THREATQUOTIENT

USE CASE

# Alert Triage

## The Challenge

Analysts are inundated by the number of alerts that require human attention, generated by noisy SIEM rules and default defense infrastructure.

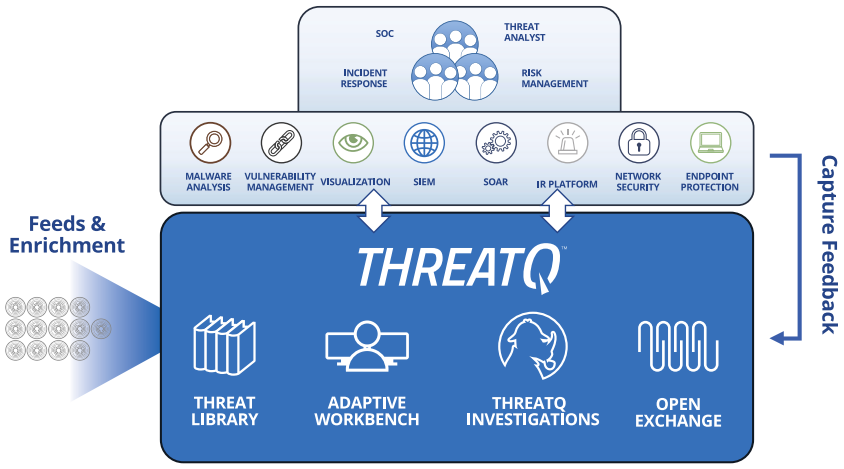
In an attempt to reduce the volume and velocity of security alerts they must tackle on a daily basis, analysts apply external threat data and threat intelligence feeds directly to the SIEM, but challenges continue for two main reasons. First, the amount of external threat data is staggering. Sending all of this data directly to the SIEM for correlation results in tons of non-contextual alerts, each of which requires significant work by an analyst to research. Second, there is a lack of decision support capabilities in current tools to provide additional context and understanding to determine relevance, before applying threat intelligence feeds directly to the SIEM. Prioritization is imperative to focus and determine the appropriate next actions.

## Our Approach

Stop the useless alerts before they happen by ONLY feeding threat intelligence that is relevant to the organization into the SIEM for correlation. Machine-to-machine communication allows the SOC analyst to work within their chosen tool, and still have impact on the continuous tuning of the company's intelligence.

For alerts in the 'gray zone' of importance (medium-high, but not high/very high priority), simplify triage with a tool that enables visualization and collaboration.

For high priority alerts, include the ability to import alerts into an investigation for visual associations and understanding, and to perform analysis and engage with various collaborators as needed.



*For alerts in the 'gray zone' of importance (medium-high, but not high/very high priority), simplify triage with a tool that enables visualization and collaboration.*

In an adjacent workflow within the SIEM where the analyst lives, gain the ability to import highly relevant investigation alert data. Most SIEMs allow three to five additional pieces of context to accompany an indicator of compromise (IOC). Including threat score, IOC source(s), existing ticket numbers and outcome, adversary attribution, etc. will allow an analyst to make very quick and accurate triage decisions.

Learn from and reduce false positives automatically and improve the quality of alerts. If a false positive does slip through, simple feedback can allow for automated tuning of the threat repository. Likewise, the ability to build more accurate SIEM rules based on threat intelligence directly improves the quality of future alerts.

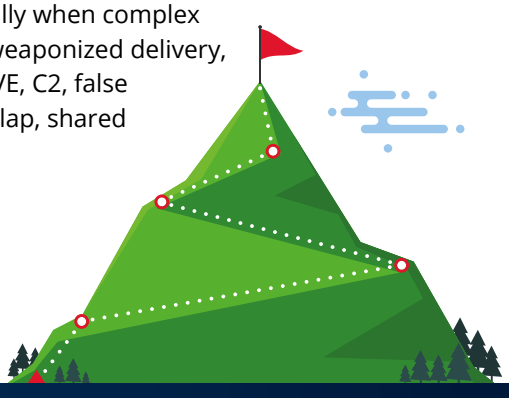
More effectively manage alert triage spikes when a wave of new STIX intelligence hits the sensors. By automatically ingesting the STIX package and transferring that text into the ThreatQ Investigations visualization, an analyst can digest that shared intelligence and take immediate actions.

## How ThreatQ meets the Alert Triage Challenge

- **Customer-defined Scoring:** Prioritize threat data automatically, understand why it is relevant and take action faster and with greater confidence.
- **Watchlist:** Add specific IoCs, adversaries or other threat-related data to your dashboard to highlight changes.
- **Threat Library Search:** Quickly research and understand context behind possible threats by keyword, attribute and object name. Group and pivot on associated data and quickly take bulk actions across a full group of data.
- **Open Exchange:** Integrate ThreatQ with existing security tools, teams and workflows through standard interfaces to extend their value, knowledge and efficacy.

## Outcomes

- Improved accuracy of alerts.
- Greater focus — get to the alerts that matter faster, by eliminating the ones that do not.
- Faster investigation response time.
- Better decision making.
- Accelerated resolution — close security alerts more quickly and accurately.
- Instant understanding with visualization of alerts and context. A picture is worth 1,000 words, especially when complex relationships exist (weaponized delivery, malware dropper, CVE, C2, false flags, adversary overlap, shared infrastructure, etc.).



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**.