Cloud Based Real-time Cyber Monitoring

Mr. Christopher Kenly
Vice President
Aveshka, Inc.

The Candor" Solution: Within the cyber security operations space, there has been a proliferation of proprietary tools that address specific mission areas (e.g., SIEMs, intrusion detection, intrusion prevention, network traffic analysis, log analysis). Aveshka�s Candor" data analytics solution helps solve a critical cyber security need to integrate, analyze, visualize and share information generated by these tools across the whole government from a unified interface. Candor" monitors cyber threats and vulnerabilities in real-time across data sets and tools in both structured (e.g., log data and IDS) and unstructured (e.g., incident reports, open-source threat feeds) formats. Candor" connects to diverse data sets, processes the data using natural language processing and advanced risk calculations, stores data in the cloud, and visualizes analyst-driven results. Visualizations include a log monitoring widget, a link analysis graph, a document viewer, a heat map, a timeline chart, a case manager, and multiple customized charts and views. Candor" applies custom analytics to not only monitor cyber attacks or malicious code in real-time, but identify trends and proactively address them before they result in compromise.

Candor" was designed and developed based on three core principles:

- Cloud-Based: Candor" is built on the industry standard Amazon Web Services platform that allows for scalability to meet the large data processing needs of cyber security stakeholders. It also leverages the use of the Government�s recent acquisitions and existing cloud environments.
- Open Source: Candor" uses open source technologies, reducing the reliance on priority software and enabling both backward and forward compatibility. This improves cyber security stakeholders� ability to fuse legacy and new data sources in one platform. With over 200+ open source software applications, Candor" conducts real-time and complex risk assessments across data sources.
- Analyst Driven: Candor" offers clients a light footprint and ease of use for analysts through its automated process of Extract-Transform-Load (ETL). Analysts can generate simple or complex queries and monitor its systems with no or minimal engineering support.

Support requirements: Candor" implementation typically include a 30-60 day assessment of needs, configuration, and deployment. This is followed by steady-state, updates, help desk support fully included in its license.

Expected Time to Market: Candor" is a mature technology that can be implemented for clients requiring cyber threat monitoring. Candor" works on an Agile software development cycle and releases updates and improvements to the platform to all clients on a monthly schedule.