공통 정보 모델을 이용한 JCIM 시스템에 관한 연구

서성민*, 김범식*, 최성호*, 김진**
*상명대학교 컴퓨터과학과
**상명대학교 빅데이터융합전공
tjtjdals3@naver.com, beomsickboom@naver.com, 98sungho@naver.com, jinkim@smu.ac.kr

A study on JCIM system using common information model

Seong-Min Seo*, Beom-Sik Kim*, Sung-Ho Choi*, Jin Kim**
*Dept. of Computer Science, Sang-Myung University
**Big Data Convergence Major, Sang-Myung University

요 약

현재 IT 보안 관제 시스템을 구축하여 사용하고 있는 기업들은 여러 보안 솔루션을 도입하고 있어 각 솔루션에 따라 서로 다른 IT 이상징후 탐지 모델을 필요로 하고 있다. 이에 따라 솔루션별로 상이한 모델이 필요하며, 유지보수에 어려움이 대두되었다.

이러한 보안 관제 시장의 문제를 해결하기 위해 요구된 것이 이기종 보안 솔루션의 공통 정보 모델로의 표준화 및 탐지 모델 체계화이다. 현재 JCIM은 보안 관제 시장에서 데이터를 공통 정보 모델로 표준화하고, 선택한 솔루션의 시나리오를 보여주며 즉시 탐지까지 가능한 제품을 구현하였다. 이를 통해 AI 기반의 이상 탐지 시나리오를 구현할 수 있는 인력을 양성하고, 이를 기반으로 다양한 고객(산업군)사에 적응하는 것을 기대한다.

Ⅰ. 서론

PC(Personal Computer)같은 정보기기에 주변장치를 연결하기 위한 단지가 제각각이라면 어떤 일이 벌어질까. 과거 1980년 때까지만 해도 주변장치를 만드는 제조사별로 포트와 케이블이 달랐고 주변장치 종류마다 모두 달랐다. 제조사에서는 여러 가지 케이블과 포트를 생산해야 하기 때문에 대량 생산에 차질이 생기고 생산 비용은 증가하며 품질은 떨어질 수밖에 없다. 표준화된 규격의 부재로 시장에서도 입지가 한정적이며 고효율을 내기에는 문제가 있었다. 소비자 입장에서도 같은 기기지만 제조사에 따라 포트와 케이블이 달랐기에 번거로울뿐더러 불필요한 지출을 야기했다. 양측의 문제를 해결할 방안은 주변기기 규격의 통일화를 이루는 것이다. 1996년 USB(Universal Serial Bus)의 표준규격의 등장으로 주변기기의 인터페이스 규격이 지정됐으며 표준화됐다. 보안 부분에서도 마찬가지이다. 현재 기업별로, 부서별로 사용하는 백신과 프로그램, 제조사가 모두 다르고 각각의 필드와 변수명도 제각각이다. 이에 맞는 대응, 탐지 시나리오를 구성하기 위해 각각의 맞게 시나리오를 작성해야 하며 비용도 들게 된다. 기술이 발전됨에 따라 수많은 백신과 프로그램들이 등장하는데 매번 환경을 구축하기에는 비용과 시간이 많이 소요된다. 제이슨은 이용자가 사용하는 프로그램에 맞춰 JCIM(JMachine Common Information Model : 제이머신 공통 정보 모델)만의 표준규격을 통해 이런 문제를 해결한다.

JCIM은 이기종의 다수 보안 솔루션의 로그 데이터를 하나의 “공통 정보 모델”로 표준화함으로써, 복잡한 로그 데이터와 이를 활용하여 구현하는 이상징후 탐지 시나리오 로직을 하나의 공통 정보 모델로 체계화한다. 이 과정에서 여러 다양한 로그 데이터의 필드 명칭과 변수명을 통일화시킨다. 통일화된 필드 명칭을 통해 이상징후 탐지 시나리오에서 데이터와 시나리오 관리가 용이해진다. JCIM은 이용자가 사용 중인 보안 솔루션의 선택만으로 “공통 정보 모델”데이터베이스에 사전 구현된 탐지 시나리오를 확인하고, 즉시 탐지 운용이 가능하도록 설계했다. 이기종의 솔루션에서 공통적인 의미로 사용되는 필드 명칭을 표준화하였고 이벤트 타입은 같은 행위를 나타내는 로그 유형별로 분류하여 로그 필드 표준화 전처리를 진행한다. 이상징후 탐지 방법으로는 일반 임계치와 AI(Artificial Intelligence)가변 임계치, AI

가변 임계 예측 등의 기술로 진행된다. 전처리된 IT 이상징후 탐지 모델을 통하여 신뢰도 높은 IT 보안 관제 시스템을 구축하게 된다. 최종적으로 유지보수 대응에 용이하며 IT 보안 관제 시스템 도입 비용과 운영관리 비용(Operating cost) 절감 효과가 있다.

Ⅱ. 이론적 배경

1. JASON

2017년 설립된 제이슨(Jason)은 데이터 과학을 기반으로 사이버 보안과 빅데이터, 인공지능(Artificial Intelligence) 기술을 IT 운영, 해킹 탐지, 정보 유출 업무에 접목한 AIPSAIOps 플랫폼인 machineJMachine 개발에 성공하였고 시장을 통해 그 우수성을 인정받고 있다. 현재, 제이슨(Jason)은 보안 관제 시장에서 데이터를 공통 정보 모델로 표준화하고, 선택한 솔루션의 시나리오를 보여주며 즉시 탐지까지 가능한 기능의 유일한 제품인 JCIM을 개발하고 있다.

2. CIM

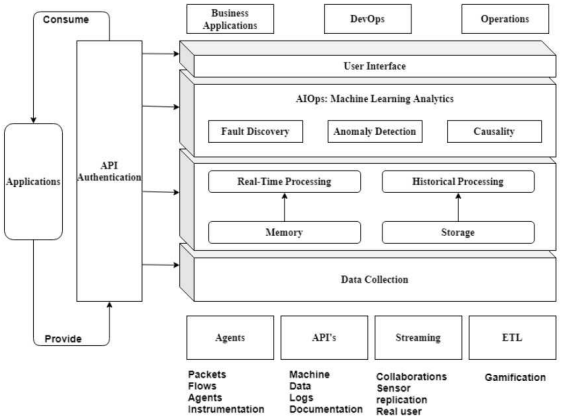
CIM은 비즈니스 컴퓨팅 및 네트워킹 환경을 기술하기 위한 개념적인 모델이며, 플랫폼 독립적으로, 그리고 동시에 기술 중립적으로 관리 정보를 교환하기 위해 제정된 획기적인 표준이다. 여기서, 비즈니스 컴퓨팅 및 네트워킹 환경이라 함은 관리 대상 실체(entity) 및 그들의 상태, 운용, 조합, 구성, 관계 등을 모두 포함한다.

CIM은 핵심모델(core model)과 이를 확장한 일련의 공통모델(common model)로 구성된다. 공통모델은 시스템, 서비스, 네트워크, 애플리케이션, 사용자, 데이터베이스 등과 같이 관리를 필요로 하는 네트워크 수준부터 운영체제 및 애플리케이션에 이르기까지 주요 기술 영역이 모두 포함되어 있다. [1]

(그림 1) CIM 공통 모델
(출처 : 김영호 외 4명, 시스템 관리 표준 정보모델(CIM)분석, 전자통신동향분석 제19권 제6호, pp. 142, 2004. 12)

3. AIOps

AIOps는 빅데이터분석과 머신러닝과 인공지능 기술간 상호 작용을 통해 IT운영의 문제를 식별하고 해결하는 과정의 자동화를 포괄하는 개념을 AIOps라고 할 수 있다. 또한, 소프트웨어 및 서비스 엔지니어가 인공지능(AI) 및 머신러닝(ML) 기술로 온라인 서비스와 애플리케이션을 효율적이고 효과적으로 구축하고 운영할 수 있도록 하는 것을 의미한다. [2]



(그림 2) 엔터프라이즈아키텍처를 위한 데이터레이크
(출처: Rise of AI for IT Operations in Data Lake, 2020.6)

4. UEBA

엔드 포인트나 네트워크 내에서 사용자의 행 위를 정밀하게 분석하고 추적하면서 이상행위를 찾아내는 사용자 행위 분석이다. UEBA는 고의를 가진 내부자의 소행이나 감염된 사용자 계정에서 발생하는 이상행위를 탐지하는 솔루션으로, 초기에는 SIEM의 탐지를 도와주는 기술로 시작했으며, 최근에는 단독 솔루션으로도 주목받고 있다. 스플렁크 UEBA의 경우, 머신러닝을 적용해 SIEM을 진화시키는 역할을 한다. 사용자 계정 감염, 데이터 유출, 계정 도용 방지 등의 기능을 제공한다. [3]

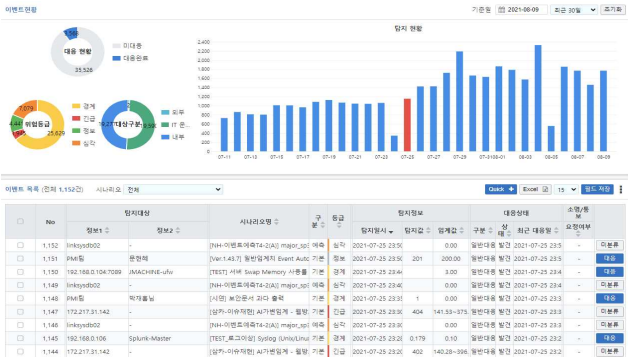
5. SIEM

초기에는 방화벽, IPS/IDS,DDoS 등의 외부경계선 방어를 목적으로 하는 경계 방어 시스템(PerimeterDefense System) 들의 로그들을 단순 분석하는 ESM솔루션으로 확장되었고 현재에는 내부통제를 수행하는 보안 시스템의 이벤트와 장기간 동안 수집된 저장 로그를 기반을 기초적인 분석이 아니라 입체적 관점으로 상관분석하는 형태로 변화하

고 있다. 따라서 보안관제 시스템은 보안 시스템과 IT 시스템들에서 발생되는 이벤트들을 장기간 수집/저장하고 통합적으로 분석하여 의미 있는 위협을 사전에 탐지 및 모니터링하는 시스템으로 정의할 수 있다. [4]

6. JMachine

JMachine은 데이터수집에 있어 Splunk를 이용하여 형식화된 틀에 맞춰 대량의 데이터를 신속하게 지능형 분석 기술로 진행되어, IT장애, 보안사고에 대해 “정밀 탐지”, “미래 예측” 후 “분석, 대응 자동화”를 실현한 AI 이상징후 탐지시스템이다.



(그림 3) JMachine AI 이상징후 탐지 현황

Ⅲ. 연구 내용

1. 연구 목표

이기종의 다수 보안 솔루션의 로그 데이터를 하나의 “공통 정보 모델”로 표준화함으로써, 복잡한 로그데이터와 이를 활용하여 구현하는 이상징후 탐지 시나리오 로직을 하나의 공통 정보 모델로 체계화한다. 또한, 여러 다양한 로그데이터의 필드 명칭을 공통화시킬 뿐만 아니라, 이상징후 탐지 시나리오 또한 공통된 필드 명칭을 통해 구현되어 데이터와 시나리오의 관리가 용이하다. 즉, 체계화된 탐지 시나리오를 구현하고 탐지 시나리오 구현 시간을 단축하여 컨설팅 인력 비용을 절감할 수 있다. 고객사가 보유 중인 보안 솔루션의 선택만으로 “공통 정보 모델”데이터베이스에 사전 구현된 탐지 시나리오를 확인하고, 즉시 탐지 운용이 가능하도록 하는 것을 목표로 한다.

2. JCIM View

(그림 4) JCIM VIEW 메인화면

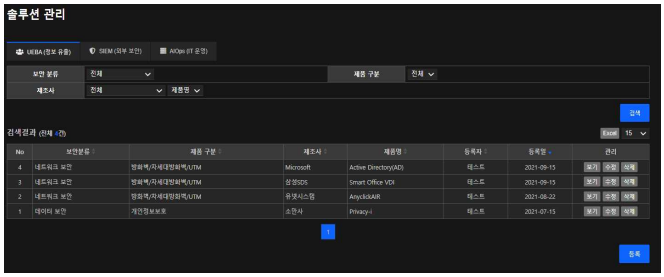
JCIM이 사용자에게 제공하는 솔루션이나 시나리오 목록을 보여주는 기능이다. 각 목록에서 UEBA, SIEM, AIOps를 선택하여 제조사 또는 제품명, 시나리오명을 검색하여 필요한 부분을 선택하면, 알맞은 시나리오나 솔루션을 제공받을 수 있다. 또한, 시나리오나 솔루션을 검증해볼 수 있다.

3. 시나리오 관리

(그림 5) 시나리오 관리 메인화면

기업에서 사용하는 다양한 보안 제품에 맞춰 이용자가 원하는 맞춤형 서비스를 제공한다. UEBA, SIEM, AIOps의 원하는 목록을 선택 후 필요한 기능을 선택하여 시나리오를 구성한다. JSON은 단일 플랫폼으로 Splunk를 이용하여 데이터를 수집한다. 수집된 데이터는 JMachine에 의해 AI 정밀 탐지와 AI분석, 대응 자동화가 진행된다. 단일 플랫폼의 이용으로 각각 다른 보안 제품을 사용하더라도 원하는 시나리오를 제공할 수 있다.

4. 솔루션 관리



(그림 6) 솔루션 관리 메인화면

제조사가 JCIM View에서 필요한 솔루션을 쉽게 찾을 수 있도록 각 제조사마다 제공했던 솔루션들을 등록해놓는 기능이다. 각각의 솔루션을 조회, 수정 및 삭제할 수 있으며, 솔루션의 보안 유형 및 제조사, 제품명을 설정하여 검색을 통해 솔루션 목록을 조회할 수 있도록 구현하였다.

5. 이벤트 타입 관리

(그림 7) 이벤트 타입 관리 메인화면

보안 솔루션에 필요한 형식, 함수를 관리하는 기능이다. Excel을 통해 이벤트타입을 새롭게 업로드 할 수 있으며 이때 Splunk APP에서 동기화가 이뤄진다. 동기화된 이벤트타입은 솔루션 작성에서 한 요소로 작용한다. 만들어진 이벤트타입은 요구와 필요에 따라 필드 수정 및 삭제가 가능하다.

6. 분류체계 관리

(그림 8) 분류체계 관리 메인화면

분류체계관리는 솔루션 관리에 필요한 보안 분류, 제품 구분, 제조사, 제품명을 각각 분류하여, 솔루션 관리에서의 체계성을 높인다. 그리고 각 목록의 등록, 수정 및 삭제가 가능하다.

Ⅳ. 기대효과

표준화된 공통 정보 모델(JCIM)을 활용해 체계적이고 높은 신뢰성을 갖춘 시스템을 구축한다면, 여러 효과를 기대해 볼 수 있다.

첫째, 이기종의 보안 솔루션에서 발생하는 빅데이터를 공통 정보 모델로 표준화함으로써 현재 데이터 분석 및 시나리오 구현 기간을 3주에서 1주 이내까지 단축할 수 있다.

둘째, 공통 정보 모델을 활용한 체계적인 탐지 시나리오를 구현함으로써 고객사에 시나리오를 사전 제시할 수 있다. 이로 인해 컨설팅 인력 비용 절감이 가능하다.

셋째, 공통 정보 모델을 이용하여 단축된 구축 기간을 통해 AI 이상탐지 분석 기간을 확대함으로써 고객사가 보유중인 보안 솔루션 활용 운영이 용이하고, 이상탐지 분석 정확도가 향상될 수 있다.

이를 종합해보면 공통 정보 모델을 이용하여 시스템 구축 및 보안 솔루션 분석 기간을 단축시켜, AI기반의 이상탐지 분석에 비용을 확대함으로써 이상탐지 분석 정확도 향상을 기대한다.

참고문헌

[1] 김영호 외 4명, 시스템 관리 표준 정보모델(CIM)분석, 전자통신동향분석 제19권 제6호, pp. 142, 2004. 12

[2] 상명대학교, AI 기반의 이상징후 탐지 및 대응 시스템 고도화에 대한 연구
A Study on the enhancement of anomaly detection and response system based on AI, pp 10~11, 2021. 01

[3] 데이터넷, “보안의 핵심 ‘사람’④ SIEM·UEBA 통합 플랫폼 부상”, 2020.04.23.

[4] 엄진국 외 1명, SIEM을 이용한 침해사고 탐지방법 모델 제안, The Journal of The Institute of Internet, Broadcasting and Communication(IIBC) Vol. 16, No. 6, pp. 44, Dec. 31, 2016