히트맵 기반 스마트팩토리 보안위협 데이터 시각화 모델

정인수*, 김의진*, 곽진**
*아주대학교 사이버보안학과 정보보호응용및보증연구실
**아주대학교 사이버보안학과
jis0727@ajou.ac.kr, dmlwls0403@ajou.ac.kr, security@ajou.ac.kr

Visualization Model for Security Threat Data in Smart Factory based on Heatmap

In-Su Jung*, Eui-Jin Kim*, Jin Kwak**
*ISAA Lab., Dept. of Cyber Security, Ajou University
**Dept. of Cyber Security, Ajou University

요 약

4차 산업혁명으로 인해 제조산업에 인공지능, 빅데이터와 같은 ICT 기술을 활용한 스마트팩토리의 제조 공정 자동화 및 장치 고도화 연구가 진행되고 있다. 제조 공정 자동화를 위해 스마트팩토리의 각 계층별 장치들이 유기적으로 연결되고 있으며, 이로 인해 발생 가능한 보안위협도 증가하고 있다. 스마트팩토리에서는 SIEM 등의 장비가 보안위협 데이터를 수집·분석·시각화하여 대응하고 있다. 보안위협 데이터 시각화에는 그리드 뷰, 피벗 뷰, 그래프, 차트, 테이블을 활용한 대시보드 형태로 제공하고 있지만, 이는 스마트팩토리 전 계층의 보안위협 데이터 확인에 대한 가시성이 부족하다. 따라서, 본 논문에서는 스마트팩토리 보안위협 데이터를 CVSS 점수 기반의 Likelihood와 보안위협 데이터 기반의 Impact를 활용하여 위험도를 도출하고, 히트맵 기반 스마트팩토리 보안위협 데이터 시각화 모델을 제안한다.

1. 서론

제조산업과 ICT 기술을 융합한 스마트팩토리의 구축에 관한 많은 연구가 진행되고 있다. 스마트팩토리에서는 생산 과정에 필요한 전체 사물들을 IIoT(Industrial Internet of Things) 기술로 연결하여 통신체계를 구축하고 디지털화하여, CPS(Cyber Physical System), 빅데이터, 클라우드, 인공지능 등 여러 ICT(Information & Communication Technology) 기술들이 제조업에 활용될 수 있도록 함으로써 생산 공정의 자동화 및 최적화 연구가 진행되고 있다[1]. 그러나 스마트팩토리에 ICT 기술이 도입되고, IT 영역과 OT 영역이 연결됨에 따라 스마트팩토리에서의 발생 가능한 보안위협이 증가하고 있으며, 이를 위해 각 계층의 보안위협 데이터를 SIEM(Security Information and Event Management) 장비를 통해 수집·분석·시각화하여 대응하고 있다. SIEM 장비를 통해 분석된 데이터는 대응팀에게 전달되어 보안 사고에 대응하고 새로운 대응체계를 구축하는데 활용되며, 피벗 뷰, 그리드 뷰, 차트, 그래프 등을 통해 시각화된다. 하지만, 이러한 시각화 기법은 스마트팩토리 전 계층의 보안위협 데이터를 확인하기에는 가시성이 부족하다. 따라서, 본 논문에서는 스마트팩토리 전 계층의 보안위협 데이터를 시각화할 수 있는 히트맵 기반 보안위협 데이터 시각화 모델을 제안한다.

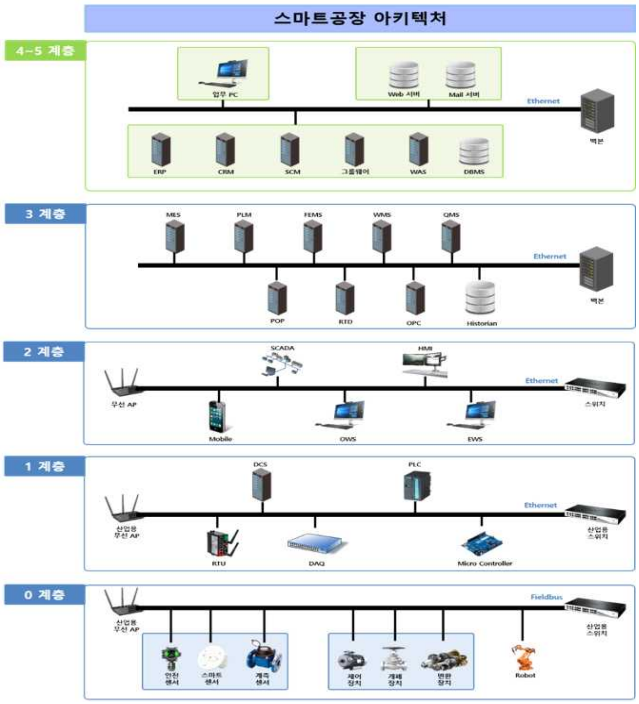
본 논문에서는 2장에서 스마트팩토리에 대한 정의와 스마트팩토리 보안위협 데이터 처리 현황에 대하여 설명한다. 또한, 히트맵에 대한 설명과 위험도 도출에 활용될 CVSS(Common Vulnerability Scoring System)를 설명한다. 3장에서는 SIEM 장비로부터 생성된 보안위협 데이터와 CVSS를 기반으로 보안위협 위험도를 도출하는 방법과 히트맵을 활용한 스마트팩토리 보안위협 데이터 시각화 모델을 제안한다. 4장에서는 히트맵 기반 시각화 모델을 통해 얻을 수 있는 기대효과를 다루고, 5장에서 결론을 맺는다.

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-01806, 스마트공장 보안 내재화 및 보안관리 기술 개발).

2. 관련 연구

2.1 스마트팩토리

스마트팩토리는 기존 제조기술에 센서, 클라우드, 빅데이터, 정밀 제어, 모바일 등 다양한 ICT 기술과의 융합을 통해 구축된다. 자동화 및 지능화된 인프라를 제공함으로써 생산성 향상, 에너지 절감, 안전한 생산환경 구현 등이 가능하다[2]. 스마트팩토리는 5계층 구조 아키텍처로 구성되어 있으며, (그림 1)을 통해 확인할 수 있다. 이는 국내외 스마트팩토리 산업제어시스템 표준(RAMI 4.0, ISA/IEC 62443, NIST 800-82, Purdue 모델 등)을 통해 구성된다[3].



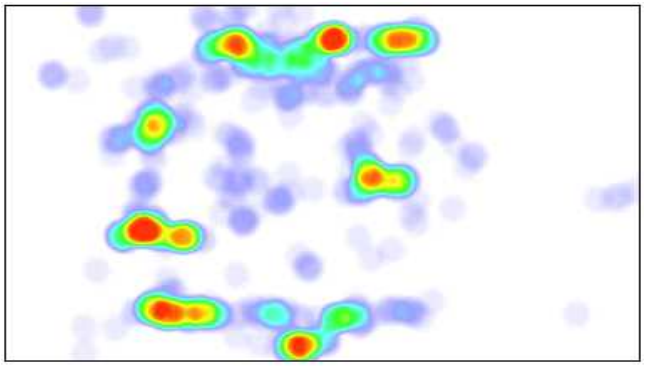
(그림 1) 스마트팩토리 5계층 아키텍처 구조

2.2 스마트팩토리 보안위협 데이터 처리 현황

스마트팩토리 보안위협 데이터는 SIEM 장비를 통해 수집·분석·시각화된다. SIEM은 SIM(Security Information Management)와 SEM(Security Event Management)를 결합한 보안 솔루션이다[4]. SIEM 장비는 스마트팩토리의 애플리케이션 및 네트워크 하드웨어에 의해 생성되는 보안 경보에 대하여 실시간 모니터링을 진행하며, 데이터 수집 및 분석, 이벤트 상관관계 도출, 리포팅 및 로그관리를 통해 보안위협 데이터를 생성한다. 생성된 보안위협 데이터는 그리드 뷰, 피벗 뷰, 차트, 그래프 등과 같은 시각화 기법을 활용하여 대시보드 형태로 대응팀에게 제공된다[5].

2.3 히트맵

히트맵은 색상을 통해 열분포 형태로 데이터를 제공하는 시각화 기법이다. 이는 대상의 전체적인 특성을 쉽고 빠르게 파악할 수 있는 장점을 갖고 있으며 웹사이트, 지리적, 주식시장 등에 아래 (그림 2)와 같은 시각화 기법이 적용된다[6].



(그림 2) 히트맵 시각화 기법

2.4 CVSS 3.1

CVSS 3.1는 소프트웨어 취약점의 특성과 심각도를 나타내기 위한 개방형 프레임워크이다. 이는 MITRE의 보안 취약점 관리체계인 CVE(Common Vulnerabilities and Exposure)의 요소 중 하나로, 보안 취약점이 동작하는 환경, 절차 및 파급력 등을 통해 취약점을 진단하고 평가할 수 있는 기준이다[7]. CVSS는 시간과 환경에 따라 분석한 취약점의 정도를 점수로 나타내어 취약점의 위험도를 제공한다. 아래 <표 1>은 CVSS 점수를 나타낸 표이다[8].

<표 1> CVSS 3.1 점수

Rating	CVSS Score
None	0.0
Low	0.1 ~ 3.9
Medium	4.0 ~ 6.9
High	7.0 ~ 8.9
Critical	9.0 ~ 10.0

3. 제안사항

본 장에서는 SIEM 장비를 통해 얻은 보안위협 데이터를 기반으로 보안위협 위험도를 시각화해주는 히트맵 기반 스마트팩토리 보안위협 데이터 시각화 모델을 제안한다. 기존의 히트맵 시각화 방법을 확장하여 스마트팩토리 전 계층 구조에 대한 보안위협 데이터 시각화를 목표로 한다. 보안위협 데이터를 히트맵으로 시각화하는데 있어서 중요한 이슈는 상이한 범위를 가지는 데이터를 동일한

중요도를 가지고 시각화하는 것이다. 이를 위해, 히트맵에 표시될 색상을 정하기 위한 위험도 수식을 도입하며[9], 수식에 사용되는 지표는 아래와 같다.

$$R = L * I \quad (1)$$

❒ Risk(R)

: Risk는 스마트팩토리 보안위협에 대한 위험도를 나타내는 변수이며, 히트맵 색상을 결정하는데 사용된다.

❒ Likelihood(L)

: Likelihood는 발생한 사고에 사용된 취약점의 CVSS 점수를 기반으로 도출된 변수로, 취약점을 활용한 공격 가능성을 의미한다. 이는 None, Low, Medium, High, Critical과 같이 5단계로 구성된다.

- None

: CVSS 0.0으로 취약점을 활용한 공격 가능성이 없는 단계이다.

- Low

: CVSS 0.1 ~ 3.9으로 취약점을 활용한 공격 가능성이 적은 단계이다.

- Medium

: CVSS 4.0 ~ 6.9으로 취약점을 활용한 공격 가능성이 있는 단계이다.

- High

: CVSS 7.0 ~ 8.9으로 취약점을 활용한 공격 가능성이 높은 단계이다.

- Critical

: CVSS 9.0 ~ 10.0으로 취약점을 활용한 공격 가능성이 높고, 치명적 공격이 가능한 단계이다.

❒ Impact(I)

: Impact는 SIEM에서 분석된 보안위협 데이터를 통해 도출된 변수로, 공격에 의해 시스템이 영향을 받은 정도를 의미한다. 이는 SIEM을 제공하는 기업의 심각도 수준을 기반으로 작성되었으며[10], Level 1, Level 2, Level 3, Level 4와 같이 4단계로 구성된다.

- Level 1

: 최소한의 시스템이 영향을 받거나 소프트웨어가 오작동하여 최소한의 영향을 미친 경우를 의미하며, 간단한 사고 대응 해결책이 존재하는 경우이다. 사용자 지정 콘텐츠 오류, 문서 오류 등이 이에 해당된다.

- Level 2

: 약간의 시스템이 영향을 받거나 소프트웨어 운영에 영향을 주지 않는 기능만 사용할 수 없는 상태를 의미하며, 사고 대응 해결책이 존재하는 경우이다. 러닝타임 지연, 애플리케이션 작동 오류 등이 이에 해당된다.

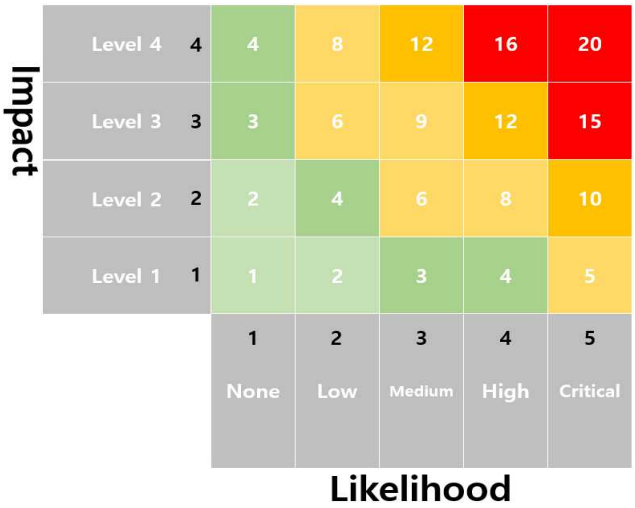
- Level 3

: 상당수의 시스템과 소프트웨어의 중요 기능들이 영향을 받거나 성능이 크게 저하되는 경우, 정상적인 시스템 운영에 영향을 미치는 경우를 의미하며, 사고 대응 해결책이 존재하는 경우이다. 애플리케이션 로드 실패, 배포 실패, 사용자에게 영향을 미치는 성능 저하 등이 이에 해당된다.

- Level 4

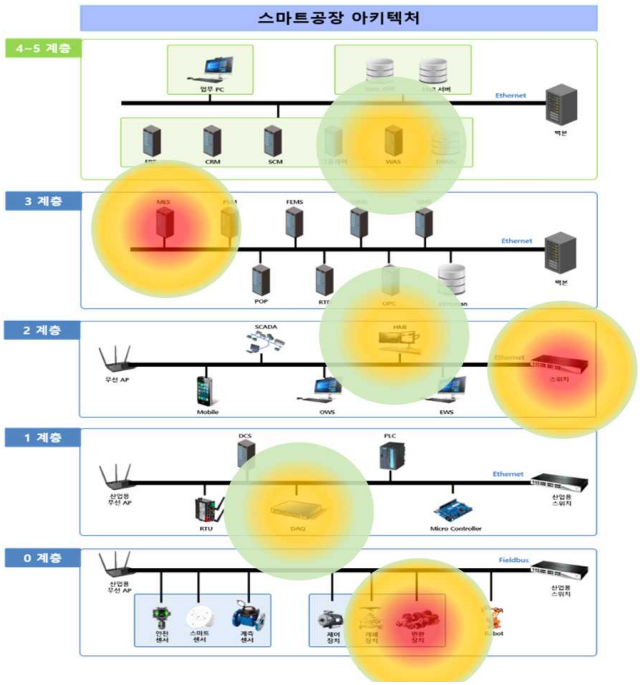
: 생산, 시스템 작동 중단 상황이 발생하는 경우, 사고 대응 해결책이 존재하지 않아 가동을 멈추고 대응 해결책을 연구해야 하는 경우를 의미한다. 모든 이벤트 상관관계 분석 기능 강제종료, 업그레이드 또는 패치 실패, 사용자 인터페이스 사용 불가능 등이 이에 해당된다.

위와 같이 CVSS 점수 기반의 Likelihood와 SIEM 장비의 보안위협 데이터 기반의 Impact를 통해 위험도를 도출할 수 있다. 이를 위해 아래 (그림 3)과 같은 Likelihood와 Impact 기반 위험도별 히트맵 색상 분포를 제안한다.



(그림 3) 위험도별 히트맵 색상 분포

히트맵에 적용하기 위한 위험도 수식을 기반으로 (그림 3)와 같은 위험도별 히트맵 색상 분포를 도출할 수 있었으며, 이는 위험도에 따라 색상별로 구성되어 있다. 최종적으로 위험도별 히트맵 색상 분포를 스마트팩토리 전 계층에 적용하여 아래 (그림 4)과 같이 스마트팩토리 보안위협 데이터를 시각화할 수 있다.



(그림 4) 히트맵 기반 스마트팩토리
보안위협 데이터 시각화 모델

4. 기대효과

본 논문의 제안사항에 대한 기대효과는 다음과 같다.

❒ 스마트팩토리의 전 계층 시각화

본 논문에서는 기존의 그리드 뷰, 피벗 뷰, 차트, 그래프 등과 같은 시각화 기법의 전 계층에 대한 부족한 가시성을 보완하기 위해, 히트맵을 통해 스마트팩토리 전 계층에 대한 보안위협 데이터를 시각화하였다. 이를 통해, 사고에 대한 신속한 분석 및 대응이 이뤄질 수 있다.

❒ 보안위협 우선순위 시각화

본 논문에서 제안한 히트맵 시각화 모델은 Likelihood와 Impact를 기반으로 위험도를 도출함으로써 위험도별 색상 분포로 보안위협 우선순위를 시각화한다. 이를 통해 신속하게 위험도를 파악할 수 있으며, 경제적으로 효율적인 위험도별 차등 대응이 가능하다.

5. 결론

본 논문에서는 기존의 스마트팩토리 보안위협 데이터 시각화 기법의 가시성을 보완하기 위해, 히트맵 기반 스마트팩토리 전 계층의 보안위협 데이터 시각화 모델을 제안하였다. 히트맵 기반 시각화 모델을 통해 신속한 사고 대응에 기여할 수 있을 것이다.

참고문헌

[1] 김현진, 김성진, 김예솔, 김신규, 손태식, “신뢰성 있는 스마트팩토리를 위한 사이버보안 아키텍처”, 정보보호학회논문지, 29, 3, 629-643, Jun. 2019.

[2] 이현정, 유상근, 김용운, “스마트공장 기술 및 표준화 동향”, 국가기술표준원, 32, 3, Jun. 2017.

[3] 한국인터넷진흥원, “스마트공장 보안 모델”, Dec. 2020.

[4] 김경신, “통합보안관리시스템 보안 분석 및 개선”, 한국인터넷방송통신학회 논문지, 15, 1, 15-23, Feb. 2015.

[5] Ryu, S., Kang, Y. J., & Lee, H., “A study on detection of anomaly behavior in automation industry”, IEEE, 377-380, Feb. 2018.

[6] Pleil, Joachim D. et al. “Heat map visualization of complex environmental and biomarker measurements.”, Chemosphere, 84, 5, 716-723, Jul. 2011.

[7] 장대일, “소프트웨어 보안 취약점 평가 체제 동향”, 한국인터넷진흥원, 2019.

[8] FIRST, “Common Vulnerability Scoring System Version 3.1”, https://www.first.org/cvss/v3.1/specification-document

[9] 김인경, 박남제, “위험 평가 모델 기반의 정량적 사이버 보안 평가 체계”, 정보보호학회논문지, 29, 5, 1179-1189, Oct. 2019.

[10] IBM Security QRadar SIEM, “How to determine your case severity level”, Feb. 2021.