KATANA GRAPH

SECURITY

Data Sheet: System Intrusion Detection

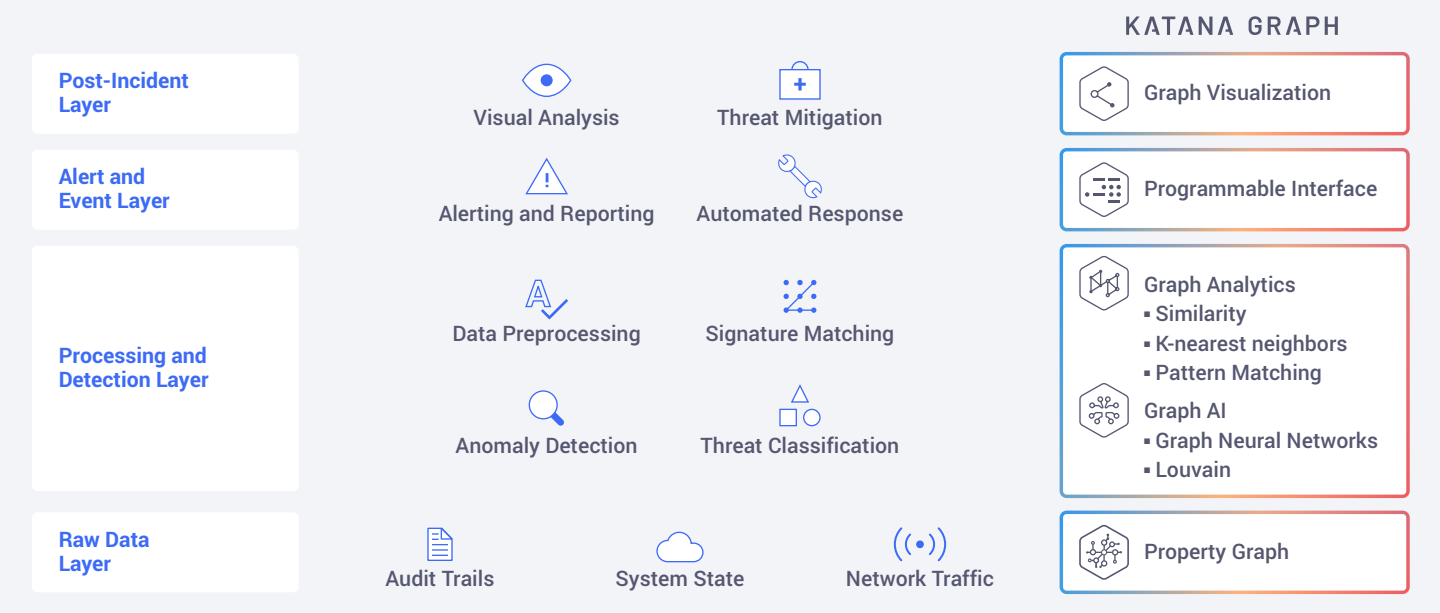
Organizations must be on constant guard against cybercrime activities including system and network intrusion. Intrusion detection systems (IDS) are a key part of any cybersecurity architecture, and yet, current IDS solutions remain relatively ineffective. Why?

Traditional IDS tools—even those with added machine learning and artificial intelligence (ML/AI) capabilities—only address isolated parts of the overall spectrum of system threats, while having common technical issues (see chart).

Hackers, knowing this all too well, deploy increasingly sophisticated tactics to slip through the cracks between existing IDS tools and evade detection. A new, modern technological approach for IDS is clearly required.

Traditional IDS types	Technical Issues
Signature-based IDS: Uses a knowledge-base of known malicious code ("signatures") to detect intrusions	▪ Only detects already known attacks ▪ Must constantly update database ▪ Risk of long delay between attack time and detection time
Anomaly-based IDS: Detects intrusions by comparing actual network traffic vs. baseline of normal activity	▪ High volume of false positive alerts ▪ Susceptible to attacks that mimic normal traffic to remain undetected until much deeper into the network
Anomaly-based IDS with ML/AI functionality to help reduce false positive alerts	▪ Limited value against real-network evolving adversarial attacks ▪ Network traffic and access flows are analyzed in isolation; no connectivity between records

Katana Graph™ Intelligence Platform detects a broad spectrum of intrusions in real time that might otherwise evade traditional IDS tools, through the power of next-generation graph analytics, mining and AI.



Unlike traditional IDS solutions, Katana Graph ingests, processes, unifies, learns and analyzes system and network data drawn from multiple sources in a relationship-based graph database structure, providing an exciting new level of intrusion detection:

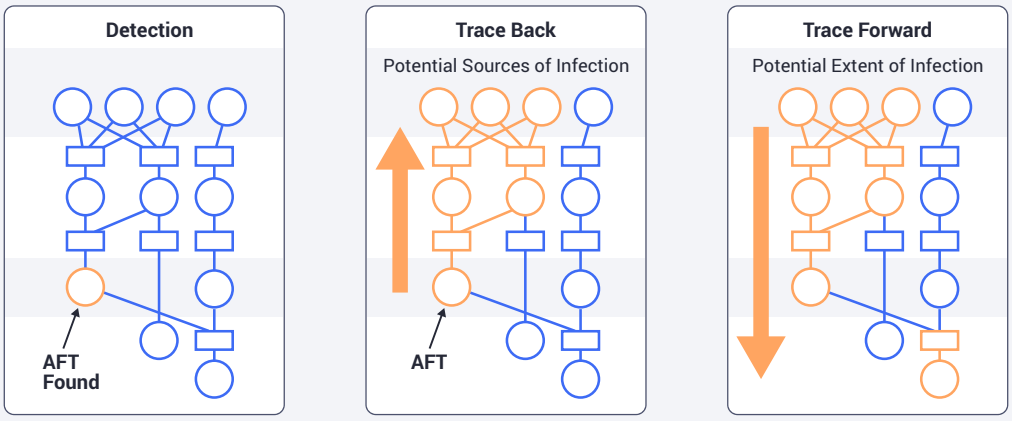
- **Synthesize all collected data into a single view** using labeled property graph data model; store and locate the structural patterns of malicious behaviors
- **Rapidly detect complex structural data patterns** using graph query and pattern recognition algorithms
- **State-of-the-art anomaly threat detection results with high accuracy** using natively supported advanced analytics and deep learning on large graphs, including Graph Neural Networks (GNN)
- **Easy integration with existing alert systems and applications** using programmable interface
- **Investigate alerts and attack groups and their connections** using native graph visualization

Katana Graph for Intrusion Detection in Action: Defense Advanced Research Project Agency (DARPA)

As part of its Transparent Computing Program, DARPA invited commercial vendors to participate in its Rapid Identification and Prevention of Exfiltration (RIPE) project. The purpose of the RIPE project was to investigate long-lived Advanced Persistent Threats (APTs) and to evaluate solutions enabling earlier detection of these attacks by preserving and processing causal relationships among activities.

Working in partnership with a government systems integrator, Katana Graph was the only vendor that presented a native-graph based technology platform approach designed to detect and analyze APTs by

- Stitching events into Katana Graph's next-generation high performance, horizontally scalable graph database
- Using graph queries to identify and detect APT behavior
- Tracing information flow from point of detection through the provenance graph around a suspicious activity node (see image, below) to infer causality and detect anomalies



During a two-week "capture-the-flag" exercise, Katana Graph and other vendors analyzed over 1.83 billion test activity records, which included attack datasets covering about 20 individual APT activity sequences. *The Katana Graph graph computing and data processing implementation achieved the highest detection rate of nearly 74%*

Contact Katana Graph today! info@katanagraph.com