SOC Data flow

Mapping the flow of data in a next-generation security operations center

Pragmatic solutions in existing and emerging technology

New challenges for SOCs

The nature of security and intelligence is dynamic.

- In the last two decades the nature of war/terrorism has changed with non-state actors defining and driving the actions and response of states. In turn, this is redefining the definition of war/aggression and defense/response.
- In the last decade the nature of communication has changed with smartphones and tablets redefining what is shared, how much is shared, how widely it is shared, how quickly it is shared, and what is trusted. This new digital paradigm is redefining politics, nation-on-nation and/or non-state-on-nation aggression, and the blurred the lines between propaganda/sedition/advocacy and crime/warfare/terrorism.
- Citizens now carry instruments that can capture images and/or videos, edit/annotate/manipulate the images and/or videos, and then transmit those videos to anywhere on the planet within seconds.

Next generation SOC

Most security operations centers (SOCs) are designed on the basis of the original needs of military and/or first-responder agencies/organizations.

Depending on the age and origin of the SOC, they may or may not have integrated emerging elements of technology, or addressed the changes brought by a digital society, non-state actors, and cyber warfare.

This presentation is an outline of the data flow in a SOC that recognizes and leverages emerging technology and the digital flow of data.

Sensor data

Although not all SOCs do or will receive sensor data, as sensors become lower in cost and integration becomes simpler, sensor data is exploding in importance. This includes cyber data and the monitoring of the Internet of things (IoT).

In parallel, the integration of cell phone images and drone images is adding to the instantly available data.

Pragmatic solutions in existing and emerging technology

Dedicated source data

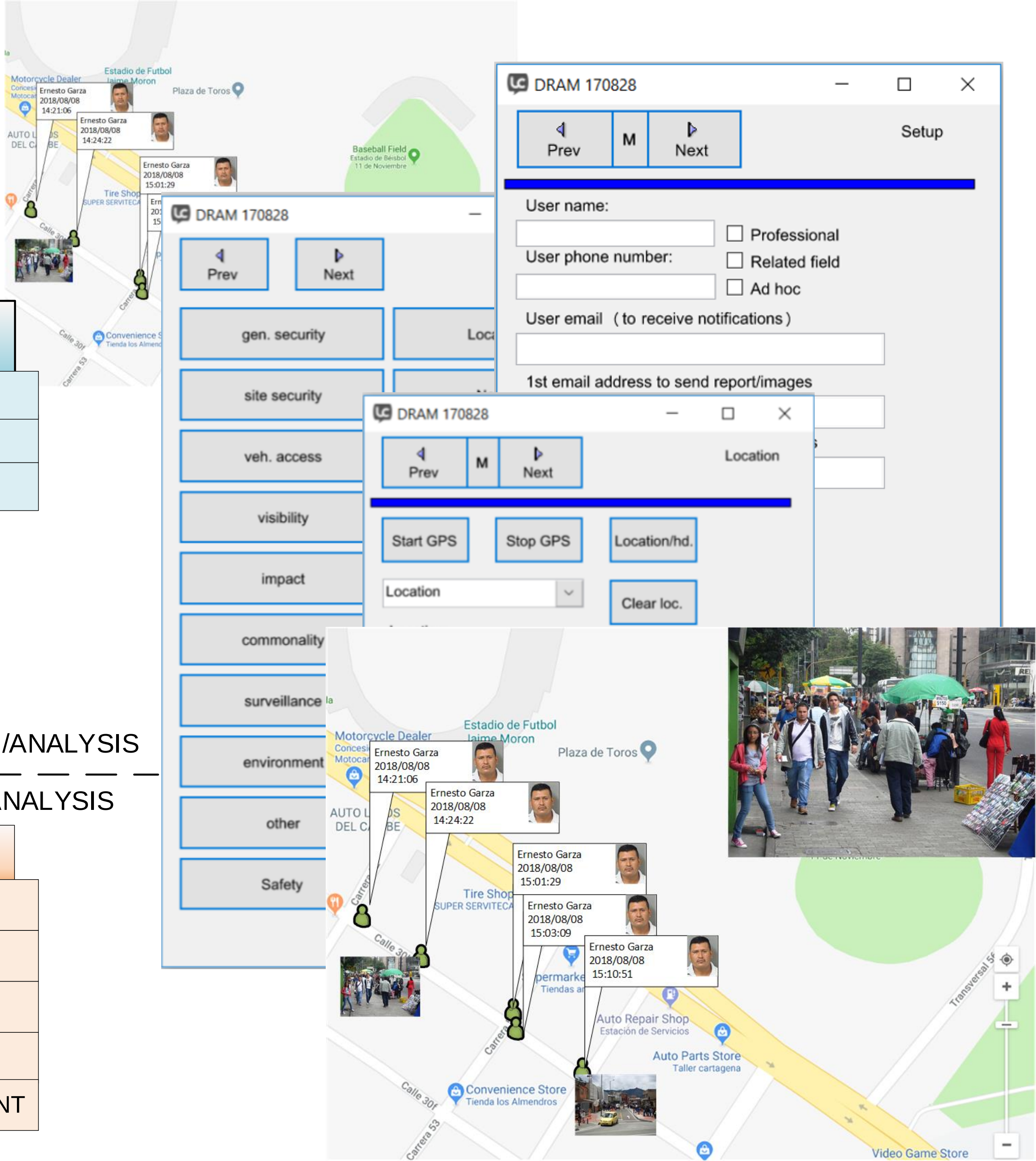
Dedicated source data from reports, assessment tools, surveillance, and more traditional HUMINT (human intelligence) and SIGINT (signal intelligence) are becoming digitized through the power of smartphones/tablets. DRAM, IF-Eyes, Trapwire, etc., are smartphone-enabled data sources leveraging the on-board capabilities of the platform.

Sensor data
- Sensors
- Cameras
- Drones

MACHINE GATHERING/ANALYSIS

HUMAN GATHERING/ANALYSIS

Dedicated source data
- Reports
- DRAM
- IF Eyes
- Trapwire
- HUMINT/SIGINT



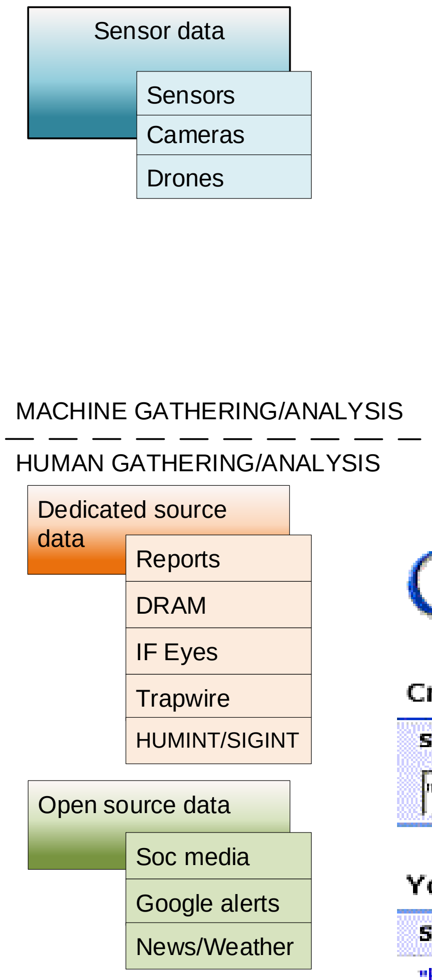
Pragmatic solutions in existing and emerging technology

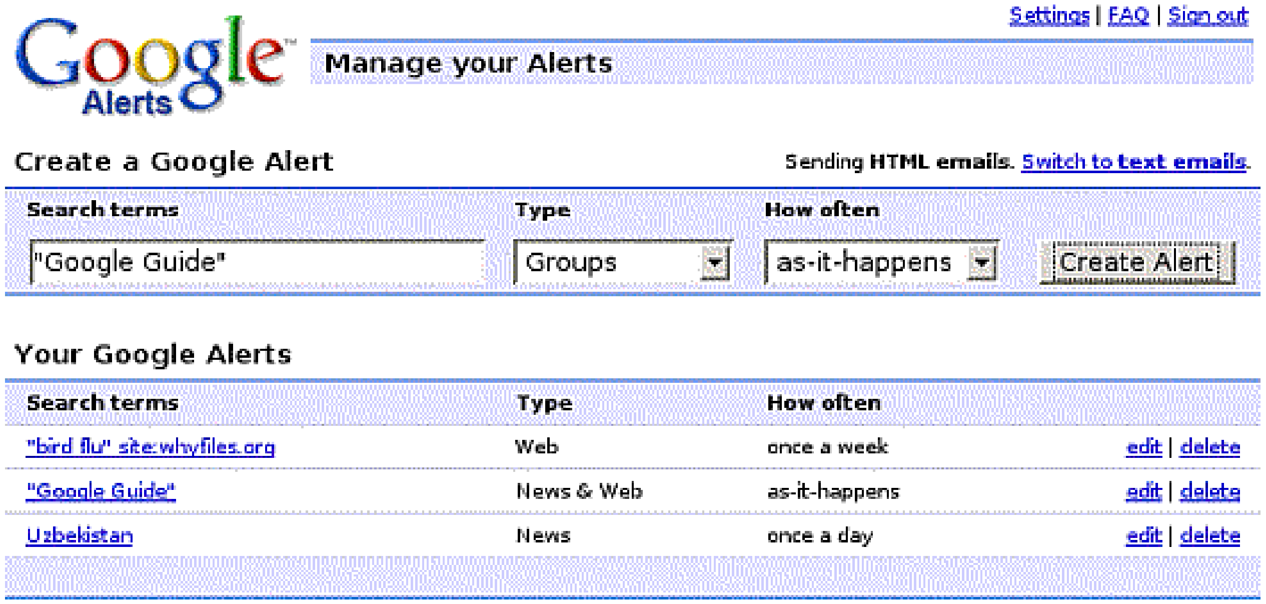
Open-source data

73% of Americans are engaged in some form of social media spending an average 135+ minutes a day on social media.(1) This makes social media one of the most prevalent and accessible sources of data in human history.

Subject-specific alerts can scan data across social media, news, blogs, and weather to automate the data monitoring process.

(1) http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/





LTL
Pragmatic solutions in existing and emerging technology

Open-source data

Through the power of digital media, vast resources are now available online. Publicly curated material (Wikipedia), maps, publications, and other sources are staggering in their scale and scope.

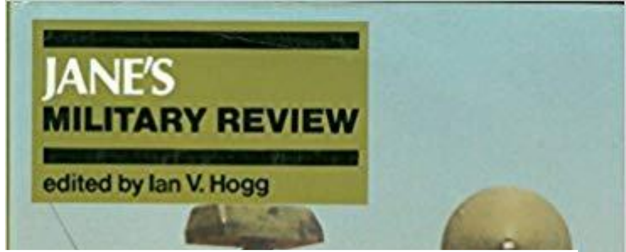
Even as SOCs struggle with the quality/reliability of publicly curated material data, the maxim has become: “the first place to look, but not the last.”

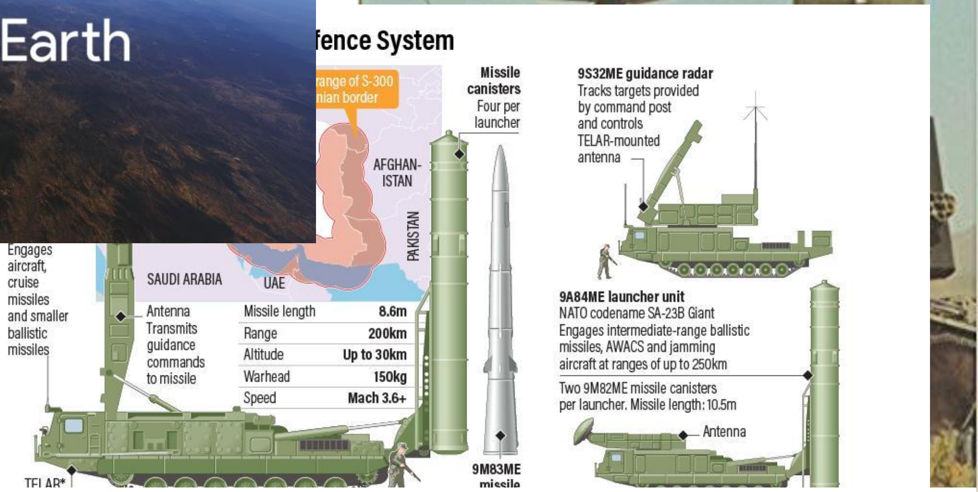
- Sensor data
  - Sensors
  - Cameras
  - Drones

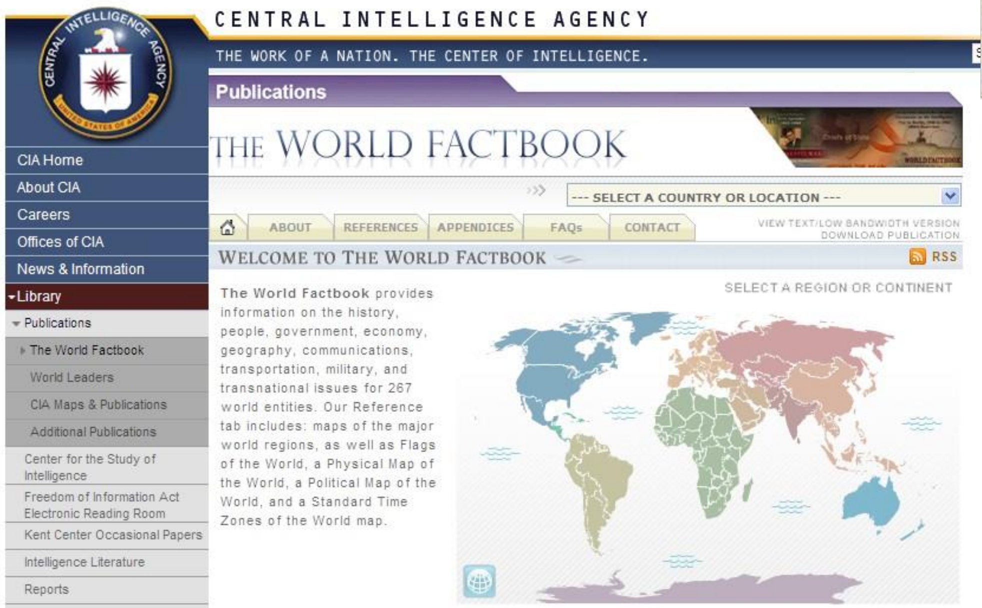
MACHINE GATHERING/ANALYSIS

HUMAN GATHERING/ANALYSIS

- Dedicated source data
  - Reports
  - DRAM
  - IF Eyes
  - Trapwire
  - HUMINT/SIGINT
- Open source data
  - Soc media
  - Google alerts
  - News/Weather
- Historic data
  - Maps
  - CIA fact book
  - Wikipedia
  - Janes



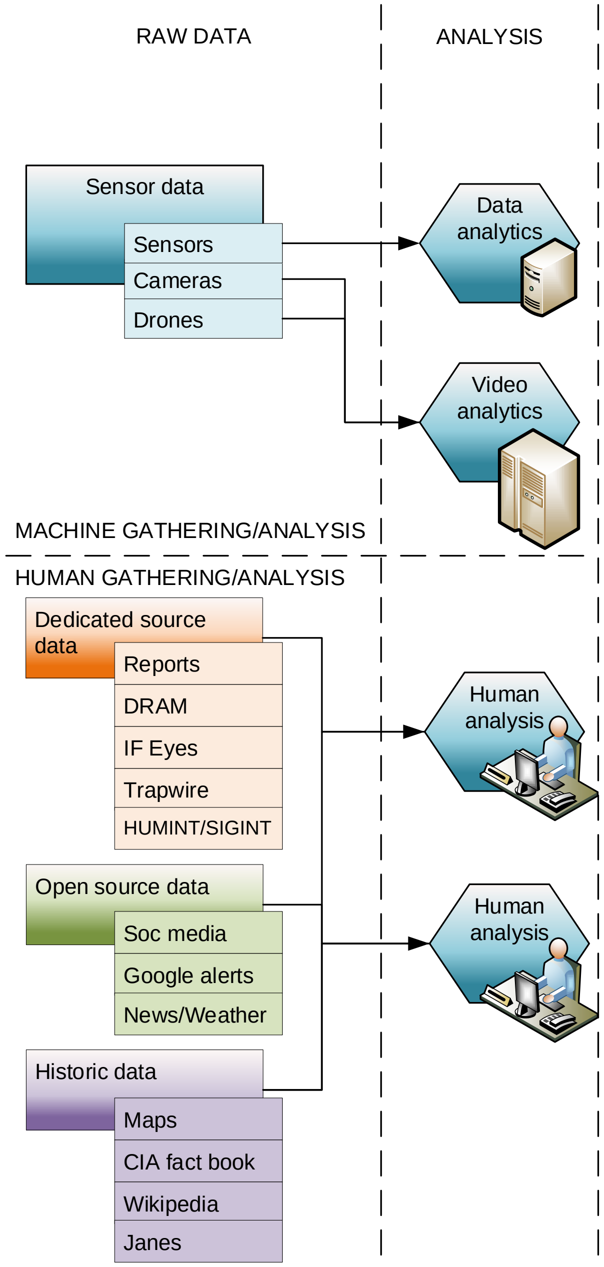


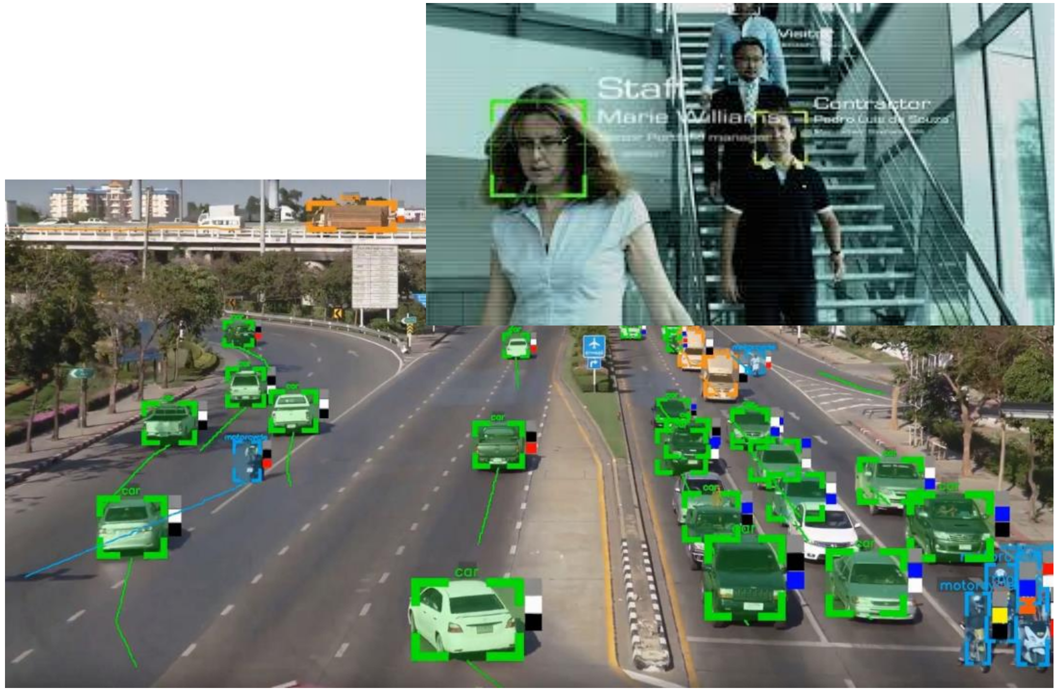


Pragmatic solutions in existing and emerging technology

Analysis

Each type of raw data is subjected to analysis. Sensor data and images are subjected to algorithmic and/or rule-based analysis, and dedicated-source, open-source, and historic data are subjected to human analysis.

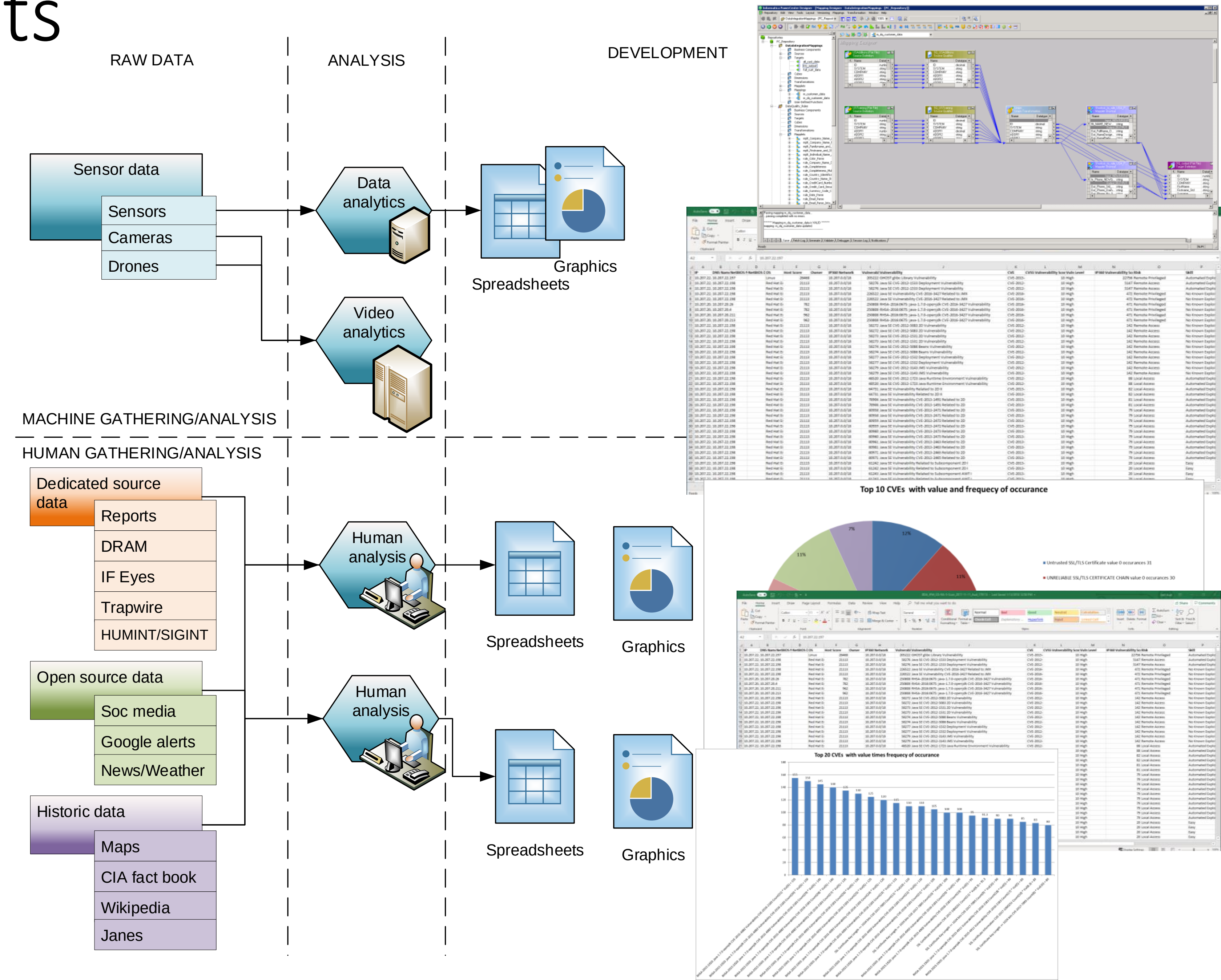




Pragmatic solutions in existing and emerging technology

Developed products

Subsequent to analysis, developed products are produced as spreadsheets and derived graphics.

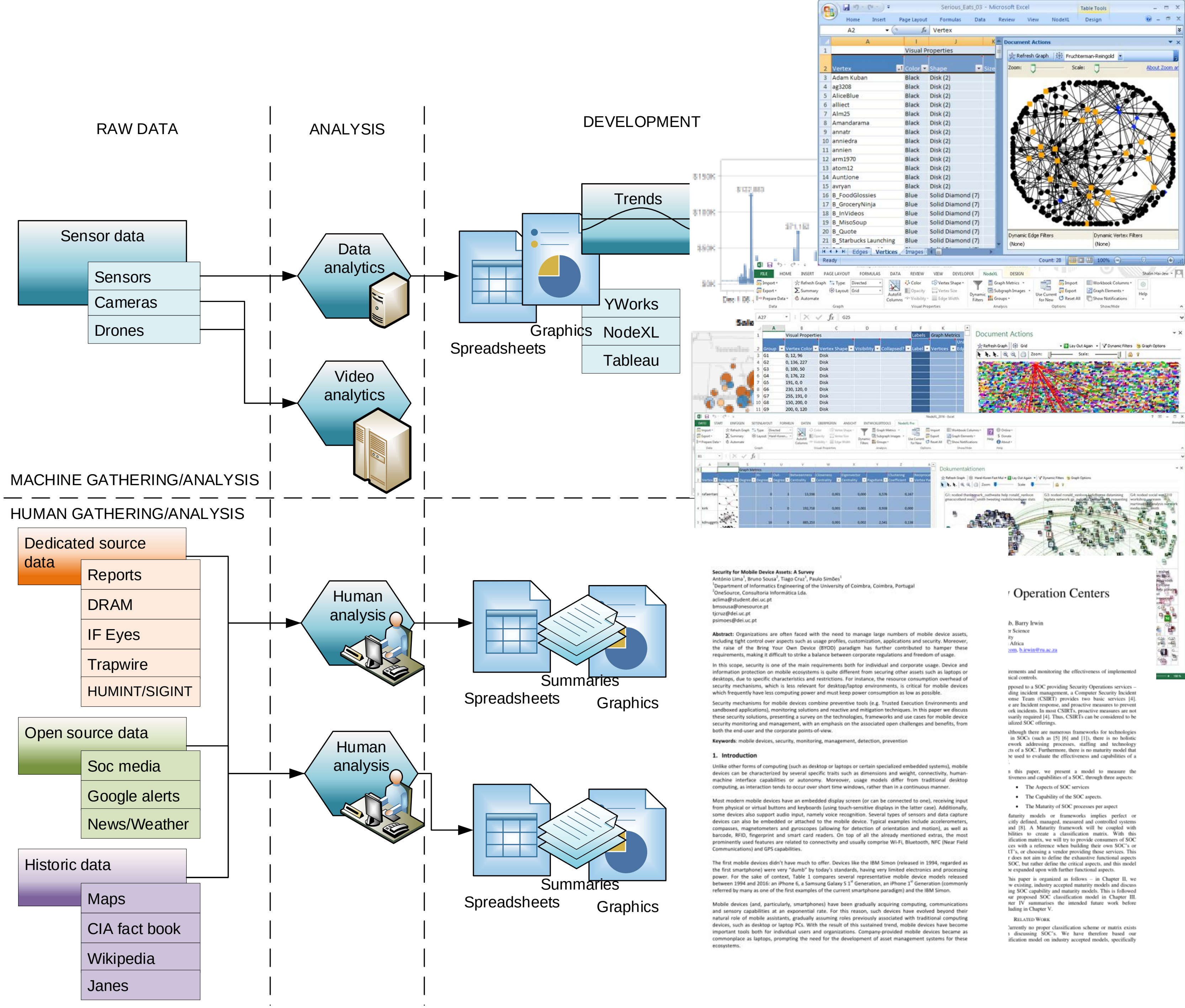


LTL
Pragmatic solutions in existing and emerging technology

Reduction

Developed products are then reduced into graphics and/or written summaries.

Popular tools for the production of graphics include: Yworks, NodeXL, and Tableau.

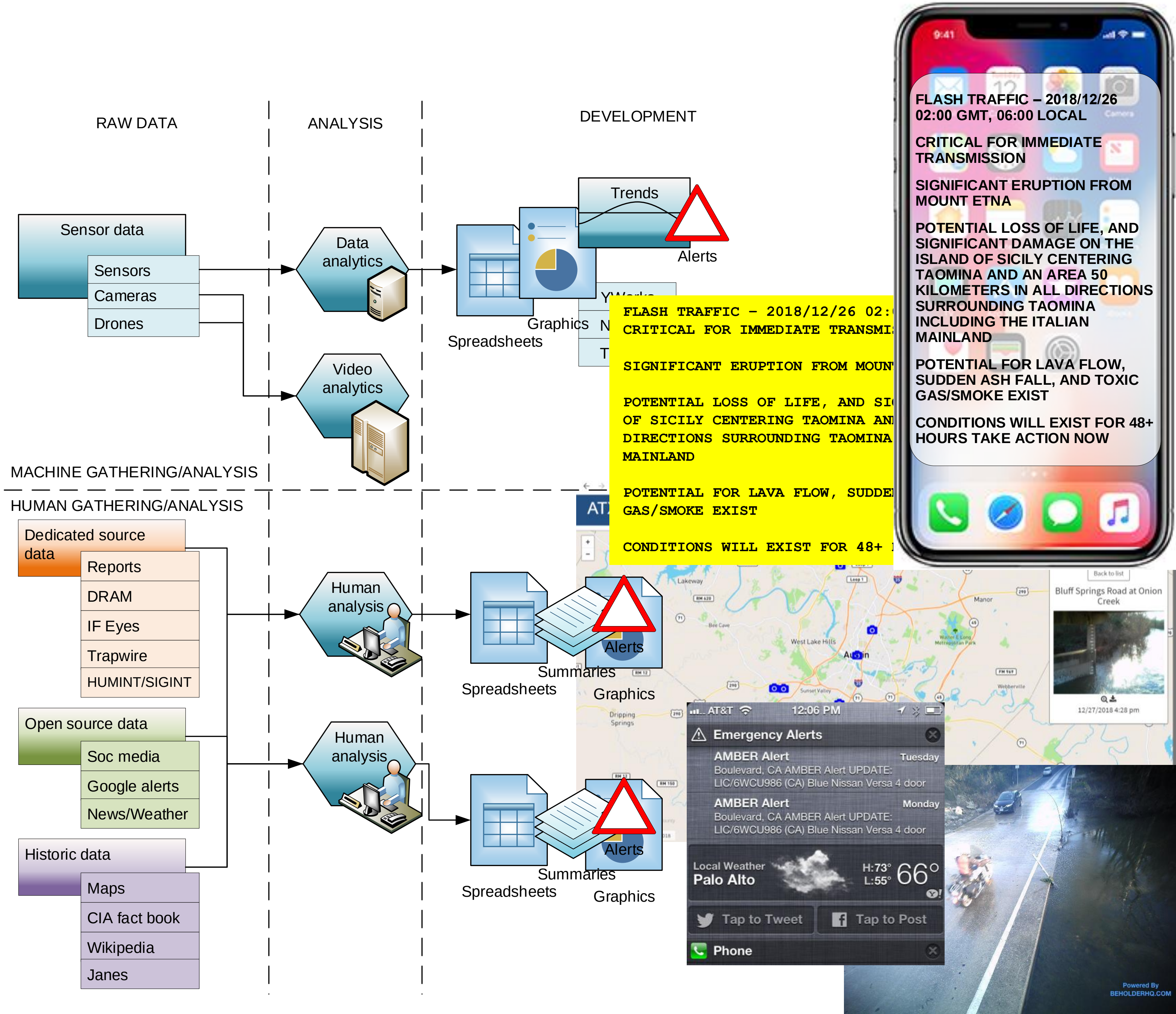


Pragmatic solutions in existing and emerging technology

Alert

In some cases, either machine- or human-generated alerts are issued based upon the analysis/development process.

Generated on an as-needed basis, the alerts are transmitted as actionable intelligence across multiple media to specific or general audiences.

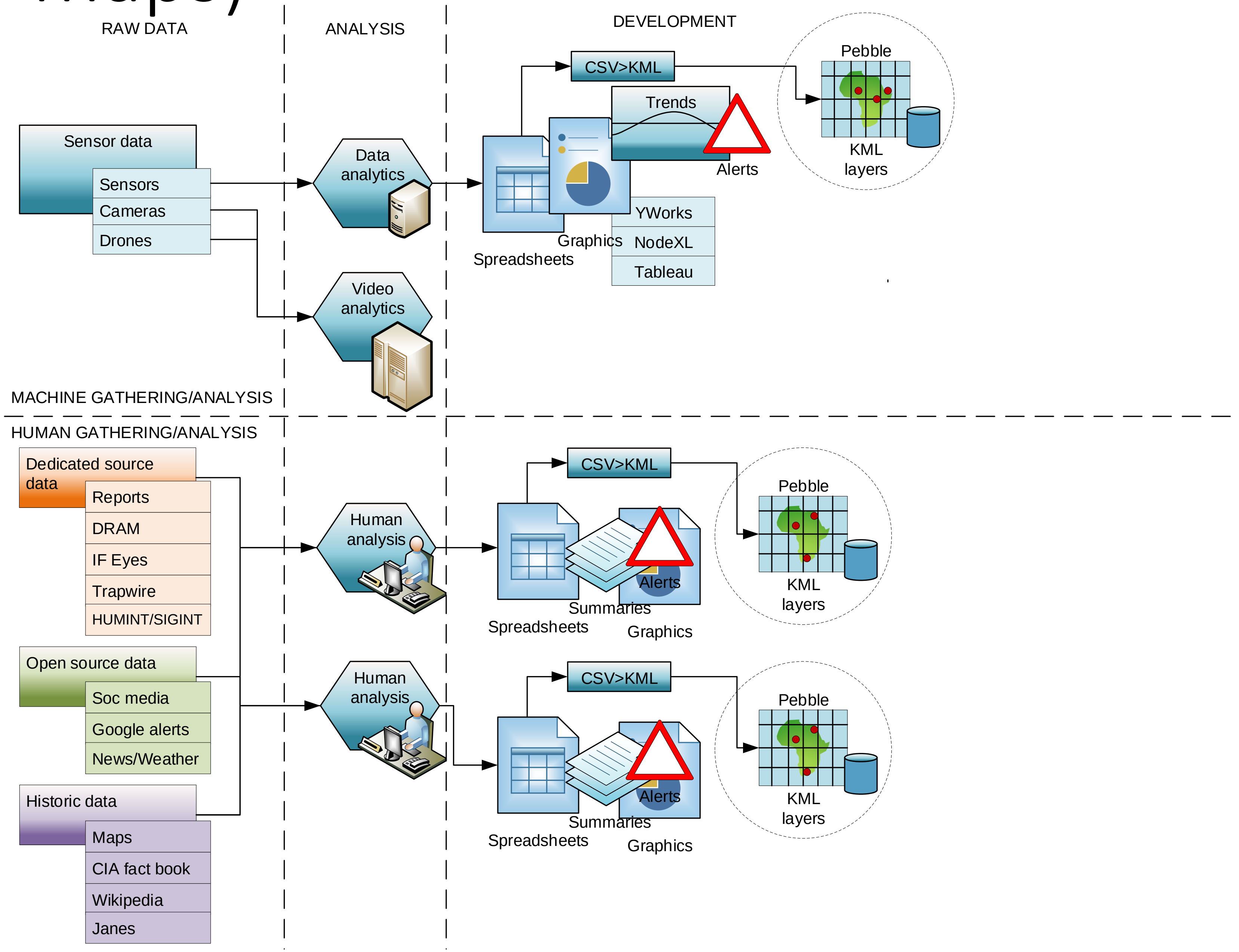


Pragmatic solutions in existing and emerging technology

CSV > KML (data to maps)

Spreadsheets with geospatial data are rendered from CSV files (comma separated variables) to KML files (keyhole markup language) to create map/database "Pebbles."

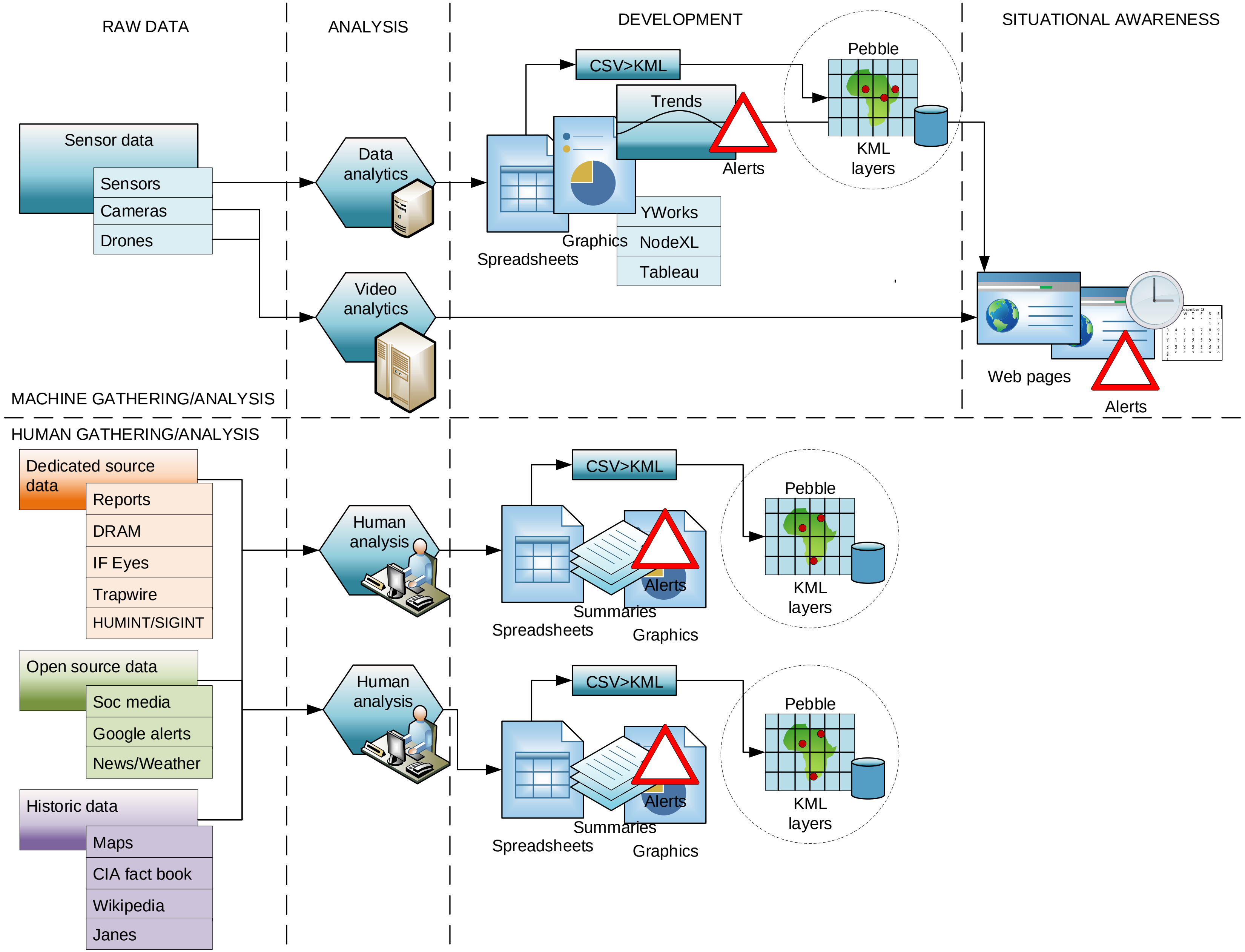
KML files can display geospatial data on Google Earth, ESRI, Mapbox, etc., and can include icons with "drill-down" data links.



LTL
Pragmatic solutions in existing and emerging technology

Situational awareness

In combination, the geospatial data, alerts, and webpages derived from the data provide automated situational awareness "dashboards" that can be updated in real time, by the hour, or by the day.

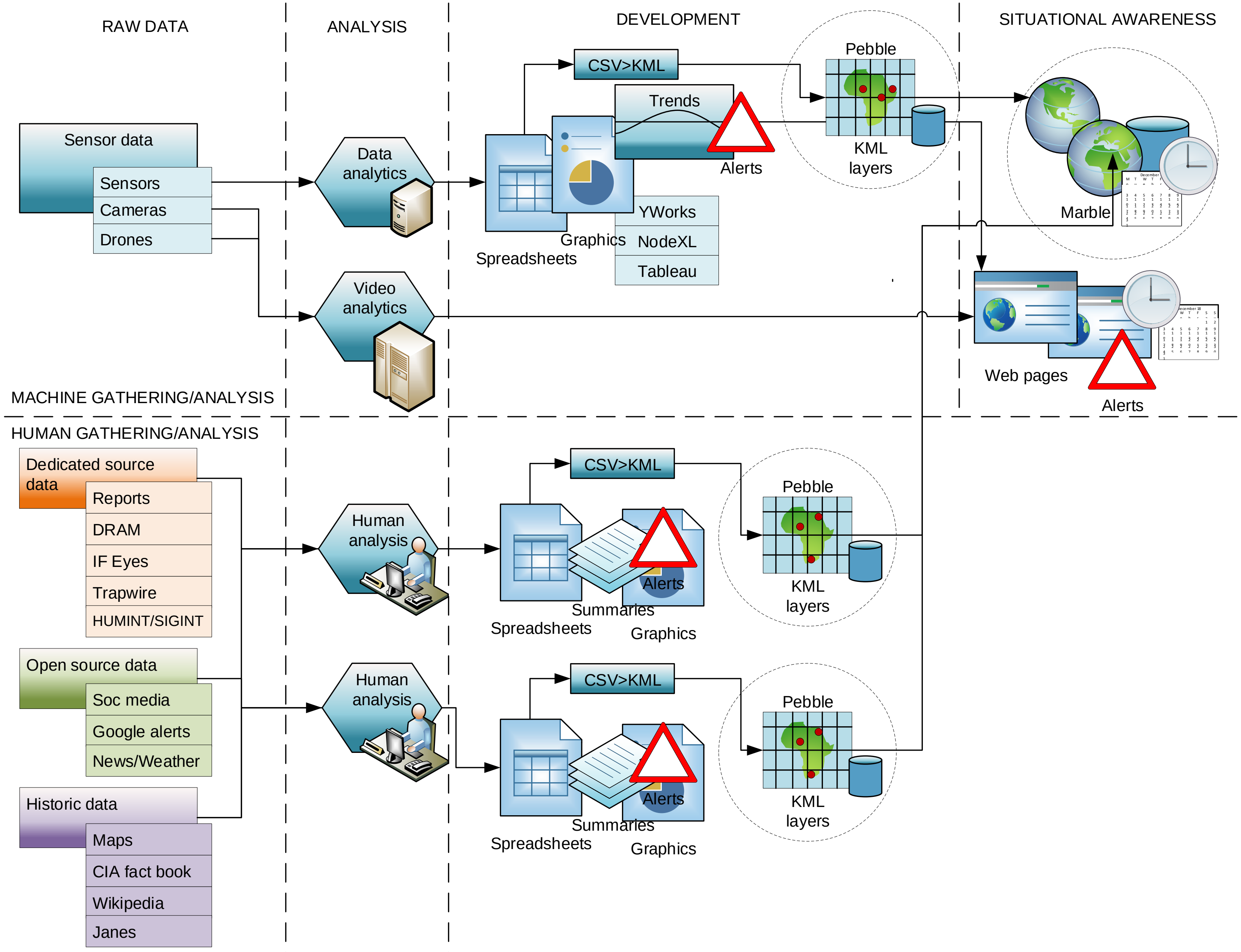


LTL
Pragmatic solutions in existing and emerging technology

The "Marble"

In parallel to the situational awareness provided by the webpages and alerts, the "Pebbles" feed the blue "Marble" as a comprehensive geospatial presentation of data.

Each layer provided by a "Pebble" contributes to the comprehensive "God's-eye-view" of the data with the embedded icons providing authorized drill-down capability to the referenced data.



Pragmatic solutions in existing and emerging technology

Flash traffic

On the basis of machine-and/or human-generated alerts, flash traffic is generated.

The flash traffic details the level of urgency (U), the impact (I), the scale (S), and the scope (S) of the alert.

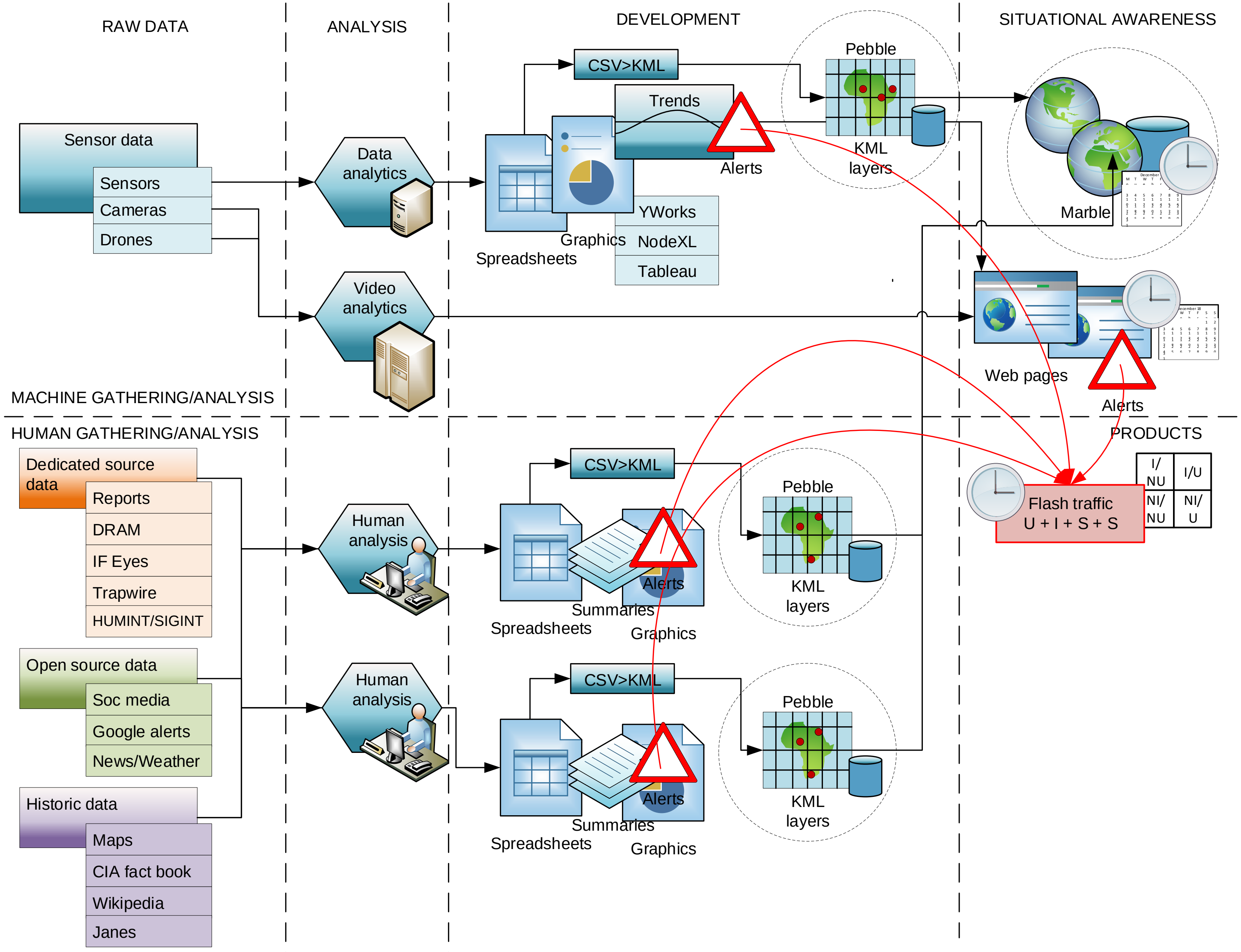
```
FLASH TRAFFIC – 2018/12/26 02:00 GMT, 06:00 LOCAL
CRITICAL FOR IMMEDIATE TRANSMISSION

SIGNIFICANT ERUPTION FROM MOUNT ETNA

POTENTIAL LOSS OF LIFE, AND SIGNIFICANT DAMAGE ON
THE ISLAND OF SICILY CENTERING TAOMINA AND AN AREA
50 KILOMETERS IN ALL DIRECTIONS SURROUNDING TAOMINA
INCLUDING THE ITALIAN MAINLAND

POTENTIAL FOR LAVA FLOW, SUDDEN ASH FALL, AND TOXIC
GAS/SMOKE EXIST

CONDITIONS WILL EXIST FOR 48+ HOURS TAKE ACTION NOW
```



LTL

Pragmatic solutions in existing and emerging technology

Important/Urgent

By a machine algorithm/rule set and/or human judgement, flash traffic follows the important/urgent paradigm.

	I/NU Important, but not urgent	I/U Important and urgent
I		
	NI/NU Not important and not urgent	NI/U Not important, but urgent
		U

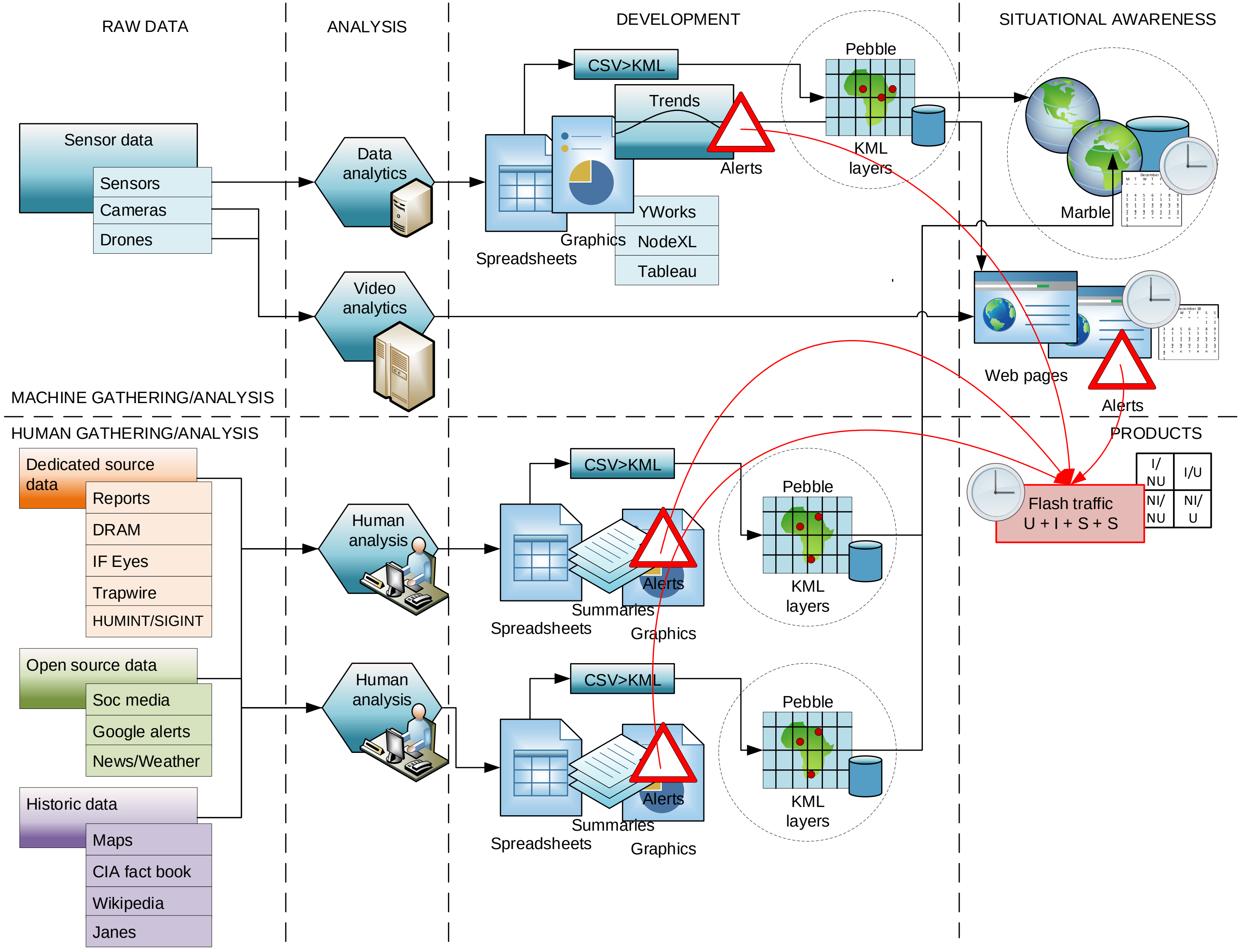
Examples:

I/NU = basic hygiene

NI/NU = social media

NI/U = typical phone call

I/U = flash traffic, alarms, etc.

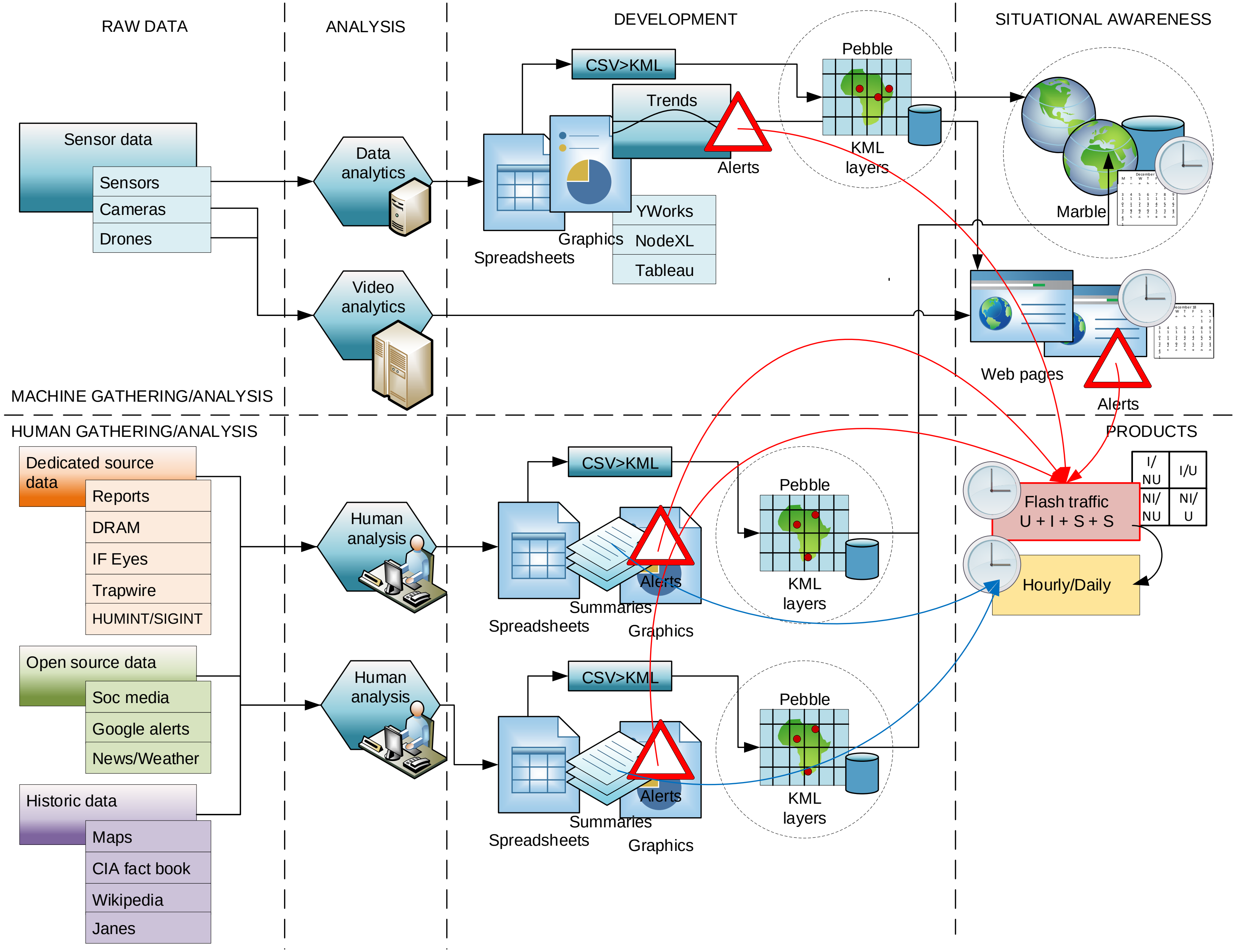


Pragmatic solutions in existing and emerging technology

Hourly/Daily

Flash traffic in combination with other analysis-produced material is combined into hourly or daily summaries, as defined by the needs of the SOC's clients.

This is not to rehash the data, but to codify and ensure capture of the data in sequence.

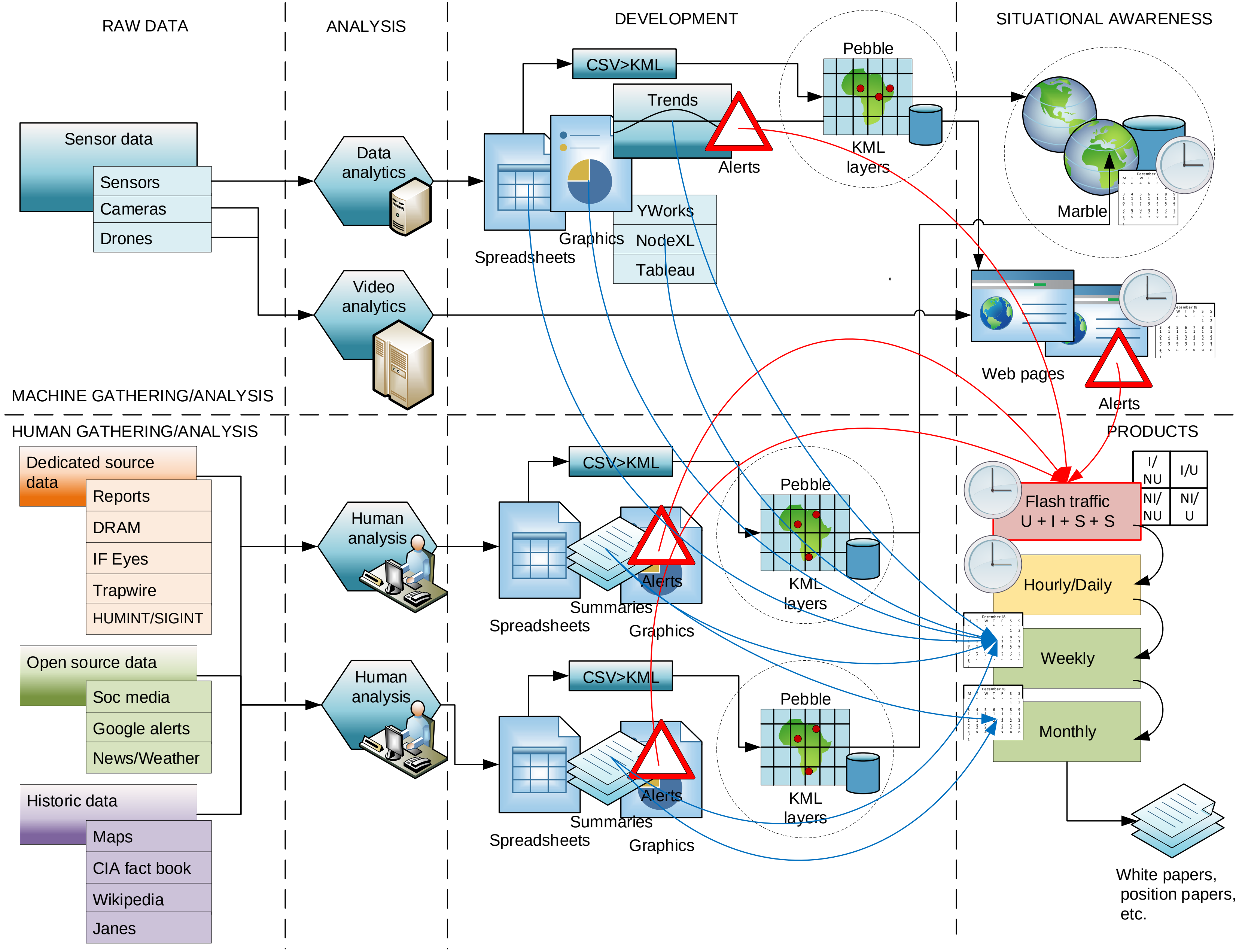


LTL
Pragmatic solutions in existing and emerging technology

Sensor data

In turn, the hourly, and/or daily, summaries feed weekly and monthly summaries.

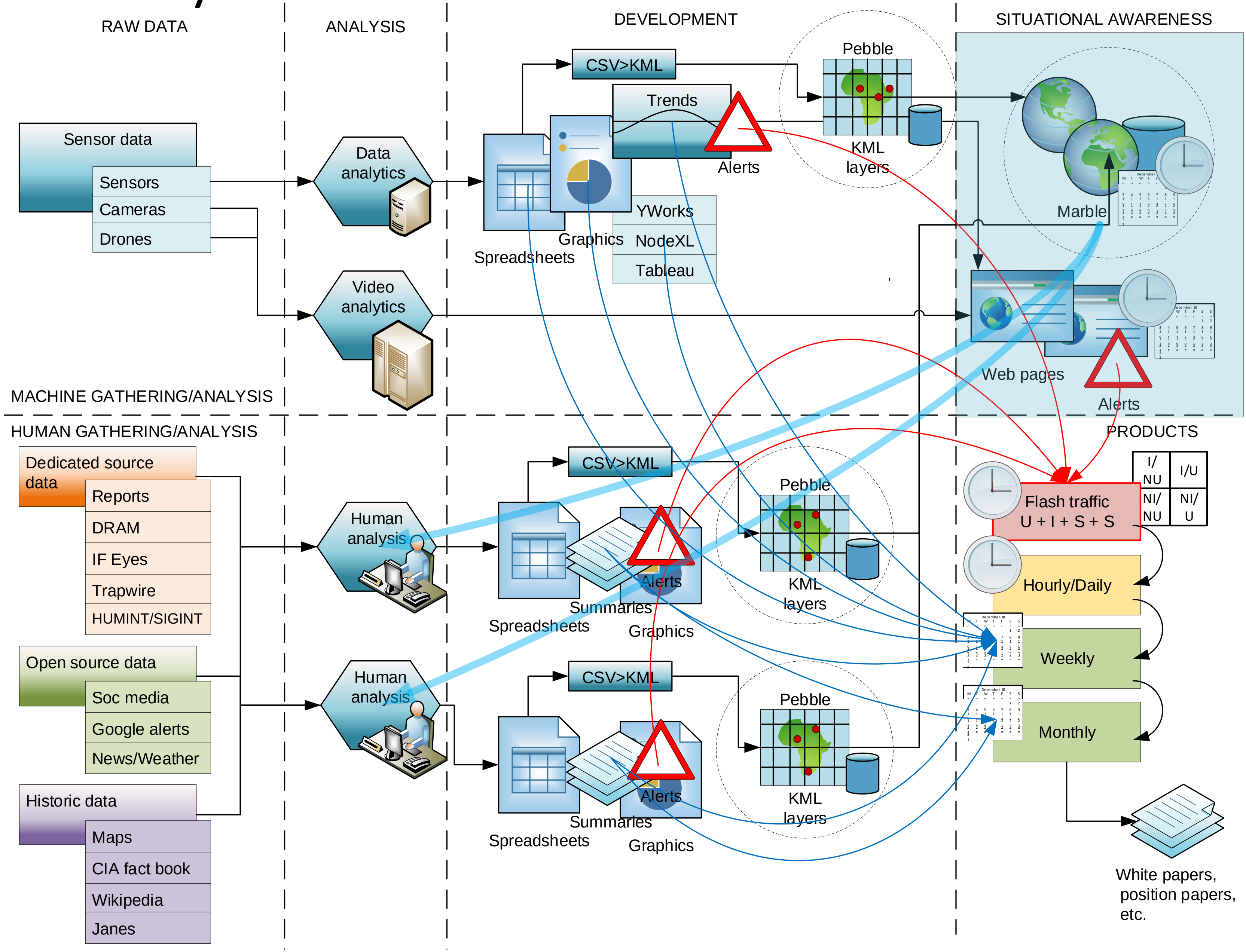
White papers, position papers, and other high-level products are produced from the summaries and machine-developed data.



Maturation of human analytics

The human analysis knowledge base and understandings are informed and matured via the situational awareness resources.

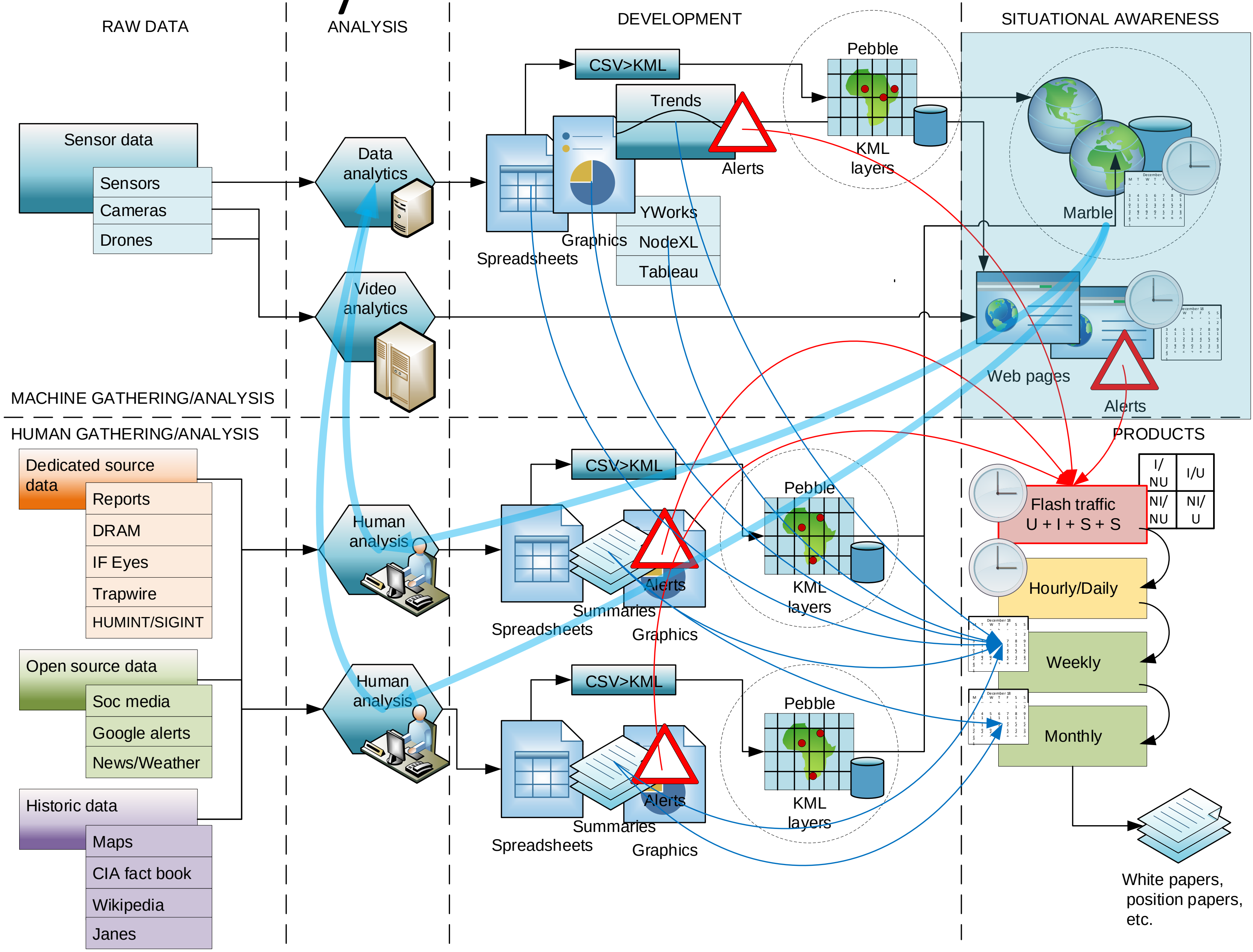
Non-obvious trends, indications, or relationships are detected and, in turn, are used to shape and define subsequent analysis.



Pragmatic solutions in existing and emerging technology

Maturation of machine analytics

In the same way that the situational awareness resources informed and matured the human analysis process, those insights guide the human analyst in refining and maturing the algorithms and protocols of the data analytics.



Pragmatic solutions in existing and emerging technology

Pragmatic solutions in existing and emerging technology

Questions and discussion?