Operation Nighthawk

Rapidly analyzing large volumes of multi-source data to provide live operational intelligence

Overview

The need
Coordinating the activities of Special Operations Forces requires analysts to analyze a vast flow of multi-source data in real-time, build up and share intelligence, and help define the next targets.

The solution
Working with IBM® Global Business Services® and IBM Business Partner Blue Light, the exercise command team used IBM i2® solutions to create a central intelligence repository, complete with powerful analytical capabilities.

The benefit
Increases efficiency, enabling limited resources to be focused on key targets. Helps analysts process extreme volumes of data to rapidly reveal hidden connections buried within massive datasets.

Special Operations Forces (SOF) from friendly countries use joint training exercises, such as Operation Nighthawk, to improve their own capabilities and to ensure that they can work together to counter cross-border and multi-national threats.

Operation Nighthawk was a 2014 multinational SOF training exercise, bringing together 1,600 personnel from military and police forces from more than 10 countries. The goal was to simulate a fast-paced deployment of SOF units to an active hotspot, and train both field operatives and support staff to plan and conduct special operations.

Finding fast answers from big volumes of data

Reporting to the central command team responsible for controlling the exercise were six Special Operations Task Groups (SOTGs) – four land/army, one maritime and one air (largely helicopter support). Each SOTG consisted of both field operatives and support staff. The exercise included elements of hostage taking, piracy, insurgency and terrorism. A key objective was for the intelligence teams to be able to identify and target key leaders within insurgency networks and terrorist cells.

"During one operation an analyst received apparently unassociated data from multiple sources, and used IBM i2 Enterprise Insight Analysis to conduct an investigation upon which an operational decision was made. This was data to decision in less than 15 minutes," says a Nighthawk Exercise Intelligence Lead.

Solution components

Software
- IBM® i2® Enterprise Insight Analysis

Services
- IBM Global Business Services®

IBM Business Partner
- Blue Light LLC

To enable the identification and prioritization of targets for ongoing operations, intelligence staff participating in the multi-day exercise were required to collect, organize and analyze data, and then disseminate the resulting information to multiple teams.

All operations were intelligence-driven and the command team deliberately designed a complicated scenario producing extreme quantities of highly diverse data for the intelligence teams to process and analyze. Deadlines were tight throughout: in the realm of Special Operations, planning cycles are typically very short. Operations must be approved, often by a local judge, and it is vital to have all data and derived intelligence readily available for rapid analysis. Any time wasted in searching for the relevant information could mean missed opportunities to apprehend suspects or prevent attacks.

During the exercise, teams were expected to fully analyze evidence within a matter of hours so that the next operational targets could be identified. Large volumes of diverse data (documents, emails, audio files, video files, websites) from multiple sources made this a major challenge.

Putting the pieces together with analytics

The Nighthawk Exercise Intelligence Lead comments: "Gathering and processing information is challenging enough, but understanding which information is the most important is even harder, particularly when the full picture is fragmented across multiple sources and across complex and evolving networks of suspects. We chose IBM i2 technologies to enable us to visualize connections and transactions across these networks, helping our analysts cut through the noise and focus on the best leads."

The central command team selected IBM i2 Enterprise Insight Analysis to power a central intelligence repository, proving an aggregated view of information that helped improve situational awareness across the SOF units participating in the exercise.

In addition, the command team deployed IBM i2 Analyst's Notebook® Premium to give analysts visualization tools that make it easier to find key information in large volumes of complex data. This solution helped analysts piece disparate data into a cohesive intelligence picture, identifying key individuals, events, connections and patterns that might otherwise have remained hidden.

"IBM i2 technologies help our analysts to analyze data rapidly and brief field operatives for the next stages of engagement."

— Exercise Intelligence Lead

Testing the solution

For this particular exercise, the analysts were working on a network comprising more than 5,000 mobile phones. To mimic a real-life deployment, analysts were given a constant flow of data and orders and were expected to plan and execute a number of overlapping missions.

The planning model used was called F3EAD. This acronym stands for: Find (identify the target), Fix (gather the required evidence), Finish (capture or nullify the target), Exploit (collect and organize evidence gathered in the field, such as maps, computers, mobile phones, notebooks, weapons and more), Analyze (establish patterns of life, relationships, ownership of vehicles and items, and then identify areas for further investigation), and finally Disseminate (document and share findings).

During the exercise, the joint teams used the central intelligence repository to store the results of the Exploit stage, making the data available over secure web-based search or through i2 Analyst's Notebook. This tool was then used to identify important relationships and help analysts understand where each person or item of interest fitted into the bigger picture. By pushing the results of this analysis back into the central repository, each team could easily share its new insights with other participants.

Revealing hidden connections to take down targets

Using the IBM technologies helped analysts on multiple teams manage large volumes of diverse data arriving in a constant flow, pick out the most interesting or significant information, and analyze it against the backdrop of the evidence already gathered to see connections and reveal the bigger picture. In turn, this enabled the analysts to steer field operatives towards the most relevant next targets, in the process gathering more information to feed back into the growing picture of the entire operational scenario.

As a concrete example of this intelligence cycle, field operatives recovered a paper notebook from a hostage taker onboard a ship early in the exercise. The contents were placed in the central repository, but no matches were found initially. The following day, the owner of a phone referenced in the notebook was captured. When it was established that the owner of the phone was a high-ranking pirate leader, the joint teams were able to establish a link between this pirate leader and a low-ranking pirate, thereby taking the first steps towards revealing the command structure of the pirate network.
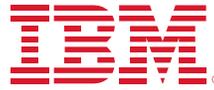
As the exercise progressed, more evidence was gathered and more links revealed, helping the joint teams to plan missions to disable the network. The Social Network Analysis capabilities of i2 Analyst's Notebook played a key role here, highlighting the most important nodes in the command structure. By focusing resources on these nodes, security forces were able to disable the whole structure more easily.

In previous exercises, information would end up in static reports shared by email. Identifying relationships between people and other forms of evidence was then dependent on analysts manually trawling through and noticing matches: a laborious and time-consuming process. Using the IBM i2 technologies, this process of cross-matching was automatic and took place in real time, providing a live view of the whole operational scenario as it evolved.

The Nighthawk Exercise Intelligence Lead concludes, "Using IBM i2 technologies enabled our joint task groups to work faster and more intelligently, helping them to identify relevant targets in a timely manner. In particular, the shared intelligence repository enabled us to collaborate in ways that were not practical previously, promoting better understanding between different SOF units and improving our joint capabilities."

About IBM Analytics

IBM Analytics offers one of the world's deepest and broadest analytics platform, domain and industry solutions that deliver new value to businesses, governments and individuals. For more information about how IBM Analytics helps to transform industries and professions with data, visit **ibm.com**/analytics. Follow us on Twitter at @IBMAnalytics, on our blog at **ibmbigdatahub.com** and join the conversation #IBMAnalytics.