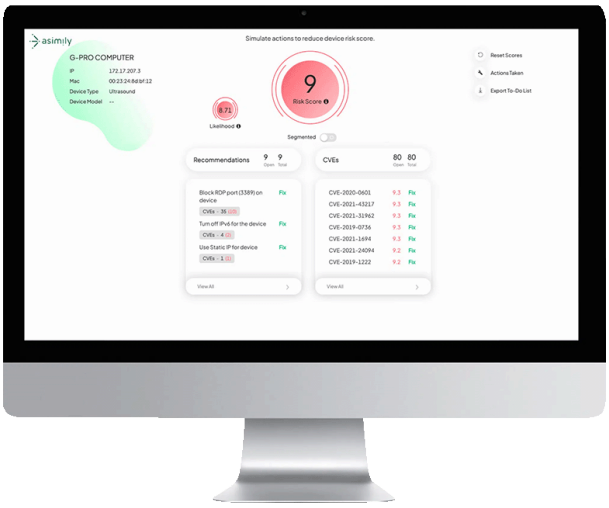
Sicherheit für IoMT und IoT

Plattform für Sicherheit von IoMT- und IoT-Geräten

Krankenhäuser mit vernetzten medizinischen Geräten (IoMT), aber auch andere stark von IoT geprägte Umgebungen wie Fertigung und Transportwesen haben komplexe Anforderungen ans Risikomanagement. Solche Organisationen müssen wissen, welche Geräte kritisch sind und welche nicht, um unnötigen Aufwand bei der Behebung von Risiken zu vermeiden. Im Fall, dass es Schwachstellen gibt, müssen sie in der Lage sein, Probleme möglichst rasch zu erkennen und zu beheben. Die Basis dafür ist eine umfassende Visibilität bis ins Detail jedes einzelnen Geräts.

Umfassende Cybersicherheitsmanagement-Plattform

Mit seiner Insight Platform liefert der US-Hersteller Asimily das perfekte Werkzeug für das Cybersicherheitsmanagement für IoT und medizinische Geräte. Die Plattform liefert kontinuierlich datengesteuerte Erkenntnisse und umsetzbare Empfehlungen zum Schutz von Assets und zur Reaktion auf Schwachstellen und Anomalien. Sie nutzt dazu Healthcare-spezifische Datenquellen wie MDS2-Angaben und SBOMs der Hersteller. Asimily unterstützt so die Risikominderung und die Reaktion auf Vorfälle und hilft bei der Sicherstellung der Geräteverfügbarkeit.



Asimily mit Hauptsitz im kalifornischen Sunnyvale wurde 2017 gegründet und hat sich seither als führender Anbieter für IoT/IoMT-Sicherheit für Healthcare, produzierende Industrie und öffentliche Hand etabliert. Asimily beschäftigt rund 100 Mitarbeitende und gilt als eines der am schnellsten wachsenden IoT-Sicherheitsunternehmen.

Asimily: Die Highlights

- Umfassende Plattform für IoT/IoMT-Cybersicherheitsmanagement
- Unterstützt Bestandsaufnahme, Risikominderung, Reaktion auf Vorfälle und Geräteverfügbarkeit
- Identifiziert und priorisiert das Risiko jedes Geräts anhand spezifischer Datenquellen und Gerätekonfiguration
- Bietet bei Schwachstellen automatisierte Behebung via «Fix»-Button
- Arbeitet mit Schwachstellenscannern wie Tenable und NAC-Systemen wie Palo Alto und Fortinet zusammen
- Als On-Premises-Lösung oder via Cloud einsetzbar
- Agentenlos, das heisst, es ist keine Software-Installation auf den Geräten erforderlich

Asimily: Maximale Sicherheit für IoMT und IoT

Die klinisch validierte Asimily Insight Platform kombiniert eine genaue Bestandesaufnahme aller IoMT- und IoT-Geräte durch sichere Erfassung von Geräte- und Aktivitätsdaten vor Ort mit effizientem Schwachstellenmanagement samt gerätespezifischer Priorisierung der Risiken und Empfehlungen zur Behebung. Asimily unterstützt zudem die agile Reaktion auf Vorfälle mithilfe kontinuierlicher, verhaltensbasierter Überprüfung auf Richtlinienverstösse.

Der Einsatz vernetzter medizinischer Geräte, auch IoMT-Geräte genannt (Internet of Medical Things), sowie die Nutzung von IoT-Geräten ganz allgemein birgt Risiken, die schwer zu messen und zu beheben sind – unter anderem deswegen, weil die Geräte oft gar nicht gepatcht werden können, die Hersteller Aktualisierungen nur selten liefern und das Risiko für ein bestimmtes Gerät kritisch oder eher unbedeutend sein kann. In vielen Organisationen fehlt zudem der Überblick über die Geräte.
Gängige Vulnerability-Management-Lösungen helfen dabei nur bedingt: Sie kennen sich mit den spezifischen Protokollen und Risiken im medizinischen und industriellen Bereich nicht aus und beschränken sich teils auf die blosse Identifizierung von Schwachstellen, ohne sofort nutzbare Empfehlungen zur Behebung zu liefern oder gar Sicherheitslecks auf Knopfdruck zu schliessen oder zu umgehen.
Die Insight Platform von Asimily sammelt alle verfügbaren Geräteinformationen in Echtzeit und präsentiert die Erkenntnisse auf einem übersichtlichen Dashboard. Dabei werden entdeckte Schwachstellen anhand medizin- respektive industrierelevanter Kriterien priorisiert. Im Hintergrund nutzt Asimily dafür spezifische Informationen wie etwa Angaben aus den MDS2-Formularen der Gerätehersteller und berücksichtigt die Art des Geräts. So stellen Geräte, die mit geschützten Gesundheitsinformationen umgehen, ein bedeutend grösseres Risiko dar als andere. Die von Vulnerability-Management-Lösungen generell beigezogene CVSS-Bewertung von Schwachstellen berücksichtigt solche Faktoren nicht. Asimily hingegen verfügt über die grösste Sammlung an MDS2-Herstellerinformationen und deckt damit weit mehr als 1000 Geräte ab.

Zur Problembehebung und Risikominderung arbeitet Asimily nach einem Vorgehen in drei Schritten:

- Falls es machbar und wirtschaftlich ist, eine Schwachstelle zu patchen → Patches einspielen
- Falls der Angriffsvektor sich entschärfen lässt → Entschärfung anwenden
- Falls nichts davon zum Ziel führt → segmentieren/mikrosegmentieren

Da Asimily Probleme mit hoher Wahrscheinlichkeit und hoher Auswirkung priorisiert, reduziert sich der Aufwand für die Behebung deutlich. Die Praxis zeigt, dass mit Asimily eine Reduktion des manuellen Aufwands für Vulnerability-Management-Analysten um bis zu 90 Prozent möglich ist.

BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 (0)56 437 60 60 / sales@boll.ch / www.boll.ch
BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 (0)21 533 01 60 / vente@boll.ch
BOLL Europe GmbH . Ringstrasse 3 / D-89081 Ulm / Telefon +49 (0)731 85 07 48 23 / info@boll-europe.com / www.boll-europe.com
BOLL Europe GmbH . Wienerbergstrasse 3–5 / A-1100 Wien / Telefon +43 (0)664 46 48 580 / info@boll-europe.at / www.boll-europe.at

BOLL