MarkLogic®

SOLUTIONS

Operational Data Hub for Cyber Threat Intelligence

Sharing Data to Improve Security

The Importance of Information Sharing

Security experts agree: we are only as safe our ability to share information about the nature and extent of breaches and cyber-attacks. The US National Institute of Standards and Technology (NIST) identifies several benefits to sharing threat information[1], including Shared Situational Awareness, Improved Security Posture, Knowledge Maturation, and Greater Defensive Agility.

And, it's not just good advice; countries including the EU, UK, Australia, US, and Singapore have begun formulating rules and policies for information sharing around cyber events – with a variety of organizations such as Information Sharing and Analysis Organizations, CERT, industry regulators, etc. These "Traffic Light Protocols" (TLP) stipulate that industry and governments triage content based on sensitivity and need-to-know.

> "The future of cyber defense is having a shared response or coordinated response. We need to break out of today's enterprise mentality of every person for themselves."
>
> Neal Ziring, Technical Director, NSA Capabilities Directorate – June 23, 2017

Obstacles

The problem is that not only do these attacks represent business threats, but there is legal and regulatory exposure as well – thus there are many dis-incentives to share. In large and complex organizations, even internal sharing information about systems and business risk is sometimes hampered because of lack of trust.

And, analyzing cyber threats is not just about looking at information traditionally thought of as 'Cyber' – such as log files. Organizations need to look at how Advanced Persistent Threats interact with the highest value business entities – accounts, customers, employees, transactions, privileges.

A large and complex organization, comprising multiple communities of interest, using siloed information systems, procured and implemented over years or decades, may have several related risk, threat, and security initiatives. Furthermore, these Risk Management, Insider Threat, Supply Chain Safety, Threat Management, Facilities security, and other initiatives themselves are creating data silos.

Integrating and analyzing this complex data usually takes significant resources – if the work is performed at all. This is primarily due to the cost, complexity, and expense of the ETL (Extract, Transform & Load) process required in traditional data integration using relational databases.

1 NIST SP 800-150, "Guide to Threat Information Sharing"

With MarkLogic, you can securely integrate cyber-related data silos along with key business entity information, to support threat intelligence analysis and information sharing.

Operational Data Hub Solution

MarkLogic® is the best database for integrating data from silos. For Government and highly regulated industries like Banking, Insurance, and Healthcare, our Enterprise NoSQL database platform has been implemented as an Operational Data Hub (ODH). An ODH is an authoritative multi-model data repository for cross-functional discovery and operations that harmonizes line-of-business data into canonical forms, frequently "entities," on an as-needed basis. It serves as a real-time data-centric interchange supporting enterprise operations and analysis/discovery throughout the data lifecycle.

Applied to the cyber threat intelligence space, this means that organizations can aggregate, monitor, and relate the most important events and entities across the enterprise and beyond. By establishing a common ODH on MarkLogic for all of the risk and threat management, insider threat, and related processes, organizations greatly reduce the cost, complexity, and time to bring on new data sources and drive monitoring and analytics.

Benefits for Cyber Threat Intelligence

At the heart of the ODH for cyber threat intelligence is the ability to bring together key transactions and entities along with the indicators of compromise, advanced persistent threats, and related system security information.

With a MarkLogic ODH, organizations can aggregate, index, and manage all information about security events, infrastructure, threats, etc., as entities – and build, maintain, semantically relate, and securely share information with data element level security, attribute and/or policy based access controls. MarkLogic's masking and redaction features can also be used to ensure that PII and other sensitive data are not exported in reports.

MarkLogic's ability to apply granular data access controls makes it the ideal platform to implement a TLP Protocol-compliant cyber threat intelligence platform.

As information is moved into the ODH so are the associated user privileges – and data lineage, stored as metadata. This can be done with unprecedented granularity including data element (cell) level security tagging.

Additionally, to complement the security investments that organizations make to maintain the 'hard shell' of network security, MarkLogic features encryption at rest, with separation of duties between security and data administrators, and frequently rotating keys.

A cyber threat intelligence ODH built on MarkLogic also goes a long way to reducing the enterprise surface area that can be exploited via malware. With MarkLogic, you relieve the application developer of the burden of handling critical security functionality and move it to the database platform.

MarkLogic, as a platform, implements best practices to mitigate the top common vulnerabilities identified by the SANS institute and OWASP – error handling and logging, data protection, configuration and operations, session management, authentication, input and output handling, and access control. In particular, moving logging, data protection, and data access controls to the database not only reduces complexity, but also extends the value of your organization's investments in endpoint, perimeter, network, and application security solutions.

Conclusion

Large and complex organizations that handle sensitive data from multiple sources for use by different communities of interest benefit from a MarkLogic ODH for cyber threat intelligence by:

- Reducing the cost, complexity, and expense of ETL
- Indexing all of the information needed for cyber threat intelligence in a single platform
- Having powerful access to search, alerting, and query
- Reducing the potential vectors for hacks and breaches

For more information on how MarkLogic is solving the toughest data integration challenges, visit www.marklogic.com.

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

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