

Gesundheitswesen

Umfassendes Risiko- management für mehr IoT- und Medizingerätesicherheit

Universitätsklinikum Ulm



Moderne medizinische Infrastruktur

Das Universitätsklinikum Ulm hat sich in 41 Jahren einen festen Platz in der universitären Krankenversorgung, Forschung und Lehre erarbeitet. Mit 29 Kliniken und 16 Instituten zählt es zu den führenden medizinischen Einrichtungen in Baden-Württemberg. Rund 6.000 Mitarbeitende an vier Standorten nutzen moderne IoT-, OT- und Medizingeräte, um neue Maßstäbe in der Patientenversorgung zu setzen. Die fortschreitende Digitalisierung bringt jedoch auch Herausforderungen mit sich: Die vernetzten IoT-, OT- und Medizingeräte mussten besser geschützt und in die übergreifende IT-Sicherheitsstrategie des Klinikums eingebettet werden.

Das Ziel war es, eine standortübergreifende Plattform zur Absicherung dieser Geräte zu etablieren und sie in ein bestehendes Security Operations Center (SOC) zu integrieren.

Starkes Teamplay für mehr Sicherheit

Das Universitätsklinikum Ulm setzte klare Prioritäten: Transparenz im Netzwerk erhöhen, Schwachstellen effizient managen und ein durchdachtes Risikomanagement etablieren. Die Asimily-Plattform bildet das Herzstück dieser Strategie. Speziell auf die Anforderungen von IoT-, OT- und Medizingeräten zugeschnitten, analysiert sie detailliert das Geräteverhalten, erkennt Schwachstellen und identifiziert frühzeitig Anomalien.

In enger Zusammenarbeit mit Axians wurde die Plattform nahtlos in die

bestehende Netzwerkinfrastruktur eingebunden. Während Axians für die Konzeption, Implementierung und den laufenden Betrieb der Infrastruktur verantwortlich ist, sorgt Asimily mit Schulungen, Updates und kontinuierlichen Optimierungen für den technischen Support.

Diese starke Partnerschaft ermöglicht eine zukunftssichere, maßgeschneiderte Sicherheitslösung, die sowohl IT- als auch OT-Bereiche optimal einbindet.

Aufgabe/Ziel


- ▶ Absicherung von IoT- und Medizingeräten
- ▶ Aufbau eines zuverlässigen Schwachstellenmanagements
- ▶ Transparente Netzwerkübersicht für Sicherheitsentscheidungen

Lösung

- ▶ Einführung einer leistungsfähigen IoT-Sicherheitsplattform
- ▶ Lokale Datenverarbeitung durch On-Premise-Betrieb
- ▶ Anpassung und Integration in bestehende Netzwerkinfrastruktur

Nutzen

- ▶ Deutlich reduzierte Angriffsflächen und erhöhte Sicherheit
- ▶ Umfassende Transparenz und priorisierte Handlungsempfehlungen
- ▶ Effiziente Ressourcen- und Risikosteuerung



Hohe Datenschutzanforderungen

Um den strengen Datenschutzstandards gerecht zu werden, betreibt das Klinikum die Lösung vollständig On-Premise. So bleiben alle sensiblen Daten sicher innerhalb der eigenen Netzwerke. Asimily ist aktuell der einzige Anbieter, der eine solche interne Umsetzung in vollem Umfang ermöglicht.

Datenschutz ist von Anfang an in die Plattform integriert und sichert so höchste Compliance-Standards. Eine weitere Herausforderung war die komplexe Netzwerkconfiguration, die die Identifikation der verschiedenen Gerätegattungen – von IoMT-/ IoT- bis hin zu OT-Systemen – erschwerte.

Asimily entwickelte hierzu eine spezielle Ad-hoc-Integration in Netflow, um die erforderlichen Informationen direkt aus dem Datenverkehr zu extrahieren. Diese Flexibilität erwies sich als entscheidend für den Projekterfolg.

Klare Prioritäten, gezielte Lösungen

Die Asimily-Plattform geht weit über klassische Schwachstellenanalysen hinaus. Sie zeigt nicht nur Sicherheitslücken auf, sondern bewertet ihre konkrete Relevanz für den klinischen Betrieb.

Damit lassen sich individuelle Zusammenhänge erkennen, Risiken präzise priorisieren und Maßnahmen mit minimalem Ressourceneinsatz umsetzen. Dabei werden IoT-, OT- und Medizingeräte ganzheitlich betrachtet, um ein umfassendes Sicherheitsniveau im gesamten Kliniknetzwerk sicherzustellen. Diese klare Priorisierung bietet genau die Orientierung, die das Klinikum benötigt, um den Aufwand für Sicherheitsmaßnahmen zu reduzieren und Risiken schnell zu minimieren. Gleichzeitig fließen spezifische Anforderungen und Rückmeldungen direkt in die Weiterentwicklung der Lösung ein.

So entsteht eine Partnerschaft, die nicht nur aktuelle Sicherheitsherausforderungen adressiert, sondern auch langfristig optimal an die Bedürfnisse des Klinikums angepasst bleibt.

Für eine sichere Zukunft gerüstet

Dank der engen Zusammenarbeit von Axians und Asimily konnte die Netzwerksicherheit des Universitätsklinikums Ulm deutlich verbessert werden. Die maßgeschneiderte Plattform bietet umfassende Transparenz, indem sie das Verhalten von IoT-, OT- und Medizingeräten kontinuierlich überwacht und Anomalien frühzeitig erkennt.

Innerhalb von nur acht Wochen wurde die Lösung in den Produktivbetrieb überführt und ist seit Herbst 2023 erfolgreich im Einsatz.

Mit der Sicherheitsmaßnahmen kontinuierlich voran – und stellt sicher, dass IoT-, OT- und Medizingeräte gleichermaßen geschützt und nachhaltig sicher in die klinische IT-Infrastruktur integriert sind.