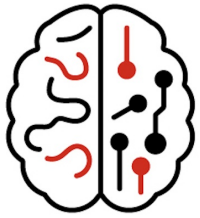
Mandiant

CREATING A CYBER THREAT PROFILE



This article focuses on the cyber defense function: **Intelligence** – the guiding light providing context and meaning to cyber activities.

Read Time: 7-10 Min

There are a variety of ways network defenders can leverage intelligence analysis to provide context and meaning to adversary and defender operations. The first case we examine here relates to **Creating and Maintaining a Cyber Threat Profile**

A **Cyber Threat Profile** (CTP) maps and tracks threats faced by an organization and how those threats impact them specifically.

Objectives and Key Actions for Application

A Cyber Threat Profile (CTP) is a living document used to identify a baseline of significant threats to an organization. The CTP distills the range of possible threats into those threats that are likely to occur and/or could have significant impact on an organization's assets or ability to operate. No two CTPs are the same – different organizations may have different threats based on their core business, geographic location, internet presence, criticality to national service functions, attractiveness of critical assets, etc.

Different Organizations, Different Threat Profiles

Imagine two different organizations – one, a high-profile bank in Australia, another a utilities provider in the Netherlands. Their respective CTP – who is likely to target these companies – will differ greatly. For example:

- An Australian bank may be targeted by globally based sophisticated financial threat groups backed by money mules on the ground
- A Dutch utilities provider may be targeted by agents of a foreign power, seeking access to security and safety controls that may disrupt productivity and supply

These two organizations may be threatened by similar threat actors. Both are critical infrastructure. However, the nature of their businesses means different threat groups would benefit from gaining access to their different assets. One threat group may just want to steal money. Another threat group may have espionage in mind. Different types of organizations will face different types of threats. A CTP needs to be calibrated to the needs of each organization and act as a guide for defense and security controls.

The CTP can be the single most critical document in maintaining an effective security posture - not just to the Cyber Threat Intelligence (CTI) team, but also for threat and risk management functions across the organization and executive decision makers. Without knowing which threats are relevant to which critical assets, how can organizations plan and budget to defend and respond effectively? How can threats be appropriately prioritized?

A regularly maintained and updated CTP is an immense benefit to numerous stakeholders throughout an organization. This document can help achieve a new level of understanding for non-technical peers and, in doing so, plays a key role in shifting from a reactive security posture to a proactive one. A CTP can provide a granular view for different departments, divisions, or business units on threats specific to their needs. Or it can provide a high-level view of potential gaps within the security perimeter.

What Does a Cyber Threat Profile Look Like?

Ultimately, the format of a CTP will be the decision of individual organizations, based on consumer needs and internal factors like resources, capabilities, and technology. A Threat Intelligence Platform (TIP) may organize relevant threats into an easily searchable format. Other organizations would be better served by a spreadsheet or tabular data with relevant column headings to understand the nature and type of threats. Still others may design specific matrixes to compare types of threats against critical assets.

Whatever the format, a CTP needs to be shareable across multiple audiences, relatively easy to understand, and able to be adapted easily when conditions change. At a minimum, we recommend a CTP include:

- A high-level overview of threats organized by categories for easy reference
- Summary of the nature and type of threat
- Clear reasoning as to why and how the business could be impacted by a given threat
- Active and maintained links to original source information that provides further context regarding the threat
- Identifiable information regarding whether the threat has successfully attacked the organization in the past
- An indication of priority (for tracking) and/or severity of potential impact
- An indication of the likelihood of targeting per threat
- At least a high-level overview of the organization's ability to detect and respond to the threat's known capabilities
- Marked recency of all information within the CTP (i.e., last update to each entry)
- Indication of responsibility or further point of contact for each threat or the document as a whole.

Despite the broad nature of this document, avoid the temptation to over-burden the CTP with too much information. The CTP works best when viewed 'at-a-glance' as stakeholders unfamiliar with CTI may become overwhelmed with too much technical detail and the document can become too bulky to use. Aim to create a CTP that demonstrates the type and nature of threats, the asset class they are likely to target, how they may fare against existing security controls, and the severity of the impact (damage) upon a successful attack. Back-stop these assessments with active links to further information that provides greater detail.

Aim for a high-level overview supported by linked context. Those that need the context can click-through or get in touch with an identified point of contact; those who need a more strategic view can be satisfied with the CTP.

How Do You Build a Cyber Threat Profile?

Building a CTP depends on knowing two critical elements: what your business does and how; and what actors are interested in compromising, abusing, or denying access to your business' data, operations, and personnel. In this way, the two concepts are complementary: threat groups will target your organization for what you have or do.

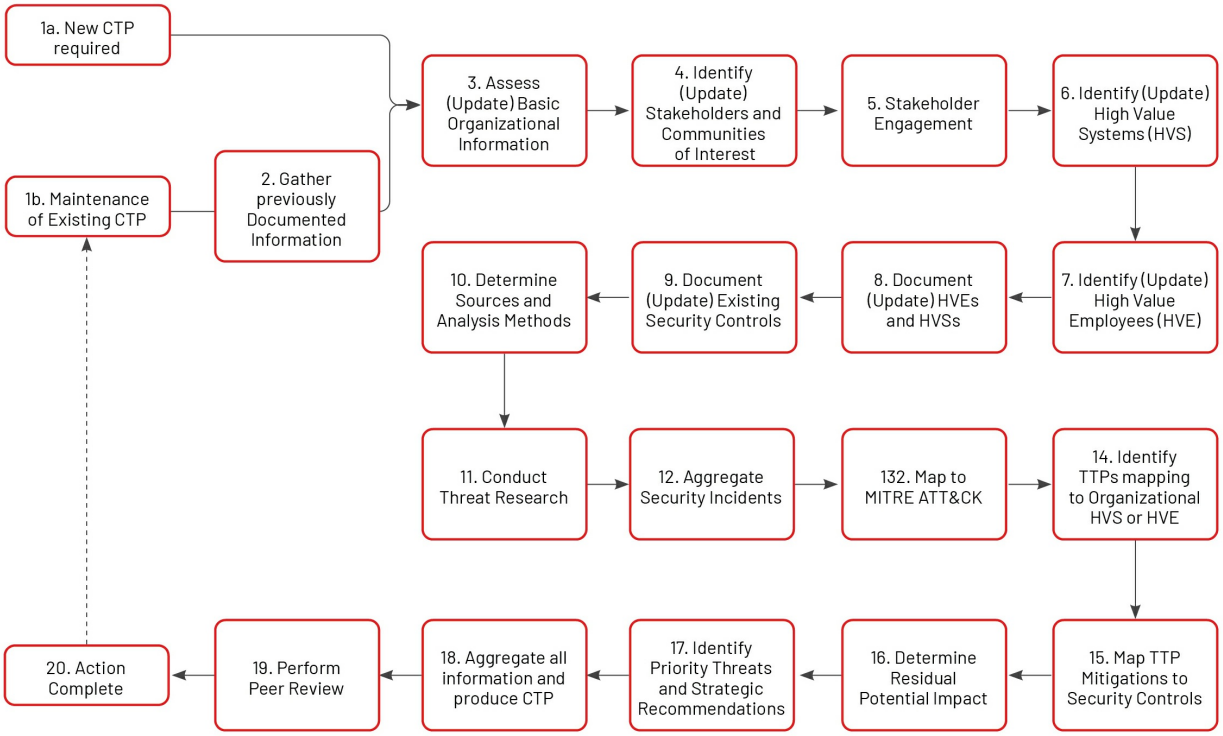
At a high level, building a CTP consists of:

1. Understanding your organization's assets and controls in place to mitigate risk
2. Overlaying this with an analysis of the threat landscape, determined either through:
    a. What you have seen in your environment (evidence-based approach relying on internal collections) and/or
    b. Interrogation of external intelligence to determine commonalities from targeting of similar organizations within your industry and/or geography (comparative- based approach)

3. Identifying and defining likely threats with significant impact based on the results from 1. & 2.

CTP Building Process

Below is a more specific process chart for building a CTP. In the following sections, we'll explore some of these key steps.



CTP Building Steps 2&3: Identify and Document Organizational Information

Collating organizational (or corporate) information helps focus intelligence collection and analysis on identifying relevant threats. Understanding the nature, scope, presence, and future plans of your organization and its operations will ensure the CTP remains relevant to the needs of the organization.

We recommend documenting the following types of organizational information, where possible:

- Industry, sector, geographic presence of the organization
- Corporate mission statement
- Products, services, brands, subsidiaries, and business processes
- Business-critical third parties, suppliers, and other trusted service providers
- Key lines of business, related stakeholders, and their mission/objectives
- Information security strategy and policy
- Cyber defense mission statement & organizational Structure
- Strategic plan / program plan for the CTI function or cyber defense
- Current security controls

Strategic Alignment of the CTP

Re-consider the major Australian bank. How might their CTP change if they'd announced strategic plans to expand into or withdraw from several SE Asian countries? How might their threat exposure differ?

CTP Building Steps 4-6: Engage Stakeholders and Communities of Interest

Every piece of threat intelligence should be produced for a stakeholder – intelligence should never be produced for its own sake. Without engaging with stakeholders on their needs, analysts can make erroneous assumptions about the nature of the business and the assets that truly matter to the organization. A stakeholder is someone whose capacity for

making decisions will improve with the application of intelligence.

In other words: CTI analysts and teams are experts on intelligence and threats; stakeholders are experts on their part of the organization. Don't second guess their needs – ask them!

In formal terms, identifying and understanding these needs is conducted by means of stakeholder analysis. Stakeholder analysis, usually conducted as a series of interviews and questionnaires, should determine stakeholder roles and responsibilities, data and assets under their control, and their processes - specifically their decision-making and risk management process (whether formal or informal). Linkages to other stakeholders or functional areas in the organization should also be determined. Give thought to how often stakeholders need to be re-engaged to revisit their needs and stay apprised of turnover that may merit reaching out to an incoming peer.

Gauging Trust and Confidence in Sources

Consider how much trust should be applied to the following information sharing networks:

- A social media feed of unverified indicators from a group of industry peers
- Internal network logs that have been cleaned and processed according to standardized procedures their threat exposure differ?

Stakeholders should also be divided into internal and external. External stakeholders most often include communities of interest-other organizations that share the same threat concerns, exposure, and risk. Participation within a community of interest may provide information to identify relevant threats not visible from other perspectives. Note: Sharing information to a community interest should adhere to strict sharing permission policies developed by your organization.

We recommend categorizing the types of information as well as the sharing networks, both internal and external. Where the information is derived from can be as important as what the information is. Knowing where the information comes from aids CTI analyst or team in processing data and determining trust and confidence in various sources.

CTP Building Steps 6-8: Identify the High Value Personas and Assets

High-value employees are often visible members of the organization. They can be attractive targets for threat actors, especially for extortion or impersonation. In a similar vein, high-value systems and applications are of intrinsic value to threat actors – these are the critical assets that will often form the basis of threat actor's tactical objectives (i.e., they are worth something to the threat actors). In many cases, threats against these high-value entities and assets will form a large bulk of the CTP.

Gather key attributes associated with high-value employees and systems or applications, especially information that an actor might find through open-source reconnaissance. These key attributes equate to the organization's attack surface, which is defined as different points an adversary can manipulate or leverage to achieve their objectives. Obtaining in-depth information about each high-value employee, system, or application can be used to align appropriate monitoring tools to proactively detect threat activity against these critical assets.

CTP Building Step 11: Survey the Global Threat Landscape

It's critical that CTI analysts maintain situational awareness of the global threat landscape. In general terms, this means analysts need to have at least a working knowledge of the various types of threats and trends, methods used to execute these threats, and main threat groups, actors, and sponsors responsible. Larger organizations can divide analysts into teams to focus by geography, industry, types of threats, subject matter expertise, etc. Smaller organizations may need analysts to remain nimble and rely on high-fidelity, third-party intelligence vendors, such as Mandiant, who often categorize intelligence into these various types for ease of processing and comprehension

Situational awareness isn't a passive state. When triaging intelligence, analysts need to derive direct or indirect meaning

from the information they read to determine the relevancy to their own organization's needs. Having gathered an understanding of stakeholder's needs and how the organization operates will provide necessary context to determine those threats likely to impact the organization. From here, analysts can draw conclusions about the most pertinent threats to the organization consistent with the stakeholder analysis needs. This is the beginning of mapping out the CTP.

Useful threat information to consider:

- Specific adversaries or threat actor groups
- Adversary motivations (i.e., cybercrime, cyber espionage, hacktivist, insider threats, etc.)
- Adversary intent and capabilities
- Observed campaigns (current and historical)
- Malware and TTPs
- Recent threat to industry or geographic region

CTP Building Step 12: Collate Observed Security Events Information

Having a historic perspective on past security events and incidents will help identify trends and focus threat analysis. Timelines, frequency of occurrences, attribution, and kill-chain or MITRE ATT&CK mapping across threat activity will help the organization anticipate future attacks and adapt this information to a concrete course of action.

Past attacks can be a strong indication of the intent or objectives of a threat adversary. Successful historical attacks may encourage similar future attacks if the situation surrounding the attack, including defenses, haven't altered. Consider what lessons can be learned from the past events or incidents. Have they been implemented?

Understanding the past to predict the future?

Historical incidents provide a handy baseline for comparison of current threats. Ask yourself – would this same threat group be motivated to continue to attack our organization? Do our critical assets still hold value for them? Has the geo-political situation changed, increasing, or decreasing, our attractiveness as a target? Was our initial response robust enough to discourage similar attacks in the future?

CTP Building Step 17: Prioritize Threats and Develop Strategic Recommendations

Following aggregation of all relevant information, strategic recommendations need to be formed. These recommendations should be specific, action-oriented, and applied to compromise scenarios of high-value employees, systems, or applications. As recommendations need to be feasible, stakeholder and executive leadership need to be consulted (and approvals given, where applicable). Such consultation ensures a consistent, organization-wide response to cyber risk that aligns with the response to other enterprise risks within the organizational risk framework.

In other words, recommendations based on cyber risks arising from the CTP need to ensure they are consistent with how other risks are managed within the organization.

Strategic recommendations should be organized around categories consistently used within the CTP, such as geographic-centric (e.g., China, Russian, Iran), motivation-based (e.g., espionage, financial, hacktivism) and/or asset-centric (e.g. criticality, value, age). Recommended responses to significant threats should be framed in the same terms. By clearly associating recommendations with prominent incidents and threat activity, decision makers may be able to properly weight the risks associated with potential adverse incidents.

Who is Responsible for the Cyber Threat Profile?

The maintenance of a CTP relies on clear custodial ownership and defined criteria for its various inputs. Broadly speaking, every incident, detection-metric, and emerging trend identified by intelligence should contribute to the maintenance of

the CTP. Not all will be deemed relevant but as the over-arching goal of the CTP is to reflect the current threat reality of your organization, the impact of each significant incident of piece of intelligence on the CTP needs to be considered.

In practical terms, the CTP should be formally reviewed at least every 6 months to ensure that it remains accurate. Remember, the CTP should inform the boundaries and appetite for risk and drive downstream intelligence collection, analysis, and production so it needs to be actively maintained.

The CTP should also be used to identify gaps in your organization's knowledge and ability to detect or respond to threat activity. These gaps will need to be filled with new sources and/or information to analyze. Hence, gaps identified within the CTP should feature within Intelligence Requirements, the key component setting the tone and focus for intelligence collection and analysis.