

ThreatQ Platform Administration Training Plan

ThreatQ Training





A SECURONIX COMPANY

Disclaimer

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.

Copyright © 2025 ThreatQuotient, Inc.

Introduction



A SECURONIX COMPANY

Introduction

Description

ThreatQuotient provides ThreatQ Platform Administration training for the deployment and configuration of the ThreatQ platform.

The training is a mix of hands-on activities and theoretical walkthroughs covering deployment, setup, and administration. The course includes:

- Slides (in PDF format)
- Reading materials
- Access to a training platform (if needed)
- Published user guides

The ThreatQ Platform Administration Training is conducted over one business day.

Platform Administration Training

The core of this course focuses on day-to-day administration of the ThreatQ platform. Hands-on exercises will help participants solidify their understanding through real-world examples tailored to their organizational roles.

Certification

Participants who complete all assigned exercises with proof of completion will receive a Certificate of Completion after the course.



A SECURONIX COMPANY

Training Logistics and Preparation

General

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

Prerequisites

The timing in this schedule is approximate and may be adjusted for deeper coverage of specific topics.

Before training starts:

- Provide a complete list of attendees (names, emails, job titles, and functions).
- Ensure the FQDN of the ThreatQ instance is whitelisted:
<https://trainingX.threatq.com>

Location and Time

Training will be conducted via MS Teams, Zoom, or Webex in the customer's time zone during regular hours (typically **09:30 – 16:00**) with a one-hour lunch break and comfort breaks.

Student Requirements

Students should have:

- Working knowledge of **Linux administration**
- Understanding of **security operations**
- Familiarity with **basic threat intelligence**
- Experience with **data feeds and intelligence management**



A SECURONIX COMPANY

ThreatQ Administration Training Plan

The main part of the course will focus on the **ThreatQ platform's operational use**. Hands-on examples simulate real-world use cases aligned with organizational needs.

Introduction to ThreatQ

- Overview of the ThreatQ platform
- Understanding what a Threat Intelligence Platform is

Platform Architecture

- Deployment options
- Minimum specifications
- ThreatQ DataLinq Engine overview
- Automated tasks using the DataLinq Engine
- Logical & internal architecture
- Data model overview

Installing the ThreatQ Platform – Ubuntu

- Demonstration of installing **ThreatQ v6.x** on **Ubuntu 22.04 LTS**

Configuring ThreatQ First Boot

- Logging in for the first time
- Applying licenses
- Analytics configuration



A SECURONIX COMPANY

Access and User Management

- Managing users within ThreatQ
- Role-Based Access Control (RBAC) with user groups
- Manual user creation
- MFA/2FA configuration options
- LDAP setup
- SAML authentication
- CAC/PIV SSL configuration

System Configurations (UI)

- Proxy and account security settings
- Login disclaimer banner setup
- General settings and parsing presets

Object Management

- Managing:
 - Indicator statuses
 - Indicator types
 - Object statuses
 - Event types
 - Attributes

ThreatQ Monitoring Platform (Cockpit)

- Overview of system monitoring and health metrics



A SECURONIX COMPANY

Integrations Management

- Installing, configuring, and managing integrations
- Using the **Marketplace** for integration research
- Managing Feeds, Connectors, and Operations
 - Commercial integrations
 - OSINT
 - TAXII

Data Controls (CTI Management)

- Scoring
- Expiration process
- Traffic Light Protocol (TLP) settings
- Manual whitelisting

Exports Overview

- Understanding **API Exports**

Data Exchange

- **TQX Data Exchange Overview**
 - TAXII Server
 - DXL (ThreatQ to ThreatQ)
- **TQO Orchestrator Overview**
 - Actions
- **TQI Investigations Overview**



A SECURONIX COMPANY

Notifications

- Notifications Center overview
- Feed health email alerts
- Sharing notifications

Job Management

- Overview of job tracking and management tools

Backing Up & Restoring

- ThreatQ backup process
- ThreatQ restore process

Upgrading ThreatQ

- ThreatQ upgrade process and versioning guidelines

Basic Troubleshooting and Support

- Troubleshooting common issues
- ThreatQuotient support processes



A SECURONIX COMPANY

Trademarks and Disclaimers

All product details are subject to change without notice. All statements and recommendations are presented **without warranty**, express or implied.

ThreatQuotient and its suppliers disclaim all warranties, including **merchantability, fitness for purpose, and non-infringement**. ThreatQuotient shall not be liable for any **indirect or consequential damages**, including loss of data or profits.

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

© 2025 ThreatQuotient, Inc. All rights reserved.

