CERIAS

The Center for Education and Research in Information Assurance and Security

# A Tool For Interactive Visual Threat Analytics and Intelligence, based on OpenSOC Framework

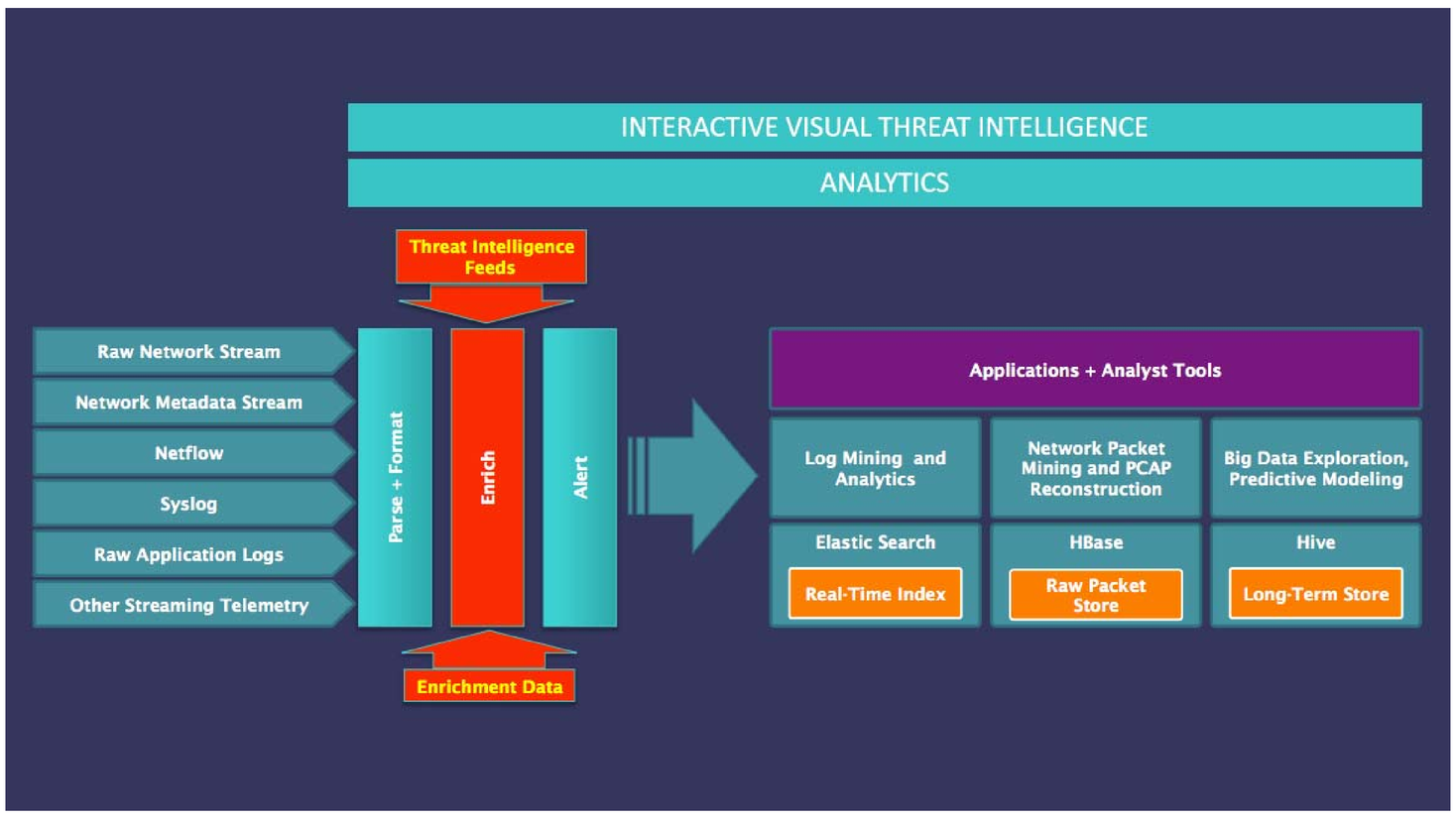
Lourdes Gino, Dheeraj Gurugubelli and Dr. Marcus K Rogers
Department of Computer and Information Technology
Purdue University

## Abstract

Cyber Threat Intelligence is a booming area in the field of Information Security that deals with aggregation, processing, evaluation and reporting of reliable information in real-time pertaining to threats posed on the cyber world that encompasses computers, smartphone, tablets and any device that's connected to the Internet. The imminent need for threat intelligence is growing rapidly as the data flowing through the cyber world is growing gargantuan and as we are moving towards Internet of Things where almost any thing is connected to the Internet. Visual Threat Intelligence takes the threat intelligence to the next step where the data is presented in a human-perceivable way so as to help in making right and quick decisions to avert the cyber threat. The OpenSOC framework provides a unified platform for ingest, storage and analytics. The purpose of this research is to build a open-source visual threat intelligence tool based on the OpenSOC framework built over the Hadoop framework.

## Implementation

| | |
|---|---|
| Phase 1: | Design the implementation framework |
| Phase 2: | Setup Hadoop Cluster and Required configuration |
| Phase 3: | Data Collection and Analysis |
| Phase 4: | Streaming Real-Time network data with Storm |
| Phase 5: | Visualization of real-time network data using D3. |
| Phase 6: | Predictive Modelling |
| Phase 7: | Threat Reporting and Results |




## The Technology Stack

- Telemetry Capture Layer: Apache Flume
- Data Bus: Apache Kafka
- Stream Processor: Apache Storm
- Real-Time Index and Search: Elastic Search
- Long-Term Data Store: Apache Hive
- Long-Term Packet Store: Apache Hbase
- Visualization Platform: The Web App built using Angularjs and D3.

## Why?

- Open Source
- Parallel and scalable computation tools
- Cheap, massively-scalable storage
- Stream computation + stream analysis
- Scaling + approximation
- Predictive Analytics
- Interactive Visualizations

## References

1. http://opensoc.github.io
2. https://blogs.cisco.com/security/opensoc-an-open-commitment-to-security

CERIAS

PURDUE UNIVERSITY