TEIREN CLOUD SIEM

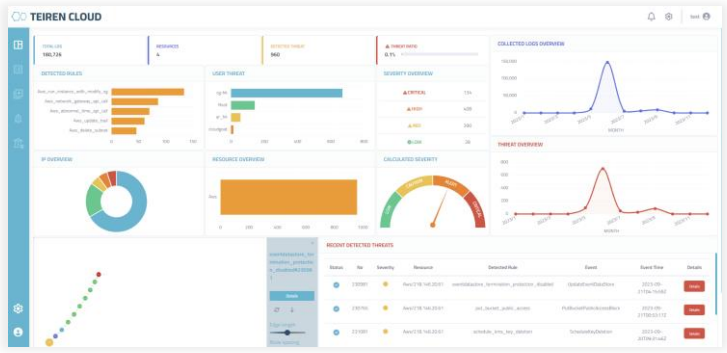
보이지 않는 공격을 본다

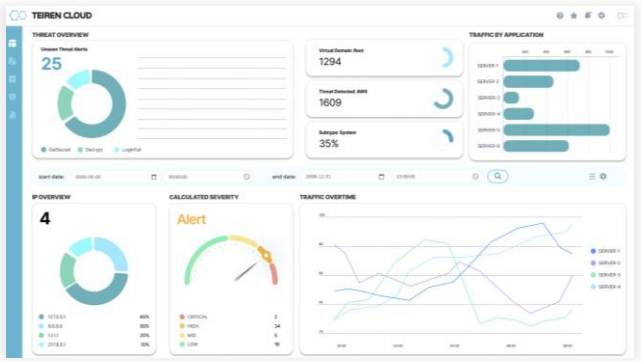
Teiren

01
About SIEM
SIEM 소개

About SIEM

SIEM이란?





SIEM이란, Security Information & Event Management (정보보안 이벤트 관리) 의 약자로, 기업 자산에 대한 *로그들을 모두 수집하고 통합해주는 솔루션입니다.

클라우드 리소스, 애플리케이션, 외부 위협 요소 등 다양한 영역에서 위협을 탐지하는 것이 가능하며, SIEM이 위협, 취약점, 공격 또는 의심스러운 행동이라 판단되는 부분이 발생하면 이에 대한 보고를 통해 즉각적인 대응이 가능하도록 합니다. 즉, SIEM은 다양한 영역에서 로그 데이터를 통합하여 분석해 통합적인 보안 체계를 제공해줍니다.

최근에는 이에 대한 보안 관리까지 수행하는 제품들이 많이 나오게 되면서 로그 수집 및 통합 뿐만 아니라 보안 관리까지 해주는 전반적인 솔루션을 SIEM이라 부르고 있습니다.

*로그 : 시스템을 사용한 내용 및 시간에 대한 모든 기록

기업이 SIEM을 사용하는 이유

기업 보안 담당자의 업무 효율성과 법적 필수 요소 준수의 이유로 SIEM의 사용은 선택이 아닌 필수로 자리 잡고 있습니다.

보안 담당자의 업무효율성

SIEM을 사용하는 주체인 보안 담당자의 입장에서 일일이 사내 시스템 및 다양한 보안장비의 데이터들을 관리하고 이에 대한 위협을 분석하는 것은 시간 소요가 많이 들고 비효율적인 부분입니다.

전체 시스템의 로그를 통합시키고 보안 관리를 해주는 SIEM은 보안 담당자의 업무 효율성을 증진시키고, 편리함을 제공해줄 수 있습니다.

법적 필수 요소 준수

개인정보 안전성 확보 조치 기준, 정보통신망법, GDPR 등의 법률에는 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악해야 함이 명시되어 있습니다.

유럽 진출 기업의 경우, 기업 규모에 상관없이 GDPR 법이 적용되어 중소 기업도 로그 점검 및 외부 공격 여부 파악을 위한 SIEM이 필요할 수 있습니다.

02
Teiren SIEM

About Teiren SIEM

Solution

위협 탐지 및 분석

Teiren은 공격경로를 찾기 어려웠던 문제점을 데이터베이스의 변화로 해결할 수 있었습니다.

공격이 발생한 지점을 기점으로 어떤 로그가 생겨났는지 그 흐름을 확인할 수 있으며 방화벽을 통해 첫 로그를 생성하고 그 다음 Cloud 내에 로그인해서 기업 정책을 변경하는 등의 공격자의 행위 흐름을 시각화해서 확인할 수 있습니다.

로그의 흐름을 시각화해 보여줌으로써 전문 지식이 뛰어나지 않은 보안 인력들도 쉽게 공격 루트를 파악할 수 있습니다.

뿐만 아니라, 그래프 데이터 베이스를 통해 기존 데이터 베이스와 비교 시 관계가 늘어날수록 180배, 1135배, 그 이상의 속도 증가를 확인할 수 있었습니다.

커스터마이징

기존 로그 관리 솔루션 혹은 SIEM은 고객의 니즈를 해소해주기에는 다소 어려운 점들이 있었습니다. 로그 관리 솔루션 사용자를 대상으로 한 테이렌 자체 설문조사에 따르면 시각화 부족, 필터링 기능 부족, 커스터마이징 하드닝, 성능 부족 등의 불편사항이 해소되지 않고 있었습니다. 타 로그 관리 솔루션과 같은 경우 조금의 변화를 위해서 솔루션 전체에 큰 영향을 줘야하는 위협이 있어 커스터마이징을 꺼려합니다.

테이렌은 고객의 불편사항을 해소시켜드리는 것을 최우선 순위로 두고 고객의 문의사항을 즉각 반영하며, 최종적으로 고객이 만족하실 수 있는 로그 관리 솔루션이 되도록 커스터마이징을 제공합니다.

컴플라이언스 인증 보고서를 통한 보안 담당자 업무효율성 증진

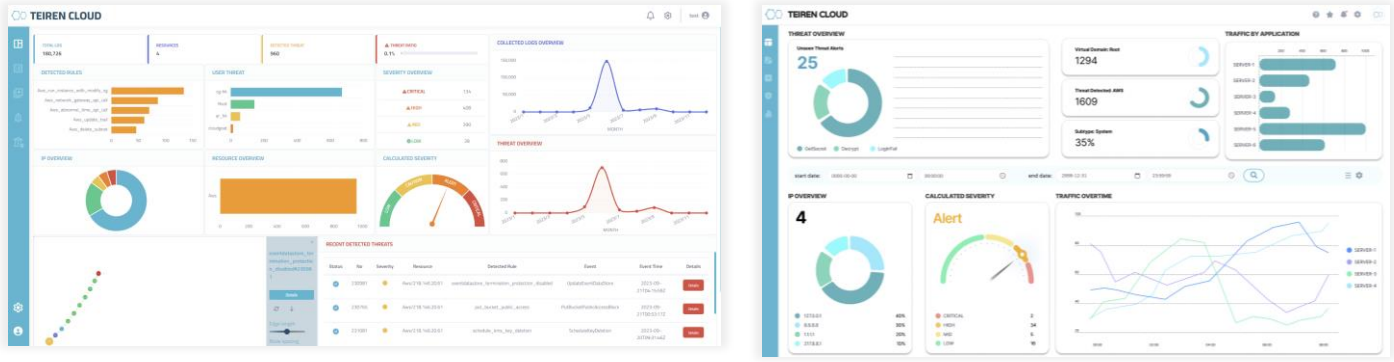
Teiren SIEM은 보안 인력들이 느끼는 업무 부담감을 덜어주기 위해 컴플라이언스 인증 보고서를 제공합니다.

보안 담당자들은 ISMS-P 등의 보안 인증 심사를 받기 위해 증적을 수집하는 단순 노동에 최소 2주이상의 긴 시간을 소비합니다. SIEM이 전체 솔루션에 대한 보안 관리를 수행한다는 점을 활용, 기업이 준수하고 있는 컴플라이언스를 확인해주고, 이에 대한 증적을 캡처본으로 만들어 제공해줍니다.

보안 담당자는 보고서에 대한 검토 작업만 함으로써 시간을 단축해 업무 효율성이 증가하게 됩니다.

TEIREN SIEM

Teiren SIEM 대시보드

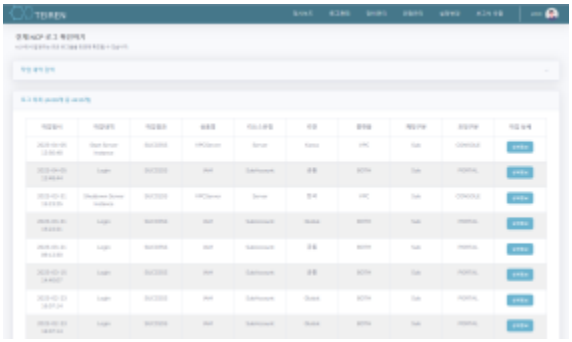


▲ 대시보드 화면

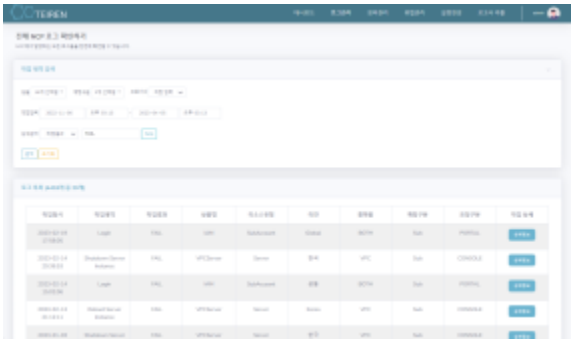
Teiren SIEM의 대시보드에서는 총 로그의 개수와 위협 로그 개수, 위협 비율, 최근 탐지 위협 등을 확인함으로써 실시간 위협에 대해 모니터링 할 수 있습니다. 각 디바이스, 솔루션 간의 상관관계 또한 대시보드에서 확인할 수 있습니다.

또 SIEM을 사용하는데 있어서 CPU /Memory 등의 사용량을 실시간 그래프로 제공해줍니다.

로그 출력 및 필터링



▲ 로그 출력 페이지



▲ 로그 필터링

로그 데이터를 수집하고, 수집한 다양한 로그 데이터를 통합해 웹상에서 테이블 형태로 제공됩니다. 사용자는 다양한 클라우드, 시스템으로부터 수집된 방대한 양의 로그 데이터들을 한눈에 보고 파악할 수 있으며, 해당 로그 데이터의 보다 상세한 내용을 보고자 하면 상세보기 버튼을 통해 더 자세한 정보와, 로그 데이터의 원본 형식인 JSON 형식으로도 볼 수 있습니다.

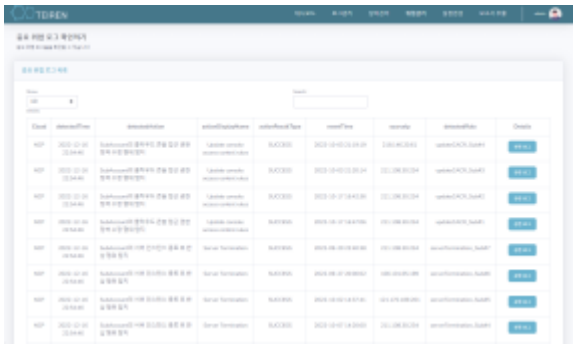
사용자는 수집된 많은 양의 로그 데이터 중 원하는 데이터를 필터링 해서 선택적으로 볼 수 있습니다. 상품명, 계정, 조회 기간 등을 각각 선택해서 선택 한 값에 따라 로그 데이터를 분류할 수 있고, 상세 검색을 위해서 정규표현식을 사용해 사용자가 직접 상세하게 검색할 수 있도록 제작하였습니다.

TEIREN SIEM

위협 탐지

Teiren SIEM은 Graph DB를 통해 향상된 성능의 보다 고도화된 위협탐지가 가능합니다.

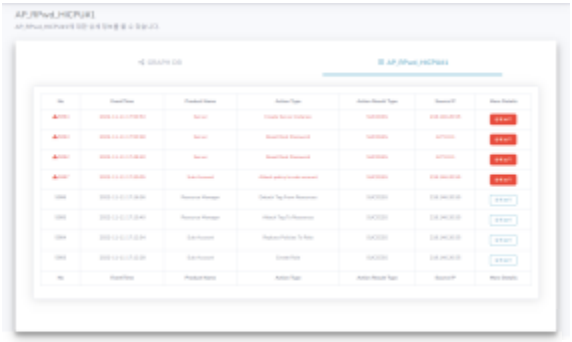
▲ 보안 정책 설정 화면



▲ 위협 알림

위협탐지를 위한 보안 정책을 설정할 수 있습니다. Teiren에서 기본적으로 정의해 제공하는 보안 정책은 약 150개이며, 이 기본 정책만으로도 간단한 위협탐지가 가능합니다. 사용자는 기본 정책에 대해서는 on/off 를 통해 제어할 수 있고, 기업의 환경에 맞춰서 상세설정 또는 정책의 흐름 지정을 통해 직접 정책을 추가할 수 있습니다. 이렇게 설정된 정책에 탐지된 위협은 위협 알림 페이지에서 확인이 가능합니다.

▲ 흐름 기반 위협탐지 화면



▲ 위협 탐지 화면

추가적으로, 단순히 1개의 이상행위가 아닌 행위의 흐름에 따라 위협을 탐지할 수 있도록 여러 개의 정책의 흐름을 지정할 수 있도록 하였습니다. 이 역시 사용자가 흐름 지정을 통해 직접 정책을 추가할 수 있습니다.

위협 탐지 시 해당 위협까지의 사용자 행위의 흐름을 한눈에 파악할 수 있도록 그래프 형식으로 시각화하여 보여줍니다. 또, 탐지된 위협은 관련 행위와 함께 표시하여 테이블 형식으로도 제공해줍니다.

Graph Database

Graph Database는 그래프 이론에 기반을 둔 NoSQL 데이터베이스로, 데이터 간의 관계를 기반으로 방대한 양의 데이터 분석이 용이합니다.

데이터 자체를 점과 선의 그래프 형태로 저장해 데이터 간의 관계를 객체 간의 선 만으로 표현하는게 가능합니다. 위협 발생 시 관련된 노드들을 인덱스 없이 손쉽게 검색할 수 있으며, 그래프를 시각화해 DB 구성을 한눈에 보기 쉽게 만들 수 있습니다.

TEIREN SIEM

위협 경로 시각화 및 머신러닝

▲ 위협 분석 시각화

Teiren SIEM은 사용자 노드부터 탐지된 보안 정책까지 한눈에 볼 수 있도록 시각화 해줍니다. 탐지된 위협이 어떤 흐름을 통해 발생한 위협인지, 해당 위협을 발생시킨 사용자의 다른 행위와는 어떠한 관련이 있는지를 한눈에 파악할 수 있으며, 이를 통해 위협 간의 상관관계 파악이 가능합니다.

보고서 추출

▲ 월간 위협 보고서.xlsx

▲ 컴플라이언스 인증 보고서

기본적인 엑셀 형식의 위협 보고서를 제공해줍니다. 해당 보고서에는 요약 보고서 및 위협으로 탐지된 로그, 연동 현황 등에 대한 정보가 담겨있습니다.

Teiren SIEM은 보안 인력들이 느끼는 업무 부담감을 덜어주기 위해 컴플라이언스 인증 보고서를 함께 제공해줍니다. 기업이 준수하고 있는, 또는 준수해야 하는 컴플라이언스 항목을 자동 매핑해주며, 이에 대한 증적을 캡처본으로 만들어 pdf 형식의 보고서로 제공해줍니다.

보안 담당자들은 제공된 보고서를 검토하는 업무만 수행함으로써, 기존의 단순 업무를 줄여 엄무 부담감을 줄이고, 효율성을 증진시킬 수 있습니다.

05
About Teiren

Teiren 소개

TEIREN

Tera Byte + Siren의 합성어로,
테라바이트(TB) 단위의 데이터를 분석해 고객에게 최고의 Siren이 되자는 의미를 담은 보안 소프트웨어 전문기업입니다.

구성원 모두 대한민국 최고의 차세대 보안 인재 양성 프로그램 Best Of the Best(BoB) 수료생으로, 기업의 보안성 향상을 위해, 고객의 사이버 보안 난제를 해결하기 위해, 보안 담당자의 업무 부담감을 해결하기 위해 설립된 회사입니다.현재는 실제적으로 이 어려움을 해결하기 위해 Graph DB라는 선진 기술을 적용해 SIEM이라는 보안 솔루션을 제공하고 있습니다.

김성연 CEO

서울여자대학교 정보보호학 학사
한국정보보호경영연구소 보안컨설팅 주임연구원(신한은행, 한국은행 등 근무)
보안 관련 논문 3건 발표, 특허출원 2건, SW 저작권 2건
과학기술정보통신부 Best of the Best(이하 BoB) 11기 보안컨설팅
과학기술정보통신부 BoB 11기 그랑프리
성균관대학교 글로벌창업대학원 G-AEP 5기 수료
벤처기업협회 Young CEO Network 부위원장, 벤처기업협회 PSWC 26기 수료
성균관대학교 글로벌창업대학원 기업가정신상 수상

조소망 CSO

해외 세일즈 및 프론트엔드 기획 역할
중앙대학교 산업보안학 학사
과학기술정보통신부 BoB 11기 보안컨설팅
과학기술정보통신부 BoB 11기 그랑프리

이현우 Developer

백엔드 개발 역할
세명컴퓨터고등학교 스마트보안솔루션학과
과학기술정보통신부 BoB 12기 보안제품개발
세명해킹보안경진대회 은상(2022)
세명해킹보안경진대회 은상(2023)

홍민표 Active Chairman

해외 진출 기획 및 제품 사업화 역할
세계 500대 Cyber Security 기업 선정
세계해킹방어대회 DEFCON Final 진출
전) 국내 보안회사 쉬프트웍스 Exit
현) 미국 보안회사 SEWORKS 대표이사

팀이력

- 과학기술정보통신부 Best of the Best 11기 그랑프리
- 정보보호학회 - Graph DB를 활용한 위협탐지 모델링 논문 발표
- 예비창업패키지 벤처기업협회
- 초기창업패키지 고려대학교
- FINEVO(KT Cloud 공식 MSP) MOU/NDA 체결
- 한국정보보호산업협회 '2024 K-Security 스타트업 글로벌 챌린지'
- 한국정보보호산업협회 'K-Shield UP 챌린지 프로그램'
- 2023 ComeUp Stars 아카데미 리그 선정
- 숭실대학교 캠퍼스타운 입주 (지점 설립)
- 소셜 벤처 판별 및 벤처기업인증 취득
- 제 13회 스마트테크코리아 시큐테크쇼(코엑스) 부스운영
- 2023 Girls Unicorn Contest 대상
- 2023 벤처기업협회 올해의벤처상(창업활성화부문) 수상
- 2024 여성스타트업 경진대회 입상(이사장상)
- 도전! K-스타트업 2024 본선 진출

Teiren