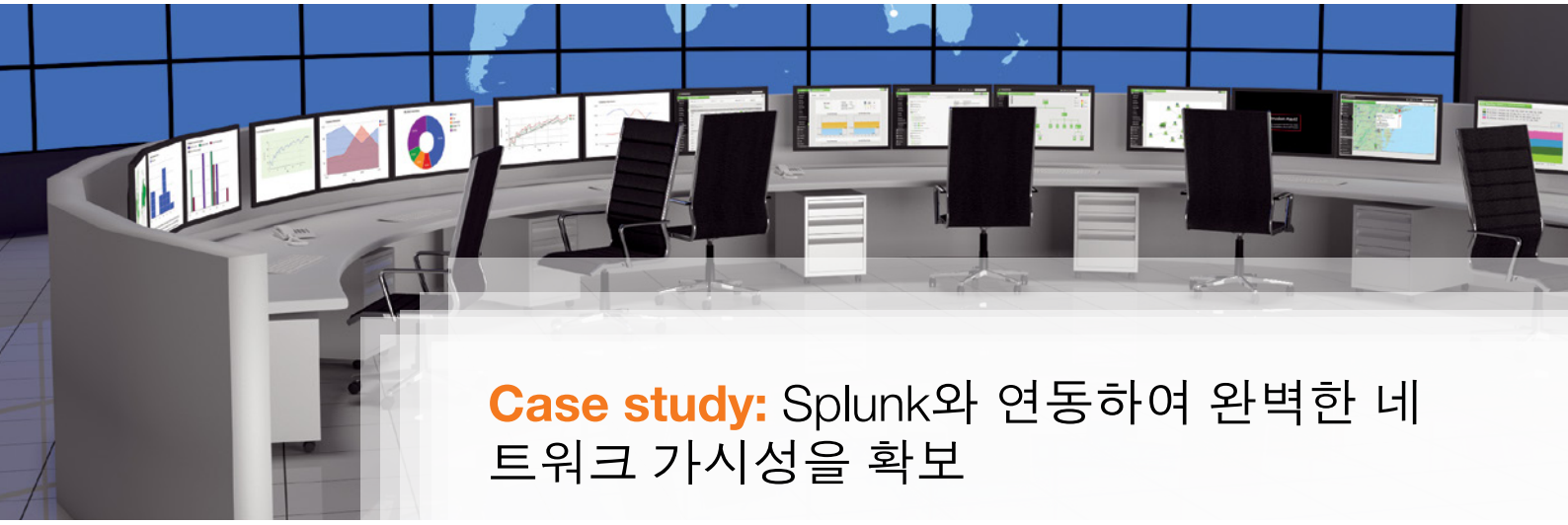
napatech



Case study: Splunk와 연동하여 완벽한 네트워크 가시성을 확보

Splunk 소개

Splunk는 머신 데이터 처리를 위한 업계 최고의 소프트웨어 플랫폼으로, 실시간 운영 인텔리전스를 제공합니다. Splunk는 IT에서 발생하는 빅데이터의 방대한 스트림 관리에 있어서 어려움을 해결하고 비즈니스 기회를 창출하는 데 중점을 두고 있습니다.

Challenge: 수십억 개의 로그 관리

시장에 출시된 다양한 이벤트 관리 시스템 중 하나인 Splunk는 여러 산업에서 기업 인프라 내의 보안, 네트워크, 서버에서 데이터 수집 등에 활용되고 있습니다. 네트워크 보안 및 성능에 요구되는 통찰력을 제공하기 위해서는 Splunk에 기록된 모든 비정상적인 활동을 우선적으로 분석해야할 필요가 있습니다.

이 작업은 일반적으로 보안 및 네트워크 운영 센터(SOC 및 NOC)에서 관리되는데, 수십억 개의 로그에서 우선 순위가 높고 대응이 가능한 이벤트 데이터를 압축해야 합니다. Splunk가 상당한 양의 이벤트 데이터를 수집하기는 하지만, 네트워크에서 송수신되는 데이터에 대한 기록 전체를 제공하지는 않습니다. SOC 및 NOC는 의심스러운 모든 이벤트를 확인하고 해결할 방법이 필요합니다.

"부정확하고 오류가 있는 인텔리전스를 분석하는 데 낭비되는 평균 시간 비용이 연간 127만 달러에 이릅니다."

Ponemon Institute Survey

Solution: Splunk/Pandion 연동

Napatech Pandion이 도와드릴 수 있는 부분은 바로 다음과 같은 점입니다. Pandion은 Splunk 이벤트 또는 기타 비정상적인 행위를 포착할 수 있는 전체 패킷 캡처를 제공합니다. 모든 데이터가 디스크에 저장되므로 운영 센터 직원은 상세한 조사를 위해 데이터를 사용할 수 있습니다.

Case 1

첫 번째 사례 연구에서는 금융 서비스 회사에 근무하는 SOC 보안 엔지니어가 Suricata에서 송신된 Splunk 이벤트에 기록된 의심스러운 도메인을 조사하는 경우를 소개합니다.

Challenge

Splunk가 상당한 양의 데이터를 수집하기는 하지만, 네트워크에서 송수신되는 데이터의 전체 기록을 제공하지는 않습니다. 따라서 보안 및 네트워크 운영 센터에는 의심스럽게 보이는 모든 이벤트를 조사할 수 있는 기능이 필요합니다.

Solution

Splunk/Pandion 연동을 통해 모든 것이 디스크에 기록되고 저장되므로, 데이터에 바로 액세스하여 상세히 조사할 수 있습니다.

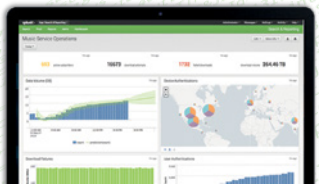
Benefits

업계 최고의 검색 속도 덕분에, Pandion은 단 몇 초 만에 통찰력을 제공하므로, Splunk 사용자는 이벤트 전체 내용을 파악하고 문제를 해결할 수 있습니다. Pandion은 기존 Splunk 솔루션과 매끄럽게 연동될 수 있으므로, 기업에서는 과거의 투자를 활용하고 비용을 절약할 수 있습니다.

DN-1038 개정 버전. 1-KO

napatech
pandion

Splunk



방화벽에 리졸빙된 주소에 대한 연결 시도가 있었음을 나타내는 이벤트가 기록되었습니다. 이 이벤트를 자세히 조사하기 위해, SOC 엔지니어는 Splunk에서 해당 이벤트를 클릭하고, Pandion 워크플로를 사용하여, 단 몇 초 만에 네임레졸루션 및 이후 해당 연결에 대응한 전체 패킷 레코드를 볼 수 있습니다.

이 정보가 없다면 이벤트를 보고할지 무시할지의 결정을 추측을 바탕으로 내릴 수 밖에 없습니다. SOC 엔지니어는 패킷 데이터를 분석하여 의심스러운 주소로 송수신된 것이 무엇인지, 해로운 문서가 다운로드 되었는지, 인프라에서 실제로 유출된 정보가 있는지 정확하게 확인할 수 있습니다. 따라서 추측이나 불완전한 정보에 의존하지 않고 Splunk 이벤트에 대한 심각도와 영향을 확인할 수 있습니다.

Case 2

두 번째 사례 연구에서는 소셜 미디어 에이전시에 근무하는 NOC 애널리스트가 Splunk에서 응답지연/응답없음으로 뜬 애플리케이션 경고를 보고 문제가 되는 정확한 영역을 식별해야 하는 경우를 소개합니다. 이러한 조사는 시간 소모가 많고 복잡한 작업입니다. 하지만 Pandion/Splunk 연동을 통해 NOC 애널리스트는 이벤트를 클릭하고, 패킷을 검색하는 것만으로 네트워크, 서버, 데이터베이스 등 어느 인프라 영역에 문제가 있을지 빠르게 확인할 수 있습니다. 불가피하게, 각 영역의 담당자들은 담당하고 있는 도메인만 감시하고 있기 때문에, "아무 문제가 없다"고 주장하기 쉽습니다. 하지만 이 솔루션을 이용하면, 원형 그대로의 패킷 데이터를 확인하여 조직의 어느 부분에서 최종적으로 이벤트를 처리해야 하고 근본 원인 분석을 해야 하는지 보여줍니다.

Case 3

세 번째 사례 연구에서는 주요 방위산업체에 근무하는 인시던트 조사 담당자가 네트워크 보안 장치에서 의심스러운 SSL 트래픽을 나타내는 경고를 Splunk로 보낸 것을 발견하는 경우를 소개합니다. 이 경우, 서버는 "하트블리드(heartbleed) 버그"에 취약할 가능성이 있습니다. 여기서 취약성이란 서버 메모리에 저장된 사용자 아이디와 비밀번호와 같은 정보가 암호화되지 않고 평문의 형태로 최근 웹 트랜잭션에서 전송되었을 수 있음을 의미합니다. 인시던트 조사 담당자는 Splunk에서 이벤트를 클릭하고 패킷을 분석하여 곧바로 다음과 같은 판단을 할 수 있습니다.

1. 버그가 악의적으로 제3자에 의해 이용되었는지
2. 취약점으로 인해 실제로 누출된 정보는 무엇인지

"한 조직이 한 주에 평균 17,000개의 맬웨어 경고를 받을 수 있습니다. 이러한 경고에 대응하는 시간은 조직의 재무 리소스와 IT 보안 담당자에게 심각한 부담입니다."

Ponemon Institute Survey

Benefits

설명드린 바와 같이, Pandion은 간편한 워크플로를 제공합니다. Splunk에서 이벤트를 클릭하면 사용자가 Splunk 이벤트에 해당되는 네트워크 패킷 정보 전체를 즉시 확인할 수 있습니다. 업계 최고의 검색 속도 덕분에, Pandion은 단 몇 초 만에 결과를 제공하므로, Splunk 사용자는 이벤트 전체 내용을 파악하고 문제를 해결할 수 있습니다.

Pandion은 기존 Splunk 솔루션과 매끄럽게 연동될 수 있으므로, 기업에서는 과거의 투자를 활용하고 실질적인 비용을 절약할 수 있습니다.

추가적인 사례 연구는 다음을 참조하십시오.
www.napatech.com/resources/case-studies

유럽, 중동 및 아프리카
Napatech A/S
덴마크, 코펜하겐

전화: +45 4596 1500
info@napatech.com
www.napatech.com

북미
Napatech Inc.
매사추세츠, 보스턴
캘리포니아, 마운틴 뷰
워싱턴 D.C.

전화: +1 888 318 8288
info@napatech.com
www.napatech.com

아시아태평양
Napatech China/South Asia
타이완, 타이베이
전화: +886 2 28164533 Ext. 319

Napatech Japan K.K.
일본, 도쿄
전화: +81 3 5326 3374

Napatech Korea
서울
전화: 02 6001 3545

ntapacsales@napatech.com
www.napatech.com