

Dashboard

The global threat alerts (formerly Cognitive Intelligence) feature helps you quickly detect and respond to sophisticated, clandestine attacks that are either already under way or attempting to establish a presence within your network. The feature automatically investigates suspicious or malicious web-based traffic. It identifies both confirmed and potential threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations, or a unique threat that you've never seen before.

As a cloud-based service, global threat alerts analyzes the information generated by your existing web security solutions, without the need for any additional hardware or software. It zeroes in on malicious activity that has bypassed security controls.

Using machine learning and a statistical modeling of networks, global threat alerts creates a baseline of normal activity and identifies anomalous traffic occurring within your network. It analyzes device behavior and web traffic to pinpoint command-and-control communications and data exfiltration.

Learning from what it sees, global threat alerts adapts to provide continuous breach identification, reducing the risk of repeat attacks or continued infection. It presents its information through an intuitive, web-based portal that's integrated with several Cisco Security products, so that you can assess the severity and scope of intrusions, understand the mission of the threat and how it works, and take immediate action.

- Overview, on page 1
- Investigate Alerts, on page 3
- Investigate Threats, on page 8
- Asset Groups, on page 10

Overview

Our analytics engine applies machine learning to incoming data streams and projects the detections into a 3-dimensional space:



- **Threat-severity dimension.** How severe is the threat? Confirmed threats and their severity. To better align with your organization's risk profile towards individual threat types, you have the option to adjust the pre-defined severity of individual threats.
- Asset-value dimension. How valuable is the asset? If all the devices connected to the network are not equally important, you have the option to adjust the business value of individual asset groups to prioritize detections for your more important devices.
- **Confidence dimension.** How confident are we in the verdict? Confidence in the verdicts that our algorithms are making about individual threats observed in the customer environment. In some instances, we observe enough behavioral indicators that our verdict is almost certain. In some other instances, despite the similar symptoms, the actual evidence might be sketchy. Therefore, the margin for error increases.

Our fusion algorithm uses these detections to identify clusters of similar threats and projections to calculate their risk levels. Our web portal then presents these as security alerts in a list prioritized by their risk levels. Each alert points to threats on your network and represents a natural unit-of-work for investigation and subsequent remediation.

Overview

Investigate Alerts

- **Step 1** In the navigation menu to the left, click **Alerts** and **New** to view all the new alerts on your network. Each alert is displayed on its own card.
 - a) Each alert card aggregates one or more threats that are concurrently affecting a set of assets on your network with similar business values.

Figure 2:

| cisco | Global | Threat | Alerts | Dashboard | Detections | Incidents | Integrations | Orchestration | Administration | () | \$~ ₽~ |
|--|------------|---------------|-------------------------|---------------------------------|----------------------------------|-------------------|-----------------|--------------------|----------------------------|----------------|-------------|
| Detectio | ons | 386 | Ne [.] Aler | w Alerts ts pointing to risk | ks on your ne | etwork | | | | | |
| Open Closed | | | Ac | tive from July 26th | ~ | to Septembe | er 9th 🗸 🗸 | Set Last day | Last 7 days Last 30 day | s Last 45 days | |
| ✓ Threat Car Detects | italog | A A 10 | Ris | k level 🗹 Critical (| 🖌 High 🖌 Me | edium 🗹 Low | Q Enter a us | sername, client IP | address, asset group, or t | hreat | |
| Suppre | essed | | Sort | by: Risk 🗡 When | Affected ass | sets 🗠 | | | | | |
| Asset Gro Affecte | oups ed | 1 24 | | Critical Risk | | | | | | | ETA |
| Suppre | essed | | | When: | June 13th - S | eptember 8th | | | | | |
| Settings | | | _ | Modified: | 10 hours ago | | | | | | |
| | | | | Threats: | WannaCry (S0 | 366), Emotet (| S0367), SMB Ser | vice Discovery (T | 1018), Excessive Commur | nication | |
| | | | | Asset Groups: | Office Lab/0, | Office Lab/1 | | | | | |
| | | | | Affected Assets: | 2 assets | | | | | | |
| | | | | Usernames: | demo_keturah | n.gaunt, dusti.hi | ilton | | | | |
| | | | | IP Addresses: | 10.122.38.6 | ∽, 10.201.3.51 | 1 🖂 | | | | |
| | | | •(| | | | | | Open | Close | lert Detail |
| | | | | Critical Pisk | | | | | | | |
| | | | | When | Contombox Ot | 2 | | | | | |
| | | | | Modified: | 10 hours ago | n M | | | | | |
| | | | | Threats: | ZeroAccess (S | 50027) | | | | | |
| | | | | Asset Groups: | Web Servers | | | | | | |
| | | | | Affected Assets: | 1 asset | | | | | | |
| | | | | Usernames: | demo_chassic | dy.phalen | | | | | |
| | | | | IP Addresses: | 192.168.0.16 | \checkmark | | | | | |
| | | | •(| ◉. | | × | R + 1 | | Open | Close | lert Detail |

• Threats. Different threats that are occurring together.

- Asset Groups. These threats are occurring on endpoints that belong to these asset groups with similar business values.
- b) The risk level is based on the severity level of the threat and business value of the asset groups. A higher risk level indicates a higher risk of the threat severely impacting the valuable asset(s) on your network.
- **Step 2** Alerts with higher risk are ordered closer to the top of the list. Prioritize your analysis by responding to the alerts based on their risk level and investigating higher risk alerts first.
 - Critical
 - High
 - Medium
 - Low
 - **Note** Alert cards can dynamically change, such as when new threats are added to the group or the asset group business value or threat severity are changed.
- **Step 3** You have the option to filter which alerts are shown by choosing age, risk level, username, IP address, asset group, and/or threat. You also have the option to sort by risk level, age, or number of affected assets.

Figure 3:

New Alerts

Note

Alerts pointing to risks on your network

| EUTED | Active from July 26th \checkmark to September 9th \checkmark Set Last day Last 7 days Last 30 days Last 45 days |
|--------|---|
| FILTER | Risk level 🗸 Critical 🖌 High 🖌 Medium 🖌 Low 🔍 Enter a username, client IP address, asset group, or threat |
| SORT | Sort by: Risk V When V Affected assets V |

Step 4 Start your investigation of an alert by changing its status to **Open**.

When its status is no longer **New**, the alert card remains unchanged and stable, to ease investigation.

Step 5Click on Alert Detail for additional content about each detected threat and affected asset. Each affected asset includes a
Threats section which lists all the threat detections made on that asset, including all the convicting security events.

Figure 4:

| ffected Assets | |
|---|--|
| Username: IP Addresses: Asset Groups: | dusti.hiiton 10.201.3.51 💟 Catch All |
| Threats From: | 2022-03-05 01:00:00 CET To: 2022-05-31 06:14:58 CEST Duration: 87 days |
| Emotet (S0 | 367) 🕔 🌒 - Infection with exfiltration capability that targets banking credentials |
| Known | n malicious hostnames |
| Comm | unication with hostnames 201.213.32.59 v and 77.55.211.77 v known to be indicative of Emotet |
| WannaCry | (S0366) 🕔 🍘 - Disk encrypting malware contains worm-like features to spread itself using the SMBv1 exploit EternalBlue |
| Know | n malicious hostnames |
| Comm | nunication with hostnames www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff.com 🖓 and www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 🕤 |
| Known | n malicious hostnames from local passive DNS inference |
| Comm and 10 to be i | unication to IP addresses 104.16.173.80 vith local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 04.17.244.81 v with local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com v. The hostnames are kr ndicative of WannaCry |
| SMB servic | e discovery (T1018) 🕔 🥥 - Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE vulnerability rotocol communication |
| Comm | unication over SMB protocol with more than 5,000 IP addresses, hosted in more than 5,000 autonomous systems and 100 to 250 countries |
| Excessive of | communication (T1498) () 🗇 - Uniform communication to many external nodes |
| Exces | sive external communication |
| Conne | ctions to more than 5,000 IP addresses, hosted in 2,000 to 5,000 autonomous systems and 100 to 250 countries |
| > Contextual e | vents From: 2022-03-05 01:00:00 CET To: 2022-05-31 06:14:58 CEST Duration: 87 days |
| ·O. | Asset 0 |
| | |

At the top of the **Threats** section is the total observation period for all the detected threats and their convicting security events on the particular asset.

Figure 5:

```
Threats From: 2022-03-05 01:00:00 CET To: 2022-05-31 06:14:58 CEST Duration: 87 d
```

Each threat detection shows its name, MITRE link, description, and:

• Severity



An event annotation may also contain a drop-down menu that enables you to pivot to other Cisco Security products and pull in additional information and intelligence about the observables.

Figure 10:



Each security event includes a timeline showing the timing and occurrence of the behavior within the context of the **Threats** total observation period.

Figure 11:



Communication with hostnames 201.213.32.59 🗸 and 77.55.211.77 🗸 known to be indicative of Emotet

The **Contextual events** section can be expanded to show more events that could provide additional context about what was happening on the asset.

Figure 12:

| ~ Contextual events | From: 2022-05-31 11:55:58 CEST | To: 2022-05-31 11:57:59 CEST | Duration: 2 minutes |
|---------------------|---------------------------------------|------------------------------|---------------------|
| Anomalous of | destination | | |
| Communicati | ion with a rarely contacted autonomou | is system | |

Step 6 Selecting one of the specific events for one user pivots you to the **Security Events** view, where you can see a detailed context of the specific events that triggered the malicious detection.

Figure 13:

| unty event | Domain | ~ | Server IP address | ~ | Autonomous system | |
|---|-------------------------|--------|--------------------------|---------|--------------------------------------|----------|
| | eg. domain1.com | ø | eg. 1.2.3.4 | ø | eg. "Amazon.com, Inc." | % |
| d Injector | | | | | | |
| ab browser plugin that injects advertisements to visited pages | | | | | | |
| | allconverterssearch.com | | 172.67.199.72 | | unknown autonomous system | |
| Pattern similar to known malicious URLs | searchconvertor.com | | 104.24.108.200 | | unknown autonomous system | |
| of threats · | | | 172.67.152.39 | \odot | | |
| | topstreamssearch.com | | 104.24.121.36 | | AS13335 | 0 |
| main Generation Algorithms (T1568.002) | | | | | | |
| ndom-string domain names used as obfuscation technique | | | | | | |
| 🗆 DGA hostnames 🕞 💽 | • fullhd720pizle3.com | | 104.18.52.231 | | Cloudflare, Inc. AS13335 | |
| Communication with hostnames created by a domain generation algorithm (DGA) | e io8b80kcom8f.com | | 192.243.59.20 | | | |
| ·O. | w00ur5z9jy3a.com | w00ur | 5z9jy3a.com | r 🕑 🔸 | DataWeb Global Group B.V. AS39572 | |
| | | Invest | igate in Threat Response | | | |

Investigate Threats

Step 1 In the navigation menu to the left, click **Threat Catalog** and **Detected** to see a list of threats reported on your network and prioritized by severity. Each card represents a different threat that will be grouped in alerts.

Figure 14:

| cisco Globa | al Threat Aler | ts Dashboard | Detections | Incidents | Integrations | Orchestration | Administration | Early access | ₽ \$~ | ad14e57fa4e \vee |
|---|----------------|---|---|-----------------------------------|------------------|---------------|--|--|----------------------|--------------------|
| Detections ~ Alerts New | | Detected Threa Threats that we dete | its ected on your n | etwork | | | | | | |
| Open Closed Threat Catalog Detected Suppressed Asset Groups Affected Suppressed Settings | 4 2 10 | ZeroAccess (S00 Botnet and rootkit with Last seen: Affected Assets: Alerts: Category: Critical Severity | 27) n click fraud capable 24 hours ago 1 1 Malware - botne | ility t | Threa | t Detail | WannaCry (S036 Disk encrypting malwa Last seen: Affected Assets: Alerts: Category: Critical Severity | 6) 15 days ago 2 1 Maiware - ransomware | s to spread itself u | sing the SMBv1 |
| | | njRAT (S0385) Malicious software for Last seen: Affected Assets: Alerts: Category: Critical Severity | remote control of 22 hours ago 9 1 Malware - remot | a target syster e access troja | m In Threa | t Detail | Emotet (S0367) Infection with exfiltration Last seen: Affected Assets: Alerts: Category: Critical Severity | on capability that targets bank 5 days ago 2 1 Malware - bot | ing credentials | Threat Detail |

- **Step 2** A specific type of threat might be involved in several alerts. There's a counter on the card indicating the number of alerts this specific type of threat is involved with and the number of assets affected by this threat.
- **Step 3** Global threat alerts threat intelligence provides references to relevant ATT&CK Tactics, Techniques, and Software entries.
- **Step 4** You have the option to adjust the threat's severity, according to your network-specific conditions and business needs.
 - Consequently, all **New** alerts that contain this type of threat will have their risk levels recalculated, weighting the new severity with asset value and confidence level.
 - Then, any change in risk level affects the relative ordering of New alerts.
 - For example, if you lower the threat's severity, the associated alert(s) risk level will be lowered, and the associated alert card(s) will appear lower in the list on the **Alerts** tab.
 - Click the drop-down list to adjust the threat's severity:

Figure 15:

| SMB Service Discovery (T1018) | Shlayer (S0402) | | | | |
|--|--|--|--|--|--|
| Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE vulnerability | Infection that can download additional malware such as droppers | | | | |
| Last seen: yesterday | Last seen: yesterday | | | | |
| Affected Assets: 2 | Affected Assets: 1 | | | | |
| Alerts: 1 | Alerts: 1 | | | | |
| Category: Attack Pattern - scanning | Category: Malware - dropper | | | | |
| Critical Severity ✓ High Severity Medium Severity | High Severity ~ | | | | |
| Low Severity Suppressed Solity | Cryptocurrency Miner (T1496) | | | | |
| File infecting modular malware | Software that uses your computing resources to mine cryptocurrencies | | | | |
| Last seen: 11 hours ago | Last seen: 21 hours ago | | | | |
| Affected Assets: 4 | Affected Assets: 3 | | | | |
| Alerts: 1 | Alerts: 1 | | | | |
| Category: Malware - file infector | Category: Tool - crypto miner | | | | |
| High Severity ~ | High Severity ~ | | | | |

Note

All other alerts that are no longer in the **New** status are not affected by a change in threat severity; they remain unchanged and stable, to ease investigation.

Asset Groups

- **Step 1** In the navigation menu to the left, click **Asset Groups** and **Affected** to see all the asset groups that have their traffic sent to global threat alerts. Each card represents a group of assets for which global threat alerts is reporting at least one alert.
- **Step 2** Determine how important or valuable the asset group is to your organization. You have the option to adjust the asset group's business value.
 - Consequently, all **New** alerts that affect this asset group will have their risk levels recalculated, weighting the new asset value with severity and confidence level.
 - Then, any change in risk level affects the relative ordering of New alerts.
 - For example, if you increase the asset group's business value, the associated alert(s) risk level will be increased, and the associated alert card(s) will appear higher in the list on the **Alerts** tab.
 - Click the drop-down list to adjust the business value of the asset group:

Figure 16:

| Detections ~ Alerts New | = 3 6 6 | Affected Asset Groups Affected asset groups that need your attention | |
|--|------------|--|--|
| Open Closed ~ Threat Catalog Detected Suppressed ~ Asset Groups Affected Suppressed | 0.0 | Web Servers Secure Network Analytics Ancestors: By Function / Servers Affected Assets: 1 Alerts: 1 Critical Value V High Value Medium Value | Catch All Secure Network Analytics Ancestors: no parent Affected Assets: 9 Alerts: 3 Medium Value ~ Group Detail |
| Settings | | Low Value Suppressed Cryo CI Secure Network Analytics Ancestors: Cryo-Users Affected Assets: 3 Alerts: 1 Medium Value ~ Group Detail | Cryogen Center Secure Network Analytics Ancestors: By Location / Room A Affected Assets: 1 Alerts: 1 Medium Value Group Detail |

Note All other alerts that are no longer in the **New** status are not affected by a change in threat severity; they remain unchanged and stable, to ease investigation.

I

Dashboard