Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 3 pp. 409-415, 2023

https://doi.org/10.5762/KAIS.2023.24.3.409
ISSN 1975-4701 / eISSN 2288-4688

기업보안사고 예측을 위한 시나리오 기반 평가 시스템에 대한 연구

홍명수[1], 이용준[2*]
[1]극동대학교 인공지능보안학과 [2]극동대학교 해킹보안학과

A Study on the Scenario-Based Evaluation System for Predicting Corporate Security Accidents

Myung-Su Hong[1], Yong-Joon Lee[2*]
[1]Department of Artificial Intelligence, Far East University
[2]Department of Hacking Security, Far East University

요 약 4차 산업시대 신기술의 융합으로 다양한 스마트기기가 네트워크 연결과 소프트웨어로 작동하고 빅데이터를 기반으로 개발된 머신러닝 등 인공지능 기술이 사이버 공간으로 융합되고 있기 때문에 신산업의 발달로 새로운 보안위협이 지속적으로 증가하고 있다. 기존의 보안사고에 대한 대응방법들이 다양하게 존재하지만 이미 발생했던 공격방식에 대해서 탐지할 경우 조치가 늦어지는 문제점 외에 새로운 공격시도에 대한 예방도 이루어지기 힘든 상황이다. 이는 기존 통합보안제품은 통합적인 상호 연관성을 제공하나 발생 가능한 보안사고를 특정하지는 못하며 보안담당자의 인적 분석에 많이 의존하기 때문이다. 따라서 본 논문에서는 알려진 보안사고뿐만 아니라 발생 가능한 전체 보안사고 유형을 보안위협의 전략과 전술로 분류하는 방법을 소개하고 MITRE ATT&CK 프레임워크 분석을 통해 보안사고 프로파일링 서비스를 시나리오 기반으로 시뮬레이션 할 수 있는 기술을 소개한다. 이로 인해 보안사고의 예측 및 대응, 관리를 종합적으로 판단할 수 있을것이라 기대한다.

Abstract New security threats continue to increase because of the development of new industries as various smart devices operate with network connections and software, and artificial intelligence technologies, such as machine learning developed based on big data, are being fused into cyberspace. There are various ways to respond to security accidents, but when detecting an attack method that has already occurred, it is difficult to prevent new attack attempts in addition to the problem of delayed action. This is because existing integrated security products provide integrated interrelationships, but do not specify possible security incidents and rely heavily on human analysis by security personnel. Therefore, this paper introduces how to classify known security incidents and all possible types of security incidents into security threat strategies and tactics and introduces a technology that can simulate security incident profiling services based on scenarios through MITRE ATT&CK framework analysis. Hence, it may be possible to judge the prediction, response, and management of security accidents comprehensively.

Keywords : Security, Attack, Artificial Intelligence, Prevent, Prediction

*Corresponding Author : Yong-Joon Lee(Far East Univ.)
email: 2020032@kdu.ac.kr
Received January 26, 2023 Revised March 2, 2023
Accepted March 3, 2023 Published March 31, 2023

1. 서론

4차 산업시대의 신기술 융합으로 다양한 스마트기기가 네트워크 연결 및 소프트웨어로 동작하면서 경제, 사회 전 분야에서 스마트화가 추진 중에 있으며 새로운 산업이 발전되면서 이로 인한 신종 보안위협도 계속적으로 증가하고 있기 때문에 이미 알려진 보안사고에 대한 예방뿐만 아니라 발생가능한 보안사고를 예측하여 공공 및 기업에서 발생하는 내·외부 보안사고를 예방할 수 있는 기술이 필요하다[1].

기존의 보안사고에 대한 대응방법들은 이미 발생했던 공격방식에 대해서만 예방할 뿐 새로운 공격시도에 대해서는 조직 내에서 발생하는 보안사고에 대한 예방이 이루어지지 않고 있다. 이는 개별 보안제품을 통합하여 정보를 제공하더라도 발생 가능한 보안사고의 예측정보를 제공하지 않기 때문인데 이러한 보안사고를 '사고 후 대응'에서 '사전 예방'으로 전환하기 위해서는 발생 가능한 보안사고를 유형별로 사전에 예측·평가하는 기술 개발이 필요하다.

따라서 본 논문은 기존 보안솔루션의 대응 중심의 한계를 파악하고 국내·외 사이버보안 프레임워크 및 ATT&CK 정보를 활용하여, 공공 및 기업의 전체 보안사고 유형을 분석하고 보안제품의 보안로그를 수집하여 보안사고 유형별 발생 가능성을 정량화하여 발생 가능한 보안사고위협을 사전에 예측·평가하여 보안사고 유형별로 사전 대응이 가능할 수 있는 방안을 제시한다.

본 논문은 다음과 같이 구성한다. 2장의 관련연구에서 기업의 보안사고 위협사례, 기존 통합보안제품의 한계, ATT&CK 프레임워크 분석을 소개한다. 제안하는 시스템으로는 보안사고 프로파일링 서비스, 보안사고 시나리오 서비스 및 생성된 시나리오 기반 시뮬레이션 실험 결과를 나타낸다. 3장에서는 제안된 기술에 대한 결론 및 향후 연구 방향을 설명한다.

2. 본론

2.1 관련 연구

2.1.1 보안사고 위협사례

1) 카세야 사태

미국 독립기념일 연휴기간동안 발생한 미국 IT 관리용 솔루션 제공 업체 '카세야(Kaseya)'의 VSA(IT 관리용 플랫폼) 제품이 랜섬웨어 유포 경로로 악용된 사건으로 레빌(REvil) 랜섬웨어 조직에 의해 감행된 공급망 공격이었다. VSA 서버를 통해 고객사 약 200여 곳에 랜섬웨어가 업데이트 되어 파일들이 암호화되는 피해를 입게 되었는데 당시 스웨덴의 슈퍼마켓 체인 COOP은 전산망 마비로 점포 800여 곳의 문을 닫은 것으로 알려졌다[2].

2) 서울성모병원 홈페이지 해킹

2021년 9월 1일에는 가톨릭대학교 서울성모병원의 구 홈페이지가 해킹을 당해 회원 개인정보가 유출된 사건이 있었다. 2013년 2월 이전에 가입한 회원을 대상으로 ID와 패스워드는 물론 민감정보인 주민등록번호가 포함된 것으로 알려졌다[3].

3) ICS/OT 관련 사이버침해사고 사례

랜섬웨어는 IT 환경에서 이미 널리 알려진 해킹 유형의 하나로 인식되어 왔으나, 최근에는 OT환경에서도 사이버 위협에 사용되는 대표적인 사이버 공격 유형으로 자리잡고 있다. 최근에는 해킹그룹이 피해 기업의 서버 및 단말기 내 전자파일을 암호화하고 몸값을 요구하는 것에 그치지 않고, 피해 기업의 내부 시스템 및 네트워크에 더 깊숙이 파고들어 추가로 금전적 수익을 창출할 수 있는 방향으로 진화하고 있다. 랜섬웨어 공격의 경우 피해기관은 해킹 피해사실이 언론에 노출되는 것을 원하지 않으며, 금전적 이익이 주된 목적의 공격그룹도 사회적으로 이슈화 되는 것을 원하지 않는다는 점이 특장점인데, 이러한 특징 때문에 랜섬웨어를 이요한 해킹공격은 하나의 서비스 형태(RaaS : Ransomeware as a Service)로 발전하면서 그 규모와 세력을 키우고 있다.

이 외에도 Table 1에서 보는 바와 같이 보안사고 위협사례는 점차 증가하고 있는 추세이다.

Table 1. Security Incident Cases

Victim organization	Nation	Year	Attack Type
Colonial Pipeline	USA	2021	Ransomware (Darkside)
Sol Oriens	USA	2021	Ransomware (REvil)
JBS Foods	USA	2021	Ransomware (REvil)
Honda	Japan	2020	Ransomware (EKANS)
Norsk Hydro	Norway	2019	Ransomware (LockerGoga)
Lake City	USA	2019	Ransomware (Ryuk)

Wood Ranch Medical	USA	2019	Ransomware
Petrochemical Plant	Saudi	2017	APT(Triton)
Power Supply Company	Ukraine	2015/ 2016	APT (Black Energy)
The Bushehr Nuclear Power Plant	Iran	2010	APT(Stuxnet)

2.1.2 기존 통합보안제품의 한계

1) SIEM(보안정보 이벤트 관리)

보안정보 이벤트 관리 솔루션인 SIEM은 조직에서 비즈니스에 문제를 일으키기 전에 보안 위협을 탐지, 분석 및 대응하도록 도와주는 솔루션으로 보안정보관리(SIM: Security Information Management, 이하 SIM)와 보안 이벤트 관리(SEM: Security Event Management, 이하 SEM)의 기능을 하나의 보안 관리 시스템으로 통합한 솔루션이다. SIEM은 여러 원본에서 이벤트 로그 데이터를 수집하고 실시간 분석을 바탕으로 정상적인 범위를 벗어나는 활동을 식별하여 조치를 취하는 방식으로 이루어진다.

Fig. 1에서 보는 바와 같이 SIEM은 보안 이벤트의 장기적 분석과 함께 실시간 보고 기능을 통해 IT 보안에 대한 포괄적 방어 체계를 제공하는데 주요기능으로는 데이터 통합, 상관관계, 알림, 대시보드 등의 기능을 제공하고 있다[4].

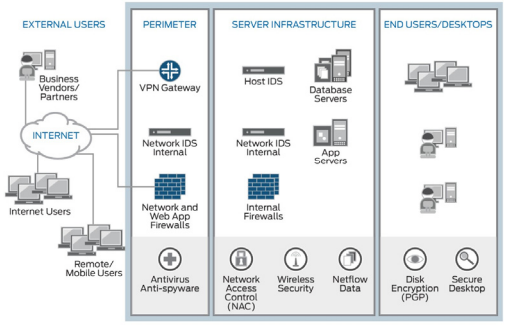

Fig. 1. SIEM Composition[5]

Table 2는 기존 통합보안제품의 주요기능 및 활용성을 나타내고 있다.

Table 2. Special Feature

Division	SIEM	ESM
Function	Integrated management of information and security events of resources within the enterprise	Centralized security information collection and management to control and operate individual security systems
Collection	Collect information, logs, and security threat information of resources generated within the enterprise. Structured/Unstructured Data	Collect security threat information required for security control Structured data
Method	Collect log events such as security systems, server systems, networks, and applications, and the security staff analyzes audit information.	Integrated security threat information such as security system and server system and provided to security control Use by security personnel as a correlation analysis in the event of a security accident
Feature	Association analysis of applications, users, protocols, etc. Apply security rules entered by security personnel Detection of new security threat information such as APT and Ransomware	Detect network through detection rules such as IP/Port Known Attack Analysis and Short/Large Analysis Simple pattern-based detection
Usability	Integrated analysis of external security threat information and internal vulnerabilities Used by security personnel to investigate security incidents (post-security audit)	Use to quickly respond to a large number of known real-time security incidents (real-time security controls)

기업들이 랜섬웨어에 취약해지고 있는 데에는 몇가지 공통적인 보안문제로 인함인데 정리하자면 다음과 같다.

1) 중요한 네트워크와 제어 시스템으로 공격이 확대되는 것을 제한하기 위한 운영기술 및 네트워크 망분리 미흡
2) 핵심자산 및 시스템에 대한 침투경로와 취약점에 대한 인식 부족
3) 회복탄력성 및 사업연속성의 효과성을 검증하기 위한 백업 및 복구테스트의 부족
4) 시스템의 관리자 권한 및 원격접속 시 강화된 인증수단의 부재(멀티펙터 인증 등)
5) 부적절한 취약점 관리와 시스템 전반적인 패칭 사이클 및 테스트 관리 미흡
6) 비즈니스 연속성을 지원하기 위한 랜섬웨어 사고대응 계획 수립 및 이행 부족
7) 비정상적인 업로드에 대해 제한적인 모니터링 역량
8) 사이버 위협에 대한 시각차이에 따른 제각기 다른 사고 대응 및 회복탄력성 계획 수립

2.1.3 MITRE의 ATT&CK 프레임워크 분석

ATT&CK(Adversary Tactics and Techniques, Common Knowledge)는 본래 미국 연방정부의 지원을 받으며 국가안보관련 업무를 수행하던 비영리 연구개발 단체인 MITRE社에서 국가간 사이버 공격의 영향력이 커지고 피해가 늘어나면서 자연스럽게 해당 부분에 대한 연구를 시작하였으며, 그렇게 만들어진 프레임워크로 볼 수 있다. 제공하는 표준 프레임워크로는 네트워크 내에 활동하는 공격자의 실제행위를 기반으로 전술, 기술, 절차, 사용한 공격소프트웨어 등 사이버 킬체인 7단계를 14단계로 폭 넓은 공격 프로세스가 존재한다. ATT&CK Framework는 MITRE에서 실제 공격 사례를 바탕으로 킬 체인(Cyber Kill Chain)의 단계를 자체적으로 개발하여 정리한 것으로, 먼저 사이버 킬체인에 대한 이해가 필요하다.

사이버 킬체인은 사이버 공격을 분석하기 위한 가장 널리 알려진 모델로 기존 군사용어인 킬체인 (Kill Chain, 타격순환체계)에서 비롯되었으며 발사된 미사일을 요격하는 것이 아닌, 선제 공격을 통해 미사일 발사 자체를 저지하겠다는 것으로서 그 개념을 사이버 공간상으로 가져와 적용한 것이다.

마이터 어택(MITRE ATT&CK)은 공격자들의 최신 공격 기술 정보가 담긴 저장소 Adversarial Tactics, Techniques, and Common Knowledge의 약어이며, 실제 사이버 공격 사례를 관찰한 후 공격자가 사용한 악의적 행위(Adversary behaviors)에 대해서 공격방법(Tactics)과 기술(Techniques)의 관점으로 분석하여 다양한 공격그룹의 공격기법 들에 대한 정보를 분류해 목록화 해 놓은 표준적인 데이터 들이다.

MITRE ATT&CK 홈페이지에서는 Matrices Mitigations, Groups, Software 등 다양한 카테고리의 정보를 제공하고 있으며, 이를 통해 해당 시스템의 Tactics와 Techniques에 관련된 공격정보 및 대응방법을 확인할 수 있다.

MITRE ATT&CK는 공격기술인 Tactic과 Technique의 개념과 관계를 시각화하였으며 각 Tactic에는 다양한 Technique가 포함된다. 이러한 Tactics와 Techniques를 ATT&CK Enterprise 버전에서는 Tactics 14개, Techniques 185개, Sub-Techniques 367개의 정보를 제공(2021년 4월 기준)하고 있다.

MITRE ATT&CK의 Matrix 정보는 Fig. 2와 같으며, 공격자 전술단계 및 전략 패턴은 Table 3과 같다.

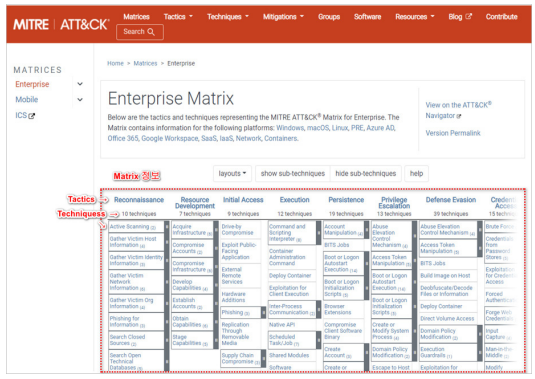

Fig. 2. MITRE ATT&CK Matrix Information[6]

Table 3. ATT&CK-Based Attacker Tactics, Strategic Patterns[7]

Tactic ID	Tactic	Explanation
TA0043	Reconnaissance	Gather information that can be used to plan future operations
TA0042	Resource Development	Attackers build resources they can use to support their operations.
TA0001	Initial Access	Intrude the network
TA0002	Execution	Run malicious code
TA0003	Persistence	Attackers continue to attempt attacks to succeed in their operations
TA0004	Privilege Escalation	Attackers steal top-level privilege
TA0005	Defense Evasion	Attackers bypass information protection systems
TA0006	Credential Access	Attacker to steal account name and password
TA0007	Discovery	Exploring the vulnerable environment of the target
TA0008	Lateral Movement	Attempt to infiltrate the target's environment
TA0009	Collection	Attackers gather information tailored to their targets.
TA0010	Exfiltration	Data leakage
TA0011	Command And Control	Attackers communicate with compromised systems to control
TA0040	Impact	Attackers manipulate and destroy systems and data.

2.2 제안하는 시스템

2.2.1 보안사고 프로파일링 서비스

발생할 수 있는 전체 보안사고 유형을 분석하고 기 설치된 보안제품의 보안 로그를 수집하여 보안사고 프로파일링을 통해 보안사고 유형별 발생 가능성을 정량화하여

평가하는 시스템이 필요하다.

발생가능성이 있는 보안사고 유형에 대한 정의, 발생 가능한 시나리오 모의공격을 통해 보안사고위협을 사전에 예측 및 평가하여 보안사고 유형별로 사전 대응할 수 있는 시스템을 구축하고 기존 통합보안제품의 보안위협 정보를 통합 수집하여 보안 로그를 연동하여 보안사고 가능성을 평가함으로써 기존 제품의 제한사항을 보완해야 한다. 이를 위해 Fig. 3과 같은 보안사고 예측 알고리즘을 개발하고 현재 네트워크내의 자산정보를 확인하여 보안사고 위협에 대응할 수 있는 서비스를 필요로 한다.

보안사고 유형은 MITRE ATT&CK를 참고하여 해당 프레임워크의 업데이트 리포트를 통해 주기적으로 시나리오를 업데이트 할 수 있도록 한다.

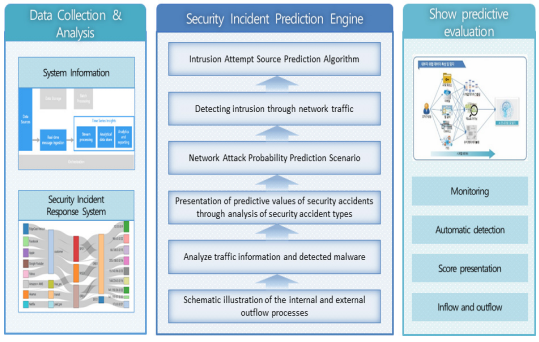

Fig. 3. Algorithm Scenarios for Predicting Security Accidents through Data Collection and Network Analysis

2.2.2 보안사고 시나리오 서비스

조직 내에서 수집된 정보와 입력한 정보를 기반으로 현 시점에서의 모든 보안사고 유형에 대해 발생 가능 여부를 판단할 수 있는 엔진을 통해 보안사고 시나리오를 생성하고 예측 및 관리할 수 있도록 시스템을 구축한다. 보안사고 시나리오 생성은 Fig. 4, Fig. 5와 같이 데이터 수집, 데이터 분석, 프로파일링, 시나리오 생성의 네가지 절차를 거친다.

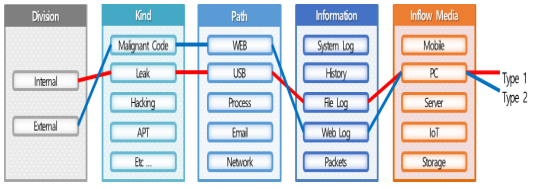

Fig. 4. Determine the type of incident by type of security incident

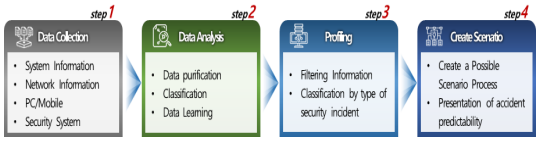

Fig. 5. Procedure for creating a security incident scenario

Fig. 5에서 보는 바와 같이 보안사고 시나리오는 데이터 수집, 분석, 프로파일링, 시나리오 생성 절차를 거쳐서 생성하며 생성된 시나리오의 결과에 따라 보안사고 레포트를 생성한다.

1) 보안사고 예측, 모니터링
   - 클라우드 통합 시스템 연동을 통한 신종 보안사고 대응 방안 제시
   - 국내외 주요 보안사고에 대한 원인 및 대응 방안을 파악할 수 있는 기능
2) 보안사고 유형별 도입 조직에 맞는 보안사고 예측 리스트 생성 기능
   - 모든 채널 암호화를 통한 수집된 정보에 대한 보안성 확보
   - 퇴근 이후의 보안사고 예방 알림을 위한 전송체계 필요(SMS, Email 등)
3) 자동화된 보안감사 보고서 생성 기능 개발
4) 보안제품, 통합보안제품(SIEM, ESM)보안 로그 자동화 수집
5) 발생 가능한 보안사고 유형을 구조적으로 분류
   - 산업별(금융, 의료, 제조 등) 특성에 따른 보안사고 유형을 외부 · 내부 · 공급망 등 대분류하고 해킹, 정보유출, 공급망 위조 등으로 보안사고 유형을 체계화
6) AI기반 보안사고 유형별 보안사고 가능성(확률) 예측 기능
7) 시스템 대시보드 및 관리자 기능

2.2.3 시나리오 기반 시뮬레이션 실험 결과

실제 발생 가능한 보안사고 시나리오 중 한개의 시나리오를 택하여 공격 시뮬레이션을 해보고 네트워크 기반 침입 탐지 시스템인 Snort에 해당 공격이 탐지가 되는지를 알아본다. 이를 위해 Snort를 미리 설치하고 탐지할 패킷에 대한 Rule을 등록해둔다.

1) 탐지할 패킷에 대한 Rule

alert ip 10.0.0.33 5001 -> any any (msg:"ESE Attack 17";content:"POST /fileUpload";nocase;sid:100004;)

2) 공격 시나리오 목록에서 〈고객정보 유출〉 공격 실행

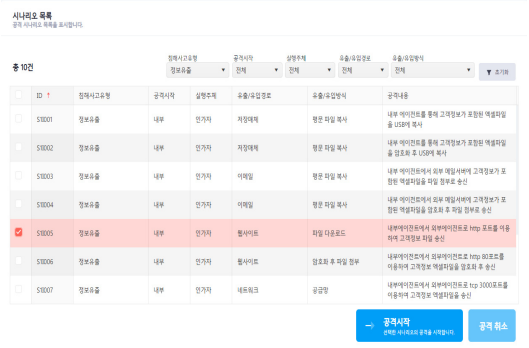

Fig. 6. Simulating a security incident scenario attack

Fig. 6은 본 논문연구를 위한 시나리오 공격 시뮬레이션을 실행해 볼 수 있는 관리자 웹 화면으로 등록된 시나리오에 대해 가상의 모의공격을 실행할 수 있는 환경이다.

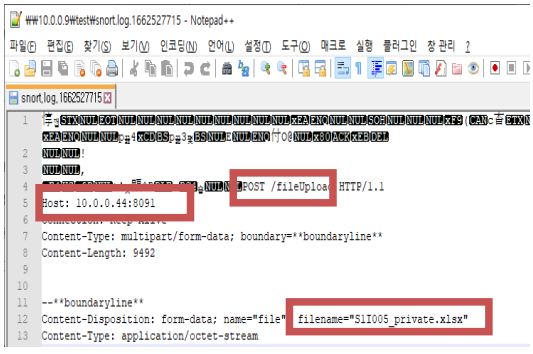

Fig. 7. Snort Log

Fig. 7에서 보는 바와 같이 10.0.0.44:8091로 HTTP POST 방식을 이용하여 S1I005_private.xlsx라는 파일을 업로드 한 고객정보 유출 공격이 Snort에 탐지되는 것을 확인할 수 있다.

3. 결론

보안 기술이 발달함에 따라 방어 기법도 강화되면서 공격자도 새로운 공격 기법을 계속해서 발전시키고 있다. 공격자들은 다양한 환경과 루트를 통해 새로운 방법을 활용해 공격침투를 시도하고 방어 기법을 계속해서 무력화시키고 있다. 이런 상황에서 기업의 보안을 지키고 위협에 대응하기 위해서는 기존의 공격 기술과 공격 과정에 대한 이해가 필요하고 해당 공격 과정의 시나리오가 필요하다.

본 연구에서는 내·외부 보안사고 유형별 분류 방안에 대한 기준을 새로 제시하고 기존에 발생한 보안사고의 대상 및 경로를 분석한 정보를 기반으로 보안사고 가능성에 대한 유형별 분류를 통해 새로운 유형 리스트를 제시하는 과정을 거쳤다. 이러한 과정을 통하여 기존 보안사고 유형 및 신규 보안사고 유형 가능성에 대한 보안사고 유형별 가상 시나리오를 수집하는 과정을 거쳐 정보유출 시나리오에 맞는 사고예측 방안 개발에 대한 전략을 제시하였다. 이 전략에서는 내부 시스템 구성에 대한 유형별 취약점과 악성코드의 특성 등을 분석하여 실제 보안사고가 일어날 수 있는 흐름도에 대한 시각화된 UI를 제공하여 시나리오 기반 모의 침투 테스트를 통해 일반 관리자도 쉽게 보안사고별 흐름을 알 수 있도록 정립하였다. 이번 연구를 통해 기업내 보안사고 예측에서 그치지 않고 내·외부 보안감사에 대응이 가능하고 조직 변경 및 인력 변경으로 인한 정보 유출에 대해 실시간 행위와 정보 판단 및 이력 조회를 통해 내부자 또는 외부의 침투로 인한 정보유출의 경위를 판단할 뿐만 아니라 원천적으로 차단할 수 있을 것으로 기대한다.

References

[1] H. B. Chan, "A Study on The Countermeasure by The Types through Case Analysis of Industrial Secret Leakage Accident", KOCOSA, Vol15, No.7, Dec. 2015. UCI: G704-001662.2015.15.7.014

[2] B. C. Won, "What were some 'cyber security incidents and accidents' that plagued 2021?", CISO, https://www.cisokorea.org/news/view.asp?idx=31525&gubun=News&kind=01&page=1&search=&searchstring, Dec. 2021.

[3] B. C. Won, "Seoul St. Mary's Hospital leaked personal information such as resident registration numbers due to hacking of the district's website.", SecurityWorld, https://www.boannews.com/media/view.asp?idx=100358, Sep.2021.

[4] Microsoft Security, "What is SIEM.", Microsoft, https://www.microsoft.com/ko-kr/security/business/security-101/what-is-siem

[5] Secure Analytics, "What is SIEM.", Juniper, https://www.juniper.net/kr/ko/research-topics/what-is-siem.html

[6] MITRE ATT&CK, https://attack.mitre.org/, Oct.2022.

[7] G. H. Ahn, J. H. Oh, S. R. Yer, W. H. Park, "MITRE ATT&CK-Based Industrial Technology Leakage Prevention Framework Technology", KIISC, Vol31, No.3, Jun. 2021.

홍 명 수(Myung-Su Hong) [정회원]

- 2006년 2월 : 한산대학교 자연과학대학 (컴퓨터학 학사)
- 2023년 2월 : 극동대학교 극동대학원 산업기술보안 (인공지능보안 석사)
- 2005년 11월 ~ 2007년 5월 : 아이티네이트 연구원
- 2008년 8월 ~ 현재 : 리턴트루 수석연구원

〈관심분야〉
정보보안, 암호학, 바이오

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구위원
- 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
인공지능보안, 국방보안, 해킹보안