a³cube

KIRA Use Cases

The Converged Elastic, High-Performance Analytics Platform that changes the way to extract value from your data

Cybersecurity

SECURITY CHALLENGES AND THE BIG DATA OPPORTUNITY

In threat detection, 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.

In insider threat detection, combining an organization's internal data (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. Real-time system log analysis, 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).

a³cube

Key Capabilities for Cybersecurity

A3Cube brings scalable computing power, GPUs accelerations, extreme IO and storage, and analytics optimized capabilities in a single integrated appliance.

A Converged, High-Performance Data-Security Platform

Run your entire analytics pipeline on a single, powerful yet flexible platform with standard tools.
Using standard Hadoop/Spark tools or any other Analitycs software available without modification

Support multiple big data workloads in near-real-time, from massive parallel jobs to complex pattern-finding analytics, while avoiding data movement, with rapid integration of data from multiple sources.

Reduce false positives and speed time to better decisions in areas like drug repurposing and precision medicine.

Ensure your analytics infrastructure is built on an open, scalable framework with standard software and an integrated design that can evolve as new technologies emerge and the regulatory environment changes.

Benefits for Cybersecurity

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 KIRA 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 KIRA 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 KIRA platform, organizations can easily adapt to changing data sources, business questions and analytical approaches and be prepared for future security-related demands.

The Solution:

The KIRA platform converges the most advanced supercomputing features with the most advanced big data capabilities in one powerful analytics solution. KIRA integrates ultra low latency interconnection, high density computing, latest accelerators (GPUs) and elastic parallel file system.