KPMG

Enhancing Cybersecurity through Data Analytics

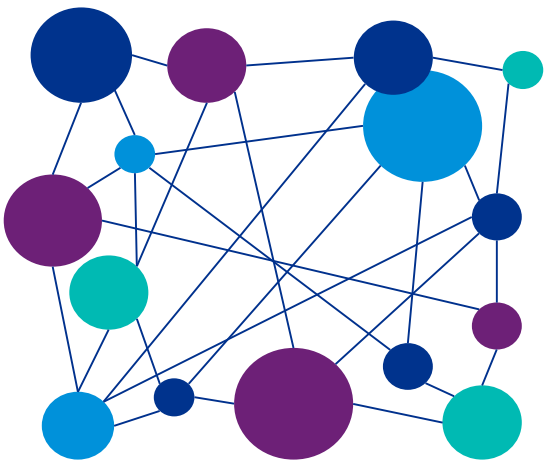
Overview

In July 2018, GAO identified four major cybersecurity challenges and ten critical actions that the federal government and other entities need to take to address them. At least eight actions Data and Analytics can play significant or important supportive roles:

- Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
- Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).
- Improve implementation of government-wide cybersecurity initiatives.
- Enhance the federal response to cyber incidents.
- Improve federal efforts to protect privacy and sensitive data.
- Address weaknesses in federal information security programs.
- Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.
- Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks.)

Services

Data, analytics and intelligent automation are fundamental to everything that we do to gain new insights and help drive successful business outcomes. KPMG's Cyber and Lighthouse teams leverage data analytics and artificial intelligence to enhance, accelerate, automate and augment business decisions and processes to accelerate enhanced data analytics methodologies and to help our clients make decisions quicker, better, and less often. Our team is proficient in the latest Data & Analytics capabilities, including statistics and modeling, supervised techniques, information extraction and retrieval, decision science, natural language processing, unsupervised learning and clustering, data mining, and machine learning. We embrace the potential of data-driven technologies and understand it must be carefully cultivated to become a trusted core capability.



KPMG combines Analytics with Security

SECURITY ANALYTICS USE CASES

Bridging Data Analytics and Security introduces a variety of use cases, from improving data visibility and threat detection to network traffic analysis and user behavior monitoring. Some of the most common security analytics use cases include:

- Employee monitoring
- Analyzing user behavior to detect potentially suspicious patterns
- Analyzing network traffic to pinpoint trends indicating potential attacks
- Identifying improper user account usage, such as shared accounts
- Detecting data exfiltration by attackers
- Detecting insider threats
- Identifying compromised accounts
- Investigating incidents
- Threat hunting
- Cyber Threat Intelligence Attribution

Above all, the primary goal of security analytics is to turn raw data from disparate sources into actionable insights to identify events that require an immediate response through the correlation of activities and alerts. In doing so, security analytics tools add a critical filter to the volumes of data generated by users, applications, networks, and other security solutions in place.

KPMG Analytics and Security as one

Cybersecurity practitioners manage the full attack lifecycle, including preparing for incidents and contingencies, detecting suspicious events and patterns, and responding to incidents and contingencies, through careful analysis of assets, users and accounts in the network in the day-to-day operations. The modern cybersecurity problems above-described have the following characteristics:

- Involve large and complex data – for example, network traffic, logs, vulnerability scanning software, etc.
- Continuously generated come in real-time.
- Hidden signals among huge noise – some events are hard to be captured.
- Fast-evolving threats – the rule-based approaches (e.g., black-list or white-list) are ineffective sometimes.
- Leveraging game theory to place cybersecurity as a strategy game between defender and attacker.
- Unknown unknowns – sometimes we don't know what patterns we are looking for.

Data & Analytics is integral to streamlining existing operations and manage risk and compliance.

For example, machine learning based behavioral analytics and stream processing frameworks can help improve security at a granular level (user or device) and a much faster rate. KPMG solutions can provide an essential layer of cyber defense to help agencies see connections that might otherwise be missed by siloed analysis of product log files or partial data analysis.

Conclusion

The introduction an analytics driven cyber strategy is integral in the deployment and support of continuing to enhance cyber security strategies within the federal government. This integration is critical to improve the overall return of not only security but an ever growing agency investment in technology. A critical part of an effective data analytics capability is building an additional means of identifying and introducing a top level layer of cyber defense that enhances, accelerates, automates and augments business decisions and processes. The introduction of this serves to accelerate enhanced methodologies and move away from a purely responsive cyber security strategy. KPMG does this by leveraging analytics driven security platforms and strategies for those entities within the federal government. In doing so, it effectively enables the transition away from traditional responsive cyber security strategies and builds a more strategic resiliency against future attacks.

Contacts

If you have questions or want more details regarding KPMG's Data Analytics services, please contact us:

Tony Hubbard
Principal, Advisory
T: 703-286-8320
E: thubbard@kpmg.com

Kevin Bauer
Manager
T: (845) 313-0088
E: kbauer1@kpmg.com

kpmg.com/socialmedia