# ThreatConnect® Upgrade Guide: Containerized Deployment

## Software Version 7.5

Technical Guide

May 7, 2024

10033-03 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

# Table of Contents

**Important**: This guide describes how to upgrade ThreatConnect on a ThreatConnect instance that is running in a containerized solution using Docker®. To upgrade ThreatConnect and keep it running directly on an OS, see *ThreatConnect Upgrade Guide: Operating System Deployment*. Note that the containerization deployment was tested on AlmaLinux OS™ and is the preferred deployment method for all production and non-production systems starting with ThreatConnect version 7.5.

# Overview

This guide describes how to upgrade ThreatConnect on a ThreatConnect instance that has been deployed to a containerized environment. As of ThreatConnect version 7.5, you will no longer be required to install Java®, Python®, OpenSearch®, and Redis® during the ThreatConnect upgrade process. Instead, these software, along with ThreatConnect, are now packaged together in a containerized solution using Docker. The only thing that is not included in the Docker environment is the database, which will not be touched during the upgrade process.

# Upgrading ThreatConnect

Follow these steps to upgrade ThreatConnect:

1. Stop and remove the containers:

```
docker-compose rm -fs tc-mon tc-app tc-job
```

2. Restore the `.env` file and update the `TC_VERSION` variable's value to the latest ThreatConnect version (e.g., `TC_VERSION=v7.5.2`).
3. Start **tc-mon**:

```
docker-compose up -d nginx redis tc-mon
```

4. Start **tc-app**:

```
docker-compose up -d nginx tc-app
```

5. Start **tc-job**:

```
docker-compose up -d tc-job
```