HOW YOUR THREAT LANDSCAPE USES AI RECOMMENDATIONS

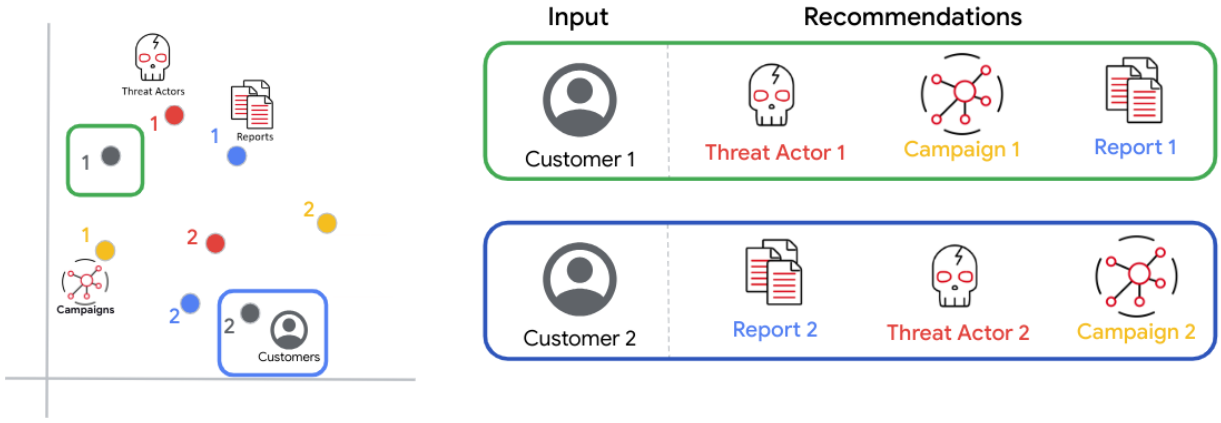
This feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to **Support.**
(https://docs.mandiant.com/home/mandiant-support-cases)

Mandiant has decades worth of threat intelligence data spanning a wide variety of contexts, including targeted locations and industry verticals. However, not every piece of that information is relevant to every customer. As a result, manual threat prioritization is not tenable and can lead to overlooked threats.
To address this problem, Mandiant's Artificial Intelligence (AI)-infused Threat Profiles can serve you personalized recommendations about threat intelligence objects, like threat actors, malware families, and **threat campaigns (https://www.mandiant.com/resources/blog/attacker-visibility-threat-campaigns)**. This automation reduces the amount of time spent on reactively deciding which threats are most important in favor of proactively providing the most relevant threat intelligence data.
The AI personalization model automatically generates a threat profile for every customer based on the following:

- **Inputs**: customer demographics including:
  - Industry verticals (for example, technology, governments, and so on)
  - Operating locations (country, region, or subregion)
- **Outputs**:
  - Threat objects including Threat Actors, Malware Families, or Campaigns
  - Relevance score for each recommendation
  - Extensions to other threat objects (Reports, Vulnerabilities, and so on)

Before this model, Threat Actors were the main entrypoint, which didn't allow for flexible pivoting. Previously, an attack would have had to have already happened to discover relevant threat objects. The AI model uses embeddings, which represent multiple object types and allow for more flexible and contextual pivoting by surfacing threats that are likely to occur based on what Mandiant knows about the global threat landscape. Feedback is incorporated directly to shape the recommendations for each user.

Semantically similar threat objects are placed close together in a learned embedding space based on the attributes of the objects themselves as well as the relationships between them. In the example diagram, Customer 1 is served specific recommendations (Threat Actor 1, Campaign 1, and Report 1) by the AI personalization model. To provide these recommendations, the model learning determined that nearest objects to the customer in this learned embedding space. Likewise, Customer 2 receives nearby recommended objects, including Report 2, Threat Actor 2, and Campaign 2.



Example of input and recommendations returned from AI personalization model

This model continuously learns and maps relationships between Threat Intel objects, such as the actors to malware relationship, so that the recommendations are fine-tuned over time.