Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.6, Dec. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.6.1601

외부 STIX 수집 정보를 이용한 내부자산과 연계한 TTP 대응 전략 자동 매핑 구조에 관한 연구*

유 현 수,[1†] 김 환 국[2‡]
[1]상명대학교 (학생), [2]국민대학교 (교수)

Automatic Mapping Structure of TTP Response Strategies Linked to Internal Assets Using External STIX Collection Information*

Hyeon-su Yoo,[1†] Hwan-kuk Kim[2‡]
[1]Sangmyung University (Undergraduate student), [2]Kookmin University (Professor)

요 약

본 논문은 지능형 사이버 보안을 위한 SOAR 기술을 접목하여 보안 위협을 탐지하고 관리하는 자동화 시스템을 제안한다. 연구의 목적은 외부 STIX/TAXII 기반 데이터를 분석하여 사이버 위협 인텔리전스(CTI)를 구축하고, 이를 통해 내부 자산의 위험도를 정밀하게 산출하며 효과적인 대응 전략을 수립하는 것이다. 제안하는 시스템은 크게 네 가지 컴포넌트로 구성된다: CTI 수집 및 정형화, CTI 기반 TTP 매핑, 내부 자산 CPE 식별, 위험도 산출 및 대응 전략 도출. 정보 수집 방법으로는 공개된 외부 보안 위협 정보를 수집하고, 이를 정형화하여 CTI 통합 데이터베이스에 적재하는 과정을 포함한다. 또한, 룰 기반 매핑 알고리즘을 활용하여 CVE, CPE, CVSS, TTP와 같은 주요 정보를 기반으로 위험도 및 대응 전략을 도출한다. 결과적으로, 본 논문에서 제안하는 자동화 시스템은 약 1시간 내에 약 2300개의 report를 자동으로 분석하고, 99.74%의 높은 정도로 정탐을 수행할 수 있음을 보여준다.

ABSTRACT

This paper proposes an automated system for detecting and managing security threats by incorporating SOAR technology for intelligent cybersecurity. The objective of the study is to analyze external STIX/TAXII-based data to build Cyber Threat Intelligence (CTI), thereby accurately assessing the risk levels of internal assets and establishing effective response strategies. The proposed system consists of four main components: CTI collection and normalization, CTI-based TTP mapping, internal asset CPE identification, and risk assessment and response strategy formulation. The information collection method involves gathering publicly available external threat intelligence and normalizing it for storage in a CTI integrated database. Additionally, a rule-based mapping algorithm is utilized to derive risk levels and response strategies based on key information such as CVE, CPE, CVSS, and TTP. As a result, the automated system proposed in this paper demonstrates the capability to analyze approximately 2,300 reports within one hour and achieve a high detection accuracy of 99.74%.

Keywords: Cyber Threat Intelligence, STIX/TAXII, Response Strategy, Automation

Received(10. 28. 2024), Modified(11. 25. 2024), Accepted(11. 27. 2024)

* 이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임 (RS-2021-II210358, AI·빅데이터 기반 사이버 보안 오케스트레이션 및 자동 대응 기술 개발)

† 주저자, hyeonsuyoo0613@gmail.com
‡ 교신저자, rinyfeel@kookmin.ac.kr(Corresponding author)

I. 서 론

사이버 보안 분야에서는 위협 감지 및 대응을 위한 효율적인 자동화 솔루션의 수요가 급증하면서, 보안 오케스트레이션, 자동화 및 대응(Security Orchestration, Automation, and Response, SOAR) 기술이 각광받고 있다[1]. 이 기술은 소중한 자원을 절약하고, 보안 팀의 업무 효율성을 향상시키는 데 핵심적인 역할을 하며, 사이버 공격의 증가와 복잡성에 대응하기 위한 유용한 도구로 자리 잡고 있다. 현재 사이버 보안 산업은 전문 인력 부족 문제에 직면해 있으며, 이는 더욱 정교해진 사이버 위협 때문에 더욱 심화되고 있다[2]. SOAR 플랫폼은 이러한 문제를 해결하기 위해 다양한 보안 툴과 시스템을 통합하여 중앙 집중적으로 관리하며, 자동으로 운영되는 작업을 지원한다[3]. 이 과정에서 보안 팀은 반복적이고 시간 소모적인 작업에서 벗어나 보다 전략적인 임무에 집중할 수 있다.

또한, CTI(Cyber Threat Intelligence)를 활용한 자동화 시스템 구축의 중요성이 강조되는 상황이다. CTI는 최신 사이버 위협 정보를 제공하여 시스템의 대응 능력을 극대화하며, 이를 통해 위협 탐지와 분석을 더욱 정교화할 수 있다[4]. 수동으로 분석하는 환경에서의 업무 부담 또한 줄이는 데 기여한다.

따라서 본 논문에서는 외부 STIX[5]/TAXII[6] 서버에서 들어오는 데이터를 분석하여 자동으로 CTI를 생성하고, 내부 자산의 CPE(Common Platform Enumeration)와 CTI의 매핑을 통해 위험도를 산출하며, 생성된 CTI의 TTP(Tactic, Technique, Procedures)를 활용하여 효과적인 대응 전략을 도출하는 자동화 프레임워크를 연구한다. 현재 내부 자산의 CPE를 조합하여 수집된 CTI 데이터와의 비교 및 일치를 수동으로 수행하고 있는 상황에서, 이 과정은 시간 소모가 크고 데이터의 일관성과 정확성을 저해할 수 있는 문제점을 가지고 있다.

이러한 문제를 해결하기 위해, 본 연구는 수동적인 분석 및 매핑 과정을 자동화하여 시간 단축을 목표로 한다. 자동화 시스템을 통해 위험도 산출 공식을 적용하여 수치적으로 위험도를 제공하고[7], CTI 구축을 통해 얻은 TTP의 값을 활용하여 대응 전략을 도출할 수 있다. 위험도 산출 및 대응 전략 도출을 자동화함으로써 모든 정보를 한눈에 볼 수 있도록 하여 효율적인 보안 관리 체계를 제공하고자 한다.

본 논문의 구성은 다음과 같다. 1장의 서론 이후에 2장은 관련 연구, 3장은 제안 시스템에 관한 설명, 4장은 알고리즘 기능 실험 및 정확성 검증 실험 결과, 5장은 결론으로 마무리한다.

II. 관련 연구

2.1 CTI 활용 보안 정보 수집

기존 IT 기술이 널리 적용된 제어 시스템을 대상으로 하여, 보안 정보 수집 방안으로 CTI 모델을 활용하고, 포맷 확장을 통해 제어 시스템 특화 정보를 수용할 수 있도록 한다. 이를 검증하기 위해 윈도우 이벤트 로그, 리눅스 로그, Snort 로그, EWS 응용 프로그램 로그 등 다양한 보안 정보 포맷을 개발하고, 이를 통해 보안 정보 표현의 불일치 문제를 해결할 수 있는 시스템을 구축하였다. 향후에는 추가적인 보안 정보 포맷 설계와 함께, 각 기관의 내부 제어 시스템뿐만 아니라 외부 제어 시스템의 사이버 위협 정보도 수집할 수 있는 연구가 필요하다. CTI 환경에서는 양질의 정보를 상호 공유하는 것이 핵심이며, 이를 통해 제어 시스템 환경에서도 효과적인 사이버 위협 대응이 가능할 것으로 기대된다[2].

2.2 CTI 결측치 처리 연구

CTI(사이버 위협 인텔리전스)의 효율적 관리를 위해 데이터 파싱 및 결측치 처리 알고리즘이 중요한 역할을 한다. 이 알고리즘은 외부 STIX/TAXII 서버에서 수집한 정보를 바탕으로 설계된 시스템으로, 데이터 파싱 컴포넌트는 JSON 형식의 row 데이터를 분석하여 CVE, CPE, TTP로 분류한다. 이 과정에서 데이터는 다음과 같은 다섯 가지 케이스로 구분된다:

Case 1: CVE만 존재 (2,673개)
Case 2: CPE만 존재 (1개)
Case 3: CVE와 CPE 존재 (2개)
Case 4: CVE와 TTP 존재 (6개)
Case 5: TTP만 존재 (64개)

이 시스템은 총 2,746개의 항목을 집계하며, 각 케이스의 데이터 수를 통해 결측치 처리와 관련된 정보도 파악할 수 있다.

결측치 처리 컴포넌트는 분류된 데이터를 CTI 통합 데이터베이스의 적절한 테이블에 저장하기 위해 결측치를 효과적으로 처리하는 과정을 포함한다. 이 DB는 CVE, CPE, CVSS 정보를 포함하는 여러 테이블로 구성되며, 각 케이스별로 존재하는 결측치를 판단하고 cve_detail 테이블을 통해 필요한 정보를 보완한다.

위의 연구 과정을 통해 TTP 매핑과 위험도 산출 및 대응 전략을 도출하는 데 필요한 기반을 마련할 수 있으며, 이후 연구에 중요한 발판이 될 것으로 확인된다.

III. 제안 시스템

3.1 제안 시스템의 구성 컴포넌트

본 연구는 내부자산의 CPE가 적재된 CTI와 일치하도록 하여, 이를 기반으로 위험도를 정밀하게 산출하고 효과적인 대응 전략을 수립하는 것을 목표로 한다. 이 연구는 크게 네 가지 컴포넌트로 구성된다. 첫 번째는 CTI 수집 및 정형화 컴포넌트로, 정형화된 CTI 소스를 활용하여 수집 블록과 전처리 블록을 거쳐 CTI 통합 DB에 데이터를 적재하는 과정을 포함한다[8]. 두 번째는 CTI 기반 TTP 매핑 컴포넌트로, 룰 기반 CTI-TTP 매핑 블록에서 기존에 적재된 CTI를 기반으로 TTP를 매핑하는 과정을 거친다[9]. 이 결과는 CTI 통합 DB에 업데이트된 형태로 저장된다. 세 번째는 내부자산 식별 컴포넌트이다. 이 모듈은 다른 내부자산 DB에서 CPE를 구하기 위해 데이터 로드 블록, CPE 추출 블록, CPE 단일화 처리 블록을 통해 CPE를 도출한 후, CTI 통합 DB에 존재하는 CPE와의 일치를 확인한다. 마지막으로 네 번째 컴포넌트인 위험도 산출 및 대응 전략 모듈에서는 위험도 산출 블록과 대응 전략 도출 블록을 통해 위험도를 산출하고 대응 전략을 매핑하는 결과를 도출한다[10].

3.2 CTI 수집 및 정형화 컴포넌트

이 모듈은 공개된 외부 보안 위협 정보를 수집하는 기능을 수행한다. Fig. 1.에서 모듈의 입출력은 외부 CTI 정형 데이터와 CTI 정보 내 필요 객체 정보 추출 후 CTI 통합 데이터베이스에 적재되는 과정을 포함한다. 이 모듈은 총 두 가지 하위 블록, 즉 수집 블록과 전처리 블록으로 구성된다.

수집 블록은 외부 CTI 소스로부터 CTI 데이터를 수집하며, 전처리 블록은 Fig. 2.에서처럼 수집한 CTI 데이터의 파싱과 결측치 발생 시 이를 처리하여 데이터를 보완하는 과정을 거친다. 구체적으로 전처리 블록은 수집한 CTI 데이터(json)를 정형화하여 CTI 통합 데이터베이스의 cti 테이블에 적재하는 역할을 한다. 이를 위해 데이터 파싱 유닛과 결측치 처리 유닛으로 나뉘며, 수집한 CTI row 데이터는 데이터 파싱을 통해 다섯 가지 케이스로 분류된다. 각 케이스에 맞춰 결측치를 처리하는 알고리즘이 적용된다.

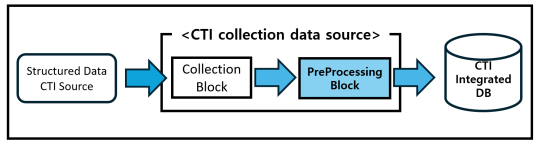


Fig. 1. Collection and preprocessing workflow of CTI data sources

Table 1. Primary CTI table generated using methods for handling missing values, excluding TTP values for the five algorithms

	Missing value	Processing Method	1st cti Table Save Result
① Only CVE exists	CPE, CVSS, TTP	After missing CVE, CPE, CVSS data processing in cve_detail table, store only TTP as NULL value	TTP only NULL value (Allow NULL for other values)
② Only CPE exists	CVE, CVSS, TTP		
③ CVE, CPE exist	CVSS, TTP		
④ CVE, TTP exist	CPE, CVSS	Missing CPE, CVSS data Preprocessing in cve_detail table	Existence of all values (NULL allowed)
⑤ TTP exists	CVE, CPE, CVSS	Save only the TTP value with the remaining NULL value CTI	Only TTP values exist

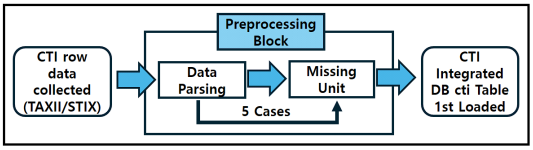


Fig. 2. Preprocessing Module: Data Parsing and Missing Value Processing Unit

결측치 처리 유닛에서는 전처리 과정에서 CVE(Common Vulnerabilities and Exposures) 객체 중 하나라도 비어 있는 경우를 결측치로 정의한다. CVE 객체는 key 값으로 CVE_ID, CPE, CVSS(Common Vulnerability Scoring System), TTP로 구성된 하나의 딕셔너리 형태를 말한다. 결측 처리가 가능할 경우, 즉 완전한 CVE 객체가 아닐 경우 cve_detail 테이블에서 데이터를 수집하여 결측치를 보완한다. 1차 결측치 처리는 cve_detail 테이블에서 결측 처리가 가능한 데이터를 1차로 처리하고, 이를 cti 테이블에 저장하는 과정을 포함한다.

3.3 CTI 기반 TTP 매핑 컴포넌트

CTI 통합 DB의 cti 테이블에서 1차로 적재된 데이터에 대해 CVE와 TTP를 매핑하는 과정이 진행된다. 이 과정의 입력은 CTI 통합 DB의 cti 테이블에 1차로 적재된 CTI 데이터이며, 출력은 모든 결측을 보완한 CVE 객체 형태로 cti 테이블에 2차로 적재되는 것이다.

이 모듈은 두 가지 하위 블록으로 구성된다. 첫 번째 블록은 CVE→TTP 매핑이며, 이는 CVE, CPE, CVSS의 결측을 보완하고 TTP의 값만 NULL인 CVE 객체를 통해 TTP의 결측을 해결하는 과정을 포함한다. 이때 CVE의 CWE를 찾아내어 Capec.json을 통해 TTP를 구하게 된다. 두 번째 블록은 TTP→CVE 매핑으로, TTP의 값만 존재하고 나머지 키 값이 결측인 CVE 객체의 결측을 보완하는 과정에 해당한다. TTP를 Capec.json에 검색하여 그에 맞는 CWE를 찾아내고 CWE에 해당하는 모든 CVE를 찾아내는 것이다. 이 두 매핑 과정을 통해 완전한 CVE 객체가 형성되며, 최종적으로 CTI 통합 DB의 cti 테이블에 2차로 적재된다.

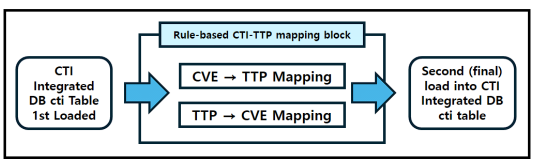


Fig. 3. Rule-Based Mapping Module: Rule-Based Mapping between CVE and TTP

Table 2. Method for handling all missing values, including TTP values, based on the results of the primary CTI table storage for the five algorithms

	1st cti Table Save Result	Processing Method
① Only CVE exists	TTP only NULL value (Allow NULL for other values)	Missing TTP Value Processing
② Only CPE exists		
③ CVE, CPE exist		
④ CVE, TTP exist	Existence of all values (NULL allowed)	
⑤ TTP exists	Only TTP values exist	CVE, CPE, CVSS missing processing

3.4 내부자산 CPE 식별 컴포넌트

이 모듈은 내부 자산의 CPE를 식별하고 이를 CTI와 일치시키는 과정이다. 우선, 내부 자산 식별 모듈을 통해 내부 자산의 시스템 정보를 이용해 CPE를 조합한다. 이후 위험도 산출 모듈과 대응 전략 모듈을 거치게 되며, 이 과정은 다음과 같이 진행된다. 먼저, 내부 자산의 데이터베이스에서 정보를 얻기 위해 데이터 로드 블록을 통해 시스템 정보 수집 유닛과 네트워크 정보 수집 유닛을 활용한다. 이 정보를 바탕으로 CPE 추출 블록을 통해 CPE 검색 유닛과 자산 정보 전처리 유닛을 거치고, 마지막으로 CPE 단일화 처리 블록으로 이동한다. 이 단계에서 검색된 CPE의 개수를 파악하고, CPE 단일화 처리를 진행한다. 이후, CTI 통합 DB의 internal_assets_network 테이블에 여러 가지 정보와 CPE를 저장함으로써 위험도 산출을 위한 CPE 조합이 완료된다.

3.5 위험도 산출 및 대응전략 도출 컴포넌트

본 연구에서는 네트워크 내부 자산의 위험도를 다

음과 같이 산출한다. 위험도 산출 공식을 통해 계산된다.

$$R = (C \times 0.3) + (\mathrm{B} \times 0.4) + (\mathrm{I} \times 0.3) \quad (1)$$

여기서 R은 네트워크 내부 자산 위험도를 나타내며, C는 수집한 CTI 위험도, B는 네트워크 자산 기본 위험도, I는 네트워크 자산 중요도를 의미한다. 각 요소는 해당 자산의 위험성을 평가하기 위해 가중치를 부여하여 계산된다. 이러한 가중치는 각 요소의 중요성을 반영하여 자산의 총 위험도를 보다 정확하게 계산하는 데 사용된다. 이 과정은 CVSS의 0에서 10까지의 점수 범위와 NVD(National Vulnerability Database)의 기준을 따르며, 모든 요소의 값이 10 미만으로 설정되어 최종 위험도의 계산에 영향을 미치지 않도록 한다.

수집한 CTI 위험도는 네트워크 내부자산의 CPE를 기반으로 CTI 테이블에서 검색했을 때 나오는 CVE ID에 대한 CVSS 값이다. 내부 자산 식별 모듈을 통해 조합된 내부 자산 CPE를 CTI 테이블에서 검색한 후, 일치하는 CPE를 가진 CVE ID에 대한 CVSS 값을 가져온다. 예를 들어, 내부자산 테이블의 CPE 중 하나인 'cpe:2.3:a:gnu:ncurses:5.9:::::::*'를 CTI 테이블에서 검색했을 때, CVSS v3는 NULL 값이고, CVSS v2는 6.9가 나타난다면, CVSS 값을 선택할 기준은 CVSS v3로 하되, 해당 값이 없을 경우 CVSS v2를 사용한다.

두 번째로, 네트워크 자산 기본 위험도는 내부 자산 CPE로 NVD에서 검색한 모든 CVE의 CVSS 평균을 의미한다. 위와 마찬가지로 CVSS 값의 평균은 CVSS v3를 기준으로 계산하되, CVSS v3 값이 없는 경우 CVSS v2를 사용한다. 세 번째로, 네트워크 자산의 중요도는 내부 자산 CPE가 갖는 고유의 중요도로, 고유값이기 때문에 계산을 위해 임시로 랜덤값으로 지정한다. 실제 계산 시에는 내부 자산에서 정한 중요도에 따라 조정해야 한다.

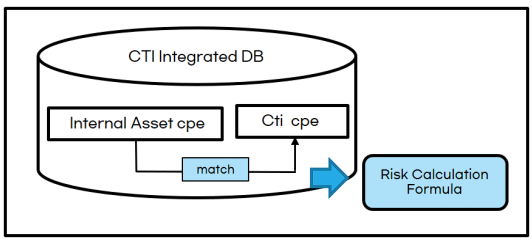


Fig. 4. Risk calculation process through risk assessment formula

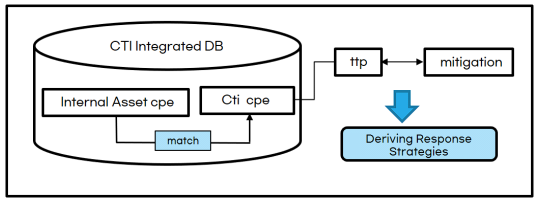


Fig. 5. Process of mapping between CTI TTP and mitigation and deriving response strategies

이러한 평가 방법은 해당 자산을 얼마나 빨리 보호해야 하는지를 결정하는 데 중요한 역할을 하며, 높은 기본 위험도와 중요한 CTI 정보가 결합될 경우 보안 조치를 즉시 강화해야 한다는 결론에 도달할 수 있다. 결과적으로, 위험도 평가는 사용자들이 각 요소가 위험에 기여하는 방식을 이해하도록 도와주어, 보안 정책과 위협 관리 전략 수립에 중요한 기여를 한다.

대응 전략 도출 과정은 다음과 같다. CTI 통합 DB에서 내부 자산 CPE와 CTI의 CPE를 비교하여 일치하는 경우, 해당 CPE에 맞는 TTP를 가져와 대응 전략(Mitigation)과 매핑하는 과정을 거친다. 이러한 과정을 통해 보다 효과적인 위험 관리와 대응 전략을 수립할 수 있다.

IV. 실험 결과

4.1 CTI-TTP 매핑 알고리즘 기능 테스트

각 5가지 케이스에서는 두 개의 입력을 가정하여 기능 테스트를 진행한다. Case 1에서는 'CVE-2010-3847'과 'CVE-2018-11776'이 외부 STIX/TAXII 서버의 report 형식으로 입력된 경우를 가정한다. 이 경우, 결측치인 CPE, CVSS v3, CVSS v2를 cve_detail 테이블에서 찾아 처리하는 과정을 진행한다. 결측치 처리 성공률은 100%에 달하지만, 처리된 CVE 객체 2개에 대해 CTI와 TTP를 매핑하는 과정에서 2개 중 1개만 매핑이 성공한다. 이는 'CVE-2018-11776'에 대한 TTP 매핑에 필요한 CWE가 NVD에 존재하지 않기 때문이다.

그러나 이 사례를 통해 CTI 기반의 TTP 도출이 가능하다는 점을 확인할 수 있다.

Case 2에서는 CPE만 존재하는 상황으로,

Algorithm 1 Taxii to CTI

```
taxii_to_cticve_id, ttp, cpecursor ← OPEN database cursor if cve_id is not NULL then
if ttp is NULL AND cpe is NULL then
  Case: CVE only
  result ← EXECUTE SQL query to get cpe, cvss_ver3, cvss_ver2
  if result is not NULL then
    CALL insert_cti(cve_id, cpe, cvss_ver3, cvss_ver2, NULL)
  end if
else if ttp is not NULL then
  Case: CVE and TTP
  result ← EXECUTE SQL query to get cpe, cvss_ver3, cvss_ver2
  if result is not NULL then
    CALL insert_cti(cve_id, cpe, cvss_ver3, cvss_ver2, ttp)
  end if
else if cpe is not NULL then
  Case: CVE and CPE
  result ← EXECUTE SQL query to get cpe, cvss_ver3, cvss_ver2
  if result is not NULL then
    CALL insert_cti(cve_id, cpe, cvss_ver3, cvss_ver2, NULL)
  end if
end if
else if ttp is not NULL then
  Case: TTP
  CALL insert_cti(NULL, NULL, NULL, NULL, ttp)
else if cpe is not NULL then
  Case: CPE
  results ← EXECUTE SQL query to get cve_id, cpe, cvss_ver3, cvss_ver2
  for each result in results do
    CALL insert_cti(cve_id, cpe, cvss_ver3, cvss_ver2, NULL)
  end for
end if
CLOSE cursor
```

Fig. 6. Five Storage Algorithms for External STIX/TAXII Server Data: 1) CVE only, 2) CVE and TTP, 3) CVE and CPE, 4) TTP, 5) CPE

'cpe:2.3:a:bumsys_project:bumsys:::::::::'와 'cpe:2.3:a:glpi-project:glpi:::::::::'를 받아온다고 가정한다. 이 경우, cve_detail 테이블에서 결측치를 처리하는 과정을 거치면 100%의 성공률을 보인다. 처리된 2개의 CPE와 매핑된 CVE의 개수는 102개로 증가하며, 이 중 TTP와 매핑에 성공한 CVE 개수는 36개이다. 따라서 이 케이스 역시 CTI 기반의 TTP 도출이 정상적으로 이루어질 수 있음을 나타낸다.

Case 3에서는 CVE와 CPE가 모두 존재하는 경우로, 'CVE-2023-42491'과 'cpe:2.3:a:busbaer:eisbaer_scada:::::::::', 'CVE-2023-37220'과 'cpe:2.3:h:synel:synergy:::::::::'이 입력으로 들어온다. 이 경우, CPE, CVSS v3, CVSS v2의 결측치를 처리하는 과정에서 100%의 성공률을 보인다. 그러나 TTP 매핑에 실패하는 이유는 두 가지로 구분된다.

첫 번째로, 'CVE-2023-42491'이 입력으로 들어올 경우, Capec.json에 CVE에 해당하는 CWE는 존재하지만, 그 CWE에 해당하는 TTP가 존재하지 않아 매핑에 실패한다. 두 번째로, 'CVE-2023-37220'이 입력될 경우, Capec.json에 CVE에 해당하는 CWE가 존재하지 않아 TTP 매핑에 실패하게 된다. 그러나, Capec.json에 CWE와 TTP가 매핑되어 있는 CVE가 있다면 성공적으로 매핑 가능하다는 것을 알 수 있다.

Case 4에서는 'CVE-2010-3847'과 'T1133', 'CVE-2004-2252'와 'T1592.002'가 입력되며, 이 경우 CVE와 TTP가 모두 존재하므로 결측치 처리 과정만 거쳐 CTI에 저장된다.

마지막으로 Case 5에서는 'T1195.001'과 'T1083'이 입력으로 들어온다. 이 경우 CVE, CPE, CVSS v3, CVSS v2의 결측치를 처리하여 저장되며, 매핑된 CVE 개수는 32개가 된다.

4.2 CTI-TTP 매핑 정확성 검증 실험

본 실험에서는 외부 STIX/TAXII 서버에서 수집한 데이터를 기반으로 TTP를 분류하였다. 총 64개의 TTP 중 Case 5에 해당하는 'T1133'이 13개의 CVE와 매핑된 결과를 확인하였다. 이를 통해 T1133만이 CVE와 매핑되는지 확인하기 위해, Capec.json에 존재하는 모든 TTP에 대한 CVE 매핑을 시도하였다.

Capec.json에 등록된 TTP는 총 189개로, 이들 TTP는 총 2,057개의 CVE와 매핑되었다. 그 결과, 189개 TTP 중에서 CVE와 매핑되기 위해 Capec.json에 TTP와 CWE가 적절히 존재하는 것은 오직 T1133뿐임을 확인하였다.

이후, CTI에 이미 TTP 매핑이 완료된 CVE-TTP 데이터 784개를 대상으로 CVE만 저장한 후, CTI 데이터베이스의 CVE - CPE - TTP 매핑 과정을 통해 TTP 탐지의 정확성을 검증

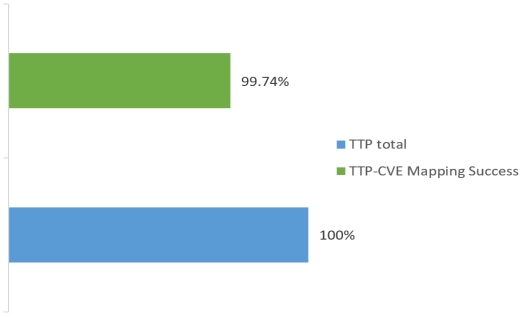
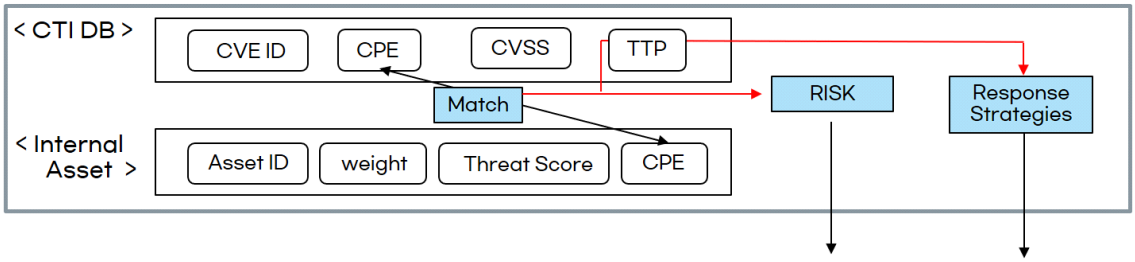


Fig. 7. Of the total 784 TTPs, 782 have successful TTP-CVE mapping, resulting in a 99.74% mapping success rate



check_id	ranking	asset_id	ip_addr	mac_a	cpe	cve_id	asset_base_score	cti_score	final_exploit_score	ttp	defense_strategy
8	NULL	1468312967383570620	73.208.219.197	NULL	cpe:2.3:a:x.org:libxi:1.7.9:*:*:*:*:*:*:*	CVE-1999-0526	5.5	10	7.3	NULL	NULL
9	NULL	16137491968187424 3	65.132.208.45	NULL	cpe:2.3:a:logrotate_project:logrotate:3.8.6:*:*:...	NULL	7.57	NULL	NULL	NULL	NULL
10	NULL	17877395140418640 85	42.1.166.127	NULL	cpe:2.3:a:fontconfig_project:fontconfig:2.13.0:*:*...	NULL	7.186	NULL	NULL	NULL	NULL
11	NULL	17969158562176027 62	9.211.141.101	NULL	cpe:2.3:a:fontconfig_project:fontconfig:2.13.0:*:*...	NULL	7.186	NULL	NULL	NULL	NULL
12	NULL	19635082612046950 28	98.114.180.198	NULL	cpe:2.3:a:avahi:avahi:0.6.31:*:*:*:*:*:*:*	CVE-2008-5081	6.237	5	6.3948	NULL	NULL
13	NULL	20350455845743290 74	108.29.141.168	NULL	cpe:2.3:a:gnu:ncurses:5.9:*:*:*:*:*:*:*	CVE-2010-3847	6.88	6.9	5.122	T1027.009, T1574.010, T1547.009, T1027.006, T1564...	M1054, M1032, M1017
14	NULL	21131387814560779 35	47.40.153.48	NULL	cpe:2.3:a:gnu:ncurses:5.9:*:*:*:*:*:*:*	CVE-2010-3847	6.88	6.9	7.222	T1027.009, T1574.010, T1547.009, T1027.006, T1564...	M1054, M1032, M1017
15	NULL	23493808485521482 85	60.120.46.80	NULL	cpe:2.3:a:alsa-project:alsa:1.1.8:*:*:*:*:*:*:*	NULL	7	NULL	NULL	NULL	NULL

Fig. 8. CTI database storing information obtained through risk assessment formulas and response strategies derived from TTP

하였다. 그 결과, 총 784개 중 782개의 TTP 매핑이 성공하여 99.74%의 높은 성공률을 기록하였다.

4.3 위험도 산출 및 대응전략 도출 성공 여부

위험도 산출을 위한 예시를 들어 설명한다. 내부자산 컴포넌트를 거쳐 얻은 cpe가 다음과 같다. 'cpe:2.3:a:gnu:ncurses:5.9:*:*:*:*:*:*:*:*'로 cti 테이블에서 해당 내부자산 CPE 검색한 결과로 일치하는 cve_id는 'CVE-2010-3847'이며 CVSS v3는 존재하지 않고, CVSS v2가 '6.9'이다. 따라서 수집한 CTI 위험도는 6.9가 된다. 네트워크 자산 기본 위험도를 계산했을 때(CPE로 NVD에서 검색해 찾은 모든 CVE들의 CVSS 평균 값)는 '6.88'이 나오고 네트워크 자산 중요도는 내부자산 CPE가 갖는 고유의 중요도이므로 계산을 위해 랜덤 값으로 임시로 '7'로 지정한다. 이 결과로 최종 위험도를 산출하면 '7.222'가 도출된다.

또한, 내부자산 CPE의 level별 분류를 통해 내부자산 CPE와 cti 데이터의 매핑율로 실험을 진행한다. 내부자산 CPE의 level 분류 기준은 3개로 level3는 '제품 버전 번호까지의 CPE', level2는 '제품명까지의 CPE', level1은 '제품 제조사명까지의 CPE'로 구분한다. CPE 한 개로 예를 들어 설명하자면, 'cpe:2.3:a:gnu:tar:1.26:*:*:*:*:*:*:*:*'는 levle3로 'cpe:2.3:a:gnu:tar:1.26:'가 되고, level2로 'cpe:2.3:a:gnu:tar:', level1으로 'cpe:2.3:a:gnu:'가 된다. 이에 따라 전체 내부자산 CPE 소스가 있는 45개를 위험도 산출 했을 경우로, level3, level2, level1 각각 순서대로 0개, 4개, 13개 도출이 성공했다.

대응전략 도출은 위의 CPE를 cti에 검색했을 때 나오는 TTP를 이용해 가장 많은 ttp에 대한 내용이 담여있는 att_to_miti_RE.json파일을 이용해 mitigation을 구한다. 최종적으로 내부자산에 있는 45개의 cpe는 TTP와 대응전략까지 level1의 수준으로 7개가 매핑된 것을 확인했다.

V. 결 론

본 논문에서는 SOAR 기술을 접목하여 보안 위협을 탐지하고 관리하는 자동화 시스템을 제안하였다. 외부 STIX/TAXII 기반 데이터를 분석하여 CTI를 구축하고, 정보를 통합하여 한눈에 볼 수 있도록 하였다. 주요 정보인 CVE, CPE, CVSS, TTP와 내부 자산 정보를 활용해 위험도와 대응 전략을 도출할 수 있도록 설계하였으며, 룰 기반 매핑 알고리즘을 통해 CTI-TTP 매핑 결과로 99.74%의 성공률을 보였다. 이 시스템은 약 1시간 내에 외부 STIX/TAXII 데이터에서 약 2300개의 report를 자동으로 분석할 수 있어 시간적 효율성을 크게 향상시킨다. 또한, 데이터를 기반으로 위험도를 판단하고 대응 전략을 한눈에 파악할 수 있어 내부 자산 관리에 용이함을 제공한다.

향후 과제로는 높은 정확도를 보여준 룰 기반 알고리즘 탐지를 넘어, 성능적인 측면에서 매핑 성공 개수를 늘려 보다 다양한 정보를 포용할 수 있도록 하는 것이 중요하다. 이를 통해 시스템의 포괄성을 높이고, 더 많은 사이버 위협 정보를 효과적으로 수집 및 분석할 수 있는 기반을 마련할 수 있을 것으로 기대된다. 이러한 발전은 궁극적으로 사이버 보안의 효율성을 더욱 강화하는 데 기여할 것이다.

References

[1] GTTKorea, "Trends in the SOAR Market," GTTKorea, [Online]. Available: https://www.gttkorea.com/news/articleView.html?idxno=10990. Accessed: Oct. 2024.

[2] J. Choi, Y. Kim, and B. Min, "A Study on ICS Security Information Collection Method Using CTI Model," Journal of the Korean Institute of Information Security and Cryptology (JKIISC), vol. 28, no. 2, pp. 471-484, Apr. 2018. doi: 10.13089/JKIISC.2018.28.2.471.

[3] S. Choi, T. Kim, K. Son, S. Lee, and T. Kim, "A Study on the Automatic Generation System of Playbooks for the Advancement of SOAR," Korea Internet & Security Agency, Jun. 2023.

[4] P. Kühn, K. Wittorf, and C. Reuter, "Navigating the shadows: Manual and semi-automated evaluation of the dark web for cyber threat intelligence," IEEE Access, vol. 12, pp. 118903-118922, Aug. 2024. doi: 10.1109/ACCESS.2024.3448247.

[5] STIX, "Introduction to STIX," [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro. Accessed: Oct. 2024.

[6] TAXII, "Introduction to TAXII," [Online]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro.html. Accessed: Oct. 2024.

[7] J. Lim and J. Lee, "3-Step Security Vulnerability Risk Scoring Considering CVE Trends," Journal of the Korean Institute of Communications and Information Sciences, vol. 27, no. 1, pp. 87-96, 2023.

[8] J. Jeong and J. Park, "A Study on the Improvement and Utilization of Public N-Day Vulnerability Databases," Journal of the Korean Institute of Information Security and Cryptology (JKIISC), vol. 34, no. 4, pp. 667-680, Aug. 2024.

[9] Heejung Kim and Hwankuk Kim, "Comparative Experiment on TTP Classification with Class Imbalance Using Oversampling from CTI Dataset," Security and Communication Networks, 2022, Article ID 5021125, Open Access, 12 October 2022. https://doi.org/10.1155/2022/5021125.

[10] A. Lawall and P. Beenken, "A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem," in Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24), pp. 210 - 216, Apr. 2024. Association for Computing Machinery, New York, NY, USA. doi: 10.1145/3655693.3661321.

〈저자소개〉

유 현 수 (Hyeon-su Yoo) 학생회원
2021년 3월~현재: 상명대학교 정보보안공학과 재학
〈관심분야〉 취약점 분석, AI 보안, 네트워크 보안 등

김 환 국(Hwan-kuk Kim) 종신회원
2017년 3월: 고려대학교 정보보호학과 박사
2005년 12월: 한국전자통신연구원 정보보호연구본부 연구원
2020년 2월: 한국인터넷진흥원 지능형사이버방어R&D 팀장
2024년 2월: 상명대학교 정보보안공학과 교수
2024년 3월~현재: 국민대학교 정보보안암호수학과 교수
〈관심분야〉 5G/6G 네트워크보안, AI 응용보안, SW 보안취약점분석 등