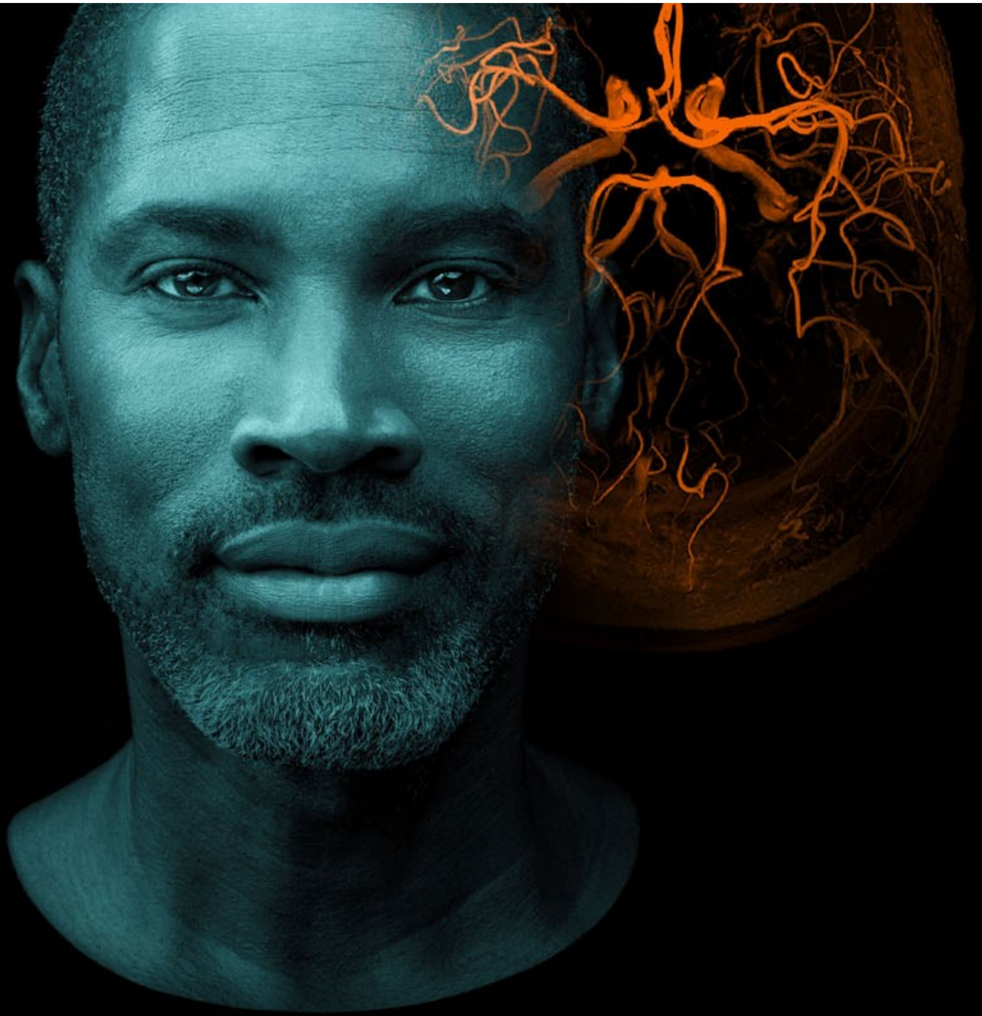
SIEMENS
Healthineers



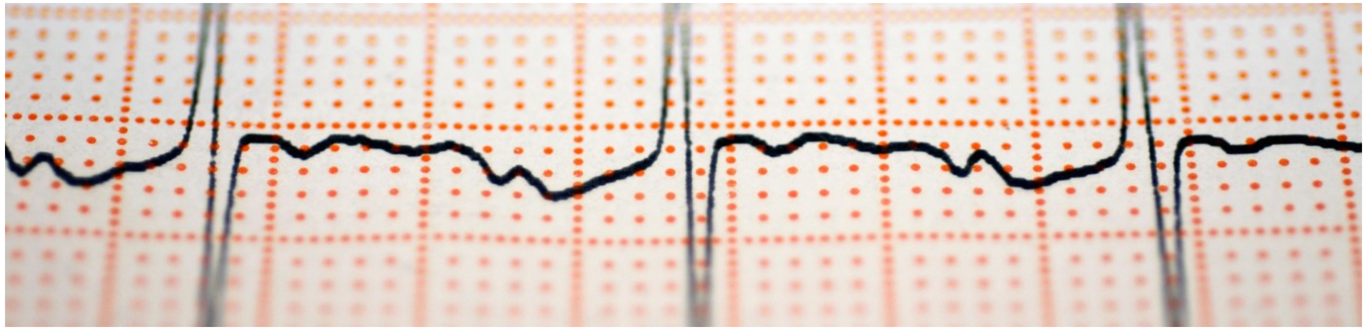
Prescribing more CyberHealth

Carlos Arglebe
Corporate Cybersecurity Officer
October 2022

Prescribing…

SIEMENS Healthineers

need
What do we have to do?
want



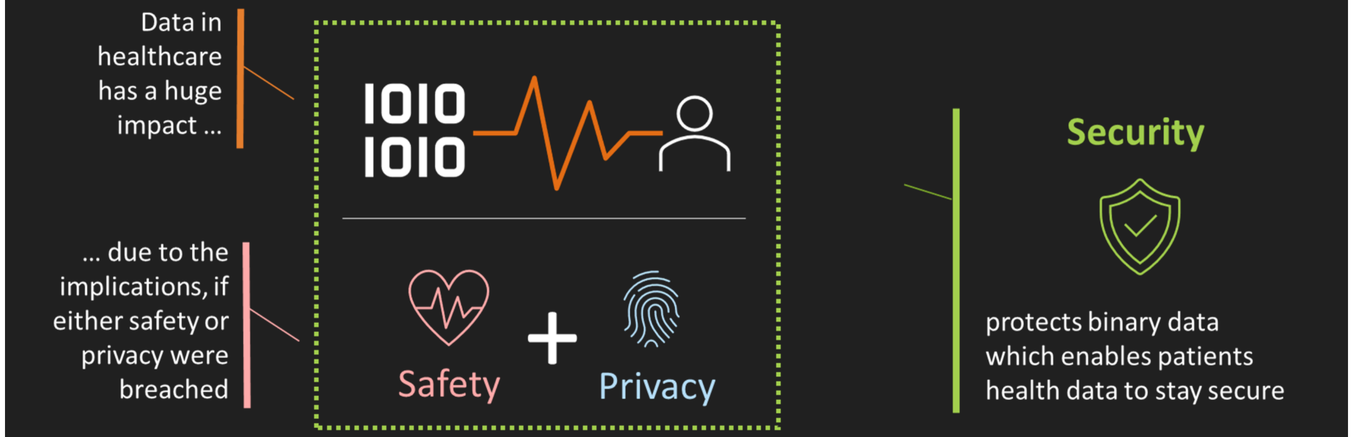
ISO 13485
ISO 27001
21 CFR 820
IVDR
MDR
GDPR
NIS 2.0
CRA
…

Healthcare has a long tradition with regulations and standards.

Cyber is complex and touches many specialties domains. Cybersecurity requires **integration and collaboration** across organizations.

Increasing regulations put more focus on Cyber with more requirements and impact (financial & reputational)

Cybersecurity is the new kid on the block enabling safety, privacy and the provision of healthcare



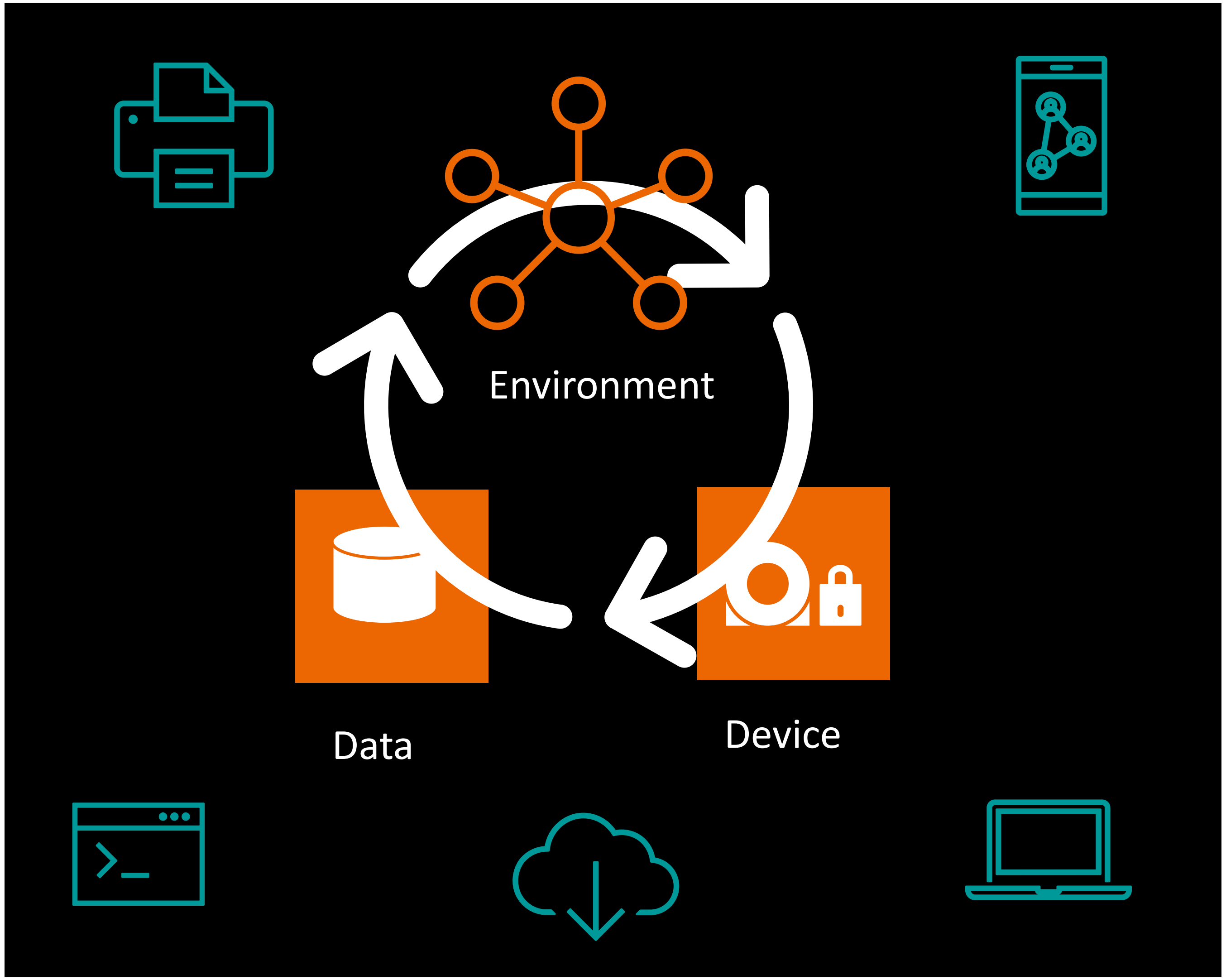
Data in healthcare has a huge impact …

… due to the implications, if either safety or privacy were breached

Security

protects binary data which enables patients health data to stay secure

more



Medical device lifecyLe
5-15 years

Operating Systems
5 years mainstream +
5 years extended support

Software components
<5 years

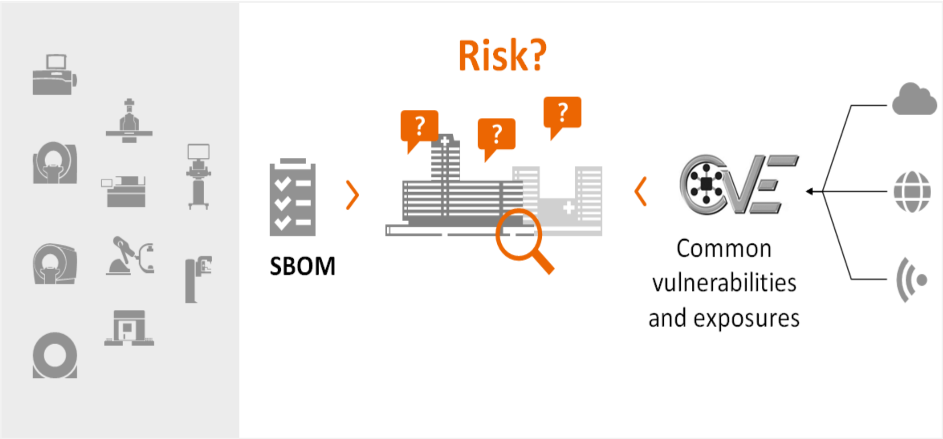
We need to move beyond a **device** centric protection and follow the **data** across the **environment**(s)

CyberHealth

Confidentiality

Integrity

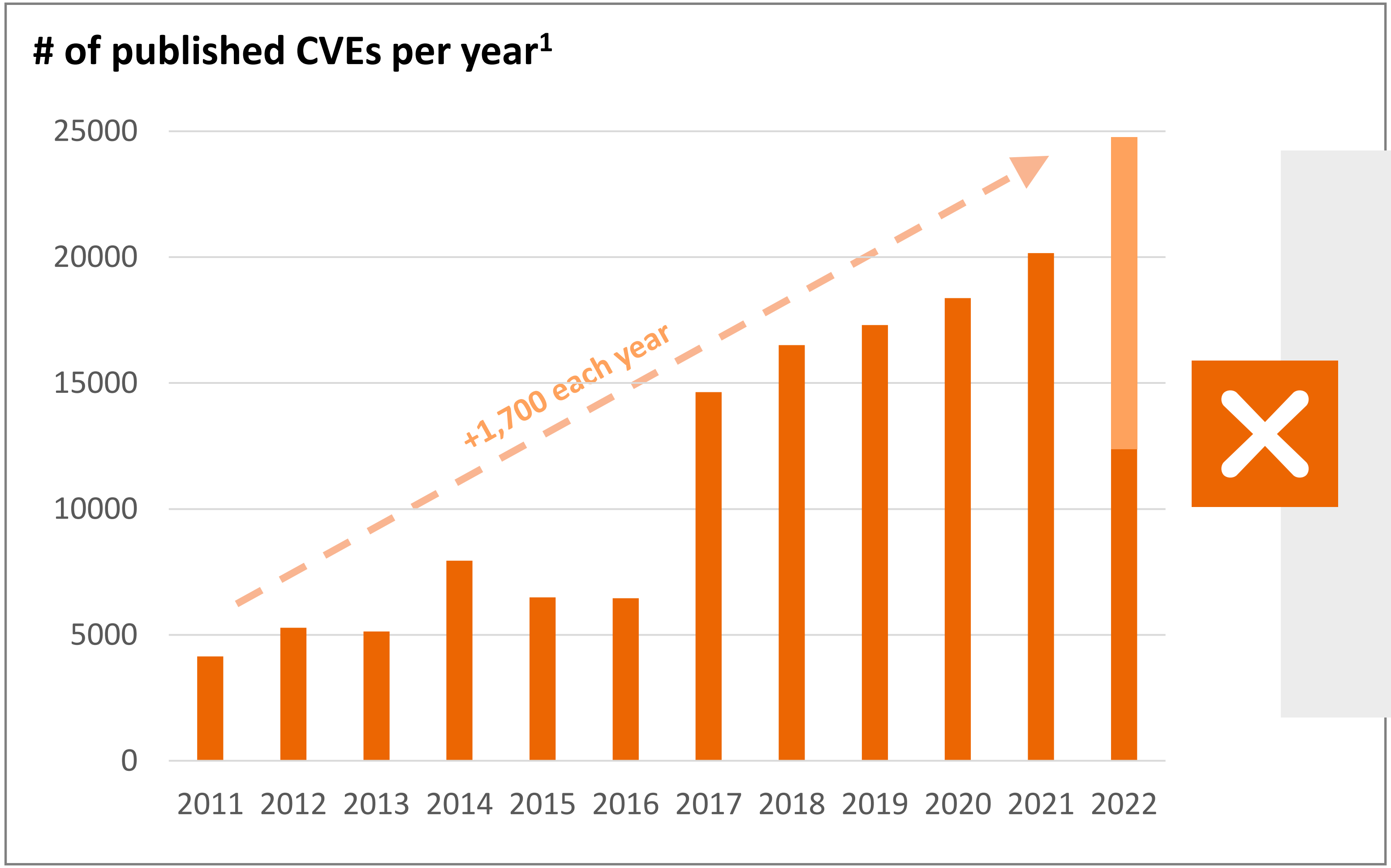
Availability



- ✓ Compliant medical devices
- ✓ Controlled changes
- ✓ Timely updates
- ✓ Secured IT environment
- ✓ Protected Information

Labeling
Training
Certification
Incident Reporting
…

Factors influencing the number of vulnerabilities a manufacturer must evaluate



×

# of products

—

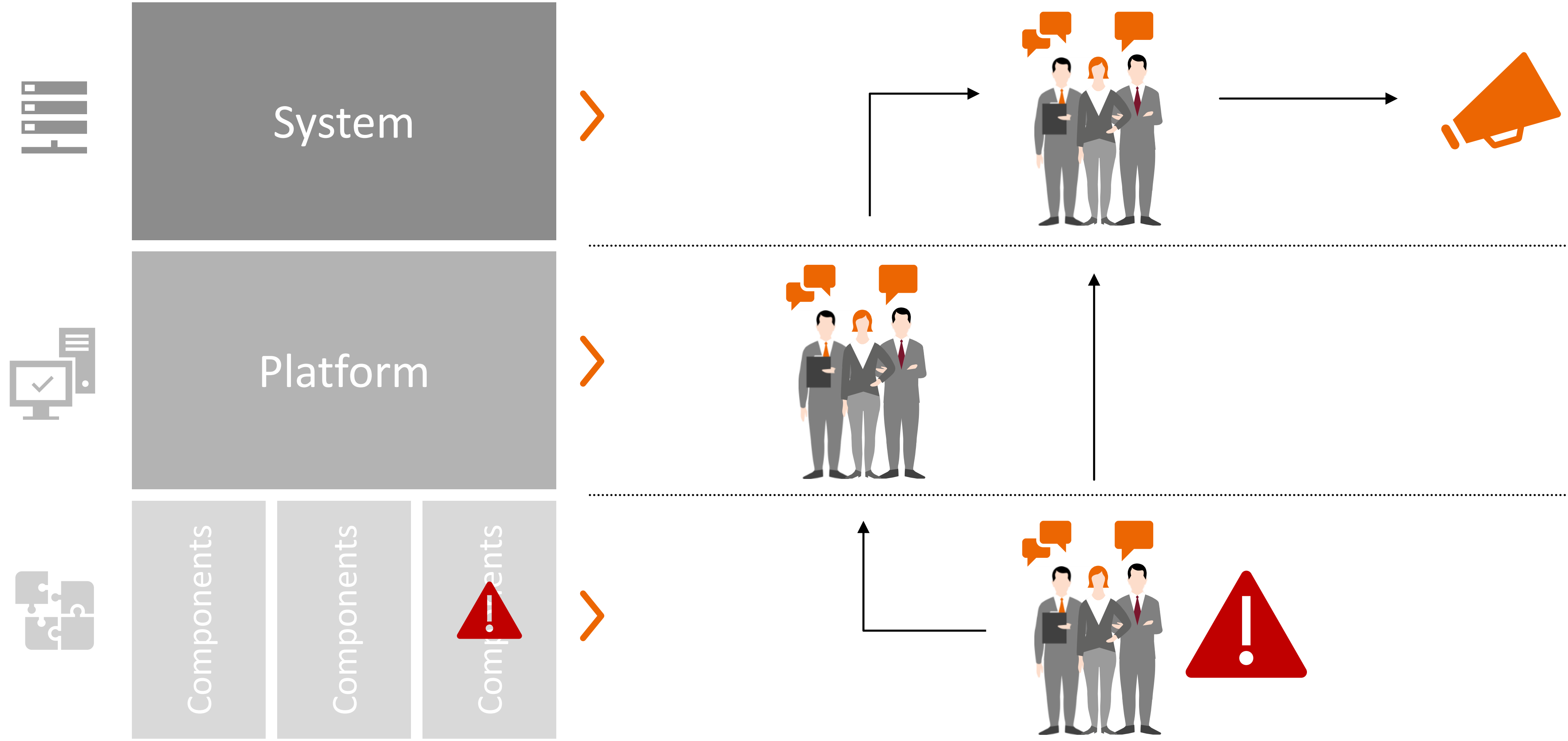
# of components in one product

—

# of occurrences of the same CVE in different sub-components

[1] https://www.cve.org/About/Metrics (final value for 2022 extrapolated from Q2 data)

System level impact of a component vulnerability is determined by an architecture aware evaluation workflow



System

Platform

Components

Components

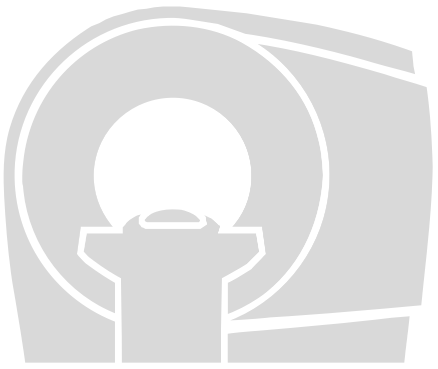
Components

Design and implementation knowledge-aware evaluation of security notifications results in system-level risk information[1]

Vulnerable and needs to be patched.

Vulnerable but not exploitable if operated as mandated.

Vulnerable but not exploitable due to mitigating controls.

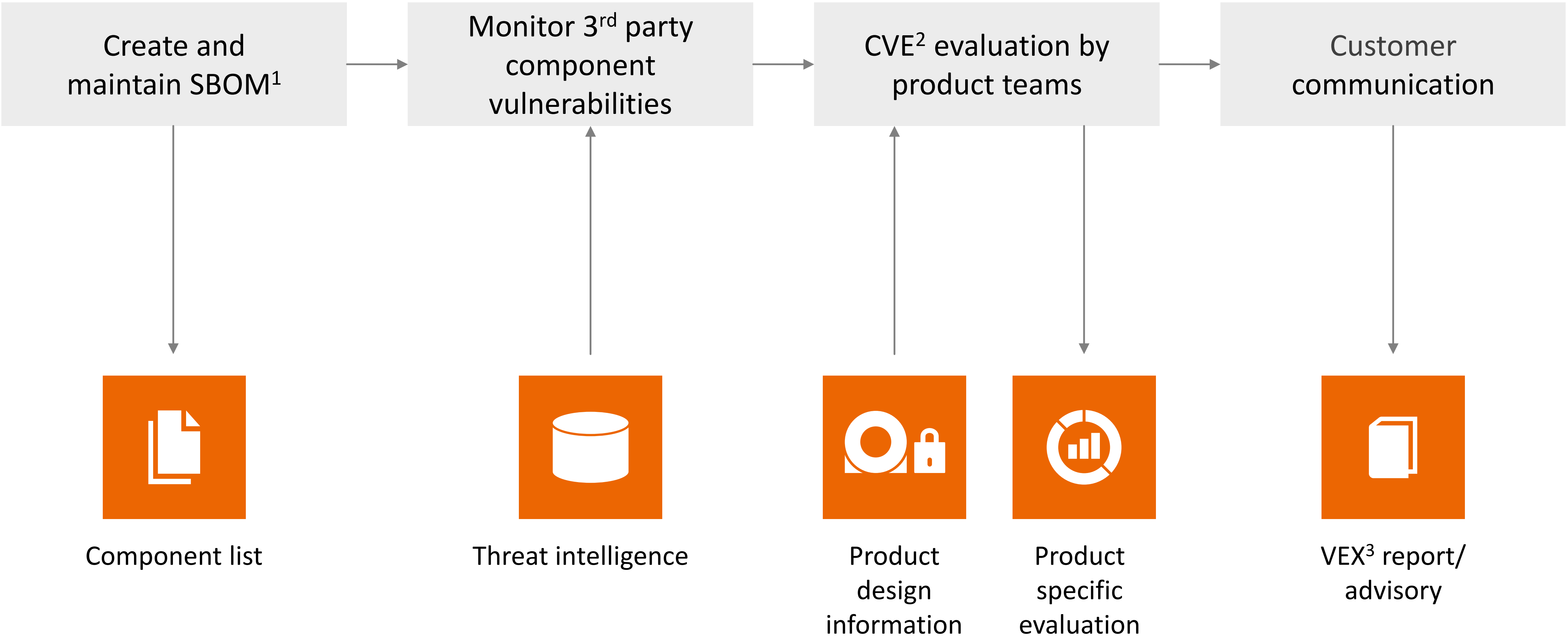


Not vulnerable, since defective part of the technology not in use.

[1] The upcoming standard for communication of vulnerabilities is VEX (Vulnerability Exploitability eXchange) driven by CISA, https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Aprill2022.pdf

Approach to fulfill regulatory requirements for vulnerability management by the manufacturer

SIEMENS Healthineers



Create and maintain SBOM[1]

Monitor 3rd party component vulnerabilities

CVE[2] evaluation by product teams

Customer communication

Component list

Threat intelligence

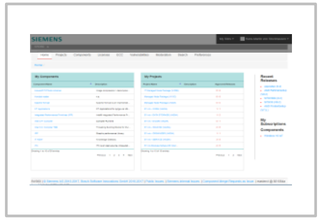
Product design information

Product specific evaluation

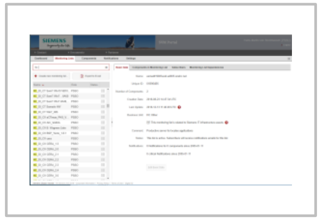
VEX[3] report/ advisory

[1] Software Bill Of Materials (SBOM)
[2] Common Vulnerabilities and Exposures (CVE)
[3] Vulnerability Exploitability eXchange (VEX)

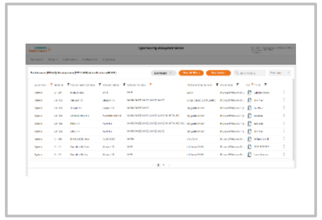
Effective vulnerability management requires a product inventory, threat intelligence, and targeted clinical operator communication



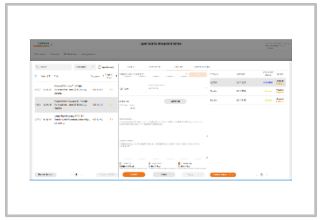
Components and product definitions



Threat intelligence

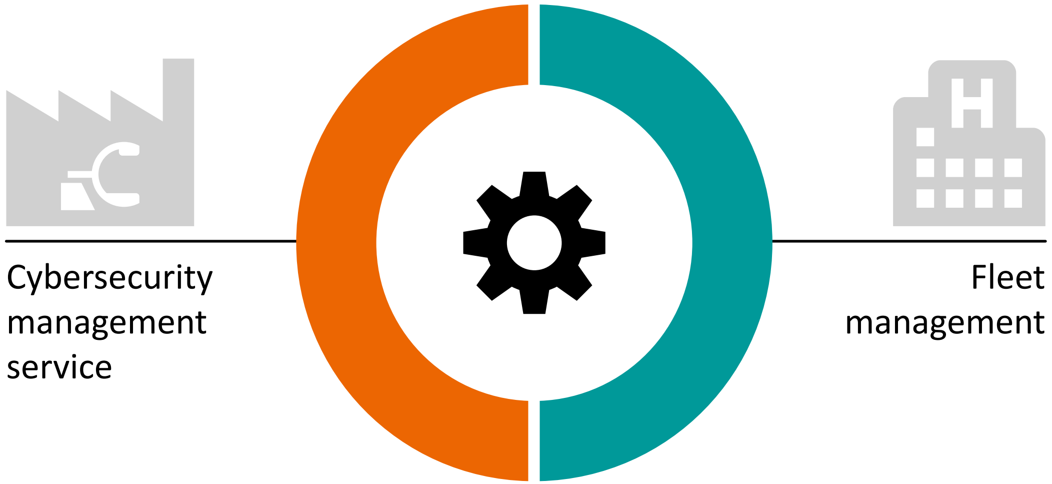


Product Security inventory



Notification evaluation workflow

Mastering the post Post-Market challenge together with data

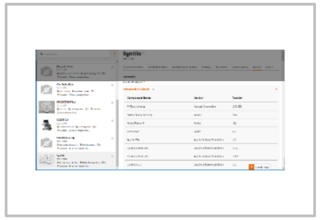


Cybersecurity management service

Fleet management

Shared responsibility for patient safety

Whitepaper and SBOM[1]



Fleet specific notifications

System specific evaluation

[1] Software Bill of Materials

We win together…and support the protection of our customers to secure their operations

Various security options for **shared responsibility** on **medical device security**[1]

Technology

We deliver built-in security for our portfolio:

- Secure configuration and hardening
- Data encryption
- Trusted machine certificates
- …

Installed base is being secured incl. various security options (e.g. upgrades, evolve program, elevate, security appliance).

Processes

Customers rely on and require our information:

- Cybersecurity whitepaper[4]
- Secure environment configuration recommendation
- …

Our capabilities are key for our customers:

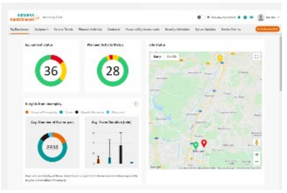
- Secure Development Lifecycle
- Regular Cybersecurity updates
- Security advisories
- Coordinated Vulnerability Disclosure

People

Data empowers people:

Our Industry-leading installed base security management gives customers full transparency on the security status of their fleet.

14.380 published vulnerabilities from January – September 2022 [2]



Personalized view in teamplay fleet

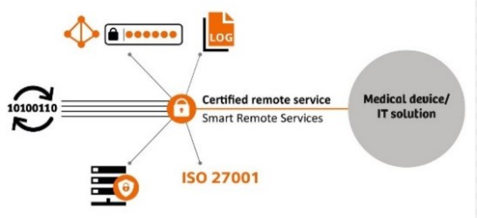
Cybersecurity **certification is key**

In the past customers compared functionality:

What do you deliver?

Today they check more if they can **trust us** and look at our organization:

How do you do it?



Our ISO 27001 certifications[3] are growing in relevance for customers

[1] Medical Device Guidance by US Regulator Food and Drug Administration (FDA)
[2] Published vulnerabilities affecting components in our products
[3] incl. ISO 27701 for Data Privacy
[4] incl. Software Bill of Materials (SBOM), Manufacturer Disclosure Statement for Medical Device Security (MDS2)

Prescribing more CyberHealth

Advise measures …in addition… for more resilience

Strengthening **cyber resilience** in healthcare
as **shared responsibility for patient safety**

Thank you

for your enthusiasm!

Siemens Healthineers
Siemens Healthcare GmbH
Hartmannstrasse 17
91052 Erlangen, Germany