THREATQUOTIENT™
A SECURONIX COMPANY

ThreatQ Security and Intelligence Operations Training Plan

ThreatQ Training

Desclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, expressed or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information. All rights reserved. This document and the software product(s) it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Introduction

Description

ThreatQuotient provides ThreatQ Operations Training. This training is a mix of hands-on activities and theoretical walkthroughs of the ThreatQ platform design and usage. The course will provide all of the slides (in pdf format), access to reference and reading materials, training platform access (where necessary), as well as published user guides required for the students. ThreatQ Operations Training is conducted over three (3) business days. The proposed schedule is as follows:

Threat Intelligence Overview

Training on the intelligence lifecycle, basic threat analysis for security operations, incident response, and threat fusion analysis. This part of the course will focus on the various intelligence sources that are available to the client, how they need to be curated, and basic stakeholder analysis for the organization to assist in determining outputs.

Threat Intelligence Platform Design

A high-level overview of the ThreatQ platform, the languages it is written in, the operating system and database it runs on, and the basic functions of the threat intelligence platform.

ThreatQ Security & Intelligence Operations Training and Use

The central part of the course will focus on the ThreatQ platform and how to use it day-to-day. Hands-on, in-platform examples for the class to work on to solidify the skills they have learned throughout the course. These exercises will be specifically designed and targeted to support the individual's role within the organization and will align with the various use cases.

Certification

All delegates that complete all the exercises given with proof of completion will be given a certificate of completion shortly after finishing the course.

Training Logistics and Preparation

General Information

Training will be delivered during business hours on business days (excluding local holidays).

Prerequisites

- List of attendees (name, email, function, and title) to be provided before training.
- The FQDN of the ThreatQ instance must be whitelisted: https://trainingX.threatq.com

Location and Time

Conducted via MS Teams, Zoom, or Webex in the customer's time zone (typically 9:30 AM – 4:00 PM) with breaks.

Student Requirements

Participants should have:

- Working knowledge of security operations
- Basic understanding of threat intelligence
- Experience with intelligence/data feeds

ThreatQ Administration Training Plan

This section focuses on intelligence source management, curation, and stakeholder analysis.

Session 1 – Cyber Threat Intelligence Basics

Introduction to ThreatQ

- Systems Check
- Connectivity check to training instance

Cyber Threat Intelligence (CTI) Basic Overview

- What is CTI
- History of the threat landscape
- Types of CTI
- The 5-Stage Intelligence Lifecycle
    1. Planning & Direction
    2. Collection
    3. Analysis & Production (including estimative language)
    4. Dissemination & Feedback
- Intelligence in Security Operations

Cyber Threat Intelligence

- Programs and Types
- Sources (OSINT, Commercial)

ThreatQ Platform Design, Architecture, and Integrations

- Enriching intelligence using SIEMs

System Access & Individual User Management

- Creation process overview
- User Roles

System Configuration Overview

- General Settings
  - Date/Time Zone
  - Indicator Parsing Options

Session 2 – The ThreatQ Platform

Hands-on exercises simulate real-world use cases.

Object Management

- Statuses Overview
  - Indicator, Object, Indicator Types, Event Types
  - Attribute Management

My Integrations

- Installing, configuring, and managing Feeds, Connectors, Operations, Actions
- Using Marketplace for research
- Managing integrations: Commercial, OSINT, Labs, STIX/TAXII

Data Controls (CTI Management)

- Expiration process
- Data retention policy
- Setting TLP
- Manual Whitelisting
- Scoring methodology

Exports Overview

- API Exports

Searching

- Finding and using CTI in the platform

Working with Indicators/Objects

- Managing indicators, events, adversaries, and signatures

IoC and Object Details Pages

- Creating indicators and objects (manual and via parser import)
- Dashboards (default and custom creation)

TQO Orchestrator Overview

- Actions and Workflows

TQX Data Exchange Overview

- TQX (DXL, TAXII)

Security Teams Use Cases

- Threat Intelligence Management
- SOC/Alert Triage
- Incident Response
- Threat Hunting
- Vulnerability Management

TQI (ThreatQ Investigations)

- Creating investigations
- Example: Spear Phishing & Vulnerability Management scenario (MITRE ATT&CK)
- Exercise completion for certification
- Q&A session

Trademarks and Disclaimers

All product details are subject to change without notice. ThreatQuotient and its suppliers disclaim all warranties, including merchantability and fitness for a particular purpose. ThreatQuotient shall not be liable for any indirect or consequential damages arising from use or inability to use this document.

All documentation and deliverables are provided in English unless otherwise agreed in writing. ThreatQuotient and the Rhino Logo are trademarks of ThreatQuotient, Inc.