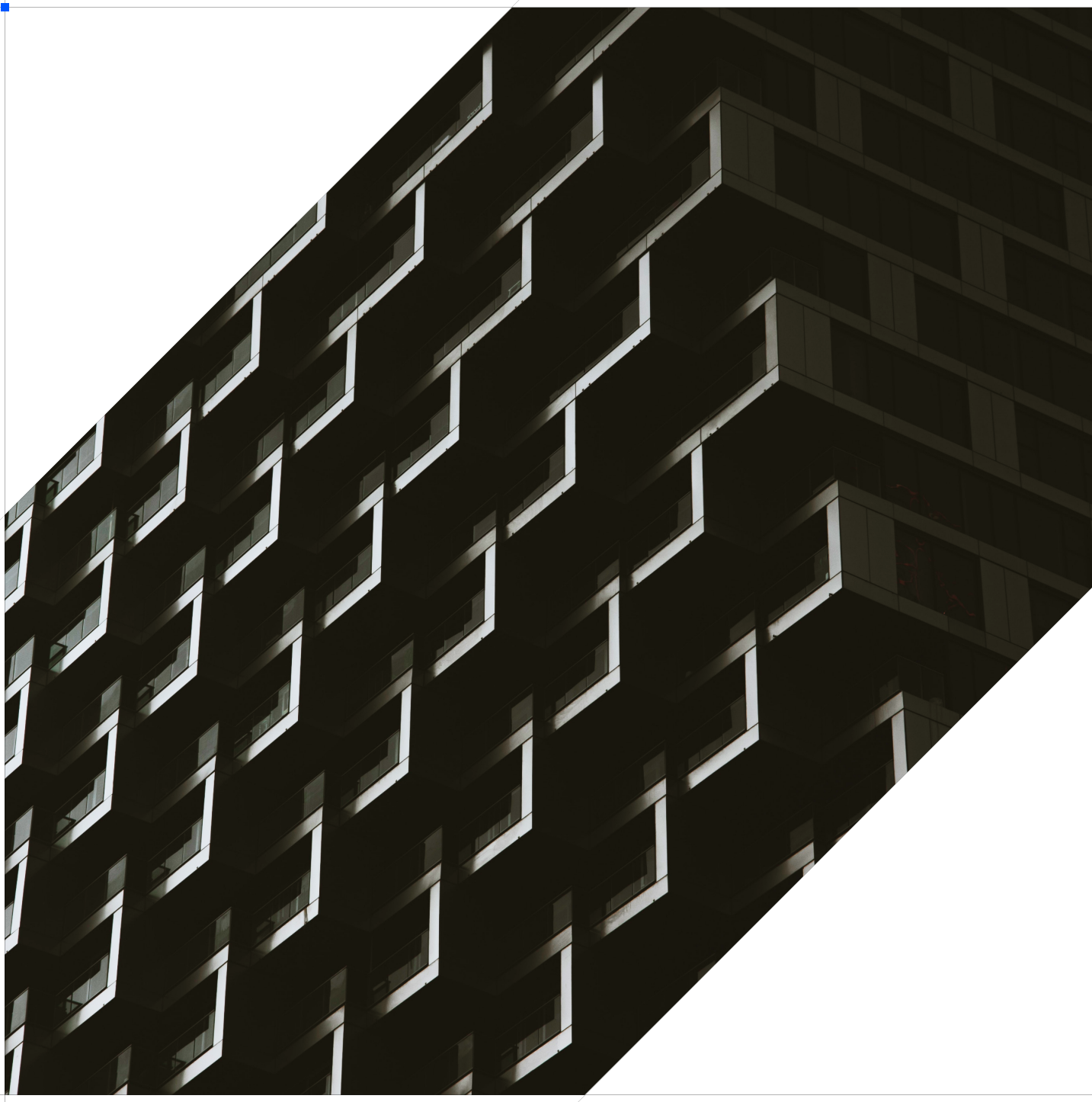
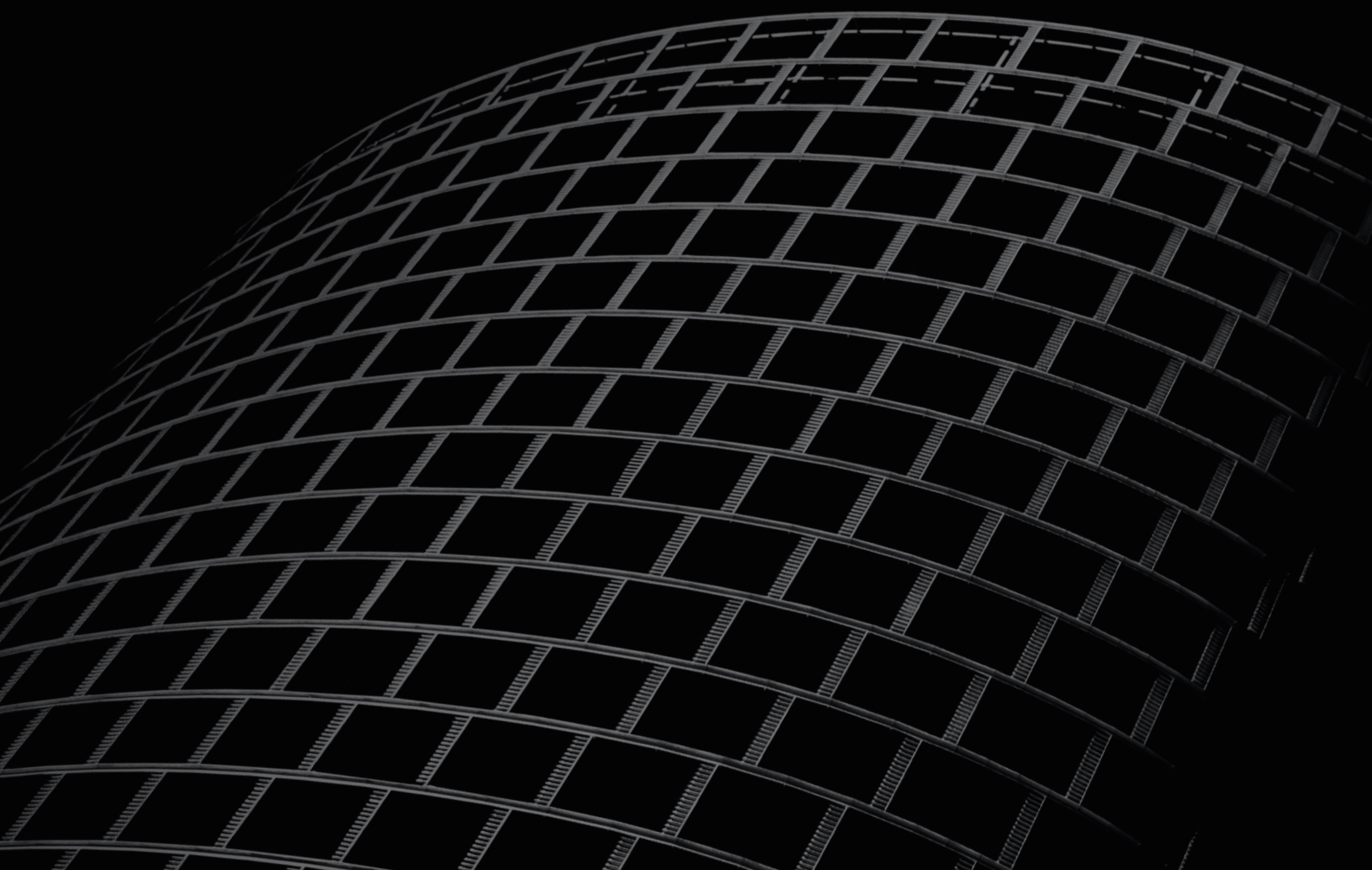
SUPERB AI.

SUPERB AI 보안 백서



SUPERB-AI

Contents



1 - 정보보안 인증

슈퍼브에이아이는 현재 국제 정보보안 및 개인정보보호 규격인 SOC-2 Type II 및 ISO 27001 인증을 획득하였습니다.

1.1 - SOC 2 Type II

- 2021년 8월, SOC 2 인증 취득
- 2022년 9월, 인증 갱신
- 2023년 9월, 인증 갱신

SOC 2 (Service Organization Control 2)는 서비스 조직이 정보 보안에 관련된 특정 기준을 충족하는지를 평가하는 데 사용되는 미국 기반의 감사 절차입니다. SOC 2 인증은 미국의 AICPA (American Institute of Certified Public Accountants)에 의해 설정된 기준에 따라 실시되며, 특히 클라우드 기반 서비스를 제공하는 기업에 있어서 중요한 인증으로 간주됩니다.

슈퍼브에이아이는 한국에서 유일하게 SOC 2 Type II 인증을 획득한 AI 개발 플랫폼 운영 회사입니다. 이 인증은 미국의 보안 및 개인정보 보호에 관한 엄격한 표준을 충족함을 의미하며, 서비스의 안정성과 보안, 개인정보 보호를 지속적으로 유지하고 있음을 보증합니다. 회사는 데이터 암호화, 외부 감사 및 정기적인 보고, 그리고 보안 사태에 대한 대응 훈련 등 최고 수준의 보안 시스템을 갖추고 있음을 인증받았으며, 주기적인 침투 테스트 (penetration test) 등을 통해 새로운 보안 취약점에 대비하고 있습니다.

(* 요청 시 SOC 2 보고서를 제공할 수 있습니다)

1.2 - ISO 27001

- 2023년 11월, ISO 27001 인증 취득 (유효기간: 2026년 11월)

ISO 27001은 국제표준화기구(ISO)에 의해 설정된 정보보안 관리 시스템(ISMS)에 대한 국제 표준입니다. 이 인증은 전 세계적으로 정보보안 분야에서 가장 권위 있는 인증 중 하나로 인정받고 있습니다.

슈퍼브에이아이는 ISO 27001 인증을 받음으로서 정보보안 위험을 적절히 식별, 평가, 관리하고 이를 통해 정보보안 위협에 대응할 수 있는 능력과 체계를 준수하고 있음을 입증하였습니다. ISO 규정에 따라 정보보안 위험의 식별, 평가, 관리 및 대응 전략을 수립하였고, 정보보안 기준을 준수하기 위한 구체적인 기술적 조치를 개발 및 실행하고 있습니다.

2 - 정보보안 정책

슈퍼브에이아이는 SOC-2 및 ISO 27001 인증 및 준수를 위해 다음과 같은 정보보안 정책을 수립하고 수행하고 있습니다.

2.1 - 운영 보안 정책 (Operations Security Policy)

슈퍼브에이아이의 운영 보안 정책은 데이터 보안 및 복원력 강화에 중점을 둡니다. 매일 데이터 백업을 진행하며, 이 백업은 7일간 보관됩니다. 또한, 최소 연 1회 백업 및 복구 테스트를 진행하여 재난 발생 시 데이터 복구 능력을 검증하고 있습니다. 유저별 로그인 및 접근 로그의 경우 365일 동안 저장되며, 보안 결함이 발견되면, 5가지 등급으로 심각성을 분류하고 각 등급에 따라 정해진 목표 기간 내에 해결합니다. 이는 정보보안 관리 및 감사에 필수적이며, 보안 위협에 대한 신속하고 효과적인 대응을 보장합니다.

2.2 - 복호화 정책 (Cryptography Policy)

슈퍼브에이아이의 복호화 정책은 데이터 보호를 위한 최신 기술을 채택하고 있습니다. 서버 사이드에서는 AES-256 (256-bit Advanced Encryption Standard)을 활용하여 데이터를 안전하게 암호화합니다. 이는 강력한 암호화 방식으로, 서버에 저장되는 고객의 중요 데이터를 안전하게 보호하는 데 필수적입니다. 또한, 데이터 전송 중에는 TLS v1.2 방식을 활용하여 data-in-transit을 복호화합니다. 이는 데이터가 전송 과정 중에도 높은 보안 수준을 유지할 수 있도록 보장합니다.

2.3 - 인시던트 대응 계획 (Incident Response Plan, IR)

슈퍼브에이아이는 데이터, 시스템, 네트워크에 발생할 수 있는 인시던트에 대비하여 체계적인 대응 계획을 수립하고 있습니다. 인시던트가 발생할 경우, 4가지 위험도 등급 별 보고 체계에 따라 조치를 수행합니다. 이벤트 보고, 위험도 분류 및 분석, 위협 통제, 복구 및 취약점 교정 등의 과정으로 진행되는 조치들은 신속하고 효과적인 대응을 가능하게 합니다. 인시던트 대응은 최고보안책임자 및 정보보안팀이 전담하여 진행되며, 필요시 워룸 (War Room)을 지정하여 인시던트가 해결될 때까지 주기적이고 반복적으로 인시던트 대응을 진행합니다.

2.4 - 업무 연속성 및 재해 복구 계획 (Business Continuity and Disaster Recovery; BC/DR)

슈퍼브에이아이는 6개월 기간 동안 99.9%의 uptime을 보장하는 업무 연속성 및 재해 복구 계획(BC/DR)을 제공합니다. 재해나 기타 예기치 못한 사건으로 프로덕션 서버 운영에 영향이 있을 경우, 서비스 운영에 필수적인 각 서비스별로 지정된 복구 시간 목표(Recovery Time Objective, RTO)와 복구 지점 목표(Recovery Point Objective, RPO)에 맞춰 시스템 복구 작업을 수행합니다. 전체 서비스는 RTO 24시간, RPO 72시간을 목표로 하며, 이는 비즈니스 연속성을 유지하고 재해 발생 시 신속한 복구를 가능하게 함으로써, 고객에게 안정적인 서비스를 지속적으로 제공하는 데 중요한 역할을 합니다.

3 - 정보보안 관련 플랫폼 기능

3.1 - 기본 보안 기능

2019년 12월 Superb Platform의 첫 출시 시점부터 다음과 같은 기본적인 보안 기능을 제공하고 있습니다.

사용자 엑세스 관리

- 슈퍼브 플랫폼의 사용자는 역할 기반으로 권한이 나뉘어져 있습니다. RBAC (Role-Based Access Control) 방식으로 구현되어있기 때문에 관리자 및 기존 사용자가 플랫폼에 초대한 유저만 가입할 수 있습니다.
- 데이터 라벨러 및 리뷰어 등의 역할을 가진 사용자는 관리자가 권한을 부여한 데이터에 대해서만 접근이 가능하며, 데이터를 복사하거나 다운로드 할 수 없습니다.

사용자 비밀번호 보안

- 플랫폼에 가입된 유저의 비밀번호 등 모든 개인정보는 슈퍼브에이아이 내부 시스템에 저장되고 있지 않으며, AWS Cognito라는 별도의 서비스를 사용하여 관리됩니다. Cognito 서비스에 의해 관리되는 정보는 슈퍼브에이아이는 물론이며 AWS 측에서도 직접 확인이 불가한 상태로 관리되어 유출을 원천적으로 차단할 수 있습니다.

데이터 업로드 방식

- 업로드 된 데이터 및 모든 정보는 전송 즉시 암호화 처리됩니다. 암호화에 대한 자세한 내용은 다음 섹션을 참고하세요.

데이터 파기 요청

- 플랫폼 내 모든 데이터는 관리자 권한의 사용자가 모두 직접 삭제 가능합니다.
- 그 외 정정 또는 파기 (예: 계정 전체 삭제)에 대한 조치가 필요한 경우, 요청주시면 즉각 대응 가능합니다.

3.2 - 정보보안 특화 신규 기능

기업 고객분들께 보다 더 높은 수준의 정보 보안을 약속 드리기 위해 다음과 같은 보안 특화 기능들을 지속적으로 추가해왔습니다.

[24년 1월 추가] IP Whitelist

기업 내부망 등 관리자가 요청한 IP 주소로만 플랫폼 접근이 가능하도록 제한할 수 있으며, 인가되지 않은 IP 주소로 접속하는 경우 로그인 단계부터 모든 행동이 차단됩니다. 인가된 IP 주소로 접속한 이후 타 IP 주소로 이동하는 경우에도 모든 접근 및 유저 행동이 차단됩니다.

[23년 2월 추가] 개인정보 비식별화

개인정보 유출 이슈를 최소화하기 위해서 슈퍼브 플랫폼에서 데이터를 활용하기 전후로 이미지 내 개인정보 비식별화 처리가 가능합니다. (예: 얼굴 영역의 블러 처리)

비식별화 처리를 위한 기능은 플랫폼 내 Apps 제품을 통해 제공 가능하며, 필요시 고객 담당자에게 요청주시면 엑세스를 드릴 수 있습니다.

[22년 5월 추가] 다중 인증 (MFA; Multi-Factor Authentication)

비밀번호와 OTP 인증으로 총 2번의 인증을 거쳐야 로그인이 가능한 다중인증 시스템을 제공합니다.

관리자가 이 기능을 활성화 하는 경우, 모든 유저는 OTP로 발송되는 6자리 코드 입력시에만 로그인 가능하며, 외부인의 플랫폼 접속 및 플랫폼 내 활동을 완전 차단할 수 있는 강력한 보안 기능입니다.

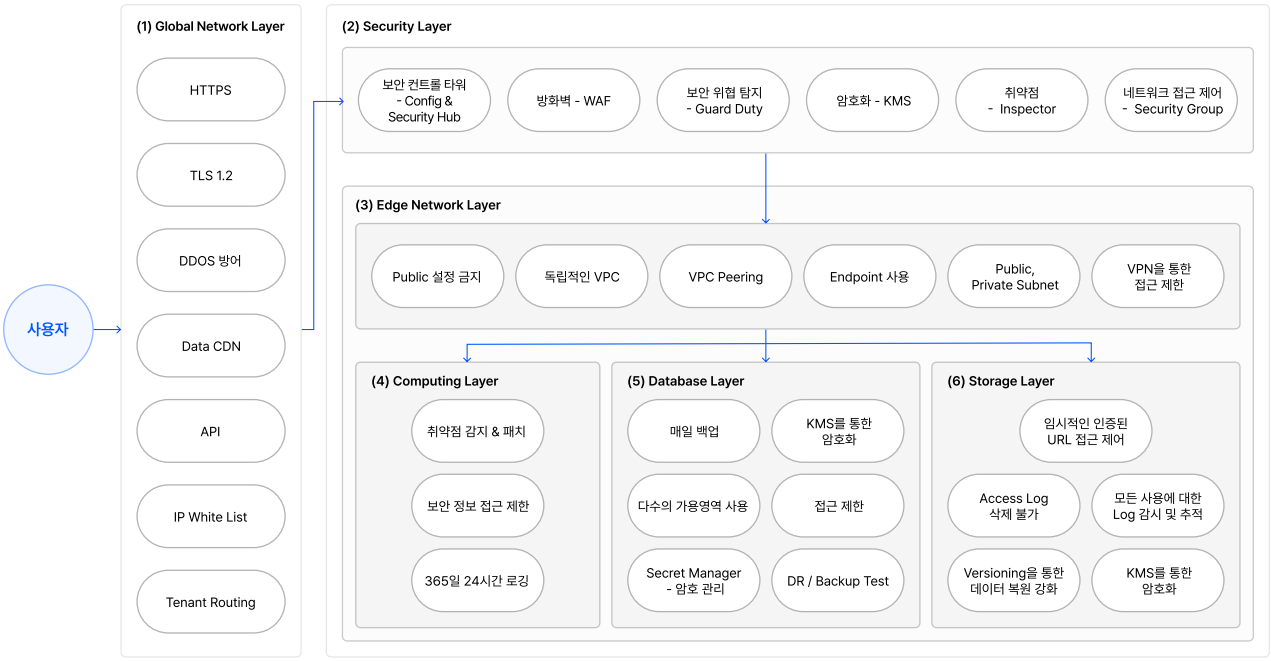
클라우드 저장소 연동 (AWS [21년 2월], Google Cloud [21년 3월], Miscrosoft Azure [22년 6월] 연동 지원)

클라우드 저장소를 사용하는 고객의 경우, 별도로 데이터를 슈퍼브 플랫폼에 재 업로드 하지 않고 클라우드 저장소와 연동하여 플랫폼을 활용할 수 있습니다. 이와 같은 연동을 통해 제 3자가 업로드 행위에 개입하거나 침입하는 것을 막을 수 있기 때문에 로컬 PC에서 웹으로 업로드 하거나 SDK를 통한 업로드 대비 안전한 데이터 전송 방식입니다.

클라우드 연동 시 “읽기전용” 옵션도 제공하여, 슈퍼브 플랫폼으로 별도의 데이터 전송과정 없이 서비스 제공이 가능합니다.

[23년 12월] 기존의 Access Key 방식의 AWS S3 연동 방식 보다 한 단계 더 강력한 보안을 제공하는 Role Delegation 방식 지원이 추가되었습니다.

4 - 정보보안 및 관리 시스템



슈퍼브 플랫폼 시스템 구성도

보안 취약점 및 침투 위험 (예: 네트워크 공격, 리소스 액세스 컨트롤)에 대해서는 SOC 2와 ISO27001을 획득할 수 있는 수준의 보안을 준수하고 있습니다. 구체적인 네트워크 관련 조치 사항은 다음과 같습니다.

4.1 - 네트워크

(1) Global Network Layer

- CloudFront를 활용, 모든 네트워크 통신은 HTTPS, TLS1.2 이상으로 설정되어 있어 안전한 데이터 통신 가능
- AWS Shield 사용하여 DDOS 공격 방어
- IP Whitelist 기능 적용 시 비인가 IP에서 접속 차단

(2) Security Layer

- WAF, Security Group 등을 이용한 Inbound, Outbound 네트워크 보안 확인
  - AWS WAF 사용하여 서버 방화벽 설정
  - AWS Managed Rule set 사용 (OWASP TOP 10 방어)
- AWS 내부 위협 감지: AWS GuardDuty 사용 (S3, EKS, Lambda, RDS, Malware 모두 적용)

- 암호화 Key 관리
  - KMS 접근 사용자 제한
  - AWS KMS 사용하여 각종 암호화 설정
  - 암호화 방식
    - 대칭키 : AES-256-GCM
    - 비대칭키 : RSA_2048 이상

(3) Edge Network Layer

- 독립적인 VPC 사용
- Private, Public Subnet을 분리해서 사용
- Database, Computing에 대한 Private Subnet 분리
- Private Subnet은 공인 IP 설정 금지
- Multi Region VPC 사이에 VPC Peering 설정
- 내/외부 서비스 연동 (Elastic Cloud) 사용 시 Endpoint 설정
- VPC 접근은 VPN IP 주소로 제한
- VPC Link를 통한 내부 네트워크 접근 제한

4.2 - 컴퓨팅 / 데이터베이스 / 데이터 스토리지

(4) Computing Layer

- 24시간 Inspector를 통한 취약점 점검 및 패치
- CloudWatch를 활용한 로그를 저장, 365일 간 보관
- Secret Manager를 사용하여 보안 정보 접근 제한

(5) Database Layer

- 매일 데이터베이스 Backup 진행, 최대 7일 동안 유지
  - DynamoDB의 경우 Point-in-time Recovery 설정
  - Backup에 대한 recovery 테스트 최소 연 1회 수행
- 2개 이상의 Availability Zone 사용
- KMS를 기반으로 Encryption 적용
- Public IP 할당을 허용하지 않고, Private Subnet에서만 운영
- Secret Manager를 통한 비밀번호 보안 관리

(6) Storage Layer

- Presigned URL를 제외하고 모든 Public 접근 제한
- KMS를 기반으로 Encryption 적용
- 모든 접근에 대한 Access Log 저장
  - Access Log Bucket은 Root Account를 제외하고 삭제 불가능

슈퍼브에이아이 소개

슈퍼브에이아이는 첫 AI 개발부터 AI 성능 고도화까지, AI 도입의 모든 과정을 지원합니다. 누구나 쉽고 빠르게 AI를 개발할 수 있도록 돕는 슈퍼브 플랫폼과, 최고 수준의 전문가가 AI 도입을 도와드리는 슈퍼브 서비스를 제공합니다.

슈퍼브 플랫폼에 대한 더 자세한 내용이 궁금하시다면, 다음 홈페이지에서 무료로 계정을 생성 하시거나, 제품 데모 및 체험판 사용을 요청해주세요. (www.superb-ai.com)

5 - 부록 : 보안, 자격 증명 및 규정 준수 체크리스트

카테고리	설명	활용 AWS 서비스
ID 및 액세스 관리	AWS 서비스 및 리소스에 대한 액세스와 ID를 안전하게 관리	AWS Identity and Access Management(IAM)
	여러 AWS 계정과 애플리케이션에 대한 인력의 액세스 권한을 중앙에서 관리	AWS IAM Identity Center(SSO의 후속 서비스)
	안전하고 마찰 없는 확장 가능한 고객 ID 및 액세스 관리 구현	Amazon Cognito
	AWS 리소스를 확장할 때 중앙 집중식으로 환경을 관리	AWS Organizations
탐지 및 대응	지능형 위협 탐지로 AWS 계정을 보호	Amazon GuardDuty
	규모에 맞는 지속적인 자동 취약성 관리	Amazon Inspector
	AWS 보안 검사 자동화 및 보안 경고 중앙 집중화	AWS Security Hub
	리소스 구성에 대한 진단, 감사 및 평가	AWS Config
	AWS, 온프레미스 및 기타 클라우드에서 리소스 및 애플리케이션을 관측하고 모니터링	Amazon CloudWatch
	사용자 활동 및 API 사용 추적	AWS CloudTrail
네트워크 및 애플리케이션 보호	VPC 전반에 네트워크 방화벽 보안 배포	AWS Network Firewall
	관리형 DDoS 보호 기능을 통해 애플리케이션 가용성과 응답성을 최대화	AWS Shield
	일반적인 익스플로잇으로부터 웹 애플리케이션 보호	AWS Web Application Firewall(WAF)
데이터 보호	데이터를 암호화하거나 디지털 서명할 때 사용하는 키를 생성 및 제어	AWS Key Management Service (AWS KMS)
	AWS 서비스 및 연결된 리소스를 통해 SSL / TLS 인증서를 프로비저닝하고 관리	AWS Certificate Manager
	보안 암호의 수명 주기를 중앙에서 관리	AWS Secrets Manager