Chainsaw의 예제 파일과

AI를 활용한

취약점 분석 보고서

작성일 2025년 8월 21일

작성자 Cyber Security 4 정현지

목차

개요

이 보고서는 Chainsaw라는 오픈 소스 포렌식 도구를 활용하여 Windows 이벤트 로그 파일을 분석한 결과를 담고 있습니다. 분석의 주된 목적은 시스템 내에 발생했을 수 있는 잠재적인 보안 취약점 및 악의적인 활동의 흔적을 식별하고, 이에 대한 구체적인 개선 방안을 제시함으로써 전반적인 시스템의 보안 태세 강화에 이바지하는 것입니다.

특히, 이번 분석은 Sigma 룰(Rule) 기반의 탐지 방식을 사용하여 진행되었습니다. Sigma는 보안 이벤트 로그에 대한 일반적인 탐지 규칙 표준으로, 다양한 보안 도구와 플랫폼에서 위협 탐지 및 분석 규칙을 공유하고 재사용할 수 있도록 돕는 역할을 합니다. 이를 통해 알려진 공격 기법 및 악성 행위에 대한 패턴을 효과적으로 식별할 수 있었습니다.

분석 대상 및 환경

이 보고서의 분석 대상은 Chainsaw 도구를 통해 처리된 Windows 보안 이벤트 로그 파일들입니다.

분석 대상 로그 파일

- 4794_DSRM_password_change_t1098.evtx: DSRM(Directory Service Restore Mode) 계정 비밀번호 변경과 관련된 이벤트 로그.
- 4765_sidhistory_add_t1178.evtx: SID History 추가와 관련된 이벤트 로그.
- privexchange_dirkjan.evtx: Pass-the-Hash (PtH) 공격 및 기타 Windows 보안 로그 관련 이벤트가 포함된 로그.

분석 환경 정보

- 사용 도구: Chainsaw
- 분석 일시: 2025년 8월 20일 오후 7시 49분
- 분석자: 정현지

분석을 위해 사용한 명령어

```
./chainsaw hunt evtx_attack_samples/ -s sigma/ --mapping
mappings/sigma-event-logs-all.yml –json >> ~/chsw_result.json
```

주요 분석 결과

제공된 JSON 파일 분석 결과, 다음과 같은 잠재적 위협 및 보안 이벤트들이 식별되었습니다.

[1] DSRM 계정 비밀번호 변경 (EventID 4794)

- 심각도: 높음(High)
- 탐지 이벤트: EventID 4794
- 발생 일시: 2017-06-09T19:21:26Z
- 관련 호스트: 2016dc.hqcorp.local
- 취약점 설명: DSRM(Directory Service Restore Mode) 계정은 도메인 컨트롤러 복구 등 비상 상황에 사용되는 특수 계정입니다. 이 계정의 비밀번호가 변경된 로그는 공격자가 시스템에 대한 영구적인 접근 권한을 확보하려는 시도일 수 있습니다. 이는 MITRE ATT&CK 전술인 **T1098 (계정 조작)**과 관련이 있습니다.
- 탐지 근거:
    - Source: EVTX-ATTACK-SAMPLES/Credential Access/4794_DSRM_password_change_t1098.evtx
    - EventRecordID: 3139859
    - 사용자: HQCORP₩administrator
- 영향: 공격자가 DSRM 계정의 비밀번호를 변경하여 도메인 컨트롤러에 대한 통제권을 획득하고, 시스템을 복구 불능 상태로 만들거나 추가적인 악성 행위를 수행할 수 있습니다.

[2] SID History 추가 (EventID 4765)

- 심각도: 중간(Medium)
- 탐지 이벤트: EventID 4765
- 발생 일시: 2017-06-12T23:39:43Z
- 관련 호스트: 2012r2srv.maincorp.local
- 취약점 설명: SID(Security Identifier) History는 계정 마이그레이션 시 기존 SID를 유지하기 위해 사용되지만, 공격자는 이를 이용해 낮은 권한의 계정에 높은 권한의 SID를 추가하여 권한을 상승시킬 수 있습니다. 이는 MITRE ATT&CK 전술인 **T1178 (SID History 추가)**과 관련이 있습니다.
- 탐지 근거:
    - Source: EVTX-ATTACK-SAMPLES/Lateral Movement/4765_sidhistory_add_t1178.evtx
    - EventRecordID: 19383
    - 사용자: MAINCORP₩Administrator가 Andrei 계정에 SID를 추가함.
- 영향: 일반 계정이 관리자 권한을 획득하여 시스템의 중요 자원에 접근하거나 횡적 이동(Lateral Movement)을 수행할 수 있습니다.

[3] Pass-the-Hash (PtH) 공격 의심 (EventID 4624)

- 심각도: 중간(Medium)
- 탐지 이벤트: EventID 4624
- 발생 일시: 2019-02-02T09:17:22Z
- 관련 호스트: ICORP-DC.internal.corp
- 취약점 설명: EventID 4624는 일반적으로 성공적인 로그온을 나타내지만, 이 로그는 NTLM 인증 패키지를 사용하는 LogonType: 3 (네트워크 로그온)과 함께 PtH (Pass-the-Hash) 공격과 연관된 패턴을 보입니다.
- 탐지 근거:
    - Source: EVTX-ATTACK-SAMPLES/Lateral Movement/Pass-the-Hash-4624_4688.evtx
    - EventRecordID: 10738
    - 사용자: EXCHANGE$ (컴퓨터 계정)
    - 로그온 유형: LogonType 3
    - 네트워크 주소: 192.168.111.87
- 영향: 공격자가 탈취한 해시 값을 사용하여 시스템에 로그온함으로써, 비밀번호를 모르더라도 시스템을 제어할 수 있는 권한을 얻게 됩니다.

[4] Windows 보안 로그 권한 열거 (EventID 4661)

- 심각도: 중간(Medium)
- 탐지 이벤트: EventID 4661
- 발생 일시: 2017-06-12T23:39:43Z
- 관련 호스트: 2012r2srv.maincorp.local
- 취약점 설명: EventID 4661은 객체에 대한 접근이 시도되었음을 나타냅니다. 이 로그는 공격자가 시스템의 보안 정책 또는 권한 설정에 대한 정보를 수집하려는 정찰(Discovery) 활동의 일부일 수 있습니다.
- 탐지 근거:
    - Source: EVTX-ATTACK-SAMPLES/Lateral Movement/4661-security_policy_enumeration.evtx
    - EventRecordID: 19383
    - 사용자: MAINCORP₩Administrator가 LSA Policy 및 DS Policy 관련 객체에 접근을 시도함.
- 영향: 공격자는 이 정보를 활용하여 권한 상승 또는 추가적인 공격 경로를 파악할 수 있습니다.

[5] 사용자 로그오프 이벤트 (EventID 4634)

- 심각도: 정보성(Info)
- 탐지 이벤트: EventID 4634
- 발생 일시: 2022-05-01T04:42:11.069064Z
- 관련 호스트: wind10.winlab.local
- 취약점 설명: 이 이벤트는 특정 사용자가 시스템에서 로그오프했음을 나타냅니다. 일반적으로 시스템의 정상적인 운영 과정에서 발생하는 로그이며, 그 자체로는 보안 위협으로 간주되지 않습니다. 그러나 특정 악성 행위(예: 특정 계정을 사용한 공격 후 흔적 제거)의 마지막 단계에서 발생할 수 있으므로, 다른 의심스러운 이벤트들과 함께 분석되어야 합니다.
- 탐지 근거:
    - Source: EVTX-ATTACK-SAMPLES/Lateral Movement/Pass-the-Hash-4624_4688.evtx
    - EventRecordID: 21375
    - 사용자: Administrator
    - Sigma Rule: user_logoff_event
- 영향: 단일 이벤트로는 직접적인 보안 위협이 아니지만, 이전에 발생한 의심스러운 로그인(EventID 4624)과 연결하여 공격자의 활동을 추적하는 데 중요한 단서로 활용될 수 있습니다.

권고 사항 및 개선 방안

발견된 각 취약점에 대한 구체적이고 실행 가능한 개선 방안을 다음과 같이 제시합니다.

[1] DSRM 계정 비밀번호 변경 (EventID 4794)

- 즉각 조치:
    - 2016dc.hqcorp.local의 DSRM 계정 비밀번호 변경이 사전에 승인된 작업이었는지 즉시 확인하십시오.
    - 만약 승인되지 않은 변경이었다면, 해당 계정을 비활성화하거나 비밀번호를 재설정하여 추가적인 악용을 방지해야 합니다.
    - administrator 계정의 활동 로그를 면밀히 분석하여 무단 접근이 있었는지 확인하십시오.
- 장기적 개선:
    - DSRM 계정의 사용은 긴급한 복구 상황으로 제한하고, 평상시에는 접근을 통제해야 합니다.
    - DSRM 계정 비밀번호 변경 이벤트(EventID 4794)에 대한 실시간 모니터링 및 경고 시스템을 구축하십시오.
    - Microsoft의 LAPS(Local Administrator Password Solution)와 같은 솔루션을 도입하여 관리자 계정의 비밀번호를 주기적으로 변경하고 관리해야 합니다.

[2] SID History 추가 (EventID 4765)

- 즉각 조치:
    - Andrei 계정에 추가된 SID History가 정상적인 마이그레이션 작업이었는지 확인하십시오.
    - 만약 비정상적인 SID 추가가 확인되면, 해당 계정의 SID History를 제거하고 비밀번호를 재설정하십시오.
- 장기적 개선:
    - 도메인 환경에서 SID History가 추가되는 이벤트(EventID 4765)에 대한 감사 및 모니터링을 강화하십시오.
    - sidhistory 속성이 포함된 계정에 대한 정기적인 감사를 수행하여 비정상적인 권한 상승 시도를 탐지해야 합니다.

[3] Pass-the-Hash (PtH) 공격 의심 (EventID 4624)

- 즉각 조치:
    - 192.168.111.87 IP 주소에서 ICORP-DC.internal.corp로의 로그온에 사용된 EXCHANGE$ 계정의 활동을 즉시 조사하십시오.

    - 이 로그온이 정상적인 행위인지 확인하고, 비정상적이라면 관련 컴퓨터 및 계정을 격리해야 합니다.
- 장기적 개선:
    - NTLM 인증 의존도를 줄이고, Kerberos 인증을 우선적으로 사용하도록 구성하십시오.
    - 시스템에 저장된 암호 해시를 보호하기 위해 Credential Guard와 같은 기술을 도입하십시오.
    - 특권 계정(administrator, EXCHANGE$)에 대한 비정상적인 네트워크 로그온(LogonType 3)을 탐지하는 모니터링 시스템을 구축하십시오.

[4] Windows 보안 로그 권한 열거 (EventID 4661)

- 즉각 조치:
    - MAINCORP₩Administrator 계정의 LSA Policy 및 DS Policy에 대한 접근 시도가 정상적인 관리 작업이었는지 확인하십시오.
- 장기적 개선:
    - 민감한 시스템 정책 객체에 대한 접근 감사 및 경고를 강화하여 공격자의 정찰 활동을 조기에 탐지해야 합니다.
    - 최소 권한 원칙(Principle of Least Privilege)을 적용하여 관리자 계정의 권한 남용을 최소화해야 합니다.

[5] 사용자 로그오프 이벤트 (EventID 4634)

- 즉각 조치:
    - EventID 4634 자체는 위협이 아니지만, 이전에 발생한 의심스러운 로그인 이벤트(EventID 4624)와 연관하여 사용자 활동을 추적하고, 공격자의 행적을 파악하는 데 활용하십시오.
- 장기적 개선:
    - SIEM(보안 정보 및 이벤트 관리) 시스템에서 로그인(EventID 4624)과 로그오프(EventID 4634) 이벤트를 상관 분석하여 비정상적인 사용자 세션 종료 패턴을 탐지하도록 구성하십시오.

일반 권고 사항

- 모든 시스템에 대한 최신 보안 패치를 신속하게 적용하십시오.
- 계정 보안을 강화하기 위해 **다단계 인증(MFA)**을 도입하고, 강력한 비밀번호 정책을 강제하십시오.
- 정기적인 취약점 분석 및 모의 해킹을 통해 시스템의 보안 취약점을 지속적으로 점검하고 개선해야 합니다.
- 보안 이벤트 로그를 중앙 집중식으로 수집하고, **자동화된 분석 및 대응 시스템(SOAR)**을 구축하여 위협 탐지 및 대응 효율성을 높이십시오.

결론

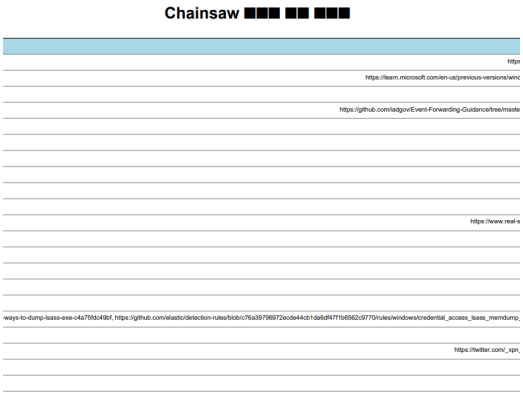
본 보고서는 Chainsaw 도구를 활용하여 Windows 보안 이벤트 로그 파일에 대한 분석을 수행하고, 잠재적인 위협 및 공격 활동을 식별한 결과를 담고 있습니다. 분석 결과, DSRM 계정 비밀번호 변경(EventID 4794)과 같은 심각한 수준의 위협부터 SID History 추가(EventID 4765), PtH 공격 의심(EventID 4624)과 같은 중간 수준의 위협에 이르기까지 총 4개의 주요 보안 이벤트가 탐지되었습니다.

이러한 결과는 현재 시스템에 알려진 공격 전술 및 기술(TTPs)을 활용한 침입 시도 또는 내부 위협의 가능성이 있음을 시사합니다. 따라서 보고서에서 제시된 권고 사항들을 즉각적으로 이행하여 잠재적 위협에 대한 방어력을 높이는 것이 매우 중요합니다.

향후에는 정기적인 보안 이벤트 로그 분석을 자동화하고, 탐지 규칙(Sigma Rule)을 지속적으로 업데이트하며, 시스템 전반에 걸친 보안 강화 대책을 마련함으로써 사이버 위협에 대한 방어 체계를 더욱 견고히 해야 할 것입니다.

실습을 진행하며

실습의 Chainsaw 도구 사용 과정에는 Chat GPT를 활용했습니다. 분석 결과 파일에 대한 분석은 OpenAI Chat GPT와 Google Gemini를 통해 진행했습니다. 보고서 작성은 Google Gemini를 이용했습니다. 실습으로 많은 것을 배울 수 있었습니다. 우선, AI의 결과물에 무조건적인 신뢰는 위험하다고 느꼈습니다. 인공지능은 간단한 파일 작성 시 뛰어난 결과물을 생성했습니다. 그러나 복잡한 과정에서는 큰 오류를 보였습니다.



첨부한 이미지는 제가 Chat GPT에 요청한 취약점 보고서 파일입니다. PDF로 파일 작성을 요청했더니 좌우 배열이 맞지 않는 결과물을 생성했습니다. 파일 형식에 맞는 작성은 물론 실습 과정에서도 많은 시행착오를 거쳤습니다. NAT 정책과 내부 스위치를 이용하여 외부 인터넷을 사용할 수 있다거나, 인코딩 오류로 글자가 깨진 csv 파일을 잘못된 방식으로 변환하도록 제안했습니다. 반복적으로 AI에게 질문하여 그 정보가 맞는지 확인해야 했습니다. AI는 제가 질문하기 전까지 취약점 결과물 파일이 확장자에 따라 다른 Field를 보여준다는 사실을 언급하지 않았습니다. (json: group, kind, document (내부에 kind, path, data 필드 포함), name, timestamp, authors, level, message, id, tags, rule, matches / csv: timestamp, detections, count, Event.System.Provider, Event ID, Record ID, Computer, Event Data) 저는 처음 chainsaw 도구를 설치할 때 악성 코드 알림을 확인했습니다. 당시 chainsaw 도구 안에 악성 코드가 있다고 생각했습니다. 실습을 진행하며 chainsaw README 파일에 적혀 있는 내용을 통해 안티바이러스 프로그램의 잘못된 감지로 인한

알림임을 깨달았습니다. 혹시 모를 취약점에 대비해 가상 컴퓨터 VM에서 리눅스 Cent OS 9에서 실습을 진행하려 했습니다. 새로 생성된 VM에서는 chainsaw가 탐지할 만한 로그가 불충분했습니다. 또한 Chat GPT가 언급하기를 chainsaw는 기본적으로 EVTX 파일만 인식합니다. 때문에 Cent OS 9의 텍스트 기반 로그로는 정상적으로 분석이 진행되지 않았습니다. AI는 편리한 도구는 맞지만, 사용자의 사용 방식이나 이해도에 따라 천차만별의 결과물을 보였습니다. 취약점 분석을 처음 진행하는 저로서는 AI에게 올바른 질문을 하는 것이 난관이었습니다.

다음으로는 취약점 분석이 굉장히 어렵다는 것을 체감했습니다. 어떤 규칙을 사용하는지에 따라, 어떤 폴더를 검사할 것인지 설정하는 것에 예상외로 많은 시간을 소모했습니다. 이벤트 로그 형식에 따라 다른 취약점 분석 도구를 사용해야 하는 것도 겨우 익혔습니다. AI가 생성한 취약점에 대한 설명을 보면서도, 아직 위험도에 대한 이해가 완전히 되지 않았습니다. 더 이해하기 위해선 취약점 분석 결과물보다도 우선 OS 같은 기본 환경 시스템이나, 다양한 해킹 사례에 대한 지식이 필요하다고 느꼈습니다. 예상보다 많은 시간이 소요되었지만 유익한 실습이었습니다.

실시간 실습 과정 기록: https://jhjcloud9.blogspot.com/2025/08/chainsaw.html