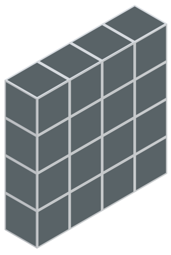
ThreatConnect™

How Mature is Your Threat Intelligence Program?

ThreatConnect's Threat Intelligence Maturity Model (TIMM) provides a systematic guide to help you understand where your organization resides on the path to a mature threat intelligence program and how you can better apply threat intelligence. The TIMM offers some general direction on the capabilities, risks, and exposures at each stage as well as things to consider as you anticipate moving to the next milestone.



○○○○

MATURITY LEVEL 0

Unclear Where to Start

- You're feeding data blindly into a SIEM.
- The data is unvalidated. It has no context.
- The raw data alone is unusable. Your team is overwhelmed with manual analysis.

Typical team: Security director or network admin.

Risks and exposures: Decisions must be made quickly which means analysts spend little time on each event. And, they have little to no information beyond what's contained in the alert.

●○○○

MATURITY LEVEL 1

Warming Up to Threat Intelligence

- Your organization integrates some level of automation into defensive controls.
- You continue to take a reactive approach.
- Threat data still lacks context and indicators.

Typical team: Network admin or solo analyst.

Risks and exposures: SIEM platforms aren't designed to handle intelligence from multiple sources in numerous formats. The reactive approach has many deficiencies.

●●○○

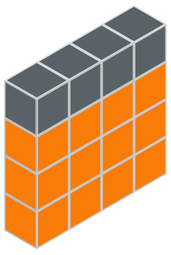
MATURITY LEVEL 2

Expanding Threat Intelligence Capabilities

- Your organization produces some actionable threat intelligence.
- Your SOC is inundated and overworked.
- You need a threat intelligence platform (TIP) to automatically analyze content of threat indicators.

Typical team: Team-based approach and a SOC.

Risks and exposures: Your organization can significantly increase the security team's capacity by using a TIP. And, you're able to act on threat data from communities, sharing at speeds previously unimagined.



●●●○

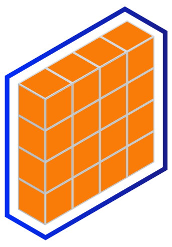
MATURITY LEVEL 3

Threat Intelligence Program in Place

- Your organization builds a structured team and begins to work with partners, vendors, and supply chain to protect network-adjacent organizations.
- Your team tracks persistent threat actors strategically.
- Your threat intelligence drives tactical business decisions.

Typical team: SOC and incident response teams with a security director at the helm, sometimes a dedicated threat intelligence analyst. Network operations and IT staff are also involved.

Risks and exposures: A TIP can still overcome the labor-intensive analysis process and improve workflow, and works best when it integrates information from upstream resources and then transforms the information for use by downstream tools.



●●●●

MATURITY LEVEL 4

Well-Defined Threat Intelligence Program

- Your organization has a stable threat intelligence program with defined processes.
- Teams collaborate effectively.
- You use threat intelligence to make C-level business decisions.
- You still need a TIP to enable communities to create advanced tools.

Typical team: CISO/security directors use TI in order to limit the ability of adversaries and successfully leverage intrusion tactics. They use the TIP for reporting to prove ROI. They build operational playbooks based on their TI to ensure maintenance of the TIP.

Risks and exposures: Organizations implement TIP with formalized processes and workflows; produce validated and actionable intelligence; and ensure appropriate threat response. A team-driven approach aligns security with business strategy, and sharing attack indicators with wider communities becomes possible.

ThreatConnect™

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit www.ThreatConnect.com.

ThreatConnect.com

Download our Threat Intelligence Maturity Model white paper for a more in-depth explanation.

https://threatconnect.com/resource/maturing-a-threat-intelligence-program/