TigerGraph

Solution Brief

Graph Analytics is a Better Way to Detect Cybersecurity Threats

Organizations Face Increasing Cybersecurity Threats

Cybersecurity attacks were estimated to cost an astounding $45 billion in 2018. The Internet Society's Online Trust Alliance, which identifies and promotes security and privacy best practices that build consumer confidence in the Internet, released its Cyber Incident & Breach Trends Report, which found the financial impact of ransomware rose by 60%, losses from business email compromise doubled, and cryptojacking incidents more than tripled, all despite the fact that overall breaches and exposed records were down in 2018.

Threats are only multiplying as more enterprises move to digital approaches to doing business, and embrace a wide array of internet-connected devices, fledgling blockchain networks, cloud and social media. Cybersecurity vulnerabilities and attacks can be both internal and external. Banking and financial institutions are often seen as the primary target for cyber attacks, however, the supply chain business, the medical/healthcare industry along with advertising, media and entertainment have sustained data breaches as well. Even as organizations implement emerging technologies into their core businesses to safeguard their crown jewels of information, malicious agents are also evolving, thereby increasing the nature of deceptive, stealth and automated cyber attacks.

Legacy defense mechanisms and security tools are unequipped to address the ever-evolving cyber threat landscape. Cybersecurity now requires advanced analytics that keep pace with the speed and scale of digital business. Organizations must leverage big data, cloud and AI-powered analytics to provide predictive insights and threat protection. The introduction of machine learning is critical in the automation of threat detection and eradication. The traditional security operations center analyst must become accustomed to working with more automation and rely on the speed it provides to ensure threat identification faster and at the pace the threat actors are attacking.

Graph Analytics is a Key Defense Against Cybersecurity Attacks

TigerGraph provides a key defense against cybersecurity threats. TigerGraph, which is native graph database with deep link analytics and in-database machine learning, is superior to the capabilities of the average SIEM solution on the market today.

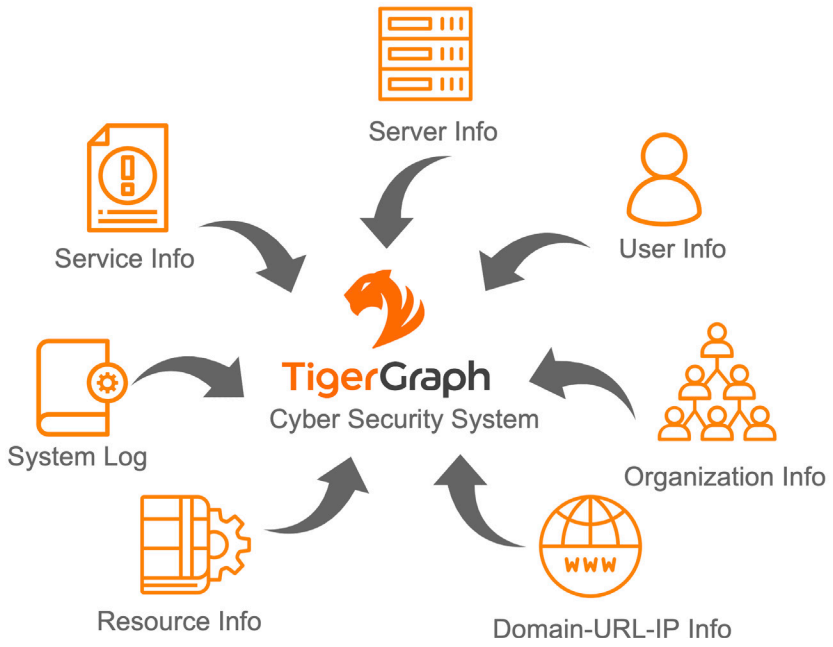

Figure 1: **TigerGraph builds a 360° views of relevant cybersecurity information**

TigerGraph provides the ability to:

- **Build 360° data views—**to gain a complete understanding of user activity patterns, data movement and more.
- **Reduce alert fatigue—**enabling SOC engineers and Analysts to focus on real threats with actionable intel in near real time responses.
- **Identify anomalies—**sooner enabling better proactive automation options ensuring that the response enacted by your analyst is more accurate and has less false positives.
- **Mitigate risks—**by enhancing the security stack investments already made through support of enhanced analytics and additional review capabilities.
- **Maintain data security—**with the world's most secure industry-standard server portfolio.
- **Achieve deployment flexibility—**that ensures easy integration with your existing solutions including all of the major cloud platforms.
- **Streamline operations—**by providing SOC and Security Analysts with tools that reduce stack review times and touch points.

TigerGraph's massively parallel processing architecture provides for both storage and computation, supporting real-time graph updates and offering built-in parallel computation. The graph database is Turing-complete and has both OLTP (Online Transaction Processing) and OLAP (Online Analytics Processing)

capability built in. TigerGraph has a comprehensive visual SDK, called GraphStudio, providing a rapid path from graph design to deployment with a robust MultiGraph service that allows for multi-tenancy. GraphStudio has strong RBAC permissioning for enterprise class security and auditing.

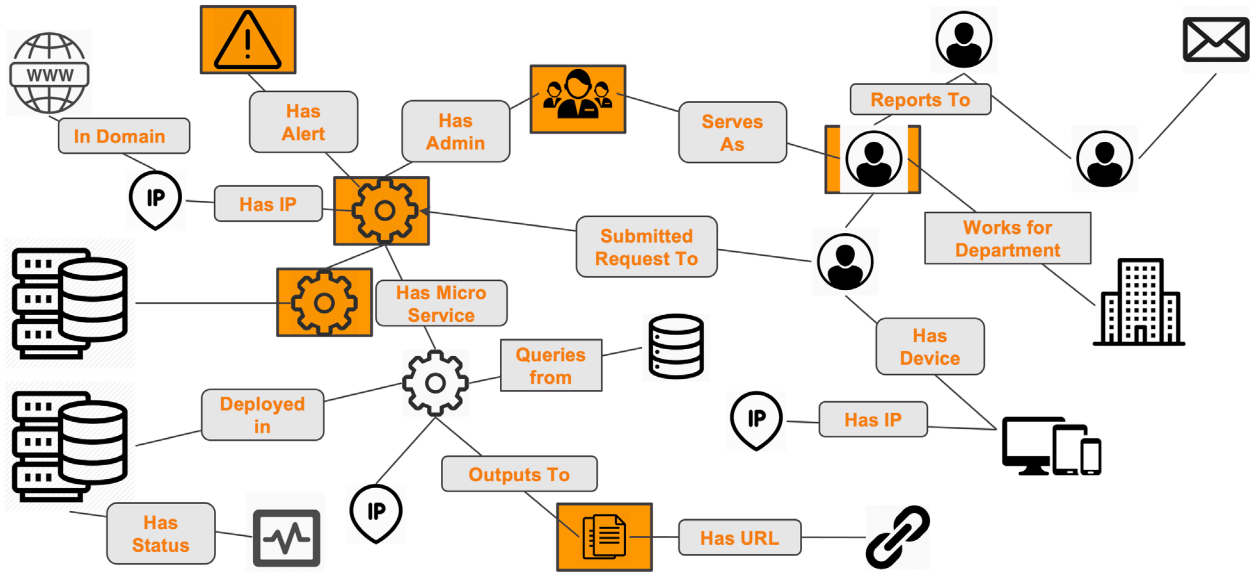

Figure 2: **TigerGraph's deep link analytics uncovers cybersecurity threats that traditional systems may miss**

Cybersecurity threat analytics helps focus on lateral movement and data mining. The identification of storage anomalies such as movements to unusual locations, culling of sensitive data & more. The data integration with robust, rest based API's ensure SOC teams can get value from data stored on any security stack solution quickly and efficiently. Advisory and professional services can power digital transformations and connect all disparate systems into a single pane of glass allowing your analysts to view automated reporting and analytics to ensure you are able to review the activities in near real time.

Organizations Are Adopting TigerGraph Graph to Fight Threats

Companies of all sizes are using TigerGraph to improve cybersecurity. With the right tools applied to the right datasets, companies can identify abnormal behavior patterns, unusual transactions, lateral movements, data mining and culling and all types of malicious actions inside their networks.

TigerGraph offers you the ability to conduct the following actions:

- Flooding detection
- Footprinting detection
- User behavior pattern matching
- Data mining tracing
- Data culling identification
- Credential compromise
- Source identification and tracing
- K nearest neighbor identification
- Blacklisted IP/Use tracking and tracing

Graph and AI/ML can be utilized to analyze aggregated data from multiple sources to predict likely future attacks and events. By analyzing data, especially with the help of artificial intelligence and/or in-database machine learning, data analysts can better predict and prevent events, enhance decision-making, dramatically reduce the time it takes to detect when breaches are occurring, and predict when and how they will occur. Keep in mind, it is not about preventing a breach. If a bad actor really wants in, they will get in. The goal should be to identify the potential threats earlier on the Mitre Attack Framework Kill Chain and stop them before your organization becomes a statistic.

About TigerGraph

TigerGraph is the only scalable graph database for the enterprise. TigerGraph's proven technology connects data silos for deeper, wider and operational analytics at scale. Four out of the top five global banks use TigerGraph for real-time fraud detection. Over 50 million patients receive care path recommendations to assist them on their wellness journey. 300 million consumers receive personalized offers with recommendation engines powered by TigerGraph. The energy infrastructure for 1 billion people is optimized by TigerGraph for reducing power outages. TigerGraph's proven technology supports applications such as fraud detection, customer 360, MDM, IoT, AI, and machine learning. **For more information visit www.tigergraph.com and follow us at:**
Facebook Twitter LinkedIn
Contact us at sales@tigergraph.com

TigerGraph | 3 Twin Dolphin Drive, Suite 225
Redwood City, California 94065
SB-GABWDCT-12012021