THREATQUOTIENT

USE CASE

Threat Hunting

The Challenge

Analysts use threat hunting to identify nefarious activity that has not triggered a sensor grid alert as well as potential hopping points an attacker might leverage in the future. While great in theory, there are several challenges to threat hunting. Many security teams don't know where to begin because they lack the ability to prioritize threats for relevance to their environment. Threat hunting also requires specific knowledge and expertise which limits the practice to a few highly skilled analysts. It is also difficult to see the big picture of what is happening across the environment when security teams and tools operate in silos.

When analysts do gain access to what they need, they must quickly find indicators that might reveal adversaries that are staying below the radar — either bending Remote Function Call (RFC) protocols or organizational policy thresholds without raising alerts. They also must be skilled at connecting historical attacks with other open source resources to understand an attacker's tactics, techniques and procedures (TTPs) and how they might move laterally when inside the environment. It is extremely time consuming to sift through logs manually to determine which are relevant and to correlate logs with massive volumes of external threat intelligence and other internal data to identify malicious activity. Organizations can end up with a few high-value resources spending inordinate amounts of time potentially chasing ghosts.

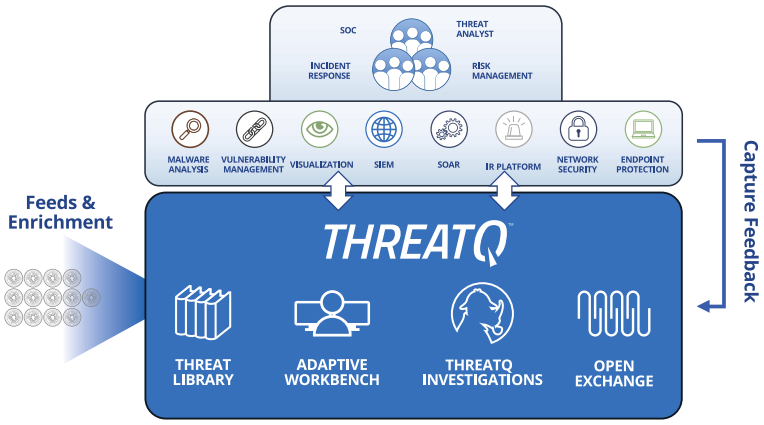
The goal of threat hunting is to mitigate the risk once an adversary infiltrates the network.

A New Approach

The goal of threat hunting is to mitigate the risk once an adversary infiltrates the network. To be effective, threat hunting must start with the threat. The ThreatQ Threat Library includes the ability to centralize and prioritize vast amounts of threat data from external and internal sources so that analysts can automatically determine the highly important items to hunt for within the environment.

ThreatQ Investigations allows analysts to conduct investigations collaboratively to search for and compare indicators across infrastructure and find matches between high-risk indicators of compromise (IOCs) and internal log data that indicate possible connections.

Once a match is discovered, analysts can slowly cast the net wider and identify second-tier indicators and attributes (i.e., malware associations, adversary relationships, similar event indicators, etc.).



These capabilities enable analysts to engage in threat hunting and follow the prescribed lifecycle, similar to that of any scientific experiment, as illustrated in these two examples.

EXAMPLE #1

1) **Identify a problem:** APT 'xyz' routinely infects my organization
2) **Create a hypothesis:** APT 'xyz' leverages DNS tunneling to exfiltrate data
3) **Gather relevant logs:** DNS egress logs
4) **Perform experiment:** look for anomalies and trends
5) **Refine data:** pivot around data to narrow the possibilities

Conclusion: develop DNS tunneling signatures to search for large DNS sessions during off-peak hours

EXAMPLE #2

1) **Identify a problem:** APT 'xyz' routinely infects my organization
2) **Create a hypothesis:** APT 'xyz' registers new domains 24 hours before sending new spearphish attacks
3) **Gather relevant logs:** cross-reference historical attack C2 FQDN hosting the malware download site with respective email registrant
4) **Perform experiment:** look for patterns: same email registrant, doppelganger email registrants, etc.
5) **Refine data:** pivot around data to narrow possibilities

Conclusion: APT 'xyz' uses a small subset of email registrants and frequently makes small spelling adjustments to register new malware download sites (e.g. John.Smith@gmail[dot]com -> Johnny.Smith@gmail[dot]com -> JSmith@gmail[dot]com). Develop signature in DomainTools to notify the team of similar email registrants.

How ThreatQ meets the Threat Hunting Challenge

- **Customer-defined Scoring:** Prioritize threat data automatically, understand why it is relevant and take action faster and with greater confidence.
- **Related Data:** Create relationships that can be used to build a holistic picture of an adversary, campaign, TTP, etc.
- **Operations:** Enrich threat intelligence data by adding attributes, as well as related indicators, from third party security services and security tools running in your environment, both commercial and open source.
- **Exports:** Output indicators and other intelligence objects from the Threat Library into security tools, allowing them to leverage curated threat intelligence for improved defenses.
- **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.

Outcomes

- Proactively block similar attacks in the future by developing a signature, or identifying new IOCs to detect and block depending on confidence rating.
- Adjust corporate policy to align with new defense rules/signatures.
- Achieve true fusion analysis, leveraging the intelligence and understanding of teams and tools across the organization.
- Develop better intelligence collection methodologies.
- Develop better intelligence practices.
- Find and stop evil before the attack.
- Mitigate risk when an adversary infiltrates infrastructure.

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**.