

Securing medical devices

Ben Kokx

Director standardization product security

2023-09-20 @ 8th ENISA eHEALTH SECURITY CONFERENCE

A photograph of an operating room. In the foreground, a surgeon in blue scrubs, a blue surgical cap, and a face mask is looking at a computer monitor. The monitor displays various vital signs and waveforms. In the background, other surgeons are visible, and the room is filled with medical equipment, including overhead surgical lights and monitors.

Cybersecurity challenges in Healthcare



Systems are increasingly connected



Systems become more 'intelligent'

A photograph of a medical control room. A woman in green scrubs is seated at a desk with multiple computer monitors displaying various data and waveforms. A man in a white lab coat stands behind her, looking at the screens. In the background, another person in a white lab coat is blurred, moving towards a window. The room has soundproofing panels on the wall and desk lamps.

Integration of networks and responsibilities?

A photograph of two men shaking hands in a medical setting. The man on the left is wearing a white lab coat and is smiling. The man on the right is wearing a dark blue polo shirt with a name tag that says "PHILIPS" and is also smiling. They are standing in front of a large piece of medical equipment, possibly a CT scanner, with the word "PHILIPS" visible on it. The background is a bright, clean clinical environment.

Shared responsibility

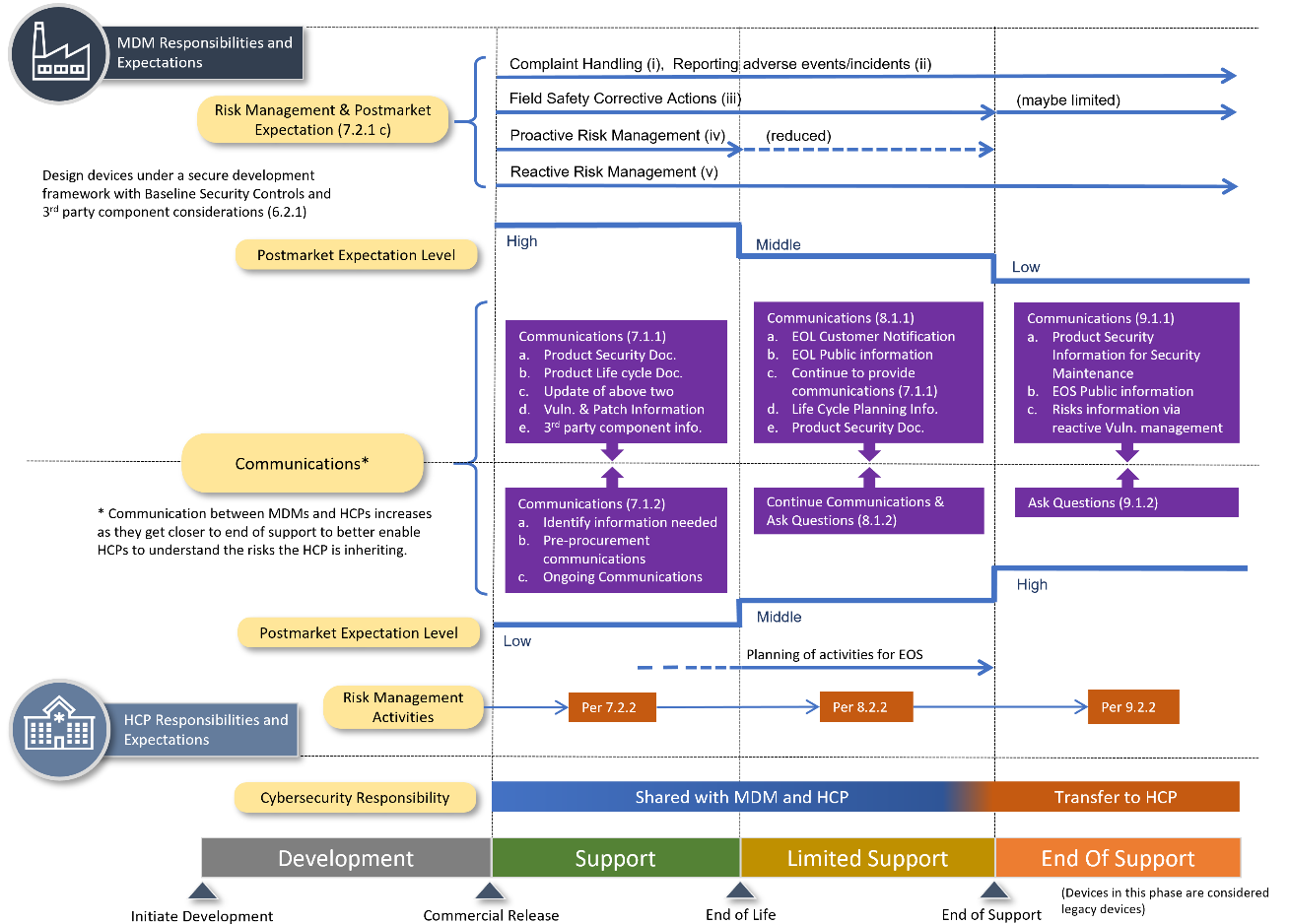


Obsolescence

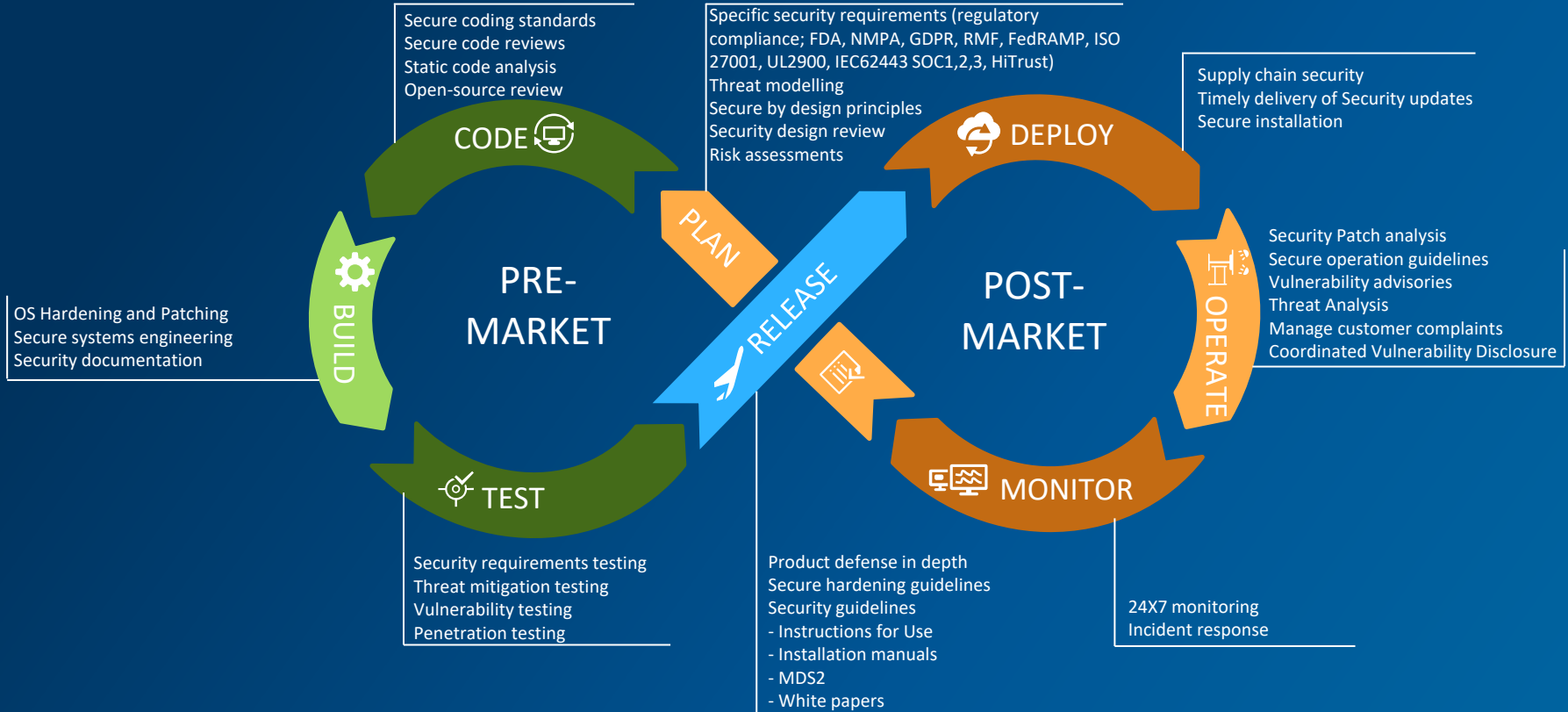
September 20, 2023

Securing Medical Devices - Ben Kokx

IMDRF N70: Principles and Practices for the Cybersecurity of Legacy Medical Devices



Philips Product Security – Overview




Standards

- ISO/IEC 81001-5-1
- IEC/TR 60601-4-5
- IEC/TR 81001-2-2*





PHILIPS For consumers For professionals About Philips 

Global

Philips coordinated vulnerability disclosure statement

Philips is committed to ensuring the safety and security of patients, operators and customers who use our products and services. Philips maintains a global network of product security officers for developing and deploying advanced best practice security and privacy features for our products and services, as well as for managing security events. Philips operates under a global product security policy, which guides our incident management and all risk assessment activities relating to potential security and potential privacy vulnerabilities identified in our products and services. Philips supports coordinated vulnerability disclosure, and encourages vulnerability testing by security researchers and by customers, with responsible reporting to Philips.

To this end, Philips maintains a product security page with information on coordinated vulnerability disclosure at www.philips.com/security

When submitting reports of vulnerability findings, please ensure the following procedures are followed, for safe and efficient support.

[Our PGP public key](#)

Reporting Procedures:

1. Please use our PGP public key to encrypt any email submissions to us at productsecurity@philips.com.
2. Please provide us with your reference/advisory number and sufficient contact information, such as your organization and contact name so



Questions?



Security



Fast response



In Control



Minimized risk



There are some
viruses doctors
can't treat.