사이버 공격에 효율적 대응을 위한 침해지표 표현 기반 정보 공유 메커니즘 설계 및 구현

이형우*
한신대학교 AISW대학 교수

Design and Implementation of an Indicators of Compromise Information Sharing Mechanism for Effective Cyber Attack Response

Hyung-Woo Lee*
Professor, School of Computing and Artificial Intelligence, Hanshin University

요 약 최근 사이버 공격이 급증하고 있어 이에 대한 효율적 대응이 필요하다. 이에 본 연구에서는 사이버 공격 발생시 이를 표현하는 방법으로 침해지표(Indicators of Compromise)가 사용되고 있다. 침해지표는 사이버 공격이 발생하였을 경우 또는 현재 진행중에 있을 경우 이를 표시하는 디지털 포렌식 증거자료로 사이버 공격 방색시 해당 위협 정보를 표현하는 방법을 제시하였으며, 제시된 침해지표 표현 구조를 사용하여 사이버 대응 시스템 간에 효율적인 위협 정보 공유 메커니즘을 설계 및 구현하였다. 제시한 메커니즘을 이용할 경우 기존 사이버 공격 대응 시스템에 비해 능동적 대응 체계를 구축할 수 있으며 사이버 공격 발생시 효율적인 위협분석 및 대응 체계를 구축할 수 있다.

주제어 : 사이버 공격, 침해지표, 위협 정보 공유, 침해지표 구조, 공유 모델

Abstract With the increasing frequency of cyber attacks, the need for an effective and systematic response has become more critical than ever. In this study, Indicators of Compromise (IoC) are utilized as a standardized method for representing cyber attack incidents. IoC serve as essential digital forensic evidence, providing a means to identify ongoing or past cyber attacks. This research proposes a structured IoC representation model that enables consistent expression of threat information and facilitates efficient intelligence sharing among cyber defense systems. Furthermore, an IoC-based threat information-sharing mechanism is designed and implemented to enhance coordination between security systems. The proposed mechanism enables a more proactive cyber defense strategy compared to conventional methods, improving the overall efficiency of threat detection, analysis, and response. Through this approach, organizations can strengthen their cybersecurity posture and establish a more resilient and adaptive defense framework against evolving cyber threats.

Key Words : Cyber Attack, Indicators of Compromise, Threat Sharing, IoC Structure, Sharing Model

이 논문은 한신대학교 학술연구비 지원에 의해 연구되었음.
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2025년 01월 22일 수정일 2025년 02월 11일 심사완료일 2025년 02월 17일

1. 서론

침해지표(Indicators of Compromise: IoC)는 사이버 공격이 발생하였을 경우 또는 현재 진행중에 있을 경우 이를 표시하는 디지털 포렌식 증거이다[1]. 이는 시스템 로그, 네트워크 트래픽, 파일 해시, 도메인 정보 등과 같은 다양한 형태 및 포맷으로 정의할 수 있으며, 사이버 대응 전문가들은 IoC를 분석하여 네트워크 또는 시스템에 대한 보안 공격에 신속하게 탐지 및 대응하는 과정에 사용하게 된다[2-5]. 정부 및 공공기관/기업에서는 IoC를 활용하여 실시간 보안 감시, 침해 사고 대응(IR, Incident Response), 보안 위협 인텔리전스(Threat Intelligence), e디지털 포렌식 조사 분석 과정 등을 수행하며 특히, 보안 시스템 간에 IoC 정보를 공유할 수 있는 메커니즘과 결합할 경우, 사이버 공격 관련 위협 정보(Threat Information)를 실시간으로 교환하여 조직 간 보안 수준을 향상시킬 수 있다. IoC를 이용하여 네트워크 트래픽, 로그 및 파일 등에 대한 이상 징후를 감지할 수 있으며, 침해사고 발생 가능성을 사전에 파악할 수 있고, 사고 발생 후 원인을 추적하고 대응 방안을 마련하는 과정에 활용하거나 조직 간 IoC 정보를 공유하여 대단위 사이버 공격에 공동 대응할 수 있는 장점을 제공한다[6-8]. 따라서 본 논문에서는 사이버 공격에 효율적으로 대응하기 위해 침해지표(IoC) 정보를 재정의하고 이를 공유할 수 있는 메커니즘을 설계 및 구현하였다.

2. 침해지표(IoC) 기반 사이버 공격 대응

2.1 사이버 공격 및 침해지표 표현

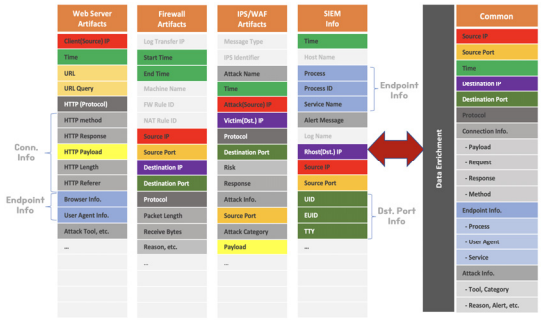
사이버 공격(Cyber Attack)은 해커 또는 공격자가 임의의 네트워크, 시스템 및 데이터에 불법적으로 접근하거나 손상 또는 정보를 유출하려는 시도이며 개인, 기업 또는 공공기관을 대상으로 금전적 이득, 기밀 정보 탈취, 서비스 중단 또는 사회적 혼란 유발 등을 목적으로 한다. 최근 머신러닝, AI 등을 활용한 자동화된 공격 방식이 급증하고 있으며 초기 침투 후 다양한 방법으로 다단계 방식으로 내부 확산 공격을 수행하고 있고, 공격자에 대한 추적을 회피하기 위해 다양한 형태의 우회 공격 기술 및 익명성에 기반한 공격 방식이 사용되고 있으며, 특히 장기간 시스템에 은닉한 상태로 대상 시스템에 대한 정보를 탈취하거나 조작하는 등의 피해가 발생하고 있다.

아래 그림과 같이 주요 사이버 공격 방식을 살펴보면 바이러스/웜/랜섬웨어 등과 같은 악성코드에 의한 공격, 피싱/스미싱 등과 같은 소셜 엔지니어링 대상 공격 방식 등이 사용되고 있으며 DDoS 공격, Zero-Day 취약점 기반 공격 및 내부자 공격 등 다양한 형태의 APT 공격이 지속적으로 증가하고 있다.

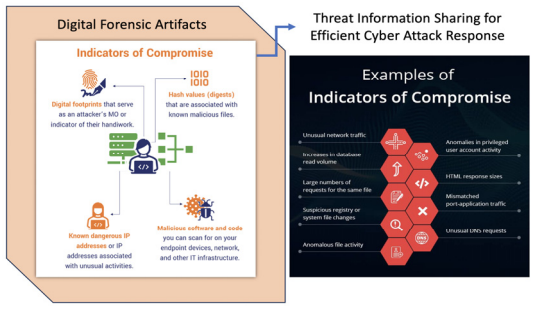
[Fig. 1] Types of Cyber Attacks

따라서, 이와 같은 사이버 공격에 능동적으로 대응하기 위해서는 (1) 최신 OS 및 소프트웨어 업데이트 등과 같은 보안 패치를 적용하고, (2) 계정 탈취를 예방하기 위해 다단계 인증(Multi-Factor Authentication)을 적용하거나, (3) 이상 트래픽을 탐지하는 등의 네트워크 모니터링 등을 수행하여야 하며, 궁극적으로는 (4) 악성 공격자 IP 주소, 공격 파일에 대한 해시 정보 분석 및 행위 기반 공격자 분석 등의 침해지표(IoC) 기반 탐지/대응 과정이 필요하다.

이상 트래픽 분석을 위해서는 웹 서버, 방화벽 및 IPS/WAF 장비와 SIEM 장비로부터 생성되는 각종 로그 정보를 대상으로 네트워크 모니터링 과정을 수행하여 아래 그림과 같이 사이버 공격 정보에 대한 데이터 강화(Data Enrichment) 과정을 수행할 필요가 있다. 이는 보안 시스템이 수집한 원시 데이터(Raw Data)에 추가적인 정보(Context)를 결합하여 분석의 정확도를 향상시키는 과정으로 각종 디바이스에서 생성되는 보안 이벤트를 더 깊이 이해하고, 사이버 공격을 효과적으로 탐지 및 대응하는 과정에 활용될 수 있다. 하지만 단순 사이버 공격 데이터 강화 과정 만으로는 점차 고도화/지능화 되고 있는 사이버 공격에 능동적으로 대응할 수 없으므로, 보안 공격에 대한 탐지 정확도를 향상시키고 실시간 대응 속도를 개선하기 위해서는 침해지표(IoC) 정보 표현 및 공유를 통해 조직내 전반적인 사이버 공격 대응 수준을 향상시킬 필요가 있다.



[Fig. 2] Cyber Attack Data Enrichments



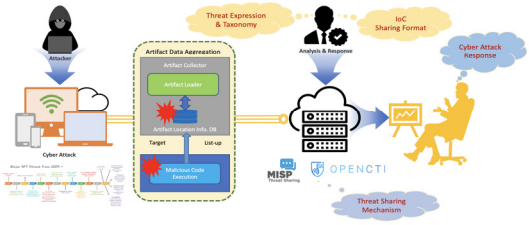
[Fig. 3] Indicators of Compromise

2.2 침해지표(IoC) 정의 및 표현 방식

침해지표(IoC)는 사이버 공격 또는 보안 침해 사건이 발생했음을 나타내는 디지털 증거 자료에 해당하는 것으로 보안 운영 센터(SOC), 침해사고 대응팀(CERT), 포렌식 전문가 등에 의해 분석을 통해 사이버 공격에 대한 사전 예방, 실시간 탐지 및 사후 대응의 핵심 정보로 활용된다[9-11].

IoC는 네트워크 기반 IoC, 파일 및 시스템 기반 IoC 및 행위 기반 IoC으로 구분되며, 이와 같은 IoC를 활용하여 각종 보안 솔루션과 위협 인텔리전스 시스템에서는 사이버 공격에 대한 탐지 및 분석 과정에 활용된다. (1) 네트워크 기반 IoC는 네트워크 트래픽에서 감지되는 침해지표로, 공격자의 명령 및 제어(C&C) 활동, 악성 도메인, 비정상적인 데이터 흐름등을 탐지하는 데 사용된다. 악성 IP 주소, 도메인 및 URL 정보와 비정상적인 트래픽 흐름과 의심스러운 사용자 에이전트 등에 의한 연결 등을 IoC 내에 표현하여 방화벽/IDS/IPS 시스템과 SIEM 시스템 등에서 보안 공격에 대응하는 과정에 활용된다. 다음으로 (2) 파일 및 시스템 기반 IoC는 컴퓨터 시스템 내에서 탐지되는 침해지표 정보로 파일 해시 정보, 악성 실행 파일과 스크립트 정보, 레지스트리 변경 사항, 비정상적인 프로세스 및 서비스 구동 현황 등에 대한 정보를 통해 악성코드 등에 대한 감염 여부 등을 분석하는 과정에 활용된다. 마지막으로 (3) 행위 기반 IoC는 공격자의 전술(Tactics)과 공격 기술(Technique)에 따라 해당 피해 시스템 내에서 발생하는 비정상적인 행위를 분석하는 것으로 비정상적인 로그인 활동, 권한 상승 및 데이터 유출, 스크립트 기반 공격과 랜섬웨어 공격 등을 통한 사이버 공격 여부를 표현하는 방식이다.

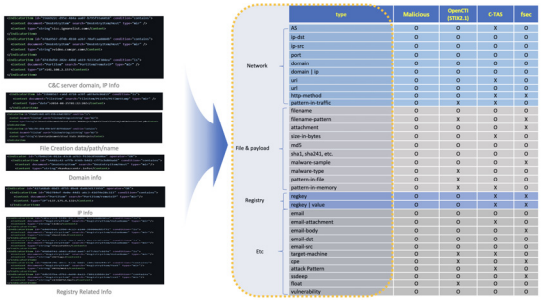
이와 같이 침해지표는 사이버 공격 발생시 실시간 탐지, 사고 대응 및 위협 인텔리전스 공유 등의 목적으로 활용될 수 있으며 엔드포인트 탐지 및 대응(EDR)과 SIEM(Security Information and Event Management) 그리고 위협 인텔리전트(Threat Ingelligence) 시스템에서 활발히 사용되기 위해서는 침해사고 정보에 대한 표현과 분류체계 정의(Threat Expression and Taxonomy), IoC 정보에 대한 공유 메커니즘(Threat Sharing Mechanism) 등에 대한 연구가 필요하다[11-14].



[Fig. 4] IoC data Representation and Sharing

2.3 기존 침해지표 표현 방식

침해지표(IoC)는 사이버 공격이 발생했을 경우 이를 표현하는 데이터 및 증거자료를 포함하고 있으며 (1) 비구조화된 텍스트 기반 IoC, (2) 구조화된 데이터 IoC 및 (3) 위협 인텔리전스 공유 포맷 형태의 IoC 등으로 구분된다. 비구조화된 텍스트 기반 IoC인 경우 보안 리포트, 이메일, PDF 파일 등의 문서로 표현되는 방식으로 표준화되어 있지 않아서 자동화 처리 과정에 어려움이 존재한다는 문제점이 있다. 이를 개선하기 위해 CSV, JSON 및 XML 등과 같은 구조화된 파일 포맷 형태로 침해사고 발생 정보를 표현하는 방법이 있다. 이 경우 데이터 처리와 자동화 과정이 상대적으로 용이하며 보안 시스템간 연동이 가능하다는 장점이 있다. 현재 SIEM 등과 같은 보안 솔루션에서 사이버 공격에 대한 자동 분석 및 연계 과정에 사용되며 시스템간 IoC 정보를 공유하는 과정에서도 CSV, JSON 및 XML 형태로 표현된 IoC 정보가 사용되고 있다[15,16].



[Fig. 5] IoC Data Representation Case Study

이와 같은 구조화된 IoC 표현 방식을 더욱 더 향상시킨 방식이 STIX(Structured Threat Information eXpression)[18]이다. 이는 사이버 위협 정보를 표현하기 위해 표준화된 형태의 구조화 언어로 IoC 뿐만 아니라 공격 기법, 공격자 정보(TTP) 및 피해 대상 정보 등을 포함할 수 있다. CTI(Cyber Threat Intelligence) 공유 및 자동화 처리 과정에 최적화된 형태로 활용 가능하며 STIX/TAXII[19] 프로토톨을 이용하여 위협 인텔리전스 플랫폼간 연계 및 사이버 공격 정보 공유가 가능하다는 장점이 있으나 구조 자체가 너무나 복잡하여 자동화된 IoC 데이터 생성 과정 및 변환 과정이 상당히 어렵다는 단점이 있다[17].

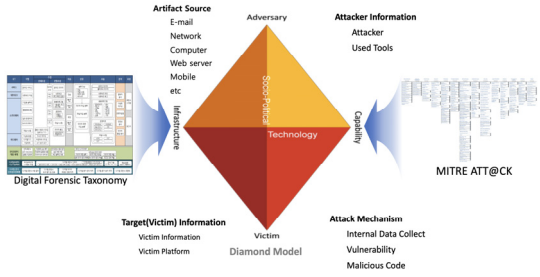
이밖에도 MISP(Malware Information Sharing Platform)[20]에서 제공하는 포맷이 있다. 이는 JSON 기반 IoC 데이터 저장 및 공유가 가능한 형태로 MISP 플랫폼 간에 실시간 위협 인텔리전스 정보 공유와 공동 대응이 가능하다는 장점이 있다. 특히 국가 기관, 공공기관, 금융권 및 기업간 IoC 실시간 공유 기능을 제공하며 MISP 플랫폼을 기반으로한 보안 커뮤니티 운영 등이 가능하다는 장점이 있다. 그리고 국내 KISA에서 제시한 C-TAS 포맷 및 금융보안원(fsec)에서 개발한 IoC 포맷도 제시되었으나 각각 상이한 형태로 개발되어 있어 이에 대한 개선 과정이 필요하다.

3. 제안하는 침해지표 표현 구조 및 정보 공유 방법

3.1 변형 다이아몬드 모델 기반 침해지표 표현

앞서 제시한 바와 같이 침해지표 표현 방식은 비구조화 텍스트, CSV/JSON 등 구조화 방식, STIX 및 MISP IoC 구조 등으로 변형/발전해 왔다. 각각의 방식은 장단점을 가지고 있다. CSV/JSON 방식은 보안 시스템 간 연동 및 자동과 과정에 적용 가능하며, STIX 방식인 경우 각종 공격 기법에 대한 표현과 같이 정교한 형태로 사이버 위협에 대한 표현 및 정보 표시가 가능한 형태이며 MISP인 경우 실시간 위협 공유 및 협업 과정에 최적화된 방식이다.

하지만, 최신 위협 인텔리전스 환경에서 사이버 공격 정보를 효율적으로 표현하고 이를 공유하기 위해서는 더욱더 새로운 형태의 IoC 표현 구조 및 메커니즘이 필요하다. 이에 본 연구에서는 아래 그림과 같은 IoC 표현 구조를 제시하였다. 제안한 방식은 다이아몬드 모델(Diamond model)에 기초하고 있으며, 공격자의 행동을 (1) 공격자(Adversary), (2) 공격 기법(Capability), (3) 공격 인프라(Infrastructure) 그리고 (4) 피해 대상(Victim)과 같은 네 가지 핵심 요소로 분류하여 침해사고를 체계적으로 분석할 수 있다. 이를 통해 보안 분석가는 공격자의 다양한 전술을 명확히 파악하고 효과적인 대응 전략을 수립할 수 있다.

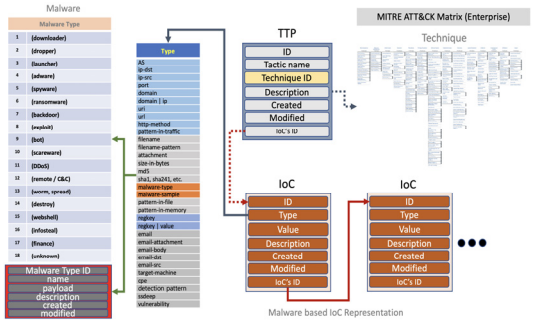


[Fig. 6] Diamond Model based IoC Representation

3.2 다이아몬드 침해지표 표현 구조 기반 공유

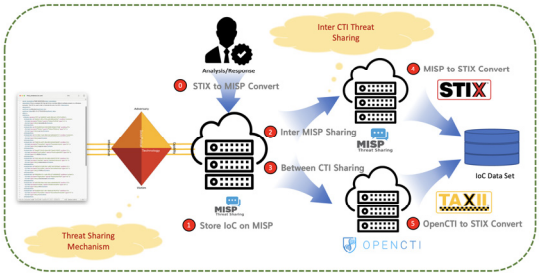
다이아몬드 모델에서 표현 가능한 4가지 요소(공격자, 공격 기법, 공격 인프라 및 피해 대상)는 서로 연결되어 있으며 공격자에 대한 전체적인 전략을 이해하는데 도움을 준다. 따라서 아래 구조와 같이 MITRE ATT@CK Matrix로 표현 가능한 TTP(Tatics, Technique, Procedure) 정보를 포함하며 악성코드 형태 정보 18개 그리고 상세 공격 인프라와 피해자에 대한 정보를 포함하는 구조이다.

이와 같이 생성된 침해지표에 대해서는 이기종 보안 위협 인텔리전스 시스템 간에 공유할 수 있어야 한다. 각 시스템 마다 다양한 형태의 IoC 포맷과 표현 방식이 존재하므로 침해지표 간 변환(Transformation) 과정이 필요하며 이를 통해서 다양한 보안 시스템과 연계 및 공유가 가능하게 된다.



[Fig. 7] IoC Data Format and Structure

침해지표 변환 과정을 수행하기 위해서는 (1) 데이터 수집, (2) 정규화, (3) 변환 및 (4) 공유의 4단계 과정을 수행할 수 있다. 각종 IoC 내에 포함된 IP 주소/도메인/URL/파일 해시 및 악성코드 패턴 등에 대해 일관된 구조로 표현하는 정규화(Normalization) 과정이 필요하다. 중복을 제거하거나 데이터를 정제하는 과정을 수행하여 통일된 포맷으로 침해사고 관련 각종 상세 정보를 표현하게 되며 이에 대한 교환/공유를 위해서 IoC 포맷 변환 과정을 수행하여야 한다. 변환 과정은 Syslog 데이터를 JSON 형태로 변환하거나, JSON/CSV 파일 포맷 형태의 IoC를 STIX 포맷으로 변환하거나, MISP 형태의 IoC를 TAXII로 변환하는 과정 등을 수행하게 된다.



[Fig. 8] IoC Data Transformation

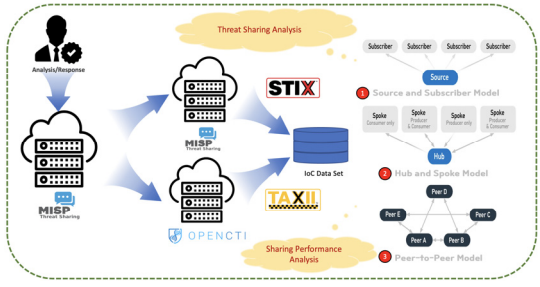
3.3 침해지표 정보 공유 방식

위협 인텔리전스 시스템 간에 생성한 IoC 정보를 공유하는 방법이 필요하다. 이를 구현하기 위해서 (1) 중앙집중형 방식의 Source & Subscriber 모델 방식을 이용하거나, (2) 분산 방식의 Peer-to-Peer 모델 또는 (3) 하이브리드 방식의 Hub & Spoke 모델 방식을 사용할 수 있다.

중앙 집중형 모델 방식은 단일 중앙 기관(국가 기관 또는 보안 기업)이 IoC를 수집하는 방식으로 개별 조직 등등 중앙 서버와 연결하여 정보를 공유하게 된다. 이는 일관성 있게 IoC 표현이 가능하며 신뢰성이 높고 데이터 검증이 용이한 반면 중앙 기관이 공격을 받을 경우 전체 네트워크에 IoC 공유/전파가 차단되는 문제점이 발생하게 된다[9,10].

분산형 모델인 경우 중앙 기관이 없어서 빠르게 정보 공유가 가능하며 단일 장애 발생시 효율적으로 대응할 수 있으나, 궁극적으로는 신뢰성이 낮은 IoC 데이터가 유입될 가능성이 높으며 데이터에 대한 표준화 및 검증 과정이 용이하지 않다는 문제점이 발생한다. 현행 분산 MISP 시스템 기반 IoC 정보 공유 방식이 이에 해당하는 것으로 각 조직이 개별적으로 IoC를 수집 및 공유하게 되어 자율성 및 확장성이 용이하나 국가기관, 공공기관 등을 대상으로 하는 경우에는 적용하기 어렵다는 특성을 확인할 수 있다.

마지막으로 하이브리드 모델 방식인 경우 중앙 집중형과 분산형을 조합한 방식으로 신뢰할 수 있는 중앙 기관이 존재하지만 개별 조직 들도 직접 IoC를 공유할 수 있는 기능을 제공한다. 신뢰성 높은 IoC 데이터를 유지하면서도 빠른 공유 기능을 제공하며 개별 조직이 필요에 따라서 직접 IoC를 검증하며 활용 가능하다는 장점이 있다. 하지만 이 방식인 경우 운영 및 관리가 복잡하다는 문제점이 존재하기도 한다.



[Fig. 9] IoC Data Sharing

[Table 1] IoC Data Sharing Model Comparison

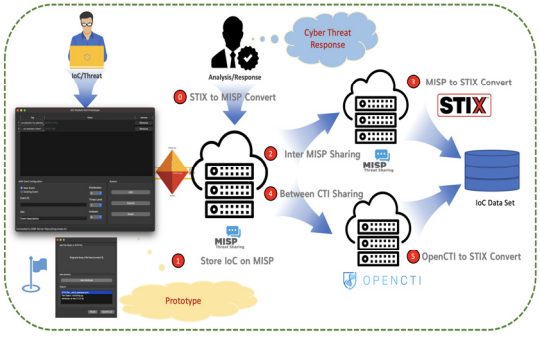
구분 \ 공유	Peer to Peer	Source & Subscriber	Hub & Spoke
정의	직접적인 연결로 데이터 Sharing	중앙 집중 시스템과의 데이터 Sharing	중앙 집중 시스템을 통해 데이터 Sharing
장점	중앙집중화된 인프라 필요 없음 수평적 사고관리/대응체계	높은 확장성과 유연성 효율적인 데이터 Collect & 분배	침해사고 통합 관리 용이 관리 체계 & 침해사고 대응 향상
단점	복잡한 연결 구조로 관리 어려움 확장성 제한 대규모 네트워크에 부적합	중앙 시스템에 대한 의존도 높음 중앙 시스템 장애 시 데이터 전달 문제 발생 수직적 사고관리/대응체계	중앙 시스템 장애 발생 시 일부 영향 중앙 시스템에 대한 의존도 높음 데이터 전송 지연 가능성 존재
복잡도	상	하	중
신뢰성	중	중	상
확장성	하	상	상
최신성	하	중	상
유연성	중	상	상
전파속도	하	상	상
중복처리	중	상	중
관리기능	하	중	상
탐지성능	하	중	상
침해대응(종합)	하	중	상

제시한 세 가지 공유 방식에 대해 각각 장단점을 비교 분석한 결과는 아래 표와 같이 최종적으로는 Hub & Spoke 모델 형태의 하이브리드 모델 방식이 우수한 성능을 제공하는 것으로 나타났다.

4. 침해지표 정보 표현 기반 공유 시스템 설계 및 구현

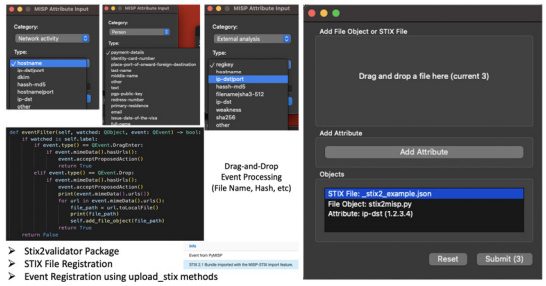
4.1 침해지표 정보 표현 시스템 설계 및 구현

본 연구에서 제안한 IoC 포맷 구조로 표현할 수 있도록 파이썬 언어를 이용하여 IoC 정보 표현 시스템을 설계 및 구현하였다. 구현한 시스템은 Python 3.10과 PySide6 모듈을 이용하여 GUI 프로그램을 제작하였으며 수집한 침해지표를 MISP 등의 위협정보 공유 플랫폼에 등록하는 기능을 제공한다.



[Fig. 10] IoC Data Representation SW 1/2

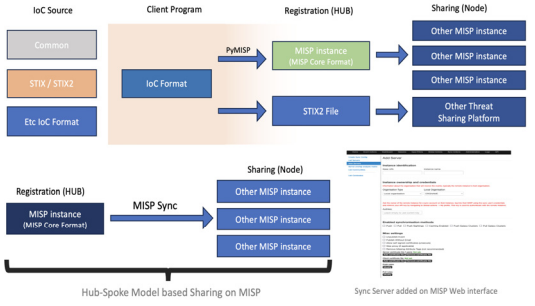
MISP 에서는 각각의 침해 사건에 대해 Event라는 단위로 묶이며, 각각의 이벤트 마다 IP 주소, 파일 해시 등과 같은 침해지표를 등록하도록 정의되어 있다. 따라서 MISP를 Hub로 하는 하이브리드 공유 모델을 채택하여 각종 IoC 이벤트 정보를 등록 및 공유할 수 있는 기능을 구현하였다. ‘IoC 추가’ 기능을 통해 이름(선택), 침해지표의 종류, 침해 정보 값, 설명 정보를 입력할 수 있도록 구현하였으며 해당 정보를 모두 입력하면 사용자가 입력한 침해지표가 JSON 형태로 변환/표현된다. 또한 ‘Submit to MISP’ 버튼을 누르면 프로그램 실행 시 pymisp 모듈과 API를 통해 해당 MISP 플랫폼에 연결한 후 MISP 인스턴스에 새 이벤트를 생성함과 동시에 사용자가 추가한 침해지표 정보가 자동 등록되도록 구현하였다. 등록시 선택 가능한 침해지표 type 정보는 IP 주소, domain 주소, URL, 해시, 이메일 주소 및 파일 정보를 선택할 수 있도록 구현하였다.



[Fig. 11] IoC Data Representation SW 2/2

4.2 시스템 설계 및 구현 상세

악성코드에 최적화된 IoC 형태로 편리하게 등록하기 위해서는 GUI 인터페이스에 대한 개선 과정을 수행하였다. 일반적으로 자주 사용하는 침해지표를 쉽게 표현하기 위하여 드래그 앤 드롭 (Drag-and-drop) 방식을 이용한 GUI 인터페이스를 제공하였으며, PySide6 라이브러리에서 사용 가능한 QEvent 객체의 minedata() 메서드를 통해 드래그 앤 드롭 기능을 효율적으로 제공할 수 있었다.

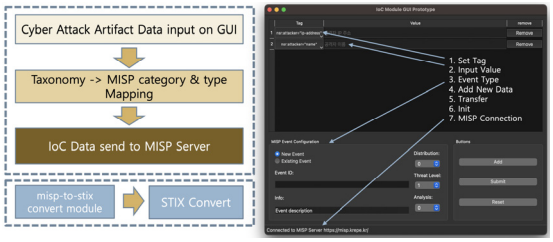


[Fig. 12] Internal Structure of IoC Rep. SW

STIX 포맷은 악성코드뿐만이 아닌 다양한 형태의 침해지표에 범용적으로 사용할 수 있을 정도로 방대한 구조를 가지고 있다. 따라서 본 연구에서 제시하는 IoC 데이터 포맷 또는 MISP에서 수집된 IoC 데이터를 STIX 포맷으로 변환하는 과정에서 손실을 최소화 할 수 있는 방법을 사용하였다.

PyMISP에서 제공하고 있는 upload_stix() 메서드를 이용해 MISP IoC 데이터를 STIX 파일 형태로 업로드하는 기능을 구현하였으며, 해당 파일이 STIX2 포맷에 해당하는지를 검증하기 위하여 stix2validator 모듈을 사

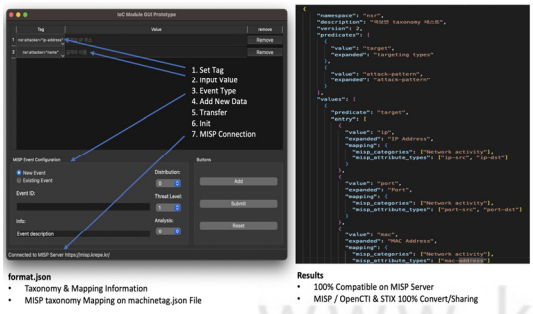
용하였다. 그리고 Python에서 제공하고 있는 dataclasses.dataclass를 이용해 IoCObject라는 클래스를 생성하였고, 악성코드 표현에 필수적인 분류 정보를 선택할 수 있도록 기능을 개선하였다.



[Fig. 13] Implementation Results 1/2

Submit 버튼을 누르면 MISPEvent 객체를 생성해 새 이벤트를 만들고, 이 이벤트를 MISP 인스턴스에 게시한 다음 그림과 같이 해당 메서드가 IoCObject 객체들을 MISPAttribute 객체로 변환하게 되며, MISPEvent 객체에 추가하면 그림에 제시된 내용처럼 Attribute 형태로 해당 침해지표가 자동 등록된 것을 확인할 수 있다.

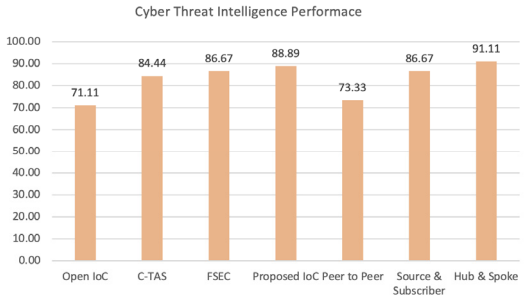
본 연구에서 구현한 시스템인 경우 기본적으로 MISP 위협정보 공유 플랫폼에 침해지표를 자동 등록할 수 있는 기능을 제공하고 있다. 하지만 이러한 형태의 IoC 표현 규격은 그 범위가 매우 방대하여 특정 조직의 환경에 적합한 자체 포맷 구조 형태의 IoC 정보를 등록하기에는 다소 번거로움이 존재한다. 따라서 자체 개발한 침해지표 규격을 활용하여 IoC 정보를 표현하고, 이를 본 연구에서 개발한 클라이언트 프로그램을 이용하여 MISP 공통 포맷 또는 STIX2 포맷 형태로 자동 변환할 수 있게 구현하여 침해지표 정보에 대한 공유 과정의 편의성을 제공하며 기존 프로그램들과의 호환성을 모두 제공할 수 있도록 하였다.



[Fig. 14] Implementation Results 2/2

4.3 성능 비교 평가

사이버 공격에 대한 정보 공유 및 대응 과정에서의 효율성을 중심으로 성능을 비교 평가하였다. 기존의 세 가지 IoC 포맷 구조와 본 연구에서 제시한 IoC 포맷 구조 기반 침해지표 표현 과정에 대해 비교하였으며 IoC 공유 모델 세 가지 방식 별 위협정보 대응 능력을 상대적으로 비교한 결과 제안한 IoC 표현 구조가 기존 방식 보다 개선된 성능을 제공하는 것을 확인할 수 있었다.



[Fig. 15] Proformance Analysis

5. 결론

본 연구에서는 기존 침해지표 표현 방식에 대한 고찰을 통해 사이버 공격 발생시 악성코드를 중심으로 침해지표 표현 구조를 제시하고 이를 토대로 효율적인 IoC 규격화 방안을 제시하였다. 또한 사고관리 프레임워크에서의 내부 위협정보 공유 방법 및 동작 프로세스에 대해 분석하여 MISP와 OpenCTI 등의 시스템에서 침해지표 기반 위협정보를 공유하는 방법과 메커니즘에 대해 분석하였으며 위협정보 공유 메커니즘에서의 특징과 침해지표 공유 모델에 대해 분석하였다. 이를 통해 본 연구에서는 최적의 침해지표 공유 모델을 제시하고 효율적인 형태로 침해지표 정보를 공유할 수 있는 모델을 제시하였다. 이를 토대로 앞으로 MISP와 OpenCTI 등과 같은 위협 인텔리전스 시스템에 적용 가능한 위협정보 정보 포맷 구조화 과정 및 효율적인 공유 메커니즘에 대한 개선 방향을 도출할 수 있을 것으로 기대된다.

REFERENCES

[1] C. Miller and D. Ward, "Cyber Attack Response and the Role of Indicators of Compromise (IoC)," Journal

of Cyber Defense and Security, Vol.18, No.1, pp.101-115, 2020, doi: 10.1016/j.jcyber.2020.02.003.

[2] J. Zhao and A. Gupta, "A Comparative Analysis of IoC Formats for Cybersecurity," International Journal of Cyber Intelligence and Security, Vol.9, No.4, pp.313-327, 2019, doi: 10.1145/3331368.

[3] M. Pawlowski and H. Schmidt, "Automated Threat Intelligence Collection and Indicator Transformation," Cybersecurity Technologies Review, Vol.16, No.2, pp.75-92, 2021, doi: 10.1007/s12345-021-00456-y.

[4] J. Stewart and S. Black, "Efficient Automated Indicator Transformation for Cyber Attack Detection," Journal of Cybersecurity Automation, Vol.5, No.1, pp.48-61, 2022, doi: 10.1016/j.jcyber.2022.01.006.

[5] D. Graham and B. Norton, "The Importance of IoC Format Standardization in Cybersecurity," Journal of Cybersecurity Policy and Governance, Vol.22, No.3, pp.195-210, 2018, doi: 10.1007/s12220-018-0084-2.

[6] J. Fruhlinger, "Understanding Threat Intelligence Sharing in Modern Cybersecurity," International Journal of Information Security, Vol.14, No.4, pp. 152-168, 2021, doi: 10.1007/s10207-021-00692-5.

[7] M. Harris and T. Stevens, "Practical Approaches to Cybersecurity Information Sharing in Government Agencies," International Journal of Cyber Defense, Vol.18, No.2, pp.120-136, 2020, doi: 10.1145/3342198.

[8] M. Blaise, "Threat Intelligence Sharing: The Role of MISP in the Modern Cybersecurity Landscape," Journal of Information Security, Vol. 14, No.3, pp.245-261, 2019, doi: 10.1007/s11042-019-08070-w.

[9] D. Reed and P. Cook, "A Study of Cyber Threat Intelligence Sharing Models," International Journal of Cybersecurity, Vol.11, No.2, pp.85-102, 2018, doi: 10.1016/j.cybersec.2018.01.003.

[10] K. Scarfone and P. Mell, "Guide to Cyber Threat Information Sharing," National Institute of Standards and Technology (NIST), NIST Special Publication 800-150, 2017. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-150.

[11] D. Johnson and B. Perry, "Cyber Threat Intelligence Platforms: Leveraging Data to Defend Against Cyber Attacks," Computer Networks, Vol. 185, pp.107-119, 2021, doi: 10.1016/j.comnet.2020.107332.

[12] J. Aicardi and S. Perrot, "Integration of IoC in Real-Time Cyber Defense Systems," Journal of Network and Computer Applications, Vol.145, pp. 42-55, 2019, doi: 10.1016/j.jnca.2019.02.011.

[13] S. Taylor and A. Matthews, "The Role of Threat Intelligence Sharing in Detecting Advanced Persistent Threats," International Journal of Information Systems Security, Vol.23, No.1, pp.5-19, 2021, doi: 10.1109/JISSEC.2021.3077032.

[14] C. Williams and G. Phillips, "IoC Sharing and Collaboration: Reducing Cyber Risk in the Digital Supply Chain," Cyber Risk Management Journal, Vol.13, No.2, pp.220-237, 2019, doi: 10.1056/CRMJ.2019.05.029.

[15] D. Schmidt and M. Howard, "Real-Time Threat Intelligence and Automated IoC Sharing: An Industry Perspective," Journal of Cloud Computing and Security, Vol.24, No.3, pp. 102-118, 2020, doi: 10.1145/3337684.

[16] H. Lee and W. Johnson, "Advanced Techniques for IoC Transformation in Modern Cybersecurity," Cyber Threats and Countermeasures Journal, Vol. 15, No.1, pp.89-101, 2021, doi: 10.1016/j.ctc.2021.01.009.

[17] R. Howard and T. Ross, "Evolution of Threat Intelligence Platforms: Challenges and Opportunities in Sharing IoC," Journal of Cybersecurity and Privacy, Vol.12, No.2, pp. 198-211, 2020, doi: 10.1007/s10004-020-00506-8.

[18] R. Shilling and D. White, "STIX™: A Structured Threat Information Expression," 2015. [Online]. Available: https://www.oasis-open.org/.

[19] D. Rothman, "TAXII™: Trusted Automated Exchange of Indicator Information," 2017. [Online]. Available: https://www.oasis-open.org/.

[20] G. Caldarelli and G. De Prato, "MISP: Malware Information Sharing Platform & Threat Sharing," in Proceedings of the European Conference on Cybersecurity, 2020.

이 형 우(Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 컴퓨터학과 (학사)
- 1996년 2월 : 고려대학교 컴퓨터학과 (석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 (박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 AISW대학 교수

〈관심분야〉
사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식, 지능형 사이버공격 대응