CYBELLUM

HOP ON THE OMNIBUS!

The Omnibus Preparedness Accelerator
Get your cybersecurity operation ready for the big deadline

The Omnibus is here. As of March 29, 2023, the FDA expects medical device manufacturers (MDMs) to have all the information ready under section 524B. Those who do not risk the FDA sending an RTA (refuse-to-accept) decision, significantly delaying new product launches. That said, until October 2023, the FDA will not refuse to accept premarket submissions for review while MDMs get up to speed with necessary requirements.

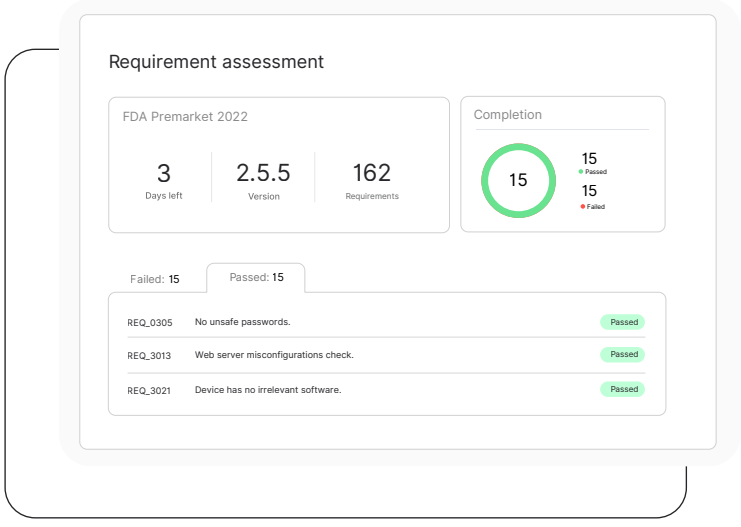
Cybellum's Omnibus Preparedness Accelerator allows MDMs to be better prepared for the October enforcement by combining two main approaches

A compliance acceleration service by product security experts

Discovery -
Reviewing existing organizational setup, assessment of Omnibus readiness, and identifying main gaps

Implementation -
Defining the main processes and tools needed to comply

Commissioning -
Implementation of relevant product security automation solutions



A dedicated Product Security Platform used by leading medical device manufacturers, enabling the automation of main processes

SBOM Management and VEX

Vulnerability Management

Incident Response

Automated Compliance Validation of Pre-Market, Cybersecurity related 510(k), and other requirements

Four main pillars of Omnibus section 524B requirements and how we help with each

Pillars

> **Manufacturers should have a plan to monitor, identify, and address postmarket cybersecurity vulnerabilities in a timely manner, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures**

How we help

A dedicated solution and services for incident response that allows you to continuously identify, prioritize, and mitigate vulnerabilities for post-market devices. The process:

- Continuous threat/vulnerability intelligence for uncovering new vulnerabilities or updating exploitation status (severity)
- Extraction of relevant information - vulnerability insights
- Correlate vulnerability with the company product BOM (SBOM & HBOM), deployment configurations, and different firmware releases
- Execution of an exploit analysis for relevant components based on the potential impact (prioritization analysis)
- Conducting vulnerability investigations (automated, based on expert support)
- Facilitating an investigation report with actionable recommendations for mitigation
- Generating a vulnerability disclosure report for internal & external usage
- Provide managed PSIRT services where we can manage the entire process above on the company's behalf

> **"Design, develop, and maintain processes that give reasonable assurance that the device and related systems are cyber secure and make available postmarket updates and patches to the device and related systems to address - (A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and (B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks"**

A vulnerability management solution that allows you to create a continuous, automated process of:

- Identifying vulnerabilities
- Prioritizing them according to their exploitability
- Receive mitigation recommendations, throughout the entire lifecycle

The process is **well documented** within the platform, allowing you to showcase a robust vulnerability management process is in place when audited

In addition, the platform allows product security teams to **compare and manage different firmware versions** and historical records, critical for auditing purposes

To complement this technology, **a dedicated service allows for a deep investigation** of the potential impact (prioritize severities) and alternative mitigation options

Pillars

> **Provide an SBOM with OSS, commercial, and off-the-shelf components**

How we help

- Build an **SBOM management process** that allows you to create, manage and validate SBOMs across teams and business units, using our platform
- **An SBOM management dashboard** allows you to keep track of and showcase your progress during an audit
- Provide **extended visibility** into external suppliers' code which today is poorly managed in many organizations
- A dedicated **managed service for SBOM verification,** facilitating the entire process on your behalf

> **Comply with future requirements that demonstrate cybersecurity**

- Enable continuous updates of new regulation requirements and map them into the production process (Gap-analysis / update reports / relevant policy updates) right within the platform
- A dedicated service helping you implement and integrate new regulatory requirements into your workflows, by leveraging our platform's compliance engine with product security expertise

About us

Cybellum is where teams do product security.

Leading manufacturers such as Jaguar Land Rover, Supermicro, Siemens, and Faurecia use Cybellum's Product Security Platform to execute and manage the main aspects of their cybersecurity operations across teams, product lines, and business units. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Ready to hop on the Omnibus?
reach out at cybellum.com/Omnibus