Gigamon

NetFlow

Lumeta uses a body of NetFlow data as the entity against which to identify threat conversations between your network and external adversaries. This NetFlow data comes to Lumeta as a result of its integration with a Gigamon solution.

Here's how the two come together:

1. First, Gigamon delivers enterprise physical and virtual network traffic streams (NetFlow) to Lumeta. This NetFlow data is voluminous-- a new wave of it is delivered every 5 minutes.
2. Next, Lumeta parses open source and subscription intelligence feeds and repositories to enumerate known bad servers and networks and associated attributes.
3. Then, Lumeta correlates the wave of NetFlow data against the threat intelligence data to identify threat conversations.
4. These filtered results are stored in Lumeta's HDFS database and are compared with Lumeta's authoritative index of network IP addresses to identify which devices are having the threat conversations.
5. Suspect devices are reported by Lumeta in dashboards, maps, and reports.
6. Based on these findings, IT security teams should investigate these machines further (perform incident response, isolate the device immediately, etc.)

Configuration