CLI 검색을 사용하여 대량의 데이터를 내보내는 방법.

적용 가능성

Splunk Enterprise

설명

단계별 가이드

대량의 데이터를 내보내려면 검색 헤드의 CLI 프롬프트에서 다음 라인을 따라 검색을 사용할 수 있습니다.

```
splunk search "index=pan_log sourcetype=pan:* src_ip!=<Internal_IP_Scheme> dest_ip!=<Int
| fillnull value=null
| dump basefilename=<insert_your_chosenfilename> compress=5 fields=_time,app,app:subcate
dest_ip,dest_port,dest_translated_ip,dest_user,dest_zone,direction,duration,filename,htt
packets_out,sig,signature,sourcetype,src_ip,src_translated_ip,src_user,target_id,threat:
```

위 검색의 세부 사항은 다음과 같습니다.

'pan_log' 인덱스에서 pan:* sourcetype을 검색하고 null을 채울 수 있는 IP 범위를 제외하며, 다음 작업을 진행하는 dump 명령으로 파이프합니다.

이 명령은 지정된 검색 쿼리를 실행하고 검색 결과를 로컬 디스크로 "$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump"에서 내보냅니다. 입력 이벤트의 특수 필드 _dstpath를 인식하며, 이 필드가 설정된 경우 최종 대상 경로를 계산하기 위해 dst에 추가될 경로로 사용됩니다.

이 프로세스의 한 가지 주요 단점은 결과의 TTL이 2분이라는 것입니다. 따라서 프로세스에서 생성한 *.gz 파일을 가져오기 전에 이러한 결과가 생성되지 않도록 저장 토큰 파일을 생성해야 합니다. 아래의 "관련" 링크를 참조하십시오.

참조:

Windows에서 확장자가 없는 파일을 만드는 방법

조사

이 문제를 조사하는 동안 전체 데이터 세트를 가져오지 않는 문제가 발견되었습니다.

검색 결과로 인해 이 데이터가 수집되었으며 예상보다 빨리 수집되었다고 판단했습니다. 조사 결과 이것은 정상적인 행동으로 확인되었습니다. 요약 인덱스 검색 및 다른 검색은 2분 검색 아티팩트 TTL로 실행할 수 있습니다. 따라서 <sid> 디렉터리에 토큰 저장 파일을 만듭니다. 이 문서의 설명 섹션에 있는 링크에서 Windows 시스템에 대해 설명합니다. *nix를 사용하면 $SPLUNK_HOME/var/run/splunk/dispatch/<sid>로 이동한 다음 'touch save' 명령을 실행합니다.

일단 달성한 아티팩트 복구 문제를 우회할 수 있습니다 [***저장 파일을 삭제하는 것을 잊지 마십시오!***]

그런 다음 좀 더 많은 트러블슈팅을 눌러 정의된 전체 데이터 집합을 생성할 작업 가능한 시간을 확보합니다. 24시간 검색을 실행하여 매일 내보내기를 완료해야 했습니다. 데이터 집합의 이벤트 수가 너무 많기 때문입니다.

해결

24시간 동안 실행되어야 하는 데이터 세트를 좁히면 24시간 PAN 로깅 범위의 전체 덤프를 생성할 수 있습니다. 또 다른 TSE는 이 방법을 최근에 사용하여 과거로 돌아가 구체적인 정보를 수집할 수 있었습니다.

관련 링크

Splunk 설명서: 덤프 명령 설명서: 검색 참조 덤프

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.