Stand der IT-Sicherheit in deutschen Krankenhäusern

Sicherheit vernetzte Medizintechnik - Herausforderungen

Organisation & Verantwortlichkeit

IT oder Medizintechnik

Prozesse für Sicherheitsvorfälle und Schwachstellenmanagement

Vorgaben und Richtlinien durch Geschäftsführung

Fehlende Visibilität

Mehrzahl der Krankenhäuser haben kein oder nur unvollständiges Asset Inventory ihrer Medizingeräte

Unkenntnis der Kommunikationsbeziehungen von Medizingeräten

Kein Security-by-design

Veraltete Betriebssysteme

Fehlende Hersteller-Patches

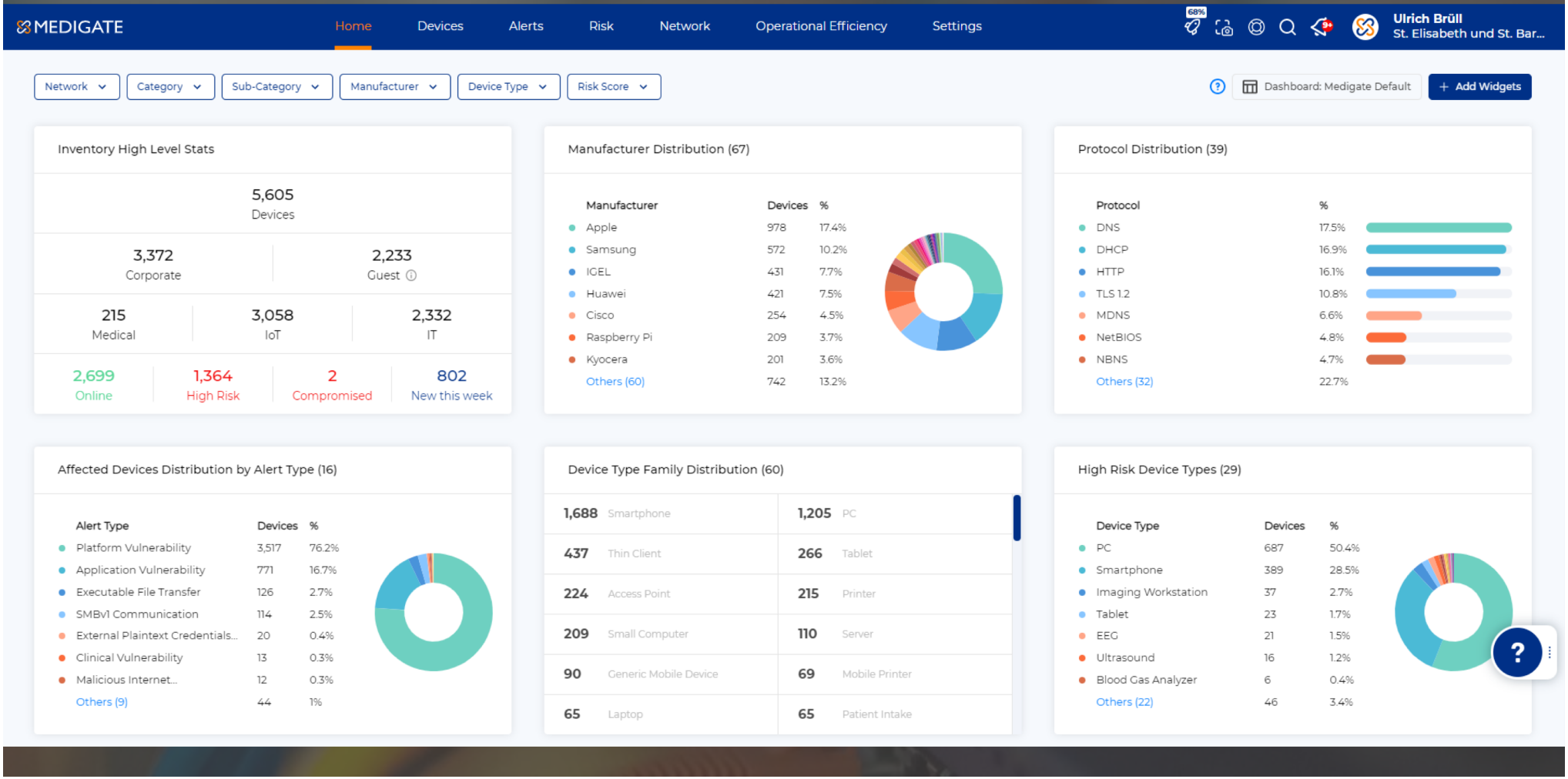
Träge Softwarepflegezyklen

Keine Endpoint Security

Netzwerkbasierte Sicherheit erforderlich


Umsetzung Netzwerksicherheit
Inventarisierung von IT, MedTech und IoT
Risikoklassifizierung & Zuordnung Sicherheitszonen & Ausfallkonzept
Regelwerk interne Firewall
Integration Netzwerk Zugangs-kontrolle
Lfd. Betrieb & Gerätemanagement
Unterstützt von
MEDIGATE

Dashboard


MEDIGATE
Home
Devices
Alerts
Risk
Network
Operational Efficiency
Settings
68%
9+
Ulrich Brüll
St. Elisabeth und St. Bar...
Network
Category
Sub-Category
Manufacturer
Device Type
Risk Score
Dashboard: Medigate Default
Add Widgets
Inventory High Level Stats
5,605
Devices
3,372
Corporate
2,233
Guest
215
Medical
3,058
IoT
2,332
IT
2,699
Online
1,364
High Risk
2
Compromised
802
New this week
Manufacturer Distribution (67)
Manufacturer Devices %
Apple 978 17.4%
Samsung 572 10.2%
IGEL 431 7.7%
Huawei 421 7.5%
Cisco 254 4.5%
Raspberry Pi 209 3.7%
Kyocera 201 3.6%
Others (60) 742 13.2%
Protocol Distribution (39)
Protocol %
DNS 17.5%
DHCP 16.9%
HTTP 16.1%
TLS 1.2 10.8%
MDNS 6.6%
NetBIOS 4.8%
NBNS 4.7%
Others (32) 22.7%
Affected Devices Distribution by Alert Type (16)
Alert Type Devices %
Platform Vulnerability 3,517 76.2%
Application Vulnerability 771 16.7%
Executable File Transfer 126 2.7%
SMBv1 Communication 114 2.5%
External Plaintext Credentials... 20 0.4%
Clinical Vulnerability 13 0.3%
Malicious Internet... 12 0.3%
Others (9) 44 1%
Device Type Family Distribution (60)
1,688 Smartphone
1,205 PC
437 Thin Client
266 Tablet
224 Access Point
215 Printer
209 Small Computer
110 Server
90 Generic Mobile Device
69 Mobile Printer
65 Laptop
65 Patient Intake
High Risk Device Types (29)
Device Type Devices %
PC 687 50.4%
Smartphone 389 28.5%
Imaging Workstation 37 2.7%
Tablet 23 1.7%
EEG 21 1.5%
Ultrasound 16 1.2%
Blood Gas Analyzer 6 0.4%
Others (22) 46 3.4%

Übersicht Medizingeräte

MEDIGATE | Home | Devices | Alerts | Risk | Network | Operational Efficiency | Settings | Ulrich Brüll, St. Elisabeth und St. Bar...

Home / Devices / Medical Devices / Overview

Total 215 | Online 167 | Offline 48 | High Risk 102 | Advanced Filters

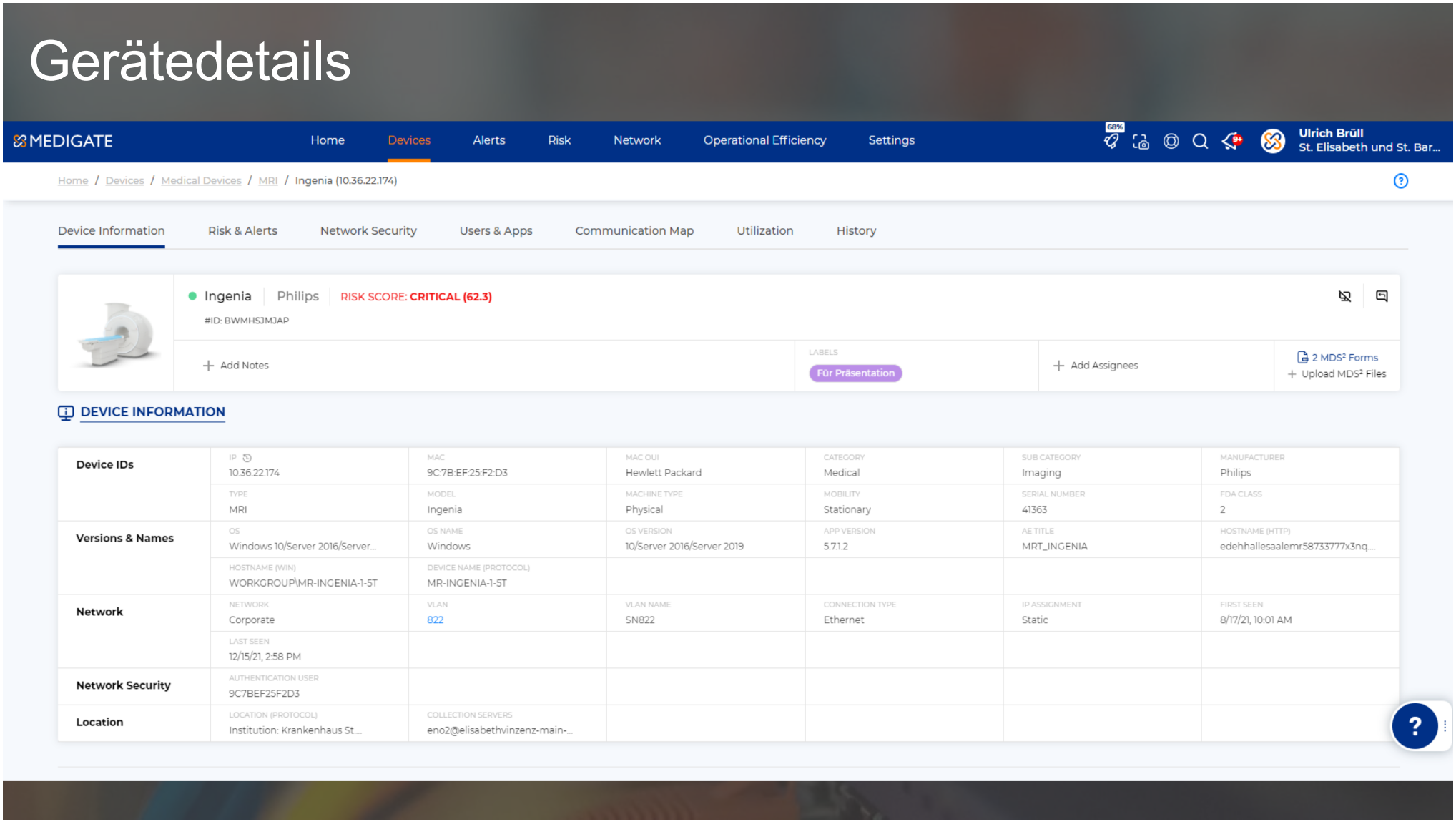
View by: Device Type Family | Sort by: Default

Showing: **215 Devices of 25 Device Type Families**

Search

Blood Gas Analyzer 6 Devices 3 Models — 6 High Risk	**Broker** 1 Device 1 Model — 1 High Risk	**Cardiac Monitor** 2 Devices 1 Model — 0 High Risk	**Central Station** 1 Device 1 Model — 1 High Risk	**Computed Radiography** 3 Devices 2 Models — 3 High Risk	**ECG** 1 Device 0 Models — 0 High Risk
EEG 22 Devices 3 Models — 22 High Risk	**EHR** 4 Devices 1 Model — 0 High Risk	**Fetal Monitor** 12 Devices 5 Models — 0 High Risk	**Hematology Analyzer** 2 Devices 1 Model — 1 High Risk	**Imaging Device** 5 Devices 0 Models — 5 High Risk	**Imaging Workstation** 39 Devices 4 Models — 37 High Risk

Gerätedetails



Risikobewertung

Device Information | Risk & Alerts | Network Security | Users & Apps | Communication Map | Utilization | History

DEVICE VULNERABILITY

Operating System	Windows 10/Server 2016/Server...
Vulnerabilities	Platform **22** | Clinical **1**
Outdated Firmware	Unknown
Endpoint Security	Installed (McAfee Agent)

NETWORK

Connection Type	Ethernet
Network	Corporate
VLAN Topology	Mixed Medical & Non-Medical...
Managed	Unknown
Internet Communication	Manufacturer
Enforcement	No

SEVERITY

PHI	Stored & Transmitted
Equipment Class	Diagnostic Device
Consequence of Failure	Inappropriate Therapy or...
Financial Cost	> $1,000,000

RISK SCORE: **CRITICAL (62.3)**

Confidence score: **High**

Risk Simulator

Internet Connection Detected

Manufacturer Internet Communication () Manufacturer VPN Communication ()

Device stores PHI

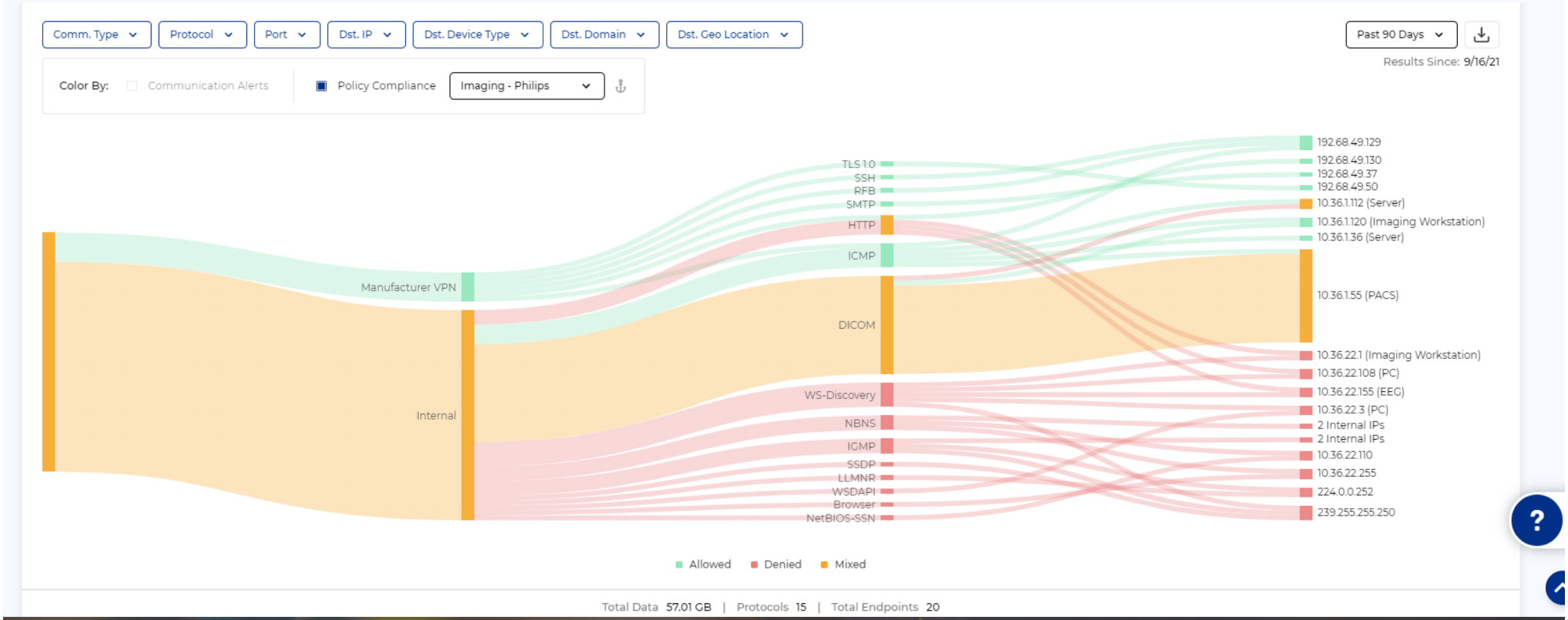
Alerts (23) — Export

ALERT CATEGORY	ALERT TYPE	DESCRIPTION	LAST UPDATE	STATUS
Device Alert	Clinical Vulnerability	A clinical vulnerability was identified. Affecting 1 Philips Ingenia device (ICSMA-21-...	12/13/21 9:28 AM	Unresolved
Device Alert	Platform Vulnerability	A platform vulnerability was identified. Potentially relevant for 1238 devices...	12/13/21 9:28 AM	Unresolved
Device Alert	Platform Vulnerability	A platform vulnerability was identified. Potentially relevant for 925 devices fro...	12/13/21 9:28 AM	Unresolved

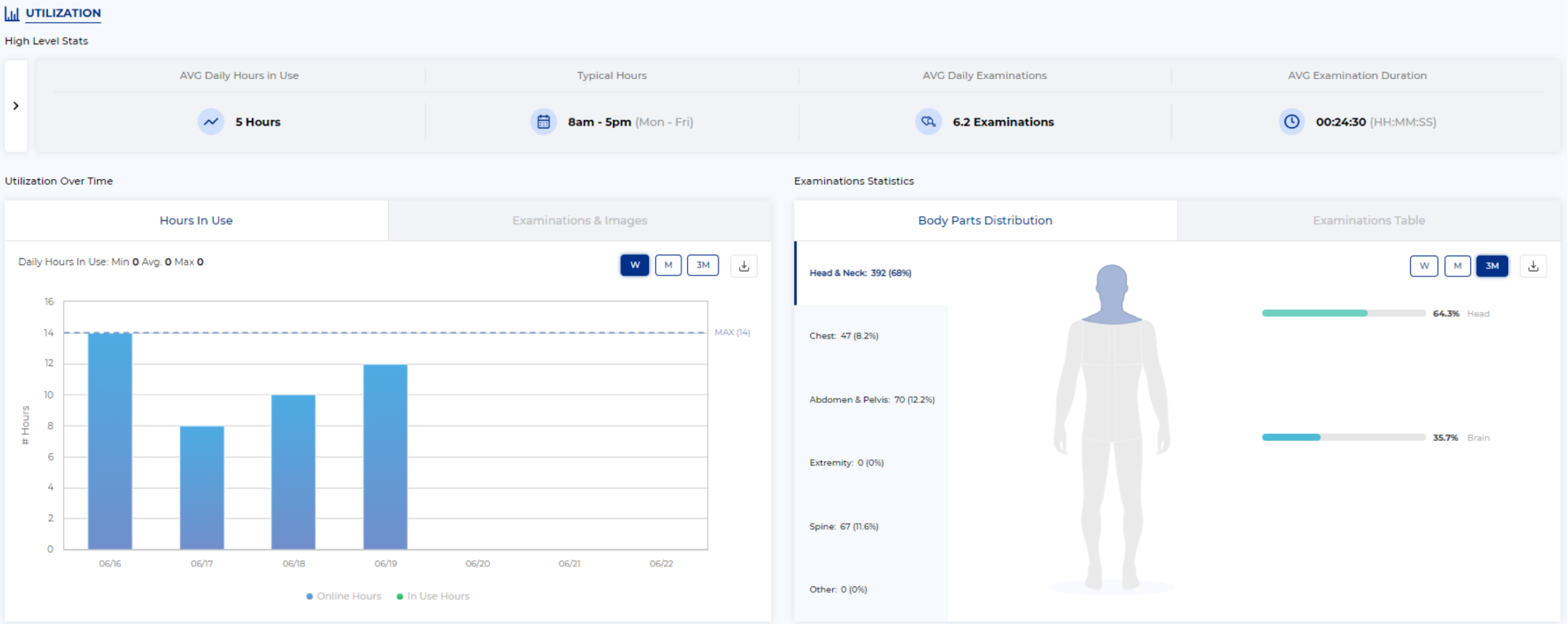
Vulnerabilities (23) / CVEs (32) — Export

VULNERABILITY NAME	TYPE	CVEs	CVSS	UPDATED BY	STATUS

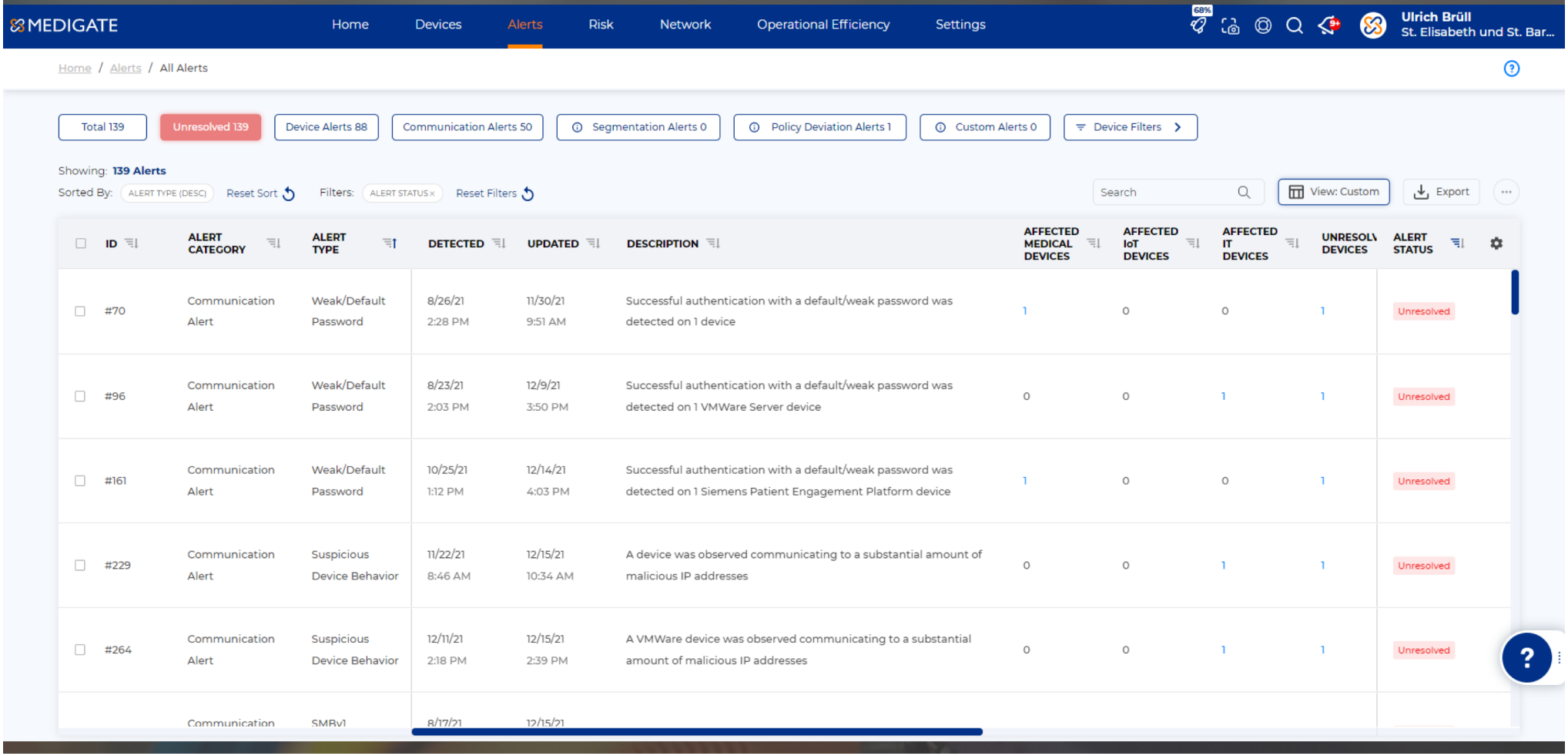
Kommunikationsbeziehungen



Nutzungsdaten



Meldungen & Workflows



xevIT Cyber Resilience Programm

- Sicherheitsbewertung
- Security Check & Analyse
- Penetrationstests
- Schwachstellenmgmt. IT & OT
- Reporting & Compliance
- Consulting

- Firewall Services
- DNS Security
- Security Awareness Training
- Multifaktor-Authentifizierung
- Endpoint Security
- Network Security
- Cloud Security

- Smart Back-up
- Disaster Recovery Plan
- Lessons Learned

- Real-time monitoring
- Threat Hunting
- Data leakage detection
- Attacker deception (Honeypots)

- Incident Response
- IR Management
- Incident Containment
- Incident Remediation

#cyberresilience

#gemeinsam

xevIT
part of conscia

Promo 1: Schwachstellen-Scan (1200,-€)
Promo 2: PoV Sicherheit in der Medizintechnik (2500,-€)

Mail an juergen.uebachs@xevit.com im Betreff
Promo 1 und/oder Promo 2