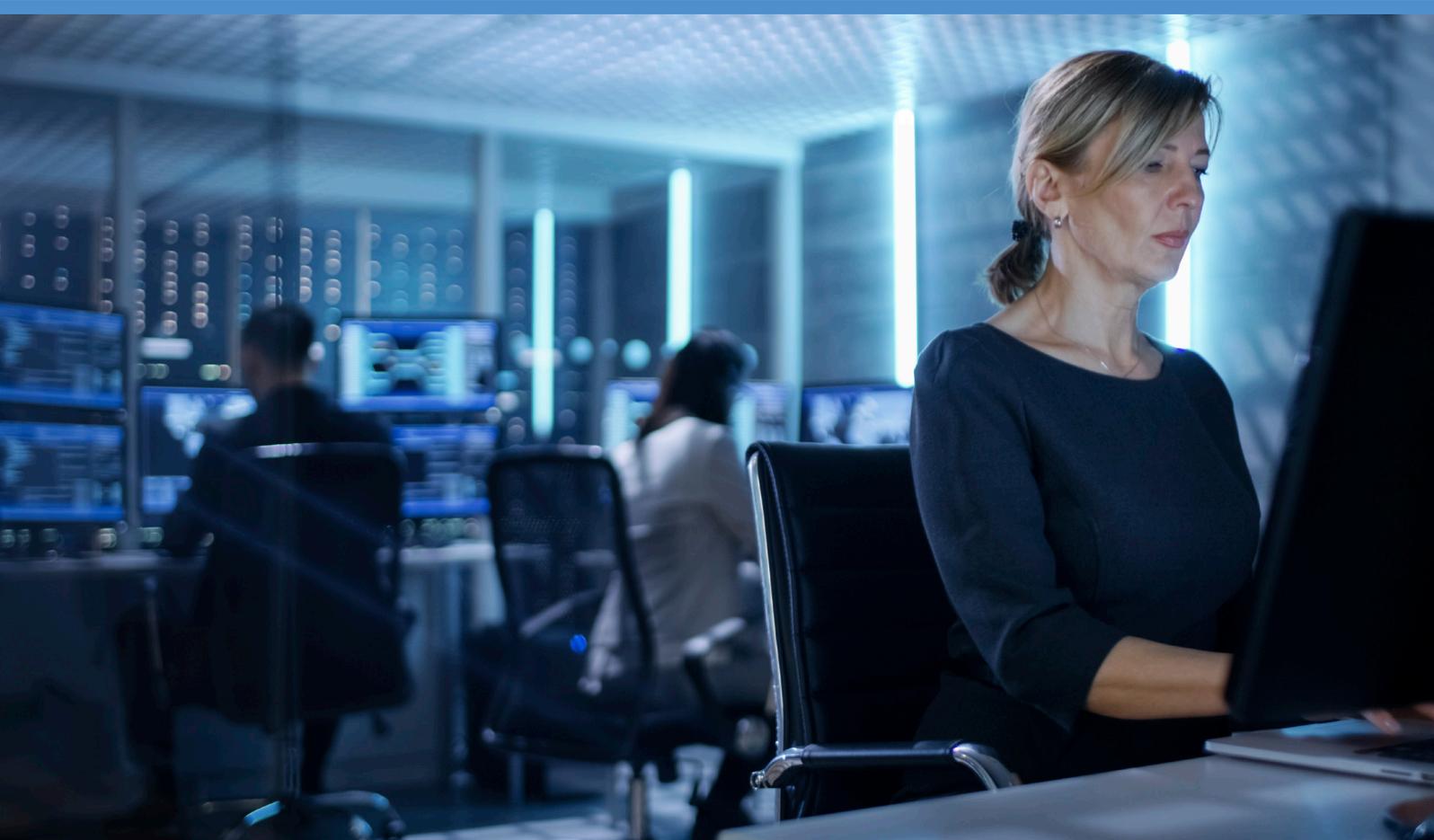


Managing the Intelligence Life Cycle: A More Effective Way to Tackle Crime



Contents

Executive Summary	1
Organizational Drivers for a Flexible Framework.....	1
Facing Up to the Challenges	2
A Workflow That Supports an Intelligence Life Cycle	4
Information Capture	4
How SAS® Can Help	4
Making Good Intelligence Matter	7

Executive Summary

What is intelligence? It's information that's been managed and processed to help drive action and prioritize resources so organizations can meet their goals and objectives. The fight against terrorism, crime and other threats depends on the availability and reliability of accurate, timely, complete intelligence. And intelligence is now seen as the cornerstone for protecting nations, organizations and citizens.

Intelligence professionals need to access all available, appropriate information, extract important elements, and process, analyze and disseminate intelligence quickly to keep ahead of potential threats. Terrorists and other criminals are already using technology to carry out their missions. The scale, complexity and changing nature of intelligence data makes it impossible to stay in front without using technology to collect, process and analyze big data.

Consumers of intelligence within investigative organizations need to be armed with the right information at the right time to make critical security decisions. To provide timely access to this intelligence, organizations require sophisticated IT applications to gather, analyze, disseminate and manage very large quantities of intelligence-related data. As information and collection techniques grow more sophisticated, so do the requirements for a technology solution that will simplify, rather than complicate, findings.

SAS offers a solution, SAS® Intelligence and Investigation Management, incorporating rigorous security workflows that reflect increasingly complex organizational structures and processes. Security is combined with efficiency to ensure information is properly shared and accessed on a need-to-know basis that reflects your users' organizational responsibilities.

Organizational Drivers for a Flexible Framework

Numerous requirements can drive the structure of an effective intelligence management system and make managing it a highly complex affair for organizations. In a successful intelligence management system, all information has potential use, but it must reside in a secure environment and be available for search, analysis, visualization and sharing in real time. The sheer volume and variety of the available data poses a huge and growing challenge.

Intelligence professionals must properly support and interlink every stage of the intelligence life cycle to be effective. Collection processes need to handle disparate, structured and unstructured information while making it easy to input information manually. In addition, processing must enable easy data access and analysis.

Organizations must base information management on a rigorous process for evaluating and grading information, and allow users to establish and visualize links among individuals, locations and organizations. Finally, appropriate intelligence must be delivered promptly to those who need it, in the format they require.

The scale, complexity and changing nature of intelligence data makes it impossible to stay in front without using technology to collect, process and analyze big data.

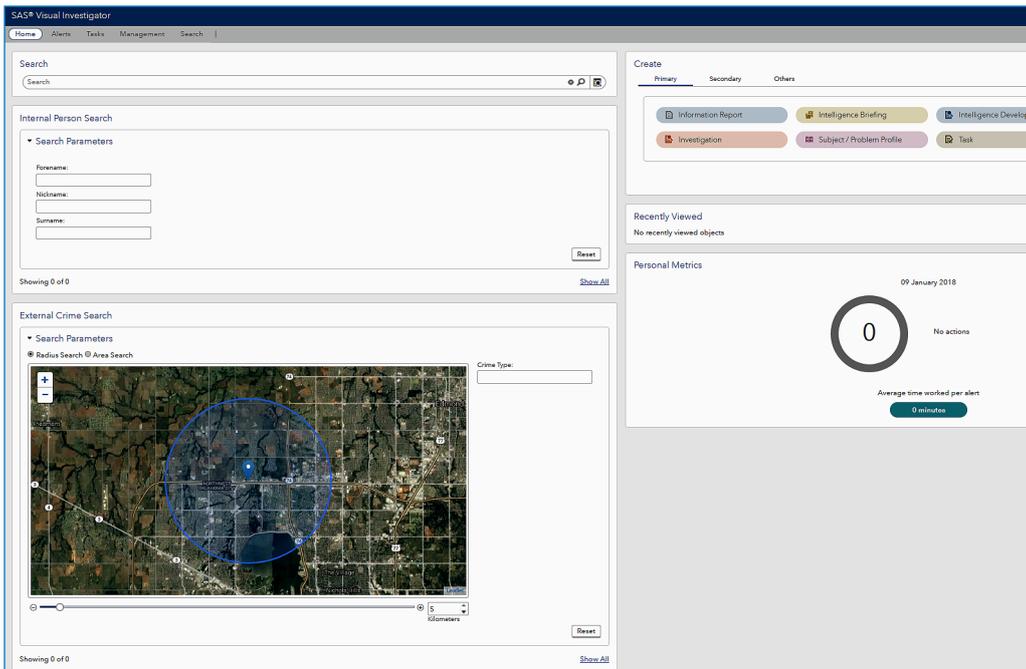


Figure 1: SAS® Intelligence and Investigation Management homepage featuring search ribbon controls.

Facing Up to the Challenges

Organizations wanting to carry out intelligence management need to set the objectives they want to achieve, see what information is available, and decide how to best process and manage that information to meet their goals. They need to evaluate the costs, resource allocation and effort required to achieve their objectives.

In general, the challenge they face is converting accessible data and information into intelligence, then making it available to those who need it without compromising security. This means an IT infrastructure needs to be in place to collate or enter all that data, store it, convert it into intelligence, analyze it and then share it among stakeholders in a timely manner. The result is thorough intelligence for investigations that provides key data points about a suspect or case, resulting in efficient investigations and added safety.

A disjointed approach could have cultural (a lack of willingness to collaborate, for instance) or technological causes that shouldn't be underestimated. Where different organizations use separate systems that don't communicate, time is wasted keying and re-keying information, with the added risk of vital intelligence being lost. This can easily lead to a lack of timely, accurate and complete information, which results in basing many vital decisions on subjective opinions rather than facts, and in faulty assessments of risks and threats to operators and the public.

Well-publicized incidents have highlighted the dangers that exist where systems are not properly linked, intelligence is not made available where it is needed, and potential targets are not identified.

Today it's becoming increasingly clear that public security organizations need properly linked enterprise systems for information management. The capability to access intelligence about entities from a central system with all related information allows you to analyze links and other social networks, then make them instantly available to all relevant stakeholders. Organizations must highlight targets at the point of contact so all personnel have the full picture at hand.

Even when relevant data is available, it will be of little benefit unless it is used effectively. If organizations don't correctly manage disparate data, different structures, formats and update rates, investigations can be delayed and decisions are likely to be slow and inaccurate. This is all avoidable with the right technology solution that helps reduce crime and threats. But it requires some operational planning.

Confronted with vast amounts of information in a variety of formats, intelligence operations may face an overwhelming task just getting the information into a consistent and usable state. Analysts' time can be unduly used on data management, resulting in delays in analytical output, overlooking key data, and out-of-date and unreliable information. This can result in analysts taking shortcuts that only offer subset views of data. Ultimately this can leave less time to carry out the skilled analysis that should be a core activity.

Technology can, of course, play a key role in addressing these issues. Investigators need to work from a single, integrated IT platform that provides access to all the critical information, eliminates duplication and streamlines processes to respond faster to threats.

It's not just about sharing and consolidating the information effectively. Organizations need analytics to reveal patterns, anomalies, key variables and relationships in the data, leading ultimately to new insights and better, faster answers.

In short, they urgently require systems that present their teams with all the relevant information, and then allow them to use analytics to effectively pinpoint and evaluate critical intelligence.

In addition, any intelligence management process must be based on the organization's needs and priorities. Appropriate personnel need information for grading, analysis, review and addressing of any queries. This requires a solution that is rigorous enough to enforce correct procedures, fast and user-friendly enough to avoid delays, and flexible enough to adapt to emerging organizational needs.

Intelligence professionals also need to access all appropriate information to extract the important elements, then process, analyze and disseminate intelligence quickly to keep ahead of potential threats. The sheer scale, complexity and constantly changing nature of this data requires a technology solution that can keep pace with changing data needs and expansion.

And lastly, if there are gaps or inconsistencies within the various stages of the intelligence life cycle, then analysts might overlook valuable information, delay sharing it, or not place it in its proper context, resulting in intelligence gaps. To address this, you need processes to manage information flow through the whole intelligence life cycle, including a record of who accessed or processed the information. Users do their best work when they have a clear and easily comprehensible view of all the information they have. Only then can they have a full understanding of the situation to make well-informed decisions.

Investigators need to work from a single, integrated IT platform that provides access to all the critical information, eliminates duplication and streamlines processes to respond faster to threats.

A Workflow That Supports an Intelligence Life Cycle

Crucial to the intelligence management challenge is the process of developing intelligence through a workflow that spans the entire intelligence life cycle.

Some organizations put large amounts of information into their intelligence systems but have no structured way to capitalize on it. Others seek to develop a minimum amount of intelligence on every item of information that comes into the system, important or not.

Managing all these information scenarios based on your organization's unique intelligence life cycle may seem like a complex problem, but SAS incorporates intelligence development functionality that manages each piece of information coming into an organization to simplify it. The process takes information from beginning to end, enabling the full development of intelligence that can then be used to counter threats more effectively.

Information Capture

The process used for entering information manually into an intelligence management system can be overly complex and time-consuming, leading to wasted time and inaccurate intelligence. Many intelligence operations require large-scale manual capture of information, which can be slow and cumbersome. The problem is compounded when information must be entered into multiple systems.

Organizations first need to ensure that information is relevant. Secondly, they need to assess whether the information needs additional work. Information captured at the beginning of the process may not have immediate relevance but needs to be kept on file for future investigations. Users need to be able to search multiple systems and easily identify the crucial bit of intelligence they need.

SAS provides an environment in which personnel can easily submit intelligence using intuitive tools, grade it using workflows, and take it to the next stage for assessment by more expert users.

How SAS® Can Help

SAS offers a lifecycle approach to intelligence management, which means organizations can configure workflow and supervisory processes to meet their own needs. They can then grade and effectively analyze information at the appropriate stages, creating intelligence to quickly share with those who need it, in the format they require.

SAS can deliver a complete, cohesive framework for total intelligence lifecycle management that allows users to expand, grow and modify their intelligence and security processes as threats change. These capabilities have been proven at agencies, large and small.

SAS enables intelligence professionals to efficiently and securely collect, process, evaluate, grade, analyze and disseminate intelligence. The solution provides powerful functionality to integrate data from virtually any source and exchange data between different platforms.

Security professionals can integrate SAS Intelligence and Investigation Management with other solutions for rapid and accurate exchange of data, supported by powerful data quality procedures and management of master data and metadata. The solution can also quickly and easily import, process and cleanse information from almost any source, so you can flexibly distribute intelligence across the organization to those who need it, when they need it, in the format they require.

A user-friendly interface helps users quickly enter information manually. Those in the field can easily add intelligence using mobile devices. Mobile input enables information to be entered as it's gathered, improving the timeliness of operations. In addition, pushing intelligence out to the field gives users access exactly when needed (for example, warning before they knock on the door of an armed individual).

SAS® Visual Investigator - Information Report

Home Alerts Tasks Management Search | Drugs 2018-01-06 x

0 Attachments

Main Report Information Location Links +

Risk of Serious Harm

Information Report Details

Category: Drugs

Title:

[Manage Source Details \(ISR\)](#)

Supervising Unit: Intel Supervisors

Event Date: 06/01/2018

Information Received: 09/01/2018

State: Unsubmitted

Control Strategy Alignment
Decrease impact of drug related crimes

Data Classification
CONFIDENTIAL

Intelligence Level
1 Local

Intelligence Grading
Source Evaluation:
1 - Reliable
Intelligence Assessment:
B - Known indirectly to the source but corroborated
Handling Code:
P - Lawful sharing permitted
Lawful Sharing Conditions

Markers

Risk of serious harm

Briefing Noteworthy

Briefing information

Brief Title
Local drug dealing

Details

Briefing Title
Local drug dealing

Briefing Summary
Drug dealing activity has been identified within this area

Record Properties

Figure 2: Information Report - quickly enter information and submit reports for supervision and evaluation.

Providing workflows for intelligence professionals, analysts and supervisors, the solution ensures information is directed to the appropriate teams to identify, grade and act on crucial intelligence. This means information is less likely to be delayed, misinterpreted or lost as it moves through the different stages of the intelligence process. It also means analysts can conduct valuable analysis and research, rather than simply preparing and processing data, to facilitate delivery of complete, accurate and timely intelligence.

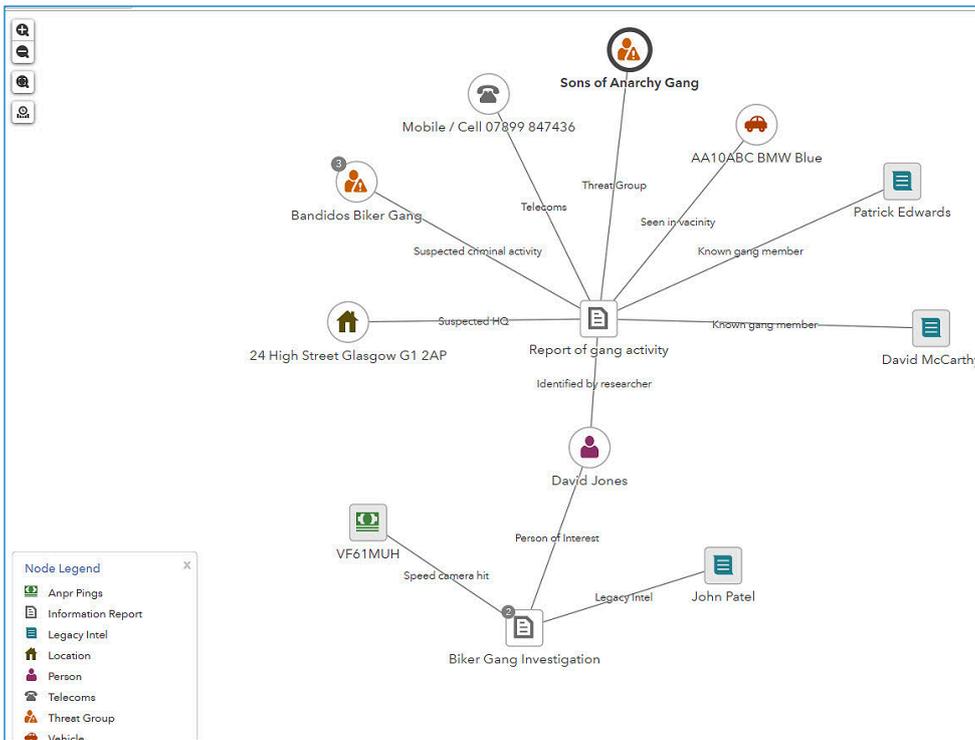


Figure 3: Link Chart - link records together by "drawing" a link line between nodes on the chart.

The solution's link analysis tools allow users to create, edit and view links to navigate through vast stores of information and build a clearer and more consistent view. The ability to create and visualize links provides insight into the structure of networks; shows how people, objects and locations are connected; and quickly forms a view of how pieces of information fit together.

Linked Records				Intelligence Development	
Firstname	Surname	DOB		Investigation	
Katie	Webb	21-Nov-1980		Legacy Intel	5
Harley	Rees	22-Oct-2044		Subject / Problem Profile	0
Madeline	Hart	11-Feb-1987		Threat Assessment	0
Bradley	Wyatt	19-Nov-1974			
John	Patel	25-Apr-1991			

Core Linked Records									ISR	
First Name	Last Name	Nickname	Date of Birth	Ethnicity	Color	Gender	Hair Color		Location	Organisation
David	Jones			White	White	Male	Brown		Person	2
Richard	Marks								Telecoms	0
									Threat Group	0
									Vehicle	0

Figure 4: Core Record Summary - view details of records linked to a specific intelligence report.

Common core records create a single version of the truth for consistent and up-to-date information using the people, objects, locations and events (POLE) methodology. When a new person appears in an intelligence report, SAS Intelligence and Investigation Management enables users to either create a new core record or link the person to an existing record. A single record kept for each entity - whether individual, object, location or event - avoids duplication and re-keying of information, enhancing data quality.

The SAS search capability makes all of this information accessible, allowing fast, accurate searching across a range of data formats. Users have instant access to real-time data so they can take account of the latest developments. Users get alerts from automated searches so they can act on new, relevant information. Intelligent search makes it easier to find inconsistently entered terms so you can base actions on relevant information. And you can search attachments to expand the scope, ensuring nothing is missed.

SAS Intelligence and Investigation Management incorporates security functions you can apply on a departmental or group basis to give the right users access to information across the whole enterprise. You can apply a covert security mode at the record level, meaning that specific users do not see the information at all, and alerts are sent to record owners to inform them that a search has taken place. The solution can also apply a protected security mode at the record level, which prevents access by specific users and alerts them that the record owner has protected the file and should be contacted for further information.

SAS also allows those with appropriate access to view the audit trail of information collected and edited at various stages of the intelligence cycle. This ability is essential to monitor, maintain and improve standards of intelligence activity, and to promptly identify and address any problems.

Making Good Intelligence Matter

The ultimate goal for any investigative organization is intelligence that can be acted on. Delivering better quality intelligence faster gives those responsible for public security the tools they need to deter threats, combat crime and protect national security. Unfortunately, good intelligence is a rare commodity.

Organizations struggle to refine vast amounts of data in a variety of formats into consistent, useful intelligence. They may also find it difficult to manage their intelligence workflow to get the best results. Information needs to be made available to the appropriate personnel for grading, analysis and review. Higher-priority items need to be routed and escalated accordingly. This requires a solution that is rigorous enough to enforce correct procedures, fast enough to avoid delays and flexible enough to change with organizational needs.

Organizations need to access all potential information, extract vital elements, and quickly process, analyze and disseminate intelligence. This can be impossible to achieve without the right technology to manage and share that intelligence. With gaps or inconsistencies between the different lifecycle stages, organizations may overlook crucial information, delay alerts or miss the proper context - putting their personnel and the public at risk as a result.

With more than 40 years of experience and proven performance supporting intelligence organizations at 170 locations around the globe, SAS is a leader in intelligence management. Our intelligence operations customers rely on the strength and power of SAS to support their missions, turning massive amounts of data into intelligence to make the world a safer place.

Delivering better quality intelligence faster gives those responsible for public security the tools they need to deter threats, combat crime and protect national security.

To contact your local SAS office, please visit: sas.com/offices

