

# SOC Data flow

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

# 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).

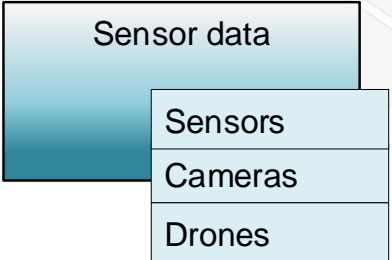
In parallel, the integration of cell phone images and drone images is adding to the instantly available data.

The collage features several data dashboards and images:

- Ruuvitag - temperature:** A line graph showing Celsius temperature from 09:00 to 12:00. The y-axis ranges from 15 to 35. Three data series are shown: 'ilmatieteen laitos' (black), 'ruuvitag' (purple), and 'ruuvitag2' (blue).
- Ruuvitag - air pressure:** A line graph showing hPa air pressure from 1005.0 to 1012.5. The data shows a slight downward trend over time.
- Ruuvitag - battery voltage:** A line graph showing mV battery voltage from 3000 to 3025. The data shows significant fluctuations between 3005 and 3020 mV.
- SecurityCenter BA-RoC Ser:** A table showing compliance information for various techniques.
- CSF - Activity Summaries (Last 72 Hours):** A table with columns for Event, Count, and Trend Data. It shows a high count of 612 for 'Domain\_Summary' and 198 for 'User\_Source\_Summary'.
- Activity Log:** A table with columns for Timestamp, Bus, Severity, and Message. It lists events such as 'Bus is on route again', 'Bus stopped', and 'Bus has crossed speed limit'.
- Dashboard:** A collection of gauges for 'BUS A SPEED', 'BUS B SPEED', 'BUS C SPEED', 'BUS D SPEED', 'BUS A FUEL', 'BUS B FUEL', 'BUS C FUEL', and 'BUS D FUEL'.
- Map:** A Google Maps view showing a route with several bus locations marked.
- Images:** A drone in flight, a drone on a truck bed, a drone on a road, and a drone on a road with a 'Home 2113m' label.
- Central Box:** A box containing the text 'Sensor data', 'Sensors', 'Cameras', and 'Drones'.

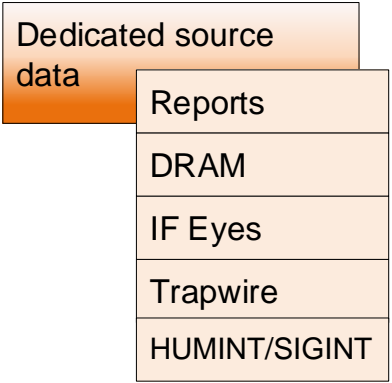
# Dedicated source data

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.



MACHINE GATHERING/ANALYSIS

HUMAN GATHERING/ANALYSIS

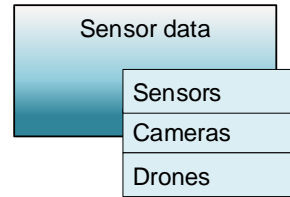


# Open-source data

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

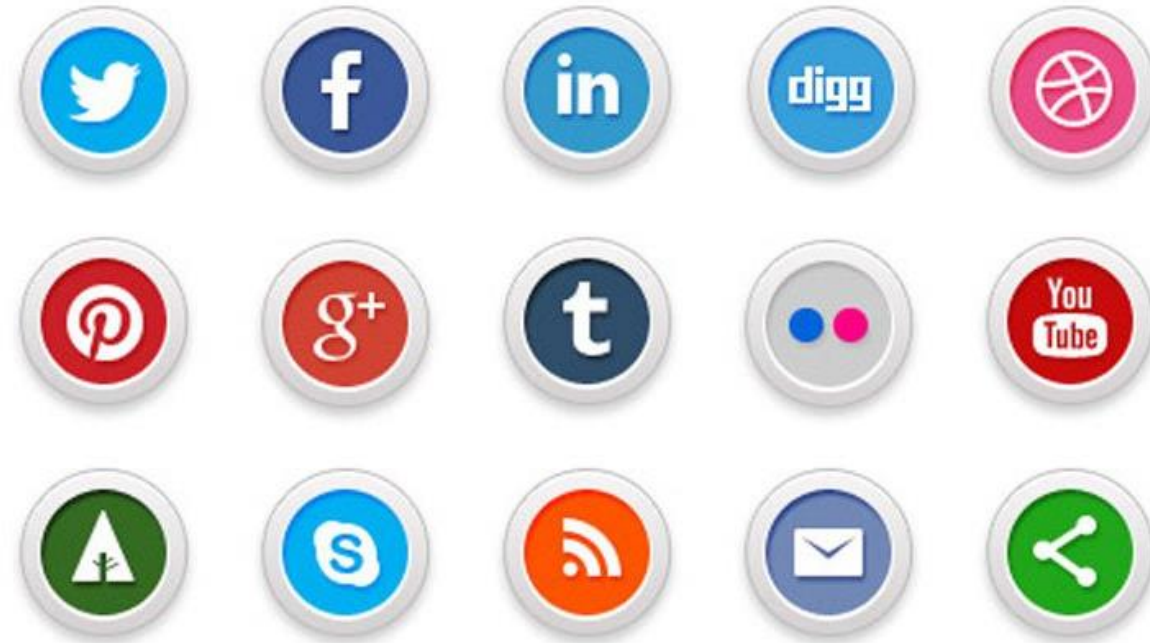
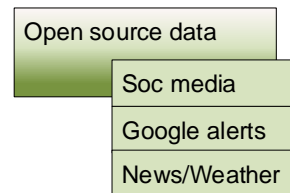
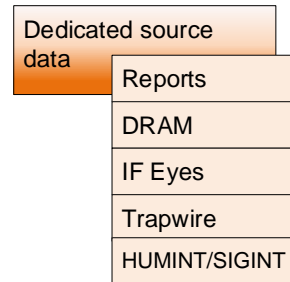
Subject-specific alerts can scan data across social media, news, blogs, and weather to automate the data monitoring process.

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



MACHINE GATHERING/ANALYSIS

HUMAN GATHERING/ANALYSIS



Settings | FAQ | Sign out

## Google Alerts

### Manage your Alerts

Create a Google Alert Sending HTML emails. [Switch to text emails.](#)

Search terms: "Google Guide"    Type: Groups    How often: as-it-happens    [Create Alert](#)

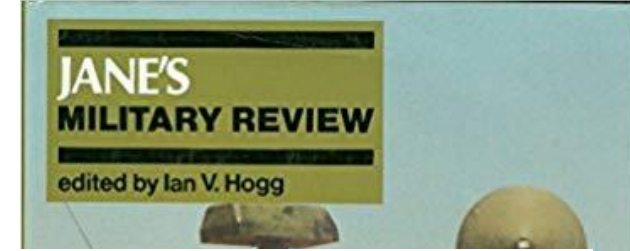
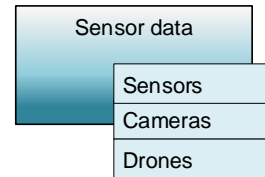
### Your Google Alerts

Search terms	Type	How often	
<a href="#">"bird flu" site:whyfiles.org</a>	Web	once a week	<a href="#">edit</a>   <a href="#">delete</a>
<a href="#">"Google Guide"</a>	News & Web	as-it-happens	<a href="#">edit</a>   <a href="#">delete</a>
<a href="#">Uzbekistan</a>	News	once a day	<a href="#">edit</a>   <a href="#">delete</a>

# 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.”

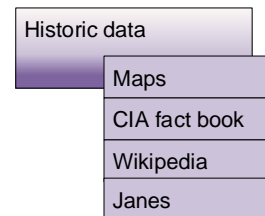
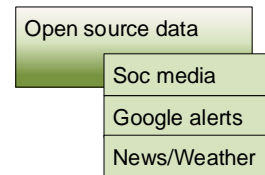
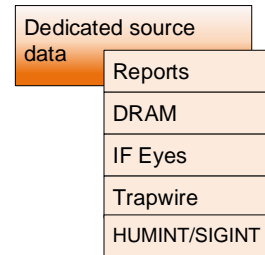


**Defense System**

- Engages aircraft, cruise missiles and smaller ballistic missiles
- Antenna Transmits guidance commands to missile
- Missile length: 8.6m
- Range: 200km
- Altitude: Up to 30km
- Warhead: 150kg
- Speed: Mach 3.6+
- 9M83ME missile
- 984ME launcher unit NATO codename SA-23B Giant Engages intermediate-range ballistic missiles, AWACS and jamming aircraft at ranges of up to 250km Two 9M82ME missile canisters per launcher. Missile length: 10.5m
- 9S32ME guidance radar Tracks targets provided by command post and controls TELAR-mounted antenna
- Missile canisters Four per launcher

## MACHINE GATHERING/ANALYSIS

## HUMAN GATHERING/ANALYSIS



**CENTRAL INTELLIGENCE AGENCY**  
THE WORK OF A NATION. THE CENTER OF INTELLIGENCE.

**Publications**

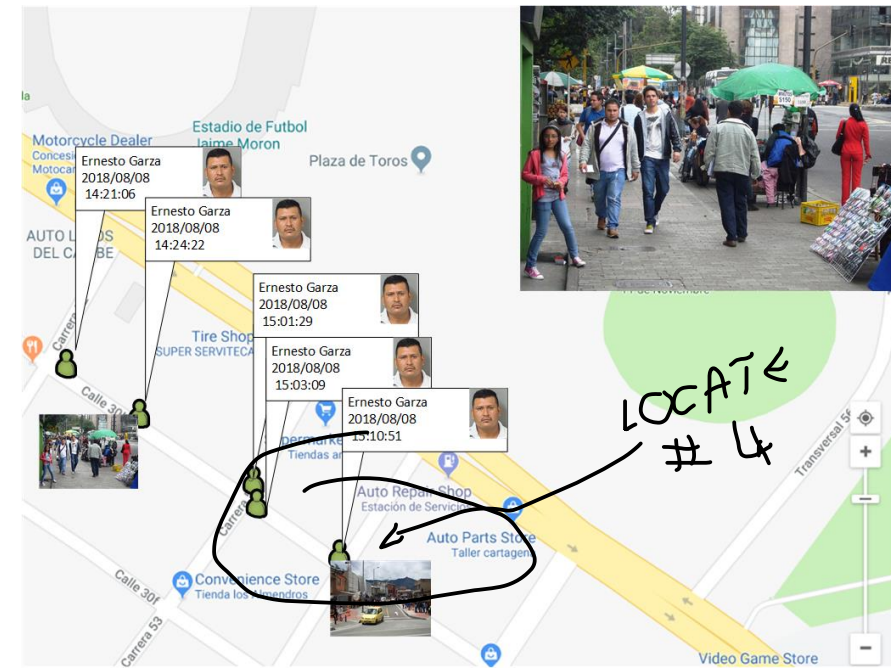
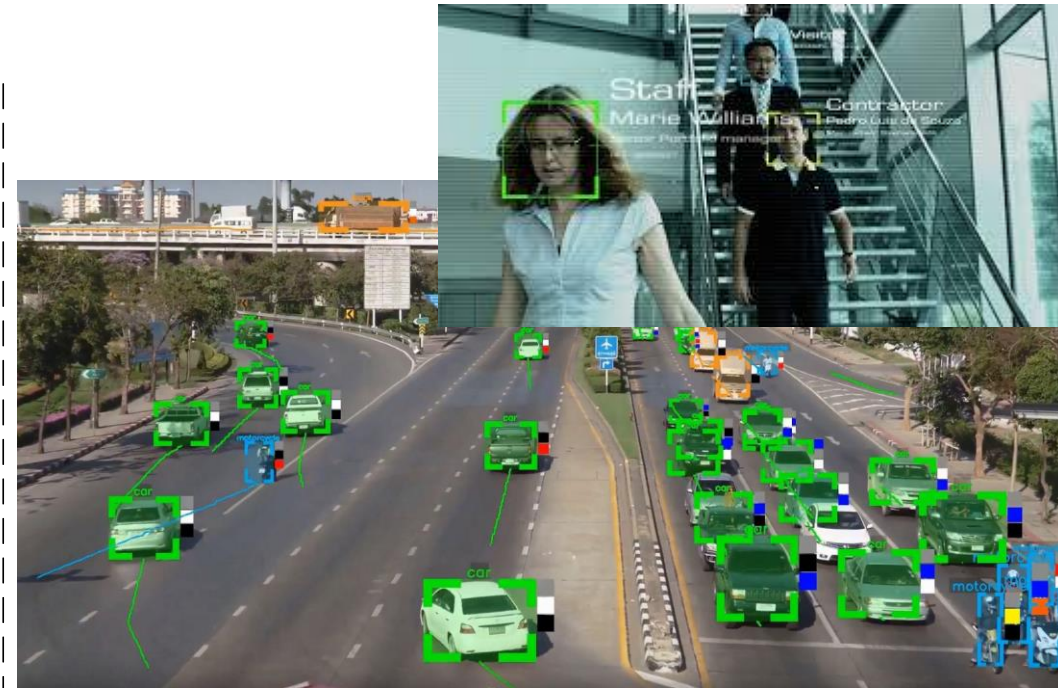
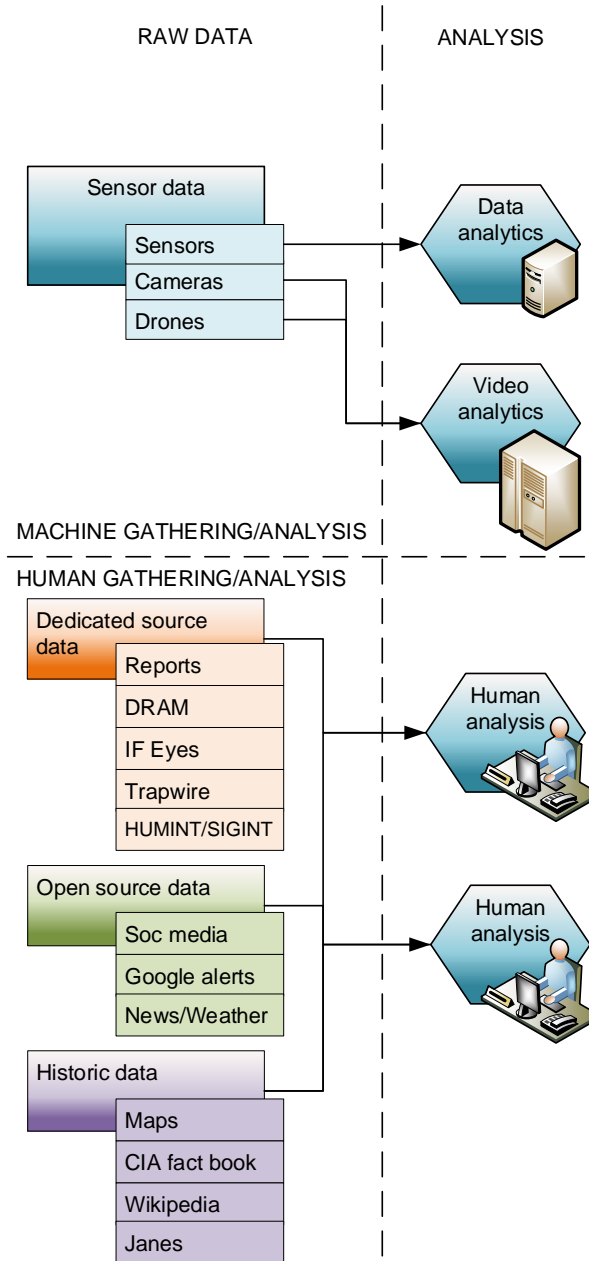
**THE WORLD FACTBOOK**

WELCOME TO THE WORLD FACTBOOK

The World Factbook provides information on the history, people, government, economy, geography, communications, transportation, military, and transnational issues for 267 world entities. Our Reference tab includes: maps of the major world regions, as well as Flags of the World, a Physical Map of the World, a Political Map of the World, and a Standard Time Zones of the World map.

# Analysis

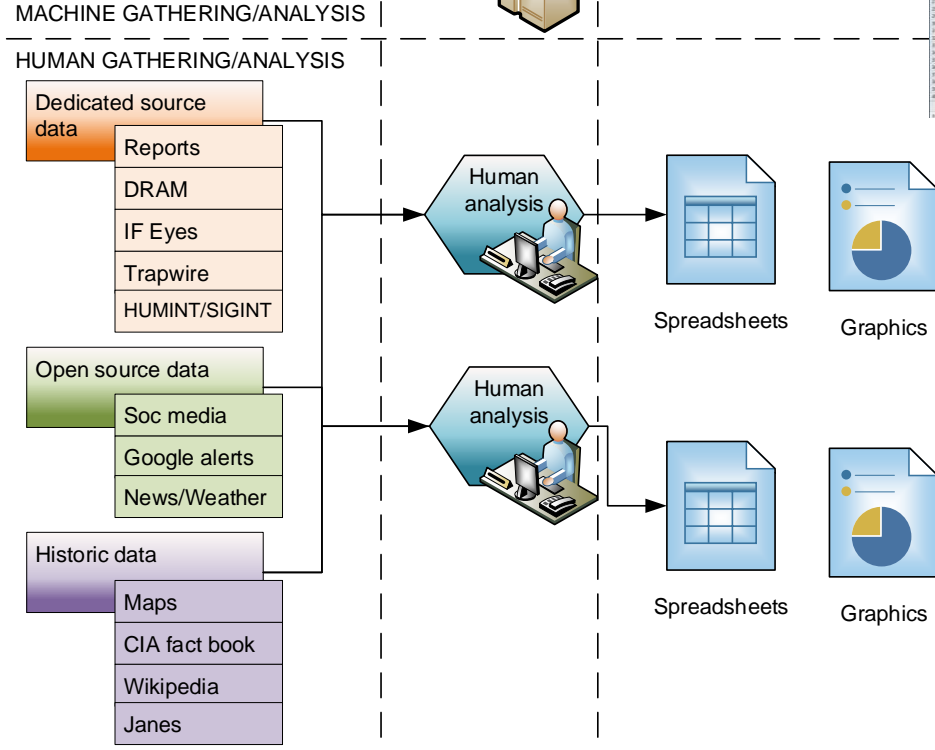
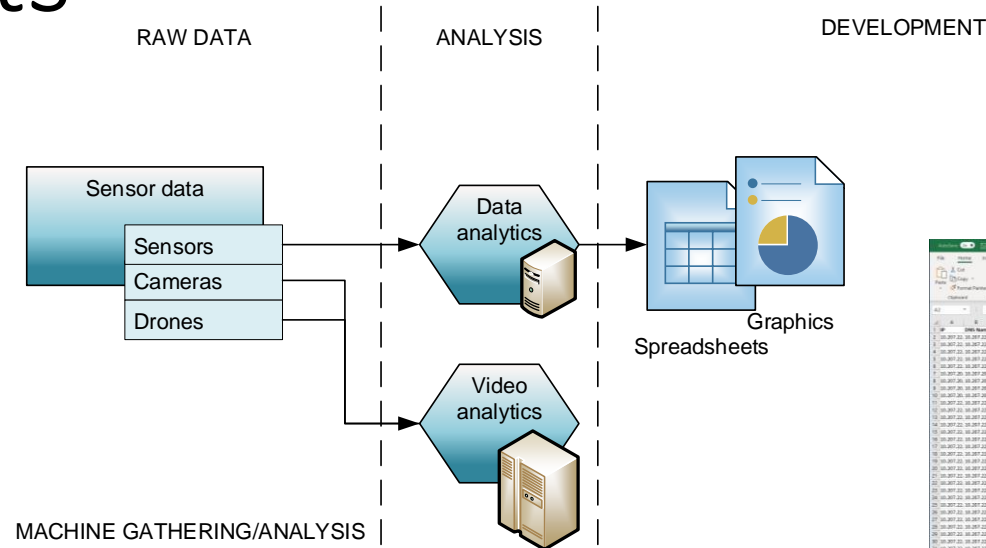
Each type of raw data is subjected to analysis. Sensor data and images are subjected to algorithmic and/or rule-based analysis, and dedicated-source, open-source, and historic data are subjected to human analysis.





# Developed products

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



**Top 10 CVEs with value and frequency of occurrence**

CVE ID	Value	Frequency
CVE-2012-0011	100	10
CVE-2012-0012	80	8
CVE-2012-0013	60	6
CVE-2012-0014	40	4
CVE-2012-0015	20	2
CVE-2012-0016	10	1
CVE-2012-0017	5	0.5
CVE-2012-0018	3	0.3
CVE-2012-0019	2	0.2
CVE-2012-0020	1	0.1

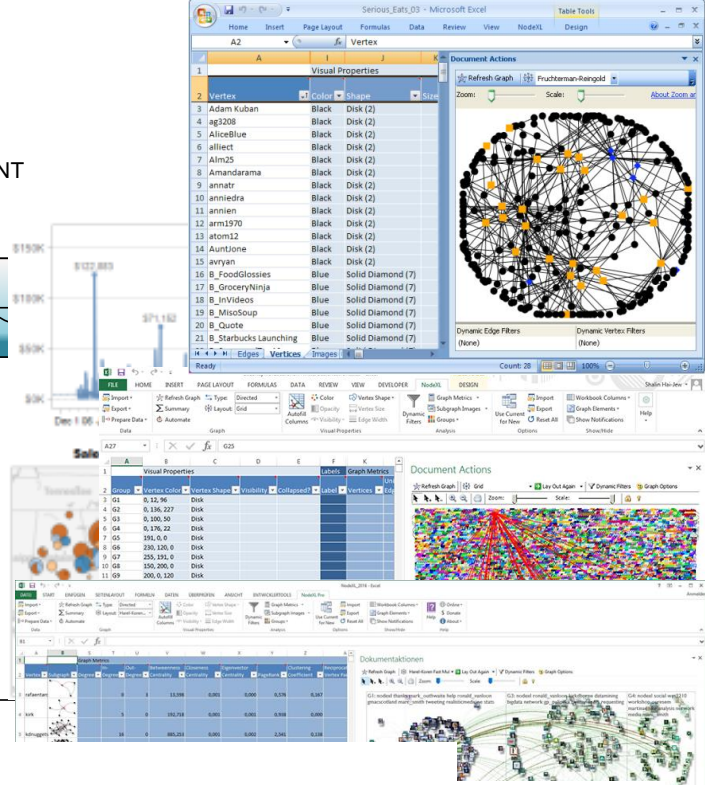
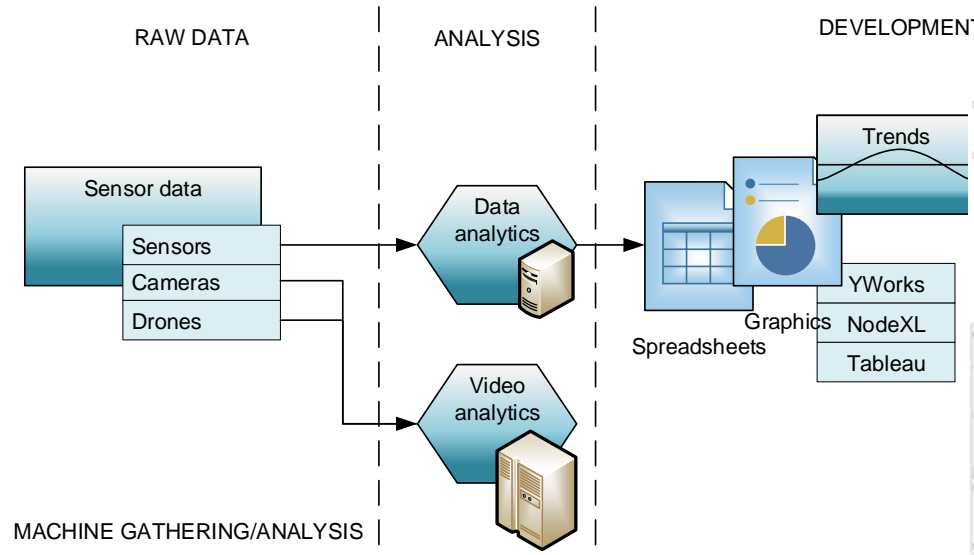
**Top 20 CVEs with value times frequency of occurrence**

CVE ID	Value * Frequency
CVE-2012-0011	1000
CVE-2012-0012	800
CVE-2012-0013	600
CVE-2012-0014	400
CVE-2012-0015	200
CVE-2012-0016	100
CVE-2012-0017	50
CVE-2012-0018	30
CVE-2012-0019	20
CVE-2012-0020	10

# Reduction

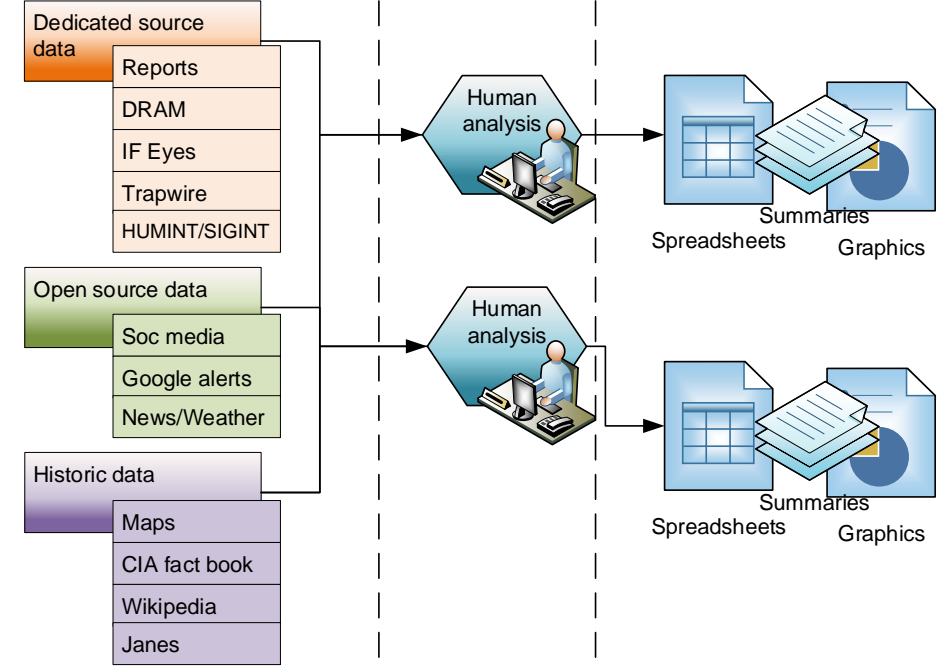
Developed products are then reduced into graphics and/or written summaries.

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



## MACHINE GATHERING/ANALYSIS

## HUMAN GATHERING/ANALYSIS



**Security for Mobile Device Assets: A Survey**  
 António Lima<sup>1</sup>, Bruno Sousa<sup>2</sup>, Tiago Cruz<sup>3</sup>, Paulo Simões<sup>4</sup>  
<sup>1</sup>Department of Informatics Engineering of the University of Coimbra, Coimbra, Portugal  
<sup>2</sup>Onesource, Consultoria Informática Lda.  
 acima@onesource.pt  
<sup>3</sup>tsma@dei.ucp.pt  
<sup>4</sup>psimoes@dei.ucp.pt

**Abstract:** Organizations are often faced with the need to manage large numbers of mobile device assets, including tight control over aspects such as usage profiles, customization, applications and security. Moreover, the risks of the Bring Your Own Device (BYOD) paradigm has further contributed to hamper these requirements, making it difficult to strike a balance between corporate regulations and freedom of usage. In this scope, security is one of the main requirements both for individual and corporate usage. Device and information protection on mobile ecosystems is quite different from securing other assets such as laptops or desktops, due to specific characteristics and restrictions. For instance, the resource consumption overhead of security mechanisms, which is less relevant for desktop/laptop environments, is critical for mobile devices which frequently have less computing power and must keep power consumption as low as possible. Security mechanisms for mobile devices combine preventive tools (e.g. Trusted Execution Environments and sandboxed applications), monitoring solutions and reactive and mitigation techniques. In this paper we discuss these security solutions, presenting a survey on the technologies, frameworks and use cases for mobile device security monitoring and management, with an emphasis on the associated open challenges and benefits, from both the end-user and the corporate points of view.

**Keywords:** mobile devices, security, monitoring, management, detection, prevention

**1. Introduction**

Unlike other forms of computing (such as desktop or laptops or certain specialized embedded systems), mobile devices can be characterized by several specific traits such as dimensions and weight, connectivity, human-machine interface capabilities or autonomy. Moreover, usage models differ from traditional desktop computing, as interaction tends to occur over short time windows, rather than in a continuous manner.

Most modern mobile devices have an embedded display screen for can be connected to one), receiving input from physical or virtual buttons and keyboards (using touch-sensitive displays in the latter case). Additionally, some devices also support audio input, namely voice recognition. Several types of sensors and data capture devices can also be embedded or attached to the mobile device. Typical examples include accelerometers, compasses, magnetometers and gyroscopes (allowing for detection of orientation and motion), as well as barocodes, RFID, fingerprint and smart card readers. On top of all the already mentioned extras, the most prominently used features are related to connectivity and usually comprise Wi-Fi, Bluetooth, NFC (Near Field Communications) and GPS capabilities.

The first mobile devices didn't have much to offer. Devices like the IBM Simon (released in 1994, regarded as the first smartphone) were very "dumb" by today's standards, having very limited electronics and processing power. For the sake of context, Table 1 compares several representative mobile device models released between 1994 and 2016: an iPhone 6, a Samsung Galaxy S 1<sup>st</sup> Generation, an iPhone 3<sup>rd</sup> Generation (commonly referred to by many as one of the first examples of the current smartphone paradigm) and the IBM Simon.

Mobile devices (and, particularly, smartphones) have been gradually acquiring computing, communications and sensory capabilities at an exponential rate. For this reason, such devices have evolved beyond their natural role of mobile assistants, gradually assuming roles previously associated with traditional computing devices, such as desktop or laptop PCs. With the result of this sustained trend, mobile devices have become important tools both for individual users and organizations. Company-provided mobile devices became commonplace as laptops, prompting the need for the development of asset management systems for these ecosystems.

## Operation Centers

h. Barry Irwin  
 r Science  
 Africa  
 bms.b.irwin@ra.ac.za

ments and monitoring the effectiveness of implemented critical controls.

posed to a SOC providing Security Operations services – one Team (CSIRT) provides two basic services (4) – an Incident response, and provide measures to prevent such incidents. In most CSIRTs, proactive measures are not usually required (4). Thus, CSIRTs can be considered to be aligned SOC offerings.

although there are numerous frameworks for technologies in SOCs (such as IS [8] and [1]), there is no industry-wide addressing processes, staffing and technology in a SOC. Furthermore, there is no maturity model that we used to evaluate the effectiveness and capabilities of a

In this paper, we present a model to measure the effectiveness and capabilities of a SOC through three aspects:

- The Aspects of SOC services
- The Capability of the SOC aspects.
- The Maturity of SOC processes per aspect

family models or frameworks implies perfect or city defined, managed, measured and controlled systems and IS). A Maturity Framework will be coupled with billions to create a classification matrix. With this classification matrix, we will try to provide consumers of SOCs with a reference when building their own SOCs or IT, or choosing a vendor providing these services. This paper aims to define the exhaustive functional aspects of a SOC, or rather define the critical aspects, and this model is expanded upon with further functional aspects.

This paper is organized as follows – in Chapter II, we we existing, industry accepted maturity models and discuss SOCs' capability and maturity models. This is followed by proposed SOCs' classification model in Chapter III, and IV summarizes the intended future work below being Chapter V.

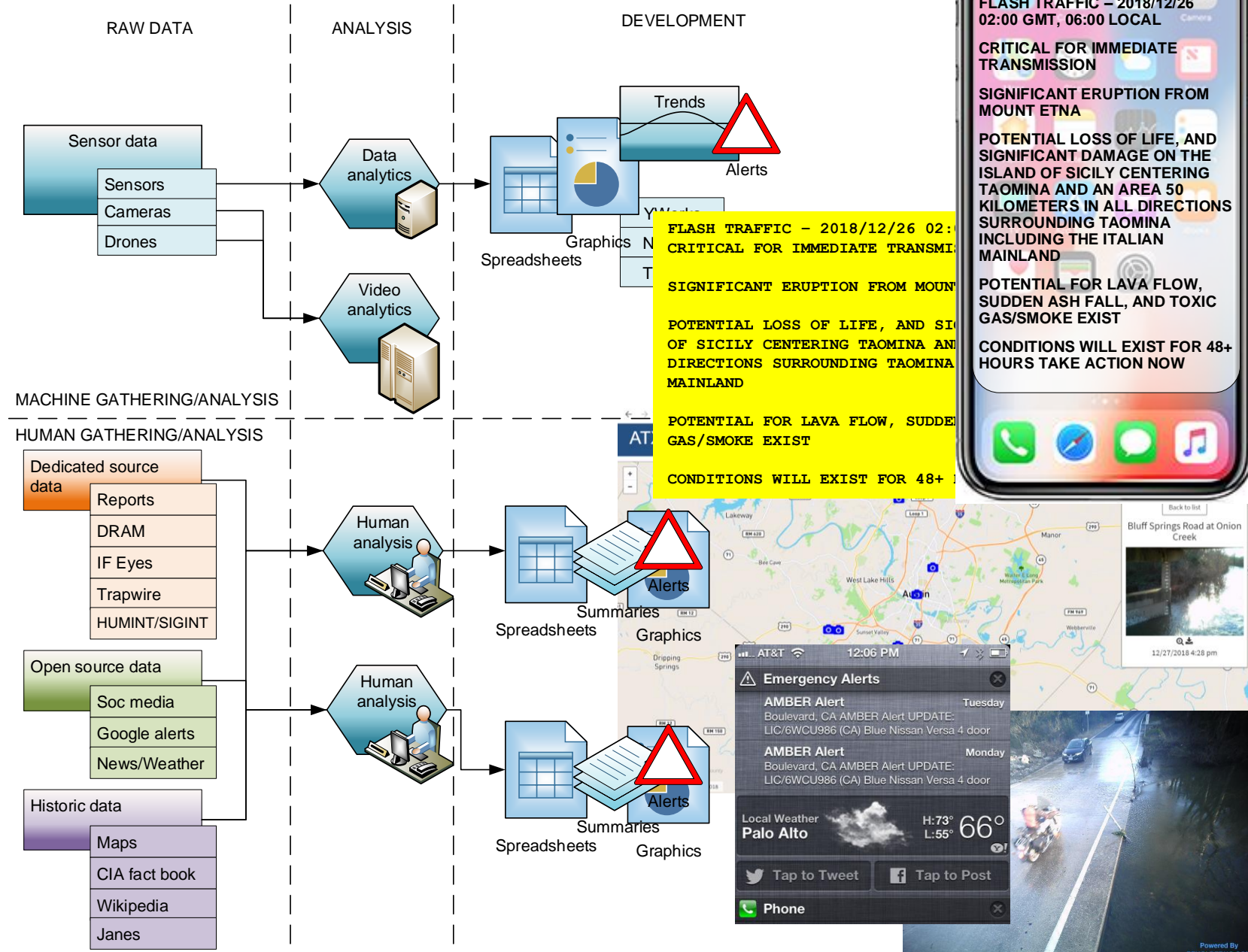
**RELATED WORK**

currently no proper classification scheme or matrix exists in discussing SOCs. We have reviewed industry based classification model on industry accepted models, specifically

# Alert

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

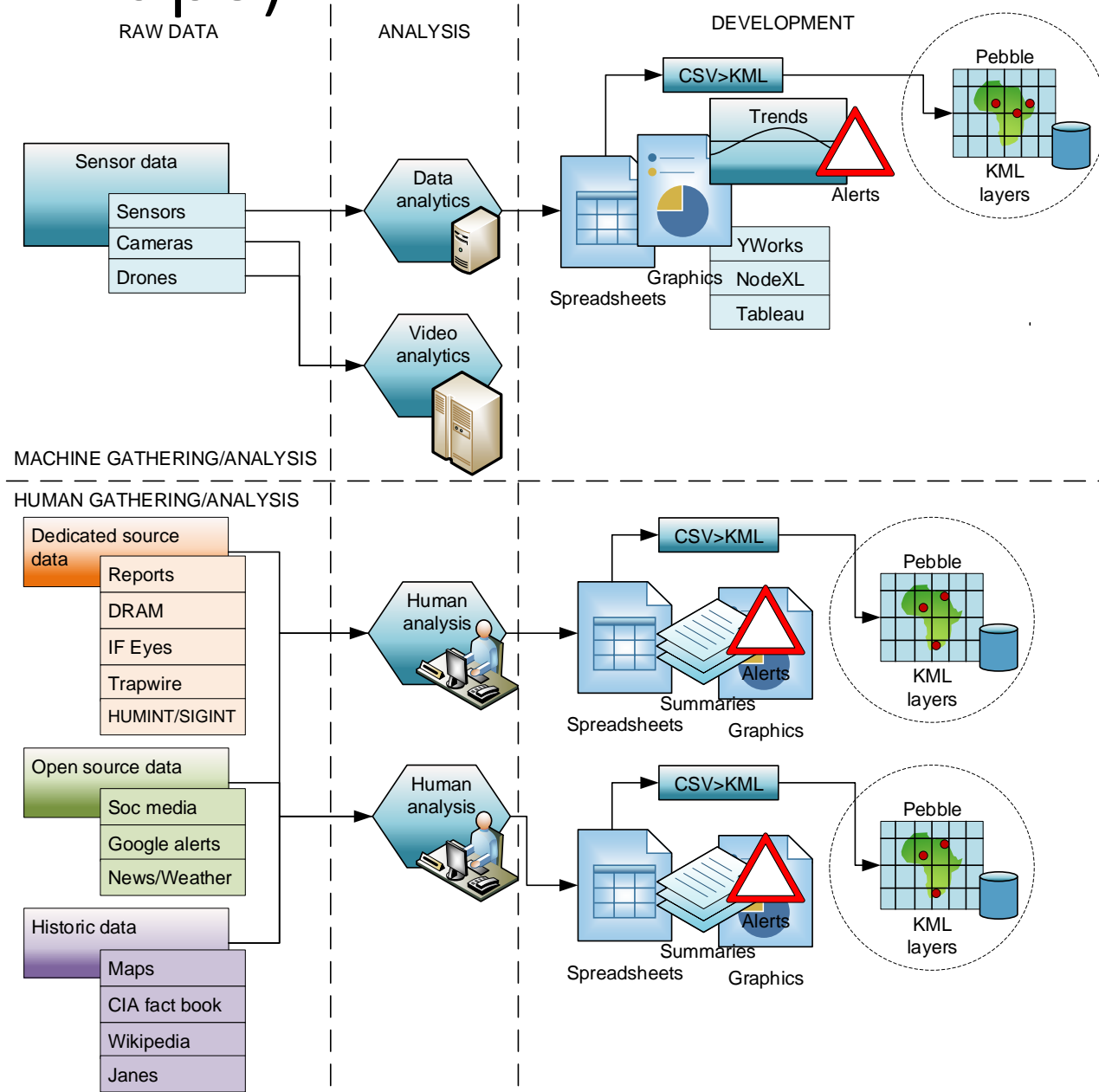
Generated on an as-needed basis, the alerts are transmitted as actionable intelligence across multiple media to specific or general audiences.



# CSV > KML (data to maps)

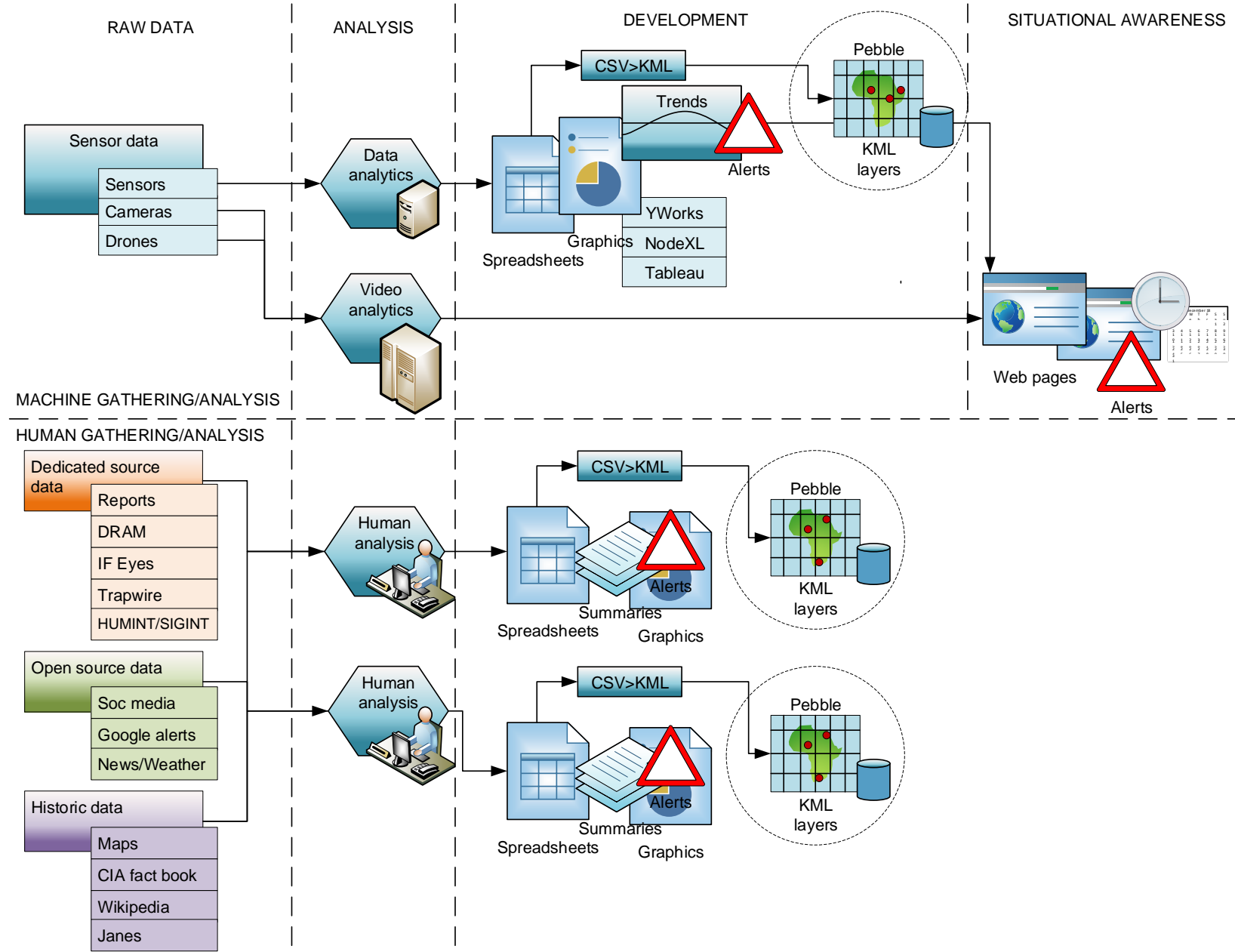
Spreadsheets with geospatial data are rendered from CSV files (comma separated variables) to KML files (keyhole markup language) to create map/database “Pebbles.”

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



# Situational awareness

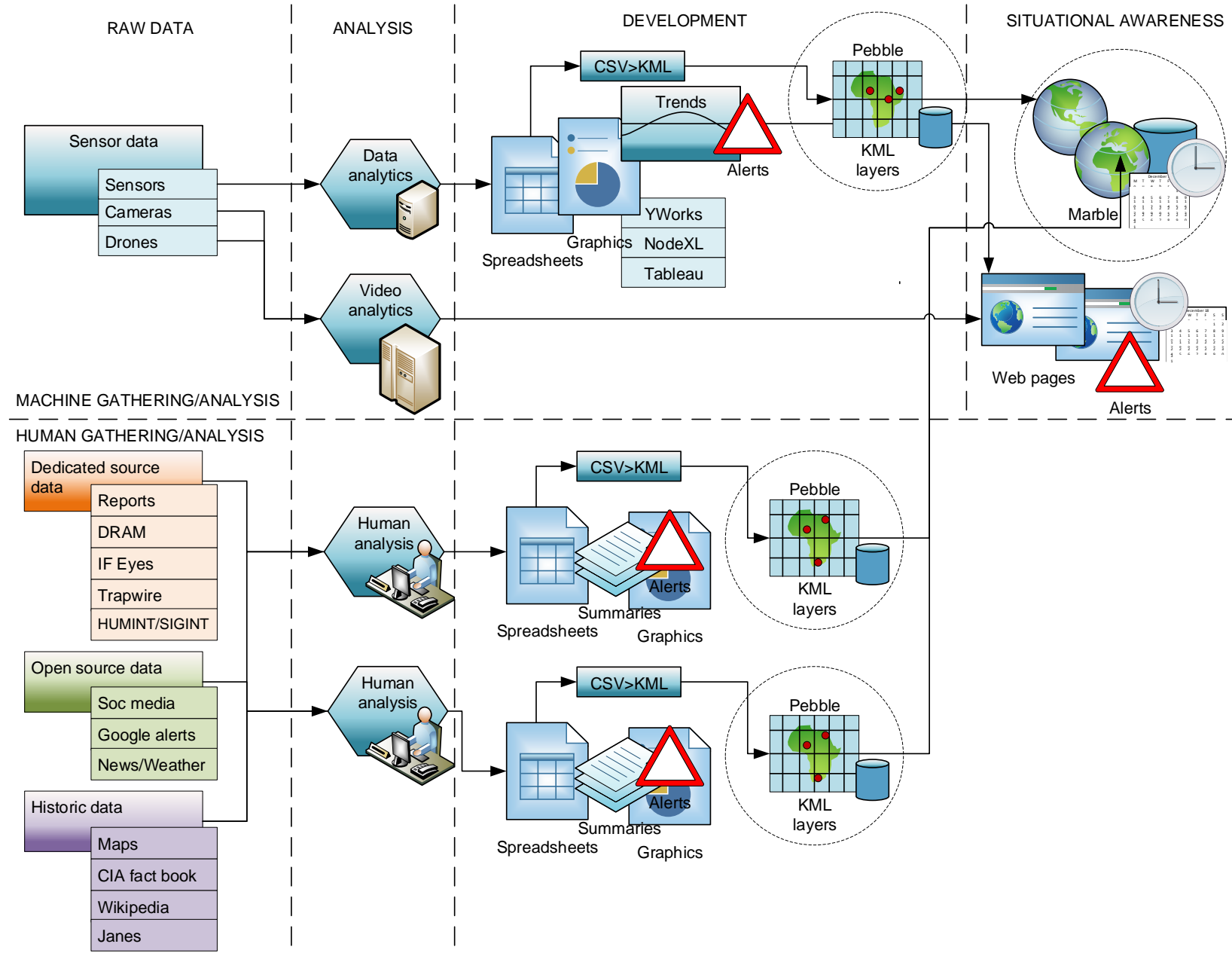
In combination, the geospatial data, alerts, and webpages derived from the data provide automated situational awareness “dashboards” that can be updated in real time, by the hour, or by the day.



# 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.



# 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.

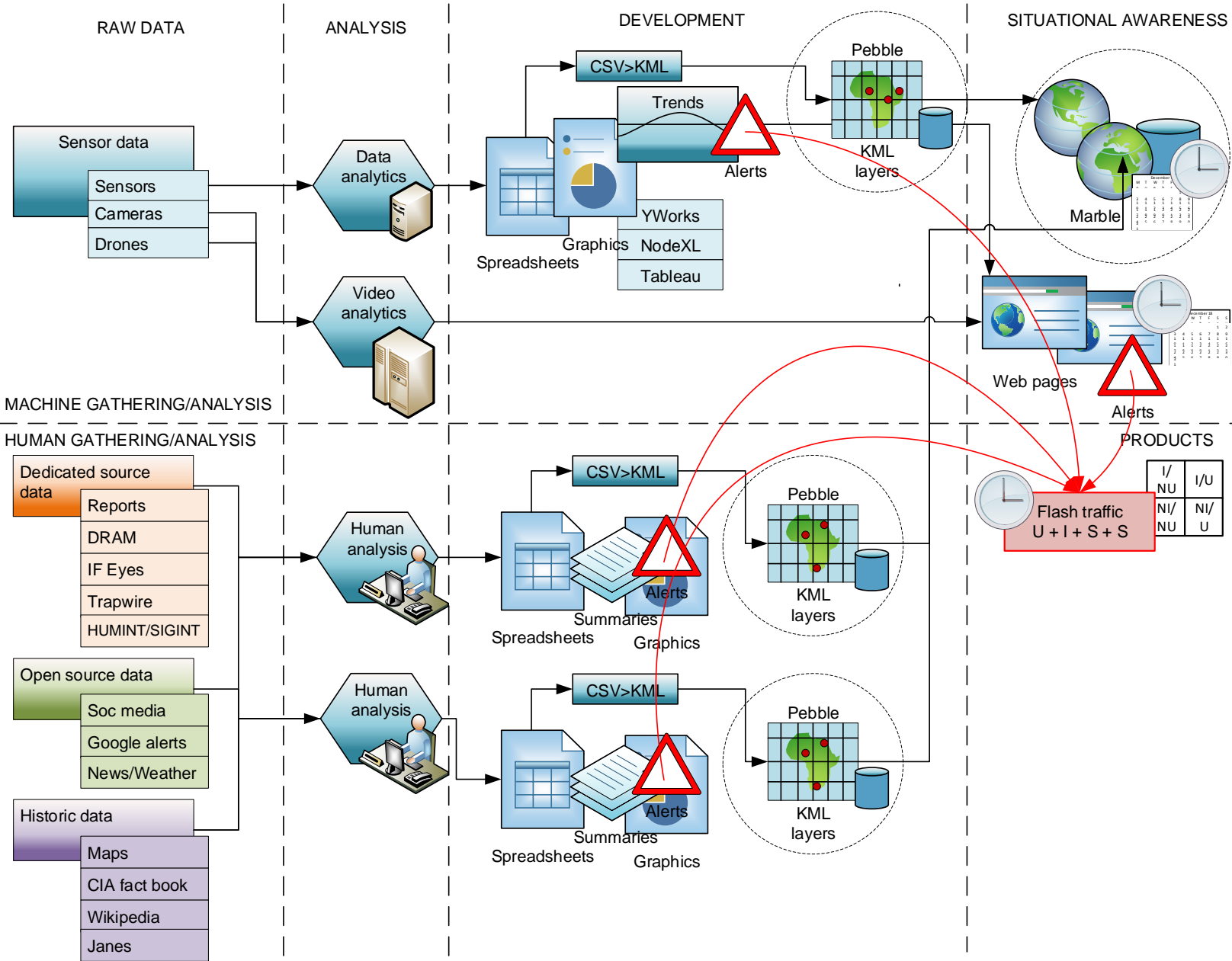
**FLASH TRAFFIC - 2018/12/26 02:00 GMT, 06:00 LOCAL  
CRITICAL FOR IMMEDIATE TRANSMISSION**

**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**



# Important/Urgent

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

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

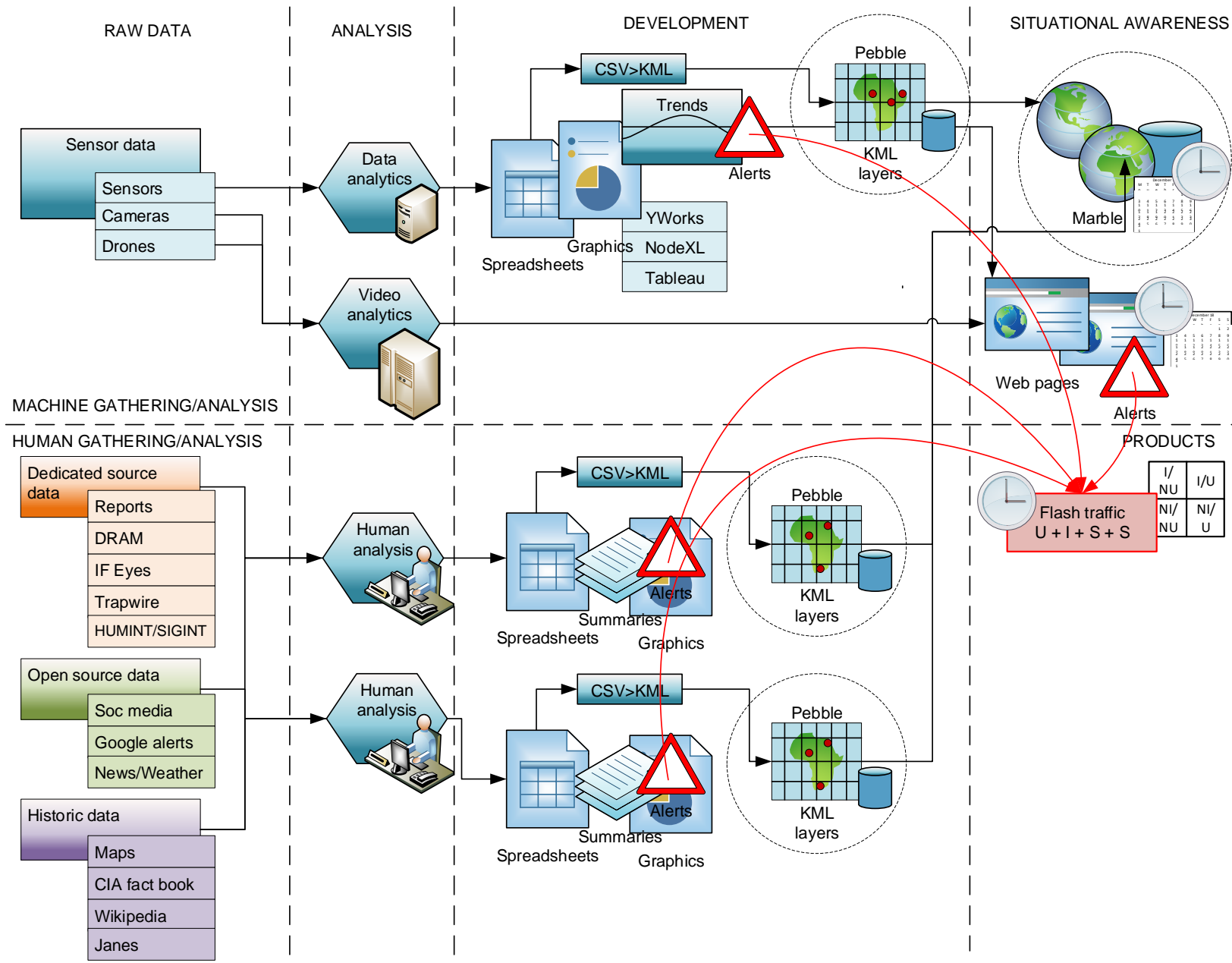
Examples:

I/NU = basic hygiene

NI/NU = social media

NI/U = typical phone call

I/U = flash traffic, alarms, etc.

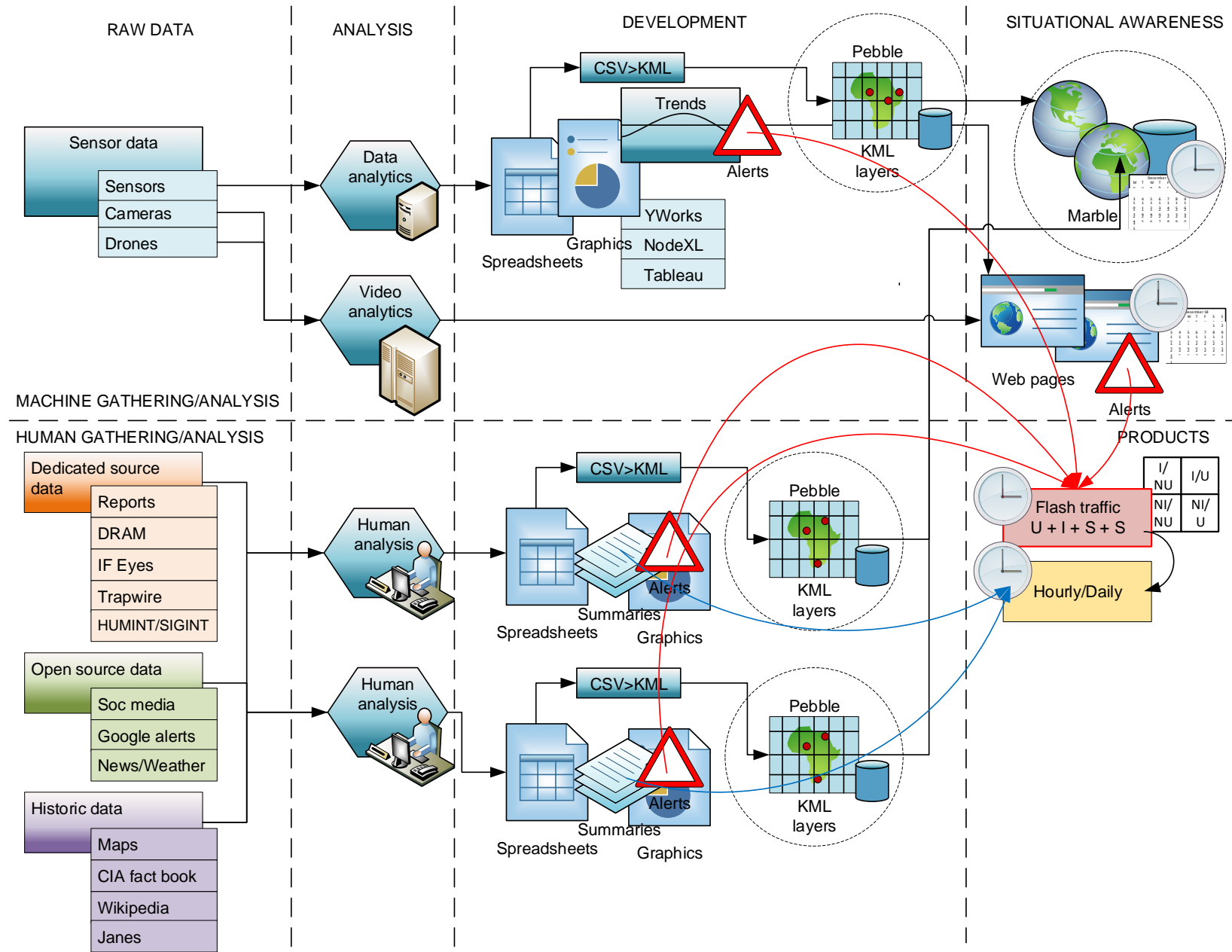




# Hourly/Daily

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.

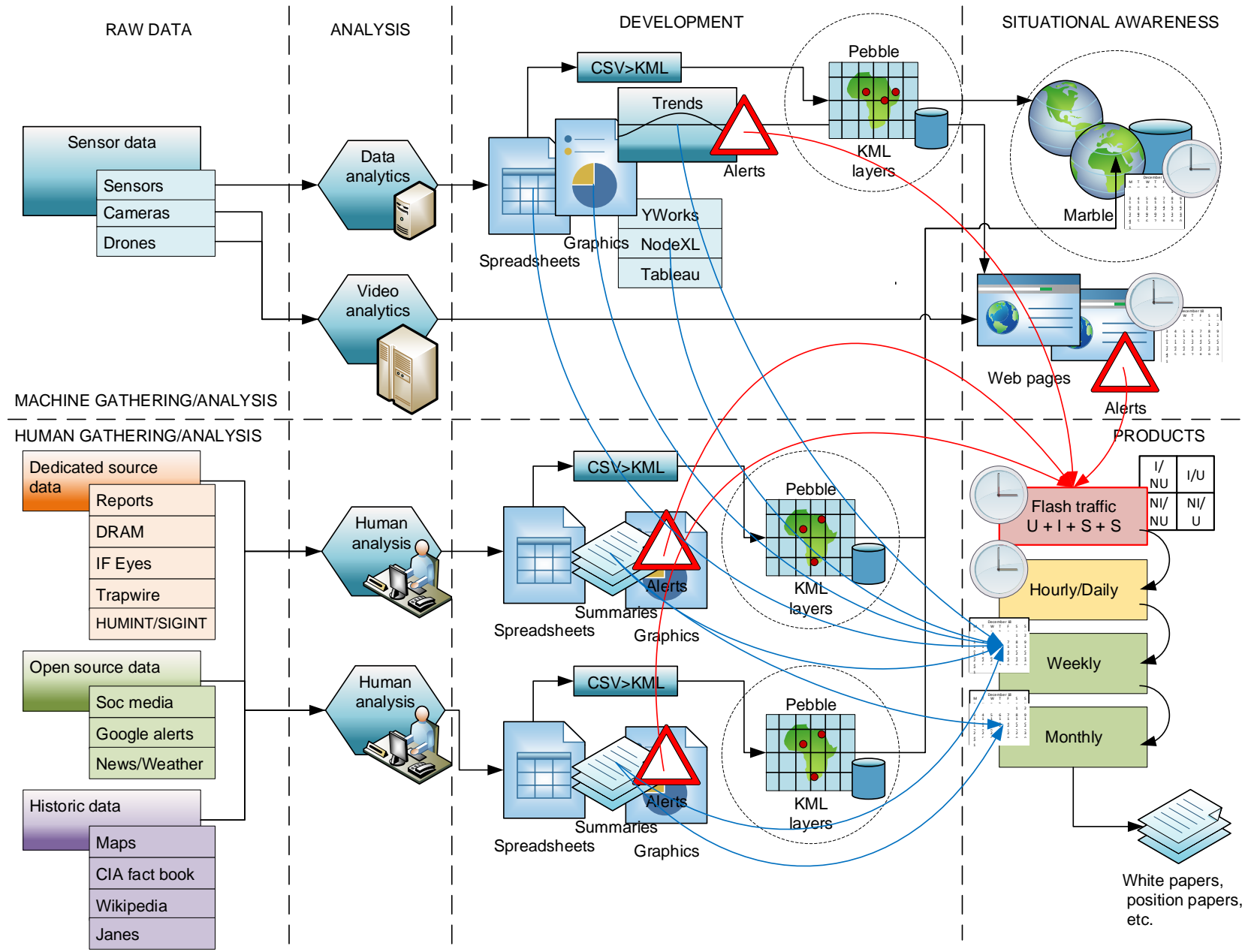
This is not to rehash the data, but to codify and ensure capture of the data in sequence.



# Sensor data

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

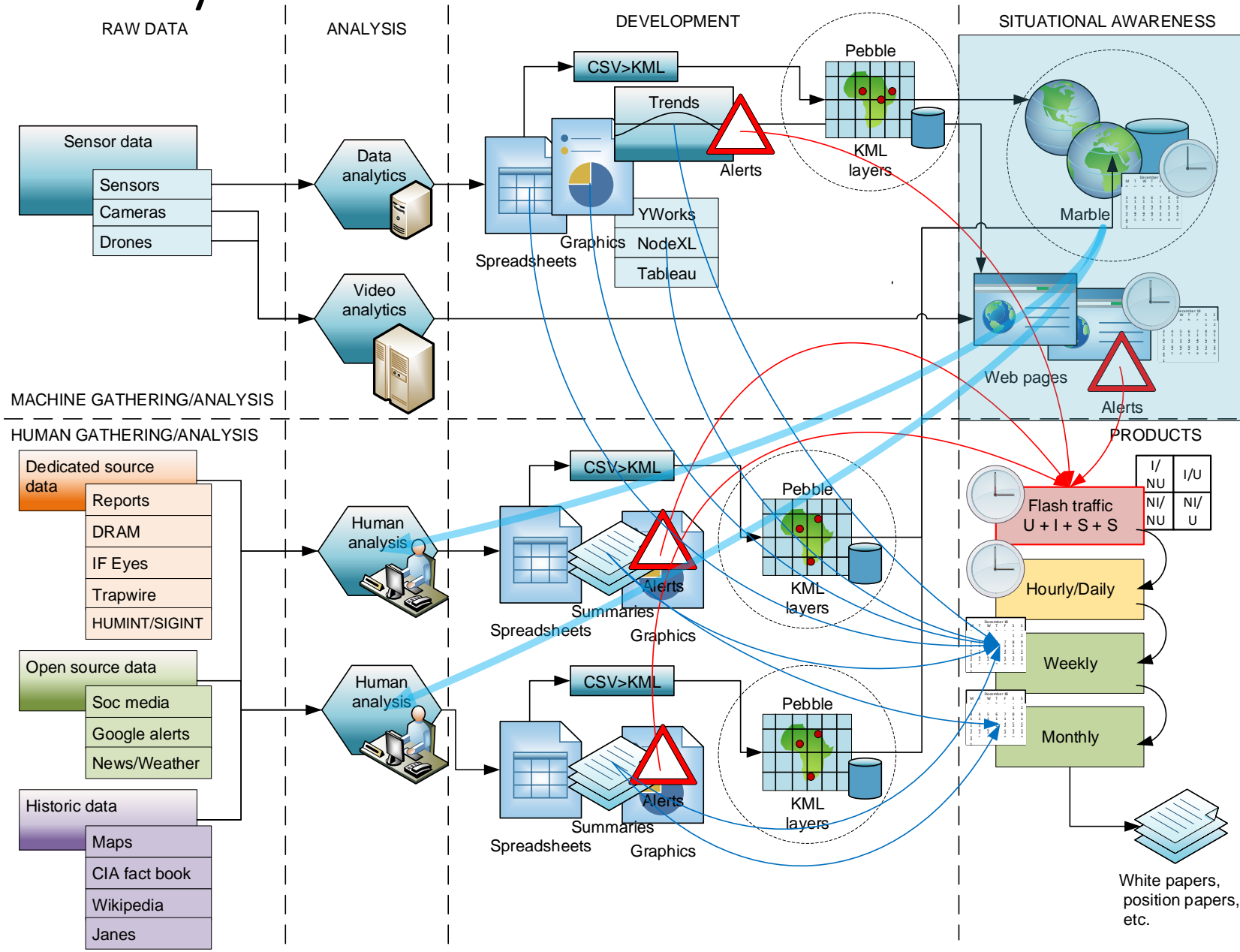
White papers, position papers, and other high-level products are produced from the summaries and machine-developed data.



# Maturation of human analytics

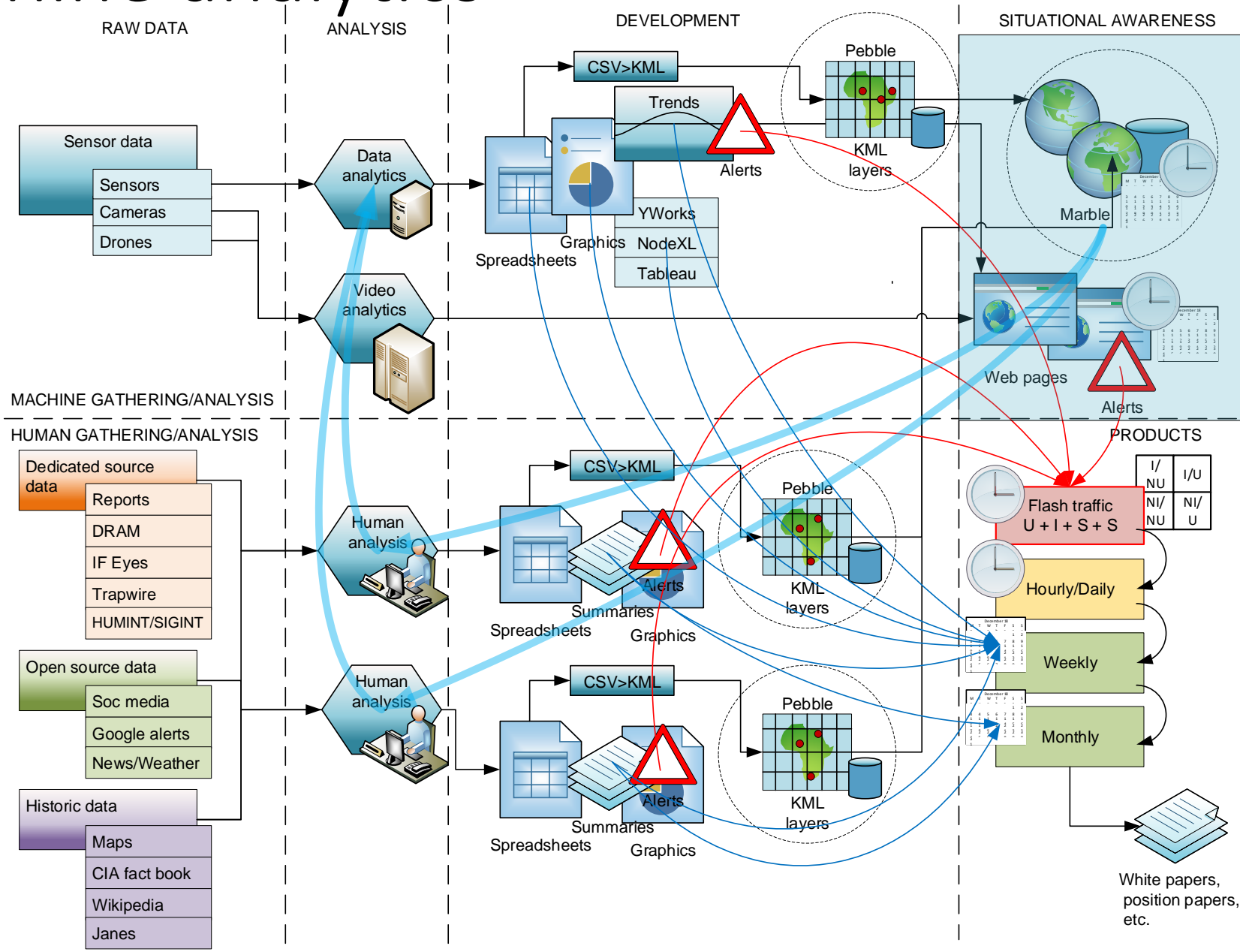
The human analysis knowledge base and understandings are informed and matured via the situational awareness resources.

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



# 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.





Questions and  
discussion?