nPulse Technologies and FireEye

Real-time Threat Detection, Actionable Intelligence, and Rapid Incident Response

Network Forensics for the 10Gig World

OVERVIEW

Capabilities

- Capture and index all network traffic for back-in-time analysis
- Quickly pivot from FireEye's real- time threat alerts to full network data analysis
- Reconstruct kill chain events before and after an alert
- Determine the nature, extent and duration of advanced threats

Benefits

- Dramatically shorten security incident response and resolution times
- Better understand security incidents to isolate root causes and improve future defenses
- Increase reach and value of existing tools without retraining analysts or changing proven workflow

Results

- A seamless integration of today's industry-leading, real-time threat analysis and rapid incident response tools

YOUR CHALLENGE

In today's sophisticated, dynamic and continually evolving threat landscape, security professionals are well aware that the enterprise is continually targeted. Enterprise networks hold enormously valuable, sensitive, proprietary, confidential information, making them irresistible targets to attackers. Well-maintained perimeter defenses are a key part of any security strategy but analyzing persistent threats and incident response for breaches is a necessary addition to any security strategy. Once attempted malware downloads or callbacks are detected, a thorough analysis of what may have been missed, and activity from possibly infected clients, is a priority. Additionally, once an ongoing breach is detected, the challenge is to determine the extent of the damage, isolate the means of entry, and patch it to avoid future repeats. Ultrafast access to historical network data is a necessity for security personnel in reducing mean time-to-resolution, as well as answering the key questions: how long has the breach been present, what data may have already left the network, and how many other hosts may already have been compromised?

OUR SOLUTION

nPulse's Capture Probe eXtreme (CPX) is the industry performance leader in packet capture, historical search, and traffic analysis. It delivers the fastest packet indexing solution at up to 30 million packets per second, enabling users to significantly reduce incident response times even when faced with massive-scale searches. The integration through CPX's Pivot2Pcap API with the FireEye NX & EX platforms provides deeper insight into network traffic and activities through simple drill-down access to captured, indexed and stored connection and packet information on the largest and busiest 10Gbps networks. By allowing FireEye users to quickly locate and decode traffic and sessions before, during, and after a security event, nPulse's CPX provides greater visibility into activity around the event, further enhancing visibility that can be crucial for rapid incident response investigations.

By capturing and indexing full packets reliably at extremely rapid speeds, nPulse's CPX platform provides a powerful complement to FireEye's comprehensive threat prevention capabilities. In addition to receiving precise alerts and correlated threat information from FireEye, analysts can also get a fine-grained view of the specific packets and sessions before, during, and after the attack to confirm what may have triggered a malware download or callback, to respond rapidly and effectively, and to apply this information to enhancing future protective strategies.

FireEye NX Platform

The FireEye NX series is a group of threat prevention platforms that stop Web-based attacks that traditional and next-generation firewalls (NGFW), IPS, AV, and Web gateways miss. The NX protects against zero-day Web exploits and multi-protocol callbacks to keep sensitive data and systems safe. Advanced targeted attacks use the Web as a primary threat vector to compromise key systems, perform reconnaissance on existing defenses, establish long-term control and access to networked systems, and exfiltrate data.

FireEye Key Advantages

- Real-time detection of advanced persistent threats and zero-day attacks
- Detection and blocking of malware discovered in web, email, or out-of-band content
- Detection of malware callback events
- Dynamic threat intelligence sharing

FireEye EX Platform

The FireEye EX series is a group of threat prevention platforms that protects against spear- phishing email attacks that bypass anti-spam and reputation-based technologies. Spear-phishing attacks have soared in popularity with the availability of user-specific information on social networks and other Internet resources. With all of the personal information available online, a criminal can socially engineer almost any user into clicking a URL, or opening an attachment with a zero-day exploit, and the cybercriminal quickly gets control of a privileged system and user accounts.

CPX Key Advantages

- Continuous, lossless packet capture with nanosecond time-stamping at recording speeds up to 20 Gbps
- Real-time indexing of all captured packets using time-stamp and connection attributes
- Export of flow index in NetFlow v5, v9 and IPFIX formats for use with other flow analysis tools
- Ultrafast search and retrieval of target connections and packets using patent-pending indexing architecture
- Web-based, drill-down GUI for search and inspection of packets, connections, and sessions
- Session decoder support for viewing and searching web, email, FTP, DNS, chat, SSL connection details, and file attachments
- Packet payload search using regular expressions (regex)
- Up to 144 TBytes of traffic recording in one appliance, or expandable to petabytes with fiber-attached storage option
- Data storage and export in industry-standard PCAP format
- Pivot2Pcap RESTful API for integration with customer utilities and other monitoring/security appliances

nPulse Technologies CPX Packet Capture & Analysis

CPX is an ultrafast, multipetabyte traffic recording and analysis platform for Security Operations Center (SOC) environments. The high-speed, continuous recording solution provides deep, fully indexed storage of network traffic for direct analysis or use with other security or monitoring applications. CPX delivers an easily searched, multi-level view of network packets, connections and session data.

Even on the busiest networks, CPX captures 100% of the traffic, time stamping every packet with nanosecond resolution, and extracting flow identification parameters. As traffic is streamed to disk, CPX generates packet connection- and time-based indexes that allow rapid search and retrieval of targeted traffic from many terabytes of capture records.

The browser-based drill-down interface allows remote analysis of selected packets and sessions without the need to export entire PCAP files. All packet data is stored, and can be retrieved, in industry-standard PCAP format. In addition, packets, session data, and extracted files are available via the API in industry-standard formats for thorough analysis by external tools.

About nPulse Technologies, Inc.

nPulse Technologies is the performance leader in network forensics. Leading financial institutions, government agencies, telecommunications carriers and other organizations rely on nPulse solutions to enhance security monitoring, shorten incident response times, and increase returns on existing security investments.

For network forensic analysts looking to significantly reduce incidence response time, nPulse solutions enable expeditious reconstruction of the kill chain. Unlike competitive solutions that are unable to operate at 10Gbps sustained and take hours to analyze network traffic, our solutions are designed to perform at 10Gbps full duplex, capturing, inspecting, and exposing indications of compromise within minutes, all at a fraction of the cost.

For more information, visit www.npulsetech.com.