

Threat Intelligence vs. Threat Hunting: What's the Difference?

TechRounder PDF Edition

Live article: <https://www.techrounder.com/security/threat-intelligence-vs-threat-hunting-whats-the-difference/>

By Vipin PG | Published July 2, 2024 | Updated July 2, 2024 | Format: Comparison | 3 min read

Bottom line

In the world of cybersecurity, two important terms you might hear are "threat intelligence" and "threat hunting." Both are important for keeping computer systems safe from bad actors. But what exactly do these terms mean, and how are they different?

In the world of cybersecurity, two important terms you might hear are "threat intelligence" and "threat hunting." Both are important for keeping computer systems safe from bad actors. But what exactly do these terms mean, and how are they different? we can examine.

What is Threat Intelligence?

Threat intelligence is like a spy. It gathers information about potential threats to computers and networks. This information helps cybersecurity experts understand what kinds of dangers exist and how to defend against them. Threat intelligence is gathered from many sources, including:

- Security Tools: Software that monitors networks for suspicious activities.
- Websites and Forums: Where hackers sometimes share information about their activities.
- Government Agencies: Who track cyber threats on a national or international level.
- Private Companies: That specialize in collecting and analyzing cyber threat data.

Once gathered, this information is analyzed and processed to create useful insights. To better understand the foundational elements of this process, one might ask, what is a threat intelligence platform?, a question that opens the door to exploring systems designed to automate and improve the analysis of cyber threats. . These insights help cybersecurity teams anticipate and prepare for potential attacks. For example, if a new type of malware (malicious software) is discovered, threat intelligence can help create defenses against it before it causes harm.

What is Threat Hunting?

Threat hunting, on the other hand, is more like a detective. It's about actively searching for signs of malicious activity within a computer system or network. Unlike threat intelligence, which often involves automated tools and data analysis, threat hunting requires human expertise and intuition. Here's how threat hunting works:

1. Define the Scope: Threat hunters decide where and what to investigate based on known threats and vulnerabilities.
2. Collect Data: They gather data from various sources like logs, network traffic, and endpoint devices (like computers and smartphones).
3. Analyze for Anomalies: They look for unusual patterns or behaviors that might indicate an ongoing or potential cyber attack.
4. Investigate: If they find something suspicious, they examine deeper to understand what's happening and how to stop it.

5. Remediate: Finally, they work to remove the threat and strengthen defenses to prevent future attacks. Threat hunting is proactive and often goes beyond automated alerts. It involves skilled professionals using their knowledge and experience to actively seek out threats that may have evaded automated detection.

Key Differences Between Threat Intelligence and Threat Hunting

1. Focus: Threat intelligence focuses on gathering and analyzing information about potential threats. Threat hunting focuses on actively searching for and identifying existing threats within a system.
2. Nature: Threat intelligence can be automated and relies on data analysis. Threat hunting requires human skills, intuition, and hands-on investigation.
3. Timing: Threat intelligence is often used to prepare defenses before an attack occurs. Threat hunting occurs during or after an attack to identify and mitigate damage.
4. Approach: Threat intelligence is broader and more comprehensive, covering a wide range of potential threats and vulnerabilities. Threat hunting is more targeted and specific, focusing on finding active threats within a known environment.

Why Both Are Important

Both threat intelligence and threat hunting play important roles in cybersecurity:

- Prevention: Threat intelligence helps organizations anticipate and defend against potential threats before they become active.
- Detection and Response: Threat hunting helps in detecting threats that may have bypassed automated systems and enables quick response and mitigation.
- Continuous Improvement: Together, they contribute to improving overall cybersecurity strategies by providing insights into emerging threats and enhancing defense mechanisms.

Conclusion

In conclusion, while threat intelligence and threat hunting are related to cybersecurity, they serve different purposes. Threat intelligence gathers and analyzes information about potential threats, while threat hunting actively searches for and identifies existing threats within a system. Both are essential for protecting computer systems and networks from cyber attacks in today's digital world. By understanding these differences, organizations can better strengthen their cybersecurity posture and stay one step ahead of cyber threats. Remember, in the battle against cybercrime, knowledge and proactive measures are key. Integrating both threat intelligence and threat hunting into cybersecurity strategies can greatly improve protection against changing threats.