THREATQUOTIENT

USE CASE

Vulnerability Management

The Challenge

It is simply impossible to patch and mitigate every software vulnerability present in an enterprise network.

Historically, organizations would prioritize mitigation based on limited and inward-facing data:

- Server versus workstation
- Employee role
- Asset criticality
- Vulnerability score
- Patch availability

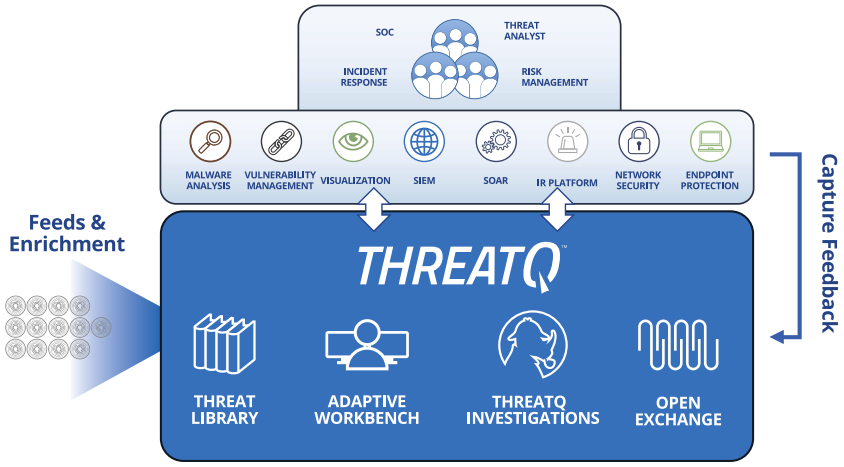
Despite this level of prioritization, patching remains one of the most time-consuming security operations tasks. This approach also has limited effectiveness because it does not take into account knowledge of how that vulnerability is actively being exploited in the wild, and the risks associated by those adversaries leveraging it to a company's specific environment.

Our Approach

A vulnerability is only as bad as the threat exploiting it and the impact on the organization. Security teams must take a risk-based approach to prioritizing vulnerabilities with knowledge about how vulnerabilities are being exploited.

ThreatQ allows security teams to focus their resources where the risk is greatest through the following three steps:

1. Understand the threats and which vulnerabilities threat actors are leveraging to determine relevance to the organization's environment and prioritize which vulnerabilities to address first. For example, a vulnerability related to a specific adversary campaign and IOCs that have been seen in an organization's SIEM and/or ticketing system should be addressed



Security teams must take a risk-based approach to prioritizing vulnerabilities with knowledge about how vulnerabilities are being exploited.

immediately. A vulnerability that has related threats and IOCs but they have not been known to target the organization's specific industry should be watched but is a lower priority. A vulnerability with no known adversaries using it or associated IOCs may indicate it is not being exploited in the real world yet, and can be deprioritized for now.

2. Overlap adversaries that target the company with CVEs the adversaries use, historical victimology targets and vulnerability scan results for those targets to create a superior risk profile.

3. Reassess and re-prioritize on a continuous and ongoing basis as adversaries change tactics, techniques and procedures (TTPs), systems and applications evolve, and their usage within the organization's environment does as well.

How ThreatQ meets the Vulnerability Management Challenge

- **Customer-defined Scoring:** Prioritize threat data automatically, understand why it is relevant and take action faster and with greater confidence.
- **Open Exchange:** Integrate ThreatQ with existing security tools, teams and workflows through standard interfaces to extend their value, knowledge and efficacy.
- **Threat Data Aggregation:** Create a single source of truth based on correlated, normalized and de-duplicated intelligence data and events across all tools and sources.
- **Threat Library:** Store global and local threat data in a central repository to provide relevant and contextual intelligence that is customized and prioritized for your unique environment.
- **Unstructured Data Import:** Parse and perform deep searching on documents and intelligence reports for threat data and clues as to the meaning of threats.

Outcomes

- Better situational awareness of attackers, their motivations and one's own environment.
- Clear priorities on what actions to take first to address which vulnerabilities.
- Ability to focus on the vulnerabilities that are the most relevant based on the organization's risk profile.
- A superior risk profile based on deeper insights into adversaries, their tactics, techniques and procedures (TTPs) and relevance to the organization.
- Better investment and resource decisions.

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**.