정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

MITRE ATT&CK 프레임워크 기반 에너지분야 기반시설 보안 모니터링 방안

최 승 오*, 김 형 천**

요 약

주요 국가기반시설에 도입되어 운영 중인 산업제어시스템은 4차 산업혁명에 따른 디지털 전환으로 지능화됨에 따라 IT 환경의 보안위협이 OT환경으로 상속되면서 제어시스템 보안위협 및 공격 양상도 복잡해지고 있다. 실제로 에너지분야 기반시설을 대상으로 한 Stuxnet, Conficker, BlackEnergy3 등 제어시스템 사이버 위협 및 사고 사례가 지속적으로 보고되고 있으나, 제어시스템을 대상으로 하는 사이버공격 대응을 위한 보안가시성 확보는 제대로 이루어지지 않고 있으며, 이를 위해서는 기존 IT 환경과는 다른 제어시스템의 특성이 반영된 보안 모니터링이 요구된다. 본 논문에서는 제어시스템 보안위협 지식 데이터베이스인 MITRE ATT&CK 프레임워크를 기반으로 제어시스템에 적합한 보안 모니터링을 수행하기 위한 요소들을 식별하고 방안을 제시한다.

Ⅰ. 서 론

주요 국가기반시설에 도입되어 운영 중인 산업제어시스템(ICS, Industrial Control System)은 빠른 속도로 지능화와 디지털화가 이루어지고 있다. 또한 4차 산업혁명으로 인한 다양한 환경의 이기종 기기 간 연결 증가는 기존 IT 환경 보안위협의 OT 환경으로의 상속과 공격표면(Attack Surface)의 확장을 촉발하여 이전보다 더 다양한 보안위협에 직면하게 하고, 공격 경로 및 양상을 복잡하게 만들고 있다[1].

다양한 분야의 기반시설에서 제어시스템은 사이버 보안위협에 노출 시 물리적 피해로 이루어지고 그 파급효과가 사회전반에 영향을 끼칠 수 있다. 특히, 에너지 분야 기반시설을 대상으로 한 제어시스템 보안위협은 이란 원심분리기를 대상으로 한 Stuxnet을 시작으로 독일 원자력발전소에서 발견한 Conficker, 우크라이나의 대규모 정전사태를 유발한 BlackEnergy3, Industroyer 등 사고 사례가 지속적으로 보고되고 있다. 또한, 제어시스템 웜(PLC-Blaster), 제어시스템 랜섬웨어(LogicLocker) 등 IT환경의 보안위협이 OT환경으로 상속되고 있는 추세가 뚜렷하다[2-4].

하지만, 이러한 보안위협에도 불구하고 기존 보안기술 및 솔루션은 제어시스템 가시성을 제공하지 못하거나 다양한 데이터소스를 활용한 보안 모니터링을 수행하고 있지 않기 때문에 IT-OT 보안위협의 수직적·수평적 전파 현황을 확인하기 어렵다[5]. BlackEnergy3의 경우, 제어시스템 보안 가시성의 부재로 인해 공격 대상인 제어시스템 운영 환경에 대한 정보수집(Reconnaissance)을 통해 6개월 이상 공격을 지속할 수 있었다[2].

따라서, 제어시스템 전 영역에 걸쳐 지속적인 보안 모니터링과 적극적인 방어 조치를 통해, 이상 및 위협을 탐지하고 대응할 수 있는 능력이 필요하다. 이를 위해 실제 제어시스템 운영 환경과 유사한 시험환경과 연구용 데이터셋 확보를 위한 연구가 활발히 진행 중에 있다[6, 7]. 이러한 연구를 토대로 제어시스템 보안 가시성을 확보하기 위해 상황 모니터링에 적합한 체계적인 보안위협 지식 데이터베이스의 활용이 필수적이다.

본 논문에서는 제어시스템 보안위협 지식 데이터베이스인 MITRE ATT&CK 프레임워크(이하, MAF)를 활용한 제어시스템 보안 모니터링 방안을 제시한다. MAF 기반 제어시스템 보안 모니터링을 위해서는 사전에 필요한 데이터가 무엇인지, 어디에 해당 데이터가 있는지, 어떻게 해당 데이터를 수집할 수 있는지를 분석해

* ETRI 부설연구소 (선임연구원, sochoi@nsr.re.kr)
** ETRI 부설연구소 (책임연구원/실장, khche@nsr.re.kr)

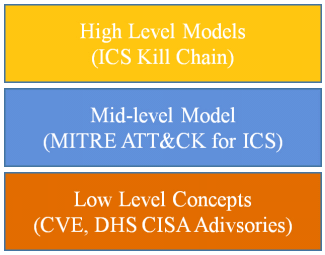
야 한다. 이를 위해 제어시스템 운영환경을 대상으로 한 MITRE ATT&CK for ICS(이하, MAF-I)을 기준으로 구성 요소를 분석한다. 제어시스템 보안위협을 감시하기 위해 필요한 정보 유형 식별을 선행하고, 제어시스템 운영환경을 고려한 해당 정보의 수집 및 분석 방안을 제시한다.

본 논문은 총 7장으로 구성되어 있다. Ⅱ장에서는 MAF를 소개하고 구성 요소에 따른 기능상의 특징을 설명한다. Ⅲ장에서는 산업제어시스템 도메인을 대상으로 MAF-I의 구성요소를 설명하고, 제어시스템 특성을 반영한 공격전략 및 기술에 대해 소개한다. Ⅳ장에서는 MAF-I 기반 제어시스템 보안 모니터링을 위해 필요한 정보 식별과 유형 분류에 대해 기술하고, 해당 정보를 수집하기 위한 방안을 Ⅴ장에서 소개한다. Ⅵ장에서는 다양한 모니터링 대상 정보를 MAF-I를 통해 통합적으로 분석하기 위한 방안과 적용 사례를 소개한다. 마지막으로 Ⅶ장에서는 본 논문의 결론을 맺는다.

Ⅱ. 배 경

일반적으로 보안위협의 상황을 모니터링하기 위해 [그림 1]과 같이 다양한 보안위협 지식 데이터베이스를 활용할 수 있다[8]. 록히드마틴의 킬체인 모델[9]은 상위 레벨의 보안위협 지식 데이터베이스로써 공격자의 일련의 행동이 전술적 공격 목표와 각 행동의 연관성을 표현하고 전달하기에 효과적이지 않다. 하위 레벨의 보안위협 지식 데이터베이스로인 익스플로잇 데이터베이스의 경우 종종 익스플로잇 예제를 제공하지만, 실제 공격 상황과 거리가 멀거나 현실적으로 적용하기 어렵다.

MAF는 실제 발생한 침해사고들의 분석을 통해 공격자들(Adversaries)의 전략(Tactics)과 기술(Techniques)에 대한 지식베이스로써 2015년 5월 공식 발표하였으며, 이후 [표 1]과 같이 지속적인 업데이트를



〔그림 1〕 보안위협 지식 데이터베이스

〔표 1〕 MAF 개정 이력

버전	일시	주요 변경내용
-	2016. 6.	위협모델 및 새로운 기능 추가 Collection 공격전략 추가 96종 공격기술 121종으로 증가
-	2017. 1.	신규 공격기술, 리포트, 내용 추가 공격기술 127종으로 증가
-	2017. 4.	신규 공격기술, 리포트, 내용 추가 공격기술 133종으로 증가
-	2017. 7.	운영체제에 따른 공격기술 분류 및 세분화를 통한 매트릭스 마련 공격기술 169종으로 증가
ATT&CK v1	2018. 1.	공격기술 188종으로 증가
ATT&CK v2	2018. 4.	Initial Access 공격전략 추가 공격기술 219종으로 증가
ATT&CK v3	2018. 10.	프레임워크별 ID 명명법 변경 Enterprise 공격기술 4종 추가, 17종 변경 Mobile 공격기술 5종 추가, 2종 변경
ATT&CK v4	2019. 4.	Enterprise- Impact 공격전략 추가 해당 전략에 대한 공격기술 14종 추가, 그 외 전략에 해당하는 공격기술 7종 추가 PRE-ATT&CK 공격기술 1종 추가, 1종 삭제
ATT&CK v5	2019. 7.	공격기술별 Mitigation 대폭 개정 40종 신규, 240종 대체
ATT&CK v6	2019. 10.	클라우드 대상 공격기술 36종 추가
ATT&CK v7 (Beta)	2020. 3.	서브공격기술(공격기술 세분화) 발표 156종 공격기술과 260종 서브공격기술로 구성
ATT&CK v7	2020. 7.	베타버전 오류 수정 서브공격기술 12종 추가

진행하고 있다.

2018년 5월에는 ATT&CK for Enterprise(이하, MAF-E), PRE-ATT&CK, ATT&CK for Mobile 데이터를 STIX 2.0 포맷으로 외부에 공개하였다. MAF는 보안 모니터링을 위해 다양한 분야에서 폭넓게 활용 중이며, 많은 보안 솔루션 제조사들이 탐지 및 대응을 위한 기반 기술로써 활용하고 있다.

최근에는 산업제어시스템을 대상으로 한 MAF-I를 공개하였다. MAF-I는 제어시스템 보안위협 관련된 다양한 형태의 보고서와 실제 사례를 분석하여 총 96종의 공격기술을 기존 MAF-E의 공격 전략에 매핑하였다.

Ⅲ. MITRE ATT&CK for ICS 분석

MAF-I는 제어시스템 관련 데이터소스 식별을 위해, SANS, CISA, NIST 등의 기관에서 발행한 분석보고서와 실제 제어시스템 공격 사례를 중심으로 MAF 기반 공격전략 및 기술, 데이터소스 등의 구성 요소를 재정립하였다.

3.1. 공격전략 및 기술

MAF-I는 총 96종의 공격기술(Technique)을 11종의 공격전략(Tactic)과 매핑하여 매트릭스를 구성하였다. MAF-I의 공격전략은 MAF-E의 12종의 공격전략 중 'Privilege Escalation', 'Credential Access', 'Exfiltration'을 제외하고 모두 상속받아 사용하고 있다. 제어시스템 운영환경에 특화된 신규 공격전략 'Inhibit Response Function'와 'Impair Process Control'를 추가하였다.

MAF-I의 공격기술은 [그림 3]와 같이 MAF-E의 공격기술을 상호 참조(29종)하거나 MAF-I만의 신규 공격기술(67종)이 추가되었다. 특히, 신규 공격전략은 모두 신규 공격기술로 구성되었다.

3.2. 데이터소스

MAF-I는 [표 2]와 같이 총 36종의 데이터소스를 식별하였다. MAF-I는 MAF-E와 같이 단일 공격기술에 대해 복수개 이상의 데이터소스가 매핑되어 있다. 제어시스템의 알람 발생 조건이 되는 임계치, 알람 내역, 컨트롤러 파라미터 및 프로그램, 운전 및 제어 관련 정보를 생성하고 저장하기 위한 이벤트 레코더와 히스토리안 서버 등 MAF-I 신규 데이터소스로 7종이 추가되었다.

3.3. 자산

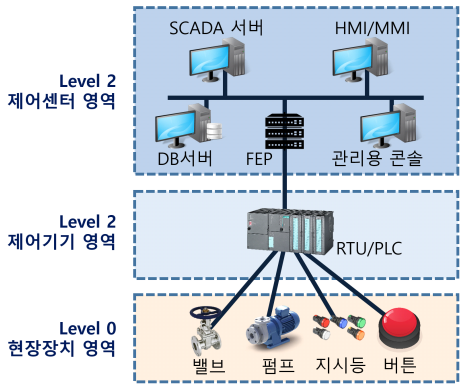
MAF-I는 [그림 3]과 같이 퍼듀 모델 기반 제어시스템 네트워크 구조를 참조하여 현장장치(Field device) 영역인 레벨 0, 프로세스 제어(Process Control)인 레벨 1, 감시 제어(Supervisory Control)인 레벨 2로 구성된

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		MSF-E 상호참조 공격기술
								System Firmware		
								Utilize/Change Operating Mode		MSF-I 신규 공격기술

〔그림 2〕 MAF-I 매트릭스 (MAF-E 내 공격기술 상호참조 포함)

〔표 2〕 MAF-I 데이터소스 유형 분류(*신규 데이터소스)

데이터소스	물리	네트워크	시스템
Alarm history*	✓		
Alarm thresholds*	✓		
Anti-virus			✓
API monitoring			✓
Application logs			✓
Asset management			✓
Authentication logs			✓
Binary file metadata			✓
Controller parameters*	✓		
Controller program*	✓		
Data historian*	✓		
Data loss prevention			✓
Detonation chamber			✓
Digital signatures*			✓
Email gateway			✓
File monitoring			✓
Host network interfaces		✓	
Mail server			✓
Malware reverse engineering			✓
Netflow/Enclave netflow		✓	
Network device logs			✓
Network intrusion detection system			✓
Network protocol analysis		✓	
Packet capture		✓	
Process command-line parameters			✓
Process monitoring			✓
Process use of network			✓
Sequential event recorder*	✓		
SSl/TLS inspection		✓	
Third-party application logs			✓
Web application firewall logs			✓
Web logs			✓
Web proxy			✓
Windows error reporting			✓
Windows event logs			✓
Windows registry			✓



〔그림 3〕 제어시스템 네트워크 구조

다[10]. 그 밖에 레벨 2의 상위 레벨은 엔터프라이즈로써 IT 영역에 속한다.

MAF-I는 [표 3]과 같이 총 11종의 독립적 자산을 제시하였다. 이를 제어시스템 네트워크 구조로 매핑 시 현장장치가 속하는 레벨 0에 해당하는 사항은 현재 식별되지 않은 상태이며, 주로 프로세스 제어(레벨 1)를 수행하는 제어시스템 및 제어기기와 운전 및 감시(레벨 2)를 수행하는 운전 및 관리 시스템으로 구성되어 있다.

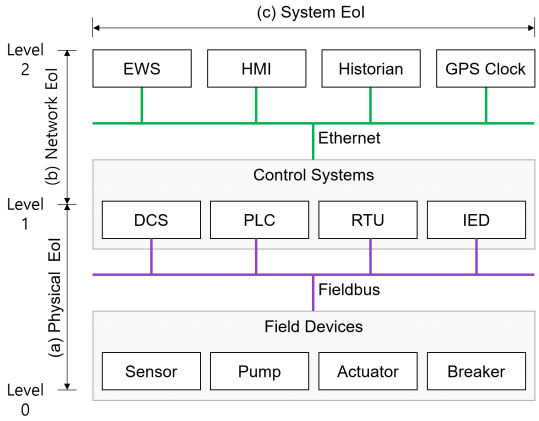
〔표 3〕 MAF-I 기반 자산 유형

구분	자산
레벨 1	· Field Controller · RTU (Remote Terminal Unit) · PLC (Programmable Logic Controller) · Protection Relay · IED (Intelligent Electric Device) · SIS (Safety Instrumented System)
레벨 2	· Control Server · HMI (Human-Machine Interface) · Data Historian · Input/Output Server · Engineering Workstation

Ⅳ. MITRE ATT&CK 기반 제어시스템 보안 모니터링 정보 유형 식별

본 장에서는 제어시스템 모니터링 정보 유형을 식별하기 위해 앞서 Ⅲ장에서 기술한 바와 같이 MAF-I의 제어시스템 네트워크 구조[1]를 기반으로 [그림 4]와 같

1) https://collaborate.mitre.org/attackics/in dex.php/All_Levels



〔그림 4〕 제어시스템 모니터링 정보 유형 식별

이 도식화하였다.

우리는 제어시스템 보안위협의 수직적/수평적 전파를 고려하여 모니터링 대상이 되는 정보를 생성하는 주체와 각 주체 간 경로를 기준으로 모니터링 관심 정보(EoI, Event of Interest)와 유형을 식별하였다.

첫째, 레벨 0와 레벨 1 사이의 경로 상의 정보를 물리 EoI로 정의하였다. 물리 EoI는 제어시스템과 현장장치 간 통신경로(Hard-wired, Fieldbus 등) 상의 물리적 신호 정보가 해당한다. 둘째, 레벨 1과 레벨 2 사이의 경로 상의 정보를 네트워크 EoI로 정의하였다. 네트워크 EoI는 운전 및 관리 시스템과 제어시스템 간 통신경로(Ethernet) 상의 네트워크 트래픽 정보를 포함한다. 셋째, 모든 레벨에 속한 시스템 및 기기가 생성하는 정보를 시스템 EoI로 정의하였다. 특히, 시스템 EoI는 시스템 특성에 따라 네트워크 및 보안장비, 서버/호스트, 제어시스템 및 제어기기 관련 모니터링 정보를 정보로 세분화하였다.

Tactics	Techniques (ICS)	EoI category	Data source
TA0001	T1190 (T819) Exploit Public-Facing Application	Network	Packet capture
		System	Web application firewall logs
			Application logs
			Web logs

〔그림 5〕 MAF 기반 제어시스템 보안 모니터링 정보 식별

이를 통해, [그림 5]와 같이 제어시스템 보안 모니터링 정보를 MAF-I의 각 공격전략 및 공격기술에 따라 EoI 유형, 데이터소스로써 식별할 수 있다.

4.1. 네트워크 정보

네트워크 정보는 레벨 1과 레벨 2에 속하는 시스템 간 통신에 의해 생성되는 네트워크 트래픽을 포함한다. 네트워크 정보는 헤더와 페이로드를 모두 포함하는 원시 데이터 수준으로 제어시스템 및 제어기기가 사용하는 프로토콜에 따라 그 형태가 다를 수 있다.

4.2. 시스템 정보

4.2.1. 네트워크 및 보안장비

상용 보안장비의 도입 및 운영 영역이 제어시스템으로 확대됨에 따라 CheckPoint사 Security Gateway, GE사 OpShield 등 기존 IT 영역 외 OT 영역의 보안 감시를 목적으로 한 다양한 상용제품이 출시되고 있다. 침입탐지 및 차단시스템, 방화벽 등 상용 보안장비의 경우, 보안위배 발생 시 탐지한 상황(공격 유형, 발생 시각, 공격 관련 IP 및 포트번호 등)에 대한 이벤트 로그, 보안장비 운영 현황(시스템 자원 현황, 시스템 설정 변경 내역 등)에 대한 감사로그 등 다양한 유형의 로그 생성 및 저장 기능이 내재되어 있다.

4.2.2. 서버 및 호스트

서버 및 호스트 정보는 시스템의 CPU, 메모리, 저장소 등에 해당하는 자원정보와 시스템 상에서 사용 중인 계정, 파일, 서비스(프로세스) 등과 관련된 감사정보로 구분된다. 자원정보의 경우, 서버 및 호스트의 운영 건전성을 확인하기 위해 활용될 수 있다. 감사정보는 서버 및 호스트 상 사용자 또는 자체 프로세스에 의해 추가/삭제/변경되는 각종 사항들에 대한 이력 등을 확인할 수 있다.

4.2.3. 제어시스템 및 제어기기

제어시스템 및 제어기기는 고성능화/고사양화에 따

라 기본적인 제어 및 감시 외 다양한 기능을 제공하고 있다. 특히, SIEMENS사의 S7-1500 모델의 경우 [표 4]와 같이 PLC로부터 다양한 진단정보를 통해 제어기기의 운전 현황 및 이력을 확인할 수 있다.

〔표 4〕 PLC 진단정보

구분	진단정보
자원	· PLC 이름, 버전, CPU 모델, 펌웨어 버전 등 · 설치 위치(랙 및 슬롯 번호) · 자원 사용률(CPU, 메모리)
감사	· 현재 운전 모드(RUN, STOP) · 운전모드 변경 여부 · 제어명령 실행 오류, 동기화 오류 등 · 사용자 계정 인증 감사(성공, 실패, 잠금)

4.3. 물리(운전) 정보

제어시스템 및 제어기기는 센서, 액츄에이터 등 현장기기와 연결되어 계측 및 운전을 수행하게 된다. 이 때, 제어시스템 및 제어기기는 제어로직에 따라 센서의 계측정보(온도, 압력, 유량 등)로 현장상황을 모니터링하거나 이 정보를 기반으로 컨트롤 밸브, 액츄에이터 등의 운전 파라미터(개돗값, 응동값 등) 결정에 활용하여 제어하게 된다. 따라서, 물리(운전) 정보는 IT 영역의 서버-호스트 간 네트워크 트래픽 정보와 유사하다. 물리(운전) 정보는 주로 Control Output (CO), Set Point (SP), Process Value (PV)로 구성된다.

Ⅴ. MITRE ATT&CK 기반 제어시스템 보안 모니터링 정보 수집 방안

5.1. 네트워크 정보

네트워크 정보 수집은 Active 방식과 Passive 방식으로 구분된다. Active 방식은 네트워크 정보 수집 대상이 되는 기존 시스템의 설정 변경을 통해 이뤄진다. Active 방식의 대표적인 네트워크 트래픽 수집 방식으로써 포트 미러링(SPAN)이 있다. Passive 방식은 네트워크 정보 수집 대상이 되는 시스템 외 별도의 장비를 이용하여 설정 변경을 최소화하여 수집이 이뤄지며 네트워크 태핑이 대표적 예이다.

5.2. 시스템 정보

5.2.1. 네트워크 및 보안장비

일반적으로 네트워크 및 보안장비는 로그 저장소의 용량 한계를 해결하고 실시간 이벤트 로그 전송을 위해 로그 관리 및 백업 서버, SIEM 등의 외부 시스템으로 로그를 전송하는 기능을 부가적으로 제공한다.

네트워크 및 보안장비로부터 이벤트 로그를 수집하기 위해 해당 장비에서 제공하는 로그 전송기능을 사용할 수 있다. 일반적으로 네트워크 및 보안장비는 'SNMP'나 'Syslog'를 통해 외부 시스템으로 로그 전송 기능을 제공하며, 정보 규격은 'Syslog', 'CEF' 등 제조사 및 모델에 따라 상이하다. 'Syslog'의 경우, Polling 방식이 아닌 Push 방식으로써 별도의 요청 메시지 없이 로그 수집이 가능하다. 또한, 네트워크 및 보안장비의 자체 로그전송 기능을 활용하기 때문에 제어시스템 운영상 영향을 미치지 않는다.

5.2.2. 서버 및 호스트

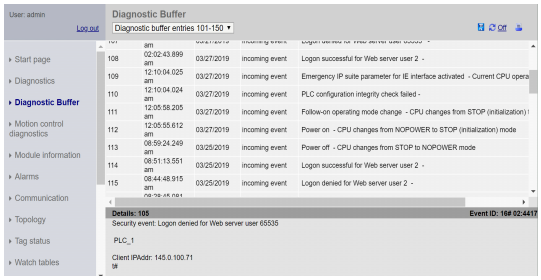
제어시스템 운영 및 관리를 위해 관리시스템(EWS, Engineering WorkStation), HMI (Human- Machine Interface), 히스토리안 서버 등 다양한 서버 및 호스트가 운영된다. 이러한 제어시스템 운영환경 내 서버 및 호스트는 모두 시스템 운영체제와 무관하게 시스템 감사정보 관리를 위한 서비스를 제공하고 있다. 리눅스 시스템의 경우 'auditd', 'syslogd' 등 다양한 시스템 감사용 데몬이 제공되며 이를 통해 생성되고 저장된 로그를 활용할 수 있다. 반면, 윈도우 시스템의 경우, 윈도우 로컬정책, 감사정책 등에서 기본 적용된 정책 또는 사용자 정의 정책에 의해 생성되고 저장되는 윈도우 이벤트 로그를 활용할 수 있다.

리눅스/윈도우 시스템의 로그를 외부로 전송하기 위해 기존 제공되는 서비스를 사용하거나 별도의 프로그램 설치가 필요하다. 하지만, 고가용성이 요구되는 제어시스템 운영환경을 감안하여 기존 시스템에 포함된 서비스 및 프로그램의 구성을 통한 시스템 정보 수집 방안에 초점을 두었다. 리눅스 시스템의 경우 대부분 기본적으로 설치되어 있는 'rsyslogd'을 통해 로컬 시스템 로그를 외부로 전송할 수 있다. 윈도우 시스템의 경우

‘Windows Event Collector[2]’을 통해 윈도우 이벤트 로그를 획득할 수 있다.

5.2.3. 제어시스템 및 제어기기

제어시스템 및 제어기기 정보를 수집하기 위해 엔지니어링 도구를 활용하거나 PLC 자체 지원기능을 활용할 수 있다. PLC의 운영현황 정보를 사용자가 확인할 수 있도록 [그림 6]과 같이 웹 인터페이스 및 화면을 제공하고 있다. 이러한 기능을 활용하여 PLC 진단정보 수집 소프트웨어를 통해 제조사 전용 통신규격으로 인한 제약 없이 다양한 PLC로부터 시스템 정보를 수집할 수 있다[11].

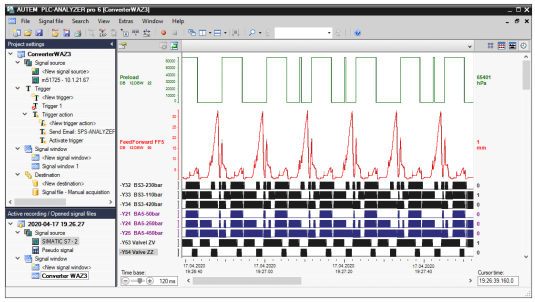


〔그림 6〕 SIEMENS사 S7 PLC 진단 웹 화면

5.3. 물리(운전) 정보

물리(운전) 정보를 수집하기 위해서는 별도의 시스템, 해당 정보를 기록한 시스템 등을 활용할 수 있다.

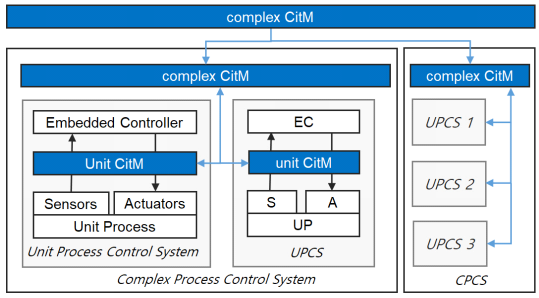
상용 제품인 Autem사의 BLACKBOX[3]는 [그림 7]과 같이 PLC와 현장장치 사이의 통신경로 상의 아날로그 신호, 디지털 신호 등 물리(운전) 정보를 수집 및 저장하는 기능을 제공한다.



〔그림 7〕 BLACKBOX3 물리(운전) 정보 수집 화면

또한, [그림 8]과 같이 PLC와 현장장치 사이에 별도의 PLC를 설치하고 상호 물리적 결선을 통해 물리(운전) 정보를 수집하는 CitM(Controller-in-the- Middle) 방식을 활용할 수 있다[12].

제어시스템 운영환경 내 OPC(OLE for Process Control) 서버를 포함할 경우, OPC를 통해 물리적 구성 변경 없이 소프트웨어 설정 만으로 물리(운전) 정보를 수집할 수 있다. 또한, 해당 정보를 저장하고 있는 히스토리안 서버가 운영 중일 경우, 데이터베이스 커넥터 등을 활용하여 저장된 물리(운전) 정보를 수집할 수 있다.



〔그림 8〕 CitM 구성

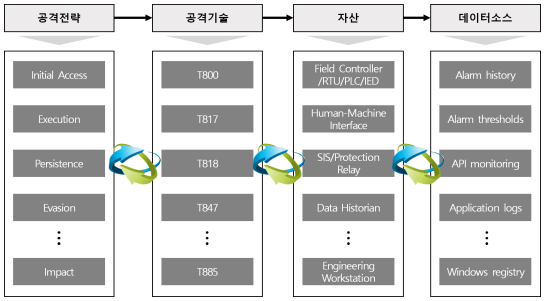
Ⅵ. MITRE ATT&CK 기반 제어시스템 보안 모니터링 정보 분석 방안

6.1. MAF-I 종속성 확인

제어시스템 보안 모니터링 정보 분석을 수행하기 위해 분석 대상으로 하는 공격전략과 공격기술에 대해 결정해야 한다. 이 후, 해당 공격기술이 대상으로 하는 자산을 식별하고, 그 자산으로부터 보안위협을 모니터링하기 위한 데이터소스를 식별해야 한다. 하지만, 이러한 작업을 위해 MAF-I 기반 제어시스템 보안 모니터링 정보 분석을 위해 [그림 9]의 구성 요소 간 상호 종속성을 사전에 고려해야 한다.

이 때, MAF-I의 구성 요소는 상호 다중 종속성을 포함할 수 있다. 예를 들어, 단일 공격전략을 위해 2개 이상의 공격기술이 사용될 수 있고, 개별 공격기술이 대상으로 하는 자산이 다양한 시스템일 수 있다. 또한, 공격

2) https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector
3) https://www.autem.de/products/blackbox_e



〔그림 9〕 MAF-I 구성 요소 간 상호 종속성

기술에 따라 각 시스템으로부터 확인해야 할 데이터소스도 서로 다를 수 있다.

6.2. MAF-I 기반 EoI 통합 분석 및 대응

기존 제어시스템 보안 모니터링은 정보 식별 및 수집 방안에 대한 부재로 근본적으로 가시성이 확보되지 않았다. 최근, 기반시설 제어시스템에 특화된 상용 네트워크 및 보안장비의 도입과 제어시스템 기능이 고도화됨에 따라 가시성 확보를 위한 노력이 진행되고 있다. 하지만, 단일 데이터소스 기반 개별 시스템을 통한 제어시스템 보안위협 분석은 제한적일 수 밖에 없다.

일반적으로 제어망은 에어갭(Air-gap)을 통해 물리적으로 외부망과 단절되어 운영되는 폐쇄망 정책을 유지하고 있다. 보안위협이 정교해지고 기술이 발전함에 따라 폐쇄망의 보안 대책만으로는 한계가 있다. Stuxnet은 이동형 저장매체를 통해 에어갭을 우회하였으며, PowerHammer와 같이 송전선을 이용한 에어갭 우회를 통해 망 분리된 컴퓨터의 데이터를 추출하기도 하였다[13]. 한편, 4차 산업혁명으로 촉발된 디지털 전환으로 기기 간 연결성이 강화되고 무선화되면서 제어망과 외부망의 경계가 모호해지고 있다.

따라서, 제어시스템 보안위협 및 기술 현황을 고려하여 MAF-I 기반 제어시스템 보안 모니터링 정보 분석을 위해 앞서 기술한 바와 같이 실제로 다양한 데이터소스로부터 수집한 EoI가 필수적이다. 또한, 제어시스템 보안위협의 수직적 전파를 모니터링 하기 위해 물리(운전) EoI, 네트워크 EoI과 수평적 전파를 감시하기 위해 시스템 EoI를 모두 분석 대상으로 해야 한다. 제한적 EoI 분석은 공격기술을 구분할 때 필연적으로 오탐 또는 미탐을 발생시킬 수 있다. 따라서, MAF-I 기반 공격기술의 정교한 모니터링을 위해 가능한 다양한 EoI를 통합적으로 활용하여 분석해야 한다.

MAF-I 기반 제어시스템 모니터링 정보 분석은 현재 보안위협이 실제 어느 단계까지 진행되었으며 공격에 영향을 받은 자산 식별 등 보안위협 전이 양상을 파악할 수 있다. 또한, 과거의 분석 결과를 통해 비슷한 양상이 확인된 경우 향후 진행될 공격전략 및 기술, 공격대상 자산을 선제적으로 파악하여 대응에 활용할 수 있다.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
(1) Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	**(5) Control Device Identification**	Default Credentials	**(8) Automated Collection**	Commonly Used Port	**(10) Activate Firmware Update Mode**	**(14) Brute Force I/O**	Damage to Property
Drive-by Compromise	**(2) Command-Line Interface**	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	**Denial of Control**
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	**(3) Network Connection Enumeration**	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	**(11) Block Command Message**	**(12) Masquerading**	**Denial of View**
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		**(11) Block Reporting Message**	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		**(11) Block Serial COM**	Modify Parameter	**Loss of Control**
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	**(4) Remote System Discovery**	Valid Accounts	Location Identification		**(9) Data Destruction**	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	**(6) Serial Connection Enumeration**		Monitor Process State		**(10) Denial of Service**	Program Download	**Loss of Safety**
Spearphishing Attachment	Scripting					Point & Tag Identification		**(10) Device Restart/Shutdown**	Rogue Master Device	**Loss of View**
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	**(15) Service Stop**	**Manipulation of Control**
Wireless Compromise						**(7) Role Identification**		Modify Alarm Settings	Spoof Reporting Message	**Manipulation of View**
						Screen Capture		Modify Control Logic	**(13) Unauthorized Command Message**	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

〔그림 10〕 MAF-I 기반 제어시스템 보안 모니터링 적용 - 2016년 우크라이나 변전소 공격 사례 (Industroyer)

〔표 5〕 MAF-I 기반 제어시스템 보안 모니터링 적용 - 2016년 우크라이나 변전소 공격 사례 (Industroyer)

공격전략	공격기술	ID	자산	데이터소스
Initial Access	Data Historian Compromise	T810	Data Historian	-
Execution	Command-Line Interface	T807 (T1059)	-	Process monitoring, Process command-line parameters, Network protocol analysis, Packet capture
Discovery	Control Device Identification	T808	Field Controller/RTU/PLC/IED	Network protocol analysis, Packet capture
	Network Connection Enumeration	T840	HMI	Process monitoring, API monitoring
	Remote System Discovery	T846 (T1018)	Control Server, Data Historian, SIS/Protection Relay, Field Controller/RTU/PLC/IED, HMI	Process monitoring, Process use of network, Process command-line parameters, Network protocol analysis
	Serial Connection Enumeration	T854	Input/Output Server, Field Controller/RTU/PLC/IED	Network protocol analysis, Packet capture
Collection	Automated Collection	T802 (T1119)	Field Controller/RTU/PLC/IED, SIS/Protection Relay, Control Server	File monitoring, Data loss prevention, Process command-line parameters
	Role Identification	T850	HMI, Control Server, Data Historian, Field Controller/RTU/PLC/IED	Network protocol analysis, Packet capture
Inhibit Response Function	Activate Firmware Update Mode	T800	Field Controller/RTU/PLC/IED, SIS/Protection Relay	Application logs, Sequential event recorder, Network protocol analysis, Packet capture
	Block Command Message	T803	Field Controller/RTU/PLC/IED	Alarm History, Network protocol analysis, Packet capture
	Block Reporting Message	T804	Field Controller/RTU/PLC/IED, Input/Output Server	Alarm History, Data historian, Network protocol analysis, Packet capture
	Block Serial COM	T805	Field Controller/RTU/PLC/IED, Input/Output Server	Alarm history, Data historian, Network protocol analysis, Packet capture
	Data Destruction	T809	Control Server, HMI, Field Controller/RTU/PLC/IED	File monitoring, Process command-line parameters, Process monitoring
	Denial of Service	T814	Field Controller/RTU/PLC/IED, SIS/Protection Relay	Alarm history, Data historian, Network protocol analysis, Packet capture, Sequential Event Recorder
	Device Restart/ Shutdown	T816	Field Controller/RTU/PLC/IED	Sequential event recorder, Alarm history, Network protocol analysis, Packet capture
Impair Process Control	Brute Force I/O	T806	Control Server, Field Controller/RTU/PLC/IED	Alarm history, Sequential event recorder, Data historian, Netflow/Enclave netflow, Network protocol analysis, Packet capture
	Masquerading	T849	HMI, Control Server	File Monitoring, Process monitoring, Binary file metadata
	Service Stop	T881	HMI, Control Server, Data Historian, Engineering Workstation	Process command-line parameters, Process monitoring, Windows Registry, API monitoring
	Unauthorized Command Message	T855	Field Controller/RTU/PLC/IED	Alarm history, Sequential event recorder, Netflow/Enclave netflow, Network protocol analysis, Packet capture

6.3. 사례 중심 MAF-I 기반 모니터링 적용 예시

우리는 2016년 우크라이나 변전소 공격을 통해 대정전을 야기한 제어시스템 멀웨어 Industroyer(일명 CrashOverride) 사례를 중심으로 MAF-I 기반의 제어시스템 보안 모니터링을 수행하기 위해 [그림 10]과 같이 공격전략 및 공격기술을 매핑하였으며, 구체적인 구성요소별 세부내용을 [표 5]와 같이 식별하였다.

Industroyer는 Impact를 제외한 5개의 공격전략에 따라 19개의 공격기술이 사용되었다. 따라서, MAF-I 기반 제어시스템 보안 모니터링 시 각 공격기술을 탐지하기 위해 최소한 15종의 데이터소스로부터 EoI를 수집하고 분석해야 함을 알 수 있다. 특히, ‘Execution’의 ‘Command-Line Interface(T807/ T1059)’, ‘Discovery’의 ‘Remote System Disco- very(T846/T1018))’, Collection의 ‘Automated Collection(T802/T1119)’의 경우, MAF-E의 공격기술을 상호 참조하고 있기 때문에 레벨 0에서 레벨 2의 제어시스템 네트워크 뿐 만 아니라 상위 레벨까지 모니터링 영역을 확장하여 IT망에서 OT망으로 침투에 의한 보안위협의 수직적 전파 또는 각 망 내 수평적 전파를 감시할 수 있다. 또한, 일반적으로 사용되는 이더넷 네트워크 통신이 아닌 시리얼 통신(COM 포트)을 통한 보안위협 전파 등 기존 IT와 다른 공격 경로 및 과정의 변형에 대해서도 보안 가시성을 확보할 수 있음을 보여준다.

Ⅶ. 결 론

본 논문에서는 MITRE ATT&CK 프레임워크를 기반으로 제어시스템 보안 모니터링 방안을 기술하였다. 본 방안 수립을 위해 제어시스템 보안 모니터링을 위해 필요한 정보를 식별하고 유형을 분류하였으며, 각 유형에 따라 모니터링 정보를 수집하고 통합적으로 분석하기 위한 방안과 적용 사례를 제시하였다. 본 논문을 통해 제시한 방안을 참조하여 제어시스템 운영환경의 보안 가시성 확보를 위한 기반기술로 활용될 수 있을 것으로 기대한다.

참 고 문 헌

[1] S. Rizvi, R. J. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, “Identifying the attack surface for IoT network,” *Internet of Things*, Vol. 9, 2020.

[2] R. Lee, J. Slowik, B. Miller, A. Cherepanov, and R. Lipovsky, “Industroyer/crashoverride: Zero things cool about a threat group targeting the power grid,” *Black Hat USA*, 2017.

[3] R.Spenneberg, M. Brüggemann, and H. Schwartke, “PLC-Blaster: A worm living solely in the PLC,” *Black Hat Asia*, pp. 1-16, 2016.

[4] D. Formby, S. Durbha, and R. Beyah, “Out of control: Ransomware for industrial control systems,” *RSA conference*, 2017.

[5] S. K. Damodaran and P. D. Rowe, “ Limitations on observability of effects in cyber-physical systems,” *In Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (HotSoS '19)*, pp. 1-10, April 2019.

[6] H. Shin, W. Lee, J. Yun, and H. Kim, “Implementation of programmable CPS testbed for anomaly detection,” *USENIX Workshop on Cyber Security Experimentation and Test (CSET '19)*, Aug. 2019.

[7] H. Shin, W. Lee, J. Yun, and H. Kim, “HAI 1.0: HIL-based augmented ICS security dataset,” *USENIX Workshop on Cyber Security Experimentation and Test (CSET '20)*, Aug. 2020.

[8] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “MITRE ATT&CK: Design and philosophy,” MP180360, MITRE Corporation, July 2018.

[9] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, pp. 80, 2011.

[10] Pascal Ackerman, “Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems,” Packt Publishing, 2017.

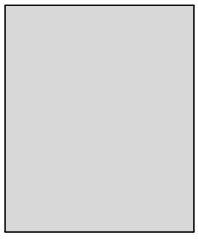
[11] J. Choi, H. Kim, S. Choi, J. Yun, B. Min, and H. Kim, “POSTER: Vendor- Independent Monitoring on Programmable Logic Controller

Status for ICS Security Log Management," *In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (AsiaCCS '19)*, pp. 682-684, July 2019.

[12] S. Choi, W. Lee, H. Shin, J. Yun, and S. Kim, "POSTER: CPS Security Testbed Development Using Controller-in-the- Middle," *In Proceedings of the 2018 on Asia Conference on Computer and Communications Security (ASIACCS '18)*, pp. 829-831, May 2018.

[13] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "PowerHammer: Exfiltrating Data From Air-Gapped Computers Through Power Lines," *in IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1879-1890, 2020.

〈저 자 소 개〉



최 승 오 (Seungoh Choi)

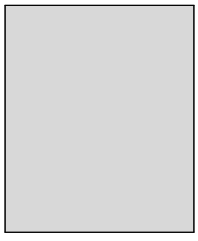
정회원

2012년 : 아주대학교 정보 및 컴퓨터공학과 졸업

2014년 : 아주대학교 컴퓨터공학과 공학석사

2013년~현재 : ETRI 부설연구소 선임연구원

<관심분야> SCADA 보안, 제어시스템 보안, 제어 프로토콜, 네트워크 보안



김 형 천 (HyoungChun Kim)

정회원

1999년 : 고려대학교 전산학과 졸업

2001년 : 고려대학교 일반대학원 전산과학전공 석사

2011년 : 고려대학교 정보보호대학원 공학박사

2001년~현재 : ETRI 부설연구소 책임연구원/실장

<관심분야> 인공지능, 제어시스템 보안, 클라우드 컴퓨팅 보안, 운영체제 보안