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.

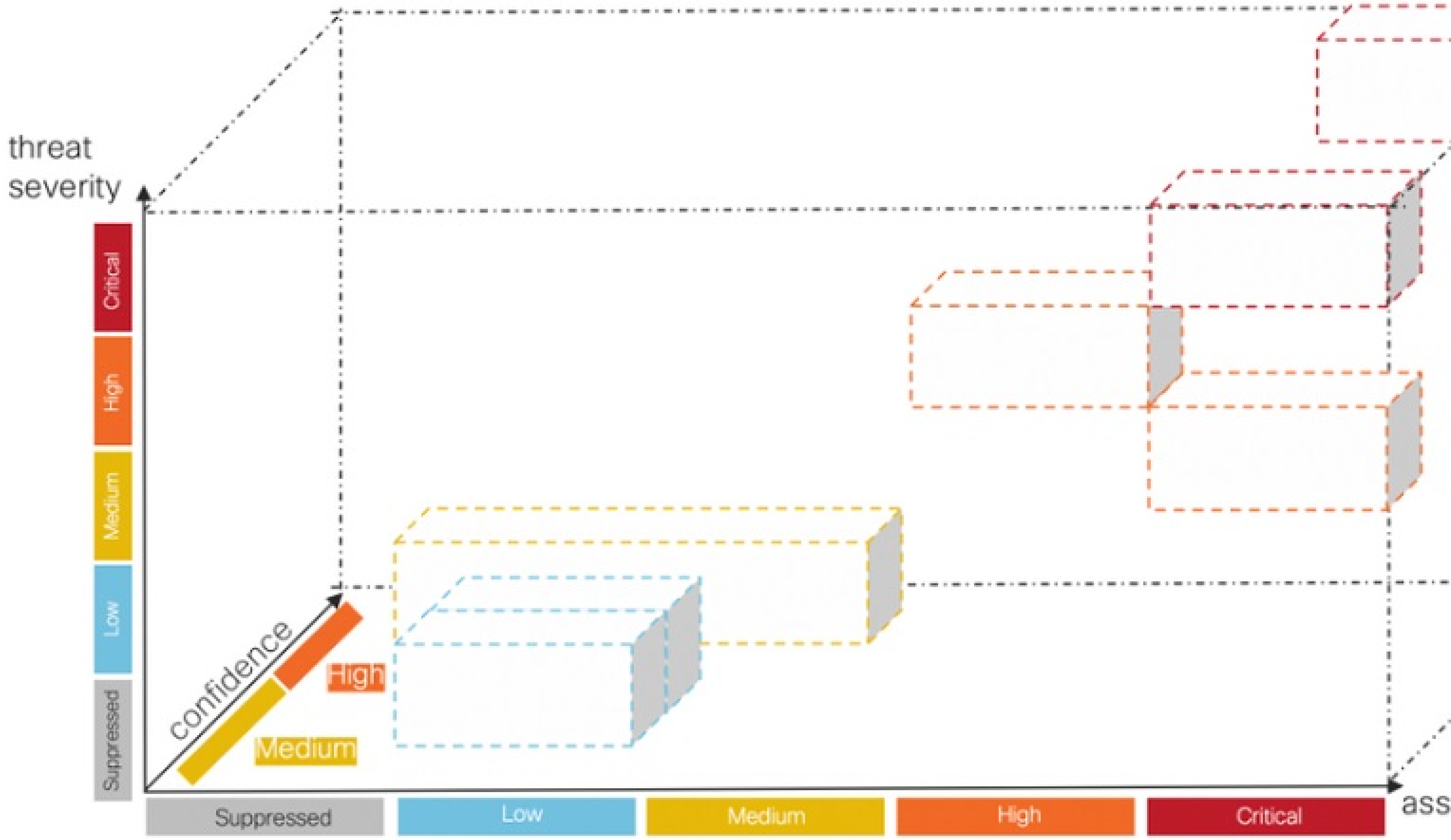
Using machine learning and a statistical modeling of networks, global threat alerts creates a baseline of normal activity and identifies anomalous traffic occurring within your network. It analyzes device behavior and web traffic to pinpoint command-and-control communications and data exfiltration.

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

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

Figure 1:



- **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.

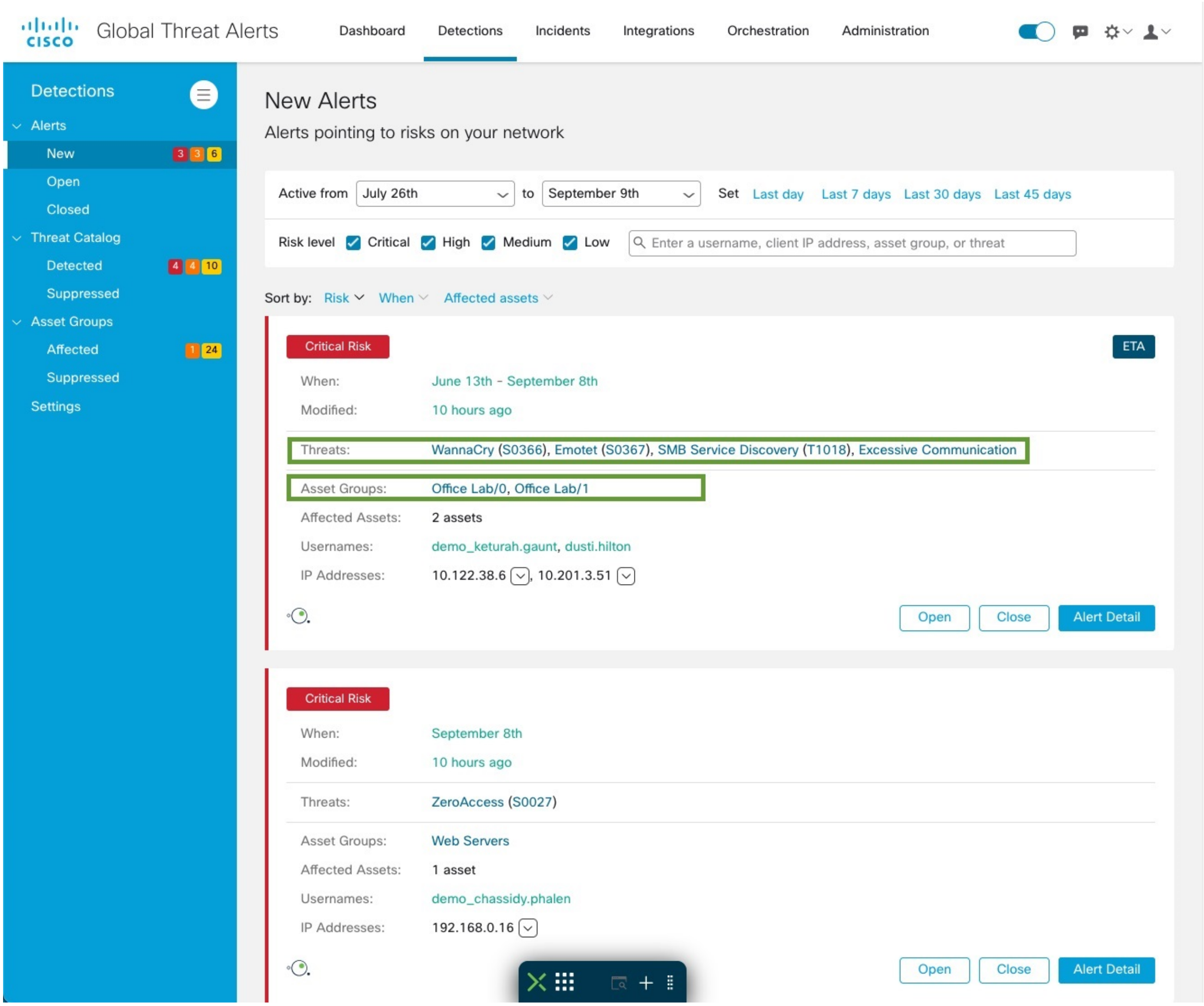
Our fusion algorithm uses these detections to identify clusters of similar threats and projections to calculate their risk levels. Our web portal then presents these as security alerts in a list prioritized by their risk levels. Each alert points to threats on your network and represents a natural unit-of-work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

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:



New Alerts

Alerts pointing to risks on your network

Active from July 26th to September 9th

Risk level ☑ Critical ☑ High ☑ Medium ☑ Low

Critical Risk

When: June 13th - September 8th
Modified: 10 hours ago
Threats: WannaCry (S0366), Emotet (S0367), SMB Service Discovery (T1018), Excessive Communication
Asset Groups: Office Lab/0, Office Lab/1
Affected Assets: 2 assets
Usernames: demo_keturah.gaunt, dusti.hilton
IP Addresses: 10.122.38.6, 10.201.3.51

Critical Risk

When: September 8th
Modified: 10 hours ago
Threats: ZeroAccess (S0027)
Asset Groups: Web Servers
Affected Assets: 1 asset
Usernames: demo_chassidy.phalen
IP Addresses: 192.168.0.16

- **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.

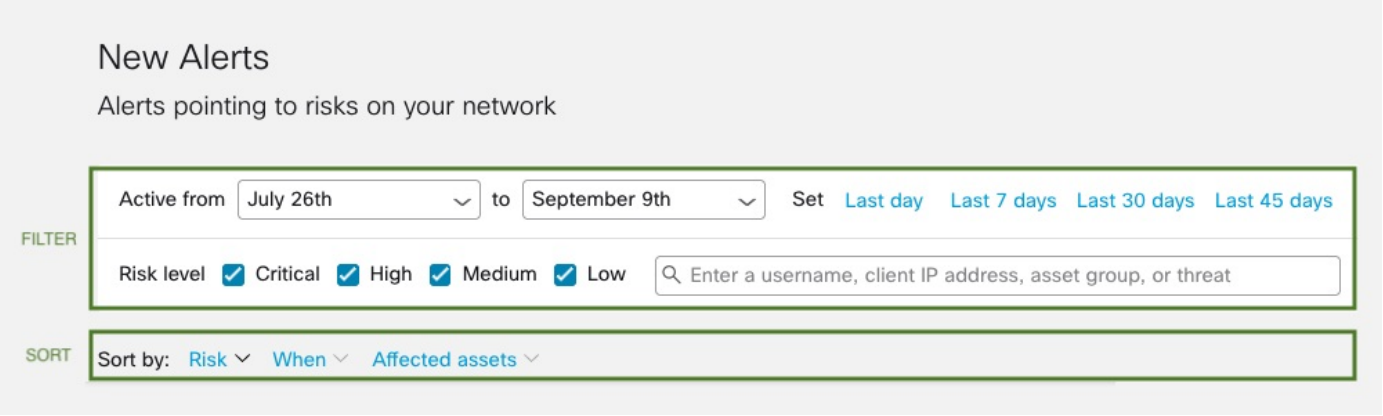
Step 2 Alerts with higher risk are ordered closer to the top of the list. Prioritize your analysis by responding to the alerts based on their risk level and investigating higher risk alerts first.

- 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

Alerts pointing to risks on your network

Active from: July 26th to September 9th

Risk level: ☑ Critical ☑ High ☑ Medium ☑ Low

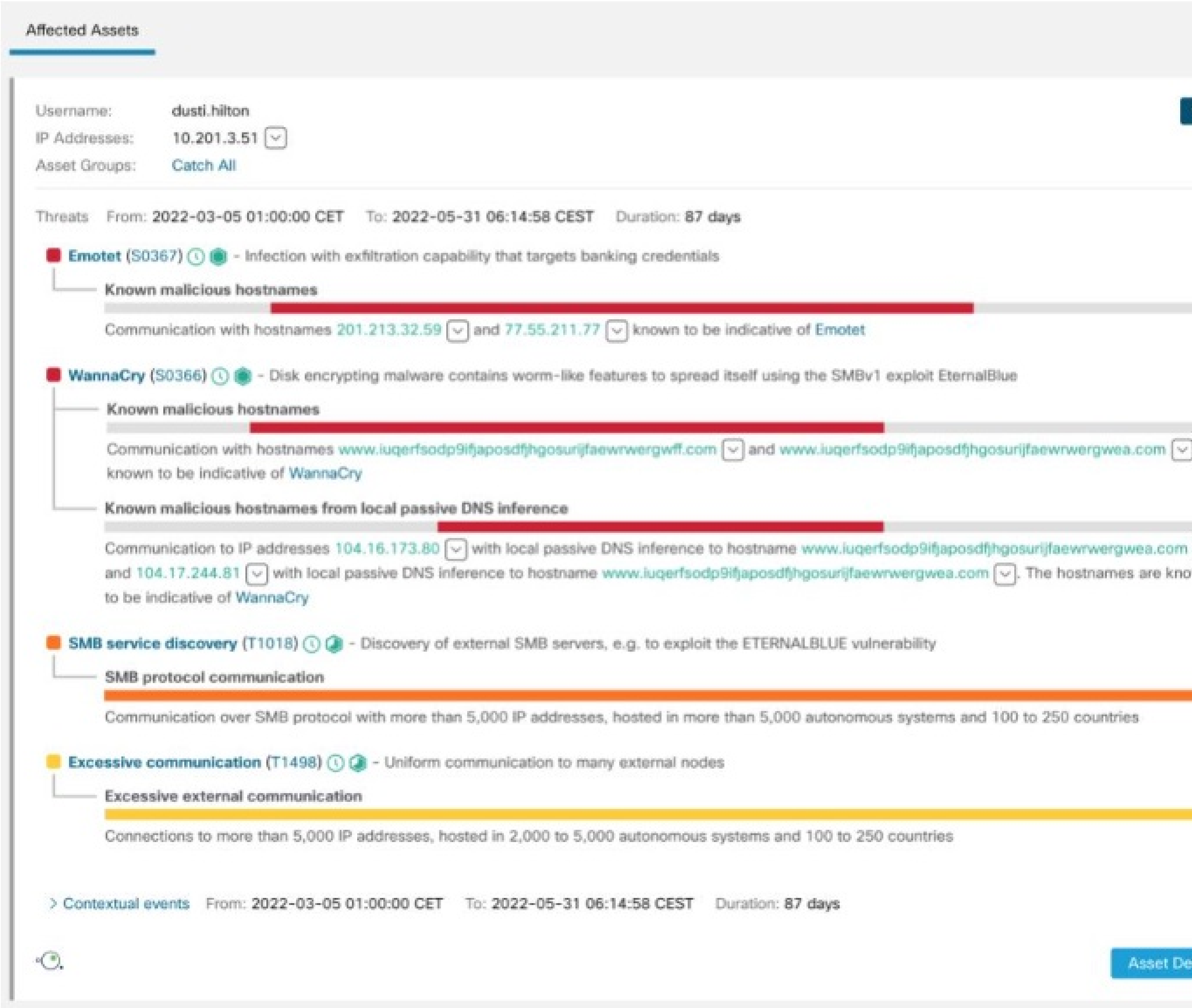
Sort by: Risk

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

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

Step 5 Click 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:



Affected Assets

Username: dusti.hilton

IP Addresses: 10.201.3.51

Asset Groups: Catch All

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

🟥 Emotet (S0367) - Infection with exfiltration capability that targets banking credentials

Known malicious hostnames

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

🟥 WannaCry (S0366) - Disk encrypting malware contains worm-like features to spread itself using the SMBv1 exploit EternalBlue

Known malicious hostnames

Communication with hostnames www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff.com and www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com known to be indicative of WannaCry

Known malicious hostnames from local passive DNS inference

Communication to IP addresses 104.16.173.80 with local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com and 104.17.244.81 with local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. The hostnames are kno to be indicative of WannaCry

🟧 SMB service discovery (T1018) - Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE vulnerability

SMB protocol communication

Communication over SMB protocol with more than 5,000 IP addresses, hosted in more than 5,000 autonomous systems and 100 to 250 countries

🟨 Excessive communication (T1498) - Uniform communication to many external nodes

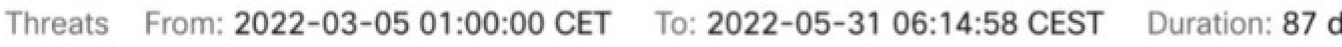
Excessive external communication

Connections to more than 5,000 IP addresses, hosted in 2,000 to 5,000 autonomous systems and 100 to 250 countries

> Contextual events From: 2022-03-05 01:00:00 CET To: 2022-05-31 06:14:58 CEST Duration: 87 days

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:

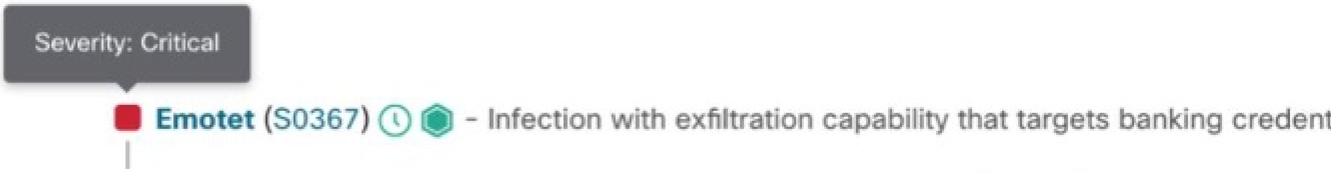


Threats From: 2022-03-05 01:00:00 CET To: 2022-05-31 06:14:58 CEST Duration: 87 d

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

- Severity

Figure 6:

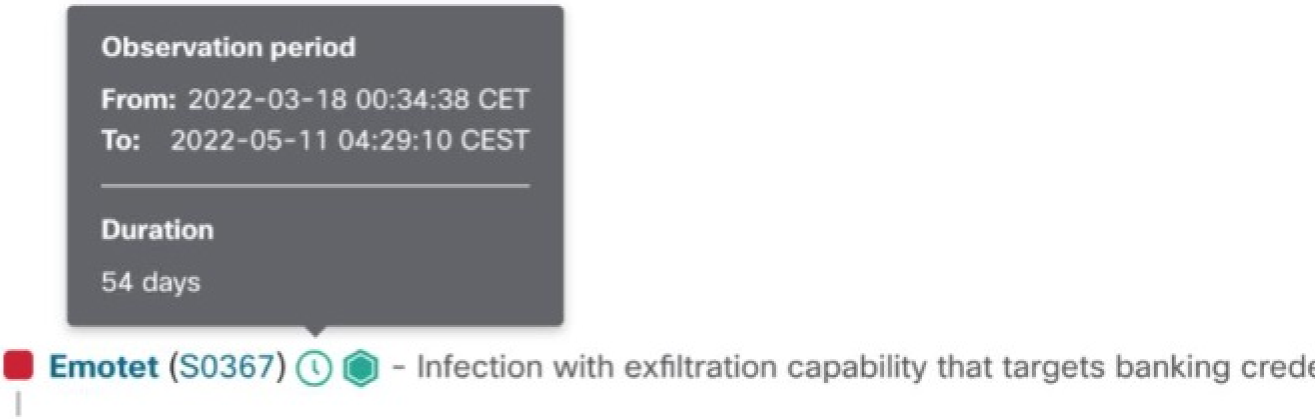


Severity: Critical

Emotet (S0367) - Infection with exfiltration capability that targets banking credent

- Observation period

Figure 7:



Observation period

From: 2022-03-18 00:34:38 CET

To: 2022-05-11 04:29:10 CEST

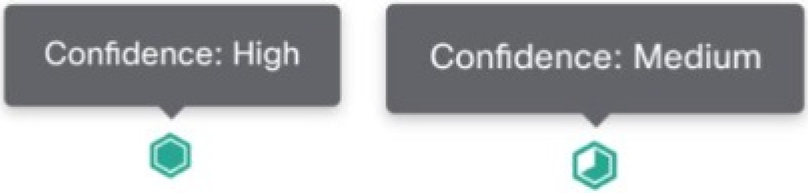
Duration

54 days

Emotet (S0367) - Infection with exfiltration capability that targets banking crede

- Confidence

Figure 8:

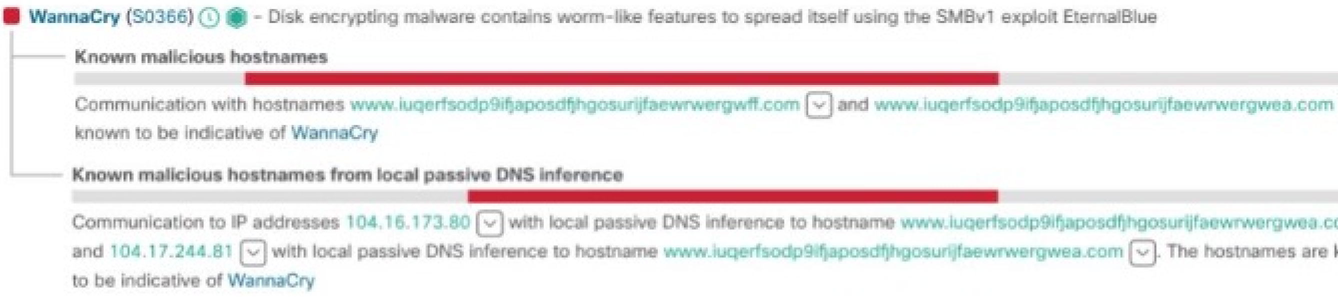


Confidence: High

Confidence: Medium

Each threat detection is backed by the security event(s) below it. Many of the events contain rich security annotations that provide the evidence which led to the creation of the event.

Figure 9:



WannaCry (S0366) - Disk encrypting malware contains worm-like features to spread itself using the SMBv1 exploit EternalBlue

Known malicious hostnames

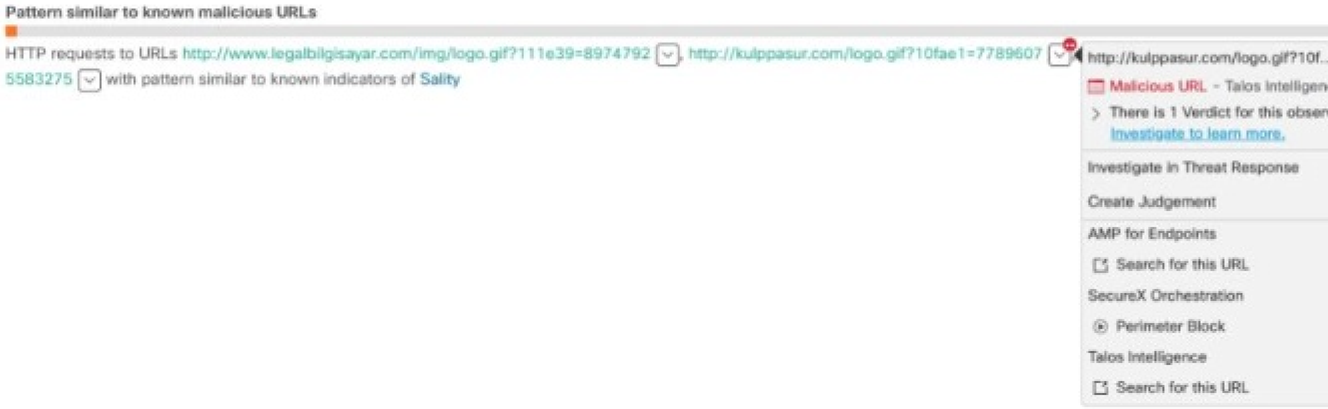
Communication with hostnames www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff.com and www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com known to be indicative of WannaCry

Known malicious hostnames from local passive DNS inference

Communication to IP addresses 104.16.173.80 with local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.c and 104.17.244.81 with local passive DNS inference to hostname www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. The hostnames are to be indicative of WannaCry

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:



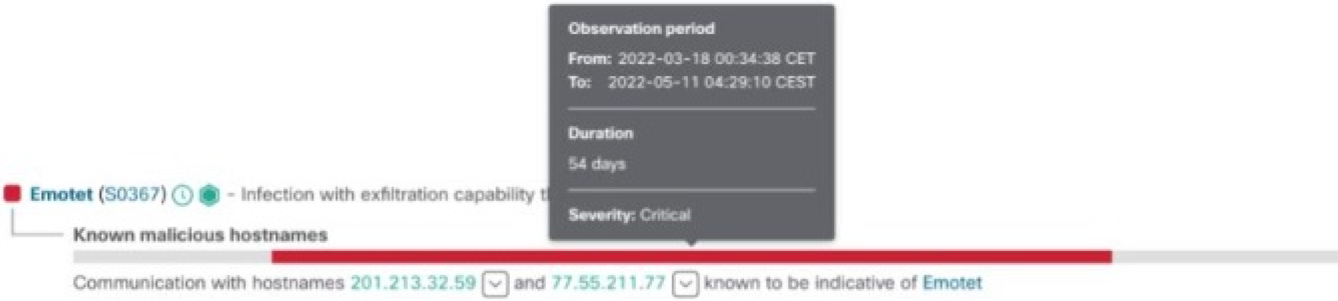
Pattern similar to known malicious URLs

HTTP requests to URLs http://www.legalbilgisayar.com/img/logo.gif?111e39=8974792, http://kulppasur.com/logo.gif?10fae1=7789607 5583275 with pattern similar to known indicators of Sality

http://kulppasur.com/logo.gif?10f...
Malicious URL - Talos Intelligen
There is 1 Verdict for this obser
Investigate to learn more.
Investigate in Threat Response
Create Judgement
AMP for Endpoints
Search for this URL
SecureX Orchestration
Perimeter Block
Talos Intelligence
Search for this URL

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:



Observation period

From: 2022-03-18 00:34:38 CET
To: 2022-05-11 04:29:10 CEST

Duration

54 days

Severity: Critical

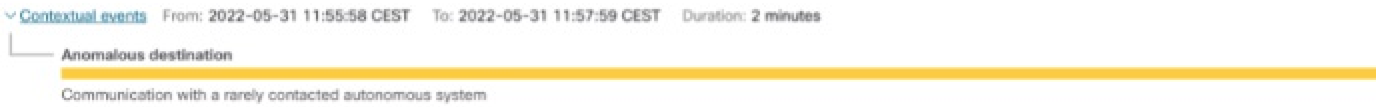
Emotet (S0367) - Infection with exfiltration capability t

Known malicious hostnames

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:



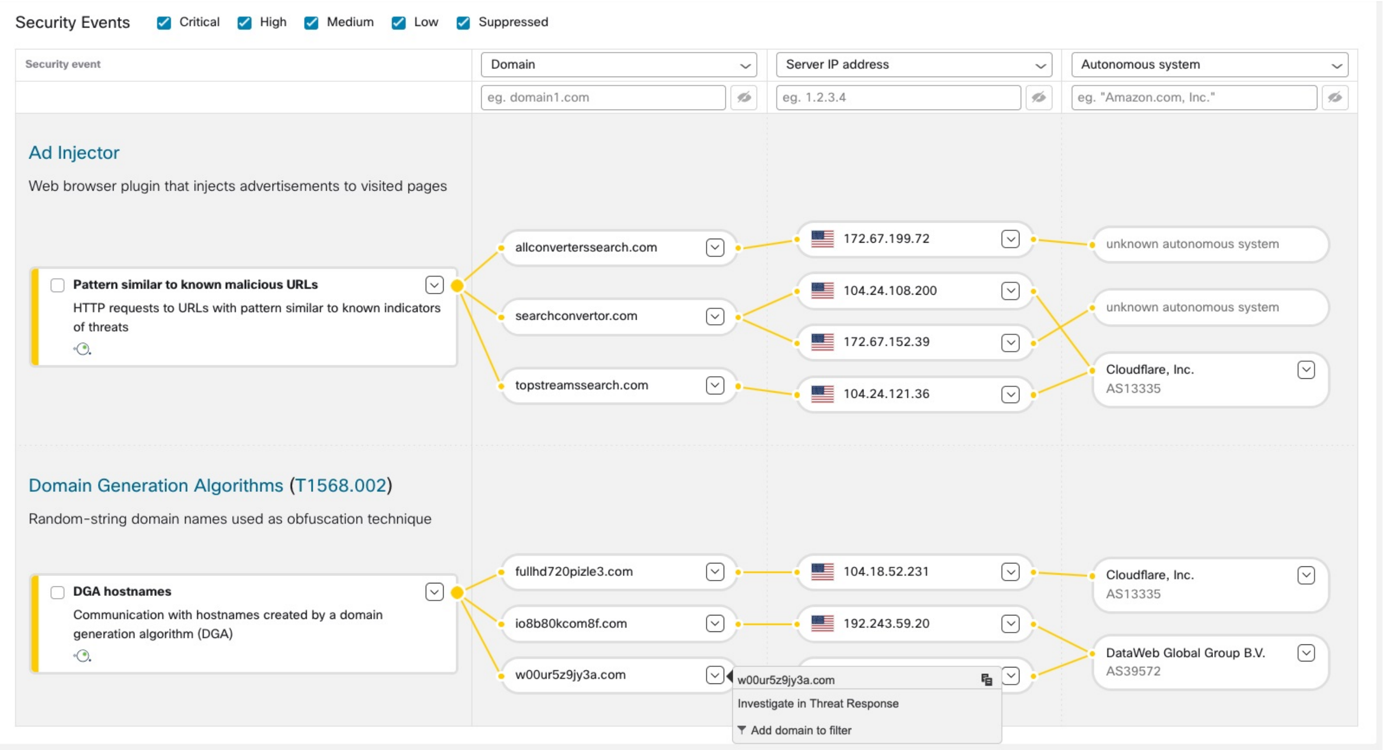
⌄ Contextual events From: 2022-05-31 11:55:58 CEST To: 2022-05-31 11:57:59 CEST Duration: 2 minutes

Anomalous destination

Communication with a rarely contacted autonomous 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:



Security Events ☑ Critical ☑ High ☑ Medium ☑ Low ☑ Suppressed

Security event	Domain	Server IP address	Autonomous system
	eg. domain1.com	eg. 1.2.3.4	eg. "Amazon.com, Inc."

Ad Injector

Web browser plugin that injects advertisements to visited pages

□ Pattern similar to known malicious URLs

HTTP requests to URLs with pattern similar to known indicators of threats

Domain Generation Algorithms (T1568.002)

Random-string domain names used as obfuscation technique

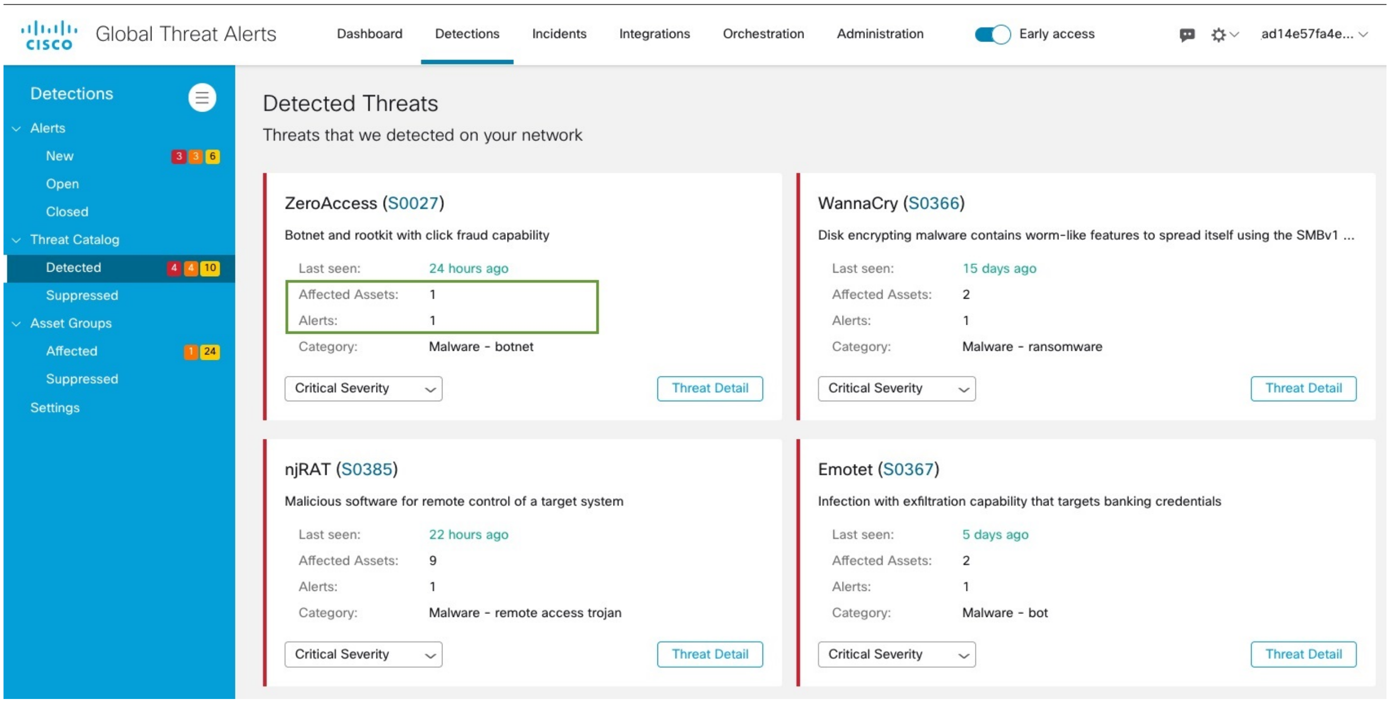
□ DGA hostnames

Communication with hostnames created by a domain generation algorithm (DGA)

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:



Detected Threats

Threats that we detected on your network

ZeroAccess (S0027)

Botnet and rootkit with click fraud capability

Last seen:	24 hours ago
Affected Assets:	1
Alerts:	1
Category:	Malware - botnet

WannaCry (S0366)

Disk encrypting malware contains worm-like features to spread itself using the SMBv1 ...

Last seen:	15 days ago
Affected Assets:	2
Alerts:	1
Category:	Malware - ransomware

njRAT (S0385)

Malicious software for remote control of a target system

Last seen:	22 hours ago
Affected Assets:	9
Alerts:	1
Category:	Malware - remote access trojan

Emotet (S0367)

Infection with exfiltration capability that targets banking credentials

Last seen:	5 days ago
Affected Assets:	2
Alerts:	1
Category:	Malware - bot

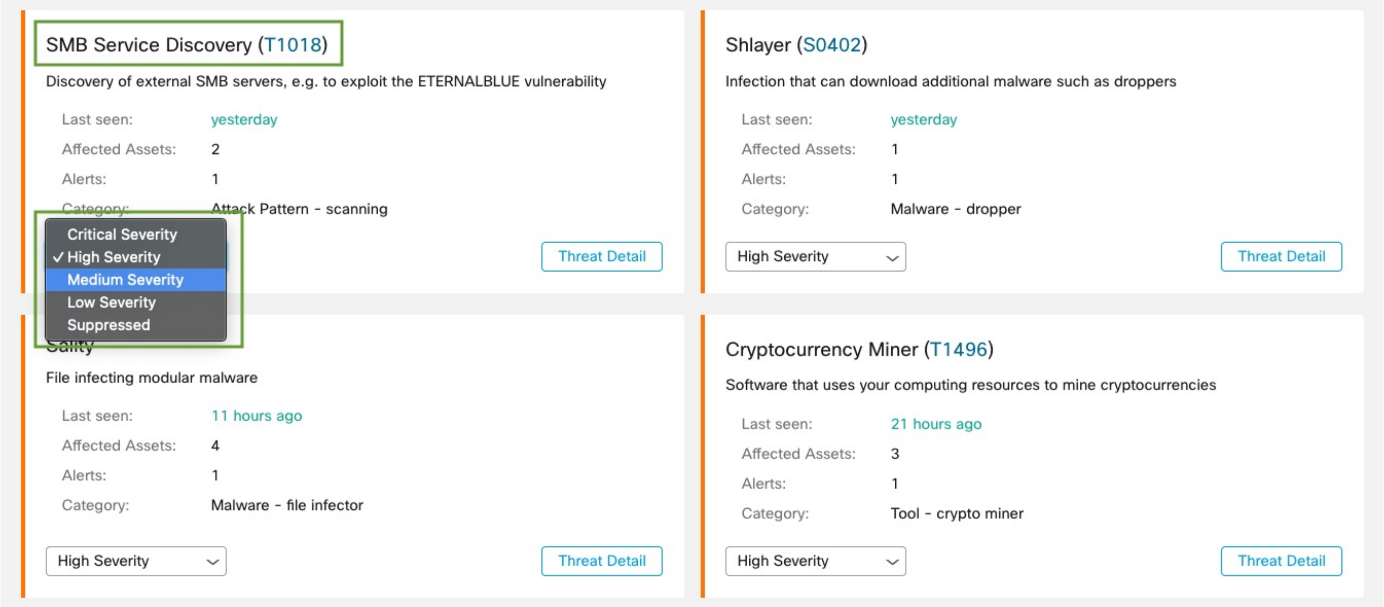
Step 2 A specific type of threat might be involved in several alerts. There's a counter on the card indicating the number of alerts this specific type of threat is involved with and the number of assets affected by this threat.

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)

Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE vulnerability

Last seen: yesterday
Affected Assets: 2
Alerts: 1
Category: Attack Pattern - scanning

Shlayer (S0402)

Infection that can download additional malware such as droppers

Last seen: yesterday
Affected Assets: 1
Alerts: 1
Category: Malware - dropper

Sality

File infecting modular malware

Last seen: 11 hours ago
Affected Assets: 4
Alerts: 1
Category: Malware - file infector

Cryptocurrency Miner (T1496)

Software that uses your computing resources to mine cryptocurrencies

Last seen: 21 hours ago
Affected Assets: 3
Alerts: 1
Category: Tool - crypto miner

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.

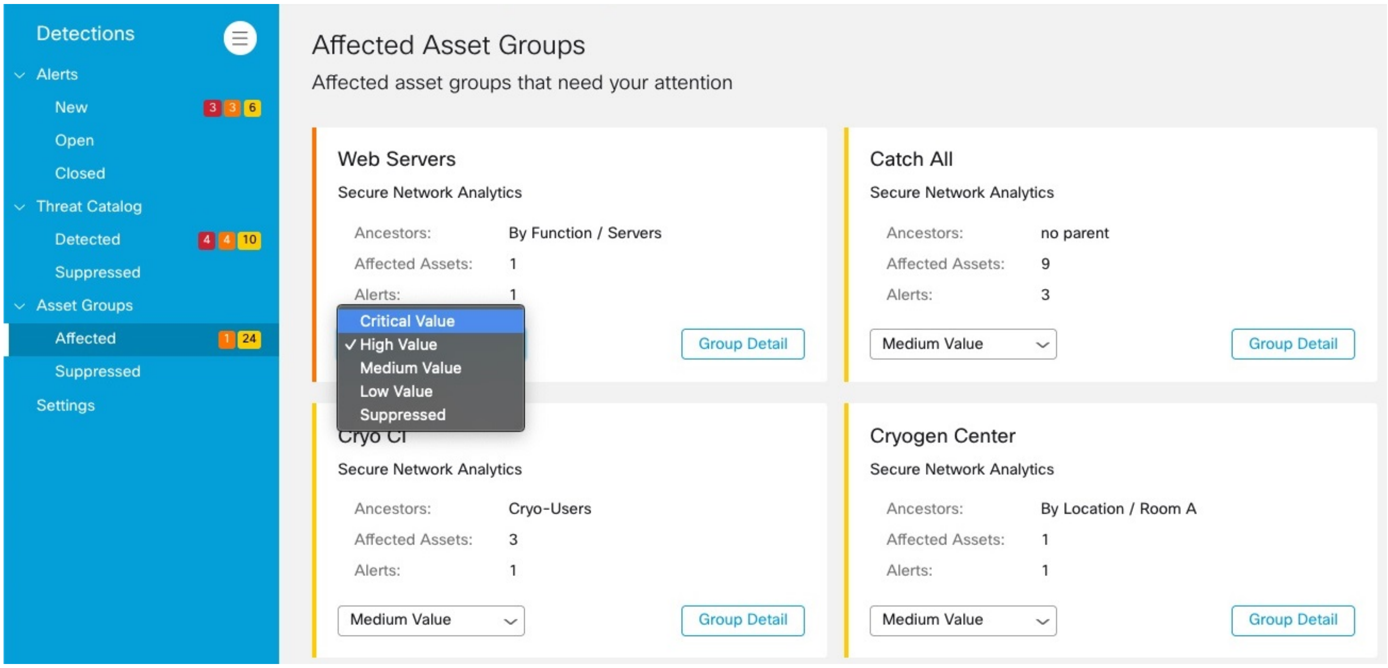
Asset Groups

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:



Affected Asset Groups

Affected asset groups that need your attention

Web Servers

Secure Network Analytics

Ancestors:	By Function / Servers
Affected Assets:	1
Alerts:	1

Catch All

Secure Network Analytics

Ancestors:	no parent
Affected Assets:	9
Alerts:	3

Cryo CI

Secure Network Analytics

Ancestors:	Cryo-Users
Affected Assets:	3
Alerts:	1

Cryogen Center

Secure Network Analytics

Ancestors:	By Location / Room A
Affected Assets:	1
Alerts:	1

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.