Security Challenges and the Big Data Opportunity

In advanced threat detection, multistructured data analysis provides a disruptive approach to identifying threats faster. The velocity of a company's intelligence-driven “kill chain” is the metric on which success is based, and optimizing this velocity means security solutions must operate in constant learning mode, adapting to adversaries’ strategies in real time. This situation, with its variety and complexity of data, is well-suited for both Hadoop®/Spark™ streaming analytics and approaches including machine learning and advanced graph algorithms.

For example, in insider threat detection, combining an organization's internal data (e.g., HR, physical security, IT logs) with external public data (criminal records, patent filings, web domain ownership, social media) and big data algorithms is highly effective in identifying the dynamic risks an organization faces. Continuous monitoring is required here, so analytics results must be updated in real time based on the ever-changing threat landscape.

In addition, for real-time system log analysis, graph algorithms have been applied to computer network data in multiple contexts, including botnet identification, unknown tradecraft/unknown threat identification and high-speed network analysis. This enables a shift in threat detection focus from finding only the most or least occurrences of an event to uncovering the most influential event(s). In these cases, graph centrality is the most effective measure, yielding fewer false positives and providing higher-fidelity detection of complex techniques and tactics meant to evade detection.

The Solution: A Converged, High-Performance Data-Security Platform

The Cray Urika®-GX platform converges supercomputing with the most advanced big-data capabilities in one powerful analytics solution. With the Urika-GX system, analysts can detect cyberattacks in real time and quickly remediate threats to the confidentiality, integrity and availability of critical business data and systems.
Cray® Urika®-GX Agile Analytics Platform for Cybersecurity
Empower Your Analysts to Detect Threats Faster

Key Capabilities for Security-Minded Companies and Organizations

• Run your entire analytics pipeline on a single, unified platform.
• Gain breakthrough insights by combining multiple big data workloads — from Hadoop and Spark for compute-heavy, memory-centric analytics to complex interactive graph data discovery for hard-to-find patterns.
• Get blazing-fast results due to Cray’s systems expertise: Aries™ interconnect, a high degree of parallelism, in-memory performance and optimized design.
• Employ machine learning methods enabling quicker adaptation to changes in techniques and tactics.
• Close the door on cyberthreats with an open analytics platform built on an open framework, with standard software and integrated design that reduces complexity and resource requirements and can evolve as new analytics technologies and regulations emerge.

Benefits for Security-Minded Companies and Organizations

• **Decrease mean time to detection:** Both faster detection and reduced infection dwell time reduce the risk to an organization's IP and sensitive data.
• **Improved responsiveness:** With the Urika-GX system, companies can adapt more quickly to changes in techniques and tactics — so you know as soon as possible when command and control traffic are indicative of malware or botnet activity.
• **Increased analyst productivity:** The Urika-GX platform reduces false positives that consume valuable research cycles, allowing analysts to focus on those incidents that present the greatest risk to the business.
• **Improved accuracy:** Create smarter behavioral-based algorithms to detect threats faster, ultimately improving organizational confidence in early threat detection.
• **Analytical agility:** With the Urika-GX platform, organizations can easily adapt to changing data sources, business questions and analytical approaches and be prepared for future security-related demands.

Getting Started

Find out how Cray's Urika-GX agile analytics platform can uncover a whole new world of insights — new connections, relationships and big opportunities — for companies concerned about cybersecurity. The key to success is understanding your data-intensive and highly iterative workflows and how Cray technology can benefit your organization.

• Learn more about the Urika-GX platform
• Find out more about Cray's solutions for cybersecurity
• Contact Cray