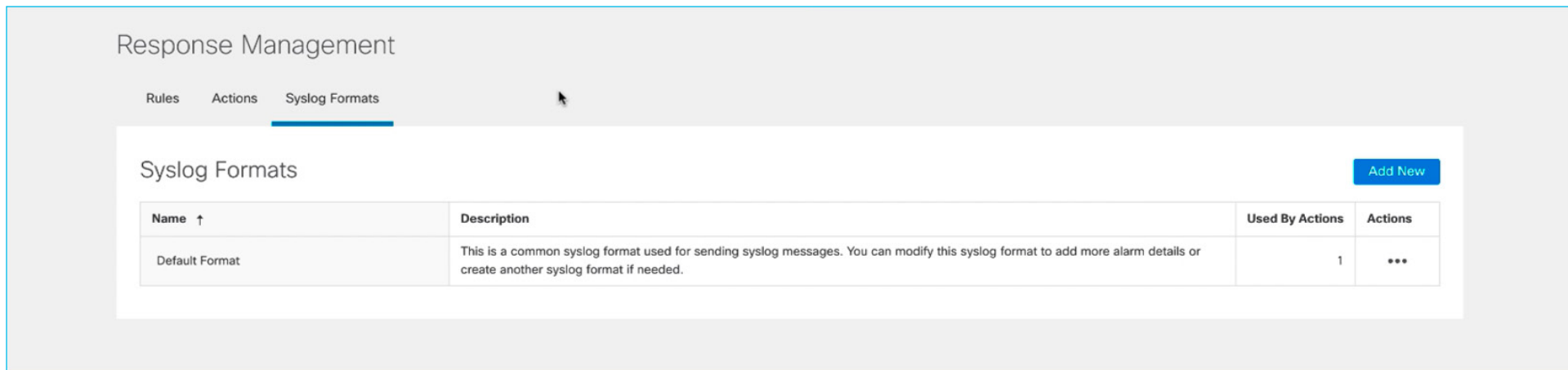
- Domain that originated the alarm is: Main
- ALL of the following is true:
 - Severity is Major only
 - Host Group of Source Host is Employee Wired or Employee WiFi
 - ANY of the following is true:
 - Type is ISE Possible Remote Access Breach
 - Type is Bot Infected Host - Successful CMC Activity

Associated Actions:

Name	Type	Description	Used By Rules	Assigned
Create a ticket	Webhook	Sends outgoing webhook to the ticket creation service.	0	<input checked="" type="checkbox"/>
Quarantine Host	ISE ANC Policy	Apply Quarantine ANC Policy to the alerted host.	1	<input checked="" type="checkbox"/>
Send email	Email	Send email message Evt to add recipients within the "To" field	2	<input checked="" type="checkbox"/>
Send to Splunk	Webhook	Send alerts to Splunk via HTTP Event Collector	0	<input type="checkbox"/>
Send to Splunk	System Message		2	<input type="checkbox"/>
Share Incident to SecureX	Threat Response Incident		0	<input checked="" type="checkbox"/>
Webex Teams	Webhook	Sends a message with alarm details to Webex Teams domain space	0	<input type="checkbox"/>



Figure 3: The response management module's syslog formats feature also allows you to create custom formats for Syslog messages to be sent to 3rd party solutions such as SIEMs and management systems.



Response Management

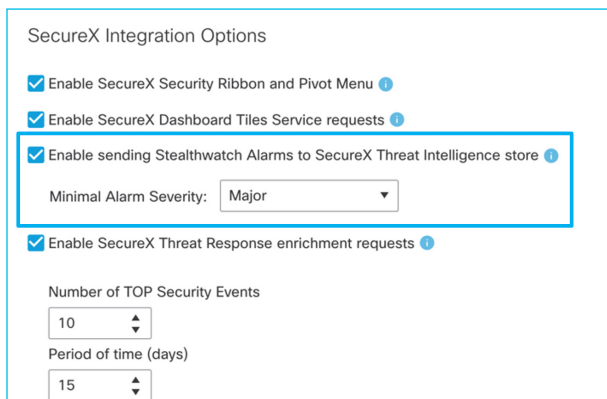
Rules Actions **Syslog Formats**

Syslog Formats [Add New](#)

Name ↑	Description	Used By Actions	Actions
Default Format	This is a common syslog format used for sending syslog messages. You can modify this syslog format to add more alarm details or create another syslog format if needed.	1	...

Response automation updates with SecureX

Cisco's SecureX platform unifies visibility, centralizes alerts, and enables automation across your entire security infrastructure on a single dashboard. Reduce noise and accelerate investigations with flexible rule configurations to define which alarms from Stealthwatch are shared with SecureX threat response. Maximize operational efficiency and eliminate repetitive tasks by automating responses with pre-built workflows through SecureX's orchestration capabilities.



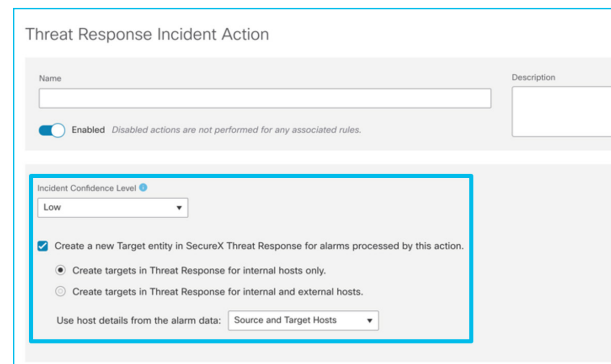
SecureX Integration Options

- Enable SecureX Security Ribbon and Pivot Menu ⓘ
- Enable SecureX Dashboard Tiles Service requests ⓘ
- Enable sending Stealthwatch Alarms to SecureX Threat Intelligence store ⓘ
 - Minimal Alarm Severity:
- Enable SecureX Threat Response enrichment requests ⓘ

Number of TOP Security Events

Period of time (days)

Figure 4: Get granular with flexible rule configurations to define which alarms from Stealthwatch are shared with SecureX threat response based off multiple parameters such as alarm severity, alarm type, and host groups.



Threat Response Incident Action

Name Description

Enabled *Disabled actions are not performed for any associated rules.*

Incident Confidence Level ⓘ

- Create a new Target entity in SecureX Threat Response for alarms processed by this action.
 - Create targets in Threat Response for internal hosts only.
 - Create targets in Threat Response for internal and external hosts.

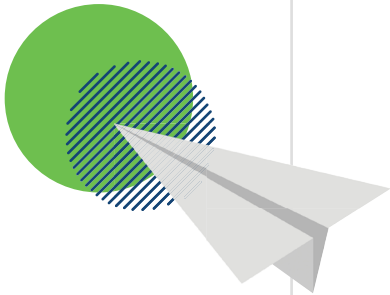
Use host details from the alarm data:

Figure 5: Be specific, by sharing alarms from mission critical services with the ability to define confidence levels of incidents, how target objects are formed, and by specifying rule conditions based off whether the target is created for internal or external hosts

Figure 6: Maximize operational efficiency, eliminate repetitive tasks, simplify business processes, and reduce human errors by automating responses with pre-built workflows through SecureX’s orchestration capabilities.

1. Automate responses with pre-built workflows through SecureX’s orchestration capabilities
2. Create your own playbooks by leveraging SecureX’s intuitive interface and all of your integrated security tools.

The screenshot displays the 'My Workflows' interface in Cisco SecureX. At the top, there are tabs for 'My Workflows' and 'Atomic Actions'. Below the tabs, there are filters for workflow status: 8 TOTAL, 1 INVALID, 2 VALIDATED, and 5 FAVORITE. A search bar and 'IMPORT' button are also visible. The main area shows a grid of workflow cards, each with a star icon and a 'Get_' prefix. A callout '1' points to the 'NEW WORKFLOW' button in the top right. Below the grid, the configuration for the 'Get_Security_Events' workflow is shown. On the left, there is a list of activities such as 'Calculate Date', 'Convert Json to Xml', and 'JSONPath Query'. A callout '2' points to this list. The main workspace shows a flowchart with steps: 'LAUNCH EVENT QUERY AND CHECK COMPLETION' (containing 'Launch Event Query' and 'Parse Query ID'), 'Check if query completed', 'Parse query completion', and 'Set Variables'. Below this is a 'WHILE LOOP' containing a 'CHECK CONDITION BRANCH' with 'Check if query completed'. On the right, the 'PROPERTIES: HTTP REQUEST' section shows a 'LAUNCH_EVENT_QUERY' request with a 'POST' method and a JSON request body. The request body is a JSON object with fields like 'startRange', 'endRange', 'hosts', 'ipAddress', and 'type'. A 'FORMAT' button is visible below the JSON. At the bottom right, there is a 'Headers' section with 'CONTENT TYPE' set to 'Select'.



Enhanced Security Analytics

We continue to update and improve Stealthwatch analytics to stay ahead of evolving threats and deliver fast and high-fidelity detections. The cloud-based machine learning engine (Cognitive Intelligence) has been updated to include enhanced detections, new classifiers, smart alert fusion in the new GUI, and [new Stealthwatch use cases](#) including [Remote Access Trojan](#) and [Emotet malware](#) detections.

Figure 7: New machine learning classifiers have been added to the hundreds already in production! Below is an example of a new content spoofing detector classifier in action. For more detail on new classifiers, see the Cognitive notes [here](#).

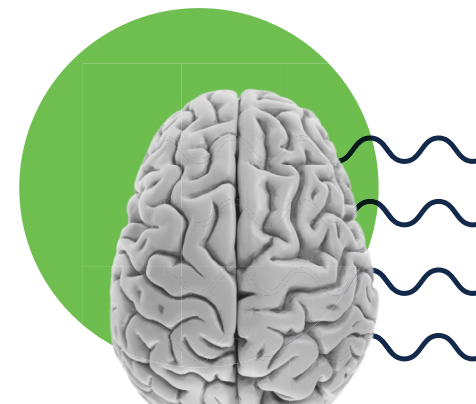
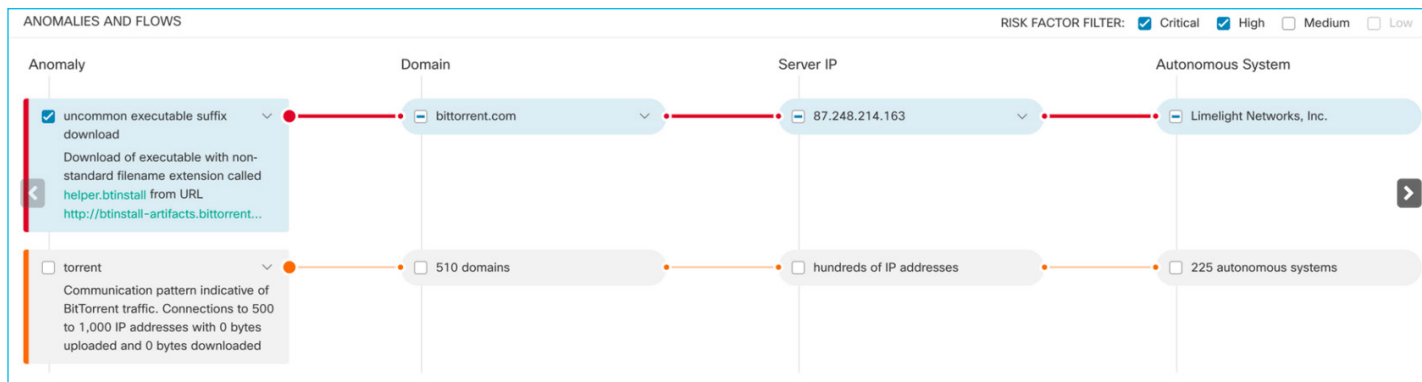
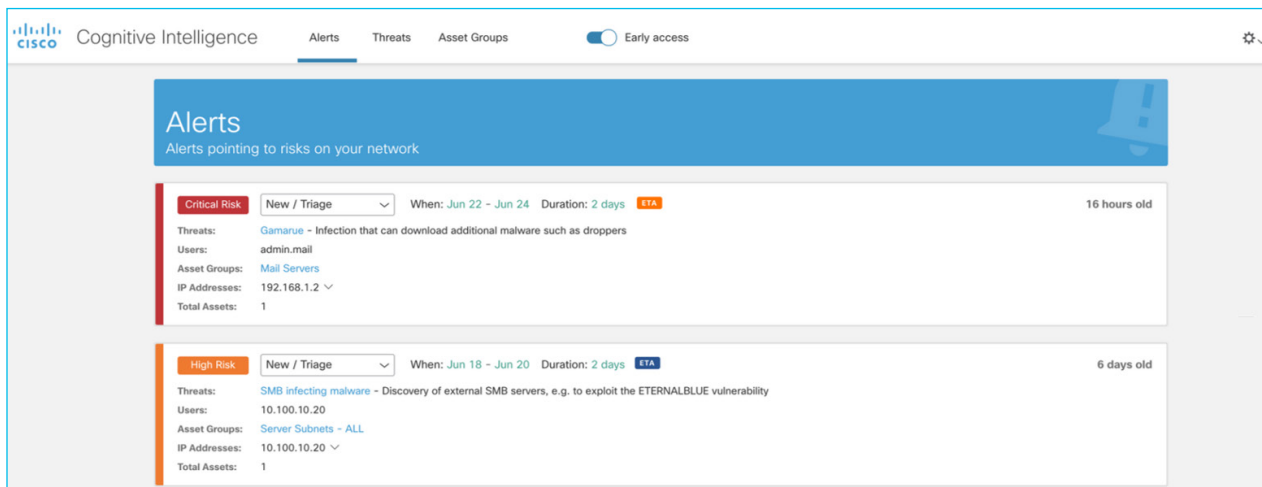


Figure 8: Stealthwatch’s new GUI with smart alert fusion has been launched in Beta. For more information on this new feature, see the Cognitive release notes [here](#).



Web UI improvements

Save time and optimize the installation process with web UI enhancements that support full appliance configuration.

Flow Sensor versatility and visibility enhancements

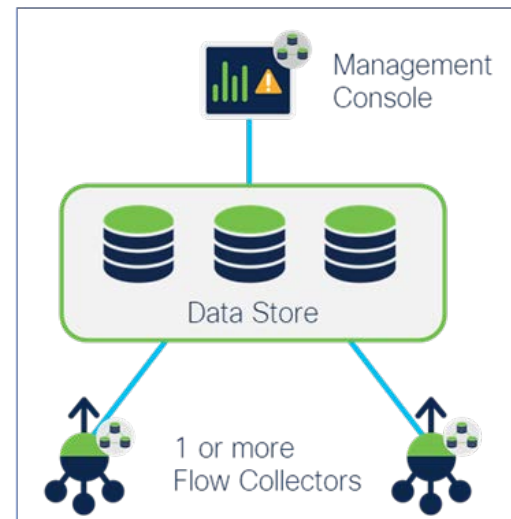
ERSPAN (Encapsulated Remote Switch Port Analyzer) support has been added to the Flow Sensor to increase versatility. Now, it also offers visibility improvements through the ability to see within VMware’s NSX-T data centers to facilitate Flow Sensor deployment and network configuration.

Introducing the Stealthwatch Data Store!

Supported by versions 7.3 and above, the Data Store offers an improved database architecture design that enables new ways of storing and interacting with data. Each Data Store appliance sits between the Stealthwatch Management Console and Flow Collectors. After Flow Collectors ingest and de-duplicate flow data, it is sent to the Data Store. This flow data is distributed equally across a Data Store, which is comprised of a minimum of three Data Node appliances. This facilitates flow data storage and keeps all your network telemetry in one centralized location as opposed to having it spread across multiple Flow Collectors in a distributed model.

This new centralized model with flow ingest by decoupled from data storage offers the following benefits:

- **Increased ingest capacity:** Data Stores can be combined to create a single cluster that is capable of monitoring over 3 million flows per second.
- **Query and reporting response times improved by a significant magnitude:** The Data Store provides drastically improved query performance and reporting response times of at least 10x faster than those offered by other standard deployment models.
- **Enterprise-class data resiliency:** Telemetry data is stored redundantly across nodes to allow for seamless data availability during single node failures helping to ensure against loss of telemetry data.
- **Storage scalability:** The Data Store offers organizations with growing networks enhanced flexibility around data storage scalability through the ability to add additional database clusters.
- **Long-term data retention:** Scalable and long-term telemetry storage capabilities enable long-term flow retention of up to 1-2 years' worth of data with no need to add additional Flow Collectors
- To learn more, check out the Stealthwatch Data Store [Solution Overview](#).



Benefits

Streamline remediation operations by customizing rules and actions to automate data sharing with 3rd party event gathering and ticketing systems

Maximize operational efficiency and eliminate repetitive tasks by automating responses with pre-built workflows through SecureX's orchestration capabilities

Reduce noise and accelerate incident investigations with flexible rule configurations to define which alarms from Stealthwatch are shared with SecureX threat response

Stay ahead of emerging threats with machine learning detection enhancements

We continue to deliver **new use cases** that cover new Stealthwatch functionalities and new malware detections

Save time with Web UI enhancements that optimize the installation process and support full appliance configuration



Next Steps

For further details about this release, please refer to the [release notes](#).

To learn more about Stealthwatch, visit <https://www.cisco.com/go/stealthwatch>

or contact your local Cisco account representative.