Blueprint

Anomaly Detection with DNS Data & Azure Databricks

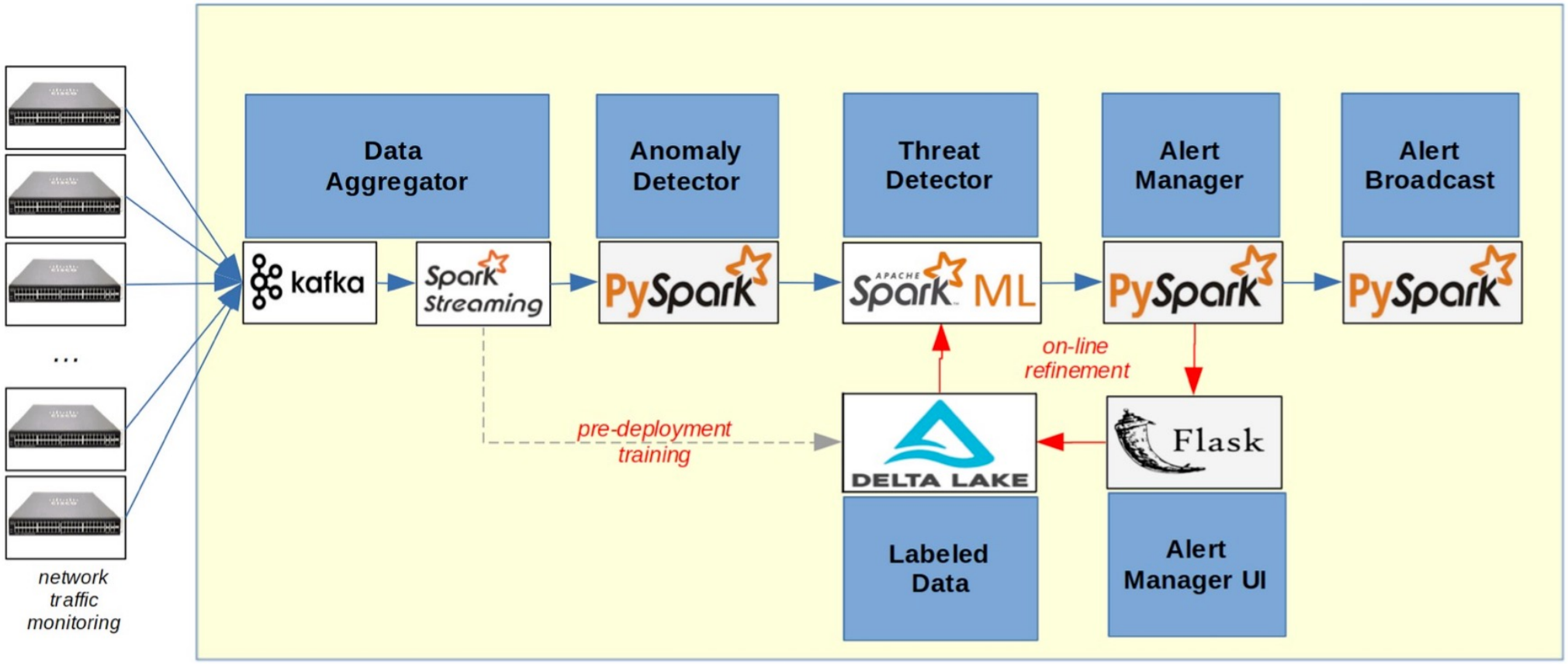
Architecture

A *Network* Threat Detection System

What might a Network Threat Detection System Look Like?

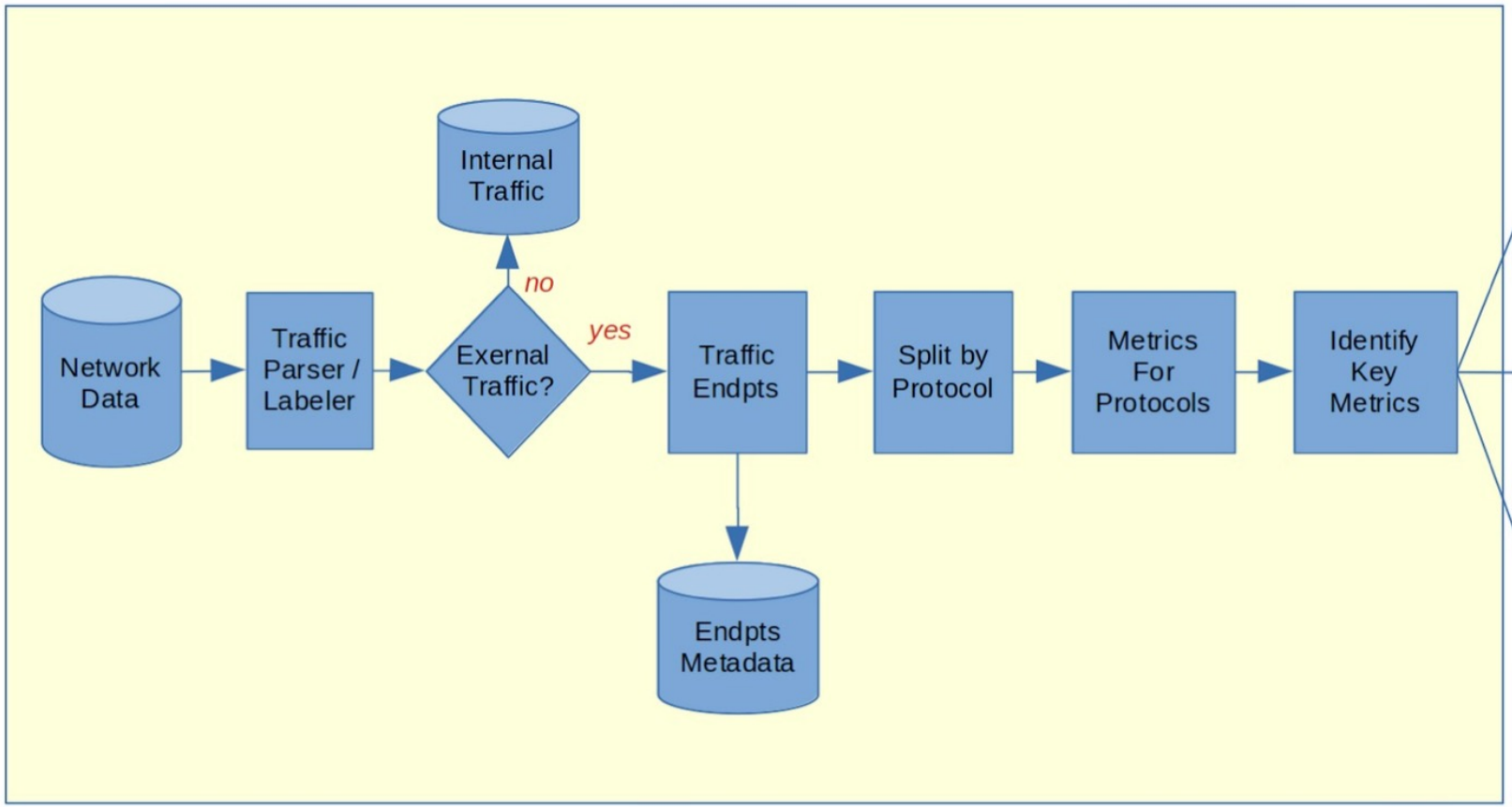
databricks

A threat-detection system must recognize anomalies in a data source and selectively report those anomalies that align with the end-user's notion of threat.

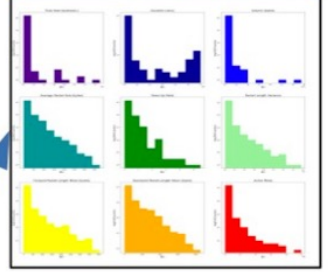


Notional Network Traffic Anomaly Detector

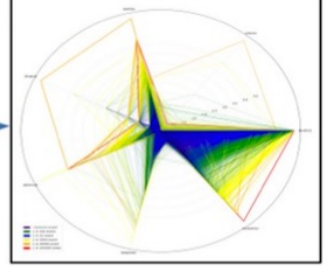
- *Focus on external traffic (entering or leaving local network)*



Protocol Histograms



Protocol Radar Plots



Protocol Geolocations





Get started for free with our accelerator

Download the code at
https://github.com/BlueprintConsulting/Blueprint-Databricks-Anomaly-Detection-Accelerator

bpcs.com • 206.455.8326 • info@bpcs.com

Blueprint Technologies • 2600 116th Ave NE, First Floor • Bellevue, WA 98004

© Copyright Blueprint Technologies. All rights reserved.