내부 시스템 이용 내역 가시화로 정보유출 위험에 대한 즉각적인 대응체계 구축

eyeCloudXOAR 기반 이상징후 분석 시스템 도입사례

"

이상징후 탐지 시나리오를 도출하여 여러 이벤트를 설정하고, 사용자 별로 발생한 이벤트 내역이 가시화 되어 이상징후 발생 시 신속한 원인 규명이 가능해 졌습니다. 도입 후, 정보 유출 방지를 위한 대책이 보완되어 보다 안심이 되는 바이며 내부 정보 유출 방지를 포함한 전사적 보안 관리를 All-in-One으로 구축하려는 기업이 있다면 eyeCloudXOAR를 도입을 적극 추천합니다.

- 매그나칩반도체 보안 담당자

고객사

매그나칩반도체 (Magnachip Semiconductor)

프로젝트 기간
2021년 9월 ~2021년 12월

도입 솔루션
eyeCloudXOAR v4.0

매그나칩반도체는

매그나칩반도체(이하, 매그나칩)는 통신, IoT, 가전, 산업, 자동차 등의 애플리케이션에 탑재되는 아날로그 및 혼성신호 반도체를 설계·생산하는 기업입니다. 매그나칩은 엔지니어링, 설계 및 제조 공정 영역에서 고도의 기술력을 가진 업체로 국내 반도체 산업을 이끌고 있는 기업 중 하나이며, 국내 최초로 뉴욕증권거래소에 직상장한 기업이기도 합니다.

매그나칩은 전자제품의 성능을 더욱 향상시키면서도 크기는 더 작게 하고 소비전력을 더 낮출 수 있는 등의 제품으로 다양한 기술을 갖추고 있으며, 약 1,150건의 특허를 보유 또는 출원 중입니다. 이렇게 다양하고 독자적인 기술을 갖추고 있는 만큼 정보 유출에 대한 민감도가 특별히 높아 정보유출 방지를 위한 보안 대책에도 많은 투자를 지속하고 있습니다.

데이터 통합 관리 + 다양한 내부위협 탐지 시나리오 필요

매그나칩은 다양한 형태의 기술 유출 위험에 대해 다각적인 탐지 및 분석이 가능한 시스템이 필요하였고 각각의 보안시스템들의 데이터 통합 관리 및 모니터링이 가능한 시스템을 찾고 있었습니다. 특히 보안시스템과 내부 업무시스템간의 상관 분석을 포함한 다양한 이벤트 설정 및 탐지 기능이 필수 요소였습니다.

매그나칩 내에서 검토한 보안 시나리오 외에도 솔루션 제안사가 정보유출이 일어날 수 있는 다양한 시나리오를 도출하여 지원해 주었으면 하는 요건이 있었고 향후 연동 대상 시스템이 추가될 경우에도 장비 연동이 수월하고 관리방안에 대한 지원도 보장되어야 했습니다.

다양한 위협 요소 탐지 및 관리 기능에 대규모 IT환경 구축 실적을 다수 보유한 eyeCloudXOAR 선택

매그나칩은 앞서 언급한 다양한 위협 요소 관리 기능 외에도 대규모 IT환경 도입 및 운용이 원활한 시스템을 찾고 있었습니다. 특히 일일 수십GB의 로그 수집이 가능한 성능에 1년 이상의 로그 보관 및 검색이 가능하여야 했습니다.

제안 요청에 응한 여러 보안 관련 업체의 제품을 검토하여 대부분의 기능 요건을 충족하면서도 대규모 IT환경 구축 실적을 다수 보유한 시큐레이어의 eyeCloudXOAR를 후보로 꼽았으며, 시큐레이어 담당자의 프레젠테이션을 통해 최종적으로 해당 제품을 선택하게 되었습니다.

모든 시스템의 데이터 및 작업 행위에 대해 해당 사용자 식별

기본적으로, 수집되는 로그와 인사 관련 정보를 연관 분석하여 모든 데이터의 사용자를 식별하도록 하였습니다. 여러 서버 장비, 엔드포인트, 휴대용 저장매체, 내/외부망 네트워크로 송수신되는 모든 데이터에 대해 사용자 기반으로 검색할 수 있도록 하였으며 각 사용자의 사용내역에 대한 통계를 시각화함으로써 보안사고에 철저히 대비할 수 있는 기반을 마련하였습니다.

업무서버에 있는 내외부 직원 정보에 대한 사용자정의 태깅으로 빠짐없는 모니터링을 가능하게 하여 이상징후나 사고 발생시 관련 사용자를 바로 검색할 수 있게 한 것입니다.

업무 분석과 협의를 통한 이상행위 탐지 시나리오 도출

내부 정보 유출이 일어날 수 있는 케이스는 너무나 다양하고 교묘한 수법도 존재하기 때문에 시큐레이어 담당자와의 협의를 통해 각각의 시나리오를 도출하였습니다.

예를 들어, 파일서버나 특정 저장매체를 과다 사용하거나, 중요파일에 접근한 후 네트워크전송이 일어나는 경우, 일과 시간 외에 과도하게 송수신하는 경우나 매체 저장하는 경우 등등 다양한 패턴이 있을 수 있습니다. 이러한 배경에 따라 우선 과다사용, 비인가접근, 통제우회, 데이터 저장/전송 등 발생 가능한 사고를 몇가지 범주로 나누어 정립한 다음 각각의 시나리오를 구체화 하는 방향으로 진행하였습니다.

다양한 이벤트 설정 기능과 매우 세부적인 탐지패턴을 설정할 수 있는 SeQL

eyeCloudXOAR는 다양한 위협 요소에 대응할 수 있도록 매우 정교하고 다양한 패턴의 이벤트 설정이 가능합니다. 특히, 시큐레이어에서 개발한 자체 쿼리언어 SeQL은 도출한 여러 탐지 시나리오를 거의 모두 설정 가능 할 만큼 정교한 언어입니다. 설정 과정에서 시큐레이어 담당 엔지니어가 SeQL 설정을 하나하나 지원해 주어 큰 도움이 되었습니다.

이렇게 설정된 각각의 탐지 시나리오를 이벤트로 등록하여 해당 이벤트가 탐지될 시 사용자 정보를 바로 식별할 수 있도록 구현하였습니다. 또한 전용 대시보드 기능으로 특정 사용자 기준으로 발생한 이벤트를 한번에 확인할 수 있게 하였습니다. 이로써 발생 가능한 여러 위협 시나리오에 대한 이벤트를 모두 탐지할 수 있게 되었으며, 시나리오 도출 작업에 있어서도 시큐레이어 담당자의 지원이 큰 도움이 되었습니다

다양한 이벤트 설정 기능과 매우 세부적인 탐지패턴을 설정할 수 있는 SeQL

이상징후 탐지 시스템 도입 완료 후, 내부 보안 시스템에서 발생되는 다양한 이벤트를 상관분석하여 즉각적으로 위협 대상을 식별하고 대응 할 수 있게 되었습니다. 사용자 별로 발생한 이벤트 내역이 가시화 되어 정보유출과 관련된 이상징후 발생 시 신속한 원인 규명이 가능해 졌으며, 도입한 시스템을 사내에도 주의환기 하였습니다.

도입 후 운영해 보니 정보 유출 방지를 위한 대책이 보완되어 보다 안심이 되는 바입니다. 내부 정보 유출 방지를 포함한 전사적 보안 관리를 All-in-One으로 구축하려는 기업이 있다면 eyeCloudXOAR를 도입을 적극 추천합니다.

- 매그나칩반도체 보안 담당자

Magnachip

(주)시큐레이어
☎ 1800-6713
contact@seculayer.com