



SEOUL | MARCH 18, 2025

Unicorn Day

블럭스(Blux)의 SaaS 서비스를 위한 보안 여정 (feat. SOC 2)

Sunhong Min (he/him)

Information Security and DevOps Lead
Blux

Agenda

Misconceptions of Security Compliances

Introducing Blux and SOC 2 Overview

Blux's SOC 2 Compliance Journey (A to Z)

Insights Gained from the SOC 2 Compliance Preparation Process

Wrap-up



Misconceptions of Security Compliances

보안 인증에 대한 오해

보안 인증은
1개월만
준비하면 받을
수 있다.

보안 인증 취득은
외부 업체에 전부
맡기면 된다.

한 번 보안 인증을
받으면 평생
유효하다.

보안 인증을 받으려면
대규모 보안 팀이
필요하다.

보안 인증을 받으려면 보안 전문가를
반드시 채용해야 한다.





Go beyond your potential.

AI를 통해 온라인 비즈니스의 고객 가치를 극대화합니다.



오프사이트 마케팅

Blux Message
초개인화 CRM 마케팅

모든 채널, 초개인화, 성과 분석, AI 리포트
이 모든 것을 하나의 솔루션에 담았습니다.



<https://www.blux.ai>

온사이트 마케팅

Blux Recommendation
초개인화 상품 추천

클라이언트의 다양한 요구를 200% 만족해
'성과'와 '고객 만족도'라는 두 마리 토끼를
모두 잡는 추천 시스템을 제공합니다.



<https://blog.blux.ai>

SOC 2 Overview

SOC 2 개요

- SOC 2: Systems and Organization Controls 2
- 조직이 고객 데이터를 무단 접근(Unauthorized Accesses), 보안 사고(Security Incidents), 기타 취약점(Other Vulnerabilities)으로부터 보호하는 방법을 규정하는 보안 프레임워크



SOC 2 Overview

SOC 2 개요

미국 공인회계사
협회(AICPA)에서 제정



미국 및 글로벌 시장 진출을
위한 사실상의 필수 보안 인증



3~12개월간 실제 운영 데이터를
기반으로 검증



SOC 2 Overview

SOC 2 개요

- 주요 검증 영역 (TSC – Trust Service Criteria)

1. 보안 (Security)*

2. 가용성 (Availability)

3. 처리 무결성 (Processing Integrity)

4. 기밀성 (Confidentiality)

5. 개인정보보호 (Privacy)



*: 필수 검증 영역

SOC 2 Overview

SOC 2 TYPE 1 VS. SOC 2 TYPE 2

| | SOC 2 Type 1 | SOC 2 Type 2 |
|----------------------|--|-------------------------------------|
| Evaluation Criteria | 특정 시점(Point-in-time)에서 보안 통제 설계 적절성 평가 | 일정 기간(보통 3~12개월) 동안 보안 통제 운영 효과성 평가 |
| Customer Trust Level | 제한적 (설계만 평가) | 높음 (운영 실효성 평가) |
| Common Use Case | 내부 프로세스 점검, 초기 신뢰 확보 용도 | 대기업 및 글로벌 고객 대상 서비스 운영 신뢰성 확보 |

SOC 2 Overview

B2B SaaS 기업에게 SOC 2 인증이 필요한 이유

고객 신뢰 확보 & 글로벌 시장 진출

- 대기업 및 해외 고객과의 계약 시 SOC 2 인증 요구 증가
- 보안 검토 과정 단축으로 세일즈 프로세스 가속화



+ Follow ...

B2B SaaS 하신다면 PMF 검증 이후 바로 보안 인증부터 따세요. 피눈물 흘리지 않으려면요 !!

1. "일단 딜 진행하고, 보안 인증은 딜 어느 정도 무르익을 때 즈음에 하면 되지 않을까요?" 엔터프라이즈를 타겟으로 하는 많은 B2B SaaS 스타트업이 이런 생각으로 시작합니다. 저도 그랬습니다. PMF는 검증됐고, 고객의 pain point도 해결하는데 "제품력으로 승부하면 되지 않을까?"라는 생각이었죠. 하지만 현실은 냉정합니다. [redacted] 도 동일한 생각을 가지고 대기업에 보안 인증 없이 영업을 시도했으나, 결과는 모두 실패였습니다.

2. 대기업 A사와의 영업에서 실무진들이 제품의 가치를 완벽히 이해하고 도입을 강력히 희망했습니다. PoC까지 성공적으로 진행했고 현업의 높은 만족도도 확보했죠. 하지만 정보보안팀 검토 단계에서 보안 인증이 없다는 이유로 승인이 지연되었고, 그 사이 비상경영체제로 인해 모든 것이 물거품이 되었습니다.

3. 핀테크 B사의 사례는 더 충격적이었습니다. 도입 실무진이 제품에 큰 관심을 보이며 상세한 제품 탐색까지 마쳤지만, 정보보안팀에서는 "기본적인 보안 인증조차 없다"는 이유로 검토 자체를 거부했습니다. "보안 인증 취득 전까지는 어떤 논의도 불가능하다"는 답변과 함께 더 이상의 커뮤니케이션이 중단되었죠.

SOC 2 Overview

B2B SAAS 기업에게 SOC 2 인증이 필요한 이유

고객 신뢰 확보 & 글로벌 시장 진출

- 대기업 및 해외 고객과의 계약 시 SOC 2 인증 요구 증가
- 보안 검토 과정 단축으로 세일즈 프로세스 가속화



+ Follow ...

B2B SaaS 하신다면 PMF 검증 이후 바로 보안 인증부터 따세요. 피눈물 흘리지 않으려면요 !!

1. "일단 딜 진행하고, 보안 인증은 딜 어느 정도 무르익을 때 즈음에 하면 되지 않을까요?" 엔터프라이즈를 타겟으로 하는 많은 B2B SaaS 스타트업이 이런 생각으로 시작합니다. 저도 그랬습니다. PMF는 검증됐고, 고객의 pain point도 해결하는데 "제품력으로 승부하면 되지 않을까?"라는 생각이었죠. 하지만 현실은 냉정합니다. [redacted] 도 동일한 생각을 가지고 대기업에 보안 인증 없이 영업을 시도했으나, 결과는 모두 실패였습니다.

보안 인증이 없다는 이유로 승인이 지연!

[redacted] 업에서 실무진들이 제품의 가치를 완벽히 이해하고 도입을 강력히 희망했습니다. PoC까지 성공적으로 진행했고 현업의 높은 만족도도 확보했죠. 하지만 정보보안팀 검토 단계에서 **보안 인증이 없다는 이유로 승인이 지연**되었고, 그 사이 비상경영체제로 인해 모든 것이 물거품이 되었습니다.

3. 핀테크 B사의 사례는 더 충격적이었습니다. 도입 실무진이 제품에 큰 관심을 보이며 상세한 제품 탐색까지 마쳤지만, 정보보안팀에서는 "기본적인 보안 인증조차 없다"는 이유로 검토 자체를 거부했습니다. "보안 인증 취득 전까지는 어떤 논의도 불가능하다"는 답변과 함께 더 이상의 커뮤니케이션이 중단되었죠.

SOC 2 Overview

B2B SAAS 기업에게 SOC 2 인증이 필요한 이유

고객 신뢰 확보 & 글로벌 시장 진출

- 대기업 및 해외 고객과의 계약 시 SOC 2 인증 요구 증가
- 보안 검토 과정 단축으로 세일즈 프로세스 가속화



+ Follow ...

B2B SaaS 하신다면 PMF 검증 이후 바로 보안 인증부터 따세요. 피눈물 흘리지 않으려면요 !!

1. "일단 딜 진행하고, 보안 인증은 딜 어느 정도 무르익을 때 즈음에 하면 되지 않을까요?" 엔터프라이즈를 타겟으로 하는 많은 B2B SaaS 스타트업이 이런 생각으로 시작합니다. 저도 그랬습니다. PMF는 검증됐고, 고객의 pain point도 해결하는데 "제품력으로 승부하면 되지 않을까?"라는 생각이었죠. 하지만 현실은 냉정합니다. [redacted] 도 동일한 생각을 가지고 대기업에 보안 인증 없이 영업을 시도했으나, 결과는 모두 실패였습니다.

보안 인증이 없다는 이유로 승인이 지연!

[redacted] 업에서 실무진들이 제품의 가치를 완벽히 이해하고 도입을 강력히 희망했습니다. PoC까지 성공적으로 진행했고 현업의 높은 만족도도 확보했죠. 하지만 정보보안팀 검토 단계에서 [redacted] 보안 인증이 없다는 이유로 승인이 지연되었고, 그 사이 비상경영체제로 인해 모든 것이 물거품이 되었습니다.

"보안 인증 취득 전까지는 어떤 논의도 불가능하다"

3. 핀테크 B사의 사례는 더 충격적이었습니다. 도입 실무진이 제품에 큰 관심을 보이며 상세한 제품 탐색까지 마쳤지만, 정보보안팀에서는 "기본적인 보안 인증조차 없다"는 이유로 검토 자체를 거부했습니다. [redacted] "보안 인증 취득 전까지는 어떤 논의도 불가능하다"는 답변과 함께 더 이상의 커뮤니케이션이 중단되었죠.

SOC 2 Overview

B2B SAAS 기업에게 SOC 2 인증이 필요한 이유

고객 신뢰 확보 & 글로벌 시장 진출

- 대기업 및 해외 고객과의 계약 시 SOC 2 인증 요구 증가
- 보안 검토 과정 단축으로 세일즈 프로세스 가속화



실질적인 보안 수준 강화

- 체계적인 보안 정책 및 절차 정립
- 위험 평가 및 지속적인 보안 개선 수행




Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



August, 2024 – 보안 인증 SaaS 선정

- 미팅 업체 (D사 등 총 3사)
- 체크리스트 
 1. Is it startup friendly?
 - Full-time compliance support team (In-app, Slack Connect)
 2. Is it fast?
 - Response
 - Overall schedule
 3. Is it affordable?



Blux's SOC 2 Compliance Journey (A to Z)



블럭스의 SOC 2 인증 여정



August 29th, 2024 – Drata와 킥오프 미팅

Drata 개요 및 역할

- 보안 및 컴플라이언스 전문가들이 설계한 SaaS
- 기업이 보안 및 규제 준수를 유지하며, 보다 안전하고 **감사 준비된(audit-ready)** 조직으로 운영될 수 있도록 지원

Drata의 주요 기능

1. AI 기반 자동화
 - SOC 2, ISO 27001 등 보안·개인정보 보호 프레임워크의 준수 업무 **최대 90% 자동화**
2. GRC(Governance, Risk, Compliance) 관리
 - 리스크 식별 및 관리, 자동화된 보안 감사 대응
3. 보안 검증(Security Assurance)
 - 보안 및 규제 준수 상태를 **실시간**으로 입증 및 모니터링 가능

Blux's SOC 2 Compliance Journey (A to Z)

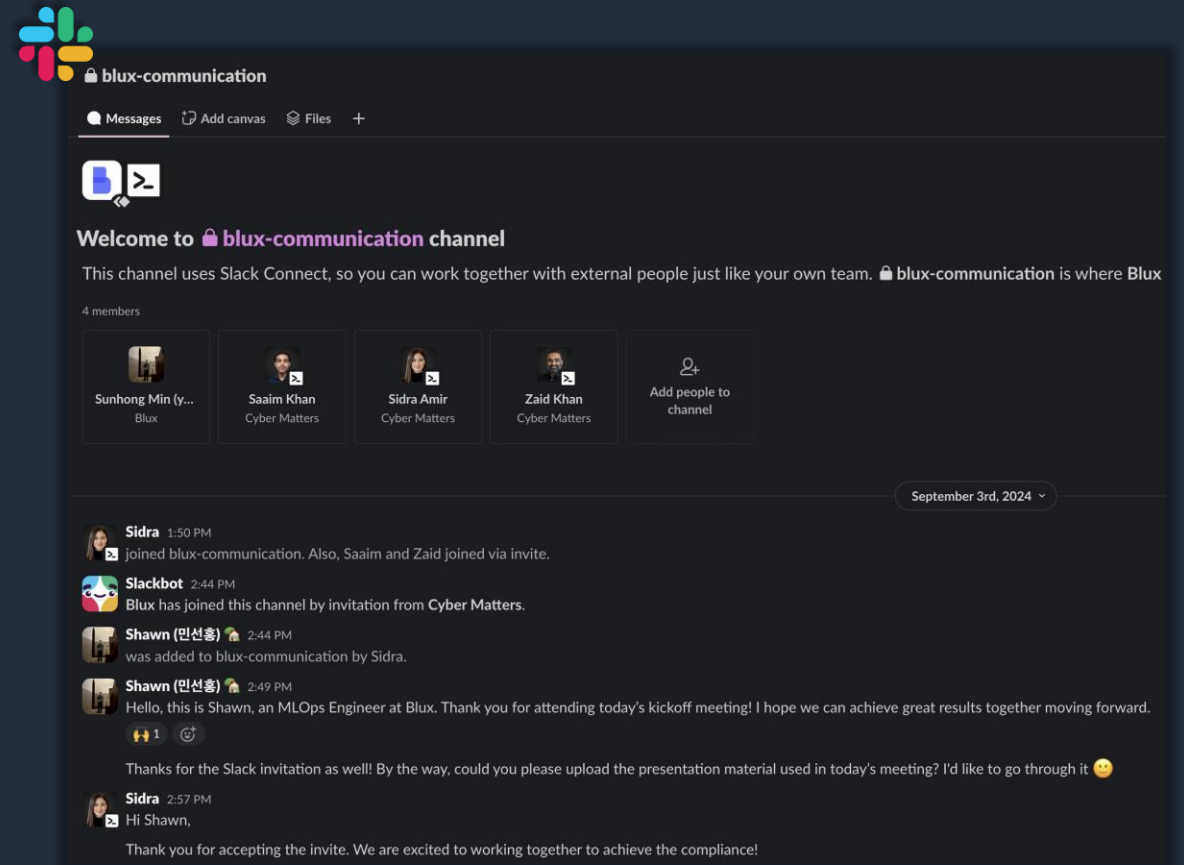


블럭스의 SOC 2 인증 여정



September 3rd, 2024 – Cyber Matters와 온보딩

- 사이버 보안 컨설팅 전문 기업
- Drata CAP(Compliance Accelerator Program)의 일환으로 Drata 측에서 블럭스와 연결해준 기업
- 호주에 팀이 있어서 아시아 고객들과 비슷한 시간대에 원활한 소통이 가능
- Slack Connect 제공



Blux's SOC 2 Compliance Journey (A to Z)



블럭스의 SOC 2 인증 여정



September 3rd, 2024 – Cyber Matters와 온보딩

- 사이버 보안 컨설팅 전문 기업
- Drata CAP(Compliance Accelerator Program)의 일환으로 Drata 측에서 블럭스와 연결해준 기업
- 호주에 팀이 있어서 아시아 고객들과 비슷한 시간대에 원활한 소통이 가능
- Slack Connect 제공



Sidra 12:25 PM

@channel Please review the Action Items from today's call:

Weekly Check-In Meeting Blux Notes 26 Sep 2024

- Zaid to provide a report with recommendations on getting controls ready, including evidences, policies, or screenshots to add. - Zaid
- Zaid and team to close the CAP program by next call and provide system description and CAP end report in the week after - Zaid
- Shawn to review and fill in information for the Business Impact Analysis tables in the Business Continuity Plan policy. - Shawn
- Zaid to confirm with his consultant about the Change Management policy template and get back to Shawn. - Zaid
- Zaid to confirm with his consultant about the Information Exchange section in the Data Protection policy and get back to Shawn. - Zaid
- Shawn to fill in the data retention table with AWS as the storage location. - Shawn
- Shawn to add AWS Inspector as the planned scanning solution in the relevant policy. - Shawn
- Shawn to add email as the ticketing system in the appropriate policy section. - Shawn
- Shawn to invite employees to acknowledge all finalized policies once they are approved and ready. - Shawn

(edited)



2 replies Last reply 5 months ago

Blux's SOC 2 Compliance Journey (A to Z)



블럭스의 SOC 2 인증 여정



September 3rd, 2024 – Cyber Matters와 온보딩

- 사이버 보안 컨설팅 전문 기업
- Drata CAP(Compliance Accelerator Program)의 일환으로 Drata 측에서 블럭스와 연결해준 기업
- 호주에 팀이 있어서 아시아 고객들과 비슷한 시간대에 원활한 소통이 가능
- Slack Connect 제공



Sidra 12:25 PM

@channel Please review the Action Items from today's call:

Weekly Check-In Meeting Blux Notes 26 Sep 2024

- Zaid to provide a report with recommendations on getting controls ready, including evidences, policies, or screenshots to add. - Zaid
- Zaid and team to close the CAP program by next call and provide system description and CAP end report in the week after - Zaid
- Shawn to review and fill in information for the Business Impact Analysis tables in the Business Continuity Plan policy. - Shawn
- Zaid to confirm with his consultant about the Change Management policy template and get back to Shawn. - Zaid
- Zaid to confirm with his consultant about the Information Exchange section in the Data Protection policy and get back to Shawn. - Zaid
- Shawn to fill in the data retention table with AWS as the storage location. - Shawn
- Shawn to add AWS Inspector as the planned scanning solution in the relevant policy. - Shawn
- Shawn to add email as the ticketing system in the appropriate policy section. - Shawn
- Shawn to invite employees to acknowledge all finalized policies once they are approved and ready. - Shawn

(edited)



2 replies Last reply 5 months ago

Zaid to confirm with his consultant about the Information Exchange section in the Data Protection policy and get back to Shawn. - Zaid
Shawn to fill in the data retention table with AWS as the storage location. - Shawn
Shawn to add AWS Inspector as the planned scanning solution in the relevant policy. - Shawn

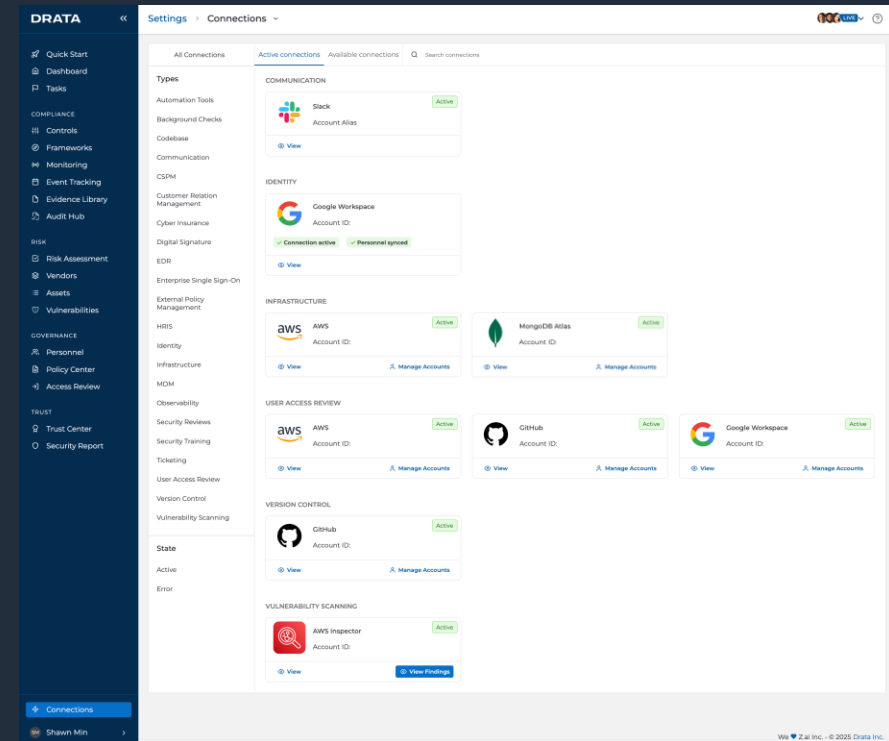
Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



September 3rd, 2024 ~ October 30th, 2024 – 보안 관련 필수 요구 사항 수행

- Connections 생성



Blux's SOC 2 Compliance Journey (A to Z)


블럭스의 SOC 2 인증 여정



September 3rd, 2024 ~ October 30th, 2024 – 보안 관련 필수 요구 사항 수행

- Connections 생성


VERSION CONTROL

 **GitHub** Active

Account ID:

[View](#) [Manage Accounts](#)

VULNERABILITY SCANNING

 **AWS Inspector** Active

Account ID:

[View](#) [View Findings](#)


DRATA Settings > Connections

All Connections Active connections Available connections Search connections

Types

- Automation Tools
- Background Checks
- Codebase
- Communication
- CSRM
- Customer Relation Management
- Cyber Insurance
- Digital Signature
- EDR
- Enterprise Single Sign-On
- External Policy Management
- HRIS
- Identity
- Infrastructure
- MDM
- Observability
- Security Reviews
- Security Training
- Ticketing
- User Access Review
- Version Control
- Vulnerability Scanning


COMMUNICATION

 **Slack** Active

Account Alias:

[View](#)

IDENTITY


 **Google Workspace**

Account ID:

✓ Connection active ✓ Personnel synced


[View](#)

INFRASTRUCTURE

 **AWS** Active

Account ID:


[View](#) [Manage Accounts](#)

 **MongoDB Atlas** Active

Account ID:


[View](#) [Manage Accounts](#)

USER ACCESS REVIEW

 **AWS** Active


Account ID:

[View](#) [Manage Accounts](#)

 **GitHub** Active

Account ID:


[View](#) [Manage Accounts](#)

 **Google Workspace** Active

Account ID:

[View](#) [Manage Accounts](#)


VERSION CONTROL

 **GitHub** Active

Account ID:

[View](#) [Manage Accounts](#)

VULNERABILITY SCANNING

 **AWS Inspector** Active

Account ID:

[View](#) [View Findings](#)

Connections

Show Min

Ver 2.0.0 Inc. © 2025 Drata Inc.

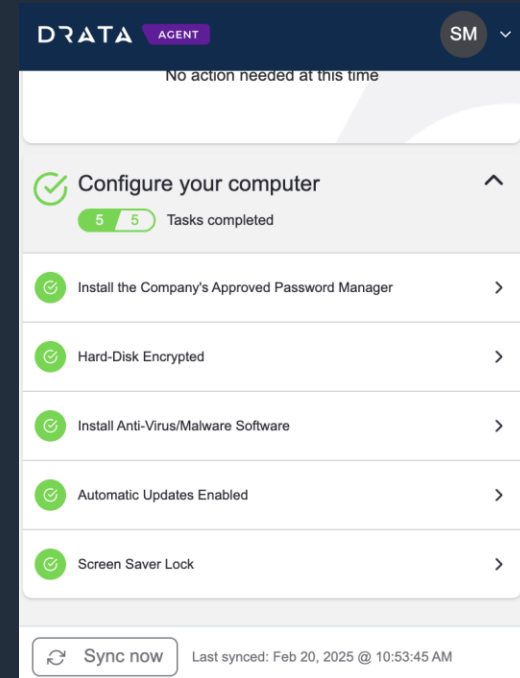
Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



September 3rd, 2024 ~ October 30th, 2024 – 보안 관련 필수 요구 사항 수행

- Connections 생성
- 구성원 보안 수준 제고
 - Antivirus Software
 - Hard Disk Encryption
 - Screen Saver Lock
 - Security Training (Annually)



























Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



September 3rd, 2024 ~ October 30th, 2024 – 보안 관련 필수 요구 사항 수행

- Policy 및 Documentation 준비

| | Policy name ^ | Version | Status | Creation date | Approved date | Published date | Renewal date |
|---|----------------------------|---------|-----------|------------------------|---------------|----------------|--------------|
|    | Acceptable Use Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
|    | Asset Management Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
|    | Backup Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
|    | Business Continuity Plan | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 23, 2025 |
|    | Change Management Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
|    | Code of Conduct | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 20, 2025 |
|    | Data Classification Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
|    | Data Protection Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 20, 2025 |
|    | Data Retention Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 20, 2025 |

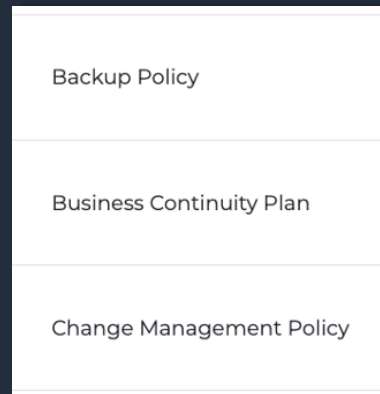
Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



September 3rd, 2024 ~ October 30th, 2024 – 보안 관련 필수 요구 사항 수행


- Policy 및 Documentation 준비



| Policy name ^ | Version | Status | Creation date | Approved date | Published date | Renewal date |
|----------------------------|---------|-----------|------------------------|---------------|----------------|--------------|
| Acceptable Use Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
| Asset Management Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
| Backup Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
| Business Continuity Plan | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 23, 2025 |
| Change Management Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
| Code of Conduct | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 20, 2025 |
| Data Classification Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 18, 2025 |
| Data Protection Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 20, 2025 |
| Data Retention Policy | V1 | Published | 5 months ago via Drata | Oct 2, 2024 | Oct 2, 2024 | Sep 20, 2025 |

Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정

 September 3rd, 2024 ~ October 30th, 2024 – 보안 관련 필수 요구 사항 수행

- Policy 및 Documentation 준비
- Risk Assessment 및 Test/Plan 준비







| | Risk | | Treatment |
|---|--|--|---|
| Name | Critical System Dependencies - DoS (R-05) | | A treatment for R-05 |
| Description | An attacker uses DoS attacks against critical information systems, components, or supporting infrastructures, based on the attacker's knowledge of dependencies. | | Utilize rate-based rule of AWS WAF to mitigate the impact of potential DoS attacks on critical systems. |
| Impact (Out of 5) / Likelihood (Out of 5) | 4 / 4 | | 3 / 2 |
| Treatment Completion Date | - | | September 16th, 2024 |

Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정





September 3rd, 2024 ~ October 30th, 2024 – 보안 관련 필수 요구 사항 수행

- Policy 및 Documentation 준비
- Risk Assessment 및 Test/Plan 준비
- 클라우드 보안 관련 주요 조치 수행
 - AWS CloudTrail 
 - Amazon Inspector 
 - Amazon GuardDuty 
 - AWS WAF 
 - Amazon S3 Bucket Versioning 
 - Security Group – IP 주소 기반 접근 제한 설정 

AWS Security Services Comparison

AWS 보안 서비스 비교

| Service | Description | Use Cases of Blux |
|---|---|---|
|  AWS CloudTrail | AWS 계정 내 사용자 활동 및 API 호출 기록 을 제공하는 감사 서비스 | <ul style="list-style-type: none">- AWS 계정 내 누가, 언제, 어떤 작업을 수행했는지 확인- 보안 사고 발생 시 과거 기록을 분석하여 원인 파악 |
|  Amazon Inspector | AWS 환경 내 취약점 및 잘못된 설정 을 자동으로 분석하는 보안 평가 서비스 | <ul style="list-style-type: none">- EC2 인스턴스 및 컨테이너 이미지의 취약점 자동 스캔 및 수정 |
|  Amazon GuardDuty | AWS 환경 내 위협 을 자동으로 탐지하는 보안 모니터링 서비스 | <ul style="list-style-type: none">- 비정상적인 로그인 시도 및 악성 활동 탐지- EKS 클러스터, S3 버킷 등에 대한 의심스러운 액세스 감지 |



AWS WAF (Web Application Firewall)

- 악성 트래픽 및 보안 위협으로부터 웹 애플리케이션을 보호하는 방화벽 서비스
 - ALB, API Gateway, CloudFront 등 보호 가능
- 주요 기능
 - **AWS Managed Rule Groups** 지원
 - 특정 IP 또는 국가별 요청 제한 가능
 - **Rate Limiting** → DDoS 등 과도한 요청 차단



AWS WAF Workshop (실습)

Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



November 29th, 2024 – AssuranceLab과 킥오프 미팅

- Drata에서 연결해준 감사 파트너 기업
- 다양한 감사 프레임워크 제공: SOC 1, SOC 2, ISO 27001, ISO 42001, CSA STAR, HIPAA 등 다양한 국제 표준에 대한 인증 서비스를 제공



Changing the world of
compliance audits

We support over 800 ambitious technology companies in 30+ countries looking to earn and keep the trust of their dream customers.



Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



November 29th, 2024 ~ December 18th, 2024 – AssuranceLab과 SOC 2 Type 1 Audit 진행



Brandon Green
to Shawn ▾

Fri, Dec 6, 2024, 10:07 AM ★ ↩ ⋮

Hi Shawn,

Hope you've had a great week so far! I've completed a review of the AI audit findings, and we now have a testing percentage of 77% with 18 controls pending your review.

You can view the results in [this folder](#), and upload evidence into the "additional evidence" sub-folder.

If you imagine any of my queries involving a back-and-forth discussion, feel free to discuss with me over email, or we can jump on another call.

Kind regards,
Brandon



Brandon Green

Consultant
he/him/his |
AssuranceLab



brandon@assurancelab.cpa

<https://assurancelab.cpa>

Lvl 3/11 York Street, Sydney, Australia

1400 Lavaca Street, Suite 700 Austin,
Texas 78702

Liability limited by a scheme approved under Professional Standards Legislation.

AssuranceLab is a B-Corporation. We are committed to social and environmental performance, public transparency, and legal accountability to balance profit and purpose.

Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



November 29th, 2024 ~ December 18th, 2024 – AssuranceLab과 SOC 2 Type 1 Audit 진행



Brandon Green
to Shawn

Fri, Dec 6, 2024, 10:07 AM

Hi Shawn,

Hope you've had a great week so far! I've completed a review of the AI audit findings, and we now have a testing percentage of 77% with 18 controls pending your review.

You can view the results in [this folder](#), and upload evidence into the "additional evidence" sub-folder.

If you imagine any of my queries involving a back-and-forth discussion, feel free to discuss with me over email, or we can jump on another call.

Kind regards,
Brandon

Hope you've had a great week so far! I've completed a review of the AI audit findings, and we now have a testing percentage of 77% with 18 controls pending your review.

Texas 78702

*Liability limited by a scheme approved under Professional Standards Legislation.
AssuranceLab is a B-Corporation. We are committed to social and environmental performance, public transparency, and legal accountability to balance profit and purpose.*

Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



November 29th, 2024 ~ December 18th, 2024 – AssuranceLab과 SOC 2 Type 1 Audit 진행

| Assurance LAB | | Z.ai | | Software as a Service System | | SOC 2 Type 1 | | Status | |
|------------------|----------|---|----------------------------------|------------------------------|--------|--|--|-----------------|--|
| AI Audit Results | | | | | | | | Pass | |
| | | | | | | | | Incomplete/Fail | |
| | | | | | | | | Descoped | |
| | | | | | | | | Percentage | |
| AL ID | Drata ID | Control Description | Type | Type - cont. | Result | Query | Client Replies - Please reply to queries here. | Auditor | |
| CHM04_1 | DCF-4 | Z.ai uses a version control system to manage source code, documentation, release labelling, and other change management tasks. | Verified by Drata - Auto Test | General | Pass | | | | |
| CHM05 | DCF-5 | When Z.ai's application code changes, code reviews and tests are performed by someone other than the person who made the code change. | Verified by Drata - Auto Test | General | Pass | | | | |
| CHM03_1 | DCF-6 | Only authorized Z.ai personnel can deploy changes into production. | Verified by Drata - Auto Test | General | Pass | Please provide Drata Autopilot report on 'Version Control Write Access To Production Code' or evidence of an approval process for releasing to production. | I have provided a screenshot of 'Drata - Event Tracking - Type: Autopilot Version Control Production Write Access' page, and the latest (Dec. 6th, 2024) Drata Autopilot report. | | |
| CHM09 | DCF-155 | Changes are automatically tested and approval flows are verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production. | Evidence Uploaded to the Control | Sample | Pass | Hi Team! Could you provide evidence of your CI/CD implementation OR If change management is a more manual process, we'll sample from a population of changes released within the examination period to confirm that changes are tested and approved. | I have provided screenshots of evidence of CI/CD using GitHub PRs, GitHub Actions, and Argo CD. | | |
| CHM03 | DCF-7 | Separate environments are used for testing and production for Z.ai's Software as a Service System. | Evidence Uploaded to the Control | General | Pass | Please provide the Drata Autopilot report with PASSED status for 'Separate Testing and Production Environments' OR A screenshot showing both environments configured. | I have provided screenshots showing both environments configured. | | |
| DIN02 | DCF-21 | Z.ai maintains an architecture diagram to document the system boundaries and support the functioning of internal control. | Evidence Uploaded to the Control | General | Pass | Please provide the necessary documentation to assess compliance with the control description. | I have provided an architecture diagram of our service. | | |
| AUT05 | DCF-75 | Access to cloud data storage is configured to restrict | Verified by Drata - | | | Please provide screenshots of limited access to | I have provided screenshots of a list of MongoDB | | |

Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



November 29th, 2024 ~ December 18th, 2024 – AssuranceLab과 SOC 2 Type 1 Audit 진행



| | A | B | C | D | E | F | G | H |
|----|---|----------------------------------|---|----------------------------------|---------|--|--|---|
| | Changes are automatically tested and approval flows are verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production. | Evidence Uploaded to the Control | Sample | Pass | | Hi Team! Could you provide evidence of your CI/CD implementation OR If change management is a more manual process, we'll sample from a population of changes released within the examination period to confirm that changes are tested and approved. | | I have provided screenshots of evidence of CI/CD using GitHub PRs, GitHub Actions, and Argo CD. |
| 10 | CHM09 | DCF-155 | Changes are automatically tested and approval flows are verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production. | Evidence Uploaded to the Control | Sample | Pass | Hi Team! Could you provide evidence of your CI/CD implementation OR If change management is a more manual process, we'll sample from a population of changes released within the examination period to confirm that changes are tested and approved. | I have provided screenshots of evidence of CI/CD using GitHub PRs, GitHub Actions, and Argo CD. |
| 11 | CHM03 | DCF-7 | Separate environments are used for testing and production for Z.ai's Software as a Service System. | Evidence Uploaded to the Control | General | Pass | Please provide the Drata Autopilot report with PASSED status for 'Separate Testing and Production Environments' OR A screenshot showing both environments configured. | I have provided screenshots showing both environments configured. |
| 12 | DIN02 | DCF-21 | Z.ai maintains an architecture diagram to document the system boundaries and support the functioning of internal control. | Evidence Uploaded to the Control | General | Pass | Please provide the necessary documentation to assess compliance with the control description. | I have provided an architecture diagram of our service. |
| | AUT05 | DCF-75 | Access to cloud data storage is configured to restrict | Verified by Drata - | | | Please provide screenshots of limited access to | I have provided screenshots of a list of MongoDB |

Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



December 18th, 2024 – SOC 2 Type 1 Report 발급



Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



December 19th, 2024 ~ March 18th, 2025 – AssuranceLab과 SOC 2 Type 2 Audit 진행

- 기본적으로는 Type 1 Audit과 동일한 절차로 진행되나, ‘보안 통제가 실제로 효과적으로 운영되고 있는가?’에 초점을 맞춰서 진행됨
- 각종 Plans 및 Tests
 - Incident Response Plans
 - Business Continuity and Disaster Recovery (BC/DR) Tests
- Sampling
 - Background Checks
 - Formal Offboarding Processes

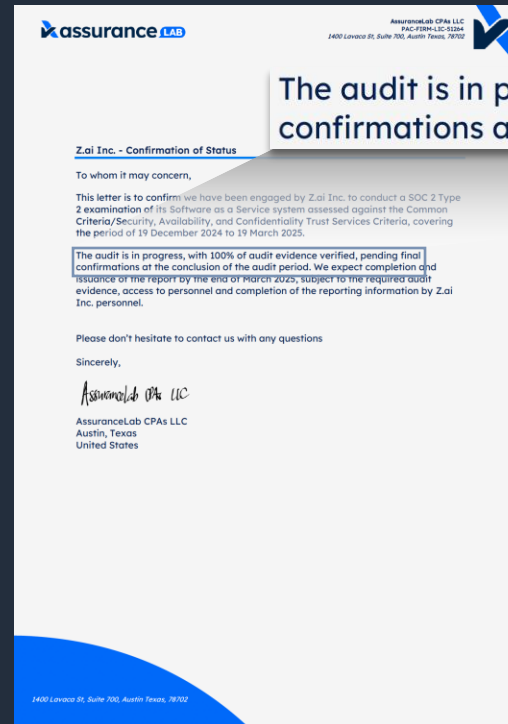


Blux's SOC 2 Compliance Journey (A to Z)

블럭스의 SOC 2 인증 여정



March 18th, 2025 – SOC 2 Type 2 Report 발급 (예정)



The audit is in progress, with 100% of audit evidence verified, pending final confirmations at the conclusion of the audit period.

Insights Gained from the SOC 2 Compliance Prep. Process

SOC 2 인증 준비 과정에서 얻은 인사이트

글로벌 감사 기관 및 외부 담당자와의 협업

- 장기전
 - 내부 일정 준수를 최우선으로 생각
- 적극성 ★★★★★
 - 사소한 부분이라도 그냥 넘어가지 말고 먼저 도움을 요청
 - 적극적인 대응이 상대방의 협조를 이끌어냄



Paola Postiglione
to Shawn,

Tue, Dec 24, 2024, 2:48 AM



Hi Shawn,

Thank you for reaching out and providing all the detailed context and screenshots—it's incredibly helpful! I'm currently looking into this for you and will circle back as soon as I have more information.

In the meantime, could you please enable **Remote App Access** in the upper right-hand corner of the Drata App? This will grant me and my technical team the ability to take a deeper look at the connection and the associated monitoring tests to better assist you.

I appreciate your patience as we investigate this further. Let me know if you have any trouble enabling access or if you have additional questions in the meantime!

Best,
Paola

—
Paola Postiglione

Customer Success Manager | Drata Inc.
[Contact Us](#) | [Love Drata?](#)
Ensuring the Future of Trust in the Cloud

Insights Gained from the SOC 2 Compliance Prep. Process

SOC 2 인증 준비 과정에서 얻은 인사이트

글로벌 감사 기관 및 외부 담당자와의 협업

- 장기전
 - 내부 일정 준수를 최우선으로 생각
- 적극성 ★★★★★
 - 사소한 부분이라도 그냥 넘어가지 말고 먼저 도움을 요청
 - Thank you for reaching out and providing all the detailed context and screenshots—it's incredibly helpful! I'm currently looking into this for you and will circle back as soon as I have more information.

In the meantime, could you please enable **Remote App Access** in the upper right-hand corner of the Drata App? This will grant me and my technical team the ability to take a deeper look at the connection and the associated monitoring tests to better assist you.



Paola Postiglione
to Shawn,
Hi Shawn,

Tue, Dec 24, 2024, 2:48 AM



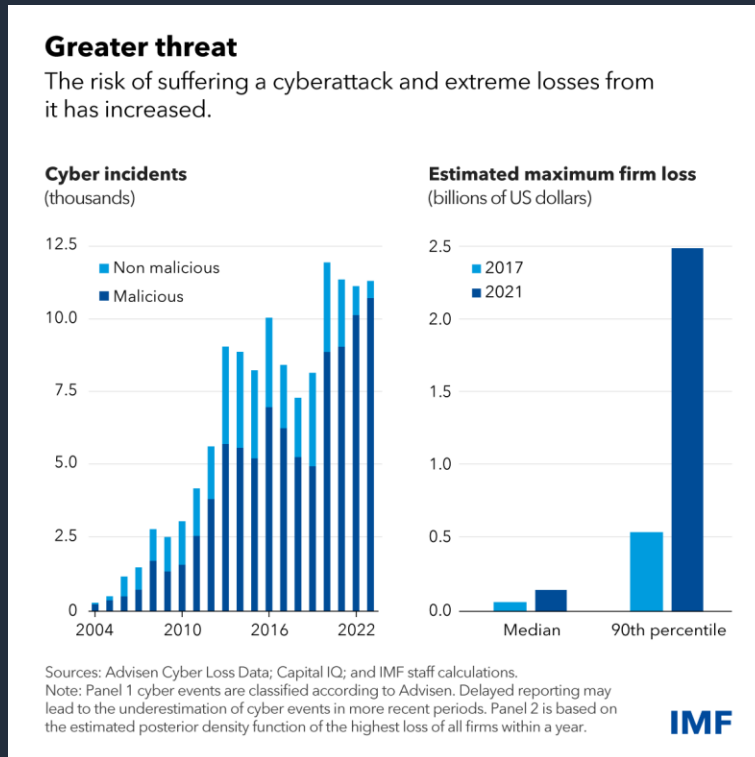
Thank you for reaching out and providing all the detailed context and screenshots—it's incredibly helpful! I'm currently looking into this for you and will circle back as soon as I have more information.

In the meantime, could you please enable **Remote App Access** in the upper right-hand corner of the Drata App? This will grant me and my technical team the ability to take a deeper look at the connection and the associated monitoring tests to better assist you.

I appreciate your patience as we investigate this further. Let me know if you have any trouble enabling

Insights Gained from the SOC 2 Compliance Prep. Process

SOC 2 인증 준비 과정에서 얻은 인사이트



품질과의 타협은 금물

- 단순히 인증 획득이 목표가 아닌, 실질적인 보안 강화에 집중

Insights Gained from the SOC 2 Compliance Prep. Process

SOC 2 인증 준비 과정에서 얻은 인사이트

AWS 파트너 되기

AWS Foundational Technical Review

AWS 파트너가 AWS에서 소프트웨어 검증하도록 지원

[AWS 파트너 네트워크 가입 >](#)

[APN 계정이 있으신가요? 로그인 >](#)

AWS Foundational Technical Review(FTR)를 이용하면 소프트웨어 또는 솔루션의 위험을 식별하고 해결할 수 있습니다. 소프트웨어를 고객이 배포하거나 SaaS 솔루션으로 제공하는 경우 FTR을 사용하면 해당 소프트웨어 또는 솔루션에 특정한 AWS Well-Architected 모범 사례를 식별할 수 있습니다. FTR은 클라우드 여정의 모든 단계에서 크게 활용할 수 있는 셀프 서비스 검토 기능입니다. 승인 날짜로부터 2년 동안 유효하며, 무료로 수행해볼 수 있습니다. [시작하기 >](#)

| 위험 완화 | 셀프 서비스 프로세스 | 파트너 혜택에 액세스 | 'AWS에서 검토' 배지 획득 |
|---|--|---|--|
| FTR은 AWS Well-Architected Framework에서 정의한 보안, 안정성 및 운영 우수성에 대한 위험을 줄이기 위해 AWS 모범 사례의 하위 세트를 채택하기 위한 구체적인 지침을 제공합니다. | FTR은 AWS 파트너 솔루션 및 AWS 서비스를 활용하여 사용자 환경에서 잠재적인 문제 탐지를 자동화하는 방법을 안내합니다. | 여러 AWS 파트너 혜택(자금 지원, 전문성을 검증해주는 AWS 컴피턴시 프로그램 , 공동 판매를 지원하는 AWS ISV 촉진 프로그램 등)을 이용할 수 있습니다. | FTR 승인을 받으면 'AWS에서 검토' 솔루션 배지를 획득하고 AWS 파트너 솔루션 파인더에 소프트웨어가 등록되어 고객이 해당 제품을 쉽게 찾고 문의해볼 수 있습니다. |

품질과의 타협은 금물

- 단순히 인증 획득이 목표가 아닌, 실질적인 보안 강화에 집중
- **Best Practices** 기반으로 보안 수준을 지속적으로 개선
 - AWS FTR에 먼저 도전해보세요!



Insights Gained from the SOC 2 Compliance Prep. Process

SOC 2 인증 준비 과정에서 얻은 인사이트

AWS 파트너 되기

AWS Foundational Technical Review

AWS 파트너가 AWS에서 소프트웨어 검증하도록

[AWS 파트너 네트워크 가입 >](#)

[APN 계정이 있으신가요? 로그인 >](#)

AWS Foundational Technical Review(FTR)를 이용하면 소프트웨어 또는 솔루션의 위험을 식별하고 해결할 수 있습니다. 소프트웨어를 고객이 배포하거나 SaaS 솔루션으로 제공하는 경우 FTR을 사용하면 해당 소프트웨어 또는 솔루션에 특정한 AWS Well-Architected 모범 사례를 식별할 수 있습니다. FTR은 클라우드 여정의 모든 단계에서 크게 활용할 수 있는 셀프 서비스 검토 기능입니다. 승인 날짜로부터 2년 동안 유효하며, 무료로 수행해볼 수 있습니다. [시작하기 >](#)

| 위험 완화 | 셀프 서비스 프로세스 | 파트너 혜택에 액세스 | 'AWS에서 검토' 배지 획득 |
|---|--|---|--|
| FTR은 AWS Well-Architected Framework에서 정의한 보안, 안정성 및 운영 우수성에 대한 위험을 줄이기 위해 AWS 모범 사례의 하위 세트를 채택하기 위한 구체적인 지침을 제공합니다. | FTR은 AWS 파트너 솔루션 및 AWS 서비스를 활용하여 사용자 환경에서 잠재적인 문제 탐지를 자동화하는 방법을 안내합니다. | 여러 AWS 파트너 혜택(자금 지원, 전문성을 검증해주는 AWS 컴피턴시 프로그램 , 공동 판매를 지원하는 AWS ISV 촉진 프로그램 등)을 이용할 수 있습니다. | FTR 승인을 받으면 'AWS에서 검토' 솔루션 배지를 획득하고 AWS 파트너 솔루션 파인더에 소프트웨어가 등록되어 고객이 해당 제품을 쉽게 찾고 문의해볼 수 있습니다. |

품질과의 타협은 금물

- 단순히 인증 획득이 목표가 아닌, 실질적인 보안 강화에 집중
- **Best Practices** 기반으로 보안 수준을 지속적으로 개선
 - AWS FTR에 먼저 도전해보세요!



Wrap-up

마무리: BLUX가 SOC 2 인증을 통해 확보한 경쟁 우위

고객사와의 신뢰 구축

- 공신력 있는 보안 인증을 요구하는 기업 고객 확보
용이
- 고객 데이터 보호에 대한 신뢰도가 높아져 보안이
특히 중요한 산업(금융업, E-commerce 등)에서
유리



Wrap-up

마무리: BLUX가 SOC 2 인증을 통해 확보한 경쟁 우위

고객사와의 신뢰 구축

- 공신력 있는 보안 인증을 요구하는 기업 고객 확보 용이
- 고객 데이터 보호에 대한 신뢰도가 높아져 보안이 특히 중요한 산업(금융업, E-commerce 등)에서 유리



내부 보안 수준 강화 및 운영 효율성 향상

- 보안 프로세스 체계화로 보안 리스크 감소 및 효율적인 운영 가능
- Drata 등 자동화 도구를 활용하여 지속적인 모니터링 및 감사 대응 용이





여러분의 소중한 피드백을 기다립니다.
강연 종료 후, 강연 평가에 참여해주세요!



감사합니다