논문 21-46-02-14 The Journal of Korean Institute of Communications and Information Sciences '21-02 Vol.46 No.02
https://doi.org/10.7840/kics.2021.46.2.302

효율적인 침해대응을 위한 보안이벤트 시스템 설계 구현

최 방 호◆, 조 주 필*, 조 기 환°

Design and Implementation of Automatic Security Event Analysis System for Effective Intrusion Response

Bang-ho Choi◆, Juphil Cho*, Gihwan Cho°

요 약

최근 사이버 공격 대응을 위해 기관 및 기업들은 빅데이터 기반의 보안로그 수집 체계를 갖추어 자체 보안관제 프로세스에 적용하고 있다. 그러나 날로 지능화되고 있는 사이버공격을 차단하기에는 한계를 드러내고 있다. 본 논문은 사이버 침해대응 보안관제 체계에 보안이벤트 자동분석 시스템의 설계 및 구현을 제시한다. 제안한 시스템은 기존 로그 수집 방식인 http header와 더불어 body를 포함해 수집하여 분석한다. 주요 보안이벤트를 중심으로 기계학습 기술을 적용하여 악의적 공격 여부를 정·오탐 판단을 기준으로 로그 자동분석을 수행한다. 또한 탐지된 공격은 보안관제 상황판을 통하여 방화벽 장비에 차단 규칙으로 적용할 수 있도록 한다. 그 결과로 기존 SIEM 시스템에 비해서 총 보안이벤트량을 40%정도 감소시키고, 공격 탐지율을 10%정도 향상 시키는 효과를 얻을 수 있다.

Key Words : Security Control, Machine Learning, Automatic Analysis, Big data, Sandbox

ABSTRACT

Recently, most organizations and companies have been establishing their own security control process that collects security logs based on big data in order to respond to cyber-attacks. However, there are some degree of limitations in responding cyber-attacks that are becoming more intelligent day by day. This paper deals with a design and implementation of security event automatic analysis system that is applied in the security control system for cyber attack response. The proposed system collects and analyzes http 'body' information along with http 'header' as the security log even if the existing system makes use of http 'header' only. On concentrating of the mail security events, an automatic analysis of security log are executed a true or false decision based on the machine learning technique, to determine whether there's a malicious web attack. In addition, the detected attack can be blocked by instructing the firewall device, in order to be applied the protection rule immediately through the security control situation panel. As a result, the proposed scheme shows that the total amount of security events are reduced about 40%, and achieved 10% improvement in the attack detection rate in compare to the existing SIEM system

※ 본 논문은 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 사회 맞춤형 산학협력 선도대학(LINC+) 육성사업의 연구결과입니다.

◆ First Author : Jeonbuk National University Dept. of Information Security Engineering, caoscos@gmail.com, 학생(박사), 정회원
° Corresponding Author : Jeonbuk National University Dept. of Computer Science and Engineering, ghcho@jbnu.ac.kr 정교수, 정회원
* Kunsan National University Dept. of Integrated IT & Communication Engineering, stefano@kunsan.ac.kr, 정교수, 정회원
논문번호 : 202012-301-B-RN, Received December 4, 2020; Revised December 15, 2020; Accepted December 15, 2020

Ⅰ. 서 론

최근 사이버 공격은 기관(정부, 금융 등), 대기업, 중소기업 등에서부터 일반 가정집의 PC까지 대상이 되고 있다. 공격유형 또한 악성코드, 분산서비스거부 공격, 지능형지속공격, 랜섬웨어, 스파이웨어 공격 등 다양하고 새로워지고 있다. 이에 대응하고자 기관 및 대기업에서는 자체 정보보안 관제센터를 구축하여 운영하고 있다.

보안관제는 보안장비들의 로그자료 분석을 통해 관제하는 ESM(Enterprise Security Management : 통합보안관리) 시스템이 등장하여 많은 기관에서 관제시스템의 핵심 기술로 사용하고 있다. 또한 침해사고시 원인분석을 위한 기관내 모든 로그를 저장할 수 있는 통합로그시스템이 활용되고 있는 추세이다. 특히 통합로그시스템에 원시로그가 저장되고, 이 원시로그를 관제에 유효하게 적용하기 위한 많은 노력이 진행되고 있다.

빅데이터 기반의 SIEM(Security Information and Event Management : 보안 정보 및 이벤트 관리)은 수집되는 모든 로그에 대해 실시간 분석한 경보 이벤트를 시작으로 위협탐지 및 분석, 대응의 보안관제 업무를 지원하는 시스템이다. 빅데이터 로그를 처리하는 경우, 지나치게 방대한 양의 데이터를 수집·처리해서 실시간으로 모니터링 해야 한다. 따라서 관제요원 1인이 모든 이벤트를 분석하기에는 불가능한 것이 현실이다[1].

이러한 상황을 개선하고자 빅데이터 처리를 기반으로 하는 SIEM 및 인공지능 기반의 관제시스템을 개발하여 적용하는 노력이 진행되고 있다. 빅데이터 기반의 SIEM은 로그의 방대함으로 인하여 체계적인 분석이 어려운 한계를 지닌다. 특히 수집된 로그가 빅데이터 처리에 적합하지 않거나, 기계학습 기능이 체계적으로 적용되지 못하는 문제를 야기하고 있다. 주요 보안이벤트를 중심으로 하는 침해탐지 체계를 구축할 필요가 있다. 또한 침해되는 공격유형이 날로 지능화되고 진화하므로 기계학습 개념을 통합관제 시스템에 구현하는 것이 쉽지 않다. 특히 새롭게 유행하는 보안침해에 대응하는 보안 관제체계를 구성할 필요성이 제기되고 있다[2].

본 논문은 사이버 침해대응 보안관제 체계에 기계학습 기법을 기반으로 보안이벤트 자동분석을 적용하는 시스템의 설계 및 구현을 제안한다. 제안한 시스템은 http header와 body를 포함한 웹 데이터 전체를 수집하는 웹 로그 수집 체계에서 출발한다. 수집된 빅데이터 형태의 대용량 로그에서 주요 보안이벤트를 중심으로 보안분석을 적용한다. 보안분석에 기계학습기법을 적용함으로써 악의적 웹 공격 여부를 판단하는 로그 자동분석을 수행한다. 탐지된 공격은 보안관제 상황판에서 방화벽 장비에 즉시 적용하여 차단할 수 있다. 제안한 방법은 기존 SIEM 환경에 대비하여 보안이벤트량을 크게 감소시키고, 웹 공격 등에 대해서 탐지율을 향상 시키는 것을 목적으로 한다.[3]

논문의 구성은 다음과 같다. 2장은 빅데이터와 기계학습 개념을 적용한 통합관제 시스템의 현황과 문제점을 정의한다. 3장에서 제안한 시스템의 설계 및 구현에 관한 구체적인 사항을 서술한다. 4장에서 제안한 시스템의 효과를 분석하고 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 SIEM 기반 보안관제

SIEM은 기관, 기업 등의 정보통신망과 장비에 있는 전체 범위의 로그를 수집, 저장, 분석하는 시스템이다. 네트워크 단에 있는 전체 로그를 수집하여 규칙 순응도(compliance) 관리와 위험을 모니터링하고, 이행확인, 보안성과 측정, 로그 상관관계에 대한 기능을 보강한다. 공격 탐지, 차단 및 대응을 위한, 기업 내·외부에서 발생하는 다양한 형태의 침해사고 시나리오를 기반으로 로그분석과 이벤트분석이 가능하도록 다양한 유틸리티를 제공한다[4].

표 1과 같이 SIEM은 로그관리, 로그분석, 보안탐지의 기능을 가지고 있다. 최근 기업들은 SIEM을 도입하여 사이버침해에 대응하여 내부자산을 보호하려고 하지만, 여러 실패 요인으로 인해 목표 달성에 어려움을 겪고 있다[5]. 가트너를 비롯한 주요 연구기관의 보고서를 종합하면, SIEM 시스템에 대한 관리와

표 1. SIEM의 주요 기능
Table 1. Main Functional Features of SIEM

구분	기능	내용
로그관리	이벤트 수집	보안 시스템, 서버, 네트워크 등에서 이벤트 수집
	무결성 관리	수집된 로그의 무결성 보장
로그분석	상관분석	규칙을 기반으로 보안성 분석
	포렌식 지원	포렌식, 워크플로우 틀 제공
공격탐지	외부공격 탐지	서버, DB 자원의 모니터링을 기반으로 외부공격 탐지
	내부침해 탐지	내부 사용자 행위적 특성을 기반으로 내부침해 탐지

대응 인력이 부족하고 현장의 빅데이터 처리기술과 비즈니스 관련 지식이 융합되지 못한 이유로 인해서 시스템 내에 불필요한 정보 순환 문제(Garbage In, Garbage Out)가 발생하여 초기 도입 취지에 부합하지 않는 방향으로 활용 범위가 제한되는 사례를 주된 실패 요인으로 꼽는다[6].

SIEM은 실시간 위협탐지 및 대응을 위해 이벤트 로그 데이터의 실시간 캡처 및 분석 기능을 기반으로 한다. 또한 침해공격 로그에 대한 포렌식과 네트워크 운영, 규칙 순응도와 법적 조사를 위해 해당 데이터의 신속한 검색 및 리포팅 기능을 제공하고 있다[4].

2.2 사이버공격 대응 문제점

SIEM은 웹방화벽, 방화벽, 침입방지시스템(IPS), 침입탐지시스템(IDS), 위협관리시스템(TMS), 패킷수집기 등의 네트워크 기반의 탐지 및 차단시스템의 보안이벤트 로그를 수집한다. 또한 EndPoint 부분인 서버 및 단말기에서 Syslog, 웹로그 등의 대용량의 로그를 SIEM Agent/Agentless 방식으로 수집하여 통합적인 로그분석을 수행한다. 이렇게 로그를 수집하여도 지능화된 사이버공격을 완벽히 대응하는 데에는 여러 가지 미흡한 사항이 도출되고 있다.

그림 1은 기존 SIEM 체계가 갖는 위협정보 수집의 한계를 도식화하고 있다. 특히 지능화·고도화된 APT 공격은 기존의 보안관제 방식으로는 탐지하기 어려운 실정이다[2]. 현재의 보안관제에서 인지되고 있는 문제점은 다음과 같다.

첫째, 네트워크와 시스템에서 생성하는 로그가 대용량인 이유로 수집된 로그에 대한 분석은 제한적일 수 밖에 없다. 특히 알려지지 않은 악성코드 및 사이버공격을 로그 분석으로 발견하기에는 미흡하다. 현재 보안관제시스템인 SIEM은 웹 로그의 http header 값만 수집하고 Body 부분을 수집하지 않으며 실시간 Post 방식의 공격시 Body 부분에서 중요 정보노출에 대한 취약점을 탐지하지 못하고 있다.

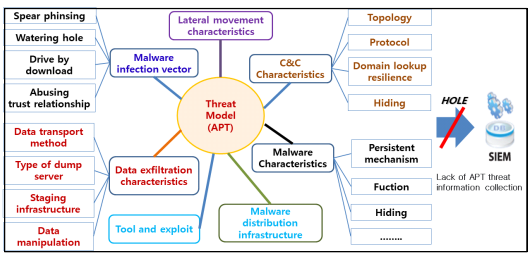

그림 1. SIEM에서의 위협정보 수집의 한계
Fig. 1. Limitations of Threat Information Collection in SIEM

둘째, 빅데이터 기반의 SIEM에서 너무 방대한 로그를 수집, 관제에 적용함으로 인해 관제요원의 업무량이 증가하고 전체 로그에 대한 검증이 사실상 불가능한 실정이다. 또한 보안장비를 우회하거나 보안장비에서 미실행되는 의심파일에 대한 효율적인 자동 분석기술이 미흡한 상황이다[7].

셋째, 현재의 보안관제는 탐지 중심의 관점에서 악의적인 IP 및 URL에 대한 공격을 탐지하지만, 즉각적인 차단 정책을 적용하지 못하는 문제점이 존재한다.

Ⅲ. 이벤트 자동분석시스템 설계 및 구현

3.1 시스템 구현방향

SIEM과 샌드박스를 기반으로 한 자동분석시스템의 전체구성은 그림 2와 같다. 데이터를 SIEM으로 수집하고, 수집된 데이터를 카테고리별로 체계화시킨 후 유의미한 사이버공격을 탐지할 때 사용할 기반 정보로 활용한다. 기존의 레퍼런스 체크를 통해 1차적으로 악의적인 행위를 검증하고, 그 외 검증이 불가능한 데이터 등 모든 사이버위협 정보에 대한 결과값을 관제요원이 실시간 확인할 수 있도록 상황판에 알람 및 시각화 시키는 구조이다[8].

제안된 시스템의 구현 목표는 위에서 언급한 SIEM 이벤트 로그 관제에 대한 문제점들을 해결하기 위해서 자동분석시스템(위협정보 매칭, 우회파일 분류, 룰기반 이벤트 머신러닝, 웹로그 Full 패킷 분석 등)을 구현하고 기존 보안관제시스템과의 차별화된 기능으로 알려지지 않은 공격에 대한 대응 수준을 한 차원 높이는데 있다. 다음 절에서는 각 단계별 기능 및 특징들을 설명한다.

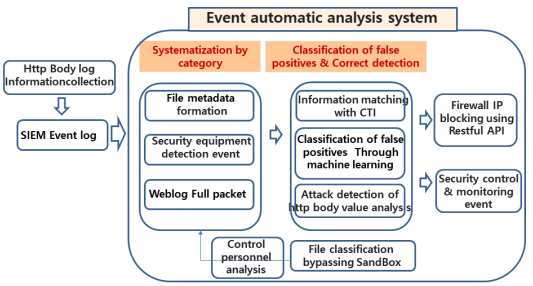

그림 2. 자동분석시스템 구성 및 프로세스 개념도
Fig. 2. Automatic Analysis System Configuration and Conceptual Process Diagram

3.2 SIEM 정보수집(1단계)

SIEM에서 정보를 수집하는 단계는 가장 기본적이면서 중요한 프로세스이지만 현재까지 모든 사이버공격 탐지에 필요한 세밀한 데이터가 수집되지 못하고 있는 실정이다[9].

빅데이터 기반의 SIEM은 ESM에서 수집하는 정보 외에도 모든 엔드포인트의 단말기에서의 시스템 보안로그, 접속로그, 장애로그 등 엄청난 데이터를 수집하고, 수집 및 분석 처리 속도는 기존 ESM보다 10배 이상 빨라지고 있다.

그림 3과 같이 원본 로그를 수집하는 SIEM의 발전에 따라 분석해야 할 로그량은 매우 방대하다. 빅데이터 로그를 잘 활용하면 다양한 공격을 대응하기에 매우 유용하므로 SIEM의 정보 수집기능이 중요하다.

그림 4는 기존의 SIEM의 미흡점을 보완하는 보안위협대응 플랫폼을 보이고 있다[10].

본 논문에서 제안한 자동분석시스템은 새로운 패러다임을 반영하고 기존의 보안관제의 한계를 극복하기 위함이다. 먼저, 웹서버에서 프록시 기능을 이용하여 HTTP 헤더 외에도 Body값을 추출하도록 한다.

그림 5와 같이 Body값에는 중요정보 및 웹해킹 시도 시 다양한 파라미터 부분을 대상으로 하기 때문에 해킹을 대응하기 위해서 매우 유용한 정보이다. 기존의 웹 로그에서는 정보의 방대함으로 인하여 수집하

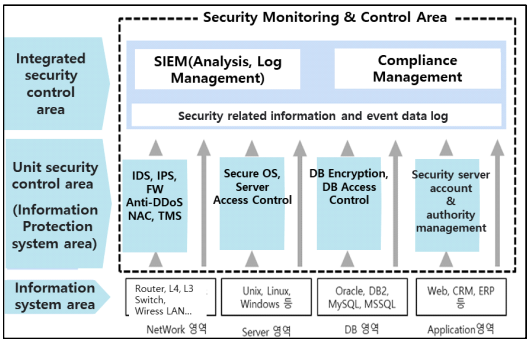

그림 3. 기존의 SIEM의 구성
Fig. 3. Configuration of Existing SIEM

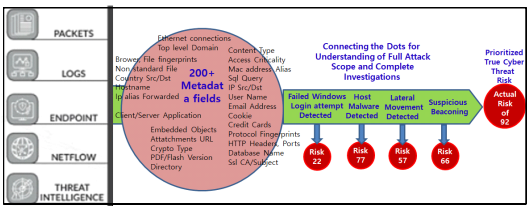

그림 4. '넷위트니스' 플랫폼 아키텍처
Fig. 4. "Net Witness" Platform Architecture

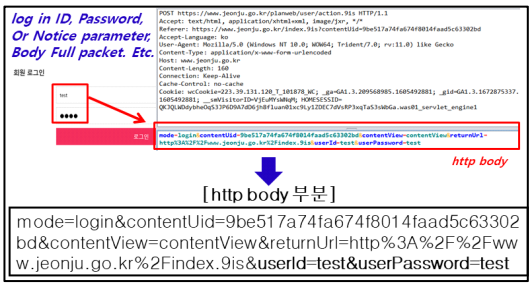

그림 5. HTTP Body 정보의 예시
Fig. 5. Example of HTTP Body Information

지 않고 있는 정보이다. IPS 및 웹 방화벽의 탐지패턴을 우회해서 침투하는 공격은 그림 5와 같이 프록시 기능을 사용하여 body값까지 수집하는 방법으로 대응이 가능하다.

또한 네트워크 구간 및 End Point 구간에서는 수집하는 파일의 메타데이터 정보가 중요하다. 이를 활용하면 알려지지 않은 공격과 다양한 사이버공격을 찾아내는 데에 매우 유용하다.

그림 6과 같이 SIEM 로그 수집시 기존에 포함되지 않은 파일 메타데이터와 http body 패킷 등을 수집하여 분석할 수 있는 범위를 확대할 것이다. 보안관제 시 모든 IT 인프라 전반의 데이터를 분석하여 위협 가시성을 제공한다.

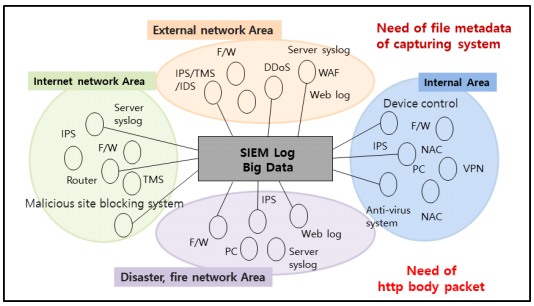

그림 6. 1단계: SIEM 수집로그
Fig. 6. Step 1: Collection of SIEM Log

3.3 카테고리별 체계화(2단계)

표 2는 메타데이터를 예로 들은 것으로 카테고리별 분류단계는 1단계 SIEM에서 수집한 정보를 파일메타데이터, 보안이벤트, 웹로그 풀패킷 등으로 그룹핑 하고, 체계화하는 단계이다. 먼저, 수집한 파일에 대한 메타정보를 데이터베이스로 구축한다[10].

여기서 특징적인 것은 3단계의 CTI(사이버위협정보: Cyber Threat Intelligence) 정보와 매칭이 적절히 가능하도록 그림 7과 같이 카테고리별 파싱 및 체계

표 2. 파일의 메타데이터 예시
Table 2. Example of Metadata for Files

File Name	HncImage.exe
Hash	MD5 : 845800d9498eca980c78bf7b3170b0d8 SHA1 : a6fddf8ab8322f434235005b1f94e0a976e4ca91 SHA265 : 7d86f6d851f0cdca98dc38837774d26f748154a838a82c89ce8408cb8e5ff0c9
Time Stamp	2020-04-04 01:03:59 (UTC)
File Type	32Bit PE EXE (실행 파일) / MFC
File Size	406,528 Bytes
Origin Name	HncPNGViewer.EXE
Product	HannSoft Png Viewer
Language	Germany

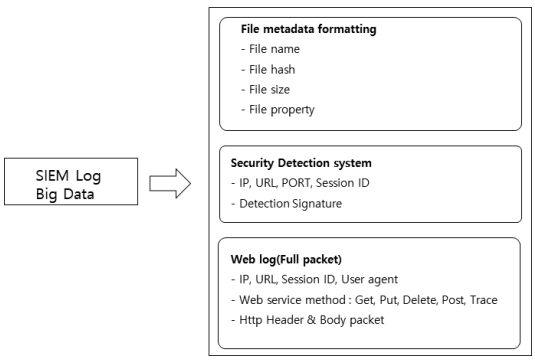

그림 7. 2단계: 카테고리별 체계화
Fig. 7. Stage 2: Systematization by Category

적인 분류를 수행한다.

3.4 정·오탐 자동분류(3단계)

정·오탐 분류단계에서는 CTI 정보를 활용하여, SIEM에서 수집, 분류된 정보와의 매칭을 통해서 1차적인 해외 Osint, 바이러스토탈, 멀웨어닷컴, 국내 KISA의 CTAS 등의 평판 조회로 악의적인 공격과 행위를 탐지한다. 표 3은 가장 많이 활용되고 있는 평판 조회 사이트를 보이고 있다[12].

그림 8은 의심스런 'BDCAMSETUP_KOR.exe' 파일을 바이러스토탈에 업로드해 본 결과, 전 세계 67

표 3. 국내외 평판 사이트
Table 3. Domestic and Foreign Reputable Sites

구분	Reference 사이트 및 정보제공
국내	한국인터넷진흥원 CTAS(Cyber Threats Analysis System)
	국가정보원 NCTI(National Cyber Threat Intelligence)
	한국지역정보개발원 CTRS(Cyber Threat Response System)
해외	Virustotal.com
	Osint(Open Source Intelligence)
	Malwares.com

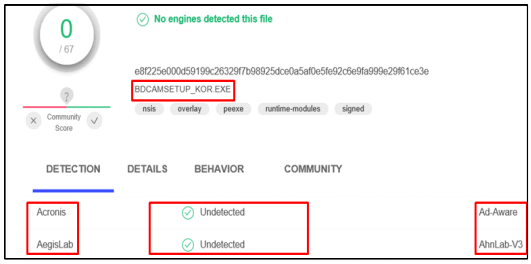

그림 8. exe 파일 바이러스 토탈 탐지 분석 결과
Fig. 8. exe File Virus Total Detection Analysis Result

개의 백신에서 악의적인 행위가 없는 것으로 판별한 것이다. 이처럼 평판 사이트들은 악성코드 등 많은 정보를 보유하고 있다. 보안전문가들은 신규 생성된 파일을 발견할 경우에는 평판 사이트를 효율적으로 활용하는 것이 매우 중요하다.

그러나 정·오탐 자동분류단계의 평판조회 사이트에서 정보 매칭이 안되거나, 샌드박스를 우회하는 특정한 파일 등 분석이 불가능한 로그에 대해서는 별도의 공간에 해당 파일을 분리 저장하여야 한다. 이 로그에 대해서는 바이너리코드를 분석하는 정적분석 및 실제 가상환경에서 동작시켜 분석하는 동적분석 등의 악성코드분석을 수동으로 수행한다. 이렇게 수동으로 분석한 결과를 다시 2단계인 자동분석시스템으로 Feed Back하여 정·오탐 자동분류 결과를 DB화하여 지속적으로 악의적인 파일에 대한 분석을 효율적으로 수행한다.

규칙 기반으로 탐지된 IPS 및 IDS 장비의 이벤트에 대해서는 동일한 공격에 대한 지도학습의 머신러닝 방식을 적용하여, 정탐률 향상을 통해 대량의 이벤트를 신속 정확하게 분석하여 관제요원의 처리시간을

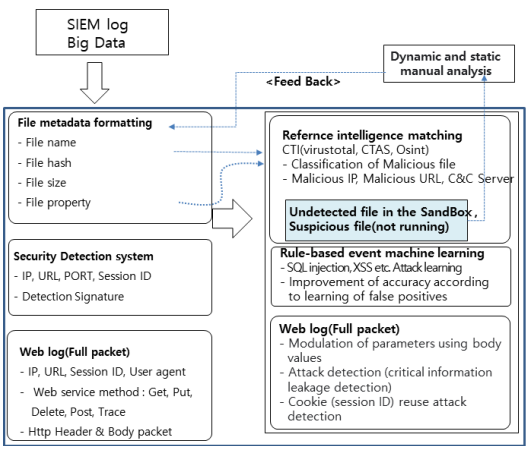

그림 9. 3단계: 정·오탐 분류
Fig. 9. Step 3: False Positive Classification

대폭 축소시켜야 한다.

3단계 정·오탐 분류단계 중 마지막 모듈인 웹로그의 풀 패킷을 활용하여, 그간의 파라미터 변조와 같은 웹 해킹 공격을 탐지·대응하지 못한 부분을 개선한다. 웹 프록시 기능을 활용하면 HTTP 요청·응답값 전부를 확인할 수 있기 때문에 기대 이상의 효과를 가져올 수 있다. 그림 9는 이러한 사항을 바탕으로 정·오탐 분류단계를 설계를 보이고 있다.

3.5 분야별 모니터링 및 관제(4단계)

4단계인 모니터링 및 관제 단계에서는 자동분석시스템을 통해서 판별된 이벤트를 상황판에 표출시켜서 최종적으로 사이버공격을 차단 및 대응하도록 한다. 표 4는 구현한 시스템의 API에 대한 특징을 보인다.

의심스런 IP, URL 접속 이력을 알람으로 발생시키고, 악성코드 파일에 대한 알람, 탐지패턴에 의해 발생한 이벤트 알람, 웹 공격에 대한 알람 등에 대하여 즉시 차단이 필요한 IP는 Restful API 호출을 통해서 방화벽에 자동으로 차단적용 되도록 구성한다. 이를 통하여 보안관제 요원이 직접 방화벽을 접속하여 IP를 차단하는 번거로움과 시간 낭비를 줄일 수 있다.

표 5와 같이 웹서비스 메소드인 GET, POST, DELETE, PUT 방식으로 원격에서 DB 등의 시스템에 정보를 조회, 등록, 삭제, 변경이 가능하며, 이런 방법을 활용하면 방화벽에 유해 IP 차단 등록이 가능하다.

표 4. REST, REST API, Restful API 의미
Table 4. Meaning of REST, REST API, Restful API

구분	주요 특성
REST	상태 전환을 표시. http 통신에서 자원에 대한 CRUD 요구는 자원, 방법, 자원의 표기 등을 특정 형식으로 전달함
REST API	자원(URI)에 대한 요청을 통일하고, 제한하는 구조적 스타일을 의미함
Restful API	REST API의 설계 의도에 정확하게 따름을 의미함

표 5. REST(Restful) API 예시
Table 5. REST(Restful) API example

구분	REST API 예시
GET 방식의 REST API	http://www.OOO.kr/users 특정 회원 정보 조회 HTTP GET
POST 방식의 REST API	http://www.OOO.kr/users?query=xxx 회원 등록 HTTP POST
DELETE 방식의 REST API	http://www.OOO.kr/users { ”name”:”terry”, : } 회원 삭제 HTTP DELETE
PUT 방식의 REST API	http://www.OOO.co.kr/users/terry 해당 회원 정보 변경 HTTP PUT

본 자동분석시스템의 분야별 모니터링 및 관제단계는 그림 10과 같다. 먼저, 유해 IP는 RestFul API 기능으로 방화벽에서 자동으로 차단한다.

그리고, CTI 및 자동분석시스템에서 악성코드로 판단된 파일은 알람으로 알린다. 악의적인 공격이 웹 방화벽 및 IPS의 탐지패턴과 일치하거나 웹로그에서 유의미한 Body 값이 검출시 관제 상황판에 나타낸다.

사이버공격 자동분석시스템의 시각화는 직관적인 사이버위협 상황을 보안관제에 맞게 커스터마이징 하는 등 사용자가 직접 필요한 정보를 정의하여 구현하도록 구성한다. 공격 유형별, 국가별 위협상황 등 보안지표를 표시하고 전반적인 사이버공격 대응 현황을 확인할 수 있도록 설계 구현한다.

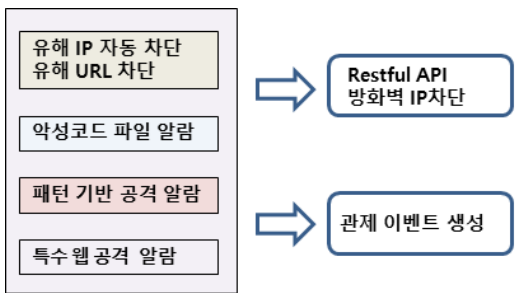

그림 10. 4단계: 모니터링 및 관제
Fig. 10. Stage 4: Monitoring and Control Stages

Ⅳ. 자동분석시스템 결과 분석

4.1 보안이벤트 생성량 비교

자동분석시스템을 적용한 결과를 기존 SIEM과 비교하기 위해 동일 조건의 환경에서 동시간대의 이벤트 자료를 추출하여 각각의 시스템에 적용시켜서 실험하였다.

CTI에서 제공한 유해IP에 대해서 적용한 부분을 그림 11과 같이 비교하면 SIEM에서는 동일 유해 IP에서 포트 3389로 원격접속을 탐지한 화면은 동일한 공격이벤트가 다수 발생할 경우 이것을 발생한 횟수만큼 알람으로 표시하는 것을 알 수 있다. 이를 동일한 조건으로 자동분석시스템에 적용시켜 표출하면 동일 공격 탐지 시에 다수 발생한 동일한 7건의 이벤트를 가장 최근에 발생한 단일 건으로 알람을 발생시키는 것을 알 수 있다.

그림 12는 패턴 기반 공격알람에 대한 분석결과를

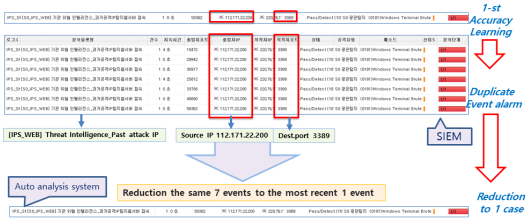

그림 11. 자동분석시스템을 통한 탐지이벤트 감소
Fig. 11. Reduction of Detection Events with Automatic Analysis System

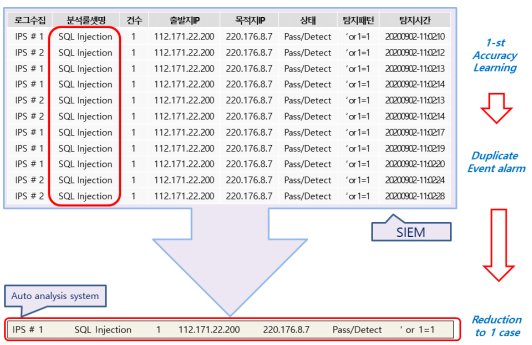

그림 12. 자동분석시스템을 통한 탐지이벤트 감소
Fig. 12. Reduction of Detection Events with Automatic Analysis System

보이고 있다. SIEM 이벤트 로그 중 IPS에서 발생한 보안이벤트의 분석 룰셋명에서 SQL Injection 공격을 분석하면 동일 출발지와 목적지의 이벤트가 11번 발생하여 관제 이벤트창에 공격으로 알람을 표시하고 있다.

자동분석시스템에서 표출한 결과값을 보면 SIEM에서 11건으로 탐지했던 것을 자동분석시스템은 동일한 공격에 대한 지도학습의 머신러닝 방식을 적용하여, 정탐률 향상을 통해 다량의 이벤트를 정확하게 분석하여 동일한 SQL Injection 11건의 공격을 1건으로 대폭 축소됨을 확인하였다.

4.2 자동분석시스템 평가

기존 SIEM에서는 발생한 보안이벤트에 대해서 유해IP 로그가 발생할 때마다 계속 알람으로 알리고 있다. 동일 패턴의 이벤트 로그가 발생해도 발생할 때마다 알람으로 나타낸다. 제안한 자동분석시스템은 CTI를 통한 유해IP에 대해서는 유해IP 임을 인지하여 동일 알람을 단일 건으로 표출하여 성능이 향상되었음을 알 수 있다.

또한 SIEM에서 발생하는 보안이벤트에 대해 자동분석을 통하여 기존 SIEM에 표출하는 중복적인 이벤트들을 줄일 수 있었고, 동일 이벤트는 머신러닝에 의해 알람에서 제외 시켜 표출하지 않는다. 총 10,000건의 기존 ESM 이벤트를 자동분석시스템에서 동일한 공격건수를 1건으로 줄이는 방법을 적용한 결과 약 6,000건 정도로 이벤트 수량을 줄일 수 있다.

결과적으로 SIEM에서 발생한 많은 양의 보안이벤트를 자동분석시스템의 성능 일부를 가지고 비교한 결과 보안이벤트를 40% 정도 줄이는 효과를 보이고 있다.

V. 결 론

본 논문에서 제안한 방안은 SIEM에서 발생한 보안이벤트는 샌드박스를 기반으로 한 사이버위협 자동분석시스템을 거치면서 악성코드 등을 찾아낼 수 있다. 중복되거나 알려진 위협에 대해서는 자동분석을 통해 보안이벤트량을 효과적으로 줄일 수 있다.

이벤트 자동분석으로 정탐률을 향상시켜서 동일한 패턴 및 공격이 발생할 경우에는 수동작업 없이 관제요원의 정탐 확인을 적용하여 매번 동일한 이벤트에 대한 검증단계를 생략한다. 대용량의 동일 이벤트 판단을 기계학습으로 자동 처리하여 수작업의 시간을 줄일 수 있다. 기존 SIEM과 동일한 이벤트를 분석한 결과, 본 자동분석시스템에서는 보안이벤트 수량을 40% 정도 줄이는 효과가 있다. 앞으로는 이런 로그수집 방식을 통하여, 가장 공격이 빈번하게 발생하고, 악의적인 웹 공격 등 대응이 어려웠던 고도화된 해킹에 대해 체계적으로 방어할 수 있는 부분을 검증할 수 있을 것이다. 또한 Restful API를 활용하여 SIEM에서 즉시 유해 IP를 차단하는 기능을 적용할 수 있을 것이다.

다량의 이벤트에 대해 정·오탐을 구분할 수 있는 샌드박스형 평판분석, 형상분석, AI체계의 보조 시스템들이 적용되어 더욱 정·오탐에서 자유로울 수 있는 관제체계에 대한 연구가 필요하다.

References

[1] S. Sohn, "Phenomenon of changes in physical security using big data," *KIPS Rev.*, vol. 26, no. 1, pp. 47-49, Jan. 2019.

[2] "The existing security control is limited, and the concept of Threat Hunting should be actively introduced," dailysecu.com, 2020. 11. 15, https://www.dailysecu.com/news/articleView.html?

idxno=16037

[3] C. Bae and S. C. Goh, “For improving security log big data analysis efficiency, a firewall log data standard format proposed,” *J. KIISC*, vol. 30, no. 1, pp. 157-159, Feb. 2020.

[4] I. Jeon, K. Han, D. Kim, and J.-Y. Choi, “Using the SIEM software vulnerability detection model proposed,” *J. KIISC*, vol. 25, no. 4, pp. 961-974, Aug. 2015.

[5] O. Rochford, “Overcoming common causes for SIEM deployment failures,” *Gartner*, Sep. 2018.

[6] M. Kim, “Incident detection model for quantitative risk assessment in SIEM environment” M.S. Thesis, Pukyong National University Graduate School of Information Protection Cooperation, Aug. 2019.

[7] B. G. Kang, J. S. Yoon, M. W. Lee, and S. J. Lee, “Automatic creation of forensic indicators with cuckoo sandbox and its application,” *KIPS Trans. Comput. and Commun. Syst.*, vol. 5, no. 11, pp. 419-426, Nov. 2016.

[8] D. Kim, S. Kim, D. Hong, J. Sung, and S. Hong, “An study on the analysis of design criteria for s-box based on deep learning,” *J. KIISC*, vol. 30, no. 3, pp. 337-347, Jun. 2020.

[9] B. Kong, et al., *Plus security control practical guide*, infothebooks, p. 74, Nov. 2017.

[10] S. Kim, “*[Next Generation Security Control ④] Providing Threat visibility suitable for business context*,” DATANET, 2019. 6. 5, http://www.datanet.co.kr/news/articleView.html?idxno=134496

[11] KISA, *Cyber Threat Trend Report* (2020-2), 2020. 7. 5

[12] KISA, *Cyber Threat Analysis & Sharing*, 2017.

최 방 호 (Bangho Choi)

1998년 2월 : 한밭대학교 전자공학과 학사 졸업

2008년 8월 : 전북대학교 컴퓨터정보학과 석사

2016년 3월 : 전북대학교 정보보호공학과 박사과정

<관심분야> 컴퓨터네트워크, 정보보호, 무선인터넷

조 주 필 (Juphil Cho)

2001년 2월 : 전북대학교 전자공학과 공학박사

2000년~2005년 : ETRI 이동통신연구단 선임연구원

2006년~2007년 : ETRI 이동통신연구단 초빙연구원

2011년~2012년 : USF, 교환교수

2005년~현재 : 군산대학교 IT정보제어공학부 IT융합통신공학전공 교수

<관심분야> 차세대LAN, LTE-A, 5G 통신, Cognitive Radio, LED-ID, 방송통신융합기술

[ORCID:0000-0003-1041-2538]

조 기 환 (Gihwan Cho)

1985년 : 전남대학교 계산통계학과 학사

1987년 : 서울대학교 계산통계학과 석사

1987년~1997년 : ETRI 컴퓨터연구단 선임연구원

1996년 : Univ. of Newcastle 전산학과 박사

1997년~1999년 : 목포대학교 컴퓨터과학과 전임강사

1999년 : 전북대학교 컴퓨터공학부 교수

<관심분야> 이동컴퓨팅, 컴퓨터네트워크, 정보보호, 무선인터넷

[ORCID:0000-0003-4923-8565]