



### EMPOWERING NEAR-REAL TIME DISCOVERY OF ADVANCED PERSISTENT THREATS

*Like many organizations, an agency had been victimized by multiple cyber attacks. With their globally dispersed network of hundreds of entry and exit points along multiple 40Gbps network channels, gaining complete situational awareness of all network traffic was impossible. They knew something more must be done.*

*Novetta Cyber Analytics was able to overcome the agency's challenges by creating an Advanced Analytics solution purpose-built to address the specific needs of network security.*

### DRAMATICALLY REDUCING TIME TO DISCOVERY

#### The Challenge

Millions had been spent on infrastructure protection appliances and network forensic tools, but they were still blind to what was occurring. Their first indication of an attack came from the outside and took months if not years to uncover. Once discovered, pulling together the required context to properly triage or begin remediation was tedious if not impossible. They needed global visibility of what was occurring. Incident responders needed response times that were measured in seconds, not minutes, days or months. They needed the full context of the information normally stored in over six other systems.

#### The Solution

Novetta Cyber Analytics was able to overcome the agency's challenges by creating an Advanced Analytics solution purpose-built to address the specific needs of network security. From day one, the Incident Response Team was able to uncover malicious behavior that had gone undetected for months. We empowered Incident Responders and made them more effective and efficient with our ability to uncover compromise. Novetta Cyber Analytics provided the context of "who, what, when, why and where" associated with possible security breaches.

#### The Results

Novetta Cyber Analytics is a force multiplier. We accelerate the ability to rapidly discover network compromises. Users can now quickly pivot to triage and remediation. Unlike the enterprise security systems this client had in place, Novetta Cyber

Analytics had the power to interrupt the attack kill chain. It has become the cornerstone of the agency's Incident Response Team, equipping them with critical network-wide situational awareness, accelerating their operational tempo, and driving more value from their existing security defense systems.

### 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**
  - **Determine next course of action**
- **Dramatically reduced the time to investigate incidents**
  - **Queries were hours, and are now seconds**
  - **Individuals were limited to 4-5 incidents a shift, now they handle 30X more**
- **Complete global visibility**
  - **100+ sensors covering 1000+ locations**
  - **Millions of network users**
- **Empowered 300 incident responders and security analysts.**

### 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