

DataAdapt Threat Detect for Security and Intelligence Analysis

Challenges

Growth of asymmetric threats

Lack of actionable intelligence to identify threats

Inability to identify threats from multi-dimensional data

Difficulties in identifying threats from network data

Results

Enterprise awareness of vulnerabilities

Integrated data feeds into single custom object model

Compliance monitoring and threat discovery enhancement

Risk management and decision making enablement

Accelerating the Data to Decision Process

The threat landscape is constantly evolving, challenging the ability of organizations in both public and private sectors to identify, analyze, and mitigate its effects in a timely manner. From the growth of asymmetric cyber threats like information warfare and critical infrastructure protection, to the inability to identify threats due to the myriad of information sources, ViON® understands these challenges and provides a comprehensive platform to allow a quick and efficient response with DataAdapt Threat Detect.

Business Problem

Today, the enterprise faces multiple threats from the cyber domain – attacks such as malware, DDoS, and phishing; and constant risks including insider threats and Advanced Persistent Threats (APTs). In many cases, the aggressor benefits from the asymmetric nature of the threat, risking little while standing to gain a lot. It is up to our organizations to manage all of these disparate threats, assimilate all available intelligence, remediate breaches while mitigating future risks, all in an information technology industry that continues to evolve and innovate every day.

ViON's Solution

DataAdapt Threat Detect is an advanced analytics and data solution that accelerates the time to actionable insight for the intelligence analyst and others. Threat Detect uses market leading software, IBM i2 Enterprise Insight Analysis - part of IBM's Safer Planet Division - working with ViON to reach the speed and scale enterprises need. Threat Detect combines the i2 domain knowledge and expertise with the broader IBM software capabilities to provide a comprehensive solution allowing organizations to react quickly and efficiently to threats and situations.

With DataAdapt Threat Detect's automated analytics running in the background across hundreds of terabytes of data, organizations increase their awareness of vulnerabilities as analysts become more efficient and accurate. The solution integrates data feeds by merging structured and unstructured data into a single custom object model. This allows users to identify weaknesses by comparing vulnerability scans from each business unit with the appropriate network criticality and threat level. Information from all business units are monitored in real-time and statistical reporting and custom dashboards are easily created, thereby simplifying the measurement of KPIs.

Threat Detect has a variety of features that support commercial, defense and national security organizations including cyber threat analysis, social media and dark web analysis, enterprise risk management, fraud investigation, and insider threats.

Investigate & Reinforce Security Measures from Ongoing Cyber Attacks

Apply advanced analytics at speed and scale across overwhelming quantities and disparate sources of intelligence data, develop a comprehensive picture of your adversaries, uncover hidden connections and patterns in near real-time.

Facilitate the Cyber Analysis Discipline

This new discipline and profession encompasses three elements:

- Information Security - blending aspects of network defense, confidentiality, assurance, and malware threats
- Intelligence Analysis - bringing the art of the intel cycle where information is directed, collected, processed, analyzed, produced, and disseminated
- Forensics Science -blending aspects of the investigative process, evidence handling, and latent evidence discovery

Visualize & Investigate

See data from multiple sources in a unique object model for exploration through **Visual Query** by querying data without needing technical or database skills; **Find Paths** by uncovering relationships among the billions of potential paths – within seconds; use **Conditional Formatting** by adding emphasis to objects and relationships to make issues immediately visible.

Provide Robust Analytics Built In

Leverage deep algorithms to continually improve detection of non-obvious events by merging objects via Entity Resolution; find out “Who is Who” and “Who knows Whom” with alerts in real-time; employ a Recommendation Engine which discovers key patterns, events and relationships that are impossible to detect through manual analysis; and use Social Network Analysis (SNA) which ranks relationships between objects using multiple network analysis algorithms including K-Core, Eigenvector, Between-ness, Degree, etc.

For more information, please visit our website at vion.com/dataadapt or contact us at info@vion.com.



Understand multi-dimensional data by merging structured and unstructured data



Visualize data from multiple sources for exploration



Discover patterns and anomalies with deep algorithms



Create actionable intelligence with custom dashboards and reporting

About ViON

Designing and implementing innovative solutions that meet dramatically changing IT requirements is ViON's mission. With over 35 years experience, we've grown from a small product reseller into a leading systems integrator. We focus on data management, so you can focus on your organization's success. We're on the leading edge of Big Data and Cyber Analytics, Cloud, and Storage.



vion.com