2024년 3/4분기

정보보호 인적자원개발위원회(ISC)

ISSUE REPORT

| SW 공급망 보안 관련 현황 및 인력양성 방안

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

CONTENTS

정보보호 인적자원개발위원회 사무국 02-6748-2011, 2039 | mhr0327@kisia.or.kr

본 이슈리포트는 한남대학교 컴퓨터공학과 이만희 교수가 작성하였습니다.

요약

□ 개요

- SW 공급망 보안은 소프트웨어의 생애 전 주기에서 발생할 수 있는 다양한 보안 위협을 식별하고 이를 방지하기 위한 일련의 활동을 의미
- 최근 IT 환경에서 국가 및 기업의 소프트웨어 의존도가 높아짐에 따라 소프트웨어 공격에 의한 대규모의 피해가 발생한 바가 있으며 이에 SW 공급망 보안의 중요성이 더욱 부각되는 추세
- SW 공급망 위협 대응 방안으로 전체적인 소프트웨어 개발 및 배포 과정의 모든 단계에서 보안 고려 필요
- SW 공급망 보안 강화 필요성에 비해, 이러한 보안 활동을 효과적으로 수행할 수 있는 인력은 매우 부족하며, 인력을 체계적으로 양성할 수 있는 교육과정이나 프로그램 또한 마련되어 있지 않은 실정
- SW 공급망 보안 인력 양성을 위하여 인력이 갖추어야 할 필수 역량과 지식을 명확히 정의한 해당 분야 NCS 개발이 현재 진행 중

□ SW 공급망 보안 분야 현황 및 전망

- SW 공급망 보안은 전 세계적으로 트렌드, 환경, 정책의 변화가 계속되고 있어 중요성이 커지고 있는 분야이기 때문에 맞춤형 보안 전략 수립, 보안 인식 강화, 전문 인력 양성은 필수적
- IT 및 보안 전문가의 84%가 소프트웨어 공급망 공격이 향후 3년 이내 가장 큰 사이버 위협 중 하나가 될 것이라고 예상하여 공급망 보안에 대한 투자와 대비책 마련이 시급함을 시사
- 국내의 국가 사이버안보전략에서도 공급망 보안 강화는 중요한 전략적 목표 중 하나이며 소프트웨어 개발 시 보안 취약점을 최소화하기 위한 소프트웨어 구성 정보 표준화 및 관리 체계 수립과 함께 공급망 보안을 위하여 교육, 훈련, 지속적 관리 및 기술 지원을 할 수 있는 역량과 환경 구축을 명시

□ SW 공급망 보안 NCS 현황

- 향후 SW 공급망 보안 분야의 NCS는 교육과 평가에 효과적으로 활용될 것으로 기대
- SW 공급망 보안은 안전한 개발 환경을 구축하고 SW 구성명세서(SBOM)와 취약점을 관리하여 SW 개발, 도입, 운영까지 SW 공급망을 안전하게 보호하는 일"로 NCS 직무정의(안) 기술

□ SW 공급망 보안 인력양성 방안 제언

- 대학에서 SW 공급망 보안을 정규 교과과정으로 포함할 수 있도록 지원하고, 유관 분야 전공자가 SW 공급망 보안 역량을 갖출 수 있도록 별도의 교육 프로그램 및 취업 연계형 프로그램 개발 필요
- 현업에 있는 IT 및 보안 인력이 실무 능력을 향상시킬 수 있도록 재직자 상시 교육을 위한 전문 교육 기관 지정 및 재정적 지원 필요
- SW 공급망 보안을 정보처리기사 또는 정보보안기사 자격증 시험의 출제 기준에 포함하거나, 관련 자격증을 신설하여 미래의 보안 전문가들이 SW 공급망 보안에 대한 지식을 습득할 수 있도록 유도

I.

개요

I 개요

1. SW 공급망 보안의 정의 및 범위

○ 소프트웨어(SW) 공급망 보안은 소프트웨어의 디자인, 개발, 배포, 운영, 유지보수, 폐기의 SW의 개발을 포함한 생애 전 주기에서 발생할 수 있는 다양한 보안 위협을 식별하고 이를 방지하기 위한 일련의 활동을 의미

○ 현대의 디지털 환경에서는 다양한 소프트웨어가 복잡한 생태계를 이루고 있으며, 이러한 소프트웨어들은 상호 연결되어 운영됨. 소프트웨어 공급망은 이러한 상호 연결된 시스템의 네트워크를 형성하며, 소프트웨어 개발자, 타사 제공업체, 오픈소스 커뮤니티, 배포 플랫폼 등 다양한 이해관계자가 관여

2. SW 공급망 보안의 중요성

○ 오늘날의 IT 환경에서 소프트웨어가 매우 중요한 역할을 하고 있음. 기업의 핵심 비즈니스 프로세스는 물론, 국가의 주요 인프라까지도 소프트웨어에 크게 의존하고 있음. 만약 소프트웨어 공급망에 보안 취약점이 존재한다면, 악의적인 행위자들이 이를 이용해 대규모의 피해를 유발할 것으로 예상

○ 특히, 최근 몇 년간 대규모 소프트웨어 공격 사건들이 발생하면서 SW 공급망 보안의 중요성이 더욱 부각되는 추세

- 2020년 말에 발생한 솔라윈즈(SolarWinds) 해킹 사건은 SW 공급망 공격의 대표적인 사례로, 전 세계적으로 막대한 파급 효과 야기

3. SW 공급망 위협 대응 방안

○ SW 공급망 보안은 전체적인 소프트웨어 개발 및 배포 과정의 모든 단계에서 보안 고려 필요

- 코드 작성 단계부터 코드 리뷰, 빌드 및 테스트, 패키징, 배포, 그리고 지속적인 모니터링에 이르기까지 모든 과정에서의 보안 관리가 필요
- 각 단계에서 발생할 수 있는 위협 요소를 사전에 식별하고 이를 체계적으로 관리하기 위한 프레임워크와 절차가 필수적
- 현재 SW 공급망 보안의 강화를 위하여 다양한 정책 및 규제를 마련하기 위해 준비 중

4. SW 공급망 보안 인력양성의 중요성

○ SW 공급망 보안 강화 필요성에 비해, 이러한 보안 활동을 효과적으로 수행할 수 있는 인력은 매우 부족

- 인력을 체계적으로 양성할 수 있는 교육과정이나 프로그램 또한 마련되어 있지 않은 실정

○ SW 공급망 보안 인력은 소프트웨어 개발 능력과 정보보안 능력을 동시에 소유한 상태에서 특별히 SW 공급망 보안에 대한 세부 지식이 필요

- 소프트웨어 개발 경험을 바탕으로, 소프트웨어의 개발, 배포, 운영 시스템에 대한 지식 필요
- 정보보안의 기본적인 이해와 함께 시스템, 네트워크, 애플리케이션 보안에 대한 높은 이해도와 경험 필수
- SW 공급망 보안과 관련된 법, 정책, 도구 등 다양한 분야의 전문 지식 필요

5. SW 공급망 보안 국가직무능력표준 (NCS, National Competency Standards)

○ SW 공급망 보안 인력 양성을 위하여 현재 해당 분야의 NCS 개발 진행 중

- 정보통신(대분류) 》 정보기술(중분류) 》 정보보호(소분류) 내 SW 공급망 보안(세분류) 신설 예정
- SW 공급망 보안 NCS는 SW 공급망 보안 인력이 갖추어야 할 필수 역량과 지식을 명확히 정의
- 향후 SW 공급망 보안 NCS를 기반으로 한 교육과정 개발 및 인력 양성 프로그램의 기초를 제공할 수 있을 것으로 기대

II.

SW 공급망 보안 분야 현황 및 전망

II SW 공급망 보안 분야 현황 및 전망

1. SW 공급망 보안의 변화

○ 미국 보안 컨설팅 기업 PurpleSec사가 미국 내 공급망에 보안에 대한 다양한 통계 정보 제공[1]

- IT 및 보안 전문가의 84%가 소프트웨어 공급망 공격이 향후 3년 이내 가장 큰 사이버 위협 중 하나가 될 것이라고 예상
- 2021년 기업을 대상으로 한 공급망 공격의 평균 재정적 영향은 140만 달러로 추산
- 소프트웨어 공급망 공격을 당한 조직의 59%는 대응 전략 부재
- 공급망 공격 중 약 58%는 데이터 접근(주로 고객 데이터, 개인 데이터 및 지적 재산 포함)이 공격 목표였으며, 약 16%는 사람에 대한 접근이 목표
- 공급업체의 자산이 표적이 된 경우, 대부분의 공격은 코드(66%), 데이터(20%), 및 프로세스(12%)의 손상이 목표인 것으로 확인

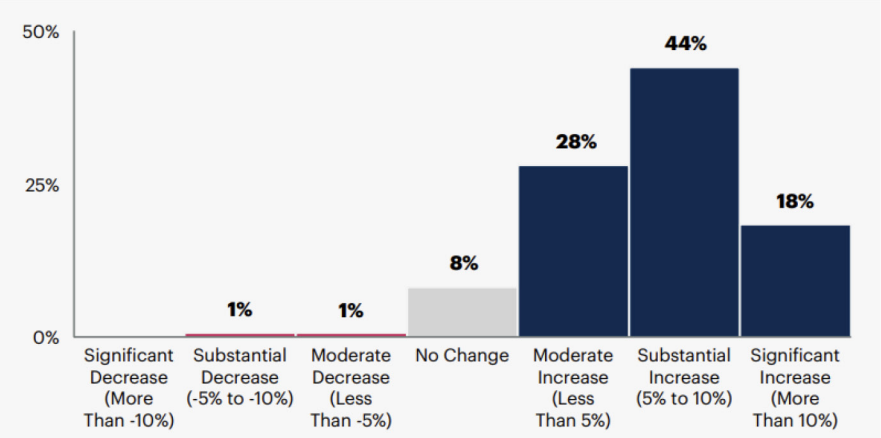
○ 화물 운송, 선박 운송, 물류, 공급망 관리, 및 교통에 대한 정보를 주로 제공하는 Forwarder Magazine사가 미국 내 공급망 보안에 대한 트렌드를 제시[2]

- 미국 대통령 행정명령 14028호 이후 3년 만에 미국 내 기업의 보안 솔루션에 대한 투자는 62% 증가했으며, 직원 교육에 대한 투자는 65% 증가[3]
- 미국 내 직장인들은 반복적인 수동작업에 업무 시간의 약 40%을 사용하고 있으며[4], 이는 보안 분야에서도 유사할 것으로 예측
- 미국 내 기업들 중 정보보안 업무 중 반복 작업에 사용되는 시간을 줄이기 위해 인공지능을 이용한 자동화 기술 도입은 200% 증가[5]

1) PurpleSec 홈페이지, https://purplesec.us/resources/cybersecurity-statistics/
2) Forwarder 홈페이지, https://forwardermagazine.com/4-supply-chain-security-trends/
3) Forbes 홈페이지, https://www.forbes.com/councils/forbestechcouncil/2023/08/01/cybersecurity-investment-trends-in-the-us/
4) Simply Flows 홈페이지, https://simplyflows.com/time-wasted-on-repetitive-tasks-is-40-percent/
5) CSO 홈페이지, https://www.csoonline.com/article/1251452/bsimm-14-finds-rapid-growth-in-automated-security-technology.html

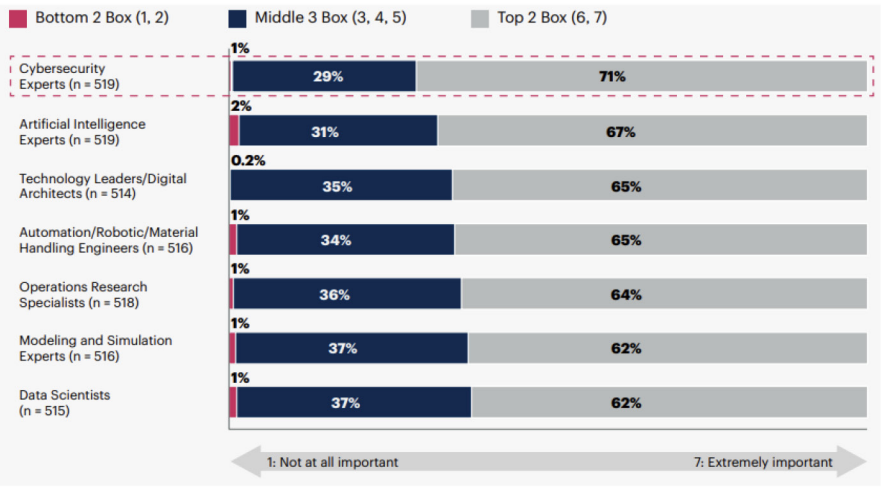
○ 미국 Gartner사에서 공급망 보안에 대한 예측 설문 보고서를 작성[6)]

▪ [그림 1]에서 대부분의 전문가들은 공급망 사이버 보안 지출이 증가할 것으로 예상하고 있음을 보여줌. 44%는 지출이 상당히 증가할 것(5%에서 10% 증가)으로 예상하고 있으며, 추가로 18%는 지출이 크게 증가할 것(10% 이상 증가)으로 기대하고 있음. 지출이 감소할 것으로 예상하는 응답자는 극소수에 불과하며, 이는 공급망 사이버 보안에 대한 투자가 전반적으로 증가하는 추세를 반영



[그림 1] 기업의 연간 공급망 사이버 보안 지출 증감 예상

▪ [그림 2]는 공급망 조직에서 사이버 보안 전문가의 중요성이 크게 부각되고 있음을 보여주며, 응답자의 71%가 향후 5년 동안 공급망 분야에서 사이버 보안 역량이 가장 필요한 역할이라고 평가함. 이는 공급망 사이버 보안 인력 양성이 필수적이며, 기술적 역량 강화를 통해 적절한 방어 체계를 구축할 필요가 있음을 반영



[그림 2] 향후 5년 동안 공급망 역할과 역량의 중요성

6) Gartner 홈페이지, https://www.gartner.com/en/supply-chain/trends/supply-chain-cybersecurity

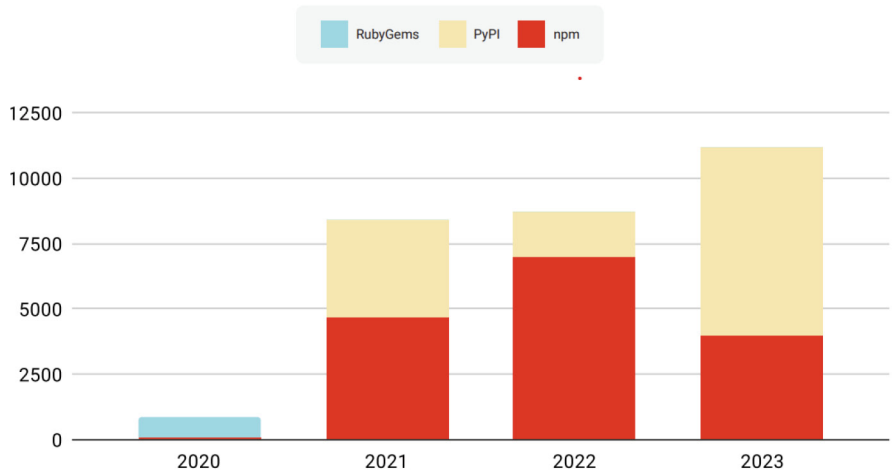
○ 시사점

- **공급망 사이버 보안의 중요성 증가:** IT 및 보안 전문가의 대다수가 향후 3년 내에 소프트웨어 공급망 공격이 주요 사이버 위협이 될 것이라고 예측하고 있으며, 공급망 보안 지출이 전반적으로 증가할 것으로 예상하므로, 공급망 보안에 대한 투자와 대비책 마련이 시급함을 시사
- **공격에 대한 대비 부족:** 공급망 공격을 받은 조직 중 59%가 대응 전략을 갖추지 않았다는 점은 많은 기업이 사이버 공격에 취약하다는 것을 보여줌. 이는 공급망 보안 전략의 필요성을 강조하며, 사전 대응 계획을 수립해야 함을 시사
- **공격 목표의 다양성:** 공급망 공격의 주요 목표는 데이터 접근(58%)과 코드 손상(66%)이었으며, 일부 공격은 사람에 대한 접근(16%)을 목표로 함. 이는 보안 대책이 데이터뿐만 아니라 코드와 인력 보호를 포함해야 함을 시사
- **보안 솔루션 및 교육 투자 확대:** 미국 내 기업들이 보안 솔루션과 직원 교육에 대한 투자를 크게 늘리고 있어, 이는 사이버 보안에 대한 인식이 강화되고 있음을 보여줌. 특히, 직원 교육의 중요성이 부각되고 있으며, 보안사고 예방 및 대응 역량 강화를 위해 지속적인 교육이 필요함을 시사

2. 악성코드와 개발환경의 변화

○ 악성코드 분석 및 공급망 보안 전문기업인 ReversingLabs사에 2024년에 발간한 The State of Software Supply Chain Security 2024에서는 공급망 보안과 관련된 다양한 통계 정보를 제공[7)]

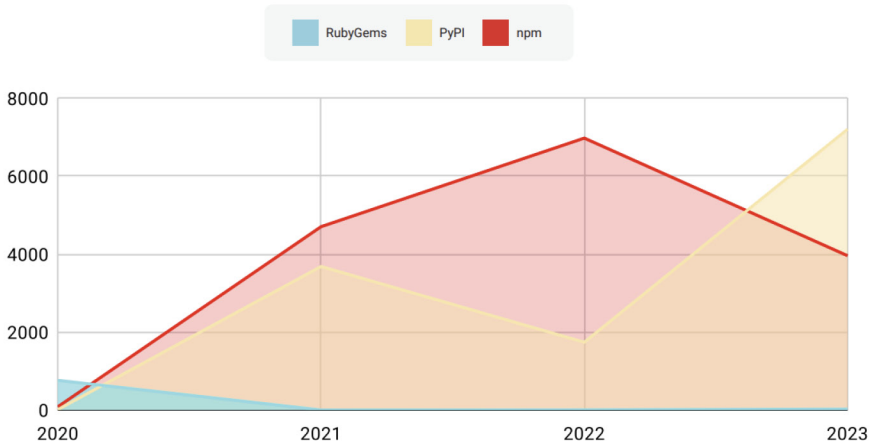
- 2023년에는 npm, PyPI, RubyGems 등 주요 오픈소스 소프트웨어 플랫폼에서 11,000개 이상의 악성 패키지가 탐지되었고, 이는 2022년에 탐지된 약 8,700개에 비해 28% 증가한 수치[그림 3]



[그림 3] 2023 악성 패키지 탐지: npm, PyPI, and RubyGems

7) Reversinglabs 홈페이지, https://www.reversinglabs.com/sscs-report

▪ 2023년 가장 주목할 만한 변화 중 하나는 PyPI가 악성 소프트웨어 배포 플랫폼으로 떠오른 것임.[그림 4] 2023년 첫 9개월 동안 PyPI에서 7,207개의 악성 패키지를 탐지했으며, 이는 2022년 전체에 탐지된 1,741개에 비해 400% 증가한 수치임. 한때 자동화된 공격을 통해 유포된 악성 패키지와 타이포스쿼팅 패키지의 급증으로 인해 PyPI에 대한 새로운 제출이 일시적으로 중단



[그림 4] 리포지토리별 악성 패키지 탐지

○ SW 개발 환경의 변화: DevOps와 CI/CD의 도입

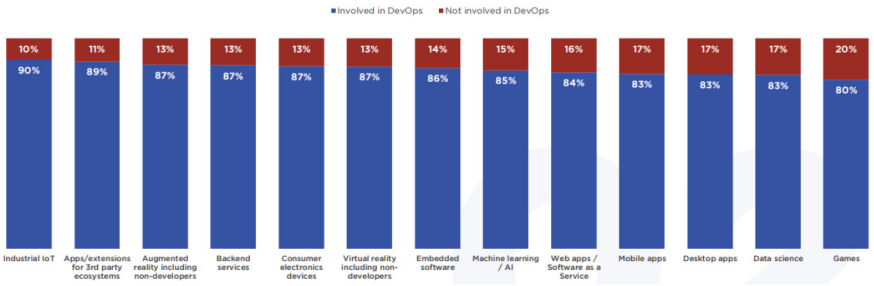
▪ DevOps는 개발(Development)과 운영(Operations)의 결합으로, 개발팀과 운영팀 간의 협업을 강화하여 소프트웨어 개발 주기를 단축하고 더 신뢰성 있는 릴리스를 가능하게 하는 문화와 관행을 의미

▪ CI/CD는 DevOps의 중요한 구성 요소로 CI/CD는 지속적 통합(Continuous Integration)과 지속적 전달/배포(Continuous Delivery/Deployment)의 약자로, 소프트웨어 개발에서 코드 변경 사항을 자동으로 빌드, 테스트, 배포하여 빠르고 안정적인 릴리스를 가능하게 하는 방법론임. 이를 통해 개발과 운영이 통합되어 협업이 강화되고, 배포 속도와 품질의 향상 가능

▪ Continuous Delivery Foundation에 따르면[8], 미국 내 개발자의 83%가 DevOps와 관련된 기술을 사용

▪ 산업별로는 산업시설을 위한 IoT 개발 분야 개발자가 가장 높은 비율(90%)로 DevOps 관련 기술을 사용하며, 게임 개발자가 가장 낮은 비율(80%)을 보임. 하지만 전반적으로 매우 높은 비율로 DevOps를 사용[그림5]

8) CD.foundation 홈페이지, https://cd.foundation/state-of-cicd-2024/



[그림 5] 리포지토리별 악성 패키지 탐지

○ 시사점

- **오픈소스 플랫폼의 보안 강화 필요성:** 2023년에는 주요 오픈소스 소프트웨어 플랫폼에서 탐지된 악성 패키지가 전년 대비 28% 증가했고, 특히, PyPI의 경우 2023년 첫 9개월 동안 악성 패키지가 400% 증가했음을 고려할 때, 오픈소스 리포지토리 내의 악성코드와 취약점을 점검하고 탐지하는 보안 조치의 필요성이 더욱 증가
- **DevOps 환경에서의 공급망 보안 통합:** DevOps와 CI/CD의 도입이 개발자들 사이에서 점점 확산되면서, 공급망 보안이 DevOps 파이프라인 내에서 수행되어야 할 필요성이 강조됨. 소프트웨어 개발 및 배포 과정에서 자동화된 빌드, 테스트, 배포가 이루어지는 만큼, DevOps 환경 내에서 오픈소스 컴포넌트에 포함된 잠재적인 악성코드나 취약점을 주기적으로 검사하고 차단하는 시스템이 필요
- **DevOps 및 CI/CD 시스템 보호의 중요성:** DevOps와 CI/CD 시스템 자체가 공격의 대상이 될 수 있으므로, 이러한 시스템의 보안도 중요함. 공급망 보안을 강화하기 위해서는 DevOps 도구와 파이프라인의 보안성을 유지하고, 자동화된 공격이나 악성 패키지 유포를 방지하기 위한 적극적인 대응이 필요
- **산업 전반에 걸친 DevOps 활용과 보안 인식 강화:** 미국 내 개발자 중 83%가 DevOps 관련 기술을 사용하고 있으며, 산업별로 도입 비율이 다소 차이가 있음. 각 산업 분야의 개발 환경에 맞춘 맞춤형 보안 전략이 필요

3. SW 공급망 보안 정책의 변화

○ 미국은 EO 14028을 통해 소프트웨어 공급망의 투명성과 보안성을 높이고 연방 정부의 사이버 보안 수준을 향상시키기 위한 다각적인 노력 중[9)]

9) NIST 홈페이지,https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

- 행정명령의 일환으로 SSDF(Secure Software Development Framework)를 업데이트함. SSDF는 NIST에서 개발한 프레임워크로, 안전한 소프트웨어 개발을 위한 보안 기준과 지침을 제시하며 소프트웨어 개발 과정에서 보안 위험을 줄이고, 소프트웨어 공급망의 투명성과 보안성을 강화하기 위한 일련의 관행을 포함[10)]
- Secure Software Development Attestation Form은 소프트웨어 개발자가 자신의 소프트웨어에 대해 SSDF 기준이 충족함을 자발적으로 선언하는 절차임. 이 제도는 연방 정부에 소프트웨어를 납품하는 모든 공급업체에 대하여 자사 소프트웨어가 SSDF 프레임워크를 준수하고 있음을 선언하도록 요구

○ 유럽은 Cyber Resilience Act(CRA)를 통해 EU 내에 판매되는 디지털 제품과 서비스의 사이버 보안 요건을 규제하는 것이 목표[11)]

- 특히, 이 법안에서는 각 기업들이 SBOM*을 작성하고 제공할 것을 요구

* SBOM (Software Bill of Materials): 소프트웨어 제품에 포함된 모든 구성 요소, 라이브러리, 모듈, 및 종속성에 대한 상세 목록. SBOM은 소프트웨어의 구성 요소와 그 출처를 명확히 하여, 소프트웨어 공급망의 투명성을 높이는 데에 기여

○ 국내 국가사이버안보전략에서 공급망 보안 강화는 중요한 전략적 목표 중 하나로 강조[12)]

- 소프트웨어 개발 시 보안 취약점을 최소화하기 위해 소프트웨어 구성 정보를 표준화하고 관리 체계를 수립할 것을 천명
- ICT 공급망 보안을 위하여 교육, 훈련, 지속적 관리 및 기술 지원을 할 수 있는 역량과 환경 구축 명시

○ 시사점

- **국내 기업의 공급망 보안 강화 필요성 및 인력 수요 증가:** 국가사이버안보전략에 따라, 국내 기업들은 ICT 제품 및 소프트웨어 개발 시 소프트웨어 구성 정보 관리 체계를 확립해야 함. 이에 따라 사이버 보안 전문가와 공급망 보안에 대한 이해도가 높은 인력의 수요 증가 예상
- **국제 표준 준수와 글로벌 시장 대응 역량 강화 필요성:** 미국과 유럽의 규제는 기업들이 소프트웨어 개발 과정에서 SSDF를 준수하거나, SBOM을 작성하고 제공할 것을 요구하고 있음. 국제 경쟁력 강화를 위해 공급망 보안 관련 지식과 경험을 가진 전문 인력 양성은 필수

10) NIST SP 800-218, 「Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities」 (2022)

11) 유럽 연합 위원회 홈페이지, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

12) 대한민국 대통령실 홈페이지 https://www.president.go.kr/newsroom/press/gdXzwtKB

III.

SW 공급망 보안 NCS 현황

Ⅲ SW 공급망 보안 NCS 현황

들어가기에 앞서 : NCS(National Competency Standards, 국가직무능력표준) 소개[13]

○ 정의

- 산업 현장에서 직무를 수행하는 데 필요한 지식, 기술, 태도를 체계적으로 정리한 기준

○ 목적

- 산업 맞춤형 인력 양성: 실무에 필요한 능력을 갖춘 인재 양성
- 교육과 훈련의 표준화: 교육기관과 훈련기관에서 일관된 교육과 훈련 제공
- 평가 및 인증 체계화: 직무 수행 능력에 대한 객관적 평가 및 인증 기준 마련

○ NCS의 구성

- 능력단위: 직무 수행에 필요한 최소 능력 단위
- 능력단위요소: 능력단위 수행을 위한 세부 작업 및 활동
- 지식, 기술, 태도: 능력단위 수행에 필요한 이론적 지식, 실기 능력, 직업윤리 등

○ NCS의 적용

- 교육기관: NCS 기반 커리큘럼 설계 및 인재 양성
- 산업계: 직원 채용, 교육훈련, 승진 기준으로 활용
- 정부 및 공공기관: 인력양성 정책 수립 및 실행 기준으로 활용

1. SW 공급망 보안 NCS 목적과 의의

○ NCS 개발 시 SW 공급망 보안 인력에게 필요한 기술과 지식을 명확히 정의하고, 이를 바탕으로 SW 공급망 보안 교육과정 개발 및 운영 기준 제공 가능

- NCS는 산업계의 요구를 반영하여 각 분야에서 요구하는 직무 능력을 체계적으로 교육하고 평가하는 데 중요한 역할을 하는 인재 양성의 필수 기준이므로, SW 공급망 보안 NCS가 개발되면 SW 공급망 보안 분야의 교육과 평가에 효과적인 활용 기대

13) 국가직무능력표준(NCS) 홈페이지. https://www.ncs.go.kr/

2. SW 공급망 보안 NCS 개발(안)

- 직무 정의를 "SW 공급망 보안은 안전한 개발 환경을 구축하고 SW 구성명세서(SBOM)와 취약점을 관리하여 SW 개발, 도입, 운영까지 SW 공급망을 안전하게 보호하는 일"로 정의
- 6개의 능력단위(SW 공급망 보안 계획수립, SW 공급망 인프라 보안, SW 개발보안 자동화 관리, SW 취약점 관리, SW 구성명세서 관리, SW 공급망 보안 운영)로 구성

[표 1] SW 공급망 보안 NCS 개발(안)

능력단위	정의	수준	능력단위요소
SW 공급망 보안 계획 수립	SW 공급망 보안 계획수립이란 SW 공급망 보안 환경 분석 결과와 국내외 컴플라이언스에 따라 보안 정책 및 세부 실행계획을 수립하는 능력	7	SW 공급망 보안 환경 분석하기
			SW 공급망 보안 정책 수립하기
			SW 공급망 보안 운영계획 수립하기
SW 공급망 인프라 보안	SW 공급망 인프라 보안이란 SW 개발 환경의 보호 대상과 이에 대한 위협을 식별하여 SW 공급망 인프라의 취약성을 관리하고 완화하는 능력	6	SW 공급망 인프라 분석하기
			SW 공급망 인프라 보호대책 수립하기
			SW 공급망 인프라 보안 적용하기
SW 개발보안 자동화 관리	SW 개발보안 자동화 관리란 SW 개발과 배포의 전 과정에 걸쳐 안전하고 효율적인 개발 및 운영을 위해 자동화 기술을 통하여 SW 개발 및 운영 체계를 구축하고 관리하는 능력	5	SW 버전 관리 환경 운영하기
			SW 배포 자동화 환경 운영하기
			SW 인프라 자동화 환경 운영하기
			SW 개발생명주기 내 보안 통합하기
SW 취약점 관리	SW 취약점 관리란 SW 전체 생명주기에서 공급망 내부의 SW 취약점을 식별, 평가, 완화하고 모니터링하는 능력	6	SW 취약점 평가하기
			SW 취약점 완화하기
			SW 취약점 모니터링하기
SW 구성명세서 관리	SW 구성명세서 관리란 공개SW를 포함한 SW 구성요소의 라이선스와 취약점을 확인하고 SW 구성명세서를 생성하는 능력	5	SW 구성명세서 구성요소 정의하기
			공개SW 라이선스 적합성 확인하기
			SW 구성명세서 생성하기
SW 공급망 보안 운영	SW 공급망 보안 운영이란 SW 공급망 보안을 위한 도구를 선정하고 SW 획득 시 무결성을 검증하며 SW 인벤토리 운영 과정에서 SW 위협에 대응하는 능력	5	SW 공급망 보안 도구 선정하기
			SW 획득 무결성 검증하기
			SW 인벤토리 운영하기
			SW 위협 대응하기

IV.

SW 공급망 보안 인력양성 방안 제언

Ⅳ SW 공급망 보안 인력양성 방안 제언

○ 대학 교과과정에 SW 공급망 보안 과목 개설 지원

- 대학에서 SW 공급망 보안을 정규 교과과정으로 포함할 수 있도록 정부의 재정적 지원을 강화. 컴퓨터공학과, 정보보호학과 등 관련 학과에 SW 공급망 보안 관련 과목을 개설할 수 있도록 지원하여 장기적으로 대학생들이 졸업 전 관련 지식을 습득할 수 있도록 유도

○ 재직자 상시 교육을 위한 교육 기관 지정 및 재정 지원

- SW 공급망 보안 교육을 위한 전문 교육 기관을 지정하고, 재직자들이 상시로 교육을 받을 수 있도록 재정 지원을 제공. 이를 통해 현업에 있는 IT 및 보안 인력들이 최신 공급망 보안 위협과 대응 방법을 지속적으로 학습하고, 실무 능력을 향상시킬 수 있도록 지원

○ 구직자 대상 교육 프로그램 및 취업 연계형 프로그램 개발

- 대학 교육과정은 빠르게 변화하기 어려우므로, 현재 대학에 재학 중이거나 졸업한 구직자들이 SW 공급망 보안 역량을 갖추는 데 어려움이 있음. 이를 위해 구직자들을 위한 별도의 교육 프로그램을 추진 필요
- 일정 시간 이상 SW 공급망 보안 교육을 이수한 구직자들을 SW 공급망 보안 인력이 필요한 기업과 매칭하여 취업으로 연계하는 프로그램 개발. 이를 통해 기업은 필요한 인력을 빠르게 확보할 수 있고, 구직자들은 변화하는 보안 환경에 적응하고 필요한 역량을 갖춘 상태로 취업 가능

○ 관련 기사 및 산업기사 시험에 출제 기준 포함

- SW 공급망 보안을 정보처리기사 또는 정보보안기사 자격증 시험의 출제 기준에 포함하여, 미래의 보안 전문가들이 필수적으로 SW 공급망 보안에 대한 지식을 습득하도록 유도

○ 자격증 신설을 통한 전문 인력 배출

- 관련 자격증을 신설하여 SW 공급망 보안 분야에서 필요한 기술과 지식을 공식적으로 인증할 수 있도록 함. 기업들은 SW 공급망 보안에 특화된 인력을 채용하거나 재직자들을 재교육할 때 자격증을 기준으로 활용할 수 있게 되어 관련 분야의 전문 인력 배출 촉진 가능

참고문헌

CD.foundation 홈페이지, https://cd.foundation/state-of-cicd-2024/

CSO 홈페이지, https://www.csoonline.com/article/1251452/bsimm-14-finds-rapid-growth-in-automated-security-technology.html

Forbes 홈페이지, https://www.forbes.com/councils/forbestechcouncil/2023/08/01/cybersecurity-investment-trends-in-the-us/

Forwarder 홈페이지. https://forwardermagazine.com/4-supply-chain-security-trends/

Gartner 홈페이지. https://www.gartner.com/en/supply-chain/trends/supply-chain-cybersecurity

NIST SP 800-218, 「Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities」 (2022)

NIST 홈페이지, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

PurpleSec 홈페이지, https://purplesec.us/resources/cybersecurity-statistics/

Reversinglabs 홈페이지, https://www.reversinglabs.com/sscs-report

Simply Flows 홈페이지. https://simplyflows.com/time-wasted-on-repetitive-tasks-is-40-percent/

국가직무능력표준(NCS) 홈페이지. https://www.ncs.go.kr/

대한민국 대통령실 홈페이지. https://www.president.go.kr/newsroom/press/gdXzwtKB

유럽 연합 위원회 홈페이지, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilien ce-act

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

ISSUE REPORT

(05717) 서울특별시 송파구 중대로 135, IT벤처타워 서관 14층
정보보호 인적자원개발위원회