THREAT ACTOR ASSURANCE MODULE (TAAM) OVERVIEW

Overview

Security Validation's Threat Actor Assurance Module (TAAM) allows you to validate the effectiveness of your defenses against known adversaries. You already capture intelligence on Threat Actors using Threat Intelligence Platforms (TIPs) and Threat Intelligence Feeds (TIFs) -- with TAAM you can now centralize and operationalize that information, continuously verifying your defenses are effective.

The following features and functionality are included with TAAM:

- Integration your Threat Intelligence Platforms (TIPs) and Threat Intelligence Feeds (TIFs) with the Validation Platform.
- The Threat Actor Library consolidates and centralizes information from your TIP and TIFs
- Threat Actor-specific Evaluations are created and updated when your TIP and TIFs sync with the platform
- View the effectiveness of your defenses against adversaries using the new TAAM Dashboard
- Captive IOC (Indicators of Compromise) Actions to safely evaluate defenses related to blocking communication with publicly routable destination addresses for a Threat Actor

See the following topics to learn more about TAAM:

- **Setting up your Threat Intelligence Integrations** (https://docs.mandiant.com/home/msv-threatintelligence-integrations)
- **Understanding TAAM Evaluations** (https://docs.mandiant.com/home/msv-taam-evaluations)
- **Getting Started with TAAM** (https://docs.mandiant.com/home/msv-getting-started-with-taam)
- **Understanding Threat Actor Information in Security Validation** (https://docs.mandiant.com/home/msv-threat-actor-library)
- **Captive IOC - Walkthrough** (https://docs.mandiant.com/home/msv-captive-ioc-actions)
- **The TAAM Dashboard** (https://docs.mandiant.com/home/msv-taam-dashboard)