Mandiant

DISCOVERY CONTEXT VISUALIZER

Mandiant Advantage Attack Surface Management (MA-ASM) collection engines carry out unique discovery tasks for each type of discoverable asset or entity. These tasks gather information and assist MA-ASM in determining whether these assets belong to your organization and the security posture of these external assets.

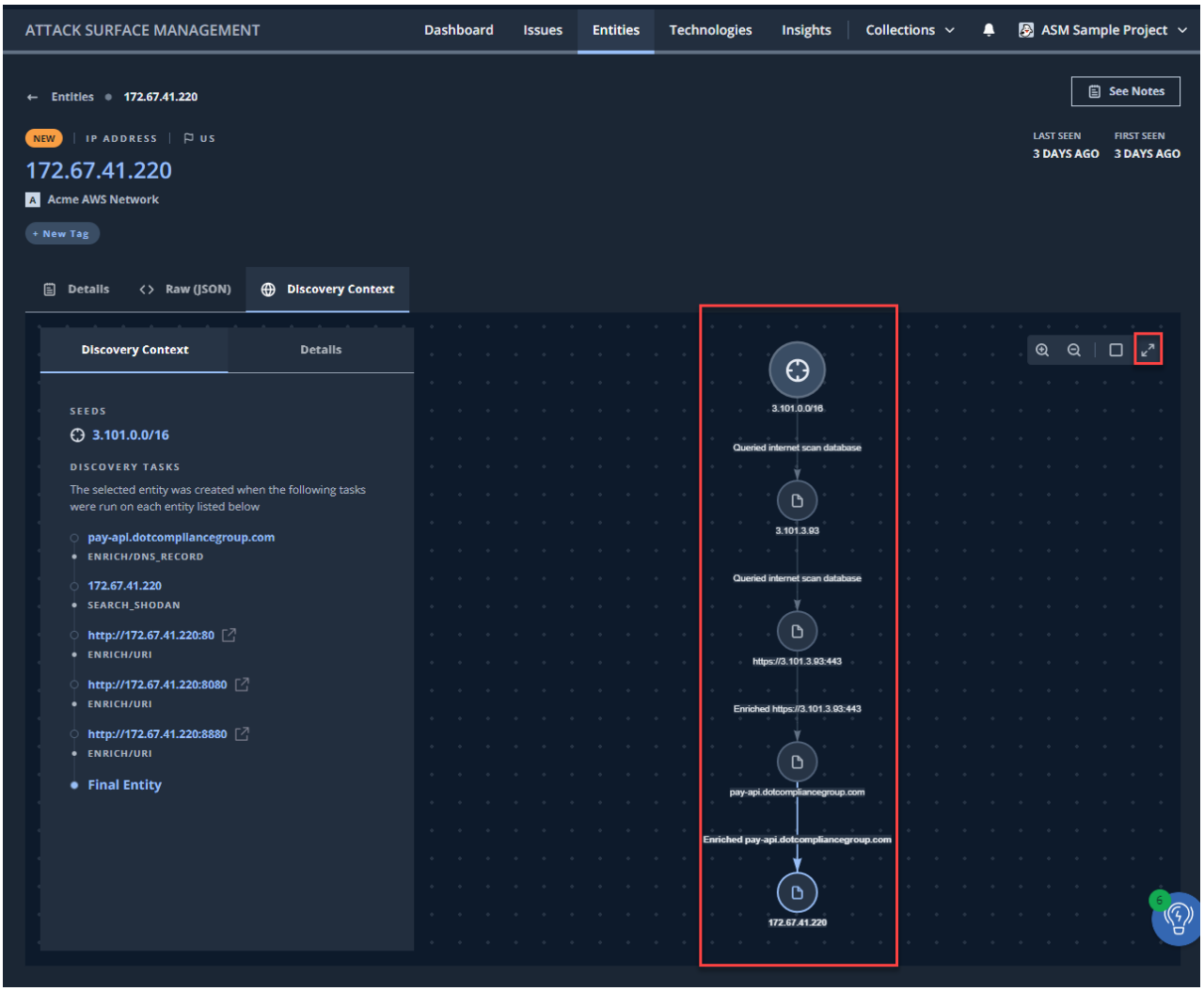
Determining asset attribution to your organization occurs when MA-ASM maps discovered assets using the Global Intelligence to assess ownership. Here, MA-ASM determines whether the asset is shared, belongs to an infrastructure, or belongs to a third party.

The Discovery Visualizer, available on each individual entity page, displays the discovery path and context that MA-ASM identified during the discovery and attribution process. This feature creates a visual connection between the seed and the child entities, allowing you to view how the entities are found.

For example, when you go to an individual entity page and see an IP address, you can click the **Discovery Context** tab to show the discovery context on the left hand panel. On this page you see a netblock defining the scope of the collection within MA-ASM, and you see each individual discovery task that is run against related entities as they are discovered. All of this information is displayed graphically on the same entity page. Selecting a child entity node highlights the graphical section and reflects its discovery tasks on the left hand panel.

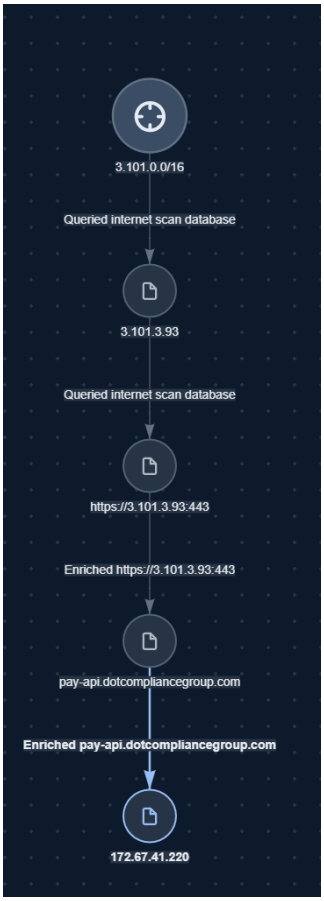
In this sample screen capture, you review the tasks graphically as follows:

1. Select the seed starter node, it highlights the task "ASM queried the internet scan database for 3.101.0.0/16 (seed)."
2. Select the following node highlights the task "ASM queried the internet scan database for 3.101.3.93."
3. Select the next node highlights the "ASM enriched https://3.101.3.93:8443" task.
4. Choose the node "pay-api.compliancegroup.com" highlights the task "ASM enriched pay-api.compliancegroup.com."
5. At the end of the discovery journey, the ultimate child entity "172.67.41.220" is discovered.



So, you're looking at here beginning from the starter seed and its following child entities how MA-ASM executes tasks and finds child entities. You have the initial seed, you can see it has queried the internet scan database. Then, the system finds a child entity and continued enrichment tasks. The process finds another additional child entity and so on until you end up at this individual entity "172.67.41.220".

The full screen button on the top right side allows you to visualize the map on full screen mode.



You find additional details on the **Details** tab. Selecting each node on the visual reveals the IP address, the open ports, and the resolution that was gathered by MA-ASM.