AI와 오픈소스로 완성하는
엔드포인트 하드닝

스타트업 보안팀이 **3일 만에**
CIS 벤치마크 하드닝을 완료한 이야기

2026.02.24

에잇퍼센트 소개

온투업(온라인투자연계금융업) 핀테크 플랫폼으로, 대출자와 투자자를 기술로 연결하는 P2P 금융 서비스입니다.
중금리 대출 시장을 개척하여 금융 사각지대를 해소합니다.

Our Mission

에잇퍼센트의 미션은 고객 가능성을 발견하고,
최적의 금융을 실현하는 것입니다.

가능성을
인정받고 싶은

대출자

이들을 **연결**하여
새로운 금융 기회를
펼칠 수 있게 합니다.

가능성을
넓히고 싶은

투자자

높은 보안 요구사항

금융 도메인 특성상 고객의 중요한 금융 데이터를 다루며, 이에 따른 엄격한 보안 규제 및 컴플라이언스 준수가 필수적으로 요구됩니다.

정대영

정보보호팀 팀장

에잇퍼센트 (8PERCENT)

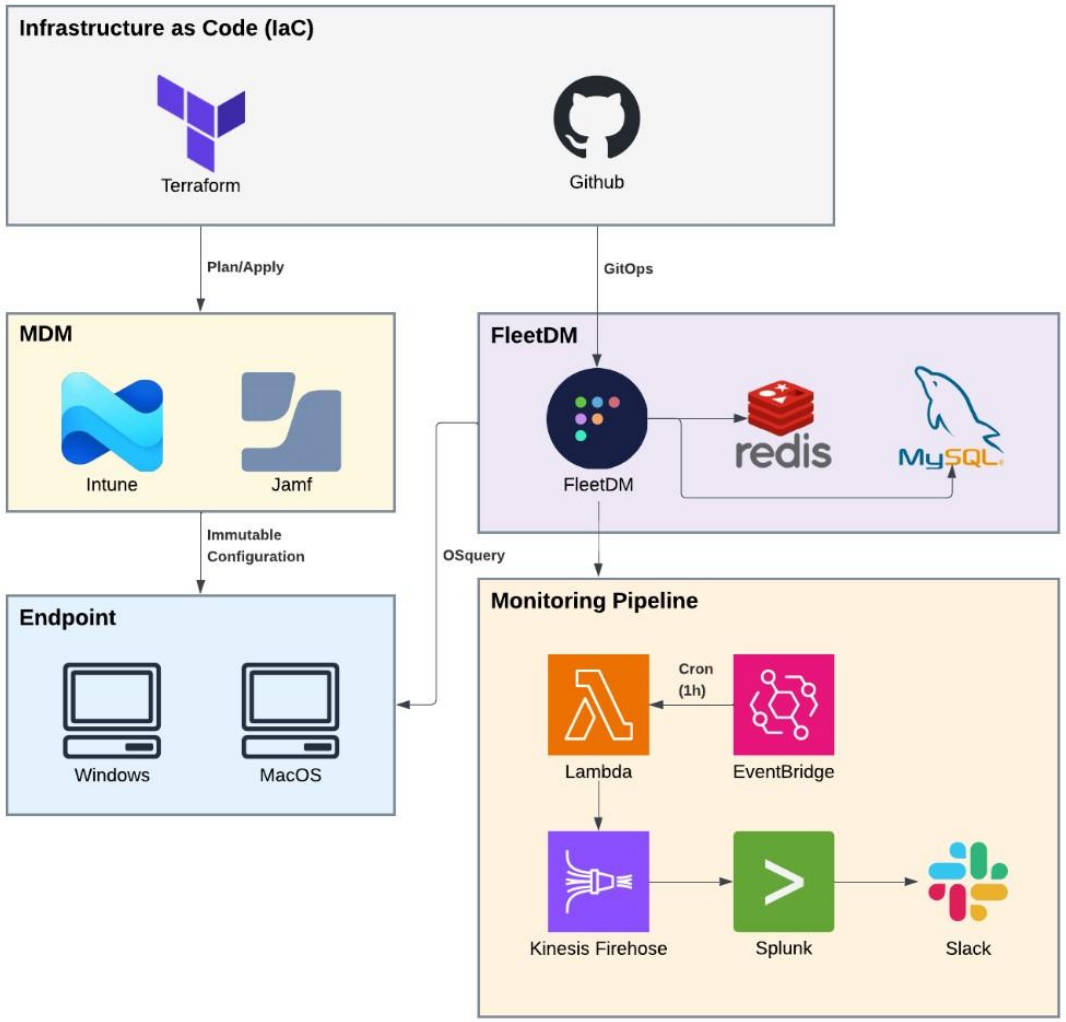
발표자 소개

- **에잇퍼센트 (3년+)**
  제로 트러스트 기반의 정보보호 관리 체계 수립 및 운영
- **스푼랩스 (3년)**
  기술 보안 매니저 - 엔드포인트 및 서비스 보안 체계 구축 및 운영
- **지니온 (4년)**
  정보보호 컨설팅 - 다양한 산업군의 모의해킹 및 컨설팅 수행

> *"작은 팀이기에 효율이 곧 생존입니다"*
>
> 한정된 인력과 예산이라는 제약 조건 속에서, 오픈소스와 자동화를 통해
> 최대의 보안 효과를 내는 방법을 고민합니다.

Agenda & 아키텍처 프리뷰

Architecture



Presentation Outline

1 **배경과 목표**
하드닝 기준 부재와 CIS 벤치마크 선택 배경

2 **도구 선택과 설계**
Fleet 도입 이유와 전체 아키텍처 설계

3 **하드닝 실행과 결과**
3-Tier 정책 분류와 실제 적용 결과

4 **총정리와 시사점**
프로젝트 성과 요약 및 향후 계획

현재 MDM 운영 방식 - 하이브리드

단일 솔루션으로 통합 시 기능 손실(Trade-off)이 발생하므로, 각 OS에 최적화된 이기종 MDM 운영이 현실적 최선입니다.

Windows Microsoft Intune

- ✓ Windows OS 네이티브 관리 최적화
  GPO, CSP 정책 완벽 호환 및 제로데이 지원
- ✓ Autopilot 등 배포 자동화 기능 우수
  Zero Touch 배포 구현 용이
- ✕ macOS 관리 기능의 한계
  Platform SSO 등 일부 최신 기능 지원 지연 또는 불안정
- ⚠ 단일 솔루션 통합 시 macOS 관리 비용 증가
  정책 관리, 패치 관리 등의 일부 기능 지원 미비로 우회 작업 증가

macOS Jamf Pro

- ✓ Apple 생태계 표준 MDM
  macOS 업데이트 즉시 지원 (Day-zero support)
- ✓ Zero-Touch Deployment
  ABM + Pre-Stage Enrollment 기반 macOS 네이티브 배포
- ✕ Windows OS 미지원
  Windows 관리를 위해서는 별도 솔루션 필수

엔드포인트 하드닝 기준의 부재

국내 주요 보안 가이드라인은 존재하지만, 업무용 PC(엔드포인트)에 대한 체계적인 기준은 부족합니다.

국내 가이드의 커버리지 한계

'주요정보통신기반시설' 가이드는 PC 기준이 있으나 극히 일부 설정에 불과하고,
'전자금융 기반시설 취약점 분석·평가' 가이드는
서버 기준 위주로 업무용 기기 보안 설정 기준은 존재하지 않습니다.

기반시설 지정 대상 여부

에잇퍼센트는 기반시설 지정 대상이 아니므로 해당 가이드의 강제성이 없으며,
단순 준수가 아닌 **실질적인 보안 강화**를 위한 체계적 기준이 필요했습니다.

글로벌 표준의 필요성

국내 가이드의 공백을 채우고 Windows/macOS 이기종 환경을 모두 아우르는
검증된 글로벌 보안 표준(Standard) 도입이 필수적이었습니다.

주요정보통신기반시설 취약점 가이드 — 제한적

PC/단말기 분야가 존재하지만 항목 수가 적고,
최신 OS 특화 설정 부족

전자금융 기반시설 취약점 분석·평가 가이드 — 부재

UNIX/Linux/Windows 서버 위주의 점검 항목.
업무용 단말기(엔드포인트) 기준 사실상 부재

ISMS-P 인증 기준 — 추상적

'단말기 보안' 통제 항목이 있으나,
구체적인 설정 값은 제시하지 않음

왜 CIS 벤치마크인가?

글로벌 전문가들의 합의를 바탕으로 한 표준인 CIS 벤치마크 L1 기본 달성을 1차 목표로 선정했습니다.

글로벌 보안 표준

CIS(Center for Internet Security)는 전 세계 전문가들의 합의로 만들어진
신뢰할 수 있는 보안 설정 가이드라인입니다.

1차 목표 선정

Windows와 macOS 이기종 환경에서 통일된 기준을 적용하며,
업무 생산성을 해치지 않는 Level 1을 우선 목표로 합니다.

국내 가이드 공백 보완

서버 중심의 국내 가이드라인이 커버하지 못하는
업무용 엔드포인트 영역의 구체적이고 체계적인 기준을 제공합니다.

CIS Benchmark

1차 목표

Level 1 (Basic)

대부분의 조직에 적용 가능한 기본 보안 설정.
시스템 성능이나 사용성에 큰 영향을 주지 않으면서
필수적인 보안 수준을 유지하는 항목들로 구성됨.

2차 목표

Level 2 (Advanced)

보안이 최우선인 환경을 위한 심화 설정.
일부 시스템 기능 사용이 제한될 수 있으며,
성능에 영향을 줄 수 있는 엄격한 항목 포함.

CIS 벤치마크 카테고리 구조

Windows (L1+BL) 371개 항목과 MacOS (L1) 87개 항목을 1차 목표로 선정하였습니다.

Windows 11

Benchmark v4.0.0

457
Items

Level 1 (337) BitLocker (34) Level 2 (86)

관리 템플릿 (Administrative Templates)	174
시스템 서비스 (System Services)	42
로컬 정책 보안 옵션 (Local Policies Security Options)	35
사용자 권한 (User Rights)	35
디펜더 (Defender)	32
+ 감사(Audit), 방화벽(Firewall), 장치 잠금(Device Lock) 등	139

macOS 15

Benchmark v2.0.0

124
Items

Level 1 (87) Level 2 (37)

시스템 설정 (System Settings)	70
시스템 접근, 인증 및 권한 부여	25
애플리케이션 (Application)	14
업데이트, 패치 및 추가 보안 소프트웨어 설치	6
로깅 및 감사	6
네트워크 구성	3

전통적 방식 vs 현대적 방식

현대적 방식은 변경 불가한 보안 설정을 배포하고, Drift를 실시간 감지하여 감사 대응까지 자동화합니다.

전통적 방식

Legacy

적용 방식

수동 설정 또는 일회성 스크립트 배포

점검 주기

분기/반기 단위 정기 점검

Drift(설정 변경) 대응

점검 때 발견하거나 미탐지 방치

변경 감지 및 추적

이력 없음 또는 수동 추적

감사(Audit) 대응

수작업 결과 취합 및 증적 생성

현대적 방식

Modern

적용 방식

MDM을 통한 Immutable Config 강제 배포

점검 주기

상시 모니터링 (Continuous Compliance)

Drift(설정 변경) 대응

PASS → FAIL 변경 시 실시간 알림

변경 감지 및 추적

GitOps로 모든 설정 변경 코드화 추적

감사(Audit) 대응

대시보드에서 즉시 현황 확인 및 증적 추출

점검 방법의 선택지와 한계

여러 가지 선택지를 고민했지만, Fleet이 속도·신뢰성·비용 모두를 만족하는 최적의 선택지였습니다

핵심 질문: "신뢰할 수 있는 CIS 점검 체계를, **합리적 비용**으로 **빠르게** 도입할 수 있는가?"

스크립트 재활용

속도 (Speed)
- 매우 빠름

신뢰도 (Reliability)
- 불확실

비용 (Cost)
- 매우 낮음 ($0)

GitHub 등에서 구한 스크립트는
CIS 벤치마크와 정확히
매핑되는지 검증 불가

직접 개발

속도 (Speed)
- 매우 느림

신뢰도 (Reliability)
- 높음 (직접 검증)

비용 (Cost)
- 인건비 높음

AI를 활용하더라도
450개 항목 스크립트 작성 및
유지보수 부담 과중

상용 솔루션

속도 (Speed)
- 빠름 (즉시 사용)

신뢰도 (Reliability)
- 매우 높음

비용 (Cost)
- 매우 높음

Tenable, Qualys 등은
훌륭하지만, 소규모 조직에겐
비용 장벽이 존재

CHOICE

Fleet (Open Source)

속도 (Speed)
- 빠름 (400+ 정책 내장)

신뢰도 (Reliability)
- 높음 (검증된 쿼리)

비용 (Cost)
- 낮음 (운영비 only)

CIS 공식 매핑 정책 기본 내장.
대규모 환경 검증 완료.
커스터마이징 유연성 확보.

역할 분담 설계

각 도구의 강점에 집중한 최적의 조합 (Best-of-Breed)을 토대로 AI를 이용하여 전 과정을 가속화하였습니다.

Intune & Jamf

MDM

- Immutable Config 배포
- OS/Software 업데이트 강제
- 최초 기기 세팅 및 앱 설치

Fleet

CORE

osquery Manager

- CIS 벤치마크 정책 점검
- 실시간 기기 상태 질의 (SQL)
- 데이터 생성 및 정규화

Splunk

Analytics & SIEM

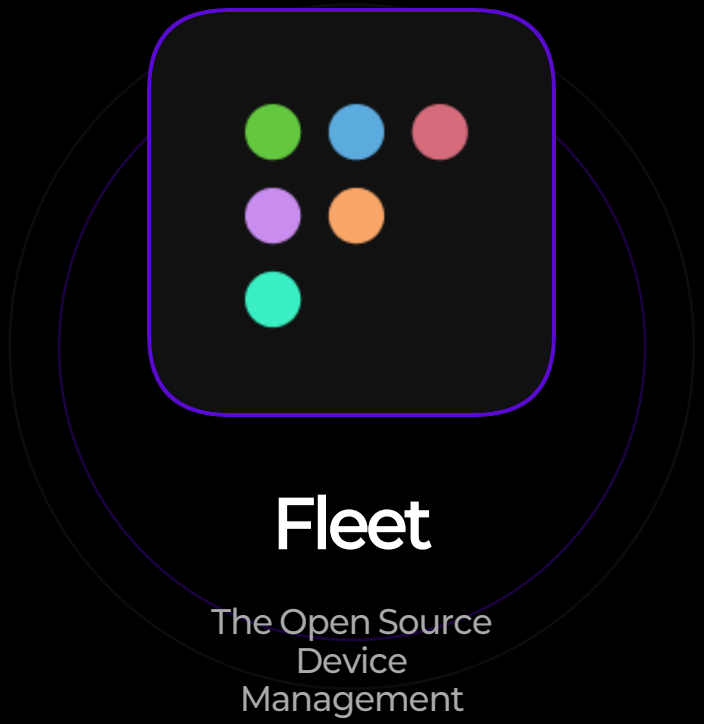
- Config Drift 탐지 및 알림
- 준수율 시각화 대시보드
- 감사 증적(Audit Log) 보관

AI 활용 방안

구축 과정 가속화 → 인프라 구성(IaC) | 보안 설정 구성 | 파이프라인 구성 | 대시보드 구성

Fleet 소개

CIS 벤치마크 정책이 내장된 오픈소스 MDM 플랫폼



CIS 벤치마크 기본 내장

400+ Policies

Windows와 macOS용 CIS 정책이 이미 포함되어 있습니다.
'fleetctl apply' 명령어 한 번으로 수백 개의 점검 항목을 즉시 배포하고 모니터링할 수 있습니다.

osquery 기반

SQL Query

Meta(Facebook)가 개발한 OSquery를 기반으로 작동합니다.
시스템 상태를 SQL 문법으로 질의하여, 가볍고 빠르며 정확한 데이터를 수집합니다.

강력한 Free 버전 (MIT)

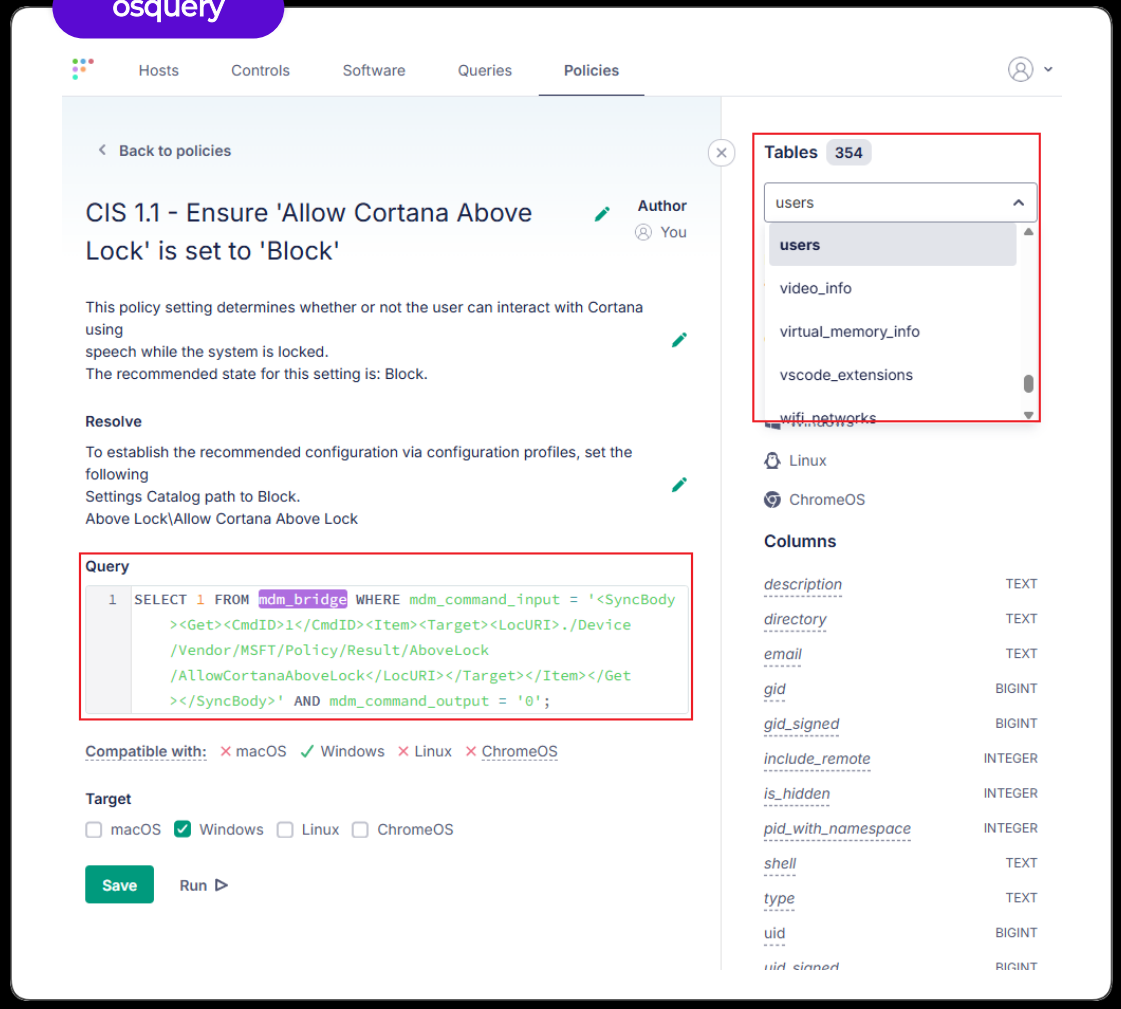
$0 License

오픈소스 버전에서도 MDM을 제외한 핵심 기능이 모두 제공됩니다.
정책 관리, GitOps 연동, REST API 등을 비용 없이 사용하여 엔터프라이즈급 운영이 가능합니다.

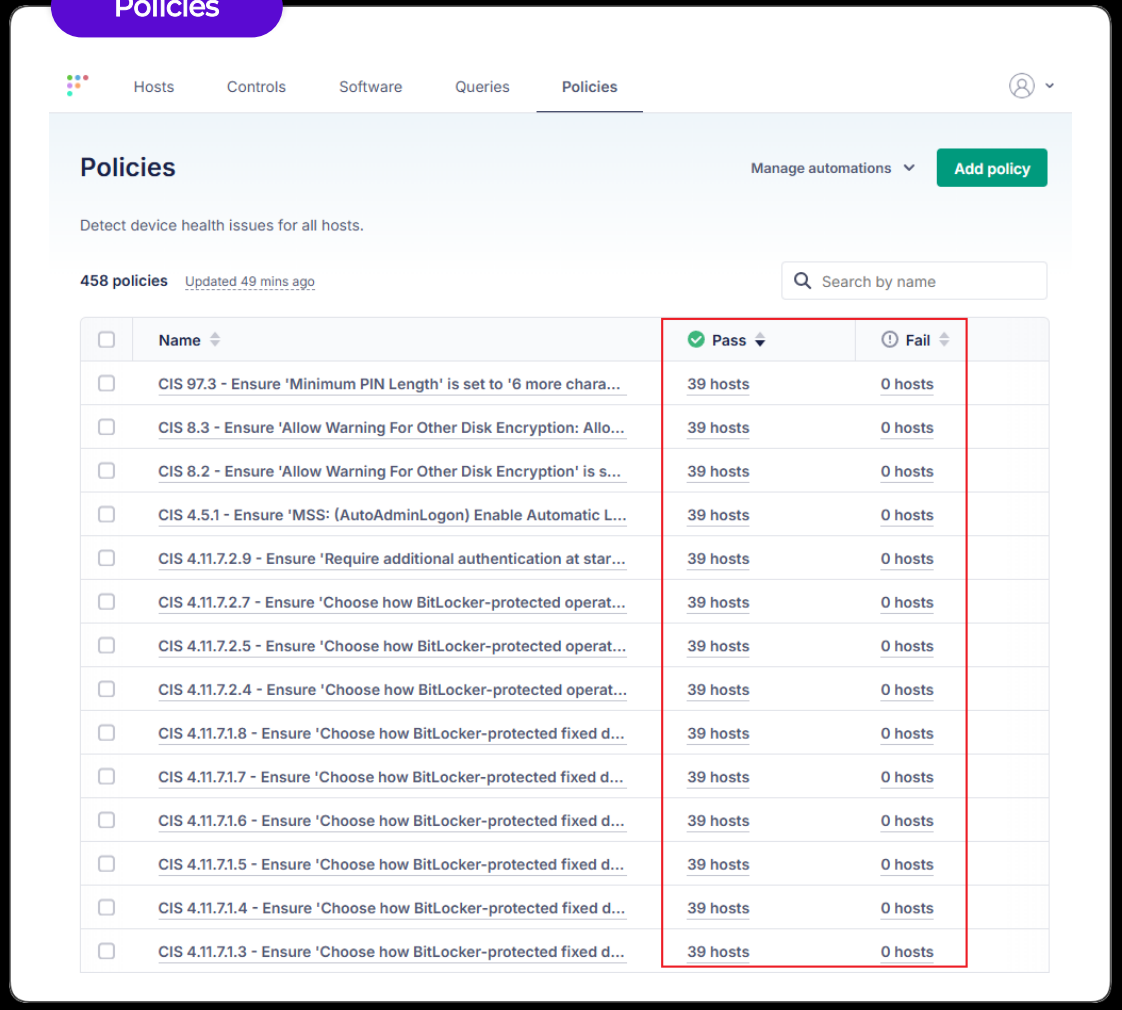
Fleet 핵심 기능

OS 종류와 관계없이 SQL 기반의 시스템 상태 조회를 토대로 정책 PASS / FAIL 여부를 판단합니다.

osquery



Policies



비용 정당성

오픈소스는 관리 복잡성이 요구되지만, AI가 진입 장벽을 현저히 낮춰주었습니다.

상용 도구 (Tenable/Qualys 등)

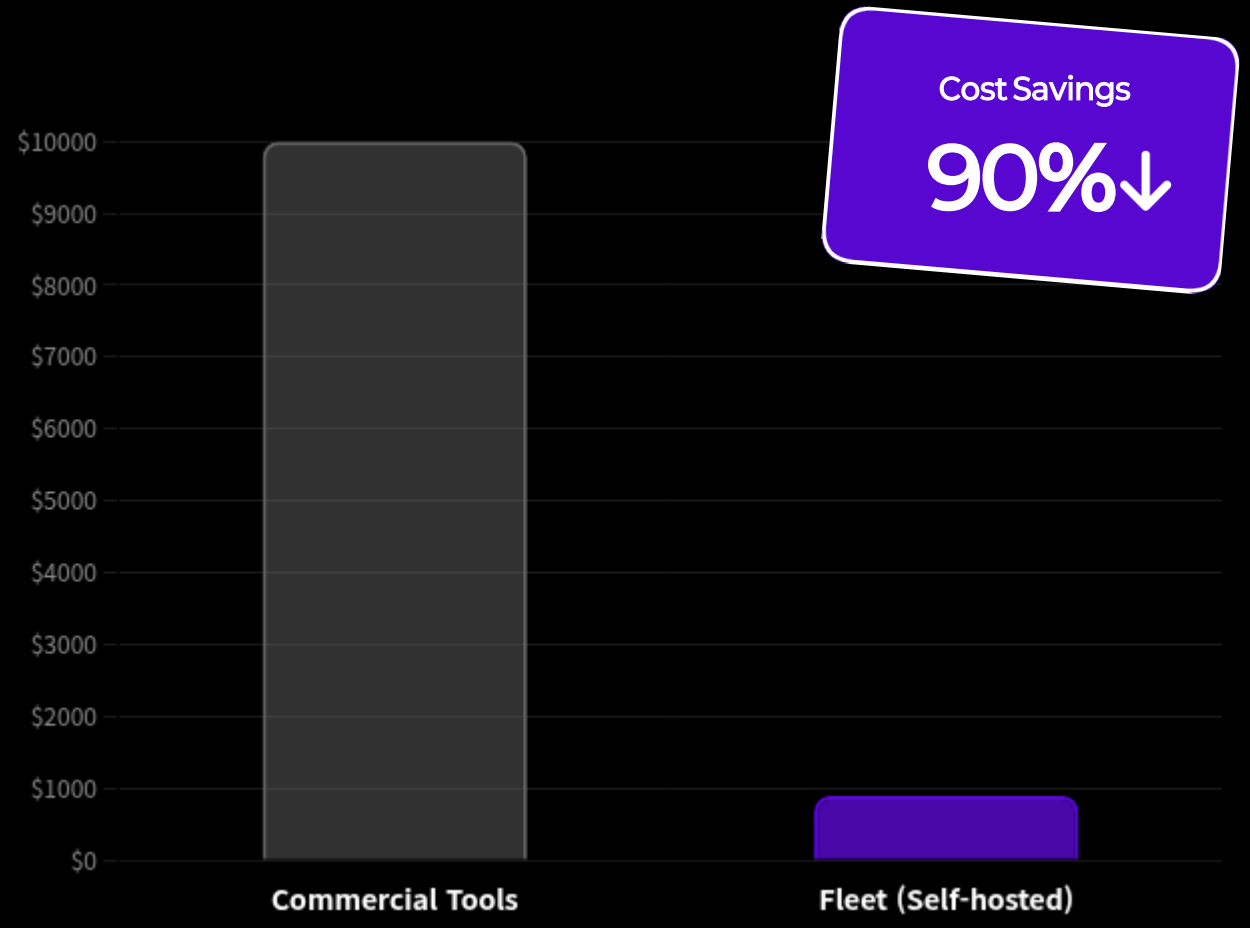
$5,000 ~ $10,000+

- 자산 수량 기반의 라이선스 / 높은 단가
- 서버 비용 또는 추가 모듈 구매 비용
- 지원 및 유지보수 포함

Fleet (Self-hosted)

~$900

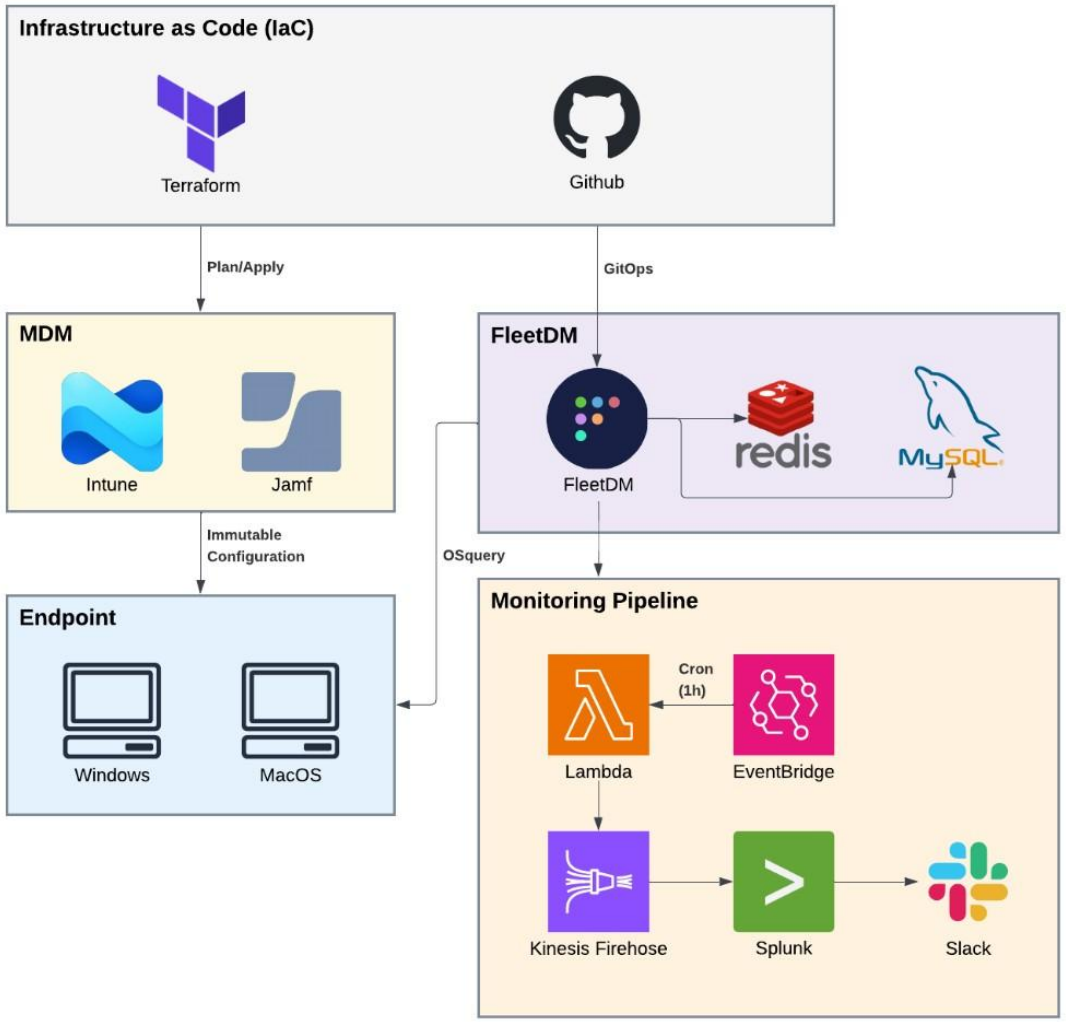
- 무료 라이선스 ($0)
- AWS EC2 (t3.medium) ~$480
- AWS Lambda & Data Transfer ~$240
- Others (Storage, etc.) ~$180



* 2025년 기준 공개 가격 및 AWS 서울 리전 요금 계산기 참고 (100~300대 기준)

아키텍처 리뷰

Architecture



AI와 함께 구성한 하드닝 완성 절차

1. Fleet 인프라 및 데이터 파이프라인 구성
2. 초기 점검 결과를 바탕으로 3-Tier 영향도 분석
3. Intune & Jamf 하드닝 적용
4. 개선 결과 확인

AI가 가속화한 구축 단계

인프라 구성부터 데이터 파이프라인, Splunk 대시보드와 알림 구성까지 AI와 함께 단 하루만에 완성하였습니다.

기존 방식 (Traditional)
2~3 Weeks → AI Accelerated ~ 1 Day

인프라 구성

Fleet 서버 및 DB 구축, Docker 설정

Before 2~3 Days
After 0.5 Day

AI Contribution
Docker Compose,
배포 스크립트 생성

데이터 파이프라인

Fleet → Lambda → Splunk 데이터 전송

Before 2~3 Days
After 0.25 Day

AI Contribution
Lambda 핸들러 코드 작성,
Splunk HEC 연동 로직

대시보드 & 알림

Splunk 시각화 및 Alert 구성

Before 2~3 Days
After 0.25 Day

AI Contribution
SPL(검색어) 쿼리 작성,
Simple XML 대시보드 생성

AI가 가속화한 하드닝 단계

초기 점검 실패 항목에 대해 3-Tier 영향도 분석 후 OIB/mSCP 정책과 매핑하여 보안 하드닝을 적용했습니다.

기존 방식 (Traditional)
Min 2~3 Weeks → Total Accelerated ~ 3 Days

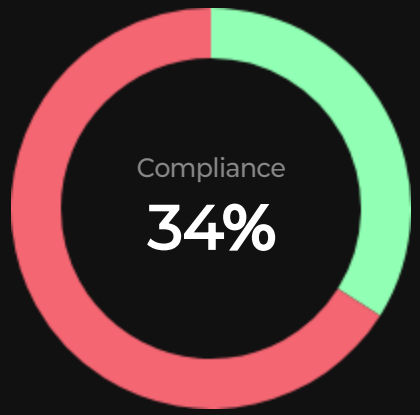
		Before	After	AI Contribution
매핑 분석	CIS ↔ OIB/mSCP 정책 매핑	1 Week	0.5 Day	CIS 문서와 배포 정책 자동 비교 분석
예외 분류 & 문서화	3-Tier 분류 및 사유 작성	2~3 Days	0.5 Day	항목별 영향도 분석 초안, 예외 사유 템플릿 작성
커스텀 정책 생성	추가 보안 정책 작성	1 Week	0.5 Day	추가 보안 설정 / Script 생성
쿼리 검증 & 디버깅	Fleet 쿼리 정확성 검증	Days	0.5 Day	OSquery SQL 구문 오류 탐지 및 수정 제안

"AI를 통해 빠른 분석 및 작업을 수행하고 **아키텍처 설계, 보안 정책 예외 결정, 근본 원인 분석 등**을 판단했습니다."

초기 점검 결과

Fleet 인프라 구성 후 초기 점검 결과 약 35%의 보안 기준선(Natural State)을 파악했습니다.

Windows 11



PASS	126
FAIL	245
Total	371

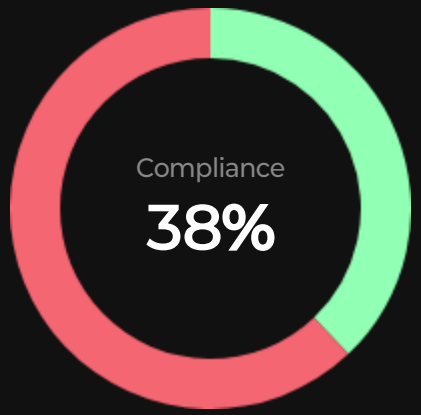
Total Failed Items

299

Risks Found

⚠ Start Point

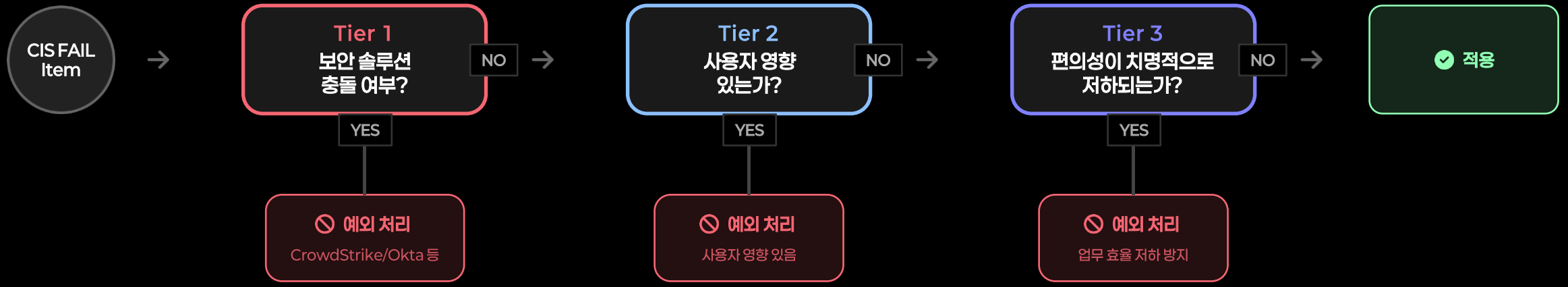
macOS 15



PASS	33
FAIL	54
Total	87

정책 적용 전략

AI에게 기존 보안 솔루션과 사용자 워크플로우 등 사내 맥락 정보를 제공한 뒤,
3-Tier 분류 체계를 활용하여 300여 개 CIS 벤치마크 항목의 정책 적용 리스크를 빠르게 파악했습니다.



설정 배포 및 적용 현황

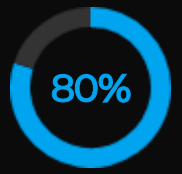
약 80%의 보안 설정 정책도 오픈 소스를 활용하여 적용하였으며, 약 20%는 AI와 협력하여 설정을 빠르게 적용하였습니다.

Windows

Open Source Project

OpenIntuneBaseline (OIB)

Microsoft Intune을 위한 커뮤니티 주도 보안 베이스라인 프로젝트



OIB를 통해 적용

사전 구성된 CIS 보안 설정 약 80%를 검토 후 즉시 적용

나머지 항목 (약 20%)

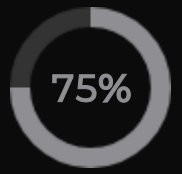
직접 구성한 Intune Configuration Profile로 적용

macOS

Open Source Project

mSCP (macOS Security Compliance Project)

Jamf가 참여한 미 연방 정부 표준 macOS 보안 규정 준수 프로젝트



Jamf Pro Compliance 기능으로 적용

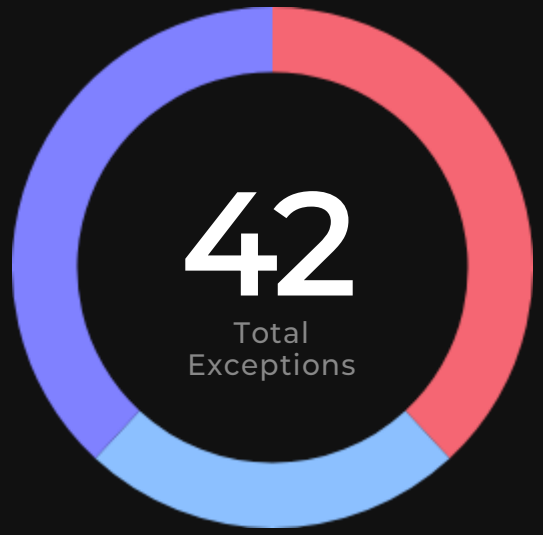
네이티브 기능을 이용하여 약 75%를 검토 후 즉시 적용

나머지 항목 (약 25%)

직접 구성한 Jamf Config Profile로 적용

예외 사항

3단계 분류를 통한 운영 환경에 리스크가 있는 14%의 항목은 예외 관리 범위로 식별하였습니다.



전체 FAIL 항목 중
14%에 해당하는 항목을
운영 환경을 고려하여 예외 처리함

Tier 1
16
Items

보안 솔루션 / 네이티브 기능 충돌

- CrowdStrike 충돌
- Windows 업데이트 링
- Okta 패스워드 규칙
- Enterprise 전용 기능

Tier 2
10
Items

사용자 영향 (업무 필수)

- IT 부서 원격 지원 업무
- 외근 시 핫스팟 이용
- BitLocker 외부의 보조저장매체
- 일반 사용자 앱 설치

Tier 3
16
Items

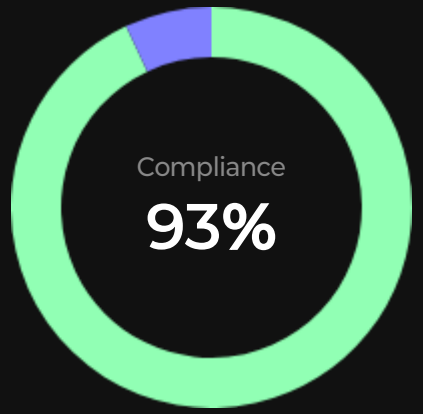
사용자 편의성 저하

- Autopilot 절차 방해
- Windows Hello 경험 방해
- 접근성 기능 방해
- 위치 기반 검색
- Apple Intelligence
- Windows PIN 패스워드 길이

개선 결과

전체 299개 항목에서 42개 예외를 제외한 나머지 적용 대상 100% 준수하도록 빠르게 개선하였습니다.

Windows 11



PASS	345
Exceptions	26
Total	371

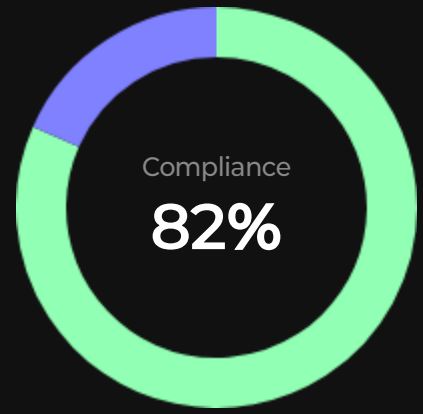
Authorized Exceptions

42

Total Items

Applicable Items 100% Compliant

macOS 15



PASS	71
Exceptions	16
Total	87

Config Drift 탐지 및 통합 모니터링

Fleet 주기적 점검 → API Polling → Splunk 통합 알림 체계

Challenge: Fleet Limitation

Config Drift와 통합 준수율 관리를 위해 Fleet 데이터를 대시보드로 구현해야 하는데, 해당 기능을 제공하지 않음 → **주기적 API 폴링 스크립트로 해결**

Data Pipeline Workflow

Fleet Server
Data Source

↓

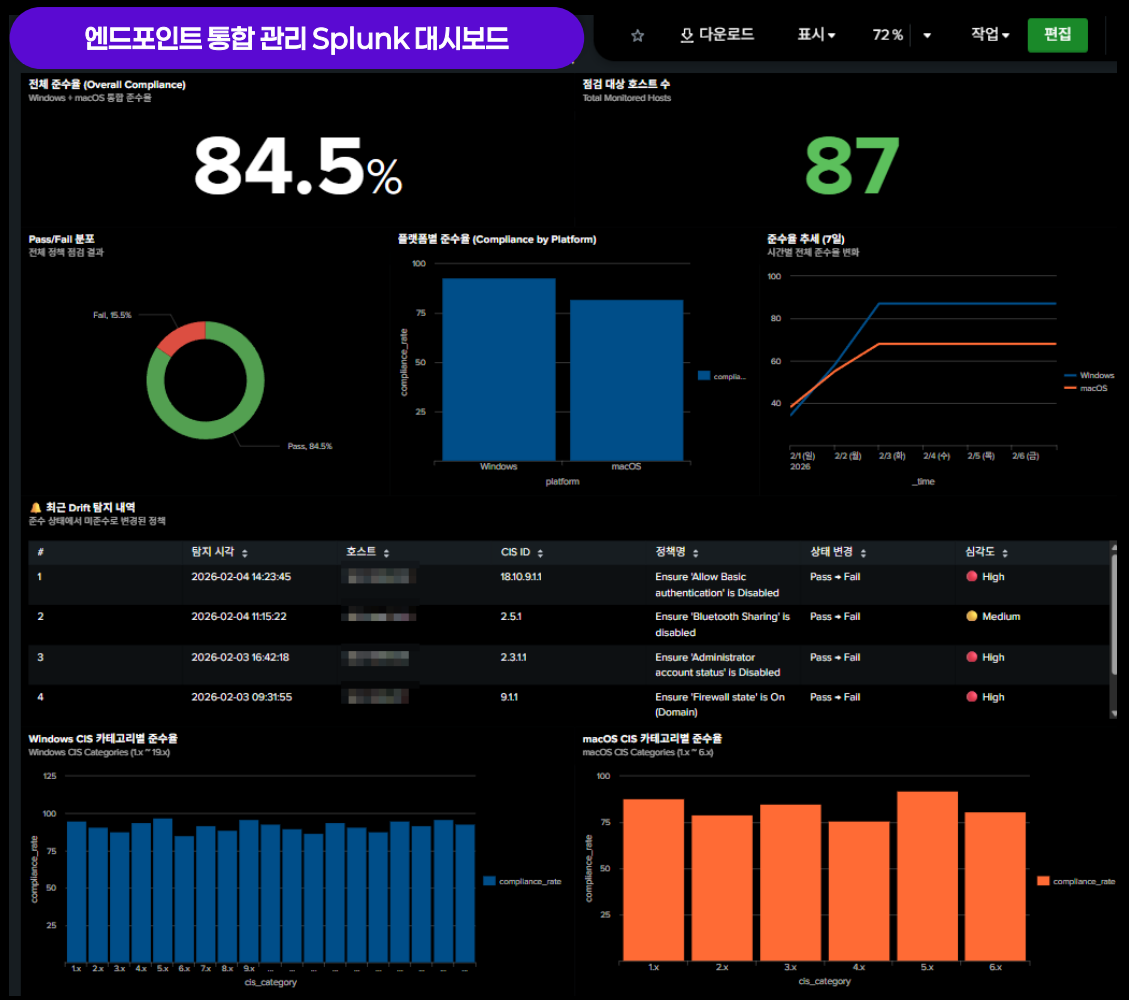
Cron Script
Periodic Polling (1h)

↓

Lambda
Data Formatting

↓

Splunk
Dashboard & Alert



결과 요약

3일, $900, 100% - 목표했던 현대적 보안 관리 달성

Time to Build

3 Days

↓ 80% Faster

From 2~3 Weeks (AI Accelerated)

Annual Cost

~$900

↓ 90% Saved

vs. Commercial Tools ($10K+)

Target Compliance

100%

✓ CIS L1 Ready

Win 93% / macOS 82%

모던 엔드포인트 보안 요구 사항

- ✓ Immutable Config
- ✓ Continuous Monitoring
- ✓ Drift Alert (Real-time)
- ✓ GitOps Tracking
- ✓ Audit Dashboard

시사점

이번 프로젝트를 통해 얻은 세 가지 핵심 메시지

01

신뢰된 점검 도구의 빠른 도입이 핵심

직접 개발하는 시간과 비용을 줄이고, Fleet과 같이 CIS 정책이 내장된 검증된 오픈소스를 활용하여 즉시 기준선을 확보해야 합니다.

✓검증된 정책 사용 + 저비용 고효율

02

AI는 대체가 아니라 강력한 가속기

아키텍처 설계와 보안 의사결정은 여전히 사람의 영역입니다. AI는 코드 생성, 데이터 분석 등 구현 단계를 가속화하여 전체 일정을 획기적으로 단축합니다.

⚡사람(설계) + AI(구현) = 10x 속도

03

보안 진입 장벽의 획기적인 하락

과거에는 막대한 예산과 인력이 필요했던 글로벌 표준 하드닝이, 이제는 소규모 보안팀도 AI와 오픈소스를 통해 충분히 달성 가능한 목표가 되었습니다.

📈 누구나 시작할 수 있는 보안

향후 계획

보안 수준의 심화(Level 2), 운영의 자동화(Remediation), 그리고 인프라 자체의 보안 강화

Phase 01

CIS Level 2 Coverage 확대

기본적인 Level 1 보안 설정을 넘어, 심층 방어 (Defense-in-depth)를 위한 CIS Level 2 벤치마크 항목으로 점검 대상을 점진적으로 확대합니다.

- 시스템 감사 정책 강화
- 불필요한 레거시 프로토콜 차단
- 브라우저 보안 설정 심화

Phase 02

Config Drift 자동 교정

단순 탐지 및 알림을 넘어, 설정 이탈(Drift) 발생 시 MDM 및 Fleet을 통해 자동으로 올바른 설정으로 복구하는 체계를 구축합니다.

- Self-healing 메커니즘 구현
- 운영자 개입 없는 Zero-touch 복구
- 교정 이력 자동 로깅

Phase 03

인프라 하드닝 강화

엔드포인트를 관리하는 중앙 서버(Fleet Server, Splunk, CI/CD Pipeline) 자체에 대한 보안을 강화하여 관리 체계의 무결성을 확보합니다.

- 관리 서버 CIS Server 하드닝
- Pipeline 보안(Supply Chain) 강화
- 접근 제어 및 감사 로그 고도화

감사합니다

경청해 주셔서 감사합니다.

Q&A: 무엇이든 질문해 주세요