# INTRO TO THREAT INTELLIGENCE & ATTRIBUTION TRAINING

**Date and Location**
- Summit Training Day: October 28, 2024
- Registration begins at 8:00am
- Training 9:00am-5:00pm
- Lunch Provided
- In person (no virtual option)

**Tuition and Registration**
There is no cost for attending this course. The course is funded by the Bay Area Urban Areas Security Initiative (BAUASI).

**For More Information**
Please contact mikyung.kim-molina@sfgov.org

**Target Audience**
Cyber Intelligence Analysts, Cyber Threat Analysts, Security Analysts and Penetration Testers

**Core Capability**
Cybersecurity

**Prerequisites/Materials**
There are no prerequisites to attend this course. A laptop is NOT required, all materials will be provided.

**Certification**
Participants will receive a certificate of course completion.

**Instructor**
Mandiant

*This document was prepared under a grant from FEMA's Grant Programs Directorate, U.S. Department of Homeland Security. Content is derived from the Bay Area Training and Exercise Program and does not necessarily represent the official position or policies of FEMA's Grant Programs Directorate or the U.S. Department of Homeland Security.*

## Description

This course is a fast-paced introduction to threat intelligence and attribution. It is designed to provide insight into attribution methodology and demonstrate the proper handling of threat intelligence information. The course explores the main components of a threat group and shows how analysts can use raw tactical intelligence and weigh connections and relationships to build a set of related activities that corresponds to a group of threat actors. Learners will become familiar with several factors they should consider when attributing related activity and view real-world examples of research and pivoting.

Course Objectives Include:
- Understand various definitions of threat intelligence and attribution.
- Distinguish between tactical, operational and strategic threat intelligence.
- Examine operational and strategic intelligence to determine the attribution and sponsorship of an attack operation.
- Consider attribution from a threat group's point of view.
- Use tactical intelligence in the early stages of a cyber- attack to evaluate data and correctly identify indicators that can be grouped into a set of related activities and attributed to a threat group.

Learning Topics: Risk and threat, Threat landscape; Threat actor examples; the attack lifecycle; the incident response (IR) process; Cyber Threat Intelligence (CTI) process lifecycle; special considerations; creating a response culture; planning a robust cybersecurity program; cybersecurity tools and best practices; vulnerability management.