GigaStor™ Security Forensics

Your Network Eyewitness

GigaStor is changing the way network and security teams do their jobs and interact. It passively captures and archives all data traversing the network for later analysis and reporting, making it an ideal tool for meeting security forensics and compliance objectives. Now, **you have a network eyewitness** to determine whether the problem relates to the network, security, or application.

The GigaStor combines massive data collection (up to 288 TB) and unique time-based analysis, to allow security and networking teams to view past network events. This **eliminates the need to recreate problems** prior to analysis, rapidly decreasing time to resolution. Archived data plays a crucial role in security investigations, providing a complete view of the incident. Use GigaStor's Expert Analysis and uploaded Snort rules to investigate security breaches and compliance issues.

The Need for Surveillance

Businesses require greater visibility to investigate security and compliance matters. Network surveillance (security monitoring) is key for:

- Monitoring internal and external threats
- Documenting evidence for investigations
- Determining the breach source
- Conducting compliance audits
- Complying with corporate HR and acceptable-use policies

Common GigaStor Uses

GigaStor's line-rate capture and analytics capabilities make it well suited to address a variety of your technical business needs through:

- Network and security forensics
- Comprehensive analysis
- Compliance audits

How GigaStor Security Forensics Can Help

Use GigaStor to investigate and prevent the virtually endless variety of mutating internal and external threats.

- Complements IDS/IPS tools by recording and analyzing network-based threats and security breaches
- Offers contextual view of attacks and other network activities
- Provides documentation for forensic investigations
- Assists with internal and federal compliance practices

Stop Pointing Fingers

A major media corporation uses GigaStor to solve internal conflicts between its network and security teams. The network team often blamed the security team for recurring weekend network slowdowns – the security team insisted it was innocent. Using the GigaStor, the security team was able to "*rewind*" the network to view and analyze weekend data. The team proved they weren't at fault and assisted the network team in diagnosing the problem.

Because "Proactive" Measures Aren't Enough

Proactive tools such as Intrusion Prevention Systems (IPS) are far from fool proof. Because these systems can and will be breached, a passive **"network security camera"** like GigaStor should be added to investigate attacks and help prevent them in the future.

Security Forensics Benefits:

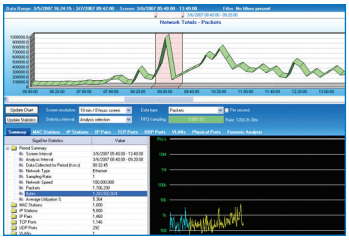
- View security and access violations in context of all network activity
- Validate and provide evidence for compliance and security issues
- Perform Snort-based filtering on terabytes of network traffic to investigate attacks
- Break down the silos of IT department factions (troubleshooting and security) by delivering data to both
- Reconstruct network communications, files, web pages, e-mails, and VoIP calls
- Use regular expressions to locate specific types of data (specific names, social security numbers, and account numbers)

The Scenario

Hackers install remote control utilities and keystroke loggers to gain access to access critical internal systems.

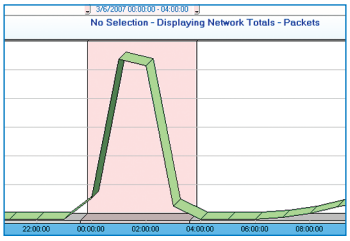
1 Capture

All packet-level data and network activities are recorded by the security forensics solution.



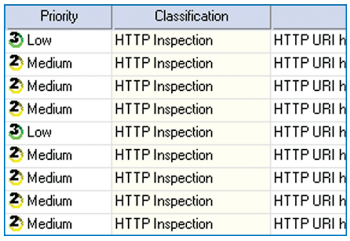
2 Isolate

Network engineer isolates the timeframe surrounding the attacks and tracks network activities.



3 Analyze

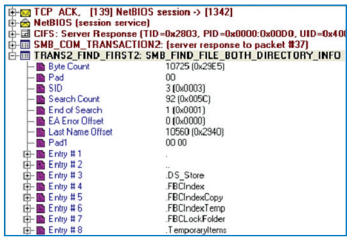
Using the latest intrusion signatures, the selected time frame is analyzed for possible exploits, internal DOS attacks, and key-logging scripts.



Priority	Classification	
Low	HTTP Inspection	HTTP URI h
Medium	HTTP Inspection	HTTP URI h
Medium	HTTP Inspection	HTTP URI h
Medium	HTTP Inspection	HTTP URI h
Low	HTTP Inspection	HTTP URI h
Medium	HTTP Inspection	HTTP URI h
Medium	HTTP Inspection	HTTP URI h
Medium	HTTP Inspection	HTTP URI h
Medium	HTTP Inspection	HTTP URI h

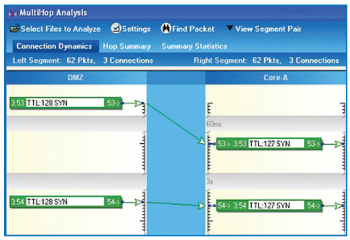
4 Uncover

With the exploit identified, the engineer drills down into the individual frame to isolate suspicious activities such as data transfer under false pretenses.



5 Respond

In addition to documenting specific cases of data theft, the security forensic appliance also identifies the intruder's path across the network, allowing the security staff to identify potentially compromised infrastructure.



About Network Instruments

Network Instruments provides in-depth network intelligence and continuous network availability through innovative analysis solutions. Enterprise network professionals depend on Network Instruments' Observer product line for unparalleled network visibility to efficiently solve network problems and manage deployments. By combining a powerful management console with high-performance analysis appliances, Observer simplifies problem resolution and optimizes network and application performance. The company continues to lead the industry in ROI with its advanced Distributed Network Analysis (NI-DNA™) architecture, which successfully integrates comprehensive analysis functionality across heterogeneous networks through a single monitoring interface. Network Instruments is headquartered in Minneapolis with sales offices worldwide and distributors in over 50 countries. For more information about the company, products, technology, NI-DNA, becoming a partner, and NI University please visit www.networkinstruments.com.

Solution Bundles

Contact a Network Instruments representative or dealer to ask about product bundles that cover all of your network management needs.

NETWORK INSTRUMENTS®

Corporate Headquarters
Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801
www.networkinstruments.com

European Headquarters
Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone + 44 (0) 1959 569880 • fax + 44 (0) 1959 569881
www.networkinstruments.co.uk

GSF-030509-V13-B1