Main Line Health Customer Spotlight

Our company relies on the SAFE platform to assess and prioritize risk by leveraging advanced analytics and real-time data. The platform empowers us to make more informed decisions and mitigate vulnerabilities effectively. It's a game-changer for maintaining operational resilience and safeguarding our business continuity.

Chris Wolfe

Sys. Dir. IT GRC, Main Line Health

Main Line Health®

Healthcare

Data Ingestion

CROWDSTRIKE | Qualys | Microsoft Defender | ARMIS

Use Case

FIRST PARTY

Positive Business Outcomes

Integrating OT devices into a cyber risk management program brings significant business advantages. It enhances visibility across critical infrastructure, enabling organizations to identify and mitigate vulnerabilities in real time, which improves operational continuity and reduces downtime. By securing OT devices, businesses can protect vital industrial processes from cyber threats, preventing costly disruptions or safety incidents. This proactive approach also helps Mainline Health comply with regulatory requirements, safeguarding their reputation and avoiding potential fines. Ultimately, incorporating OT devices into cyber risk management strengthens overall resilience and supports long-term business growth.

Before Safe

Failure to understand the risk on critical OT devices at a hospital can lead to significant vulnerabilities, resulting in potential system failures or disruptions in patient care. This lack of visibility increases the likelihood of cyberattacks that can compromise patient safety and disrupt essential medical services. Unidentified risks can also lead to non-compliance with healthcare regulations, potentially incurring fines and damaging the hospital's reputation. Additionally, response times to incidents are delayed without a clear risk profile, hindering swift action to mitigate threats and protect patient data.

After Safe

Knowing the risk on critical OT devices at a hospital enables proactive mitigation, ensuring uninterrupted operation of vital medical equipment and patient care. This understanding enhances the hospital's overall security posture, reducing the likelihood of cyberattacks and system failures. It also ensures compliance with healthcare regulations, fostering trust with patients, regulators, and stakeholders. Additionally, clear risk awareness supports better allocation of resources and swift incident response, minimizing potential damage and maintaining patient safety.