THREATQUOTIENT

USE CASE

# Spear Phishing

## The Challenge

Spear phishing emails contain a wealth of hidden evidence that can be used to track and understand the methods used by attackers to target the organization. By extracting that information, analysts can better understand what to look for to identify other users that may have succumbed to the trick.

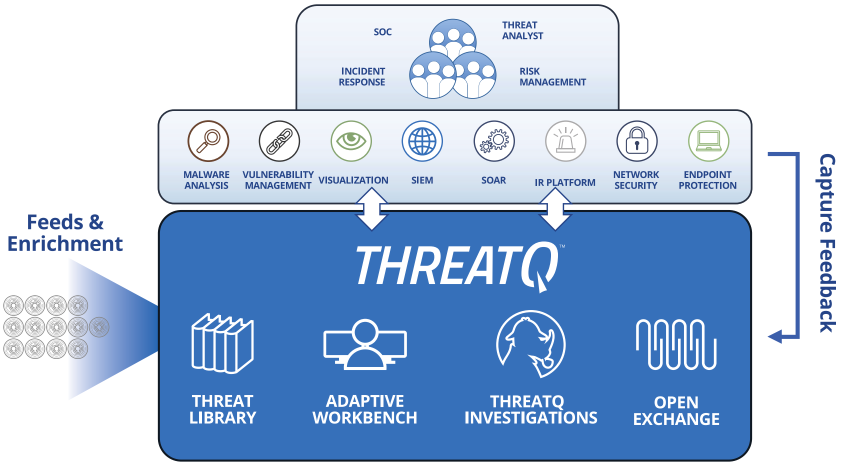
Armed with this evidence, analysts can discover associations between multiple spear phishing messages to understand a wider campaign that can be underway. Identifying malware samples across campaigns, and associating them with adversary profiles (and therefore intentions) notably improves the ability to respond.

Conducting this level of analysis can be difficult and laborious. Typically, analysts must discover these associations by manually sifting through messages and correlating the information they discover about the campaign with external data on adversaries and their methods.

## Our Approach

ThreatQ simplifies the process of parsing and analyzing spear phish emails for prevention and response. With a centralized Threat Library that aggregates all the external threat data organizations subscribe to along with internal threat and event data for context and relevance, analysts are in a position to begin to analyze and determine which emails to focus on.

Recipients of suspicious emails forward the email to an inbox that ThreatQ monitors continuously. Comparing indicators from the email against the data in the Threat Library, ThreatQ determines high risk emails versus low risk, allowing prioritization and noise reduction.



*ThreatQ automatically performs rear-view mirror searches on email logs using SMTP-specific indicators of compromise.*

On high-priority items, ThreatQ automatically performs rear-view mirror searches on email logs using SMTP-specific indicators of compromise (IOCs) — email subject, email sender, email filename/ attachments. Analysts are able to identify spear phish attacks that might have fallen through the cracks because they were not identified as malicious at the time.

Going a step further, analysts can query to identify all the spear phish recipients and then overlap those findings with vulnerability scan results to determine the scope and help accelerate response and containment.

## How ThreatQ meets the Spear phishing Challenge

- **Spear Phish Parser:** Automatically import and parse spear phish emails to identify threat data with intelligence value.
- **Events:** Track and analyze events to assess their severity, relevance and relationship to broader campaigns.
- **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.
- **Customer-defined Scoring:** Prioritize threat data automatically, understand why it is relevant and take action faster and with greater confidence.

## Outcomes

- Triage spear phishing faster and more effectively based on analyst familiarity of adversary TTPs.
- Improved spear phish attribution.
- Increased understanding of the environment and susceptibility to spear phish attacks.
- Proactive protection against spear phish attacks.

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**.