RAPID7

Rapid7 and Medigate

Delivering Full IoMT and IoT Visibility to SecOps

Superior Clinical Risk & Vulnerability Management

RAPID7

InsightVM, Rapid7's leading Vulnerability Management platform, directly discovers and assesses whether a connected device is open to known cybersecurity attacks. It does so by scanning the device and checking if certain vulnerabilities or misconfigurations can be successfully exploited on the device. In these ways, Rapid7 continues on its mission of closing the security achievement gap.

MEDIGATE

Medigate provides the leading healthcare IoT security platform, dedicated to protecting healthcare providers' clinical networks and delivering safer connected care to patients. Medigate leverages passive scanners to identify medical and IoT devices via Deep Packet Inspection (DPI) techniques, which collect and parse network traffic and fingerprint all connected medical devices.

Superior Clinical Risk & Vulnerability Management

The Problem

Healthcare organizations need to assess everything in their network

- Risky to actively scan medical devices (and IoT)
- Hard to drive security action without clinical context

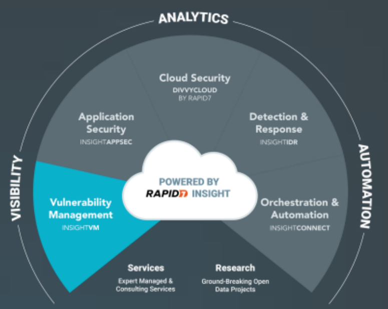
The Solution

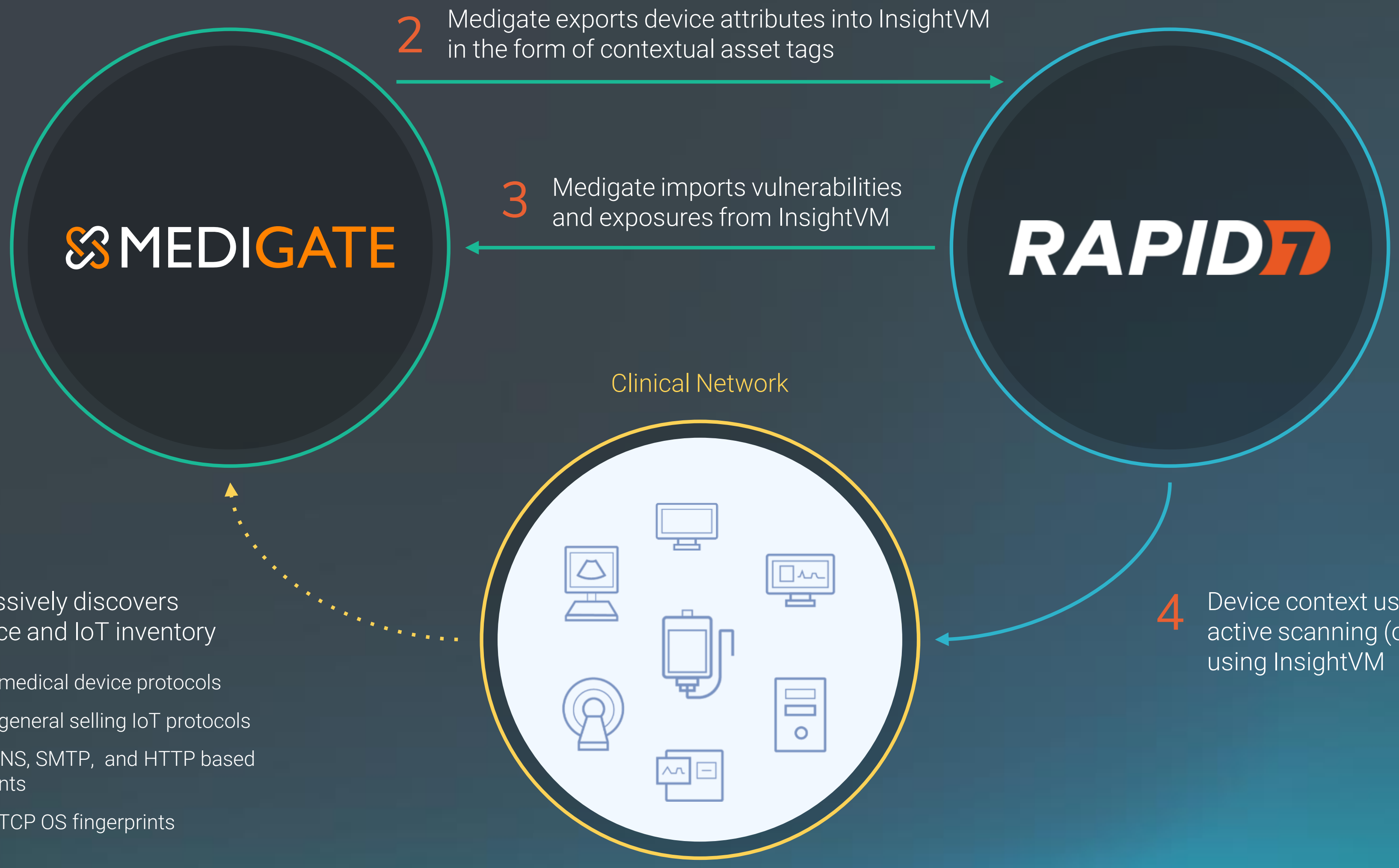
RAPID7 + MEDIGATE

- Full visibility into your hybrid environments
- Business context to make informed risk management decisions
- Perform safe, comprehensive scans
- Unify Information Security and Clinical/BioMed teams to drive actions

Rapid7 and Medigate bring safety and security together through visibility, assessment, and governance.

Integrated Solutions





2 Medigate exports device attributes into InsightVM in the form of contextual asset tags

3 Medigate imports vulnerabilities and exposures from InsightVM

Clinical Network

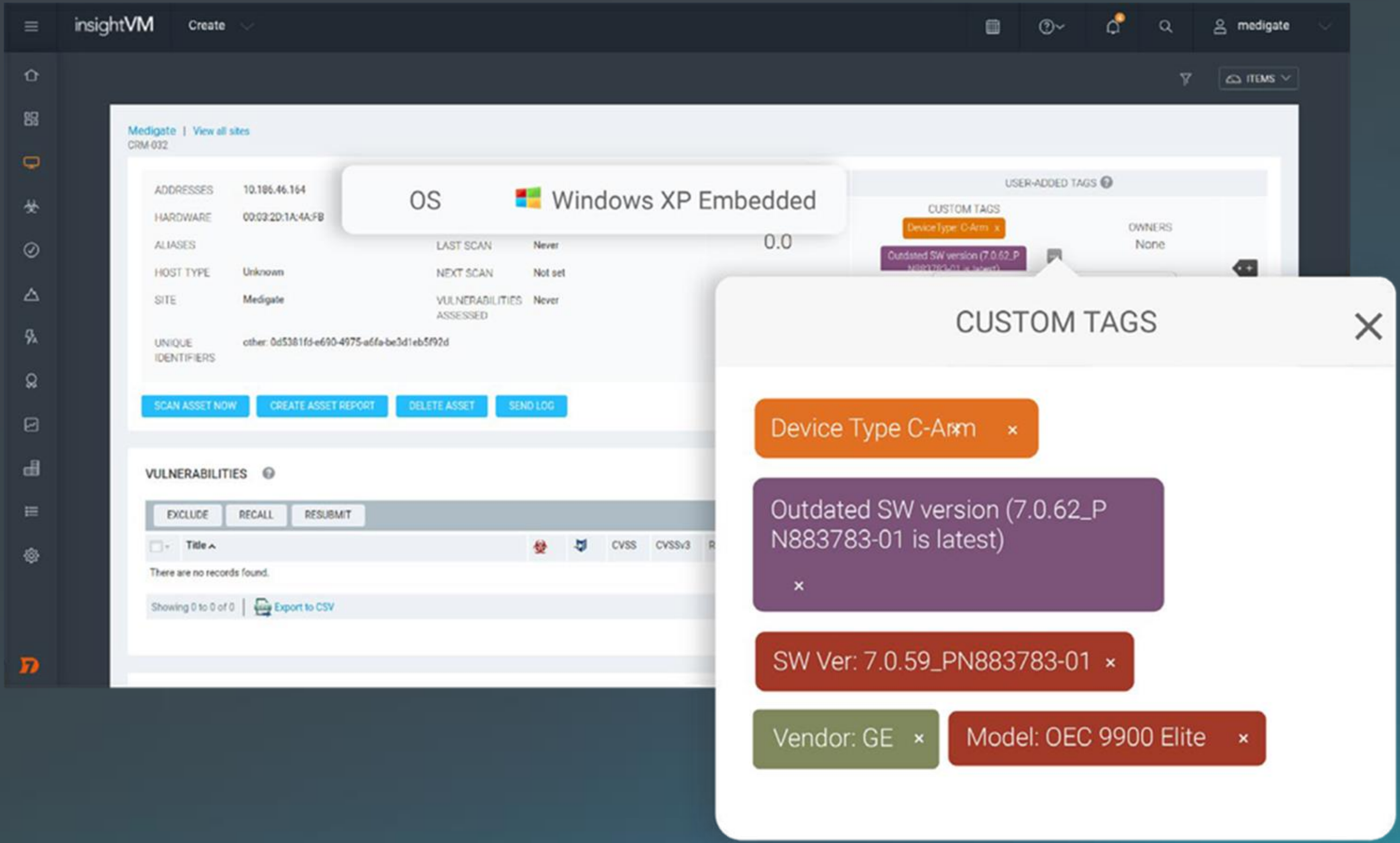
1 Medigate passively discovers medical device and IoT inventory

- Over 80 medical device protocols
- Over 40 general selling IoT protocols
- DHCP, DNS, SMTP, and HTTP based fingerprints
- General TCP OS fingerprints

4 Device context used to perform active scanning (or exclusions) using InsightVM

https://extensions.rapid7.com/extension/medigate_medical_iot_device_security_platform

Integration Screenshots



ADDRESSES 10.186.46.164

HARDWARE 00:03:2D:1A:4A:FB

ALIASES

HOST TYPE Unknown

SITE Medigate

UNIQUE IDENTIFIERS other: 0d5381fd-e690-4975-a6fa-be3d1eb5f92d

OS Windows XP Embedded

0.0

LAST SCAN Never

NEXT SCAN Not set

VULNERABILITIES ASSESSED Never

VULNERABILITIES

There are no records found.

Showing 0 to 0 of 0

CUSTOM TAGS

Device Type C-Arm ×

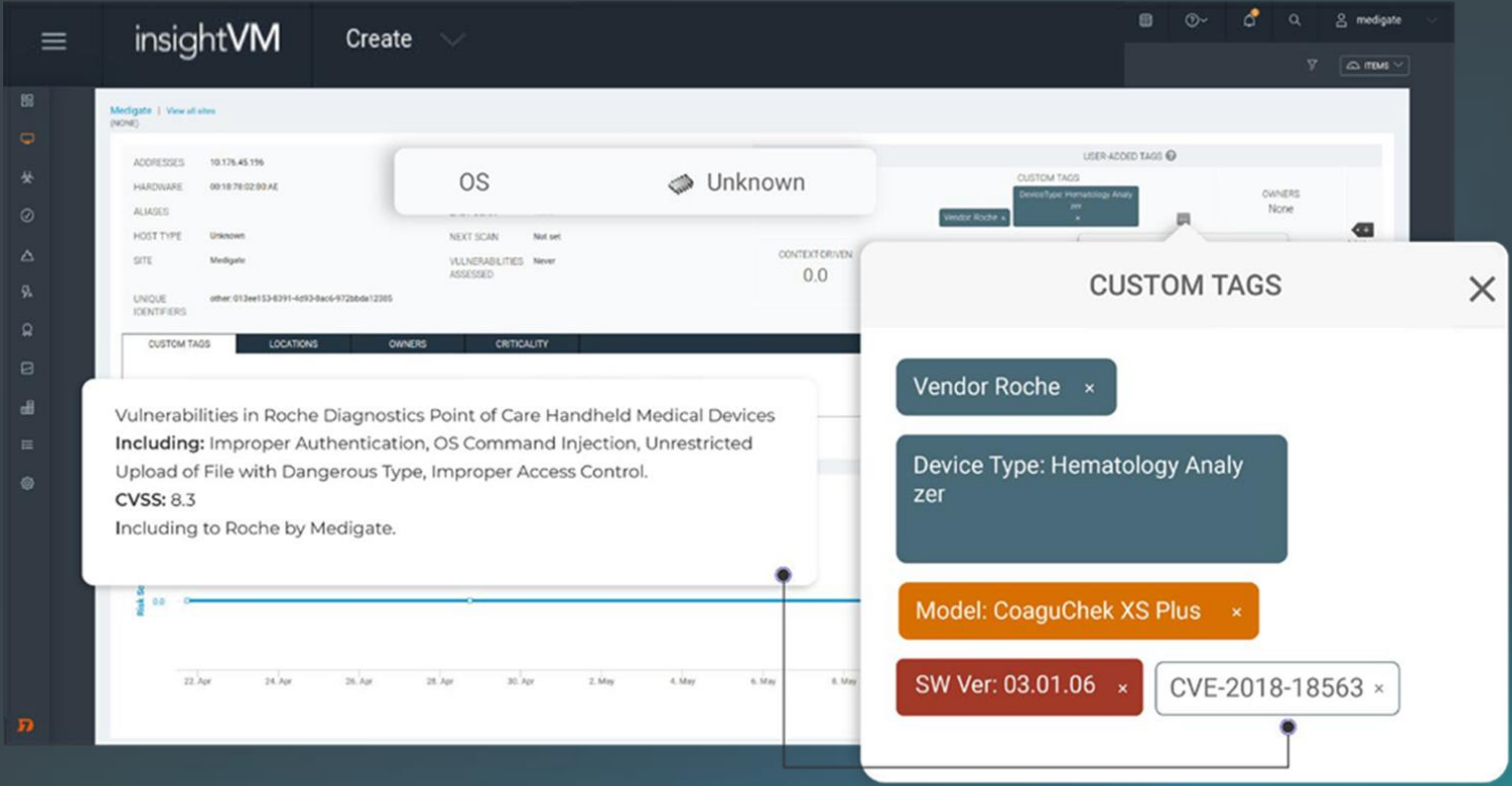
Outdated SW version (7.0.62_P N883783-01 is latest) ×

SW Ver: 7.0.59_PN883783-01 ×

Vendor: GE ×

Model: OEC 9900 Elite ×

Device information



ADDRESSES 10.176.45.196

HARDWARE 00:18:78:02:00:AE

ALIASES

HOST TYPE Unknown

SITE Medigate

UNIQUE IDENTIFIERS other: 013ee153-8391-4d93-8ac6-972bbda12385

NEXT SCAN Not set

VULNERABILITIES ASSESSED Never

CONTEXT DRIVEN 0.0

OS Unknown

CUSTOM TAGS: Vendor Roche × | DeviceType: Hematology Analyzer ×

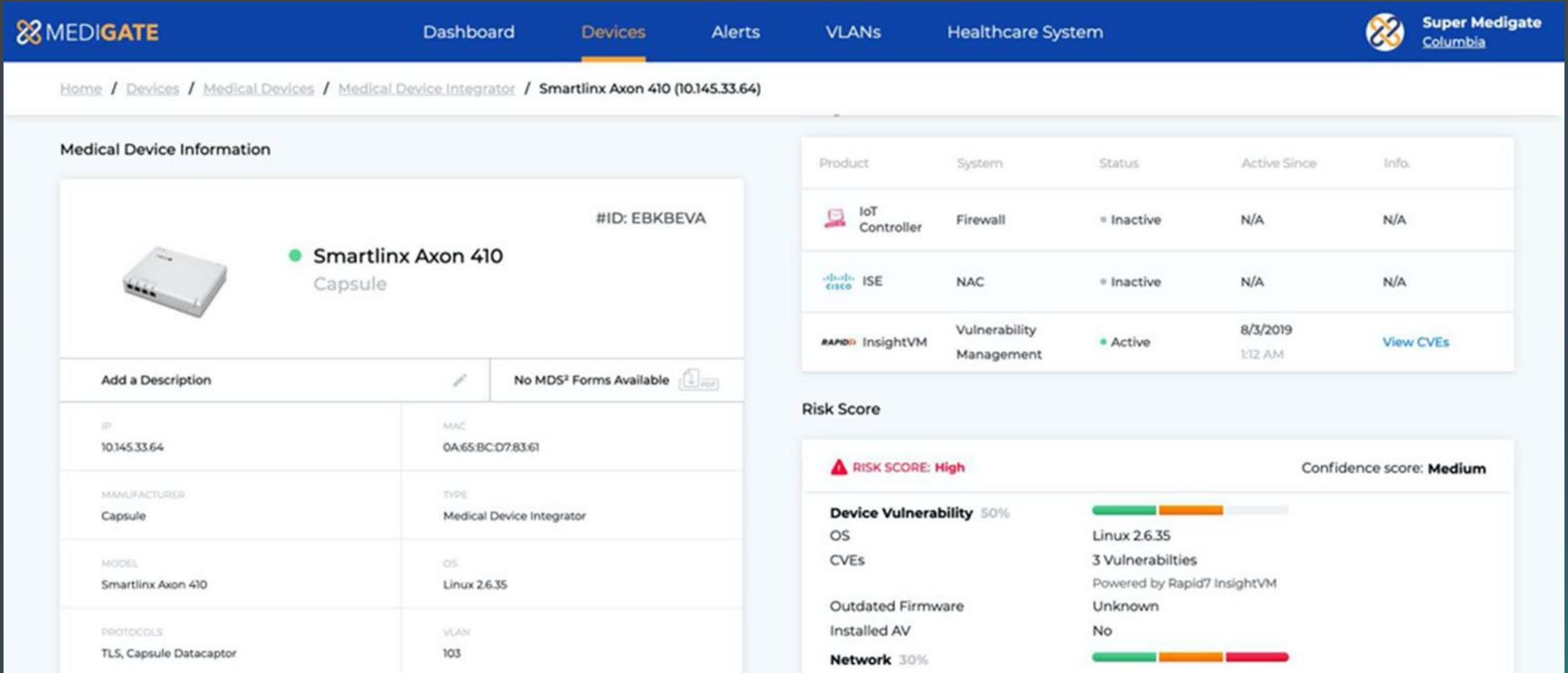
OWNERS None

Vulnerabilities in Roche Diagnostics Point of Care Handheld Medical Devices
Including: Improper Authentication, OS Command Injection, Unrestricted Upload of File with Dangerous Type, Improper Access Control.
CVSS: 8.3
Including to Roche by Medigate.

CUSTOM TAGS

- Vendor Roche ×
- Device Type: Hematology Analy zer
- Model: CoaguChek XS Plus ×
- SW Ver: 03.01.06 ×
- CVE-2018-18563 ×

Clinical CVEs



Home / Devices / Medical Devices / Medical Device Integrator / Smartlinx Axon 410 (10.145.33.64)

Medical Device Information

#ID: EBKBEVA

● Smartlinx Axon 410
Capsule

Add a Description

No MDS² Forms Available

IP 10.145.33.64	MAC 0A:65:BC:D7:83:61
MANUFACTURER Capsule	TYPE Medical Device Integrator
MODEL Smartlinx Axon 410	OS Linux 2.6.35
PROTOCOLS TLS, Capsule Datacaptor	VLAN 103

Product	System	Status	Active Since	Info.
IoT Controller	Firewall	● Inactive	N/A	N/A
ISE	NAC	● Inactive	N/A	N/A
RAPID7 InsightVM	Vulnerability Management	● Active	8/3/2019 1:12 AM	View CVEs

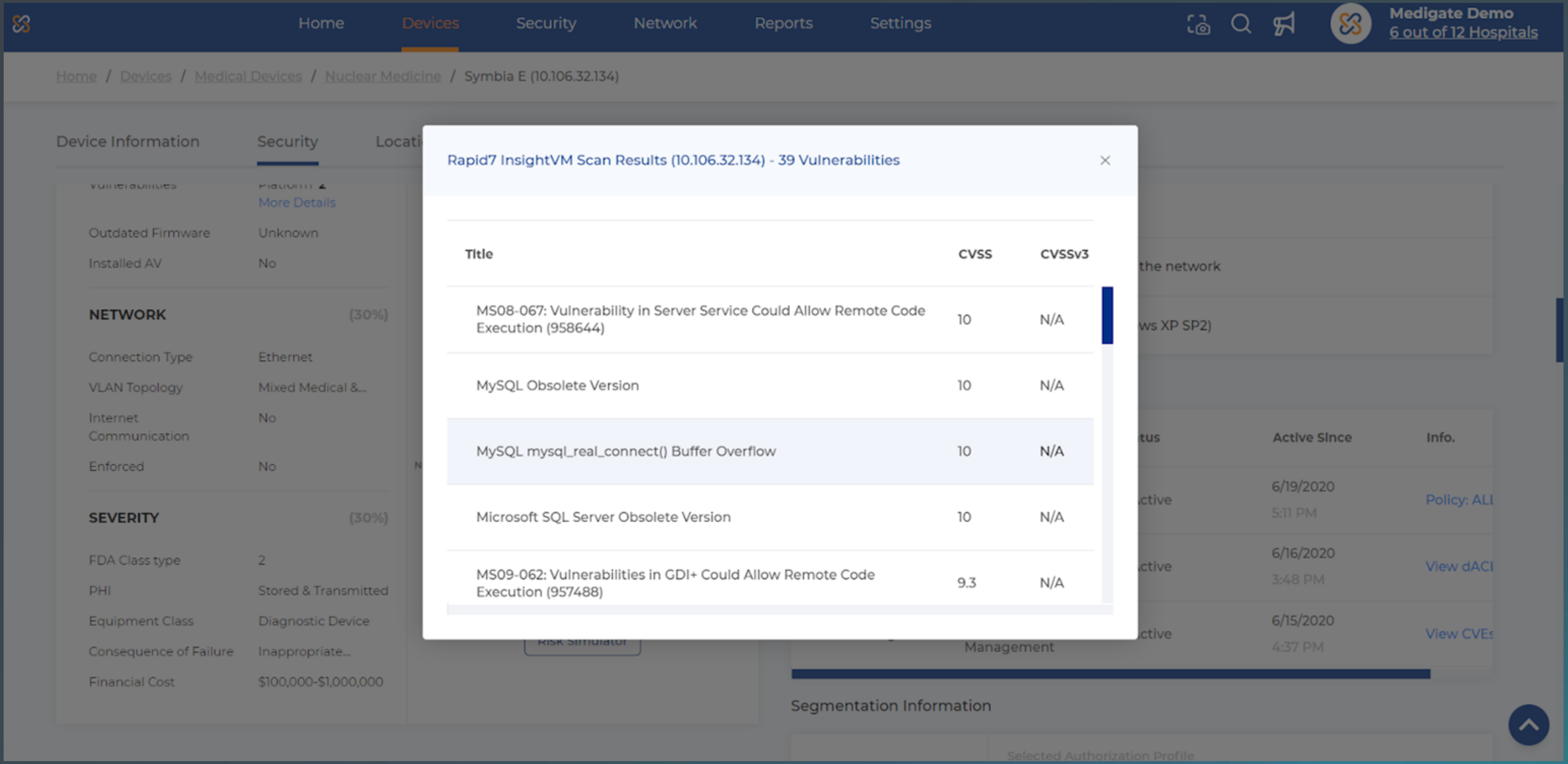
Risk Score

RISK SCORE: **High**

Confidence score: **Medium**

Device Vulnerability 50%	🟩🟧
OS	Linux 2.6.35
CVEs	3 Vulnerabilties Powered by Rapid7 InsightVM
Outdated Firmware	Unknown
Installed AV	No
Network 30%	🟩🟧🟥

Clinical Risk Score in Medigate



Home / Devices / Medical Devices / Nuclear Medicine / Symbia E (10.106.32.134)

Outdated Firmware	Unknown
Installed AV	No
NETWORK	(30%)
Connection Type	Ethernet
VLAN Topology	Mixed Medical &...
Internet Communication	No
Enforced	No
SEVERITY	(30%)
FDA Class type	2
PHI	Stored & Transmitted
Equipment Class	Diagnostic Device
Consequence of Failure	Inappropriate...
Financial Cost	$100,000-$1,000,000

Rapid7 InsightVM Scan Results (10.106.32.134) - 39 Vulnerabilities

Title	CVSS	CVSSv3
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	10	N/A
MySQL Obsolete Version	10	N/A
MySQL mysql_real_connect() Buffer Overflow	10	N/A
Microsoft SQL Server Obsolete Version	10	N/A
MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	9.3	N/A

...tus	Active Since	Info.
...ctive	6/19/2020 5:11 PM	Policy: ALL
...ctive	6/16/2020 3:48 PM	View dACL
...ctive	6/15/2020 4:37 PM	View CVEs

Segmentation Information

Selected Authorization Profile

InsightVM Scan Results in Medigate

RAPID7

Thank You.