nPULSE TECHNOLOGIES

cyclone

Network Forensics for the 10Gig World

Cyclone Network Forensics Platform

A Costly Attack

Incident responders strive for a one-hour response time from detection to containment of network breaches. Yet, according to a recent study conducted by the Ponemon Institute, the average time to resolve a cyber attack is 32 days, with an average cost incurred during the resolution period of $1,035,769, or $32,469 per day.

A Timely Response

The Cyclone Network Forensics Platform is designed to dramatically slash incident response times. For analysts looking to significantly reduce Mean-Time-To-Resolution (MTTR) of cyber attacks, the Cyclone platform enables reconstruction of kill chains within minutes — not days. Unlike competitive solutions that are unable to operate at 10 Gbps and take hours to retrospectively analyze network traffic, Cyclone is designed to perform at 10 Gbps full duplex, sustained, capturing, inspecting, and exposing potential indicators of compromise expeditiously, all at a fraction of the cost.

A Real-Time Solution

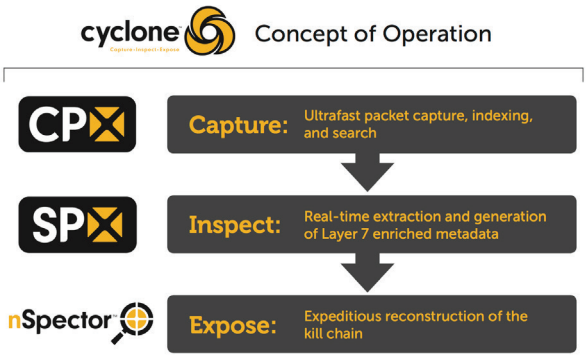
The Cyclone Network Forensics Platform gives incident responders real-time insights by automating significant portions of the IR process using a streaming Big Data framework. This enables security professionals to immediately pivot from overwhelming amounts of data and disparate security alerts to precise, actionable information on malicious activity. With this capability, security professionals are empowered with the necessary visibility to defeat today's advanced persistent threats (APTs).

Expeditiously reconstructing the kill chain

Cyclone Network Forensics Platform

Reconstructing the Kill Chain

The Cyclone Network Forensics Platform is a scalable, distributed, high-performance, Big Data framework for continuously monitoring and processing streams of network traffic. Specifically, Cyclone is designed to capture, extract, and index packets and sessions along with Layer 7 enriched metadata such as IP addresses, DNS records, HTTP header fields, and file hashes at ultrafast speeds.



CAPURE: The Cyclone Capture Probe eXtreme (CPX) captures 100% of the traffic and time stamps every packet with nanosecond resolution while streaming packets to disk. It generates a patent-pending, multi-tiered index for all packets and connections while simultaneously streaming flow records (IPFIX and/or Netflow v9) to the Cyclone FlowScope for additional stream processing.

CPX searches are typically 160 times faster than the rate of capture, delivering results in under a minute that normally take the competition up to a day. Furthermore, the CPX's session analysis capabilities enable full reconstruction of network traffic, as well as file extraction for malware and data loss analysis.

All in all, the scalability and ultrafast performance of the CPX provides for cost-effective packet capture from the fastest data center links down to remote office connections, helping organizations expand visibility to the entire enterprise.

INSPECT: Real-time visibility into application layer is key to providing actionable information for security and incident response analysis. The Cyclone Security Probe eXtreme (SPX) inspects, extracts, and generates Layer 7 enriched metadata from network traffic at wire speeds. It is designed to enhance visibility into network traffic at a deeper level by decoding common protocols like DNS, SSL, FTP, IRC, SMTP, HTTP, as well as identifying embedded URLs, files, and file extraction. Like the CPX, the SPX streams Layer 7 enriched metadata as IPFIX records to FlowScope for additional data mining, storage, and indexing.

EXPOSE: The Cyclone nSpector, built on a purpose-built data storage system and the ElasticSearch engine, is designed to significantly reduce the Mean-Time-To-Resolution (MTTR) of a cyber attack by exposing forensic data in the form of Layer 7 enriched metadata and indicators within minutes — not days.

With nSpector, actionable information is readily available for analysis. There is no waiting for batch processes to complete because everything is streamed in real-time. Your investigation begins immediately by searching across the entire enterprise for clues. Centralized searches allow you to expeditiously locate and reconstruct security events no matter where they occur within your enterprise. User-configurable dashboards allow for different views of network data for analysis. Once threat vectors in the kill chain have been identified, the built-in case management allows you to save sessions of interest including all the associated packets.

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.