Portable Network Forensics Empower Threat Detection and Incident Response

Sera-Brynn is a global "Top 10" cybersecurity audit and advisory firm. Their U.S.-based cybersecurity experts are dedicated to helping clients secure their computing and network environments, and meet applicable (and in some cases mandatory) industry and government regulatory compliance requirements.

With services that span clientele across the globe, Sera-Brynn works closely with internationally recognized accounting firms, insurance companies, legal offices, and law enforcement at all levels to provide the highest level of cyber protection with the least amount of economic impact. Additionally, the company's security professionals offer penetration testing, incident response, post-breach forensics, and security consulting.

The Challenge

Turning Network Data into Actionable Information

Networks are critical for business operations as they process and ensure the transfer of hundreds of terabytes of data per minute. Thus, networks have become crucial sources of data to gather indicators of compromise and gain visibility into an IT environment.

Monitoring and understanding network data for cybersecurity purposes has traditionally been difficult. Manual collection and analysis of network data to effectively detect breaches is not efficient—nor is it feasible. While open-source tools are available to collect and analyze network data, capturing and processing traffic with these tools is complex and requires a great deal of experience.

For Sera-Brynn, the inability to use network data efficiently as part of cybersecurity investigations was a major challenge. When it comes to breaches, time is of the essence. Every minute a hacker operates on a network, the greater the potential losses for the breached company. Sera-Brynn required a traffic analytics and network forensics solution that could speed up analysis, deliver results quickly, provide intuitive features, and could be set up easily in the field.

The Solution

Mobile, User-Friendly Network Investigations with Network Monitor

To solve these challenges, Sera-Brynn turned to LogRhythm Network Monitor—a network forensics and traffic analytics solution. Network Monitor provides full packet capture and deep network visibility for threat detection and incident response in one easy-to-use package.

Sera-Brynn's consultants have seen immediate results from Network Monitor. The tool has given analysts the ability to see broadly and deeply into their clients' networks, allowing them to quickly understand and triage compromised environments.

SERABRYNN®
CYBER RISK MANAGEMENT

Organization
Sera-Brynn

Industry
Cybersecurity risk management

Deployment Size
Dozens of portable Network Monitor devices in support of vulnerability assessments and incident response.

Key Impacts

- Full visibility into unknown environments
- Detection of secondary breaches
- Portable, non-intrusive network forensics and traffic analytics

In one case, Sera-Brynn used Network Monitor to mitigate a cybersecurity attack against a major defense contractor. Sera-Brynn was called in to investigate after law enforcement detected the breach, which had already existed for about nine months.

"Within a period of three to four days, we were able to identify the who, the what, and the where," said Darek Dabbs, chief information officer (CIO) at Sera-Brynn. By allowing analysts to analyze network data across multiple subnets and physical sites on the client's network, Network Monitor facilitated rapid investigation of the breach, which had been executed by state-sponsored expert attackers skilled at hiding their tracks.

This increased visibility, combined with the intuitive interface and search capabilities, has drastically reduced the time required to investigate breaches. "The GUI-driven product interface, and the Elasticsearch-powered query capabilities just completely changed the game for us in terms of the speed of investigations," according to Dabbs.

The mobility of Network Monitor was a great help to the Sera-Brynn team. By running Network Monitor on portable Intel NUC mini computers, Sera-Brynn's consultants can bring the solution wherever they need to go as part of their incident response "go bag." They can then deploy it quickly across all choke points of a client's network to rapidly begin capturing network data—all without burdening the client's existing information technology stack.

Network Monitor also provides Sera-Brynn with stealthy data collection techniques. Because the product collects network data passively, attackers are not able to detect when and where it is deployed. "We can put Network Monitor online for a small amount of time, and the attackers will not know we are there, listening and identifying exactly what they are doing," Dabbs said. This prevents attackers from "cleaning up shop and leaving" before Sera-Brynn's analysts complete their full investigation, identify the source and scope of the intrusion, and remediate all pieces of the cyber attack.

Above and Beyond

Detecting Carefully Hidden Attacks

In many cases, Dabbs said, Network Monitor helps Sera-Brynn detect secondary compromises that the client did not previously know about. As an example, Dabbs cited a case in which Sera-Brynn was hired by a real estate and property management company after attackers compromised its online reservation system, creating a critical threat to business operations.

With the assistance from Network Monitor, consultants were able not only to recover the reservation data and mitigate business disruption, but they also discovered other illicit activity on the client's network. This included the detection of the Zeus malware strain—exposed to the network through the unsanctioned usage of BitTorrent file-sharing clients and Tor software. Remediation was possible by rapid detection.

> "There is no question LogRhythm's Network Monitor helps Sera-Brynn quickly respond to cyber incidents. It enables us to detect lateral movement, command-and-control activity and other tell-tale actions of cyber adversaries with speed and precision so we can eliminate the threat quickly and mitigate risk for our clients."
>
> –Darek Dabbs, chief information officer (CIO), Sera-Brynn