데이터시트

Vigil 비즐

보안 포렌식을 위한 장기간 패킷 저장

보안 침해 포렌식 어플라이언스 솔루션 새비어스 비즐(Vigil)

정보 보안 분야에서 새비어스 비즐(Savvius Vigil)은 침입 탐지 시스템과 연동하여 보안 사건에 대한 대응 능력을 획기적으로 향상시킵니다.

보안 침해 포렌식이 필요한 이유는 보안 침해는 피할 수 없고 그 손실이 크기 때문입니다. 최근 미국 내 보안 트렌드 보고서에 따르면, 피해자의 33%가 보안 침해 사실을 내부적으로 발견하였고 피해자의 67%는 외부의 제3자에 의하여 보안 침해 사실을 알게 되었습니다.
탐지 후 사이버 공격을 해결하는 평균 시간은 27일이고, 해커가 탐지되기 전 네트워크에 접근하는 기간은 229일이며, 매주 기업별 성공하는 보안 공격 사건은 1.4개이고, 매년 기업별 보안 침해에 관하여 드는 평균 비용은 85억원입니다. 마치 사이버 보안이 운영되고 있지 않은 것처럼 보이게 하는 수치입니다. 또한 미국 내 대형 유통 기업인 타겟의 4천만 명의 고객 신용카드와 현금(직불) 카드 정보 유출 사건은 이로 인하여 11% 이상 이 기업의 주가가 폭락하고 법정 소송에서 100억원 이상의 피해 보상금을 지불하게 되었고, 이 사례를 통하여 보안 침해에 대한 대응 지연 시 그 손실이 매우 크다는 것을 알 수 있습니다.

SIEM/IDS/IPS 솔루션과의 연동

새비어스 비즐은 보안 이벤트와 패킷을 동시에 수집하지만, 보안 이벤트의 발생 전과 후의 내용과 관련되는 IP 주소에 해당되는 패킷들만 지능적으로 선별하여 저장 보관합니다. 그리고 중요한 특정 IP 주소들의 모든 트래픽을 추가적으로 저장하도록 설정할 수도 있습니다.

보안 침해 포렌식을 위한 장기간의 패킷 보관 및 분석 솔루션

문제

보안 조사에 있어서 네트워크의 패킷은 매우 중요합니다. 패킷들은 공격을 위한 운송 수단이기 때문입니다.
그렇지만 일반적으로 보안 침해와 그것을 발견하기까지 오랜 시간이 걸린다는 것은 대부분의 보안 조사관들이 네트워크의 패킷에 접근하지 않고 업무를 진행해야 했었다는 것을 의미합니다. 새비어스 비즐(Savvius Vigil)이 있기 전에는 패킷을 전수 저장해야 하는 과도한 투자 만이 장기간의 네트워크 패킷을 저장 할 수 있는 방법이었습니다.

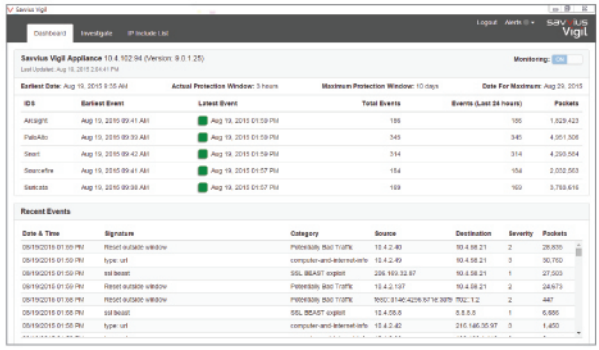
솔루션

새비어스 비즐 (Savvius Vigil)은 지능적이며 자동적으로 보안 조사에 있어서 유용한 패킷들이 무엇인지 결정하여 수개월 간의 패킷들을 저장하는 합리적인 동작을 합니다.

직관적인 인터페이스는 각 이벤트에 관련된, 저장된 패킷과 데이터에 직접 또는 고급 분석 과정을 통하여 빠르게 접근할 수 있도록 합니다.
보안 이슈 발생 전 효과적인 보안 조사를 위해 매우 중대한 정보를 기록 보관함으로써 MTTR(평균 해결 시간)과 보안 사건의 위험성을 감소시킵니다.

비즐과 통합 운영이 가능한 SIEM/IDS/IPS 솔루션 제품은

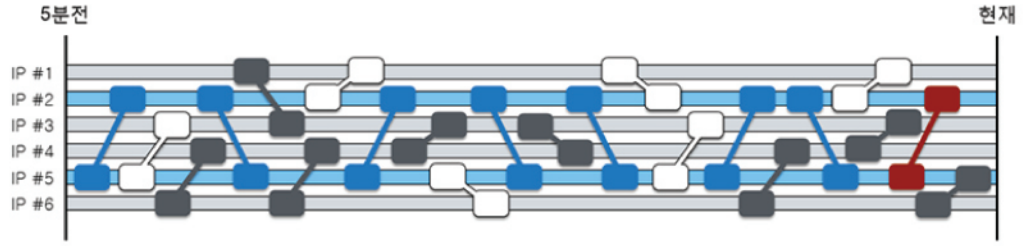
HP ArcSight, Cisco FireSight, Snort, Suricata 등이며 연동 제품이 계속 추가 되고 있습니다.
연동에 관한 협력은 항상 열려 있으며 새비어스한국지사로 문의하시면 됩니다.



보안 포렌식을 위한 장기간 패킷 저장

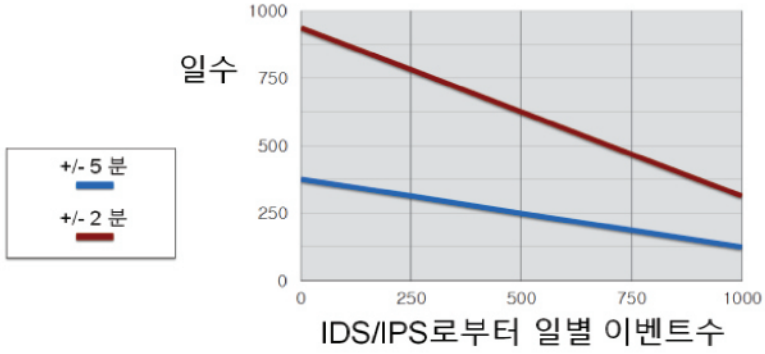
비즐의 동작 방법

새비어스 비즐 (Savvius Vigil)은 기존의 보안 정보 및 이벤트 관리 솔루션(SIEM)의 침입 탐지 시스템/침입 방지 시스템 (IDS/IPS) 기능들과 연동하여 보안 이벤트가 발생할 때만 네트워크 패킷들을 저장합니다. 보안 이벤트와 관련된 IP주소의 대화 내용에 해당되는 모든 패킷을 저장하며, 다수의 소스들로부터 발생한 이벤트들을 통합하여 운영합니다. 관련된 노드들 간의 트래픽은 이벤트 발생 전과 후 기간에 대해 캡처됩니다. 선택적으로 이벤트 내용의 IP주소에 의해 송신 및 수신된 모든 관련된 트래픽도 추가로 캡처 할 수 있습니다.



비즐은 모든 네트워크 트래픽을 버퍼링하고 있습니다.

1단계 IDS 이벤트가 들어오면 두 IP에 대해서 알람을 줍니다.
2단계 이들 IP주소의 전/후 최대 5분간의 모든 패킷들을 저장합니다.
3단계 선택적으로 이들 IP중에서 한 개라도 연관이 있는 IP의 패킷들도 저장 할 수 있습니다.
4단계 이들 두 패킷과 관련이 없는 패킷들은 무시됩니다.



날짜 범위, 이벤트 경고 수준, IP 주소 등으로 이벤트를 구분하여 선택하고, 이벤트 발생 전후 시간과 대화의 관련된 다른 IP 주소의 패킷을 포함할지 설정하며, 표준 패킷 파일로 저장하여 옴니피크(OmniPeek) 또는 타사의 패킷 뷰어를 이용하여 패킷을 분석합니다

새비어스 비즐은 이런 상황에 필요합니다.

보호할 자산이 있다.
예를 들어 금융 정보, 환자 기록 등과 같은 데이터가 곧 비즈니스 자산인 경우 네트워크 포렌식 솔루션의 운용이 필요합니다.

주변 보안이 완벽하지 않다.
다양한 형태와 크기의 모든 조직에 지금 즉시 공격이 침투될 가능성이 있는 경우입니다.

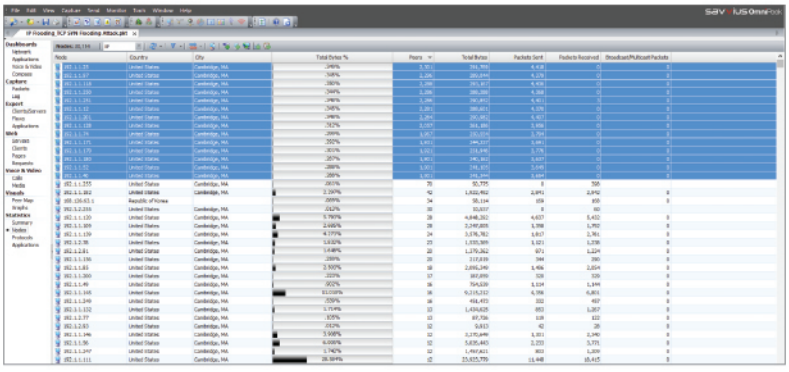
일부 보안 사건들은 즉시 발견되지 않는다.
평균적으로 데이터 침해는 발생 후 6개월 이상 지나서 발견됩니다. 장기간 패킷 저장은 이러한 침해 사고 발생에 대해 증거 취득이 가능하도록 합니다.

보안 조사를 위해서 네트워크 패킷은 중요한 가치를 갖습니다.
로그, 이벤트 및 기타 메타데이터 등은 보안 조사에 한계성이 있습니다. 패킷 레벨의 조사를 통해서만이 근본 원인과 파생 문제를 확인 할 수 있습니다.

수 개월 간의 네트워크 트래픽을 저장하는 것은 실현하기 어렵습니다.
초고속 네트워크에서 한 달에 페타바이트의 데이터를 발생시킵니다. 보안 솔루션과 연동하여 선별적으로 패킷을 저장하는 비즐만이 수개월치의 유용한 패킷을 저장 할 수 있습니다.

옴니피크(OmniPeek)를 이용한 보안 공격 및 침해에 대한 행위 분석

비정상 과다 TCP/UDP 세션이 발생된 IP Pair 및 비정상 과다 IP 커넥션이 발생된 호스트 IP를 확인하여, 각 IP Pair별 발생된 TCP/UDP 총 세션 수와 각 세션 내용을 감시/확인하고, 각 IP별 IP 커넥션(Peers) 수를 확인하여, 특정 IP Pair에서 발생되는 포트 스캔 증상과 특정 IP에서 유발하는 IP 스캔 행위를 발견하여 조치할 수 있습니다.



DDoS, 비정상적 포트스캔, IP스캔, TCP SYN Flooding, IP Flooding, MAC Flooding 등과 같은 보안 침해 행위를 정밀 진단하고, 그 원인이 되는 소스 IP 또는 MAC 주소를 확인할 수 있습니다.

"...유용한 네트워크 패킷 만을 자동적으로 저장함으로써, 새비어스 비즐은 보안 분석 담당자가 새롭게 발견되는 위협에 대해 빠르게 이해하고 대응할 수 있도록 그 능력을 강화시킵니다.
즉, 침해 경고의 이벤트 발생 이후 분석을 완료하기까지의 시간을 훨씬 빠르게 단축시킵니다."

- 키트론 이반스(Keatron Evans), 대표이사(Principal),Blink Digital Security -

하드웨어

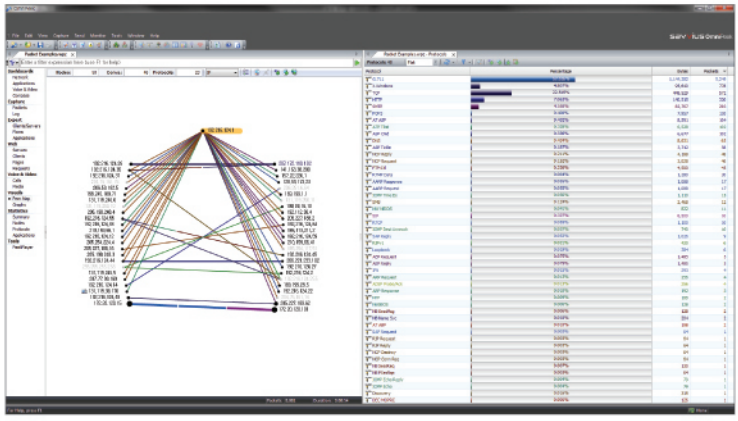
- 64TB HDD
- 선택 사항: 64TB 확장 스토리지 추가
- RAID 6 구성
- 4 Port 1/10G 네트워크 어댑터
- 3U rack mountable

소프트웨어

- 다수의 어플라이언스를 이용하여 모니터링하고 보안 포렌식을 수행하는 새비어스 비즐 소프트웨어
- 개요 보기, 스토리지 이용 상태, 이벤트 관리 등을 지원하는 모니터링 대시보드
- 날짜, 이벤트, IP주소, 경고 수준 및 기타 등의 조건으로 복합적인 검색이 가능한 보안 포렌식 기능

보안 포렌식을 위한 장기간 패킷 저장

의심스러운 특정 IP가 보안 침해를 위해 인가 받지 않은 다양한 서버에 접속하는 행위를 시각적인 IP/MAC 주소 커넥션 (피어맵) 화면으로 쉽게 확인하며 어떤 종류의 어플리케이션 데이터 서비스를 하는 서버에 접근했는지 서버의 도메인 이름으로 쉽게 확인하고 데이터의 불법 다운로드의 용량이 많은 서버와 이름을 즉시 확인할 수 있습니다.



사용자별 인터넷 행위를 추적하고 과거 행위를 정확하게 파악하기 위하여, 요청구문, 인터넷서버 도메인이름, URI, 사용자 URL(Referer), 응답코드, 데이터(파일) 형식과 내용 등을 파악하여, 사용자별 시간에 따른 인터넷 접속 흔적을 모두 추적하고 송수신했던 파일과 데이터 내용을 재현/재생하여 인터넷 행위를 정확하게 확인할 수 있습니다.

옴니피크® 네트워크 분석 소프트웨어

비즐에 접속 할 수 있는 콘솔기능을 가진 소프트웨어로서 옴니피크는 직관적이고 사용하기 쉬운 사용자 인터페이스를 제공하고 있습니다. 또한 Expert(전문가) 분석은 엔지니어가 관리하고 있는 네트워크에 대해 신속하고 정확하게 트러블 슈팅 할 수 있게 도와 줍니다. 네트워크 엔지니어는 옴니피크의 직관적인 UI와 top-down 메뉴를 이용해 네트워크에 대한 상태, 어플리케이션 판별, 다양한 네트워크 세그먼트에 대한 장애 분석 그리고 아주 작은 문제까지도 정확하게 찾아낼 수 있습니다.

새비어스(Savvius) 기업 정보

패킷 수준의 네트워크 분석 기반의 네트워크 성능과 보안 포렌식 솔루션을 개발하고 선도하는 새비어스(Savvius, Inc.) 기업은 네트워크 및 보안 전문가들이 네트워크 성능과 보안에 관한 문제들을 확인하고 빠르게 이해하며 대응할 수 있도록 그 능력을 강화시켜 드립니다. 이전에 와일드패킷(WildPackets)이었던 새비어스(Savvius)는 60개국 이상과 모든 산업 분야에서 제품들을 판매하였습니다. 고객사는 애플(Apple), 보잉(Boeing), 시스코(Cisco), 도이치 텔레콤(Deutsche Telecom), 피델리티(Fidelity), 마이크로소프트(Microsoft), 네이션와이드(Nationwide) 등을 포함하여, 포천(Fortune) 1000의 높은 비율의 고객을 가지고 있습니다. 새비어스(Savvius)는 시스코(Cisco) 솔루션 파트너입니다.

더욱 자세한 내용에 대해서는 www.savvius.com 웹사이트를 방문해 주십시오.

savvius
새비어스 코리아
Tel: 070 8257 0458
Mail: korea@savvius.com
www.savvius.com

VIGIL 데모 신청을 하세요!

Copyright© 2015 Savvius, Inc. All rights reserved. OmniPeek and Omnipliance are registered trademarks and Savvius, the Savvius logo are trademarks of Savvius, Inc. All other product names and trademarks are the property of their respective companies

VIGIL-20150820-KO