Paper 611-2017

Counter Radicalization through Investigative Insights and Data Exploitation Using SAS® Viya™

Lawrie Elder, SAS Institute Inc.

ABSTRACT

This end-to-end capability demonstration illustrates how SAS Viya can aid intelligence, homeland security, and law-enforcement agencies in counterterrorism activities. Many of us are familiar with recent examples of agency failure to apportion significance to isolated pieces of information that, in context, are indicative of an escalating threat, and that require intervention. Recent terrorist acts have been carried out by radicalized individuals who should have been firmly on the organizational radar. Although SAS products perform analysis and interpretation of data that enables the law enforcement and homeland security communities to recognize and triage threats, intelligence information must be viewed in its full context. SAS Viya can rationalize previously disconnected capabilities in a single platform, empowering intelligence, security, and law enforcement agencies. SAS® Visual Investigator functions as a hub for SAS® Event Stream Processing, SAS® Visual Scenario Designer, and SAS® Visual Analytics, combining network analysis, triage, and, by leveraging the mobile capability of SAS, operational case management to drive insights, leads, and investigation. This hub provides the capability to ingest social media data, and to cross-reference both internally held data and, crucially, operational intelligence gained from normal policing activities. This presentation chronicles the exposure and substantiation of a radical network and describes tactical and strategic disruption.

INTRODUCTION

This paper begins with an overview of the terrorist threat currently faced by the European and Transatlantic communities and then explains how SAS capabilities can support agencies engaged in counterterrorism efforts. While acknowledging that the origins and nature of current terrorism threats vary significantly, this paper focuses primarily on the Salafist (radical Sunni) extremist threat.

Environment and History

Recent military success against Salafi jihadist terrorist groups has seen the Islamic State in Iraq and the Levant (ISIL) losing their foothold in territories that have been considered the heartlands of Iraq and Syria. A notable consequence of these developments has been a strengthening of these groups' commitment to target Europe and North America. This approach has met with some success, drawing on the experience of European ISIL fighters returning from the frontlines. Simultaneously, they have set out to motivate "lone-wolf" activities by developing localized networks of extremists through the use of propaganda.

These ISIL activities have driven several recent high-profile, high-casualty attacks, primarily against European civilian targets in heavily populated public areas. Their tactics have varied greatly, ranging from sophisticated, highly coordinated attacks to crude, blunt-force strikes. Perhaps more significantly, these attacks have served to highlight failings in the local, national, and international intelligence and enforcement services who are perceived to have missed opportunities to preemptively disrupt them.

The changing nature of the terrorist threat has required intelligence and enforcement agencies to shift their focus and adjust their tactics. Perhaps the greatest influence on this change has been that recent attacks have been largely perpetrated by individuals who have subsequently been revealed to be known criminals. Indeed, many of ISIL's successes can be directly attributed to this ability to radicalize individuals whose history has previously been marked by petty crime.

These factors are driving changes in the counterterrorism dynamic and have exposed weaknesses in the traditional capabilities around gathering, exploiting, and sharing of intelligence within and between agencies and nations. While counterterrorism has traditionally been the domain of intelligence and homeland security agencies, recent terrorist attacks (born out of and planned within criminal networks) have to a large extent ranged beyond these services' purview. This change in dynamic has placed law enforcement at the center of counterterrorism endeavors and has, as a direct consequence, seen general policing or community information elevated to being among the most critical of data sources.

Examples

Sophisticated and Coordinated: In November 2015 a brutal, highly coordinated attack took place in Paris when ISIL-inspired terrorist cells, using assault rifles and wearing suicide vests, simultaneously attacked multiple soft targets, including the Bataclan Theatre, where 89 died. The terrorist network behind the attack was led by Salah Abdesalam, a radicalized individual with strong links to known criminal networks. The group also included individuals who had previously fought in Syria.

Michael Leiter, former director of the United States' National Counterterrorism Center, commented afterward that "the attacks demonstrated a sophistication not seen in a city attack since the 2008 Mumbai attacks, and would change how the West regards the threat" of terrorism generally.

Blunt Force: In July 2016 Mohamed Lahouaiej Bouhlel drove a lorry into a Bastille Day celebration in Nice, France, killing 84 people. This blunt-force attack might have lacked the sophistication and planning of the Paris attack, but it ultimately had a similarly deadly effect. Although Bouhlel was known to law enforcement for involvement in petty criminality, there were no reports of his having any direct links with a terrorist group. However, he was subsequently described by ISIL as a "soldier of Islam." Significantly, he was known to have psychiatric problems, a characteristic increasingly common in these incidents.

The evidence indicated that Bouhlel had been radicalized by ISIL propaganda, and he was subsequently classified by elements of the mainstream media as a "lone-wolf" actor. Nevertheless, he did not act alone in the planning and development of his attack, and his actions were facilitated by criminal contacts through which, among other activities, he procured a firearm.

Future

Transatlantic law-enforcement communities have publicly acknowledged their current weaknesses and their vulnerability to future terrorist attacks. This recognition has resulted in a number of initiatives to assist with building understanding of possible ways to mitigate such threats in the future.

A significant body of work is to be found in the GLOBSEC Intelligence Reform Initiative (GRI), which recently published a paper, "Reforming Transatlantic Counter-Terrorism". One of the important observations of this paper was the following:

> *"The key problem the Globsec Intelligence Reform Initiative addresses is that of intelligence and personal data sharing and its operationalisation at the domestic as well as transnational level. Although many intelligence agencies have been at the centre of counter-terrorism efforts since 9/11, this report recognises that as terrorism is fundamentally viewed as a crime in both Europe and North America, law enforcement is increasingly at the centre of better pan-European and transatlantic counter-terrorism cooperation. Crucially, better fusion of intelligence processes, and intelligence and law enforcement agencies, is needed to provide the means for pre-empting terrorist attacks before they occur, rather than relying on effective investigation after the event."*

While the need for data sharing and the operationalization of intelligence products is widely accepted, there is also a recognition that to be effective, agencies must enhance the information technology capabilities around collation, analysis, and the associated management of operational processes.

The related significant challenges are often magnified rather than lessened by the volume of data that exists for agencies to exploit. Information sources are vast and varied, a complexity that is only increased by this now essential inclusion of day-to-day community and policing data.

SAS VIYA PLATFORM

Supported by SAS Data Management services, the SAS Viya platform can help law enforcement, security, and intelligence agencies to address the many challenges associated with counterterrorism. SAS Viya comprises solutions built with embedded analytical capabilities at their core, allowing the exploitation of information through alerting, triage, enrichment, and operationalization. The open architecture of SAS Viya also ensures that operatives at all levels within participating organizations (including executives, analysts, investigators, and front-line officers) are always able to access their data and related insights in the most effective and relevant manner and are not tied to a single application or device.

With SAS Viya, it is possible to integrate all aspects of the intelligence and investigation life cycles through standard, unified components that provide a foundation for sharing and communicating. The major components of such a system to handle data for intelligence purposes would include (but not be limited to) the following SAS solutions:

- SAS® Visual Analytics
- SAS® Event Stream Processing
- SAS® Mobile Investigator
- SAS® Visual Investigator

SAS VISUAL ANALYTICS

Business Challenge

In tackling the terrorist threat, law enforcement, security, and intelligence agencies must use their finite resources to the best possible effect. Decisions must be based on accurate assessments, and the strategic direction must always be made clear and be justifiable.

The development of an effective Strategic Assessment is dependent on skilled operatives' undertaking detailed research and analysis of all available information sources. To develop this "big-picture" document and truly understand the nature and level of the threats, agencies should not restrict their information sources to only those that are routinely maintained or accessed in the course of day-to-day operations. External influences, such as information about public perceptions, health, welfare, and education, must also be taken into consideration, as such factors can provide valuable insight into the fears, vulnerabilities, and threats extant in local communities.

By making a comprehensive and complete assessment available, agencies are better able to set a strategic direction, prioritize, make defensible decisions, and allocate resources intelligently, fully considering the operational options available to them. Counter-radicalization is a related priority, and agencies must take all necessary actions to understand the terrorist ideology, identify those who promote it, and prevent people from being drawn into terrorism. Tactical options when seeking to prevent radicalization or to preempt a terrorist attack would include proactive investigation, surveillance, education, and engaging with sectors and institutions where the risks of radicalization are greatest.

This practice of centering activity on a strategic assessment is universal among the European and Transatlantic law-enforcement, security, and intelligence agencies, and this commonality facilitates collaboration on an interagency, national, and international basis. There are many examples where this type of joint assessment has been adopted: for example, a joint endeavor of the European Council to develop the EU Counter-Terrorism Strategy[1]

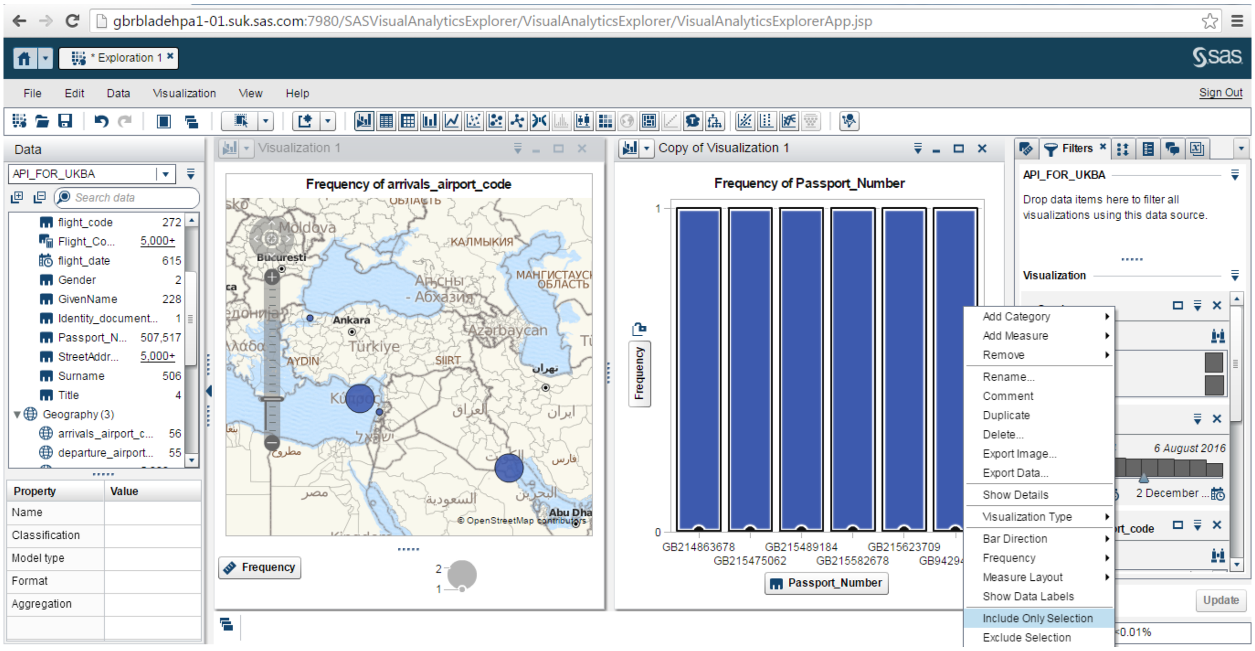
[1] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/.

Applicable SAS Viya Module

SAS Visual Analytics supports agencies in creating, sharing, and acting upon interactive and meaningful intelligence products, such as strategic assessments.

By using SAS Visual Analytics, analysts gain the ability to explore the corpus of information available within the organization as well as that shared through collaboration. Products will include the vital and overarching strategic assessment, together with tactical reports reflecting priorities and supporting ongoing operations.

Given the dynamic nature of the terrorist threat, the interactive features of SAS Visual Analytics reports are crucial. These reports enable recipients to focus on the information facets that are most appropriate and in whatever manner is most relevant to the task at hand, using filters and drill-through capabilities to further explore the data and develop insights.



flight_code	272
Flight_Co...	5,000+
flight_date	615
Gender	2
GivenName	228
Identity_document...	1
Passport_N...	507,517
StreetAddr...	5,000+
Surname	506
Title	4
Geography (3)	
arrivals_airport_c...	56
departure_airport...	55

Property	Value
Name	
Classification	
Model type	
Format	
Aggregation	

Figure 1. Example of SAS Visual Analytics dashboard

A standard response to a terrorist incident will see different levels of commanders taking control of the various aspects of activity (for example, overall command, referred to as Gold; tactical: Silver; and operational: Bronze). SAS Visual Analytics gives commanders easy access to explore dashboards and reports to aid in their decision-making process. The ability to access this information from mobile devices is of particular importance to bronze commanders who are often required to operate from the field (for example, taking responsibility for hostage situations or bomb scene management).

SAS EVENT STREAM PROCESSING

Business Challenge

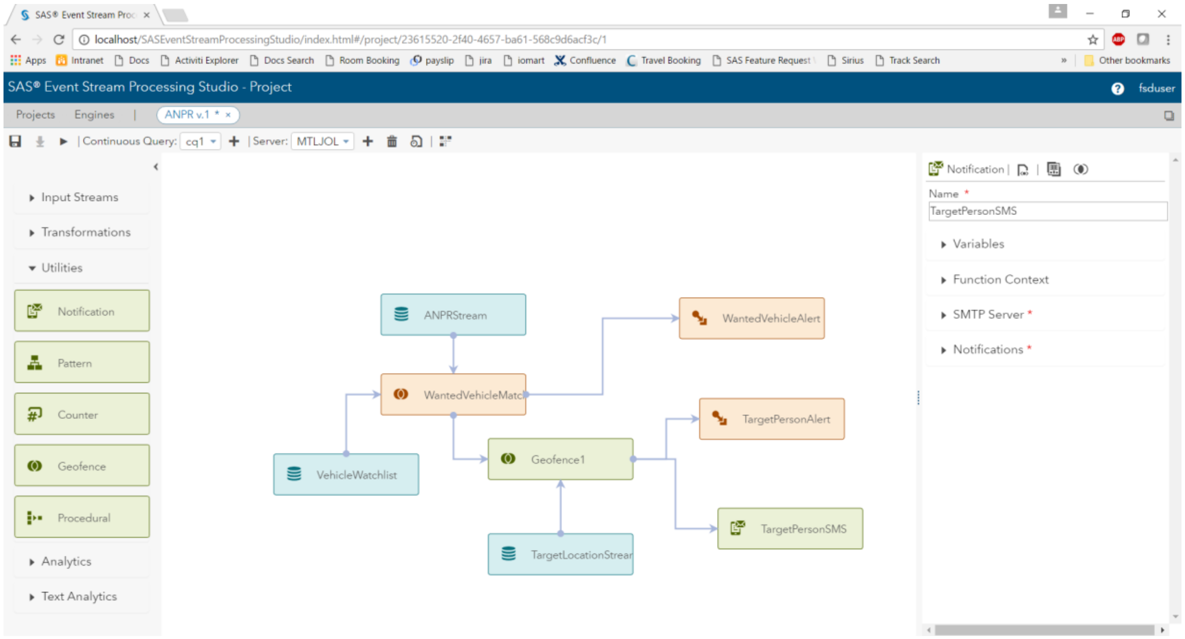
There is an expectation--however unrealistic--that law enforcement and intelligence agencies have the capability to manage and exploit (at least in some form) **all** of the information sources held by or made available to them. However, even within a single organization data management can be challenging, as disparate information sets are often held in discrete "silos" – with different schemas, access rights, and organizational practices. Multi-agency collaboration only serves to increase this potential complexity, leaving practitioners with the task of interpreting significant quantities of ever-changing information, presented in a variety of ways. By adding layers of third-party, high-volume data sources (such as communications data or automatic license plate recognition data), the challenge only increases almost exponentially.

The limitation of software tools that have previously been available to agencies is that they may only be able to exploit available information after the event. An analysis of circumstances surrounding recent terror attacks would seem to indicate that investigators were unaware of critical information that was already held by their organization, which might therefore be seen to have missed opportunities for preemptive action. Inevitably, starting an investigation after an event has occurred leaves analysts and investigators playing catch-up as they try to keep pace with new investigative streams and evolving events.

Applicable SAS Viya Module

SAS Event Stream Processing can support agencies in addressing the challenges presented by the attempt to keep up with such potentially vast quantities of information by applying analytics to the data as it becomes available.

With SAS Event Stream Processing, huge volumes of data streaming in real time from multiple jurisdictions, organizations, and nations can be filtered, categorized, aggregated, and cleansed before being stored, saving operatives from having to sort through and interpret disconnected and often polluted data sources.



Continuous Query: cq1

Server: MTLJOL

Name * TargetPersonSMS

Figure 2. SAS Event Stream Processing identifying vehicle on watch list

SAS Event Stream Processing is a powerful tool that is capable of enhancing an organization's capacity to respond to emerging threats and take preemptive action. It can apply analytical models simultaneously to both fast-moving and static data, ensuring that relevant information is isolated and that analysts receive timely alerts related to significant events; identified criminal networks and activity; or anomalous behavior.

As an example: An alert is generated by two seemingly unconnected individuals traveling separately to a country with known affiliation to terrorism, their travel being paid for using the same credit card.

While alerts to items of significance are of great value, organizations are further challenged with converting such insights into operational action.

SAS MOBILE INVESTIGATOR

Business Challenge

The previously discussed acceptance that community and general policing data is now essential to the counterterrorism effort has exposed the weaknesses in existing systems. In most nations, the responsibility for the individual facets of such “day-to-day” policing is managed by distinct departments or units, potentially even split across multiple agencies or organizations (for example, road traffic, community policing, or criminal investigation units). An unfortunate--but natural--consequence of this reality has been that vital data is held in disparate stores, and with the limitations of legacy software, there is often no simple means to search across, rationalize, or identify information of significance within these “siloed” repositories.

While this situation is generally most prevalent among law enforcement agencies, similar architectural and functional challenges exist within the wider intelligence and security communities. The need for the modernization of systems is widespread, as these agencies seek to increase their access to and their exploitation of the data available to them.

Of particular note is a recognized need to improve the ability to obtain intelligence as quickly as possible (“fast time intelligence”) in the aftermath of a significant event. Weakness in this area was clearly evidenced in reviews of the post-incident responses of law-enforcement agencies to many of the recent European attacks. And while there is no argument that officers responding to those incidents deserve the highest praise, their actions would undoubtedly have been hampered by inevitable delays in identifying crucial investigative leads within such disconnected information stores.

Applicable SAS Viya Module

SAS Mobile Investigator is designed to meet the specific needs of intelligence, enforcement, and investigative agencies. It provides a comprehensive operational environment capable of supporting the nuanced processes of intelligence and law-enforcement agencies–an environment that is essential to ensure legislative and regulatory compliance–through key capabilities such as advanced search; tasking; operational reporting; a robust configurable security model; and comprehensive auditing.

SAS Mobile Investigator is a web-based application that uses responsive design to alter the ways that the various components are presented, ensuring that all functionality is easily available on whatever type of device is used to access the system (for example, mobile, desktop, and so on). Further, this design enables the capabilities of each device to be used as appropriate. For example, a user accessing the system via a mobile phone would be able to use the GPS capabilities of the device to log the precise location of an incident, and use the camera to capture an image or video, which could be immediately uploaded and made available.

While seemingly straightforward, the value associated with this type of mobile access cannot be overstated. Officers in the field can receive tasks, comply with due process, and upload what could prove to be invaluable information without having to return to an office or to a vehicle.

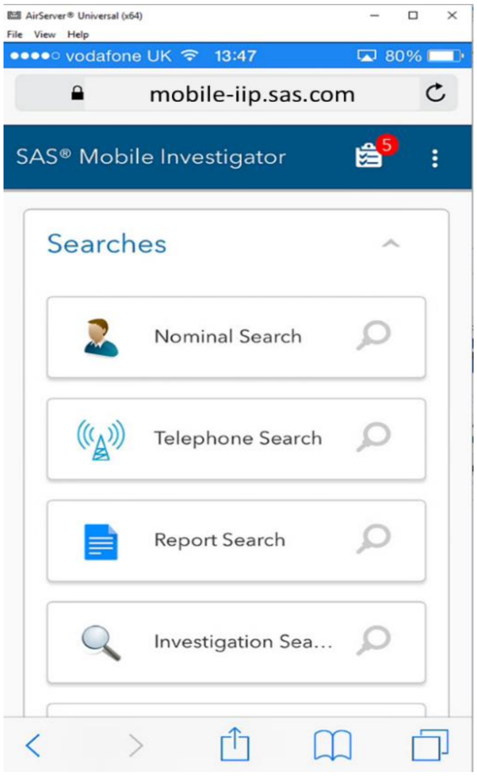


Figure 3: SAS Mobile Investigator

The enabling of officers to feed “street-level” intelligence directly into the corpus of knowledge about a particular individual, group, or community will enhance the agencies’ ability to spot behavioral patterns and anomalies, perhaps indicative of changing social dynamics, and to prioritize appropriate intervention, for example, investigation, education, or disruption.

Having field access to the totality of organizational data allows officers (in near real time) to review information relevant to live incidents, assess risks, and customize their responses appropriately while remaining cognizant of the "bigger picture". While these capabilities are clearly important for ongoing investigations and routine operational activity, the ability to facilitate fast time intelligence gathering and exchange of information in the immediate aftermath of a terrorist incident could prove crucial in facilitating early arrests, or preempting further attacks.

SAS VISUAL INVESTIGATOR

Business Challenge

The working practices of intelligence and law enforcement communities have evolved over many years and are generally well defined, reflecting the needs and priorities of individual organizations and their practitioners. These practices might still be valid today, but they must now be applied against the modern environment where the volume, variety, and velocity of data have reached unprecedented (and continually increasing) levels. In meeting these challenges, agencies require modern analytical tools that are able to refine and offer focus on relevant data while also supporting existing operational practices, so essential for intelligence development, for information sharing, and for ensuring the integrity of evidence collection.

Successful outcomes are often dependent on the early identification of factors that signify risk and require prioritization. These could include, for example, patterns within the data identifying known criminal networks, or a collection of (sometimes related; sometimes seemingly disparate) elements that indicate escalating risk. A real life example relating to the Salafi jihadist threat would be a pattern of actions, travel, communications, and lifestyle changes known to be a precursor to radicalization.

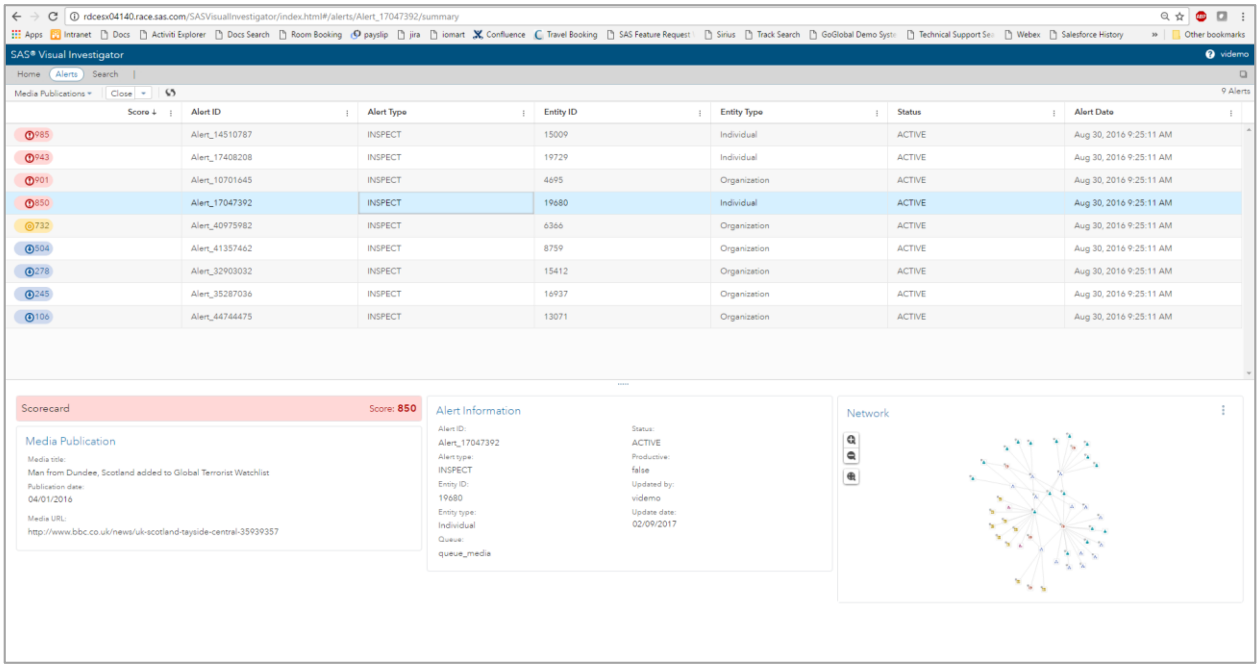
Applicable SAS Viya Module

SAS Visual Investigator provides an environment where operatives can–through the processes of alert generation, search, and the application of advanced analytics--work on and keep pace with the volume and variety of data that is now available to be exploited. Similar to SAS Mobile Investigator, SAS Visual Investigator supports (and where required, enforces) the nuances of operational process that are required for legislative and regulatory compliance.

As the nature of terrorist threats evolves, agencies will be required to adjust their focus to seek out objects and patterns within their data that could be of significance and require action. Alert generation through the application of rules and algorithms can highlight items of interest and, where possible, support early intervention.

Importantly, the graphical scenario builder feature in SAS Visual Investigator gives agencies the flexibility to address changing threats by designing, testing, and iterating rules that can automatically generate alerts on matching patterns within the data. This process can generate an alert based on the identification of a range of factors that, in isolation, might seem unrelated or of little significance, but when viewed as a whole, could be indicative of an escalating risk. For example, analysis might identify a pattern of behavioral factors, travel, and communications that could be associated with radicalization.

Scenarios that are designed within SAS Visual Investigator can also be enhanced using SAS Event Stream Processing to generate alerts from volume data in motion.



rdcesx04140.race.sas.com/SASVisualInvestigator/index.html#/alerts/Alert_17047392/summary

9 Alerts

Score	Alert ID	Alert Type	Entity ID	Entity Type	Status	Alert Date
985	Alert_14510787	INSPECT	15009	Individual	ACTIVE	Aug 30, 2016 9:25:11 AM
943	Alert_17408208	INSPECT	19729	Individual	ACTIVE	Aug 30, 2016 9:25:11 AM
901	Alert_10701645	INSPECT	4695	Organization	ACTIVE	Aug 30, 2016 9:25:11 AM
850	Alert_17047392	INSPECT	19680	Individual	ACTIVE	Aug 30, 2016 9:25:11 AM
732	Alert_40975982	INSPECT	6366	Organization	ACTIVE	Aug 30, 2016 9:25:11 AM
504	Alert_41357462	INSPECT	8759	Organization	ACTIVE	Aug 30, 2016 9:25:11 AM
278	Alert_32903032	INSPECT	15412	Organization	ACTIVE	Aug 30, 2016 9:25:11 AM
245	Alert_35287036	INSPECT	16937	Organization	ACTIVE	Aug 30, 2016 9:25:11 AM
106	Alert_44744475	INSPECT	13071	Organization	ACTIVE	Aug 30, 2016 9:25:11 AM

Scorecard Score: 850

Media Publication

Media title:
Man from Dundee, Scotland added to Global Terrorist Watchlist

Publication date:
04/01/2016

Media URL:
http://www.bbc.co.uk/news/uk-scotland-tayside-central-35939357

Alert Information

Alert ID: Alert_17047392
Alert type: INSPECT
Entity ID: 19680
Entity type: Individual
Queue: queue_media
Status: ACTIVE
Productive: false
Updated by: videmo
Update date: 02/09/2017

Network

Figure 4. Example of SAS Visual Investigator alert management dashboard

The operationalization of data (including analytically derived alerts) is of paramount importance in counterterrorism efforts. SAS Visual Investigator supports triage, prioritization, and assignment of responsibility. Advanced analytical capabilities allow agencies to develop intelligence insights and uncover investigative streams.

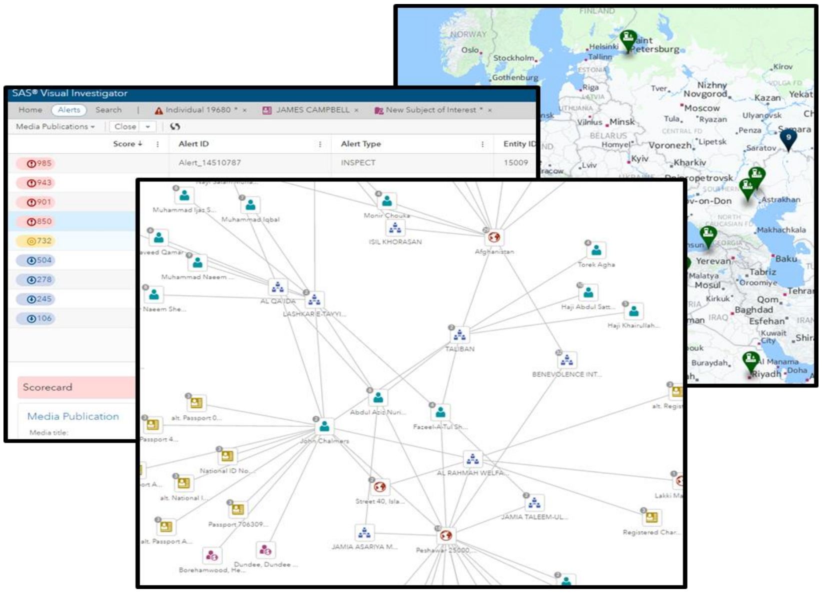


Figure 5. SAS Visual Investigator network diagrams, map views

In addition, insights that are derived from the data (such as network diagrams, timelines, or map views) can be used to create operational products that are essential to advance the work of agencies. For example, the data in SAS Visual Investigator can be used in the development of subject profiles, target packages, or threat assessments.

Crucially, data that is managed and developed within SAS Visual Investigator will be accessible through SAS Mobile Investigator, enabling officers to conduct research while in the field and receive tasks stemming from deskbound research.

CONCLUSION

The European and Transatlantic intelligence, security, and law-enforcement agencies are well aware of the changes and improvements required to be successful in meeting the real and growing threat of terrorism. While significant progress has been made in international and interagency collaboration, clear weaknesses remain.

It is widely accepted that organizational disconnects can exist in all areas and at every level of an agency and are regularly manifested in ineffective communication between stakeholders and an inability to fully exploit the available information assets.

The magnitude of the counterterrorism challenge cannot be overstated. While there is no "magic bullet" to solve the problems that global terror poses, SAS Viya represents a unique opportunity to work toward the much needed cohesion in approach and to build on the existing corporate knowledge of the threat. In a single platform, SAS Viya offers a comprehensive set of capabilities to manage huge volumes of data while simultaneously facilitating strategic and operational activities through a combination of advanced analytics and business process support.

REFERENCES

GLOBSEC Intelligence Reform Initiative - Reforming Transatlantic Counter-Terrorism

(http://www.cepolicy.org/sites/cepolicy.org/files/attachments/giri_report_1.pdf)

European Council to develop the EU Counter-Terrorism Strategy
(http://www.consilium.europa.eu/en/policies/fight-against-terrorism/)

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Lawrie Elder
SAS Investigation and Intelligence Practice
lawrie.elder@sas.com