The Threat Actor Profile Guide for CTI Analysts

Curated Intelligence

About

This guide was created by Will T
Edited by Freddy M and Steve R
July 2023

Foreword:
Threat actor profiles are developed for several reasons. A common reason for profile creation centres on post-incident review, e.g., an internal detection or supply chain breach has been observed. Alternatively, another common generation event happens when CTI research has identified that the organisation(s) or client(s) they defend are likely to be targeted by the threat actor due to several factors.

The 'Threat Actor Profile Guide for CTI Analysts' was created after multiple Curated Intelligence members requested advice about threat actor profiles and their creation. Addressing a general need for those having difficulty, individuals in our community shared their experiences around the challenges stemming from the development of threat actor profiles and relaying vital information to key stakeholders.

This guide offers a templated introduction for CTI analysts getting started with profiling threat actors. Experienced CTI analysts and mature teams will likely have a more refined methodology, and even different types of threat actor profiles tailored towards a specific stakeholder type.

Let's be honest: Senior business leaders are not likely to read past the Executive Summary. This makes it the most important part of the report.

Include the most significant findings and assessments upfront.

The Executive Summary should be tailored to the stakeholder who requested the Threat Actor Profile.

Executive Summary

Introduction: "As of $Month 20XX, the Cyber Threat Intelligence team has researched the $ThreatActor"

- An Executive Summary should ideally be no longer than 10-15 lines (2-3 paragraphs)
- The main three questions to answer are "What?" "So What?" and "What Now?"

- Explain the level of threat to the organisation / client, which includes the following:
    - Highlight whether the $ThreatActor has targeted your organisation's / client's sector, country, or region as early as you can.
    - Make a short assessment of why your organisation / client could be targeted (or why they have been targeted) by the $ThreatActor.
    - Make a short evaluation of the ability of your organisation's / client's defence mechanisms to mitigate the threat.

Executive Summary

Stakeholder	Their Needs
The Executive Leadership Team (ELT)	Talk about the potential losses that could be caused by a successful attack. Think about intellectual property theft, customer data theft, and financial theft. Focus on the impact to the organisation's / client's investments.
Operational (SOC, CERT, Security Engineering, Security Awareness, etc.)	Talk about what tactics, techniques, and procedures (TTPs) that $ThreatActor uses. Highlight significant technical findings, like the fact the $ThreatActor exploits a certain CVE that is highly present in the organisation's / client's environment.

The first part of the about section is the "What?" part of the Threat Actor Profile.

Researching and listing known aliases of the $ThreatActor is key to highlighting what is being discussed.

Top Tip: It might be easier to complete the next section first on the $ThreatActor Diamond Model Attributes before writing the introduction.

About $ThreatActor

- Creating a Table of Threat Actor Aliases (sometimes referred to as cryptonyms) helps lay the foundation for the analysis in the profile.
- The table helps readers quickly understand that multiple organisations are tracking what is essentially the same $ThreatActor using their own moniker.
- The analyst can discuss the attribution to a named $ThreatActor if it is not clearly defined and can use diagrams as needed.
- For additional guidance, Curated Intelligence has blogged previously on Threat Actor Naming Schemes.

Threat Actor Aliases (Example)				
CrowdStrike	Mandiant	Microsoft (New)	Microsoft (Old)	Recorded Future
Cozy Bear	APT29	Midnight Blizzard	NOBELIUM	BlueBravo

- After a bit of Threat Actor Alias housekeeping is done, the CTI analyst can then begin to introduce the $ThreatActor.
- The introduction should ultimately answer the following questions:
    - What type of threat actor (i.e., group) is it? Common labels include cybercrime, espionage, hacktivist, etc.
    - What areas does $ThreatActor specialise in?
    - What type of campaign does $ThreatActor launch?
    - Make a short assessment of how advanced the $ThreatActor is, based on reason X, Y, and Z.
    - Discuss notable technical observations, such as software and TTPs.

This can help identify risks in the supply chain and help guide the focus of a threat hunt or risk assessment, demonstrating the value of CTI.

Targets of $ThreatActor

- Which sectors/verticals does $ThreatActor target?
    - Think: Proximity to organisation's / customer's sector/region
    - Think: Recentness of attacks, or timelines applicable
- What does the $ThreatActor do once they are inside a victim's environment?
- How long have they been known to persist inside a victim's environment?
- Are the targets of $ThreatActor related to each other?
    - Think: Cyber-enablement campaigns

$ThreatActor Diamond Model Attributes

- The Diamond Model Attributes are the key pieces of information required to rapidly understand the $ThreatActor.
- After these are filled out by the CTI analyst, they can then be added to a Diamond Model Diagram.
- Once the diagram is complete, the CTI analyst can introduce the threat actor and hit on the key points from their research and extraction of threat data.

The Diamond Model consists of the four key components of a threat actor, and is an industry standard, taught by SANS FOR578 and many other courses.

Adversary	Origin: Motivation: Activity:
Victim	Targeting: Locations: Systems:
Capabilities	IN: THROUGH: OUT:
Infrastructure	Attack Infrastructure: Support Infrastructure:

$ThreatActor Tactics, Techniques, and Procedures (TTPs)

This section of the Threat Actor Profile is for more technical stakeholders who consume operational and tactical intelligence.

It is often preferred by stakeholders for CTI analysts to provide operational and tactical intelligence in the form of diagrams and tables for easier consumption.

- The first few lines of this section should include a summary of technical details at a high level that can be useful for all stakeholders.
    - This can be done by borrowing the Unified Kill Chain's three stages: IN, THROUGH, and OUT
    - https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf
- To discuss the $ThreatActor TTPs in detail, the MITRE ATT&CK framework is recommended.
    - https://attack.mitre.org
- It is also recommended to create a table for TTPs.

ATT&CK ID	Description	Observable	Source

- The point of this exercise is to demonstrate our technical understanding of the $ThreatActor.
- The TTPs can also be used for other activities by other stakeholders.
- Security Engineering will find these helpful in implementing detection for the activities.
- Red Teamers may use these for adversary emulation during engagements.
- The SOC will find these helpful for situational awareness and supporting their triaging of events.

References

It is vital to include all citations. These are fundamental for supporting your assessments.

- Add all external references you intend to cite in your report.
- Use in-line citations to show the source of information (in paragraphs).
- Consider highlighting problematic sources and perform source evaluation.
    - This can be a footnote on a page of the threat actor card if there is contention around technical aspects or attribution assessments.
    - Only include the reference if it is important for readers to know about.