GraphAware®

FILE NAME

THREAT CATEGORY

FILE CONTACTED

HAS THREAT

CONTAINS

HAS RESULTS

VIRUS SCANNED

FOUND THREAT

THREAT LABEL

ANALYSIS RESULT

VIRUS SCAN

CASE STUDY

Connected Data Analytics & Intelligence For National Security

GraphAware's client is a cyber defence company dedicated to protecting critical infrastructure and vital industry for national security purposes by combining open-sourceand commercially available intelligence.

Background

With the aim to monitor, prevent, and predict cyber attacks on various systems and infrastructures, the company deployed GraphAware Hume, a connected data analytics platform, to ingest all available data and discover threat patterns.

Using the platform to create a single knowledge graph allows intelligence analysts to investigate and track threat patterns, while collaborating on a unified canvas that connects technical details to the political threat level of such attacks.

BEFORE

- Disconnected attacks and actors
- Time-consuming manual process
- Difficult to share intelligence across teams

AFTER

- A single view of intelligence across any datasets
- Work that took a week, now takes a day
- Connected intelligence shared with ease across teams

Challenge

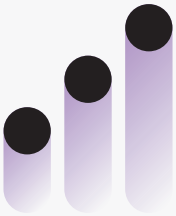
GraphAware Hume's flexibility allowed teams to perform with independence and creativity in creating a unified view of intelligence from diverse datasources.

The goal was to connect, structure, and match data, in a single view of intelligence so that information can be shared among multiple teams – from intelligence analysts, to political analysts.

Secondly, the client's team needed a way to bi-directionally navigate their data, to be able to identify actions that might be connected in the inherently hybrid nature of such attacks.

For example, an attack could come from a military-adjacent hacking group, or an unknown individual – being able to rapidly connect similar attacks via indicators of compromise, malware, or known associates enables exponentially faster response times.

The company's goal was to leverage its team's extensive experience with knowledge graphs to integrate all levels of intelligence, identify threats and vulnerabilities, and ultimately alert stakeholders to prevent hybrid attacks.



Solution

GraphAware Hume's flexibility allowed the company's team to fully utilise their independence and creativity in creating a unified view of intelligence from all siloed and diverse data sources.

The combination of advanced experience in graphs and machine learning from both the client and GraphAware resulted in a fully tailored solution that met the company's unique needs.

The connected data analysis platform allowed users to build their own advanced queries, allowing them to naturally understand and interrogate data coming from various sources in real-time. The company considered this independence and flexibility lacking from other solutions and providers.

Through Orchestra, all the data in the knowledge graph is constantly maintained and up-to-date to model the reality of threats and security. Intelligence analysts across the agency can rapidly share their newly acquired intelligence.

Results

The main goal to have a joint, single-source tool which ingested, connected, and matched the threat data was achieved.

According to plan, the solution was complete and brought significant value to the teams within 6 months.

The connected data analysis platform empowers the company to identify threats and connect malicious actors more efficiently and effectively within teams.

Work that took a week, now takes a day — allowing the agency to enact advanced analysis for all customers, with a very small team. This has resulted in a significant boost in reputation: the agency now seen as the go-to source for answers to complex technical and political questions, with rapid, demonstrably factual opinion-forming.

The agency's most top-level goals are now more achievable: better security for the nation, by having the intelligence capability to act on threats before they become a problem. They anticipate increasing the impact of the solution even more significantly over time.

We can warmly recommend working with the GraphAware team and their product Hume. Hume has already met our initial requirements and we are confident it will meet the extended requirements whereas Hume is constantly evolving in unison with our own requirements.

It's the best product we have encountered on the market that has a strong internal amount of creativity and allows you to maintain control.

GraphAware®
Hume

The power of Connected-data analytics

Flexibility and Creativity

When choosing a solution provider, our client prioritised flexibility. With their team's advanced experience, the ability to create custom data workflows was crucial for leveraging their expertise in data science and machine learning.

Connecting Levels of Intelligence

Bridging the top-down view of national security with the bottom-up view of tactics is crucial for our client's mission. Connected data analytics enhances the agency's key capability: comprehensive threat assessment from both strategic and tactical perspectives.

Predictive Power

Ultimately, the goal is to leverage the connected data analytics platform to integrate with the organisation's existing tools. This integration will enable advanced searches across departments, more effective identification of trends and patterns, early threat warnings, and prediction of future attacks.