elastic

SIEM으로 더 많은 운영 가치 창출

elastic.co/kr →

목차

머리말

기업이 시장 변화에 적응하기 위해 디지털 혁신 이니셔티브를 채택함에 따라 많은 기업이 보안 접근 방식을 재평가해야 했습니다. 새로운 웹 제품 및 서비스, 모바일 앱, 원격 근무 인력 지원의 필요성이 새로운 유형의 사이버 공격에 점차 확산되고 있습니다. **이러한 공격에 대처하려면 보안 팀이 신속하게 진화할 수 있어야 합니다**.

보안 팀의 최선의 노력에도 불구하고 비즈니스를 위협할 수 있는 비효율성을 피하는 것이 지속적인 대처의 핵심 과제입니다. SaaS 채택의 급증, 지속적인 개인 정보 보호 의무 및 보안 기능을 통합하기 위한 지침은 운영상의 복잡성을 가중시킬 뿐입니다.

운영 효율성을 유지하면서 제어력을 유지하는 비결은 보안 정보 및 이벤트 관리(SIEMt) 플랫폼 내에서 즉시 사용할 수 있는 데이터로부터 시작됩니다. 클라우드, 사물 인터넷(IoT), 모바일 소스, 통합 가시성 데이터 등 보안 팀에 필요한 데이터의 양과 다양성이 폭발적으로 증가하고 있습니다. 그 결과, 비즈니스 보호에 필요한 인사이트를 확보하는 데 중요한 이벤트 활동이 크게 증가합니다.

이러한 데이터 급증으로 인해 SIEM 제한으로 인한 운영 문제가 발생하는 경우가 많습니다. **SIEM에 대한 접근 방법을 검토하여** 이러한 새로운 과제에 대한 준비가 되었는지 확인해야 합니다.

175ZB

IDC는 2025년까지 전 세계 데이터가 175제타바이트로 증가할 것으로 예측합니다.

416억

2025년까지, 416억 개의 연결된 장치들이 79.4제타바이트의 데이터를 생성할 것입니다.

420억

PwC의 글로벌 경제 범죄 및 부정 행위 조사 2020에 대한 응답자들은 총 420억 달러의 부정 행위 손실을 보고했습니다.

진화하는 보안 요구 사항

조직이 보다 클라우드 중심적인 비즈니스 모델을 채택함에 따라 보안 팀은 사용자, 애플리케이션, 엔드포인트 및 데이터 등 비즈니스의 가장 중요한 자산이 보호되도록 보장하는 데 더 많은 책임을 져야 합니다. 보안 팀이 KPI 및 메트릭을 충족하기 어려운 다음과 같은 동향을 고려하세요.

사람들

새롭고 더욱 정교한 공격 방법론을 앞서가는 것이 필수적입니다.

- 보안 기술이 부족합니다
- 부담스러운 보안 팀은 더 나은 협력, 더 빠르고 더 효율적으로 협력하기 위해 노력하고 있습니다

프로세스

클라우드 이니셔티브가 폭발적으로 증가함에 따라 운영 효율성과 속도를 유지해야 한다는 압력이 높아지고 있습니다.

- 막대한 양의 데이터가 클라우드로 이동하고 있습니다
- 원격 직원 및 파트너가 더 많은 클라우드 솔루션에 대한 지원이 필요합니다

기술

대량의 데이터 소스에 대한 지원은 위협을 상황별로 파악하는 데 필요한 회피 활동과 세부 정보를 제공하는 데 필수적입니다.

- 온프레미스 및 클라우드 전반에 걸쳐 대응적인 질의 및 분석을 수행하기가 어렵습니다.
- 많은 시스템에서 대용량 데이터 소스에 액세스하는 것은 비용이 많이 들지 않을 수 있습니다.

보안 팀은 디지털 혁신이 더 많은 공격 표면을 추가한다는 사실을 뼈저리게 인식하고 있습니다. 각각의 새로운 연결 장치 또는 클라우드 서비스는 적에게 악용할 수 있는 새로운 잠재적 벡터를 도입할 수 있으며 심각한 보안 위협이나 비즈니스 위험을 가중시키는 노출 자산을 초래할 수 있습니다. **가장 기본적인 요건은 더 나은 의사결정을 더 빨리 하기 위해 적절한 시기에 적절한 컨텍스트를 갖추는 것입니다.**

데이터를 프레임워크로 사용하여 보안 전략을 다시 생각해 보세요

동적 증가 공격 표면의 가시성을 유지하는 것은 종종 비현실적입니다. 클라우드 확장 요구사항을 충족하지 못하는 최신 또는 이벤트별 라이선싱 모델 및/또는 아키텍처가 절충을 강제할 수 있습니다. 팀은 종종 일상적인 운영에서 어떤 데이터를 포함하거나 제외할지를 결정하는 데 시간과 리소스를 투자하여 SIEM에 대한 가시성이 제한되므로 운영 사일로(데이터 사일로, 팀 사일로 및 프로세스 사일로)가 발생합니다.

대량 데이터 소스나 과거 데이터와 같이 SIEM에 포함시키기 어려운 데이터를 보존하기 위한 일회성 접근 방식과 트레이드오프 방식을 사용하는 대신, 보안 팀은 점점 더 데이터 요구 중심의 다른 접근 방법을 취하고 있습니다. 최신 SIEM의 기반은 모든 데이터를 수용해야 하므로 보안 팀이 사일로를 분리할 수 있습니다. **최신 SIEM을 통해 보안 팀은** 기존 데이터 소스, 비전통 데이터 소스, 대용량 데이터 소스 등 다양한 종류의 데이터를 빠르고 정확하게 검색할 수 있습니다. 일단 기반이 구축되면 보안 팀은 모니터링 및 컴플라이언스, 위협 탐지 및 방지, 검색 및 사고 대응 등 **보안 사용 사례를 규모에 맞게 운영하면서 부정 행위, 개인 정보 침해 및 비즈니스 위험의 기타 우선 순위 문제를 해결할 수 있는 막대한 이점을 얻을 수 있습니다. 핵심은 보안 운영 팀이 통합된 방식으로 보안 통찰력을 수집, 분석, 시각화 및 작업할 수 있는 능력에 있습니다.**

SOC가 통합된 접근 방법을 통해 얻는 이점

통합된 접근 방법은 보안 팀에게 여러 가지 이점을 제공합니다. 강력한 데이터 보안, 데이터 처리 및 데이터 시각화 기능을 갖춘 단일 데이터 저장소는 모든 데이터에서 중요한 보안 인사이트를 추출하는 데 필요한 컨텍스트를 분산 환경에 제공합니다. 보안 팀은 높은 충실도의 탐지, 검증된 머신 러닝 작업 및 사내 및 클라우드에 걸친 기타 기본 제공 방법을 통해 보안 상태를 개선하고, 알려진 것과 알려지지 않은 것을 탐지하며, 신속하게 대응하여 피해를 방지하고, 향후 사고를 예방할 수 있습니다. 전략적으로, **전략적으로 동적인 변화가 발생할 경우 보안 팀은 신속하게 진화할 수 있습니다.** 실무자는 다음과 같이 광범위한 기술을 활용할 수 있습니다.

더 많은 컨텍스트를 활용하여 데이터 조작 및 거래 크래프트 분석

협업하여 새로운 연구를 발굴하거나 새로운 탐지를 구현

새로운 시각화 및 운영 절차 개발

위협 요인을 프로파일링하고 적대적 행동을 에뮬레이트

더 많은 팀들이 헌팅의 책임을 맡을 수 있습니다. 강력한 플랫폼 수준의 통합 기능을 통해 새로운 종류의 위협 및 새롭게 등장하는 규제 의무에 적응하는 것을 단순화하는 매우 효율적인 절차를 수행할 수 있습니다.

SOC는 통합된 접근 방법을 통해 위협 검색, SIEM, 위협 조사, 컴플라이언스, 보안 모니터링 및 조사, 디지털 포렌식 및 사고 대응, 엔드포인트 보호, 부정 행위 방지 등과 같은 다양한 보안 기능에 대한 복잡한 보안 문제를 해결할 수 있습니다.

종합적인 가시성

보안 인사이트를 수집하고 비즈니스 조정 결과를 도출하는 데 필요한 모든 데이터 소스를 포함합니다.

클라우드 확장성

조직 전체에서 필요한 컨텍스트를 확보하여 수년간의 과거 컨텍스트를 포함하여 위협을 확인합니다.

높은 SOC 효율성

가장 우선순위가 높은 문제를 빠르고 쉽게 다른 도구 및 기술과 통합하여 더 빠르게 조사하고 대응합니다.

전체 보안 팀에 대한 가치

보안 엔지니어 및 관리자

- 데이터 소스가 얼마나 다른지 상관없이 전체 환경에서 중앙 집중식으로 로그, 흐름 및 상황별 데이터 분석
- 복잡한 분산 환경에서 빠르게 액세스하고 검색할 수 있는 빠른 연합 검색
- 과도한 비용 없이 대용량 데이터 소스를 쉽게 인덱싱 및 액세스

보안 분석

- 복잡한 위협을 더 빨리 탐지하는 정확도
- 응답 속도 및 효율성 가속화
- 자동화된 위협 탐지 및 MTTD 최소화

SOC 관리자

- 환경 전반에서 높은 수준의 인식 유지로 보안 상태 개선
- 알 수 없는 문제를 식별하면서 알려진 문제의 재발 방지
- 높은 비용 부담 없이 보안 KPI 충족

elastic

SIEM이 걸림돌이 되고 있나요?

오늘날 보안 관련 데이터는 클라우드 서비스, 네트워크 및 사용자 활동, 엔드포인트, 애플리케이션, 연결된 장치 및 기타 많은 소스에서 얻을 수 있습니다. 이러한 모든 데이터 소스에 액세스하려는 SIEM 솔루션의 경우 "커피-브레이크" 분석 시간이 느려지거나 비용이 많이 드는 구축이 가능합니다.

일부 SIEM은 머신 러닝용, 이벤트 기반 상관 관계용 등 다양한 유형의 보안 분석을 위해 별도의 데이터 저장소에 구축되어 있으므로 위협 검색 컨텍스트 또는 범죄 증거 등을 위한 별도의 데이터 저장소에 데이터를 보관할 수 있습니다. 위에서 언급한 바와 같이, 이러한 사일로는 팀이 컨텍스트를 공유하고, 협업하고, 사례를 관리하고, 위협에 대응하는 방식에 비효율성을 초래합니다.

SIEM은 SOC의 발전 속도를 높일 수 있도록 지원하지만, 많은 SIEM 제품은 보안 팀이 데이터 사일로 또는 태스크 사일로의 분해를 지원할 수 있는 확장성 또는 유연성을 제공하지 못합니다. 따라서 이러한 사일로에 의해 제한되는 조사 워크플로우가 발생합니다. 그 결과, 운영 사일로로 인해 보안 팀이 더 빠르고, 더 스마트하고, 더 효율적으로 이동할 수 없습니다.

기존 SIEM 솔루션의 운영 효율성 측면에서 공통적으로 해결해야 할 과제는 다음과 같습니다.

- 보안 데이터 소스는 전사적으로 서로 다른 데이터스토어에 통합되어 있지 않으므로 종합적인 가시성을 확보하기가 어렵습니다.
- 보존 시간이 너무 짧기 때문에 탐지, 조사 컨텍스트 및 위협 검색에 대한 타협이 불가피합니다. 체류 시간이 긴 공격에 대한 위반 범위를 지정하기는 어렵다.
- 보안 분석가는 지속적인 지능적 위협을 나타내지 않을 수 있는 활동에 대한 컨텍스트를 얻는 데 필요한 적절한 데이터 소스가 부족하지만 여전히 비즈니스에 대한 실질적인 위협입니다.
- SOC 팀은 모델을 개발할 내부 데이터 과학자와 컨텍스트를 해석할 수 있는 숙련된 위협 헌터가 없는 한 머신 러닝 도구를 활용할 수 없습니다.
- 보안 엔지니어는 컨텍스트가 풍부한 새로운 데이터 소스(예: 대용량 데이터)를 추가해야 할 경우 데이터 표준화 프로젝트에 막대한 투자를 하거나 SIEM의 기본 데이터 패브릭을 지속적으로 재설계해야 합니다. 이미 데이터를 "알고" 있어야 합니다.
- 연구 팀은 취약하고 회피 기술에 탄력적이지 않으며 올바른 데이터로부터 높은 충실도의 컨텍스트가 부족한 SIEM 규칙을 개발하는 데 너무 많은 시간을 할애합니다.
- 티어 1-2 분석가는 데드엔드를 초래하거나 다른 데이터스토어에서 추가 컨텍스트를 검색해야 하는 경고를 추적하는 데 너무 많은 시간을 할애하여 지연과 비효율성을 유발합니다.
- 개발자는 대부분의 시간을 통합 문제를 해결하거나 공급업체 업데이트에 맞추려고 노력합니다.

최신 SIEM을 사용하여 향상된 보호 기능 제공

현대 SIEM — 관계 없이 크기, 규모, 또는 위치의 모든 보안 데이터에 액세스할 수 있습니다. 전체 환경에 대한 가시성을 통해 보안 팀은 위협을 더 빨리 감지하고 정확하게 대응하여 위협에 대한 우선순위를 결정하는 데 필요한 풍부한 컨텍스트 및 과거 검색 기간을 이용할 수 있습니다.

모든 데이터에 대한 액세스

실시간 및 과거 인사이트

최대 SOC 속도 달성

Elastic Security를 SIEM으로 사용하여 운영 효율성 향상

보안 팀은 점점 더 많은 양의 데이터를 관리하고 있으며 모든 데이터를 신속하고 정확하게 검색, 분석 및 자동 탐지할 수 있어야 합니다. 효과적인 조사 작업, 검색, 위협 프로파일링 및 기존 보안 데이터, 클라우드 인프라, 애플리케이션 데이터 및 수년간의 과거 데이터에 대한 대응을 위해서는 즉각적인 상관 관계가 필요합니다.

보안 팀은 Elastic Security를 사용하여 통합 데이터에 액세스하고, 위협 및 비즈니스 컨텍스트를 사용하여 결과를 상황별로 파악하고, 기록 데이터를 사용하여 최적의 해결 경로를 신속하게 찾습니다. Elastic Security는 SIEM, 엔드포인트 보안, 위협 검색, 클라우드 모니터링, 부정 행위 탐지 및 기타 많은 사용 사례를 해결하므로 SOC는 검색 및 시각화 기능을 활용하여 위협 탐지, 예방 및 대응에 대한 통합된 접근 방법을 통해 조직을 보호할 수 있습니다.

Elastic Security으로 더 스마트하게 작업

종합적인 가시성 확보

Beats를 사용하여 Elastic Common Schema로 정규화된 데이터를 수집하고 보안 관련 데이터를 모두 인덱싱하여 조직 전체에서 데이터 사일로를 제거합니다. 직관적인 즉시 사용 가능한 대시보드와 상호 작용하고 Kibana, Lens 및 Canvas를 통해 사용자의 요구에 맞는 드래그 앤 드롭 사용자 지정 시각화를 개발합니다.

신속하게 보안 인사이트 확보

최적의 쿼리 성능과 가져오기 후 필드를 추가하거나 변경할 수 있는 유연성을 위해 쓰기 및 읽기 형식의 스키마를 모두 사용하여 데이터를 수집합니다. Elastic Stack이 알려진 속도로 몇 초 만에 대시보드에 결과를 가져옵니다. 우선 순위 상관 관계를 사용하여 경보 피로를 해소합니다.

다년간의 과거 데이터 포함

검색 가능한 스냅샷을 활용하여 탐지, 조사 컨텍스트, 위협 검색, 클라우드 모니터링 등에 필요한 만큼의 보안 데이터를 비용 효율적으로 활용할 수 있습니다. 체류 시간(개월 또는 심지어 년)으로 위반 범위를 지정합니다.

체류 시간 단축

Elastic의 내부 보안 연구 팀이 개발한 MITRE 매핑 즉시 탐지 및 강력하고 직관적인 EQL(Event Query Language)을 활용하여 지능적 위협의 도구, 전술 및 절차를 탐지하는 상관 관계를 수행하는 사용자 지정 탐지를 통해 탐지를 자동화합니다.

악의적인 비정상적인 활동 찾기

감독되지 않은 머신 러닝 작업을 타임스탬프가 있는 데이터 소스에 적용하여 잠재적 위협을 구성하는 독립 실행형 이상 징후 또는 관련 이상을 식별합니다. 감독 및 비지도 머신 러닝을 결합하여 거짓 양성률이 낮은 도메인 생성 알고리듬(DGA)과 같은 방법을 탐지합니다.

SecOps 워크플로우 간소화

Elastic Security의 대화형 작업 공간을 사용하여 위협을 탐지 및 대응하고 이벤트를 추적하며 직관적인 대화형 타임라인에서 증거를 수집합니다. 기본 제공 사례 관리 및 주요 SOA(Security Orchestration, Automation, Response) 및 워크플로우 벤더와의 통합을 활용하여 대응 및 해결 시간을 단축합니다.

최신 SOC 구현

Elastic Security는 전 세계 최신 보안 팀의 기술 기반 역할을 합니다. Elastic의 개방형 플랫폼 보안 접근 방식을 통해 통합의 용이성, 유연성 및 커뮤니티 중심의 기여와 협업을 활용하여 SOC 팀이 신속하고 효과적으로 의사 결정을 내릴 수 있습니다.

결론

보안 팀은 계속 확대되는 보안 환경으로부터 조직을 보호하므로 운영 효율성을 유지해야 하는 필요성을 간과해서는 안 됩니다. 모든 보안 관련 데이터와 과거 데이터에 액세스할 수 있는 비용 효율적인 방법을 통해 Elastic Security를 SIEM으로 구현함으로써 더 많은 사용 사례를 해결하고 SIEM 구축의 운영 가치를 전반적으로 높일 수 있습니다. 최고의 **보안 팀들이 Elastic Security를 SIEM으로 선택하고 있는 이유는 감지, 예방 및 대응에 대한 통합된 접근 방식이 필요하기 때문입니다.**

Elastic은 전체 환경에 걸쳐 신속하고 효율적으로 전체적인 가시성을 제공하여 문제를 파악하고 해결할 수 있도록 하며, 전체 하이브리드 환경에 걸쳐 클라우드 확장성을 제공하며, SOC가 분산된 팀의 방식 또는 현재 운영 중인 사일로 수에 관계없이 효율성을 극대화할 수 있도록 지원합니다. Elastic Security를 통해 SIEM에 대한 새로운 접근 방식을 통해 비즈니스를 지속적으로 보호하세요.

Elastic Security를 직접 사용해 보고 싶으신가요?

Elastic Cloud에서 Elastic Security를 사용해 보세요(14일 무료, 신용 카드 필요 없음).
또는 온프레미스로 배포하세요. 언제나 무료입니다.

무료로 Elastic Security 시작하기 ⟶

Search. Observe. Protect.

Elastic은 엔터프라이즈 검색, 통합 가시성, 보안을 위해 실시간으로 그리고 대규모로 데이터를 이용할 수 있게 해드립니다. Elastic 솔루션은 어디에서나 배포될 수 있는 단일한 무료 개방형 기술 스택을 기반으로 구축되어 문서 찾기에서부터 인프라 모니터링과 위협 헌팅에 이르기까지 모든 종류의 데이터에서 실행 가능한 인사이트를 즉시 찾아낼 수 있습니다. Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia, Verizon 같은 전 세계 수천 개의 기업이 Elastic을 이용해 업무상 중요한 시스템을 구동합니다. 2012년에 설립된 Elastic은 NYSE에 상장되어 기업 심볼 ESTC를 사용하고 있습니다. 보다 자세한 내용은 elastic.co/kr에서 확인하세요.

미주 본사
800 West El Camino Real, Suite 350, Mountain View, California 94040
일반 +1 650 458 2620, 영업 +1 650 458 2625

info@elastic.co