ThreatConnect

Security Operations Maturity Model

ThreatConnect's Security Operations Maturity Model provides a systematic guide to help you understand where your organization resides on the path to fully leveraging the power of a SOAR Platform. Identifying your current level allows you to put a plan in place to progress up the Maturity Model to a more advanced steady state. The Security Operations Maturity Model offers general direction on the capabilities and risks at each stage as well as things to consider as you anticipate moving to the next milestone.

MATURITY LEVEL 1

Unclear Where to Start

Current State: 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. High levels of team and alert fatigue due to an overload of false positives most likely caused from using too many data feeds and not looking for high fidelity items or relevant information specific to their business objectives.

- Majority of processes are ad hoc and undocumented
- Unvalidated data is being sent blindy to the SIEM with no context
- Fragmented teams, processes, and tools
- Alert overload is a common theme
- Reactive instead of proactive due to the volume of work and inability to get ahead
- Frustration exists across the team which could lead to a high turnover rate.

MATURITY LEVEL 2

Ready to Address the Problem

Current State: At this level, your team has improved visibility into threats, but lacks efficient processes across people and tools. Some actionable threat intelligence is produced, but your organization has a hard time fully operationalizing it. There are no formal incident response processes, making escalation and investigation even more difficult.

- Little to no automation exists
- Team is often small, inundated, and overworked.
- Processes are documented, but mostly completed manually
- Tools in place are disparate and not communicating the way that they should
- Team members express desire to do more advanced, or different, types of work

MATURITY LEVEL 3

Defined Team and Processes

Current State: You have invested in the organizational processes, technology, and headcount to significantly improve your ability to detect and respond to threats. Your team has operational metrics, documented workflow, and experienced analysts. You may have an established SOC and are leveraging automation and supported technology integrations to improve the efficiency and speed of threat investigation and incident response processes.

- Your organization has a stable security program with defined processes.
- You have a TIP, SAO, and/or Incident Response Platform in place
- Reports are being generated but you may still have trouble demonstrating the business value & selling security to other departments
- Beginning to see a reduction in team fatigue, morale or turnover
- Removed immediate need for additional headcount to meet requirements

MATURITY LEVEL 4

Fully Functioning Program

Current State: Your organization has extremely clearly defined processes where the security team is working collaboratively across the department. Threat intelligence is used across your program to increase efficiency and accuracy across all functional areas. SOAR is used to prove ROI and improve security and business goal alignment.

- Improved collaboration among the security team and existing technology investments
- Team builds and consistently deploys operational Playbooks and Workflows for threat detection, analysis, investigation, and incident response
- Team morale is higher due to focus on strategy and career development
- Existing investments leveraged more strategically

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 ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708