

# HOW TO CYBER A PRODUCT FOR FDA

**DANIEL KLEINBERG**  
Matrix Medika  
19.03.2024



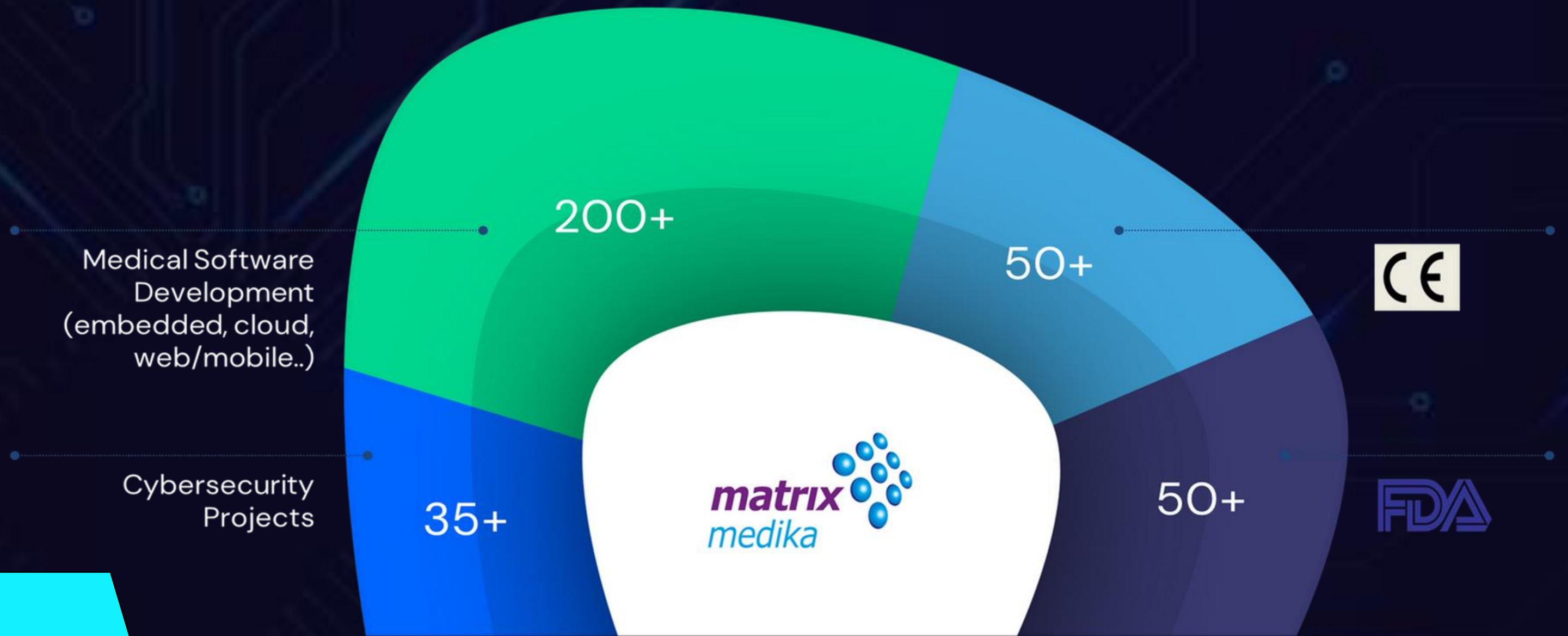
## ABOUT ME

- QA/RA Cyber Expert at Matrix Medika
- Believes Cybersecurity is not only a rubber stamp
- Experience with vast amount of project types, medical devices and technologies
- Always looking for updates on Medical and on Cyber
- Believes QA is an integral part of QA/RA



# ABOUT MATRIX MEDIKA

Israel's leading provider of software development, regulation and cyber security services for the healthcare industry.





# REGULATION, CYBERSECURITY, PRIVACY

## FDA submissions

- CE submissions
- IEC 62304 compliance

---

## Cyber Security & Compliance

- Compliance assessment (per FDA and CE guidance)
- Penetration Testing
- FDA/CE Cyber Report

---

## HIPAA, GDPR Compliance

- Compliance assessment and Gap analysis in product and company level
- Company adoption (procedures, terms & conditions, training)

---

## ISO 27001 \ 27799 \ 27017





# WHAT WE'RE ALL ABOUT

- What do we need for the cyber section of the FDA?
- Why do we need it?
- Why do we need it now more than ever?
- What can go wrong?
- How do we fix it?





# CYBERSECURITY STANDARDS, FDA GUIDANCES

- FDA Guidance: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions 2023
- FDA Guidance: Postmarket Management of Cybersecurity in Medical Devices 2016
- FDA Guidance: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software 2023
- MDCG 2019-16 - Guidance on Cybersecurity for medical devices
- ANSI/AAMI TIR57:2023 – Principles for Medical device security
- NIST.SP.800-53r5 Security and Privacy Controls for Information Systems and Organizations
- ANSI/AAMI SW96:2023 Standard For Medical Device Security - Security Risk Management For Device Manufacturers



# POSSIBLE FDA REMARKS

Not all controls are measured (Risk should cover authorization, authentication, hardening, cryptography, updatability etc...)

You declared Cloud connection but didn't enough add Risks/added as system part

You didn't add a Cyber column In unresolved anomalies

You Wrote probabilities and not likelihood



# C-FMEA - IMPORTANT TO REMEMBER

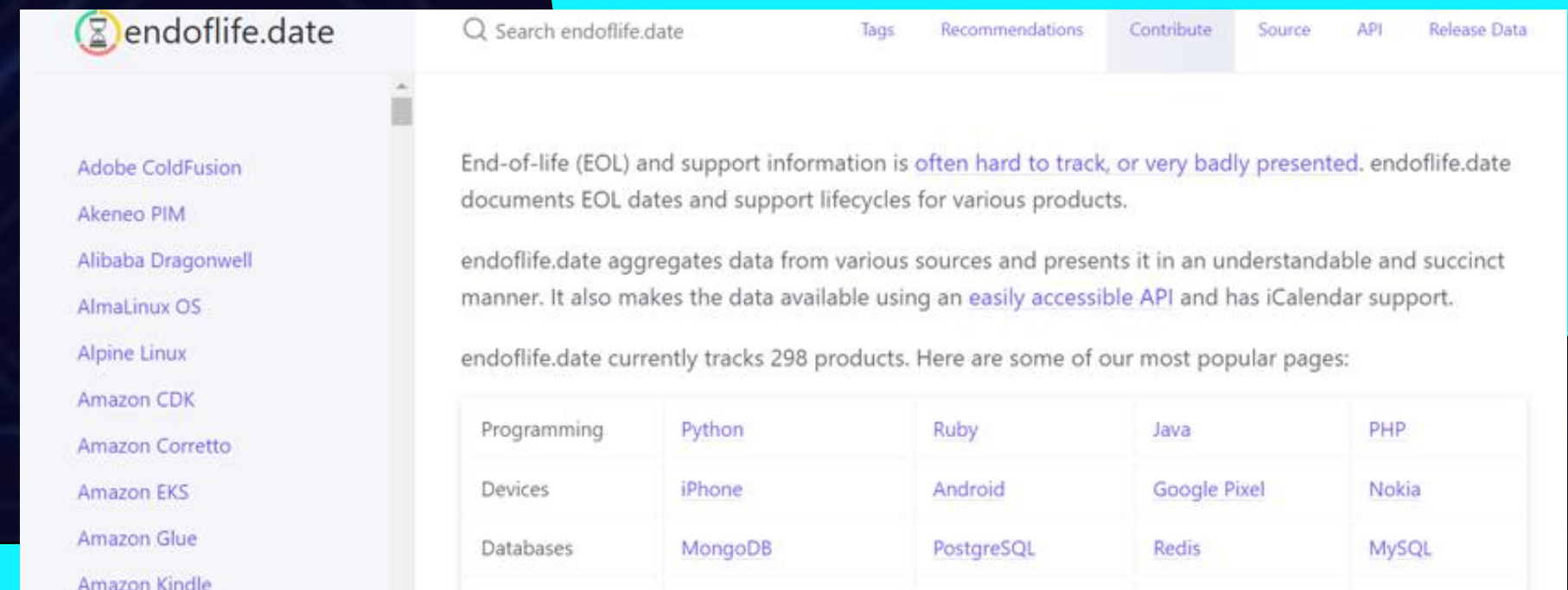
- LIKELIHOOD, NOT PROBABILITY
- Clinical Severity description – take from RMP
- Severity – always from FMEA
- Likelihood – Think cyber!
- Physical access – a great mitigation
- If it's mitigated – it's actually there





# ➤➤➤ S-BOM - IMPORTANT TO REMEMBER

- <https://endoflife.date/> - your new best friend
- Not all libraries have EOL – but if they do, it's important to find it
- EOL is due? We need to add justification!
- Manual or automatic? Depends on budget, technology, and amount of libraries
- Searching for vulnerabilities manually? More than 1 database, smart search term, when in doubt call Dr. Google.



The screenshot shows the endoflife.date website. The header includes the site name, a search bar, and navigation links for Tags, Recommendations, Contribute, Source, API, and Release Data. The main content area features a list of product categories on the left and a descriptive paragraph on the right. Below the paragraph is a table of popular pages.

Programming	<a href="#">Python</a>	<a href="#">Ruby</a>	<a href="#">Java</a>	<a href="#">PHP</a>
Devices	<a href="#">iPhone</a>	<a href="#">Android</a>	<a href="#">Google Pixel</a>	<a href="#">Nokia</a>
Databases	<a href="#">MongoDB</a>	<a href="#">PostgreSQL</a>	<a href="#">Redis</a>	<a href="#">MySQL</a>



# PLAN + REPORT- IMPORTANT TO REMEMBER

- When announcing post-marketing actions – be sure you can actually do it
- Visual aids are always good – screenshots are better
- Assets are not only the device/app
- Controls and C-FMEA mitigation - should be intertwined
- When updating C-FMEA and adding/removing risks, remember to update the conclusion in the report



# ARCHITECTURE VIEWS + THREATS ANALYSIS

Microsoft Threat Modeling Tool  
Version: 7.3.31026.3

**Threat Model:**

- Create A Model**  
Model your system by drawing diagram (s). Make sure you capture important details.
- Open A Model**  
Open an existing model file and analyze threats against your system.
- Getting Started Guide**  
A step-by-step guide to help you get up and running now.

**Template For New Models**  
Azure Threat Model Template(1.0.0.33) [Browse...](#)

**Recently Opened Models**  
[XSense\\_TM.tm7](#)  
[Sample\\_Threat\\_Model.tm7](#)

**Threat Modeling Workflow**  
1. Select your template.  
2. Create your data flow diagram model.  
3. Analyze the model for potential threats.  
4. Determine mitigations.

**Template:**

- Create New Template**  
Define stencils, threat types and custom threat properties for your threat model from scratch.
- Open Template**  
Open an existing Template and make modifications to better suit your specific threat analysis.
- Template Workflow**  
Use templates to define threats that applications should look for.  
1. Define stencils  
2. Define categories  
3. Define threat properties  
4. Define threat  
5. Share your template

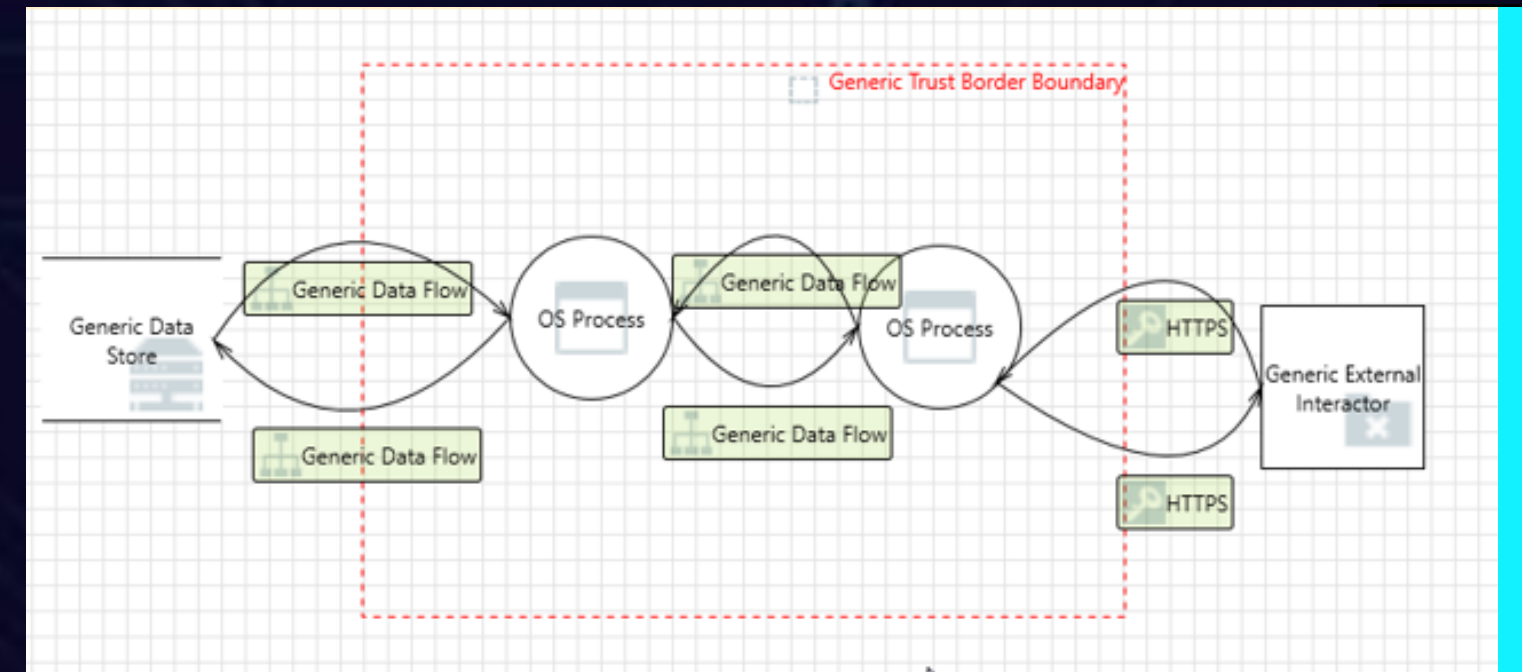


Diagram 1

**Threat List**

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority	Countermeas	Risk
1	Diagram 1		Generated	Not Started	Weak Access Co	Information Dis	Improper data p		SQL	High		High
25	Diagram 1		Generated	Not Started	Potential SQL In		SQL Injection is		SQL	High		High
43	Diagram 1		Generated	Not Started	Spoofing the W	Spoofing	WAF may be spc		HTTP	High		High
44	Diagram 1		Generated	Not Started	Potential Lack o	Tampering	Data flowing aci		HTTP	High		High
45	Diagram 1		Generated	Not Started	Potential Data F	Repudiation	Web Application		HTTP	High		High
47	Diagram 1		Generated	Not Started	Cross-Site Requ	Elevation Of Pri	Cross-site requ		HTTP	Medium		Medium
48	Diagram 1		Generated	Not Started	Elevation Using	Elevation Of Pri	Web Application		HTTP	High		High
49	Diagram 1		Generated	Not Started	Elevation by Ch	Elevation Of Pri	An attacker maj		HTTP	High		High
50	Diagram 1		Generated	Not Started	Spoofing of the	Spoofing	WAF may be spc		HTTP	High		High

Export Csv 12 Threats Displayed, 12 Total

**Threat Properties**

ID: 44 Diagram: Diagram 1 Status: Not Started

Title: Potential Lack of Input Validation for Web Application

Category: Tampering

Description: Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Web Application or an elevation of privilege attack against Web Application or an information disclosure attack against Web Application. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an appropriate validation approach.

Justification:

Interaction: HTTP

Priority: High

Threat Properties Notes - no entries



# ARCHITECTURE VIEWS + THREATS ANALYSIS - IMPORTANT TO REMEMBER

- You have an SDD -Take diagrams from there.
- Not all threats found on the threat list are realistic/reliable – used as a point of reference for C-FMEA, not instead
- FDA favorite – after the likelihood FDA will search for this





**Cybersecurity**

**Risks**

When not considering mitigation measures for the cybersecurity risks, could your device(s)/ system result in either of the following:  ?

- multi-patient harm (resulting in temporary or medically reversible adverse events), or
- serious adverse events or death in the event your device(s)/system is compromised?

**Risk Management - Report**

**Add Attachment** Please attach your security risk management report detailing a separate, parallel, and interconnected security risk management process. This is different from your safety risk management process. ?

**Risk Management - Threat Model**

**Add Attachment** Please attach your threat model addressing all the end-to-end elements of the system. ?

List the Threat Methodology (e.g. STRIDE, Attack Trees, Kill Chain, DREAD) that you used. ?

**Add Attachment** Please attach a safety and security assessment of cybersecurity vulnerabilities in the component software used by the device for all software components in the SBOM and a description of any controls that address the vulnerability. ?

**Assessment of Unresolved Anomalies**

**Add Attachment** Please attach an assessment of any unresolved anomalies for cybersecurity impact. If none exist, attach a document stating that no unresolved anomalies exist. ?

**Open Attachment** Cybersecurity Unresolved Anomalies.pdf **Delete Attachment**

**Cybersecurity Metrics**

**Add Attachment** Please attach data from monitoring cybersecurity metrics. If metric data are unavailable, please attach a justification. ?

**Cybersecurity Controls**

**Add Attachment** Please attach information on the security controls categories included in the device. ?

Please cite the page number(s) of the attachment directly above where you addressed the following controls listed in the textbox below (e.g. "A) Authentication Controls: Page 2"). ?

A) Authentication controls:  
 B) Authorization controls:  
 C) Cryptography controls:  
 D) Code, data, and execution integrity controls:  
 E) Confidentiality controls:  
 F) Event detection and logging controls:  
 G) Resiliency and recovery controls:  
 H) Firmware and software update controls:

**Risk Management - Cybersecurity Risk Assessment**

**Add Attachment** Please attach your Cybersecurity Risk Assessment ?

Please cite the page number(s) of the attachment directly above where you describe your methodology and your acceptance criteria. ?

Does the Cybersecurity Risk Assessment avoid using probabilities for the likelihood assessment and use exploitability instead?  ?

**Risk Management - Software Bill of Materials (SBOM) and Related Information**

**Add Attachment** Please attach your Software Bill of Materials (SBOM). ?

**Add Attachment** Please attach a document to provide the software level of support and end-of-support date for each software component (e.g. OTS software) identified in the SBOM. For any component where this information was not available, provide a justification. ?

List the supported operating system(s) and associated version(s) your device(s)/system uses. Be aware that if you list any operating systems that are no longer supported (e.g. Windows 7, Mac OS 9) or nearing end of support, this will be considered an inaccurate response. Type "N/A" if your device(s) does not use an operating system. ?



# THANK YOU



054-5992364



Daniel@medi-software.com

