의료기기 사이버보안을 위한 소프트웨어 자재명세서 원칙 및 실무

(Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity)

2023. 11.

식품의약품안전처
의 료 기 기 안 전 국

본 문서의 원문(Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity)은 전 세계 의료기기 규제당국자들이 자발적으로 구성한 국제의료기기규제당국자포럼(IMDRF)에서 이해당사자 간 협의를 통해 개발되었습니다.

본 문서는 IMDRF에서 발행한 원문을 식품의약품안전처가 알기 쉽게 기술한 것입니다.

본 문서는 대외적으로 법적 효력을 가지는 것이 아니므로 본문의 기술방식('~하여야 한다' 등)에도 불구하고 민원인 여러분께서 준수하셔야 하는 사항이 아님을 알려드립니다. 또한, 본 문서는 2023년 11월 현재 과학적·기술적 사실 등을 토대로 작성되었으므로 이후 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

※ 본 문서에 대한 의견이나 문의 사항이 있으면 의료기기안전국 의료기기정책과에 문의하시기 바랍니다.

전화번호: 043-719-3766

팩스번호: 043-719-3750

목 차

1.0 소개

의료기기가 디지털 연결이 가능해지면서 더욱더 효율적이고 데이터 중심적이며 효과적인 환자 치료가 가능하게 되었다. 서드파티 소프트웨어 컴포넌트의 활용과 의존으로 인해 이러한 의료기기를 더욱 경제적이고 안정적으로 개발할 수 있게 되었으며 혁신의 속도도 빨라졌다. 서드파티 소프트웨어 컴포넌트를 활용하면 많은 이점이 있는 반면에, 환자의 안전과 네트워크 연결 의료기기의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 사이버보안 위험을 초래할 수 있다.

사이버보안 취약점은 다양한 의료기기 제조업체(이하 MDM: Medical Device Manufacturers)에서 개발된 안전한 것처럼 보이는 다양한 의료기기가 공통 소프트웨어 컴포넌트를 사용한다는 이유로 영향을 받을 수 있다는 점에서 독특한 특성을 가진다. 이러한 문제는 의료기기 내 공통 컴포넌트의 추적성이 낮기 때문에 더욱 복잡해진다. 이러한 글로벌 문제를 해결하기 위해 미국의 국가통신정보국(이하 NTIA: National Telecommunications and Information Administration)은 2018년 다양한 이해관계자가 참여하는 다분야 이니셔티브를 소집하여 소프트웨어 투명성에 대해 논의했다. 그 결과물 중 하나가 소프트웨어 자재 명세서(이하 SBOM: Software Bill of Materials) 개념으로, NTIA는 이를 ‘하나 이상의 식별된 컴포넌트와 그 관계 및 기타 관련 정보의 목록’으로 정의하였다. 이 이니셔티브는 국제적으로 SBOM 개발 및 채택에 영향을 미쳤다.

SBOM은 시판 전 및 시판 후 활동들(즉, 제품 수명 전주기(이하 TPLC: Total Product Life Cycle)) 안에서 사이버보안 위험 관리 절차를 개선하는 데 활용할 수 있는 자원이다. 예를 들어, 시판 전 단계에서 MDM은 기기 개발 중에 SBOM 자원을 사용하여 알려진 소프트웨어 취약점을 추적하고 사이버보안 위험이 있는 기기가 출시되는 것을 방지할 수 있다. 시판 후 단계에서 MDM은 SBOM을 취약점 모니터링 절차를 보완하기 위한 자원으로 사용하여 이미 시장에 출시된 위험에 노출된 기기를 식별할 수 있다.

SBOM은 기본 또는 보조 자원으로서 TPLC 전반의 사이버보안 위험 관리 절차 개선을 지원할 수 있다. 이점으로는 다음이 포함될 수 있지만 이에 국한되지는 않는다.

- 기기의 소프트웨어 컴포넌트를 더 빠르고 포괄적으로 식별할 수 있다.
- 더 나은 정보에 기반한 의사 결정을 통해 더욱 안전한 소프트웨어 개발을 지원한다.
- 공급업체와 이해관계자 간의 소프트웨어 투명성을 높인다.

SBOM의 이점을 최대한 활용하려면 의료기기 사이버보안을 위한 원칙 및 실무(이하 IMDRF N60 지침: IMDRF/CYBER WG/N60FINAL:2020)에서 제시하는 사이버보안 위험 관리 도구 및 절차와 함께 SBOM을 사용해야 한다. IMDRF N60 지침에는 MDM이 작성하여 의료기기 사용자에게 제공해야 하는 고객 보안 문서의 일부로 SBOM이 포함되어 있다. 의료기기 SBOM은 TPLC 전반에 걸쳐 MDM과 의료서비스제공자(이하

HCP: Healthcare Providers) 모두에게 도움이 된다. 예를 들어, SBOM은 소프트웨어 컴포넌트의 수명 종료(이하 EOL: End of Life)를 추적하고 대비하는 데 효과적인 관리 도구이다. MDM이 소프트웨어 컴포넌트들과 그 수명 종료 날짜를 알고 있으면 MDM은 관련 위험에 대해 자신과 고객에게 더 나은 대비를 할 수 있도록 하여 MDM의 품질 관리 역량을 향상한다. 의료기기 사용자는 향상된 투명성과 사이버보안 정보 공개를 통해 개별 위험 프로필과 사이버보안 역량에 따라 사이버보안 활동을 실행할 수 있는 이점을 누릴 수 있다. 예를 들어, 구매 및 설치 이전에 제공된 SBOM을 통해 HCP는 구매 전에 어떤 기기가 위험 프로필에 맞게 배치될 수 있는지 또는 사이버보안 문제를 일으킬 수 있는 오래된 소프트웨어가 포함되어 있을 수 있는지 알 수 있다. MDM은 제품과 함께 SBOM을 제공해야 한다. SBOM은 이러한 모든 HCP의 다양한 요구 사항, 자원 및 기능을 지원해야 한다. SBOM 채택이 증가함에 따라 도구, 서비스, 사이버보안 성숙도가 발전하면 HCP는 SBOM을 최대한 활용할 수 있을 것이다. 또한 SBOM이 제공되면 고객(HCP 또는 환자)은 의료기기의 사이버보안 위험을 더 잘 평가할 수 있다.

규제 기관에 시판 전 제출 시 제공되는 SBOM은 MDM이 성숙한 사이버보안 프로그램을 갖추고 있음을 나타내는 하나의 지표이다. 또한 SBOM을 통해 규제 기관은 제품에 대한 보다 완벽한 유익성-위험성 평가를 수행할 수 있다. 시판 후에는 시판된 의료기기가 SBOM에 접근할 수 있다는 보다 포괄적인 이해를 통해 MDM, HCP 및 규제 당국이 위협, 취약점 및 취약점 공격(익스플로잇) 영향을 예측하고

해결하는 데 MDM의 의견을 활용할 수 있다.

여러 부문에서 SBOM 채택이 증가함에 따라 각 기관에서 SBOM의 가치도 높아질 것이다. 이해관계자는 SBOM 생성, 관리, 배치, 수집, 활용과 같은 SBOM의 다양한 역할과 용도를 가지고 있다.

이 지침은 SBOM에 대한 개괄적인 설명과 SBOM의 생성 및 사용에 대한 모범 실무를 제공한다. 이 문서의 목적은 MDM, HCP, 규제 기관과 같은 의료기기 이해관계자와 관련된 SBOM 및 소프트웨어 투명성 구현에 대해 보다 자세히 설명하는 것이다. 이 지침에서 HCP는 의료 제공기관(이하 HDO: Healthcare Delivery Organizations)이 포함된다.

SBOM 혜택에 대한 추가 정보는 NTIA의 FAQ 문서와 ‘공급망 전반에서 SBOM의 역할 및 혜택’ 문서에서 확인할 수 있다.

2.0 범위

이 문서는 소프트웨어(펌웨어 및 프로그램 가능 논리 제어기(이하 PLC: Programmable Logic Controller)를 포함)를 내장한 의료기기(예: 페이스메이커, 인퓨전 펌프 등)나 소프트웨어 의료기기(이하 SaMD: Software as a Medical Device)에 대한 사이버보안을 고려한다. 이 문서는 의료기기 MDM과 HCP의 역할과 책임을 강조하고 체외진단 의료기기를 포함한 의료기기에서 소프트웨어 사용의 투명성을 높이고 SBOM을 구현하는 데 대한 권장 사항을 제공한다. 주로 MDM과 HCP에 초점을 맞추고 있지만 그 외의 이해관계자(의료기기 사용자, 규제 기관, 소프트웨어 컴포넌트 벤더(Vendor)등을 포함)에게도 이 문서에서 논의된 개념이 유용할 수 있다.

사이버 의료 환경을 보호하는 것은 HCP와 MDM의 공동 책임이다. SBOM은 환자 피해 가능성을 완화하는 데 도움이 될 수 있으므로 안전을 지원하는 공통 도구이다. 이 문서의 목적은 다음과 같다.

- MDM에게 SBOM 생성, 관리 및 배포에 대한 권장 사항 제공
- HCP에게 SBOM 수집 및 관리에 대한 권장 사항 제공
- MDM과 HCP의 관점에서 위험 관리, 취약점 관리 및 사고 대응에 대한 SBOM 사용 사례를 시연

SBOM은 종합적인 보안 위험 평가를 대체할 수 없으며, 기기 수준에서

보안 위험 평가를 수행하려면 해당 기기의 의도된 용도, 아키텍처 및 설계에 대한 지식이 필요하다.

대부분의 규제 기관이 의료기기 안전성과 성능에 대한 권한을 가지고 있기 때문에, 이 지침의 범위는 규제 대상 의료기기와 관련된 환자 피해 가능성을 고려하는 것으로 한정된다. 의료기기의 타입 및 규정 관할권 사이의 차이로 인해 다른 또는 추가적인 사항이 필요한 특정한 상황이 발생할 수 있다. 예를 들어, 성능에 영향을 줄 수 있는 위협, 임상적 운영에 부정적인 영향을 미칠 수 있는 위협, 오진단 또는 잘못된 치료를 초래할 수 있는 위협이 이 문서의 범위에 포함된다. 개인정보(데이터) 보호 침해와 같은 다른 유형의 피해는 이 문서의 범위에 포함되지 않지만, 이러한 문제가 중요하며 SBOM이 유용한 피해 완화 도구가 될 수 있다고 여겨진다.

이 문서는 원격 컴퓨팅 환경에서 제공되는 클라우드 서비스에 한정된 SBOM 이슈 및 권장 사항을 다루지 않는다. (이때, 클라우드 서비스는 컴퓨팅(예: 네트워크, 서버, 스토리지, 애플리케이션) 서비스에 대한 주문형 인터넷 접근을 의미한다.) 규제 대상 의료기기 시스템의 컴포넌트로 포함되는 클라우드 서비스도 안전성과 유효성에 위험을 초래할 수 있다. MDM은 위험 평가 시 클라우드 서비스 및 클라우드 소프트웨어도 검토 대상에 포함해야 한다는 점을 인지해야 한다. MDM이 통제하는 사설 클라우드가 아닌 서드파티(Third Party) 제공 클라우드를 활용할 경우 클라우드 서비스가 더욱 복잡해지기 때문에, 본 첫 번째 IMDRF SBOM 지침(N73)에서는 클라우드 기술이 아직은 SBOM에 명시적으로

포함되지 않았다. 그러나 기술이 발전하고 규제적 관점에서 클라우드에 대한 이해가 높아짐에 따라 SBOM의 맥락에서 클라우드 기술의 잔존 위험을 다루는 것이 중요해질 것이고 향후 작업에서 다뤄질 것으로 예상된다.

이 문서는 이전 IMDRF N60 지침을 보완하는 것으로, 관련 의료기기의 범위와 환자 피해 가능성에 대한 초점은 변함이 없으며, 사이버보안이 이해관계자 간의 공동 책임이라는 점을 인식하고 있다.

SBOM은 라이선스 및 지적재산권을 포함한 다양한 소프트웨어 투명성 문제를 다룰 수 있지만, 이 문서에서는 SBOM과 관련된 사이버보안 문제에 중점을 둔다.

3.0 정의

이 문서의 목적상, 용어 및 정의는 IMDRF/GRRP WG/N47 FINAL: 2018에 명시된 것과 아래 용어가 적용된다.

3.1 **애플리케이션 프로그래밍 인터페이스(API)**: 애플리케이션 프로그램에서 네트워크 서비스, 기기 또는 운영 체제에 접근하는 데 사용할 수 있는 표준 소프트웨어 인터럽트, 호출, 함수 및 데이터 형식의 집합(ISO 10303-1:2021)

3.2 **자산(Asset)**: 개인, 조직 또는 정부에 가치가 있는 물리적 또는 디지털 개체(ISO 81001-1:2021)

3.3 **자산 관리(Asset Management)**: 자산에서 가치를 실현하기 위한 조직의 조정된 활동(ISO/IEC 9770-5:2015)

3.4 **변경 관리(Change Management)**: 모든 변경 사항을 기록, 조정, 승인 및 모니터링하는 절차(ISO 81001-1:2021)

3.5 **구성(Configuration)**: 정보 처리 시스템의 하드웨어와 소프트웨어가 구성되고 상호 연결되는 방식(ISO/IEC 2382:2015)

3.6 **사이버보안(Cybersecurity)**: 정보와 시스템이 무단 접근, 사용, 유출,

중단, 수정 또는 파괴와 같은 비인가 활동으로부터 보호되어 기밀성, 무결성, 가용성과 관련된 위험을 수명 주기 전체 동안 수용할 수 있는 수준으로 유지되는 상태(ISO 81001-1:2021)

3.7 **사이버보안 사고(Cybersecurity Incident)**: 조직에 영향을 미치는 것으로 판단되어 대응과 복구가 필요한 사이버보안 사고(미국 국립 표준 기술 연구소(NIST) 2018 중요 인프라 사이버보안 개선 프레임워크, 버전 1.1)

참고: 사이버보안 사건(Event)은 조직 운영에 영향을 미칠 수 있는 사이버보안 변경 사항(임무, 역량 또는 평판을 포함하되 이에 국한되지 않음.)을 말한다.

3.8 **컴포넌트(Component)**: (a) 시스템의 물리적 또는 논리적 부분을 형성하고, (b) 특정한 기능과 인터페이스를 가지며, (c) 시스템의 다른 부분과 독립적으로 존재하는 것으로 취급되는(예: 정책 또는 사양) 시스템 자원의 모음(ISO 81001-1:2021)

참고: 의료기기에서 컴포넌트에는 완제품, 포장 및 라벨이 부착된 기기의 일부로 포함되도록 의도된 모든 원자재, 물질, 조각, 부품, 소프트웨어, 펌웨어, 라벨 또는 조립품이 포함된다.

3.9 **해시(Hash), 해시값(Hash Value)**: 임의적인 길이의 데이터에서 고정된 길이의 랜덤 값을 생성하는 계산 방법인 해시 함수로

계산된 값(ISO 17090-4:2020)

3.10 **레거시 의료기기(동의어: 레거시 기기)(Legacy Medical Device, syn. Legacy Device)**: 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 없는 의료기기(IMDRF/CYBER WG/N60FINAL:2020)

3.11 **수명 주기(Life Cycle)**: 제품 또는 시스템의 초기 구상부터 최종 폐기 및 처분에 이르는 일련의 모든 수명 단계(ISO 81001-1:2021)

3.12 **제품(Product)**: 조직과 고객 간에 어떤 트랜잭션 없이도 생산될 수 있는 조직의 산출물(ISO 81001-1:2021)

3.13 **출시와 업데이트(Releases and Update)**: 의료기기 소프트웨어에 진행하는 수정, 예방, 적응형 또는 완벽형 수정 사항

참고 1: ISO/IEC 14764:2006에 설명된 소프트웨어 유지 관리 활동에서 파생된 개념

참고 2: 업데이트에는 패치 및 구성 변경 사항이 포함될 수 있다.

참고 3: 적응형 및 완벽형 수정 사항은 소프트웨어의 개선 사항이다. 이러한 수정사항은 의료기기의 설계 사양에 포함되지 않았던 수정사항이다.

3.14 **리포지터리(Repository)**: 데이터 검색을 허용하는 조직화된 지속적인 데이터 저장소(ISO/IEC/IEEE 26511:2018)

3.15 **리스크 관리(Risk Management)**: 위험을 분석, 평가, 통제 및 모니터링하는 업무에 관리 정책, 절차 및 실무를 체계적으로 적용하는 것(ISO/IEC 지침 63:2019)

3.16 **소프트웨어 자재 명세서(SBOM: Software Bill of Materials)**: 하나 이상의 식별된 컴포넌트, 컴포넌트 간의 관계 및 기타 관련 정보의 목록

참고: 종속성이 없는 단일 컴포넌트에 대한 SBOM은 해당 컴포넌트의 목록일뿐이다. '소프트웨어' 는 '소프트웨어 시스템'으로 해석될 수 있으므로 하드웨어(펌웨어가 아닌 실제 하드웨어)와 매우 낮은 수준의 소프트웨어(예: CPU 마이크로코드)도 포함될 수 있다.(미국 국가통신정보국(NTIA :National Telecommunications and Information Administration), 소프트웨어 컴포넌트 투명성 프레임워크: 공통 소프트웨어 자재 명세서(SBOM) 수립 2021-10-21).

3.17 **소프트웨어 컴포넌트(Software Component)**: 소프트웨어 시스템 또는 모듈, 단위(Unit), 데이터 또는 문서와 같은 요소를 지칭하는 데 사용되는 일반적인 용어(IEEE 1061)

참고: 소프트웨어 컴포넌트에는 여러 개의 단위가 있거나 하위 수준의 소프트웨어 컴포넌트가 여러 개 있을 수 있다.

3.18 **소프트웨어 구성 분석(Software Composition Analysis)**: 하나 이상의

도구를 사용하여 코드 베이스를 스캔하고 어떤 코드(예: 비공개 소스 소프트웨어, 무료 및 오픈 소스 소프트웨어, 라이브러리 및 패키지)가 포함되어 있는지 식별

참고: 이러한 도구는 포함된 코드와 관련된 보고된 취약점도 체크할 수 있다. (https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf)

3.19 **소프트웨어 투명성(Software Transparency)**: 소프트웨어의 개략적 구조로서, 소프트웨어의 모든 프레임, 계층 및 컴포넌트를 검토

3.20 **시스템(System)**: 하나 이상의 기능을 수행하기 위해 구성된 상호 작용하는 엘리먼트 또는 자산의 조합(ISO/IEC/IEEE 12207:2017)

3.21 **서드파티 소프트웨어(Third-party Software)**: 관련 당사자와 독립적인 것으로 인정되는 개인 또는 단체가 제공하는 소프트웨어 (ISO/IEC 지침 2로부터 수정됨)

참고: 관련 당사자는 일반적으로 공급자(‘제1 당사자’) 및 구매자(‘제2 당사자’)의 이해관계이다.

3.22 **사용 사례(Use Case)**: 시스템(또는 다른 개체)이 시스템의 사용자(Actor)와 상호 작용하면서 수행할 수 있는 일련의 활동(Action) 및 변형 사항을 명시한 것(ISO/IEC 23643:2020)

3.23 **취약점 악용 가능성 교환(VEX: Vulnerability Exploitability eXchange)**: 특정 제품의 취약점 상태에 대한 기계 판독할 수 있는 표현

3.24 **취약점(Vulnerability)**: 하나 이상의 위협에 의해 악용될 수 있는 자산 또는 통제 약점(ISO/IEC 27000:2018)

3.25 **취약점 관리(Vulnerability Management)**: 소프트웨어 취약점을 식별, 분류, 우선순위 지정, 수정 및 완화하는 주기적인 실무

4.0 SBOM 프레임워크 개요

높은 수준에서 SBOM 콘텐츠는 MDM에 의해 수집되어 소프트웨어 컴포넌트 리포지터리에 보관된다. (또한 NTIA의 '소프트웨어 공급업체 플레이북: SBOM 생산 및 제공' 참조) 그 후 MDM은 HCP가 활용할 수 있도록 기기 SBOM을 컴파일 및 생성하여 배포용으로 출시한다. 본 장에서는 MDM 및 HCP 관점에서 SBOM의 생성, 배포 및 수집에 대해 자세히 알아본다.

그림 1은 SBOM 생성/수집을 통해 MDM과 HCP 간의 정보 공유가 가능해지고, 소프트웨어 투명성이 강화되는 상위 수준 프레임워크를 보여준다. 이 프레임워크는 MDM과 HCP 모두를 위한 고려 사항을 다룬다.

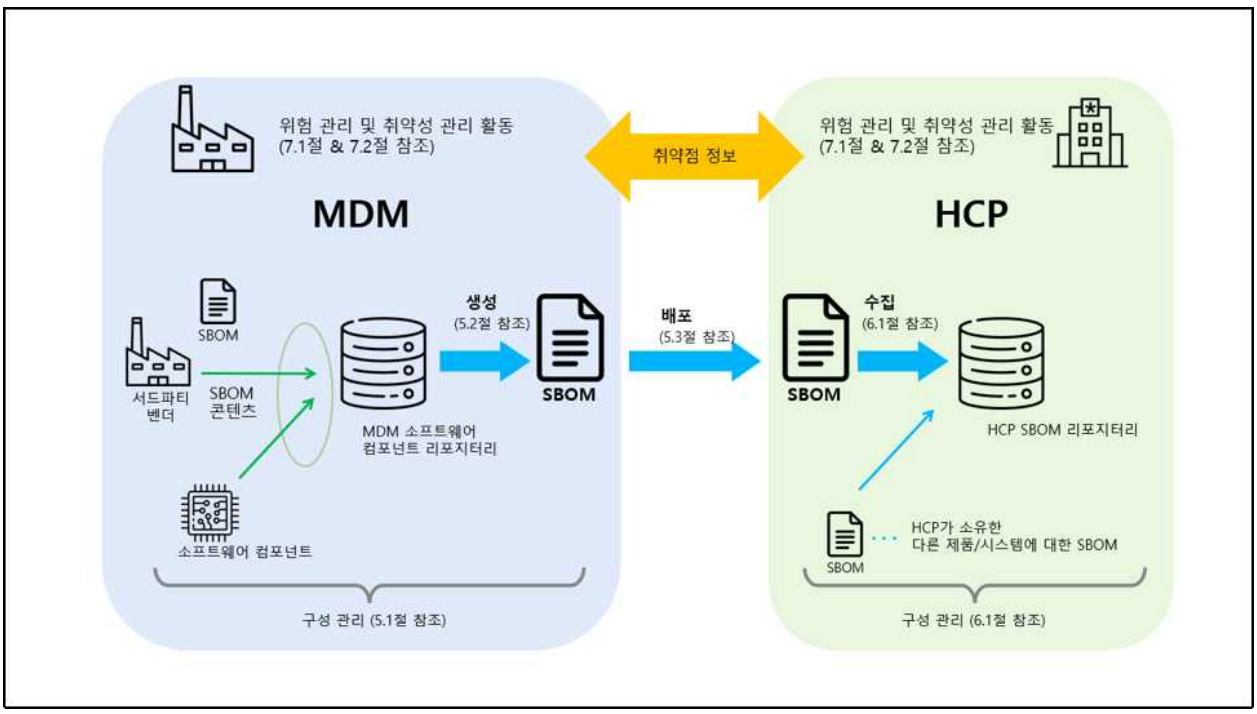

그림 1 SBOM을 위한 상위 수준 프레임워크

5.0 MDM 고려 사항 개요

본 장에서는 SBOM에 대한 MDM의 고려 사항에 대한 개요를 제공하며, SBOM 콘텐츠 수집, SBOM 생성, SBOM 배포, SBOM 콘텐츠 유지(취약점 모니터링 및 변경 관리 포함) 등을 다룬다. 한 가지 유의해야 할 점은 기기 SBOM 자체는 유지되지 않는다는 점이다. 즉, 기기의 새로운 버전이 만들어지면 새로운 기기 SBOM이 생성되고 출시되는 것이다. 그러나 기기의 최종 사용자 관점에서는 새로운 기기 SBOM이 기존의 기기 SBOM에 대한 업데이트라 볼 수 있고, 이 업데이트를 가능하게 하려면 SBOM 콘텐츠에 대한 관련 문서 및 절차를 유지해야 한다. ‘SBOM 콘텐츠 유지’라는 용어와 이 설명의 의도는 그림 2에서 좀 더 자세히 설명한다.

소프트웨어 개발 수명 주기(SDLC: Software Development Life Cycle)의 설계-코드-제작-테스트 단계에서 다양한 타입의 소프트웨어 컴포넌트가 의료기기에 통합된다. 이러한 컴포넌트에 대한 SBOM 콘텐츠는 구성 관리 작업의 일환으로 MDM 소프트웨어 컴포넌트 리포지터리에 수집되고 저장되어야 한다. SBOM은 이 리포지터리에서 생성되어 배치/출시 작업을 통해 HCP에게 배포되어야 한다. HCP는 구매 과정 중이나 소프트웨어 출시 시점에 SBOM을 얻을 수 있다. SBOM이 출시된 후, 취약점 모니터링을 통해 관련 소프트웨어 컴포넌트에 대한 변경 관리가 트리거되고, 다시 SBOM 콘텐츠 수집과 소프트웨어 컴포넌트 리포지터리로 피드백된다. 그림 2는 SDLC를 통한 SBOM

관리를 좀 더 자세히 보여준다.

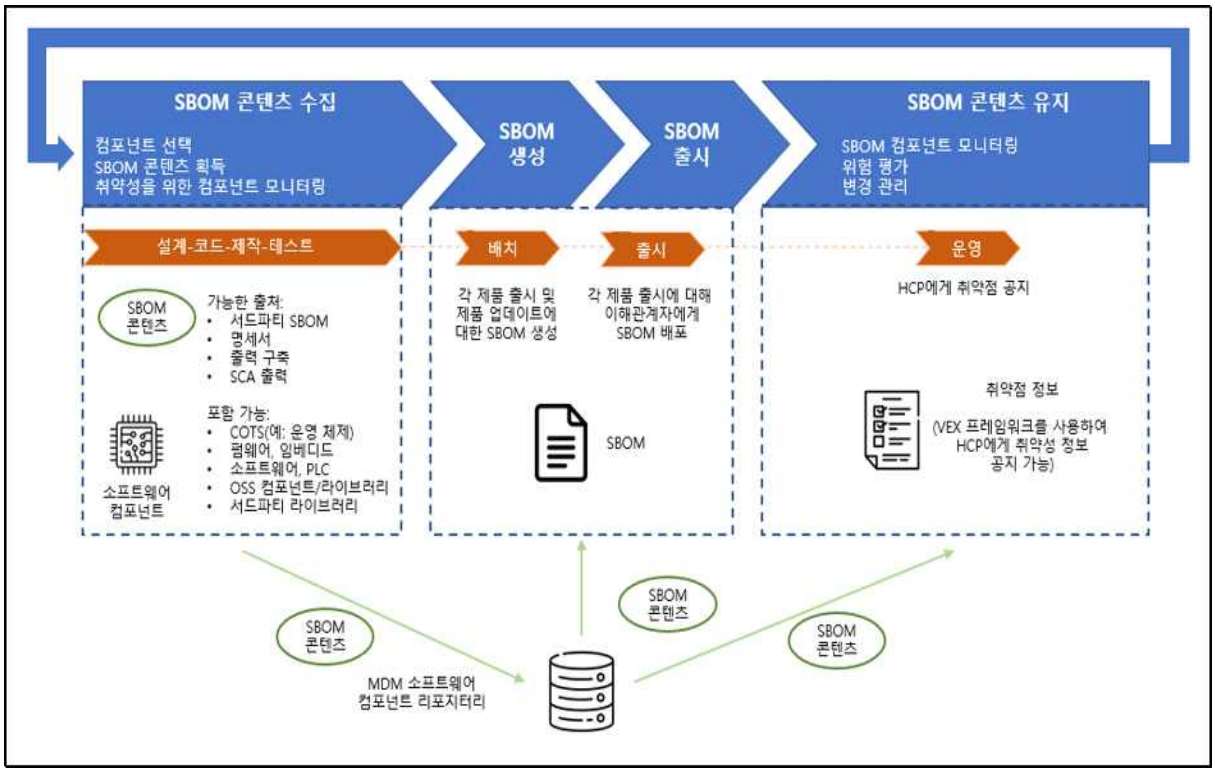

그림 2 소프트웨어 개발 수명 주기(SDLC)에 걸친 SBOM 관리

5.1 SBOM 콘텐츠 수집

SBOM 콘텐츠 수집은 SDLC의 설계 단계에서 시작된다. SBOM 콘텐츠는 다음과 같은 다양한 소스에서 수집될 수 있다.

- 소유권이 있는 소프트웨어 개발 문서
- 상용 소프트웨어 벤더가 제공하는 서드파티 SBOM 문서
- 오픈 소스 소프트웨어(이하 OSS: Open Source Software)와 함께 제공되는 문서
- 소프트웨어 구성 분석(이하 SCA: Software Composition Analysis) 도구에 의해 생성된 출력물

적용할 수 있는 SBOM 콘텐츠는 설계-코드-제작-테스트 단계에서 수집되며, MDM 소프트웨어 컴포넌트 리포지터리에 유지 관리된다. 이때 의료기기 시스템 전체에 대해 SBOM 콘텐츠를 수집해야 하며, 의료기기 시스템의 일부인 주변 기기 내의 컴포넌트에 대해서도 수집되어야 한다. 이를 위해 다양한 소스와 도구가 필요할 수 있다. 예를 들어, 컴포넌트 식별을 위해 SCA 도구를 이용한 제품 스캔 방법이 사용될 수 있다. 또한 펌웨어, 임베디드 소프트웨어 및 PLC와 같은 컴포넌트에 대해서는 공급업체가 SBOM 콘텐츠를 제공할 수도 있다. 위와 같이 다양한 방법으로 수집된 SBOM 콘텐츠는 MDM의 소프트웨어 컴포넌트 리포지터리에서 통합된다.

MDM 소프트웨어 컴포넌트 리포지터리에 포함될 수 있는 컴포넌트 타입 및 콘텐츠를 수집하는 데 사용되는 도구에 대한 추가적인 세부 정보는 9.1. 부록에서 확인할 수 있다.

5.2 SBOM 생성

MDM은 전체 소프트웨어 공급망을 고려하여 적용할 수 있는 SBOM 콘텐츠를 집계하고 각 제품 출시 및 제품 업데이트 시 하나의 최종적인 기기 SBOM을 생성한다. 또한, SBOM은 일관된 출력을 보장하기 위해 정의되고 확립된 방법론을 따라 생성되어야 하며, 각 제품 출시 및 업데이트 시 생성된 최종 기기 SBOM은 제품의 수명 주기 동안 업데이트되고 유지 관리되어야 한다.

다음에서는 SBOM 요소 및 형식에 대한 고려 사항을 설명한다. SBOM 생성 및 도구에 대한 추가 정보는 NTIA의 ‘SBOM 생성을 위한 지침(How to Guide for SBOM Generation)’에서 찾을 수 있다.

5.2.1 SBOM 요소 및 형식

각 SBOM 항목에는 각 소프트웨어 컴포넌트를 식별할 수 있는 정보가 포함되어야 한다. SBOM 항목에 포함될 수 있는 정보는 다양할 수 있지만, 일반적으로 SBOM의 수준에 따라 유용성이 영향을 받는다. 가능한 한 완전한 정보를 담은 SBOM을 만들어야 더 빠른 취약점 식별과 평가가 가능해지고, 기기의 사이버보안이 향상된다. NTIA의 권고 사항에 따라 의료기기 사이버보안을 위해 기본 SBOM은 다음 요소를 포함해야 한다.

- 작성자 이름: SBOM 파일을 생성한 개체(예: 개인, 조직 등)를 의미한다.
- 타임 스탬프: SBOM 데이터의 날짜 및 시간 기록
- 소프트웨어 컴포넌트 벤더(공급업체): 컴포넌트를 생성, 정의, 식별하는 개체이다. 소프트웨어 컴포넌트 벤더 이름은 일반적으로 상용 소프트웨어의 법적 비즈니스 이름을 지칭해야 한다.
- 소프트웨어 컴포넌트 이름: 최초 공급업체가 정의한 소프트웨어 단위에 할당된 명칭
- 소프트웨어 컴포넌트 버전: 공급업체가 이전에 식별된 버전으로부터 소프트웨어의 변경 사항을 지정하는 식별자
- 고유 식별자: 컴포넌트를 식별하기 위해 사용되거나 관련 데이터베이스에 대한 조회 키로 사용되는 식별자
- 관계: 하위의 부품 컴포넌트 X가 소프트웨어 Y에 포함되는 관계

SBOM에 포함된 요소는 식별을 가능하게 하는 기본 정보로 구성되지만, 필요에 따라서는 다른 정보를 추가 요소로 SBOM에 추가하거나 핵심

SBOM에 대한 보충 정보로 추가할 수 있다. 예를 들어 컴포넌트 해시는 컴포넌트의 존재를 관련 데이터 소스에 매핑하는 데 도움이 될 수 있으므로 권장된다. 또한, 기기의 수명 주기와 관련된 고려 사항(예: 소프트웨어 컴포넌트의 EOS 날짜)는 TPLC 전반에 걸쳐 의료기기 위험 관리에 도움이 되므로 보충 정보로 제공될 수 있다.

MDM은 포함될 기본 요소를 고려하는 것뿐만 아니라 SBOM의 형식도 고려해야 한다. 현재 사용할 수 있는 몇 가지 자동화된 SBOM 형식에는 사이클론 DX(CycloneDX), 소프트웨어 패키지 데이터 교환(이하 SPDX: Software Package Data Exchange), 소프트웨어 식별(이하 SWID: Software Identification) 등이 있다. 이러한 형식에 대한 추가 정보(SPDX 및 SWID를 위한 자세한 의료기기 예시 포함)는 NTIA의 'SBOM 생성 지침(How to Guide for SBOM Generation)'에서 찾을 수 있다.

5.3 SBOM 배포

SBOM 배포는 SBOM 정보를 제조업체에서 HCP 또는 사용자에게 전송하는 절차이다. MDM은 인식 제고, 접근 권한 제공, 업데이트 푸쉬 등 SBOM을 배포하는 최선의 방법을 고려해야 한다. 배포 방법 중에는 전자 파일 또는 제품이나 MDM의 웹사이트에 있는 애플리케이션 프로그래밍 인터페이스(API)를 고려할 수 있다. 현재로서는 SBOM을 가장 잘 배포하는 하나의 방법은 없지만, 표준화된 자동 검색 및 교환 메커니즘의 사용이 권장된다.

첫째, HCP는 SBOM의 존재를 인지할 필요가 있다. SBOM은 처음에 구매 절차의 일부로 HCP에게 제공되어야 한다. 예를 들어, 제품의 고객 보안 문서(IMDRF/CYBER WG/N60FINAL:2020), 의료기기 보안을 위한 제조업체 공개 진술서(MDS^2, ANSI/NEMA HN 1-2019), 출판/구독 시스템과 같은 공유 통신 채널 또는 의료기기의 출판 인터페이스와 같은 형태로 포함될 수 있다. 의료기기는 자주 업데이트되므로 네트워크를 통해 제품 및 소프트웨어 버전을 표준화된 방식으로 쉽게 식별할 수 있는 메커니즘이 권장되며 이를 통해 자동화된 업데이트가 가능하게 될 것이다.

둘째, MDM은 SBOM을 HCP에게 배포하거나 HCP가 접근할 수 있게 해야 한다. 기존 방법은 일반적으로 다음 세 가지 범주 중 하나에 속한다:

- SBOM이 MDM에서 HCP로 직접 제공된다. 또는
- SBOM이 의료기기에 저장된다. 또는
- SBOM이 리포지터리를 통해 HCP에게 제공된다. SBOM 리포지터리에는

동일하거나 또는 다른 MDM의 여러 다른 제품의 SBOM 모음이 포함된다.

- MDM 관리 리포지터리에는 단일 MDM의 기기에 대한 SBOM만 포함되지만, 중앙 리포지터리에는 여러 MDM이 만든 서로 다른 기기에 대한 SBOM이 포함된다.
- 중앙 리포지터리는 서드파티 서비스가 관리하거나 HCP가 관리할 수 있다. (즉, HCP는 MDM으로부터 받은 기기 SBOM을 중앙 집중화된 위치에 통합하여 사용 편의성을 높일 수 있다.) HCP가 관리하는 리포지터리에 대한 추가 정보는 6.1.1.절을 참조하면 된다.

완전한 전체 목록은 아니지만, 다음 표는 SBOM 배포 방법에 대해 MDM이 고려해야 할 장단점을 개요로 보여준다:

표 1 SBOM 생성 방법에 따른 장점 및 단점

배포 방법	장점	단점
MDM의 고객 보안 문서에 포함	• 특수 도구 불필요	• 자동화되어 있지 않음. • 문서를 자주 업데이트하여 사용자에게 배포하여야 함. • 문서를 기기 자체에 재연결하는 방법이 필요함. (강력한 자산 관리) • SBOM 접근을 통제하기 어려움.
MDM에서 별도 문서 (전자 문서 포함)로 제공	• 특수 도구 불필요 • SBOM 접근 통제 강화 • 기계 판독 선호	• 자동화되어 있지 않음. • 문서를 자주 업데이트하여 사용자에게 배포하여야 함. • 문서를 기기 자체에 재연결하는 방법이 필요함. (강력한 자산 관리)
디스플레이, (간접) 참조 또는 다운로드를 통해 의료기기에서 접근 가능	• 항상 올바른 버전이 가능 • 사용자의 통제가 가능 • SBOM 접근에 대한 통제 강화	• 자동화되어있지 않음. • 정보를 접근하기 위해서는 먼저 기기에 접근해야 함.

		• 기기에 정보를 추출할 수 있는 수단이 없을 가능성이 있음. (예: 사용자 인터페이스, USB 포트, 네트워크 연결 등) • 기기에 충분한 메모리 공간이 필요함. • (배터리로 작동하는 의료기기의 경우) 추가적인 배터리 용량을 필요로 할 수 있음.
의료기기의 API에서 접근 가능	• SBOM 정보에 대해 강화된 접근통제 가능 • 자동화된 절차 사용 가능	• 표준 API가 정의되지 않음. • 도구가 필요함. • 의료기기에 네트워크 연결이 필요함.
MDM 관리 리포지터리	• SBOM 정보에 대해 강화된 접근통제 가능 • 자동화된 절차에서 사용 가능	• 고객이 다수의 MDM의 사이트/리포지터리를 체크해야 함.
중앙 리포지터리	• 고객이 정보에 효율적으로 접근할 수 있는 방법 (예: 개별 제조업체 사이트/리포지터리 확인 불필요) • 자동화된 절차에서 사용 가능	• 서드파티 서비스 이용 시 MDM에 대한 지적재산권, 책임 및 기타 고려 사항이 있음. • 한 기관에서 동일 기기에 대해 업데이트 상태가 다른 복수의 의료기기가 있는 경우 최신 SBOM 뿐만 아니라 버전마다 다른 SBOM을 관리하여 버전 관리 문제를 해결해야 함.

SBOM 배포에서 고려해야 할 또 다른 사항은 SBOM 정보를 보호해야 한다는 것이다. 의료기기 SBOM은 업계 모범 실무에 따라 민감/기밀 정보로 분류되어야 한다. MDM에서 외부 수신자, 규제 기관 및 HCP로의 통신 채널은 보호 조치를 지원해야 한다. 이렇게 함으로써 문서가 유출/침해되어 위험에 노출될 가능성을 줄여 준다. 또한 이러한 외부 조직(즉, 기기 SBOM 수신자)은 엄격한 내부 보안 정책과 방침을 유지하여 SBOM의 무결성, 진본성, 기밀성을 보호해야 한다.

5.4 SBOM 콘텐츠 유지 관리

SBOM은 소프트웨어 컴포넌트에 취약점이 있는지를 명시적으로 나타내지 않는다. 대신 SBOM은 다른 자원과 함께 사용되어 의료기기 취약점을 모니터링하는 데 사용될 수 있다. MDM이 HCP에 취약점 정보를 알리는 방법의 하나는 취약점 악용 가능성 교환(이하 VEX: Vulnerability Exploitability Exchange)를 이용하는 것이다.

의료기기의 수명 주기 동안 각 이해 관계자는 서드파티 소프트웨어 컴포넌트에 대한 정확하고 최신 정보에 의존한다. MDM은 의료기기의 소프트웨어 취약점과 관련된 잠재적인 환자 안전 위험을 SBOM을 사용하여 식별, 평가 및 완화할 수 있다. HCP는 SBOM을 사용하여 의료기기의 구매 전과 배치 중에 기기를 평가하며, MDM과 협력을 통한 사이버보안 위험을 관리할 수 있다.

취약점 모니터링은 관련 소프트웨어의 변경이 필요하다고 판단될 때 변경 통제 사건을 발생시킬 수 있다. MDM은 기기 소프트웨어에 대한 모든 변경 사항이 SBOM에 반영되고 적절한 후속 조치가 취해질 수 있도록 하기 위해 기존의 변경 관리 통제(즉, IT 환경의 변경 사항을 식별, 문서화 및 승인하는 데 사용되는 절차)를 활용해야 한다. 궁극적으로 SBOM 내용이 변경되면 변경된 소프트웨어 컴포넌트를 포함하는 업데이트된 기기 SBOM을 생성하고 적절한 이해관계자에게 배포해야 한다.

5.4.1 SBOM 및 변경 관리

최근 의료기기 개발의 시판 전 및 시판 후 변경 관리 절차에 소프트웨어 개발 수명 주기(SDLC)가 통합되었지만, 서드파티 컴포넌트 변경 관리는 여전히 많은 MDM에게 새로운 영역이다. 기기 소프트웨어를 변경하는 모든 사건은 새로운 SBOM을 생성해야 함을 이해하는 것이 중요하다. 이러한 사건에는 다음과 같은 사항이 포함되며, 이에 국한되지는 않는다.

- 취약점 해결을 위한 업그레이드, 업데이트, 또는 패치
- 의료기기 소프트웨어에 새로운 기능 추가
- 한 소프트웨어 컴포넌트를 다른 소프트웨어 컴포넌트로 교환
- 소프트웨어 컴포넌트 추가 또는 삭제
- EOL 또는 EOS 결정, (보안) 패치 또는 시장에 나오는 새로운 버전으로 인해 기기 하드웨어 또는 운영 체제 내에 있는 서드파티 컴포넌트의 변경

소유권이 있는 의료기기 소프트웨어 및 서드파티 소프트웨어 라이브러리를 포함하는 SBOM에는 변경 통제를 적용해야 한다. 변경 통제 정보는 내부 버전 관리에 중요할 뿐만 아니라 MDM이 HCP에게(보안 취약성) 완화 조치가 취해졌음을 알리는 데도 도움이 된다.

SBOM의 변경 사항은 정기적으로 HCP에게 전달되어야 하며, 적절한 배포 플랫폼에서 실행 가능하고 기계 판독이 가능한 형식으로 제공되어야 한다.

5.5 도전 과제

SBOM은 소프트웨어 투명성을 통해 환자 안전을 강화할 수 있는 큰 잠재력을 가지고 있다. 시판 전 및 시판 후 활동의 일부로 종합적인 SBOM을 생성, 모니터링 및 배포하는 것은 MDM에게는 어려운 과제일 수 있다. 적절한 도구와 내부 절차가 필요하다.

이 절에서는 SDLC 전반에 걸쳐 SBOM을 구현하는데 따른 일부 중점적인 도전 과제를 설명한다.

- **현재 시판 중인/레거시 기기용 SBOM**: SBOM은 비교적 최근 개념으로, 아직 채택 중인 단계이다. 일반적으로 과거에 생산된 오래된 기기에 대한 SBOM을 생성하는 경우 기본적인 정보 및 요소가 포함된 SBOM을 확보하기마저도 어려움을 겪을 수 있다. MDM은 서드파티 공급업체가 제공한 SBOM을 통합할 때 최선의 판단을 내려야 하며, 서드파티 공급업체로부터 정보를 얻을 수 없는 경우 구성 분석 도구를 사용하여 해당 SBOM을 보완할 수 있는 방법도 고려해야 한다. 가능한 경우, 운영 체제, 상용 소프트웨어(이하 COTS: Commercial Off-The-Shelf), 오픈 소스 소프트웨어(OSS)와 같은 주요 소프트웨어 컴포넌트에 대해서는 최소한의 범위와 깊이로 SBOM을 구축하는 것이 바람직하다. 이렇게 함으로써 SBOM의 핵심 내용을 확장하고 개선할 수 있다. SBOM의 생성은 HCP 또는 다른 기관에 의해서도 다양한 도구를 사용하여 수행될 수 있다. MDM은 조직의 요구에 가장 적합한 기능을 갖춘 도구(예: MDM의 비즈니스와

관련된 위험에 대한 최적의 인사이트 제공)를 선택하는 데 주의해야 한다. SCA 도구를 잘 선정한다면 원하는 범위와 깊이를 갖춘 SBOM을 생성할 수 있다. 더 나아가서 SCA 도구는 보안/강화를 촉진하기 위해 컴파일러 설정이 올바르게 설정되었는지, 취약점이 있는 코드를 제외하는지, 예기치 않은 시스템 네트워킹 도구의 포함 여부, 디버그 정보가 포함된 파일의 포함 여부 등을 확인할 수도 있다.

- **표준 및 도구**: SBOM 수집, 생성, 배포 및 취약점 모니터링에 사용을 지원하기 위해 표준 및 도구가 사용될 수 있다. 아래에는 표준 및 도구에 대한 높은 수준의 고려 사항이 제시되어 있으며, SBOM 콘텐츠 수집에 사용되는 도구에 대한 좀 더 자세한 내용은 부록 9.1에서 확인할 수 있다. 소프트웨어와 저작자에 대한 안정적이고 글로벌한 식별을 위해서는 좀 더 명확한 표준이 필요한데, 최신의 기술 표준을 정의하기 위해 국제표준이 만들어지고 있다.
  - 표준과 도구는 계속 발전하고 성숙해지므로 MDM은 표준과 도구의 최종본을 기다려서는 안 된다. 대신, MDM은 기본/기초적인 SBOM 개념을 적용하여 초기 SBOM을 생성해야 한다. 예를 들어, SBOM 콘텐츠를 식별하는 도구는 존재할 수 있지만, 이를 기계판독 가능한 형식으로 변환하고 중앙 데이터베이스(예: NIST 국가 취약점 데이터베이스(NVD: National Vulnerability Database))에서 취약한 소프트웨어 컴포넌트를 식별하는 데에는 어려움이 있을 수 있다. 취약점 데이터베이스는 시간이 지남에 따라 변경될 수 있으며 완전하지 않을 수 있다.

- 많은 기관이 표준과 도구를 만들어 내기 위해 노력하고 있으므로, 중장기적으로 MDM은 사용할 수 있는 최신 플랫폼으로(초기 버전의) SBOM을 변환시킬 수 있을 것이다.

- **SBOM 깊이**: SBOM은 각 제품의 출시 또는 업데이트마다 생성되므로 시간이 지남에 따라 동적으로 변할 수 있다. SBOM에 포함할 SBOM 콘텐츠의 적절한 깊이를 정의하는 것은 SBOM을 최신 상태로 유지하기 위해 필요한 자원의 양과 타입에 영향을 미친다. 더 깊은 SBOM 콘텐츠는 더 높은 품질의 SBOM을 생성하고 최종 사용자에게 더 높은 가치를 제공한다. 그러나 더 깊은 콘텐츠는 SBOM을 생성하고 분석하는 데 더 많은 복잡성과 어려움을 동반하게 된다.

- **SBOM 배포**: SBOM 배포와 관련하여 여러 가지 도전과제가 있다고 인정되고 있으며 다음과 같은 과제가 포함된다:(a) 소프트웨어 업데이트 빈도(b) 이에 상응하는 SBOM 업데이트 필요성(c) 사용자 자산 관리 시스템에서 배포된 SBOM의 유지 관리 필요성. HCP는 같은 기기지만 구성이 다른 여러 버전을 운용하고 있을 수 있으며, 이러한 기기는 서로 다른 시기에 새롭게 출시된 소프트웨어로 업데이트될 수도 있다. HCP는 각 기기에 대해 적절한 SBOM을 보유해야 한다.

6.0 HCP 고려 사항 개요

지난 10년 동안 의료 환경은 디지털화되었으며, 디지털 기술은 의료 산업의 모든 부분에 걸쳐 확산되고 있다. 이러한 디지털 혁신으로 인해 관리 및 임상 기능을 수행하기 위한 소프트웨어와 소프트웨어 기반 기기에 대한 의존도가 높아졌다. 불행히도 이러한 디지털화는 사이버 보안 위협의 급격한 증가와 동시에 이루어졌다. HCP 환경은 점점 더 디지털에 의존하고 연결되고 있기 때문에, 대규모 의료 시스템, 소규모 농촌 시설, 홈케어를 포함하는 증가하는 외래진료 등 다양한 HCP 조직에 영향을 미치고 있다.

MDM은 의료기기와 함께 SBOM을 제공해야 한다. 이 장에서는 HCP가 SBOM에 대해 고려해야 할 사항(SBOM의 수집, 적용, 관리 포함)에 대한 개요를 설명한다. 그림 1은 SBOM의 전체 프레임워크를 보여준다.

6.1 SBOM 수집 및 관리

SBOM은 HCP의 위험 관리의 일부로 구매 단계부터 사용된다. HCP는 조직의 네트워크 인프라에 통합하려고 계획하는 모든 기기에 대해 MDM으로부터 SBOM을 요청해야 한다. SBOM을 활용하려면 HCP는 조직이 SBOM을 수집할 수 있는 역량을 보유해야 한다. SBOM을 활용하기 위해서, HCP는 완전하고 정확한 자산 인벤토리를 보유하는 것이 중요하다. 자산 인벤토리에는 고유한 기기 식별자가 있는 최신 의료기기 목록이 포함되어 있어야 하며, 이를 통해 다른 자산 관리 시스템 및 SBOM과 같은 자산 강화 데이터 소스와 상호 연관시킬 수 있어야 한다. HCP는 네트워크에서 실행되는 하드웨어 자산 및 그 연관된 소프트웨어를 이해할 필요가 있다. 수집된 SBOM은 조직의 이익을 극대화할 수 있도록 관리되어야 한다.

이 절에서는 HCP가 SBOM에 대해 고려해야 할 사항에 대한 개요를 보여주며, SBOM 수집 및 관리와 HCP가 관리하는 SBOM 리포지터리에 대한 구체적인 고려 사항 등을 다룬다.

6.1.1 SBOM 수집 및 관리에 대한 고려 사항

HCP는 조직의 네트워크 환경에서 운영되고 있는 하드웨어 자산 및 그 연관된 소프트웨어뿐만 아니라 SaMD도 이해할 필요가 있다. HCP는 개발자로부터 직접 구매한 소프트웨어 또는 맞춤형 개발 소프트웨어를 목록화하려고 할 때 확립된 정보 기술 및 자산 관리 실무를 사용할 수 있다. 그러나 구매한 기기에서 실행되는 소프트웨어는 이러한 확립된 실무를 통해 목록화하기 어렵다. SBOM은 MDM과 HCP 간에 이러한 정보를 투명하게 공유하기 위한 방법이다. 다음은 SBOM 및 HCP가 관리하는 SBOM 리포지터리와 관련된 고려 사항이다.

- **구매**: SBOM은 구매 절차 중에 제공될 수 있으며, 이를 통해 HCP는 기기 컴포넌트를 검토할 수 있다. HCP는 구매와 배송 사이에 SBOM이 변경될 수 있다는 점을 인식해야 한다.

- **표준 형식 및 전달**: SBOM의 전달은 표준 형식과 자동화된 배포 및 수집 메커니즘을 통해 이루어져야 한다. 이를 통해 HCP가 정보를 효율적으로 수집하고 안전한 위치에 저장하여 데이터의 무결성을 보호할 수 있다. 고려해야 할 세 가지 주요 형식은 CycloneDx, SPDX, SWID이다.

- **고유 기기 식별자(UDI: Unique Device Identifier)**: 기기 SBOM은 이상적으로 UDI에 매핑되어야 한다. 즉, HCP는 조직 내의 다양한 모델과 버전이 존재할 수 있는 기기에 기기 SBOM과 정확한 상관

관계를 가지게 할 수 있다. IMDRF UDI 애플리케이션 지침에서 설명된 대로, UDI는 기기 및 MDM에 대한 정확한 매핑을 보장하기 위해 제품 수준에서 참조되어야 하고, 의료기기 소프트웨어 버전 번호 또는 기기 자체의 버전 번호도 가능하다면 포함해야 한다. 기기의 소프트웨어 및 하드웨어 컴포넌트에 대한 표준화된 UDI가 없다면 수동 매핑이 필요할 수도 있다.

- **완성도**: SBOM의 완성도 수준은 SBOM을 활용할 수 있는 범위에 영향을 미친다. SBOM 콘텐츠 정보에는 최소한 작성자 이름(회사명 및/또는 개인 이름), 타임스탬프, 소프트웨어 컴포넌트 공급업체(공급자), 소프트웨어 컴포넌트 이름, 소프트웨어 컴포넌트 버전, 고유 기기 식별자 및 관계가 포함되어야 한다. (5.2.1.절 참조)

- **통신**: 기기 SBOM에서 알려진 취약점이 있는 소프트웨어 컴포넌트가 발견되면, MDM과 HCP간의 통신이 강력히 권장되며, 이를 통해 취약점 해결을 위한 조치가 MDM에 의해 제공되고, 필요한 경우 HCP의 국가/지역 당국의 승인을 받을 수 있게 한다.

- **향상된 기기 관리**: HCP는 향상된 기기 관리를 위해 운용하고 있는 각 기기를 특정 SBOM과 연결하게 해주는 내부 SBOM 리포지터리를 설립 및 관리할 수 있는 능력이 필요하다.
  - 검색 및 질의 능력: 리포지터리에는 알려진 취약점을 가지고 있는 여러 기기를 포함하여, HCP의 다양한 기기 간의 위험을 정확하게

식별하고 관리하기 위한 검색 및 질의 능력이 있어야 한다.

HCP는 취약점 포함 여부를 파악하기 위해 구매한 기기에 포함된 소프트웨어의 중첩 수준을 추적하길 원할 수도 있다.

- 업데이트 및 유지 관리: 리포지터리는 기기의 수명 주기 내내 정확한 최신 SBOM 컨텐츠로 업데이트하고 유지 관리 할 수 있는 능력이 필요하다. 또한 리포지터리는 관리 용이성을 확보하기 위해 자동화된 절차를 가질 필요가 있다.

  기기 및 리포지터리의 수명 주기 동안 형식과 소프트웨어 식별자가 변경될 가능성이 높으므로, SBOM 정보를 문서화하는 임의의 형식의 문서와 UDI간의 매핑을 할 수 있는 일반적인 능력이 SBOM 리포지터리의 가장 중요한 기능이라고 할 수 있다. (ISO/IEC 19770-2:2015에 따르면 SWID 태그는 소프트웨어를 태깅하는 방법 중 하나이다.)

- 보안 리포지터리: SBOM 리포지터리는 정보가 악의적인 개인에 의해 수정되거나 기기 또는 HCP의 네트워크를 공격하기 위한 로드맵으로 사용되는 것을 방지하기 위해 보안이 유지되어야 한다. (예: HCP내에서 필요한 사람만 제한적인 접근이 가능하도록 역할 기반 제한적 접근 제한)

참고: 위의 항목은 일반적인 SBOM 고려 사항이며, 이러한 고려 사항은 MDM에도 적용되므로 5장에서도 논하였다.

6.1.2 SBOM 수집 및 관리 방법

SBOM은 수동 또는 자동화된 절차를 통해 수집할 수 있다. 그러나 수동 절차는 금방 번거로워질 수 있으므로, 모든 규모의 HCP에서는 관리 부담을 줄이기 위해 자동화된 절차가 권장된다. 또한 시간이 지남에 따라 SBOM이 업데이트될 수 있으므로, 자동화는 향후 SBOM 관리에도 도움이 된다. HCP는 운영의 일환으로 무엇보다도 보안 정보 및 사건 관리(이하 SIEM: Security Information and Event Management) 소프트웨어 솔루션을 활용할 수 있으며, SIEM은 네트워크에 연결된 기기, 서버 등에서 데이터를 수집, 저장, 집계 및 분석할 수 있는 장점이 있다. 이러한 SIEM이 SBOM 형식을 읽을 수 있다면, SBOM을 수집하는 데에도 사용할 수 있다.

일부 HCP는 SBOM을 지속적으로 사용하기 위해 구성 관리 데이터베이스(이하 CMDB: Configuration Management Database) 또는 전산화된 설비 유지 관리 시스템(이하 CMMS: Computerized Maintenance Management System)을 통해 벤더 위험 관리(이하 VRM: Vendor Risk Management)) 시스템 내의 SBOM과 연결하거나 통합하는 방법을 모색하고 있다. 경우에 따라, HCP는 이러한 기술을 통해 SBOM을 직접 수집하는 방법을 모색하거나, 맞춤 개발된 소프트웨어 도구 또는 스크립트를 사용해 수집할 수도 있다. 직접 수집 및/또는 맞춤형 도구를 사용하는 경우, HCP는 자신의 데이터 관리 시스템에서 사용하는 전자 형식의 소유권 적인 특성을 고려할 필요가 있다.

전체 목록은 아니지만, 다음 표에는 HCP가 SBOM을 수집하고 관리하는 데 사용할 수 있는 방법의 장단점이 요약되어 있다.

표 2 SBOM 수집 및 관리 방법에 따른 장점 및 단점

SBOM 수집 또는 관리 방법	장점	단점
SIEM	• 직접 수집 가능	• SBOM 형식과의 호환 • 소유권이 있는 SBOM과 함께 사용할 수 있는 기능 • 검색을 위한 접근 감소
CMDB / CMMS	• 높은 검색 가능성 • 직접 수집 가능(일부 벤더가 NTIA 안내집에 참여 - Nuvolo 및 ServiceNow) • 개별 자산과 직접적인 연결 가능	• SBOM 형식과의 호환성 • 소유권이 있는 SBOM과 함께 사용할 수 있는 기능
VRM	• 검색 가능, 직접 수집 가능	• SBOM 형식과의 호환성 • 소유권이 있는 SBOM과 함께 사용할 수 있는 기능 • 개별 자산에 대한 연결성 부족
사용자 지정 스크립트	• HCP의 고유한 요구 사항에 맞게 조정 가능	• 긴 생성 시간 또는 높은 자원 소모율 가능성 • 높은 오류 발생 가능성

SBOM 관리와 관련된 특정 사용 사례에 대한 자세한 내용은 7장 SBOM 사용 사례에서 확인할 수 있다.

7.0 SBOM 사용 사례

SBOM은 이해관계자에 의해 다양한 목적으로 활용된다. 예를 들어, SBOM은 HCP의 기기 수명 주기 관점에서 배치, 통합, 구성, 사용, 유지보수 및 기기 구성 관리 등의 단계에서 도움이 된다. (예: 기기가 동시에 업데이트되지 않기 때문에, HCP는 동일한 기기라 할지라도 여러 가지 버전을 가질 수 있다.)

또한 SBOM은 설계 단계부터 지원 종료 및 폐기에 이르기까지 의료기기의 TPLC 전반에 걸쳐 MDM에 의해 활용될 수도 있다. 종합적으로 SBOM은 조직에서 기기의 전체 수명 주기에 걸쳐 보다 적극적인(사전 예방적인) 보안 입장을 취할 수 있도록 지원이 가능하다.

이 장에서는 다음과 같이 SBOM을 부가 도구로 사용하는 사용 사례에 대한 예시를 제공한다:

- 위험 관리
- 취약점 관리
- 사고 관리

본 장에서는 이러한 사용 사례에 대한 개요를 제공한다. 이 장은 주로 MDM 또는 HCP의 관점에 초점을 맞추고 있지만, 이러한 사용 사례 중 일부는 다른 이해관계자 그룹에도 적용될 수 있다.

자산 관리 및 구매 사용 사례는 이 문서에 포함되지 않았으며, 이러한 사용 사례에 대한 자세한 내용은 NTIA 소프트웨어 컴포넌트 투명성 헬스케어 개념 증명 보고서(NTIA Software Component transparency Healthcare Proof of Concept Report)를 참고할 수 있다.

7.1 위험 관리

7.1.1 MDM의 관점

일반적인 위험 관리 활동은 IMDRF 사이버보안 지침(IMDRF/CYBER WG/N60FINAL:2020)의 5.2.절에 설명되어 있다. SBOM 생성을 위해 MDM은 전체 소프트웨어 공급망을 고려해야 한다. 여기에는 기기에 통합된 소프트웨어 컴포넌트가 포함된다. SBOM은 외부 취약점 정보 소스를 활용하여 기기 내의 소프트웨어 컴포넌트의 기존 취약점을 식별하는 데 도움을 줄 수 있다. 취약한 소프트웨어 컴포넌트가 발견되면, 소프트웨어 종속성도 고려하는 위험 분석 절차를 시작하게 된다.

의존성에는 라이브러리, 운영 체제, TCP/IP 인터넷 스택, 소프트웨어 및 시스템 실행에 필요한 기타 컴포넌트 등이 포함될 수 있다. 다음은 SBOM을 사용하면 도움이 되는 몇 가지 위험 관리 활동 목록이다:

- **위험 평가**: SBOM은 외부 취약점 정보 소스와 연계하여 잠재적 취약점을 식별하는 데 사용할 수 있다. SBOM은 잠재적인 악용 가능성 및 영향을 포함하여 존재할 수 있는 잠재적 취약점에 대한 정보를 제공한다. 이 취약점 정보는 특정 취약점과 관련된 위험 수준을 추정하고 평가하는 데 사용할 수 있다.

- **위험 통제**: SBOM에 나열된 컴포넌트에 취약점이 존재하는지를 모니터링하고 정기적으로 확인함으로써 위험을 통제 가능한 수준으로 유지하는 데 도움이 된다. (사용 사례 7.2.절 취약점 관리 참조)

- **평가 및 모니터링**: 새로운 소프트웨어 출시할 때 필요에 따라 SBOM을 업데이트 한다.

- **수명 주기 위험 관리**: 기기의 구매시나 수명 주기 동안의 업데이트 시, 제품 보안 문서의 일부로 기계 판독 가능한 형식의 SBOM을 HCP에게 제공 한다 (기기가 EOS에 가까워지면, HCP의 관리를 용이하게 하기 위해 최신 SBOM을 제공함. 자세한 내용은 IMDRF/CYBER WG/N70DRAFT:2022 참조).

7.1.2 HCP의 관점

SBOM은 구매 단계부터 시작하여 HCP의 위험 관리의 일부로 활용된다. SBOM은 기기 내의 소프트웨어에 포함된 컴포넌트와 연관된 위험을 투명하게 제공한다. 이를 통해 HCP는 기기의 TPLC 동안의 혜택과 위험성을 더 잘 이해하게 되고, 기기의 수명 주기 동안 위험 통제 및 완화 전략을 좀 더 효과적으로 적용하는 방법을 파악하게 해준다.

7.2 취약점 관리

이 절에서는 의료기기 취약점 관리를 위해 SBOM을 효과적으로 사용하기 위한 사용 사례와 고려 사항에 관해 설명한다.

7.2.1 MDM의 관점

취약점 관리는 아주 중요한 MDM의 시판 후 접근 방식으로서 의료기기가 통제할 수 있는 위험 프로필을 유지할 수 있게 해준다. MDM은 사이버 보안의 일부로 위협 및 취약성 정보 소스를 모니터링한다. SBOM은 새롭게 출현하고 시간이 지남에 따라 변화하는 잠재적인 의료기기 취약점을 적시에 식별할 수 있도록 지원해주는 필수적인 자원이다. MDM은 확보된 취약점 정보로부터 영향을 받는 소프트웨어 컴포넌트를 확인하고, SBOM을 활용하여 해당 컴포넌트를 포함하고 있는 의료기기를 식별할 수 있게 해준다. 의료기기 SBOM 정보와 보고된 취약점의 영향을 받는 소프트웨어 컴포넌트 정보를 자동으로 비교할 수 있다면 취약점 식별의 적시성과 정확성을 더욱 향상할 수 있다. 이는 MDM의 위험평가, 소통 및 필요에 따른 수정 능력을 향상시킨다. 위험 평가를 통해 얻을 수 있는 한 가지 가능한 산출물로서는 취약한 컴포넌트를 교체하는 것이고, 이에 따른 SBOM의 업데이트도 수행하는 것이다.

7.2.2 HCP의 관점

취약점 관리는 HCP가 IT 환경의 취약점을 지속해서 탐지, 평가 및 수정할 수 있도록 하는 중요한 절차이다. 매일 새로운 취약점이 발견되고 있는 상황에서 핵심적인 취약점을 적시에 탐지하고 수정할 수 있는 효과적인 방법이다. 이 절에서는 HCP의 취약점 관리 절차를 지원하기 위한 다양한 SBOM 사용 사례를 살펴본다.

전체 목록은 아니지만, 다음은 SBOM을 사용하면 도움이 되는 몇 가지 취약점 관리 활동 목록이다.

- **새로운 취약점이 나타날 때 HCP의 자산 모니터링**: SBOM은 새로운 취약점이 나타날 때 HCP의 의료기기가 어떤 영향을 받는지 이해하기 위해 취약점 정보와 함께 사용될 수 있다. VEX는 취약점에 대한 보완적인 통신 메커니즘이다.

- **임시 완화 조치 추진**: SBOM 정보는 MDM 또는 공급업체가 정확한 영향을 평가하거나 취약점을 해결하기 위한 업데이트를 개발하는 동안, HCP가 필요한 경우 임시 조치를 수행할 수 있도록 돕는다.
  - HCP는 여전히 임시 조치에 대해 MDM과 협력하는 것이 권장되는데, 이는 MDM이 기기의 의도된 사용 방법에 임시 조치가 미치는 영향을 더 잘 파악할 수 있기 때문이다. MDM은 VEX를 통해 임시 조치 지침을 제공할 수도 있다.

- **수명 주기 관리**: SBOM은 새로운 기기 및 이미 사용 중인 기기에 대해 현재 지원되거나 지원되지 않는 소프트웨어를 파악하는 데 도움을 준다. HCP가 기기를 교체할 수 없는 경우 HCP가(기업 및 환자 모두에게 영향을 주는) 위험을 평가할 충분한 시간을 제공하는 지원 일정을 포함하는 것이 MDM에게는 유용하다.

- **HCP의 선제적인 보안 활동 지원**: 보안 검색이 불가능하거나 적절하지 않은 경우(임베디드 기기, SaMD등), SBOM이 취약점 식별 및 보안 검색 활동을 보완한다.

7.3 사고 관리

의료기기에 영향을 미칠 수 있는 보안 사고를 MDM이나 HCP가 인지하는 방법은 다양하다. 어떤 방식으로 인지하게 되었든, SBOM은 견고한 사고 대응 절차와 함께 사용될 경우 MDM 및 HCP가 사이버보안 사건을 다루는 5단계의 침해 사고 관리 절차에서 더 나은 관리를 할 수 있도록 도와주는 여러 자원 중 하나이다. MDM의 경우, SBOM 리포지터리는 위험을 가진 기기를 식별하고 평가하는 데 걸리는 시간을 단축할 수 있다. HCP의 경우, SBOM 리포지터리는 HCP의 일차 지원팀과 사이버보안 팀의 작업을 지원할 수 있다. 구체적으로 리포지터리는 사이버보안 사고를 탐지하기 위한 정보의 체계적인 수집, 연관, 및 평가를 향상하며, 이를 통해 궁극적으로는 사고 처리가 개선된다. 이로써 불완전한 위험 평가와 증거 파기로 이어지는 데이터 손실로 인한 위험을 감소시킬 수 있다.

8.0 참고 문헌

8.1 IMDRF 문서

1. 소프트웨어 의료기기(SAMD): 위험 분류 및 해당 고려 사항에 대한 가능한 프레임워크 IMDRF/SaMD WG/N12:2014(2014년 9월)

2. 의료기기 및 체외진단의료기기의 안전과 성능에 대한 필수 원칙 IMDRF/GRRP WG/N47 FINAL:2018(2018년 11월)

3. 의료기기 사이버보안을 위한 원칙 및 실무 IMDRF/CYBER WG/N60: FINAL:2020(2020년 4월)

4. 레거시 의료기기의 사이버보안을 위한 원칙 및 실무 IMDRF/사이버 WG/N70 FINAL:2023(2023년 4월)

8.2 표준

5. AAMI TIR57:2016 의료기기 보안 원칙-위험 관리

6. AAMI TIR 97:2019, 의료기기 보안 원칙-기기 제조업체를 위한 시판 후 위험 관리

7. ANSI/NEM HN 1-2019, 의료기기 보안을 위한 제조업체 공개 성명서

8. IEC 60601-1:2005+AMD1:2012, 의료용 전자 장비-파트 1: 기본 안전 및 필수 성능에 대한 일반 요구 사항

9. IEC 62304:2006/AMD 1:2015, 의료기기 소프트웨어-소프트웨어 수명 주기 절차

10. IEC 62366-1:2015, 의료기기-파트 1: 의료기기에 사용 적합성 엔지니어링 적용

11. IEC 80001-1:2010, 의료기기를 통합하는 IT-네트워크에 대한 위험 관리 적용-파트 1: 역할, 책임 및 활동

12. IEC TR 80001-2-2:2012, 의료기기를 통합하는 IT-네트워크에 대한 위험 관리 적용-파트 2-2: 의료기기 보안 요구 사항, 위험 및 통제의 공개 및 통신에 대한 지침

13. IEC TR 80001-2-8:2016, 의료기기를 통합하는 IT-네트워크에 대한 위험 관리 적용 - 파트 2-8: 적용 지침-IEC 80001-2-2에서 식별된 보안 기능을 확립하기 위한 표준 지침

14. ISO 13485:2016, 의료기기-품질 관리 시스템-규제 목적에 대한 요구 사항

15. ISO 14971:2019, 의료기기-의료기기에 대한 위험 관리 적용

16. ISO/TR 80001-2-7:2015, 의료기기를 통합하는 IT-네트워크에 대한 위험 관리 적용-적용 지침-파트 2-7: 의료 서비스 제공 조직(HDO)이 IEC 80001-1을 준수하는지 자체 평가하는 방법에 대한 지침

17. ISO/IEC 27000 조직-정보 보안 관리 시스템

18. ISO/IEC 27035-1:2016, 정보 기술-보안 기술-정보 보안 사고 관리 -파트 1: 사고 관리 원칙

19. ISO/IEC 27035-2:2016, 정보 기술-보안 기술-정보 보안 사고 관리 -파트 2: 사고 대응 계획 및 준비를 위한 지침

20. ISO/IEC 29147:2018, 정보 기술-보안 기술-취약점 공개

21. ISO/IEC 30111:2013, 정보 기술-보안 기법-취약점 처리 절차

22. ISO/IEC 5962:2021 정보 기술-SPDX® 사양 V2.2.1

23. ISO/IEC 19770-2:2015 정보 기술-IT 자산 관리-파트 2: 소프트웨어 식별 태그

24. ISO/TR 24971:2020, 의료기기-ISO 14971 적용에 대한 지침

25. UL 2900-1:2017, 네트워크 연결할 수 있는 제품에 대한 소프트웨어 사이버보안 표준, 파트 1: 일반 요구 사항

26. UL 2900-2-1:2017, 네트워크 연결할 수 있는 제품을 위한 소프트웨어 사이버보안, 파트 2-1: 의료 및 웰니스 시스템의 네트워크 연결할 수 있는 컴포넌트에 대한 특정 요구 사항

8.3 규정 지침 및 초안 지침

27. ANSM(초안): 수명 주기 동안 소프트웨어를 통합하는 의료기기의 사이버보안(2019년 7월)

28. 중국: 의료기기 시판 전 사이버보안 검토 지침(2022년 3월)

29. 유럽 위원회: 의료기기에 관한 2017년 4월 5일자 유럽 의회 및 이사회 규정(EU) 2017/745, 지침 2001/83/EC, 규정(EC) 제178/2002호 및 규정(EC) 제1223/2009호를 개정하고, 이사회 지침 90/385/EEC 및 93/42/EEC를 폐지하는 내용(2017년 5월)

30. 유럽 위원회: 체외 진단 의료기기에 관한 2017년 4월 5일 유럽 의회 및 이사회 규정(EU) 2017/746 및 지침 98/79/EC과 위원회 결정 2010/227/EU을 폐지하는 내용(2017년 5월)

31. 의료기기 조정 그룹(MDCG: Medical Device Coordination Group) 2019-16: 의료기기 사이버보안 지침(2019년 12월)
https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native

32. FDA(초안): 의료기기의 사이버보안: 품질 시스템 고려 사항 및 시판 전 제출물 내용(2022년 4월) [이 지침은 본 N73 출판 시점에 초안 상태이며 시행 대상이 아니다. 최종 지침으로 대체될 예정이다.

33. FDA: 상용 소프트웨어(OTS: Off-the-Shelf)를 포함한 네트워크된 의료기기의 사이버보안(2005년 1월)

34. FDA: 가정용 기기의 설계 고려 사항(2014년 11월)

35. FDA: 의료기기 사이버보안의 시판 후 관리(2016년 12월)

36. 독일: 네트워크에 연결된 의료기기에 대한 사이버보안 요구 사항(2018년 11월)

37. 캐나다 보건부: 의료기기 사이버보안에 대한 시판 전 요구 사항(2019년 6월)

38. 일본: 의료기기의 사이버보안 보장: PFSB/ELD/OMDE 고시 제 0428-1(2015년 4월)

39. 일본: 의료기기의 사이버보안 보장에 관한 지침: PSEHB/MDED-PSD 고시 제0724-1호(2018년 7월)

40. 싱가포르 표준 위원회 기술 참조 67: 의료기기 사이버보안(2018년)

41. TGA: 의료기기 사이버보안 - 소비자 정보(2019년 7월)

42. TGA: 산업용 의료기기 사이버보안 지침(2019년 7월)

43. TGA: 사용자를 위한 의료기기 사이버보안 정보(2019년 7월)

8.4 기타 자원 및 참고 자료

44. NTIA FAQ
https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf

45. NTIA '소프트웨어 컴포넌트 투명성 프레임화: 공통 소프트웨어 자재 명세서(SBOM) 수립' 제2판
https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

46. NTIA '소프트웨어 컴포넌트 투명성 프레임화: 공통 소프트웨어 자재 명세서(SBOM) 수립'
https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

47. NTIA '공급망 전반에서 SBOM의 역할과 이점'
https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

48. NTIA 소프트웨어 컴포넌트 투명성 헬스케어 개념 증명(POC: Proof of Concept) 보고서
https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf

49. NTIA 헬스케어 POC 'SBOM 생성을 위한 안내서'
https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf

50. NTIA 취약점 악용 가능성 교환(VEX: Vulnerability-Exploitability eXchange) 개요
https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf

51. NTIA 소프트웨어 공급자 플레이북: SBOM 생산 및 제공
https://ntia.gov/files/ntia/publications/software_suppliers_sbom_production_and_provision_-_final.pdf

52. 미국 상무부(Dept of Commerce), 국가 사이버보안 개선에 관한 행정명령 14028에 따른 SBOM의 최소 엘리먼트
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

53. OASIS 프로필 5: VEX
https://docs.oasis-open.org/csaf/csaf/v2.0/csd01/csaf-v2.0-csd01.html#45-profile-5-vex

54. CERT® 조율된 취약점 공개 지침
https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

55. NIST 사이버보안 프레임워크

https://www.nist.gov/cyberframework

56. NIST의 시큐어 소프트웨어 개발 프레임워크(SSDF: Secure Software Development Framework)
https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

57. NIST SP 800-115:2008, 정보 보안 테스트 및 평가에 대한 기술 지침
https://doi.org/10.6028/NIST.SP.800-115

58. 의료기기 및 보건 IT 공동 보안 계획(2019년 1월)
https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

59. MITRE 의료기기 사이버보안 플레이북(2018년 10월)
https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

60. MITRE CVSS 헬스케어 루브릭
https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

61. 의료 산업 사이버보안 실무: 위협 관리 및 환자 보호(HICP: Health Industry Cybersecurity Practices)
https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf

62. 오픈 웹 애플리케이션 보안 프로젝트(OWASP: Open Web Application Security Project)
https://www.owasp.org/index.php/Main_Page

63. 의료기기 보안을 위한 제조업체 공개 진술서(MDS^2 : Manufacturer Disclosure Statement)
https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

64. 미국 국가통신정보국(NTIA: National Telecommunications and Information Administration)/미국 상무부, 취약점 공개 태도 및 조치: NTIA 인식 및 채택 그룹의 연구 보고서
https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

65. https://republicans-energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf

66. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

9.0 부록

9.1 SBOM 컴포넌트 타입 및 도구

SBOM 콘텐츠는 다양한 소스에서 제공될 수 있다. 포함될 수 있는 컴포넌트 타입과 SBOM 콘텐츠를 생성하는 도구의 예시는 다음과 같다.

● **서드파티 소프트웨어 컴포넌트 타입**

SBOM에 통합되는 컴포넌트 타입의 범위는 MDM의 능력, HCP의 기대치, 이용할 수 있는 SBOM 소프트웨어의 성숙도, 잠재적 또는 예상되는 규제적 SBOM 요구 사항 등을 포함하여 여러 요인에 따라 달라질 수 있다.

그러나 SBOM을 관리할 때, 다양한 타입의 컴포넌트를 인식하는 것이 중요하다. 컴포넌트마다 인벤토리 및 운영 관리를 위해 다른 방법과 도구가 필요할 수 있기 때문이다. 다음과 같은 타입으로 구분할 수 있다:

- 소유권이 있는 의료기기 소프트웨어에 연결되거나 내장된 서드파티 소프트웨어 라이브러리
- 가상 머신, 운영 체제 및 운영 체제 포함되는 서드파티 소프트웨어 컴포넌트(드라이버, 데이터베이스 소프트웨어, 관리 도구 및 애플리케이션 프레임워크 등 포함)
- 의료기기와 같이 사용되는 벤더 제공 하드웨어에 있는 서드파티 소프트웨어 컴포넌트: 펌웨어, 임베디드 소프트웨어 및 PLC

본 항에서는 이러한 다양한 타입의 컴포넌트에 대한 SBOM 인벤토리,

운영 관리 및 사용할 수 있는 도구에 대해 자세히 설명한다.

● **서드파티 소프트웨어 라이브러리**

현대 소프트웨어 개발에서는, 단일 소프트웨어에서 제조업체가 자체적으로 작성한 소유권이 있는 코드에 비해 서드파티 라이브러리의 코드를 훨씬 더 많이 사용하는 경우가 많다. 이러한 라이브러리가 포함된 SBOM을 작성하고 관리하려면, MDM이 모든 라이브러리의 리스트를 추적 및 작성하고 사용된 라이브러리에 영향을 미치는 모든 소프트웨어 변경 사항에 대해 해당 목록을 업데이트하도록 해야 한다. 이러한 수동 추적 및 업데이트는 SBOM 사용을 개발 절차에 통합하기 위한 첫 번째 기본 절차로 간주할 수 있다. 조직이 좀 더 성숙해짐에 따라 절차를 보다 효율적이고 정확하게 만들기 위해 자동화와 같은 고급 절차를 도입할 수 있다. 고급 절차의 예로는 기존 개발 플랫폼과 데브옵스(DevOps: development and operations) 환경을 활용하는 것을 들 수 있다. 특히, 자동화된 도구/플러그인은 개발 파이프라인의 하나 또는 그 이상의 단계에 통합될 수 있다. (DevSecOps)

SBOM의 장점은 서드파티 라이브러리 및 그 취약점을 가능한 한 빠르게 식별할 수 있게 해준다는 점이다. 알려진 취약점을 초기에 감지함으로써, 초기 조치가 가능하며, 늦은 감지에 비해 비용 효율적이다. 즉, 취약한 컴포넌트를 취약하지 않은 컴포넌트로 소프트웨어 개발 절차 초기 단계에 교체한다면 초기 단계의 절차적 작업량이 검증 및 유효성 검사 단계 이후보다 훨씬 적기 때문에 비용이 절감된다. 또한,

코딩 재작업의 양도 줄어든다고 볼 수 있는데, 코드가 SDLC의 최종 단계에 도달하면 코드의 복잡성과 종속성이 증가하기 때문이다. 또한 일반적으로 소프트웨어가 변경될 때마다 SBOM 구성이 업데이트되므로, 초기 감지를 통해 SDLC 전반에 걸쳐 SBOM을 관리할 수 있게 된다.

이러한 도구 또는 플러그인은 소프트웨어를 분석하여 내장되거나 또는 링크된 오픈 소스 소프트웨어를 탐지하며, 일부는 상업용 서드파티 소프트웨어도 탐지할 수 있다. 또한 대표적인 보안 패치가 존재하는 최신이 아닌 라이브러리와 같은 알려진 취약점도 식별할 수 있다. 다음과 같은 시기에 취약점 모니터링을 통해 SBOM 콘텐츠 수집에 기여를 하게 된다:

- 코딩: 예를 들어, 정적 코드 분석을 실행할 때(즉, 실행 중이지 않은 소스 코드의 취약점을 찾아주는 도구를 활용하는 경우)
- 빌딩: 예를 들어 스프린트 종료 시점에 소프트웨어를 빌드하는 때 (여기서 스프린트는 특정 작업을 하는 코드를 완성하고 실행-검토-준비까지의 셋업기간)
- 테스팅: 예를 들어, 정적 애플리케이션 보안 테스트(SAST: Static Application Security Testing)를 실행할 때

이러한 도구 또는 플러그인(일반적으로 소프트웨어 구성 분석(SCA) 소프트웨어라고 함)은 SBOM을 생성하기 위해 수동 입력이 필요하지 않고, 일반적으로 사용할 수 있는 리포지터리를 사용하여 다음을 식별한다:

- 소프트웨어 컴포넌트 이름
- 소프트웨어 컴포넌트 벤더(공급업체)

- 소프트웨어 컴포넌트 버전
- 컴포넌트 해시
- 관계(하나 이상의 의존성 계층)
- 컴포넌트 취약점
- 라이선스 모델 및 규정 준수 정보

대형 SCA 벤더 외에도 코드-제작-테스트 중에 사용할 수 있고 유사한 결과를 생성하는 다른 도구와 플러그인이 있다는 점에 유의한다. 일부는 무료로 사용할 수도 있어 모든 규모의 MDM에 자동화를 제공할 수 있으나, MDM은 MDM에 필요한 기능에 가장 적합한 능력을 갖춘 도구를 신중하게 선택해야 한다.

● **운영 체제 컴포넌트**

의료기기에서 사용 중인 가상 머신과 운영 체제는 SBOM의 필수 컴포넌트이다. 기기 소프트웨어가 실행되는 운영 체제에 의존하는 기존 서드파티 컴포넌트에는 데이터베이스, 애플리케이션 프레임워크, 보안 소프트웨어, 시스템 관리 도구, 원격 지원 소프트웨어, 네트워킹 컴포넌트 등이 포함된다.

운영 체제에서 서드파티 소프트웨어 컴포넌트의 검색 및 관리를 자동화하는 여러 가지 옵션이 있다. 일부 SCA 벤더는 이전 항에서 설명한 컴포넌트과 함께 그 외의 다른 소프트웨어 컴포넌트(즉, 소유권이 있는 소프트웨어에 직접 링크되거나 내장되지 않은, 운영 체제에

존재하는 컴포넌트) 모두에 중점을 둔다. 한편, 소프트웨어 자산 관리(SAM: Software Asset Management)에 전념하는 벤더도 있는데, SAM은 소프트웨어에 내재된 위험과 가치를 관리하는 거버넌스 실무이다.

MDM이 이러한 도구를 사용할 수 없는 경우, 전용 스크립트(예: 윈도우즈의 파워쉘(PowerShell) 스크립트 또는 리눅스의 배시쉘(BashShell) 스크립트)를 실행하여 운영 체제에서 소프트웨어 인벤토리를 생성할 수 있다. 또 다른 옵션은 취약점 관리 스캔 도구를 사용하는 것이다. 후자의 경우 발견된 컴포넌트의 취약점 정보도 제공한다는 장점이 있다.

- **펌웨어, 임베디드 소프트웨어 및 PLC**

서드파티 펌웨어, 임베디드 소프트웨어 및 PLC는 취약점이 발견되지 않는 한 수명 주기 동안 의료기기에서 변경될 가능성이 가장 적은 컴포넌트이다. 임베디드 소프트웨어는 보드 서포트 패키지, 바이너리 드라이버, 소프트웨어 개발 키트(SDK), CPU 마이크로코드 및 기타 라이브러리를 기반으로 구축된다. 임베디드 소프트웨어는 오픈 소스 소프트웨어에 대한 의존도가 높을 수 있으므로 최종 제품에 포함된 모든 소프트웨어 컴포넌트를 식별하는 것이 중요하다.

이러한 타입의 소프트웨어 컴포넌트는 기기의 하드웨어와 엮여 있으므로 의료기기의 정규 BOM에 포함된다. BOM은 기기를 제조하는 데 필요한 재료와 컴포넌트의 포괄적인 목록이므로 소프트웨어 컴포넌트를 포함하여 다양한 내용을 포함하게 된다. 따라서 BOM은 이러한 서드파

티 소프트웨어 컴포넌트의 인벤토리 와 관리를 위한 좋은 출발점을 제공한다. SBOM과 마찬가지로 정규 BOM은 MDM의 개발 활동 또는 서드파티에서 제공하는 BOM을 포함하여 다양한 출처에서 얻을 수 있다. 소스 코드 관리 시스템과 바이너리 소프트웨어 구성 분석의 조합을 사용하여 이 정보의 생성을 자동화하거나 검증할 수 있다. 사용되는 모든 도구는 임베디드 시스템과 호환되어야 함을 유의해야 한다.

제품 수명 전주기 관리(PLM: Product Lifecycle Management) 또는 전사적 자원 관리(ERP: Enterprise Resource Planning) 소프트웨어를 통해 BOM을 관리하는 경우, 내보내기 기능을 사용하여 소프트웨어 컴포넌트를 추출할 수 있다. 만일 펌웨어, 소프트웨어, 또는 PLC 벤더가 제공하는 SBOM이 사용 가능하다면, 필요한 경우 서드파티 컴포넌트에 대해 추가적인 깊이의 계층을 추가할 수 있다.

이러한 소프트웨어 컴포넌트가 소유권이 있는 소프트웨어, 예를 들면 MDM에 소유권이 있는 소프트웨어인 경우, 9.1.절의 서드파티 라이브러리에서 언급된 것과 동일한 방식이 적용된다.