사물인터넷융복합논문지 Vol. 9, No. 5, pp. 101-107, 2023 https://doi.org/10.20465/KIOTS.2023.9.5.101

IoT 시스템을 대상으로 한 침해사고 위협 정보 공유 방법

이형우*
한신대학교 컴퓨터공학부 교수

IoT System Cyber Threat Information Sharing Method

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

요 약 이기종 IoT 시스템을 대상으로 점차 지능화·고도화되는 사이버 공격에 능동적으로 대응하기 위해서 침해사고 발생 시 수집되는 위협정보를 효율적으로 공유할 수 있는 기법이 필요하다. 각종 IoT 기기 등으로부터 수집된 각종 디지털 포렌식 아티팩트를 IoC 정보로 생성한 후에 이를 MISP 등과 같은 CTI 시스템을 통해 공유할 수 있는 기법이 제시되어야 한다. 이에 본 연구에서는 IoT 기기를 대상으로 침해사고 발생 시 각종 아티팩트가 수집되면 상세 공격 정보를 침해지표(IoC)로 생성하고 MISP와 같은 CTI 시스템에서 Hub&Spoke 모델을 적용하여 위협정보를 공유하여 잠재적인 위협 행위에 효율적으로 대응할 수 있는 방법을 제안하였다. 제안한 위협정보 공유 모델을 적용할 경우 사이버 침해사고 분석 과정 시 대응 시간 및 검출 성능을 향상시킬 수 있어 최근 급증하고 있는 IoT 기기를 대상으로 한 지능형 사이버 공격에 대한 탐지/대응 능력을 더욱더 향상시킬 수 있을 것으로 기대된다.

주제어 : 사물인터넷, 사이버 위협 인텔리전스, 침해사고 대응, 침해지표, 공유 모델

Abstract In order to proactively respond to increasingly intelligent and sophisticated cyber-attacks targeting heterogeneous IoT systems, there is a need for techniques that efficiently share threat information collected when intrusion incidents occur. Techniques should be presented for generating various IoC(Indicators of Compromise) information from various digital forensic artifacts collected from various IoT devices, and for sharing this information through CTI(Cyber Threat Intelligence) systems such as MISP. In this study, when various artifacts are collected upon intrusion incidents in IoT devices, we propose a method for generating detailed attack information as IoCs and sharing threat information efficiently by applying the Hub & Spoke model in CTI systems like MISP. The application of the proposed threat information sharing model is expected to enhance response time and detection performance in the cyber incident analysis process, thus improving the ability to detect and respond to intelligent cyber-attacks targeting IoT devices.

Key Words : IoT, Cyber Threat Intelligence, Cyber Incident Response, Indicators of Compromise, Sharing Model

이 논문은 한신대학교 학술연구비 지원에 의하여 연구되었음
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2023년 8월 26일 수정일 2023년 9월 30일 심사완료일 2023년 10월 3일

1. 서론

지능화·고도화되는 사이버 공격에 능동적으로 대응하기 위해서는 IoT 이기종 시스템을 대상으로 한 공격에 대한 상세 위협정보를 공유할 수 있는 기법이 필요하다[1-3]. 최근 급증하고 있는 IoT 기기 등으로부터 수집된 각종 디지털 포렌식 아티팩트를 침해지표(Indicators of Compromise : IoC)로 생성한 후에 이를 사이버 위협 인텔리전스(Cyber Threat Intelligence : CTI) 시스템을 통해 공유할 수 있는 기법이 구축되어야 한다[4-6].

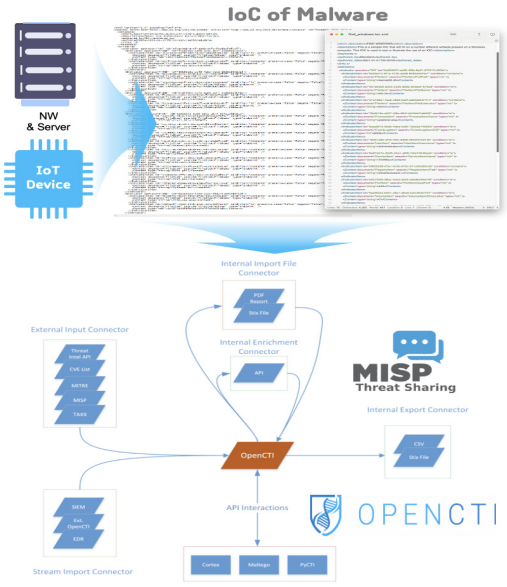
IoT 기기에 대한 침해사고 발생시 IP 주소, 도메인, URL, 해시, 이메일 주소 또는 파일 이름 등과 같은 아티팩트 들을 수집할 수 있으며 상세 공격 정보를 침해지표(IoC)로 생성할 수 있다. 따라서, 이와 같은 IoC 지표를 통해 IoT 기기에서 발생한 침해사고를 파악하고 CTI 시스템을 기반으로 공유하여 앞으로 발생하게 될 잠재적인 위협 행위에 선제적으로 대응할 수 있다[7,8].

이를 위해 본 논문에서는 사고관리 프레임워크 구축 개발 시 IoT에서 수집되는 침해지표(IoC)를 이용하여 CTI 시스템을 통해 각종 위협정보를 효율적으로 공유하는 방법을 비교 분석하였다. 분석 결과 Hub&Spoke 모델을 토대로 위협정보를 공유할 경우 사이버 침해사고 발생 시 대응 시간 및 검출 성능을 향상시킬 수 있어 최근 급증하고 있는 지능형 사이버 공격에 대한 탐지/대응 기술을 더욱더 향상시킬 수 있을 것으로 기대된다.

2. IoC 수집 및 공유

2.1 CTI 시스템에서의 IoC 수집

해지표(IoC)는 “여러 가지 형태의 침해사고의 흔적들을 일정한 포맷으로 정리해 놓은 문서 또는 파일” 또는 “각종 침해 혹은 감염 여부를 확인할 수 있는 디지털 포렌식 아티팩트”로 정의할 수 있다. 그림 1과 같이 IoC에는 일반적으로 IP 주소, 악성코드 해시 값, Host 정보 및 Internet 접속 정보, Cache 파일 정보 등이 포함되며, 정적/동적 분석을 통해 악성코드 등의 실행 흔적을 탐지하거나 조직 내부 망에서의 추가적인 감염 시스템을 찾아내는데 활용될 수 있다[9,10].



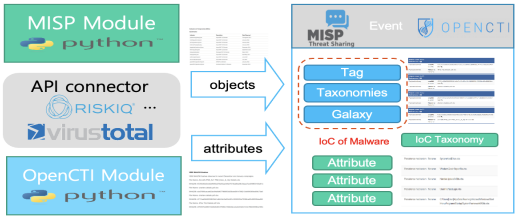
[Fig. 1] Expression of IoC-based Threat Information on IoT Device Attack

그러므로 최근 급증하는 침해사고에 능동적으로 대응하기 위해 사용되는 사이버 위협 인텔리전스 시스템[8,9,10]에서는 침해사고 발생시 침해지표 정보인 IoC 정보를 수집 및 저장하고 이를 토대로 지능형 위협을 지속적으로 모니터링 및 대응하고 있다.

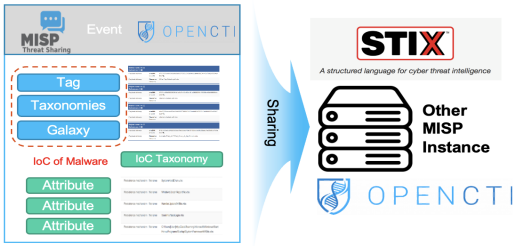
그림 2와 같이 MISP[11]와 OpenCTI[12] 시스템 등과 같은 CTI 시스템을 사용하여 사이버 공격 발생시 수집된 아티팩트를 IoC 정보로 생성한 후 이를 CTI 시스템 내에 저장하게 사용된다. 또한 아래 그림 2와 같이 CTI 시스템 내부에서는 수집된 IoC 정보에 (1) 분류/식별을 위한 테그(Tag) 정보를 추가하고, (2) 분류체계(Taxonomy)를 적용하여 IoC 정보를 체계화하며, (3) 겔럭시(Galaxy) 정보를 이용하여 사이버 공격에 대한 상세 공격 정보를 표현하여, 해당 조직 내에서 운영하고 있는 다른 도구로는 탐지하지 못했던 각종 보안 사고를 더욱 더 신속/정확하게 식별하고 공격을 탐지할 수 있는 기능을 제공한다[13,14].

2.2 IoC 위협정보 공유

컴퓨터 시스템 및 IoT 기기에서 수집된 침해지표(IoC) 정보는 그림 3과 같이 CTI 시스템을 이용하여 타 CTI 시스템과 STIX(Structured Threat Information eXpression) 포맷[15]을 이용하여 공유할 수 있다.



[Fig. 2] MISP instance event storage for IoC information



[Fig. 3] Convert MISP events to STIX2.0 Data Format

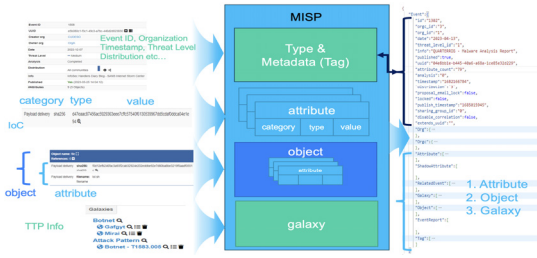
STIX는 JSON 기반 어휘를 사용하여 위협 인텔리전스 정보를 읽을 수 있고 일관된 형식으로 표현한 후 이를 공유할 수 있도록 제작된 표준화된 언어다. 이와 같이 STIX 표준을 사용하면 공통 언어 포맷을 사용하여 전세계 CTI 시스템에서 수집된 위협정보를 효율적으로 공유할 수 있는 기능을 제공한다. 따라서, STIX는 IoT 기기 등을 대상으로 한 공격이 수행될 경우 위협의 동기, 능력, 기능 및 대응 방식을 일관성 있게 표현하고 이를 공유할 수 있는 공통 구문을 제공한다.

3. IoC 공유 방식 상세 분석

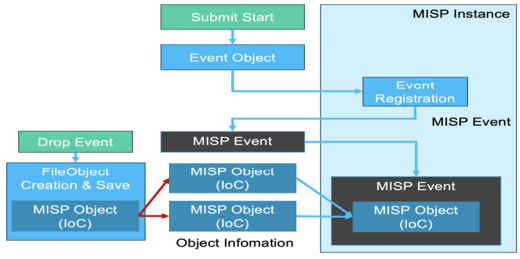
3.1 MISP 기반 IoC 표현

우선 MISP(Malware Information Sharing Platform)에서 IoC를 수집 및 저장하고 타 시스템과 공유하는 과정을 살펴보면 다음과 같다. 아래 그림과 같이 외부 연동 모듈이나 Feed 등의 방법을 통해 외부로부터 IoC를 수신 받을 수 있다. 아래 그림 4와 같이 외부 연동 모듈과 Feed 연결을 사용하여 수집된 IoC 정보를 MISP 내부로 변환/입력 및 저장한다.

IoC 기기를 대상으로 악성코드 기반 공격이 실행될 경우 공격에 대한 이벤트 정보는 아래 그림 5와 같이 MISP 내부에 IoC 인스턴스 형태로 저장/보관된다.



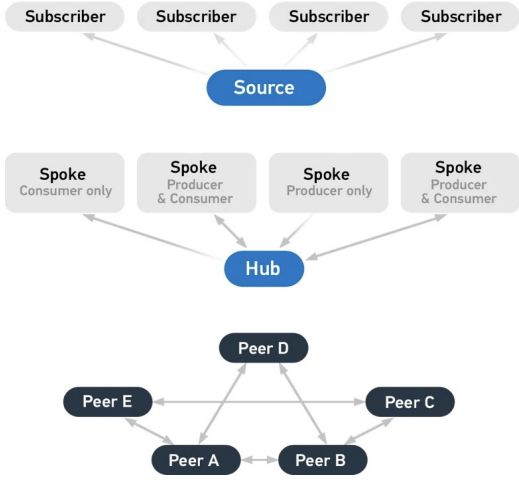
[Fig. 4] MISP Instance Events Registration and Conversion



[Fig. 5] Detailed Storage Process of MISP Instance Events

3.2 MISP 서버간 IoC 위협정보 공유 모델

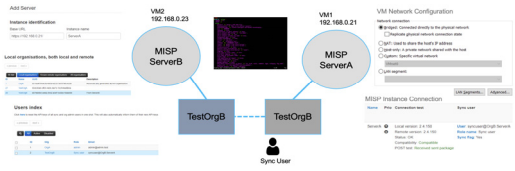
MISP 등과 같은 CTI 시스템에서 IoC 기기를 대상으로 공격이 발생하였을 경우 이에 해당하는 위협정보를 공유하는 방식은 아래 그림 6과 같이 (1) Source & Subscriber 모델, (2) Hub & Spoke 모델 그리고 (3) Peer-to-Peer 모델 등 세 가지 방식을 사용할 수 있다.



[Fig. 6] Inter-MISP IoC Threat Information Sharing Model

- Source & Subscriber Model : 중앙 집중형 데이터 공유. 확장성과 유연성 제공. 서버 장애 시 IoC 공유 문제 발생 가능
- Hub & Spoke Model : 중앙 집중형 데이터 공유. 관리가 용이하고 대규모 시스템에 적용 가능. 중앙 의존도 저하 방식 필요
- Peer to Peer Model : 개체 간 상호 연결 방식. 수평적 사고관리/대응체계 구축 가능. 복잡한 연결로 확장성 문제 해결 필요

MISP 시스템 간에 IoC 정보 기반 위협정보가 CTI 시스템 간에 공유되는 과정을 살펴보면 다음과 같다. 아래 그림 7과 같이 VM1(192.168.0.21, ServerA)과 VM2(192.168.0.23, ServerB)를 설정한 후에 두 MISP 서버간 연동 과정을 확인할 수 있다. 아래 구성도와 같이 서버 간 IoC 위협정보를 공유할 수 있으며 ServerB에서 Pull 과정을 통해 ServerA에 있는 위협정보 IoC 이벤트 정보가 상호 공유되는 것을 확인할 수 있다.



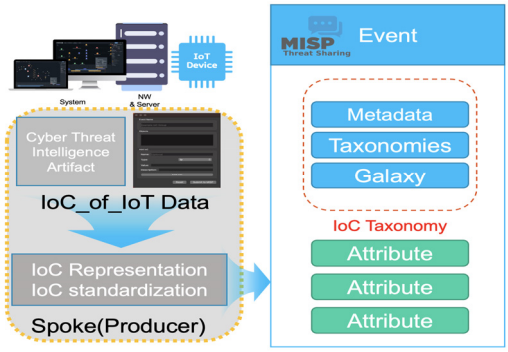
[Fig. 7] Inter-MISP IoC Threat Information Sharing Process

4. 개선된 위협정보 공유 메커니즘

4.1 기존 방식의 문제점 및 해결방안

IoT 기기 등이 설치된 End Point에서 수집되는 IoC 침해지표 정보의 특성을 살펴보면 다음과 같다. 우선 IoT 기기의 특성상 대단위 CTI 시스템을 IoT 기기 내에 설치할 수는 없다. 따라서 IoT 기기에서 발생/수집 가능한 각종 침해지표와 위협정보를 MISP 등과 같은 CTI 시스템에 전달/공유하기는 상당히 어렵다.

따라서, 악의적인 공격자가 IoT 기기를 대상으로 공격을 수행하였을 때 사이버 공격에 해당하는 각종 위협정보를 IoT 기기 외부에 설치/운영하고 있는 MISP 시스템에 전달하고 이를 입력한 후에 CTI 시스템 간에 공유할 수 있는 방식이 제공[16,17]되어야 한다. 이에 본 연구에서는 아래 그림 8과 같이 각종 IoT 기기에서 수집/획득되는 위협정보를 MISP 시스템에 입력하여 각종 CTI 시스템 간에 공유될 수 있도록 IoC 정보 입력 모듈 및 Spoke 방식으로 공유할 수 있는 방식을 제안한다. 제안한 방식을 사용하면 IoT 기기를 대상으로 한 IoC 정보에 대해 TTP 정보와 Malware에 대한 정보를 연계하여 CTI 시스템 간에 공유할 수 있게 되며 이를 통해서 사이버 침해사고에 대해 능동적으로 대응할 수 있는 기반을 제공할 수 있다.

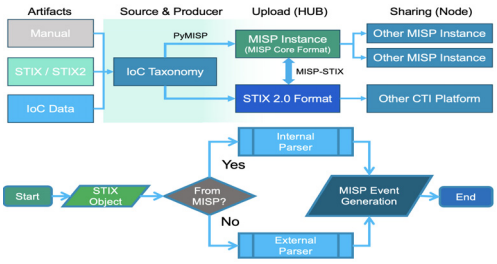


[Fig. 8] Conversion & Sharing of IoC_of_IoT into MISP

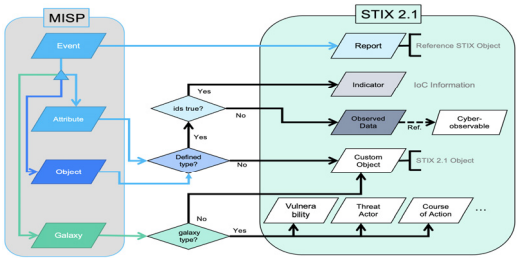
4.2 제안하는 위협정보 공유 구조

구체적으로 본 연구에서 새롭게 제안하는 IoC 위협정보 공유 방식은 다음 그림 9와 같다. 각종 IoT 기기를 대상으로 사이버 공격이 발생하였을 경우 TTP 정보와 악성코드에 대한 상세 정보 등이 포함된 공격 아티팩트가 수집되면 이를 MISP 시스템 등에 저장 및 입력 될 수 있도록 인스턴스 데이터를 생성하는 메커니즘을 제시한다. 아래 그림 9와 같이 (1) IoT 기기에서 다양한 형태의 IoC 정보가 생성[16,17]되면, (2) 이를 IoC 분류체계(Taxonomy)를 적용하여 MISP 인스턴스로 변환하여 MISP 시스템 내에 저장 될 수 있도록 모듈을 구현하며, 또한 (3) OpenCTI 등과 같은 타 CTI 시스템과 공유할 수 있도록 STIX2.0 포맷으로 변환하는 시스템을 구현하였다. 이와 함께 공격 탐지 성능 향상을 위해 IoT 기기 이외의 일반적인 컴퓨터 시스템/기기에서 획득된 침해지표(일반적으로 STIX2.0 포맷으로 표현된 데이터)에 대해서는 출처 정보(MISP 시스템에서 생성된 데이터 여부를 판단)에 대해서 내부/외부 파싱 과정을 수행하여 MISP 인스턴스간 호환성을 높일 수 있도록 구현하였다.

MISP 인스턴스 형태의 MISP 시스템 내부에서 생성되는 이벤트에 대해서 STIX2.0 데이터로 변환하는 과정은 그림 10과 같다. MISP 인스턴스 이벤트에 포함된 각종 속성(attribute) 정보, 객체(Object) 정보에 대해서는 각각 IoC 구조로 표현하며, IoT 기기에 대한 상세 공격 방식에 해당하는 갤럭시(Galaxy) 정보는 MITRE ATT@CK[18]에서 정의한 TTP(Tactic, Technique and Procedure) 형태로 데이터를 생성한다.



[Fig. 9] Data Transformation Structure and Algorithm for IoT Device Threat Information Sharing



[Fig. 10] Conversion of MISP Instance Event into STIX

이와 같은 방법을 제공할 경우 기존의 IoC 포맷 기반 침해사고 공유 방식 보다 상세하고 명료한 형태로 위협 정보를 공유할 수 있으며 MISP[11] 등과 같은 CTI 시스템[7,8]에게 침해사고 발생 시 이를 토대로 더욱 유용한 대응 체계를 구축할 수 있다.

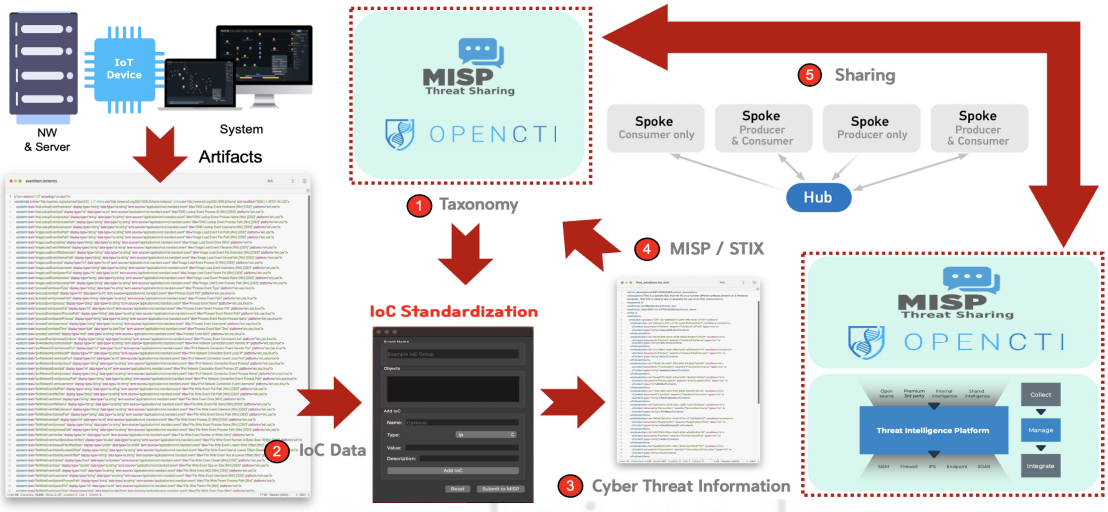
4.3 개선된 위협정보 생성 및 공유 메커니즘

본 연구에서 제안하는 개선된 위협정보 생성 및 공유 메커니즘은 다음과 같다. 각종 IoT 기기로부터 사이버 공격과 같은 침해사고 발생시 다양한 형태의 아티팩트가 수집되면 이를 본 연구에서 개발한 IoC_of_IoT 에디터를 이용하여 MISP 시스템에 입력 가능한 인스턴스 정보로 변환 생성하도록 구현하였다. Python 언어를 이용하여 구현하였으며, PyMISP 모듈 등을 이용하여 수집된 아티팩트를 JSON 형태로 변환/저장할 수 있도록 IoC_of_ICT 에디터를 구현하였다.

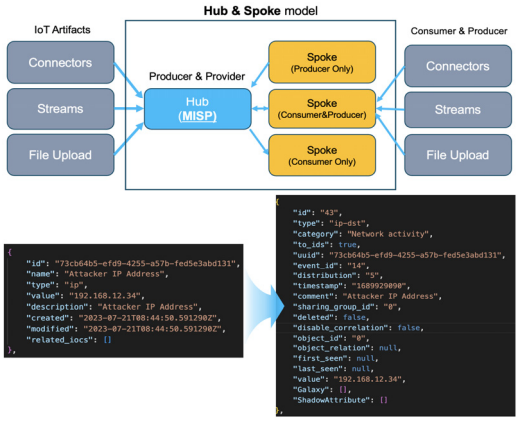
구현한 에디터를 통해 그림 11과 같이 IoT 기기에서 획득한 각종 아티팩트에 대해 (1) 아티팩트 획득 방법, (2) 공격자 정보, (3) 피해자 정보 그리고 (4) 공격 방식에 대한 내용을 JSON 형태로 IoC 데이터를 생성한다.

개선된 침해지표 상세 구조를 이용할 경우 각각의 침해사고에 대한 TTP 정보와 악성코드에 대한 상세 정보들을 포함하여 표현할 수 있으며, STIX2.0 구조[15]로 저장 가능하기 때문에 MISP 또는 기타 CTI 시스템 간에 위협정보를 공유하는 것이 가능하도록 구현하였다. 또한 CTI 시스템 간에 Hub&Spoke 모델 방식으로 위협정보를 공유하는 과정에 적용할 수 있다.

본 연구에서 제안한 IoC 표현 방식을 적용하여 MISP 간에 위협정보를 공유하는 방식을 도식화하면 아래 그림 12와 같으며, 개발한 에디터를 이용하여 생성된 JSON 파일(전/후)에 대해 확인할 수 있다.



[Fig. 11] Structure for Conversion and Sharing of IoC Threat Information Obtained from IoT Device



[Fig. 12] Hub & Spoke Model based Threat Information Sharing and its Representation

4.4 기존 기법과의 비교 분석

본 연구에서 제시한 방식을 적용하였을 경우 세 가지 모델에 대한 성능을 비교 분석하였다. 제안한 방식을 사용하여 Peer-to-Peer 모델, Hub&Spoke 모델 및 Source&Subscriber 모델[2,5,7,13]을 각각 적용하였을 경우 특성별 장단점에 대해 비교 분석하였다. 구체적으로 아래 표 1과 같이 각종 IoT 기기를 대상으로 사이버 침해사고 발생 시 위협정보를 공유하는 과정에서의 복잡도, 신뢰도, 확장성, 신규성 및 유연성에 대해 비교하였다. 그리고 침해지표를 통한 위협정보 전파 속도, 중복처리 성능, 위협정보에 대한 관리 및 탐지 성능에 대해 5단계 척도로 각각 측정하고 이를 종합하여 침해대응 정도를 측정하였다. 비교 결과 Hub&Spoke 공유 모델을 이용한 위협정보 공유 기법이 다른 모델(Peer-to-Peer 71.1%, Source&Subscriber 86.6%) 보다 상대적으로 우수한 성능(93.3%)을 제공하는 것으로 확인되었다.

〈Table 1〉 Comparative Analysis of Threat Information Sharing Model Functionality

Model	Peer to Peer	Hub & Spoke	Source & Subscriber
Complexity	3	4	5
Reliability	3	5	4
Scalability	5	4	4
Novelty	3	5	4
Flexibility	4	5	5
Propagation Speed	4	5	4
Duplicate Elimination	3	4	5
Management Efficiency	3	5	4
Detection Rate	4	5	4
Incident Response (Comprehensive)	3.5/5 (71.1%)	4.6/5 (93.3%)	4.3/5 (86.6%)

[Likert scale (5-poing scale)] : 1 strongly disagree, 2 disagree, 3 neutual, 4 agree, 5 strongly agree

5. 결론

본 연구에서는 IoT 이기종 시스템을 대상으로 점차 지능화·고도화되는 사이버 공격에 능동적으로 대응하기 위해서 침해사고 발생 시 수집되는 위협정보를 효율적으로 공유할 수 있는 기법에 대해 제시하였다. 각종 IoT 기기 등으로부터 수집된 각종 디지털 포렌식 아티팩트를 IoC 정보로 생성한 후에 이를 MISP 등과 같은 CTI 시스템을 통해 공유할 수 있는 기법을 제시하였다.

IoT 기기에 대한 침해사고 발생시 IP 주소, 도메인, URL, 해시, 이메일 주소 또는 파일 이름 등과 같은 각종 아티팩트가 수집되면 이를 IoC_of_IoT 에디터를 이용하여 상세 공격 정보를 침해지표(IoC)로 생성하고 이를 MISP 시스템에서 Hub&Spoke 모델을 적용하여 이벤트 정보를 공유하여 향후 발생하게 될 잠재적인 위협 행위에 효율적으로 대응할 수 있다. 제안한 위협정보 공유 모델을 적용할 경우 사이버 침해사고 분석 과정 시 대응 시간 및 검출 성능을 향상시킬 수 있어 최근 급증하고 있는 IoT 기기를 대상으로 한 지능형 사이버 공격에 대한 탐지/대응 능력을 더욱더 향상시킬 수 있을 것으로 기대된다.

향후 IoT 기기를 대상으로 한 다양한 서비스가 제공되면서 해당 기기의 보안 취약점을 악용한 사이버 공격이 급증할 것으로 예상된다. 따라서 IoT 기반 대단위 네트워크 환경에서 사이버 침해사고 및 사고관리 대응 체계의 유효성을 향상시키기 위해서는 수집된 아티팩트에 대해 지능화되고 자동화된 침해지표 생성 및 공유 프로세스를 개발할 필요가 있다. 또한 공유되는 위협정보에 대한 중복을 최소화하면서 효율적으로 침해사고에 대응할 수 있는 방안이 마련되어야 한다.

REFERENCES

[1] Johnson, C., Badger, L., Waltermire, D., Snyder, J. and Skorupka, C., "Guide to Cyber Threat Information Sharing", NIST Special Publication 800-150, 2016.

[2] Vasil Rizov, "Information Sharing for Cyber Threats", International Journal of Information Security, Vol.39, No.1, pp.43-50, 2018.

[3] A. Pala, J. Zhuang, "Information sharing in cybersecurity: A review," Decis. Anal., Vol.16, No.3, pp.172-196, 2019.

[4] S. Ghernaouti, L. Cellier, and B. Wanner, "Information sharing in cybersecurity : Enhancing security, trust and privacy by capacity building," 2019 3rd Cyber Security in Networking Conference (CSNet), pp.58-62,

2019.

[5] Wagner, T.D., Mahbub, K., Palomar, E. and Abdallah, A.E., "Cyber threat intelligence sharing: Survey and research directions", Computers & Security Vol.87, pp.1-13, 2019.

[6] D. Preuveneers, W. Joosen, J. B. Bernabe and A. Sharmeta, "Distributed Security Framework for Reliable Threat Intelligence Sharing", Security and Communication Networks, Vol.2022, Article ID 8833765, Hindawi, 2022.

[7] R. Brown, R. M. Lee, "SANS Cyber Treat Intelligence (CTI) Survey," SANS Institute, Scandinavia, UK, 2021, https://www.sans.org/white-papers/40080/Tech. Rep.

[8] S. Abu, S.R. Selamat, R. Yusof and A. Ariffin, "An Enhancement of Cyber Threat Intelligence Framework", J. Adv. Res. Dyn. Control. Syst, 10, pp.96-104, 2018.

[9] Mavroeidis, V., Bromander, S., "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence", Intelligence and Security Informatics Conference (EISIC), pp.91-98, 2017.

[10] T. D. Wagner, E. Palomar, K. Mahbub and A. E. Abdallah, "A Novel Trust Taxonomy for Shared Cyber Threat Intelligence", Security and Communication Networks, Vol.2018, Article ID 9634507, Hindawi, 2018.

[11] MISP Threat Sharing, https://www.misp-project.org

[12] OpenCTI, https://filigran.io/solutions/products/opencti-threat-intelligence/

[13] Burger, E. W., Goodman, M. D., Kampanakis, P. and Zhu, K. A., "Taxonomy model for cyber threat intelligence information exchange technologies", ACM Workshop on Information Sharing & Collaborative Security, pp.51-60. 2017.

[14] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues", IEEE Communications Surveys & Tutorials, Vol.22, No.2, pp.1191-1221, 2020.

[15] STIX(TM) Version 2.0. https://www.oasis-open.org/standard/stix2-0/

[16] H. W. Lee, "Analysis of Cyber Incident Artifact Data Enrichment Mechanism for SIEM Model", Journal of Internet of Things and Convergence, Vol.8, No.5, pp.1-10, 2022.

[17] H. W. Lee, "Indicators of Compromise Data Generation Method for Malware on Cyber Incident Occurrence in IoT Environments", Journal of Internet of Things and Convergence, Vol.9, No.4, pp.1-8, 2023.

[18] MITRE ATT&CK, https://attack.mitre.org

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 컴퓨터공학부 교수

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