IntelliDefend®

Powerful forensics in a compact, solid state device

Features & Benefits

- *Remote & branch office high-availability, robust forensics ideal for departmental level surveillance*
- *Lightweight, small and portable solution for field personnel*
- *Lossless full packet capture (FPC): known for not dropping packets; chosen by the U.S. Government Department of Defense (DoD) for FPC up to and exceeding 100 Gbps system throughput*
- *Real-time alerts of different IOCs, regulatory and internal company policy violations*
- *Rich Executive Dashboards and comprehensive reports for automated and optimized workflows*
- *Forensics: Advanced analytics for granular forensic analysis, including Application Reconstruction and artifact extraction*
- *Threat Intelligence: Ability to ingest NIKSUN out of the box and third party threat feeds*
- *Integrated Signature & Anomaly based detection with retrospective analysis*
- *Application Recognition: Classify and analyze many applications based on content*
- *Geo IP analytics and alerting: Upload custom GeoIP mappings*
- *Plug-and-play device with web-based intuitive user interface and role-based access control (RBAC)*

Challenge

Targeted cyber attacks across global networks have increased in impact as well as frequency. Web-based cyber threats, distributed denial-of-service (DDoS) attacks, incidents due to malicious code, and information loss due to malicious insiders, are having huge financial consequences on organizations. The loss associated with an attack is directly proportional to the time taken to resolve it. This puts organizations under pressure to quickly and accurately pinpoint the cause of a security breach.

Cyber security analysts need advanced network forensic solutions that can rapidly search through terabytes of data to provide them with the comprehensive visibility to detect, investigate and resolve attacks and breaches.

Solution

NIKSUN IntelliDefend is a full-featured appliance for network security monitoring built on NIKSUN's award-winning NikOS architecture. It is the only security monitoring appliance that integrates signature-based IDS functionality with statistical anomaly detection, analytics and deep forensics with full-application reconstruction and packet level decodes. Recognized as the industry's best security monitoring and forensics appliance to safeguard against increasingly sophisticated cyber attacks.

Users are informed of security breaches and attacks as they occur and can automatically initiate interdiction actions to prevent the malicious traffic from entering the network. Users can quickly answer critical questions such as how a breach occurred, what data was exfiltrated, what was compromised, who was affected, and what corrective measures need to be initiated.

Security Overview

Dynamic Application Recognition and Plug-ins

IntelliDefend further improves modularity and scalability by using the Dynamic Application Recognition (DAR) mechanism and plug- in framework for network traffic recognition and processing.

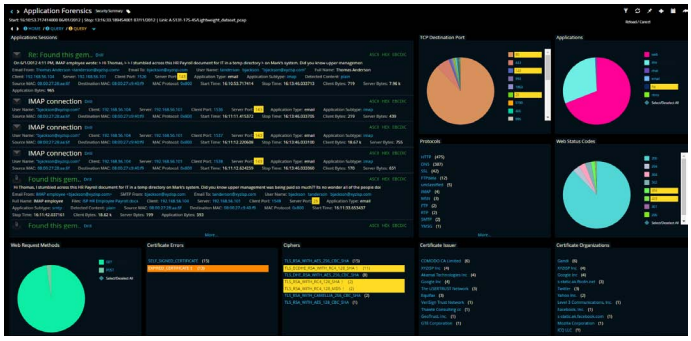
Port-based or TCP-based classification methods are insufficient to accurately identify the different types of traffic. The DAR recognition mechanism uniquely recognizes applications using signatures based on the payload as well as header information, providing the ability to identify all rogue applications and malware.

Integrated Anomaly and Signature-based IDS

NIKSUN NikOS Everest IntelliDefend offers an integrated anomaly and signature-based IDS solution for fast and accurate detection of intrusions and zero-day attacks. The anomaly-based detection utilizes user-defined and threshold-based anomalies. Apart from guarding proactively against new threats, integrated detection capabilities can be used retroactively on already captured traffic to identify existing victims of cyber attacks.

Application Forensics and Session Reconstruction

The application and session reconstruction feature provides the deepest forensics with hundreds of types of metadata. A network security analyst keen on quickly parsing through terabytes of data can utilize the new GUI in NikOS Everest for both fast reconstruction and in-depth forensics. Full reconstruction of DNS protocol exchanges comes standard with the IntelliDefend. This enables users to quickly and easily detect interactions with blacklisted DNS servers, which is often a precursor to sophisticated cyber attacks. It also provides faster tracing of occurrences of DNS spoofing or DNS Denial of Service attacks.



Application Forensics

Technical Information

- *Network Interfaces Supported (Full-duplex, Half-duplex)* - 1GigE (copper)
- *Protocols Supported - 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 - Portable or 1U half-depth, Internal storage to several TB*
- *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.*

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