Case study: IBM QRadar boosts network forensics

Industry pain points

The average time to identify a malicious attack is 191 days. The corresponding average time to contain an attack is 66 days*. These stats clearly underpin the importance of fast and conclusive threat detection; an activity that demands total traffic visibility at all times. But as most security solutions are designed to spot attacks as they occur in real time, it is often impossible to retrieve the needed evidence – especially if the attack took place months, even years ago. The outcome, as many companies are painfully aware, can be devastating.

In addressing this issue, IBM has created the QRadar SIEM – a state-of-the-art security platform that helps companies to detect anomalies and uncover advanced threats.

Client challenge

When developing the QRadar SIEM, IBM needed to ensure that the platform would seize and store all network data, providing the end user with uncompromised, high-fidelity evidence in the event of an attack. To achieve this, IBM was searching for an industry collaborator to guarantee 1) that absolutely all data was captured in real time and 2) that selected data could be promptly retrieved for incident forensics in the event of a breach.

IBM needed a partner with a strong track-record, a profound understanding of the industry, and undisputed, best-of-breed technology. Napatech was a natural choice, and the only candidate able to meet all requirements.

> *“Working with Napatech, we don’t lose any sleep. With the excellent integrity of their engineering team and technology, we have absolute confidence in their ability to deliver a world class product.”*
>
> Dr. Russell Couturier, CTO Forensics
> IBM Security Division

Challenge

IBM needed to ensure that their QRadar SIEM platform would seize and retrieve 100% of network data, providing the end user with high-fidelity evidence in the event of a cyberbreach.

Solution

Napatech was selected as a strategic partner, bringing the needed best-of-breed technology. This ensured
1) that absolutely all data was captured in real time and
2) that selected data could be promptly retrieved for incident forensics in the event of a breach.

Benefits

- Guaranteed availability of all evidence
- Ultra-fast data extraction
- Exceptional retention time
- Holistic and intelligent traffic insights

---

* Ponemon Institute

Our solution

IBM was already deploying Napatech technology to accelerate their analytics appliance, which ensured that 100% of the network data was captured in real time. To guarantee that the full network history would also be available on demand, the capture-to-disk technology from Napatech was integrated. This ensured that all packets would be recorded with nanosecond accuracy while also allowing quick and easy data extraction. This would enable the QRadar SIEM to promptly reconstruct the complete picture of a given incident; not just provide a semi-accurate outline.

Benefits

With this solution in place, IBM could deliver a leading-edge security platform with an exceptional level of data integrity – providing end users with assurance and peace of mind that all data would be available at their fingertips whenever needed. Key benefits included:

- Zero packet loss – guaranteed availability of all evidence
- Ultra-fast extraction of critical information
- Holistic and intelligent traffic insights

Added benefits

To optimize system performance and ensure seamless integration across the platform, a number of bespoke enhancements were developed, including:

2x performance improvement

By physically dividing the traffic and transmitting the flows directly to the right CPU cores, a 2x performance improvement was achieved. This facilitated the heavy data analysis required for a forensic investigation.

Unique session ID

A unique session ID was engineered as a mechanism to adjoin all information from the multiple SIEM components, providing an intelligent link between the network packets and the reconstructed information. By associating every packet from a given communication session with a unique ID, specific packets could be instantly retrieved.

Increased retention

By assembling multiple capture-to-disk appliances in one network, we successfully increased the retention time without impacting the search performance. This extended the time window for forensic investigation – while also affording end users a fully scalable storage solution.

Napatech

Napatech helps companies to reimagine their business, by bringing hyper-scale computing benefits to IT organizations of every size.

We enhance open and standard virtualized servers to boost innovation and release valuable computing resources that improve services and increase revenue.

Our Reconfigurable Computing Platform™ is based on a broad set of FPGA software for leading IT compute, network and security applications that are supported on a wide array of FPGA hardware designs.

Find out more at:
www.napatech.com

Find more case studies at:
www.napatech.com/resources/case-studies

EUROPE, MIDDLE EAST AND AFRICA
Napatech A/S
Copenhagen, Denmark

Tel. +45 4596 1500
info@napatech.com
www.napatech.com

NORTH AMERICA
Napatech inc.
Boston, Massachusetts
Los Altos, California
Washington D.C.

Tel. +1 888 318 8288

info@napatech.com
www.napatech.com

APAC
Napatech China/South Asia
Taipei City, Taiwan
Tel. +886 2 28164533 Ext. 319

Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374

ntapacsales@napatech.com
www.napatech.com