Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.471

CTI 모델 활용 제어시스템 보안정보 수집 방안 연구

최 종 원,† 김 예 솔, 민 병 길‡
ETRI 부설연구소

A Study on ICS Security Information Collection Method Using CTI Model

Jongwon Choi,† Yesol Kim, Byung-gil Min‡
The Attached Institute of ETRI

요 약

최근 정부기관, 기반시설, 제조 기업 등의 제어시스템을 대상으로 사이버 위협이 빈번히 발생하고 있다. 이러한 사이버 위협에 대응하기 위해서는 제어시스템의 다양한 자산에서 발생하는 보안정보를 일괄 수집하여 상관관계 분석 등을 수행하고, 그 결과를 공유하는 CTI(Cyber Threat Intelligence) 도입이 필요하다. 이를 위해서 제어시스템의 보안정보 수집이 필요한데, 가용성이 최우선적으로 고려되는 제어시스템 특성상 PLC(Programmable Logic Controllers) 등과 같은 제어장치에 보안 솔루션 도입의 제약이 있어 보안정보를 수집하기에 어려움이 따른다. 또, 제어시스템에 존재하는 다양한 자산에서 발생하는 보안정보 포맷이 상이한 문제도 존재한다. 따라서 본 논문에서는 효율적인 제어시스템 보안정보 수집을 위한 방안을 제안한다. 기존 IT의 CTI 모델 중 제어시스템 도입에 용이한 CybOX/STIX/TAXII를 활용하여 제어시스템 자산의 보안정보를 수집할 수 있도록 포맷을 설계하였다. 포맷 설계 대상은 윈도우 및 리눅스 등의 범용 OS를 사용하는 제어시스템 자산의 OS 수준의 시스템 로그, 정보보호 시스템 로그, 제어시스템 PLC 관리를 위한 EWS(Engineering Workstation System) 응용프로그램 로그로 선정하였다. 또, 설계한 포맷이 반영된 보안정보 수집 시스템을 설계 및 구현하여 제어시스템 통합 관제 시스템 구축 및 CTI 도입에 활용할 수 있도록 한다.

ABSTRACT

Recently, cyber threats are frequently occurring in ICS(industrial control systems) of government agencies, infrastructure, and manufacturing companies. In order to cope with such cyber threats, it is necessary to apply CTI to ICS. For this purpose, a security information collection system is needed. However, it is difficult to install security solution in control devices such as PLC. Therefor, it is difficult to collect security information of ICS. In addition, there is a problem that the security information format generated in various assets is different. Therefore, in this paper, we propose an efficient method to collect ICS security information. We utilize CybOX/STIX/TAXII CTI models that are easy to apply to ICS. Using this model, we designed the formats to collect security information of ICS assets. We created formats for system logs, IDS logs, and EWS application logs of ICS assets using Windows and Linux. In addition, we designed and implemented a security information collection system that reflects the designed formats. This system can be used to apply monitoring system and CTI to future ICS.

Keywords: Industrial Control System, Cyber Threat Intelligence, Cyber Security Monitoring, Security Information Collection, Security Event and Log

Received(12. 13. 2017), Modified(01. 29. 2018), Accepted(01. 29. 2018)

† 주저자, jwchoi5790@nsr.re.kr
‡ 교신저자, bgmin@nsr.re.kr(Corresponding author)

I. 서 론

최근 정부기관, 기반시설, 제조 기업 등의 제어시스템을 대상으로 사이버 위협이 증가하고 있다. 2010년 이란 원자력 발전소를 대상으로 수행되었던 스턱스넷(Stuxnet)[1]을 비롯하여 2011년 듀크(Duqu)[2], 2015년 블랙에너지3(BlackEnergy3)[3] 등 특정 기관의 제어시스템을 대상으로 지속적으로 사이버 위협 행위를 수행하는 APT(Advanced Persistent Threat) 사례가 빈번히 발생하고 있다. 이러한 제어시스템은 사이버 사고 발생 시 국가적 재난, 혼란 등으로 직결되기 때문에 사이버 위협 행위자의 주요 표적이 되고 있다.

PLC, RTU(Remote Terminal Unit), HMI(Human Machine Interface), EWS[4] 등의 중요 제어기기 및 장비들이 주를 이루는 제어시스템에서 최근 운영의 효율성을 높이기 위해 다수의 IT 기술을 도입하려는 시도 또한 사이버 위협 증가의 원인이다. IT 기술 도입으로 제어시스템은 유기적으로 동작할 수 있도록 상호 통신을 수행할 수 있게 되었고, 운영 데이터를 네트워크를 통해 일괄 수집하기도 한다. 전 세계적으로 제어시스템 분야의 스마트화를 추진하기 위한 움직임이 가속화되고 있어 기존 IT 기술의 제어시스템 도입은 더욱 증가할 것으로 보인다. 이러한 제어시스템의 IT 기술의 도입은 제어시스템 운영에 있어 효율성 및 편의성을 증진시켰지만 반대로 사이버 보안 취약점 및 사고 발생 가능성을 높이는 결과를 가져왔다. IT 기술 도입으로 인해 외부와의 접점이 늘어나게 되었으며, 제어시스템 내부 또한 상호 네트워크를 통해 연결되어 있어 악성행위를 일으키는 Malware 등의 확산이 용이해졌기 때문이다. 따라서 제어시스템을 대상으로 수행되는 APT 공격에 대한 대응이 필요하다.

이러한 지능형 사이버 위협에 대응하기 위해서는 시그니처 기반 악성행위 탐지 등의 단일 보안솔루션으로 방어하기에는 한계가 있다. 제어시스템 내부 다양한 자산에서 발생하는 보안정보를 통합 수집하여 상관관계 분석 등을 수행하는 통합 보안관제 시스템을 구축해야 한다. 그러나 제어시스템 통합 보안관제 시스템 구축에는 두 가지 어려움이 존재한다. 첫째는 제어시스템에 존재하는 다수의 이기종 장비에서 발생하는 보안정보가 상이하여 수집 및 분석이 어렵다. 둘째는 제어시스템의 PLC, RTU 등의 제어장치는 고유한 운영체제 및 응용프로그램을 사용하여 보안정보를 수집하기 위한 솔루션을 직접 설치할 수 없다.

따라서 본 논문에서는 제어시스템의 계층적 구조에서 주로 범용 OS를 활용하는 EWS, HMI, 히스토리안 서버 등이 속한 영역을 대상으로 보안정보를 수집하기 위한 방안을 제시한다. 이때 기존 IT의 CTI 모델을 활용한다. 기존 IT 영역에서는 CTI를 위한 연구 수행 및 표준 제정 등이 활발히 수행되고 있으나 제어시스템을 포괄하는 연구 및 활동은 미비한 실정이다. 관련 표준을 분석하여 포맷 확장을 통해 추가 요구되는 이벤트 및 제어시스템의 보안정보 표현까지 수용할 수 있어야 한다. 또한 기존 IT의 CTI 모델을 활용하여 IT 사이버 위협과 더불어 제어시스템에서 분석된 사이버 위협을 함께 공유할 수 있어야 한다. 분석결과 CTI 모델 중 CybOX[5]/STIX[6]/TAXII[7]는 이러한 요구사항을 충족하였고 이를 활용하여 제어시스템 보안정보를 수집하기 위한 포맷을 추가 설계하였다.

본 논문의 구성은 다음과 같다. 2장에서는 본 연구의 배경에 대해 설명한다. 3장에서는 일반적인 제어시스템의 현황을 통해 보안정보 수집 방안에 대해 설명하고 포맷을 설계한다. 4장에서는 제안하는 시스템의 설계 및 구현에 대해 기술하며, 5장에서 결론을 맺는다.

II. 배 경

2.1 CTI 모델을 활용한 보안정보 수집

앞서 언급하였듯이 최근 제어시스템을 대상으로 다수의 APT 공격이 발생하고 있으며, 이러한 이유로 제어시스템에도 CTI의 도입이 필요하다. CTI는 APT 공격의 컨텍스트를 인식하고 이에 적절한 행위를 취할 수 있도록 정보를 제공하는 것을 말한다. 다시 말해 APT 공격 수행 과정에서 그 방법과 일련의 절차에 대한 지식을 공유하여 대응하는 것이다. 이를 위한 전제조건은 제어시스템에서 발생하는 모든 보안정보를 수집할 수 있어야 한다는 것이다. APT 공격은 다양한 보안 위협을 종합적으로 활용해 대상에 접근하기 때문이다. 이렇게 수집된 보안정보는 CTI 환경 구축에 중요한 역할을 차지한다.

Fig.1.처럼 수집·분석·공유의 사이클로 구성된 CTI에서 수집된 보안정보를 기반으로, 분석을 통해 APT 행위에 대한 지표를 생성하고 다른 기관과 공유한다.

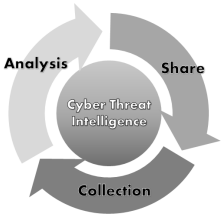


Fig. 1. Cyber Threat Intelligence Cycle

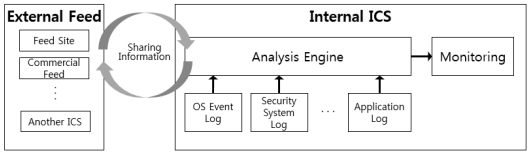


Fig. 2. Industrial Control System CTI Overview

이러한 APT 행위 지표는 위협 발생 시 정확하고 신속한 위협 탐지에 활용할 수 있으며, 사후에 피해 확산을 방지하기 위한 위협 대응에 활용할 수 있다.

따라서 제어시스템 보안정보를 통합 수집, 분석, 공유하기 위해서는 공통 정보 표현 및 교환 포맷이 필요하며 기존 IT 영역의 CTI 모델을 활용하여 이를 해결할 수 있다.

기존 IT 영역에서는 목적과 활용영역에 따라 다양한 정보표현 및 교환 표준[8-11]이 개발되었다. 기존 IT 장비 또한 다수 도입되어있는 제어시스템의 특성상 이러한 표준을 활용할 경우 기존 IT 영역의 보안정보를 수집 및 교환할 수 있을 뿐만 아니라 제어시스템 특화 보안정보까지 수집 및 교환할 수 있어 도입 시 효율성을 극대화할 수 있다.

관련 다양한 표준 분석 결과 CybOX/STIX/TAXII 모델이 제어시스템 적용에 가장 적합하였다. 다음 절에서는 CTI 제어시스템 적용 고려사항에 대해 알아보고 CybOX/STIX/TAXII를 제어시스템에 적용하고자 하는 이유에 대해 이어 설명한다.

2.2 CTI 모델 제어시스템 적용 고려사항

CTI 모델의 제어시스템 도입을 위하여 고려사항이 존재한다. CTI 모델을 통해 기존 IT의 보안정보를 충분히 표현할 수 있어야 한다. 또, 추가 식별되는 보안 이벤트 및 제어시스템 특화 정보를 표현하기 위한 확장 기능을 포함하고 있어야 한다. 마지막으로 위협 공유 시 다른 표준을 통해 생산된 지표 또한 수용할 수 있어 함께 공유할 수 있어야 한다.

먼저 CybOX/STIX/TAXII에는 기존 IT영역에서 식별되는 시스템 정보(프로세스, 드라이브, 메모리 등), 네트워크 정보(주소, ARP 정보, 패킷 등), 어플리케이션 정보(웹, E-mail 등)를 표현할 수 있는 88개의 객체를 사전 정의한다. IT 자산이 다수 도입되어 있는 제어시스템에서도 이러한 객체를 즉각 활용하여 발생하는 보안정보 수집에 활용 가능하다.

또, 사용자가 객체를 생성하여 문서화할 수 있는 확장 기능을 가지고 있다. 제어시스템에는 기존 IT 영역에서 존재하지 않는 PLC, EWS, HMI 등의 자산이 존재하며 여기서 발생하는 보안정보 또한 포맷이 다양하다. 전송 프로토콜에 있어서도 Modbus, DNP3 등의 특화 프로토콜이 사용되며 이마저도 벤더사마다 환경에 맞게 수정하여 사용하는 경우가 대부분이다. 따라서 제어시스템 보안정보 포맷 설계 시 제어시스템 특화 정보를 포함하고 추가로 식별되는 정보도 포함하는 확장 기능이 반드시 필요하다.

CybOX/STIX/TAXII의 또 다른 장점은 다른 시스템에서 생성해낸 지표를 활용할 수 있다는 것이다. 특정한 위협상황 발생 시 그 위협을 식별할 수 있도록 다양한 표준에서 지표를 각각 생성하는데 CybOX는 이러한 지표까지 공유할 수 있는 기능을 지원한다. 이 경우 해당 지표는 다른 표준을 사용하는 도구에서 동작함은 물론이고 STIX에서도 이를 활용할 수 있다. 예를 들어 다른 표준에 맞게 정의된 스턱스넷의 위협 지표를 수정할 필요 없이 CybOX/STIX/TAXII에서도 활용 가능하다.

2.3 CybOX/STIX/TAXII Project

IT 영역의 CTI의 필요성을 인지한 미국 국토안보부에서 사이버 위협 정보 공유 체계를 정립하고 MITRE에서 개발을 하였다. 금융, 지자체, FBI, US-CERT 등 정보보호 산업군에서 주로 활용하고 있으며 규격 및 포맷을 공개하고 있다. 해당 프로젝

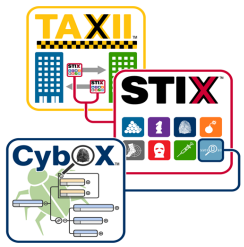


Fig. 3. CybOX/STIX/TAXII Relationship[5-7]

트는 사이버 관측 정보 표현 규격(CybOX, Cyber Observable eXpression), 사이버 위협 정보 표현 규격(STIX, Structured Threat Information eXpression), 사이버 위협 정보 전송 규격(TAXII, Trusted Automated eXchange of Indicator Information)으로 세분화하여 표준을 제작하였다.

이를 통해 각 조직에서 사용하는 사이버 위협 정보 개념을 표준화 및 구조화하여 일관된 분석과 자동화된 해석이 가능하게 하였다. 본 절에서는 각각의 규격에 대해 설명한다.

2.3.1 CybOX[5]

운영하는 사이버 도메인에서 관찰되는 상태나 이벤트에 대한 정보를 표현하기 위한 규격이다. 각 제조사, 도메인마다 사이버 관측 정보에 대해 표현이 상이하여 발생하게 되는 일관성, 효율성, 상호 운용성이 떨어짐을 개선하기 위해 개발하였다. 해당 포맷은 사이버 보안에 특화된 정보는 아니지만, 사이버 위협 지능, 악성코드 분석, 보안 운영, 로깅, 보안정보 통합 분석, 위협 대응·공유, 포렌식 등 다양한 분야에서 활용할 수 있는 공통 플랫폼을 제공한다.

CybOX는 확장성을 보장하기 위하여 식별되는 정보를 사용자가 직접 객체를 설계하여 문서화할 수 있도록 구현되었다. 이를 위해서 객체 설계 방법 및 규칙을 정의하여 제공하고 있으며 이를 기반으로 관측되는 상태나 이벤트를 표현할 수 있는 88개의 객체를 사전 정의하여 공식 배포하고 있다. 해당 객체는 호스트 관련(파일, 네트워크, 시스템), 네트워크 관련, 기타 정보(API, 제품 등) 등을 표현한다.

2.3.2 STIX[6]

각 조직에서 사용하는 사이버 위협 정보 개념을 표준화 및 구조화하여 일관된 분석과 자동화된 해석이 가능하게 한 정보 표현 규격이다. 이를 위하여 8개의 구성요소로 위협정보를 구조화하고 있다.

먼저 Observable은 모든 사이버 보안 이벤트와 관련된 CybOX 기반 기본 정보이다. 제어시스템의 PLC, DCS, HMI 등의 자산과 각 자산에서 발생한 로그, 경고 등도 Observable로 표현되어 STIX에서 활용한다.

Indicator는 발생한 로그 및 이벤트 등을 패턴화하고 해당 패턴을 통해 관련 사이버 위협이 발생 하였다고 판단할 수 있는 조건을 지정한다.

Incident는 Indicator 중 사이버 공격으로 밝혀진 정보를 표현한다. 실제 발생한 스턱스넷, 듀크, 블랙에너지3도 Incident에 의해 표현된다.

TTP(Tactics, Techniques and Procedure)는 Incident를 수행하기 위한 전략 및 기술, 절차 등을 표현한다. APT 공격 수행에 활용된 웜, 네트워크를 통한 전파기술, 일련의 과정 모두 TTP를 통해 표현된다.

ThreatActor는 TTP를 수행한 주체와 분석 결과 추정된 수행 주체의 의도 등을 표현한다.

Campaign은 ThreatActor가 목표달성을 위해 수행한 행위를 표현하는데 1개 이상의 Incident와 TTP로 구성된다.

ExploitTarget은 TTP 실행을 위한 소프트웨어 및 시스템, 네트워크, 설정 정보의 취약점 등을 표현한다.

COA(Course Of Action)은 ExploitTarget의 조치내역, Incident 대응 등을 표현한다.

이러한 정보는 Fig.4.와 같이 상호 연관되어 활용되며 타 기관과의 위협정보를 공유하여 APT 공격에 공동 대응할 수 있도록 돕는다.

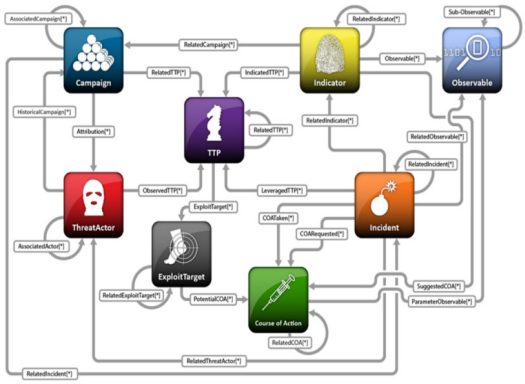


Fig. 4. STIX Structure[6]

2.3.3 TAXII[7]

MITRE에서 STIX, CybOX와 같이 개발된 보안정보 전송 프로토콜 및 플랫폼이다. 생성한 사이버 위협 정보를 자동을 표준화하여 전송하는 메커니즘으로 HTTP이 프로토콜을 사용한다. 전송을 위한 서비스 규격과 정보 공유 모델을 지원한다.

III. 보안정보 수집 대상 식별 및 포맷 설계

앞장에서 설명한 것과 같이 CTI 모델을 제어시스템에 적용하여 APT 공격에 대응할 수 있다. 그러나 제어시스템 각 기관의 운영 목적과 역할에 따라 각기 다른 자산이 도입되어 있어 공통된 정보를 수집하고 공유하기에 어려움이 존재한다. 따라서 제어시스템의 공통 모델을 도출하여 수집해야할 보안정보를 식별할 필요가 있다. 따라서 본 장에서는 제어시스템의 공통된 보안정보 수집 대상에 대해 알아보고 이를 통해 CTI 적용을 위한 포맷 설계를 수행한다.

3.1 제어시스템 보안정보 수집 대상 식별

ISA-99/IEC62443[12] 표준에서는 제어시스템을 일반적으로 기능과 레벨에 따라 zone으로 구분하여 계층적 구조를 제시한다.

레벨 0은 센서와 엑츄에이터 등의 현장장치로 구성된다. 센서는 온도 및 압력 등을 감지하고, 엑츄에이터는 밸브 및 모터를 조정하는 역할을 수행한다.

레벨 1은 RTU와 PLC 등의 제어장치로 구성된다. RTU는 현장장치로부터 데이터를 수집하여 아날로그 신호를 디지털 신호로 변환한 후 상위 레벨로 전송하고, PLC는 아날로그 또는 디지털 입출력 값을 바탕으로 주어진 로직에 따른 연산을 수행한다.

레벨 2는 제어시스템 운영자가 제어장치를 관리 및 제어할 수 있는 EWS, HMI 등의 장비와 제어시스템 운영 데이터를 관리하는 히스토리안 서버 등으로 구성된다.

마지막으로 레벨 3에는 제어시스템의 다양한 정보를 모니터링 하고 업무에 활용하는 내부 업무망이 존재한다.

앞선 사례 분석에서 살펴보았듯이 제어시스템 운영에 영향을 미치는 사이버 위협은 주로 레벨 1과 레벨 2에서 발생한다. 레벨 0은 디지털화가 되지 않아 주로 아날로그 신호를 사용하기 때문에 물리적 접근이 아니면 악성행위를 수행하기가 어렵다. 레벨 3은 주로 운영상황을 모니터링하기 위한 구간으로 하위 레벨과는 단방향 통신[13], 망분리 등의 솔루션이 도입되어 있어 제어시스템 동작에 직접적인 영향을 끼치는 사이버 위협을 수행하기에 어려움이 따른다. 따라서 제어시스템의 사이버 위협 행위를 분석하기 위해서는 레벨 1, 레벨 2의 보안정보를 수집할 수 있어야 한다.

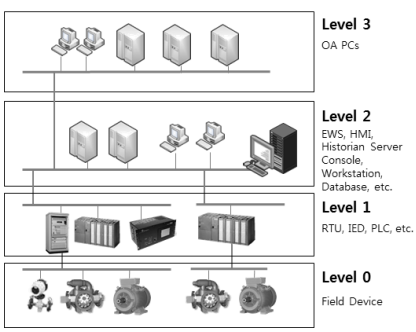


Fig. 5. General ICS Architecture

최근 제어시스템의 레벨 1 구간은 IP 및 이더넷 기술 등의 도입으로 디지털화가 진행되고 있다. 따라서 해당 구간에 보안 솔루션을 적용하기 위한 연구 및 개발이 진행되고 있다. 그러나 가용성 저해와 고유한 운영체제 사용의 문제로 보안정보를 수집하기 위한 에이전트 등의 솔루션을 직접 설치하기에 어려움이 따른다. 이와 같은 이유로 레벨 1구간은 대부분 침입탐지, 방화벽 등의 네트워크 수준[14, 15]의 보안 연구만 적용되고 있는 실정이다. 문제는 이러한 정보만으로 제어시스템 통합관제를 수행하기가 어려운 것이다. 더불어 해당 구간에 직접적으로 사이버 위협 행위가 수행되는 경우가 많지 않아 분석이 어렵기도 하다. 제어시스템 통합관제 수행을 위해서는 다른 구간의 시스템 및 네트워크 보안정보 등을 활용하여 상관관계 분석을 할 수 있어야 한다.

레벨 2에 존재하는 자산은 대부분 기존 IT 기술을 활용하고 있다. EWS, HMI, 히스토리안 서버 등은 윈도우 및 리눅스 등의 범용 OS를 활용하고 있다. IDS/IPS 등의 기존 IT 정보보호 시스템을 적용하기 위한 움직임도 활발하다. 또 제어시스템의 핵심 장비인 PLC를 관리하기 위한 응용프로그램이 EWS에 설치되어 운용된다. 여기서 발생하는 다양한 이벤트 및 로그 등의 보안정보는 제어시스템 통합관제 분석을 위한 훌륭한 자료가 된다. 대부분의 제어시스템 사이버 위협 취약점이 해당 구간에서 발생한다는 점도 이러한 정보를 수집해야만 하는 이유 중 하나이다. 해당 구간에서 발생 가능한 다양한 보안정보를 분석하고 이를 일괄 수집하기 위한 포맷을 설계할 필요가 있다. 따라서 본 논문에서는 제어시스템의 레벨 2 구간에서 수집 가능한 보안정보를 식별하고 이를 위한 포맷설계를 수행하였다.

3.2 제어시스템 보안정보 수집 포맷 설계

사이버 보안 위협에 대응하기 위해서 각기 다른 자산에서 발생하는 보안정보를 수집하여 분석할 필요가 있다. 대부분의 조직들은 자체적으로 이러한 보안정보 수집의 체계를 구성하려하고 있으나 조직 내부에 존재하는 자산의 벤더사 및 장비마다 상이한 보안정보가 수집되어 분석에 어려움이 존재한다. 이와 같은 이유로 CREST[16], NIST[17] 등의 기관에서 보안정보 수집에 활용되는 로그의 요구사항을 제시하고 있다. 관련 문서에 따르면 제어시스템에서 수집해야 할 보안정보는 OS 수준의 시스템 로그, 정보보호 시스템의 로그, 응용프로그램 로그로 분류할 수 있다.

본 논문에서는 제어시스템 보안정보 수집 포맷 설계를 위하여 OS 수준, 정보보호 시스템 로그, 응용프로그램 로그 중 대표를 선정하였다. OS 수준에서는 윈도우 이벤트 로그 및 리눅스 로그, 정보보호 시스템의 IDS/IPS 로그, 응용프로그램에서는 EWS 소프트웨어를 대상으로 수행한다. 선정한 대상의 보안정보를 상세 분석하여 포맷 설계를 수행하였다.

포맷은 CybOX XML 스키마로 개발되어 관리된다. 이는 다수의 각기 다른 제어시스템에서 공통된 정보를 수집할 수 있도록 라이브러리로 제작되어 배포될 수 있다.

포맷 설계 시 필드 또는 속성의 데이터타입을 결정할 때 기존 CybOX와의 호환을 위해서 CybOX에서 제공하는 기본 데이터타입과 우선 비교하여 활용하였다. CybOX의 기본 데이터타입을 활용하지 못할 경우에만 각 스키마 내부에 새로운 데이터타입을 정의하였다. 이를 통해 CybOX의 일관성을 유지할 수 있었으며 추후 통합관제 시스템에서 다양한 자산의 로그를 분석할 때 데이터타입을 통한 검색에 활용할 수 있다. 예를 들어 로그 발생 시각을 표현하는 데이터타입을 공동으로 사용하여 침해사고 발생 시 타임라인 분석에 활용할 수 있도록 한다.

3.2.1 윈도우 이벤트 로그

윈도우 운영체제 기반의 시스템에 사이버위협 발생 시 공격자의 행위를 추적하기 위해서 다양한 분석이 수행된다. 레지스트리 분석, USB 접근 기록, 인터넷 사용 기록 분석 등이 수행되는데 윈도우 이벤트 로그 분석은 중요도가 높아 가장 먼저 선행되어야할 분석 중에 하나이다. 윈도우 시스템은 이벤트 로그를 통하여 계정 로그인, 서비스 상태, 응용프로그램에서 발생한 로그 등을 통합 관리하고 있다.

윈도우 이벤트 로그는 기본적으로 시스템 로그, 보안 로그, 응용프로그램 로그로 분류한다. 시스템 로그는 주로 윈도우 시스템의 운영에 대한 정보가 저장된다. 시스템이 시작 및 종료되거나, 서비스가 실행 및 종료될 경우 이를 기록하기 때문에 분석에 활용될 수 있다. 보안 로그는 계정 생성, 로그온, 파일 생성 및 접근에 대한 정보를 기록한다. 어떠한 사용자 계정이 리소스를 생성 및 삭제 하였는지 등에 대한 분석을 수행할 수 있다. 응용프로그램 로그는 다양한 응용프로그램이 발생하는 이벤트를 기록한다.

이러한 정보를 바탕으로 침해사고 발생 시 분석가는 컴퓨터 부팅 시점, 로그온을 시도한 사용자, 리소스 사용 흔적, 서비스 실행 여부, 응용프로그램 이벤트 흔적 등을 시간별로 추적하여 분석할 수 있다.

윈도우 이벤트 로그의 주요한 Event ID는 Table 1.과 같다. 제어시스템의 레벨 2 영역에는 윈도우 환경 시스템이 다수 존재하는데 윈도우 이벤트 로그를 통합 수집하면 각 자산의 보안정보 상관관계 분석 및 CTI를 위한 지표 생성에 활용할 수 있다.

윈도우 이벤트 로그는 기존 CybOX에 포맷이 설계 되어있지만 윈도우 이벤트 로그를 실제 분석한 결과 기존 포맷 활용이 적합하지 않아 Fig.6.과 같이 재설계하였으며, 설계한 내용은 Table 2.와 같다.

Table 1. Important Event ID in Windows Event Log[18]

EventID	description
4624	logon success
4625	logon fail
4634	logoff
4720	create user account
4726	delete user account
4738	change user account
4732	add local group member
4688	create process
4689	exit process
4608	start windows
4609	shut down windows
4612	loss of windows event log

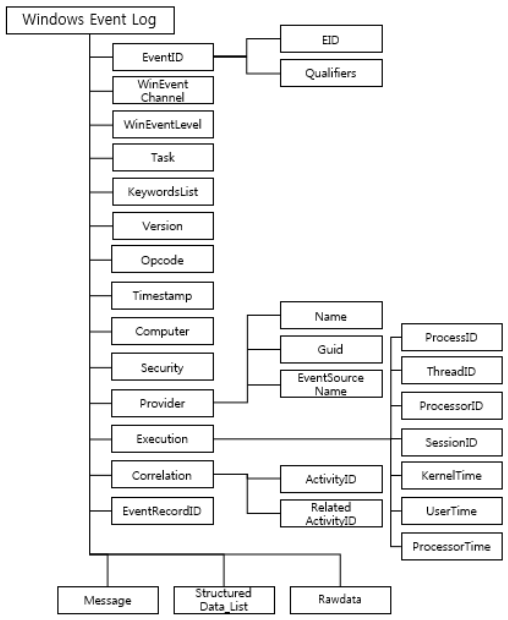


Fig. 6. Windows Event Log Diagram

Table 2. Important Fields in Windows Event Log

Field Name	Type
EventID	EventIDType
Channel	WinEventChannelTypeEnum
Level	WinEventLevelTypeEnum
Task	StringObjectPropertyType
Keywords List	KeywordsListType
Version	StringObjectPropertyType
Timestamp	TimeType
Computer	StringObjectPropertyType
Security	SecurityType
Provider	ProviderType
Execution	ExecutionType
ProcessID	UnsignedIntegerObjectProperty Type
ThreadID	UnsignedIntegerObjectProperty Type
ProssesorID	UnsignedIntegerObjectProperty Type
Correlation	CorrelationType
Event RecordID	StringObjectPropertyType
Message	StringObjectPropertyType
Structured_ Data_List	StructuredDataListType

데이터 분석 시 Task, Version, Opcode, Computer, Message와 같은 단순 문자열 정보일 경우 CybOX에서 제공하는 기본 데이터타입 중 StringObjectPropertyType을 활용하였다. Timestamp의 경우 TimeType을 활용하였고 EventRecordID 필드의 경우 숫자를 표현할 수 있는 LongObjectPropertyType을 활용한다. 나머지 필드의 경우 CybOX에 매핑되는 기본 타입이 존재하지 않아 새롭게 정의하였다.

3.2.2 리눅스 로그

일반적으로 리눅스 운영체제 기반의 시스템에서는 syslog 로깅 솔루션을 사용하여 로그를 기록하고 통합 관리한다. syslog는 일반적인 시스템 외에도 리눅스 계열의 네트워크 장비, 프린터 등 다양한 장치를 지원하며, 발생하는 다양한 유형의 이벤트와 로그를 로컬 또는 서버에서 통한 수집·관리할 수 있다. 또한 리눅스 시스템은 사용자의 로그인과 수행 작업에 관련하여 헤더파일을 따로 관리하며, 별로의 로그 파일로 관리하고 있다.

Syslog는 관리자가 로그를 생성하는 서브시스템과 로그의 심각도를 고려하여 로그를 수집할 수 있다. 수집하는 서브시스템은 Table 3.과 같이 계정 로그인, 인증, 부팅 및 커널, 시스템 정보 등을 수집할 수 있으며, local 서브시스템을 통해 원하는 응용프로그램의 로그를 추가적으로 수집 가능하다.

또한 리눅스 커널에서는 로그인에 관한 상세정보(utmp), 사용자별 최종 로그인 정보(lastlog), 실패한 로그인 내역(btmp), 로그인한 사용자의 작업 및 명령어 내역(pacct)에 관한 헤더 파일을 통해 따

Table 3. Major Subsystem of Linux

#	name	description
0	kern	kernel-level message
1	user	user-level message
2	mail	mail system
3	daemon	system daemon
4	auth	security & authentication
5	syslog	general message
9	cron	cron daemon
10	authpriv	security & privilage
11	ftp	ftp daemon
16-23	local 0-7	local using

로 관리한다. 수집된 정보는 바이너리 로그로 따로 관리하며 명령어를 통해 확인할 수 있다.

이러한 정보를 바탕으로 침해사고가 발생하면 분석가는 컴퓨터 부팅, 로그인, 사용자, 사용자 작업 내역, 서비스(daemon)와 시스템의 중요 로그를 확인할 수 있으며 이를 통해 사고 당시의 흔적을 시간별로 추적 및 분석할 수 있다.

Fig.7.의 Terminal, User_Name, Provider, Message의 단순 문자열 정보와 Timestamp는 윈도우 이벤트 로그와 마찬가지로 CybOX의 기본 타입을 활용하였고 나머지 필드는 타입을 정의하였다.

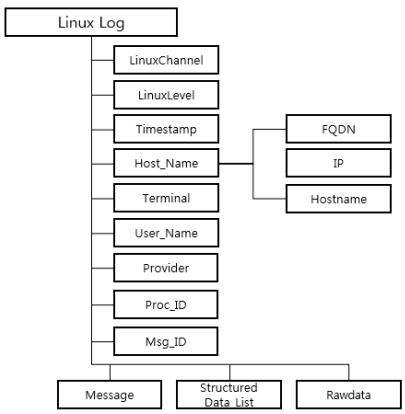


Fig. 7. Linux Log Diagram

3.2.3 정보보호 시스템 로그

제어시스템을 대상으로 지속적인 사이버 위협 행위가 발생하고 있어 다양한 제조사나 운영사 등에서 정보보호 시스템 도입을 고려하고 있다. 이러한 정보보호 시스템 도입에 대비하여 발생하는 알람 및 로그를 공통된 포맷으로 수집할 수 있어야 한다. 정보보호 시스템 중 IDS/IPS는 정의한 규칙을 통해 네트워크상의 이상행위를 탐지하는 대표적인 솔루션이다. 따라서 정보보호 시스템 중 IDS/IPS를 대상으로 발생 로그를 수집한다. 그 중 다양한 IDS/IPS SW와 장비에서 기반으로 사용하는 Snort[19]를 대상으로 보안 정보를 수집하였다.

Snort는 규칙을 통해 실시간 트래픽 분석 및 패킷 로깅을 수행할 수 있는 오픈소스 IDS/IPS이다. 이러한 IDS/IPS 정보를 수집하면 제어시스템 사이버 위협 상관관계 분석 등에 활용할 수 있다.

Snort 로그 중 Signature_ID, Src_IP, Dest_IP, Classification은 단순 문자열 정보로 CybOX 기본 타입에 매핑되었다. 마찬가지로 Port 번호나 Generation_ID는 숫자로 생성되는 정보로 해당 필드는 CybOX의 기본 타입으로 설계하였다. Timestamp의 경우 TimeType을 활용한다. 이외의 나머지 필드의 데이터타입은 새롭게 정의하였다.

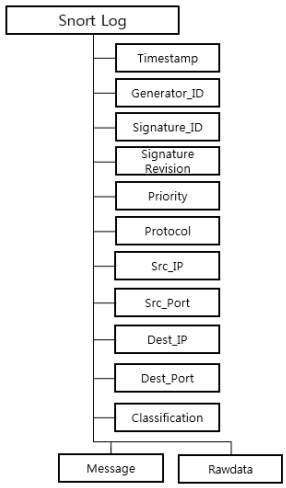


Fig. 8. Snort Log Diagram

3.2.4 EWS 응용프로그램 로그

제어시스템에는 산업 프로세스 제어를 위하여 PLC, DCS, HMI 및 현장장치 등을 활용한다. 그 중 PLC는 수십 개의 I/O(Input or Output) 모듈의 데이터를 바탕으로 주어진 로직을 실행시켜 현장장치가 작동할 수 있도록 하고, 그 결과를 연결된 네트워크를 통해 다른 시스템으로 전달하여 제어시스템이 유기적으로 동작할 수 있도록 하는 제어시스템 핵심 장비 중 하나이다. PLC는 자체적으로 로그를 생산하는데 이는 PLC와 연결된 EWS 소프트웨어에서 확인 가능하다. EWS 로그를 통하여 PLC 로직 변경, 메모리카드 정보, 상태 변화 등을 분석할 수 있기 때문에 제어시스템 통합 관제 시 해당 로그를 수집할 필요가 있다.

본 논문에서는 Siemense社[20]의 SIMATIC S7 PLC를 대상으로 EWS 로그 포맷 설계를 수행하였으며, 이를 위해 EWS 소프트웨어인 TIA Portal을 활용하였다. TIA Portal은 중앙 집중형 엔지니어링 프레임워크 제공하고 데이터 및 프로젝트, 자동화 작업에서 일관성을 보장하기 위한 소프트

Table 4. EWS Application Log Class[20]

Class	description
standard OB events	OB block standard events, such as the reason for restart an OB block
synchronous errors 1	synchronous errors in program logic
synchronous errors 2	synchronous errors during program execution
stop events and other mode changes	stop reason, mode change detection, etc.
status runtime events	parameters, interrupt information, etc.
communication events	connection information, memory information, etc.
diagnostic events for modules	module diagnostic events, sensor information, signal detection, etc.
standard user events	process information, command execution error, etc.

웨어이다. 이를 통하여 SIMATIC STEP 7에 포함하는 PLC의 로직을 개발하거나 업로드 할 수 있으며 Siemense社의 HMI 소프트웨어 개발을 위한 WinCC 또한 포함하고 있다.

해당 소프트웨어를 통해 온라인 액세스된 PLC에 대한 'Diagnostic Buffer'를 확인할 수 있다. Diagnostic Buffer는 PLC CPU의 메모리 영역인데 여기에 CPU에서 발생한 이벤트를(에러, 인터럽트, 시작/종료 등) 기록한다. Table 4.는 TIA Portal 소프트웨어서 수집 가능한 로그를 정리한 내용이다.

TIA Portal에서는 관련 로그를 클래스별로 분류하여 생성하고 있다. 다른 로그와 마찬가지로 해당 로그는 제어시스템에 발생한 APT 공격의 컨텍스트를 분석하는데 중요한 자료가 된다. 본 논문에서는 특정 벤더사의 EWS 응용프로그램을 대상으로 포맷 설계를 수행하였으나 추후 제어시스템의 다양한 벤더사의 소프트웨어에서 발생하는 로그를 수집할 수 있도록 포맷을 확장할 필요가 있다.

EWS 응용프로그램 로그의 단순 문자열 정보는 EventID, Event, Description이 있다. 다른 보안정보들과 마찬가지로 Timestamp 정보가 존재하며 EventNumber와 같은 숫자로 표현되는 정보 또한 존재한다. 이러한 필드는 모두 CybOX 기본 타입을 활용하고, 이외의 나머지 필드의 데이터타입

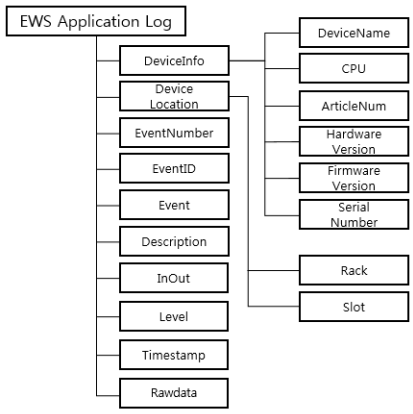


Fig. 9. EWS Application Log Diagram

은 새롭게 정의하였다.

IV. 보안정보 수집 시스템 설계 및 구현

4.1 보안정보 수집 시스템 설계

앞서 설계한 제어시스템 보안정보 수집 포맷을 활용하는 제어시스템 보안정보 수집 시스템에 대해 설명한다. 해당 시스템은 Agent와 Server로 구분된다. Agent는 제어시스템 내 윈도우 및 리눅스 등의 범용 OS를 사용하는 수집 대상에 직접 설치된다. 제어시스템 내부 다양한 자산에서 발생하는 보안정보는 해당 Agent를 통해 수집되어 Server로 일괄 수집되는 구조이다. 제어시스템은 보안을 위해 폐쇄망으로 운영되므로 보안정보 수집을 위해 단방향 솔루션이 적용된다. 해당 Agent 또한 보안정보를 수집하여 상관관계 분석 등에 활용하기 위한 목적으로 개발되며 보안정보 수집 외의 다른 정보는 교환할 수 없도록 설계되어야 한다. Agent는 크게 수집 모듈, 변환 모듈, 통신 모듈로 구성된다. Server는 통신 모듈, 데이터 저장소, Web UI로 구성된다.

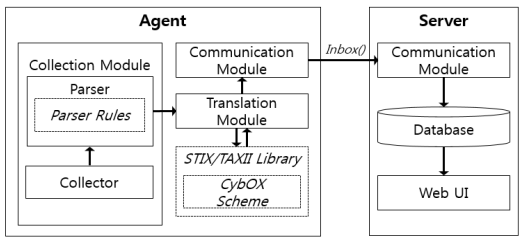


Fig. 10. Components of System

Agent의 변환 모듈에서 활용하는 STIX/TAXII 라이브러리가 탑재된다. 해당 라이브러리는 앞서 설계한 CybOX 제어시스템 관련 포맷을 반영하고 있다. 이 라이브러리는 다양한 자산에서 공통된 포맷으로 보안정보를 수집하도록 돕고, 기관 내부뿐만 아니라 다른 기관에서도 해당 라이브러리를 활용하여 공통된 포맷으로 보안정보를 수집할 수 있는 시스템을 구축할 수 있도록 편의를 제공한다.

4.1.1 Collection Module - Agent

수집 모듈의 수집기(Collector)는 설치 대상별로 구분하여 윈도우 이벤트 로그, 리눅스 로그, Snort 로그, EWS 응용프로그램 로그를 수집한다. 이러한 보안정보는 원본 파일 형태로 수집되기 때문에 포맷 변환을 위한 파서(Parser)가 필요하다. 파서에는 설계한 포맷 결과를 반영한 파서 규칙(Parser Rules)이 포함되어 있으며, 수집된 원본 파일은 이 규칙에 의해 각각의 필드로 구분된다. 이렇게 구분된 필드는 포맷 변환 모듈로 전달된다.

4.1.2 STIX/TAXII Library - Agent

변환모듈에서 활용하는 라이브러리이다. 수집한 보안정보의 포맷을 변환하기 위해서 이 라이브러리를 호출하여 사용한다. 이는 기존 CybOX/STIX/TAXII의 구조를 반영할 뿐만 아니라 앞서 제어시스템 보안정보 수집을 위해 추가 개발한 윈도우 이벤트 로그, 리눅스 로그, Snort 로그, EWS 응용프로그램 로그의 CybOX 스키마 또한 반영되어 개발되었다. 이 라이브러리를 바탕으로 다양한 자산의 보안정보를 공통 포맷으로 수집이 가능하다.

4.1.3 Translation Module - Agent

변환 모듈에서는 파싱된 데이터를 STIX/TAXII API를 호출하여 개발한 스키마에 맞춰 XML 구조의 데이터 포맷으로 변환한다. STIX 구조 상 CybOX를 포함하고 있고, STIX는 TAXII 규격에 의해 전송되기 때문에 순차적으로 변환이 수행된다.

4.1.4 Communication Module - Agent

TAXII 포맷으로 변환된 데이터를 TAXII 프로토콜을 이용하여 전달한다. 이때 TAXII에서 제공하는 Inbox Service를 활용한다. Inbox Service는 데이터 제공자가 데이터를 전송하는 서비스로 지정한 서버에 Inbox 메시지를 이용하여 서버에 전송하면 서버에서는 전송된 메시지를 처리한다. 이를 통해 포맷이 변환된 보안정보가 서버로 일괄 전송된다.

4.1.5 Server

통합 보안정보 수집 및 관리를 위한 서버는 보안정보 수집을 위한 통신 모듈, 수집된 보안정보를 저장하는 데이터베이스, 보안정보 활용을 위한 Web UI로 구성된다. 통신 모듈의 Inbox 메시지를 통해 전달된 보안정보는 서버 내 데이터베이스에 통합하여 저장된다. Web UI는 이 데이터베이스에 저장된 보안정보를 활용할 수 있도록 돕는다. 본 시스템에서는 보안정보 검색 기능을 제공한다. 이러한 기능은 보안정보 상호간의 상관관계 분석을 수행하는 통합관제 시스템에서 활용할 수 있다.

4.2 보안정보 수집 시스템 구현

4.1의 설계 내용을 기반으로 보안정보 수집 시스템을 구현하였다. Agent의 수집 모듈에서 획득한 데이터는 파서에 의해 분류되어 변환 모듈로 전달된다. 변환 모듈에서는 STIX/TAXII API를 호출하여 STIX 변환(CybOX 포함), TAXII 변환을 차례로 수행한다. 해당 결과는 Agent 내에 저장되어 Agent 측에서도 확인 가능하다.

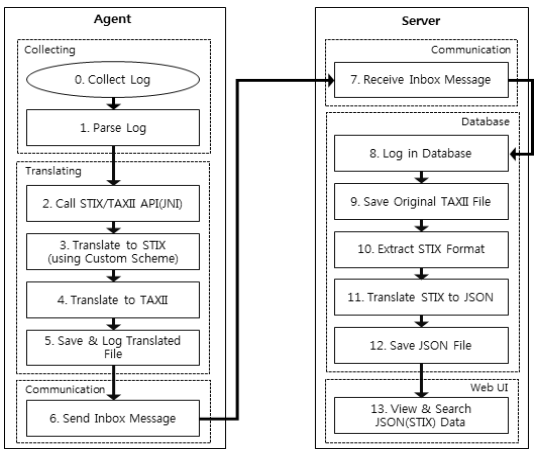


Fig. 11. Security Information Collection System Process

이어서 통신 모듈로 전달된 변환된 보안정보는 Inbox 메시지를 통해 Server로 전달된다. 해당 통신 모듈에는 필수적으로 단방향 솔루션이 도입되어야 한다. 해당 시스템의 통신 모듈은 보안정보 수집을 위해서만 동작하며 역방향으로 제어명령 등이 전송되지 않도록 설계되어야 한다. 더불어 전송하는 보안정보가 공격자에게 노출되지 않도록 암호화 및 무결성 검증 등의 보안 솔루션 또한 적용되어야 한다.

Server에 전송된 보안정보는 데이터베이스에서 관리된다. 원본 TAXII 파일과 STIX 포맷만을 추출하여 JSON 형태로 동시에 저장 및 관리한다. Fig.12.는 Server에서 확인 가능한 결과물 예시이다. 리눅스 로그를 수집한 결과물로 사전 정의한 필드와 타입에 맞추어 보안정보가 수집된 것을 확인할 수 있다. 이러한 보안정보는 Fig.13.과 같이 Server의 Web UI에서 확인 가능하다. 각 로그 타입으로 분류하였으며 필드 명, 타입 종류 등을 통해 검색이 가능하도록 구현하였다.

Fig. 12. Result File Translated to STIX

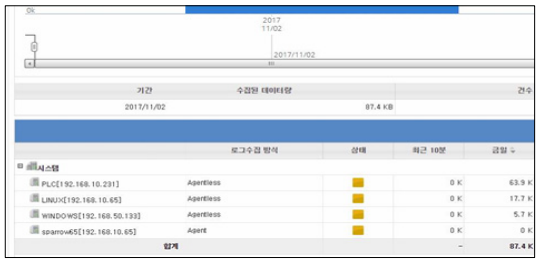


Fig. 13. Screen Capture of Server Web UI

4.3 구현 결과 및 기대효과

4.2의 Fig.13.의 Web UI를 통하여 수집된 보안정보를 조회할 수 있으며, 구현 결과는 다음과 같다.

Fig.14.는 윈도우 이벤트 로그 중 계정 로그오프 시도 시 발생하게 되는 보안(Security)로그가 수집된 결과이다. Fig.15.는 리눅스 로그 중 로그인 관련 정보를 포함하는 utmp 로그가 수집된 결과이다. Fig.16.은 Snort가 ICMP 패킷을 탐지한 결과를 로그로 수집한 결과이다. 마지막으로 Fig.17.은 EWS 응용프로그램에 연결된 PLC의 전원이 꺼질 경우 발생하는 로그를 수집한 결과이다. 개발한 보안정보 수집 시스템을 통해 제어시스템 내부의 다수의 자산에서 발생하는 윈도우 이벤트 로그, 리눅스 로그, 정보보호 시스템 로그, EWS 응용프로그램 로그를 동일한 구조로 수집 및 관리할 수 있음을 확인할 수 있다.

Fig. 14. Screen Capture of Windows Event Log

Fig. 15. Screen Capture of Linux Log

Fig. 16. Screen Capture of Snort Log

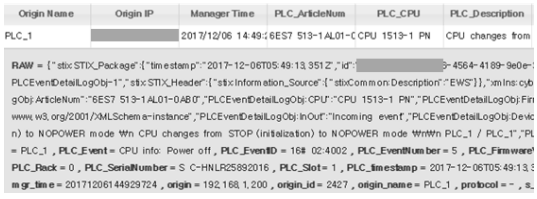


Fig. 17. Screen Capture of EWS Application Log

수집된 정보는 SIEM(Security Information and Event Management)의 분석엔진 등에서 보안정보 상관관계 분석에 효율적으로 활용할 수 있으며, 제어시스템 사이버 위협 분석가 및 의사 결정자가 제어시스템 CTI를 위한 지표 생성을 위해서도 활용 가능하다. 또한 보안정보 수집 시스템의 포맷 변환 라이브러리는 제어시스템에 새로운 자산을 도입할 때 해당 자산의 보안정보를 추가 수집하기 위해 활용할 수 있으며, 타 기관과도 동일한 구조로 보안정보를 자동으로 공유할 수 있도록 활용할 수 있다.

최근 제어시스템 대상 APT 공격이 발생하면서 Westinghouse社[21]의 Westinghouse SIEM, Rafael社[22]의 SCADA Dome 등과 같은 보안관제 솔루션이 개발되고 있다. 그러나 이러한 솔루션은 단일 기관을 대상으로 보안 관제를 수행하는 한계가 존재한다. 특정 사이트의 제어시스템 보안정보 수집만으로 APT 공격에 대응하기에는 데이터가 불충분하다. APT 공격 대응의 핵심은 다양한 기관에서 발생한 사이버 위협에 대한 데이터를 축적하여 다른 기관에서는 동일한 피해를 입지 않도록 관련 정보를 공유하는 것이다. 다시 말해 다양한 기관에서 공통적으로 사용하고 있는 제어시스템 자산의 보안정보를 수집하여 APT 공격에 공동 대응할 필요가 있다. 본 논문에서 제안한 방법으로 대다수 제어시스템에 동일하게 도입된 범용 IT 자산에서 발생하는 보안정보를 공통된 포맷으로 수집 및 공유한다면 사이버 위협에 공동으로 대응할 수 있는 기반을 마련할 수 있다. 더불어 CVE(Common Vulnerabilities and Exposures), OSVDB(Open Source Vulnerability Database), ICS-CERT(Industrial Control System Computer Emergency Response Team)와 같은 취약점 정보를 공유하는 사이트의 정보 또한 공유하는 시스템을 구축하여 제어시스템 CTI 환경을 구축할 수 있다.

V. 결론 및 향후 계획

본 연구는 제어시스템 CTI 도입을 위해 기존 IT 기술이 많이 도입된 구간을 대상으로 보안정보를 수집하기 위한 방안을 제시하였다. 해당 구간은 대부분의 제어시스템의 사이버 보안 취약점이 발생하는 구간으로 여기서 발생하는 보안정보를 일괄 수집하여 통합분석에 활용할 수 있어야 한다. 이때 보안정보 수집에 활용하기 위해 기존 IT의 CTI 모델을 활용한다. 기존 IT 기술이 많이 적용된 제어시스템을 대상으로 활용 가치가 높으며 포맷 확장으로 제어시스템 특화 정보 또한 수용이 가능하기 때문이다. 이를 검증하기 위해서 제어시스템 보안정보 수집 대상 중 윈도우 이벤트 로그, 리눅스 로그, Snort 로그, EWS 응용프로그램로그를 대표로 선정하여 포맷 개발을 수행하였고, 이를 활용하는 시스템을 개발하였다.

해당 시스템을 통해 보안정보 표현 불일치로 인하여 발생하게 되는 분석 및 공유의 어려움을 해결할 수 있다. 또한 포맷 변환 모듈은 라이브러리 형태로 개발하여 타 시스템 및 기관에 보안정보 수집 시스템 도입 시 즉시 활용하여 보안정보 시스템 구축의 초기 비용을 줄이는 효과가 있다.

향후에는 4종의 포맷 이외에 제어시스템에서 추가로 식별 가능한 보안정보를 수집하기 위한 포맷 설계가 필요하다. 또한, 각 기관의 내부 제어시스템 사이버 위협 정보뿐만 아니라 외부의 제어시스템 사이버 위협 정보를 수집할 수 있는 연구가 필요하다. CTI 환경에서는 양질의 다수 정보를 상호간에 공유하는 것이 핵심인데 CTI 모델을 활용하여 제어시스템 환경에서도 이와 같은 효과를 얻을 수 있을 것이라 기대한다.

References

[1] N. Falliere, L.O. Murchu and E. Chien, "W32. stuxnet dossier," White paper, Symantec Corp., Security Response, vol. 10, no. 6, pp. 29, Feb. 2011.

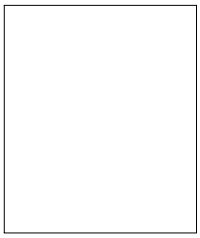
[2] E. Chien, L.O. Murchu and N. Falliere, "W32. duqu: the precursor to the next stuxnet," Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats, Apr. 2012.

[3] S. Raval, "BlackEnergy a threat to industrial control systems network security," International Journal of Advance Research in Engineering Science and Technology, vol. 2, no. 12, pp. 120-125, Dec. 2015.

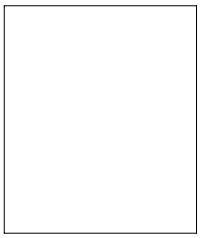
[4] K.A. Stouffer, J.A. Falco and K.A. Scarfone, "Guide to industrial control systems(ICS) security," NIST Special

Publication 800-82, May. 2015.
〔5〕 S. Barnum, R. Martin, B. Worrell and I. Kirilov, "The CybOX language specification," The MITRE Corporation, Apr. 2012.
〔6〕 S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression(STIX)," The MITRE Corporation, Jul. 2012.
〔7〕 J. Connolly, M. Davidson and C. Schmidt, "The trusted automated exchange of indicator information (taxii)," The MITRE Corporation, Feb. 2014.
〔8〕 Telecommunications Technology Association, "The System Log Information Message Exchange Format For The Security Control," TTAK.KO-12.0256, Dec. 2017
〔9〕 H. Debar, D. Curry and B. Feinstein, "The Intrusion Detection Message Exchange Format," RFC 4765, Mar. 2007.
〔10〕 R. Danyliw, J. Meijer and Y. Demchenko, "The Incident Object Description Exchange Format," RFC 5070, Dec. 2007.
〔11〕 W. Gibb and D. Kerr, "OpenIOC: back to the basics," https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html, accessed Feb. 2018.
〔12〕 ISA99/IEC62443, "Industrial automation and control systems security," https://www.isa.org/isa99/, accessed Feb. 2018.
〔13〕 Waterfall, "Unidirectional Security Gateways," https://waterfall-security.com/products/unidirectional-security-gateways, accessed Feb. 2018.
〔14〕 V. Igure, S. Laughter, and R. Williams, "Security issues in SCADA networks," Computer & Security, vol.25, issue 7, pp. 498-506, Oct. 2006.
〔15〕 S. Patel, G. Bhatt, and J. Graham, "Improving the cyber security of SCADA communication networks," Communications of the ACM, vol. 52 issue 7, pp. 139-142, Jul. 2009.
〔16〕 J. Creasey and I. Glover, "Cyber Security Monitoring and Logging Guide," CREST, ver. 1, 2015.
〔17〕 K. Kent and M. Souppaya, "Guide to Computer Security Log Management," NIST Special Publication 800-92, Sep. 2006.
〔18〕 Microsoft, "Appendix L:Events to Monitor," https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l—events-to-monitor, accessed Feb. 2018.
〔19〕 Snort, "Snort Users Manual," https://www.snort.org/documents, accessed Feb. 2018.
〔20〕 Siemens, "Totally Integrated Automation Portal," https://www. siemens.com/global/en/home/products/automation/industry-software/automation-software/tia-portal.html, accessed Feb. 2018.
〔21〕 Westinghouse, "Cyber security services: event management and intrusion prevention," http://www.westinghousenuclear.com/, accessed Feb. 2018.
〔22〕 Rafael, "Scada dome: cyber defense for industrial systems," http://www.rafael.co.il/, accessed Feb. 2018.

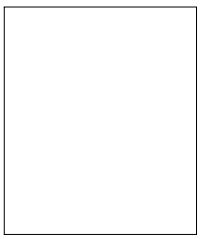
〈저자소개〉



최 종 원 (Jongwon Choi) 정회원
2013년 2월: 숭실대학교 컴퓨터학부 졸업
2015년 2월: 숭실대학교 컴퓨터학과 석사
2016년 8월~현재: ETRI 부설연구소 연연구원
〈관심분야〉 제어시스템 보안, 정보보호, 사이버 위협 인텔리전스



김 예 솔 (Yesol Kim) 정회원
2014년 2월: 단국대학교 컴퓨터학부 졸업
2015년 8월: 단국대학교 컴퓨터학과 석사
2016년 3월~현재: ETRI 부설연구소 연구원
〈관심분야〉 정보보호, 제어시스템 보안



민 병 길 (Byung-gil Min) 정회원
2002년 2월: 충북대학교 컴퓨터공학과 졸업
2004년 2월: 포항공과대학교 컴퓨터공학과 석사
2004년 3월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 제어시스템 보안, 침입탐지 시스템, 취약성 분석