THREATQUOTIENT™

THREATQ™ AND CISCO

Technology Segment: Commercial Intelligence, EDR, Enrichment & Analysis, Sandbox

Maximizing Threat Intelligence ROI By Making It Actionable

Together, ThreatQuotient and Cisco offer a comprehensive approach to managing and leveraging threat data. This combination offers the intelligence to detect attacks before they launch, the visibility to protect access everywhere, and the authority to stop threats before connections are made.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

INTEGRATION HIGHLIGHTS

Provides threat analysis with detailed and historical indicator data.

Deep visibility into traffic both on and off network.

Helps security teams respond appropriately when investigating a threat.

CISCO INTEGRATIONS

Together, ThreatQuotient and Cisco offer a comprehensive approach to managing and leveraging threat data.

This combination offers the intelligence to detect attacks before they launch, the visibility to protect access everywhere, and the authority to stop threats before connections are made.

1. **Cisco AMP for Endpoints**

   Description: The ThreatQ integration with Cisco AMP for Endpoints enables bi-directional communication between the platforms, allowing indicators to be sent for blocking as well as allowing detection events to be ingested into ThreatQ.

   Use-Cases:

   - Bring detection events into ThreatQ, along with relevant hashes and other context.
   - Export hashes to an AMP for Endpoints application blocklist.
   - Search for sightings of malicious hashes, from within ThreatQ.

2. ## Cisco Threat Grid

Description: The ThreatQ integration with Cisco Threat Grid enables the submission of samples to the sandbox, as well as the retrieval of the detonation reports.

Use-Cases:

- Submit samples to be detonated in Threat Grid, directly from ThreatQ.
- Retrieve sample detonation reports from within ThreatQ.

3. ## Cisco Threat Response (SecureX)

Description: The ThreatQ integration with Cisco Threat Response enables threat collections to be exported to Threat Response, giving Threat Response incidents visibility into what ThreatQ knows about a given threat.

Use-Cases:

- Export malicious IOCs to Threat Response to be used to corroborate evidence within an incident.
- Export IOCs to Threat Response to be integrated with other Cisco products that utilize intelligence from Threat Response.

4. ## Cisco SecureX Orchestrator

Description: The ThreatQ integration with Cisco SecureX Orchestrator enables bi-directional workflow communication between Cisco & ThreatQ.

Use-Cases:

- Using ThreatQ as the single-source-of-truth; automatically perform IOC lookups to drive workflow decisions.
- Send valuable context back to ThreatQ so that connected services will have access to the most up to date information.
- Send context back into ThreatQ to drive workflows executed within ThreatQ.

5. ## Cisco Umbrella

Description: The ThreatQ integration with Cisco Umbrella enables analysts to investigate threats as well as enforce policies, directly from ThreatQ.

Use-Cases:

- Perform IOC lookups from within ThreatQ to find out what Cisco Umbrella knows about a given threat.
- Automatically or manually block threats directly from ThreatQ to decrease your response time.
- Bring security events/activities from Cisco Umbrella, into ThreatQ, in order to increase visibility across your organization.

6. ## Cisco Firepower

Description: The ThreatQ integration with Cisco Firepower enables analysts to automatically block connections from known malicious IOCs.

Use-Cases:

- Automatically block malicious IOCs.

7. ## Cisco Threat Intelligence Director (TID)

Description: The ThreatQ integration with Cisco TID enables analysts to automatically block known malicious IOCs.

Use-Cases:

- Automatically block malicious IOCs.

8. ## Cisco AMP for Endpoints CDF

Description: The Cisco AMP for Endpoints CDF enables a ThreatQ user to ingest events from Cisco AMP for Endpoints.

Use-Cases:

- Alerts are brought into ThreatQ to be correlated with external intelligence, and to be used within investigations.

9. ## Cisco AMP for Endpoints Connector

The Cisco AMP for Endpoints Integration for ThreatQ allows a user to automatically export hashes to a Cisco AMP for Endpoints blacklist.

10. ## Cisco AMP for Endpoints Operation

This operation allows a ThreatQ user to execute 2 actions on their Cisco AMP for Endpoints instance. The first action allows users to submit a SHA-256 hash from ThreatQ to a Cisco AMP for Endpoints application block list. The second action allows users to query their Cisco AMP for Endpoints events for any hits on a specific SHA-256 hash.

11. Cisco Threat Grid

The ThreatQuotient for ThreatGrid Application pulls indicators from the Cisco Threat Grid API, both cloud-based and appliance-based. Understand and prioritize threats faster. Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

Bring your Threat Grid analysis data into ThreatQ as an internal intelligence source. The Cisco Threat Grid CDF is a sandbox which allows the detonation of samples to generate analysis reports. The Cisco Threat Grid CDF for ThreatQ enables a user to ingest their organization's sample analysis reports from Threat Grid. These samples can be filtered down by their threat score, so you are able to ingest only the detonations that your organization deems important to track.

The CDF provides the following feeds:

- Cisco Threat Grid - ingests analyses as Report Objects within ThreatQ. Any metadata surrounding the reports will be included, as well as related IOCs, related TTPs, and their relevant attribution.
- Get Analysis (Supplemental) - fetches the full analysis report JSON from Threat Grid's API.

The integration ingests the following system object types:

- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes
- TTPs
  - TTP Attributes

12. Cisco Threat Grid Operation

The ThreatQuotient for Threat Grid Operation gives users the ability to submit files, URLs, and domains to Threat Grid's analysis engine, directly from ThreatQ. Understand and prioritize threats fasterThreat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

13. Cisco Threat Response (SecureX) - Enrichment

The Integration enables a ThreatQ User to enrich IOCs with judgements and other context from Cisco Threat Response (SecureX).
Use Case: Auto Enrichment on a schedule.
Notes: Enrichment comes from all modules that Integrate with Cisco Threat Response, It Includes Cisco Threat Grid, Cisco RAT DNS feed, Cisco Umbrella and more.
Checkout:

- Cisco Threat Response (SecureX) Exporter
- Cisco Threat Response (SecureX) Operation

14. Cisco Threat Response (SecureX) Exporter

The Cisco Threat Response Exporter for ThreatQ allows a ThreatQ user to export indicator/observable judgements from ThreatQ to Cisco Threat Response via the Cisco Threat Intelligence API (CTIA)
Notes: Due to an API limitation, the CTIA (Cisco Threat Intelligence API) will only allow TLP amber and/or red. As a result, all indicators being sent over to Cisco AMP will receive an Amber TLP (unless TLP red is applied in ThreatQ) This integration will push judgements to your organization's private instance. This will not publish information to Cisco's public sources.
Checkout:

- Cisco Threat Response (SecureX) Enrichment
- Cisco Threat Response (SecureX) Operation

15. Cisco Threat Response (SecureX) Operation

The Cisco Threat Response Operation for ThreatQuotient enables a user to query Cisco Threat Response for contextual information on a given indicator of compromise.

Checkout:

- Cisco Threat Response (SecureX) Exporter
- Cisco Threat Response (SecureX) Enrichment

16. Cisco Umbrella

As the industry's leading Secure Internet Gateway, Cisco Umbrella provides the first line of defense against threats on the Internet wherever users go. Leveraging their global infrastructure, which resolves over 120 billion Internet requests a day, Umbrella is able to see where imminent attacks are being staged. It also delivers complete visibility into Internet activity across all locations, devices and users, and blocks threats before they ever reach your network or endpoints. Additionally, Umbrella is an open platform and integrates easily with your existing security stack and delivers live threat intelligence about current and emerging threats. By analyzing and learning from Internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for attacks, and proactively blocks requests to malicious destinations before a connection is even established — without adding any latency for users. With Umbrella, you can stop phishing and malware infections earlier, identify already infected devices faster and prevent data exfiltration.

INTEGRATION HIGHLIGHTS

- Provides threat analysts with detailed and historical indicator data.
- Deep visibility into traffic both on and off network.
- Helps security teams respond appropriately when investigating a threat.

INTEGRATION USE CASES

- Add malicious domains curated by the ThreatQ platform to Umbrella domain lists for blocking.
- Use Umbrella's passive DNS data to query a domain or IP address' historical record.
- Use Umbrella Investigate's integration with Cisco Threat Grid to uncover file hashes associated with malware campaigns and build out a full view of an attacker's Internet infrastructure.
- Pull in domain tags, security scores and other metadata associated with domains and IP addresses.
- Automatically send IP Addresses, FQDNs and URLs to critical infrastructure for blocking.

ABOUT THREATQUOTIENT™

ThreatQuotient 's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit www.threatquotient.com.

ABOUT CISCO

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. At Cisco, customers come first and an integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success.

For more information, visit www.cisco.com.