



August 2022

Updates released in August of 2022 to Cisco cloud-based machine learning global threat alerts:

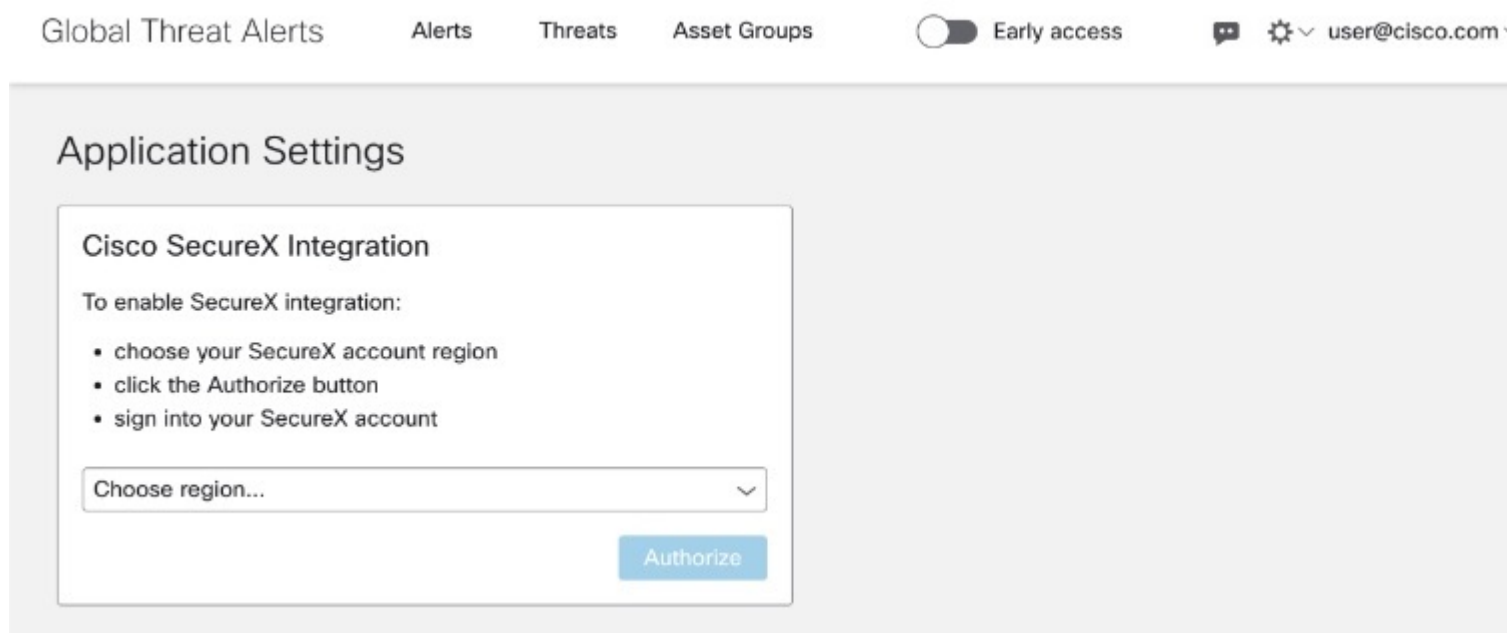
- [Improved Alert Workflows, on page 1](#)
- [Additional Threat Detections, on page 6](#)

Improved Alert Workflows

We've improved the ways you can work with alerts in **Early access** and promote alerts in global threat alerts to the SecureX incident manager.

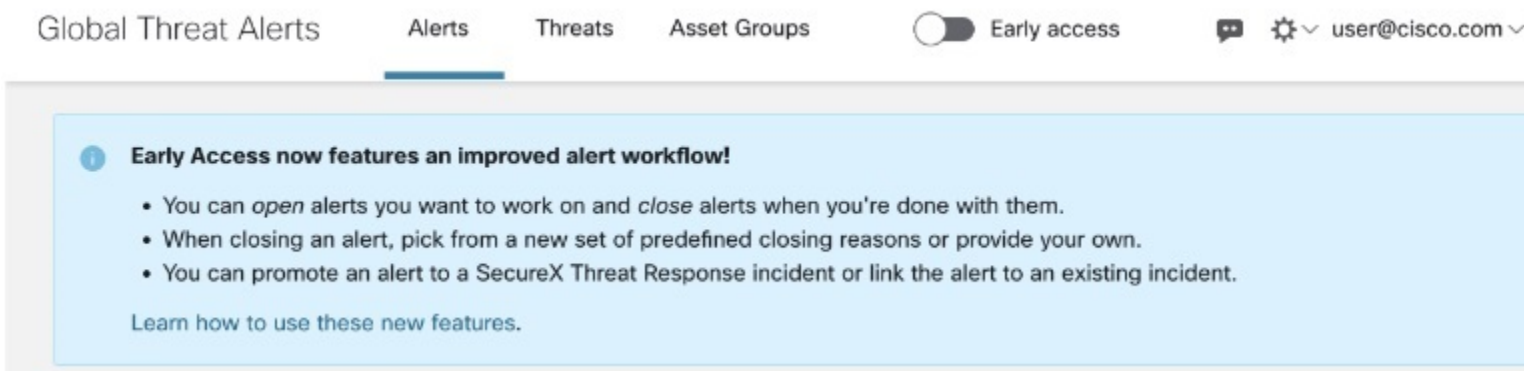
To enjoy the benefits of integrating with SecureX incident manager, enable SecureX integration in the **Application Settings** of the global threat alerts console:

Figure 1: Authorize SecureX Integration in Application Settings



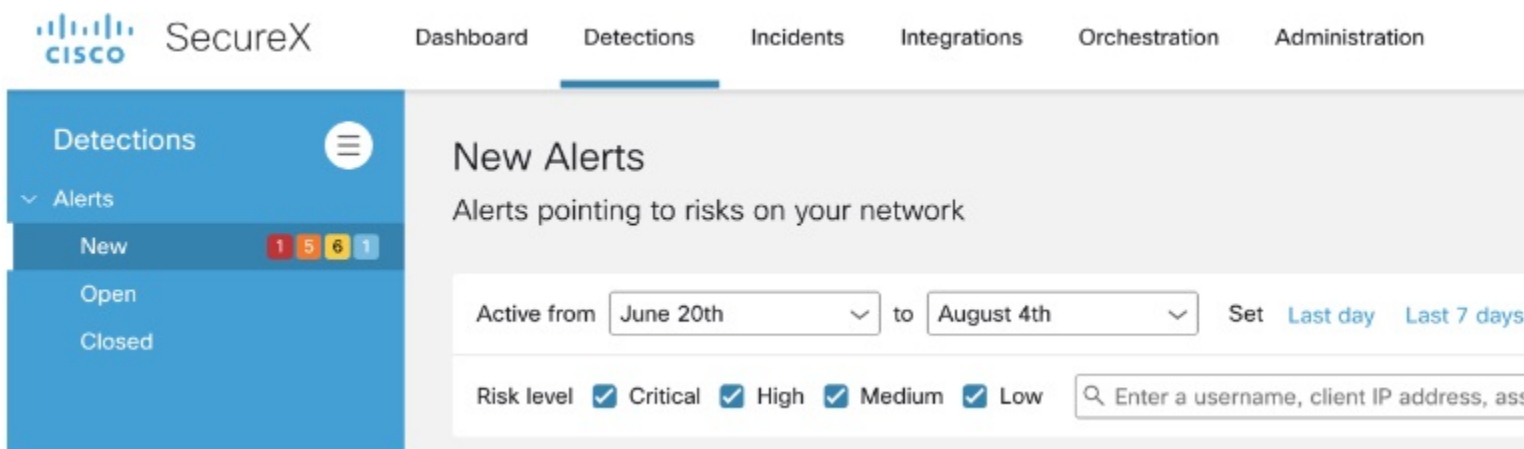
In the header of the global threat alerts console, click **Early access** to enable it:

Figure 2: Switch On Early Access to Activate New Features



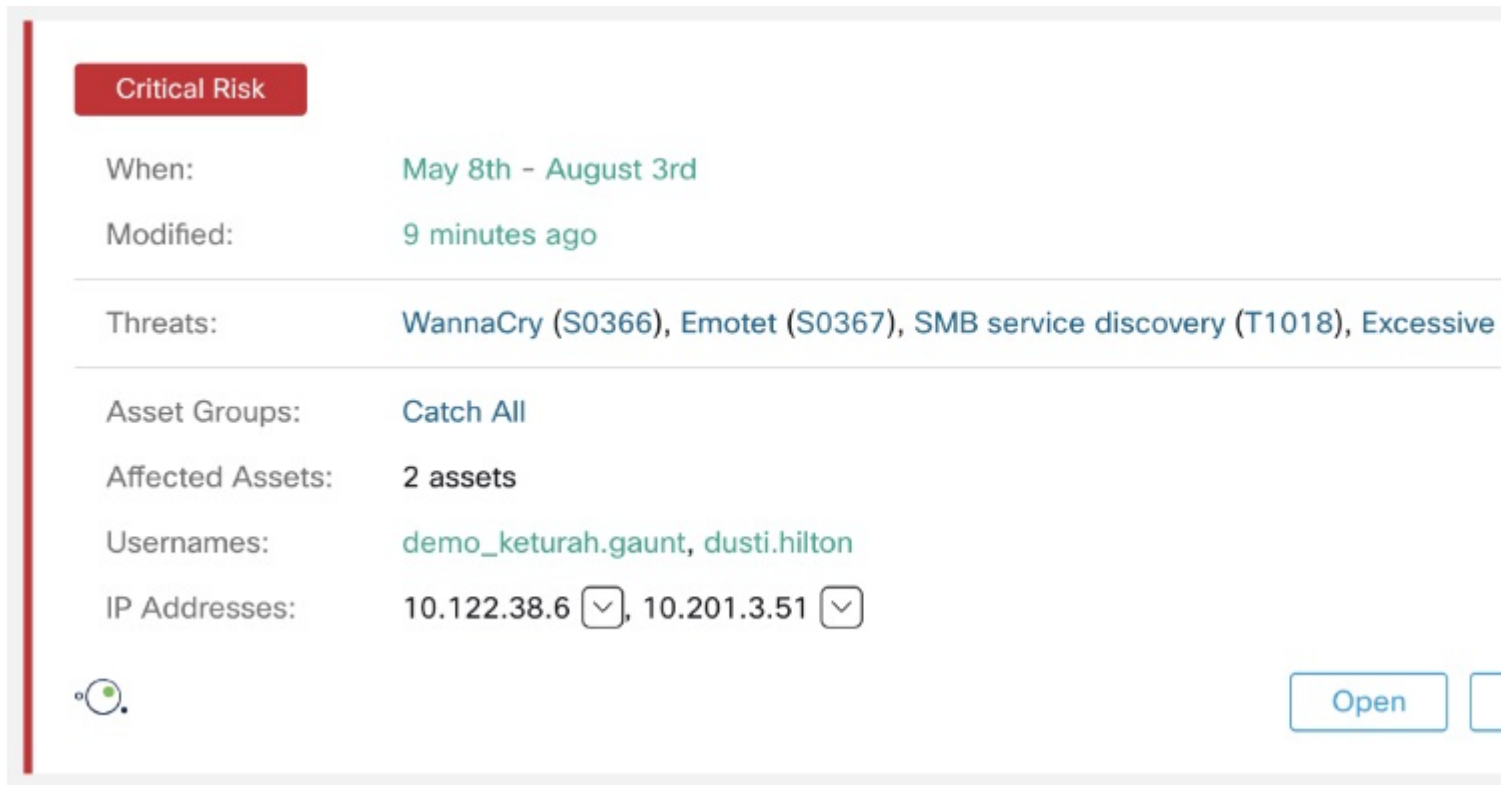
Once **Early access** is enabled, alerts are categorized as **New**, **Open**, or **Closed**:

Figure 3: Alerts in New, Open, and Closed Status Categories



A **New** alert status can be changed using the **Open** or **Close** button:

Figure 4: Open or Close Alert



The screenshot displays a security alert interface. At the top left, a red button labeled "Critical Risk" is visible. Below it, the alert details are listed:

- When:** May 8th - August 3rd
- Modified:** 9 minutes ago
- Threats:** WannaCry (S0366), Emotet (S0367), SMB service discovery (T1018), Excessive
- Asset Groups:** Catch All
- Affected Assets:** 2 assets
- Username:** demo_keturah.gaunt, dusti.hilton
- IP Addresses:** 10.122.38.6 (dropdown), 10.201.3.51 (dropdown)

At the bottom left, there is a magnifying glass icon. At the bottom right, there is a blue "Open" button and a partially visible "Close" button.

While global threat alerts continues to focus on its core competencies, such as extended detections and efficient alert triage, it now integrates more tightly with the SecureX ecosystem, using just one click to promote detections to the incident response workflow in SecureX.

When an alert is opened, you have the option to:

- Open and link the alert to a new incident
- Open and link the alert to an existing incident
- Open only

Figure 5: Open Alert with Option to Link to Incident

Open Alert

Add a note to this alert

Open and link to a new incident

Title (required)

Response to critical risk alert

Open and link to an existing incident

Use Lucene syntax to filter incidents

Response to critical risk alert

Response to critical risk alert

Response to critical risk alert

Response to critical risk alert

Response to critical risk alert

Open only

< Previous Next >

Cancel Open

In the SecureX incident manager, the incident contains details such as a **Summary** and all the security **Events** and **Observables** from the original alert. You can then investigate and respond further, using SecureX features such as investigation, enrichment, and orchestration.

When it's undesirable to promote an alert as an incident, you can still **Open only** and track the work only on the global threat alerts console.

In both cases you can **Close** alerts when you're done with them. When closing an alert, pick from a new set of predefined **Closing reasons** or provide your own:

Figure 6: Close Alert with Reasons for Closing

Close Alert

Conditions for alert creation can be modified on the Threats and Asset Groups pages.

Closing reasons

- Communication or endpoint behavior was added to be blocked
- Endpoint was scanned and cleaned
- Endpoint was reimaged
- Internal case was created to resolve the problem

- The threats represent legitimate or tolerated behavior
- The affected assets are unmanaged or insignificant
- We could not verify the findings
- The alert is not actionable (unable to remediate)
- Communication or endpoint behavior is already blocked

Additional reason

Feedback

Contact me to discuss this feedback

When closing an alert, you can close it as **useful** or **not useful**. You can also provide additional feedback about the alert to the team at Cisco; your valuable feedback helps us improve future detections.

Closing reasons will be recorded as part of the alert for future reference:

Figure 7: Closing Reasons Shown on Alert Detail Page

The screenshot shows the Cisco SecureX interface. The top navigation bar includes Dashboard, Detections, Incidents, Integrations, Orchestration, and Administration. The left sidebar shows the Detections menu with sub-items: Alerts (New: 5, Open: 6, Closed: 1), Threat Catalog (Detected: 3, Suppressed: 5, 10), and Asset Groups (Affected: 1, 23, Suppressed: 1, Settings). The main content area is titled 'Alert Detail' and shows 'Closing Reasons' with a single reason: 'Communication or endpoint behavior was added to be blocked'. Below this, a red 'Critical Risk' tag is displayed along with 'When: May 8th - August 3rd', 'Modified: 3 seconds ago', and 'Affected assets: 2'. There is a text input field for 'Add a note to this alert' and a 'Linked Incident: Not linked' status.

Closed alerts can be opened. Re-opening an alert will remove all its closing reasons. It will also remove any references to previously linked SecureX incidents. However, you can choose to link the alert again, even to the same SecureX incident as before.

Additional Threat Detections

We've added a new threat detection, SocGholish, to our portfolio. And we've updated indicators for our existing threat detections.

SocGholish

SocGholish, also known as FakeUpdates, is a downloader malware that mimics legitimate software updates. It is based on Javascript (T1059.007) and spreads through drive-by downloads (T1608.004). It is capable of collecting endpoint (T1005) and network data such as user permissions (T1069), domain trusts (T1482), domain account information (T1087.002), services running (T1007), files containing credentials (T1083), and so on. It also leads to further infections by different malware families.

To see if SocGholish has been detected in your environment, click [SocGholish Threat Detail](#) to view its details in global threat alerts.

Figure 8:

SocGholish

Javascript based malware mimicing legitimate software updates

High Severity



5+ affected assets in 5+ companies

SocGholish, also known as FakeUpdates, is a downloader malware that mimics legitimate software updates. It is based on Javascript (T1059.007) and spreads through drive-by downloads (T1608.004). It is capable of collecting endpoint (T1005) and network data such as user permissions (T1069), domain trusts (T1482), domain account information (T1087.002), services running (T1007), files containing credentials (T1083), etc. It also leads to further infections with different malware families.

Category: Malware - downloader

