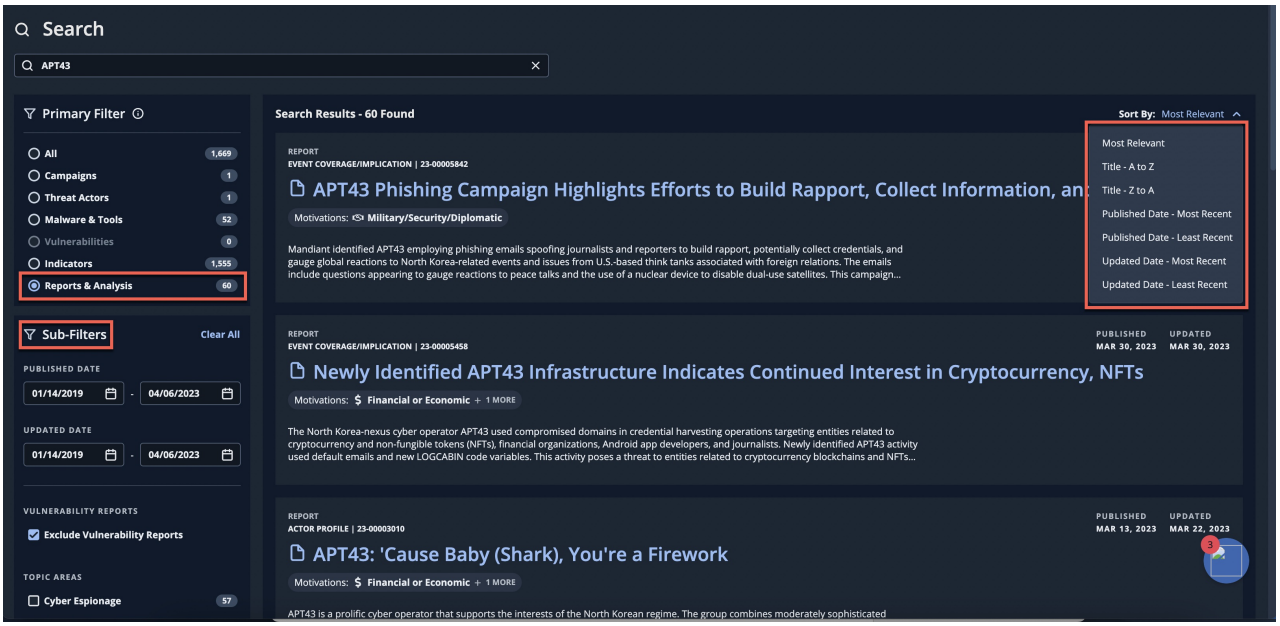
SEARCH THREAT INTELLIGENCE CONTENT IN MATI

Mandiant Advantage Threat Intelligence (MATI) provides Advanced Search capabilities to help you easily navigate Mandiant's vast knowledge base of threat intelligence data to drill down to what's relevant and quickly pivot to explore associated campaigns, threat actors, vulnerabilities, indicators, malware, tools, and reports & analysis.

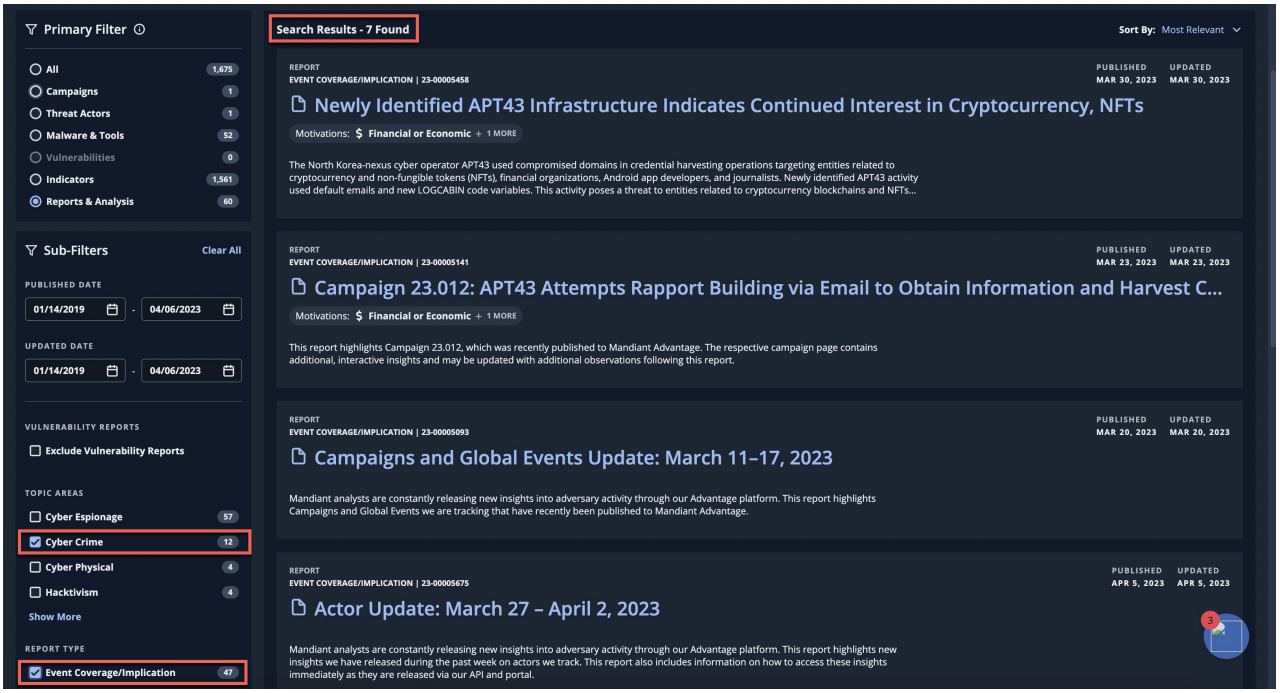
Initial search results will be sorted by **Most Relevant**; no other sorting options are available until a **Primary Filter** is applied.

Filtering

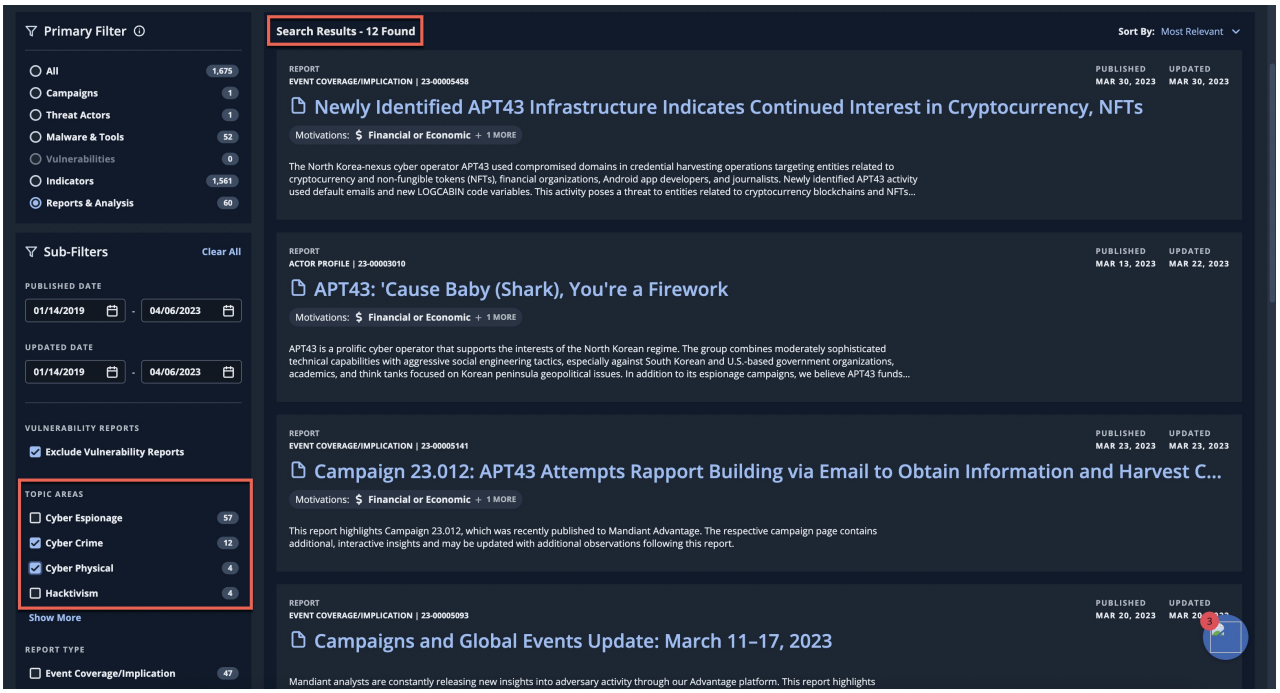
Once a **Primary Filter** has been selected, additional **Sub-Filters** and **Sort By** options that are specific to the **Primary Filter** will become available.



Once you select a primary filter for the search criteria, each sub-filter will display the number of associated matches for that search criteria. If sub-filters are selected from different sub-filter categories, the AND operator is used to combine the total search results.



If multiple sub-filters are selected within the same sub-filter category, the OR operator is used to combine the total search results.



Keep in mind that search criteria may appear in multiple sub-filters, even within the same sub-filter category. As different combinations of sub-filters are selected (using AND across categories, and OR within categories), the match count at the top of the list of search results will update accordingly.

Video overview

The following video provides a quick walk through of Advanced Search capabilites:

Gemini search notice

After Nov 7, 2024, the Gemini search functionality in Mandiant Advantage is no longer available. We are excited to offer you a more powerful and comprehensive platform for investigating and responding to threats through Google Threat Intelligence (Google TI). We have incorporated your feedback from the Gemini search in MATI into the Google TI version of the product.

Google TI offers a more comprehensive and powerful search experience, leveraging the latest Gemini models and incorporating a broader range of data sources.

What to expect

- **More Comprehensive Data:** Google TI combines threat intelligence from Mandiant, Google, and VirusTotal, providing a more complete view of the threat landscape. This includes signals from VirusTotal's massive threat database and Google's own telemetry, giving you a richer understanding of potential threats.
- **Faster and More Informative Answers:** The search functionality in Google TI utilizes the latest Gemini models, enabling faster and more relevant search results. You'll be able to find the information you need more quickly and efficiently.
- **Enhanced Features:** Google TI offers an improved search experience with new features, including the ability to search across OSINT articles. This provides you with even greater insights and context when investigating threats.

Need help?

Visit **our website** or **contact our team** to learn more and get started with Google TI. Our team is available to assist you and answer any questions you may have.