THREATHUNTER.AI

PTOLEMY:TEMPEST

Billions of threat intelligence messages and events are generated each day.

But what do you do with it? How do you keep up with the waves of intel and powerful rip currents that keep pulling you out into the abyss? More importantly, how do you manage it to improve your perimeter security?

The hard truth is that you can't. Until now.

Ptolemy:TEMPEST is the most accurate and up-to-date, zero hour threat intelligence feed for your perimeter security devices.

What is Ptolemy:TEMPEST?

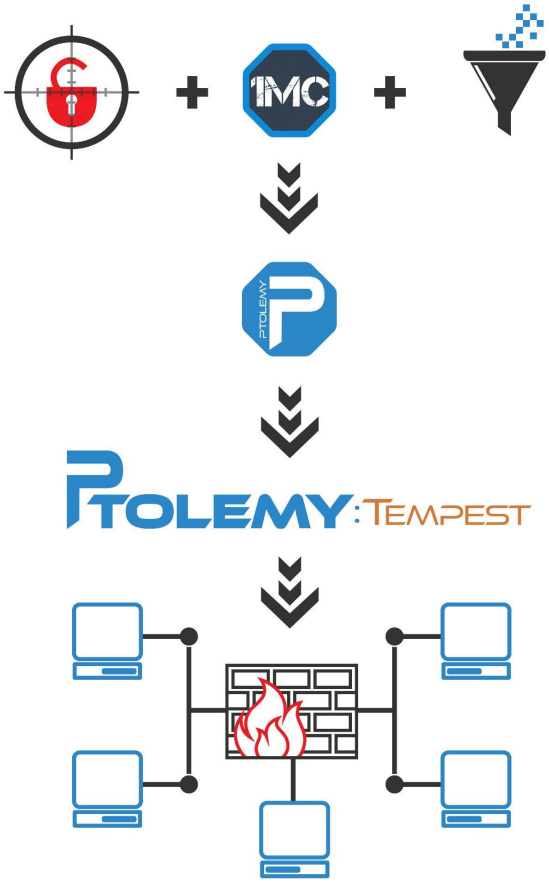
Ptolemy:TEMPEST is a service that effectively increases perimeter security by providing an actionable threat feed which can be ingested directly into Cisco, Sonicwall, and Palo Alto devices. Live, active threats are auto blocked and false positives are removed from your edge devices.

The TEMPEST intel feed is powered by Ptolemy, our Threat Intelligence Aggregation System, and is a curated data set based on intel auto-gathered by Ptolemy, deep research by our 1MC-Labs, and discovery of threats found across our customers by our SOC Threat Hunters.

The feed updates hourly with highly time-sensitive, zero-hour focused intelligence around known, active malicious threat actors.

This provides a unique stream of zero-hour threat intel that our teams are actively hunting, known active live attackers, and other malicious actors that we have seen.

> *Most other services continually add malicious actors to an ever growing list and leave it up to organizations to remove them as they get cleaned and white-listed. Ptolemy:TEMPEST works both ways, adding new threats as they are analyzed, but also removes them once they are no longer considered malicious, reducing the potential for future false positives.*



How it works

The SOC Threat Hunters are constantly hunting and triaging hundreds of thousands of events and attacks per day, so we know a bad actor when we see one.

Add in the data from our Threat Intel 1MC-Labs Team which keeps tabs on the dark web for future threats that are in the works.

Finally, we ingest all of that, plus over 270M event messages, telemetry, and sources every hour into Ptolemy, our proprietary threat intelligence engine, and let it do the heavy lifting, adding active malicious threat actor infrastructure.

The resulting TEMPEST data feed is a curated list of active, malicious threat actors that can be used to increase perimeter security in Cisco, Sonicwall, and Palo Alto devices.

All you need to do is configure your Cisco, Sonicwall, or Palo Alto device to pull the feed every hour and just like that, you've got a zero-hour perimeter defense

Threat hunting and response

Threathunter.ai Threat Hunters staff our state-of-the-art SOC in a true 24x7x365 fashion. Our SOC Analysts are trained and certified with the latest skills and techniques that threat actors are actively using against organizations. Across our customer base, they analyze, hunt, and triage hundreds of thousands of events each day.

Utilizing their vast experience and knowledge of IOCs, IOAs, and various Attack Surfaces, Threathunter.ai Threat Hunters have personally seen and responded to suspicious activity before it became an active incident. Our Hunt Team specializes in identifying and mitigating activity that has not yet been seen or reported on. This allows us to gather intelligence before it becomes publicly available.

Organizations are not always so lucky which is where Threathunter.ai's Incident Response Team comes into play. Working closely with our SOC Analysts, we bring a wealth of understanding on how adversaries work, quickly assessing the situation, mitigating the attack surface, and reducing the impact of the attack.

All of this knowledge and experience of zero-hour threats is fed into Ptolemy, ultimately expanding the impact of Ptolemy:TEMPEST. By including data from threat hunting and response, you can rest assured that your edge security devices are informed with the most current threat intel.

Threat intelligence

1MC-Labs is our threat intelligence and malware analysis team. They are the ones who hang out in the dark corners of the web where all the malicious actors congregate. Between keeping up with various ransomware groups and nation-state actors, they also build and test hacking tools and analyze the software that is being shared among the different threat groups.

If your only plan is to take a reactive and preventative approach to security, then your defense is based around what is already widely available. While preventative security measures are definitely a necessity in business, this is just not how malicious actors operate. Once they are “outed” they vary their methods to either find new vulnerabilities or worse, retain the hold they have already gained. Using the log4j vulnerability, for instance, how long after the 2.15.1 patch was released did it take for that to be exploited?

Hours.

As the Threathunter.ai 1MC-Labs Team feeds data into Ptolemy, your perimeter defense has a clear line of sight into potential future threats.

Threat AI

Ptolemy is our proprietary threat intelligence engine and the workhorse behind Ptolemy:TEMPEST. Ingesting over 200 Billion event messages, telemetry, and sources, in addition to intel from our SOC and 1MC-Labs Teams, Ptolemy correlates all of the data. While it is important to add new threats every hour, there are also hosts which have been cleaned and are no longer an active threat. Rather than continuing to build a never ending list that could result in a strain on edge devices, Ptolemy removes these whitelisted entries, keeping a sanitized list of only the bad actors.

What does this mean for my org?

Your edge security devices will be updated with a curated list of known, actively malicious threats. The feed is highly time sensitive and meticulously updated with Threathunter.ai's knowledge and experience.

Ptolemy:TEMPEST does the work for you, updating your edge device every hour with only the most current, active threats. This means new threats are added and ensures that false positives and hosts that are no longer a threat are removed from the feed.

When those changes are pulled in by your edge security device you have confidence that your organization and brand is protected in near-real time.

Now your team can get back to the tasks that matter most - driving critical initiatives and growing the business.

Requirements

- Sonicwall must be v6.5 or higher and must have the Content Filtering license (CFS v4.0) to enable external API pulls
- Cisco must have FirePower