JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 20, No. 6, pp. 1173-1180, Jun. 2019

스마트시티의 보안을 위한 사이버보안위협정보 활용 연구

김 현 진[1] · 손 태 식[1,2*]
[1]아주대학교 컴퓨터공학과
[2]아주대학교 사이버보안학과

A Study on Cyber Security Threat Intelligence(CTI) Utilization for Smart City Security

HyunJin Kim[1] · Taeshik Shon[1,2*]
[1]Department of Computer Engineering Ajou University, Suwon, Gyeonggi-do, Korea
[2]Department of Cyber Security, Ajou University, Suwon, Gyeonggi-do, Korea

[요 약]

세계 각 국에서는 도시화의 심화로 인해 발생되는 도시문제를 해결하기 위해 스마트시티의 활성화를 위한 사업을 진행하고 있다. 그러나 스마트시티는 다양한 도메인들의 사물들이 연결되어 공격 경로가 증가할 수 있으며 다양한 ICT 기술이 융합되기 때문에 기존 및 새로운 보안 취약점이 승계될 수 있다는 우려가 존재한다. 또한 이전 공격기술을 변형하거나 새로운 공격기술을 사용하는 사이버 공격들이 매년 증가하고 있어 사이버공격 징후를 사전에 탐지하여 차단하는 것은 현재의 보안 인력과 사이버 방어 기술로는 한계인 상황으로 이에 대한 보안연구가 필수적이다. 이러한 한계점을 극복하기 위해 본 논문에서는 스마트시티에서 사이버보안위협정보를 이용하여 위협을 탐지하는 활용 모델을 제시하였으며 이후 스마트시티 주요 도메인의 테스트베드에서 활용 모델을 적용하는 세부방법에 대해 제시하여 향후 실 도입에 있어 활용되고자 한다.

[Abstract]

Countries around the world are carrying out projects to revitalize smart cities to solve urban problems caused by deepening urbanization. However, there are concerns that smart cities can succeed in existing security vulnerabilities because objects from different domains can be connected and attack paths can increase and various ICT technologies converge. Also, as cyberattacks that alter previous offensive technologies or use new offensive technologies are increasing every year, detecting and blocking cyberattacks in advance is a critical situation with current security personnel and cyber defense technologies. In order to overcome these limitations, this paper proposes a utilization model for detecting threats using cyber security threat intelligence in SmartCity, and then presents the details of how to apply the utilization model in the test bed of the smart domain to be utilized for the future.

색인어 : 스마트시티, 산업기반시설, 사이버보안위협정보, 위협헌팅

Key word : Smart City, Industrial Control System, Cyber Threat Intelligence(CTI), Threat Hunting

http://dx.doi.org/10.9728/dcs.2019.20.6.1173

Received 24 April 2019; **Revised** 15 May 2019
Accepted 25 June 2019

***Corresponding Author; Taeshik Shon**

Tel: +82-31-219-1898
E-mail: tsshon@ajou.ac.kr

Ⅰ. 서 론

스마트시티는 “도시의 경쟁력과 삶의 질의 향상을 위하여 건설・정보통신기술 등을 융・복합하여 건설된 도시기반시설을 바탕으로 다양한 도시서비스를 제공하는 지속가능한 도시”로서 기존의 도시 인프라 고도화 차원의 단순 ICT 기술 접목이 아닌 교통, 헬스케어, 건설, 인프라, 에너지 등 도시를 유지시키는 영역의 다양한 기기와 서비스를 서로 연결하고 수집·분석된 데이터를 하나의 플랫폼과 같이 연동하여 운영되는 통합된 개념의 도시이다[1].

이러한 스마트시티는 도시화 문제들을 해결하고 새로운 부가가치를 창출할 것으로 기대되고 있으나, 스마트시티의 구축을 위해서는 다양한 기기들이 연결되고 다양한 서비스가 연동되기 때문에 공격 침입 경로가 많아질 수 있으며 사용되는 ICT 기술들의 기존 보안 취약점이 승계될 수 있어 보안을 위한 대비책도 필요한 실정이다. 특히 단순 호기심이나 금전적 이득을 위해 사이버 공격을 수행하였던 과거와 달리 국가 수준에서 대상 국가에 대한 사이버 전쟁의 양상으로 심화되어 가고 있는 현황에서 스마트시티는 주요한 공격대상이 될 수 있으며 이러한 공격이 성공할 경우 사회혼란과 경제피해는 매우 클 것으로 예상된다. 실제로 스마트시티의 핵심 구성 도메인 중 하나인 스마트그리드 도메인(전력망)을 대상으로 한 사이버공격으로 인해 2015년 우크라이나의 광역정전과 2016년 우크라이나 키예프시의 140만 가구에 정전이 발생하는 등 도시 규모의 피해 사례가 발생되고 있다[2][3]. 또한 스마트시티의 다른 도메인들에 대한 공격 사례도 다수 발표되고 있으며, 스마트시티의 핵심 기술 중 하나인 사물인터넷기술에 대한 취약점, 공격 기법, 공격 사례 등도 여러 보안학회와 해킹대회에서 발표되고 있어 스마트시티의 보안에 대한 고려는 매우 필수적이다.

그러나 스마트시티의 경우 다양한 영역이 융합되며 해당 영역의 기기들은 사물인터넷 기술을 통해 연결되어야 하는 환경으로 보안시스템의 담당 영역과 기기들이 매우 많아지게 되어 단일의 보안 기술 및 시스템으로 보안을 대비하기에는 한계가 존재한다. 또한 이전 공격기술을 변형하거나 새로운 공격기술을 사용하는 사이버공격이 매년 증가하고 있으며, 무작위적인 대상에게 단기간 공격을 수행하던 예전 공격과는 달리 파급효과가 큰 대상을 목표로 지속적이고 지능적으로 공격하는 APT(Advanced Persistent Threat) 공격 형태로 변화하고 있어 사이버공격 징후를 사전에 탐지하여 사이버공격을 완벽하게 차단하는 것은 현재의 보안 인력과 사이버 방어 기술로는 한계인 상황이다.

이러한 한계점을 극복하기 위한 방안 중 하나로는 사이버위협정보(CTI, Cyber Threat Intelligence)를 수집 및 공유하는 체계를 구축하는 것으로 대표적인 사례로는 미국 CTIIC(Cyber Threat Intelligence Integration Center), NATO의 CDXI(Cyber Defence Data Exchange and Collaboration Infrastructure) 그리고 국내의 C-TAS(Cyber Threats Analysis System) 등이 있다.

스마트시티에서 사이버위협정보를 수집하고 공유할 경우 다양한 영역의 새로운 보안 위협정보를 신속하게 전파할 수 있기 때문에 보다 빠른 대응이 가능하여 전체 스마트시티의 보안성을 높일 수 있다. 또한 상위 관리 기기에서 하위 기기로 사이버위협정보를 전파하는 방식을 이용할 경우 보안 연산, 기능 그리고 모듈 등을 경량화 하는데 도움을 줄 수 있기 때문에 하드웨어 사양이 낮은 기기들에서도 활용 가능하여 사물인터넷 환경에 있는 스마트시티의 기기와 네트워크에 적용할 수 있을 것으로 예상된다.

따라서 본 논문에서는 스마트시티에서 사이버보안위협정보를 활용하는 방안으로 사이버보안위협정보를 수집하여 위협을 탐지하고 이후 공유하는 절차에 대해 모델링하였으며 이를 스마트시티의 주요도메인 중 하나인 스마트팩토리의 테스트베드에 적용함으로써 활용 예시를 제시하였다.

본 논문의 구성은 2장에서 사이버보안위협정보 관련 표준과 Threat hunting 모델에 대해 살펴본다. 3장에서는 Threat hunting 모델을 확장하여 사이버보안위협정보를 활용한 위협탐지 절차 모델을 도출하였으며 제 4장에서는 이를 스마트팩토리 테스트베드에 적용하였다. 마지막으로 제 5장에서는 결론과 향후 연구를 논의한다.

Ⅱ. 관련 연구

2-1 사이버보안위협정보 포맷 및 공유 표준

사이버 위협정보(CTI, Cyber Threat Intelligence)는 증거를 기반하는 지식으로, 기업의 IT나 정보자산에 위협이 될 수 있는 부분에 실행 가능한 조언을 콘텍스트나 메커니즘, 지표 등으로 제시하는 정보를 의미한다[4]. 이러한 사이버 위협정보를 협력업체 및 기관 간 서로 수집하고 공유하여 보안 시스템에 적용할 경우 다양하고 알려지지 않은 사이버 공격 징후를 사전에 탐지하여 사이버 공격을 차단하는데 큰 도움이 되고 있다. 따라서 세계 각국의 기관들과 보안 회사들은 사이버 위협정보를 공유하기 위한 협의체를 구성하고 있으며 사이버 위협정보의 포맷과 공유를 위한 전송프로토콜 등의 표준들도 제정되고 있다. 이 중 STIX(Structure Threat Information eXpression) /TAXII(Trusted Automated eXchange of Indicator Information) 표준의 경우 시스템 정보, 네트워크 정보, 어플리케이션 정보 등 다양한 정보를 객체로 사전 정의하고 있으며 다른 표준과의 연동이 가능하여 기존 IT영역뿐 아니라 스마트시티의 다양한 도메인에서 확장하여 활용가능하다.

1) STIX

STIX는 미국의 국토안보부에서 지원하여 개발한 사이버 위협정보 관련 표준으로 사이버 위협정보의 개념을 표준화하고 구조화하여 사이버 위협에 대한 일관된 분석과 자동화된 해석이 가능하게 한 정보 표현 규격이다[5]. STIX는 총 8가지 구성

요소(Observable, Indicator, Incident, TTP, ThreatActor, Campaign, ExploitTarget, COA)로 사이버 위협정보를 구조화하여 XML 언어로 표현하고 있으며 구성 요소 간 관계는 그림 1.과 같다. 각 구성요소의 설명은 다음과 같다.

- Observable: 사이버공간에서 관찰가능한 모든 이벤트 관련 구조체로 STIX의 기반 구성요소
- Indicator: 위협지표 관련 구조체로 'Observable'중 위협지표를 위한 데이터 모음
- Incident: 사고 관련 구조체로 'Indicator'중 사이버 공격으로 밝혀진 결과
- TTP(Tactics, Techniques and Procedure): 공격기법 관련 구조체로 'Incident' 배후의 전략 및 기술, 절차 등 공격기법
- Threat Actor: 공격자 관련 구조체로 TTP의 수행주체를 표현
- Campaign: 전체공격 관련 구조체로 Threat Actor의 의도를 달성하기 위한 1개 이상의 사건 및 TTP로 구성된 행위
- ExploitTarget: 취약점 관련 구조체로 Threat Actor의 TTP실행을 위한 SW 및 시스템, 네트워크, 설정 정보의 취약점을 표현
- Course of Action(COA): 대응 관련 구조체로 Exploit 대상 조치내역 및 사건 대응 등을 표현

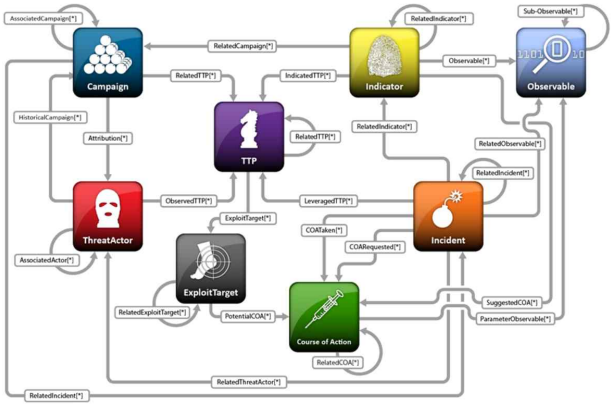

그림 1. STIX 구조
Fig. 1. STIX Structure

2) TAXII

TAXII는 사이버 위협정보의 표현 규격인 STIX를 실시간으로 공유하기 위한 자동 전송 규격으로 HTTP(HyperText Transfer Protocol) 및 HTTPS(HyperText Transfer Protocol over Secure Socket Layer) 프로토콜을 지원하며, 향후 XMPP(eXtensible Messaging and Presence Protocol) 및 SMTP(Simple Mail Transfer Protocol), SOAP(Simple Object Access Protocol) 등 멀티프로토콜을 지원 할 예정이다[6]. TAXII는 4가지 서비스(Push, Pull, Discovery, Feed Management) 규격을 이용하여 네트워크를 통해 전송한다. 이러한 서비스 기능을 구현하기 위한 TAXII 아키텍처는 TAXII 메시지의 송수신을 위한 네트워크 연결 기능을 담당하는 TTA(TAXII Transfer Agent), TAXII 메시지의 생산과 소비를 위한 기능을 담당하는 TMH(TAXII Message Handler), TTA와 TMH 기능 이외의 모든 TAXII 기능을 담당하는 TAXII Back-end로 3가지 구성요소를 가지나 기능별로 모듈화 한 것이기 때문에 구현에 있어서 나눠질 필요는 없다. TAXII의 주요 서비스는 다음과 같다.

- Push Service: 생산자가 소비자에게 정보를 전송하는 서비스 규격
- Pull Service: 소비자가 생산자의 정보를 요청하는 서비스 규격
- Discovery Service: 정보 정보의 알림을 위한 서비스 규격
- Feed Management Service: 정보구독 관리를 위한 서비스 규격

2-2 Threat Hunting 모델

Threat hunting이란 능동적이고 반복적으로 대상의 위협을 파악하여 보안대책을 수립하고 적용하는 일련의 프로세스들로 대상의 자산, 시스템 그리고 사용기술들을 이해하고 공격자의 TTP를 예측하는 반복적인 과정을 통해 기존 보안 시스템을 우회하는 고도화된 위협을 사전에 발견하고 격리할 수 있는 방안이다. Threat hunting은 공격자를 찾기 위한 침해지표(IoC, Indicator of Compromise) 정보를 수집하고 가설을 세워 분석함으로써 사이버공격절차인 사이버 킬 체인(Cyber Kill chain)의 사전단계에서 공격을 탐지하고 방어하는 것에 초점을 두고 있다. 이러한 Threat Hunting 기법의 주요 모델에는 Sqrrl사의 The hunting Loop[7]와 그림 2.와 같은 Dragos사의 Threat Hunt Cycle[8]이 있으며 이 두 모델의 Threat hunting의 절차 단계를 종합하면 아래와 같다.

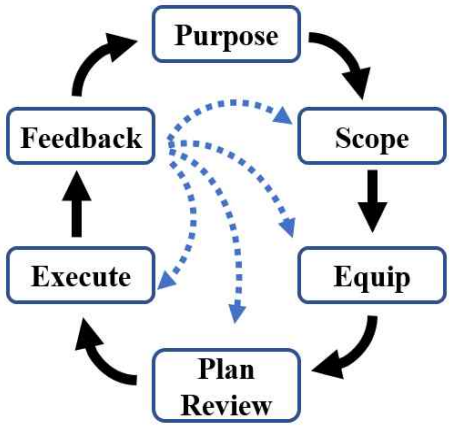

그림 2. 위협 헌팅 모델, Dragos 社
Fig. 2. Threat Hunt Cycle, Dragos INC

- 목적 설정 단계: Threat hunting을 하려는 목적을 명확히 수립하고 예상되는 결과물을 도출

- 범위 설정 단계: Threat hunting의 대상이 되는 시스템, 네트워크, 시설 그리고 사용기술 등에 대한 식별과 이해를 바탕으로 대상에 대해 가능한 위협 가설을 세움
- 도구 및 기술 조사 단계: Threat hunting에 사용될 수 있는 정보 파악과 새로운 정보의 수집 및 저장방안을 조사하고 가용할 인력 및 사용할 도구들을 식별하여 할당
- 계획 평가 단계: Threat hunting의 수립된 위협 가설의 검토와 함께 실행가능 여부 등을 파악하여 평가
- 실행 단계: Threat hunting을 수행하며 진행 결과물들을 수집
- 실행 분석 및 평가 단계: 실행 단계에 수집된 결과물을 분석하여 각 단계들의 개선방안을 도출

2-3 보안위협정보 외부 정보원

외부에서 수집된 다양한 형태의 사이버 위협정보로 활용하기 위해서는 획득된 데이터와 해당 데이터를 수집한 곳에 대한 신뢰성의 검증이 필요하나 이를 위해서는 보호대상 시스템에 대해 지식이 있는 보안전문가의 분석을 통해 수집된 보안 위협정보를 검증하고 해당 위협정보가 획득된 수집지에 적정 중요가중치를 주는 휴리스틱 방식이 선행되어야 한다. 그러나 보안위협정보공유 프레임워크를 위해 구조화되어 있는 보안위협정보를 제공하는 신뢰성이 있는 보안위협정보원을 활용할 경우 검증과 가공에 대한 절차를 생략할 수 있다. 사이버위협정보표현구조체인 STIX로 구조화하기 용이한 사이버보안위협정보를 제공하는 외부 정보원에는 ICS-CERT, NIST NVD(National Vulnerability Database), MITRE CVE(common Vulnerabilities and Exposures) 그리고 MITRE CRIT가 있다 [9][10][11][12].

Ⅲ. 스마트시티를 위한 사이버보안위협정보 활용 모델 도출

스마트시티는 매우 다양한 도메인을 포함하고 있기 때문에 사이버보안위협정보 수집 및 공유 방안의 도출을 위해서는 대상이 되는 네트워크 구성요소 및 구조를 국한할 필요성이 있다. 이후 사이버보안위협정보을 활용하여 위협을 탐지하는 절차 모델을 도출하여 선별된 대상에 적용하고자 한다.

3-1 적용 도메인 선정 및 네트워크 구성 모델 도출

스마트시티는 교통, 에너지 및 환경, 안전, 의료, 교육 등 다양한 도메인을 포함하고 있으나 해외에서는 국가지원사업 및 프로젝트의 약 70%를 에너지, 교통, 안전의 3개 중점 분야에 우선적으로 집중하여 기술 개발 및 적용하고 있으며 국내의 경우에도 에너지 분야의 스마트그리드, ESS(Energy Storage System), 제로에너지빌딩, 교통 분야 ITS(Intelligent Transport System) 등이 활발하게 스마트시티에 적용되고 있는 현황이다.[13] 따라서 본 논문에서는 스마트시티의 주요 중점 분야인 에너지, 교통, 안전 도메인을 적용 도메인을 대상으로 사이버보안정보 활용 방안을 적용하고자 한다. 이러한 에너지, 교통, 안전 분야는 일종의 제어시스템으로 산업제어시스템과 동일한 네트워크 구조를 따른다. 물론 각 도메인별 특성에 따른 차이점과 구현에 따른 차이점은 존재하지만, 이를 모두 반영하는 것은 불가능하기 때문에, 일반적인 ICS(Industrial Control System) 네트워크 구조를 본 연구의 네트워크 모델로 선정하였다. ICS 네트워크의 주요 참조 아키텍처에는 Purdue 모델, ISA 99 모델, NIST 800-82 모델 그리고 ICS-CERT의 참조모델이 있으나 계층구조의 세분화 정도의 차이를 제외한 네트워크의 구성요소 및 구성요소 간 연결 흐름은 동일하다. 이 중 그림 3.는 ICS-CERT의 ICS 네트워크 참조 아키텍처로 ICS 네트워크의 계층 별 특징들에 대해 가장 잘 식별하고 있기 때문에 이를 본 논문의 네트워크 모델로 선정하였다.

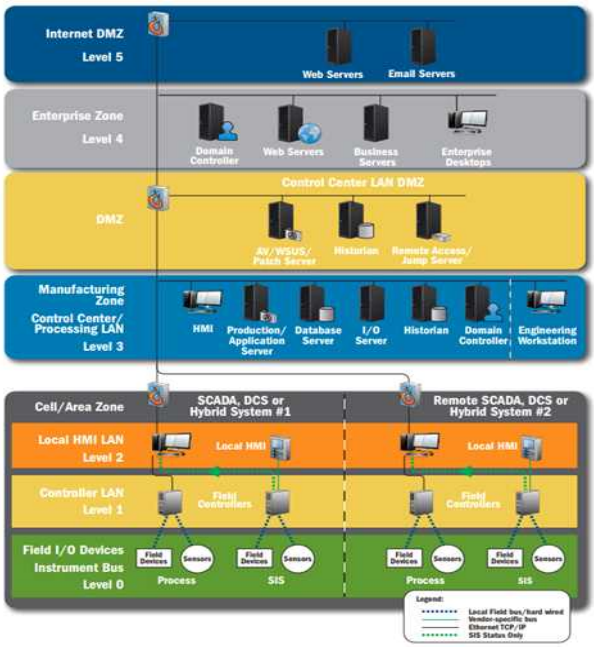

그림 3. 미국 ICS-CERT 보안 네트워크 참조모델[14]
Fig. 3. Recommended secure network architecture, US ICS-CERT[14]

3-2 사이버보안위협정보 활용 절차 모델

관련 연구의 Threat hunting 모델은 위협을 찾기 위한 수행 단계를 구분한 것으로 구체적인 절차 및 기술 등에 대해서는 명시하고 있지 않다. 본 논문에서는 이를 사이버보안위협정보 활용에 초점을 맞추어 세부 절차를 그림 4.와 같이 도출하였으며 각 절차의 설명은 다음과 같다.

- 범위 설정: 사이버보안위협정보의 수집을 위한 대상이 되는 시스템, 네트워크, 시설 그리고 사용기술 등에 대한 식별

- 내부/외부 사이버보안위협정보 수집: 대상의 내부 정보원와 외부 정보원에서 사이버보안위협 정보를 획득하는 단계로 외부의 정보원의 경우 정보원의 신뢰성 및 정보의 사실 검증이 필요하나 관련 연구에서 기술된 검증된 외부 정보원에서는 STIX 포맷의 검증된 사이버보안위협정보를 수집할 수 있음
- 사이버위협정보 분석: 수집된 사이버위협정보를 분석하여 대상의 위협 가능성이 존재하는지 확인하는 단계
- 위협 탐색: 분석된 사이버위협정보를 활용하여 대상의 위협을 실제로 탐색하는 단계
- 시스템 적용: 위협 탐색의 결과물을 토대로 보안 정책에 반영하거나 보안 시스템에 적용하는 단계
- 사이버보안위협정보 공유 단계: 확인된 보안위협 정보를 공유를 위한 포맷(STIX)으로 변경한 뒤 공유프로토콜(TAXII)을 사용하여 공유하는 단계
- 평가 단계: 사이버보안위협정보를 활용한 위협탐지과정의 결과물을 평가하며 이를 통해 각 단계의 개선방안을 도출하는 단계

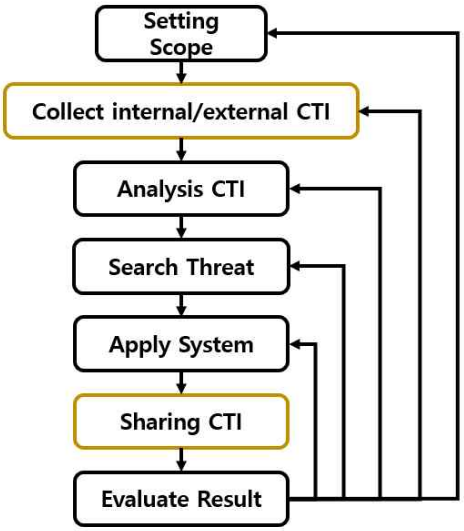

그림 4. 사이버보안위협정보(CTI) 활용 절차 모델
Fig. 4. Process Model for utilizing CTI

Ⅳ. 사이버보안위협정보 활용 모델 적용 연구

본 장에서는 사이버보안위협정보 활용 모델의 적용 예시로서 스마트시티의 주요 네트워크 구성모델인 산업제어시스템의 테스트베드에서 각 절차에 대한 세부 수행 내용을 제공한다.

4-1 분석대상 범위 설정

제 3장의 산업제어시스템 네트워크 구성모델은 Level 0에서 실제 생산 및 제어 직접적으로 관여하는 장치가 있으며 Level 1에서는 해당 장치로부터 데이터를 취득하고 Level 3에서는 데이터를 활용하여 모니터링 및 제어명령을 지시하는 장치로 구성되어 있다. 본 장에서는 N사의 스마트팩토리 연구를 위한 제조공정 자동화 테스트베드를 대상으로 사이버위협정보 활용 모델을 적용하였다. 해당 테스트베드는 실제 현장에서 사용되는 표 1.의 기기들로 계층적 네트워크를 구성하였으며 산업용 이더넷 프로토콜 중 하나인 Ethernet/IP을 통해 통신하고 있다.

표 1. 테스트베드 구성기기
Table 1. component device in testbed

Layer(Level)	Product Company	Product Name
Level 0(Actuator)	Allen-bradley	PowerFlex
Level 1(PLC)	Allen-bradley	CompactLogix
Level 2(HMI)	Allen-bradley	PanelView Plus

4-2 내부/외부 사이버보안위협정보 수집

일반 ICS 네트워크의 보안 위협 정보의 경우 ENISA(European Union Agency for Network And Information Security)의 문서[15]를 통해 취약성을 활용하였으며 스마트팩토리에 특화된 취약성 및 위협 분석에는 IIC(Industrial Internet Consortium)의 문서[16]와 PI 4.0(Platform Industrie 4.0)의 문서[17]를 참고하였다. 각 구성 기기의 알려진 취약점에 대해서는 CVE(Common Vulnerabilities and Exposures)를 참고하였다. 예를 들어 테스트베드의 Level 1 제품인 CompactLogix의 취약점 중 CVSS(Common Vulnerability Scoring System)가 높은 취약점은 아래 표 2.와 같다. 이 중 CVE-2012-6442 취약점에 대해 향후 절차들의 세부내용을 제공하고자 한다.

표 2. CompactLogix 제품의 CVE 취약점 예시
Table 2. CVE vulnerability of CompactLogix product

CVE number	description
CVE-2012-6442	remote attackers to cause a denial of service (control and communication outage) via a CIP message that specifies a reset
CVE-2012-6441	remote attackers to obtain sensitive information via a crafted CIP packet
CVE-2012-6440	man-in-the-middle attackers to conduct replay attacks via HTTP traffic
CVE-2012-6439	remote attackers to cause a denial of service (control and communication outage) via a CIP message that modifies the (1) configuration or (2) network parameters
CVE-2012-6438	remote attackers to cause a denial of service (NIC crash and communication outage) via a malformed CIP packet
CVE-2012-6437	not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image
CVE-2012-6436	remote attackers to cause a denial of service (CPU crash and communication outage) via a malformed CIP packet
CVE-2012-6435	remote attackers to cause a denial of service (control and communication outage) via a CIP message that specifies a logic-execution stop and fault

4-3 사이버위협정보 분석

CVE-2012-6442 보안 취약점은 공격자가 그림 5.의 최하단의 Service Code 필드를 reset 명령어로 설정한 CIP message를 공격 대상 기기에 지속적으로 보낼 경우 기기의 재설정이 반복되기 때문에 시스템의 가용성이 저해되는 것이다. 해당 취약점에 사용되는 공격 패킷은 정상 포맷과 명령을 사용하기 때문에 테스트베드에서 공격이 수행될 경우 방어하지 못하고 공격이 성공할 확률이 높아 위협가능성은 매우 높다고 판단된다.

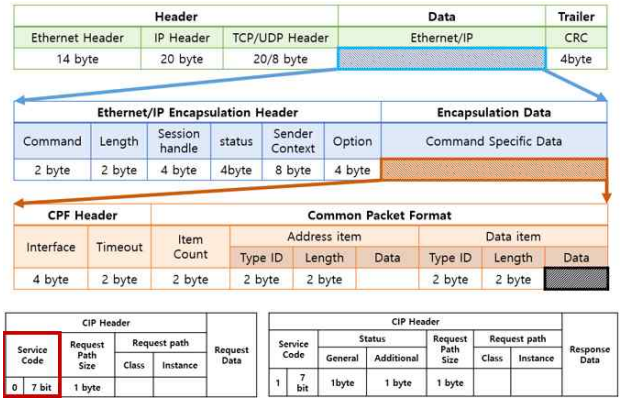

그림 5. 산업용 이더넷 프로토콜(Ethernet/IP)의 패킷 필드
Fig. 5. packet field of Ethernet/IP protocol

4-4 사이버위협 탐색

테스트베드에는 보안시스템이 적용되지 않아 표 3.과 같은 주요 산업용방화벽과 침입탐지시스템들이 테스트베드에 구축되어 있을 경우를 가정하였다. 그러나 해당 보안제품들과 같이 대부분의 산업특화보안제품들은 Serial 기반의 기존 산업용 네트워크프로토콜을 대상으로 하고 있어 테스트베드에서 사용되고 있는 IP 기반의 Ethernet/IP 통신 프로토콜은 지원하지 않는 경우가 많다. 또한 CVE-2012-6442 보안취약점의 경우 정상적인 CIP 메시지 형식과 명령어를 악용한 취약점으로 MAC 및 IP 기반의 단순한 탐지규칙으로는 발견하기 어려워 위협 탐색이 되지 않았다고 가정하였다.

표 3. 산업용 보안 제품 예시
Table 3. Examples of industrial security products

category	company	product name	control level
Firewall	Belden Security	Tofino SA	L2,1
	ETRI	IndusCAP	L2,1
	NSR	F.Switch	L2
IDS/IPS	Digital Bond	Quickdraw	L2,1
	NSR	anomaly detection	L2
	Radflow	iSID	L2,1

4-5 시스템 적용

해당 보안취약점에 대응하기 위해서는 보안 사이버위협정보 분석에서 식별된 바와 같이 Application 계층의 CIP 메시지의 명령어 필드의 값을 식별할 수 있어야 하며 메시지 포맷 및 명령은 정상이기 때문에 이를 판별하기 위한 방안이 필요하다.

제조 공정과 같은 산업제어시스템에서는 일반 IT 시스템에 비해 구성기기가 정적이며 동일한 프로세스가 지속적으로 수행되기 때문에 네트워크상에서 주고받는 패킷들도 주기적인 특성이 나타난다. 따라서 산업제어시스템에서는 화이트리스트 기반의 보안이 효과적이며 정상행위의 특성에 대한 세부 분석이 필요하다.

이를 위해 테스트베드에서 정상 환경의 제조 공정 네트워크 패킷을 수집하였으며 주요 특성을 파악하기 위해 NSL-KDD의 41개 feature 중 산업네트환경을 고려한 feature를 선별하여 클러스터링을 수행하였다[18]. 사용된 클러스터링 알고리즘은 DBSCAN, K-means 그리고 hcluster이며 각 클러스터링 알고리즘을 사용한 결과는 그림 6.과 같다. 클러스터링을 결과의 분석을 통해 테스트베드의 네트워크 패킷 특성은 다음과 같다.

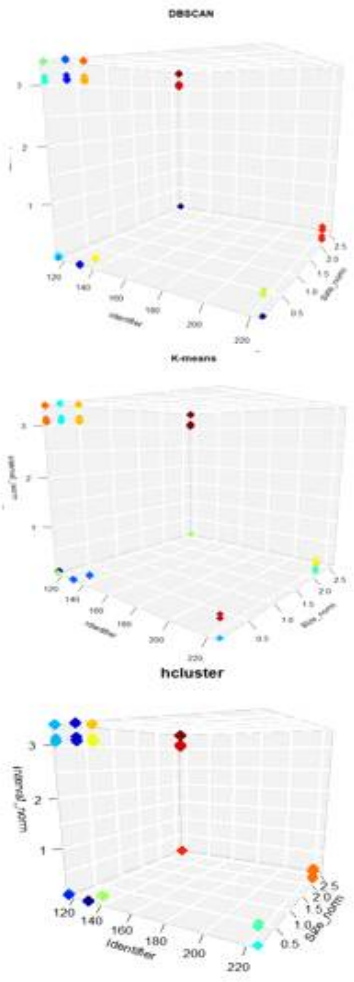

그림 6. 수집된 패킷의 클러스터링 결과
Fig. 6. Clustering result of collected packet

- 사용되는 명령어(Service Code) 종류의 한정: 수집된 Ethernet/IP 패킷의 경우 CIP Read Data와 CIP Get attribute all 명령어로 한정되어 있음
- 정적 기기 간 통신: 수집된 Ethernet/IP 패킷의 경우 IP주소 192.168.1.76과 192.168.1.10을 가진 기기 간 1:1 통신
- 고정된 Ethernet/IP 패킷 크기: CIP 0xAC class의 CIP Read Data의 Request 패킷 사이즈는 102/106 byte이며 Response 패킷 사이즈는 462 byte로 고정이며, CIP get attribute all의 request 패킷 사이즈는 100 bytes 그리고 response 패킷 사이즈는 130 bytes로 고정
- Ethernet/IP 패킷 interval Time: CIP Get Attribute ALL 명령은 5초 간격으로 CIP Read data 명령의 경우 0.5초 간격으로 보내고 있음

위와 같이 도출된 네트워크 패킷 특성을 바탕으로 MAC/IP 주소와 사용되는 명령어를 화이트리스트 규칙으로 추가하고 명령어 별 interval time을 측정하여 설정한 threshold를 벗어나는 패킷을 탐지할 경우 CVE-2012-5422 보안 취약점을 대응할 수 있을 것으로 파악된다.

Ⅴ. 결 론

본 논문에서는 스마트시티에서 사이버보안위협정보를 활용하기 위해 사이버보안위협정보를 수집하고 이를 위협탐지에 활용하며 다시 공유하는 절차에 대한 모델을 제시하였다. 이후 스마트시티의 주요 네트워크 환경에 대한 테스트베드에서 제안 모델의 각 단계에 맞추어 수행 예시를 제시함으로써 향후 스마트시티의 다양한 도메인에 실 적용에 있어 활용되고자 하였다.

하지만 외부 사이버보안위협정보를 자동으로 수집하고 검증하며 내부 사이버보안위협정보와 통합하여 사용자가 쉽게 분석할 수 있도록 제공하는 연구와 위협에 대한 분석이 완료 후 이를 자동으로 사이버보안위협정보 포맷 표준인 STIX로 변환하여 TAXII 프로토콜을 통해 공유하는 연구가 추가로 필요할 것으로 판단된다.

감사의 글

본 연구는 2018년도 산학협동재단의 학술연구 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

참고문헌

[1] ACT ON THE PROMOTION OF SMART CITY DEVELOPMENT AND INDUSTRY, Act No. 15309 (Dec. 26, 2017), Ministry of Land, Infrastructure and Transport

[2] Robert M. Lee, Michael J. Assante and Tim Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” SANS & E-ISAC, Technical Report, Mar. 2016

[3] Anton Cherepanov, “WIN32/INDUSTROYER A new threat for industrial control systems,” ESET, Technical Report, Jun. 2017

[4] WEBROOT, “Threat Intelligence: What is it, and How Can it Protect You from Today’s Advanced Cyber-Attacks?,” Gartner, Technical Report, 2014

[5] S. Barnum, “Standardizing cyber threat intelligence information with the structured threat information expression(STIX),” The MITRE Corporation, Jul. 2012.

[6] J. Connolly, M. Davidson and C. Schmidt, “The trusted automated exchange of indicator information (TAXII),” The MITRE Corporation, Feb. 2014.

[7] Sqrrl, “Hunt Evil: Your Practical Guide to Threat Hunting“, contents Pub, 2017

[8] Dan Gunter, Marc Seitz, “A Practical Model for Conducting Cyber Threat Hunting,” SANS, Mar. 2019

[9] ICS-CERT Alerts website, https://ics-cert.us-cert.gov/alerts

[10] NIST NVD website, https://nvd.nist.gov/

[11] MITRE CVE website, https://cve.mitre.org/

[12] MITRE CRIT website, https://github.com/crits

[13] Jaeyong Lee, “Smart City Policy and Future Direction,” National Assembly Research Service, 2017.03.

[14] Mark Fabro, Ed Gorski and Nancy Spiers, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” DHS ICS-CERT, Sept. 2016

[15] ENISA, “Communication Network dependencies for ICS/SCADA Systems,” ENISA, Dec. 2016

[16] S. Schrecker, H. Soroush, J. Molina, M.Buchheit, JP LeBlanc, R. Marthin, F. Hirsch and A. Ginter, “Industrial Internet of Things Volume G4: Security Framework,” Industrial Internet Consortium, Sept. 2016

[17] Wolfgang Bokämper, “Industrie 4.0 Security Guidelines - Recommendation and Actions,” VDMA, 2016

[18] Shilpa lakhina, Sini Joseph, and Bhupendra Verma. "Feature reduction using principal component analysis for effective anomaly–based intrusion detection on NSL-KDD," *International Journal of Engineering Science and Technology*, Vol. 2, No. 6, pp. 1790-1799, 2010.

김현진(HyunJin Kim)

2014년 : 아주대학교 정보통신대학 정보컴퓨터공학과(공학사)
2016년 : 아주대학교 대학원 컴퓨터공학과 (석사)
2018년~현재 : 아주대학교 대학원 컴퓨터공학과 박사과정

※관심분야 : 산업제어시스템, 사이버보안 등

손태식(Taeshik shon)

- 2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)
- 2002년 : 아주대학교 정보통신전문대학원 졸업(석사)
- 2005년 : 고려대학교 정보보호대학원 졸업(박사)
- 2004년 ~ 2005년 : University of Minnesota 방문연구원
- 2005년 ~ 2011년 : 삼성전자 통신·DMC 연구소 책임연구원
- 2017년 ~ 2018년 : Illinois Insitute of Technology 방문교수
- 2011년 ~ 현재 : 아주대학교 정보통신대학 사이버보안학과 교수

※관심분야 : ICS/SCADA, DFIR, Anomaly Detection