Intelligence-Led Decision Making:

The difference between data, information and intelligence

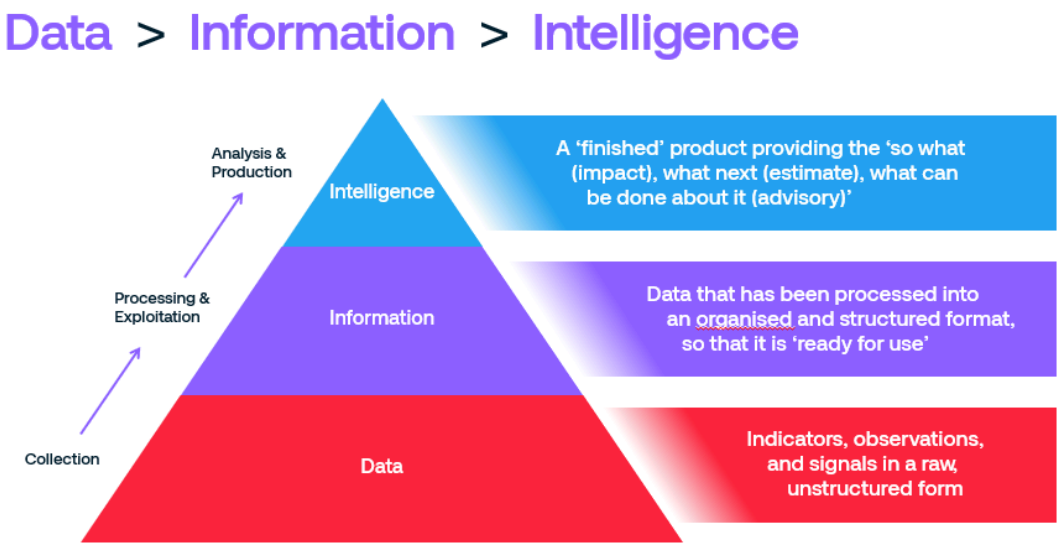
By: Michael Evans, Director, Securitas Risk Intelligence Center

In today's interconnected world, there is ever more opportunity for organizations and individuals to flourish. But where there is opportunity, there is also risk, and decision makers need every advantage when making decisions – and the confidence that those decisions are the right ones – to safeguard their organization and realize their opportunities.

The challenges this presents are further compounded by information disorder (a.k.a. misinformation, disinformation and malinformation) and emerging technologies such as artificial intelligence (particularly the rise of large language models, LLMs) and advances in targeted advertising and algorithms in search platforms and social media creating "echo chambers" in the information landscape.

Misinformation	Disinformation	Malinformation
False, but not created or shared with the intention of causing harm	Deliberately created to mislead, harm or manipulate	Based on fact, but used out of context to mislead, harm or manipulate

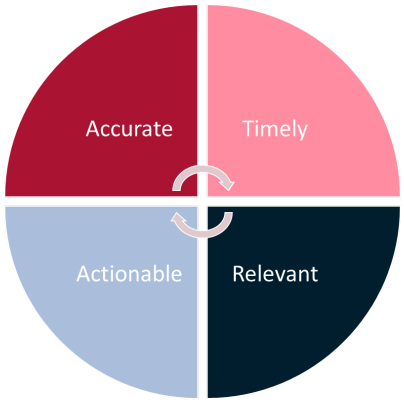
There is where intelligence, and the importance of understanding the difference between data > information > intelligence, come in.



Data > Information > Intelligence

Data, information and intelligence are definitions and terms that are often used interchangeably to describe evidence or knowledge of something; however, there are fundamental differences, and misunderstanding of these can lead to mistakes in how they are used.

Term	Description	Examples
Data	Data is raw indicators and observations in an unprocessed format. It can be considered "noise," and somewhere within it may be a signal. Another way of looking at data is to consider that individual data points taken alone "no nothing" but combined with other data points they may "know something."	• Media articles • Websites • Social media posts • Anecdotes from other people
Information	Information is data that has been combined with other data to provide a summary record. Think of it as establishing the facts. It takes multiple data points, collates them, ensures they are accurate and provides a summary of what is happening, including who, what, when, where, why and how (a.k.a. 5WH).	• A timeline of events • An overview of a location • A profile on a person • A report on an event
Intelligence	Intelligence takes information and analyzes it to provide customers/decision makers with an assessment, including an assessment of the impact of the information/incident (referred to as the "so what?"), a forecast of the future ("what if/next?") and advisory of effective courses of action ("what you can do about it").	• A threat assessment of a criminal organization • A travel security report for overseas travel • An event security threat assessment for a major conference



To ensure that intelligence meets the threshold of a decision maker's needs, intelligence should be accurate, timely, relevant and actionable. Additionally, if any one of these thresholds is not met, there is a risk that the intelligence is stuck in the information stage (i.e., if a report is missing an assessment including impact to the customer and guidance on what they can do about it), or worse, still in the raw data stage (i.e., if the analyst shares a URL to a web page or a post on social media without any accompanying explanation on why they are sharing it).

Source Intelligence

All good intelligence needs to start somewhere, and that includes using data readily available on the internet and provided by other sources. Intelligence in the world of security is often regarded as something used by the public sector, including policing, military and three-letter-agencies, for national security, espionage, and other clandestine purposes. The differences in how intelligence is sourced lies in the accessibility of the data/information. You will hear OSINT, CSINT and SOCMINT as a few examples of where information is sourced in a security operations center.

OSINT (Open Source Intelligence):
This involves gathering and analyzing information from publicly accessible sources like websites, social media, news articles and other publicly available data. OSINT is a valuable tool for various purposes, including cybersecurity, threat detection and monitoring public opinion.

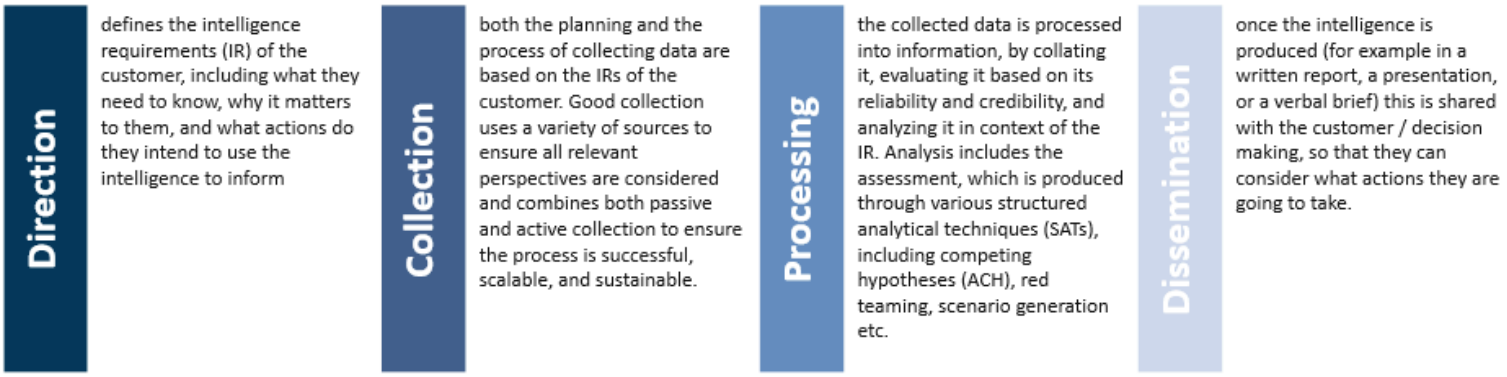
CSINT (Closed Source Intelligence):
This type of intelligence involves accessing information from sources that are not openly available to the public. These sources might include internal company documents, proprietary databases or restricted reports. CSINT often requires specific permissions or access privileges to obtain.

SOCMINT (Social Media Intelligence):
SOCMINT goes beyond simple social media monitoring, focusing on extracting detailed, meaningful information that can inform strategic decisions and optimize various operations. SOCMINT has three primary uses: threat analysis, cybersecurity and crisis management.

Intelligence in security is more often used to assess a threat (i.e., threats posed by a criminal operation) or to protect an asset (i.e., an assessment on the security of a CEO). Intelligence can be used for anything that relates to decision making (and not just security), as intelligence's fundamental purpose is to provide advantage. Decision makers need every available advantage when making decisions, and as such intelligence can be used for:

- **Raising the ALARM:** Warning decision makers of a potential threat that has the potential to cause harm or disruption.
- **Providing ASSURANCE:** Informing decision makers about something, assuring them that it is being monitored and providing them with peace of mind.
- **Maintaining AWARENESS:** Providing ongoing proactive intelligence on what is happening and why it matters, to keep decision makers informed and aware, while they focus on what matters most to them.

To turn data into information, then intelligence, analysts use the Intelligence Cycle, a systems -based approach for managing and operating intelligence. The result is finished intelligence. Feedback closes the loop, ensuring the intelligence cycle remains effective and relevant.



The real magic of intelligence comes in the assessment, which provides the alarm, assurance and/or awareness. An intelligence assessment includes the all-important so what, what if and what can be done about it.

- **So what?** Providing an assessment of what the data/information means to the customer/decision maker.
- **What if?** Forecasting what could happen next (including in the immediate and long term, as well as responses from other interested parties, i.e., how law enforcement will respond to criminality).
- **What can be done about it?** Advisory for effective actions and measures to mitigate threats, manage risks and make the most of opportunities.