LogWave™

SIEM and Case Management for log and event collection, correlation, and analytics

Features & Benefits

- *SIEM capabilities for real-time log and event collection, correlation, and analytics*
- *Case management to easily log, track, prioritize, report on, and close out incidents*
- *Correlate from network data to within the device for ultimate root-cause analytics*
- *Real-time as well as historical analysis*
- *Supports hundreds of pre-classified log types such as firewall, system, authentication, networking logs, etc.*
- *Rich Executive Dashboards, IOC Dashboards, and comprehensive reports for automated and optimized workflows*
- *Super-fast full or partial string search*
- *Seamlessly interoperate with every existing NIKSUN solution*
- *Can be deployed as a standalone product or add-on to NIKSUN appliances*
- *SOAR (Security, Orchestration, Automation , and Response) integration for consolidated intelligence and immediate response*
- *Reduce the mean-time-to-resolution (MTTR) for incidents, thereby reducing operational costs*
- *Flexible and scalable on-demand and scheduled reporting for both real-time operations and strategic decision making*
- *Plug-and-play device with minimal training and absolutely no network downtime*

Challenge

Network analytics for security and performance only takes us as far as identifying the device or node (server, router, etc.) where the problem resides. Looking inside the device requires the use of agents to collect data from within the device or correlation of network analytics with device logs.

Analyzing encrypted tunnels is also a challenge from observation of network data alone. Using logs can help pinpoint applications and/or users responsible for malicious activities.

Compliance requirements also demand that logs be stored for a period of time.

Using logs as another source of information satisfies both compliance requirements as well as pinpointing the root-cause of a problem. Thus, storing logs and events and being able to search on them closes a gap in security or performance incident analytics.

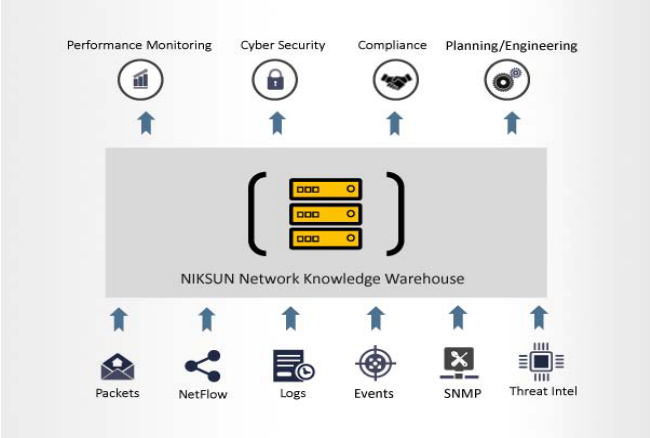
Solution

NIKSUN® LogWave is a next-generation Security Information and Event Management (SIEM) engine that provides real-time analysis of security alerts generated by applications and services. It ingests hundreds of log and event types into the NIKSUN Network Knowledge Warehouse (NKW) for powerful and reliable root-cause analytics while satisfying compliance requirements for log retention.

LogWave records, aggregates, and indexes logs and events and correlates them with network information in the NKW (packets, flows, application data, SNMP, etc.) to detect root-cause of any security or performance incident in record time. LogWave ingests events from various devices for a holistic view of any organization's network. With correlated analysis, incidents can be immediately pinpointed to an application, service, or task inside a device resulting in quicker restoration of business processes and assets. Leveraging logs with other data provides users with powerful and actionable intelligence into application and user characteristics not accessible before.

Strong SSL encryption such as Diffie-Hellman obscures detection and analytics of malicious activity hidden inside encrypted tunnels. The need to identify users being targeted for attack via various application services necessitates the access to metadata not readily available from outside the endpoints of communication. Network data sourced from packets correlated with logs offers insights that provide the full picture of network transactions, by offering visibility into the source of the activity such as applications and users even if the session itself was encrypted. NIKSUN's ability to correlate packets and logs and generate reports combining intelligence from all data types provides an edge over other tools in the market.

LogWave also alerts on issues via statistical, anomaly, and expert analytics. It can simultaneously monitor a virtually unlimited number of servers with various log types at extremely high speeds. It is capable of storing log data for days, months, or even years.



Consolidated Network Intelligence

LogWave is a cost-effective solution for achieving maximum visibility into the network, user behavior, and more by monitoring and analyzing network endpoints. Optionally, it can include a seamlessly integrated Case Management suite to allow users to open, prioritize, investigate, and close out incidents. By leveraging both features in tandem, users can easily tag discovered intelligence and data from the deep forensics capabilities and dashboards of LogWave to any created Case. It interoperates seamlessly with NIKSUN's NetOmni™ Suite and additionally leverages the NIKSUN NKW for a contextual perspective of application performance, service delivery impediments, network integrity, and security breaches.

Flexibility and Scalability

NIKSUN LogWave scales to meet any organization's needs, large or small. LogWave can store log and event data in the order of hundreds of gigabytes all the way up to petabytes. LogWave's scalable technology is able to aggregate, correlate and search up to hundreds of petabytes today. It seamlessly ingests logs and immediately gives actionable information from the generated metadata and correlates that data with any other data in the NIKSUN ecosystem. LogWave is customizable to meet one's distinct requirements. Through NIKSUN NetOmni, multiple LogWave units can be easily accessed in a grid manner providing actionable data and reporting across the entire network, even across physical-cloud hybrid environments.

With the availability of LogWave from NIKSUN, IT and business users are now equipped to correlate events across all their data sources – Packets, Flow, SNMP, Logs, and Events.

Technical Information

» *Log Types Supported - Hundreds pre-classified, including firewall, system, authentication, networking logs, and more. All log types are ingestible.*

» *Form Factors - 1U, 3U, and 4U physical solutions, with public and private cloud solutions available. Compatible with unlimited external storage.*

» *Integration - Authentication - TACACS+, RADIUS, LDAP and Active Directory. All NIKSUN products integrate with NIKSUN NetOmni™ Full Suite for enterprise-wide data aggregation, reporting and visualization.*

Interested in learning more?

For more information, please visit us online at *niksun.com*.

457 North Harrison St. • Princeton • NJ 08540 • USA
t: +1.609.936.9999 • toll free: +1.888.504.3336
f: +1.609.419.4260
info@niksun.com • www.niksun.com