

Streaming

Metron Streaming is a module that deals with stream processing including telemetry ingest, enrichment, threat intelligence referencing, alerting, and real-time scoring of machine learning models. Metron Streaming is built on top of [Apache Storm](#), which is a massively scalable stream processing engine with unique properties that make it a good fit for processing networking and logging data. Telemetry generated by various sensors is processed by Metron's Storm topologies. There are three topology types.



Topology Name	Description	Architecture Reference
Parsing /Normalizing Topology	Receives a telemetry message in it's native format and normalizes it to a common Metron JSON format. There is one topology per source and the output is piped to the Enrichment/Threat Intel topology	Parsing Topology
Enrichment /Threat Intel Topology	Takes an normalized Metron JSON, enriches it, cross-references it against threat intelligence, tags it with alerts (where appropriate), runs the result against the scoring component of machine learning models (where appropriate) and stores the telemetry in a data store supported by Metron	Enrichment /Threat Intel Topology
PCAP Topology	The PCAP topology is designed to process telemetry produced by Metron's PCAP Probe and it's output is designed to be visualized by Metron's PCAP Service .	PCAP Topology