Myricom nVoy Series Automated Investigative Response

Intelligent Cyber-Threat Identification for Rapid Response

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

To fully meet compliance time constraints, organizations need an investigative 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 and provide a focus for breach investigation.

An Automated Investigative Response Solution

Security resources receive a staggering number of alert events from their firewalls, SIEMs or other security technologies. Even organizations with large, highly trained security teams are struggling to keep up with the volume. Manually combing through the events to determine which are worth further investigation takes time and adds the risk of error and missing a critical alert.

To address this challenge CSPi's Myricom nVoy Automated Investigative Response (AIR) application automates two critical elements of the incident investigation process. When our nVoy AIR application is paired with our Myricom nVoy packet recorder it assesses all alerts issued by a firewall or IDS/IPS to determine if any are against a user specified list of critical assets (devices, applications or combination). If so, the nVoy AIR

SPECS

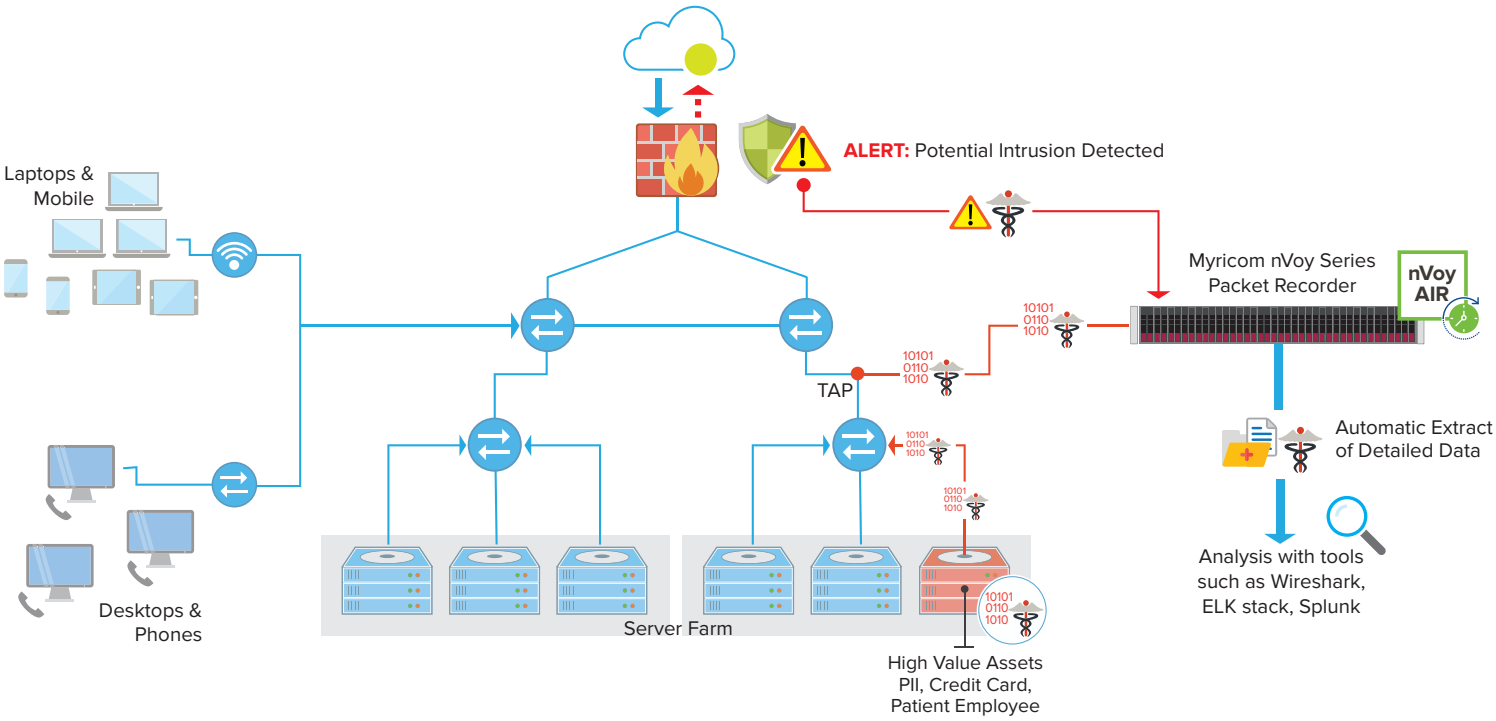
Benefits

- Gain complete insight: Gain superior visibility into breaches involving your critical assets. Know which records were exposed - which weren't.
- Focus efforts, act faster: Reduce time from intrusion - to detection – to response to a few hours.
- More Effective: Get automated threat-conversation extractions and notifications that allow for a focused but complete analysis of any breach.
- Significant ROI: Shorten investigation time to a few hours compared to a few weeks using today's traditional IR techniques.
- Better 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.

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.

By automating these two pieces – the alert identification and extraction of conversations – it eliminates manual intervention and thus drastically reduces the risk of missing an alert, puts resources to better use and most importantly saves crucial time during the investigation.

An additional benefit is that this process can run 24 x 365 and generates the data required to remain in compliance with minimal human effort. The production of an extract file is rare and when it happens it can be used as the trigger point to commence investigative response activities. There is no system to watch – nVoy AIR can notify your analyst team or your managed service provider when an extract is created so that work can immediately commence.



A Comprehensive and Cost-effective Investigative Response Solution

The Myricom nVoy Series can be dropped into any existing security infrastructure by tapping into the network directly above critical databases or storage repositories and dramatically changes the approach to visualizing and verifying breaches of critical data. Leveraging the combined strengths of today's firewalls and nVoy Series solutions, any organization can deploy an effective, timesaving, and cost-efficient threat defense solution to protect their critical assets.

The nVoy recorder captures data provided by the tap, filters the traffic down to just that going to and/or emitted from the critical device/applications and records these conversations, as it does so it timestamps, and indexes all recordings – at full line rate. This allow for quick search and creation of a file containing the extraction of particular data conversation of interest. Such extractions are saved on the recorder for detailed breach analysis, as well as evidence for compliance purposes. Because the recording is continuous, an analyst can "go back in time" to create extractions prior to the triggered breach notification that contain all prior conversations by the "intruder" and all the critical assets. Recordings can also be saved for extended periods on any optional network attached storage (NAS) device and pulled back to the recorder for extractions.

CSPi's Myricom nVoy Series of packet recorder provides and preserves the critical evidence needed to verify a breach and view the entire scope of records exposed and accessed. Security analysts perform forensics against the actual data set – not just the log metadata, which does not provide enough definitive detail as to what happened. The other problem is that logs can be turned off and erased by skilled attackers once they breach a system. That can't happen with a passive data recording system that captures everything.

Grows With Your Infrastructure

The Myricom nVoy solution scales through the use of a packet broker, such as the Myricom nVoy Packet Broker, which can aggregate traffic from many taps, filter the traffic on the broker, and then load-balance traffic so that an appropriate number of recorders can be used to scale and be effectively utilized. The solution installs and sets up with minimal effort with an easy-to-use, web-based interface. With the dramatic reduction in extracted data to analyze it is easy, and cost effective, to leverage third-party tools like Splunk to visualize the output and Wireshark to perform the detailed analysis.

Speed up your cyber-attack Investigative 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

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.

MYRICOM Network Products