엔드포인트 탐지 및 모니터링 솔루션

팀명 : FSF (For security first)
지도 교수 : 양환석 교수님
팀장 : 91913309 김채원
팀원 : 91913579 손경현
91913141 곽화종
91514763 박세연

2024.11
중부대학교 정보보호학과

목차

4. 분석

5. 결론

6. 별첨

1 . 서 론

1.1 연구배경

4차 산업혁명 시대에 접어들면서 IoT 시장이 빠르게 확대되고 있으며, 이에 따라 전체 시장의 규모도 꾸준히 커지고 있다. 이러한 기술 발전은 많은 편리함과 새로운 비즈니스 기회를 제공하고 있지만, 동시에 해킹과 같은 사이버 공격에 대한 위협도 함께 증가하고 있다. 랜섬웨어, 피싱, 웹 취약점 등의 공격 수법이 더욱 다양해지고, 그 방법도 복잡해지면서 많은 조직이 큰 피해를 보고 있다. 특히, 디지털 장치와 네트워크에 대한 의존도가 높아지는 오늘날, 비즈니스 활동을 안전하게 수행하기 위해서는 보다 철저한 보안 대책이 필수적이다. 이에 따라 끝점 보안의 중요성도 더욱 부각되고 있다. 조직들이 사용하는 다양한 디지털 장치들이 해커의 주요 타깃이 되면서, 이들 장치의 보안을 강화하는 것이 기업의 핵심 과제가 되고 있다. 안전한 네트워크 환경을 유지하고, 데이터를 보호하는 것은 비즈니스의 연속성과 신뢰성을 확보하는 데 필수적이다.

1.2 연구 필요성

엔드포인트란 네트워크망에 연결되는 모든 장치들을 의미하며, 이에 따라 대부분의 보안 사고는 엔드포인트를 타깃으로 시작된다. 또 지능화된 사이버 공격과 다양한 경로를 통한 제로데이, 랜섬웨어 등등 공격이 급증하고 있고 방식 또한 고도화되어 피해가 급증하고 있다. 이러한 공격을 수동으로 관제하기는 많은 시간과 인력이 필요하지만 자동화된 프로그램을 통해 실시간 모니터링하여 보안 위협에 빠른 대응이 가능하고 효율성이 향상된다. 또 취약점을 진단하여 악성 프로그램을 방지하여 엔드포인트 보안에 도움이 되고자 한다.

1.3 연구목적 및 주제선정

해당 연구의 주된 목적은 엔드포인트 탐지 및 모니터링 솔루션으로 Anti-Virus, EDR, 취약점 관리, 패치 관리 등 엔드포인트 위협에 있어 보호하고 관리하는 게 목적이다.

주제 선정 이유는 엔드포인트에 의존하는 조직들이 많아지고 있고 공격의 대부분은 엔드포인트를 타깃으로 시작되므로 엔드포인트 보안의 중요성을 강조하며, 실시간 탐지 및 대응을 강화한 엔드포인트 탐지 및 모니터링 솔루션을 개발하는 것이다.

2. 관련연구

2.1 Python

파이썬은 '귀도 반 로섬'이 발표한 고급 프로그래밍 언어로 다양한 분야에서 활용되는 범용적인 언어다. 웹 개발, 데이터 분석, 인공지능, 자동화 등 여러 영역에서 널리 사용되며, 풍부한 라이브러리와 커뮤니티 지원으로 인해 초보자부터 전문가까지 폭넓게 활용할 수 있는 것이 특징이다. 또한 파이썬은 객체 지향 프로그래밍, 함수형 프로그래밍 등을 지원하며, 생산성 높은 코드 작성과 빠른 개발을 가능하게 한다.

2.2 Linux

리눅스는 '리누스 토발즈'가 개발한 유닉스 계열 운영체제다. 리눅스는 오픈 소스 운영체제로 무료로 사용할 수 있고, 소스 코드가 공개되어 있어 누구나 쉽게 수정하고 개선할 수 있다. 이에 따라 많은 개발자가 참여하여 지속적인 개발과 업그레이드가 이루어지고 있다.

2.3 Window

Window는 마이크로소프트가 개발한 컴퓨터 운영 체제다. MS-DOS에서 멀티태스킹과 GUI 환경을 제공하기 위한 응용 프로그램으로 처음 출시되었다. 현재 전 세계 90%의 개인용 컴퓨터에서 쓰고 있으며, 서버용 운영 체제로도 점차 영역을 넓혀 나가고 있다. 윈도우 운영 체제의 경우 큰 시장 점유율을 차지하고 있는 까닭에 일반 사용자들에게 매우 익숙할뿐 아니라 호환되는 유명한 응용 프로그램이 많다는 장점을 지니고 있다.

2.4 Zabbix

Zabbix는 서버 및 네트워크의 상태를 실시간으로 모니터링 할 수 있는 오픈소스 기반의 모니터링 솔루션으로 시스템 및 네트워크 리소스 상태를 실시간으로 모니터링하고 관리하는데 사용되며, 대규모 환경에서도 사용할 수 있다. 또한 유연한 알림 메커니즘, 그래픽 표시 기능, 폴링과 트래핑, 웹 인터페이스 기능 등등 다양한 기능과 확장성을 가지고 있어 많은 기업 및 조직들이 사용하고 있다.

2.5 Elasticsearch & ELK

Elasticsearch는 Apache Lucene 라이브러리 기반으로 하는 Java 오픈 소스 검색 및 분석 엔진으로, 방대한 양의 데이터를 신속하게 저장, 검색, 분석을 수행할 수 있다. 이와 같이 대규모 데이터를 빠르게 처리해야 하는 경우 유용하게 사용 된다. Elasticsearch는 단독으로 사용 되기도 하며, ELK(Elasticsearch / Logstash / Kibana) 스택으로 사용되기도 한다.

Logstash는 데이터를 수집하여 변환한 후, Elasticsearch 같은 stash로 전송하는 데이터 처리 파이프라인이다.

Kibana는 Elasticsearch에서 차트와 그래프를 이용해 데이터 시각화를 가능하게 해주는 도구다.

2.6 Bash

Bash는 Unix 계열 운영체제에서 사용되는 명령 줄 인터페이스를 위한 쉘이다. Bash는“Bourne Again Shell”의 약자로 Stephen Bourne 쉘을 기반으로 개발되어 Unix, Linux, macOS 등에서 기본 쉘로 많이 사용 된다.

2.7 Sysmon

Sysmon은 Window 시스템 서비스 및 장치 드라이버로, 시스템에 설치되면 시스템 재부팅 후에도 상주하여 시스템 활동을 모니터링하고 Windows 이벤트 로그에 기록한다. 프로세스 생성, 네트워크 연결, 파일 생성 시간 변경 사항에 대한 자세한 정보를 제공한다. 이벤트를 수집한 후 이를 분석함으로써 악의적이거나 비정상적인 활동을 식별한다.

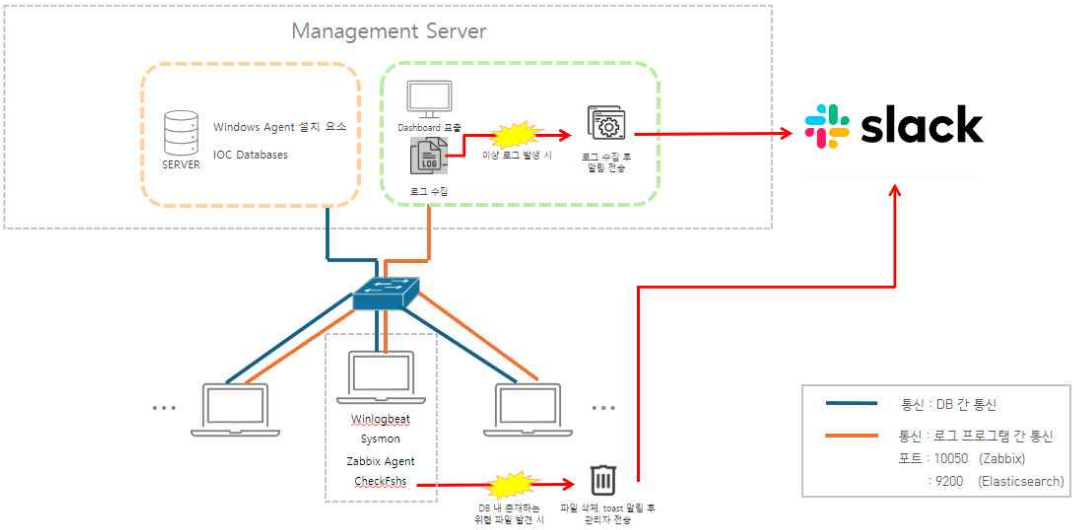
2.8 Winlogbeat

Winlogbeat는 경량 Windows 이벤트 로그 수집기로써, Windows 기반 인프라의 상태를 추적할 수 있게 해주며, Windows 이벤트 로그를 Elasticsearch와 Logstash로 스트리밍할 수 있도록 해준다.

3. 본 론

3.1 시스템 구성

시스템은 구성은 아래와 같이 이루어진다.

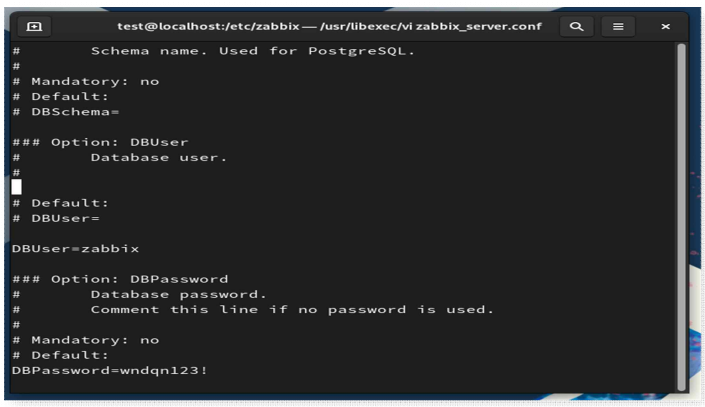


[그림1]

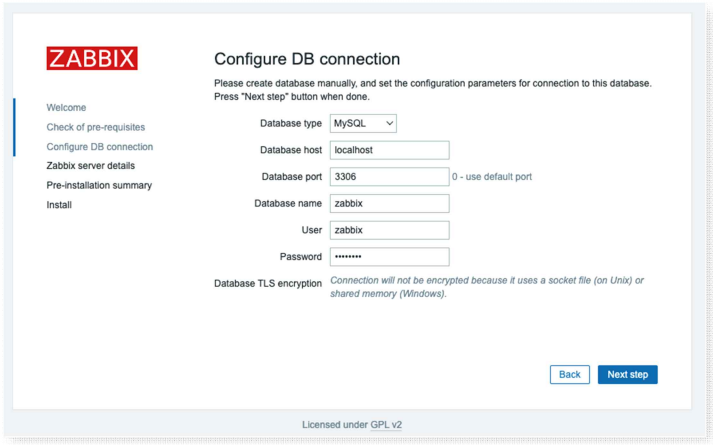
1. Managment Server에 Rocky_server, Agent, IOC Databases 구성한다.
2. 대상 PC를 모니터링하기 위해 endpoint는 Winlogbeat, Sysmon, Zabbix, checkFSF 구성한다.
3. DB 내 존재하는 위협 파일 발견시 즉시 삭제 및 알림을 주고 slack로 전송한다.
4. 관리자 서버에서 여러 도구들을 이용해 대상 pc의 로그를 수집한다.
5. 이상 로그 발생시 로그 수집 후 알림을 전송하고 slack 으로 전송한다.

3.2 프로그램 구성

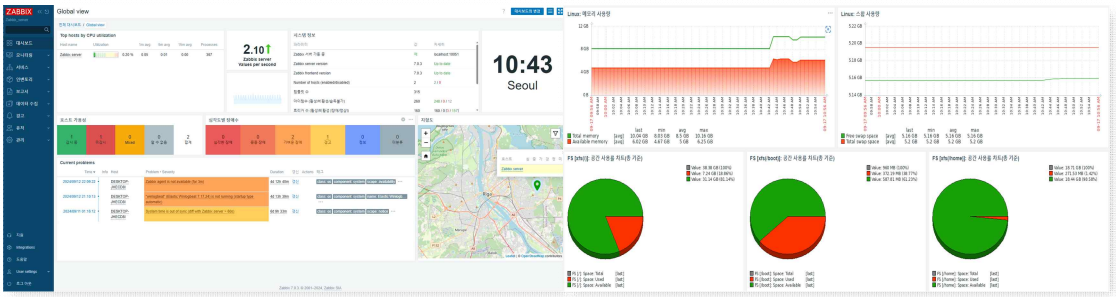
3.2.1 Zabbix



[그림2.1]



[그림2.2]

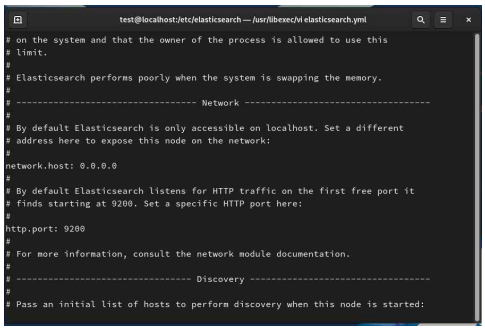


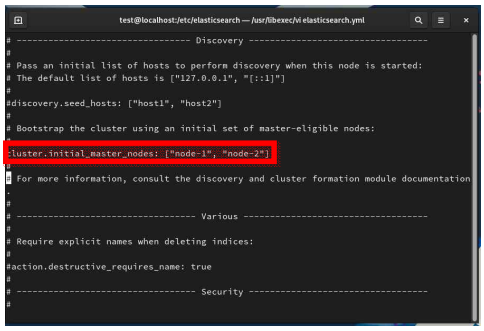
[그림2.3]

[그림2.4]

[그림 2.1]에서는 Zabbix 유저의 ID와 비밀번호를 설정하고, [그림 2.2]에서는 Zabbix DB를 설정한다. Zabbix의 [그림 2.3]은 Main Dashboard를 나타내며, 여기에서는 전체 Endpoint의 현황을 확인하고, 대상 PC에 위협이 발생할 경우 이를 감지할 수 있다. 또한 Endpoint의 대략적인 위치를 파악할 수 있다. [그림 2.4]는 개별 Endpoint의 대시보드를 나타내며, 시스템 및 네트워크 사용량, 작업 스케줄러, Windows 서비스 상태 등을 확인할 수 있는 단일 Endpoint 대시보드이다.

3.2.2 Elasticsearch



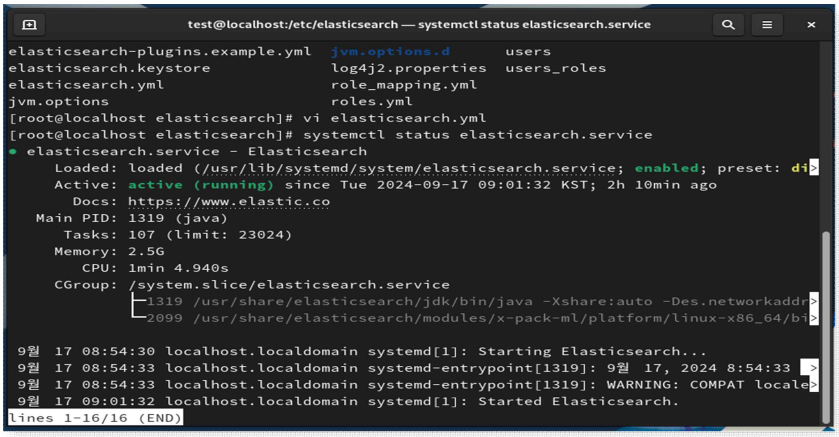


[그림3.1]

[그림3.2]

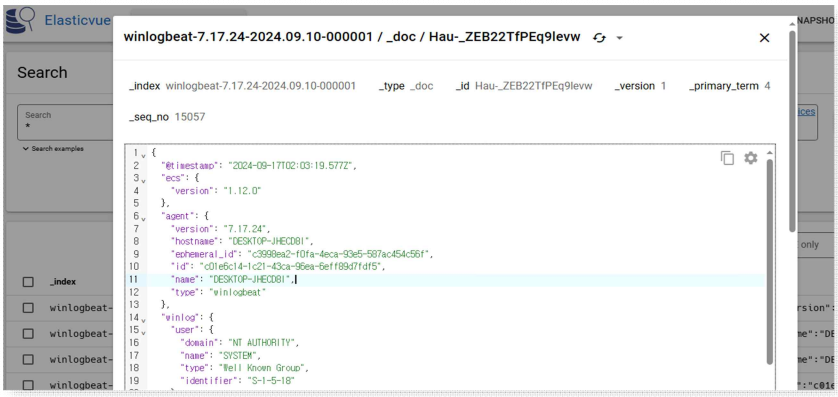
[그림3.1] 에서는 host 와 port를 나타낸다.

[그림3.2] “cluster.initial_master_nodes”에서 master 후보 노드의 리스트를 나타낸다. [그림3.2]에서는 두 개의 후보를 나타낸다.



[그림3.3]

systemctl 명령어를 사용하면 현재 실행 중인 Elasticsearch의 상태를 쉽게 확인할 수 있다. 이 명령어는 시스템 서비스의 상태를 표시하며, Elasticsearch가 정상적으로 동작하고 있다면 "active(running)"이라는 메시지가 나타난다. 이 상태는 서비스가 오류 없이 실행 중임을 의미한다. [그림3.3]에서는 active 상태임을 보아 Elasticsearch가 실행 중임을 알 수 있다.



[그림3.4]

[그림3.4]는 Elasticsearch Indexf를 나타낸다. 이는 Endpoint로부터 수집된 다양한 데이터를 저장하는데, 여기에는 윈도우 이벤트 로그, 프로그램 시작 정보, 해시 정보 등 중요한 시스템 정보가 포함된다. 이러한 데이터를 통해 시스템의 작동 상태를 모니터링하고, 보안 위협을 감지하거나 분석할 수 있다.

3.2.3 Bash

```bash
#!/bin/bash

# Elasticsearch 서버 URL과 인덱스
ES_URL="http://192.168.0.112:9200"
INDEX_NAME="winlogbeat-7.17.24-2024.09.10-000001"
SLACK_WEBHOOK_URL="https://hooks.slack.com/services/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"

# 중요 이벤트 탐지 시 Slack으로 알림 보내기
send_slack_alert() {
    local message=$1
    curl -X POST -H 'Content-type: application/json' \
        --data "{\"text\":\"$message\"}" \
        $SLACK_WEBHOOK_URL
}
```

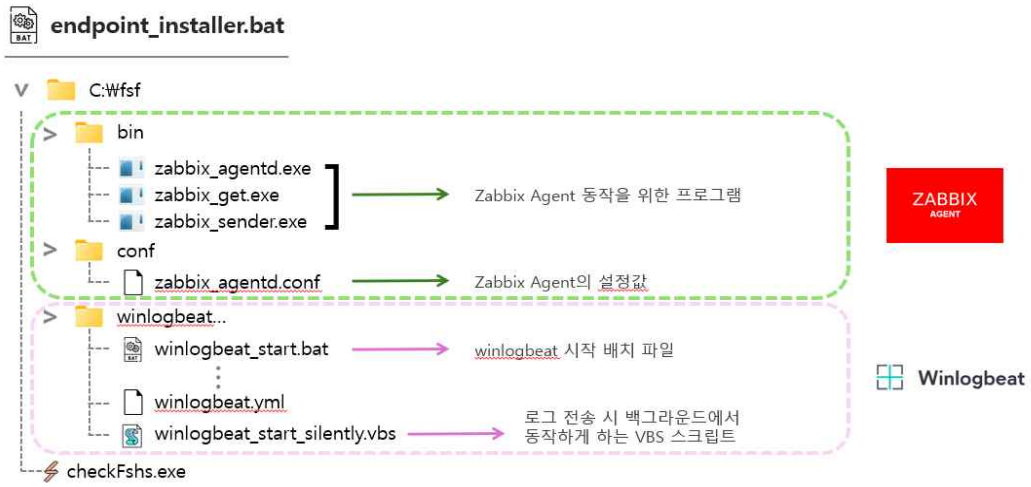
[그림4.1]

[그림 4.1]에서는 환경변수를 통해 Elasticsearch 서버 URL과 INDEX_NAME을 설정하여 Elasticsearch_index를 지정하여 데이터를 효율적으로 저장하고 관리하기 위한 기반을 제공한다. 이어지는 문단에서는 중요한 이벤트가 탐지될 때 알림을 보내도록 설정하였다. 또 Slack Webhook을 통해 발송될 메시지와 그 URL을 지정하고 있다.

[그림4.2]

[그림 4.2]에서는 Elasticsearch 검색 쿼리문이 작성된 내용을 보여준다. 이 코드에서는 10초 간격으로 인덱스 상태를 확인하고 Elasticsearch에서 중요한 보안 이벤트를 검색하도록 설정하였다. 또한, 중요한 이벤트가 발생할 경우 Slack으로 알림이 전송되도록 구현하였으며, 이 역시 10초 간격으로 확인하도록 코딩하였다.

3.2.4 Endpoint



[그림5.1]

[그림 5.1]을 통해 Zabbix Agent 동작을 위한 프로그램과 Zabbix Agent의 설정값을 확인할 수 있다. 또한, Winlogbeat의 시작 배치 파일과 로그 전송 시 백그라운드에서 동작하게 하는 VBS 스크립트도 포함되어 있다. 이외에도 파이썬으로 개발한 checkFshs.exe 파일에 대한 정보도 확인할 수 있다.

```
:: 1. 파일 다운로드 및 압축 해제
echo 1. test.zip 파일 다운로드 및 압축 해제 중...
powershell -Command "(New-Object System.Net.WebClient).DownloadFile('http://192.168.0.10/windows_agent/test.zip', 'C:₩test.zip')"
powershell -Command "Expand-Archive -Path 'C:₩test.zip' -DestinationPath 'C:₩test₩' -Force"
powershell -Command "rm -Path 'C:₩test.zip'"

:: 2. Zabbix Agent 실행 및 서비스 시작
echo 2. Zabbix Agent 실행 및 서비스 시작 중...
start /b "" "C:₩test₩bin₩zabbix_agentd.exe" -c "C:₩test₩conf₩zabbix_agentd.conf" -i
sc start "Zabbix Agent"

:: 방화벽 인바운드 10050 포트 개방
netsh advfirewall firewall add rule name="Zabbix 포트 개방" protocol=TCP dir=in localport=10050 action=allow

:: 3. Sysmon 다운로드 및 설치
echo 3. Sysmon 다운로드 및 설치 중...
powershell -Command "(New-Object System.Net.WebClient).DownloadFile('https://download.sysinternals.com/files/Sysmon.zip', 'C:₩test₩Sysmon.zip')"
powershell -Command "Expand-Archive -Path 'C:₩test₩Sysmon.zip' -DestinationPath 'C:₩test' -Force"
:: 4. Winlogbeat 실행 및 시작 프로그램 등록
echo 4. Winlogbeat 백그라운드 실행 및 시작 프로그램 등록 중...
start /b "" "C:₩test₩winlogbeat-7.17.24-windows-x86_64₩winlogbeat_start_silently.vbs"
reg add "HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run" /v "Winlogbeat" /d "₩"C:₩test₩winlogbeat-7.17.24-windows-x86_64₩winlogbeat_start_silently.vbs₩"" /f

:: 5. CheckFs 파일 다운로드 및 실행
echo 5. CheckFs 파일 다운로드 및 실행 중...
powershell -Command "(New-Object System.Net.WebClient).DownloadFile('http://192.168.0.10/windows_agent/chfsIOC.exe', 'C:₩test₩chfsIOC.exe')"
start /b "" "C:₩test₩chfsIOC.exe"

:: CheckFs 시작 프로그램 등록
reg add "HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run" /v "CheckFs" /d "₩"C:₩test₩chfsIOC.exe₩"" /f


pause
echo 모든 작업이 완료되었습니다 ! 프로그램을 종료해도 좋습니다.
exit /b
```

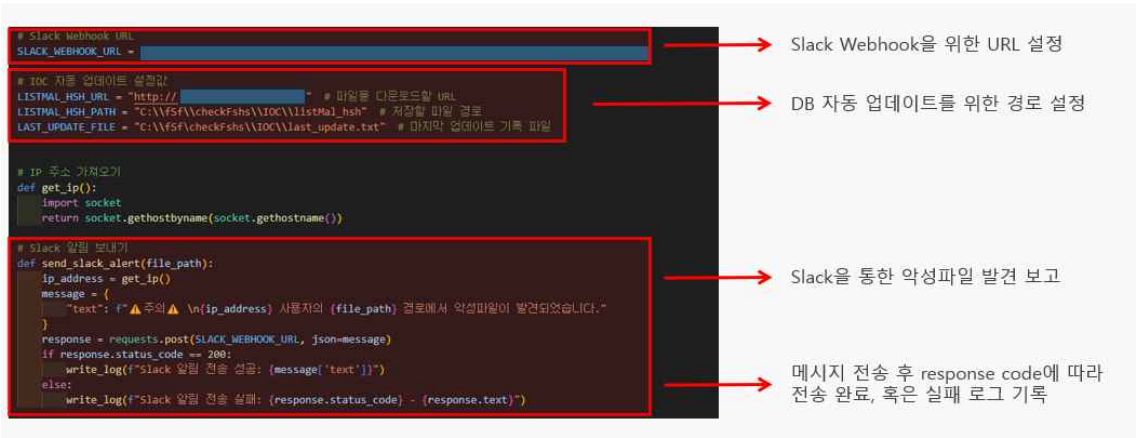
[그림5.2]

[그림 5.2]에서는 프로그램이 다음과 같은 순서로 진행된다. 먼저, 최소 필수 파일을 다운로드하고 압축을 해제한 후, 설정된 파일을 기반으로 Zabbix Agent 서비스를 시작한다. 이후 Zabbix Agent의 통신을 위해 10050 포트를 개방하고, MS 서버로부터 Sysmon을 다운로드하여 압축을 해제한다. 다음으로, Winlogbeat를 백그라운드에서

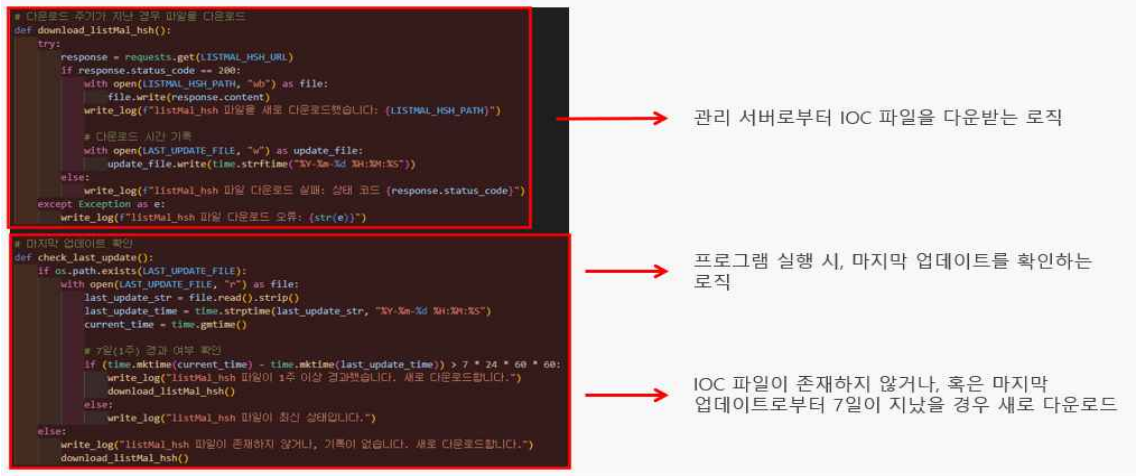
실행하고 시작 프로그램에 등록한 후, 자체 개발한 checkFshs 파일을 실행하여 시작 프로그램에 등록한다. 마지막으로, 작업이 종료된다.

3.2.5 FSF

FSF는 [그림5.1]에서 CheckFshs.exe를 나타내며 파이썬으로 자체 개발한 엔드포인트 탐지 및 모니터링 솔루션이다. FSF는 실시간 엔드포인트를 모니터링하고 엔드포인트 주요 이벤트로그를 탐지한다. 또 IOC기반 및 관리자 정의를 통한 악성 프로그램을 방지하며 위협 발생 시 Slack 등을 통한 알림 서비스를 제공한다.



[그림6.1]



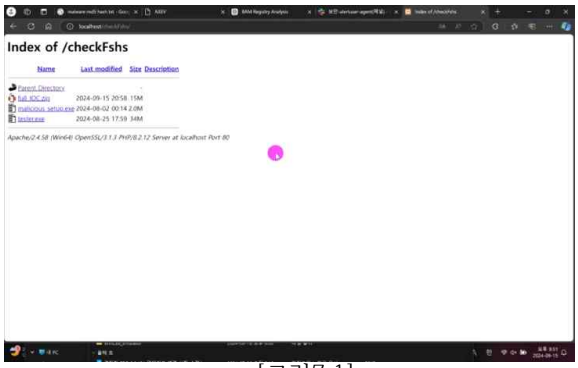
[그림6.2]

[그림6.3]

[그림 6.1], [그림6.2], [그림6.3]에서 FSF의 기능들을 코딩한 것을 나타낸다.

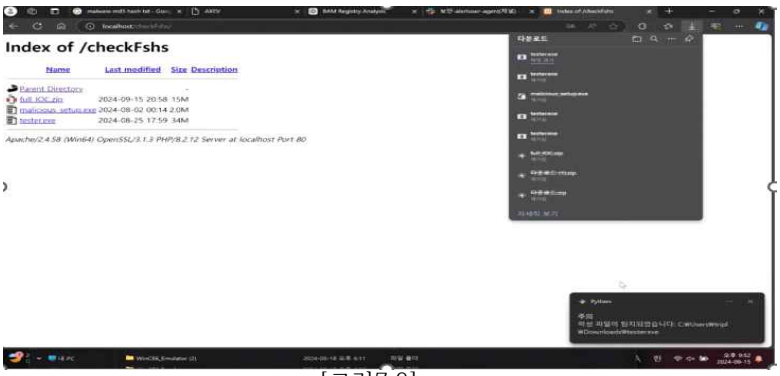
4. 분 석

4.1 활용결과 및 성능



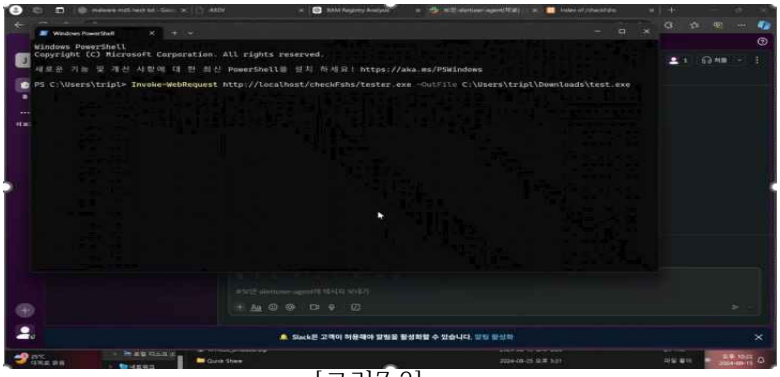
[그림7.1]

[그림7.1]와 같이 tester.exe(악성파일)을 웹에서 다운로드하고 실행 시



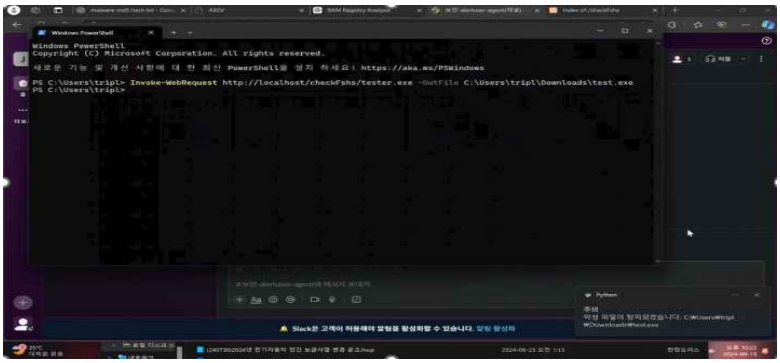
[그림7.2]

“주의, 악성 파일이 탐지되었습니다” 라고 fsf가 작동하여 막는다.



[그림7.3]

[그림7.3]과 같이 CTL에서 악성파일을 다운로드시



[그림7.4]

위와같이 악성파일을 발견하고 막는다.

위와 같은 악성파일이 아니더라도 모니터링 하면서 별첨에 있는 “정보보호프로젝트 침해사고보고서”에 따른 악성파일, 악성코드들을 탐지하고 당장 위협하면 삭제하고 알림 및 slack을 통해 전송한다. 또 로그를 수집하면서 slack에 로그를 수집하고 판단 및 진단한다.

4.2 추후 보완사항

AWS 클라우드를 활용하면 프로세스와 웹 서비스를 효율적으로 관리하고, 다양한 로그를 안전하게 보관할 수 있다. 또한, 바이러스 토탈 및 ATT&CK와 같은 도구를 이용해 악성코드를 AI로 학습시켜 표본을 늘리고, 이를 통해 더욱 효과적으로 악성코드를 예방할 수 있다. 또 확장 가능한 구조로 향후 새로운 보안도구를 추가할 수 있다.

5. 결 론

5.1 결 론

본 연구는 4차 산업혁명 시대에 빠르게 확대되는 IoT 시장에서 엔드포인트 보안의 중요성을 강조하며, 자동화된 탐지 및 모니터링 솔루션을 개발하여 사이버 공격에

효과적으로 대응하는 방안을 제시하였다. 엔드포인트가 주요 타겟이 되는 다양한 사이버 공격이 증가함에 따라, 조직은 실시간 모니터링 및 신속한 대응 체계를 갖추는 것이 필수적이다.

본 연구에서 개발한 솔루션은 Zabbix, Elasticsearch, Sysmon, Winlogbeat 등 다양한 도구를 통합하여 엔드포인트의 상태를 지속적으로 모니터링하고, 위협 발생 시 즉각적인 알림을 제공함으로써 보안 위협에 효과적으로 대응할 수 있도록 설계되었다. 실험 결과, 악성 파일 탐지 및 차단에 성공하였으며, 이는 시스템의 안전성을 높이는 데 기여할 것이다.

향후 연구에서는 AWS 클라우드를 활용하여 데이터 저장 및 분석 효율성을 더욱 높이고, 바이러스 토탈 및 ATT&CK와 같은 도구를 통해 악성코드 탐지 및 예방 체계를 강화할 계획이다. 이러한 노력은 조직의 사이버 보안 역량을 한층 강화하고, 비즈니스 활동의 연속성과 신뢰성을 확보하는 데 중요한 역할을 할 것이다.

결론적으로, 엔드포인트 보안은 현대 비즈니스 환경에서 필수적인 요소이며, 본 연구에서 제안한 솔루션은 이를 효과적으로 지원할 수 있는 기반을 마련하였다고 할 수 있다. 앞으로도 지속적인 발전과 연구를 통해 더욱 강화된 보안 체계를 구축해 나가야 할 것이다.

5.2 기대효과

본 연구에서 개발한 엔드포인트 탐지 및 모니터링 솔루션은 여러 가지 기대효과를 제공한다. 첫째, 실시간 위협 탐지 및 모니터링을 강화하여 시스템이 즉각적으로 위협을 식별하고 대응할 수 있어 보안 사고를 사전에 예방할 수 있다. 둘째, 중앙 집중화된 로그 분석을 통해 보다 효과적인 보안 인사이트를 제공하며, 잠재적인 위협을 조기에 발견할 수 있다. 셋째, 조직의 특성에 맞춘 커스텀 IOC를 활용하여 특정 위협에 대한 탐지 및 대응 능력을 증가시킨다. 넷째, 자동화된 설치 및 구성으로 배포 효율성을 높여 빠르고 손쉬운 시스템 설치가 가능해진다. 다섯째, 다양한 데이터 소스를 통합하여 보다 포괄적인 보안 분석을 수행할 수 있으며, 이는 전체 보안 체계를 한층 강화하는 데 기여한다. 마지막으로, 확장 가능한 구조를 통해 새로운 보안 도구를 손쉽게 추가할 수 있어 변화하는 위협 환경에 유연하게 대응할 수 있다. 이러한 기대효과를 통해 조직은 더욱 강력한 보안 체계를 구축하고 사이버 공격에 대한 저항력을 강화할 수 있을 것으로 기대된다.

6. 별 첨

6.1 팀원소개

팀장 : 김채원
(악성코드 및 Elasticseach 쿼리문 제작, 모의해킹 및 침해사고 분석 보고서 작성)
팀원 : 손경현
Linux 관리 서버 제작, Window Agent Installer 제작, IOC 기반 악성파일 제거 프로그램 제작
팀원 : 곽화종
악성코드 제작 및 프로젝트 진행

6.2 발표자료

졸작PPT최종.ppt

6.3 침해사고분석보고서

정보보호프로젝트 침해사고보고서.pdf

6.4 소개자료

졸작 폼보드.pdf

6.5 시연영상

https://www.youtube.com/watch?v=Werk9WuPEUY