OCHRANA MEDICÍNSKYCH INFORMAČNÝCH AKTÍV

Kongres NIS 2022

Martin ŠUTÁK

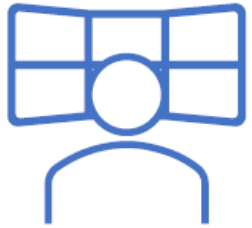
msutak@aliga.sk +421 905 407 717

TRENDY OVPLYVŇUJÚCE DIGITÁLNY TERÉN

Growth of Assets & Threats

Distributed Enterprise & Anywhere Operations

Fragmented Solutions



Shortage in Cybersecurity Personnel

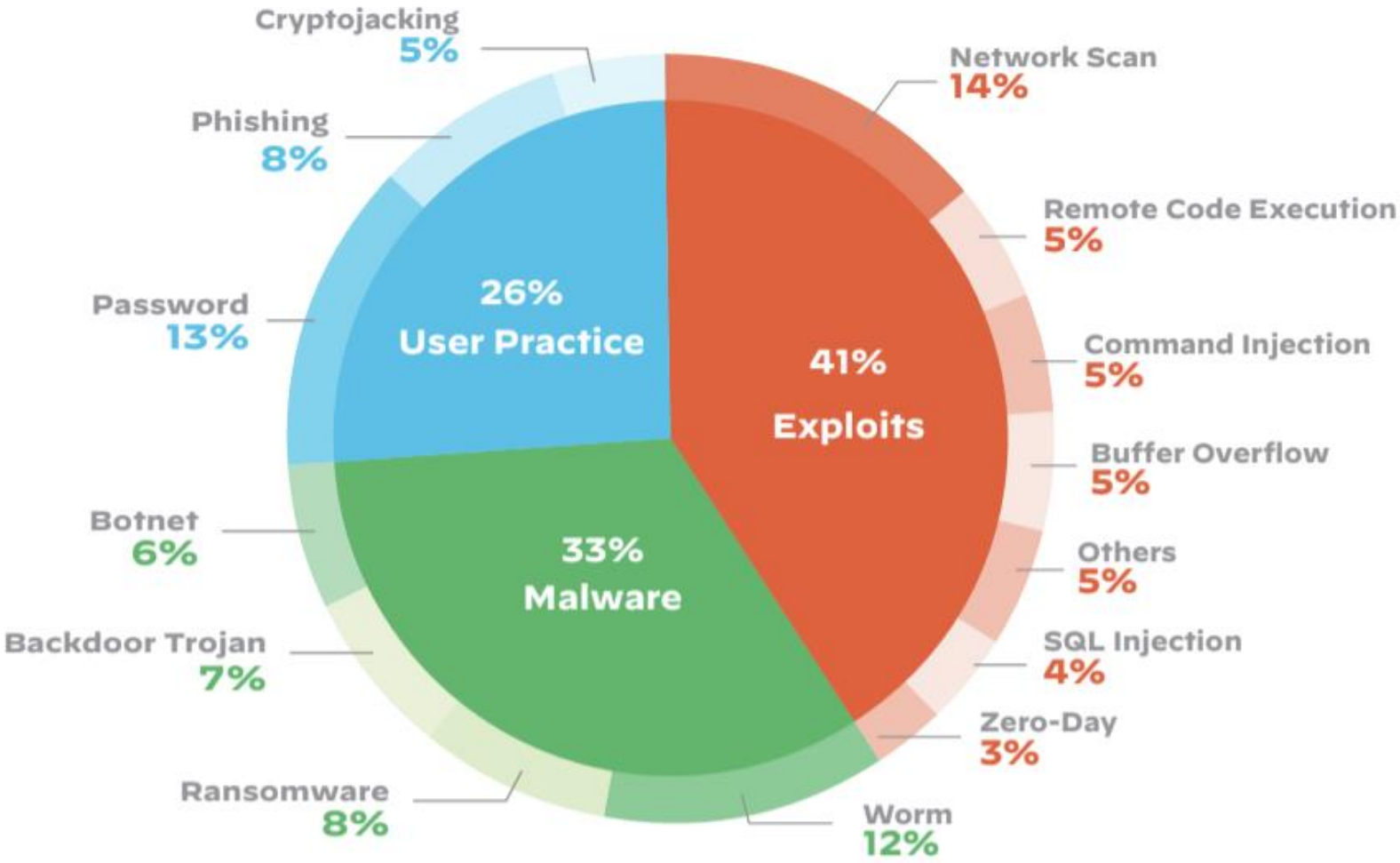
NAJRIZIKOVEJŠIE ZARIADENIA (by Unit 42)

Medical Imaging Systems

51%

Medical Devices Gateways

9%



Unit 42 IoT Threat Report

Kyberútoky na české nemocnice

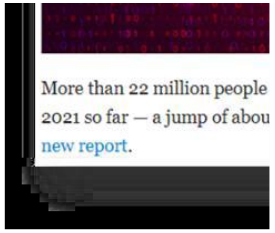
Ransomware v Nemocnici Rudolfa a Stefanie Benešov

V nemocnici v Benešově došlo k útoku na konci roku 2019. Kvůli omezení lékařských výkonů, zrušení plánovaných vyšetření, operací, výroby a nákladům na obnovu se škody za necelé tři týdny omezení provozu vyšplhaly na 59 milionů korun.

Při útoku na nemocnici byl použit ransomware Ryuk. Ten je běžně instalován pomocí dalších kmenů malwaru jako Emotet a Trickbot. Celý tento infekční řetězec zpravidla začíná phishingovým e-mailem s infikovanou přílohou, kterému neopatrný příjemce uvěří a přílohu otevře.

Fakultní nemocnice u sv. Anny v Brně (FNUSA)

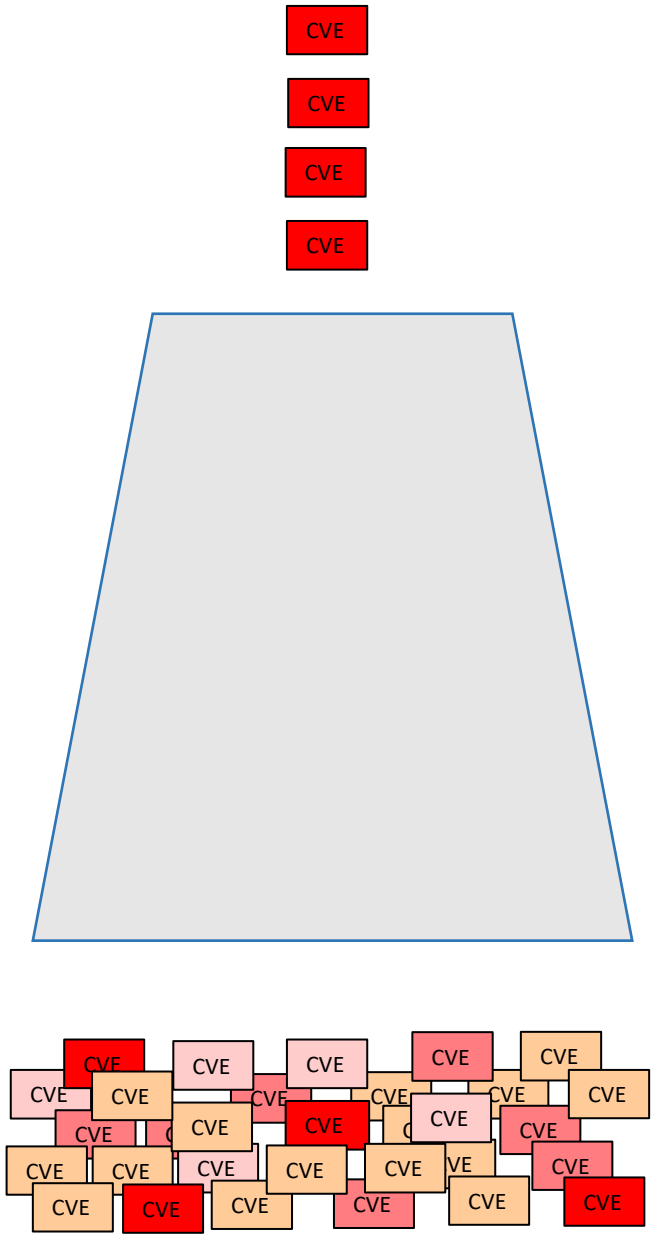
Útok oficiálně začal 13. března minulého roku, a tentokrát šlo o cílený útok ransomwaru Defray (Defray777). Útočníci se po úspěšném napadení zařízení pokusili z instituce vymámit výkupné, které jim však neposkytla, naopak se zaměřila na forenzní analýzu útoku společně s NÚKIBem a Avastem, jeho investigaci a co nejrychlejší nápravu. Provoz byl obnoven po čtyřech týdnech.



Psychiatrická nemocnice v Kosmonosech

Následoval útok na psychiatrickou nemocnici, který proběhl jen o několik málo dnů později. 27. března došlo k ransomwarovému útoku, který s největší pravděpodobností zneužil slabá, nedostatečně zabezpečená místa na serverech. Útočníci se v takovém případě přihlásí, vypnou v zařízení bezpečnostní řešení a ručně spustí škodlivý kód, jenž ze zařízení zašifruje všechny dostupné lokální a síťové disky. Takový útok není nijak náročný a jde s největší

ZRANITEĽNÝ ≠ ZNEUŽITEĽNÝ (Vulnerability ≠ Exploit)



Kriticky zneužiteľné zraniteľnosti

Posúdenie schopnosti dopadov pri realizácii rizika

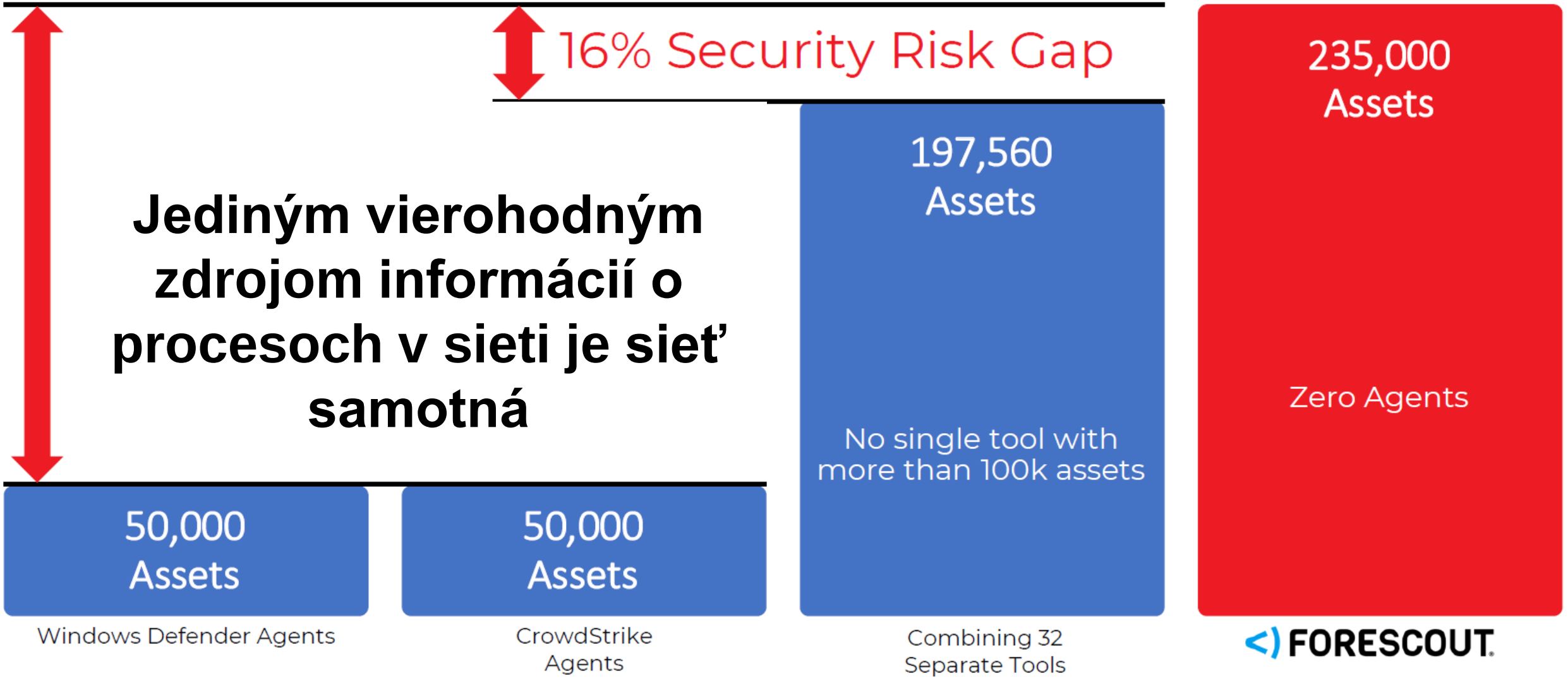
Zneužiteľné zraniteľnosti 2-3%

Potvrdenie zneužiteľnosti

Identifikované zraniteľnosti (CVE = Common Vulnerabilities and Exposures)

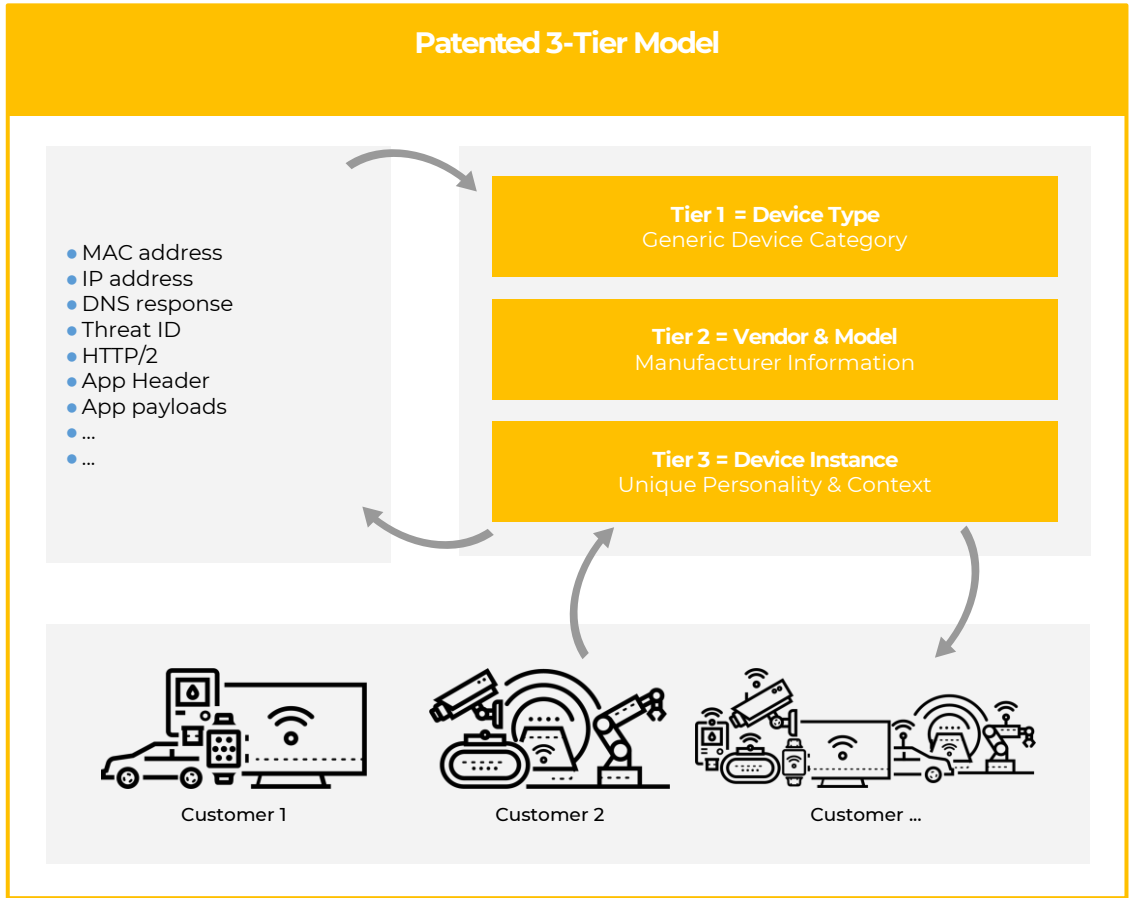
Potreba okamžitej reakcie

Zneužiteľné zraniteľnosti sú zreťazené s kompromitáciou osobných údajov, nesprávnou konfiguráciou a /alebo defaultnými nastaveniami

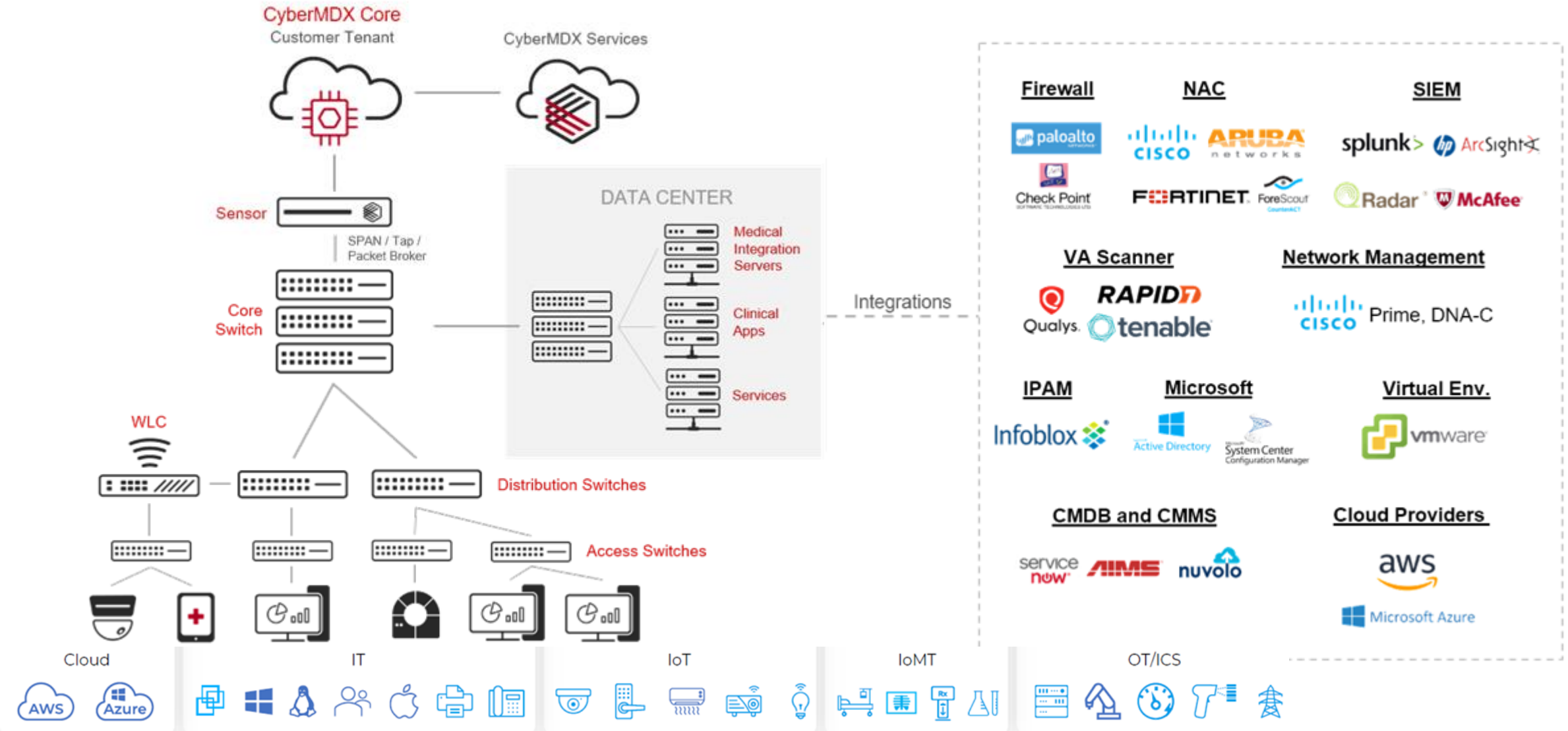

16% Security Risk Gap
Jediným vierohodným zdrojom informácií o procesoch v sieti je sieť samotná
50,000 Assets
Windows Defender Agents
50,000 Assets
CrowdStrike Agents
197,560 Assets
No single tool with more than 100k assets
Combining 32 Separate Tools
235,000 Assets
Zero Agents
FORESCOUT

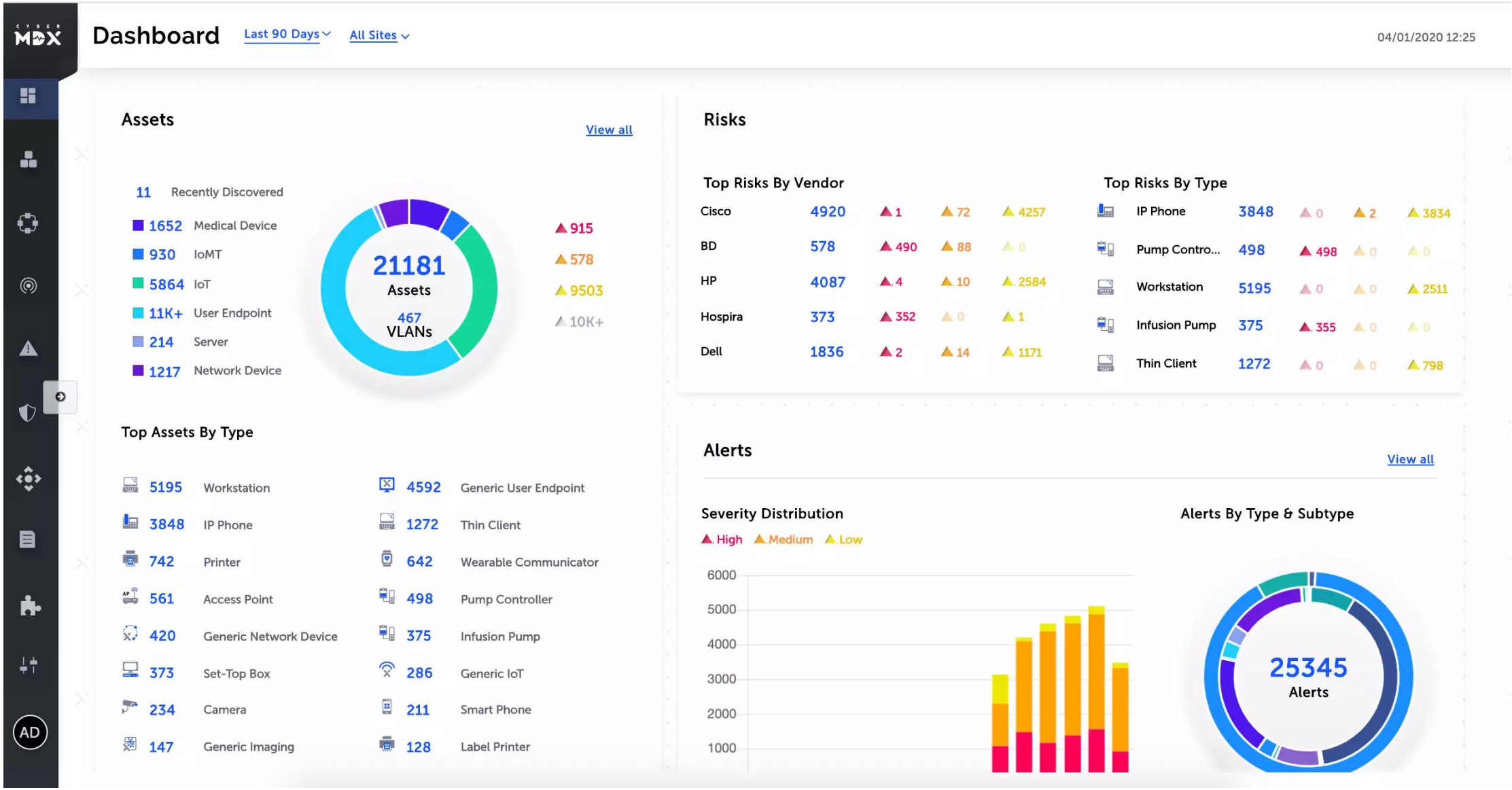
ROZPOZNANIE ZARIADENÍ S DETAILNÝM KONTEXTOM

00:*0:7*:73:37:5*	AmbiCom-Device	Carefusion Infusion Pump Base Station
c8:2*:*4:56:27:06	Apple-Device	Medical Workstation
08:60:6*:*8:06:83	Asus-Device	Medical Workstation
00:08:74:*2:50:*5	Dell-Device	DICOM-Viewer
00:2*:5*:6*:06:72	HP-Device	DICOM-Imager
00:09:6*:*6:60:7*	IBM-Device	Medical Workstation
00:*0:*4:2*:*0:94	INSIDE-Technology-Device	Medical Workstation



ARCHITEKTÚRA RIEŠENIA




CYBER MDX
Dashboard
Last 90 Days
All Sites
04/01/2020 12:25
Assets
View all
11 Recently Discovered
1652 Medical Device
930 IoMT
5864 IoT
11K+ User Endpoint
214 Server
1217 Network Device
21181
Assets
467
VLANs
915
578
9503
10K+
Top Assets By Type
5195 Workstation
3848 IP Phone
742 Printer
561 Access Point
420 Generic Network Device
373 Set-Top Box
234 Camera
147 Generic Imaging
4592 Generic User Endpoint
1272 Thin Client
642 Wearable Communicator
498 Pump Controller
375 Infusion Pump
286 Generic IoT
211 Smart Phone
128 Label Printer
Risks
Top Risks By Vendor
Cisco 4920 1 72 4257
BD 578 490 88 0
HP 4087 4 10 2584
Hospira 373 352 0 1
Dell 1836 2 14 1171
Top Risks By Type
IP Phone 3848 0 2 3834
Pump Contro... 498 498 0 0
Workstation 5195 0 0 2511
Infusion Pump 375 355 0 0
Thin Client 1272 0 0 798
Alerts
View all
Severity Distribution
High
Medium
Low
6000
5000
4000
3000
2000
1000
Alerts By Type & Subtype
25345
Alerts
AD

Cyber Risks

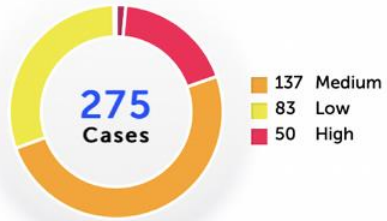
All Time | Search devices, device type, etc. | Vulnerabilities | Compliance | Threats

Vulnerabilities

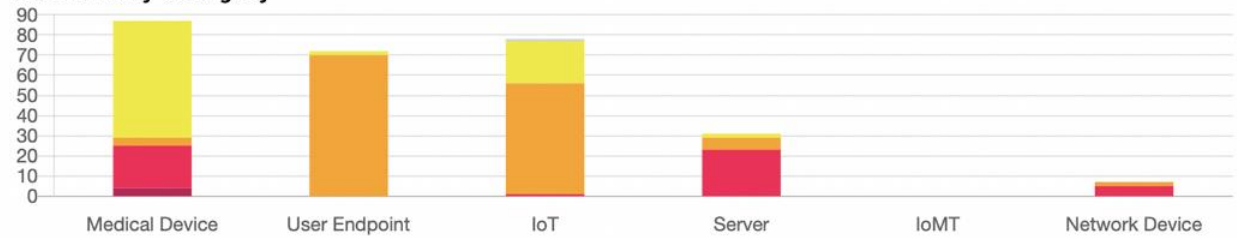
Group by Case

You are screen sharing | Stop Share

Cases by Risk



Case Risk by Category



46
New Cases

1087
Total Affected Assets

0 / 275 Cases Selected | Assign | Create Ticket | Resolve | Include Resolved (0) | Export | Columns | Reset Filters

Risk	Case Score	Case ID	Vulnerability...	Description	Asset Group	Equipment Function	Affected...	Resolv
Critical	94	V-000200	ACCESS:7	A bundle of Vulnerabilities affecting t...	Sysmex | Lab Machine	5: Analyt...	1	0/7
Critical	94	V-000022	Microsoft RDP Vulner...	A bundle of BlueKeep and DejaBlue Vulnerab...	Siemens | CT	6: Diagn...	1	0/3
Critical	93	V-000011	MDhex-Ray	Affected modalities are deployed with defaul...	GE | CT	6: Diagn...	1	0/1
Critical	93	V-000040	CVE-2019-0736	This device is possibly exposed to a memory ...	Siemens | CT	6: Diagn...	1	0/1
High	90	V-000002	Ripple20	A bundle of vulnerabilities caused by improp...	Baxter | Infusion Pump	9: Thera...	208	0/104
High	86	V-000003	Ripple20	A bundle of vulnerabilities caused by improp...	DigiBoard | Terminal Server		32	0/160
High	86	V-000004	NAME:WRECK	A bundle of vulnerabilities on DNS/DHCP im...	BD | Pump Controller	8: Thera...	146	0/146
High	86	V-000008	ICSA-19-211-01	This device is exposed to the 'URGENT11' vul...	BD | Pump Controller	8: Thera...	146	0/146
High	85	V-000032	CVE-2017-6738	The Simple Network Management Protocol (...	Cisco | Switch		112	0/112
High	85	V-000033	CVE-2017-6739	The Simple Network Management Protocol (...	Cisco | Switch		112	0/112
High	85	V-000197	CVE-2017-6744	The Simple Network Management Protocol (...	Cisco | Switch		112	0/112

Items per page: 50 | 1 – 50 of 275

KG

Cyber Risks

All Time

Search devices, device type, etc.

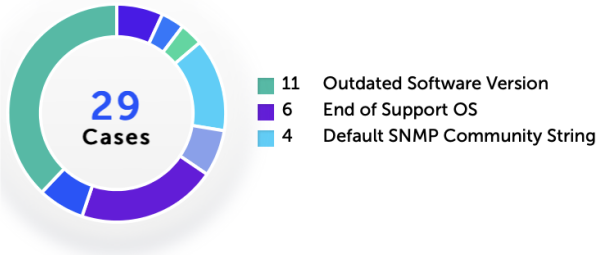
Vulnerabilities | Compliance | Threats

Compliance Issues

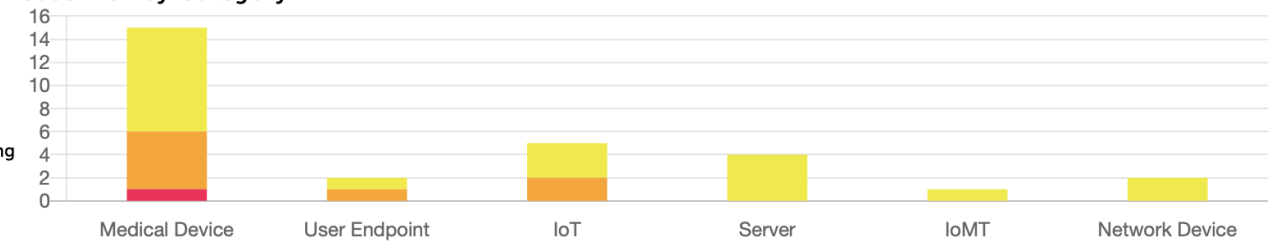
Group by Case

You are screen sharing | Stop Share

Case by Issue Type



Case Risk by Category



0
New Cases

1546
Total Affected Assets

0 / 29 Cases Selected Assign | Create Ticket | Resolve

Include Resolved (0) | Export | Columns | Reset Filters

Risk	Case Score	Case ID	Issue Type	Description	Asset Group	Equipment Function	Affected...	Resolv
High	81	C-000021	Default Credentials	These assets are configured with default cre...	GE | ECG	6: Diagn...	18	0/18
Medium	60	C-000024	End of Life OS	Operating system is no longer supported.	Axis | Camera		112	0/112
Medium	60	C-000001	Outdated Software V...	These assets are running outdated software ...	BD | Syringe Pump	9: Thera...	101	0/101
Medium	47	C-000018	Default Credentials	These assets are configured with default cre...	Axis | Camera		1	0/1
Medium	46	C-000030	Asset on Guest Netw...	These medical devices were seen communic...	BD | Pump Controller	8: Thera...	1	0/1
Medium	46	C-000008	Deprecated Protocol ...	These assets use deprecated protocol versio...	Siemens | CT	6: Diagn...	1	0/1
Medium	46	C-000031	End of Life OS	Operating system is no longer supported.	GE | CT	6: Diagn...	1	0/1
Medium	45	C-000025	Deprecated Protocol ...	These assets use deprecated protocol versio...	HP | Workstation		1	0/1
Medium	45	C-000010	Outdated Software V...	These assets are running outdated software ...	Siemens | CT	6: Diagn...	1	0/1
Low	30	C-000014	Outdated Software V...	These assets are running outdated software ...	Cisco | IP Phone		392	0/392
Low	26	C-000003	Outdated Software V...	These assets are running outdated software ...	BD | Pump Controller	8: Thera...	114	0/114

Items per page: 50 1 – 29 of 29

KG

Host Details

Profile | Compliance | All Policies | Policy Actions

IPv4 Address: 192.168.155.6 **Domain:** WORKGROUP **Operating System:** Windows XP
MAC Address: 000b59c465a4 **Function:** Medication Dispensing System
Vendor and Model: ScriptPro

Search

- Classification
- General
- User
- Network Access
- Security
- Classification Details
- More

General

IPv4 Address:		192.168.155.6
Admission:		Offline host became online
		DHCP Request
		New Host
DNS Name:	+	medstation-e5dc95
Linux Manageable (SecureConnector):		No
MAC Address:	+	000b59c465a4
Is behind NAT/SASE:		No
NetBIOS Domain:	+	WORKGROUP
NIC Vendor:		SCRIPTPRO, LLC
Open Ports:	+	80/TCP
	+	104/TCP
	+	135/TCP
	+	137/UDP
	+	161/UDP
	+	8080/TCP
OS Class (Obsolete):		Windows Machine
OS Fingerprint:	+	Windows XP Professional Service Pack 3
Windows SecureConnector Deployment Type:		None
Windows SecureConnector Systray Display:		None
Windows SecureConnector Version:	+	None
Windows Manageable Domain:		No
Windows Manageable Domain (Current):		No
Windows Manageable SecureConnector:		No
Network Function:		Windows Machine

User

Logged In Status:		Not logged in

Network Access

Switch IP/FQDN:	+	192.168.155.1
Switch IP/FQDN and Port Name:	+	192.168.155.1:Gi0/38
Switch Port Configurations:	+	pae authenticator

Host Details

Profile | Compliance | All Policies | Policy Actions

IPv4 Address: 192.168.155.6 **Domain:** WORKGROUP **Operating System:** Windows XP
MAC Address: 000b59c465a4 **Function:** Medication Dispensing System
Vendor and Model: ScriptPro

Search

- Classification
- General
- User
- Network Access
- Security
- Classification Details
- More

Network Access

Switch IP/FQDN:	+	192.168.155.1
Switch IP/FQDN and Port Name:	+	192.168.155.1:Gi0/38
Switch Port Configurations:	+	pae authenticator
	+	snmp trap mac-notification
	+	switchport mode access
Switch Port Name:	+	Gi0/38
Switch Port PoE Connected Device:	+	IEEE PD
Switch Port PoE Power Consumption:		2176
Switch Port VLAN:		50
Switch Vendor:	+	Cisco
WLAN Client Connectivity Status:		No

Security

Last Reported IOC:

Low Severity:		10/13/21 5:41:00 PM
Medium Severity:		4/19/22 8:15:10 AM
High Severity:		3/31/22 3:57:24 PM
Critical Severity:		10/21/21 3:47:32 AM
SIEM Message:		alert_syslog: host=10.100.10.105:514, Facility:Cisco ASA Priority:1 Options:No Action
		alert_syslog: host=10.100.10.105:514, Facility:Fortinet Priority:4 Options:No Action
		alert_syslog: host=10.100.10.105:514, Facility:InfoBlox Priority:10 Options:Port Block
		alert_syslog: host=10.100.10.105:514, Facility:LogRythm Priority:8 Options:HTTP Notification
		alert_syslog: host=10.100.10.105:514, Facility:Snort Priority:1 Options:No Action
		Show more

Classification Details

Vendor Classified By:	CounterACT Device Classification Engine
Class Vendor Classified By:	Device Profile Library
Matched Classification Profiles:	ScriptPro
	Windows XP Professional
	Windows XP Professional SP3
	Windows XP_1
	Windows_1

Host Details

Profile | Compliance | All Policies | Policy Actions

IPv4 Address: 192.168.155.22 **Domain:** WORKGROUP **Operating System:** Unknown
MAC Address: c400adbdd6d2 **Function:** PACS System
Vendor and Model: Advantech

Search

- Classification
- General
- User
- Network Access
- Security
- Classification Details
- More

Classification

Function:	+	PACS System
Operating System:	+	Unknown
Vendor and Model:	+	Advantech
Class Vendor:	+	Advantech

General

IPv4 Address:		192.168.155.22
Admission:		Offline host became online
		DHCP Request
		New Host
DNS Name:	+	ultrasound-e5ea34
Linux Manageable (SecureConnector):		No
Linux Manageable (SSH Direct Access):		No
MAC Address:	+	c400adbdd6d2
Is behind NAT/SASE:		No
NetBIOS Domain:	+	WORKGROUP
NIC Vendor:		ADVANTECH TECHNOLOGY (CHINA) CO., LTD.
Open Ports:	+	80/TCP
	+	104/TCP
	+	161/UDP
	+	443/TCP
	+	8081/TCP
Windows SecureConnector Deployment Type:		None
Windows SecureConnector Systray Display:		None
Windows SecureConnector Version:	+	None
Windows Manageable Domain:		No
Windows Manageable Domain (Current):		No
Windows Manageable SecureConnector:		No

User

Logged In Status:		Not logged in

Host Details

Profile | Compliance | All Policies | Policy Actions

IPv4 Address: 192.168.155.22 **Domain:** WORKGROUP **Operating System:** Unknown
MAC Address: c400adbdd6d2 **Function:** PACS System
Vendor and Model: Advantech

Search

- Classification
- General
- User
- Network Access
- Security
- Classification Details
- More

User

Logged In Status:	Not logged in

Network Access

Switch IP/FQDN:	+	192.168.155.1
Switch IP/FQDN and Port Name:	+	192.168.155.1:Gi0/30
Switch Port Configurations:	+	dot1x port-control auto
	+	pae authenticator
	+	snmp trap mac-notification
	+	snmp trap mac-notification added
Switch Port Name:	+	Gi0/30
Switch Port PoE Connected Device:	+	IEEE PD
Switch Port PoE Power Consumption:		2176
Switch Port VLAN:		50
Switch Vendor:	+	Cisco
WLAN Client Connectivity Status:		No

Security

Last Reported IOC:

Low Severity:		10/13/21 5:41:00 PM
Medium Severity:		4/19/22 8:15:10 AM
High Severity:		3/31/22 3:57:24 PM
Critical Severity:		10/21/21 3:47:32 AM
SIEM Message:	✎	alert_syslog: host=10.100.10.105:514, Facility:Cisco ASA Priority:1 Options:No Action
	✎	alert_syslog: host=10.100.10.105:514, Facility:Fortinet Priority:4 Options:No Action
	✎	alert_syslog: host=10.100.10.105:514, Facility:InfoBlox Priority:10 Options:Port Block
	✎	alert_syslog: host=10.100.10.105:514, Facility:Security Priority:3 Options:No Action

Classification Details

Vendor Classified By:	CounterACT Device Classification Engine
Class Vendor Classified By:	Device Profile Library
Matched Classification Profiles:	Advantech
	Advantech PACS Server
Function Classification Source:	Device Profile Library

CT
10.104.131.253
Site Hospital3

Quarantine | Group

MDS2

Asset Attributes

Category	Medical Device
Type	CT
Vendor	GE
Model	LightSpeed VCT
Equipment Function	6: Diagnostic - Other Physiological Monitoring
Classification Fidelity	High
MAC	18:60:24:88:EF:29
Location	Hospital3 > Building C > Floor 4 > Room 412
Serial Number	22558
Asset Tag	
Criticality	Critical
FDA Classification	Class II
Last Seen	04/19/2022 18:07
First Seen	12/24/2021 14:06
Last Vendor Access	04/19/2022 12:01
Last Scan Time	
Last Queried by CyberMDX	

Tags

Risk Assessment

You are screen sharing | Stop Share

93 Critical
CMDX Score

1 Vulnerabilities

1 Threats

1 Compliance Issues

Device

Criticality	Critical
PHI	Yes
Recalls	Yes (10)

Software

Outdated Version	Yes
Default Credentials	
Known Vulnerabilities	Yes

Mitigations

Endpoint Protection	
Managed	No

Network

VLAN Type	MD Only
Internet Connection	Yes
Threats Detected	Yes

Take Action

All | Device Level | Network Level | Perimeter Level

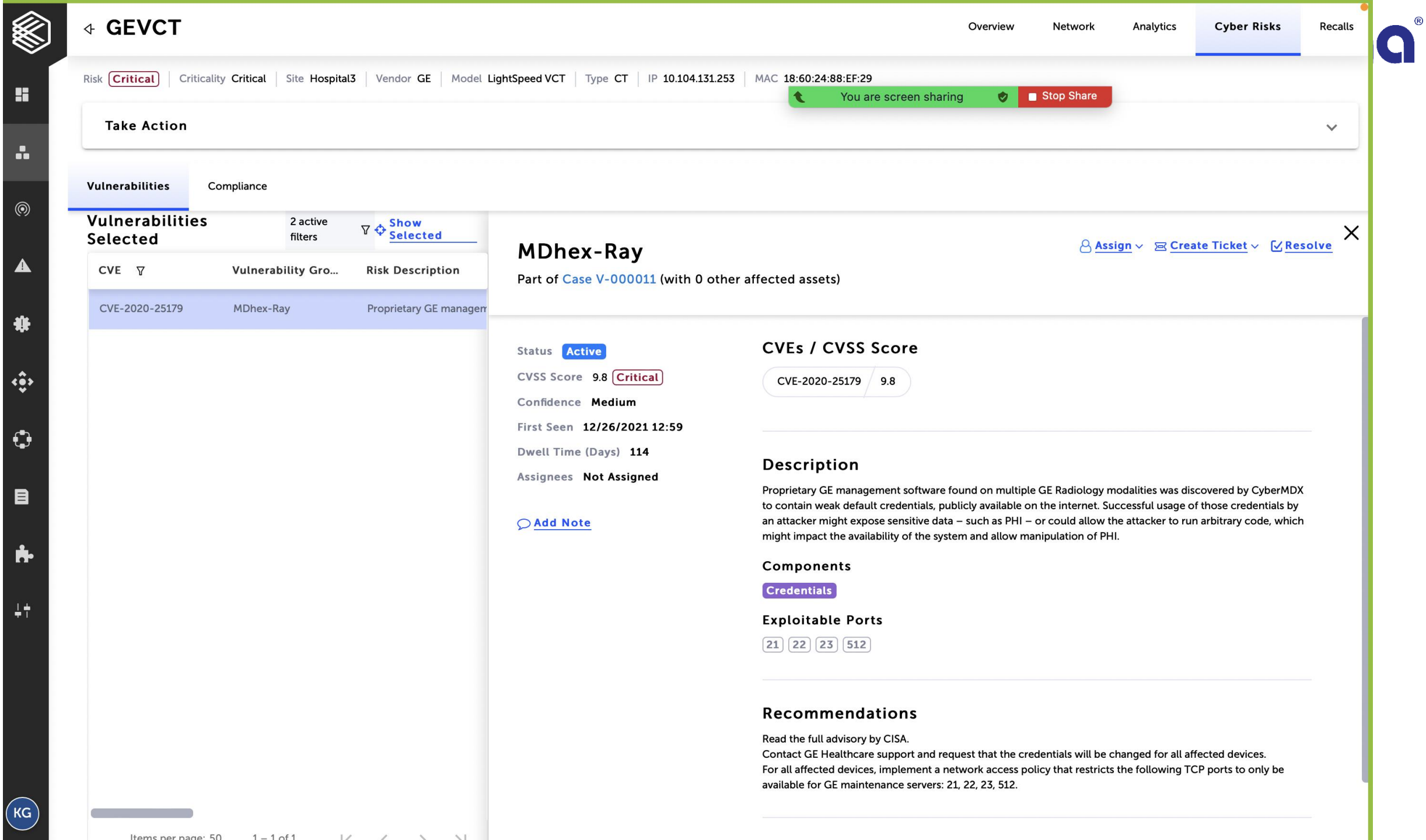
Blocklist
Disabled
Risk Reduction
Reduce Attack Surface

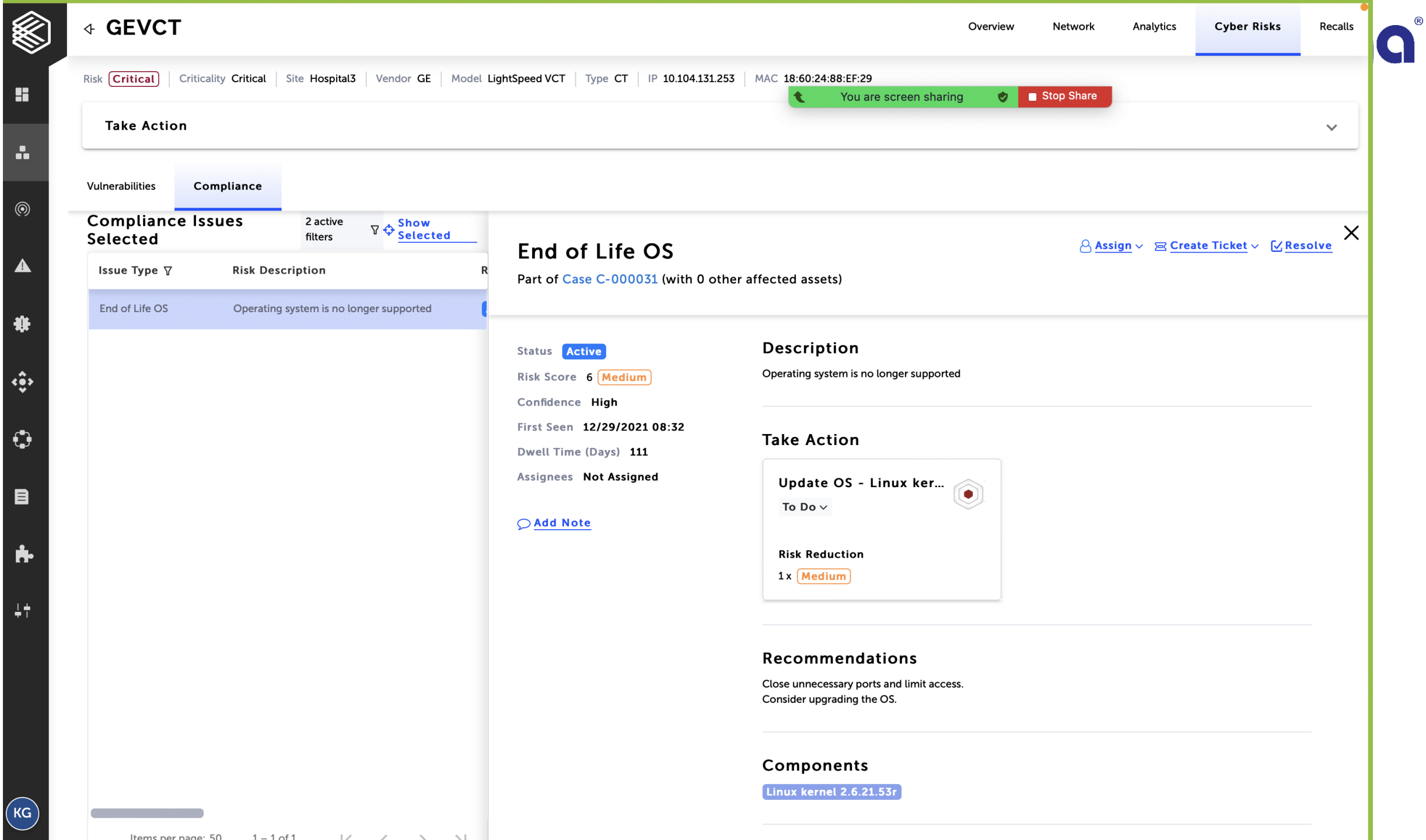
Allowlist
Disabled
Risk Reduction
Reduce Attack Surface

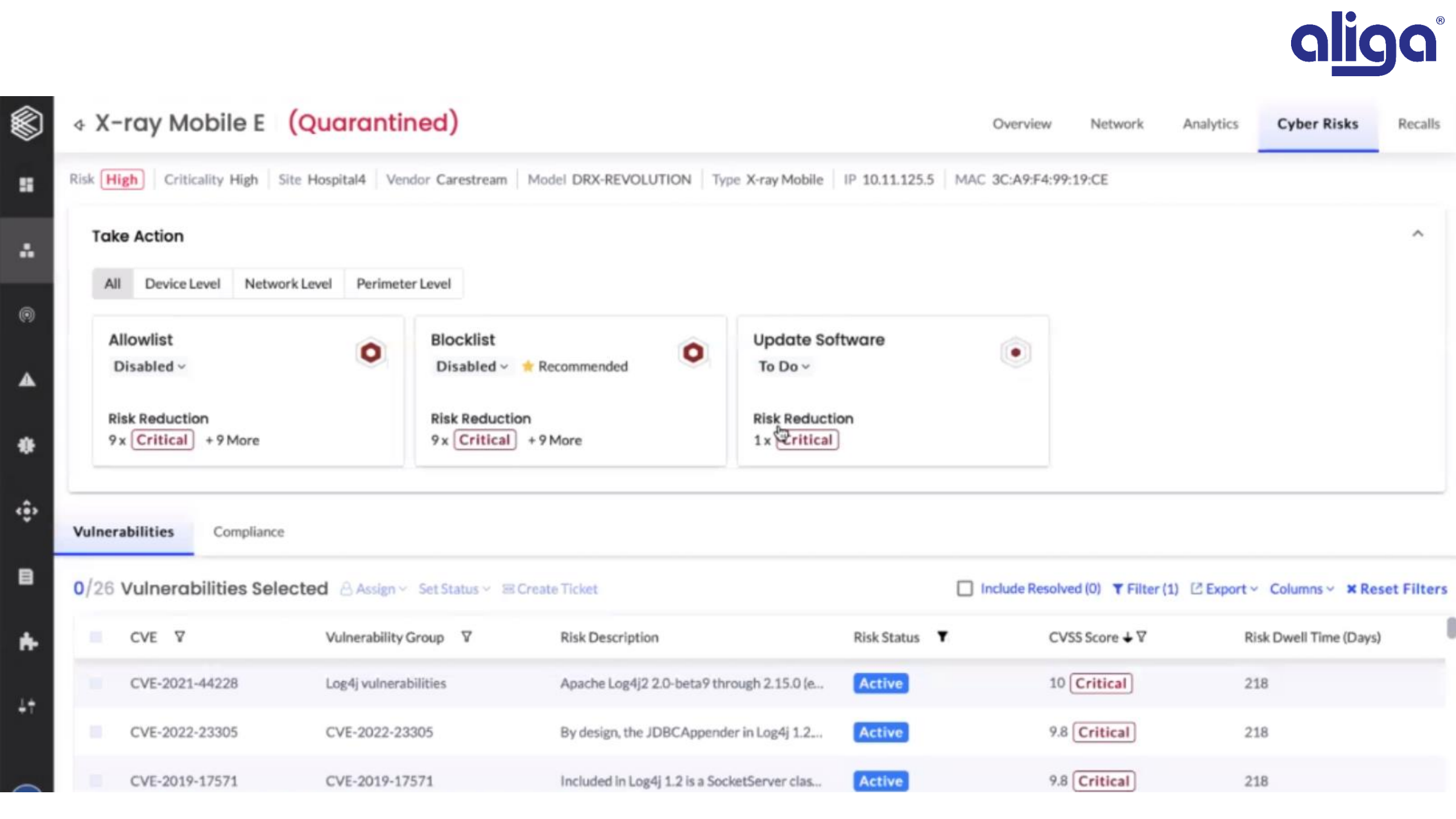
Update OS - Linux ker...
To Do
Risk Reduction
1 x Medium

Network Context

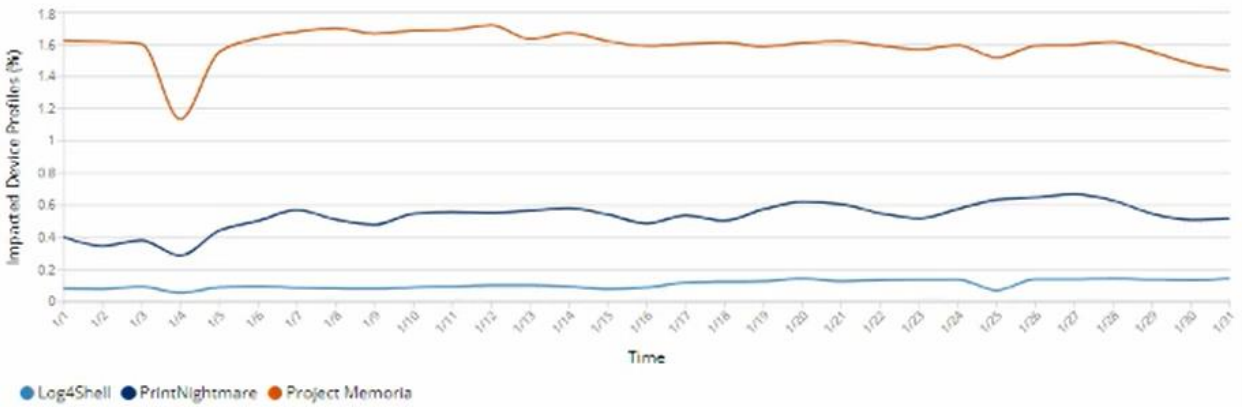
IP	10.104.131.253	MAC	18:60:24:88:EF:29
VLAN	20	NIC Vendor	HP
Subnet Name	Hospital3	Binding Expiration Ti...	
Connection Type	Wired LAN	Binding Source	


GEVCT
Overview
Network
Analytics
Cyber Risks
Recalls
Risk Critical | Criticality Critical | Site Hospital3 | Vendor GE | Model LightSpeed VCT | Type CT | IP 10.104.131.253 | MAC 18:60:24:88:EF:29
You are screen sharing
Stop Share
Take Action
Vulnerabilities
Compliance
Vulnerabilities Selected
2 active filters
Show Selected
CVE
Vulnerability Gro...
Risk Description
CVE-2020-25179
MDhex-Ray
Proprietary GE managem
Items per page: 50
1 – 1 of 1
KG
MDhex-Ray
Part of Case V-000011 (with 0 other affected assets)
Assign
Create Ticket
Resolve
Status Active
CVSS Score 9.8 Critical
Confidence Medium
First Seen 12/26/2021 12:59
Dwell Time (Days) 114
Assignees Not Assigned
Add Note
CVEs / CVSS Score
CVE-2020-25179
9.8
Description
Proprietary GE management software found on multiple GE Radiology modalities was discovered by CyberMDX to contain weak default credentials, publicly available on the internet. Successful usage of those credentials by an attacker might expose sensitive data – such as PHI – or could allow the attacker to run arbitrary code, which might impact the availability of the system and allow manipulation of PHI.
Components
Credentials
Exploitable Ports
21
22
23
512
Recommendations
Read the full advisory by CISA.
Contact GE Healthcare support and request that the credentials will be changed for all affected devices.
For all affected devices, implement a network access policy that restricts the following TCP ports to only be available for GE maintenance servers: 21, 22, 23, 512.


GEVCT
Overview
Network
Analytics
Cyber Risks
Recalls
Risk Critical | Criticality Critical | Site Hospital3 | Vendor GE | Model LightSpeed VCT | Type CT | IP 10.104.131.253 | MAC 18:60:24:88:EF:29
You are screen sharing
Stop Share
Take Action
Vulnerabilities
Compliance
Compliance Issues Selected
2 active filters
Show Selected
Issue Type
Risk Description
End of Life OS
Operating system is no longer supported
Items per page: 50
1 – 1 of 1
KG
End of Life OS
Assign
Create Ticket
Resolve
Part of Case C-000031 (with 0 other affected assets)
Status Active
Risk Score 6 Medium
Confidence High
First Seen 12/29/2021 08:32
Dwell Time (Days) 111
Assignees Not Assigned
Add Note
Description
Operating system is no longer supported
Take Action
Update OS - Linux ker...
To Do
Risk Reduction
1 x Medium
Recommendations
Close unnecessary ports and limit access.
Consider upgrading the OS.
Components
Linux kernel 2.6.21.53r


aliga®
X-ray Mobile E (Quarantined)
Overview
Network
Analytics
Cyber Risks
Recalls
Risk High | Criticality High | Site Hospital4 | Vendor Carestream | Model DRX-REVOLUTION | Type X-ray Mobile | IP 10.11.125.5 | MAC 3C:A9:F4:99:19:CE
Take Action
All
Device Level
Network Level
Perimeter Level
Allowlist
Disabled
Risk Reduction
9 x Critical + 9 More
Blocklist
Disabled
Recommended
Risk Reduction
9 x Critical + 9 More
Update Software
To Do
Risk Reduction
1 x Critical
Vulnerabilities
Compliance
0/26 Vulnerabilities Selected
Assign
Set Status
Create Ticket
Include Resolved (0)
Filter (1)
Export
Columns
Reset Filters
CVE
Vulnerability Group
Risk Description
Risk Status
CVSS Score
Risk Dwell Time (Days)
CVE-2021-44228
Log4j vulnerabilities
Apache Log4j2 2.0-beta9 through 2.15.0 (e...
Active
10 Critical
218
CVE-2022-23305
CVE-2022-23305
By design, the JDBCAppender in Log4j 1.2...
Active
9.8 Critical
218
CVE-2019-17571
CVE-2019-17571
Included in Log4j 1.2 is a SocketServer clas...
Active
9.8 Critical
218

Threats of Interest



10 Most Exploitable Vulnerabilities

CVE ID	CVE TITLE	CVSS	EPSS (0-1)	IMPACTED DEVICES
CVE-2018-3639	Multiple Intel CPU's information disclosure...	5.40	0.94	0.9%
CVE-2020-12695	Open Connectivity Foundation UPnP specification su...	7.40	0.91	0.9%
CVE-2021-3156	Sudo buffer overflow...	7.80	0.67	0.7%
CVE-2017-3881	Cisco IOS and Cisco IOS XE CMP code execution...	9.80	0.62	0.5%
CVE-2018-4162	Apple Safari WebKit code execution...	6.80	0.41	0.4%
CVE-2018-8897	Multiple operating systems hardware debug privileg...	7.80	0.34	0.3%
CVE-2020-14871	Oracle Solaris unspecified...	10.00	0.33	0.3%
CVE-2020-7388	Sage X3 command execution...	9.80	0.32	0.3%
CVE-2018-4121	Apple Safari WebKit code execution...	6.80	0.29	0.3%
CVE-2017-3629	Oracle Sun Systems Solaris Kernel unspecified...	7.80	0.26	0.3%

Most Concerning Vulnerabilities (High CVSS/EPSS) - IT

CVE ID	CVE TITLE	CVSS	EPSS (0-1)	IMPACTED DEVICES
CVE-2021-3156	Sudo buffer overflow...	7.80	0.67	0.7%
CVE-2017-3881	Cisco IOS and Cisco IOS XE CMP code execution...	9.80	0.51	0.5%
CVE-2018-4162	Apple Safari WebKit code execution...	6.80	0.40	0.4%
CVE-2018-8897	Multiple operating systems hardware debug privileg...	7.80	0.34	0.3%
CVE-2020-14871	Oracle Solaris unspecified...	10.00	0.33	0.3%

Most Concerning Vulnerabilities (High CVSS/EPSS) - IoT

CVE ID	CVE TITLE	CVSS	EPSS (0-1)	IMPACTED DEVICES
CVE-2020-12695	Open Connectivity Foundation UPnP specification su...	7.50	0.91	0.9%
CVE-2021-3156	Sudo buffer overflow...	7.80	0.67	0.7%
CVE-2017-3881	Cisco IOS and Cisco IOS XE CMP code execution...	9.80	0.51	0.5%
CVE-2018-10661	Axis IP Cameras mod_authz_axisgroupfile.so securit...	9.80	0.25	0.3%
CVE-2018-10662	Axis IP Cameras dbus action weak security...	9.80	0.25	0.3%

Most Concerning Vulnerabilities (High CVSS/EPSS) - OT

CVE ID	CVE TITLE	CVSS	EPSS (0-1)	IMPACTED DEVICES
CVE-2018-3639	Multiple Intel CPU's information disclosure...	5.50	0.93	0.9%
CVE-2017-3881	Cisco IOS and Cisco IOS XE CMP code execution...	9.80	0.51	0.5%
CVE-2018-0171	Cisco IOS and Cisco IOS XE Smart Install buffer ov...	9.80	0.15	0.1%
CVE-2020-7207	HPE Proliant Gen10 Servers privileges escalation...	6.80	0.09	< 0.1%
CVE-2020-3161	Cisco IP Phones code execution...	9.80	0.07	< 0.1%

Most Concerning Vulnerabilities (High CVSS/EPSS) - IoMT

CVE ID	CVE TITLE	CVSS	EPSS (0-1)	IMPACTED DEVICES
CVE-2020-7388	Sage X3 command execution...	9.80	0.31	0.3%
CVE-2020-7387	Sage X3 path disclosure...	5.30	0.17	0.2%
CVE-2018-5407	Multiple SMT/Hyper-Threading architectures and pro...	4.65	0.12	0.1%
CVE-2019-15792	Ubuntu shiftfs implementation code execution...	7.80	0.07	< 0.1%
CVE-2021-29998	Wind River VxWorks buffer overflow...	9.80	0.03	< 0.1%

Vedere Labs Latest Research Findings

December 13th, 2021

Log4Shell

The evolving Log4Shell story: analysis of ongoing and future exploits. Read More

Latest Critical Vulnerabilities

10.0	Remote Code Execution in cominput.jsp and comoutput.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to inject and execute arbitrary system commands...	CVE-2021-29393	View

KONTINUÁLNE ZISŤOVANIE BEZPEČNOSTNÝCH AKTÍV

Discover all devices

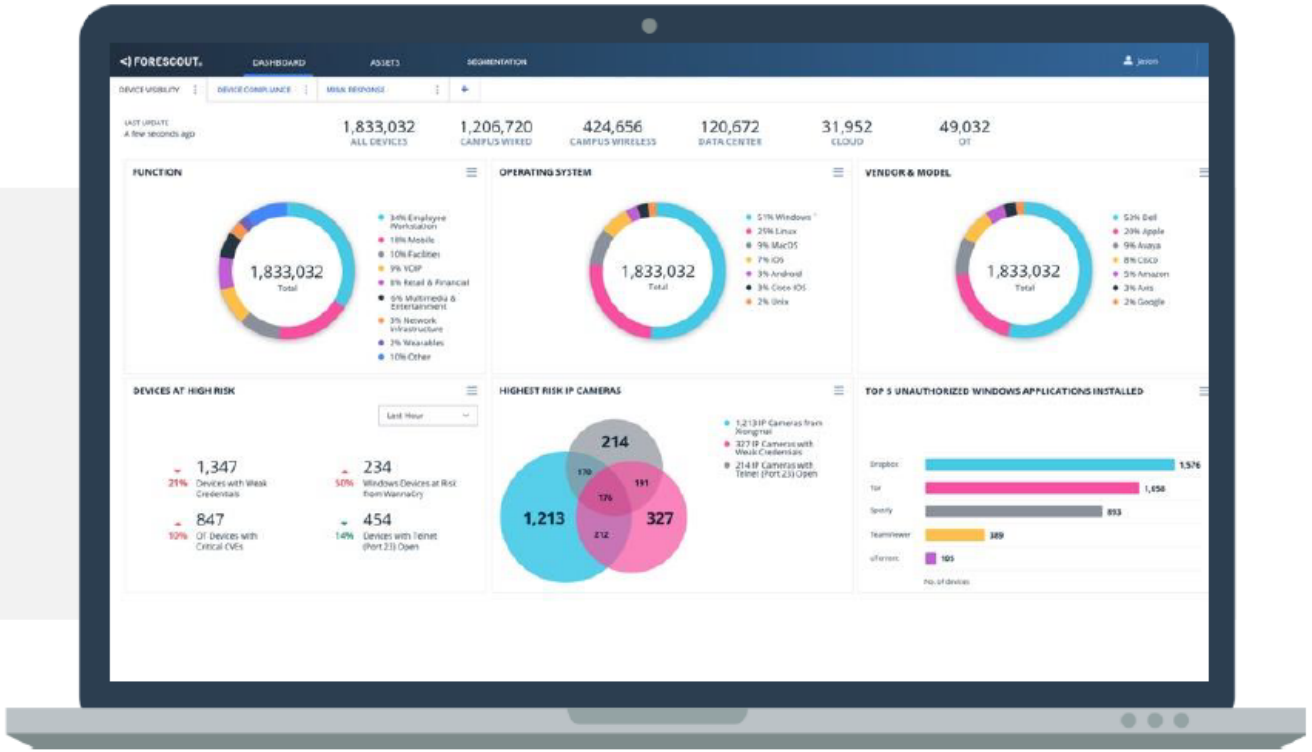
Inventory of all connected cyber assets with the industries most robust choice of 30+ techniques, without agents or disruption

Rich Context with High Fidelity

| Manufacturer | Model | MAC | IP | Serial Number | Firmware, OS | Software | Location | Vulnerabilities | Recalls | Traffic Analysis | Threat Detection | Risk Assessment |

Leverage insights

Derived from tens of millions of assets across many of the world's largest companies heavily targeted by threat actors



- **Globálne informácie o pripojených zariadeniach**
- **Plný kontext v jednej platforme**
- **Kontinuálne aktualizované informácie**

MOŽNOSTI OTESTOVANIA (PoC)

1. Inštalácia technológie v reálnej sieti
2. PCAP
3. Pasívna cesta – zoznam zariadení IoMT, ku ktorým by boli priradené aktuálne zraniteľnosti

Kritická zraniteľnosť Fortinet

Oznámenia a varovania Varovanie

9. októbra 2022

V produkte FortiOS a FortiProxy sa nachádza zraniteľnosť, ktorá môže umožniť vzdialenému a neoverenému útočníkovi obísť autentifikáciu administračného webového rozhrania.

Opis činnosti:

CVE-2021-40684 (CVSSv3 9.1)

Obídenie autentifikácie pomocou alternatívnej cesty alebo kanála vo FortiOS a FortiProxy môže umožniť neoverenému útočníkovi vykonávať operácie na administračnom rozhraní prostredníctvom špeciálne vytvorených požiadaviek HTTP alebo HTTPS," vysvetľuje Fortinet v dnes vydanom bulletine zákazníckej podpory.

Zraniteľné systémy:

FortiOS: 7.0.0 do 7.0.6 / 7.2.0 do 7.2.1
FortiProxy: od 7.0.0 do 7.0.6 a 7.2.0

Opravená verzia: 7.2.2

Závažnosť zraniteľnosti: Kritická

Možné škody:

- **Kompromitácia firewallu Fortinet**
- **Vzdialené vykonávanie kódu**
- **Kompromitácia siete organizácie**

Odporúčania:

V rámci prevencie útokov odporúčame skryť administrátorský portál za VPN a aktualizovať firmvér na opravenú verziu.

Odkazy:

https://cwe.mitre.org/data/definitions/88.html

Nahlásiť incident

Nahlásiť zraniteľnosť

Registrácia Achilles

Aktuality

22. septembra 2022
Mesačná správa CSIRT.SK – August 2022

9. septembra 2022
Mesačný prehľad kritických zraniteľností august 2022

15. augusta 2022
Mesačná správa CSIRT.SK – Júl 2022

Oznámenia a varovania

9. októbra 2022
Kritická zraniteľnosť Fortinet

9. októbra 2022
Závažné zraniteľnosti vo firmvéri BIOS na zariadeniach Lenovo

Opatření pro zabránění nebo zmírnění dopadů kybernetického bezpečnostního incidentu v souvislosti s obsahem varování

1.1 Základní informace k doporučeným úkonům uvedeným ve varování

1.1.1	Mimořádně upozornit uživatele o hrozbách spear-phishingu a připojit výzvu, aby se uživatelé, kteří v posledních dnech otevřeli podezřelé přílohy, obrátili na správce infrastruktury a dále upozornit uživatele na možnost „maskování“ spustitelných souborů v phishingu, např. „obrazek.png.exe“, „text.txt.exe“, „dokument.pdf.exe“ apod.
1.1.2	Zabránit pomocí centrálního nastavení spouštění aktivního obsahu a maker, zejména v .doc a .docx dokumentech
1.1.3	Okamžitě zablokovat vzdálené přístupy do infrastruktury a zablokovat otevřené služby do veřejné sítě, vyjma těch nezbytně nutných (veřejné IP rozsahy lze zkontrolovat v dostupných vyhledávačích zařízení připojených do sítě a zjistit tak i historicky otevřené či zapomenuté porty, nebo služby dostupné z veřejné sítě)
1.1.4	Okamžitě vytvořit offline zálohy a postupovat v zálohování dle důležitosti dat v organizaci
1.1.5	Zkontrolovat konzistenci již vytvořených záloh
1.1.6	Aktualizovat antivirové řešení v infrastruktuře

1.2 Další doporučení, která lze provést pro zabránění nebo zmírnění dopadů kybernetického bezpečnostního incidentu

1.2.1	V rámci systémů provést změnu hesel u privilegovaných účtů. Překontrolovat a popřípadě nastavit vhodnou politiku pro využití privilegovaných účtů.
1.2.2	Ověřit a zajistit, že systém záloh je od ostatních systémů oddělen tak, že ani získání nejvyššího oprávnění k systému, který je zálohován, nemůže umožnit smazání záloh.
1.2.3	Zamezit přístup a propojení mezi systémy důležitými pro zajištění fungování organizace a systémy nebo sítěmi, které nejsou důležité pro poskytování služeb nebo bezpečnost systému.
1.2.4	Zkontrolovat segmentaci sítě a řízení provozu mezi segmenty, situaci vyhodnotit a přijmout nezbytná opatření k zajištění alespoň elementární segmentace.
1.2.5	Zvážit aktualizaci všech používaných systémů, za podmínky, že bude taková aktualizace otestovaná. Pokud je aktualizace otestovaná a funkční, tak ji provést.
1.2.6	Prověřit platné plány kontinuity činnosti a havarijní plány související s provozováním systémů s cílem ověřit jejich platnost, účinnost a použitelnost zejména s ohledem na možnou nedostupnost těchto systémů.
1.2.7	Zajistit uchování plánů kontinuity činností a havarijních plánů souvisejících s provozováním systémů odděleně od systémů, pro které jsou tyto plány zpracovány (např. na odděleném paměťovém médiu, v tištěné podobě, apod.).
1.2.8	Pokud plány kontinuity činností a havarijní plány související s provozováním systémů nejsou aktuální či nebyly zpracovány, zpracovat tyto plány alespoň pro nekritičtější systémy důležité pro poskytování služeb.
1.2.9	Nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení Policie ČR nebo NÚKIB, a poučit o této povinnosti všechny administrátory a všechny relevantní bezpečnostní a IT (provozní) role.
1.2.10	Pouze pro poskytovatele zdravotních služeb: Vyčlenit komunikační síť lékařských přístrojů – modality (např.: CT, rentgeny), od zbytku sítě.
1.2.11	Obecná doporučení NÚKIB pro administrátory

https://www.nukib.cz/cs/uredni-deska/

Ďakujem za pozornosť