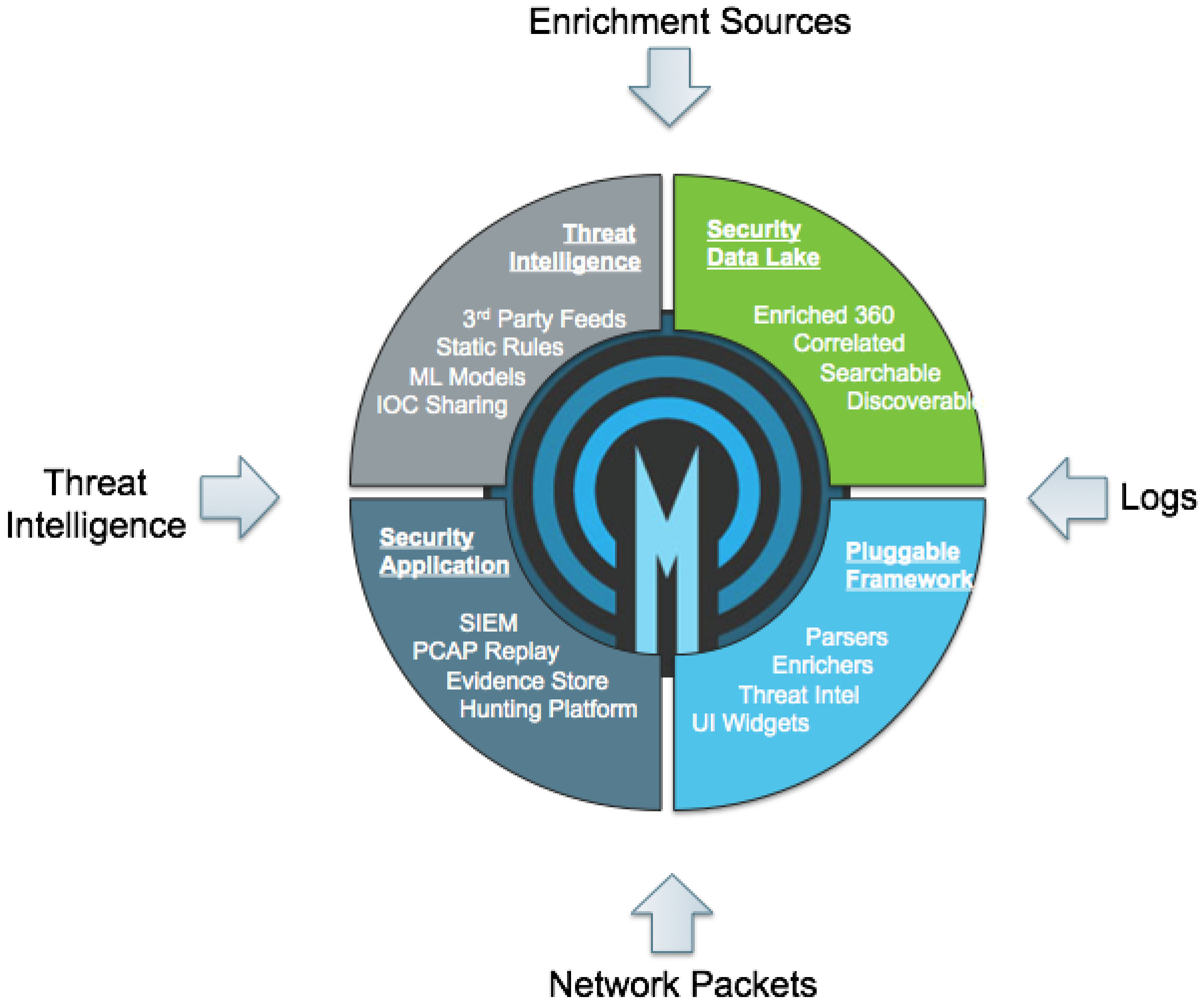
# Metron Core Capabilities and Functional Themes

## Core Functional Capabilities

Apache Metron is a cyber security application framework that provides organizations the ability to ingest, process and store diverse security data feeds at scale in order to detect cyber anomalies and enable organizations to rapidly respond to them.



As the diagram above indicates, the Metron framework provides 4 key capabilities:

1. Security Data Lake / Vault - Platform provides cost effective way to store enriched telemetry data for long periods of time. This data lake provides the corpus of data required to do feature engineering that powers discovery analytics and provides a mechanism to search and query for operational analytics.
2. Pluggable Framework - Platform provides not only a rich set of parsers for common security data sources (pcap, netflow, bro, snort, fireye, sourcefire) but also provides a pluggable framework to add new custom parsers for new data sources, add new enrichment services to provide more contextual info to the raw streaming data, pluggable extensions for threat intel feeds, and the ability to customize the security dashboards.
3. Security Application - Metron provides standard SIEM like capabilities (alerting, threat intel framework, agents to ingest data sources) but also has packet replay utilities, evidence store and hunting services commonly used by SOC analysts.
4. Threat Intelligence Platform - Metron will provide next generation defense techniques that consists of using a class of anomaly detection and machine learning algorithms that can be applied in real-time as events are streaming in.

## Core Functional Themes

There are four core functional themes that Metron will focus on. As the community around Metron continues to group, new features and enhancements will be prioritized across these four themes.

The 4 core functional themes are the following:

blocked URL