논문 19-44-08-21 The Journal of Korean Institute of Communications and Information Sciences '19-08 Vol.44 No.08
https://doi.org/10.7840/kics.2019.44.8.1605

위협정보 공유시스템 구축을 위한 내부정보 연동방안

김 갑 수•, 류 동 주*, 강 성 훈**, 김 용 민°

Interoperability of Internal Information for Implementing External Threat Information Sharing Systems

Kab-soo Kim•, Dong-ju Ryu*, Sung-hoon Kang**, Yong-min Kim°

요 약

본 논문은 외부 기업과 기관에서 제공하고 있는 위협 정보를 공유하기 위한 시스템을 구축하는 과정에서 발생 가능한 문제점을 제시하고 이를 극복하기 위한 대응 방안을 작성하였다. 국내 기관의 특성상 신규 위협 정보의 공유가 사후 대응 체계에 맞춰지다 보니 실시간성을 확보하여 관제 업무에 반영하기에는 인프라와 정책에서 상당 부분 어려운 점이 있다. 따라서 본 논문에서는 향후 국내 기반시설과 기관에서 도입 운영하고자 하는 미국 사이버 위협정보 공유 표준(STIX/TAXII)을 국내에 적용하는 방법을 제시하여 효과적인 보안관제 업무에 반영하고자 한다. 또한, 본 논문을 통해서 위협정보 공유시스템을 신규로 구축 시 필요한 사전 지식으로 활용이 가능할 것으로 예상된다.

Key Words : Cyber Threat Intelligence, STIX, TAXII, Threat Information Sharing System, Internal Information Interworking

ABSTRACT

This paper presented possible problems in the process of establishing a system for sharing threat information that is being provided by external enterprises and institutions and drew up alternatives to overcome them. Because of the nature of domestic institutions, sharing of new threat information is geared to the post-response system, there are many difficulties in infrastructure and policies to secure real-time functionality and reflect it in control work. Therefore, this paper presents a method of applying the US Cyber Threat Information Sharing Standard (STIX /TAXII), which is intended to be introduced and operated by domestic infrastructure and institutions in the future, to the domestic market, and is intended to be reflected in effective security system work. In addition, through this paper, it is expected to be possible to use the prior knowledge required for the new threat information sharing system.

Ⅰ. 서 론

최근 정교해진 사이버 공격의 다변화로 인해 정보기관과 사람에 의한 최신 위협 정보의 수집 및 공유 방식의 한계점이 발생하고 있다. 이러한 정보 공유의 한계를 극복하고 최신 위협에 대한 실시간성 정보와 그에 따른 기관 내 파급력 등을 고려한 사전 정보 분석과 영향도 분석의 필요성이 대두되었다. 이와 같은

• First Author : Interdisciplinary Program of Information Security, Chonnam Nat'l Univ, 136027@jnu.ac.kr, 학생회원
° Corresponding Author : Interdisciplinary Program of Information Security, Chonnam Nat'l Univ, ymkim@jnu.ac.kr, 정회원
* Far East University, ryu@btress.com, 종신회원
** National Information Resources Service, rain9780@korea.kr
논문번호 : 201905-071-C-RE, Received May 6, 2019; Revised June 23, 2019; Accepted June 28, 2019

분석의 효과를 극대화하기 위해서는 최신 위협 정보 등에 대한 수집, 가공, 전달 방식의 데이터를 표준화하여 설계 구축하는 것과 외부로부터 수집된 위협공유 공격지표를 즉시 활용 가능하도록 시스템을 이용한 정보의 정형화, 그리고 위협 정보의 재가공이 불필요하도록 정보를 표준화하여 사용해야 한다[1-3].

이러한 장점에 입각하여 기존 시스템 영역은 극대화 시키고, 신규 구축 범위에 대한 영역을 사전에 기획, 설계하여 정보의 원활한 흐름을 만들고 위협 정보에 대한 외부와 내부 관점의 위협 비교 검증으로 실질적인 파급력과 영향도를 가늠할 수 있을 것으로 판단된다. 따라서 본 논문에서는 미국 표준인 STIX(The Structured Threat Information eXpression) / TAXII(Trusted Automated eXchange of Indicator Information)를 이용하여 국가기관 중 가장 많은 정보를 관리하는 국가정보자원관리원에서 위협정보 공유 시스템 구축을 준비하면서 발생 가능한 문제점을 공유하고, 이를 통해 신규 구축 시 고려사항과 내부 시스템과의 연동 방안을 제시하고자 한다[4].

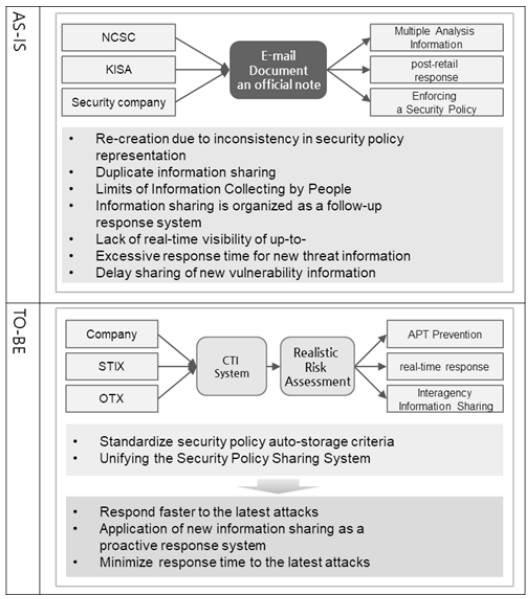


그림 1. 사이버 위협지능 시스템 도입 기대 효과
Fig. 1. Expected Effect of Cyber Threat Intelligence Sharing System

Ⅱ. 본 론

2.1 국내 사이버 위협정보 공유 현황

국내 정보통신기반보호를 위한 공공 및 민간 지원기관으로 한국인터넷진흥원(KISA), 국가보안기술연구소(NSRI), 정보공유·분석센터(ISAC), 한국침해사고대응팀협의회(CONCERT) 등이 있다[4,5]. 이들 기관에서 공유하는 정보는 일방향으로 공유되고 있으며, 공유된 정보는 기업을 위한 정보로 기관과의 연동보다는 사후 대응을 위한 정보 공유이다. 역관점에서 평가하면 다른 기관이나 업체가 보유하고 있는 사이버 위협 정보들이 공유되지 않기 때문에 같은 형태의 침해사고들이 중복 발생하더라도 원활한 대응이 어려운 상황이다[6][7]. 따라서 실시간성에 대한 정보 공유는 이루어지지 않고 있는 현황이다. 또 국가정보원에서 제공 중인 정보 역시 일부만이 실시간으로 전달되며 메일이나 해당 긴급정보를 파일로 전달하거나 일부 데이터를 공유하는 형태로 공유된다. 이렇게 공유된 정보로는 지능형 지속 위협(APT, Advanced Persistent Threat) 공격과 같은 사이버 공격을 선제적 대응하기에는 어려운 상황이다. 이를 극복하기 위해 각 기관에서는 외부기관 및 보안업체와 위협정보의 연동을 통해 최신 공격에 대한 신속한 대응 및 공격 대응에 대한 소요 시간 최소화, 신규 위협 정보 공유로 사이버 공격에 사전대응체계 구축 등의 효과를 기대하고 있다. 그림 1은 내부 정보와 외부 정보를 연동시에 가능한 기대 효과를 예시한 것이다[8].

2.2 STIX / TAXII

미국 국토안보부(DHS)와 국립기술표준연구소(NIST)는 사이버 위협에 대응하기 위하여 효율적이고 안전한 정보공유 체계 구축의 필요성을 인지하였으나, 사이버 위협 정보가 표준화되지 않아 일관성 있는 분석의 어려움을 느끼고 이를 극복하기 위해 2012년부터 사이버위협 정보에 대한 표현 및 전송에 대한 표준화 작업을 추진하여 STIX/TAXII 버전 1.0을 2013년 10월에 공개하였다[5,9].

STIX는 여러 보안 위협 탐지 장치로부터 수집된 사이버 위협의 정보를 표준화된 형태로 표현하고 그 정보로 위협을 분석하는데 사용하거나, 특정한 위협을 탐지하기 위한 패턴을 표현하는데 사용할 수 있다. 이를 표 1과 같이 사이버 위협 분석, 사이버 위협에 대한 지표 패턴 지정, 사이버 위협 대응 활동 관리, 사이버 위협 정보 공유 등으로 활용 할 수 있다.[10].

2.2.1 STIX

STIX[11]는 사이버 위협 정보를 규격화하고, 각 위협 정보의 특성을 명시 및 공유하기 용이한 형태의 구조적인 방법의 표현법을 채택하였다. STIX는 일관성, 효율성, 상호 운용성 및 일반적인 상황에서의 위협 인

표 1. STIX 활용 방안
Table 1. STIX Use Cases

Use Cases	Description
Analyzing Cyber Threats	A cyber threat analyst reviews structured and unstructured information regarding cyber threat activity from a variety of manual or automated input sources.
Specifying Indicator Patterns for Cyber Threats	A cyber threat analyst specifies measurable patterns representing the observable characteristics of specific cyber threats along with their threat context and relevant metadata for interpreting, handling, and applying the pattern and its matching results.
Managing Cyber Threat Response Activities	Cyber decision makers and cyber operations personnel work together to prevent or detect cyber threat activity and to investigate and respond to any detected incidences of such activity.
Sharing Cyber Threat Information	Cyber decision makers establish policy for what sorts of cyber threat information will be shared with which other parties and how it should be handled based on agreed to frameworks of trust in such a way as to maintain appropriate levels of consistency, context and control.

식 기능을 제공하기 위한 메커니즘을 제공하며, STIX를 이용하면 지능형 사이버 위협(CTI, Cyber Threat Intelligence) 대응을 일관성 있고 기계 판독이 가능한 방식으로 서로 공유할 수 있으므로 공격을 빠르고 효과적으로 예측하고 대응할 수 있게 된다.

STIX 2.x에서는 파일 형식이 XML(Extensible Markup Language)에서 JSON(JavaScript Object Notation)으로 변경되었으며, “STIX Cyber Observables”라는 관찰정보(Cyber Observable eXpression)가 포함된 12개의 Domain Object와 2개의 Relationship Object 요소로 구성되며, 각각의 객체(Object)의 이름과 내용을 표 2에 설명하였다.

2.2.2 TAXII

TAXII[12]는 STIX로 표현된 사이버 위협 정보를 HTTPS를 통해 공유하기 위한 전송 규격으로서 HTTP의 장점을 최대한 활용하는 RESTful(REpresentational State Transfer) API와 TAXII 클라이언트 및 서버에 대한 요구사항의 집합을 정의하고 있다. TAXII는 그림 2와 같은 hub-and-spoke, peer-to-peer,

표 2. STIX 2.x SDOs 및 SROs
Table 2. STIX 2.x SDOs and SROs

Name	Description
SDOs(STIX Domain Objects)	
Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
Course of Action	An action taken to either prevent an attack or respond to an attack.
Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
Malware	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim’s data or system.
Observed Data	Conveys information observed on a system or network (e.g., an IP address).
Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
Tool	Legitimate software that can be used by threat actors to perform attacks.
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
SROs(STIX Relationship Objects)	
Relationship	Used to link two SDOs and to describe how they are related to each other.
Sighting	Denotes the belief that an element of CTI was seen (e.g., indicator, malware).

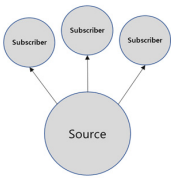
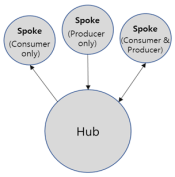
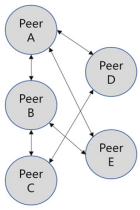
Source/Subscriber	
	Source/Subscriber is a sharing model where one organization functions as the single source of information and sends that information to subscribers.
Hub and Spoke	
	Hub and Spoke is a sharing model where one organization functions as the central clearinghouse for information, or hub, coordinating information exchange between partner organizations, or spokes. Spokes can produce and/or consume information from the Hub.
Peer to Peer	
	Peer to Peer is a sharing model where two or more organizations share information directly with one another. A Peer to Peer sharing model may be ad-hoc, where information exchange is not coordinated ahead of time and is done on an as-needed basis, may be well defined with legal agreements and established procedures, or somewhere in the middle.

그림 2. TAXII 위협정보 공유 모델
Fig. 2. TAXII Threat Sharing Models

source-subscriber 등의 다양한 위협공유 모델을 지원한다.

국내외 기업과 기관에서 STIX/TAXII를 포함한 다양한 방법으로 정보 공유 시스템을 운용중이지만 본 논문에서는 위협정보 공유시스템을 구축하기 위한 플랫폼을 STIX/TAXII로 구성하였으며 해당 정보만을 표기한다[13].

Ⅲ. 내부정보 연동 위협정보 공유시스템

3.1 목표 시스템

국가정보자원관리원에서는 STIX/TAXII의 2.x버전을 이용하여 그림 3의 Source/Subscriber 모델 같이 외부 위협정보 제공사로부터 신규 위협정보를 수집, 처리, 공유하는 위협정보 공유시스템을 구축하여 신규 위협정보를 분석하여 최신 공격 탐지에 활용하고, 표준화된 공유 방식으로 신속하게 위협정보를 공유하여

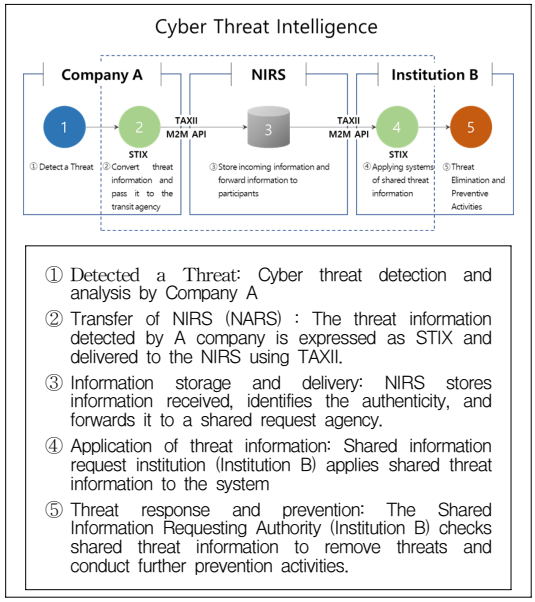


그림 3. 사이버 위협정보 공유 흐름도
Fig. 3. Cyber Threat Information Sharing Flowchart

최신 공격에 대한 대응 소요 시간 최소화를 기대하고 있다.

그림 3은 위협정보 공유시스템을 통한 사이버 위협정보의 내부 정보와 외부 정보 연동 과정을 도시한 것이다. 위협정보를 공유하기 위해서는 위협 정보의 공유가 명확하게 상호 협의 하에 제시되어야만 하고, 공통 플랫폼이 구축되어야 한다. 플랫폼 구축 시 반영한 구조는 위협정보 표준으로 구성한 공유 시스템(TAXII)을 기관에 맞게 재구성하였다[14,15].

위협정보 공유시스템 구축 시 고려사항을 나열함에 있어 국가정보자원관리원의 내부 환경에 대한 자세한 설명은 보안상 일반적인 내용으로 대체하거나 축약하여 설명하였다.

3.2 구축 시 고려사항

위협정보 공유시스템 구축 시 사용되는 소스코드는 대부분 오픈소스로 되어 구축이 용이하지만 해당 소스코드를 그대로 사용하기엔 상당 부분의 취약점과 소스의 불안정성을 내포하고 있다[16]. 특히, 공공 기관은 내부 정보가 외부에 유출 가능한 구조이므로 위험요소들을 최대한 배제하여야 하는 문제점을 갖는다[17].

인터넷이 연결된 환경에서 오픈소스로 개발된 시스템을 인터넷 연결이 차단된 내부에 구축하기 위해서는 소스코드의 취약성 점검 및 악성코드 포함 여부와

소스코드 및 라이브러리의 최신버전 확인, 내부 네트워크 및 시스템 환경을 고려한 소스코드의 의존성 문제 등을 확인해야 한다.

국가정보자원관리원에서 위협정보 공유시스템을 내부에 구축하기 위해서 앞에서 설명한 오픈소스의 문제점과 폐쇄망에서의 시스템 구축 시 고려사항외에 신규 위협 탐지 및 대응과 신규 위협정보 공유를 위해 다음의 5가지 항목을 고려하였다.

- 내부 환경 정보에 대한 명확한 분석
- 내부 환경에서 보안 시스템과의 연동
- STIX / TAXII의 버전 선택
- 위협정보 연동을 위한 정책 수립 및 체계 구축
- 공개망과 내부망 연동을 위한 망연계 방안수립

첫째, 내부 환경 정보에 대한 명확한 분석이 필요하다. 이는 불필요한 정보 공유와 시스템 확장만을 고려한 나머지, 네트워크 구조에 대한 이해가 부족하면 시스템 정보가 외부에 유출 가능한 취약한 구조로 구축될 가능성이 있다. 그리고 위협정보 공유시스템에서 사용할 신규 위협정보의 위험도 평가와 신규위협 탐지 및 대응에 사용되는 자산 정보가 현행화되지 않으면, 위협이 탐지되더라도 신속하고 정확한 대응이 어렵게 된다.

둘째, 내부 환경에서 보안 시스템과의 연동을 고려해야 한다. 신규 위협에 신속한 대응을 위해서는 실제 STIX / TAXII를 통해서 얻고자 하는 정보의 유형을 내부 위협 탐지 시스템의 특징을 고려하여 STIX의 객체에서 활용 가능한 정보로 식별해야 한다. 그리고 외부 정보가 내부 시스템에 전달될 때는 JSON 또는 XML 구조를 가진 파일의 형태이므로 이를 수집하여 저장할 Database 유형에 대한 고민과 저장되는 정보에는 신규 위협 정보의 분석된 악성코드가 포함될 수 있어 격리 조치를 고려해야 한다.

셋째, 현재 STIX / TAXII는 1.x버전과 2.x 버전 두 가지가 존재하므로 버전을 선택하여 구축해야 한다. 1.x 버전은 XML구조로 되어 있으며, 2.x 버전보다 많은 곳에서 사용되고 있다. 2.x 버전은 JSON 구조로 되어 있어 해당 파일을 이용한 다양한 개발이 용이하다. 각각 버전은 파일 형태와 파일 공유 방식, 문서 구조가 완전히 변경되었기 때문에 호환되지 않으므로 하나의 버전을 선택하여야 한다.

넷째, 위협정보 연동 시 기존 시스템에서의 정책 적용과 적용된 정책을 반영하기 위한 체계 구축이 선행되어야 한다. 시스템만을 도입하면 모든 것이 가능할 것으로 예상되는 관리자들로 인해 심각한 문제점들이 초래되는데 이런 문제점을 줄이기 위해 상당 부분은 기관 내부에서 사전 공유와 협의가 필요하다. 또한, 외부 위협에 대한 대응과 정책 공유를 위한 내부 환경에서의 신규 위협 위험도 재평가가 필요하다.

다섯째, 폐쇄형 내부망과 외부망의 연동을 고려할 때에는 망연계 장비를 도입하되 일방향으로 연동되도록 구성해야 한다. 신규 위협 수집을 위해서는 내부망와 외부망의 연동이 필수이며 내부 정보가 외부로 연결되는 구조를 갖게 된다. 양방향 파일전송 시스템을 이용할 때는 내·외부의 정보가 공유되므로 기관에서는 원하는 정보의 가치와 기준에 따라 제어가 되어야 하며, 설계 및 구축 단계에서 시스템 구축 시 운용 위치에 대한 명확한 설계가 반영되어야 한다. 내부망으로 정보를 전송하는 방법으로는 내부망에서 직접 외부망에 질의를 수행하고 결과를 망연계 시스템을 통해 전달받는 방법과 내부망이 아닌 외부망에서 질의를 수행하고 결과만 시스템에 반영하는 방법이 있다.

3.3 STIX 정보와 내부정보 연동 방안

3.3.1 위협정보 공유 시스템 흐름도

위협정보 공유시스템을 구축하기 위하여 기관 내부에서 수집할 수 있는 정보의 식별과 외부에서 공유하는 위협 정보와 실제 사용되는 STIX 샘플 분석, 신규 위협의 위협식별 및 위험도 재평가 등을 수행하였다. 본 논문에서는 신규위협 정보와 기관 내부의 탐지된 위협정보를 비교 분석하여 알려지지 않은 위협행위에 대한 대응과 입주 기관과의 신규 위협정보 공유 방안에 대한 내용 중심으로 설명하였다.

위협정보 공유시스템은 그림 4와 같은 업무 흐름을 갖으며, 기관 외부의 위협정보 공유 서비스로부터 정보를 전달받거나, 내부에서 탐지된 위협정보로 외부 기관에 위협정보를 질의하여 신규 위협정보를 수집한다. 수집된 정보는 내부 보안장비에 의해 탐지된 위협

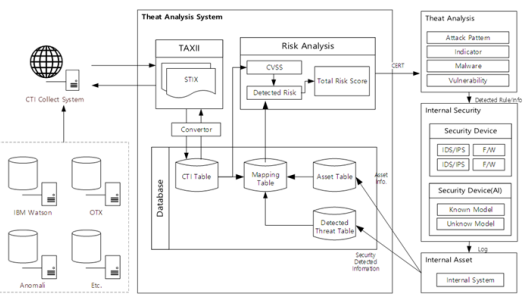


그림 4. 위협정보 분석 시스템 구축 흐름도
Fig. 4. Threat Information Sharing System Deployment Flowchart

정보와 내부 자산 정보를 비교하여 새로운 보안 위협을 탐지하게 된다. 탐지된 신규 위협은 기관에 맞게 위험도를 평가하고 위험도에 따라 위협에 대응하고 탐지된 신규 위협 정보를 공유하게 된다.

3.3.2 신규위협 탐지 및 대응

신규위협 탐지는 그림 5와 같은 단계를 갖으며, 신규위협 탐지를 위해 기관의 네트워크 방화벽, IPS/IDS, 백신프로그램, 웹방화벽 등 다양한 보안장비의 로그정보와 내부 자산정보에서 사전에 정의된 항목을 수집하게 된다. 신규 위협정보는 위협정보 공유서비스로부터 공유받거나, 필요 시 외부 위협공유 서비스에 질의하여 결과를 수집하게 된다. 수집된 보안장비의 로그정보와 내부 자산정보, 신규 위협정보는 위협정보 공유 시스템에서 비교 및 분석하여 내부의 신규위협을 탐지하는데 사용하게 된다. 내부의 신규위협이 식별되면 내부 위험평가 방법에 따라 신규위협의 위험도를 산정하게 되고, 위험도에 따라 위협 분석 및 대응 우선순위를 정하게된다.

신규위협 정보에 포함된 공격유형과 기관에서 사용하는 공격유형이 상이하므로 신규위협의 공격유형 특징을 분석하여 기관에서 사용하는 공격유형과 비교할 수 있도록 STIX의 객체 속성 중에 공격유형을 판단하는데 사용될 수 있는 속성 값을 표 3과 같이 분류하였다. 분류한 STIX의 객체 속성 값과 내부자산 및 보안장비의 로그 값을 비교하기 위한 매핑 테이블을 표 4와 같이 작성하였다. STIX 객체 속성 값과 비교한 내부 자산정보는 자산의 IP, URL, 설치된 소프트웨어 종류 및 버전 정보 등을 사용하였으며, 보안장비 로그정보는 방화벽, IPS, 백신 등의 로그를 사용하였다.

신규 위협 탐지 및 대응 예를 들면, 기관 내부의 보안장비에서 exploit.exe 라는 악성파일이 탐지되면, 위협정보 공유시스템은 먼저 수집된 위협정보에서 관련 정보를 조회하고 정보가 없을 경우 외부 위협정보 공유서비스에 악성파일을 조회하여 신규 위협을 찾게 된다. 이렇게 정보를 조회하여 위협정보를 찾게되면, 위협정보에 포함된 다른 정보를 내부 자산 정보 및 보안탐지 로그정보와 비교·분석하여 신규 위협을 탐지하고 대응하게 된다.

외부 위협정보 공유서비스에서 윈도우 서버를 대상으로 하는 신규 위협정보가 공유되면 내부 자산정보에서 윈도우 서버와 관련된 정보를 조회하고 기관에 미칠 위험도에 따라 신규위협을 대응하게 된다.

표 3. 공격유형과 STIX 객체 속성 값 비교
Table 3. Compare Attack types with STIX Object property values

Attack Type	Observed Data	RelationShip	Object
Malicious mail	email-message email-addr	indicates	attack-pattern
Malicious URL/IP	domain-name url ipv4-addr ipv6-addr mac-addr	indicates	attack-pattern malware
Malware	file process windows-registry-key directory network-traffic	indicates	malware
vulnerability	software network-traffic	indicates	attack-pattern

표 4. 내부정보와 STIX Indicator Pattern의 매핑 테이블
Table 4. Mapping table of internal Asset Info. and and STIX Indicator pattern

Internal Asset Info.		**STIX Indicator Pattern**
Asset Field	IP	ipv4-addr ipv6-addr
	URL	url domain-name
	Email	email-address email-message
	Software Name	Software
	Software Version	Software
Security Log Field	Detected IP	ipv4-addr ipv6-addr
	Detected URL	url domain-name
	Attack Pattern	network-traffic Software
	Filename	File
	Email Address	email-address

3.3.3 신규 위협정보 공유

기관에서는 IPS, 네트워크 방화벽, DDoS 장비 등 보안장비에서 탐지된 위협정보나 정보통신기반보호를 위한 공공 및 민간 지원기관 관제 및 관리하는 기관에서 공유된 위협정보를 내부 입주 기관에 공유하고 있다.

신규 위협정보 공유는 그림 6과 같은 흐름으로 진행되며, 신규 위협정보가 수집되면 위협정보를 분석하여 신규 위협정보의 위협에 노출되는 장비를 식별하고 해당 내부 기관에 공유하게 된다.

신규 위협정보가 탐지되면 신규 위협에 노출되는 장비를 식별하기 위해서 신규 위협정보 중 Indicator Object, Vulnerability Object, Malware Object, Observed data Object, Target Object에서 공격자 및 공격 대상의 IP나 URL, 공격 대상 소프트웨어 종류 및 버전정보, CVE(Common Vulnerabilities and Exposures)의 vendor, product, version 정보를 내부 자산정보와 비교하여 위협이 존재하거나 위협에 노출될 가능성이 있는 장비를 식별하여 표 5와 같은 보안공지를 해당 기관에 공유한다. 표 5는 내부 입주 기관에 공유하는 위협정보 예시로 실제 공유 정보는 공개할 수 없어 한국인터넷진흥원에서 공유하는 위협정보로 대체하였다.

기존 위협정보를 신속하게 STIX로 작성하여 공유

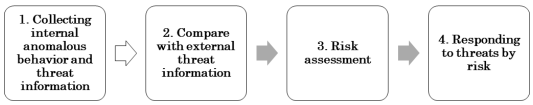


그림 5. 신규 위협 탐지 및 대응 흐름도
Fig. 5. Threat Detection and Response Flowchart

표 5. 보안공지 예시
Table 5. Security Notification Example

- Security Notification -

Cisco IOS XE Patch Update Advisory

☐ Description
o A vulnerability in the Web Services Management Agent (WSMA) function of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary Cisco IOS commands as a privilege level 15 user.
o CVE-2019-1755

☐ Affected Products
o This vulnerability affects Cisco devices that are running an affected release of Cisco IOS XE Software with the web server feature enabled.

☐ Fixed Software
o Cisco has released free software updates that address the vulnerability described in this advisory.

☐ Contact
o NIRS Cert 118

표 6. 공유 위협정보와 STIX 객체의 매핑테이블
Table 6. Mapping table of Shared Threat Information and STIX Object

Security Notification	STIX Object
Description	Attack Pattern Indicator Vulnerability malware observed data
Affected Products	Target
Fixed Software	Course of Action
Contact	Identity

할 수 있도록 기존 위협정보 형태를 STIX 객체의 속성 값과 비교하여 표 6과 같은 공유 위협정보와 STIX 객체 매핑 테이블을 작성하였다. 위협정보를 STIX로 작성하면, 해당 위협이 존재하는 내부 자산을 식별하여 해당 자산을 보유한 내부 입주 기관이나 해당 부서에 위협정보를 공유하게 된다.

Ⅳ. 결론 및 향후연구

본 논문은 미국 표준인 STIX / TAXII를 이용하여 국가기관 중 가장 많은 정보를 관리하는 국가정보자원관리원에서 위협정보 공유시스템 구축을 수행하면서 겪은 고려사항과 애로사항에 기반하였다.

기존 보안장비의 보안 로그와 내부 자산 정보를 위협정보 공유 포맷인 STIX와 매핑함으로서, 위협정보 공유시스템은 신규 위협정보를 수집된 자산 정보와 비교 분석하여 위협을 탐지하고, 위협이 발견될 수 있는 자산을 식별하게 된다. 탐지된 위협은 위험도에 따라 위협에 대응하며, 위협이 발견된 자산의 부서나 내부 입주 기관에 위협정보를 공유하여 지능형 지속 위협 공격과 같은 사이버 공격에 선제적 대응이 가능할 것으로 기대한다. 외부의 위협정보나 기관에서 탐지한 위협정보를 표준화된 STIX 기반의 위협정보 형태로 변환은 위협정보를 TAXII 클라이언트를 이용하여 내부 입주 기관에 신속하게 공유할 수 있는 장점을 갖게 된다.

따라서 본 논문을 통해 향후 구축을 수행하거나 계획을 갖고 있는 기관과 기업에게 좀 더 현실적인 사례를 제시하여 시간적 물질적 손실을 최소화하고, 충분한 사전 지식으로써 활용이 가능할 것으로 예상된다. 향후 실제 시스템을 구축하면서 발생 가능한 위협정보 공유시스템의 활용방안에 대한 제시할 계획이다.

References

[1] E. J. Park and S. J. Kim, "Derivation of security requirements of smart factory based on STRIDE threat modeling," *J. KIISC*, vol. 27, no. 6, pp. 1467-1482, Dec. 2017.

[2] M. A. Huq Shahi, "*Tactics, techniques and procedures (TTPs) to augment cyber threat intelligence (CTI): A comprehensive study,*" St. Cloud State Univ., May 2018.

[3] M. M. Han, S. S. Hong, J. H. Kong, and D. U. Kim, "*A study on construction plan of intelligence security system for response of advanced persistent threat*," Ind.-Univ. Joint Research Institute of Gachon Univ., Nov. 2015.

[4] D. H. Kim, S. D. Park, S. J. Kim, and O. J. Yoon, "A study on establishment of cyber threat information sharing system - focusing on U.S. cases," *Convergence Secur. J.,* vol. 17, no. 2, pp. 53-68, Jun. 2017.

[5] H. S. Jin, M. N. Shim, and M. H. Yang "*A Study on software safety information sharing system - Focusing on overseas cases*," Software Policy & Research Institute(SPRi), Apr. 2018.

[6] C. M. Park and J. S. Cho, "INTERNET & SECURITY FOCUS," *KISA*, pp. 47-59, Jan. 2014.

[7] S. J. Jeon and J. H. Kim, "A study on cyber threat intelligence system to respond effectively to advanced cyber threats," in *Proc. KICS ICC 2018 Fall*, pp. 584-585, Seoul, Korea, Jun. 2018.

[8] O. J. Yun, C. S. Cho, J. K. Park. H. J. Seo, and Y. T. Shin, "A study on the improvement model for invigorating cyber threat information sharing," *Convergence Secur. J.*, vol. 16, no. 4, pp. 25-34, Jun. 2016.

[9] Sean Bamum, "*Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX^{TM})*," MITRE Corporation, Feb. 2014.

[10] D. Chismon and M. Ruks, "*Threat intelligence: Collecting, analysing, evaluating*," MWR InfoSecurity Ltd., 2015.

[11] OASIS, *Introduction to STIX*, Retrieved Apr. 30, 2019, from https://oasis-open.github.io/cti-documentation/stix/intro

[12] OASIS, *Introduction to TAXII*, Retrieved Apr. 30, 2019, from https://oasis-open.github.io/cti-documentation/taxii/intro

[13] A. Lemay, "*Cyber Threat Data Model and Use Cases*," International Safety Research (ISR), Sep. 2017.

[14] C. H. Lee and B. H. Kang, "*System Structure for Interoperability between STIX based Cyber Threat Intelligence Sharing Systems and Legacy Detection Systems*," Telecommunications Technology Association, Jul. 2017.

[15] B. Kim, N. Kim, S. Lee, Cho, and J. Park, "A study on cyber threat intelligence analysis (CTI) platform for proactive detection of cyber attacks based on automated analysis," in *Proc. KICS ICC 2017 Fall*, pp. 578-579, Daegu, Korea, Nov. 2017.

[16] J. H. Jeong and Y. H. Cha, "*Using Threat Modeling for Risk Analysis of SmartHome*," KITRI BoB, Nov. 2015.

[17] V. Mavroeidis and S. Bromander, "*Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence,*" Oslo Univ., Sep. 2017.

김 갑 수 (Kab-soo Kim)

2010년 2월 : 세종사이버대학교 정보보호학과 학사

2013년 3월~현재 : 전남대학교 대학원 정보보안협동과정 석사과정

<관심분야> 모의침투, 정보보호관리체계, 개인정보보호

[ORCID:0000-0002-6608-4820]

류 동 주 (Dong-ju Ryu)

현재 : 한국통신학회 정회원
2009년 : 전남대학교 정보보안협동과정 박사
2019년 : 비트레스 대표이사
현재 : 극동대학교 산업보안학과 조교수
<관심분야> 사이버추적, 블록체인보안, 인공지능보안

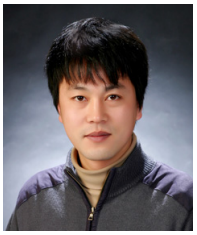
[ORCID:0000-0003-3856-1391]

김 용 민 (Yong-min Kim)

2002년 8월 : 전남대학교 전산통계학과 박사
2006년~현재 : 전남대학교 문화콘텐츠학부 전자상거래전공 / 정보보안협동과정 교수
<관심분야> 시스템 및 네트워크 보안, 전자상거래 보안, 융합보안 등

[ORCID:0000-0002-5066-3908]

강 성 훈 (Sung-hoon Kang)



현재 : 국가정보자원관리원 사이버안전과 주무관
<관심분야> 인공지능 보안관제, 통신보안

[ORCID:0000-0001-5149-1055]