한국융합보안학회 2025년 추계학술대회 논문집

BAS-SIEM 연동을 통한 예측형 공격 시뮬레이션과 탐지 자동화 프레임워크

윤현식[1], 서동민[1], 김동현[1]*, 윤지현[1] 이병천[1]
중부대학교[1]

A Framework for Predictive Attack Simulation and Detection through BAS-SIEM Interconnection

HyunSik Yonn[1], Dongmin Seo[1], DongHyun Kim[1*] , JiHyeon Yoon[1], Byoungcheon Lee[1]

요약 : 본 연구는 BAS(Caldera)와 SIEM(ELK) 그리고 피해자(Agent) 서버로 구성된 작은 SOC환경에서 BAS솔루션을 보다 효율적으로 사용하기 위해 연구 결과, BAS와 SIEM통합 워크플로우를 제시하여 예측 가능한 공격 시뮬레이션을 통해 보안 장비의 탐지 여부의 자동 매칭을 통해 검증 과정을 자동화를 통하여 공격 시뮬레이션을 통한 탐지 체계의 효과적인 정비를 할 수 있음을 확인했다.

Key Words : Breach and Attack Simulation, Security Information and Event Management, Security Operations Center

1. 서 론

보안 운영 환경에서는 침해사고가 여러 단계를 거쳐 진행되는 다단계 공격(Multi-Stage Attack)에 효과적으로 대응하기 위해, 탐지 규칙의 자동화된 검증 체계 구축이 요구되고 있다. 이를 위해 공격자의 전술/기법/절차(TTP)를 실제 환경에서 모의 수행해보는 BAS (Breach and Attack Simulation) 도구가 활용되고 있다.

그러나 대부분의 오픈소스 BAS 솔루션은 공격 실행 이후의 탐지 결과를 SIEM 시스템과 연동하는 기능이 부족하여, 탐지 로그를 수동으로 확인해야 하는 비효율성이 존재한다. 또한 공격 재현 과정이 수동으로 이루어질 경우, 실험 조건이 일정하게 유지되지 않아 검증 결과의 재현성도 낮아진다.

이에 본 연구에서는 MITRE Caldera 기반 BAS 도구와 오픈소스 SIEM(ELK/Wazuh)을 통합하고, 공격-탐지 결과를 자동으로 매칭하는 Plugin 모듈을 설계·구현하여, 탐지 검증 절차를 자동화하고, 보안 운영의 효율성과 실험의 재현성을 동시에 향상시키는 것을 목표로 한다.

2. 선행 연구

BAS 솔루션과 SIEM의 통합 운영하는 사례로는 다음과 같은 연구가 있다.

먼저 MITRE ATT&CK기반의 자동화된 Red Team 공격 시뮬레이션 설계 및 구현연구[2]는 ATT&CK 프레임워크를 이용하여 공격 시나리오를 자동화하는 방법을 제시하여 BAS 솔루션을 통해 공격의 재현성과 효율성을 증가시켰다.

ELK Stack 과 Wazuh 통합 플랫폼 연구[1]는 오픈소스 SIEM의 구성요소인 Wazuh(Agent, Manager, Indexer)와 ELK 스택을 결합하여 SOC 플랫폼을 구현하며 SIEM의 구성 및 데이터 흐름을 구체적으로 분석하였다.

로그 기반 행위 이상탐지 아키텍쳐 연구[3]는 Wazuh Agent를 통해 행위 로그를 수집하여 Wazuh 룰을 기반으로 실시간 이상행위를 탐지하는 시스템을 설계하여 로그 기반 탐지의 효율성을 입증하였다.

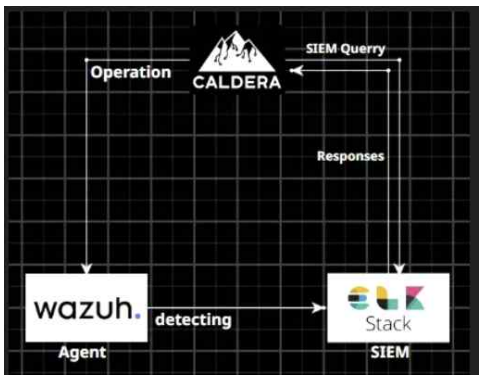
결과적으로 기존 연구들은 각각의 공격 자동화, 오픈소스 SIEM의 통합, 로그 분석 기반의 탐지체계와 같은 부분적인 분야에 집중하였다. 하지만 이 논문에서 제시하는 BAS 솔루션은 예측 가능한 공격을 통해 기존 보안체계를 점검하는 목적에 집중하여 BAS와 SIEM간의 연동을 통해 기존의 수동적인 점검 방식을 자동화하고자 한다.

3. 본론

3.1 시스템 개요 및 설계

본 연구에서 제안하는 시스템은 공격 시뮬레이션 솔루션과 보안 이벤트 관리 시스템간의 통합을 통해, 공격 수행 결과와 탐지 로그를 자동으로 매칭하는 구조로 설계하였다. 시스템은 크게 Caldera 기반 BAS, Plugin 모듈, Wazuh Agent, ELK Stack 구성이며 시스템의 전체 구성도는 <그림 1>과 같다.

1) Caldera는 공격 시나리오를 실행하여 각 Ability(공격 단계)의 결과 데이터를 생성하게 된다.
2) Plugin 모듈은 Caldera 내부에서 SIEM API와 통신하여 공격 로그와 SIEM에서 수집된 탐지 로그를 자동으로 조회 및 매칭하며 Operation ID를 기반으로 Ability별 이벤트 데이터를 수집하고, ELK에 동일한 명령 또는 PID를 포함한 로그를 쿼리하여 탐지 여부를 제공하게 된다.



<그림 1> System overview

3) Wazuh Agent는 피해자 서버에 설치되어 다양한 행위 데이터를 실시간으로 수집한다. 수집된 로그는 Wazuh Manager를 통해 ELK Stack으로 전송되어, SIEM 내에서 탐지 규칙에 따라 분석 및 저장된다.
4) ELK Stack은 수집된 로그를 통합 관리하고 Plugin 모듈의 쿼리 요청을 처리하는 역할이다.

이러한 구조를 통해 Caldera에서 발생한 공격 행위가 SIEM에서 실제로 탐지되었는지를 자동으로 검증할 수 있으며 공격-탐지의 매칭 결과는 Caldera 웹 인터페이스를 통해 실시간으로 확인할 수 있다. 따라서 본 시스템은 기존의 수동 로그 확인 과정을 자동화함으로써 탐지 검증의 효율성과 반복 실험의 재현성을 동시에 확보할 수 있다.

3.2 탐지 검증 자동화 구현

탐지 검증 자동화를 담당하는 Plugin 모듈은 Operation 안에서 실행되는 각각의 Ability의 pid, command 등과 같은 정보를 수집하여 Agent에서 수집된 탐지 로그 중 해당 pid와 command가 사용된 로그가 존재하는지 ELK에 쿼리를 진행하여 각각의 Abilty별로 탐지 여부를 매칭해주게 된다.

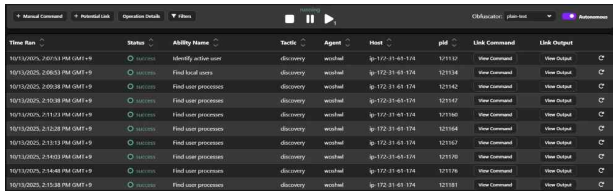
실험은 Caldera에서 지원하는 기본 시나리오는 Discovery 시나리오를 통해 진행했다. 이 시나리오에서는 사용자 조회 T1087.001 프로세스 정찰행위인 T1057 활성사용자 검색 T1033으로 이루어진 시나리오로 탐지 검증의 편의성을 위해 Wazuh의 기본 룰 중 T1057을 탐지하는 92604번 룰을 사용하였다

```
<group name="audit,T1057,">

  <rule id="92604" level="6" overwrite="yes">
    <if_sid>80792</if_sid>
    <field name="audit.exe" type="pcre2">(^/usr/bin/ps$)|(^/bin/ps$)</field>
    <description>Processes running for all users were queried with ps command.</description>
    <group>audit_detections,</group>
    <mitre>
      <id>T1057</id>
    </mitre>
  </rule>

</group>
```

<그림 2> Rule Settings



<그림 3> Discovery Operation

Discovery 시나리오를 실행했을때 각 Ability는 피해자 서버에 위치한 Caldera Agent를 통해 실행되며 각각의 행위는 30~60초 사이의 간격을 두고 실행한다.

<그림 4> Detection Matching

이때 Plugin 모듈을 통해 Ability별로 탐지가 될 경우 각각의 Ability와 탐지로그를 매칭하여 <그림 4> 처럼 제공하게 된다.

3.3 결과 분석

본 연구에서 제안한 Plugin 모듈을 활용하여 탐지 검증을 자동화하는 시스템의 효과성을 확인하기 위해서 Caldera의 Discovery 시나리오로 실험을 진행하였다.

실험 결과, Discovery 시나리오 실행시 Ability들은 피해자 서버에서 순차적으로 수행되었으며, Plugin 모듈은 Operation ID를 기반으로 Ability별 PID와 Command 정보를 수집하여 ELK에 DSL 쿼리를 전송함을 확인하였다. 총 3개의 Ability 중 T1087.001은 Wazuh 룰에 의해 부분적으로 탐지되었고, PID 기반 매칭에서 80%의 정확도를 보였다. T1057은 92604번 룰과 매칭되어 100% 매칭되었으며 T1033은 Command 키워드를 통해 90% 매칭률을 달성하였다. 전체 시나리오의 매칭 평균 시간은 Ability당 5~10초 정도로 수동 확인 방식 대비 약 80%의 시간 단축 효과를 확인하였다.

이러한 결과는 Plugin 모듈이 공격 로그와 탐지 로그 간의 자동 매칭을 통해 보안 검증의 효율성을 향상시킬 수 있음을 확인했다. 예를 들어 T1057 Ability의 경우 피해자 서버에서 실행된 'ps' 또는 'tasklist' 등의 명령이 Wazuh Agent에 의해 실시간으로 수집되고 ELK에 저장된 후 Plugin 모듈의 쿼리가 해당 로그를 정확히 식별해내었다. 그러나 일부 T1087.001 같은 Ability에서 낮은 매칭률을 보인 이유는 Wazuh 룰의 세밀한 튜닝 부족으로 분석된다. 이는 향후 연구에서 동적 룰 업데이트 기능을 추가하여 보완이 가능하다고 생각된다.

4. 결론

본 연구에서 제시한 Plugin 모듈을 이용한 BAS 솔루션 체계는 기존 공격 시뮬레이션 이후 탐지로그를

수동적으로 SIEM에서 분석해야 했던 점을 자동화하여 보안 운영의 효율성을 향상시켰다. 이를 통해 Caldera 기반 BAS와 ELK/Wazuh 기반 SIEM 간의 통합이 이루어졌으며, Operation ID를 기반으로 한 Ability별 로그 매칭이 실시간으로 수행되었으며 이를 통해 검증 과정의 시간을 줄일 수 있었다.

실험 결과, Discovery 시나리오에서 평균 80% 이상의 매칭 정확도와 시간 단축 효과를 확인하였고 제안된 시스템의 실무적 유용성을 입증하였다. 향후 연구에서는 Shuffle 기반 SOAR를 추가하여 동적 룰 수정 기능을 확장하고, Terraform과 Ansible을 활용한 클라우드 배포 자동화를 구현하여 시스템의 확장성을 강화할 계획이다.

참고문헌

[1] Kim, H.-J. and Kwak, J., “A Study on the Integration of ELK Stack and Wazuh Platform (ELK Stack 과 Wazuh 통합 플랫폼 연구),” Proceedings of ASK 2025 (Annual Conference of KIPS), Vol. 32, No. 1, 2025, pp. 830-831

[2] Oh, Y.-G. and Kwak, J., “Design and Implementation of Automated Red Team Attack Simulation Based on MITRE ATT&CK Framework (MITRE ATT&CK 기반의 자동화된 Red Team 공격 시뮬레이션 설계 및 구현),” Proceedings of ASK 2025 (Annual Conference of KIPS), Vol. 32, No. 1, 2025, pp. 832-833.

[3] Hong, L. and Kwak, J., “Architecture Design for Log-Based Behavioral Anomaly Detection System (로그 기반 행위 이상 탐지 체계 아키텍처 설계),” Proceedings of ASK 2025 (Annual Conference of KIPS), Vol. 32, No. 1, 2025, pp. 836-837.