

Stand der IT-Sicherheit in deutschen Krankenhäusern



EV

**Elisabeth Vinzenz
Verbund**



xevIT
part of conscia

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

Netzwerkbasierete 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

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%
Raspberrry 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

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

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



Gerätedetails

Device Information

Risk & Alerts

Network Security

Users & Apps

Communication Map

Utilization

History



Ingenia | Philips | RISK SCORE: CRITICAL (62.3)

#ID: BWMHSJM3AP

+ Add Notes

LABELS

Für Präsentation

+ Add Assignees

2 MDS² Forms
+ Upload MDS² Files

DEVICE INFORMATION

Device IDs	IP	MAC	MAC OUI	CATEGORY	SUB CATEGORY	MANUFACTURER
	10.36.22.174	9C:7B:EF:25:F2:D3	Hewlett Packard	Medical	Imaging	Philips
Versions & Names	TYPE	MODEL	MACHINE TYPE	MOBILITY	SERIAL NUMBER	FDA CLASS
	MRI	Ingenia	Physical	Stationary	41363	2
Network	OS	OS NAME	OS VERSION	APP VERSION	AE TITLE	HOSTNAME (HTTP)
	Windows 10/Server 2016/Server...	Windows	10/Server 2016/Server 2019	5.7.1.2	MRT_INGENIA	edehhalesaalemr58733777x3nq...
Network Security	HOSTNAME (WIN)	DEVICE NAME (PROTOCOL)				
	WORKGROUP\MR-INGENIA-1-ST	MR-INGENIA-1-ST				
Location	NETWORK	VLAN	VLAN NAME	CONNECTION TYPE	IP ASSIGNMENT	FIRST SEEN
	Corporate	822	SN822	Ethernet	Static	8/17/21, 10:01 AM
Network Security	LAST SEEN					
	12/15/21, 2:58 PM					
Location	AUTHENTICATION USER					
	9C7BEF25F2D3					
Location	LOCATION (PROTOCOL)	COLLECTION SERVERS				
	Institution: Krankenhaus St...	eno2@elisabethvinzenz-main...				



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

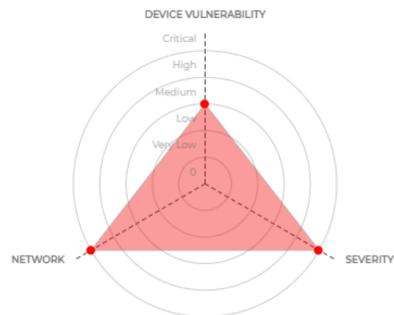
Connection Type Ethernet
Network Corporate
VLAN Topology Mixed Medical & Non-Medical...
Managed Unknown
Internet Communication Manufacturer
Enforcement No

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

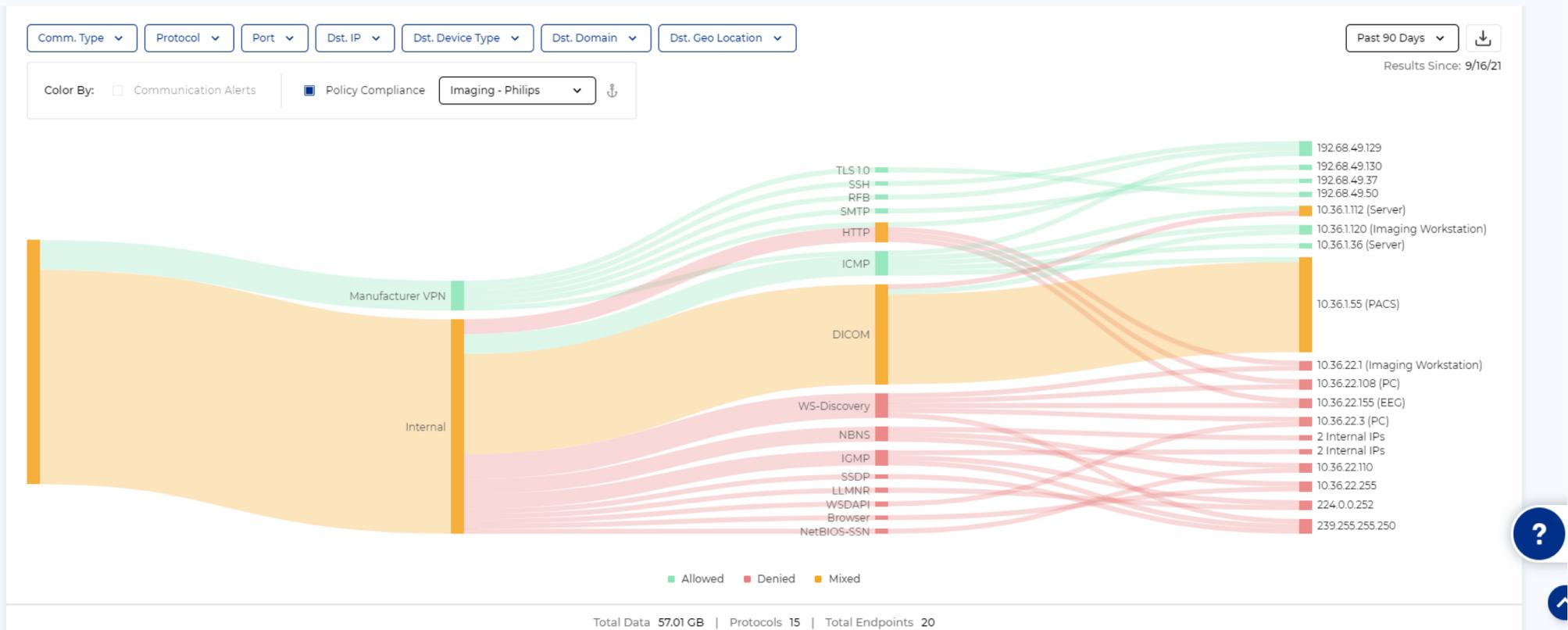
ALERT CATEGORY	ALERT TYPE	DESCRIPTION	LAST UPDATE	STATUS
Device Alert	Clinical Vulnerability	A clinical vulnerability was identified. Affecting 1 Philips Ingenia device (ICSMA-21-...	12/13/21 9:28 AM	Unresolved
Device Alert	Platform Vulnerability	A platform vulnerability was identified. Potentially relevant for 1238 devices...	12/13/21 9:28 AM	Unresolved
Device Alert	Platform Vulnerability	A platform vulnerability was identified. Potentially relevant for 825 devices fro...	12/13/21 9:28 AM	Unresolved

Vulnerabilities (23) / CVEs (32)

Export

VULNERABILITY NAME	TYPE	CVEs	CVSS	UPDATED BY	STATUS
--------------------	------	------	------	------------	--------

Kommunikationsbeziehungen



Nutzungsdaten

UTILIZATION

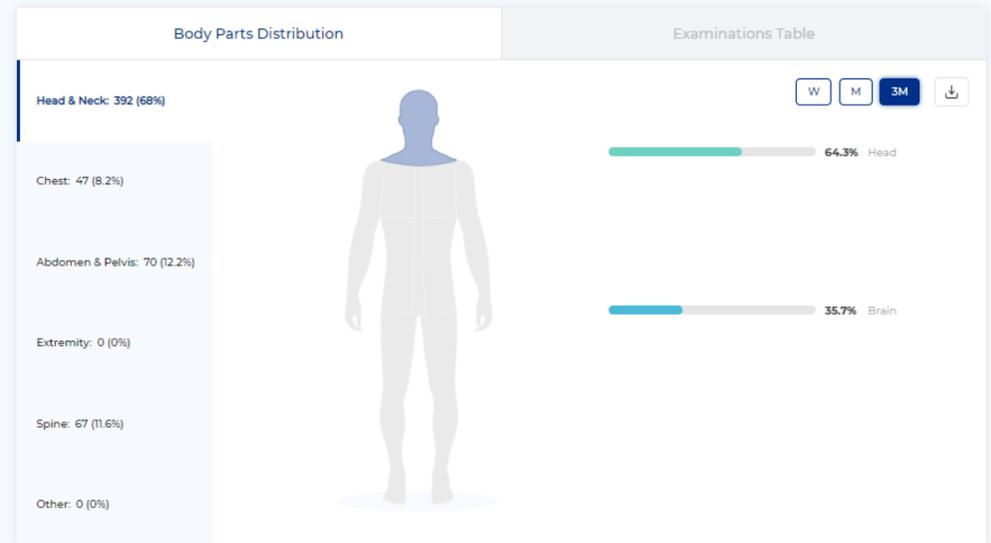
High Level Stats

AVG Daily Hours in Use 5 Hours	Typical Hours 8am - 5pm (Mon - Fri)	AVG Daily Examinations 6.2 Examinations	AVG Examination Duration 00:24:30 (HH:MM:SS)
--	---	---	--

Utilization Over Time



Examinations Statistics



Meldungen & Workflows

Home / Alerts / All Alerts



Total 139
Unresolved 139
Device Alerts 88
Communication Alerts 50
Segmentation Alerts 0
Policy Deviation Alerts 1
Custom Alerts 0
Device Filters >

Showing: 139 Alerts

Sorted By: ALERT TYPE (DESC) Reset Sort Filters: ALERT STATUS Reset Filters

View: Custom
Export

ID	ALERT CATEGORY	ALERT TYPE	DETECTED	UPDATED	DESCRIPTION	AFFECTED MEDICAL DEVICES	AFFECTED IoT DEVICES	AFFECTED IT DEVICES	UNRESOLV DEVICES	ALERT STATUS
#70	Communication Alert	Weak/Default Password	8/26/21 2:28 PM	11/30/21 9:51 AM	Successful authentication with a default/weak password was detected on 1 device	1	0	0	1	Unresolved
#96	Communication Alert	Weak/Default Password	8/23/21 2:03 PM	12/9/21 3:50 PM	Successful authentication with a default/weak password was detected on 1 VMWare Server device	0	0	1	1	Unresolved
#161	Communication Alert	Weak/Default Password	10/25/21 1:12 PM	12/14/21 4:03 PM	Successful authentication with a default/weak password was detected on 1 Siemens Patient Engagement Platform device	1	0	0	1	Unresolved
#229	Communication Alert	Suspicious Device Behavior	11/22/21 8:46 AM	12/15/21 10:34 AM	A device was observed communicating to a substantial amount of malicious IP addresses	0	0	1	1	Unresolved
#264	Communication Alert	Suspicious Device Behavior	12/11/21 2:18 PM	12/15/21 2:39 PM	A VMWare device was observed communicating to a substantial amount of malicious IP addresses	0	0	1	1	Unresolved
	Communication	SMRv1	8/17/21	12/15/21						



xevIT Cyber Resilience Programm

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

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



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

- 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

www.xevit.com