Event-Driven Data Recording

Automated Cyber-Threat Detail Visibility for Rapid Incident Response

Reacting quickly and effectively to a cyber breach is difficult, time-consuming, and expensive. New and pending personally identifiable identification (PII) regulations at the state level, as well as the EU, are significantly tightening the notification period on breaches, including inadvertent access to the systems, in many cases to just a few days.

To fully meet compliance time constraints, organizations need an incident response solution that not only validates that a breach occurred, but also enables them to determine the entire scope of the breach, including identification of the accessed data. To be truly effective, such a solution should be automated in order to minimize time delays in breach detection.

A Complete Security Solution

Leveraging the combined strengths of today's firewalls and CSPi's Myricom® nVoy Series solutions, any organization can deploy an effective, timesaving, and cost-efficient threat defense solution to protect their critical assets. CSPi's Myricom nVoy Series of packet broker and packet recorder solutions can provide the critical evidence needed to verify a breach and view the entire scope of records exposed and/or accessed. This is possible because of their ability to perform targeted data capture and recording, making it possible for security analysts to perform forensics against the entire data set – not just the alert metadata.

In a network architecture, the nVoy Series Packet Broker can tap into the network directly above critical data or storage repositories and ingest the most relevant conversations to and from your most critical assets and

SPECS

Benefits

- **Gain complete insight:** Gain superior visibility into threats involving your critical assets.
- **Focus efforts, act faster:** Reduce time from intrusion to detection of all critical assets to a few hours.
- **Reduce complexity:** Get automated threat-conversation extractions that allow for a complete analysis of any breach.
- **Effective analysis:** Enhance forensic analysis with the ability to pivot around events and use the information to look at what other critical assets an intruder or malicious insider may have attempted to access by triggering new extractions of those conversations.

then send this data to the nVoy Series Packet recorder. The nVoy recorder then captures, filters, timestamps, and indexes all recordings – at full line rate – for on-demand quick file extraction. Such extractions are saved for analysis as well as evidence of a breach for compliance purposes. Because the recording is continuous, an analyst can "go back in time" to review extractions prior to the triggered breach notification and look for all prior conversations by the assets.

While functional, using a manual extraction process takes time and adds the risk of error and missing a critical alert; to address this challenge CSPi's Event Driven Data Recording (EDDR) application automatically ingests alert events from a firewalls or IDS systems. The EDDR application uses the alert event data, including the source and/or target address, along with the recorded timestamps to drive the nVoy Packet Recorder to produce an extraction file of all the conversations between those devices.

The benefit is this process can run 24 x 365 and generate the data required to remain in compliance with minimal human effort.

Enhanced Cyber-Threat Visibility and Data Capture Analysis

The Myricom nVoy Series can be dropped into any existing security infrastructure and dramatically changes the approach to visualizing and verifying threats against critical data.

The Myricom nVoy Series 10Gbit Packet Recorder makes it easy to droplessly record and index 10Gbit network traffic.

By filtering and recording all of the traffic flows involving just your critical data on particular devices or subnets, you reduce the amount of network traffic looked at while maintaining a high-fidelity record of the traffic that you are most interested in. This benefits security teams that may want to analyze the extracts with forensic tools where operating costs are based on the amount of data ingested, like Splunk, as it provides a cost-savings benefit since the scope of the data has been dramatically reduced.

The nVoy solution scales through the use of a packet broker, such as the Myricom nVoy Packet Broker, which can aggregate, filter, and load-balance traffic so that an appropriate number of recorders can be used and effectively utilized.

The nVoy Series also offers a range of security benefits, including the ability to:

- Automatically fetch specific packet flow records triggered by intrusion detection alerts.
- Meet strict data privacy compliance specifications, such as those found in GDPR, MiFID II, PCI DSS, NIST, and state statutes regulating PII.
- Capture, extract, and index specific data conversations through an easy-to-use, web-based interface.
- Leverage third-party tools like Splunk or Wireshark to analyze the extracted data files.

Myricom nVoy Series Packet Recorder Configurations

	nVoy Recorder 10 Gbit	nVoy Recorder 10 Gbit
Form Factor	1U Rackmount	2U Rackmount
Sustained Capture	Up to 14.88 Mpps	
Capture ports	2 x 1/10G SFP/SFP+ but the combined bandwidth to disk is limited to a single, saturated port	
Timestamp Accuracy	± 50 ns	
Packet extraction Filtering	Allows filtering content by IP source address, IP destination address, protocol and or application. It allows for conditional filtering after thresholds or time of day filters have been met.	
Management Port	RJ45 modular connector supporting up to 1 Gbit Ethernet	
Standard Storage Capacity	8 x 1.2 = 9.6TB	24 x 1.2 = 28.8TB
Additional Storage Capacity	Drives larger than 1.2 TB are available. Or add additional drive-only storage expansion boxes.	
Configuration and Management	Web Interface	
Software	10G packet capture and recording license	
Hardware	Single CPU with hardware RAID and Myricom ARC Series 2-port adapter	Dual CPU with hardware RAID and Myricom ARC Series 2-port adapter
Warranty	3 years hardware, 1 year software maintenance	
Order Number	10G-REC-8x1.2	20G-REC-24x1.2

Speed up your cyber-attack incident response. Contact us at myricom.sales@cspi.com

About CSPi

CSPi (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPi Corporate Headquarters
175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPi High Performance Products
800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPi Technology Solutions
800.940.1111
us-ts-sales@cspi.com
us-hpp-sales@cspi.com

www.linkedin.com/company/csp-inc
@ThisIsCSPi
us-hpp-sales@cspi.com
www.cspi.com

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.