AIRIS 2025
Regulation for AI, Together for Tomorrow
AI Regulatory & International Symposium

Cybersecurity for AI-based Digital Medical Devices

Sept. 11, 2025

Jiho Bang, KTC
(Director of Intelligence & Information Business Division, jhbang@ktc.re.kr)

KTC Korea Testing Certification institute

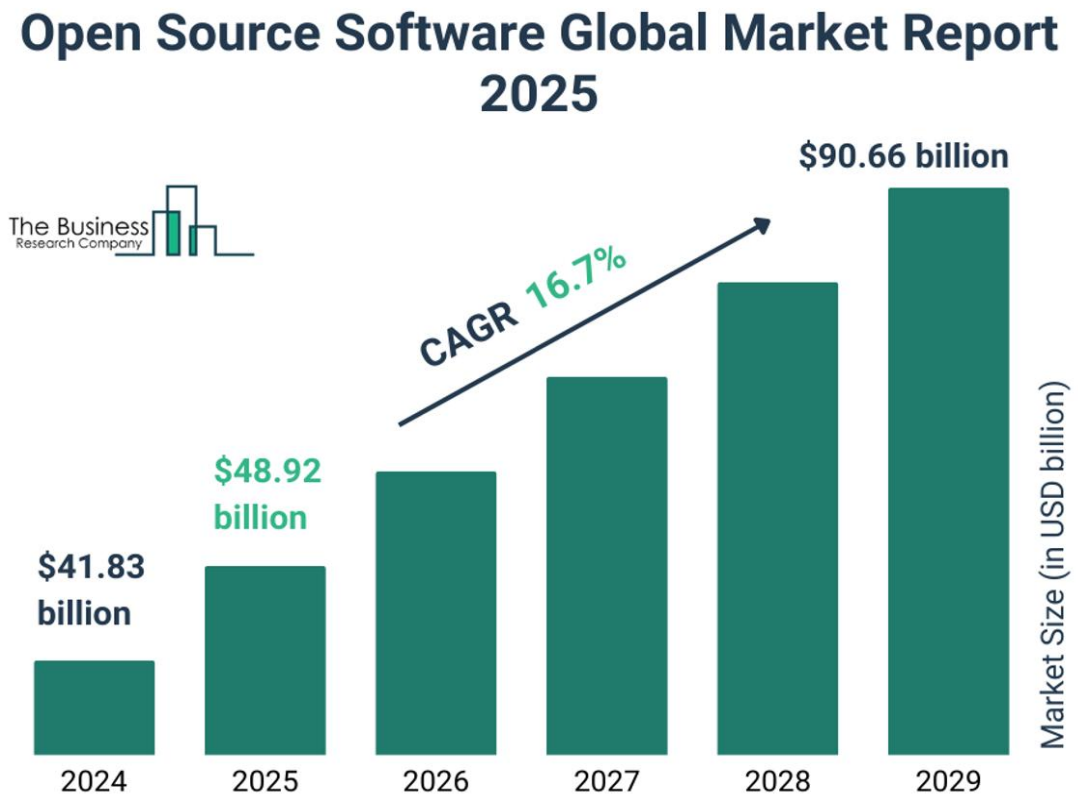
1 Increase in cybersecurity vulnerabilities of digital medical devices

- **Recently, as software and network connectivity in medical devices have increased, reports of security vulnerabilities have also been on the rise. The following are recent medical device vulnerability cases reported on the U.S. FDA website.**

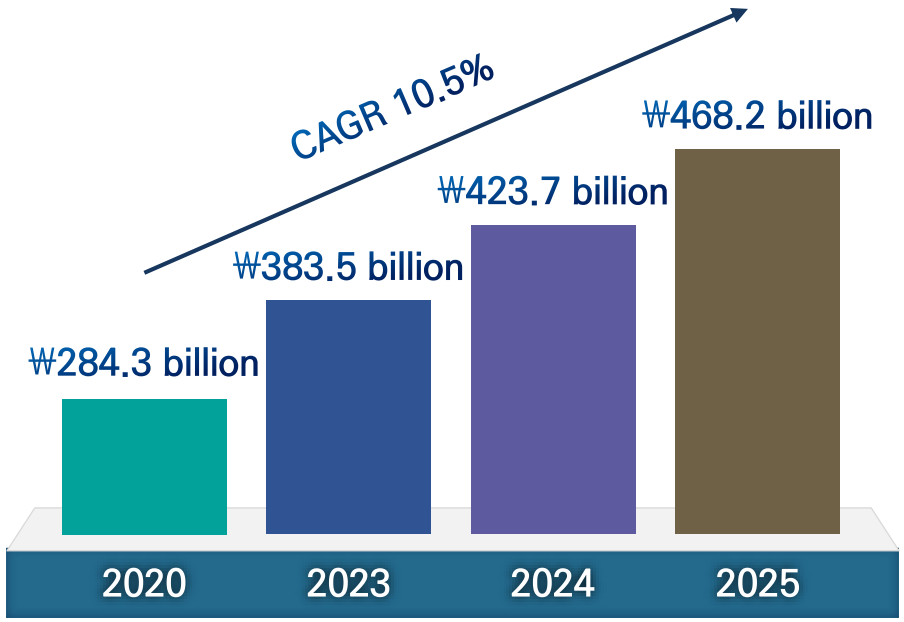
연도	월	Safety Communication or Alert by U.S. FDA
2025	1	• Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication 1) The patient monitor may be remotely controlled by an unauthorized user or not work as intended. 2) The software on the patient monitors includes a backdoor. 3) Once the patient monitor is connected to the internet, it begins gathering patient data, including personally identifiable information (PII) and protected health information (PHI), and exfiltrating (withdrawing) the data outside of the health care delivery environment.
2022	3	• Cybersecurity Alert: Vulnerabilities identified in medical device software components: PTC Axeda agent and Axeda Desktop Server • Related Vul. : Use of hardcoded credentials, lack of authentication for critical functions, etc.
	6	• Illumina Cybersecurity Vulnerability May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers • Related Vul. : execution with unnecessary privileges(CWE-250), improper access control(CWE-284), etc.
	9	• Medtronic MiniMed 600 Series Insulin Pump System Potential Cybersecurity Risk
2021	8	• CISA Alert: Cybersecurity Vulnerabilities with BlackBerry QNX (BadAlloc, CVE-2021-22156)
	12	• Cybersecurity Vulnerability with Apache Log4j
	12	• Cybersecurity Alert: Fresenius Kabi Agilia Connect Infusion System • Related Vul. : use of hardcoded credentials, use of unmaintained third-party components, store passwords in plain text, etc.

2 Increased utilization of open source in software development

Global Market Size

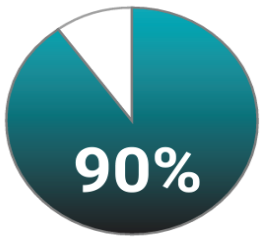


Domestic Market Size

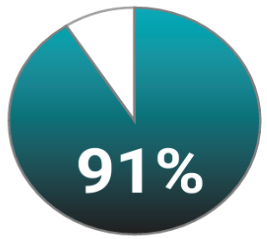


[출처] The Business Research Company, “Open Source Software Global Market Report 2025”, 2025.01.
ETnews, “Domestic open source software market to reach nearly 500 billion won by 2025”, 2024.12.18.

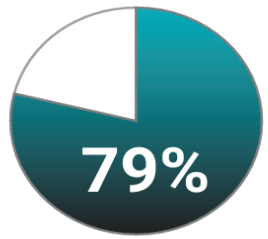
2 Supply Chain Security Trends: Open Source Vulnerabilities



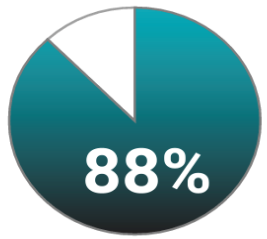
of codebases contain open source components that are more than four years out-of-date



of codebases have components that have not seen new development in the past two years



of codebases contain components with no activity for the last 24 months, while still using the latest version of the component



of codebases have components with no activity for the last 24 months and are not using the latest version of the component

- 86% of scanned codebases* contain vulnerable open source components (2024, 1,658 projects).

* All source code used to build a specific software system, application, or software component.

- 90% include open source that is over 4 years out of date.
- 91% contain components with no new development in the past 2 years.
- 88% use inactive components and not the latest versions.
- 79% use inactive components, but have updated to the latest versions.

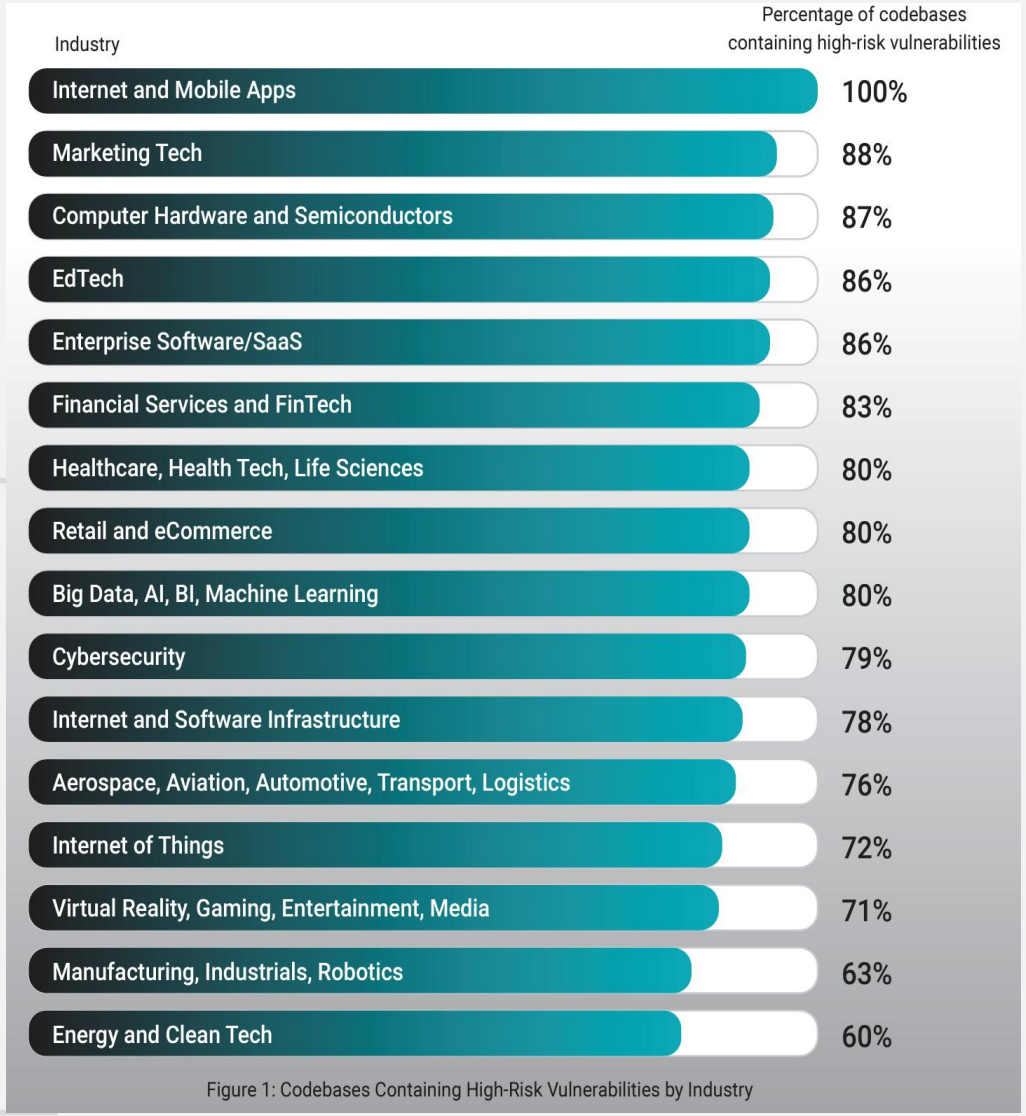


Figure 1: Codebases Containing High-Risk Vulnerabilities by Industry

(출처) Synopsys, 2025 Open Source Security and Risk Analysis Report

3 Examples of AI-Related Vulnerabilities

- With the increasing vulnerabilities related to generative AI, AI agents, and training data, it is necessary to consider appropriate security measures

CYBERSECURITY DIVE

Research shows AI agents are highly vulnerable to hijacking attacks

Experts from Zenity Labs demonstrated how attackers could exploit widely deployed AI technologies for data theft and manipulation.

Published Aug. 11, 2025

David Jones
Reporter

AI agent touch screen. Alexander Sikov via Getty Images

Some of the most widely used AI agents and assistants from Microsoft, Google, OpenAI and other major companies are susceptible to being hijacked with little or no user interaction, according to new research from Zenity Labs.

During a presentation at the Black Hat USA cybersecurity conference, Zenity researchers showed how hackers could exfiltrate data, manipulate critical workflows across targeted organizations and, in some cases, even impersonate users.

Beyond infiltrating these agents, the researchers said, attackers could also gain memory persistence, letting them maintain long-term access and control.

TechTarget ComputerWeekly.com

NEWS | This article is part of our Conference Coverage: The latest from Blac...

Agentic AI a target-rich zone for cyber attackers in 2025

At Black Hat USA 2025, CrowdStrike warns that cyber criminals and nation-states are weaponising GenAI to scale attacks and target AI agents, turning autonomous systems against their makers

By **Brian McKenna**, Enterprise Applications Editor

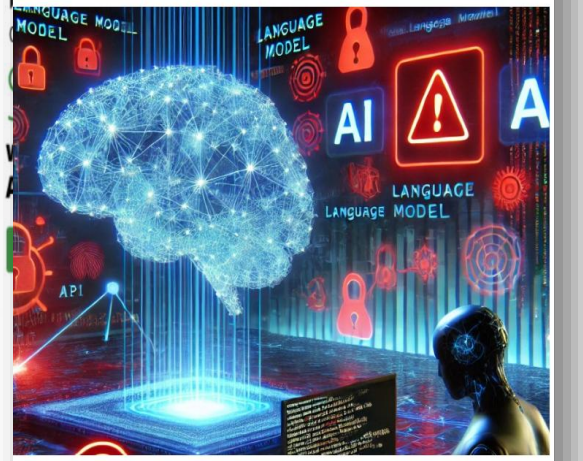
Published: **04 Aug 2025 15:39**

Cyber criminals and nation-states hostile to Western countries are weaponising artificial intelligence (AI) with gusto to carry out attacks and targeting AI agents as a novel attack vector, according to cyber security company CrowdStrike.

데일리시큐

LLM 학습 데이터에서 1만2천개 이상 API 키 및 비밀번호 노출 확인

길민권 기자 | 승인 2025.03.01 16:17

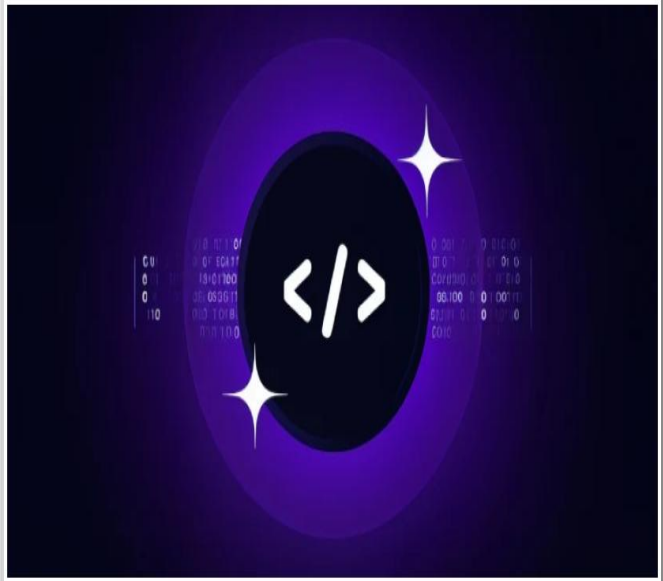


최근 보안 연구진이 거대 언어 모델(LLM) 학습에 사용되는 데이터셋에서 약 1만2천개의 활성 API 키와 비밀번호가 포함된 사실을 발견했다. 이 조사 결과는 AI 학습 과정에서 보안이 제대로 관리되지 않을 경우, 심각한 보안 취약점으로 이어질 수 있음을 다시 한번 경고하고 있다.

The Hacker News

GitLab Duo Vulnerability Enabled Attackers to Hijack AI Responses with Hidden Prompts

May 23, 2025 Ravie Lakshmanan



Cybersecurity researchers have discovered an indirect prompt injection flaw in GitLab's artificial intelligence (AI) assistant Duo that could have allowed attackers to steal source code and inject untrusted HTML into its responses, which could then be used to direct victims to malicious websites.

[출처] https://www.cybersecuritydive.com/news/research-shows-ai-agents-are-highly-vulnerable-to-hijacking-attacks/757319/
https://www.computerweekly.com/news/366628359/Agentic-AI-a-target-rich-zone-for-cyber-attackers-in-2025
https://dailysecu.com/news/articleView.html?idxno=164161
https://thehackernews.com/2025/05/gitlab-duo-vulnerability-enabled.html

☞ Prompt injection attacks in AI coding assistants could potentially lead to the leakage of personal source code

4 Regulatory Trends in Cybersecurity for Digital Medical Products

U.S.

- (December 2022) The Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law.
  - ✓Section 3305 of the Omnibus – "Ensuring Cybersecurity of Medical Devices" – amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices.
  - ✓The law grants the FDA official authority to ensure that medical devices meet minimum cybersecurity standards.
  - ✓Submission of an SBOM is required to meet medical device cybersecurity requirements.

EU

- MDR 745/2017 Annex I lists the general safety and performance requirements, and also includes six explicit cybersecurity requirements.
- The cybersecurity requirements are described in detail in the “MDCG 2019-16 rev.1, Guidance on Cybersecurity for Medical Devices” published by the Medical Device Coordination Group.
- (November 2024) Under the Cyber Resilience Act, products with digital elements are required to submit an SBOM for approval to be marketed in Europe.

5 Status of the MFDS's Medical Device Cybersecurity Review and Authorization Guideline

2019 — **Regulation Revision** (Mandatory submission of "cyber security data" for authorization of medical devices)

2020 — **Operation of Digital Health Device TF Team** (Dedicated to cybersecurity reviews)

2021 — **Establishment of the Digital Health Device Division**

2022 — **Application of IMDRF cybersecurity requirements**

2023

2024 — **Enactment of the Digital Medical Products Act**

2025 — **Enforcement of the Digital Medical Products Act**

Revision of Security Requirements Based on International Standards (e.g, IEC 81001-5-1, IECTR 60601-4-5)

Guideline publication

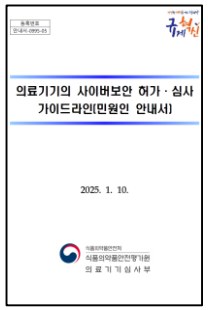
Guideline publication

Guideline revision

Guideline revision

Guideline revision

Guideline revision

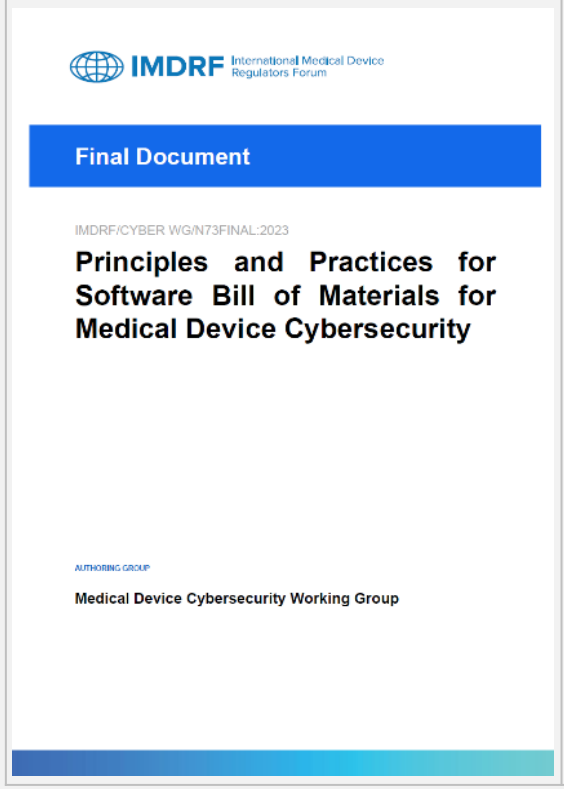


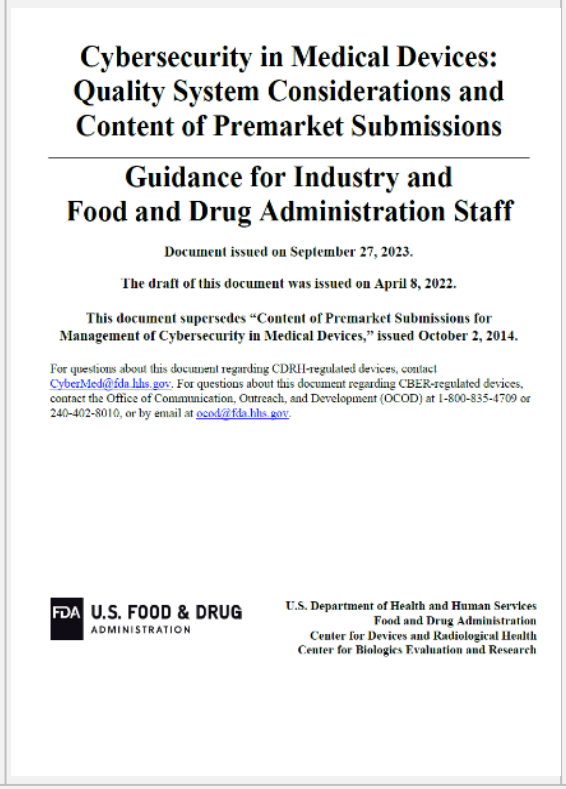
[Ref.] Modified "Cybersecurity Seminar Materials by MFDS, Korea"

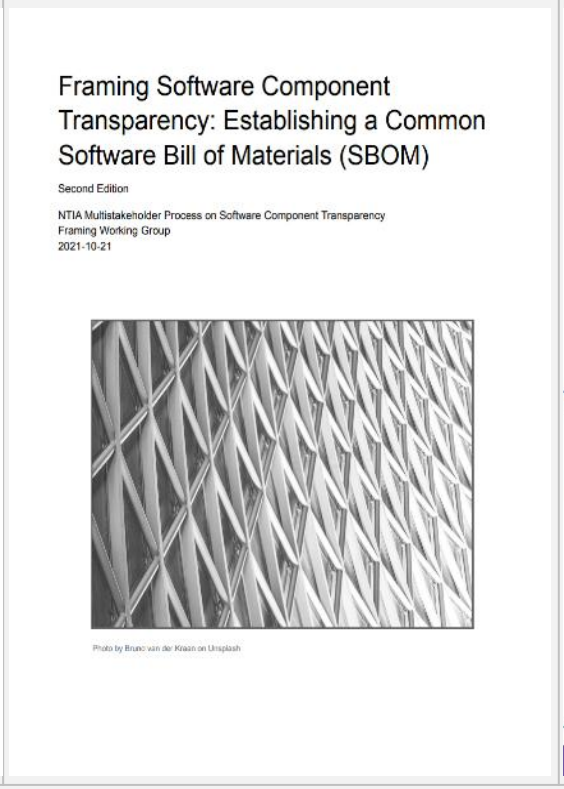
6 Defining Minimum SBOM Elements for Digital Medical Products

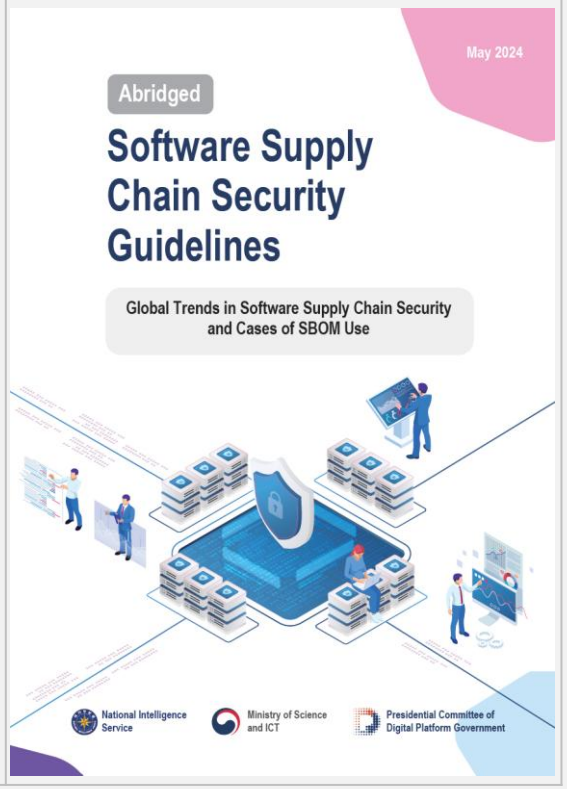
Minimum SBOM Elements Applicable to Domestic DMPs

IMDRF Doc.	FDA Doc.	NTIA/CISA Doc.	NIS Doc.





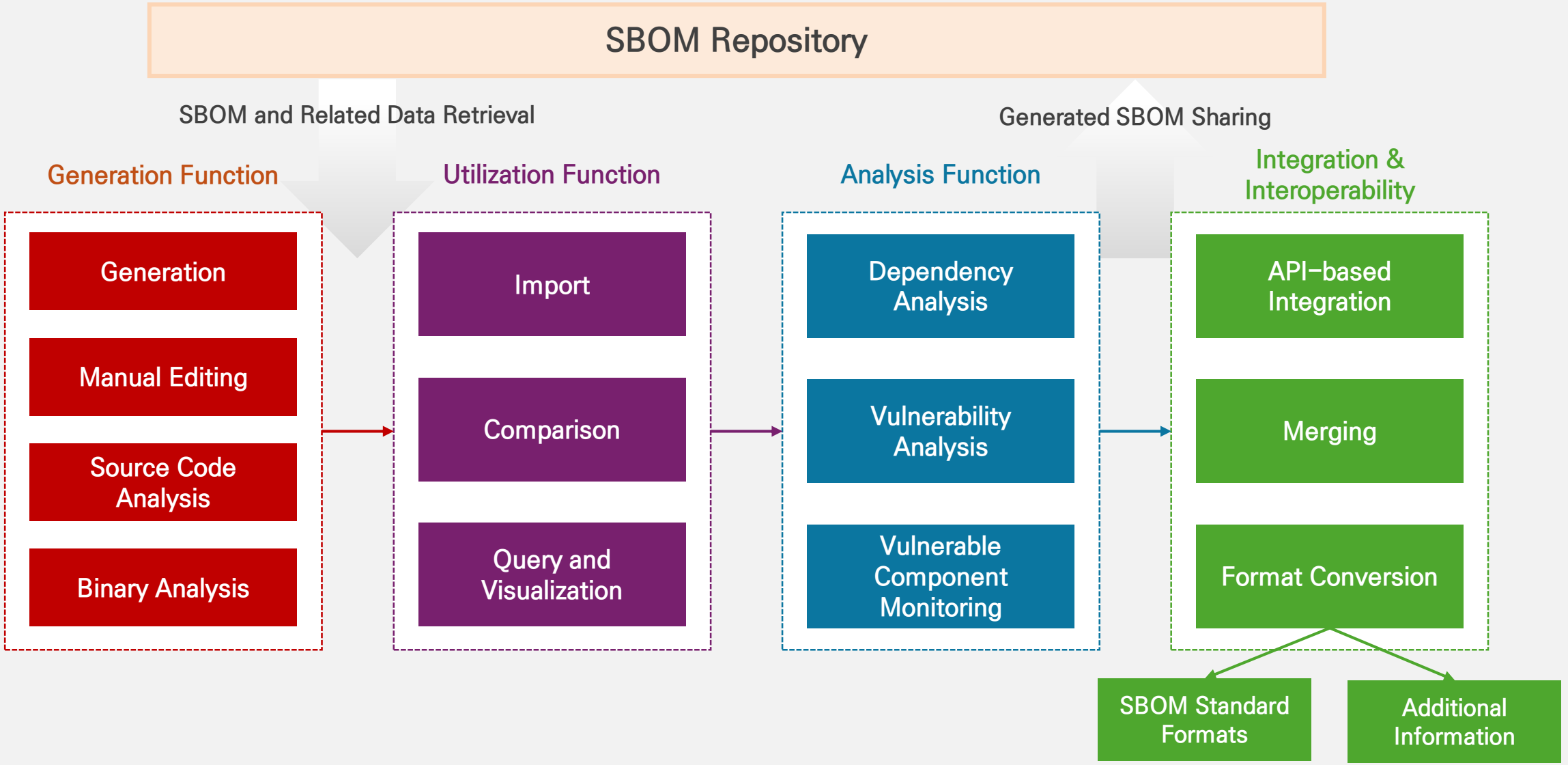




6 SBOM : U.S. FDA vs. NTIA & CISA

구분	U.S. FDA(2023/2025)	1st (2019, NTIA)	2nd (2021, NTIA)	3rd (2024, CISA)
SBOM Meta Info.	Author Name	Author Name	Author Name	SBOM Author Name
	Timestamp	–	Timestamp	SBOM Timestamp
	–	–	–	SBOM Type
	–	–	–	SBOM Primary Component
Basic Component Info.	Supplier Name	Supplier Name	Supplier Name	Component Supplier Name
	Component Name	Component Name	Component Name	Component Name
	Version String	Version String	Version String	Component Version String
	Component Hash	Component Hash	Component Hash	Component Cryptographic Hash
	Unique Identifier	Unique Identifier	Unique Identifier	Component Unique Identifier
	Relationships	Relationships	Relationships	Component Relationships
	–	–	–	Component License
	–	–	–	Component Copyright Notice
Additional Elements & Attributes	SW level of support, End-of-Support dates	End-of-Life Dates	End-of-life or End-of-Support dates for components	End-of-life date or level-of-support for Components
	–	Authenticity	Authenticity and Integrity	Authenticity and integrity capability
	–	–	Mechanisms to group components	Grouping of Components
	–	Implemented Technologies	The ability to indicate what technologies a component implements or supports	Indication of what technologies a Component implements or supports

7 SBOM Generation Tool Development for Digital Medical Products



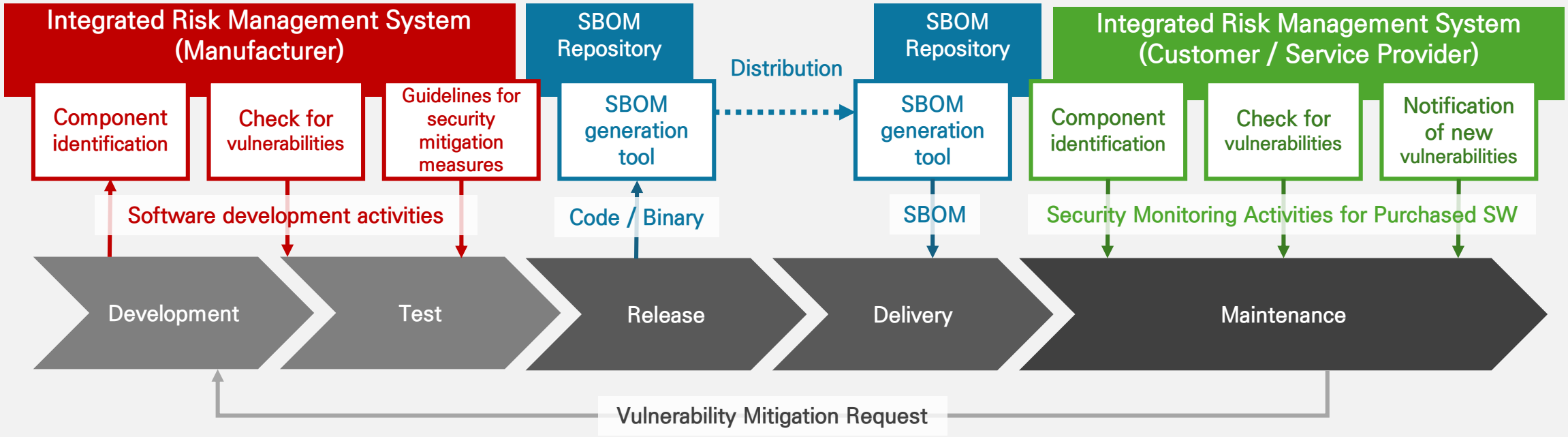
8 SBOM-based Risk Management Service

Medical Device Manufacturer

- Identify software components
- Verify and remediate vulnerabilities related to components
- Generate and distribute SBOM and VEX

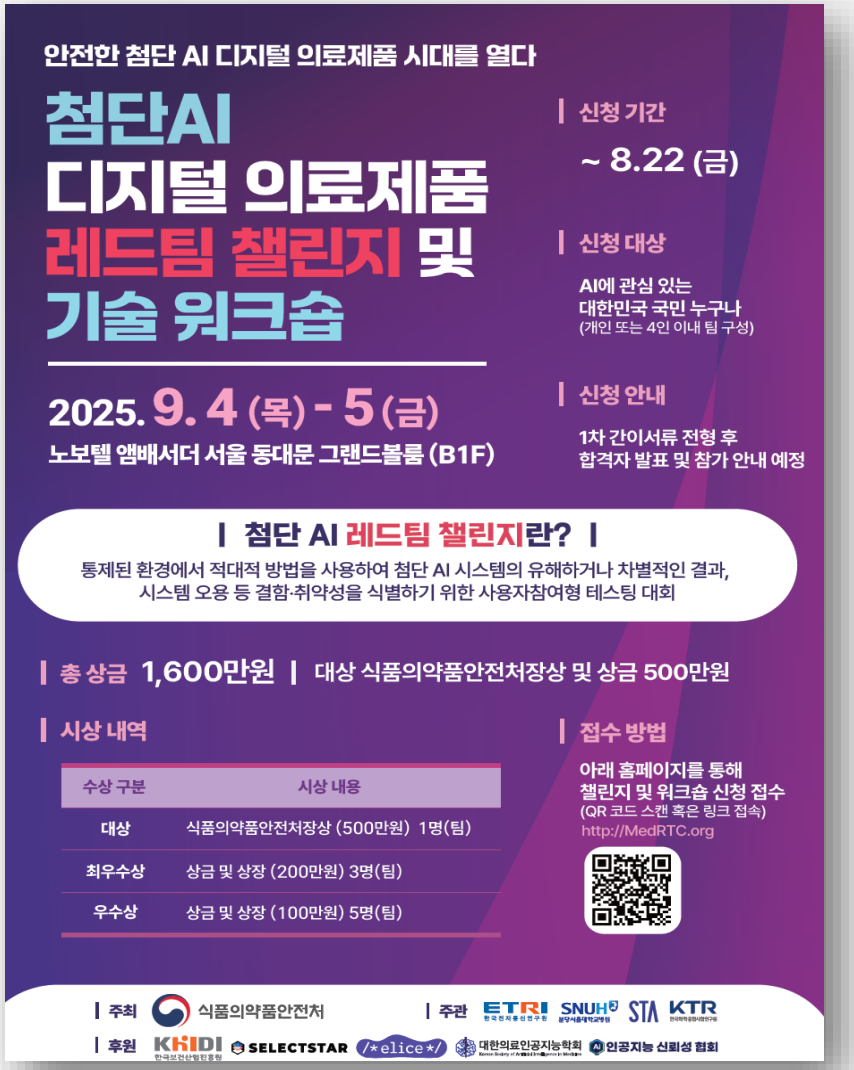
Healthcare Provider

- Manage SBOMs of purchased software
- Continuously monitor components and associated vulnerabilities
- Request remediation actions from the manufacturer when new vulnerabilities arise

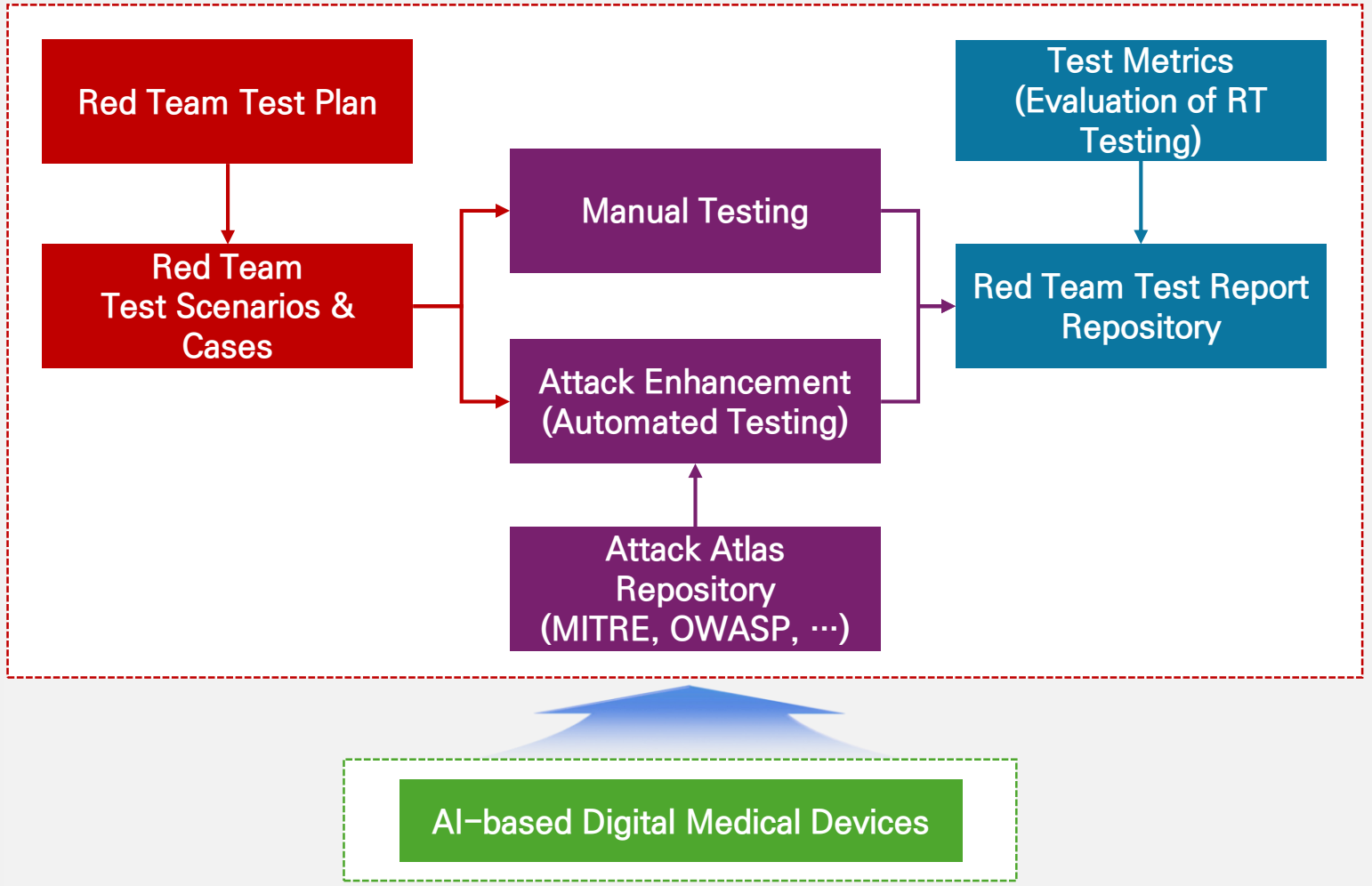


9 AI Red Teaming Methodology and Framework Development

Red Team Challenge (Sept. 4 to 5, 2025)



AI Red Teaming Framework



10 Additional Cybersecurity Research Topics for Digital Medical Products

Subject : BOM	Subject : AI Feature	Subject : Cybersecurity
SBOM Generation Tool Usage Guide, AI-BOM and HBOM for Digital Medical Devices	AI-Specific Risk Management and Mitigation Measures	Cybersecurity Risk Management Model, Supply Chain Security, and Governance throughout the entire lifecycle of digital medical products

+ Demonstration

Thank You

KTC Korea Testing Certification institute