KHIKA Threat Detection and Response Platform

Identify cyber-attacks as they are happening. Improve resilience with scalable & cost-effective platform for Threat Management and IT Compliance.

Most companies spend substantial effort on Perimeter solutions such as firewall and antivirus but pay little attention to detecting and responding to smart attacks. Monitoring what is happening 'inside' your perimeter is critical to a holistic security strategy.

Khika believes that security need not be expensive or time consuming and does comprehensive log and network monitoring, correlating it to external intelligence such as threat feeds

Features

Scalable NoSQL architecture

Affordable pricing

Ability to ingest custom, application and multiline logs easily

Correlation ability in real time and for historical data

Khika's readymade adapters are constantly updated to give you a seamless experience. Our custom adapters are enabled to assimilate non-standard logs with commodity scripts in multiple languages thus enabling new data sources such as custom applications

Khika provides access to real time threat information by integrating with community based and paid threat feeds from third parties. We track vulnerabilities with available exploits thus giving a quick view of essential patching required.

Khika's distributed architecture enables fetching endpoint logs from multiple geographies and correlating them with alerts from endpoint protection tools. Our machine learning expertise identifies anomalous behavior and sends alerts to take further action. Finally, our threat labs not only monitor threats constantly but also make sure that only credible data is consumed.

COMPREHENSIVE MONITORING

Readymade adapters

Custom adapters for applications

THREAT FEED INTEGRATION

Context based alerts

Vulnerability integration

BEHAVIORAL ANALYTICS

Endpoint View

Correlation & Anomaly detection

info@khika.com
+91 976 984 8849

How we do it?

Khika relies on NoSQL architecture for vertical and horizontal scaling of data storage along with our proprietary indexing engine. This ensures that the performance stays intact in spite of comprehensive log and flow monitoring. The scalability makes effective correlations possible over a period of time. This enables early detection of cyber threats and ability to respond effectively.

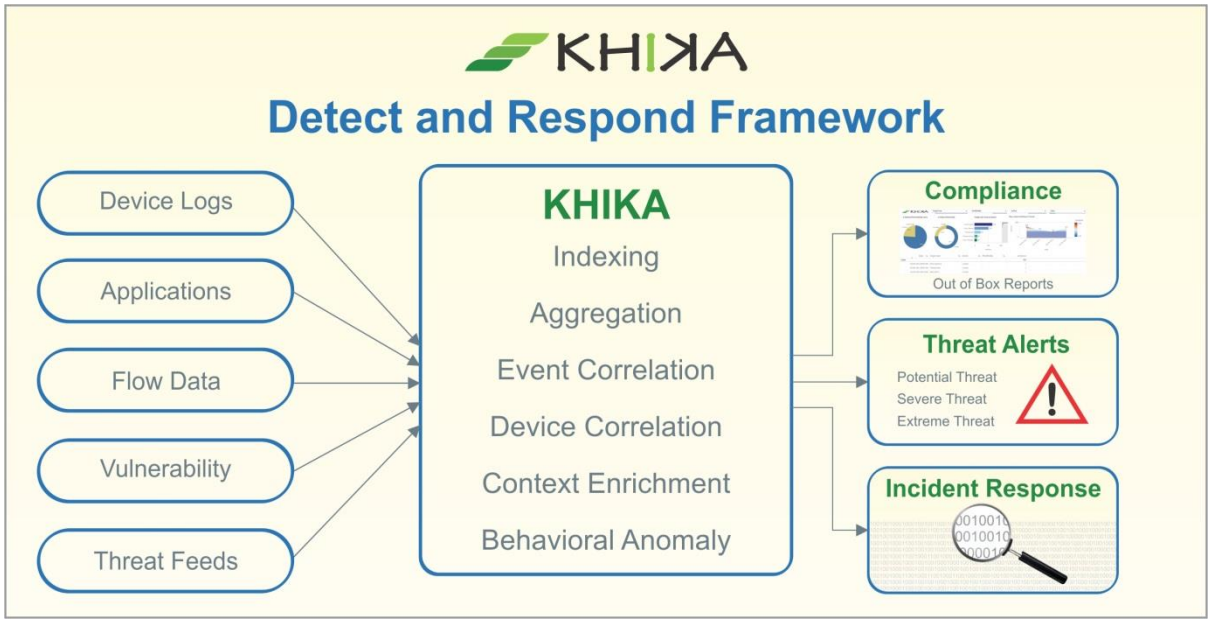

Figure 1: Khika functional architecture

THREAT MANAGEMENT

Threat Intelligence
Integrate multiple threat feeds and see potential attacks crossing your IPS

Alert Prioritization
Prioritize alerts based on severity and impact and focus on the critical incidents

Privileged Access Monitoring
Monitor anomalous behaviour likely to compromise privileged user access to get credentials to multiple systems

Application Monitoring
Select from our set of application adapters or develop custom adapters easily

COMPLIANCE

Comprehensive Log Monitoring
Collect, Store, Analyze and Correlate logs in a single system at scale

Compliance Reporting
Automate compliance reports with out of box modules which can be customized

Server Hardening/Policy Monitoring
Ensure that your servers are actually configured for the policy defined, identify gaps and fix them to ensure smooth audits

File Integrity Monitoring (FIM)
Enable FIM for Windows as well as Linux servers.

INCIDENT RESPONSE

Forensics
Search large quantities of data at a great speed and decipher kill chain rather than hoping that the search will complete

Contextual Enrichment
Have contextual information readily available in the Khika console instead of manual lookups

Incident Management
Get timely alerts by email/SMS and integrate with ticketing system to ensure nothing is missed.

info@khika.com
+91 976 984 8849