# infoteam Software

## CySecMed 2022

# Das Big Picture für Cyber-Security in der Medizintechnik

## Organisatorische Maßnahmen
Verantwortung der Leitung – CS Policy – CS Goals
Einführung und Implementierung ISMS/ IEC 27001
DSGVO- Checkliste
Asset Management

## Mitarbeiter-Awareness
Aus- und Weiterbildung
Phishing-Mails
Denken wie ein Hacker

## Prozessuale Maßnahmen
Attack Surface Reduction
Härten von Entwicklungsprozessen
Secure Product Development Life Cycle
Härten von Produktionsprozessen
Härten von Zulieferketten und -produkten

## Normen und Gesetze
EU-MDR/ EU- IVDR
IEC 81001-5-1
60601-4-5/ 62443
AAMI TIR57
FDA
DiGAV
Überwachung und Benannte Stellen

## Risiko-Beherrschende Maßnahmen
Integriertes RM Safety & Security
Wechselwirkungen, Risk Control Options: Inherent oder System oder Produktion
Implementierung von Risikomindernde Maßnahmen

## State of the art
Codierrichtlinien
Internetplattformen
CVE, OWASP, CWE, MITRE, ATT&CK
SBoM
Integration von Checks aus CVE-DB
Schwachstellenmanagement
(Versionen von IT-Komponenten)

## Technische Maßnahmen
Architektur und Design (Datenminimierung, Rechtevergabe, Update-Planung, Segregation …)
Defense in Depth
Code-Signierung
IT-Struktur

## Permanente Wachsamkeit/ Vigilanz
CAPA
Audit Trail
Product Security Incident Response Team (PSIRT)
Pre-Market- Surveillance
Post-Market-Surveillance

## Überwachungs-Maßnahmen
SOUP-Monitoring
Schwachstellen-Monitoring
Penetrationtests
Tools und Angebot des Einsatzes

# Das Big Picture für Cyber-Security in der Medizintechnik

## Organisatorische Maßnahmen
Verantwortung der Leitung – CS Policy – CS Goals
Einführung und Implementierung ISMS/ IEC 27001
DSGVO- Checkliste
Asset Management

1

## Mitarbeiter-Awareness
Aus- und Weiterbildung
Phishing-Mails
Denken wie ein Hacker

2

## Prozessuale Maßnahmen
Attack Surface Reduction
Härten von Entwicklungsprozessen
Secure Product Development Life Cycle
Härten von Produktionsprozessen
Härten von Zulieferketten und -produkten

3

## Normen und Gesetze
EU-MDR/ EU- IVDR
IEC 81001-5-1
60601-4-5/ 62443
AAMI TIR57
FDA
DiGAV
Überwachung und Benannte Stellen

4

## Risiko-Beherrschende Maßnahmen
Integriertes RM Safety & Security
Wechselwirkungen, Risk Control Options: Inherent oder System oder Produktion
Implementierung von Risikomindernde Maßnahmen

5

## State of the art
Codierrichtlinien
Internetplattformen
CVE, OWASP, CWE, MITRE, ATT&CK
SBoM
Integration von Checks aus CVE-DB
Schwachstellenmanagement
(Versionen von IT-Komponenten)

6

## Technische Maßnahmen
Architektur und Design (Datenminimierung, Rechtevergabe, Update-Planung, Segregation …)
Defense in Depth
Code-Signierung
IT-Struktur

7

## Permanente Wachsamkeit/ Vigilanz
CAPA
Audit Trail
Product Security Incident Response Team (PSIRT)
Pre-Market- Surveillance
Post-Marke ce

8

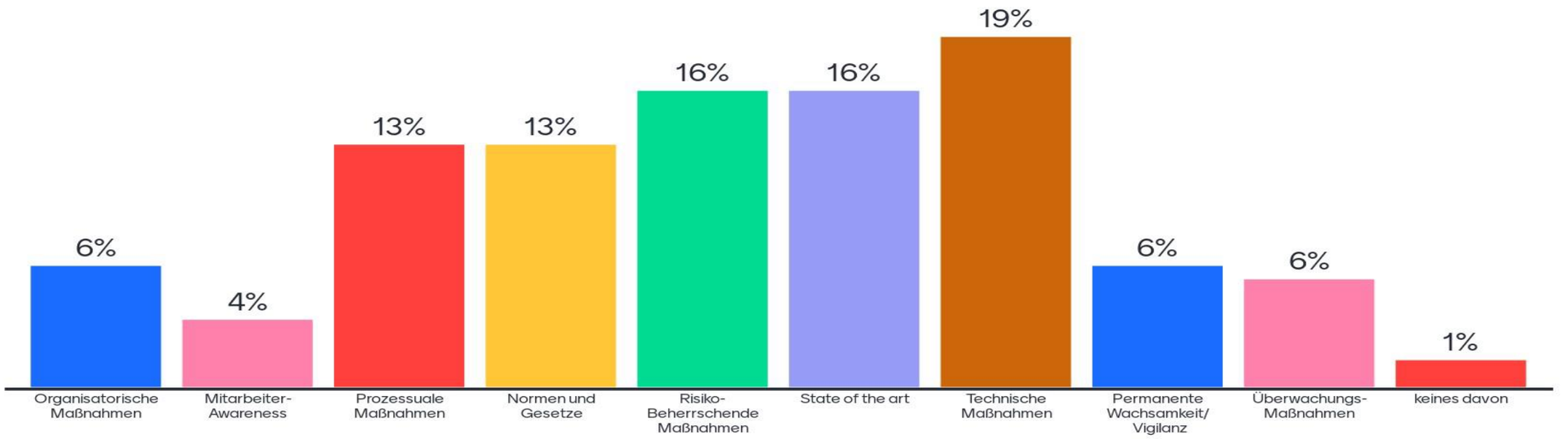
## Überwachungs-Maßnahmen
SOUP-Monitoring
Schwachstellen-Monitoring
Penetrationtests
Tools und Angebot des Einsatzes

9

# Aus diesen Bereichen kommen die Teilnehmer

## Das Big Picture für Cyber-Security in der Medizintechnik

Mentimeter




48

# Das Big Picture für Cyber-Security in der Medizintechnik – Konferenztag 1

## Organisatorische Maßnahmen
Verantwortung der Leitung – CS Policy – CS Goals
Einführung und Implementierung ISMS/ IEC 27001
DSGVO- Checkliste
Asset Management

Vortrag von Daniel Mesereit

## Mitarbeiter-Awareness
Aus- und Weiterbildung
Phishing-Mails
Denken wie ein Hacker

Vortrag von Urs Anliker und Torben Rühl

Vortrag von Lukas Fey

## Prozessuale Maßnahmen
Attack Surface Reduction
Härten von Entwicklungsprozessen
Secure Product Development Life Cycle
Härten von Produktionsprozessen
Härten von Zulieferketten und -produkten

infoteam software

## Normen und Gesetze
EU-MDR/ EU- IVDR
IEC 81001-5-1
60601-4-5/ 62443
AAMI TIR57
FDA
DiGAV
Überwachung und Benannte Stellen

Vortrag von Jan Küfner

## Risiko-Beherrschende Maßnahmen
Integriertes RM Safety & Security
Wechselwirkungen, Risk Control Options: Inherent oder System oder Produktion
Implementierung von Risikomindernde Maßnahmen

Vortrag von Alastair Walker

## State of the art
Codierrichtlinien
Internetplattformen
CVE, OWASP, CWE, MITRE, ATT&CK
SBoM
Integration von Checks aus CVE-DB
Schwachstellenmanagement
(Versionen von IT-Komponenten)

## Technische Maßnahmen
Architektur und Design (Datenminimierung, Rechtevergabe, Update-Planung, Segregation …)
Defense in Depth
Code-Signierung
IT-Struktur

Vortrag von Gerd Dautel

## Permanente Wachsamkeit/ Vigilanz
CAPA
Audit Trail
Product Security Incident Response Team (PSIRT)
Pre-Market- Surveillance
Post-Market-Surveillance

## Überwachungs-Maßnahmen
SOUP-Monitoring
Schwachstellen-Monitoring
Penetrationtests
Tools und Angebot des Einsatzes

Vortrag von Lars Kriesel

# Das Big Picture für Cyber-Security in der Medizintechnik – Konferenztag 2

## Organisatorische Maßnahmen
Verantwortung der Leitung – CS Policy – CS Goals
Einführung und Implementierung ISMS/ IEC 27001
DSGVO- Checkliste
Asset Management

Vortrag von Martin Neumann und Wolfgang Merz

## Mitarbeiter-Awareness
Aus- und Weiterbildung
Phishing-Mails
Denken wie ein Hacker

Vortrag von Oliver Brahmstädt

## Prozessuale Maßnahmen
Attack Surface Reduction
Härten von Entwicklungsprozessen
Secure Product Development Life Cycle
Härten von Produktionsprozessen
Härten von Zulieferketten und -produkten

## Normen und Gesetze
EU-MDR/ EU- IVDR
IEC 81001-5-1
60601-4-5/ 62443
AAMI TIR57
FDA
DiGAV
Überwachung und Benannte Stellen

## Risiko-Beherrschende Maßnahmen
Integriertes RM Safety & Security
Wechselwirkungen, Risk Control Options: Inherent oder System oder Produktion
Implementierung von Risikomindernde Maßnahmen

Vortrag von Sebastian Wittor

Vortrag von Hans Wenner

## State of the art
Codierrichtlinien
Internetplattformen
CVE, OWASP, CWE, MITRE, ATT&CK
SBoM
Integration von Checks aus CVE-DB
Schwachstellenmanagement
(Versionen von IT-Komponenten)

Vortrag von Frank Büchner

Vortrag von Georg Heidenreich

## Technische Maßnahmen
Architektur und Design (Datenminimierung, Rechtevergabe, Update-Planung, Segregation …)
Defense in Depth
Code-Signierung
IT-Struktur

## Permanente Wachsamkeit/ Vigilanz
CAPA
Audit Trail
Product Security Incident Response Team (PSIRT)
Pre-Market- Surveillance
Post-Market-Surveillance

## Überwachungs-Maßnahmen
SOUP-Monitoring
Schwachstellen-Monitoring
Penetrationtests
Tools und Angebot des Einsatzes

# Das Big Picture für Cyber-Security in der Medizintechnik – Gesamte Konferenz

## Organisatorische Maßnahmen
Verantwortung der Leitung – CS Policy – CS Goals
Einführung und Implementierung ISMS/ IEC 27001
DSGVO- Checkliste
Asset Management

Vortrag von Daniel Mesereit

Vortrag von Martin Neumann und Wolfgang Merz

## Mitarbeiter-Awareness
Aus- und Weiterbildung
Phishing-Mails
Denken wie ein Hacker

Vortrag von Oliver Brahmstädt

Vortrag von Urs Anliker und Torben Rühl

Vortrag von Lukas Fey

## Prozessuale Maßnahmen
Attack Surface Reduction
Härten von Entwicklungsprozessen
Secure Product Development Life Cycle
Härten von Produktionsprozessen
Härten von Zulieferketten und -produkten

## Normen und Gesetze
EU-MDR/ EU- IVDR
IEC 81001-5-1
60601-4-5/ 62443
AAMI TIR57
FDA
DiGAV
Überwachung und Benannte Stellen

Vortrag von Jan Küfner

## Risiko-Beherrschende Maßnahmen
Integriertes RM Safety & Security
Wechselwirkungen, Risk Control Options: Inherent oder System oder Produktion
Implementierung von Risikomindernde Maßnahmen

Vortrag von Sebastian Wittor

Vortrag von Hans Wenner

## State of the art
Codierrichtlinien
Internetplattformen
CVE, OWASP, CWE, MITRE, ATT&CK
SBoM
Integration von Checks aus CVE-DB
Schwachstellenmanagement
(Versionen von IT-Komponenten)

Vortrag von Frank Büchner

Vortrag von Georg Heidenreich

## Technische Maßnahmen
Architektur und Design (Datenminimierung, Rechtevergabe, Update-Planung, Segregation …)
Defense in Depth
Code-Signierung
IT-Struktur

Vortrag von Gerd Dautel

## Permanente Wachsamkeit/ Vigilanz
CAPA
Audit Trail
Product Security Incident Response Team (PSIRT)
Pre-Market- Surveillance
Post-Market-Surveillance

## Überwachungs-Maßnahmen
SOUP-Monitoring
Schwachstellen-Monitoring
Penetrationtests
Tools und Angebot des Einsatzes

Vortrag von Lars Kriesel

# Das Big Picture für Cyber-Security in der Medizintechnik

## Organisatorische Maßnahmen
Verantwortung der Leitung – CS Policy – CS Goals
Einführung und Implementierung ISMS/ IEC 27001
DSGVO- Checkliste
Asset Management

1

## Mitarbeiter-Awareness
Aus- und Weiterbildung
Phishing-Mails
Denken wie ein Hacker

2

## Prozessuale Maßnahmen
Attack Surface Reduction
Härten von Entwicklungsprozessen
Secure Product Development Life Cycle
Härten von Produktionsprozessen
Härten von Zulieferketten und -produkten

3

## Normen und Gesetze
EU-MDR/ EU- IVDR
IEC 81001-5-1
60601-4-5/ 62443
AAMI TIR57
FDA
DiGAV
Überwachung und Benannte Stellen

4

## Risiko-Beherrschende Maßnahmen
Integriertes RM Safety & Security
Wechselwirkungen, Risk Control Options: Inherent oder System oder Produktion
Implementierung von Risikomindernde Maßnahmen

5

## State of the art
Codierrichtlinien
Internetplattformen
CVE, OWASP, CWE, MITRE, ATT&CK
SBoM
Integration von Checks aus CVE-DB
Schwachstellenmanagement
(Versionen von IT-Komponenten)

6

## Technische Maßnahmen
Architektur und Design (Datenminimierung, Rechtevergabe, Update-Planung, Segregation …)
Defense in Depth
Code-Signierung
IT-Struktur

7

## Permanente Wachsamkeit/ Vigilanz
CAPA
Audit Trail
Product Security Incident Response Team (PSIRT)
Pre-Market- Surveillance
Post-Marke ce

8

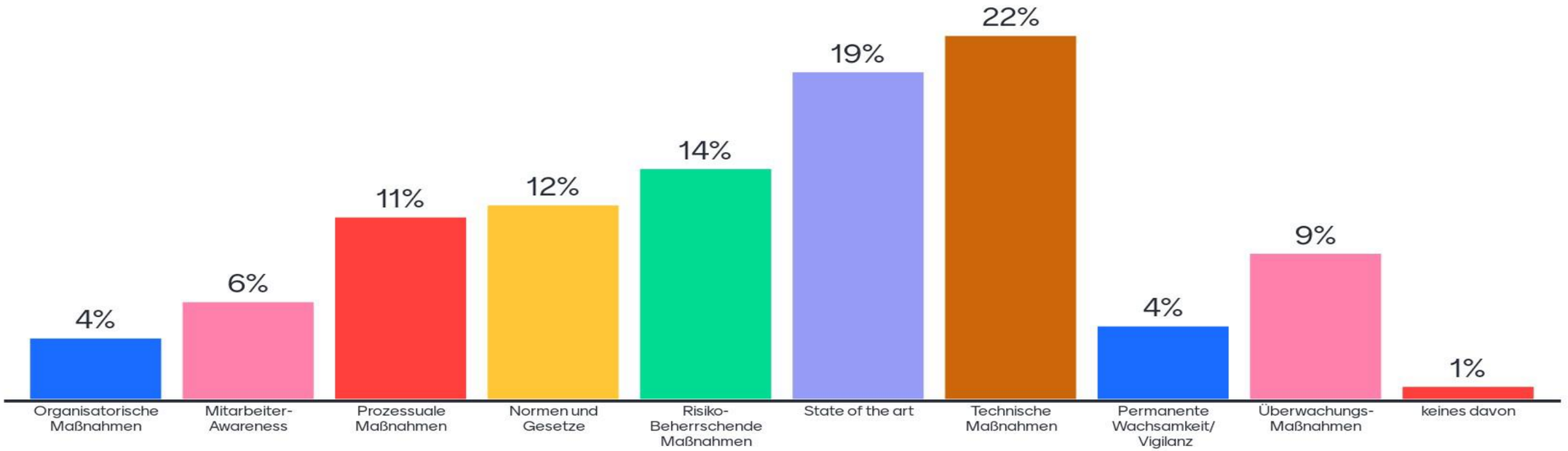
## Überwachungs-Maßnahmen
SOUP-Monitoring
Schwachstellen-Monitoring
Penetrationtests
Tools und Angebot des Einsatzes

9

# Zu diesen Themen wünschen sich die TN Vorträge beim nächsten Mal

## Das Big Picture für Cyber-Security in der Medizintechnik

Mentimeter




48

## Kontakt


Thomas Franke
Key Account Manager/ Consultant
Business Segment Life Science/Healthcare
Tel: +49 (0) 9131 7800-0
Mobil: +49 (0) 151 6245 1699
Mail: thomas.franke@infoteam.de

**infoteam Software AG**
Am Bauhof 9 | 91088 Bubenreuth | Deutschland

Telefon: +49 9131 78 00-0
Telefax: +49 9131 78 00-50
info@infoteam.de | www.infoteam.de