TEIREN CLOUD SIEM

보이지 않는 공격을 본다

Teiren

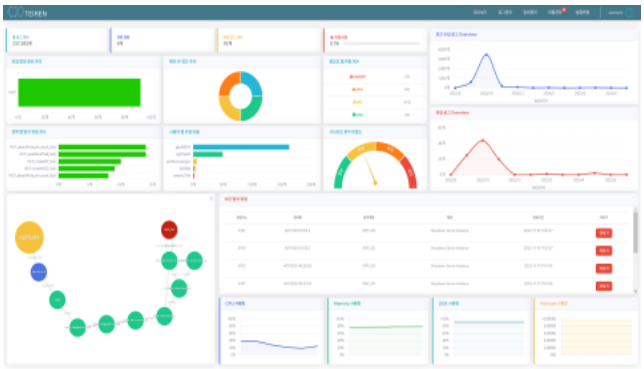
Contents

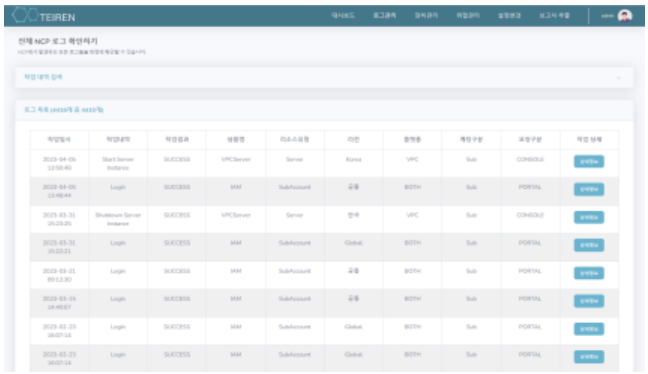
01
About SIEM

SIEM 소개

About SIEM

SIEM이란?





SIEM이란, Security Information & Event Management (정보보안 이벤트 관리) 의 약자로, 기업 자산에 대한 *로그 들을 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 일일히 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

개인정보안전성확보조치기준, 정보통신망법, GDPR 등의 법률에는 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악해야 함이 명시되어 있습니다.

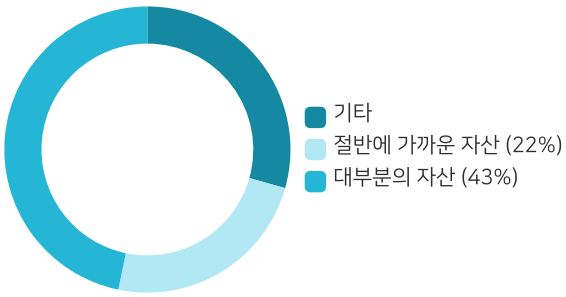
유럽 진출 기업의 경우, 기업 규모에 상관없이 GDPR 법이 적용되어 중소 기업도 로그 점검 및 외부 공격 여부 파악을 위한 SIEM이 필요할 수 있습니다.

02
Teiren SIEM

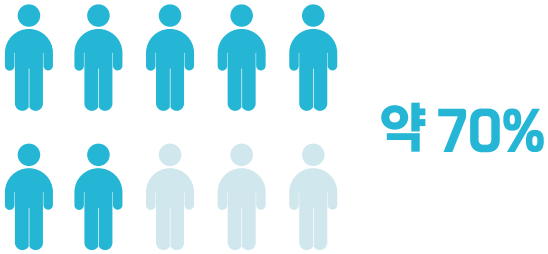
About Teiren SIEM

Problem

현 기업 보안의 문제점



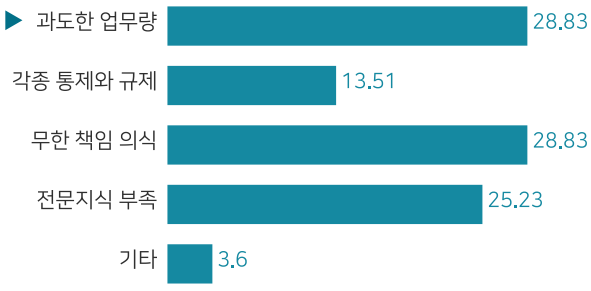
클라우드 내 자산 비율



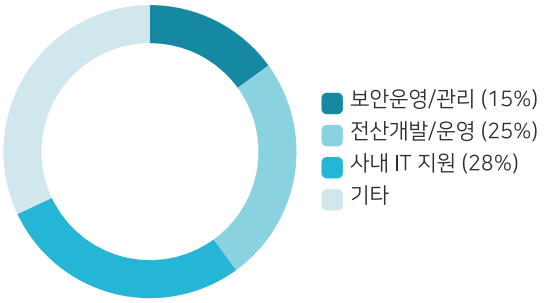
관리되지 않은 자산에 대한 공격 경험

클라우드를 도입한 기업 중 40%이상이 대부분의 자산을 클라우드 내에 구축해둔 상태입니다. 이렇게 기업의 자산을 클라우드에 구축하게 됨에 따라 기업 내에서는 이전보다 더 많은 이벤트들이 발생하게 되면서 실제로 관리되지 않은 자산에 대한 사이버 공격의 비중도 높은 현황입니다. [출처 : 2021 MIT Technology Review Insight 설문조사]

따라서 이전과는 다르게 늘어난 기업 자산을 기반으로, 사이버 공격이 발생했을 때 이 공격이 어디서, 어떻게, 어떤 흐름으로 발생했는지 공격 경로를 알아차리는 것이 더욱 더 어려워졌습니다. 즉, 실제로 클라우드 도입에 따른 보안 대상 범위 확장으로 인해 보안 대응의 어려움이 증가하고 있다는 의미입니다.



정보보호 담당자의 업무 부담감 발생 사유



사내 다른 IT 지원으로 인한 보안 운영 / 관리 소홀

보안 담당자들은 과도한 업무량으로 인해 보안 업무에 큰 부담감을 느끼고 있다고 응답했고, 심지어 인력과 예산부족으로 업무에 큰 애로사항이 있다고 응답했습니다. [출처 : 2022년 국정원 국가정보보호백서]

또, 중소기업 보안인력들은 자신들의 업무에서 보안관리가 가장 중요하지만, 사내 다른 IT 지원으로 인해 보안 운영과 관리가 소홀해지고 있다고 답해, 중소기업 역시 보안이 미비하다는 것을 알 수 있습니다. [출처 : 지란지교 중소기업 정보보안 설문조사]

Solution

위협 탐지 및 분석

Teiren은 공격경로를 찾기 어려웠던 문제점 데이터 베이스의 변화로 해결할 수 있었습니다.

공격이 발생한 지점을 기점으로 어떤 로그가 생겨났는지 그 흐름을 확인할 수 있으며 방화벽을 통해 첫 로그를 생성하고 그 다음 Cloud에 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 담당자의 업무효율성 증진

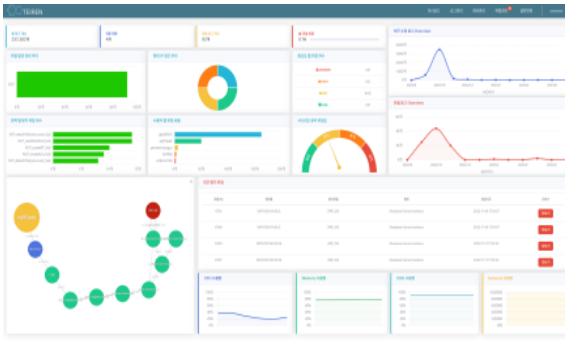
Teiren SIEM은 보안 인력들이 느끼는 업무 부담감을 덜어주기 위해 컴플라이언스 인증 보고서를 제공합니다.

보안 담당자들은 ISMS-P 등의 보안 인증 심사를 받기 위해 증적을 수집하는 단순 노동에 최소 2주 이상의 긴 시간을 소비합니다. SIEM이 전체 솔루션에 대한 보안 관리를 수행한다는 점을 활용해, 기업 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

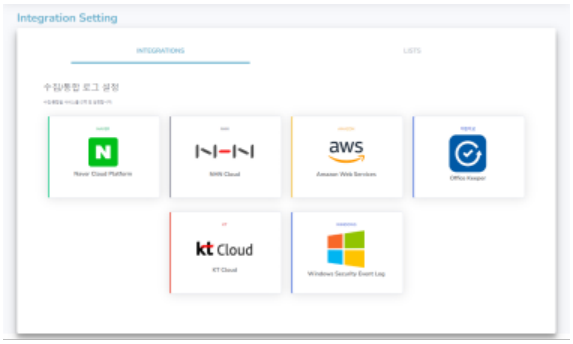


대시보드 화면

Teiren SIEM의 대시보드에서는 총 로그의 개수와 위협로그 개수, 위협 비율, 최근 탐지 위협 등을 확인함으로써 실시간 위협에 대해 모니터링 할 수 있습니다.

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

제품 연동

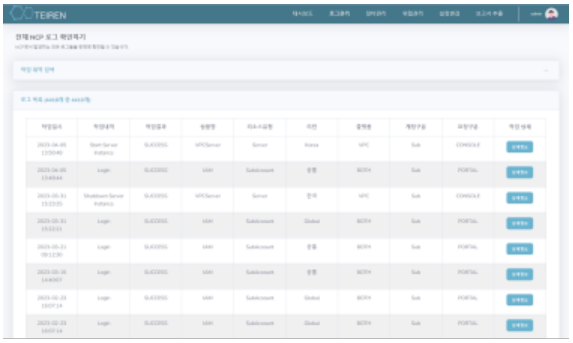


제품 연동 화면

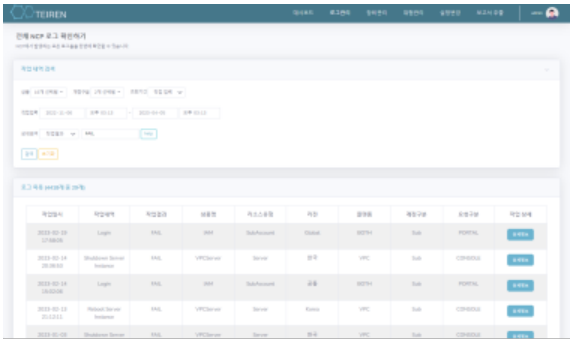
제품 연동 페이지에서 API를 위한 키를 입력해 연동할 다양한 클라우드 및 시스템을 등록할 수 있습니다.

현재 Naver, NHN, AWS 클라우드, 윈도우즈 보안 이벤트 로그, 지란지교의 보안 솔루션 Office Keeper를 연동해 해당 시스템을 지원하고 있습니다.

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.

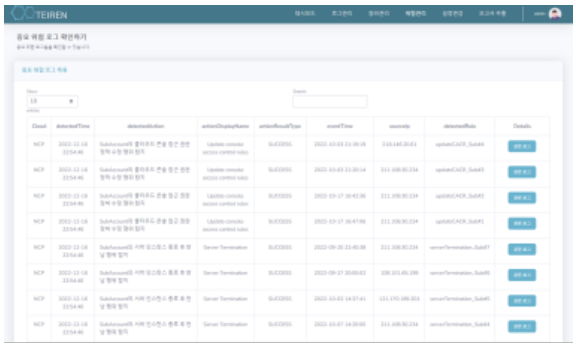
사용자는 수집된 많은 양의 로그 데이터 중 원하는 데이터를 필터링 해서 선택적으로 볼 수 있습니다. 상품명, 계정, 조회 기간 등을 각각 선택해서 선택 한 값에 따라 로그 데이터를 분류할 수 있고, 상세 검색을 위해서 정규표현식을 사용해 사용자가 직접 상세하게 검색할 수 있도록 제작하였습니다.

TEIREN SIEM

위협 탐지

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

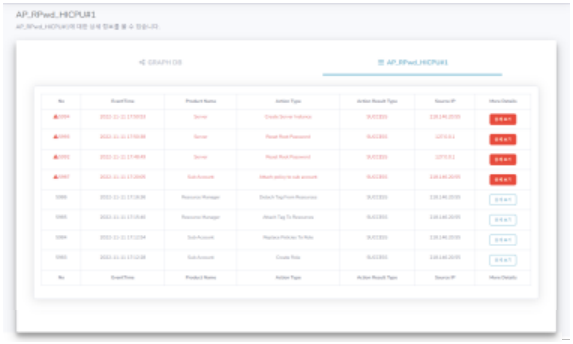
▲ 보안 정책 설정 화면



▲ 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

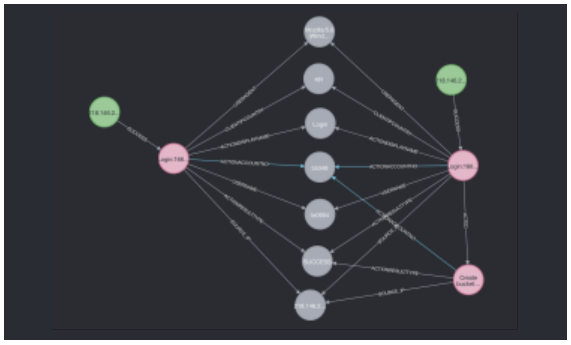
Graph Database는 그래프 이론에 기반을 둔 NoSQL 데이터베이스로, 데이터 간의 관계를 기반으로 방대한 양의 데이터 분석이 용이합니다.

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



사용자 행위 패턴 기반 머신러닝

Teiren SIEM은 사용자 노드부터 탐지된 보안정책까지를 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 위협간의 상관관계 파악이 가능합니다.

더 나아가, 사용자의 행위 패턴을 기반으로 인공지능을 학습시킵니다. 각각의 사용자 행위 로그 간의 유사도를 측정해 평소와 다른 패턴의 행위가 발생한다면 이를 위협으로 간주하고 보안 알림을 보내줍니다.

보고서 추출

월간 위협 보고서 요약(2023/02)

근 5개월 위협

날짜	2022/8	2022/9	2022/10	2022/11	2022/12	근 5개월 합계
위협개수	0	0	1	0	0	1

이번달 요약

내용	총 로그 수(개)	총 위협 로그 수(개)	연동 제품 수(개)	총 위협 비율(%)
결과	238822	87	3	1.97

최근 탐지 위협 top 5

No	장비명/IP	탐지 위협	행위
1	NCP/218.146.20.55	serverTermination_S	Server Termination
2	NCP/106.101.66.81	attachPolicyAccount	Attach policy to sub
3	NCP/106.101.65.2	serverTermination_S	Server Termination
4	NCP/106.101.65.2	RRP_SSH#1	Shutdown Server
5	NCP/106.101.65.2	RRP_SSH#2	Shutdown Server

탐지 로그 전체 리스트

정책명	행위 결과
Create Role	SUCCESS
Create Role	SUCCESS
Create Role	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS

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 업무 부담감을 줄이고, 효율성을 증진시킬 수 있습니다.

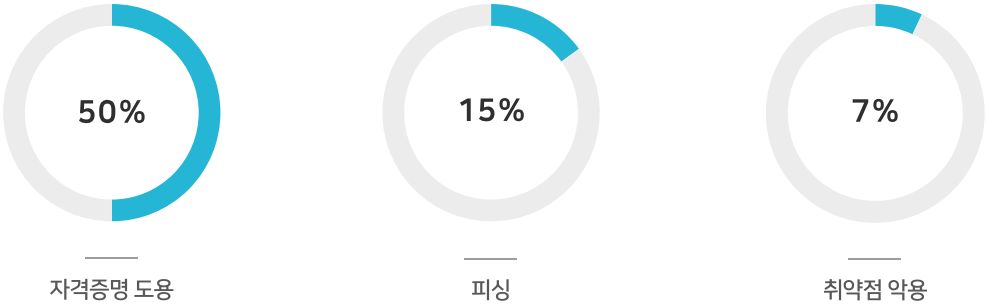
03
Teiren SIEM use-case

Teiren SIEM 활용 예시

TEIREN SIEM 활용 예시 1

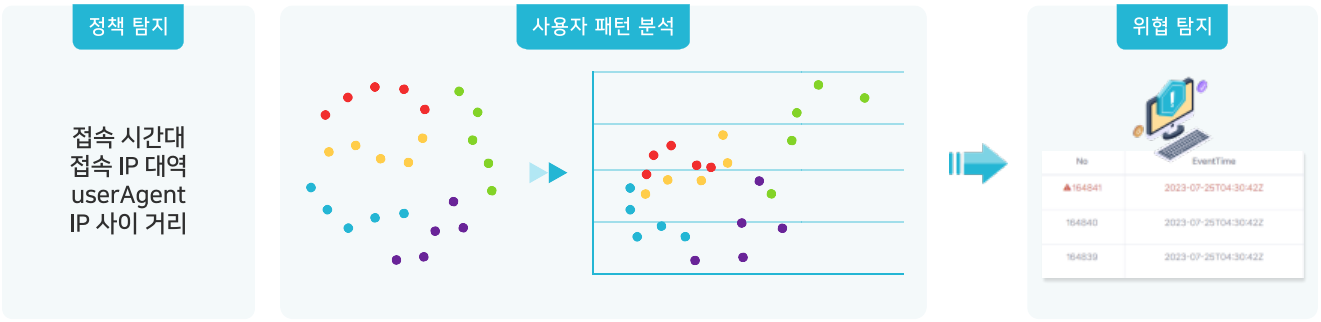
손상된 사용자 자격 증명 (계정 탈취) 탐지

클라우드 사용량 증가 및 covid-19 로 인한 원격 근무 확장으로 근무 환경에 대한 제약이 줄어들면서, 다양한 지리적 위치에서 클라우드 환경으로의 액세스가 보편화되었습니다. 이로 인해 클라우드 환경 구성의 취약점을 악용한 악의적인 액세스 역시 증가하고 있는 추세이며, 데이터 유출 및 침해 사고를 방지하기 위해 클라우드 내에서의 악의적인 행위 패턴을 가려내는 일이 필수로 자리 잡고 있습니다.
Verizon 2023 데이터 침해 조사 보고서의 내부자 위협 통계에 따르면, 자격 증명 도용이 공격의 세가지 주요 방법 중 하나로 나타났습니다.



클라우드 환경에 대한 관리자 권한을 보유하고 있는 사용자의 경우 확대된 자산에 대한 액세스가 허용되기 때문에 공격자가 해당 사용자의 계정을 탈취해 악의적인 활동을 수행하면, 클라우드 환경에 치명적인 피해가 발생할 수 있습니다. 또한, 신뢰 관계가 형성된 내부자의 권한을 사용해 활동을 이어가기 때문에, 이러한 행위는 합법적으로 보이며, 보안 솔루션에서 쉽게 이를 구분하고 위협으로 간주하지 못합니다.

Teiren SIEM은 사용자가 사용하는 IP대역, 클라우드 리전, 정상 행위 시간대 등을 분석하여 정상 패턴 대비 비정상 행위 패턴을 식별합니다. 더 나아가, 정책 만으로는 탐지할 수 없는 사용자 행위 패턴 간의 유사도를 인공지능 학습을 통해 측정해 이를 바탕으로 평소와 상이한 패턴의 행위 발생 시, 이를 탐지해 분석을 제공합니다.

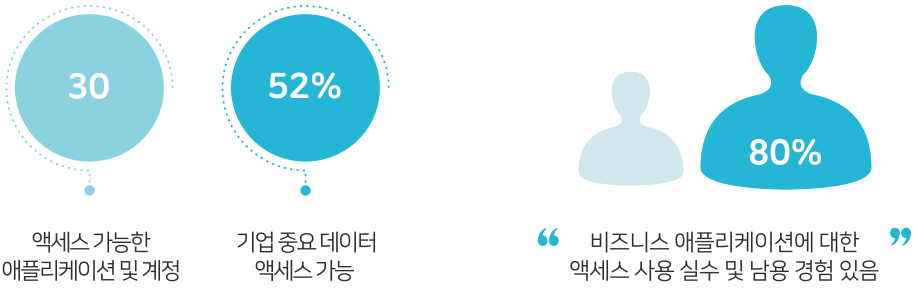


예를 들어, 물리적으로 불가능한 거리의 IP주소에서의 API호출, 정상 근무 시간 외 시간대 클라우드 액세스 등 정상적으로 판단되지 않는 행위 발생 시 테이렌은 이를 위협으로 간주하고 사용자에게 위협 경고를 전송합니다.
사용자는 해당 경고 확인 후 경고의 내용과, 해당하는 로그 및 행위의 흐름을 확인할 수 있으며, 이에 따른 대응으로 보다 체계적인 클라우드 보호가 가능하도록 합니다.

TEIREN SIEM 활용 예시 2

클라우드 인프라 권한 남용

CyberArk의 조사에 따르면, 평균적으로 직원은 30개 이상의 애플리케이션과 계정에 액세스 할 수 있으며, 조직의 직원 중 52%가 중요한 기업 데이터에 액세스 할 수 있습니다. 또한 조직의 80%가 2022 한 해 동안 비즈니스 애플리케이션에 대한 액세스를 잘못 사용하거나 남용한 경험이 있어 사용자 세션 및 활동에 대한 가시성이 향상되어야 한다는 필요성이 나타났습니다.



팔로알토 네트웍스 Unit42의 클라우드 위협 보고서에 따르면 잘못된 구성은 알려진 클라우드 보안 사고의 대부분의 중심에 있는 경향이 있으며, 잘못 작성된 IAM(ID 및 액세스 관리) 정책이 원인인 경우가 많았습니다. 또한 클라우드 사용자, 역할, 서비스 및 리소스의 99%에 60일동안 사용하지 않은 과잉 권한이 부여된 것으로 나타났고, 취약한 암호 정책을 사용하거나 클라우드 리소스를 공개 노출하는 등의 구성 실수가 많았습니다.
이와 같은 클라우드 인프라 구성의 틈을 악용한 공격은 늘어나고 있으며 이에 따라 보다 더 안전하고 철저한 보안 관리가 가능한 인프라 구성은 필수입니다. 취약한 보안을 뚫고 공격자가 클라우드 환경에 액세스 성공했을 시, 피해를 최소화 하기 위해서는 이를 방지하기 위한 적절한 구성이 필요합니다.

Teiren은 클라우드 인프라 및 IAM에 대한 자체적인 권장 구성법을 제공합니다.
예를 들어, 이벤트 로깅 중지, IAM 암호 정책 완화, 인스턴스 퍼블릭 공개 등의 이벤트 발생 시 가능한 위험에 대한 정보 제공과 동시에 개선 사항 및 방법을 담은 수정가이드를 제공합니다.

취약한 구성으로 인한 위험 가능성에 대한 정보와 클라우드 콘솔, cli 상에서의 수정 방법을 담은 가이드를 통해 사용자는 손쉽게 구성 변경을 할 수 있으며, 이를 통해 보다 안전한 인프라 구성이 가능합니다.

TEIREN SIEM 활용 예시 3

ISMS-P 준수

최근 해킹사고, 랜섬웨어 감염, 개인정보 유출 사고 등 침해사고가 지속적으로 발생하고 있고, 동시에 공격 기법은 점점 지능화되고 있습니다. 또한 클라우드 도입으로 인해 기업 이벤트가 많이 발생하게 되었고 이에 따라 침해사고로 인한 기업의 피해는 막대해졌습니다. 이처럼 기업의 정보보호 및 개인정보보호 관리가 중요해짐에 따라 정보보호에 대한 체계적인 인증제도에 대한 필요성이 대두됨에 따라, ISMS-P (정보보호 및 개인정보보호 관리체계) 인증 취득은 더 중요해지고 있습니다.

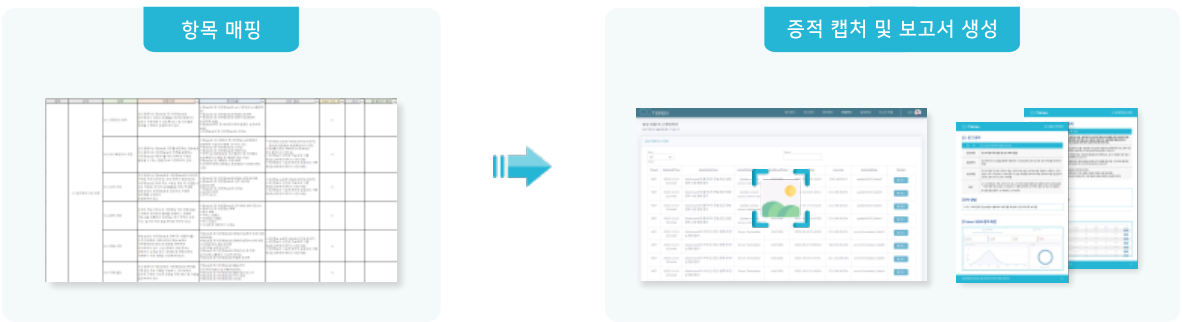
ISMS-P 인증은 정보통신망의 안정성 확보 및 개인정보 보호를 위해 조직이 수립한 일련의 조치와 활동이 인증기준에 적합함을 인증기관이 평가하여 인증을 부여하는 제도로, 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구 사항 3가지 범주에 기준을 두고 있습니다.

ISMS-P
인증 의무 대상

- 1500억 이상의 매출 기업
  - 의료 분야 (상급 종합 병원)
  - 교육 시설 (재학생 수 1만명 이상인 학교)
- 정보 통신 서비스 기업
  - 100억 이상의 매출액
  - 3개월 간 일일 평균 이용자 100만 명 이상의 기업

ISMS-P 인증 의무 대상은 위와 같으며, 의무 대상이 아니더라도 정보보호 관리체계를 구축, 운영을 하거나 필요로 하는 기업들은 인증 취득이 가능합니다. 기업이 ISMS-P를 취득하게 되면 보다 체계적이고 종합적인 보호대책을 구현해 기업의 정보보호 및 개인정보보호 관리 수준 향상시킬 수 있으며, 침해사고 및 개인정보 유출사고 발생 시 신속하게 대응하고 피해 및 손실을 최소화할 수 있습니다.

Teiren SIEM은 이중 테이렌 SIEM을 사용함으로써 증명할 수 있는 항목들을 자동으로 매핑하고, 해당 측면에서 자동으로 증적을 수집해 ISMS-P에서 요구하는 대로 보고서를 생성합니다.



Teiren SIEM은 이런 기업들이 사용하면 좋습니다.

금융기관, 공공기관, ISMS-P 인증기업(직전사업연도 말을 기준으로 자산이 2조 원이고, 상시 종업원 수가 300명인 기업), 사용자의 개인정보를 다루는 개인정보처리기업, ICT 기업, 클라우드 사용 기업(AWS, GCP, Azure 등), 국내 클라우드 사용 기업(NCP, NHN, KT Cloud 등) 및 그 외 로그 관리가 필요한 기업들이 사용할 수 있습니다.

04
Price Plan

Teiren SIEM 가격 정책

Price Plan

보안 담당자들은 제품을 선택할 때 먼저 우리 회사에서 구매할 예산이 있는가를 고려하는데요, Teiren SIEM은 Basic, Standard, Premium 월간 라이선스를 도입해 영구 라이선스의 비싼 요금에 대한 문제점을 해소할 수 있도록 가격구조를 책정했습니다. 현 시장에 나와있는 SIEM들 에 비해 보다 가격적인 측면에서 합리적인 제품이 되어 접근성을 높이고자 하였습니다.

BASIC	STANDARD	PREMIUM
30만 ₩ / 월	300만 ₩ / 월	가격 별도 조정
Account 100개 (*추가 비용 별도) 로그 수집 로그 필터링 정책 설정 및 추가 흐름 기반 위협 탐지 공격 경로 시각화	Account 100개 (*추가 비용 별도) 로그 수집 로그 필터링 정책 설정 및 추가 흐름 기반 위협 탐지 공격 경로 시각화 컴플라이언스 보고서 머신러닝 + UEBA	Account 100개 (*추가 비용 별도) 로그 수집 로그 필터링 정책 설정 및 추가 흐름 기반 위협 탐지 공격 경로 시각화 컴플라이언스 보고서 머신러닝 + UEBA 위협탐지 커스터마이징

라이선스 별 대상 고객

SIEM과 같은 보안 솔루션을 사용하는 이유는 기업마다 다릅니다. Teiren은 불필요한 기능 및 가격 부담감으로 생기는 문제를 해소하고, 각 기업의 보안 운영의 목적에 맞게 합리적인 기능과 가격으로 SIEM을 사용할 수 있도록 하였습니다.

라이선스	가격	대상 고객
Basic	30만원 / 월	- 저렴한 보안 솔루션을 찾는 기업 - 단순 법률 준수 기업 ✓개인정보보호법 '로그관리' 필수
Standard	300만원 / 월	- 1500억 이상 매출 기업, 정보통신서비스 업체 등 ISMS-P 등의 보안 인증 필수 기업 - 보안 인증 취득 및 법률 준수 기업 ✓보안 인증 시 '로그 관리' 필수 ✓금융거래법 등 '로그 관리' 필수 - 제로트러스트 기반 보안 전략 기업 'KISA 제로트러스트 가이드라인 1.0' SIEM사용 명시
Premium	350만원 이상 (개별측정) / 월	- 개별적으로 받아야 하는 다양한 인증이 존재하는 기업 - 기업의 환경에 최적화된 SIEM을 사용하고자 하는 기업

05
About Teiren

Teiren 소개

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.

Teiren History

저희 Teiren은 안전한 세상을 위해 더욱 더 빠르고 고도화 된 보안 제품을 만들어 나갈 것 입니다.
고객의 목소리에 귀를 기울이며, 여러분들의 사이버 보안에 대한 무거운 짐을 덜어줄 수 있도록 힘을 쏟겠습니다.

2022

12
Best of the Best 그랑프리 진출
한국정보기술연구원 창업 지원 선정

2023

3
Best of the Best 11기 수료

4
2023 창업중심대학 선정

5
(주)테이렌 설립
2023 예비창업패키지 우수기업 선정

6
2023 COMEUP Stars 선정
2023 BoomUP 스타트업 리그 선정

8
소셜벤처기업 인증
침입탐지 분야 SW 저작권 등록

9
Pre-Seed 투자 유치
2023 Girls Unicorn Contest 대상

Teiren