elastic

Elastic을 활용한 데이터 보안 규정 준수 지원

개요

사이버 공격이 더욱 빈번해지고 표적화되며 은밀하고 기술적으로 고도화됨에 따라, 사이버 보안 위협 환경이 점점 더 정교해지고 있습니다. 이에 따라 강력하고 포괄적인 데이터 보안의 필요성이 그 어느 때보다 중요해졌습니다. 사이버 보안과 관련된 법적 요구 사항과 잠재적 책임이 더욱 복잡하고 까다로워지고 있습니다. 이에 따라 보안에 대한 위험 기반 접근 방식이 절대적으로 필요합니다.

계속 늘어나는 보안 관련 규제 요구 사항을 준수하고, 잠재적으로 치명적인 비즈니스 중단을 방지하며, 보안 침해로 인한 비용이 많이 드는 소송의 위험을 줄이기 위해 기업은 총체적이고 전략적인 사이버 보안 접근 방식을 채택해야 합니다. 그렇게 하지 않으면 기업은 중대한 법적 및 재정적 결과에 노출될 뿐만 아니라, 회복할 수 없는 운영 및 평판상의 피해를 입을 수 있습니다.

이 백서는 조직이 Elastic을 사용하여 보안 의무를 충족하고 사이버 위협에 진정한 탄력적 방어를 구축할 수 있는 방법을 탐구합니다. Elastic의 강력하고 유연하며 확장 가능한 솔루션은 기업이 다음을 포함한 다양하고 복잡한 규정 준수 및 운영 사이버 보안 요구 사항을 충족하는 데 도움이 됩니다.

- 공격 표면 전반에서 데이터의 가시성과 검색 가능성 향상
- 규정 준수 요청을 위한 데이터 추출 간소화
- 위협 해결을 위한 간소화된 탐지 및 자동화
- 보안 상태 모니터링 및 시연
- 강화된 위협 인텔리전스

아래에서 법적 프레임워크 전반에 걸쳐 공통적으로 사용되는 기본 보안 개념에 대한 개요를 제공하고, 이러한 개념을 위험 기반의 준수 방식으로 구현하지 않을 경우의 잠재적 결과를 검토하며, 조직이 Elastic 플랫폼과 솔루션을 활용하여 준수 의무를 충족하고 보안 위험을 완화하는 방법을 확인해 보겠습니다.

참고: *이 백서는 정보 제공 목적으로만 제공되며 법률적인 조언을 구성하거나 대체하기 위한 것이 아닙니다. 구체적인 법률 조언은 법률 고문에게 문의하시기 바랍니다.*

기본 보안 원칙 및 관련 규정 준수 의무

현대의 보안 규정 준수 환경은 관할 지역별, 산업별, 데이터별 요구 사항이 복합적으로 얽혀 있는 구조입니다. 따라서 조직의 책임은 조직이 위치한 곳, 사업을 하는 곳, 처리하는 데이터와 그 방식, 해당 데이터의 민감도 및 사업의 성격에 따라 달라지게 됩니다.

예를 들어, 글로벌 금융 기관은 미국 연방 그램-리치-블라일리법('GLBA'), 뉴욕 금융서비스부('NYDFS') 사이버 보안 규정, EU 디지털 운영 복원력 법('DORA'), EU 네트워크 및 정보 보안 지침 2('NIS2 지침') 등 여러 법률을 동시에 적용받을 수 있습니다.

반면, 미국 본사의 상장 소매업체는 결제 카드 보안을 위한 PCI 데이터 보안 표준(PCI-DSS), 재무보고 시스템 보안을 위한 사베인스-옥슬리(SOX) 요건, 미국 주 정부의 유출 통지법 등 다양한 요구 사항을 적용받을 수 있습니다. 물론 개인정보 보호를 위한 개인정보 보호법과 정보 보안 요건도 잊지 말아야 합니다.

이러한 필수 요구 사항 외에도 많은 회사는 ISO 27001, SOC 2, NIST CSF 또는 UK Cyber Essentials와 같은 다양한 서드파티 보안 프레임워크에 대한 자발적인 인증을 유지합니다.

이러한 차이에도 불구하고 법률, 규제, 자율 규제, 산업 프레임워크와 일반 보안 모범 사례는 대체로 핵심 보안 원칙에 수렴합니다. 아래에서는 이러한 원칙의 주요 부분을 검토하고, 다양한 프레임워크에 맞춘 조정 방식을 예시를 들며 설명합니다.

데이터 인벤토리, 매핑 및 분류

우선 조직에서 보유한 데이터(데이터 인벤토리라는 프로세스), 데이터의 위치(데이터 매핑), 해당 데이터의 민감한 특성(데이터 분류)을 이해하지 않고는 조직이 위험 기반 보안 제어를 배포할 수 없습니다.

이러한 프로세스는 데이터 유출 사고 발생 시 기업이 영향을 받은 데이터가 법적, 규제적, 또는 계약상 데이터 유출 통지 의무를 발생시키는지를 더 잘 파악하는 데 매우 중요합니다. 이러한 이유로 데이터 인벤토리, 매핑 및 분류는 여러 프레임워크를 준수하기 위한 필수 요건이거나 해당 프레임워크 준수에 있어 명시적으로 요구되는 사항입니다. 그 예는 다음과 같습니다.

- *FTC 안전장치 규정*(16 CFR § 314)은 GLBA가 적용되는 특정 금융기관에 대한 요건을 시행하며, 적용 대상 금융기관이 위험 평가 과정의 일환으로 고객 정보의 민감도를 식별하고 평가할 것을 요구합니다.
- *HIPAA 보안* 규정(45 CFR § 164.308)은 이와 유사하게 전자 보호 건강 정보('ePHI')의 인벤토리 작성 및 보호를 의무화합니다.
- EU 일반 데이터 보호 규정('GDPR') 제30조에 따라 조직은 처리 활동 기록을 반드시 유지해야 하며, 준수를 입증하기 위해 데이터 목록과 매핑이 사실상 요구됩니다.
- 각 미국 주의 침해 통지 의무는 일반적으로 해당 주 거주자와 관련된 특정 유형의 민감한 개인 데이터가 손상된 경우에만 발동됩니다. 따라서 데이터 유출 사고 발생 시 기업은 유출된 데이터 세트에 어떤 범주의 데이터가 포함되는지 파악할 수 있어야 합니다.
- NIST SP 800-53 및 CIS Controls와 같은 프레임워크는 데이터의 민감도에 일치하는 보호 수준의 데이터 분류를 강조합니다. 명확한 인벤토리 및 분류 체계를 구축함으로써 기업은 접근 제어를 더욱 확실하게 구현하고, 민감한 데이터 흐름을 모니터링하며, 규제 의무를 준수하고, 무단 정보 유출 위험을 줄일 수 있습니다.

역할 기반 액세스 제어

역할 기반 액세스 제어('RBAC')는 개인이 자신의 책임을 수행하는 데 필요한 시스템과 데이터에만 액세스할 수 있도록 설계된 조치입니다(일명 '최소 권한' 개념). RBAC를 지속적으로 적용하면 악의적인 내부자의 무단 액세스 위험을 줄이고 침입 범위를 제한하는 데 도움이 됩니다. 많은 법률 및 산업 프레임워크에서는 RBAC를 명시적으로 요구하거나 강력히 권장합니다.

- EU GDPR에 따라 정당한 권한을 가지고 알 필요가 있는 개인만 개인 데이터에 접근할 수 있습니다. 더 나아가, 해당 규정은 무단 접근을 데이터 유출로 정의합니다.
- 매사추세츠 개인정보 보호 기준(201 CMR 17.04)은 매사추세츠에서 사업을 운영하는 기업이 업무 수행에 필요한 직원에게만 민감한 개인정보를 포함한 기록 및 파일에 접근할 수 있도록 안전한 접근 제어 조치를 구현하도록 요구합니다.
- HIPAA 보안 규정은 ePHI에 대한 접근을 정당하게 알 필요가 있는 사람으로 제한할 것을 요구합니다.
- EU DORA 제9조 (4)항은 해당 금융 기관이 자산에 대한 물리적 또는 논리적 액세스를 정당하고 승인된 기능 및 활동에 필요한 범위로 제한하는 정책을 구현할 것을 요구합니다.
- NIST SP 800-53, ISO/IEC 27001, CIS Controls(예: CIS Control 6)와 같은 업계 표준에서도 RBAC를 기본적인 액세스 관리 관행으로 강조합니다.

로깅 및 모니터링

보안 이벤트 로그는 기업이 보안 사고를 탐지하는 데 필요한 가장 중요한 리소스 중 하나입니다. 액세스 날짜 및 시간, 수행한 작업, 해당 작업을 수행한 사용자 등의 정보를 반영하는 로그는 시스템 액세스가 승인되었는지 확인하고 잠재적인 무단 활동을 조사하는 데 필수적입니다. 실시간 또는 거의 실시간으로 로그를 모니터링하는 것도 위협을 적시에 탐지하고 해결하는 데 중요합니다.

하지만 복잡하고 다양한 시스템을 보유하고 있어 매일 대량의 로그를 생성하는 조직의 경우 로그 관리가 어려운 과제가 될 수 있습니다. 이러한 조직은 기술 솔루션에 의지하여 로그를 효과적으로 수집하고 이상 활동을 모니터링해야 합니다. 법률 및 산업 프레임워크는 로깅 및 모니터링의 중요성을 강조합니다.

- 결제 카드 산업 데이터 보안 표준(PCI-DSS)은 결제 카드 데이터를 저장, 전송 또는 처리하는 모든 회사가 시스템 구성 요소 및 카드 소유자 데이터에 대한 모든 접근을 로그하고 모니터링할 것을 요구합니다.
- HIPAA 보안 규정은 ePHI가 포함된 시스템에서 활동을 기록하고 검사하기 위한 감사 통제를 의무화합니다.
- SOX법 404조는 경영진과 감사인이 상장 기업의 재무 보고에 대한 내부 통제의 효과성을 평가하고 보고할 것을 요구합니다. 해당 감사인은 COBIT과 같은 프레임워크에 따라 사용자 활동의 감사 로깅, 재무 시스템에 대한 액세스 및 재무 데이터 변경을 요구하는 제어를 평가합니다.
- NIST CSF의 '탐지' 구성 요소는 기업이 보안 이벤트를 로그하고 지속적인 보안 모니터링을 유지관리할 것을 규정하고 있으며, 이는 EU GDPR 제32조, EU NIS2 제23조 또는 EU DORA 제19조에 따라 통보해야 하는 사고의 적시 보고에도 필수적입니다.

침입 탐지 및 대응

안타깝게도 오늘날의 위협 환경에서 모든 조직은 사이버 공격의 잠재적 표적입니다. 조직은 불가피하게 침입 시도가 발생하는 경우, 보안 사고에 대응하기 위한 침입 탐지 시스템과 프로세스를 반드시 유지관리해야 합니다. 이러한 시스템은 기업에서 공격이 심각한 사고로 번지기 전에 신속히 식별하고 대응할 수 있도록 하는 데 매우 중요합니다. 하지만 침입 탐지 시스템과 인시던트 대응 프로세스는 기본적으로 즉효성이 떨어집니다. 그보다 기업은 활동의 기준선을 설정하고 기업의 고유한 속성에 맞추어 경보 기준을 조정해야 합니다. 이러한 조정은 경고의 정확성을 높이고, 사고를 적절히 분류하여 그 중요성에 따라 처리하는 데 도움이 됩니다. 침입 탐지 및 대응은 수많은 법률 및 산업 프레임워크의 핵심입니다.

- 미국 연방, 주 및 국제 데이터 유출 통지법은 데이터 유출 발생 시 특정 기간 내에 보고할 것을 요구합니다. 흔히 가장 빠른 보고 시간을 요구하는 것이 GDPR이라고 생각하지만(보고 대상 데이터 침해가 발생했다고 확인된 후 72시간 이내), DORA에서는 주요 정보 통신 기술('ICT') 관련 사고는 발견 후 4시간 이내에 보고하도록 규정하고 있다는 점에 유의할 필요가 있습니다.
- NYDFS 사이버 보안 규정 500.16조는 규제 대상 기관이 사이버 보안 인시던트에 신속하게 대응하고 복구할 수 있는 인시던트 대응 계획을 갖출 것을 요구합니다.
- 또한 DORA는 규제 대상 금융 기관에 상세한 인시던트 대응 계획을 개발하도록 요구합니다.
- NIST CSF는 기업이 보안 사고를 탐지하고 대응하기 위해 상세한 '탐지' 및 '대응' 통제를 유지관리해야 한다고 명시합니다.

규정 미준수로 인한 비용

규정을 준수하고 효과적인 보안 통제를 시행하지 못하면 기업, 경영진 및 이사회가 상당한 법적, 재정적, 평판상의 위험에 노출될 수 있습니다. 실용적인 관점에서 볼 때, 비효율적인 모니터링 도구나 프로세스를 가진 조직은 장기적인 무단 액세스 위험에 처하게 됩니다. 이에 따라 공격자는 회사를 정찰하여 인증된 활동을 더 면밀하게 모방하는 동시에 데이터를 유출하거나 랜섬웨어 공격의 기반을 마련할 수 있습니다. 또한 불완전한 로깅은 의심스럽거나 예상치 못한 활동이 승인되었는지 확인하는 것을 불가능하게 만들어 과다하거나 불충분한 알림으로 이어질 수 있습니다.

데이터 침해 또는 사이버 보안 사고가 발생할 경우, 부적절한 데이터 매핑 및 인벤토리는 영향을 받은 데이터를 식별하는 데 어려움을 초래할 수 있습니다. 이로 인해 영향을 받는 당사자 및 규제 기관에 대한 통지가 지연될 수 있습니다. 이러한 지연은 결과적으로 피해자가 입을 수 있는 잠재적 피해를 증가시키고, 규제 기관의 보고 기한을 위반하며, 추가적인 손해 배상 청구, 규제 기관의 제재, 추가적인 집행 및 소송 비용으로 복구 및 시정 조치로 인한 즉각적인 부담을 가중시킵니다. 비즈니스 간 공급업체의 경우, 사고로 인해 영향을 받은 고객을 파악하기가 더 어려울 수 있습니다.

개인 정보를 보호하기 위한 개인정보 보호법에서 요구하는 긍정적 보안 요건을 준수하지 않을 경우, 상당한 벌금 및 기타 법적 책임으로 이어질 수 있습니다. 또한 모든 기업은 정보 유출 사고로 인한 과실, 계약 위반 또는 기타 소송(종종 집단 소송)의 위험에 직면합니다. 특히, 캘리포니아 소비자 개인정보보호법(CCPA)은 회사가 '합리적인' 보안 조치를 유지관리하지 못하여 민감한 데이터를 침해당한 원고의 사적 소송권을 인정합니다. HIPAA, CCPA, EU GDPR 같은 규정에 따른 제재 및 손해배상은 순식간에 엄청난 배상금으로 이어질 수 있습니다.

직접적인 법규 위반 벌금 외에도, 부실한 보안으로 인한 평판 손상도 심각할 수 있습니다. 데이터 유출 사고를 겪거나 보안 규정을 준수하지 못한 기업은 고객 신뢰를 잃고, 대중의 비난에 직면하며, 사업 운영에 심각한 차질이 생겨 브랜드 가치에 장기적인 악영향을 받을 수 있습니다. 상장 기업도 보안 사고가 널리 알려지는 경우 주가가 영향을 받을 위험이 있습니다. 위험 요소에 고객 이탈 및 고객 데이터를 적절하게 보호하지 못한 것에 대한 요구가 포함될 수 있어 비즈니스 및 수익 손실로 이어질 수 있습니다. 이렇게 심각한 결과를 고려할 때, 기업은 규정 준수 의무에 적절하게 투자하고 보안 위험을 줄여 보안을 심각하게 생각해야 합니다.

규정 준수를 위한 Elastic 활용

Elasticsearch Platform은 Elastic의 즉시 사용 가능한 두 가지 솔루션인 Elastic Observability와 Elastic Security의 기반이 되는 플랫폼입니다. 조직은 Elastic의 개방적이고 유연한 플랫폼을 사용하여 규정 준수 의무를 충족하고 다양한 채널을 통해 주요 사이버 보안 위험에 대응할 수 있습니다. 가장 중요한 것은 Elastic 솔루션은 본질적으로 민첩성과 확장성이 뛰어나며, 다양한 시스템과 플랫폼에 배포하여 데이터를 수집할 수 있고 수많은 사용 사례에 검색 기능을 활용할 수 있다는 점입니다. 다음은 Elastic을 활용하여 보안 프로그램의 핵심 원칙을 지원하는 몇 가지 예시입니다.

데이터 매핑 및 분류

Elastic은 환경 전반에서 정형 및 비정형 데이터를 색인하여 데이터 매핑 작업을 지원함으로써 조직이 데이터의 유형과 위치에 대한 중앙 집중식 가시성을 확보할 수 있도록 지원합니다. Elastic은 사용자 정의 태그, 메타데이터 및 머신 러닝을 사용하여 데이터(예: 개인 데이터, 금융 기록, 시스템 로그)의 패턴을 식별하는 데 도움이 되므로 민감도 또는 규제 의무에 따라 데이터를 더욱 쉽게 분류할 수 있습니다. Elastic은 데이터 분류 전용 엔진은 아니지만, 더 광범위한 데이터 거버넌스 프로그램에 강력한 검색 및 분석 기능을 연동할 수 있으며, 이를 통해 클라우드 및 온프레미스 시스템 전반에 걸쳐 데이터를 추적 및 목록화할 수 있습니다.

역할 기반 액세스 제어(RBAC)

Elastic은 RBAC 도구는 아니지만, 플랫폼이 조직의 시스템 전반에서 로그를 인제스트하여 권한 관리의 격차를 파악하는 데 도움을 줄 수 있습니다. 조직은 접근 패턴을 분석하여 사용자 그룹이 접근해야 할 시스템과 그렇지 않은 시스템을 파악하고, 이를 바탕으로 접근 권한을 할당할 수 있습니다. 또한 Elastic은 고객이 시스템 전반에서 그룹 액세스 정책을 인제스트하는 것을 지원하기 때문에 기업이 감사 또는 규정 준수 조사에서 액세스 권한의 시행을 입증할 수 있도록 해당 데이터에서 보고서를 생성하는 것이 가능합니다. 또한 Elastic은 Elastic Security와 Kibana 인터페이스에 기본 제공 RBAC 기능을 포함하고 있습니다. 관리자가 사용자 액세스를 특정 인덱스, 대시보드 또는 작업(예: 보기 vs 편집)으로 제한하는 역할을 정의할 수 있기 때문에 최소 권한 액세스 원칙을 지원합니다.

로깅 및 모니터링

Elastic의 핵심 강점 중 하나이자 가장 일반적인 사용 사례는 대규모 로그 집계, 저장 및 분석에 있습니다. 기업은 Elastic Agent를 사용하여 엔드포인트, 서버, 클라우드 서비스, 애플리케이션에서 로그를 수집할 수 있습니다. 이러한 로그는 Elasticsearch에서 색인되어 Kibana에서 실시간으로 분석 및 시각화할 수 있습니다. Elastic은 장기 로그 보존, 알림, 이상 징후 탐색을 지원하므로 이상적인 로그 집계 및 보안 모니터링 솔루션이자 효과적인 규정 준수 보고 도구입니다. 또한 통합 가시성 제품군은 종합적인 인프라 가시성을 위한 애플리케이션 성능 모니터링(APM), 메트릭, 가동 시간 모니터링도 제공합니다.

미국 연방 정부 기관에 적용되는 M-21-31과 같은 여러 규정은 조직이 정해진 기간 동안 로그를 저장할 것을 요구합니다. Elastic의 데이터 계층화 구조를 통해 데이터를 액세스 및 사용 빈도 및 속도에 따라 비용 효율적으로 저장할 수 있습니다. Elasticsearch logsdb 인덱스 모드는 로그 데이터의 **저장 공간을최대 65%까지 줄여주며,** 모든 데이터를 분석에 즉시 액세스할 수 있도록 유지하면서 가시성과 규정 준수를 향상시킵니다.

한 가지 예를 들자면, University of York는 사이버 보안 기능 강화, 운영 효율성 향상, 비용 절감을 위해 보안 정보 및 이벤트 관리(SIEM) 시스템을 Elastic Security로 전환했습니다. 서버, 데스크톱, 노트북에 약 9,000개의 Elastic 에이전트를 배포하고 Google Cloud, AWS, Azure, 온프레미스 서버를 포함한 대학의 하이브리드 클라우드 인프라 전반에서 로그를 수집하여 대학이 하루에 500기가바이트의 데이터를 인제스트하고 35테라바이트의 로그를 저장소에 저장합니다. 또한 Palo Alto Networks 방화벽, Cloudflare, Duo 같은 보안 도구와 연결하여 다양한 플랫폼에 포괄적인 모니터링이 보장됩니다. 이 설정을 사용하면 방대한 양의 데이터를 신속하게 검색할 수 있어 쿼리 시간이 몇 시간에서 몇 초로 단축됩니다.

침입 탐지 및 대응

Elastic Security에는 엔드포인트 위협 탐색 및 대응(EDR) 기능이 포함되어 있으며, 위협 인텔리전스 피드가 통합되어 침입 탐지를 지원합니다. 이 기능을 통해 보안 팀은 행동 분석, 공격 매핑 및 사용자 지정 탐지 규칙을 사용하여 알려진 위협과 알려지지 않은 위협을 모니터링할 수 있습니다. 분석가들은 중앙화된 로깅을 통해 시스템 전반에서 이벤트를 신속하게 상호 연관시키고, 컨텍스트에 따라 알림을 조사하며, 응답 워크플로우를 오케스트레이션할 수 있습니다. Elastic은 타사 보안 오케스트레이션, 자동화 및 응답(SOAR) 플랫폼과의 통합을 통해 자동화된 응답을 지원하며, 이는 인시던트 대응 준비와 위협 헌팅을 개선하는 강력한 도구입니다. 이러한 고급 기능은 침해 가능성을 줄이고 성공적인 침입 시 응답 시간을 단축하며, 결과적으로 사고와 관련된 잠재적인 법적 책임을 완화합니다.

AHEAD는 선도적인 디지털 플랫폼이자 변혁 제공업체로서 Elastic Security를 관리형 보안 서비스에 통합하여 침입 탐지 및 대응 능력을 크게 강화했습니다. 현재 AHEAD는 클라이언트 보안 데이터를 Elastic Cloud에서 실행되는 Elastic에 인제스트하며, 데이터를 풍부하게 수집하고 위협 인텔리전스 피드와 연결합니다. 또한 Elastic은 조직 SOAR 시스템의 데이터 소스이기도 합니다. AHEAD 보안 분석가들은 보안 이벤트 내 관련 정보를 강조하는 AI 기반 경보를 활용해 방대한 데이터를 수동으로 선별하는 시간을 줄이고 오탐 부담을 줄일 수 있도록 돕습니다.

결론

사이버 보안 위협 환경이 조직에 점점 더 복잡한 문제를 제기함에 따라, 끊임없이 확대되는 보안 및 데이터 개인정보 보호 관련 규제 요건을 준수하고 위험을 줄이는 것 또한 더욱 복잡해지고 있습니다. 그렇게 하지 않으면 기업은 중대한 법적 및 재정적 결과에 노출될 뿐만 아니라, 운영 및 평판상의 피해를 입을 수 있습니다. Elastic은 특히 데이터 매핑 및 분류, RBAC, 로깅 및 모니터링, 침입 탐지 및 대응 영역에서 CIO와 CISO가 조직의 이러한 다양한 법적 요건 준수를 강화하는 데 도움이 됩니다.

