Building a Cybersecurity Metrics Data Lake

Future of Cyber Analytics

KPMG Advisory, Technology Enablement

KPMG offers a approach that integrates data from various enterprise technology security platforms to provide them with actionable metrics to assess and remediate their effectiveness. Using a cloud data platform, cyber security teams can obtain timely, actionable, and thorough feedback on cyber protection.

Reduce Data Silos

Cyber security teams often rely on observation, inquiry, or sampling of disparate data sources, systems, and teams to evidence control effectiveness. As a result, effectiveness testing is potentially subjected to reduced accuracy and limited visibility into performance across the cyber security landscape. Disparate data sources that cause such operational inefficiencies are frequently a byproduct of:

- Lack of data standardization across various sources, creating an absence of "one source of truth"
- No centralized data model that can easily load source data
- Absent or poor existing data dictionary and understanding of data definitions

By leveraging cloud data platforms to centralize and host disparate data sources, organizations can reduce silos and build a thorough, unified view of enterprise environments, and gather meaningful insights

Automate Powerful Analytics

Control effectiveness testing, using ad-hoc observation, inquiry, or sampling results, in inconsistent or incomplete feedback to control owners.

By creating and unifying standardized effectiveness metrics with a common data model that centralizes siloed data sources and a cyber security asset inventory that serves as single source of truth, organizations can drive powerful analytics that provide the right information to the right people to make critical cyber decisions.

With high-capability enterprise technology approach tools for storage and ETL pipelines, organizations can improve the accuracy, frequency, and efficiency of controls monitoring with automated effectiveness tests to determine if organization standards and compliancy is being met.

Track Remediation in Near Real-Time

When cyber security teams heavily rely on anecdotal evidence and delayed feedback, visibility is lost into the true effectiveness of remediation projects. Timely and consistent high-quality input for control owners is vital to enable actionable and informed decision-making processes. Through high frequency scheduled updates and reports, control owners can monitor remediation lifecycles, reduce resolution times, and increase operational efficiency.

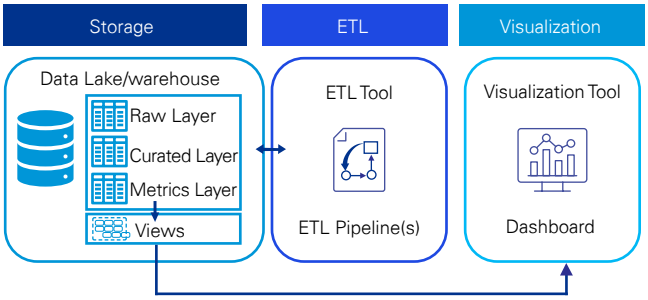
Technology Tooling

By leveraging a Cloud Data Platform to build a Cybersecurity Metrics Data Lake, organizations can plug and play various data sources to centralize and manage historical and point-in-time technical security platform source data and metrics results.

KPMG utilizes various ETL tool for metrics calculations, in conjunction with Cloud Data Platforms as a storage layer to effectively:

- Migrate data from an SFTP server to an KPMG hosted Cloud or host data directly within a client's Cloud environment
- Cleanse data from the RAW schema in the Cloud Data Platform
- Transform data into a CURATED layer using ETL tools such as Informatica
- Analyze output and migrate results to the METRICS schema in the Cloud Data Platform
- Automate and schedule pipeline deployment

Using Cloud Data Platform's plug and play capabilities through its ODBC driver connection, metrics can be visualized near real-time in BI tools. With powerful and automated analytics dashboards that cater to strategic, program, and operation perspectives, organizations can drive informative decision-making across all business units.



We're happy to meet with you to discuss our approach and discuss your organizations cybersecurity analytics needs. Please contact us if you are interested in:

Conducting a scoping meeting to review your organization's cyber metrics needs

Conducting a pilot phase for high-priority security platforms

Contact us

Thomas Haslam
Principal
T: 201-637-6024
E: thomashaslam@kpmg.com

Matthew Miller
Principal
T: 572-225-7842
E: matthewpmiller@KPMG.com

GiaPhu Dao
Managing Director
T: 919-800-9077
E: gdao@kpmg.com

Jean-Gabriel Prince
Director
T: +1 212-954-8717
E: jeangabrielprince@kpmg.com

Ryan Budnik
Director
T: 512-320-5200
E: rbudnik@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia