2019 S&T Cybersecurity and Innovation Showcase

Solutions Now I Innovations for the Future

Homeland Security

Science and Technology

HI-CUBE: Hub for Internet Incident Investigation

Alberto Dainotti | CAIDA, UC San Diego

March 18, 2019

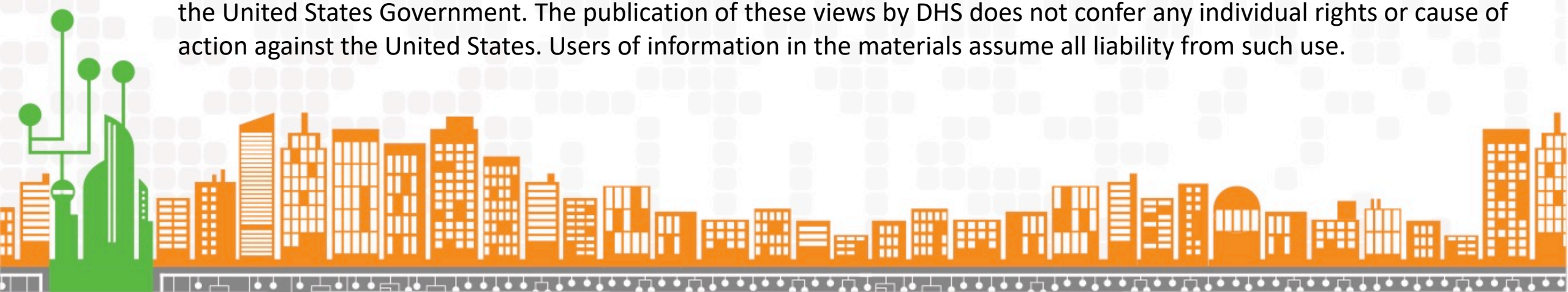
Homeland Security
Science and Technology

Funded Contract Information
This material is based on research sponsored by the Department of Homeland Security, Science and Technology Directorate via contract number FA8750-18-2-0049.

No Endorsement Notification
Any reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the Department of Homeland Security or the United States Government.

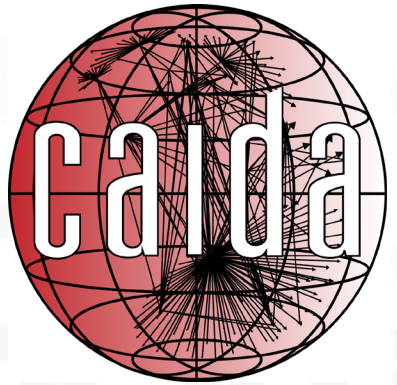
Hyperlinked Web sites do not constitute endorsement by DHS of the Web site or the information, products, or services contained therein. DHS does not exercise any editorial control over materials on this website or the information on non-DHS Web sites.

Disclaimer Notification
The views, opinions, findings, conclusions, or recommendations expressed in this presentation are those of the authors and do not necessarily reflect the official policy or position of the Department of Homeland Security (DHS) or the United States Government. The publication of these views by DHS does not confer any individual rights or cause of action against the United States. Users of information in the materials assume all liability from such use.



Team Profile

- PI: Dr. KC Claffy – Director
- CoPI: Dr. Alberto Dainotti – Research Scientist
- CAIDA – Center for Applied Internet Data Analysis
  University of California, San Diego



Customer Need

- Large-scale Internet incidents are a major threat to public safety and to both public and private strategic and financial assets
  - *E.g., hijacks, outages, spam and fishing campaigns, botnet activities, scanning, large-scale bug exploitation*
- They are often undetected and hard to understand (dynamics, motivation, infrastructure used, source, target)
- We need timely and effective detection and analysis

Approach - Overview

- A web-based collaborative environment
- with trusted groups of vetted experts
- producing analyses with interactive and visual tools
- based on diverse sets of streamed (and historical) data

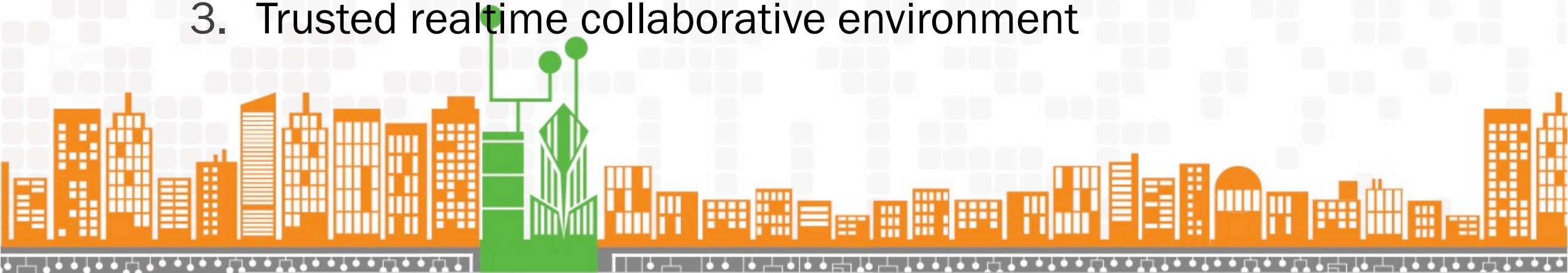
HUB Internet Incident for Investigation

Approach – Main Concepts

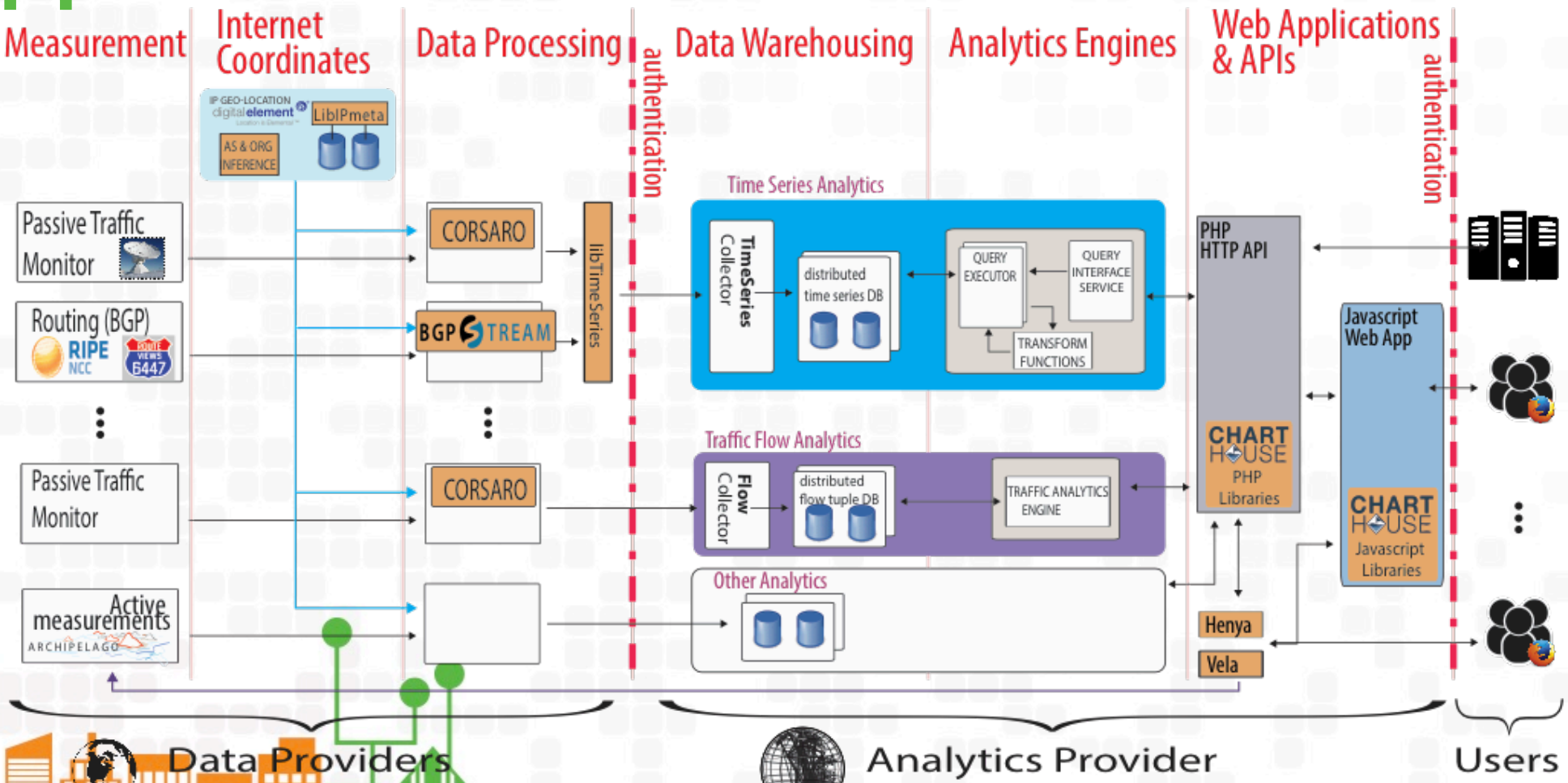
1. Combination and correlation of diverse Internet cyber-security data streams around a set of common dimensions: *time and Internet Coordinates*

2. Data analytics in the form of *interactive exploratory data analysis* and configurable event detection

3. Trusted realtime collaborative environment

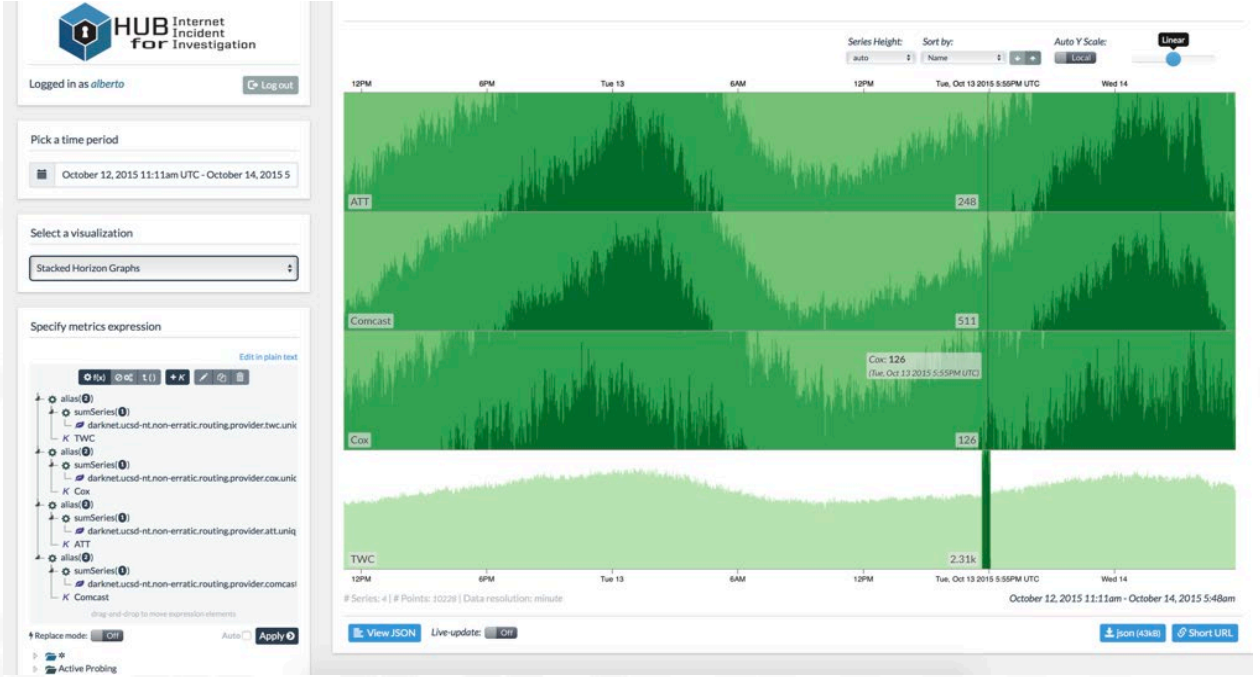


Approach - Architecture



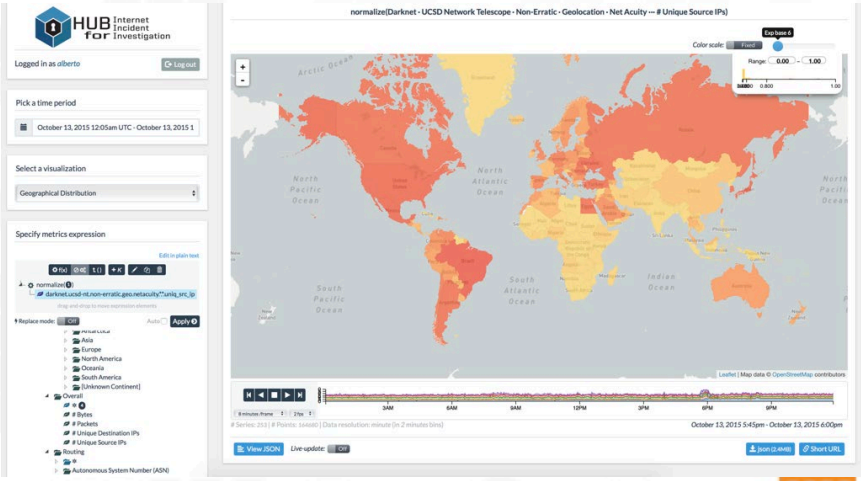
Benefits

- Enhances our ability to understand large-scale incidents
- Provides live streams of data
- Combines multi-source data
- Enables collaborative analysis
- Extensible
- Lowers the barrier for data provision/consumption



Investigation of a 25 min event: UDP port 1900 traffic reaching our Darknet and originating from every country except China. Among top 5 US providers, such traffic appears as originating only from TWC

(Oct 2015)



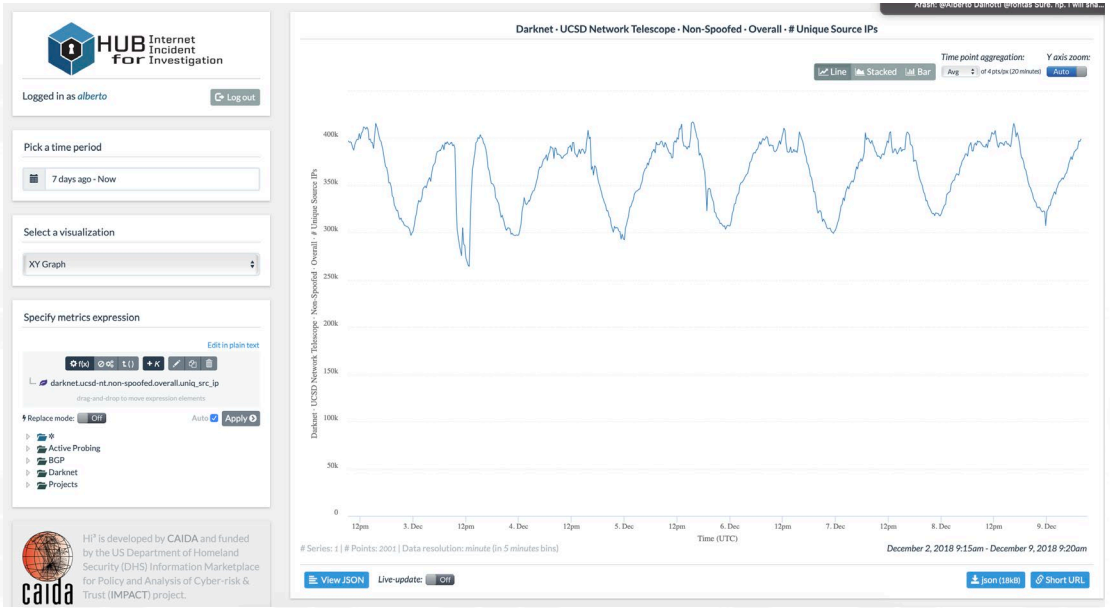
Competition/Alternatives

- Internet telemetry data analysis and event detection systems typically
  - focus on a single type of data or one class of events
  - are non collaborative
- Potential synergy with
  - DHS IMPACT performers
  - Threat intelligence platforms

Current Status 1/2

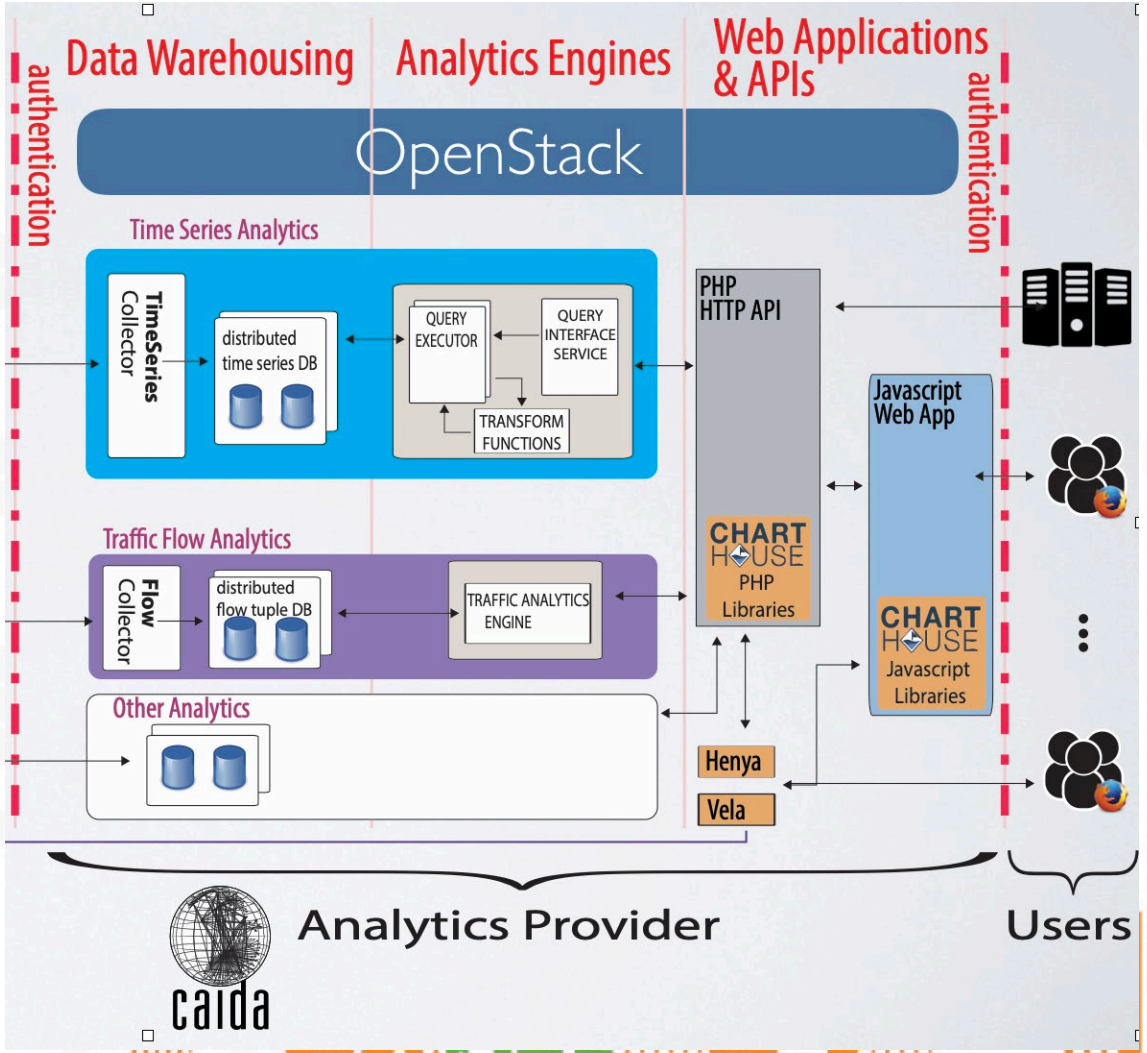
- Proof of concept is online!
  - Time-series exploration
  - Visualizations include geographic dimension
- Live streams + historical data:
  - Passive traffic from Network Telescopes
  - Internet outage alerts and raw signals
  - Denial of Service attack data
  - Global Internet routing data

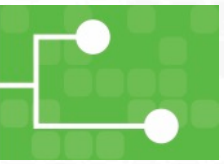
https://hicube.caida.org



Current Status 2/2

- Authentication and Authorization system
  - OAuth 2.0
  - OpenID Connect
- OpenStack-based private cloud
- Data Warehousing infrastructure
  - Distributed Object Storage (Swift)
    - HTTP API
    - High-throughput (> 20Gbps) + Large Capacity (1.2 PB)
    - Reliability + Scalability
  - SSD Cluster
    - Low latency + Reliability + Scalability





Next Steps

- Beta Users
- Case studies
- Time Series Analytics Engine
  - distributed database for time-series analytics
  - data analytics query engine
- Traffic Flow Analytics Engine (pending funding)
- More data sources
  - BGP Hijacking events, …

Potential Transition Activities

- USG situational awareness and decision support
- Industry consumption, quid pro quo
  - E.g. Internet security, threat intelligence, Internet telemetry, fusion centers, …
- Open source certain components
- Crowdsource analyses
- Education & training engagement

Contact Info

Alberto Dainotti
CAIDA, University of California San Diego
alberto@caida.org
+1-858-534-9249
@AlbertoDainotti
https://hi-cube.caida.org
http://www.caida.org/funding/impact-assists/

2019 S&T Cybersecurity and Innovation Showcase

Solutions Now I Innovations for the Future

Homeland Security

Science and Technology