NOVETTA

Novetta Cyber Analytics
Case Study: Department of Defense

DISCOVERING THE SIGNALS OF ADVANCED PERSISTENT THREATS THAT OTHER SYSTEMS MISS

When a large government agency was hit with multiple attacks, they needed answers. Even though they were actively using leading network forensics and packet capture (PCAP) tools, they were unable to execute queries and analysis quickly enough to uncover what had occurred.

ENHANCING SYSTEM EFFICIENCY AND EXPOSING CRITICAL INFORMATION

The Challenge

This frustrating process left them with more questions than answers. At the same time, they had made a large investment in placing these third party sensors to maintain a large archive. Processing and analyzing huge volumes of batch PCAP data collected from these sensors was impossible.

The Solution

Leveraging our years of experience in Advanced Analytics, Novetta delivered the Novetta Cyber Analytics Hub to empower the client with a large scale sensor-less analytics solution. The Novetta Cyber Analytics Hub provided not only the ability to scale and process terabytes of data in seconds but provided the analytics necessary for context and visibility into the surrounding suspicious activity associated with a network compromise. Within the first week of deployment, the agency was able to uncover the compromises that had gone undetected.

The Results

With Novetta Cyber Analytics, the agency was able to dramatically reduce time to discovery, finding previously hidden compromises and attacks within days of the initial deployment. We closed the gap, accelerated discovery and triage, reduced damage and subsequent expense. Perhaps most importantly, the agency was empowered to find critical key insights – the 'who, what, when, where, and why' of attacks, information that had been eluding them. With this insight, there were able to smartly design processes to thwart attacks, turning the tables on invasive techniques and hackers. Today this process is the cornerstone of their threat response team and it continues to help them protect their network from malicious attacks.

FROM COMPLEXITY TO CLARITY

Novetta delivers agile big data solutions and services to government and commercial organizations worldwide. Our advanced analytics cut through the clutter and enable our customers to quickly extract value from massive amounts of data. Our solutions—which include Data Analytics, Cyber Analytics, and Social Analytics—provide the clarity and actionable insight needed to meet our customers' most challenging business and mission requirements.

ROI in Action

- **Discovered previously hidden compromises and attacks**
  - **Within seconds and minutes able to triage**
  - **Uncovered who, what, when, where, why to empower data driven decisions**
- **Dramatically reduced the time to investigate incidents**
  - **Queries were hours or days, and are now seconds**
  - **Individuals were limited to 2-4 incidents a shift, now they handle 30X more**
- **Enhanced and provided immediate value of existing systems**
  - **Novetta Cyber Analytics Hub using third party PCAP sensors data**
  - **Improved process and feedback loop of Enterprise Security System**
- **Powered by Cyber Analytics Hub**
  - **Intelligent extraction**
  - **Packet in context**
  - **Threat intelligence and Enrichment Data**
  - **Integrated Network Behavioral Analytics**
  - **Right information at the right time**

LET US PROVE TO YOU JUST HOW EFFECTIVE THIS SOLUTION CAN BE.

For more information:
(844) NOVETTA (Toll Free)
(844) 668-3882
cyber-info@novetta.com
novetta.com/cyber-analytics