

# 실시간 이상 행위 탐지 및 시각화 작업을 위한 보안 정보 관리 시스템 구현

김남균<sup>1)</sup>, 박상선<sup>2)</sup>

## Implementation of Security Information and Event Management for Realtime Anomaly Detection and Visualization

Nam Gyun Kim<sup>1)</sup>, Sang Seon Park<sup>2)</sup>

### 요 약

지난 수년간, 정부 기관 및 기업들은 취약성을 악용하고 운영을 혼란시키며 중요한 정보를 훔칠 수 있도록 은밀하고 정교하게 설계된 사이버공격에 대하여 적절한 대응을 못하고 있는 상태이다. 보안정보 및 이벤트 관리(SIEM)는 이러한 사이버 공격에 대응할 수 있는 유용한 도구이지만, 시중에서 판매되고 있는 SIEM 솔루션은 매우 비싸며 사용하기가 어렵다. 그래서 우리는 차세대 보안 솔루션을 제공하기 위한 연구 및 개발을 진행하여 기본적인 SIEM 기능을 구현하게 되었으며 우리는 호스트로부터 실시간 로그 수집과 집계 및 분석에 중점을 두었다. 이 툴은 포렌식을 위한 로그데이터의 파싱과 검색을 제공한다. 이는 기존의 단순한 로그관리 이외에 침입을 탐지하고 보안이벤트의 순위를 이용하여 사용자에게 경고를 할 수 있다. 이러한 보안정보의 운영과 시각화를 위해 Elastic Stack를 사용하였는데, Elastic Stack은 대량의 데이터로부터 정보를 탐색하고 상관관계를 식별하며 모니터링을 위한 풍부한 시각화를 생성 할 수 있는 유용한 툴이다. 본 논문에서는 취약성으로부터 정보를 수집하는 기능을 SIEM에 추가하는 방식을 제안하였다. 호스트를 공격하며 보안정보관리 체계를 기반으로 모니터링, 경고 및 보안감사에 대한 실시간 사용자의 대응을 확인할 수 있었다.

핵심어 : 사이버공격, 보안정보 및 이벤트관리, 로그관리, 경고, 시각화

### Abstract

In the past few years, government agencies and corporations have succumbed to stealthy, tailored cyberattacks designed to exploit vulnerabilities, disrupt operations and steal valuable information. Security Information and Event Management (SIEM) is useful tool for cyberattacks. SIEM solutions are available in the market but they are too expensive and difficult to use. Then we implemented basic SIEM functions to

Received (February 16, 2018), Review Result (February 25, 2018)

Accepted (April 6, 2018), Published (May 31, 2018)

<sup>1)</sup>(Corresponding Author) 05807 R&D Center, Korea System Assurance KOSYAS, Munjeong-ro 4-gil Songpa-gu 12, Seoul, Korea  
email: kimng@kosyas.com

<sup>2)</sup>05807 R&D Center, Korea System Assurance KOSYAS, Munjeong-ro 4-gil Songpa-gu 12, Seoul, Korea  
email: sspark@kosyas.com

\* 이 논문은 2018년도 산업통상자원부의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임.(N0001994, 클라우드 인프라의 보안 이벤트를 관리하는 클라우드 서비스 기반 보안 정보 관리 시스템 개발)

research and development for future security solutions. We focus on collection, aggregation and analysis of real-time logs from host. This tool allows parsing and search of log data for forensics. Beyond just log management it uses intrusion detection and prioritize of security events inform and support alerting to user. We select Elastic Stack to process and visualization of these security informations. Elastic Stack is a very useful tool for finding information from large data, identifying correlations and creating rich visualizations for monitoring. We suggested using vulnerability check results on our SIEM. We have attacked to the host and got real time user activity for monitoring, alerting and security auditing based this security information management.

Keywords : SIEM, Log Management, Vulnerability, Elastic Stack, SIEM

## 1. 서론

클라우드 컴퓨팅 서비스는 인터넷 기술을 이용하여 인프라와 개발환경, 어플리케이션 서비스를 제공하고 이용자(또는 사용자) 요구에 따라 실시간으로 유연하게 컴퓨팅 자원을 제공하고 사용한 만큼 과금하는 서비스이다.[1] 이에 따라 국내에서는 클라우드 컴퓨팅 서비스 활성화 방안으로 2015년 공공 분야 클라우드 활성화를 위해 '클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(클라우드 발전법)'을 제정했다. 국내 클라우드 컴퓨팅 진행은 민간 클라우드 시장은 서비스형 인프라(IaaS)가 중심으로 이루어지고, 공공분야는 보안 등을 이유로 서비스형 소프트웨어(SaaS) 도입이 어려운 상태이다. 클라우드 서비스의 보안 문제는 이용자의 데이터가 자신의 영역을 벗어나 클라우드 서비스 제공업체의 외부 영역에 존재하기 때문에 더욱 위협적인 요소이다.[2] 이에 따라 클라우드 서비스 제공업체가 이용자에게 신뢰성을 확보하기 위한 보안 대책을 마련해야 하고 다양한 위협들이나 취약점으로부터 이용자의 데이터를 안전하게 지켜줄 수 있어야 한다. 또한 클라우드 서비스를 이용하고 있는 사용자들도 자신이 사용하고 있는 자원에 대한 보안은 스스로 관리 하게 클라우드 서비스 제공업체와 계약이 되어 있다. 따라서 이용자 자신이 이에 대한 보안 대책을 마련해야한다. 따라서, 클라우드 서비스형 소프트웨어 도입을 위해서는 보안에 대한 대응을 종합적인 진행하여야한다. 즉, 제공업체와 사용자들 공통으로 클라우드 자원들에 대한 취약점을 바로 파악하고 대처할 수 있어야하고, 신규로 발생하는 공격을 실시간으로 탐지하여 막을 수 있는 도구에 대한 필요성이 크게 대두되고 있는 중이다.

보안 사고를 발생을 미리 예방하고, 사후 분석을 제공하며 지능형 지속가능위협(APT, Advanced Persistent Threat)공격과 같은 지능형 공격에도 빠르게 탐지, 분석, 대응이 가능한 보안 이벤트 정보관리 기술인 SIEM(Security Information & Event Management)의 개발은 많은 정보보안 기업들을 통하여 연구 및 개발이 진행되고 있다.[3] 현재 판매되고 있는 대부분의 SIEM 솔루션은 외산 소프트웨어 위주이고 비싼 가격과 공공기관에서의 사용에 제한이 있다. 본 연구에서는 우선 클라우드의 호스트에 이루어지는 이상행위를 탐지, 분석하여 사용자에게 알려주는 침입 탐지 시스템(Intrusion Detection System, IDS)기반으로 SIEM을 개발하였다. 신규 개발된 SIEM에서는 실시간 로그 수집과 집계 및 분석에 중점을 두었으며, 사용자가 로그 분석과 경고 이벤트들을 쉽게 확인하고 처리 할 수 있도록 구현하였다.

자원 자체에 대한 취약점 파악 및 이에 대한 조치에 대한 사항은 다른 도구에 의존하여야 한다. 보안 취약점 분석의 경우, 다양한 보안 취약점 탐지 도구를 활용하여 보안 제품 및 시스템 등의 취약한 부분들을 탐지하는데 사용된다. 보안 취약점 탐지 도구 또한 대부분 외산제품의 의존도가 높다. 본 연구팀은 기존에 클라우드 서비스 환경에서 보안 취약점 탐지 도구인 “Cloud-SCAN” 이라는 제품을 개발하여서 출시를 하였고, 현재도 클라우드 취약점 분석에 가장 선두적인 프랑스 업체와 협업을 진행 중이다. 본 논문에서는 신규로 개발 중인 SIEM 시스템과 기존에 본 연구팀이 개발한 클라우드 취약점 점검 도구의 연동을 위한 설계 및 구현방법에 대하여 설명을 진행한다. 즉, 취약점 탐지 분석에 대한 실시간 처리 결과를 이상행위 탐지를 위한 SIEM의 기능과 통합한 새로운 기능의 시스템 제안한다.

본 논문 2장에서는 보안 취약점 점검 도구와 IDS를 이용한 SEIM에 대하여 살펴보고, 3장에서는 본 연구에서 제시하는 통합 방안 및 설계 및 구현, 검증방법에 대해 설명한다. 4장에서는 구현결과를 보이며, 마지막으로 5장에서는 결론을 맺는다.

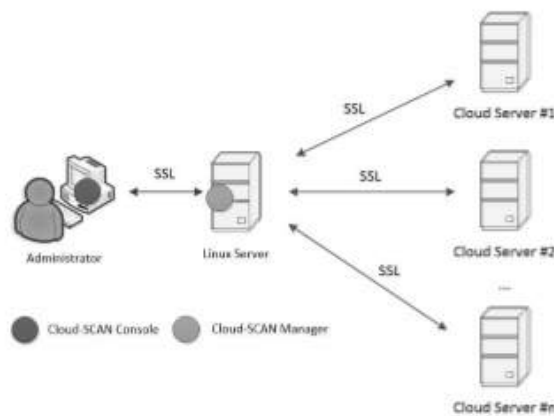
## 2. 배경 및 이론

본 장에서는 “취약점 탐지” 도구와 “SIEM”의 구현 배경 및 기능에 대하여 설명하였다. 또한 이 두 개의 도구들의 결과들을 취합하여 처리 및 분석에 사용되는 데이터 처리 기술인 “엘라스틱 스택 (Elastic Stack)”에 대하여 살펴본다.

### 2.1 취약점 (Vulnerability) 탐지

본 연구팀이 개발하였던 클라우드 환경 보안 취약점 탐지 도구인 Cloud-SCAN 을 기준으로 기본 개념 및 소프트웨어 구조를 소개한다.[4]

다음 [그림 1]은 Cloud-SCAN 의 운영환경이다. 기본 구성은 크게 관리자 UI를 지원하는 콘솔과 클라우드 보안 취약점을 관리, 탐지, 수집하는 매니저로 구성된다.



[그림 1] 클라우드 취약점 탐지 시스템 운영체제

[Fig. 1] Operation Process of Cloud-SCAN

Cloud-SCAN은 클라우드 환경의 보안 취약점 탐지가 가능한 스크립트 기반의 “보안 취약점 탐지 정책(Cloud Vulnerability Policy, CVP)”을 이용하여 개발하였다. CVP를 최신으로 업데이트를 진행하면서 이를 이용하여 가상머신을 사용하는 클라우드 자원에 대해 보안 적으로 취약한 부분을 주기적으로 점검하고, 탐지 결과를 사용자에게 알리게 된다. 보안 취약점 탐지 프로세스는 타겟 지정으로 접속 단계, 패키지 및 릴리즈 정보요청 단계, 패키지 및 릴리즈 정보 획득 단계, 패키지 및 릴리즈 정보 분석 단계, 취약점 판별 결과 전송 단계로 구분된다. 취약점 분석에 대한 처리 및 관리의 웹페이지 형태의 콘솔을 이용하게 되고, 분석 결과에 대한 보고서는 PDF 파일 형식이나 엑셀형식으로 따로 출력이 가능하다. 주기적인 점검 결과는 전자 메일이나 휴대폰 문자 형식으로 사용자에게 알릴 수 있도록 구성하였다. 다음 [그림 2]는 클라우드 상 가상머신들에 대한 취약점 탐색 결과를 보인다.

Severity	Env. Scoring	Name	Exploit	Category	Service	CVSS	Status	Date discovered	#Instances	Actions
Critical		OpenSSH Multiple Vulnerabilities Jan17 (Linux)	⚠	Operating system	2003/tcp	7.5	Current	04 Aug 09:17	1	[Copy] [Refresh]
Critical		OpenSSH Privilege Escalation Vulnerability - May16		Operating system	2003/tcp	7.2	Current	04 Aug 09:17	1	[Copy] [Refresh]
Warning		WEB Application Vulnerabilities - Missing X-Frame-Options header		Web application	7676/tcp	5.8	Current	04 Aug 09:42	1	[Copy] [Refresh]
OK		TCP timestamps		Operating system	-	2.6	Current	04 Aug 09:17	2	[Copy] [Refresh]

[그림 2] 클라우드 취약점 탐지 결과

[Fig. 2] Vulnerability Detection Result

취약점의 위험 수위와 간단한 설명을 보여주며, 사용자가 각 취약점 항목을 클릭하면 해당 취약점에 대한 상세 설명 및 수정 방법을 사용자에게 상세히 알려준다.

## 2.2 침입 탐지(IDS) 방식의 SIEM

지속적으로 변화하면서 여러 가지 공격을 시도하는 지능형 공격(Intelligent Attack)에 대한 대응을 위하여서는 단순히 사용자에게 발생한 문제만 알려주는 모니터링의 개념의 보안도구 이상의 기능들이 필요하다. 이를 위하여 보안정보 및 이벤트 관리(SIEM)이 제안되었다. SIEM은 전체 시스템의 중앙 집중적인 로그 관리와 실시간으로 발생하는 로그들을 이용하여 상관관계 분석/포렌식 및 대응, 원본 로그에 대한 감사 등을 다양한 기능들을 통합하여 종합적으로 문제점을 도출할 수 있다.

SIEM의 기본적인 요구사항으로 시스템/보안/네트워크 등의 종합적인 로그 및 이벤트를 수집, 분석, 관리할 수 있는 기능과 여기서 나온 데이터들을 실시간으로 처리 하여 사용자가 쉽게 이용할 수 있는 기능이다. SIEM에서 요구되는 기능들을 정리하면 [표 1]과 같다.

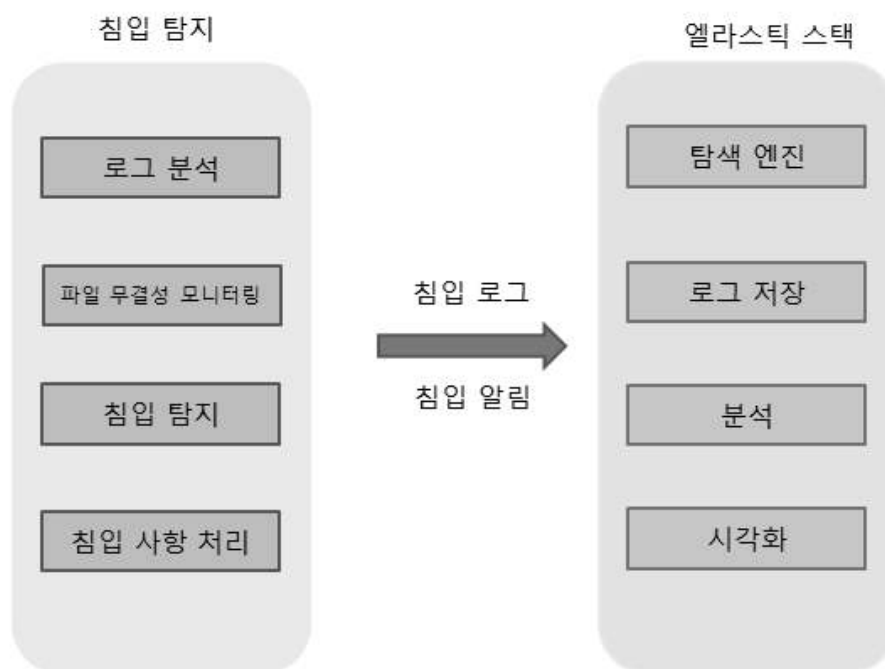
[표 1] 보안정보 및 이벤트관리 기능

[Table 1] SIEM Capabilities

로그 수집	실시간 경고
로그 분석	사용자 활동 감시
상관	대시보드
포렌식	보고
IT 컴플라이언스	파일 완결성
응용 프로그램 로그 분석	시스템과 디바이스 모니터링
접근 감사	로그 보존

SIEM의 기본적인 동작을 위하여, 본 연구에서는 침입 탐지 기능의 소프트웨어를 이용하여 클라우드 상의 가상머신에 대한 위협 문제 발생의 확인과 이에 대한 로그를 수집하였다. 침입 탐지 기능은 크게 네트워크에 대한 침입 방지와 호스트에 대한 침입 방지로 구분할 수 있다. 본 연구에서는 취약점 분석과 마찬가지로 연구의 초점을 클라우드 상의 가상머신의 관리에 맞추어서, 호스트 기반에 대한 침입 탐지인 HIDS(Host-based Intrusion Detection System) 기반으로 클라우드에서 서버로 이용되는 가상 머신 호스트에 Agent를 설치 후 침입에 대비해 로그나 프로세스를 감시하였다. 침입이 감지되면 Agent에서 그 결과를 Manager로 전송하고, 침입에 대한 경고 및 이에 대한 처리를 하게 된다. HIDS의 침입 탐지는 OSSEC을 이용하여 구현하였다.[5] 현재의 구현에서는

“Pattern Matching” 방식의 침입 탐지를 사용하였다. “Pattern Matching” 방식은 “Signature based”라고도 불리며, 이는 미리 정의된 공격 패턴 또는 규칙에 따라 트래픽이 일치될 경우 공격 또는 비정상 행위로 판단한다. 정의된 공격 패턴은 기본적인 사이버 공격이외에도 최신 공격이 발생하게 되면 이를 분석하여 바로 업데이트를 진행하고 있다. [표 1]에서 보인 SIEM 기능을 위해서는 추가 기능들이 필요하다. 즉 기본적인 HIDS를 사용한 침입 탐지 도구에서 나온 로그 및 이벤트를 실시간으로 수집, 분석, 관리하고 사용자가 쉽게 이용할 수 있는 추가 기능들을 현재 가장 큰 주목을 받고 있는 오픈소스 데이터 처리 기술인 엘라스틱 스택 (Elastic Stack)을 사용하여 구현하였다.[6] 엘라스틱 스택의 가장 큰 장점은 확장성과 실시간 분석이라 할 수 있다. 이를 이용하여 보안과 관련된 많은 종류의 로그 및 이벤트들을 실시간으로 검색 및 분석을 하였다. 엘라스틱 스택은 데이터들에 대한 검색을 담당하는 “Elasticsearch”, 데이터들의 수집하고 목적지로 보내는 기능을 담당하는 “Logstash”, 데이터 처리 결과를 시각화 하는 도구인 “Kibana”로 구성되어 있으며, 실시간으로 데이터를 분류 하고, 정보를 확인, 처리에 사용할 수 있다.[7] 이러한 엘라스틱 스택의 기능들을 활용하여 HIDS 기능에 [표 1]에서 보인 SIEM을 위한 기능들을 충족시키도록 하였다. 구현 구조를 도식화하여 아래 [그림 3]처럼 정리하였다.



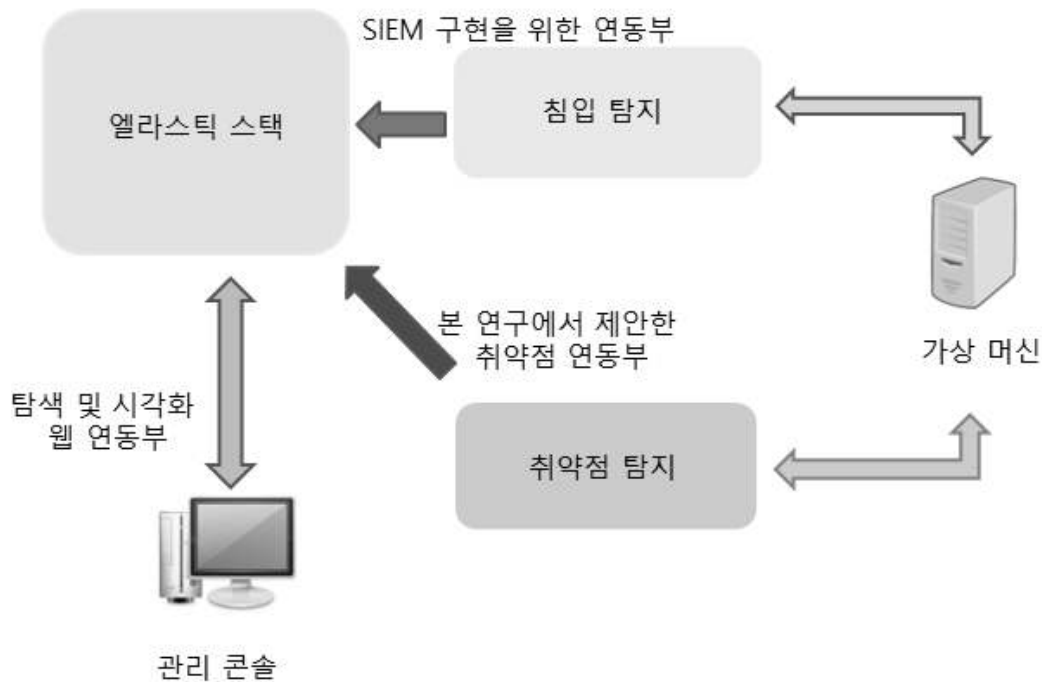
[그림 3] 호스트 기반 침입 탐지 기반의 SIEM 구조

[Fig. 3] Architecture of SIEM based HIDS

### 3. 통합 설계 및 검증 방안

클라우드 상에 가상머신에 대한 보안을 위하여 본 연구에서는 가상머신에 대한 취약점 분석 및


사이버 공격에 대한 탐지를 통합하는 방안 제안하고 설계를 진행하였다. 이를 위해 취약점 분석 결과를 SEIM에 통합하도록 구조를 잡고 설계하였다. 즉, 취약점 분석단계에서 취약점에 대한 로그 및 알람을 만들어서 SEIM에서 이용하는 엘라스틱 스택으로 전달하게 하도록 흐름제어를 조정하였다. 이는 기존에 시도되지 않았던 방식으로 공동의 엘라스틱 스택을 이용함으로써 제한된 클라우드 자원을 효율적으로 사용할 수 있고, 관리적인 측면에서도 관리자가 동일 웹 화면을 이용하여 취약점 정보와 SEIM의 결과를 종합적으로 판단할 수 있다. 대부분의 사이버 공격이 호스트의 취약한 부분을 노리며 장기적으로 해당 부분이 있는 곳을 집중적으로 공격하는 방식이므로 이에 대한 즉각적인 대응에 이루어 질 수 있다. 즉, 보안관리 및 취약점에 대한 즉각적인 대처, 침입 문제 발생 시 호스트의 취약점과 비교 및 이를 처리하는데 효율성을 제공함과 동시에 별도의 도구들을 사용함으로써 나타나는 관리의 어려움을 제거함으로써 사용의 편의성이 증대될 것으로 기대된다. [그림 4]에서 새로 제안된 통합 시스템 구조의 설계를 보였다.



[그림 4] 신규 제안된 시스템 구조

[Fig. 4] Architecture of SEIM with vulnerability

기본 개념은 클라우드 상 가상머신에 대하여 기본적으로 침입탐지와 엘라스틱 스택을 연동하여 이를 관리 콘솔을 통하여 보안 관리를 하는 SIEM 구조에 취약점 탐지를 추가한 설계이다. 중요 개념은 엘라스틱 스택을 통한 통합 관리이다.

	#	Description	Module	Port	Payload fmt
	1	Bruteforce against FTP with ncrack	bruteForce		command
<ul style="list-style-type: none"> <li>• Start: 2017-06-29 14:42:07.539559</li> <li>• End: 2017-06-29 14:42:28.563484</li> <li>• Sig match: (?)brute</li> </ul>					
<b>Payload:</b> /usr/local/bin/ncrack -f -U data/ncrack-users.txt -P data/ncrack-passwords.txt 192.168.0.113:21					

[그림 5] 공격 도구를 사용한 Brute Force 공격 시도

[Fig. 5] Example of Brute Force Attack

기능에 대한 검증을 위하여 다음과 같은 환경을 설정하고 실험을 진행하였다. 우선 취약점 분석을 위하여 클라우드 상 가상 서버에 대하여 기본적인 서버로 설정하고 취약점 분석 도구는 최신의 취약점 탐지 정책을 적용하였다. 침입 탐지에 대한 환경은 실제 모의 공격에서 기본적으로 사용되는 Id/Password를 무차별로 시도하는 “Brute Force” 공격을 시도하는 도구를 사용하여 정해진 시기에 공격이 이루어지게 설정하였다. 매 공격은 [그림 5]처럼 공격에 대한 자세한 정보를 확인할 수 있다. 이에 대한 탐지 및 공격에 대한 검색, 시각화 기능이 공격시점과 공격을 시도한 서버를 실시간으로 진행되는지 비교하면서 기능 검증을 하였다.

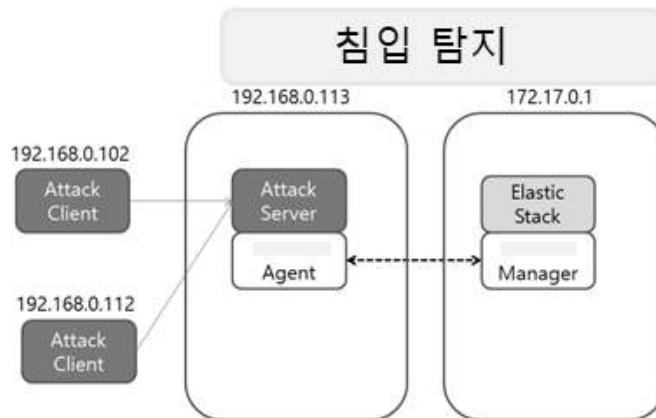
## 4. 구현 및 결과

엘라스틱 스택에서 취약점 분석도구와 침입 탐지도구에서 보내는 로그들과 이벤트들을 수집하게 하였다. 즉, 로그/이벤트 수집 기능을 담당하는 “Logstash”로 각 도구들이 데이터를 보낼 수 있도록 연동 API를 구현하였고, 시각화 기능을 담당하는 “Kibana”에서 각 도구들이 보낸 데이터들을 표시하여 사용자가 현재의 상태를 바로 확인하게 만들었다.[8]

### 4.1 침입 탐지 연동부

침입탐지 도구의 경우, 공격을 받는 가상머신에 설치된 Agent에서 비정상적인 활동에 대한 커널의 로그와 특정 사건에 대한 로그들을 수집하고, 이 로그들을 실시간으로 침입 탐지 서버로 전달되어져서 분석된다. 분석(Analysis)은 이상행동에 대해서 정의된 각 규칙(Rule)들과 비교하는 절차이다. 이 비교를 통하여 정상/이상여부가 판단 내려지고, 이상행동일 경우는 경고(Alert) 이벤트가 생성된다. 이 생성된 이벤트를 엘라스틱 스택에게 전달할 수 있는 Logstash 연동 부를 구현하였다. 엘라스틱 스택에서는 전달 받은 경고들을 사용하여 보안 관리자가 공격 패턴이나 공격을 시도한 서버 등에 대한 정보를 추려 낼 수 있고, 이를 통하여 이상 증후에 대한 판단을 할 수 있게 된다.[9]





[그림 6] SIEM 구조 및 환경

[Fig. 6] Structure and Environment of SIEM

[그림 6]는 침입 탐지와 엘라스틱 스택을 연동한 SIEM 환경에서 진행된 공격이 이루어진 환경을 보였다. 공격을 받은 호스트 “192.168.0.113”에서는 공격에 대한 관련 정보를 보안 정보관리를 하는 서버인 “172.168.0.1”에 전달한다. 서버 “172.168.0.1”에서는 주어진 공격에 대해 실시간으로 이상행위 분석을 하고 처리 결과를 [그림 7]처럼 표시한다.

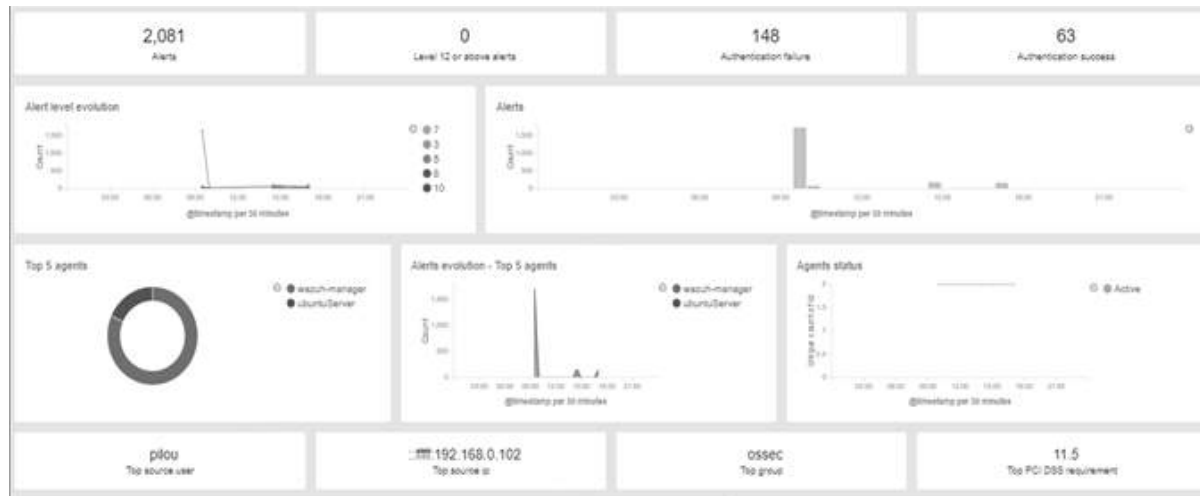


[그림 7] 전체 경고 로그들에 대한 화면

[Fig. 7] DISCOVER View of Total Alert Log

[그림 7]의 결과를 분석하여 보면 3개의 사각형으로 별도 표시한 것과 같이 공격자 IP, 공격 유형, 이상 행동, 시도한 시간, 로그의 정보를 확인 할 수 있다.

다음 실험으로 “192.168.0.112”에서 다른 패턴의 공격들을 시도를 하였다. 이 경우 기존의 인덱스들에 추가로 시도된 공격들의 실시간 인덱스들이 포함하여 공격시도들이 계속하여 발생한 것을 보여 주었다. 이에 대하여 엘라스틱서치를 이용하면 필요한 정보를 찾을 수 있다. “Brute Force”에 대한 공격 시도를 찾기 위하여 “brute”를 검색하면, 엘라스틱 스택에서 탐색을 담당하는 elasticserach에서는 해당되는 항목들만 선별하여 다시 표시를 한다. 또한 공격자에 대해서도 선별 탐색하여 분류할 수 있다. 또한 로그 형식으로 된 방식이외에 사용자가 [그림 5]와 같은 대쉬보드(Dashboard)를 구성하여 원하는 정보에 대하여 즉각적인 결과를 얻을 수 있고, 이 대쉬보드에서 사용자가 원하는 각 항목을 선택하면, elasticserach는 이에 대해 다시 자동분류를 진행하고, 결과를 명시적으로 보여주게 하였다.



[그림 8] “192.168.0.102”와 “192.168.0.112” 공격들에 대한 대쉬보드 화면

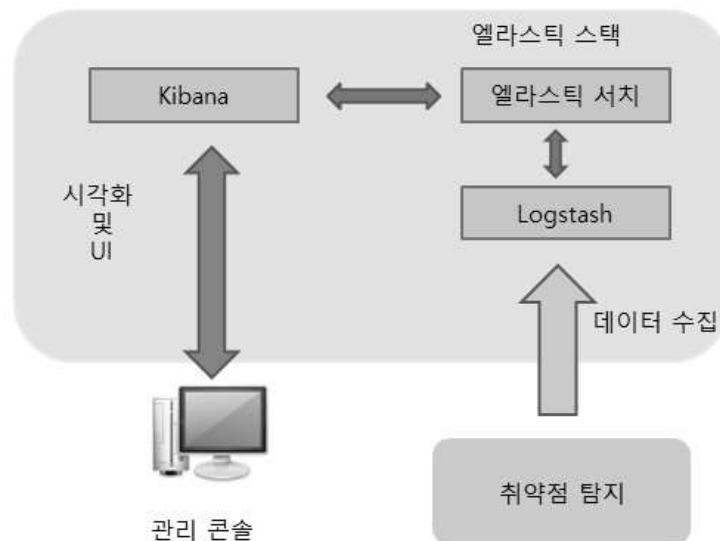
[Fig. 8] Dashboard of Total Attacks - “192.168.0.102” and “192.168.0.112”

[그림 8]의 결과를 보면 2곳의 공격자가 시간 간격을 가지고 다른 공격 패턴으로 호스트에 접근하여, 호스트에서는 지금까지 2,081의 이상행동이 발생하였다고 표시한다. 이 시각화 기능에서 사용자가 필요한 각각 개별사항에 대한 자세한 사항들은 GUI(Graphic User Interface)기능을 이용하여 세분화하고 검색 및 분류하여 확인 할 수 있다. 즉, 사용자가 알고 싶은 시간대, 공격 패턴, 공격 IP등에 대하여 직관적인 GUI를 사용하여 선택하면, 엘라스틱 스택이 바로 분류하여 데이터를 보내고, 시각화된 상태로 보여주게 구성하였다. 위 그림에서 사용자가 분류를 원하는 화면을 선택하게 되면 시각화로 각 상황별 분류 및 구분이 가능하게 만들고, 공격에 대한 패턴과 반복되는 시점들, 경고들에 대한 추이를 나타내는 그래프, 경고의 순위가 높은 위험한 공격에 대한 시도 들을

확인할 수 있게 만들어서 공격에 대한 연관성 추론을 지원하게 구성하였다.

## 4.2 취약점 탐지 연동부

취약점 탐지에 대한 연동부는 침입탐지 연동부와 동일하게 엘라스틱 스택의 logstash에 취약점 분석 진행 중 나온 결과 로그들을 전달할 수 있는 API를 구현하였다. 취약점 탐지가 진행되면 기본적인 도구에 대한 로그 및 취약점 탐지 결과, 도구에서 발생한 이벤트 로그, 가상머신 상태에 대한 로그들이 생성하게 하였다. 이 데이터들을 구현된 API를 이용하여 logstash로 전달하고 이후는 엘라스틱 스택에서 처리된다. [그림 9]는 취약점 도구와 엘라스틱 스택간의 연동과 관리콘솔을 이용하는 구조를 보인다. 관리 콘솔을 통하여 취약점 탐지도구에서 받은 데이터들을 엘라스틱 스택을 통하여 사용자가 원하는 항목에 대한 표시 및 사용자와의 연동은 Kibana에서 필요한 데이터들을 표시하는 기능을 추가하게 설정할 수 있게 하였다.



[그림 9] 엘라스틱 스택과 취약점 탐지부 연동

[Fig. 9] Connection Elastic Stack with Security Vulnerability Detection

## 5. 결 론

본 논문에서 제시한 클라우드 보안 정보관리 플랫폼은 클라우드 상의 가상머신에 대한 취약점을 동적으로 모니터링하고 사이버 공격에 대하여서 탐지 및 시각화를 실시간으로 수행함으로써 APT공격과 같은 지능적 공격을 대비할 수 있도록 만든 도구이다. 본 도구는 클라우드 상 자원에 대한 주기적 취약점 분석을 통하여 문제점 분석 및 파악을 하여 보안에 관련된 문제들을 사전에 예방할 수 기능과 실제로 공격이 이루어질 때 이 사항을 실시간으로 모니터링, 자동분석, 문제에

대한 역추적 할 수 있는 기능을 가지고 있다. 취약점 판단 정보와 공격 패턴에 대한 정보를 최신으로 유지하게 되면, 신규 공격에 대하여 능동적으로 대비할 수 있다.

신규로 제안된 취약점 분석을 통하여 얻은 정보와 공격 탐지 기능을 통합한 현재의 구현의 경우, 동일 인터페이스로 사용자에게 두 개의 정보를 제공함으로써 자원에 대한 취약점 파악을 통한 악성공격에 대한 대비 및 실제 침입 시도에 대한 탐지와 차단할 수 있다. 현재 시스템의 활용 방안으로 호스트의 취약점에 특정된 공격이 발생하면, 가장 높은 경고를 알리고, 최우선적으로 차단을 하도록 구현을 진행 중이다. 이러한 방식을 통해서 호스트에서의 취약점과 공격탐지 및 조치에 대해 상관관계를 도출하여 적용함으로써 좀 더 진화된 형태의 방어 시스템을 구축함으로써 동적으로 이상 행위를 식별할 수 있는 방법을 연구하는 중이며 또한 보안 관리자의 행동 양식을 좀 더 간소화할 수 있도록 시각화 기능도 개선 할 예정이다.[10]

## REFERENCE

- [1] “Cloud computing”, Wikipedia [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing) (accessed April., 3, 2017), (2017).
- [2] “Cloud computing security”, Wikipedia [http://en.wikipedia.org/wiki/Cloud\\_computing\\_security](http://en.wikipedia.org/wiki/Cloud_computing_security) (accessed April., 3, 2017), (2017).
- [3] B.Ramachandran, “NAVIGATING THE MAZE OF CYBER SECURITY INTELLIGENCE AND ANALYTICS“, connectedtechnbiz, (2014).
- [4] Jae-in Shin, Kwan-Yeol Park, Hyun-Jung Lee, Chan-Ho Ryu, Kab-Seung Kou, “Development of Cloud-SCAN V1.0 for Security Evaluation in Cloud Service Environment”, Journal of Security Engineering, (2014), Vol.11, No.6, pp. 567-580.
- [5] Open Source HIDS Security, <https://ossec.github.io/> (accessed April., 28, 2017), (2017).
- [6] Elasticsearch, <https://www.elastic.co/> (accessed April., 8, 2017), (2017).
- [7] J.M Park, B.W Hwang, W.D Jo, G.S, Kim, G.H Kim, “An Example and Application of Statical Anomaly Detection using Elasticsearch” Proceeding of the Winter Conference of the Korea Communication Society, (2017), pp. 1232-1234.
- [8] Open Source Host and Endpoint Security, <https://wazuh.com/> (accessed May., 28, 2017), (2017).
- [9] A.Chernysh. “OSSEC (Wazuh) and ELK as a unified security information and event management system (SIEM)“. Medium. (2017).
- [10] Introducing Machine Learning for the Elastic Stack, <https://www.elastic.co/kr/blog/introducing-machine-learning-for-the-elastic-stack> (accessed May., 19, 2017), (2017).