ICS 환경에서의 사이버보안 훈련을 위한 사례 기반 보안 위협 시나리오 개발 방법론 연구

[1] 전규현, [2] 김광수, [3] 강재식, [4] 이승운, [5*]서정택

Study on Method to Develop Case-based Security Threat Scenario for Cybersecurity Training in ICS Environment

[1]GyuHyun Jeon, [2]Kwangsoo Kim, [3]Jaesik Kang, [4]Seungwoon Lee and [5*]Jung Taek Seo

요 약

기존 ICS(Industrial Control System)의 격리망 환경에 IT 시스템을 적용하는 사례가 계속 증가함으로써 ICS 환경에서의 보안 위협이 급격히 증가하였다. 보안 위협 시나리오는 사이버공격에 대한 분석, 예측 및 대응 등 사이버보안 훈련에서의 보안 전략 설계에 사용된다. 성공적인 사이버보안 훈련을 위해 유효하고 신뢰할 수 있는 훈련용 보안 위협 시나리오 개발 연구가 필요하다. 이에 본 논문에서는 ICS 환경에서의 사이버보안 훈련을 위한 사례 기반 보안 위협 시나리오 개발 방법론을 제안한다. 이를 위해 ICS 대상 실제 사이버보안 사고 사례를 분석한 내용을 기반으로 총 5단계로 구성된 방법론을 개발한다. 위협 기법은 MITRE ATT&CK 프레임워크를 기반의 객관적인 데이터를 사용하여 동일한 형태로 정형화한 후 위협 기법과 대응되는 CVE 및 CWE 목록을 식별한다. 그리고 CWE와 ICS 자산에서 사용 중인 프로그래밍내 취약한 함수를 분석 및 식별한다. 이전 단계까지 생성된 데이터를 기반으로 신규 ICS 대상 사이버보안 훈련용 보안 위협 시나리오를 개발한다. 제안한 방법론과 기존 연구간 비교 분석을 통한 검증 결과, 제안한 방식이 기존 방식보다 시나리오에 대한 유효성, 근거의 적절성, 그리고 다양한 시나리오 개발에 있어서 더 효과적임을 확인하였다.

Abstract

As the number of cases of applying IT systems to the existing isolated ICS (Industrial Control System) network environment continues to increase, security threats in the ICS environment have rapidly increased. Security threat scenarios help to design security strategies in cybersecurity training, including analysis, prediction, and response to cyberattacks. For successful cybersecurity training, research is needed to develop valid and reliable security threat scenarios for meaningful training. Therefore, this paper proposes a case-based security threat scenario development methodology for cybersecurity training in the ICS environment. To this end, we develop a methodology consisting of five steps based on analyzing actual cybersecurity incident cases targeting ICS. Threat techniques are standardized in the same form using objective data based on the MITER ATT&CK framework, and then a list of CVEs and CWEs corresponding to the threat technique is identified. Additionally, it analyzes and identifies vulnerable functions in programming used in CWE and ICS assets. Based on the data generated up to the previous stage, develop security threat scenarios for cybersecurity training for new ICS. As a result of verification through a comparative analysis between the proposed methodology and existing research confirmed that the proposed method was more effective than the existing method regarding scenario validity, appropriateness of evidence, and development of various scenarios.

Keywords: *ICS, Cybersecurity, Training, Methodology, MITRE ATT&CK, CVE, CWE*

[1] *가천대학교 정보보호학과 석사과정 (pengchan88@gachon.ac.kr)*
[2] *LIG 넥스원(주) 사이버전자전개발단 수석연구원 (kwangsoo.kim@lignex1.com)*
[3] *LIG 넥스원(주) 사이버전자전개발단 선임연구원 (jaesik.kang@lignex1.com)*
[4] *LIG 넥스원(주) 사이버전자전개발단 선임연구원 (seungwoon.lee@lignex1.com)*
[5*] *교신저자 가천대학교 컴퓨터공학부 컴퓨터공학전공 교수 (seojt@gachon.ac.kr)*

Received: Jan. 23, 2024, Revised: Feb. 08, 2024, Accepted: Feb. 16, 2024

I. 서론

Industry 4.0 의 등장으로 인해 급격히 발전한 산업제어시스템은 수력, 화력, 전력, 원자력 발전소 및 배전 시스템 등 발전 시설과 같은 산업 부문 및 기반시설에서 사용하는 여러 유형의 제어시스템을 포함하여 나타내는 용어이며, ICS(Industrial Control System)라고 한다. ICS 는 산업 환경에서의 프로세스를 규제하는 등 공정 운영을 위한 기술 및 시스템을 나타내는 OT(Operational Technology)환경의 세부 요소에 포함되며, SCADA(Supervisory Control and Data Acquisition), DCS(Distributed Control System), PLC(Programmable Logic Controller), HMI(Human Machine Interface), EWS(Engineering Workstation) 등 다양한 제어 요소들로 구성되어 있다[1][2]. ICS 는 오랜 기간 외부 네트워크와 연결되지 않는 격리망 환경을 유지하였지만, 간편한 유지보수 및 효율적인 ICS 관리·감독을 위해 원격 관리, IoT, 클라우드 컴퓨팅 등 IT 시스템을 ICS 환경에 적용하는 사례가 증가함에 따라 최근까지도 IT 와 OT 의 융합이 활발하게 진행되고 있다. 하지만, IT 네트워크와 ICS 가 연결됨에 따라 IT 환경에서의 사이버보안 위협이 ICS 환경에서도 발생 가능해졌고, 이는 IT 시스템에서의 보안 결함을 악용하여 ICS 환경을 공격할 수 있음을 의미한다. 실제로 2010 년, 이란 원자력 핵 시설을 대상으로 하는 Stuxnet 악성코드 공격으로 인해 약 1,000 개의 원심분리기가 파괴된 사례를 시작으로 Duqu(2011)[3], BlackEnergy(2015)[4][5][6][7][8], Industroyer(2016)[9][10][11], Darkside(2021)[12] 등 최근까지도 ICS 대상 사이버보안 사고로 인한 큰 피해가 계속 발생하고 있다[13][14][15].

이러한 ICS 환경에서의 보안 위협으로 인한 공정 중단, 시설 파괴, 인명 피해 등 실제 물리적인 보안 사고를 방지하기 위해 사이버보안 훈련을 진행하여 ICS 대상 사이버공격으로부터 보안 위협을 사전에 인지하고 적합한 방어 전략을 세워야 한다. 해당 과정에서 ICS 대상 사이버보안을 위해 보안 위협 시나리오가 사용되며 이는, 위협 기법 및 위협 행위를 탐지하여 적대자의 전술적인 행위 및 위협 대응 시나리오 설계 등 사이버보안 훈련에서의 보안 전략 설계에 핵심적인 역할을 수행한다. 보안 위협 시나리오는 적대자, 방어자, TTP(tactics, techniques, and procedures) 등 다양한 구성요소를 고려하여 설계되어야 한다. 이때, 실제 적대자의 위협 행위 프로세스와 유사할 수록 보안 위협 시나리오의 유효성 역시 높아지므로 시나리오에 대한 신뢰성을 높일 수 있다. 또한, 시나리오에 다양한 위협 전술 및 기법, 위협 벡터를 사용하여 복잡성 및 완성도를 증가시킬 경우, 더 많은 보안 결함 및 취약점에 대한 식별이 가능하므로 이후 발생할 여러 공격에 대한 방어 전략을 설계하는데 유용하다.

하지만, ICS 환경에서의 사이버보안 훈련을 위한 위협 시나리오 개발과 관련하여 체계적인 방법론에 대한 연구는 아직까지 부족한 실정이다. 일반적으로 정형화된 네트워크 및 시스템으로 구성된 IT 환경과는 다르게, ICS 환경에서는 SCADA, PLC, RTU 등 산업 시설에서 사용하는 다양한 특수 공정 장비와 Modbus, DNP3, PROFIBUS 등 산업용 프로토콜을 통한 통신 네트워크로 구성되어 있다. 이처럼, 서로 다른 수많은 공정 장비 및 네트워크 구성 환경을 각각 고려해야 하므로 완성도 높은 보안 위협 시나리오를 개발하는 것에 어려움이 있다 [1][2][13][16].

이와 관련된 기존 연구로는 먼저 Kim. D. H et al.[17]은 MTD(Moving Target Defense)를 활용하여 허니시스템의 능동적인 방어 전략을 구축하는 방안을 위한 과정에서 MITRE ATT&CK 기반의 위협 시나리오를 제작했지만, 시나리오 설계 기준과 사용한 취약점에 대한 자세한 내용을 파악하기 어렵다. Ahn. M. K et al.[18]은 사이버 전투실험 분석을 위한 모의 공격에서의 침투 시뮬레이션을 위해 사이버 킬체인 기법을 적용하였지만, 각 위협 단계별 정확한 분류와 TTP(Tactics, Techniques, and Procedures)를 자세하게 알 수 없었다. Liao, Y. C [19]는 ICS 환경을 위한 MITRE ATT&CK 기반 보안 위협 기법 통합 및 인프라 가용성을 위해 CVE, CICAT, NMAP 등을 활용하여 보안 위협 시나리오를 생성했지만, ICS 자산에서 사용하는 프로그래밍 언어를 고려하지 않았다. Hacks, S et al.[20] 보안 위협 시나리오를 시뮬레이션 하기 위한 MAL 기반 언어를 개발했지만 취약점 및 보안 약점에 대해 작성하지 않았으므로 다른 ICS 보안 위협 시나리오에 적용할 때 유효할 지 해당 연구에서는 잘 알 수 없다. 따라서, ICS 환경에서 실제로 유효하며 ICS 자산에서 사용 중인 프로그래밍 언어를 고려한 사이버보안 보안 위협 시나리오를 도출할 수 있어야 한다.

이에 본 연구에서는, ICS 환경에서의 사이버보안 훈련을 위한 사례 기반 보안 위협 시나리오

개발 방법론을 제안한다. 제안하는 방법론은 ICS 대상 실제 사이버보안 사고 사례를 분석한 내용을 기반하여 총 5 단계로 구성된다. 4 단계까지는 사례 분석으로부터 도출된 데이터들을 데이터베이스화하는 단계이다. 먼저, 사이버보안 사고 사례에서 위협 기법을 도출한다. 위협 기법은 MITRE ATT&CK 프레임워크를 기반의 객관적인 데이터를 사용하여 동일한 형태로 정형화한다. 이후, 위협 기법이 성공적으로 수행되기 위해 필요한 보안 결함을 식별하기 위해 CVE 및 CWE 목록을 사용한다. 그 중, 식별한 CWE 와 대응 가능한 ICS 자산에서 사용하는 프로그래밍내 취약한 함수를 분석 및 식별한다. 해당 과정을 통해 생성된 데이터는 데이터베이스화 하여 저장한다. 5 단계에서는 앞선 단계로부터 생성된 데이터를 기반으로 신규 ICS 대상 보안 위협 시나리오를 개발한다. 검증은 본 논문에서 제안한 방법론과 기존 연구간 비교 분석을 통해 진행했으며 그 결과, 제안한 방식이 기존 방식보다 시나리오의 유효성, 근거의 적절성, 그리고 다양한 시나리오 개발에 있어서 더 효과적임을 확인하였다. 본 논문이 기여하는 바는 다음과 같다:

- ICS 사이버보안 사고 사례를 분석을 통한 보안 위협 전술 및 기법의 정형화, 취약점 및 보안 약점 식별, 취약한 함수를 사용하는 훈련용 보안 위협 시나리오 개발 방법론 설계
- 도출된 데이터들의 데이터베이스화를 통한 다양하고 유효한 ICS 대상 사이버보안 훈련용 보안 위협 시나리오 생성
- 제안한 방법론과 기존 연구들간 정형화, 보안 결함, ICS 자산내 프로그래밍 언어, 시나리오 유효성, ICS 환경 여부를 평가 기준으로 비교 분석을 수행

본 논문은 다음과 같이 구성된다. 2 장에서는 배경 및 관련 연구, 3 장에서는 ICS 대상 사이버보안 훈련용 보안 위협 시나리오 개발 방법론, 4 장에서는 연구 결과, 마지막으로 5 장에서는 결론 및 향후 연구계획에 대해 기술하였다.

II. 배경 및 관련 연구

2.1 MITRE ATT&CK

Table 1. MITRE ATT&CK Tactics
표 1. MITRE ATT&CK 전술

Tactics	Descriptions
Resource Development	Involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting
Initial Access	Use various entry vectors to gain their initial foothold within a network
Execution	Result in adversary-controlled code running on a local or remote system
Persistence	Adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access
Privilege Escalation	Adversaries use to gain higher-level permissions on a system or network
Evasion	Adversaries use to avoid technical defenses throughout their campaign
Discovery	Adversaries use to survey your ICS environment and gain knowledge about the internal network, control system devices, and how their processes interact
Lateral Movement	Adversaries use to enter and control remote systems on a network
Credential Access	Stealing credentials like account names and passwords
Collection	Adversaries use to gather domain knowledge and obtain contextual feedback in an ICS environment
Command and Control	Adversaries use to communicate with and send commands to compromised systems, devices, controllers, and platforms with specialized applications used in ICS environments
Inhibit Response Function	Adversaries use to hinder the safeguards put in place for processes and products
Impair Process Control	Adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment
Exfiltration	Adversaries may use to steal data from your network
Impact	Adversaries use to disrupt, compromise, destroy, and manipulate the integrity and availability of control system operations, processes, devices, and data

MITRE ATT&CK(MITRE Adversarial Tactics, Techniques, and Common Knowledge)은 적대자의 위협적인 행위를 탐지하고 TTP 문서화 및 분류를 위해 2013 년에 개발된 프레임워크이다[21][22]. 이는 ICS, Mobile, IoT 등 다양한 환경 및 기술과 관련된 광범위한 분야의 다양한 사이버 위협에 대한 모델링 및 연구에 활용된다. MITRE ATT&CK 프레임워크의 핵심 구성 요소는 공격 수행을 위한 목표인 전술(Tactics), 전술적 목표를 위해 적대자가 수행하는 기법(Techniques), 전술적 목표를 달성하기 위한 구체적인 방법인 하위 기법(Sub-techniques), 기법 또는 하위 기법의 실제 사용을 나타내는 절차(Procedures), 마지막으로 위협 행위를 예방하고 보호하기 위한 완화(Mitigations)로 구성되어 있다.

[표 1]은 MITRE ATT&CK 의 전술 및 세부 설명을 나타낸 것이다. 전술은 자원 개발, 실행, 지속성, 탐색 등 공격 목표에 따른 적대자의 행동을 의미하며, 보안 위협 환경에 따라 Enterprise, Mobile, ICS 로 구분된다. 본 연구에서 사용할 전술은 MITRE ATT&CK for Enterprise 및 ICS 버전에서 중복되는 전술을 제외한 총 15 개이다.

2.2 관련 연구

Kim. D. H et al.[17] 은 MTD 를 활용하여 허니시스템 능동방어를 수행하기 위한 방법론을 제안했다. 총 5 단계의 단계별 능동방어 프로세스를 구성하였으며, 악성코드를 탐지한 후, 1 차적으로 적극적인 대응을 수행한다. 이후, 적대자가 위협 행위에 필요한 자원을 증가시키기 위해 MTD 기술을 사용하여 적대자를 기만한다. 그리고 위협 인텔리전스 정보를 수집 및 분석한 후, 공격 패턴 및 목표를 확인한다. 해당 프로세스를 구현 및 검증하기 위해 MITRE ATT&CK 기반의 보안 위협 시나리오를 제작했지만, 시나리오를 설계한 명확한 기준과 보안 위협 시나리오에서 사용한 보안 결함에 대한 설명이 존재하지 않아 자세한 내용을 파악하기 어렵다.

Ahn. M. K et al.[18]은 사이버 전투실험 분석을 위한 모의 침투 시뮬레이션을 위해 사이버 킬체인 기법을 적용하였다. 해당 과정에서 네트워크 구성 정보 기반의 시스템 및 네트워크 모델을 사용하였다. 그러나, 사이버 킬체인 프레임워크 특성상 제안한 보안 위협 시나리오를 통해 각 위협 단계별 정확한 분류와 TTP(Tactics, Techniques, and Procedures)를 잘 알 수 없다.

Liao, Y. C[19]는 ICS 환경을 위한 MITRE ATT&CK 기법 통합 및 인프라 가용성을 위한 보안 위협 시나리오를 생성하는 방법론을 제안했다. 해당 과정에서 ICS 대상 위협 기법을 다루기 위해 CVE, CWE 등을 MITRE ATT&CK 기법과 매핑하였다. 하지만, ICS 자산에서 사용하는 프로그래밍 언어의 취약점으로 인해 추가적인 위협 벡터가 발생할 수 있다.

Hacks, S et al.[20]은 보안 위협 시나리오를 시뮬레이션 하기 위한 MAL 기반 언어를 개발했다. 이후, MITRE ATT&CK 프레임워크를 기반으로 사이버보안 위협 시나리오 아키텍처를 설계하여 IT 및 OT 인프라에 대한 사이버 보안 평가 수행을 통해 사이버보안 위협에 대한 높은 안전성과 복원력을 목표로 하였다. 그러나, 연구에서는 취약점 및 보안 약점에 대해 확인할 수 없으므로, 다른 ICS 보안 위협 시나리오에 적용할 경우, 제안한 방법이 유효할 지에 대해 해당 연구에서는 잘 알 수 없다.

III. ICS 대상 사이버보안 훈련용 보안 위협 시나리오 개발 방법론

본 장에서는 사이버보안 훈련에 사용하기 위해 ICS 환경을 대상으로 하는 실제 사이버보안 사고 사례를 기반으로 보안 위협 시나리오를 개발하기 위한 방법론에 대해 설명한다. 먼저, 방법론의 단계별 구성요소에 대해 기술한다. 이후, 단계별 세부 과정에 대해 설명한다.

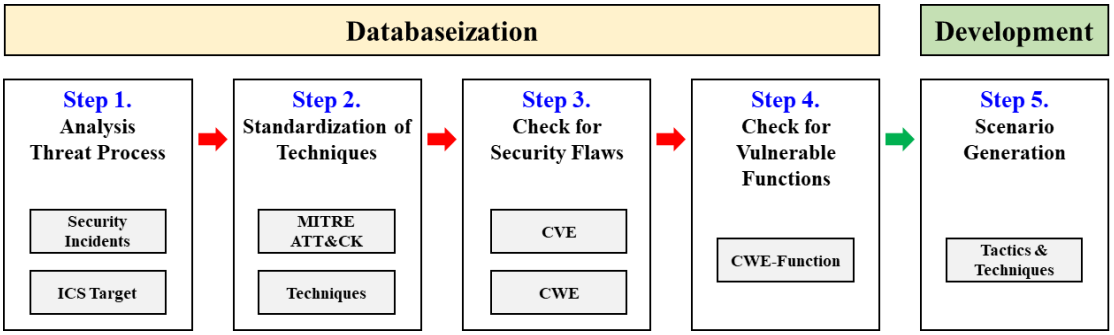


Figure 1. Methodology for Developing Security Threat Scenario for Cybersecurity Training in ICS
그림 1. ICS 대상 사이버보안 훈련용 보안 위협 시나리오 개발 방법론

제안하는 ICS 대상 사이버보안 훈련용 보안 위협 시나리오의 방법론은 [그림 1]과 같이 총 5 단계로 구성된다. 4 단계까지는 보안 위협 시나리오 개발을 위한 데이터베이스화 과정을 진행한다. 1 단계에서는 ICS 대상 실제 사이버보안 사고 사례를 선정하여 보안 사고 사례의 프로세스를 분석한다. 보안 사고 사례는 기술 보고서 및 관련 논문을 기반으로 분석하여 나타내었다. 2 단계에서는 분석한 보안 사고 사례에서 도출된 위협 기법을 MITRE ATT&CK 프레임워크를 사용하여 정형화한다. 3 단계에서는 위협 기법을 통한 성공적인 위협 기법의 수행을 위해 사용하는 보안 결함인 CVE 및 CWE 를 확인한다. 4 단계에서는 앞서 분석한 CWE 와 연관성 높은 취약한 함수를 확인한다.

Table 2. Development for New Cybersecurity Training Security Threat Scenarios in ICS
표 2. ICS 대상 신규 사이버보안 훈련용 보안 위협 시나리오 개발

<table>
<tr><td colspan="5">Cybersecurity Training Threat Scenario Name</td></tr>
<tr><td>Overview</td><td colspan="4">Tactic 1 ○ Techniques 1 ○ Techniques 2 ○ Techniques 3
Tactic 2 ○ Techniques 4 ○ Techniques 5 ○ Techniques 6
Tactic 3 ○ Techniques 7 ○ Techniques 8 ○ Techniques 9
⋮ ⋮</td></tr>
<tr><td>1. Threat Process</td><td colspan="4">1.
2.
⋮</td></tr>
<tr><td rowspan="2">2. Standardization of Techniques</td><td>Tactic</td><td>Technique</td><td>ICS Asset</td><td>Descriptions</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">3. Check for Techniques Vulnerabilities</td><td>Step</td><td>CVE List</td><td>CVE Descriptions</td><td>CWE List</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">4. Check for Vulnerable Functions</td><td colspan="2">CWE List</td><td colspan="2">Vulnerable Function</td></tr>
<tr><td colspan="2">-</td><td colspan="2">-</td></tr>
</table>

5 단계에서는 앞선 단계로부터 분석 및 도출한 데이터를 기반으로 보안 위협 시나리오를 개발한다. [표 2]는 새롭게 생성한 보안 위협 시나리오의 구성 요소를 나타낸 것이다. 시나리오는 Cybersecurity Threat Scenario Name, Overview, Threat Process, Standardization of Techniques, Check for Security Flaws, Check for Vulnerable Functions 로 구성된다. Cybersecurity Threat Scenario Name 은 개발한 보안 위협 시나리오의 이름을 의미한다. Overview 는 생성한 보안 위협 시나리오의 과정을 위협 전술과 기법을 사용하여 표현한 것이다. Threat Process 는 보안 위협 프로세스를 의미하며 시나리오의 수행 과정을 순서대로 나타낸다. Standardization of

Techniques 은 정형화 과정을 의미하며 위협 전술 및 기법, ICS 자산, 그리고 세부 설명을 나타낸다. Check for Security Flaws 는 위협 기법을 성공시키기 위해 사용 가능한 보안 결함을 나타내며 CVE 및 CWE 로 구성되어 있다. 마지막으로 Check for Vulnerable Functions 은 CWE 에 상응하는 취약한 함수로 구성되어 있다.

3.1 위협 과정 분석

본 단계에서는, ICS 대상 사이버보안 사고 사례 분석을 통한 보안 위협 프로세스 도출을 진행한다.

Table 3. Cases of Cybersecurity Incidents Targeting ICS
표 3. ICS 대상 사이버보안 사고 사례

Nation	Name(Incident)	Case of Cybersecurity Incidents Targeting ICS	Year
Iran	Stuxnet[23][24][25][26]	Nuclear Enrichment Facility	2010
U. S	Night Dragon[27]	Energy Sector	2011
Iran	Duqu[3]	Nuclear Enrichment Facility	2011
Ukraine	BlackEnergy[4][5][6][7][8]	Power Grid	2015
Ukraine	Industroyer[9][10][11]	Power Grid	2016
Saudi Arabia	Triton[28]	Petrochemical Plant	2017
U. S	sPower[29]	Renewable Energy Provider	2019
India	Dtrack[30][31]	Nuclear Power Plant	2019
U. S	Darkside[12]	Colonial Pipeline	2021
Ukraine	Industroyer 2[32]	Energy Company	2022

[표 3]은 분석한 ICS 대상 사이버보안 사고 사례를 사고가 발생한 국가, 사이버보안 사고 이름, 대상 ICS, 발생 연도로 구분하여 나타낸 것이다. 본 논문에서는 총 10 개의 ICS 사이버보안 사고 사례를 대상으로 분석을 수행하였다. 분석을 통해 도출된 보안 위협 프로세스에는 위협 시작지점과 위협 행위가 최종적으로 수행되는 지점까지의 순서가 포함되어 있다. 3.1.1 부터 3.1.3 까지, 대표적인 ICS 대상 사이버보안 사고 사례인 Stuxnet(2010), BlackEnergy(2015), Triton(2017) 3 건을 선정 및 분석한 결과에 대해 기술한 후, 각 보안 사고 사례 별 보안 위협 프로세스에서의 순서, 위협 기법, ICS 자산을 표 형태로 나타내었다.

3.1.1 이란, Stuxnet (2010)

Table 4. Cases of Stuxnet Threat
표 4. Stuxnet 사고 사례

Step	Threat Technique	ICS Asset
1	PC infection via USB	PC (IT)
2	Send infected PC information to attacker	
3	Internal system attack (infection) from infected PC	System (ICS)
4	Share internal system attack commands with the infected PC (if the version is lower, install higher version malware)	
5	Send attack command (Send code to change control commands from attacker)	
6	PLC control logic modulation	EWS
7	Facility failure due to change in operating values due to PLC equipment infection	PLC

[표 4]는 Stuxnet 악성코드 사고 사례를 정리한 것이다[23][24][25][26]. Stuxnet 사고 사례의 경우, 외부 USB 를 상용망 PC 에 연결하는 것으로부터 시작되었다. USB 에 포함된 악성 프로그램을 윈도우 .LNK 취약점을 이용하여 실행하였고, C&C 서버로 감염된 PC 의 시스템 정보를 전송하였다. 내부 네트워크에서는 취약점이 악용되어 악성코드가 유포되었다. 이 과정에서, 감염된 메인 PC 와 추가 감염된 내부 시스템 간의 악성코드의 버전을 체크한 후, 상위 버전의 악성코드를 설치하는 방식으로 악성 명령이 공유되었다. 마지막으로, 악성코드 제작자의 명령이 전송되면, 변조된 PLC 제어 명령이 PLC 에 업로드되어 시설에 장애가 발생하였다. 해당 Stuxnet 사례는 사이버공격으로 인한 최초의 물리적인 피해가 발생한 사례이며, 망분리 형태의 ICS 운영방식임에도 사이버공격이 수행된 사례이다. 이후, 동일한 악성코드에 감염된 사례가 발견되고 변종이 발견되는 등 ICS 를 대상으로 하는 사이버공격에 많은 영향을 미쳤다.

3.1.2 우크라이나, BlackEnergy (2015)

Table 5. Cases of BlackEnergy Threat
표 5. BlackEnergy 사고 사례

Step	Threat Technique	ICS Asset
1	Distribute Office documents containing malicious code through spear-phishing	PC (IT)
2	Collect internal authentication information and conduct network reconnaissance	PC (ICS)
3	Identify assets and attack targets existing in the network through domain servers	Server
4	Collection of ICS network asset information	HMI
5	Schedule an outage for UPS	Field Device
6	Disruption of power distribution through breaker operation	
7	Call center paralysis through phone DoS	System
8	Internal server power cut due to power outage due to UPS outage	Field Device
9	Delete MBR and system log data	PC (ICS)

[표 5]는 BlackEnergy 악성코드 사고 사례를 정리한 것이다[4][5][6][7][8]. BlackEnergy 사고 사례의 경우, 적대자는 전력망에 대한 정보를 사전 입수하여 조기에 악성코드를 개발하였다. 이후, 시설 관련 직원들에게 이메일을 통해 트로이 목마가 포함된 MS Office 첨부 파일 피싱 이메일을 보내고 매크로를 실행하도록 유도한다. 감염된 시스템에서는 우선적으로 C&C 서버로 연결을 설정한 이후, 위협 행위 수행 기능을 포함한 플러그인을 로드하여 내부 인증정보를 수집 및 정찰을 시작한다. 네트워크에 존재하는 자산과 공격 표적을 식별하기 위해 기업 내부에 존재하는 도메인 서버를 사용한다. 그리고 내부 자산 정보를 정찰하기 위해 ICS 네트워크까지 침입한다. 해당 과정을 통해 수집된 정보를 기반으로 악성코드를 개발되었다. 개발된 악성코드는 기업 내부망에 존재하는 PC 로 전달되고, 시스템 내부에 존재하는 UPS (Uninterruptible Power Supply) 시스템의 작동 중단을 예약한다. 이후에 ICS 네트워크 내부에 존재하는 차단기를 열어 배전을 중단시킨다. 악성코드는 컨버터에 전달하여 컨버터가 작동할 수 없게 하고, 이후 전력망 기업의 콜센터 DoS 공격을 실시하여 전력망 시설 주변의 고객들의 문의전화를 차단한다. 앞서 예약 설정한 UPS 중단으로 인해 정전이 발생하면서 전화 통신 서버와 데이터 센터 서버의 전원이 차단된다. 마지막으로 BlackEnergy 는 시스템의 MBR (Master Boot Record)와 시스템 로그 데이터를 삭제한다.

3.1.3 사우디아라비아, Triton (2017)

[표 6]은 Triton 악성코드 사고 사례를 정리한 것이다[28]. Triton 사고 사례의 경우, 최초 감염은 상용망 PC 에서 스피어피싱을 통해 발생한 것으로 추정된다. 내부망으로 침투하기 위해 방화벽 취약점을 통해 우회한다. 이후 적대자는 SIS(Safety Instrumented System) 컨트롤러 및 펌웨어

버전 등 민감한 정보를 수집한다. SIS 컨트롤러가 'PROGRAM' 모드로 설정돼 있을 때, 시스템을 공격하게 설정한다. 메모리에 악성코드 삽입을 수행할 준비를 완료하여 적대자가 원할 때 컨트롤러에 접근할 수 있도록 하였지만, SIS 기능 무력화 시험을 하던 중, 예기치 못한 중단이 발생하면서 Triton 악성코드가 발견되었다.

Table 6. Case of Triton Threat
표 6. Triton 사고 사례

Step	Threat Technique	ICS Asset
1	Distribute attachments containing malicious code through spear phishing	PC (IT)
2	Access using vulnerable firewall settings	Server (ICS)
3	Access EWS by obtaining account information	EWS
4	Collect information such as SIS controller, firmware version, among others.	
5	Payload transfer to SIS	RTU, PLC
6	Cause conditions that make the facility unsafe	

3.2 위협 기법 정형화

본 단계에서는, 앞서 보안 위협 프로세스에서 작성한 위협 기법을 MITRE ATT&CK 프레임워크를 사용하여 정형화한다.

Table 7. Standardization Process
표 7. 정형화 과정

Name	Step	Technique (Raw)	Technique (Standardization)
Stuxnet (2010)	1	PC infection via USB	T0847
	2	Send infected PC information to attacker	T1071.001
	3	Internal system attack (infection) from infected PC	T1021
	⋮	⋮	⋮
BlackEnergy (2015)	1	Distribute Office documents containing malicious code through spear-phishing	T0865
	2	Collect internal authentication information and conduct network reconnaissance	T1552.001
	3	Identify assets and attack targets existing in the network through domain servers	T1021.002
	⋮	⋮	⋮
Triton (2017)	1	Distribute attachments containing malicious code through spear phishing	T0865
	2	Access using vulnerable firewall settings	T1210
	3	Access EWS by obtaining account information	T1005
	⋮	⋮	⋮

[표 7]은 1 단계에서 분석한 3 건의 ICS 보안 사고 사례에서 도출된 위협 기법을 정형화한 것이다. 사례 분석을 통해 도출된 위협 기법은 서로 다르게 표현되어 있어 주관적이며 불균일하다. 이에, MITRE ATT&CK 프레임워크의 Techniques 기반의 객관적인 데이터를 이용하여 위협 기법의 표현 및 형식을 통일시키는 정형화 과정을 진행한다.

3.3 보안 결함 식별 및 도출

본 단계에서는, 보안 위협이 성공적으로 수행되기 위해 악용된 보안 결함을 확인한다.

Table 8. Security Flaws: Identify and Extract CVE and CWE
표 8. 보안 결함: CVE 및 CWE 식별 및 도출

Name	Step	CVE List	CVE Descriptions	CWE List
Stuxnet (2010)	1	CVE-2010-2568	Execute arbitrary code via .LNK or .PIF files	• CWE-20 (Improper Input Validation) • CWE-134 (Use of Externally Controlled Format String)
	2	CVE-2008-4250	An attacker remotely executes arbitrary code through an RPC (Remote Procedure Call) request	• CWE-94 (Improper Control of Generation of Code ('Code Injection'))
	3	CVE-2010-2729	An attacker sends a remotely crafted print request to create a directory file and execute arbitrary code	• CWE-20 (Improper Input Validation)
	⋮	⋮	⋮	⋮
BlackEnergy (2015)	1	CVE-2014-4114	An attacker executes arbitrary code via a crafted OLE object	• CWE-20 (Improper Input Validation) • CWE-134 (Use of Externally Controlled Format String)
	⋮	⋮	⋮	⋮
Triton (2017)	1	CVE-2018-8872	Attacker data can be copied anywhere in memory	• CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)
	⋮	⋮	⋮	⋮

[표 8]은 위협 기법이 성공하기 위해 사용된 보안 결함인 CVE(Common Vulnerabilities and Exposures) 및 CWE(Common Weakness Enumeration) 취약점을 식별 및 도출한 것이다[33]. 취약점은 공개적으로 알려진 소프트웨어의 보안취약점 목록인 CVE 을 통해 표현하고, CVE 가 발생하기 위한 조건을 나타낸 하드웨어 및 소프트웨어 취약점 목록인 CWE 을 사용한다. 즉, CVE 식별 및 도출을 통해 보안 위협 발생 요소를 확인하고, CWE 식별을 통해 보안 위협이에서의 취약점 발생 원인을 확인 가능하다. 또한, CVE 및 CWE 에 영향을 받는 시스템(예: Windows, Siemens Simatic Series, Tricon Series 등) 역시 확인 가능하다.

3.4 취약한 함수 식별 및 도출

Table 9. CWE and Vulnerable Function Mapping
표 9. CWE 및 취약한 함수 매핑

CWE List	Vulnerable Function
CWE-134 (Uncontrolled Format String)	Incompatible Function Declaration
	⋮
CWE-20 (Improper Input Validation)	syslog()
	⋮
CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)	realloc()
	GetMachineName()
	mkstemp()
	getchar()
	fscanf()
	⋮
⋮	⋮

본 단계에서는, 앞서 식별 및 정형화한 CWE 를 통해 CVE 를 발생 또는 비슷한 결과를 발생시킬 수 있는 취약한 함수를 도출할 수 있다. 이러한 취약한 함수를 통해 ICS 시스템에 존재하는 취약점 표현이 가능해지므로 최종적으로 ICS 환경에서의 사이버보안 훈련용 보안 위협 시나리오를 개발할 수 있게 된다. ICS 환경은 전력, 원자력 발전소, 배전 시스템 등 변화에

민감한 시설이 대다수이며, 약간의 오차 또는 오류만으로도 큰 사고가 발생할 가능성이 높다. 이에, 레거시(Legacy)한 시스템을 유지하여 ICS 자산(예: OS, System, Devices 등)를 교체하지 않고 수십년간 사용하는 경향이 높다. 따라서, 여전히 많은 ICS 환경에서 C 언어 기반의 자산(예: HMI, PLC 등)을 사용하고 있다[34][35][36][37][38]. 따라서, 취약한 함수와 관련하여 프로그래밍 언어는 C 언어로 선정하였다.

[표 9]은 CWE 와 매핑되는 취약한 함수의 일부분을 나타낸 것이다[39][40][41]. 취약한 함수는 국내 시큐어코딩 가이드라인 문서 2 건 '소프트웨어 보안약점 진단 가이드' 및 'C 시큐어코딩 가이드'와 국외 시큐어코딩 가이드라인 문서 1 건 'SEI CERT C Coding Standard' 총 3 건을 통해 보안약점을 지닌 함수들을 후보군으로 1 차 선정한다. 이후, 이전 단계를 통해 식별된 보안 약점과 문서 내 보안 약점을 비교한 후, 동일한 함수를 취약한 함수로써 최종 선정한다.

3.5 보안 위협 시나리오 생성

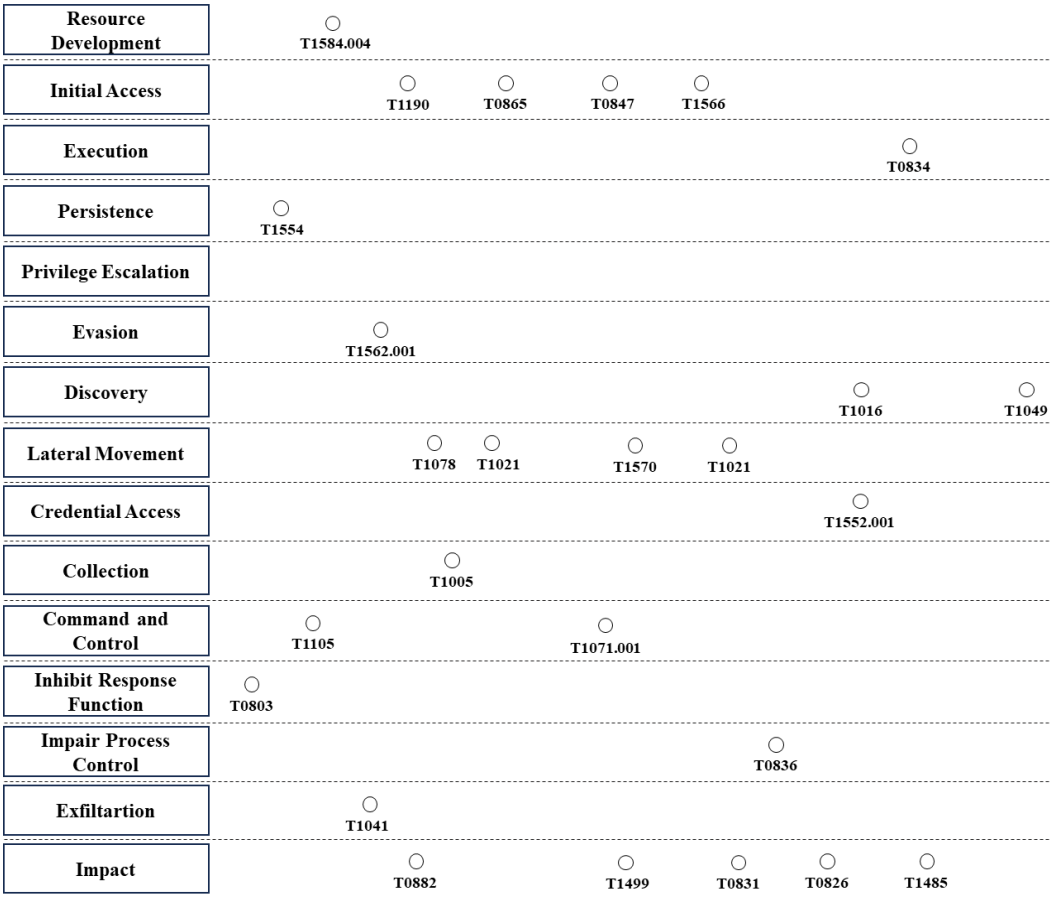
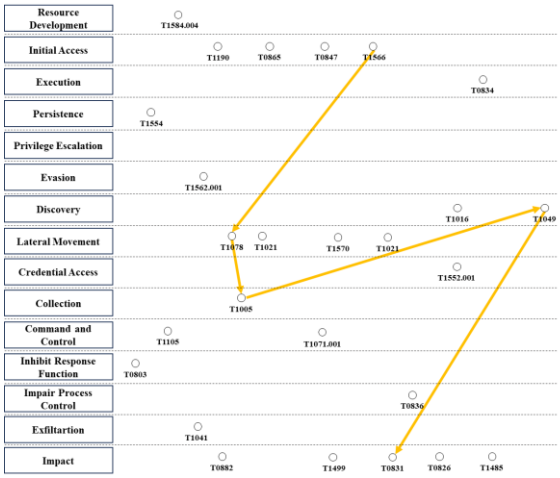


Figure 2. Overview of Case-based Security Threat
그림 2. 사례 기반 보안 위협 시나리오 개요

[그림 2]는 앞서 데이터베이스화 하였던 ICS 대상 사이버보안 사고 사례 분석을 통해 도출된 결과들을 MITRE ATT&CK Matrix 를 기반으로 개요 형태로 표현한 것이다. 좌측 15 개의 네모는 MITRE ATT&CK 의 Tactics, 원은 실제 사고 사례에서 식별한 Techniques 를 의미하며, 각 원 사이에 화살표 선을 연결하여 위협 진행 순서와 사용된 위협 전술을 표현 가능하고 이를 통해, 보안 위협 프로세스를 나타낼 수 있다. 해당 방법을 기반으로 다양한 조합을 사용하여 유효한 보안 위협 시나리오를 생성할 수 있다.

VI. 신규 보안 위협 시나리오 생성 결과

Table 10. New Training Security Threat Scenario: Loss of PLC Functionality
표 10. 신규 훈련용 보안 위협 시나리오: PLC 기능 상실

<table>
<tr><td colspan="6">Loss of Plc Functionality</td></tr>
<tr><td>Overview</td><td colspan="5"> 
</td></tr>
<tr><td>1. Threat Process</td><td colspan="5">1. Distribution of malware through spear phishing
2. Hijacking of VPN account through malware and then attacking internal network through VPN
3. Access EWS by obtaining account information after entering the internal network
4. Collect important information from EWS and PLC
5. After seizing control through an attack on the PLC's memory and registers, normal function is disabled</td></tr>
<tr><td rowspan="6">2. Standardization of Techniques</td><td>Tactic</td><td>Technique</td><td>ICS Asset</td><td colspan="2">Descriptions</td></tr>
<tr><td>Initial Access</td><td>T1566.001</td><td>PC (IT)</td><td colspan="2">• Distribute word documents containing malicious code through spear-phishing</td></tr>
<tr><td>Persistence</td><td>T1078</td><td>Server, PC (ICS)</td><td colspan="2">• Internal network attack through leaked VPN account</td></tr>
<tr><td>Collection</td><td>T1005</td><td>EWS</td><td colspan="2">• Access EWS by obtaining account information after entering the internal network</td></tr>
<tr><td>Discovery</td><td>T1049</td><td>EWS</td><td colspan="2">• Collection of information such as EWS and PLC H/W information, firmware version, among others.</td></tr>
<tr><td>Impact</td><td>T0831</td><td>RTU/PLC</td><td colspan="2">• Facility failure due to change in operating values due to PLC equipment infection</td></tr>
<tr><td rowspan="4">3. Check for Security Flaws</td><td>Step</td><td>CVE List</td><td colspan="2">CVE Descriptions</td><td>CWE List</td></tr>
<tr><td>1</td><td>CVE-2011-3402</td><td colspan="2">• A vulnerability that could allow arbitrary code execution via crafted font data in a Word document or web page.</td><td>• CWE-787</td></tr>
<tr><td>2</td><td>CVE-2018-8872</td><td colspan="2">• A Vulnerability that allows attacker data to be copied anywhere in memory</td><td rowspan="2">• CWE-119</td></tr>
<tr><td>3</td><td>CVE-2018-7522</td><td colspan="2">• A vulnerability that could allow an attacker to gain administrator-level access and control system state by modifying memory data</td></tr>
<tr><td rowspan="3">4. Check for Vulnerable Functions</td><td colspan="2">CWE List</td><td colspan="3">Vulnerable Function</td></tr>
<tr><td colspan="2">CWE-787</td><td colspan="3">find(), malloc(), strcpy(), gets(),among others.</td></tr>
<tr><td colspan="2">CWE-119</td><td colspan="3">realloc(), GetMachineName(), mkstemp(), strrchr(), getchar(), among others.</td></tr>
</table>

[표 10]은 제안한 방법론을 기반으로 새로 개발된 ICS 대상 사이버보안 훈련용 보안 위협 시나리오 중 하나인 PLC 의 기능 상실을 위한 훈련용 보안 위협 시나리오를 나타낸 것이다. 먼저, 악성코드가 포함되어 있는 word 문서를 스피어피싱을 통해 배포한다. 이후, 악성코드를 통해 유출된 VPN 계정을 탈취하여 내부망에 접근한다. 내부 네트워크 접근에 성공하여 진입한 후, 로컬 데이터 수집을 통해 계정 정보를 획득하여 EWS 에 접근한다. 그리고 시스템 네트워크 연결 검색을 통해 EWS 와 연결된 PLC 의 H/W 정보, 펌웨어 버전 등 민감한 정보를 수집한다. 마지막으로, PLC 장비의 감염으로 인해 취약한 함수가 조작되어 작동 값이 변경됨으로써 공정

시설에 장애가 발생한다. 해당 보안 위협 시나리오에서 대상으로 하는 ICS 자산은 각각 PC(IT), Server(ICS), PC (ICS), EWS, RTU/PLC 이다. 사용된 보안 위협 전술은 각각 Initial Access, Persistence, Collection, Discovery, Impact 이고, 사용된 보안 위협 기법은 각각 T1566.001, T1078, T1005, T1049, T0831 으로 정형화한다. 해당 보안 위협 기법을 수행하기 위해 악용한 보안 결함은 CVE-2011-3402, CVE-2018-8872, CVE-2018-7522 취약점이며, 보안 약점은 CWE-787 및 CWE-119 으로 식별하였다. 마지막으로, 식별된 CWE 에 대응되는 취약한 함수를 도출하였다.

Table 11. Comparison of the Proposed Paper with Related Research
표 11. 제안한 논문과 관련 연구의 비교

Evaluation Criteria	Kim. D. H et al. (2022) [17]	Ahn. M. K et al. (2020) [18]	Liao, Y. C (2021) [19]	Hacks, S et al. (2020) [20]	Proposed
Standardization	△	√	√	√	√
CVE	×	√	√	×	√
CWE	×	×	√	×	√
Programming Languages for ICS assets	×	×	×	×	√
Scenario Validity	△	√	√	√	√
ICS Environment	×	×	√	√	√

[표 11]은 [표 10]에서 생성한 훈련용 보안 위협 시나리오를 기반으로 본 논문과 관련 연구 논문을 비교 분석한 것이다. 평가 기준에 대하여 '√'는 만족함, '△'는 부분적으로 만족함, '×'는 만족하지 않음을 나타낸 것이다. Kim. D. H et al.[17]은 시나리오 설계에 필요한 위협 기법의 선정 기준과 유효한 위협 수행을 위해 반드시 사용되어야 하는 취약점 및 보안 약점에 대한 명확한 근거가 부족하다. 또한, 앞선 내용과 같이, 위협 기법의 상세 과정이 없어 정확한 정형화 과정에 대한 내용을 알기 어렵다. 제안한 방법론은 Analysis Threat Process 분석을 통해 도출한 Tactics 및 ICS Asset 정보에 대한 상세 설명을 기반으로 정형화를 수행하므로 정형화 기준에 대한 충분한 근거를 만족한다. 또한, CVE List 및 CVE Description 과 대응되는 CWE List 를 식별하므로 취약점 및 보안 약점을 통한 위협 기법의 유효성이 높다. Ahn. M. K et al.[18]은 보안 위협 시뮬레이션을 위해 사이버 킬체인 기법을 적용하여 보안 위협 시나리오를 생성했지만, 사이버 킬체인은 적대자의 활동을 단순화하여 표현하므로 위협 전술과 행위간 연관성을 파악하기 어렵다. 또한, 외부에서의 침입 탐지에 중점을 두어 시스템 내부 보안 위협과 관련된 시나리오를 생성하는 것에 한계가 존재한다. 제안한 방법론은 MITRE ATT&CK 프레임워크를 사용하여 내부 위협에 대한 TTP 정보를 확인 가능하므로 외부 및 내부 위협에 대한 시나리오 생성에 모두 효과적이다. Liao, Y. C[19] 및 Hacks, S et al.[20]은 ICS Asset 에서 사용하는 프로그래밍 언어의 취약점을 고려하지 않았으므로 해당 부분과 관련된 추가적인 보안 위협 시나리오를 생성하는데 제한적이다. 제안한 방법론은 보안 약점에 대응되는 취약한 함수를 도출하여 추가 위협 벡터를 생성하므로 다양한 보안 위협 시나리오를 개발할 수 있다.

이와 같이, 본 논문에서 제안한 방법론에서는 실제 보안 사고 사례 분석을 통한 위협 기법 도출 및 정형화 작업을 수행했으며, 대응되는 보안 결함인 CVE 및 CWE 를 식별하여 위협 기법에 대한 명확한 근거를 제시하였다. 또한, ICS 자산에서 사용 중인 프로그래밍에서의 취약한 함수 식별을 통해 CVE 및 CWE 이외의 추가적인 취약점을 도출하였다.

V. 결론 및 향후 연구계획

본 논문에서는 ICS 대상 사이버보안 사고 사례를 기반으로 훈련용 보안 위협 시나리오를 개발하는 방법론을 제안하였다. 실제 ICS 환경을 대상으로 발생하였던 보안 사고 사례를 분석한 후, 보안 위협 프로세스를 도출하였다. 그리고 MITRE ATT&CK, CVE, CWE 식별을 통해 위협 기법의 정형화 작업 및 취약점 매핑을 수행하였다. 이후, CWE 와 연관성 높은 취약한 함수를 선정하였다. 설계한 보안 위협 시나리오 방법론을 통해 도출된 데이터들을 기반으로 MITRE

ATT&CK Matrix 에 적용하여 각각 보안 위협 전술 및 기법으로 구분하였다. 해당 과정에서 보안 위협 전술 및 기법 간 여러 조합을 사용하여 다양한 훈련용 보안 위협 시나리오를 생성할 수 있음을 확인하였다. 마지막으로 본 논문과 기존 연구 간 비교 분석을 진행하여 제안한 방법론이 더 효과적임을 확인하였다.

향후 연구로는 본 제안 방식의 실제 검증을 위한 사이버보안 훈련 환경 ICS 테스트베드 구축 및 ICS 대상 사이버보안 위협에 대응하기 위한 방어 시나리오를 개발할 것이다.

VI. 감사의 글

이 논문은 2021 년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-21-037)

VII. 참고문헌

[1] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N, “Cybersecurity for industrial control systems: A survey”, computers & security, Vol. 89, 101677. Feb. 2020.
[2] Ackerman. P, “Industrial Cybersecurity: Efficiently secure critical infrastructure systems”, in Packt Publishing, England, 2017, pp. 30-39
[3] “Duqu: A Stuxnet-like malware found in the wild”, CRYSYS, [Online]. Available: https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf
[4] “BlackEnergy & Quedagh: The convergence of crimeware and APT attack”, F-Secure Labs, [Online]. Available: https://blog.f-secure.com/wp-content/uploads/2019/10/BlackEnergy_Quedagh.pdf
[5] “BE2 custom plugins, router abuse, and target profiles”, SECURELIST, [Online]. Available: https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/
[6] “BE2 extraordinary plugins, Siemens targeting, dev fails”, SECURELIST, [Online]. Available: https://securelist.com/be2-extraordinary-plugins-siemens-targeting-dev-fails/68838/
[7] “BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry”, weliveserucrity, [Online]. Available: https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
[8] “UK exposes series of Russian cyber attacks against Olympic and Paralympic Games”, UK NCSC, [Online]. Available: https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
[9] “Win32/Industroyer: A new threat for industrial controls systems”, ESET LLC, [Online]. Available: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf
[10] “CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations”, DRAGOS, [Online]. Available: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf
[11] “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack”, DRAGOS, [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
[12] “Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign”, Varonis, [Online]. Available: https://www.varonis.com/blog/darkside-ransomware
[13] Ekisa, C., Briain, D. Ó., & Kavanagh, Y, “An open-source testbed to visualise ics cybersecurity weaknesses and remediation strategies–a research agenda proposal”, In 2021 32nd Irish Signals and Systems Conference (ISSC), IEEE, pp. 1-6. Jun. 2021.
[14] Koay, A. M., Ko, R. K. L., Hettema, H., & Radke, K, “Machine learning in industrial control system (ICS) security: current landscape, opportunities, and challenges”, Journal of Intelligent Information Systems, Vol. 60(2), pp. 377-405. Oct. 2023.
[15] Alwakeel, A. M, “An overview of fog computing and edge computing security and privacy issues”, Sensors, Vol.21(24), 8226, Dec. 2021.
[16] “SANS Institute Information Security Reading Room Secure Architecture for Industrial Control Systems”, Semantic Scholar, [Online]. Available: https://www.semanticscholar.org/paper/SANS-

Institute-Information-Security-Reading-Room-Obregon/cf1193740974922c2fd29733ac204f06a3de7b08
[17] Kim. D. H., Choi. S. H, "A Study on the Active Defense Strategy of Honey System Using MTD", Korea Institute of Information Technology Magazine, Vol. 20(1), 27-32, Dec. 2022
[18] Ahn. M. K., Lee. J. R, "Research on System Architecture and Methodology based on MITRE ATT&CK for Experiment Analysis on Cyber Warfare Simulation", Journal of the Korea Society of Computer and Information, Vol. 25(8), pp. 31-37, Aug. 2020
[19] Liao, Y. C, "Generating Targeted Attack Scenarios against Availability for Critical Infrastructures", In 2021 14th CMI International Conference-Critical ICT Infrastructures and Platforms (CMI), IEEE, pp. 1-7, Nov. 2021.
[20] Hacks, S., Katsikeas, S., Ling, E., Lagerström, R., & Ekstedt, M, "powerLang: a probabilistic attack simulation language for the power domain", Energy Informatics, Vol. 3, pp. 1-17, Nov. 2020
[21] "ICS Matrix", MITRE ATT&CK, [Online]. Available: https://attack.mitre.org/matrices/ics/
[22] Georgiadou, A., Mouzakitis, S., & Askounis, D, "Assessing mitre att&ck risk using a cyber-security culture framework", Sensors, Vol. 21(9), 3267, May. 2021.
[23] "W32.Stuxnet Dossier (Version 1.4)", Symantec, [Online]. Available: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en
[24] "ICS Advisory (ICSA-10-272-01)", CISA, [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-10-272-01
[25] "Stuxnet Under the Microscope", ESET LLC, [Online]. Available: http://www.rpac.in/image/ITR%201.pdf
[26] "To Kill a Centrifuge", The Langner Group, [Online]. Available: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
[27] "Global Energy Cyberattacks: "Night Dragon"", McAfee, [Online]. Available: https://www.mcafee.com/blogs/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf
[28] "Attackers deploy new ICS attack framework "TRITON" and cause operational disruption to critical infrastructure", Mandiant, [Online]. Available: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton
[29] "First-of-a-kind U.S. grid cyberattack hit wind, solar", Energywire, [Online]. Available: https://subscriber.politicopro.com/article/eenews/1061421301
[30] "DTrack: previously unknown spy-tool by Lazarus hits financial institutions and research centers", Kaspersky, [Online]. Available: https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers
[31] "Hello! My name is Dtrack", SECURELIST, [Online]. Available: https://securelist.com/my-name-is-dtrack/93338/
[32] "Industroyer2: Industroyer reloaded", weliveserucrity, [Online]. Available: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded
[33] "Vulnerabilities", NIST, [Online]. Available: https://nvd.nist.gov/vuln
[34] Korodi, A., Nicolae, A., & Drăghici, I. A, "Proactive decentralized historian-improving legacy system in the water industry 4.0 context", Sustainability, Vol. 15(15), 11487, Jul. 2023.
[35] Michalec, O., Milyaeva, S., & Rashid, A, "When the future meets the past: Can safety and Cybersecurity coexist in modern critical infrastructures?", Big Data & Society, Vol. 9(1), Jun. 2022.
[36] "HMI Works C Programming pt3", ICP DAS USA, [Online]. Available: https://www.icpdas-usa.com/HMI-works-CProgramming-pt3.html
[37] "SIMATIC M7 Only Available on a Spare Part Basis as of October 2003", Siemens, [Online]. Available: https://support.industry.siemens.com/cs/document/14044569/simatic-m7-only-available-on-a-spare-part-basis-as-of-october-2003-?dti=0&lc=en-WW
[38] "Touch HMI Devices", ICP DAS, [Online]. Available: https://www.bbrc.ru/upload/iblock/cf1/i8z9k9u6vd9enme563mqkw7jxwc177hx/603adb8b_0fed_11e8_80d8_0cc47a1243ef_58fbaa64_2692_11e8_80d8_0cc47a1243ef.pdf
[39] "Software Security Weakness Diagnostic Guide", KISA, [Online]. Available: https://www.kisa.or.kr/2060204/form?postSeq=9&page=1
[40] "Secure Coding Guide C", MOIS, [Online]. Available: https://www.mois.go.kr/
[41] "SEI CERT C Coding Standard", Carnegie Mellon University SEI, [Online]. Available: https://resources.sei.cmu.edu/downloads/secure-coding/assets/sei-cert-c-coding-standard-2016-v01.pdf

저자소개

전규현 (*GyuHyun Jeon*)

2023 년 2 월 가천대학교 컴퓨터공학과 학사
2023 년 3 월 ~ 현재 가천대학교 정보보호학과 석사과정

관심분야 : CPS 보안, AI 보안

김광수 (*Kwangsoo Kim*)

2009 년 아주대학교 정보컴퓨터공학과 학사
2017 년 아주대학교 컴퓨터공학과 박사
2017 년 ~ 현재 LIG 넥스원(주) 사이버전자전개발단 수석연구원

관심분야 : 네트워크 보안, 사이버전, 사이버전 훈련, 네트워크 M&S, 가상화 기술

강재식 (*Jaesik Kang*)

2015 년 충남대학교 컴퓨터공학과 학사
2020 년 충남대학교 컴퓨터공학과 석사
2022 년 ~ 현재 LIG 넥스원(주) 사이버전자전개발단 선임연구원

관심분야 : 사이버전, 사이버전 훈련, 인공지능

승운 (*Seungwoon Lee*)

2017 년 아주대학교 소프트웨어특성화학과 석사
2022 년 아주대학교 AI 융합네트워크학과 박사
2022 년 ~ 현재 LIG 넥스원(주) 사이버전자전개발단 선임연구원

관심분야 : 네트워크 보안, 사이버전, 사이버전 훈련, 네트워크 M&S, 가상화 기술

서정택 (*Jung Taek Seo*)

2006 년 고려대학교 정보보호공학과 박사
2016 년 ~ 2021 년 순천향대학교 정보보호공학과 교수
2021 년 ~ 현재 가천대학교 컴퓨터공학부 컴퓨터공학전공 교수

관심분야 : CPS 보안, ICS 보안