KDware
Knowledge Discovery in Security

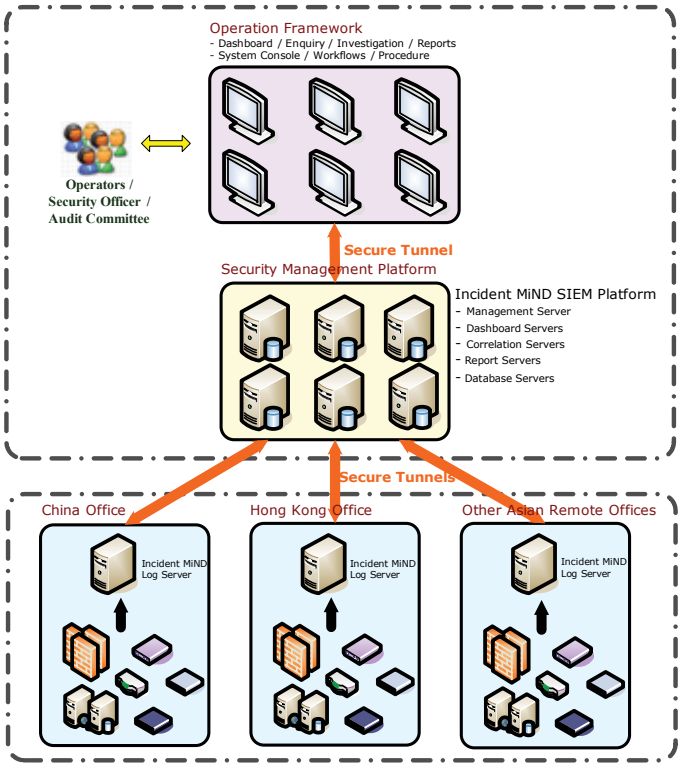
Incident MiND Your EYE to Security Incident

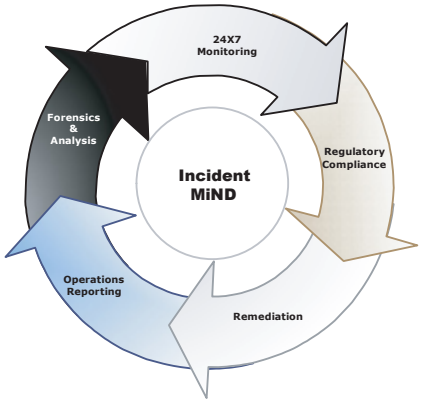
YOUR CHALLENGE »

Today's security architecture is complex with multi-layers. Many different brands of security devices are employed to protect servers, hosts and applications running on the network from threats in a more comprehensive way. Log data management is hence a vital element in managing network security, regulatory compliance and network availability in enterprises nowadays. Unmanageble of enormous logs which fired from different devices located diversely, or even within one site, are difficult and time-consuming to interpret and analyze. This implies a great loss of information, which is an important evidence for revealing abnormal events and attacks after accurate and effective correlation and analysis. The security vulnerability is thus increased due to inadequate information for monitoring network activities. Immediate, efficient and effective responses to attacks cannot be made either. This rising security concern is now proceeding into both managerial and operational views in enterprises.

OUR SOLUTION »

Incident MiND is an innovative product of Security Information and Event Management (SIEM). It enables security cross-product integration with real-time security incident handling in a centralized management console as integrated Security Incident Solution. Logs from all disparate security infrastructures are centrally collected, normalized, correlated and analyzed into meaningful information. Threats and attacks, which may not be detected when logs are viewed in separate consoles, can be visualized when logs are correlated and analyzed centrally with the time lapse consideration. Real-time events and post-event analysis benefit enterprises in focusing on threats and attacks which pose the greatest risk to business. The network security threats hence can be resolved efficiently and effectively in a cost-saving manner.





PRODUCT HIGHLIGHT

KDware Incident MiND is an edge Security Information and Event Management (SIEM) solution with in-depth real-time analysis of security incidents with prioritization facilitating intelligent decision for resolution.

PRODUCT FEATURES

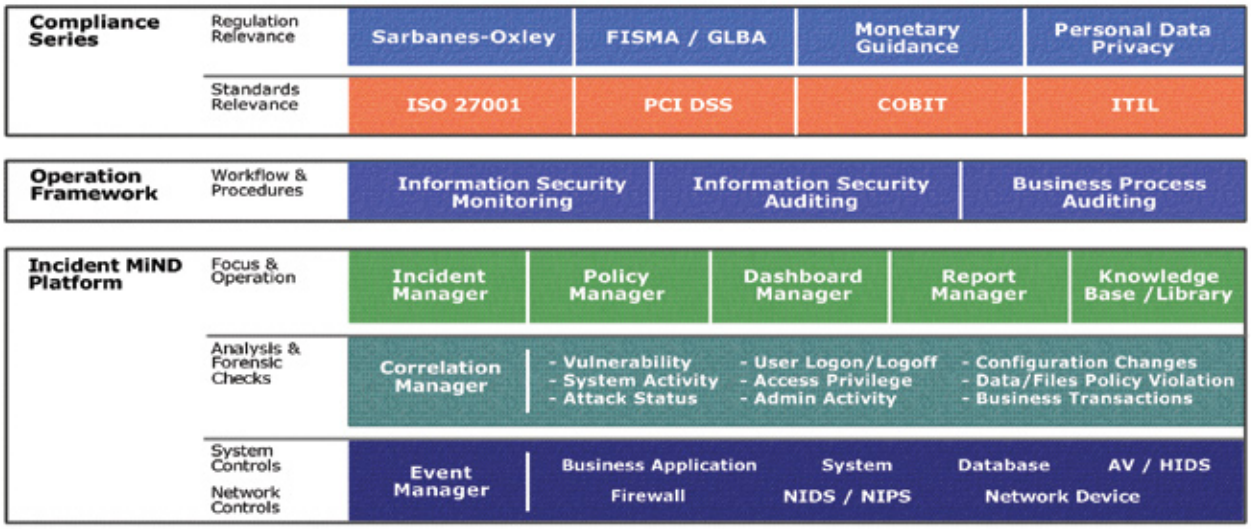
» Centralized Management
» Security Audit and Management
» 24 x 7 Security Monitoring
» Support multi-brands security devices
» Intelligence Filtering to False Positive
» Real-time Incident Identification and Workflow Control
» Event Correlation and Cross-Product Analysis
» Comprehensive Report

CUSTOMER BENEFITS

» Identifies threats in real-time
» Minimizes business loss by responding instantly
» Centralizes administration enhances operational efficiency
» Reduces false positive resulting in better resources utilization
» Discovery of previously undetectable threats
» Value-added to current security investment
» Low TCO for installation, deployment and administration with high valued returns

Copyright © 2009 KDware Ltd. All rights reserved.

KDware
Knowledge Discovery in Security



Incident MiND - Security Information and Event Management (SIEM) Platform for Multiple Compliance

EVENT MANAGER

Aggregates different event information

Event Manager provides a centralized collection and normalization via secure tunnels for system and network cross-product security alarms and event logs. Event logs from multi-vendor devices are transformed into a common format. This is convenient for correlation analysis which can be visualized in a single management console.

CORRELATION MANAGER

True-path to real-time performance

Correlation Manager builds in *Stateful Correlation* technology. It is designed to give the consistent high speed performance, throughput and scalability that global enterprises and telecommunication industry require. It utilizes parallelism of stateful correlation analysis to mitigate risk by flagging threats real-time before they compromise key business processes. The real threats are identified according to the level of coincidence with the sequent rules set in Policy Manager, which follow users' priorities, with the consideration on the business impacts. High potential attacks can truely idenified in real-time to reduce business impacts.

POLICY MANAGER

Address unique organization needs

Policy Manager provides a convenient path to enable and implement policies for Correlation Manager to execute. Pre-configured stateful correlation policies are offered which simplify configuration and system fine-tuning process. Enterprises can also tailor the out-of-the-box correlation to address the unique network environment and enhance the correlation accuracy.

DASHBOARD MANAGER

Real-time gobal view of complex environment

Dashboard Manager provides path for real-time close monitoring for vital recources which are critical to the network and business. Effective real-time control over the network and instant recovery of affected recources are facilitated.

INCIDENT MANAGER

Threat identification & incident response

Incident Manager determines severity levels for each security incident with business impact in fuzzy prioritization. All security incidents are presented in a single simple console which allows security administrators to focus resources on solving the highest risk security threats in visualization of intrusion scenario cases more efficiently.

REPORT MANAGER

Generating whole security pictures

Report Manager generates different types of reports for management or technical needs with whole security pictures for your network environment, instead of pieces of information from individual security devices. It offers instant and schedule report generation with standardized templates. Customization of clients' own report types and formats are welcomed.

KNOWLEDGE LIBRARY

Window to security world

Knowledge Library is a reference database with most updated information to various significant security bodies for security operations. It offers security event information as well as a database of security best practice references, such as sources from CERT, CVE and Security Focus. Operators and analysts command powerful decision support capabilities which, in turn, make incident handling a much easier and more streamlined process. In order to keep our security windows always open, KDware offers automatic online-update in Knowledge Library.

MULTI-COMPLIANCE APPROACH

Comprehensive complaince delivery

Compliance Series delivers comprehensive, best-practice-based, pre-defined set of compliance reports, correlation policies and dashboards which assist enterprises to address common regulations and starndards. Log-related audit requirements and practices are catered by compliance managers which delivers the most relevant and complete set of compliance content in the SIM market nowadays.

About KDware

KDware, means "Knowledge Discovery Ware", is a leading provider and innovator of hidden pattern discovery solutions and applications, specialized in security logs, events, and incidents analysis, using Data Mining technology. Our applications, serve for telecommunication industry, government, global enterprises, and small businesses, are widely adopted and distributed.

www.KDware.com **info@KDware.com**

Copyright © 2009 KDware Ltd. All rights reserved.