THREATQUOTIENT

CASE STUDY

The U.S. Department of Defense Arms and Unifies Cyber Warfighters through Shared Threat Intelligence with ThreatQ

Overview

Today's defenders are faced with new obstacles, seemingly daily, that aim to derail and prevent them from successfully carrying out their mission. In the cyber arena, these obstacles are not only growing, but also changing at a rapid pace. Adversaries are constantly evolving and finding new ways to try to inflict their desired result. For example, defenders must be hyper-vigilant of threat actors connecting to internet-accessible assets, breaching supply chains and leveraging ransomware to conduct malicious cyber activity against critical infrastructure essential to the missions of U.S. federal government agencies.

A host of tools have been made available to arm the cyber warfighter, from endpoint detection and threat hunting to network monitoring and incident response. Yet, defenders are still at a disadvantage, often finding themselves:

- Overloaded with data and alerts
- Mired in the complexity of juggling multiple tools to collect necessary information
- Forced to make a determination of a threat's validity without a complete picture or context
- Unable to easily share threat data and context to accelerate detection and response
- And, in some cases, undermanned

The ThreatQ Platform

The ThreatQ platform accelerates security operations through streamlined threat operations and management. The integrated, self-tuning Threat Library, Adaptive Workbench, and Open Exchange allow organizations to aggregate data, quickly understand and prioritize threats, make better decisions and automate the right intelligence to the right tools at the right time to accelerate detection and response. ThreatQ Data Exchange makes it easy to set up bidirectional sharing of any and all intelligence data within the ThreatQ platform and scale sharing across many teams and locations. ThreatQ Investigations serves as a virtual cybersecurity situation room designed for collaborative threat analysis, shared understanding and coordinated response.

ACCELERATE SECURITY OPERATIONS BY AUTOMATING REAL-TIME THREAT SHARING:

Instantly share intel on known threats

Enforce without human intervention for known threats

Automatically prioritize information from internal and external threat intelligence and enrichment sources

Integrate with existing infrastructure enforcement technologies

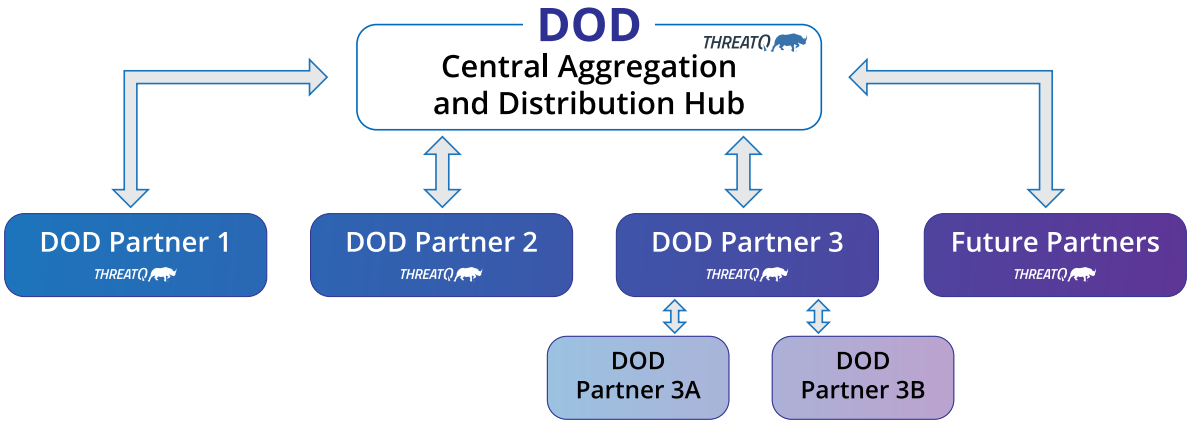
The ThreatQ platform works with existing processes and technologies and applies a threat-centric approach to security operations to support a variety of use cases beyond threat intelligence management, including threat hunting, incident response, spear phishing, alert triage and vulnerability management.

Having been granted Authority to Operate (ATO) by the Defense Information Systems Agency (DISA) at the Department of Defense Information Network (DoDIN) level as part of the Host Based Security System (HBSS) Infrastructure, allows the ThreatQ platform to be deployed more swiftly by the DoD to meet their cybersecurity challenges.

The ThreatQ Platform and the Department of Defense

Today, the U.S. Department of Defense (DOD) is leveraging the ThreatQ platform to support the warfighter in tackling the vast amounts of data they have access to, understanding relevance and priority, and effectively and efficiently taking action. Not only is it being used by various Security Operation teams within separate DOD services, with ThreatQ Data Exchange those services can share curated, vetted threat intelligence with their peers across the DOD. Because the exchange is bi-directional and point-to-point, any one of the participating partners has the ability to identify and share threat intelligence in the form of Indicators of Compromise and known related indicators to the central aggregation point for distribution to the other partners.

The ability to share curated threat intelligence with security counterparts creates a force multiplier for all participants. Each team is able to take advantage of the knowledge base and skill sets of all involved. They also gain a more global understanding of security posture with respect to specific threats they are tracking, and have the ability to highlight trending intelligence and pinpoint areas of insufficient coverage.



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, APAC and MENA. For more information, visit **www.threatquotient.com**.