NIKSUN Knowledge Warehouse

A Comprehensive Solution for PCAP Analysis

Features & Benefits

- *Forensics: Advanced analytics with granular forensic analysis, including application reconstructions and object extraction on your existing packet captures (PCAPs)*
- *Inbound and outbound application monitoring with granular application content search*
- *IDS and Anomaly Retrospective Detection Analysis on your existing packet captures (PCAPs)*
- *End-to-end Application and Service performance analysis (Network latency / application response, throughput, etc.) on your existing packet captures (PCAPs)*
- *Measure and analyze per-call CDRs, QoS, and QoE metrics of VoIP applications and services on your existing packet captures (PCAPs)*
- *Compare VoIP media traffic with control traffic for true insight*
- *Detailed Analytics and Alerts for DNS and other protocols such as HTTP, SSL, and more*
- *Intuitive and powerful UI: "Google-like" interface for actionable intelligence; Ingest, correlate and search a wide variety of data for Indicators of Compromise (IoC) or by comprehensive metadata (e.g., IPs, domains, etc.)*

Security Overview Report

Challenge

The threat of a catastrophic cyber-attack that can cripple an organization has becoming increasingly real over the last few years. Insider threats, zero-day exploits, malware, advanced persistent threats (APTs), and other cyber-attacks are now occurring on an unprecedented scale with extraordinary sophistication. Similarly, expectations of service availability and faster response times are of the utmost importance to survive and retain customers in this day and age. Advanced and tactical missions today and in the future require that network data be collected and analyzed both in real-time as well retrospectively / in offline mode.

Solution

NIKSUN® Knowledge Warehouse (NKW) allows data scientists and network analysts around the world to convert offline captured packets (PCAPs) into NIKSUN's award-winning NikOS and NKW architecture. Doing so allows them to conduct deep post-capture forensics as well as Artificial Intelligence (AI) research. NIKSUN is the only security analytics appliance that integrates signature-based IDS functionality with statistical anomaly detection, analytics and deep forensics with full-application reconstruction, end-to-end application and service performance analysis, and packet-level decodes. It is recognized as the industry's best security, forensics, and performance analytics solution to safeguard against increasingly sophisticated cyber-attacks and achieve the highest performing SLAs.

Integrated Anomaly and Signature-based IDS

NKW Security includes an integrated anomaly and signature-based IDS solution for the fast and accurate detection of intrusions and zero-day attacks. The anomaly-based detection utilizes user-defined and threshold-based anomalies.

Application Forensics and Session Reconstruction

The application and session reconstruction feature provides the deepest forensics with hundreds of types of metadata. It monitors all data flowing across the IP network and uses deep packet inspection techniques to accurately recognize, classify and analyze all applications, sessions, and content traversing the network. Metadata is created on all content including email, IM, FTP, HTTP, and DNS.

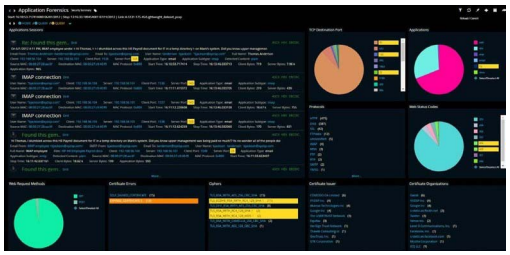
End-to-End QoS and Performance Monitoring

NIKSUN NKW Performance also provides rich QoS and performance metrics for

inbound and outbound traffic, applications, and services. It simultaneously captures, timestamps, and indexes packets to analyze and alert users immediately to service interruptions and infrastructure/application degradation.

Rich VoIP Metrics

NKW NetVoice offers rich VoIP metrics and analytics which eliminates the manual element in troubleshooting by providing all relevant statistical and packet information on a per-call basis (including MOS, jitter, delay, loss, CDR, QoE, etc.). NKW NetVoice minimizes the Mean Time to Discover (MTTD) and Resolve (MTTR) the root-cause of VoIP incidents. Tools, such as the color-coded multi-stage bounce diagrams, provide visual diagnostics of delay experienced in the network.



Application Forensics Report

Technical Information

- *Network Interfaces Supported (Full-duplex, Half-duplex) - 1GigE, 10GigE, or 40GigE*
- *Protocols Supported - TCP, TCP, UDP, SCTP, IPv4, IPv6, fragmented IP, IEEE 802.3 (Ethernet), Ethernet MPLS, VLAN (ISL, IEEE 802.1q and stacked 802.1q), DNS, ICMP, HTTP, HTTPS, SSL/TLS, SMB, MSSQL, Oracle QinQ , Multicast, ISO8583, FIX, GTP, SIP, CDMA2000, RADIUS, Diameter, FTP, Email, Chat, SSH, and many more.*
- *Applications Reconstructed - Several hundred, including voice, video, web, FTP file transfers, chats, email, images, NetBIOS, peer-to-peer, IRC, DNS, wireless (LTE, CDMA2000, IMS), and desktop applications (Microsoft, Adobe, etc.).*
- *Form Factors - A variety of 1U, 2U and 4U+ form factors are available. Internal storage scales to tens of terabytes. Unlimited external storage options are available.*
- *Integration - Authentication - TACACS+, RADIUS, LDAP, Active Directory, and CAC. All NIKSUN products integrate with NIKSUN NetOmni™ Full Suite for enterprise-wide data aggregation, reporting, and visualization.*

Features	NKW Performance	NKW VoIP	NKW Security + Performance	NKW Comprehensive
Performance Metadata generation on Layers 2-7 (Network Latency, Bandwidth, application response, etc.) on existing packet capture files	•	•	•	•
Security Metadata generation on Layers 2-7 (application reconstructions, IOC detection, etc.) on existing packet capture files			•	•
VoIP rich metadata generation on SIP and RTP media protocols (MoS, SEER, Failed calls, etc.) on existing packet capture files		•		•

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