InSight2

The InSight Advanced Performance Measurement System

NSF Grant No. IRNC AMI-1450959

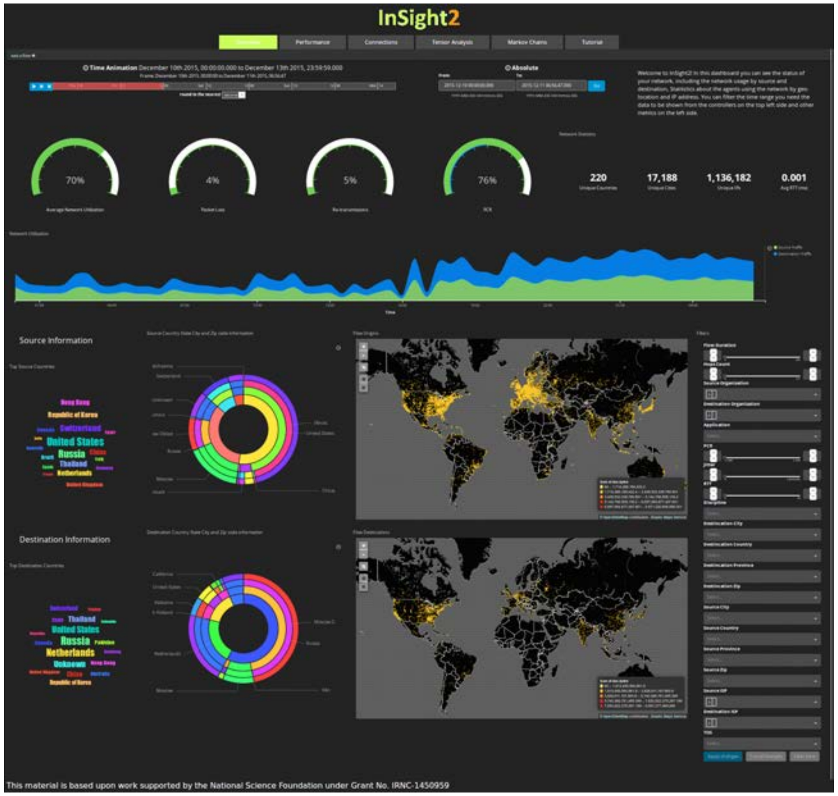
Jens Gregor & Angel Kodituwakku, Univ. Tennessee
Carter Bullard, QoSient
Buseung Cho, KISTI
John Gerth & Alex Keller, Stanford University

What is InSight2 ?

- Interactive web based platform for real-time network traffic monitoring, modeling and analysis
- Argus flow data enriched with GeoIP, bad actor, and Global Science Registry (GSR) information
- Data modeling and visualization based on free software: Python, Elasticsearch, and JavaScript
- Multi-threaded, scalable, and easily extendible

InSight2 Overview Dashboard

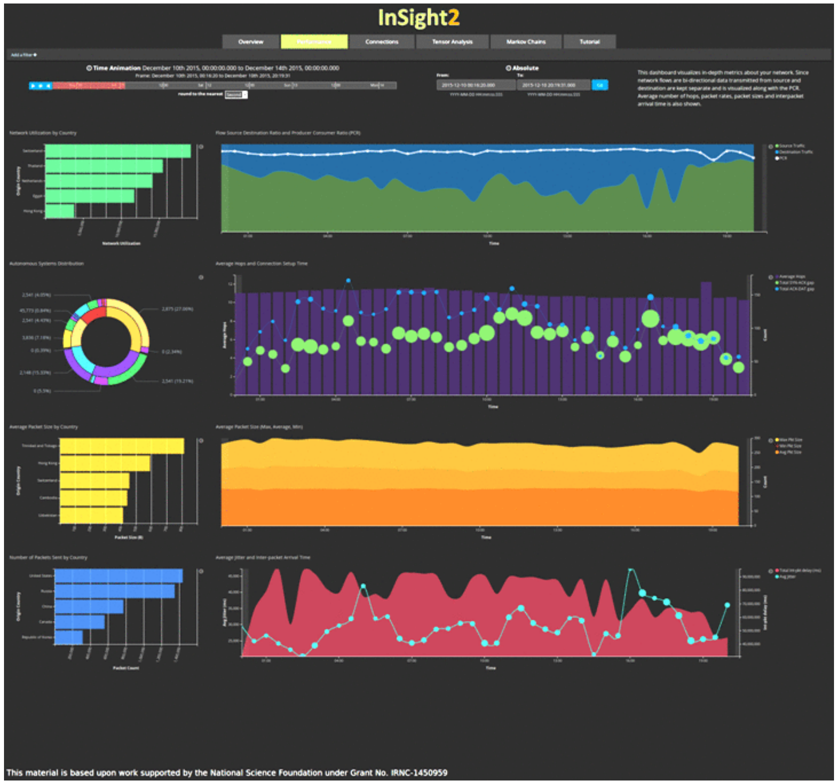
- Activity gauges, plots
- Country tag clouds
- Interactive geomaps
- Main player listings
- Intuitive data filtering
- Automatic data zoom



This material is based upon work supported by the National Science Foundation under Grant No. IRNC-1450959

InSight2 Performance Dashboard

- Traffic ratio and PCR
- Setup time and hops
- Packet Size
- Jitter and inter-packet arrival time



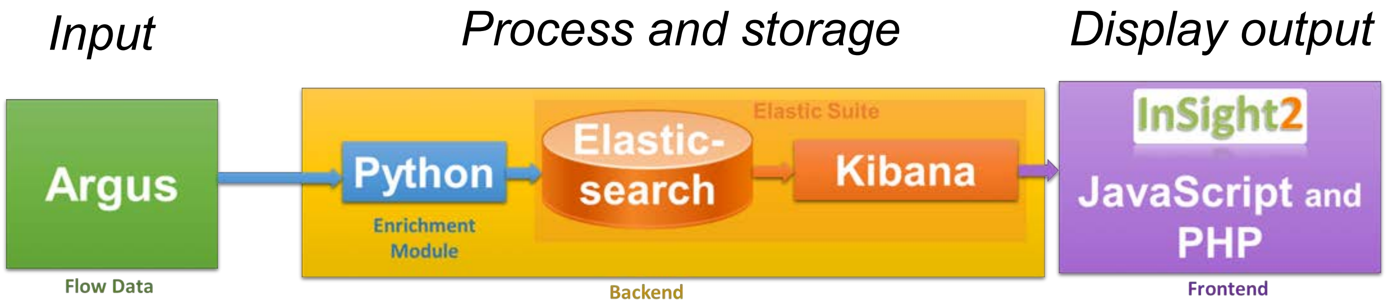
InSight2
Overview
Performance
Connections
Tensor Analysis
Markov Chains
Tutorial
Add a filter
Time Animation December 10th 2015, 00:00:00.000 to December 14th 2015, 00:00:00.000
Frame: December 10th 2015, 00:16:20 to December 10th 2015, 20:19:31
round to the nearest Second
Absolute
From: 2015-12-10 00:16:20.000
To: 2015-12-10 20:19:31.000
Go
Network Utilization by Country
Flow Source Destination Ratio and Producer Consumer Ratio (PCR)
Source Traffic
Destination Traffic
PCR
Autonomous Systems Distribution
Average Hops and Connection Setup Time
Average Packet Size by Country
Average Packet Size (Max, Average, Min)
Number of Packets Sent by Country
Average Jitter and Inter-packet Arrival Time

This dashboard visualizes in-depth metrics about your network. Since network flows are bi-directional data transmitted from source and destination are kept separate and is visualized along with the PCR. Average number of hops, packet rates, packet sizes and interpacket arrival time is also shown.

This material is based upon work supported by the National Science Foundation under Grant No. IRNC-1450959

Goals Completed 1/5

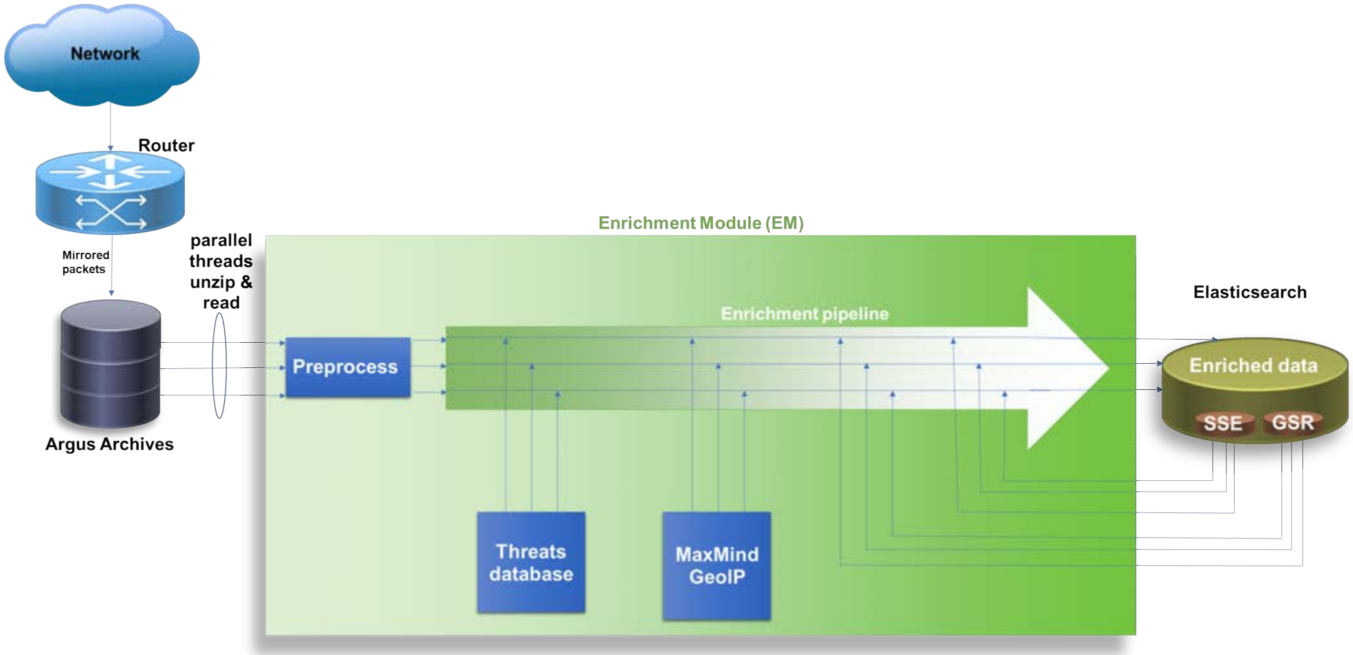
- Object oriented design and implementation
- Developed from scratch using simplified and robust software architecture



InSight2 Architecture

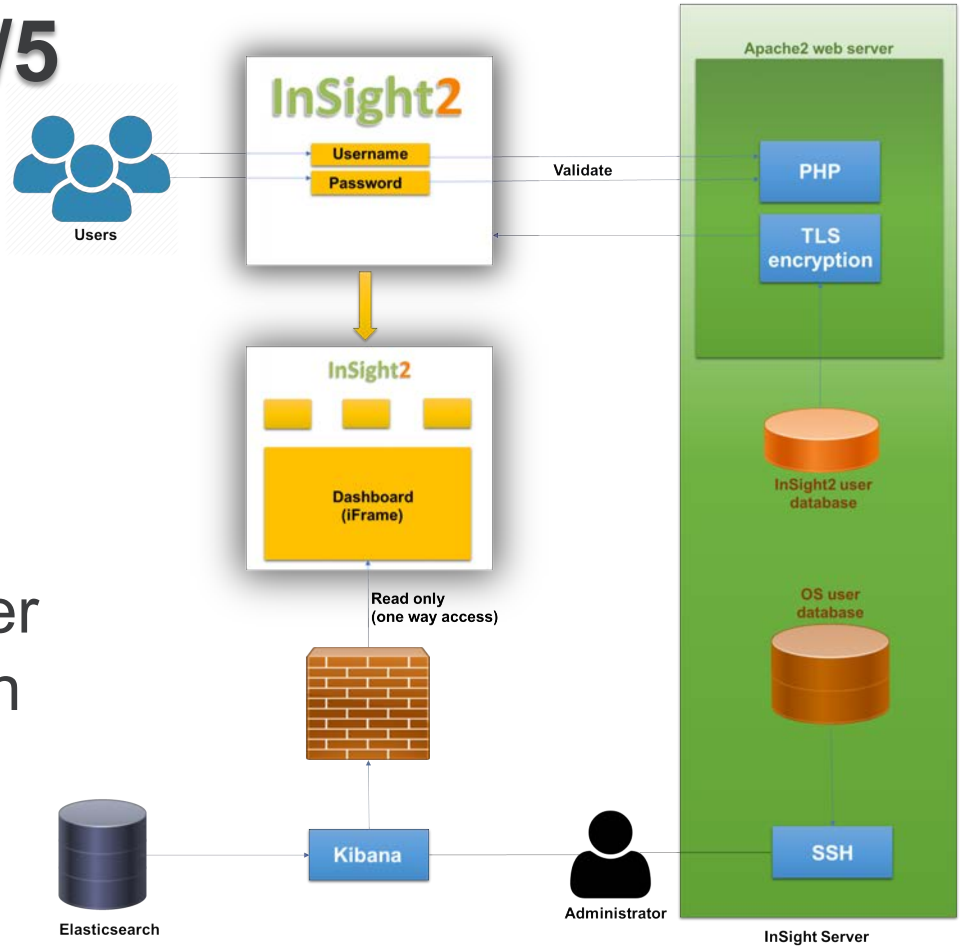
Goals Completed 2/5

- Python based multi-threaded data enrichment



Goals Completed 3/5

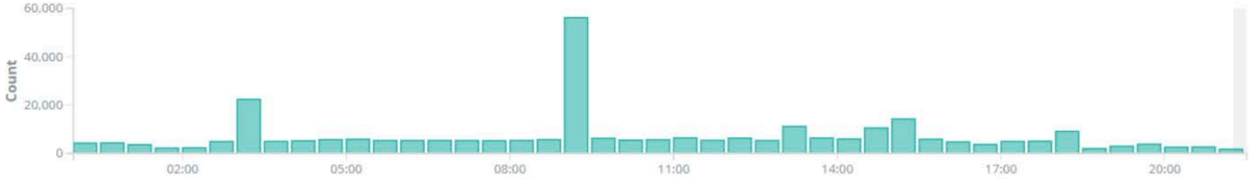
- Security features:
  - ✓ Authentication
  - ✓ TLS encryption
  - ✓ System admin and user dashboard segregation



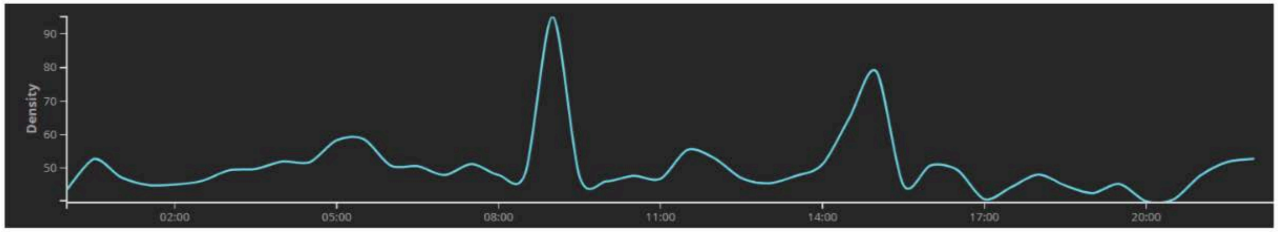
Goals Completed 4/5

- Tensor based event detection: RED Alert
- Example: Connectivity → Botnet detection

Num. active known Botnets



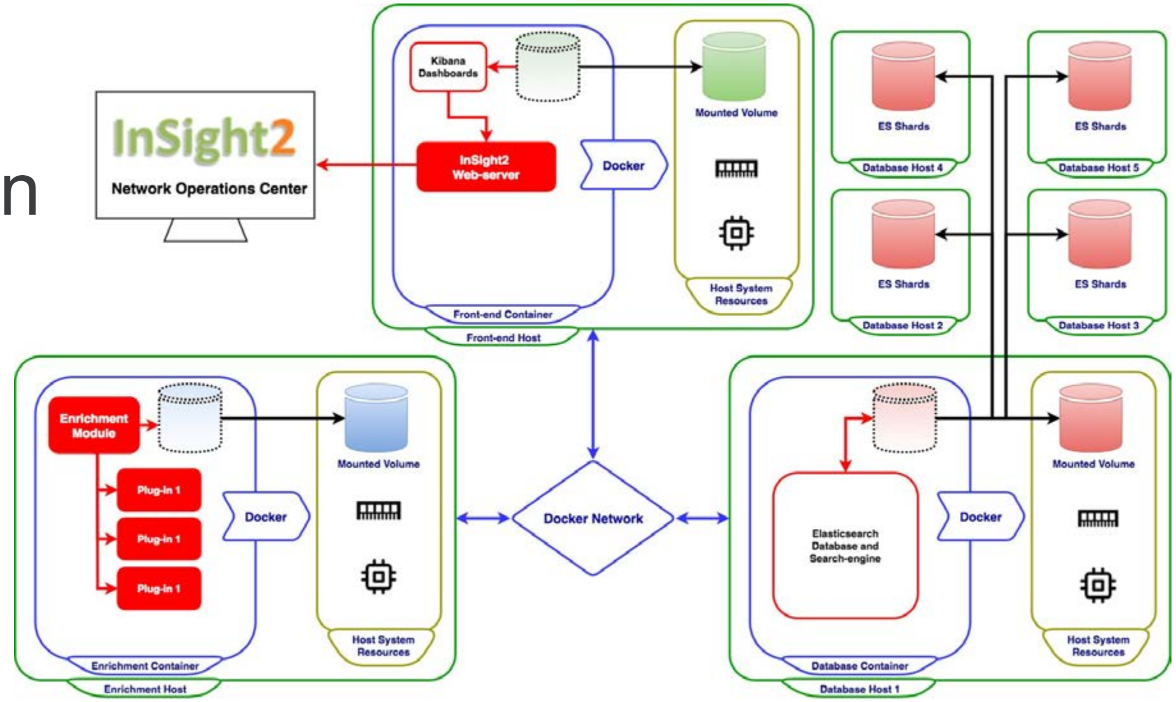
Botnet presence estimate based on num. conn.



Host IPs identified by automatically filtering data. Some false pos/neg alerts.

Goals Completed 5/5

- Docker based code distribution
- Third-party plugin support
- Available via GitHub soon!



Work in Progress

- Markov chain based prediction and analysis
  - Multiple simultaneous models (different data)
  - Run-time inference (user-defined data, model)
- Deep learning based data analysis
  - Example: identification of compromised host IPs
- Live-data testing at KISTI and Stanford Univ.
- Building user community (want to be part of it?)