CASE STUDY:

Healthcare System Gains Security Intelligence & Network Traffic Visibility with IBM QRadar SIEM

West Tennessee Healthcare is trusted with the health and wellbeing of more than half a million people living across 9,000 square miles, covering 19 counties in West Tennessee and southeast Missouri. It's a trust built over more than 70 years by the thousands of compassionate physicians, nurses, and caregivers working in the 90 locations that make up West Tennessee Healthcare.

THE BUSINESS CHALLENGE

Healthcare providers are being specifically target for ransomware attacks. As a major healthcare system serving a wide area, West Tennessee Healthcare needed to enhance their security program to stay in front of the threat. As the result of a security controls review, Mainline identified that West Tennessee lacked visibility into end user activity and network traffic and was in need of a security intelligence platform to monitor and investigate security events.

The healthcare system also had a small staff with a shortage of security expertise. West Tennessee had considered other security solutions, such as Splunk, but found them too expensive and complicated.

Identifying, assessing, and managing risks were priorities for West Tennessee. However, with a limited budget and resources, the healthcare system's key considerations in adopting a solution included cost and reliable performance.

Clayton Phillips, System Vice President & Chief Information Officer at West Tennessee Healthcare, explained that "Being charged with the responsibility of ensuring the confidentiality, integrity, and availability of patient data, coupled with the ever-increasing front-page news stories of healthcare organizations being attacked, I quickly concluded that 'I need to know what I don't know.'"

THE SOLUTION

IBM QRadar

With IBM QRadar, organizations gain a robust security information and event management (SIEM) solution. QRadar is easy to use and compatible with existing security solutions, smoothly integrating into the current environment. In addition to SIEM functionality, QRadar also provides user behavior analytics (UEBA), as well as integration with vulnerability platforms to prioritize risk-based investigations or threat hunting efforts.

QRadar exceeded West Tennessee's requirements, providing capabilities that otherwise would have overrun their budget. The analysts now have full visibility of the enterprise via a central dashboard.

Security Assessments

Mainline provided a broad range of security assessments, including a vulnerability assessment, HIPAA compliance assessment, and a controls review. These assessments identified gaps in the client's security program, highlighting the priorities for the West Tennessee and Mainline architect teams.

Company:	West Tennessee Healthcare
Customer:	Healthcare Provider
Industry:	Healthcare

THE BUSINESS CHALLENGE

- Lack of security intelligence platform
- Need for a security program (SIEM) and expertise
- Absence of incident logging capabilities
- Need to reinforce HIPAA compliance
- Lack of visibility into end user activity & network traffic

THE SOLUTION

- IBM QRadar SIEM
- Security Controls Review
- Vulnerability Assessment
- Integration Services

THE RESULT

- Power to identify risks and threats
- Able to recover from outages in hours instead of weeks
- Ease of use
- Compatibility with other security solutions
- 90% out-of-the-box functionality
- Cost-efficiency
- Central dashboard

Matthew Likes, CISSP and Security Architect at Mainline, noted that "West Tennessee liked working with Mainline because a lot of organizations need to rotate between different providers. With Mainline, they could provide different vendors to give different perspectives from assessments."

Implementation and Support

Ongoing integration services from Mainline saves the client time and money. Maintaining any SIEM is by no means an easy chore. But by partnering with Mainline to maintain the solution West Tennessee receives support for QRadar, including refreshes, and on-the-job training for their analysts.

THE RESULT

With QRadar, West Tennessee Healthcare was able to build a security program using a single platform. The healthcare provider was excited to find that the use cases it needed were available straight out of the box reducing the need for custom searches. West Tennessee even discovered new use cases it hadn't considered. Now, West Tennessee can identify threats and risks using modern controls. West Tennessee gained full visibility, even seeing devices on the network they didn't know existed.

Phillips stated, "First, QRadar has provided value to our business in the area of compliance. Today's network traffic is generated from routers, switches, desktops, servers, medical devices, and IoT. Logs from these devices are key to demonstrating compliance in times of audits. QRadar has provided us with 'one-stop shopping' for log ingesting, massaging, and providing an automatic alert for compliance violations where before these were manual processes."

Phillips went on to say: "Secondly, the elimination of manual processes has saved time and allowed us to shift resources to focus on other mission-essential activities."

Mainline has a long-standing relationship with West Tennessee, having worked with the organization since 2001, supplying them with technology solutions that have lasted over the years. Phillips summed up the relationship by saying, "I am extremely satisfied with the strategic partnership that has been established with Mainline, which has been in existence for over 10 years. Mainline is a valuable asset that is instrumental in planning, implementing, and delivering ongoing support for our organization."

"Mainline partnered with our newly developed security team and provided superior subject matter experts not only to implement but also to bring the team up to speed to manage with confidence day-to-day operations. Without reservation, I would recommend Mainline as a partner that will provide exceptional services beyond the purchase order," Phillips explained.

West Tennessee was able to establish a security program and get more value out of QRadar. Likes added, "Their relationship with the Mainline security team has matured and grown tighter since the implementation of the QRadar platform."

Phillips' staff works closely with the Mainline engineering team providing them with new ways to view network data and how to leverage the data as a supplement to threat intelligence. Now, West Tennessee can review network health stats and the flow of network traffic, as well as drill into specifics at the application layer.

As West Tennessee expands, Mainline continues to work with the organization to further develop and mature their security program through additional technology and services offerings.

> ***"Mainline partnered with our newly developed security team and provided superior subject matter experts not only to implement but also to bring the team up to speed to manage day-to-day operations with confidence. Without reservation, I would recommend Mainline as a partner that will provide exceptional services beyond the purchase order."***
>
> \- Clayton Phillips
> System Vice President & Chief Information Officer
> West Tennessee Healthcare

For more information, call your Mainline account representative or call Mainline directly at 866.490.MAIN(6246).