MarkLogic®

Cyber Situational Awareness Solution

Integrating Cyber Data Silos

Large and complex organizations house multiple systems containing physical and network security. Log files for databases, servers, and applications, emails, firewalls, routers – as well as physical security such as building access, badge readers, and biometrics – are just a small list of areas to sweep when identifying a cyber threat. Over the years, a great deal of energy, innovation, and infrastructure has been invested in malware, threat detection, and logging – although there is still a lack of infrastructure, analysis, and best practices and protocols for sharing critical information that lies underneath all data. Data that can be used to prevent or analyze a cyber-attack on an organization can be buried in daily activities of employees, contractors, security offices, corporate risk management, workforce protection, and general security – all of which exist in various data silos.

Current cyber systems are largely dependent on legacy, rigid relational database management systems (RDBMS) or brittle over-engineered open source platforms that cannot easily accommodate changing sources or use aggregated data in ways that they were originally intended. The data output from security operations and security information event management systems (SIEM) and intrusion detection systems (IDS) are frequently stored in device and system specific formats. Realizing this, some organizations have invested in Hadoop-centric architectures along with rudimentary NoSQL platforms to support analytics and data science. These types of architecture fall short of providing a way to operationalize the data and the insights gained which leads to only a observation of events in a static manner.

Current limitations in today's cyber solutions include:

- A siloed view of all cyber threat indicators and warnings. Agencies and organizations are not able to see the continuum between indicators of compromise, advanced persistent threats, cyber alerts, cyber advisories, technical notes, and the individuals or groups that can harm systems
- Cannot view cyber threats in context of regulatory, policy, governance – which requires more than 'check the box' cyber defense.
- Limiting cyber data to mostly investigating log files

A Changing Landscape

Advances in malware and cyber-attack detection via newer methods of machine learning, artificial intelligence, and other approaches are replacing fingerprinting techniques – such as anti-virus packages manually installing anti-malware signatures to servers, workstations, and laptops. Still, there has been a lack of innovation to capture and characterize events that occur before and after an attack.

Today's Cyber Situational Awareness

- CERT messages
- Suspicious Activity Reports
- Incident Reports
- System documentation
- Bug/Patch/Fix systems and history from manufacturers
- Configuration management database (CMDB)
- Cyber alerts; advisories
- Technical Reports
- Reference Docs and Research Reports
- Industrial Control System Security and Training
- Hardware Scan Reports (IRIS Scanning)

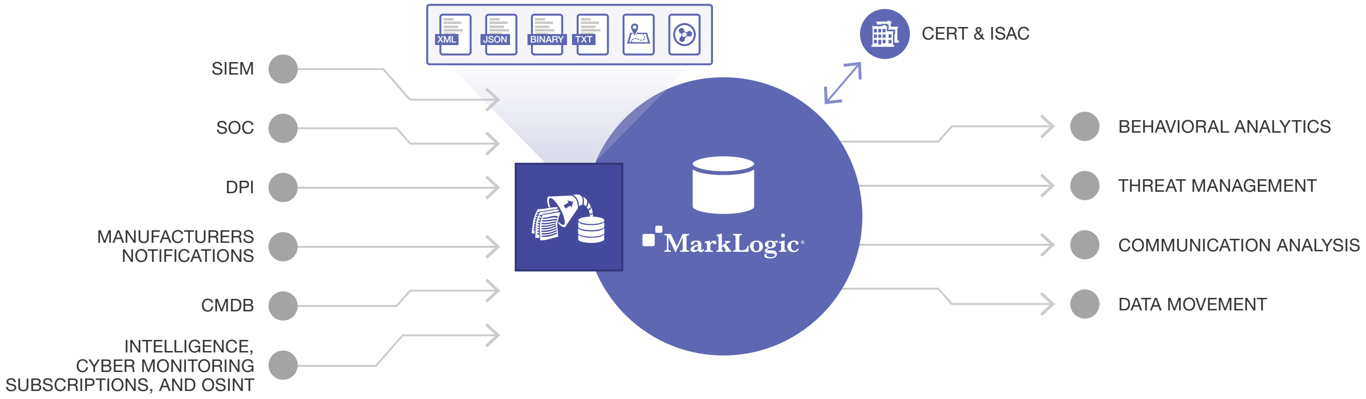
In the US Department of Defense, the Joint Improvised Explosive Device (IED) Defeat Organization (JIEDDO) put the focus on “left of boom” – which means instead of focusing how to protect themselves from the problem (the IED) they are focusing on how to prevent the problem – by studying the financing and funneling of funds, and going after the network of terrorists deploying the IEDs. To do the same in cyber security, you need the full understanding of cyber and operational vulnerabilities including social engineering – which requires a new way of looking at the cyber threat space.

National security and defense industries are faced with “all source” intelligence challenges – inter-agency collaboration is difficult because of the sensitivity of the data. For example, signal processing needs to be combined with cyber information, human intelligence, geospatial data, and other information to create a complete operational picture of threats and vulnerabilities. Combatting modern cyber threats is an all source problem that requires a flexible database to easily integrate all data trapped in silos.

A Modern Cyber Situational Awareness Solution

The MarkLogic® Cyber Situational Awareness solution integrates cyber data silos and provides transactional support between the various data sources and feeds and multiple communities of interest, delivering an integrated data set that can be used for analytical tools to exploit and disseminate information. Implementing this solution will eliminate the extensive cost and effort of performing (and maintaining) point-to-point integration between all of the sources and downstream analytics. It can complement existing SOA and/or Enterprise Services Buses, and allows legacy and existing systems to stay operational, while building new applications atop of all integrated data. With all data indexed and exposed via RESTful services, the solution decreases integration costs and complexity – while allowing secure information sharing of all cyber events. The Cyber Situational Awareness solution manages dissemination and redaction according to recommended US-CERT and similar international ‘traffic light protocols’ which need compartmented security for tags such as caveats, classifications, and communities of interest.

Deploying the MarkLogic cyber situational awareness solution drives real-time analysis and operational capabilities while reducing implementation and operations and maintenance costs. As industries and governments stand up new information sharing and analysis centers and cyber integrated threat centers, MarkLogic understands the need to bring together all aspects of cyber situational awareness in semantic, temporal, and geospatial context. To better integrate and share cyber data, information security analysis centers (ISACs) have been recently stood up in order to share community-specific information about cyber threats in areas such as finance, health, industrial control systems, oil & gas, energy and public safety. The MarkLogic solution can support and enhance these important efforts.



MarkLogic can be deployed as an Operational Data Hub providing read/write integration with multiple data silos and indexing it for search, sharing, analytics, and dissemination

Implementing a MarkLogic Cyber Situational Awareness Solution will:

- Integrate real-time and retrospective analysis to quickly organize and share information
- Expose all data to allow for easy search using drill down, faceted search
- Operationalize the insights driven by data science
- Provide a flexible persistence layer and alerting method for all signatures and filters created with deep packet inspection
- Support expression of indicators of compromise, advanced persistent threats, people, accounts, organizations, IT assets, and other high value cyber information as entities/objects to greatly aid in situational awareness and investigations

Proven Success

MarkLogic has been cited by multiple industry analysts as a leader in the operational and NoSQL database markets. We and our partners have deployed data integration, search, discovery, analysis, and content delivery solutions to some of the largest organizations in the world. These organizations need the unique combination of reliability, flexibility, and security that only the MarkLogic Enterprise NoSQL platform can provide.

About MarkLogic

For over a decade, organizations around the world have come to rely on MarkLogic to power their innovative information applications. As the world's experts at integrating data from silos, MarkLogic's operational and transactional Enterprise NoSQL database platform empowers our customers to build next generation applications on a unified, 360-degree view of their data. Headquartered in Silicon Valley, MarkLogic has offices throughout the U.S., Europe, Asia, and Australia.

MARKLOGIC CORPORATION
999 Skyway Road, Suite 200 San Carlos, CA 94070
+1 650 655 2300 | +1 877 992 8885 | www.marklogic.com | sales@marklogic.com