Elastic Cloud 정보 보안 개요

2023 년 10 월

elastic.co/kr

목차

서비스 및 범위

Elastic 은 Enterprise Search, Observability 및 Security 솔루션을 통해 사람들이 필요한 것을 더 빨리 찾고, 중요 업무용 애플리케이션을 원활하게 실행하고, 사이버 위협으로부터 보호할 수 있도록 지원합니다. Elastic Cloud 는 특정 사용 사례에 맞게 배포를 조정하고 관리할 수 있는 유연성을 제공하여, 복잡성을 제거하고 속도, 규모 및 정확도로 검색 경험을 강화하는 기본 플랫폼을 관리하도록 설계되었습니다.

Elastic 은 여러분의 데이터를 보호하면서 최고의 검색 경험을 제공하기 위해 Elastic 을 신뢰하는 고객 여러분에 대한 중요한 책임을 이해하고 있습니다. Elastic 은 여러분의 신뢰를 얻기 위해 부단히 노력하고 있습니다. 조직 최고위층의 이사회 감독과 경영진 거버넌스부터 모든 Elastic 직원을 온보딩하고 지속적으로 교육하는 방법에 이르기까지 보안은 Elastic 이 하는 모든 일에서 매우 중요합니다. Elastic 은 Elastic Cloud 서비스와 정보 보안 관리 시스템(ISMS)에 대해 광범위한 업계 최고의 규정 준수 보고서 및 인증 제품군을 획득했습니다. 이러한 보고서와 인증은 제품 개발 및 배포, 취약점 관리, 사고 관리, 위협 처리 프로세스를 포함한 Elastic 의 모든 활동에 효과적인 보안 관행이 내재되어 있다는 증거로 사용됩니다.

이 문서에서는 여러분이 Elastic Cloud 로 솔루션을 강화할 자격이 있다는 확신을 주기 위해 마련된 Elastic 의 정책, 절차 및 기술 제어에 대해 간략하게 설명합니다. Elastic Cloud 및 관련 소프트웨어 솔루션은 온프레미스, 퍼블릭 또는 프라이빗 클라우드, 하이브리드 환경에 배포되어 다양한 사용자 및 고객 요구 사항을 충족할 수 있습니다. 그러나 자체 관리형 배포에 대한 제어는 이 문서의 범위를 벗어납니다.

Elastic Cloud 개요

Elastic 은 고객 및 직원 검색 환경을 개선하고, 업무상 중요한 애플리케이션을 원활하게 실행하며, 사이버 위협으로부터 보호하는 클라우드 네이티브 엔터프라이즈 검색, Observability 및 보안 솔루션을 제공합니다. Elastic 제품은 검색, 분석, 시각화를 수행하기 위해 모든 소스와 형식의 데이터를 수집하고 저장합니다.

Elastic Cloud 는 Elasticsearch Service(ESS), Enterprise Search, Observability 및 Elastic Security 를 포함하는 서비스형 소프트웨어(SaaS) 제품군입니다. Elastic 은 Amazon Web Services(AWS), Google Cloud Platform(GCP), Microsoft Azure 및 IBM 을 포함한 여러 퍼블릭 클라우드 서비스 제공자의 고객이 선택한 인프라에서 Elasticsearch 와 Kibana 를 포함한 Elastic Stack 구성 요소를 호스팅하고 관리합니다. Elastic Cloud 제품에는 보안, 경보, 모니터링, 보고, 머신 러닝, 시각화 기능과 같은 고급 Elastic Stack 기능이 포함되어 있습니다.

Elastic Cloud 의 구성 요소에 대한 자세한 내용은 다음과 같습니다.

Elastic Cloud 구성 요소	**구성 요소 설명**
Elasticsearch Service(ESS)	ESS 는 텍스트, 숫자, 위치 기반 정보, 정형 및 비정형 데이터를 포함한 모든 데이터 유형을 위한 분산형 실시간 검색 및 분석 엔진이자 데이터 저장소입니다.
Enterprise Search	Elastic Enterprise Search 는 원활하게 확장하면서 검색 경험을 신속하게 제공할 수 있는 강력한 도구를 제공합니다. **Workplace Search** 는 조직의 콘텐츠 플랫폼(Google Drive, Slack, Salesforce 등)을 개인 맞춤화되고 자연스러운 검색 환경으로 통합하는 도구입니다. **App Search** 는 개발자가 Elasticsearch 의 강력한 기능을 활용하여 웹 크롤러, 개선된 API, 직관적인 대시보드 및 조정 가능한 정확도 제어 기능을 갖춘 모바일 및 SaaS 앱에 검색을 추가할 수 있는 도구 상자입니다. **Site Search** 를 사용하면 필요한 경우 검색 상자를 포함하여 웹사이트에 강력한 검색 기능을 추가할 수 있습니다.

Observability	Elastic Observability 는 로그, 메트릭, 애플리케이션 성능, 가동 시간 모니터링 정보에 대한 통합 분석을 지원합니다. 데이터 수집을 위해 Elastic Agent 와 사전 구축된 통합 커넥터를 사용하면 조직은 DevOps 및 SecOps 팀을 모두 지원하는 머신 러닝 및 기본 탐지 규칙을 통해 이상값을 표면화할 수 있습니다.
Security	Elastic Security 는 단일 사용자 인터페이스를 통해 위협 예방, 탐지 및 대응을 지원합니다. **Elastic SIEM** 은 기존의 로그 집계 및 상관 관계를 제공하여 위협 탐지 및 대응을 지원할 뿐만 아니라 머신 러닝을 통한 위험 평가, 통합 사례 관리, SOAR 과 같은 고급 보안 기능도 제공합니다. **Elastic Agent** 는 하이브리드 환경을 포함하여 거의 모든 곳에서 작동하는 작은 설치 공간으로 무한한 다양성을 제공합니다. 위협을 예방하고, 데이터를 전달하고, 다양한 사용 사례를 지원하여 보안 정보와 보호를 강화할 수 있습니다. **Limitless XDR** 은 보안 운영을 현대화하여 SIEM 과 엔드포인트 보안을 통합하고, 수년간의 데이터에 대한 분석을 지원하고, 탐지 및 대응 프로세스를 자동화하고, 모든 호스트에 기본 엔드포인트 보호 기능을 제공합니다.

클라우드 규정 준수 프로그램

Elastic Cloud 는 보안을 핵심으로 설계되었습니다. Elastic 은 보안, 규정 준수, 개인 정보 보호 및 신뢰성에 대한 Elastic 의 약속을 입증하는 업계 최고의 인증 및 증명 보고서를 획득하고 유지하고 있습니다.

Elastic 의 글로벌 ISMS 는 ISO 27001 에 대해 인증을 받았으며 Elastic Cloud 상용 서비스는 ISO 27017, ISO 27018, SOC 2 Type 2, CSA Cloud 규정 준수 매트릭스(CCM), HIPAA 및 PCI-DSS 에 대해 감사 또는 인증을 받았습니다. Elastic 은 또한 침투 테스트 요약뿐만 아니라 산업 및 지역별 인증(예: TISAX)도 제공합니다. Elastic 가 평가받는 규정 준수 기준과 보고서 및 인증 사본을 얻는 방법에 대한 자세한 내용은 이 문서의 규정 준수 기준 섹션을 참조하세요.

또한 Elastic Cloud 는 AWS GovCloud 의 Moderate Impact Level 에서 FedRAMP 인증을 받았습니다. 인증 세부정보를 검토하려면 FedRAMP 승인 클라우드 서비스 페이지를 방문하세요. 관련 정부 고객 및 잠재 고객은 FedRAMP 패키지 액세스 요청 양식을 사용하여 FedRAMP 마켓플레이스를 통해 FedRAMP 보안 패키지에 액세스할 수 있습니다.

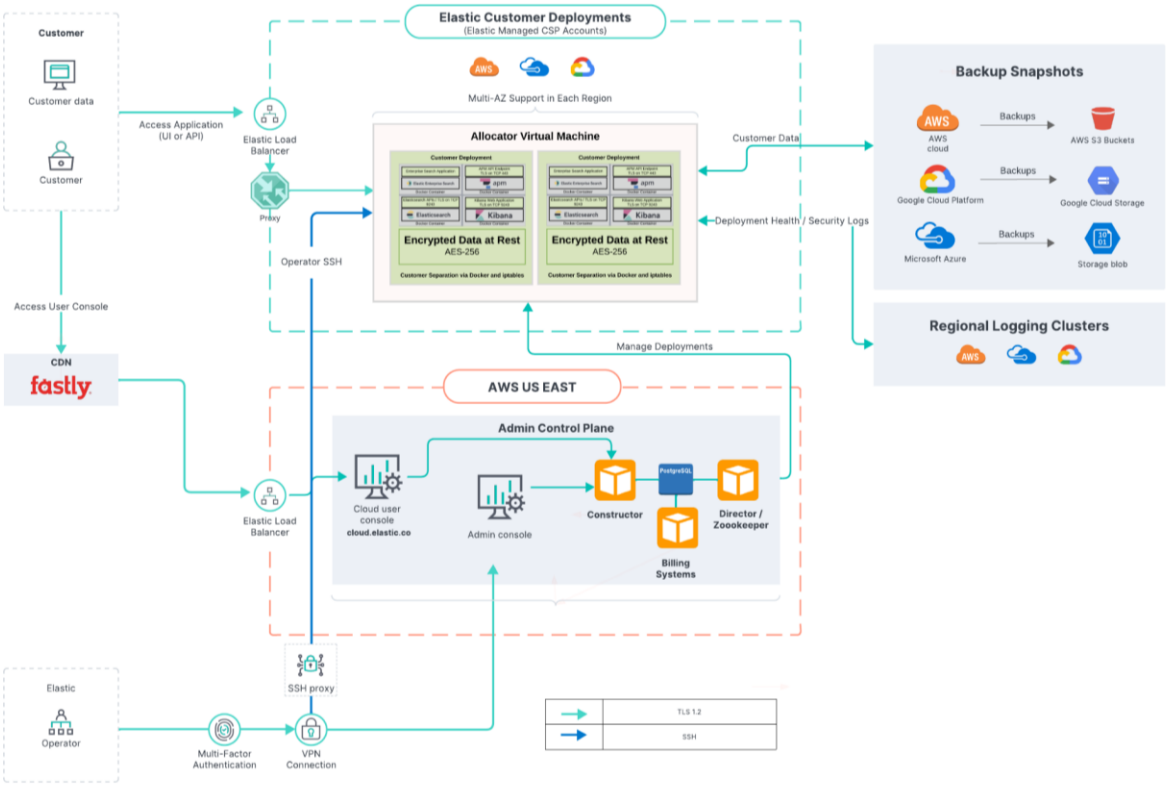
제품 사용 데이터 및 고객 콘텐츠

Elastic 은 고객의 정보를 최대한 신중하게 취급합니다. 이 문서 전반에 걸쳐 설명된 보호 조치는 고객 콘텐츠를 보호하기 위해 마련되었습니다. 제품 사용 데이터와 고객 콘텐츠의 차이점은 아래에 자세히 설명되어 있습니다.

제품 사용 데이터: 이는 Elastic 이 제품 제공을 촉진하고, 인프라를 관리 및 모니터링하고, 지원을 제공하고, 제품 분석 및 개선을 위해 사용하는 데이터입니다. 제품 사용 데이터는 엄격하게 통제되고 보호되며, 이 데이터의 보안과 무결성을 테스트하는 내부 및 외부 평가를 받습니다. 그러나 이 문서는 고객 콘텐츠를 보호하기 위해 심층 방어를 배포하는 방법에 중점을 두고 있습니다.

고객 콘텐츠: 이는 고객이 Elastic 의 제품 및 서비스에 수집, 업로드 또는 제출하는 데이터입니다. Elastic 은 제품이나 서비스를 제공하는 데 필요한 경우와 법률을 준수하는 데 필요한 경우에만 이 데이터를 처리합니다. 고객은 Elastic Cloud 에 어떤 데이터를 수집할지 항상 완벽하게 제어할 수 있습니다.

Elastic Cloud 서비스 다이어그램



Elastic Cloud 아키텍처 설명

컨트롤 플레인

Elastic Cloud 의 컨트롤 플레인에는 **ZooKeeper, Director** 및 **Constructor** 관리 서비스가 포함되어 있으며 아래에 자세히 설명되어 있습니다.

- **ZooKeeper** - ZooKeeper 는 프록시 라우팅 테이블, 할당자가 광고하는 메모리 용량, 관리 콘솔을 통해 커밋된 변경 사항 등 Elastic Cloud 구성 요소에 대한 필수 정보를 보관하는 분산 데이터 저장소입니다. 이는 서비스 간 통신을 위한 메시지 버스 역할을 합니다. 또한 Elastic Cloud 설치 상태와 Elastic Cloud 에서 실행 중인 모든 배포 상태도 저장합니다.

- **Director** - Director 는 ZooKeeper 데이터 저장소를 관리하고 ZooKeeper 와 통신하려는 내부 클라이언트에 대한 인증서 서명 요청(CSR)에 서명합니다. 또한 ZooKeeper 가 통신에 사용하는 STunnels 를 유지 관리하고 새 ZooKeeper 노드가 생성될 때 쿼럼을 설정합니다.

- **Constructor** - Constructor 는 관리 콘솔의 요청을 모니터링하는 스케줄러처럼 작동합니다. 변경해야 할 사항을 결정하고 할당자가 모니터링하는 ZooKeeper 노드에 변경 사항을 기록합니다. 또한 클러스터 노드를 할당자에 할당하고 기본 할당자의 활용도를 최대화하여 새 배포를 위해 추가 하드웨어를 가동할 필요성을 줄입니다. Constructor 는 클러스터 노드와 인스턴스를 다양한 가용성 영역 내에 배치하여 배포가 영역 오류를 견딜 수 있도록 합니다.

이러한 배치 기본 설정은 데이터 주권 요건에 맞게 사용자 정의할 수 있습니다.

- **클라우드 UI 및 API** - 이러한 기능은 관리자가 설치를 관리하고 모니터링할 수 있는 웹 및 API 액세스를 제공합니다.

프록시

프록시는 사용자 요청을 처리하고 컨테이너에 대한 요청 URL 로 전달된 배포 ID 를 실제 Elasticsearch 클러스터 노드 및 기타 인스턴스에 매핑합니다. 배포 ID 와 컨테이너의 연결은 프록시에 의해 캐시된 ZooKeeper 에 저장됩니다. ZooKeeper 가동 중단 시간이 발생하는 경우, 플랫폼은 캐시를 사용하여 기존 배포에 대한 요청을 계속 처리할 수 있습니다.

또한 가용성이 높은 Elasticsearch 클러스터가 있는 경우 영역의 상태와 가용성을 추적합니다. 영역 중 하나가 다운되면 프록시는 해당 영역으로 요청을 라우팅하지 않습니다. 또한 가동 중단 시간 없는 확장 및 업그레이드에 도움이 됩니다. 업그레이드를 수행하기 전에 스냅샷이 생성되고 데이터가 새 노드로 마이그레이션됩니다. 마이그레이션이 완료되면 프록시는 트래픽을 새 노드로 전환하고 이전 노드의 연결을 끊습니다. 일반적으로 시스템을 계속 사용할 수 있도록 로드 밸런서 뒤에 여러 프록시가 구성됩니다.

할당자

할당자는 Elasticsearch 노드와 Kibana 인스턴스를 호스팅하는 모든 시스템에서 실행됩니다. 다음을 통해 클러스터 노드의 수명 주기를 제어합니다.

- 요청 시 새 컨테이너 생성 및 Elasticsearch 노드 시작
- 응답하지 않는 경우 노드 다시 시작
- 더 이상 필요하지 않은 경우 노드 제거

또한 생성자가 배포할 위치에 대해 정보에 근거한 결정을 내릴 수 있도록 기본 호스트 시스템의 메모리 용량을 ZooKeeper 에 광고합니다.

위험 관리

Elastic 은 비즈니스에 대한 위험을 식별 및 평가하고 위험 완화 활동의 우선순위를 지정하기 위해 선도적인 정량적 위험 평가 및 분석 방법론인 FAIR 를 활용하여 보안 및 규정 준수에 대한 위험 기반 접근 방식을 채택했습니다.

Elastic 의 위험 평가 프로세스는 고객에게 믿을 수 있고 신뢰할 수 있는 서비스를 제공하는 능력에 영향을 미칠 수 있는 위험을 식별하고 관리합니다. Elastic 가 식별하고 통제에 중점을 두고 있는 주요 위험은 다음과 같습니다.

- 조직 관리
- 인적 자원 보안
- 자산 관리
- 액세스 제어
- 암호화
- 보안 통신
- 시스템 획득, 개발 및 유지 관리
- 공급업체 관계
- 정보 보안 사고 관리
- 비즈니스 연속성 관리

위험 식별 프로세스에서는 내외부 요인과 이들이 목표 달성에 미치는 영향을 모두 고려합니다.

식별된 위험은 비즈니스 목표와 관련하여 가능한 위협 및 취약점에 대한 분석과 위험의 잠재적 중요성을 추정하는 프로세스를 통해 분석됩니다.
위험 평가 프로세스에서는 위험을 관리하는 방법과 위험을 수용, 회피, 완화 또는 이전할지 여부를 고려합니다.
Elastic 은 식별된 위험에 대한 완화 전략을 결정합니다. 전략에는 통제의 설계, 개발 및 구현, 정책 및 절차의 채택 또는 개정이 포함될 수 있습니다.

집단적인 위험 식별, 분석 및 평가 프로세스는 FAIR 방법론을 사용하여 평가되고 Elastic 에 대한 예상 재정적 영향을 기준으로 순위가 매겨진 위험 시나리오인 리스크 등록부에 정보를 제공합니다. 리스크 등록부는 내외부 위험 요소, 비즈니스 우선 순위 및 진화하는 완화 전략의 변경 사항을 설명하기 위해 반년마다 재평가됩니다. 또한 이 프로세스는 정보 보안 팀이 이사회 감사 위원회에 보고할 때 위험 기반 접근 방식을 주도합니다.

거버넌스

정보 보안 관리 시스템(ISMS) 및 감독

Elastic 은 고객 및 회사 데이터를 보호하기 위해 함께 작동하는 정책, 절차, 운영 구조 및 기술 제어를 포함하는 ISMS 를 구현했습니다. ISMS 는 ISO 27001 에 대해 인증되었으며 거버넌스, 신뢰, 위험 및 취약점 관리, 보안 아키텍처 및 엔지니어링, 제품 보안, 위협 탐지 및 사고 대응을 포함한 모든 보안 및 규정 준수 영역을 포괄적으로 다루도록 구성되었습니다.

Elastic 이사회(감사 위원회)는 ISMS 에 대한 감독을 제공하고 최고 정보 보안 책임자(CISO)와 정기적으로 만나 정보 보안 프로그램이 비즈니스 목표와 목적에 맞춰 운영되고, 업계 모범 사례를 채택하고, 역동적인 위협 환경과 함께 진화하고 있는지 확인합니다.

Elastic ISMS 는 글로벌 데이터 법률 및 규정 준수를 보장하는 조직 솔루션에 대해 정보 보안 팀과 긴밀히 협력하는 전담 비즈니스 무결성 및 개인 정보 보호 팀으로 강화됩니다.

정보 보안 정책

Elastic 은 NIST 및 ISO 27001 을 포함한 업계 기준을 기반으로 정보 보안 관행을 관리하고 회사 전체에 관리 기대치를 전달하기 위한 포괄적인 정책 세트를 개발했습니다. 매년 정책 소유자는 모든 정보 보안 정책을 검토하고 경영진이 승인합니다. Elastic 의 정책은 다음 도메인을 다룹니다.

- 정보 보호 프로그램
- 허용되는 사용
- 위험 관리
- 자산 관리
- 데이터 분류
- 기록 보존
- 액세스 제어
- 워크스테이션 및 서버 보안
- 보안 분석 및 로깅
- 취약점 관리
- 변경 관리
- 보안 소프트웨어 개발
- 사고 대응
- 비즈니스 연속성 및 재해 복구

모든 Elastic 직원은 고용 시 그리고 이후 매년 Elastic 행동 규범과 정보 보안, 개인 정보 보호 및 허용 가능한 사용 정책을 검토하고 인정했음을 증명해야 합니다.

Elastic 은 정보 보안 정책의 전문을 외부와 공유하지 않습니다. 그러나 각 정책의 정기적인 검토, 업데이트 및 승인에 대한 증거와 함께 각 정책에서 다루는 도메인에 대한 명확성을 제공하기 위해 각 정책의 목차 및 버전 기록이 포함된 정보 보안 정책 번들이 제공됩니다. 이 문서의 사본을 원하시면 Elastic 계정 담당자나 Elastic 지원팀에 문의하세요.

공식적인 정책 외에도 Elastic 은 보다 구체적인 프로세스 요구 사항이 있거나 클라우드 암호화, 인증서 및 키 관리, 서드파티 위험 관리와 같이 지속적으로 발전하는 모범 사례가 있는 도메인에 대한 플레이북, 프로세스 문서 및 계획을 유지 관리합니다.

인사 관리

Elastic 은 포괄적인 보안 프로그램이 경영진의 강력한 목소리에서 시작되고 모든 Elastic 직원이 참여한다는 것을 알고 있습니다. Elastic 의 소스 코드, 직원 핸드북, 행동 규범에는 모든 Elastic 직원이 준수해야 하는 명시적인 지침과 윤리 기준이 포함되어 있습니다. Elastic 은 직위, 연공서열, 재직 기간에 상관없이 이러한 약속을 위반한 것으로 밝혀진 모든 사람에 대해 무관용 정책을 시행하고 있습니다.

Elastic 은 또한 공식적인 보고 라인을 통해 기업 수준의 보안 모범 사례를 확립했습니다. 이는 관련 직원에게 정보 흐름을 촉진하고 직원 행동 및 성과에 대한 적절한 책임과 감독을 보장합니다. 역할과 책임은 기능적 요구 사항에 따라 분리되며 직무 역할은 명시적으로 정의됩니다.

모든 채용 및 해고는 문서화된 정책 및 절차에 따라 수행되며, 여기에는 직원 및 계약자의 안전하고 신속한 온보딩 및 오프보딩 절차가 포함됩니다.

기타 기업 수준 보안 관행에는 입사 전 신규 채용 및 계약자에 대한 배경 조사 수행이 포함됩니다. 또한, 경영진과 고위 경영진을 포함한 모든 Elastic 직원은 보안 인식 교육을 이수하고 채용 시 및 이후 매년 정보 보안 및 개인 정보 보호 정책, 행동 규범, 직원 핸드북을 검토하고 인정해야 합니다.

자산 관리

자산 관리 기준은 자산 재고, 자산 소유권, 자산 반환 및 파기, 감사 추적 요구 사항을 포함하는 자산 관리 수명주기를 관리합니다. Fleet 관리와 엔드포인트 관리 간의 자산 관리 프로세스는 서로 다릅니다. 각각의 독립적인 프로세스는 아래에 설명되어 있습니다.

Fleet

Elastic 의 파트너인 클라우드 서비스 제공자(CSP), AWS, GCP, Azure 및 IBM 은 Elastic Cloud 를 지원하는 인프라를 관리합니다. Elastic Cloud 고객은 배포별로 데이터에 대한 기본 CSP 와 지리적 지역을 유연하게 선택할 수 있습니다. 물리적 보안, 미디어 및 하드웨어 제어는 CSP 의 책임입니다. Elastic 은 서드파티 위험 관리 프로그램의 일환으로 수행되는 서드파티 재인증 중에 파트너 클라우드 서비스 제공자의 미디어 및 하드웨어 수명주기 관리 제어의 설계 및 운영 효율성을 검토합니다.

Elastic Cluster 는 Elastic Observability 를 활용하여 성능 및 가동 시간 메트릭을 추적합니다. 중요한 자산은 자산 목록에 등록되며 자산 목록의 완전성과 정확성을 정기적으로 검토합니다.

직원 엔드포인트

Elastic IT 는 직원 엔드포인트를 중앙에서 추적하고 관리합니다. 장치 관리 소프트웨어는 기본적으로 활성화되어 있는 암호화, 비밀번호 관리, 세션 관리 및 화면 잠금을 포함한 보안 설정을 적용하는 데 사용됩니다. 이러한 설정은 로컬에서 비활성화하거나 수정할 수 없습니다. 엔드포인트는 EDR 기능과 실시간 모니터링 및 경보를 제공하는 Elastic Security 로 보호됩니다. 직원 엔드포인트를 Malware 로부터 보호하는 방법에 대한 자세한 내용은 Malware 보안 섹션을 참조하세요.

Elastic 에서 발급한 모든 장치는 장치 관리 수명 주기에 따라 처리됩니다. Elastic 직원이 해고되면 논리적 액세스가 비활성화되고 회사에서 관리하는 엔드포인트가 데이터 정리 및 폐기 절차를 수행하는 서드파티 프로세서로 직접 전송됩니다. Elastic 의 서드파티 파트너는 Elastic 노트북 처리 기준에 따라 기계의 폐기 및 재발급 또는 파기 인증서를 Elastic 에 제공합니다. Elastic IT 는 Elastic 관리 엔드포인트의 감사 추적을 유지하여 데이터 폐기 수명주기 내에서 각 장치의 상태를 추적합니다.

정책에 따라 관리되지 않거나 개인용 모바일 장치는 고객 데이터를 저장할 수 없으며 Elastic Cloud 의 개발 또는 지원에 사용되지 않습니다.

구성 관리

Elastic 은 코드를 통해 구성을 관리하며, 구성 변경은 승인, 동료 검토 및 승인, 자동화된 테스트 모음을 포함하는 기준 변경 관리 절차를 따릅니다. 파일 무결성 모니터링 및 의심스러운 활동 탐지를 통해 프로덕션 구성 파일에 대한 직접적인 변경 사항을 탄력적으로 모니터링합니다.

데이터 보호

데이터 분류 및 보관

Elastic 데이터 분류 기준에서는 민감도에 따라 데이터를 분류하고 각 분류에 대해 액세스 및 공유 제한을 정의하도록 요구합니다. 고객 콘텐츠 및 제품 사용 데이터는 가장 민감한 분류인 제한되는 데이터로 분류되며 이 데이터의 기밀성, 무결성 및 가용성을 보존하기 위해 고안된 가장 강력한 데이터 보호 기준의 적용을 받습니다. 고객 콘텐츠 및 제품 사용 데이터에 대한 정의는 이 문서의 제품 사용 데이터 및 고객 데이터 섹션을 참조하세요.

Elastic 기록 보존 기준은 데이터 유형과 운영, 계약, 법률 및 규제 요구 사항을 기반으로 정의된 보존 일정에 따라 데이터를 폐기하도록 요구합니다. 고객은 자신의 정보를 삭제하기 위해 언제든지 Elastic 지원에 계정 삭제 요청을 제출할 수 있습니다. 데이터 액세스 요청을 제출하는 방법에 대한 자세한 내용은 이 문서의 데이터 개인정보 보호 섹션을 참조하세요.

데이터 수집, 처리, 파기

데이터 수집(Data Collection)

Elastic 은 서비스를 제공, 지원, 유지, 보안 및 개선하는 데 필요한 정보만 수집합니다. 이 정보는 절대로 서드파티에게 판매되지 않습니다. 당사가 고객으로부터 수집하는 정보에 대한 자세한 내용은 Elastic 의 제품 개인정보 보호정책을 참조하세요.

데이터 수집(Data Ingestion)

Elastic 은 고객이 Elastic 배포에서 저장, 전송 또는 처리하기로 선택한 데이터를 제어하거나 액세스하지 않습니다. 고객의 Elastic 배포로 수집된 모든 데이터는 고객의 단독 재량에 따라 항상 통제됩니다.

데이터 폐기

Elastic 기록 보존 기준 및 자산 관리 기준은 데이터 폐기 요구 사항을 관리합니다. Elastic 의 클라우드 서비스 제공자 파트너는 호스팅 인프라에 대한 보안 삭제 및 데이터 폐기를 관리합니다. 고객은 Elastic 인스턴스에 저장한 콘텐츠에 대한 완전한 제어권을 가지며 언제든지 Elastic 인스턴스에서 콘텐츠를 제거하거나 삭제할 권리가 있습니다.

암호화

전송 중 암호화

Elastic Cloud 의 전송 중 암호화는 기본적으로 전송 계층 보안(TLS)을 통해 시행됩니다. 허용되는 최소 암호화 강도는 TLS 1.2 입니다. TLS(HTTPS) 연결은 Elastic Cloud Service 다이어그램에 표시됩니다.

Elastic Cloud 를 지원하는 데 사용되는 인증서는 Digicert 에서 제공되며 2048 비트 키로 RSA 공개 키 인증을 활용합니다. Elastic 은 클라우드 배포를 위한 유효한 인증서를 유지 관리하며 Qualys SSL Labs 에서 A+ 등급을 받았습니다. 이러한 테스트 결과는 SSL Labs 를 방문하여 재현할 수 있습니다.

휴면 암호화

Elastic 의 클라우드 서비스 제공자 파트너는 기본적으로 활성화되어 있는 저장 데이터 암호화를 제공합니다. Elastic 의 모든 클라우드 서비스 제공자는 NIST 지침(256 비트)에 따라 최소 키 길이를 제공합니다.

키 관리

암호화 키는 생성된 호스트를 떠나지 않으며 일회용으로 간주됩니다. 가상 머신 호스트가 생성되거나 교체될 때마다 자동으로 생성됩니다. 백업되거나 노출되거나 호스트를 떠나지 않습니다. 기본 IaaS 서비스의 암호화를 위한 키 관리는 공급자의 키 관리 서비스를 사용하여 자동화됩니다.

Elastic 서비스에 대한 키 관리는 코드형 인프라 및 적용 가능한 각 구성 요소 또는 서비스에 대한 운영 문서의 일부로 유지됩니다.

네트워크 및 기기 보안 관리

방화벽

Elastic 의 클라우드 서비스 제공자 파트너는 프로덕션 인프라를 위한 하드웨어 방화벽을 관리합니다. Elastic 은 또한 소프트웨어 방화벽을 유지 관리하여 인터넷에서 승인되지 않은 인바운드 트래픽을 필터링하고 들어오는 네트워크 연결 중 명시적으로 승인되지 않은 연결을 모두 거부합니다(거부하도록 기본 설정됨). 환경 내의 논리 영역 간에 추가 네트워크 분할 및 방화벽이 적용됩니다. 방화벽 규칙 세트는 최소한 반년마다 검토됩니다. 방화벽 규칙 변경은 기준 변경 관리 프로세스를 따르며 변경 관리 제어의 적용을 받습니다. 또한 방화벽에 대한 모든 액세스는 RBAC 를 사용하여 구현됩니다.

Elastic Cloud 고객은 트래픽 필터링 기능을 활용하거나 PrivateLink 를 구성하여 배포에 대한 트래픽을 추가로 제한할 수 있습니다.
IP 트래픽 필터 | Elasticsearch Service 설명서 | Elastic
AWS PrivateLink 트래픽 필터 | Elasticsearch Service 설명서 | Elastic

Malware 보안

중앙에서 관리되는 IT 구성을 통해 모든 직원 엔드포인트에서 Malware 방지 기능이 활성화됩니다. 로컬 관리자는 이러한 설정을 비활성화하거나 수정할 수 없습니다. Elastic Security Solution 은 정보 보안 검토 및 조치 알림 내에서 EDR 기능과 연중무휴 대기 팀을 제공합니다.

Elastic Security 는 Elastic Cloud 프로덕션 환경을 보호하는 데 활용됩니다. 시그니처와 행동 패턴은 자동으로 지속적으로 업데이트됩니다. 새로운 위협에 대해 탐지 기능을 신속하게 배포할 수 있으며 전담 위협 인텔리전스, 탐지 및 대응 팀이 가능한 Malware 감염에 대한 탐지, 분석, 대응 및 치료를 관리합니다.

시간 동기화

시간 동기화는 공통 시간 소스(NIST 서버)를 사용하는 NTP 를 통해 이루어집니다.

논리적 액세스

역할 기반 액세스 제어

Elastic 은 내부 사용자에게 액세스 권한을 제공할 때 최소 권한 원칙을 준수합니다. Elastic 직원에게는 자신의 직무에 필요한 액세스 수준만 부여됩니다. 직무 변경이나 사용자의 접근이 더 이상 필요하지 않은 기타 상황이 발생하는 경우 접근 권한은 정기적으로 검토되고 수정됩니다.

Elastic 제품에는 또한 역할 기반 액세스 제어 기능이 있어 고객이 Elastic 배포 및 Elastic Cloud 관리 플랫폼 내에서 사용자에 대한 세분화된 액세스 관리를 구현할 수 있습니다.

온보딩 및 종료

신입 사원에게는 중앙 집중식 ID 및 액세스 관리(IAM) 시스템의 사전 구성된 규칙을 기반으로 기업 클라우드 기반 SaaS 애플리케이션에 대한 액세스가 자동으로 프로비저닝됩니다. 자동 프로비저닝 규칙 세트는 감독 조직, 직무군, 직무 수준, 관리 구조 등 HR 기록 시스템의 직무 속성을 활용하여 해당 개별 사용자에게 필요한 특정 액세스 권한을 부여합니다. 이를 초과하는 액세스에는 티켓에 문서화된 공식 요청이 필요하며 관리 검토 및 승인이 필요합니다.

직원이 Elastic 내의 다른 직무 역할이나 조직으로 이동하는 경우, HR 기록 시스템 내의 직무 속성이 변경되면 자동으로 중앙 집중식 IAM 시스템 내에서 워크플로우가 시작되어 새 역할에 대한 적절한 액세스 권한으로 계정을 다시 프로비저닝하게 됩니다. 이전 역할의 액세스 권한은 프로비저닝 해제되고 새 역할의 작업 속성을 기반으로 새 액세스 권한이 프로비저닝됩니다.

해고 시 중앙 집중식 IAM 시스템을 통해 부여된 액세스는 HR 관리 시스템에서 고용 상태가 변경되면 자동으로 일시 중지됩니다. 이 유효성 검사는 하루에 여러 번 발생합니다.

프로덕션 액세스

제한된 수의 Elastic 직원에게 Elastic Cloud 프로덕션 환경에 대한 액세스 권한이 부여되었습니다. Elastic 은 플랫폼 관리, 유지 관리, 지원 목적으로 이러한 액세스 권한을 유지합니다. Elastic 데이터 처리 정책은 유지 관리 또는 문제 해결 시나리오에서도 Elastic 직원이 고객 데이터에 액세스하는 것을 명시적으로 금지합니다. 지원이나 문제 해결 목적으로 자발적으로 공유된 데이터를 Elastic 직원이 보기 전에 고객은 서면 동의를 해야 합니다. Elastic 은 Elastic Cloud 에 업로드되거나 수집된 고객 데이터를 사전에 확인하지 않습니다. 고객은 Elastic 과 공유하기 전에 데이터를 수정하거나 삭제하도록 선택할 수 있습니다.

또한 정보 보안 위협 탐지 및 대응 팀은 파일 무결성 모니터링 및 계정 탈취 또는 데이터 유출 메트릭을 포함하여 의심스러운 내부 계정 활동 및 무단 액세스에 대한 탐지 기능을 개발하고 구현했습니다. 이러한 탐지는 위협 탐지 및 대응에 의심스러운 활동을 알리고 분석가 조사를 시작하는 자동화된 워크플로우의 일부입니다.

사용자 액세스 검토

Elastic 은 최소 권한 원칙을 준수하며 각 직무 역할 수행에 필요한 액세스 권한만 부여합니다. 분기별 사용자 액세스 검토 중에 시스템 소유자 및 관리 검토 및 권한 있는 액세스를 포함한 사용자 액세스 권한을 다시 확인합니다. 더 이상 필요하지 않은 액세스 권한은 프로비저닝 해제됩니다.

변경 관리

변경 관리 기준은 변경 관리 프로세스를 관리하고 안전하고 관리되는 방식으로 프로덕션 환경에 대한 소프트웨어 및 인프라 변경의 개발 및 배포를 제어하도록 설계된 요구 사항을 설정합니다.

변경 관리 프로세스에서는 제안된 변경 사항이 통제된 방식으로 승인, 동료 검토, 테스트, 구현 및 릴리즈되고 제안된 각 변경의 상태가 문서화되고 모니터링되도록 보장합니다. 긴급 변경이 필요한 경우에도 문서화된 승인과 자동화된 테스트가 필요합니다. 긴급 변경에 대한 수동 검토도 필요하지만 구현 후에 발생할 수도 있습니다.

공급망 보안

프로덕션 환경에 대한 소프트웨어 배포는 자동화된 CI/CD 파이프라인을 통해 관리됩니다. 변경 사항은 각 리포지토리 내의 지정된 브랜치에 저장됩니다. 개발 브랜치는 활성 개발에 사용되며 기본 브랜치에는 프로덕션 준비 코드가 포함되어 있습니다. 변경 사항은 버전 관리되며 메인 브랜치에 병합하기 전에 보안 검사를 포함한 일련의 자동화된 테스트가 수행됩니다. 변경 사항이 기본 브랜치에 병합되도록 승인되기 전에 테스트 스위트를 통과해야 하는 브랜치 보호가 활성화됩니다. 변경 사항이 완전히 인증되면(테스트 및 보안 검사 통과, 동료 검토 및 승인 획득, 통합 검사 통과) 자동 배포 소프트웨어가 수동 개입 없이 변경 사항을 프로덕션에 적용합니다.

Elastic 의 소스 코드는 액세스가 제어되고 모니터링되는 버전 제어 시스템에 저장됩니다. 사용자 활동은 감사 기간 동안 캡처되며 예기치 않거나 의심스러운 수정 및 빌드 프로세스에 대해 경보하기 위한 탐지 기능이 마련되어 있습니다. 각 리포지토리 내에서 코드를 수정하는 기능은 직무 역할에 따라 제한됩니다.

보안 개발

SDLC

시스템 개발 수명 주기(SDLC)에 대한 보안 요구 사항은 보안 소프트웨어 개발 프레임워크에서 유지 관리됩니다. 이 프레임워크는 모든 Elastic 소프트웨어를 안전하게 설계, 개발, 배포, 추적 및 유지 관리하는 프로세스를 규정합니다. 또한 빌드 시스템을 보호하고 빌드 체인 손상 위험을 완화하기 위한 요구 사항도 포함되어 있습니다. 빌드 시스템에는 소프트웨어 제공 파이프라인, 패키지 레지스트리, 아티팩트 리포지토리, CI/CD 및 소스 코드 관리 시스템이 포함됩니다. 보안 소프트웨어 개발 프레임워크는 테스트용 및 비프로덕션 시스템에서 프로덕션 데이터를 사용하는 것을 금지합니다. 또한 프로덕션 환경과 비프로덕션 환경을 분리해야 합니다. 환경 세분화는 서드파티 침투 테스팅 중에 평가됩니다.

보안 설계 및 아키텍처

Elastic 소프트웨어 개발은 설계 및 아키텍처의 보안 모범 사례를 따라 "설계상 보안" 및 "기본적으로 보안"된 소프트웨어를 생성합니다.

보안 소프트웨어 개발 프레임워크는 다음을 포함하여 모든 설계가 따라야 하는 데이터 보호 요구 사항 및 보안 원칙을 간략하게 설명합니다.

- 기밀성 - 데이터는 전송 중 및 저장 시 무단 관찰 또는 공개로부터 보호됩니다.
- 무결성 - 데이터는 무단 생성, 변경 또는 삭제로부터 보호됩니다.
- 가용성 - 필요에 따라 승인된 사용자가 데이터를 사용할 수 있으며 정의된 가용성 SLA 를 충족합니다.
- 식별, 인증, 승인
- 부인 방지
- 감사 및 로깅
- 액세스 제어 및 최소 권한 원칙
- 보안 통신 및 암호화 기준
- 보안 기본값 및 오류 방지/실패 보안

위협 모델링 및 보안 아키텍처 검토도 소프트웨어 개발 프로세스의 일부로 설계에서 필수 보안 원칙을 고려했는지 확인합니다.

보안 코딩

SaaS 제공업체로서 Elastic 은 보안 코딩 관행의 중요성을 인식하고 있습니다. OWASP Top 10 및 CWE Top 25 와 같은 일반적인 코딩 취약점은 매년 관련 팀 및 개인에게 발행되는 보안 소프트웨어 개발 교육에서 해결됩니다. 소스 코드를 변경하려면 변경 사항을 병합하기 전에 변경 작성자가 아닌 한 명 이상의 검토자의 검토 및 승인(병합 요청을 통해)이 필요합니다. 변경 사항을 검토하여 변경 사항으로 인해 발생할 수 있는 잠재적인 보안 영향을 식별합니다. 또한 보안 코드 검토를 포함하는 독립적인 침투 테스팅은 일반적인 안전하지 않은 코딩 관행에 더욱 중점을 둡니다. 위협 모델링, 보안 검토 또는 소스 코드 검토 중에 식별된 모든 문제는 취약점 관리 기준에 따라 평가된 위험을 기반으로 추적, 평가 및 해결됩니다.

Elastic 은 또한 안전한 소프트웨어를 유지하고 고객을 취약점으로부터 보호하기 위한 노력의 일환으로 버그 포상금 프로그램을 후원합니다. 자세한 내용은 취약점 및 패치 관리 섹션의 취약점 공개 프로그램을 참조하세요.

오픈소스 및 서드파티 소프트웨어 검토

보안 소프트웨어 개발 프레임워크에서는 오픈 소스 및 서드파티 라이브러리의 코드 종속성을 식별하고 추적해야 합니다. 종속성 관리 소프트웨어는 취약한 종속성을 식별, 검색 및 해결하는 데 도움을 줍니다.

취약점 및 패치 관리

취약점 관리 기준은 취약점 관리 프로그램을 관리하고 Elastic 리소스 검색은 물론 취약점 분류, 분석, 교정 및 공개에 대한 요구 사항을 설정합니다. Elastic 은 취약점 스캔을 수행하고 Elastic Cloud 를 지원하는 인프라와 Elastic Cloud 구성 요소 자체에 패치를 적용합니다. 각각에 대한 프로세스는 아래에 자세히 설명되어 있습니다.

인프라 취약점 및 패치 관리

Elastic 은 상용 취약점 스캐너를 활용하여 지속적으로 자산을 스캔합니다. 모든 프로덕션 자산이 이러한 스캔에 포함됩니다. 서드파티 소프트웨어 공급업체는 지속적으로 규칙 세트를 업데이트합니다. 취약점의 심각도는 CVSS 등급을 기준으로 하며 패치 일정도 CVSS 등급과 일치합니다. 긴급 및 높음 취약점은 즉시 패치하거나 예정된 다음 릴리즈의 일부로 우선적으로 적용됩니다.

제품 취약점 및 패치 관리

Elastic 은 서드파티 침투 테스팅, 자동 및 수동 코드 스캔 및 검토, OSS 스캔, 세분화 테스팅, 취약점 공개 프로그램을 통해 제품의 보안 취약점을 엄격하게 테스트합니다. Elastic 제품에서 취약점이 발견되면 Elastic 은 취약점 관리 기준에 따라 이를 평가하여 심각도와 해결 계획을 결정합니다. 필요한 경우 Elastic Security Advisory(ESA)를 발행합니다. 이는 Elastic 제품의 보안 문제에 대해 Elastic 이 사용자에게 보내는 공지입니다. Elastic 은 요약, 교정 및 완화 세부 정보와 함께 CVE 및 ESA 식별자를 각 권고에 할당합니다 모든 새로운 권고 사항은 보안 공지 포럼에 발표됩니다.

취약점 관리 기준은 공개 공개에도 적용됩니다. 공개 프로세스에는 필요한 경우 새 제품 버전을 출시하고 자문 페이지에 공지하는 것이 포함됩니다. 취약점의 성격에 따라 개별 고객에게 연락하고, 블로그 게시물을 게시하고, CVE 를 MITRE 에 제출할 수도 있습니다.

고객은 RSS 피드를 통해 ESA 를 추적할 수 있습니다.

취약점 공개 프로그램

Elastic 은 보안 연구원들이 책임감 있게 내부 검토를 위해 취약점을 제출할 수 있는 공개 취약점 공개 프로그램을 후원하게 된 것을 자랑스럽게 생각합니다. Elastic 제품 보안 팀은 제출물을 검토하고, 위험 노출을 평가하고, 평가된 위험에 따라 수정합니다. 버그 바운티(Bug Bounty) 정책을 확인하거나 보고서를 제출하려면 HackerOne 의 Elastic Bug Bounty 프로그램을 방문하세요.

서드파티 위험 관리

서드파티 온보딩

하위 프로세서를 포함한 모든 서드파티는 철저한 접수 및 검토 과정을 거칩니다. 각 공급업체의 위험 프로필은 제공하는 서비스, 처리할 데이터 유형, 내부 시스템에 대한 액세스 수준, 공급업체의 중요도와 위험 프로필을 포착하는 기타 요소를 기반으로 평가됩니다.

공급업체의 위험 프로필과 Elastic 에서 제공할 서비스 유형을 기반으로 검토 워크플로우가 실행됩니다. 민감한 정보에 접근하거나 내부 시스템에 접근하거나 중요한 기술 서비스를 제공하는 모든 공급업체는 정보 보안, 법률 및 개인 정보 보호 검토를 포함하되 이에 국한되지 않는 추가 조사가 필요합니다. 이러한 추가 조사에는 보안 관행, 보안 인증 및 서드파티의 규정 준수 보고 검토가 포함됩니다. 데이터가 처리, 저장 및 전송되는 국가의 법률 준수가 고려되며, 필요하다고 판단되는 경우 Elastic 은 서드파티 계약에서 추가 보안 요구 사항을 모색할 수 있습니다.

Elastic 에는 또한 공급업체와 파트너에게 기대되는 윤리적 요구 사항을 문서화한 공급업체 행동 규범이 게시되어 있습니다. 여기에는 윤리 및 규정 준수, 직원 건강 및 안전, 인간 및 노동 권리, 환경 관리 요구 사항이 포함되지만 이에 국한되지는 않습니다.

서드파티 재인증

기존 공급업체에 대한 재인증을 수행하기 위해 지속적인 서드파티 정보 위험 관리 프로세스가 마련되어 있습니다. 서드파티는 위험 수준에 따라 분류되며 Elastic Information Security 팀은 각 위험 수준에 대한 요구 사항에 따라 서드파티의 보안 관행을 검토합니다.

Elastic Cloud 에 인프라 서비스를 제공하는 모든 클라우드 서비스 제공자는 최소 1 년에 한 번씩 검토 및 재인증을 받습니다. 재인증 프로세스에는 공급업체의 위험 프로필을 검토하고 공급업체 보안 및 규정 준수 보고를 검토하여 예상되는 보안 및 규정 준수 통제 수단이 Elastic 가 소비하는 서비스를 적절하게 포괄하고 통제 수단이 효과적으로 설계 및 운영되는지 확인하는 작업이 포함됩니다.

위협 탐지

모니터링 및 경보

Elastic 은 Elastic Security 를 SIEM 솔루션으로 활용하여 새로운 위협 및 공격 패턴은 물론 의심스러운 행동 탐지, 파일 무결성 모니터링 탐지, 일반적인 Malware 행동 패턴에 대한 탐지를 신속하게 개발하고 배포할 수 있습니다. 환경 모니터링은 자동화된 탐지를 통해 실시간으로 수행됩니다. 의심스러운 메트릭이 있는 경우 적절한 Elastic 직원에게 알리기 위해 사전 구성된 변경 워크플로우가 마련되어 있습니다. Elastic 의 연중무휴 24 시간 대기 위협 탐지 및 대응 팀은 이러한 경보를 조사하고 조치를 취합니다.

인증을 받고 지속적으로 교육을 받은 직원은 사고 대응 기준 및 사고 대응 계획에 따라 보안 이벤트 및 사고를 처리합니다. 사고 관리 프로세스에 대한 자세한 내용은 이 문서의 사고 대응 섹션을 참조하세요.

로그 관리 및 보관

Elastic 은 Elasticsearch 를 로그 관리 솔루션으로 활용합니다. Elastic 은 탐지 엔진, IaaS 공급자, 취약점 관리 도구, 클라우드 관리 콘솔 등을 포함한 다양한 소스에서 로그를 수집하고 중앙화하여 강력한 로깅, 감사 및 포렌식 능력을 개발할 수 있습니다. Elastic 로그는 변조를 방지하기 위해 액세스가 제어되며 편집 액세스는 최소 권한을 기반으로 보안 엔지니어링으로 제한됩니다. 또한 파일 무결성 모니터링을 포함한 자동 탐지 및 경보 기능은 로깅 시스템을 보호하고 위협 탐지 및 대응 팀에 의심스러운 활동을 거의 실시간으로 알립니다.

로그는 비즈니스, 법률 및 계약 요구 사항에 따른 데이터 보존 기준에 따라 보존됩니다. 데이터 액세스 요청 제출에 관심이 있는 고객은 이 문서의 데이터 개인정보 보호 섹션을 참조할 수 있습니다.

사고 대응

Elastic 정보 보안에는 보안 이벤트 및 사고 관리를 전담하는 연중무휴 위협 탐지 및 대응 팀이 있습니다. 사고 대응 기준은 사고 대응 기능을 관리하고 이벤트 식별, 이벤트 처리, 보고 및 교육 요구 사항을 규정합니다. 별도의 사고 대응 계획에는 보안 사고에 대한 준비, 탐지, 분석, 억제, 근절, 복구 및 보고 방법이 자세히 설명되어 있습니다. 사고 대응 계획을 정기적으로 실행하고 테스트하는 숙련된 사고 대응자가 모든 사고를 처리합니다. 사고에는 문서화된 사후 조치 보고서와 교훈을 얻은 실습도 필요합니다.

위반을 탐지하거나 시스템이나 데이터에 대한 무단 액세스를 인지하게 되는 경우, Elastic 법무팀과 정보 보안팀은 법률에서 요구하는 대로 또는 계약 조건에 따라 과도한 지체 없이 고객에게 커뮤니케이션을 발행할 것입니다.

보안 사고로 인해 외부 규제 기관이나 산업체에 보고해야 하는 경우 Elastic 사고 대응 계획에는 현재 시나리오에 따른 보고 의무에 대한 자세한 지침이 포함되어 있습니다. 또한 이 계획에서는 적절한 개인과의 적절한 의사소통을 보장하기 위해 문서화된 역할과 책임을 가진 공식 컴퓨터 보안 사고 대응팀(CSIRT)을 지정합니다.

안정성

웹사이트 가용성 및 상태 확인

고가용성 아키텍처는 향상된 SLA 를 갖춘 Elastic Cloud 에서 사용 가능하며 권장됩니다. 이 옵션이 여러분에게 도움이 될 경우 여러분의 계정 팀과 논의하세요.

Elastic Cloud 서비스 성능에 대한 실시간 및 과거 데이터는 Elastic 에서 확인할 수 있습니다.

비즈니스 연속성 및 재해 복구

Elastic 은 재해에 대비하고, 대응하고, 복구하기 위해 비즈니스 연속성 및 재해 복구 기준 외에도 포괄적인 비즈니스 연속성 및 재해 복구 계획을 유지합니다.

Elastic 은 전 세계적으로 분산된 회사이며 창립 이래로 그래왔습니다. 직원들은 원격으로 작업할 수 있는 완벽한 장비를 갖추고 있으며 전 세계에 분산된 팀에는 지리적 중복성을 염두에 두고 직원이 배치됩니다. Elastic 사무실에는 직원 연결이나 고객에게 Elastic 서비스 및 지원을 제공하는 데 필요한 인프라나 IT 시스템이 포함되어 있지 않습니다.

Elastic 은 최소한 1 년에 한 번씩 테스트되는 Elastic Cloud 에 대한 재해 복구 계획을 유지 관리합니다. 테스트는 매년 정의된 중점 영역을 통해 고유하며 기술 복구 기능의 지식 격차와 약점을 식별합니다. RTO 및 RPO 는 각 테스트마다 추적되고 문서화되어 복구가 내부 정의 기준을 충족할 수 있는지 확인합니다. 재해 복구 테스트는 시나리오 세부 정보, 이벤트 타임라인, 개선을 위한 작업 항목과 함께 철저하게 문서화됩니다.

독립 평가

침투 테스팅

Elastic 은 개인 보안, 내부 확산, 권한 상승 및 지속적인 위협을 고려하여 심층 방어의 강점과 중요성을 인식하고 있습니다. 이를 염두에 두고 Elastic 은 여러 독립적인 침투 테스팅 서비스 제공업체와 협력하여 네트워크 및 애플리케이션 계층 침투 테스팅, 세분화 테스트, 보안 코드 검토를 수행합니다. 침투 테스팅은 적어도 매년 수행됩니다. 침투 테스팅 결과는 중요도에 따라 수정됩니다. 또한 침투 테스팅 결과는 고위 경영진에게 보고되어 결과를 수정하고 필요한 경우 추가 예방 및 탐지 제어를 구현하는 데 있어 부서 간 조정 및 책임성을 촉진합니다. 고객이 요청하면 침투 테스팅 요약 보고서와 문제 해결 상태 보고서를 이용할 수 있습니다.

독립적인 침투 테스팅 외에도 Elastic 은 공식 취약점 공개(버그 바운티) 프로그램을 후원하고 유지합니다. 보안 연구원은 취약점 공개 프로그램을 통해 취약점을 보고하도록 권장됩니다. Elastic 제품 보안 팀은 중요도에 따라 제출물을 분류하고 수정합니다. 버그 바운티 정책에 대한 자세한 내용을 알아보거나 보고서를 제출하려면 HackerOne 의 버그 바운티 프로그램을 방문하세요.

규정 준수 기준

Elastic 은 고객에게 최고의 가치를 제공하는 보안 및 규정 준수 인증과 증명을 추구하고 유지하기 위해 최선을 다하고 있습니다. Elastic 은 규제가 엄격한 전 세계 산업과 지역에서 고객의 검색, Observability 및 보안 요구 사항을 강화하기 위해 고객이 Elastic 에 대한 신뢰를 진지하게 받아들입니다. Elastic Cloud 가 제공하는 전체 인증 및 증명 목록을 보려면 Elastic 보안 및 규정 준수를 방문하세요.

데이터 개인정보 취급방침

Elastic 에서는 데이터 개인정보 취급방침이 고객 신뢰를 얻고 유지하는 데 중요한 역할을 합니다. Elastic 은 Elastic Cloud 에서 여러분의 데이터를 처리하고 보호하는 방법에 대한 투명성을 고객에게 제공하기 위해 최선을 다하고 있습니다.

데이터 호스팅

Elastic 은 Amazon Web Services(AWS), Microsoft Azure, Google Cloud Platform(GCP)과 같은 클라우드 서비스 제공자를 사용하여 Elastic Cloud 를 제공합니다. Elastic 은 각 클라우드 서비스 제공자를 통해 전 세계적으로 호스팅 옵션을 지원합니다. 고객은 데이터 주권 요구 사항을 가장 잘 충족하기 위해 Elastic Cloud 배포를 호스팅하려는 지역을 선택할 수 있습니다. 또한 선택한 지역에 고객 백업을 유지하도록 백업이 구성됩니다.

계약상 약정

Elastic 은 글로벌 개인 정보 보호 원칙을 준수할 수 있도록 회사 전체에 프로세스, 조직 구조, 기술적 조치를 구축했습니다. 이러한 약속은 Elastic Cloud 에 대한 고객 데이터 처리 수정안("DPA")에서 여러분에게 제공하는 계약상의 개인정보 보호 조항에 의해 뒷받침됩니다.

Elastic 은 다음 조항을 포함하여 적용 가능한 데이터 개인 정보 보호 요구 사항을 반영하기 위해 DPA 를 정기적으로 검토하고 업데이트합니다.

- 여러분은 여러분의 데이터를 소유합니다. Elastic 의 개인 데이터 처리는 여러분의 지시에 따라서만 수행됩니다.
- Elastic 이 처리하는 데이터에는 해당하는 법적 데이터 보호 요구 사항이 적용됩니다.
- Elastic 은 해당하는 경우 유럽 위원회 결정 2021/914/EU("SCC")에 따른 표준 계약 조항을 포함하는 적절한 기술 및 조직적 조치를 구현했으며 계약상으로 이를 약속합니다.

- 개인 데이터를 처리하도록 승인된 모든 직원에게는 엄격한 기밀 유지 정책 및 절차가 적용됩니다.
- 고객은 데이터 주체의 요청에 대한 경보를 받습니다. Elastic 은 고객의 동의 없이는 응답하지 않으며 고객이 그러한 요청에 응답할 때 요구 사항을 충족할 수 있도록 지원합니다.
- Elastic 은 정부 기관으로부터 고객 개인 데이터에 대한 액세스 요청을 받는 경우 SCC 에 따라 고객에게 이를 알릴 의무가 있습니다. Elastic 이 그러한 공개를 법적으로 금지하는 경우, Elastic 은 SCC 에 따라 그러한 금지에 이의를 제기하고 권리 포기를 구할 계약상 의무가 있습니다.
- Elastic 은 개인 데이터 처리에 관여하는 모든 직원이 기밀을 유지하도록 보장하기 위해 기밀 유지 계약과 직원 교육 프로그램을 활용합니다. 이러한 계약은 직원의 Elastic 재직 기간 종료 이후에도 적용됩니다.
- Elastic 의 하위 프로세서에는 동일한 기준 및 조직 요구 사항이 적용됩니다. Elastic 은 당사가 직접 서비스를 수행하는 경우와 동일한 정도로 하청 처리자의 작위 및 부작위에 대해 책임을 집니다.

하위 프로세서

Elastic 은 여러분에게 서비스를 제공하는 데 필요한 만큼 엄격하게 고객 개인 데이터를 (하위 프로세서로서) 처리하도록 요구할 수 있는 Elastic Cloud 를 제공하기 위해 특정 외부 서비스 제공업체 및 내부 계열사를 이용합니다.

현재 Elastic 이 참여하고 있는 외부 하위 프로세서는 https://www.elastic.co/kr/agreements/external_subprocessors 에 명시되어 있으며 내부 하위 프로세서는 https://www.elastic.co/kr/agreements/internal_subprocessors 에 명시되어 있습니다.

국제 데이터 전송 및 Schrems II

Elastic 은 글로벌 회사이며 EEA 와 영국에서 제 3 국으로 데이터를 Elastic 의 비유럽 직원은 물론 당사 서비스 제공에 필요한 서드파티 조직으로 전송할 수 있습니다. 이러한 위치는 위의 하위 프로세서 섹션에 명시되어 있습니다. 이러한 경우 Elastic 은 강력한 보완 조치 외에도 고객의 컨트롤러-프로세서 모듈, 하위 프로세서의 프로세서-프로세서 모듈을 포함한 SCC 에 의존합니다.

Elastic 은 Schrems II 이후 국제 데이터 전송에 대한 보충 조치에 관한 EDPB 지침을 검토했습니다. Elastic 의 실제 경험, 개인 데이터에 대한 정부의 관심 가능성이 낮다는 점, Elastic 프로세스, Elastic 이 고객 개인 데이터를 보호하기 위해 마련한 보호 장치 등을 고려하여, Elastic 은 유럽 이외의 지역에서 고객 개인 데이터를 처리하는 것이 개인의 권리에 대한 위험으로 인해 Elastic 이 SCC 에 따른 "데이터 수입자"로서의 의무를 이행하지 못하게 됩니다.

- 내부 분석 및 외부 자문 검토 결과 Elastic 데이터 전송은 감시법의 일반적인 초점에 속하지 않는 것으로 결론지었습니다. 또한 전송된 데이터를 보호하기 위한 보완 조치도 제공합니다.
- Elastic 의 서비스 및 데이터 처리 활동의 성격에 따라 공공 기관의 요청은 거의 발생하지 않습니다. Elastic 은 FISA, EO12333 또는 CLOUD Act 요청을 받은 적이 없습니다.
- SCC 는 해당 고객 데이터 전송을 보호하기 위해 적용됩니다. 유럽에서 시작된 개인 데이터가 (i) 고객이 Elastic 으로 직접 전송하거나, (ii) Elastic 그룹 엔터티 간에 그룹 내에서 Elastic 에 의해 전송되거나, (iii) Elastic 에 의해 외부 하위 처리자에게 전송되는 경우, Elastic 은 그러한 당사자와 SCC 에 가입합니다.
- 데이터는 전송 중 및 저장 중 암호화됩니다.
- 고객은 서비스 애플리케이션을 위해 EU 서버를 선택할 수 있습니다.
- Elastic 은 데이터 전송을 보호하기 위해 계약적, 기술적, 조직적 보호 장치를 지속적으로 평가하고 개발합니다.

공공기관 액세스 요청

Elastic 은 고객 콘텐츠에 대한 공공 기관 액세스 요청에 응답하기 위한 정책과 프로세스를 확립했습니다. 이러한 정책과 프로세스는 관련 데이터 보호법과 고객 계약을 준수합니다.

Elastic 은 공공 기관 액세스 요청 및 필수 공개와 관련된 약속을 준수하는 능력에 영향을 미칠 수 있는 관련 법률을 인식하지 못합니다. 어떠한 경우에도 Elastic 은 민주 사회에서 필요한 수준을 넘어서는 대규모, 불균형 또는 무차별적인 방식으로 개인 데이터를 공개하지 않습니다.

위의 내용에도 불구하고 Elastic 은 702 FISA 조항을 포함하여 공공 기관으로부터 고객 콘텐츠에 대한 액세스 요청을 받은 적이 없습니다. 또한 EO 12333 에 따라 고객 콘텐츠에 직접 액세스한 사례도 없습니다. Elastic 은 당사 제품이나 서비스에 대한 백도어나 마스터 키를 만든 적이 없으며 정부 기관이 당사 서버에 자유롭게 또는 직접 액세스하도록 허용한 적이 없습니다.

기업으로서의 개인 데이터 보호

개인정보 보호정책

Elastic 이 Elastic Cloud 에서 개인 정보를 수집, 사용, 공개, 전송, 저장하는 방법에 대한 자세한 내용은 제품 개인정보 보호정책을 참조하세요.

글로벌 개인정보 보호 규정

Elastic 은 GDPR 및 CCPA 를 포함한 글로벌 개인 정보 보호 규정을 준수하기 위해 최선을 다하고 있습니다. 데이터 주체 요청을 제출하려면 일반 개인정보 보호정책의 문의 방법 섹션을 확인하세요. Elastic 배포가 GDPR 을 준수하는지 확인하는 방법에 대한 자세한 내용은 Elasticsearch GDPR 및 Elastic Stack GDPR 규정 준수를 참조하세요.

