CompIOps를 소개합니다.

ft. Integration & Automation

Security Compliance Analyst | Security Compliance Team

Yohan Kim

September 2025

HYPERCONNECT®

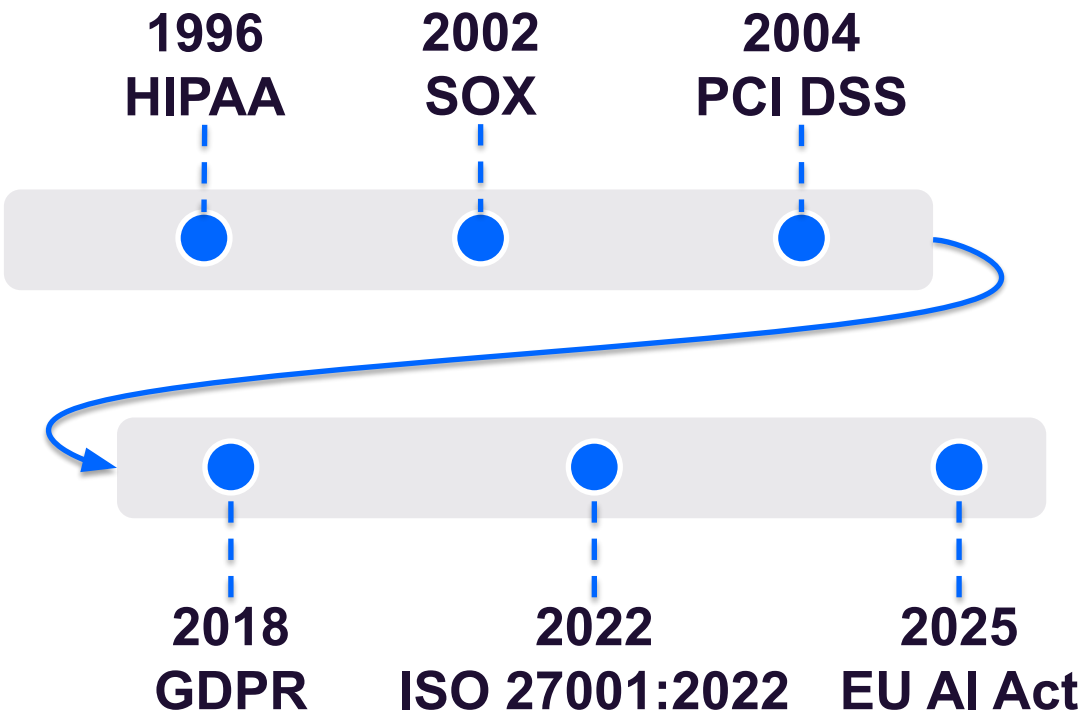
TABLE OF CONTENTS

1. CompIOps를 소개합니다

보안 컴플라이언스를 준수하는
데에는
많은 어려움이 있습니다

변화하는 시대 흐름

전세계적인 보안 컴플라이언스 요구사항 증가



최신 기술 사용의 증가

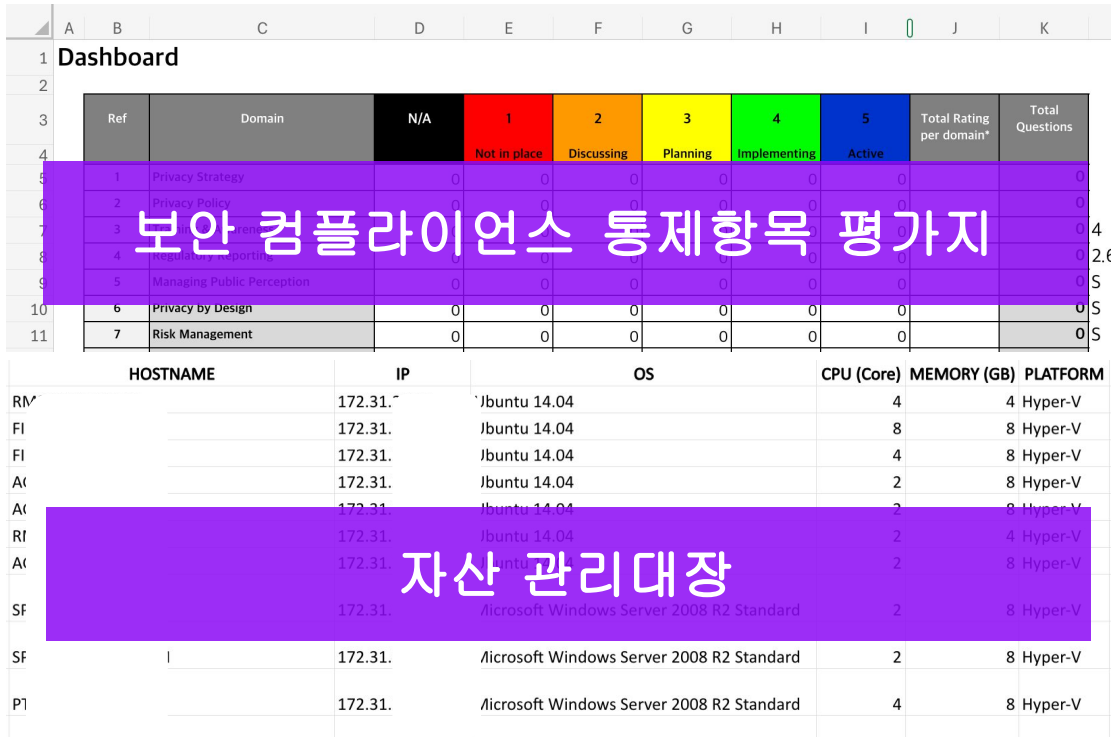
Services	2024 Spending	2024 Growth(%)	2025 Spending	2025 Growth(%)
Cloud PaaS	172,449	20.6	211,589	22.7
Cloud SaaS	247,203	20.0	295,083	19.4
Cloud DaaS	3,062	13.1	3,437	12.3
Cloud IaaS	180,044	25.6	232,391	29.1
Total Market	675,433	20.4	824,763	22.1

(Millions of U.S. Dollars)

출처: Gartner (May. 2024) Worldwide Public Cloud Services End-User Spending Forecast

기존 보안 컴플라이언스 운영 방법

OA 도구에 대한 높은 의존도 (a.k.a “ExcelOps”)



Dashboard

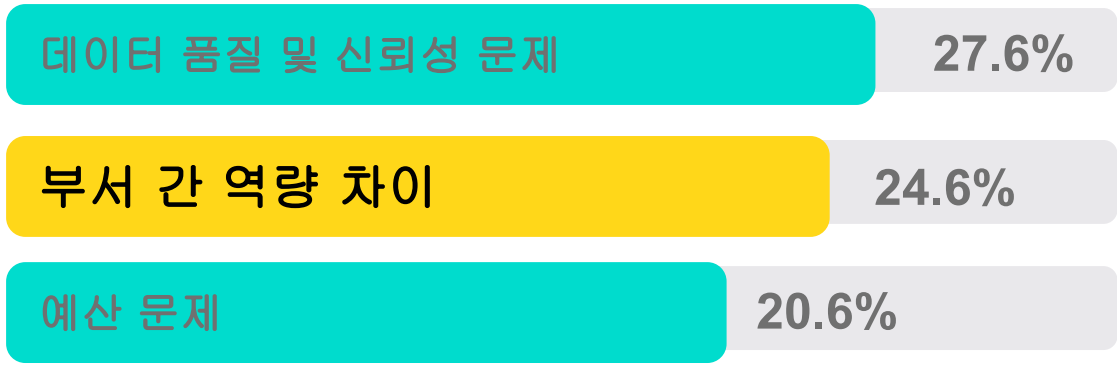
Ref	Domain	N/A	1 Not in place	2 Discussing	3 Planning	4 Implementing	5 Active	Total Rating per domain*	Total Questions
1	Privacy Strategy	0	0	0	0	0	0		0
2	Privacy Policy	0	0	0	0	0	0		0
3	[illegible]	0	0	0	0	0	0		0
4	Regulatory Reporting	0	0	0	0	0	0		0
5	Managing Public Perception	0	0	0	0	0	0		0
6	Privacy by Design	0	0	0	0	0	0		0
7	Risk Management	0	0	0	0	0	0		0

보안 컴플라이언스 통제항목 평가지

HOSTNAME	IP	OS	CPU (Core)	MEMORY (GB)	PLATFORM
RM	172.31.	Ubuntu 14.04	4	4	Hyper-V
FI	172.31.	Ubuntu 14.04	8	8	Hyper-V
FI	172.31.	Ubuntu 14.04	4	8	Hyper-V
A(	172.31.	Ubuntu 14.04	2	8	Hyper-V
A(	172.31.	Ubuntu 14.04	2	8	Hyper-V
RI	172.31.	Ubuntu 14.04	2	4	Hyper-V
A(	172.31.	Ubuntu 14.04	2	8	Hyper-V
SF	172.31.	Microsoft Windows Server 2008 R2 Standard	2	8	Hyper-V
SF	172.31.	Microsoft Windows Server 2008 R2 Standard	2	8	Hyper-V
PT	172.31.	Microsoft Windows Server 2008 R2 Standard	4	8	Hyper-V

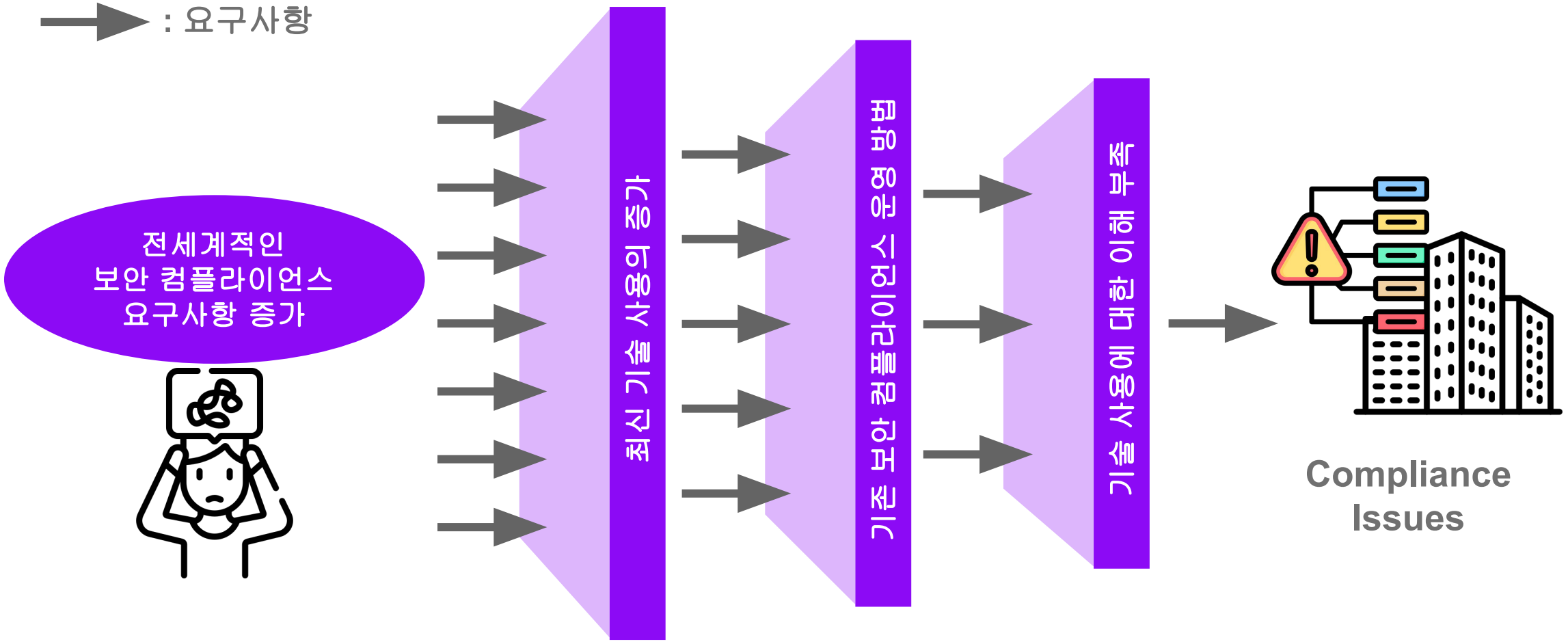
자산 관리대장

기술 사용에 대한 이해 부족



출처: EMA (Oct, 2021) NetSecOps: Aligning Networking and Security Teams to Ensure Digital Transformation

우리가 직면한 현재의 문제



그렇다면 현재 우리는 이러한 문제를
극복하기 위해
어떤 변화를 시도하고 있을까요?

Case Study - DB 백업 현황 점검

- **A.8.13 정보 백업**
- 정보, 소프트웨어 및 시스템의 백업 사본은 합의된 백업 관련 정책에 따라 유지되고 정기적으로 테스트되어야 한다.

대상 자산: **AWS RDS**

AWS Dynamo DB

담당자: **Data Team / DB 매니저**

초기: DB 매니저에게 점검 요청

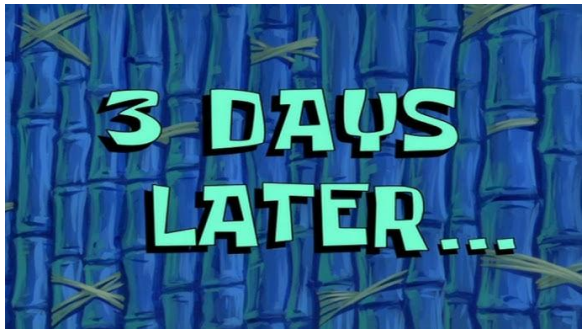
보안 컴플라이언스 운영 단계

Initial — 담당자에게 요청

Yohan.K (Yohan) Kim 5:06 PM

안녕하세요.

혹시 ISO 27001 대상 DB 자산들에 대해서 현재 백업 정책 현황을 확인해 주실 수 있을까요?



NoName 3:19 AM

앗, 죄송합니다! 바빠서 이 메시지를 놓쳤네요.

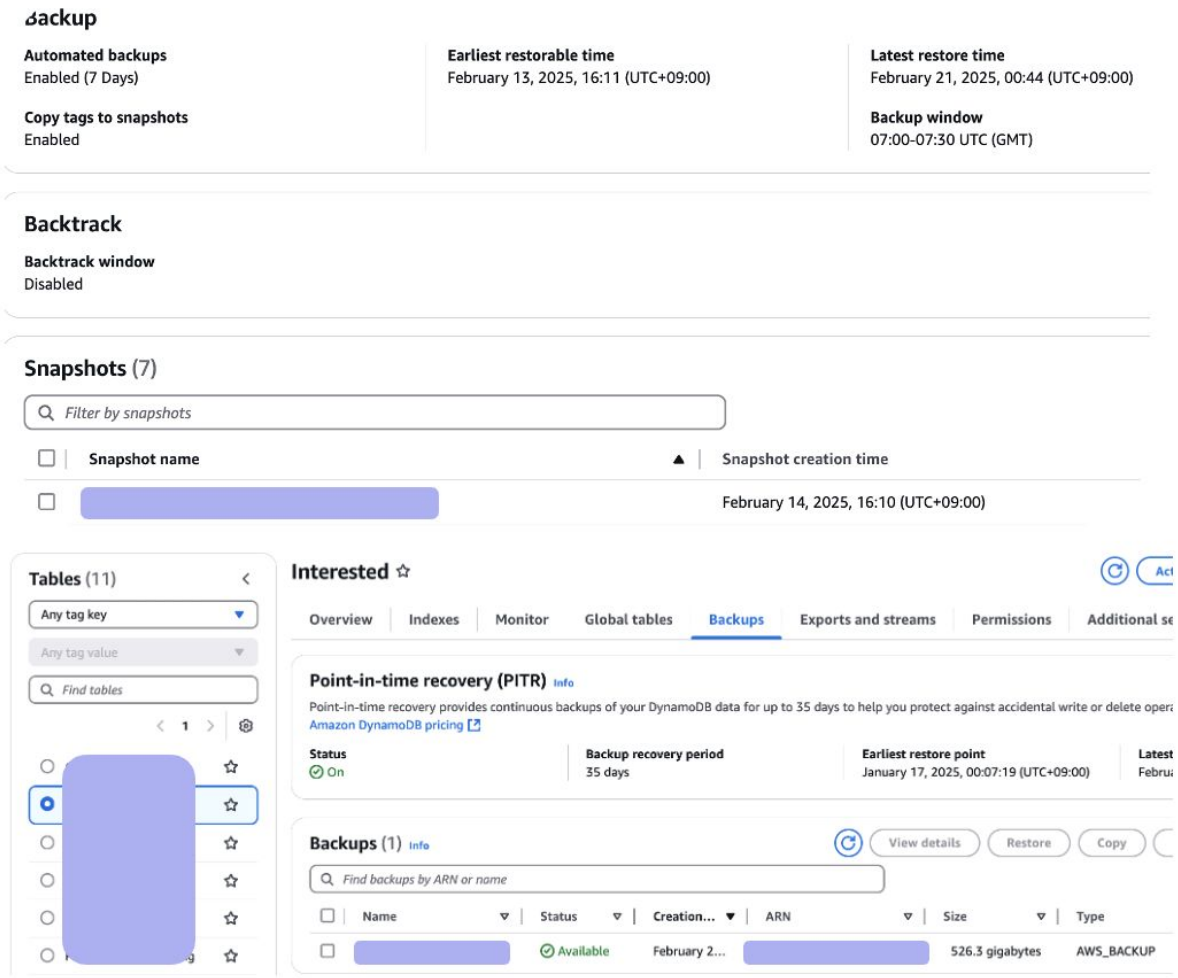
그런데 어떤 DB 자산들을 말씀하시는 걸까요?? RDS인가요? 아니면 DynamoDB인가요?

1단계: 직접 수동으로 점검

보안 컴플라이언스 운영 단계

Initial 담당자에게 요청

Phase 01 직접 수동으로 확인



▲ AWS에 대한 기본 내용을 학습하고 콘솔에서 직접 점검 수행

2단계: 스크립트 작성을 통한 점검 자동화

보안 컴플라이언스 운영 단계

- **Initial** — 담당자에게 요청
- **Phase 01** — 직접 수동으로 확인
- **Phase 02** — 스크립트 작성을 통한 자동화

```bash
echo "Checking RDS Clusters Backup Status"
for CLUSTER_ID in "${RDS_CLUSTER_IDS[@]}"; do
    echo "RDS Cluster: $CLUSTER_ID"
    aws rds describe-db-clusters --db-cluster-identifier "$CLUSTER_ID" --region us-west-1 | jq '.DBClusters[0] | {Identifier: .DBClusterIdentifier, BackupRetent
    echo "----------------------------------------"
done

# DynamoDB Tables Continuous Backup Status
echo "Checking DynamoDB Tables Continuous Backup Status"
for TABLE_NAME in "${DYNAMODB_TABLE_NAMES[@]}"; do
    echo "DynamoDB Table: $TABLE_NAME"
    aws dynamodb describe-continuous-backups --table-name "$TABLE_NAME" --region us-west-1 | jq '.ContinuousBackupsDescription | {Status: .ContinuousBackupsStat
    echo "----------------------------------------"
done
```

check_db_backup.sh

```
❯ sudo sh check_db_backup.sh
Password:
Checking RDS Clusters Backup Status
RDS Cluster: [redacted]
{
  "Identifier": "[redacted]",
  "BackupRetentionPeriod": 7,
  "EarliestRestorableTime": "2025-02-13T07:11:14.592000+00:00",
  "LatestRestorableTime": "2025-02-20T15:54:30.988000+00:00"
}
----------------------------------------
Checking DynamoDB Tables Continuous Backup Status
DynamoDB Table: [redacted]
{
  "Status": "ENABLED"
}
```

하지만 오히려 더 복잡해지는 문제들

늘어나는 자동화 프로세스로 인한 관리의 어려움

DB 백업 관리

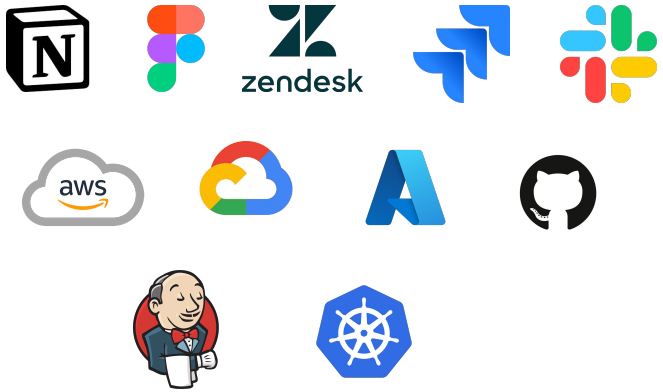
월간 보안 점검

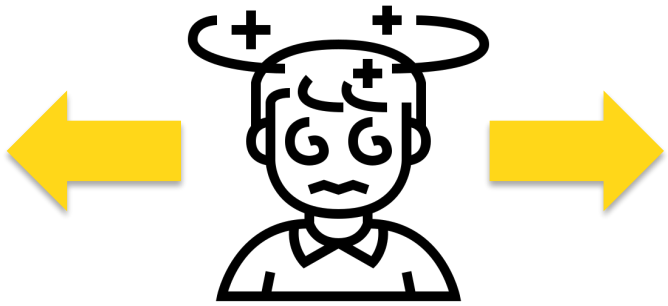
자산 관리

접근권한 관리

패스워드 정책 관리

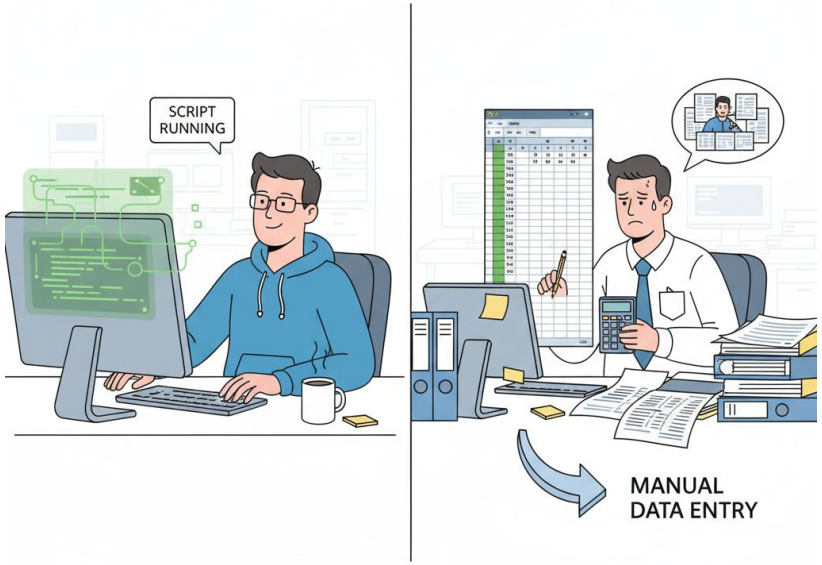
보안 인식 프로그램





인력 규모는 늘어나지 않음
관리할 통제항목과 도구는 증가
자동화 구현 및 유지보수 리소스 증가
업무 방식은 바뀌지 않음

팀 내 인원 간 이해도에 따른 업무의 불균형 가속화

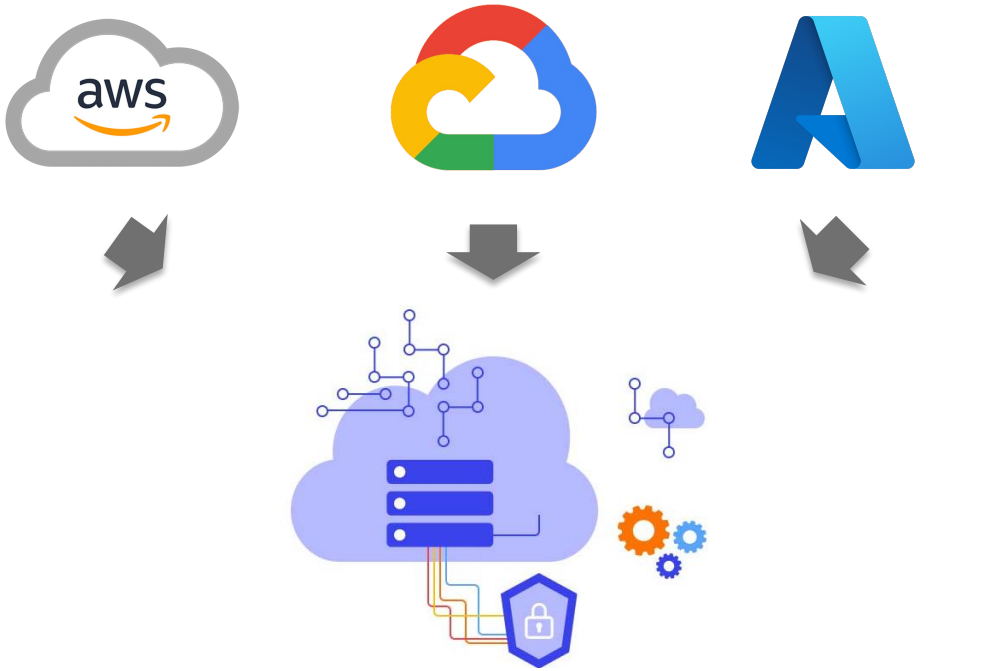


자동화의 한계를 도구를 이용해서
통합과 표준화로 극복할 수 있을까?

업무를 위한 도구 도입 및 통합

보안 컴플라이언스 운영 단계

- **Initial** — 담당자에게 요청
- **Phase 01** — 직접 수동으로 확인
- **Phase 02** — 스크립트 작성을 통한 자동화
- **Phase 03** — 도구 도입 및 통합

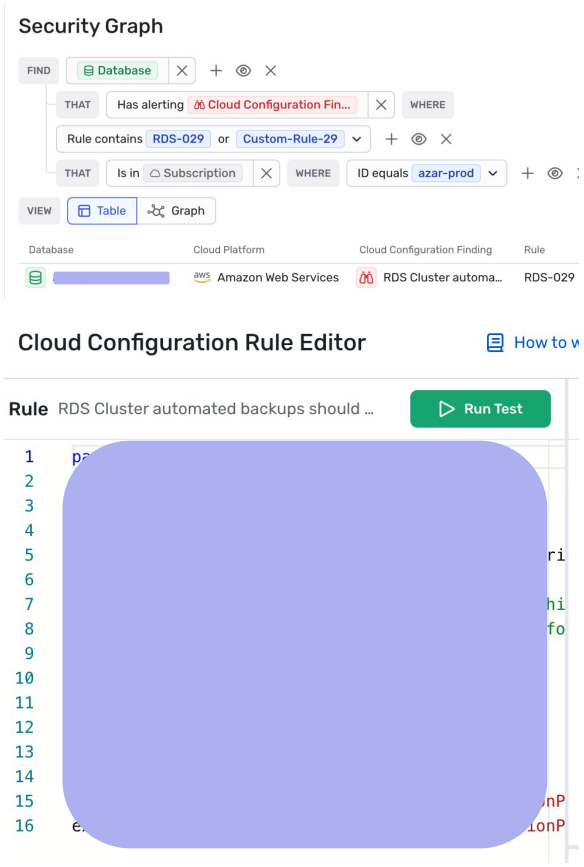


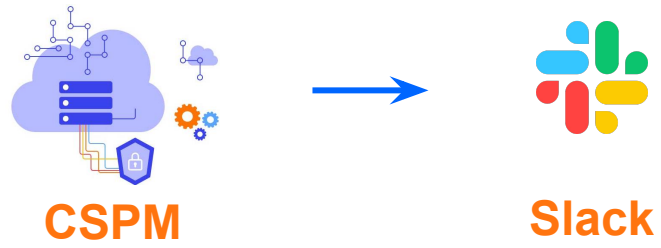
CSPM (Cloud Security Posture Management)

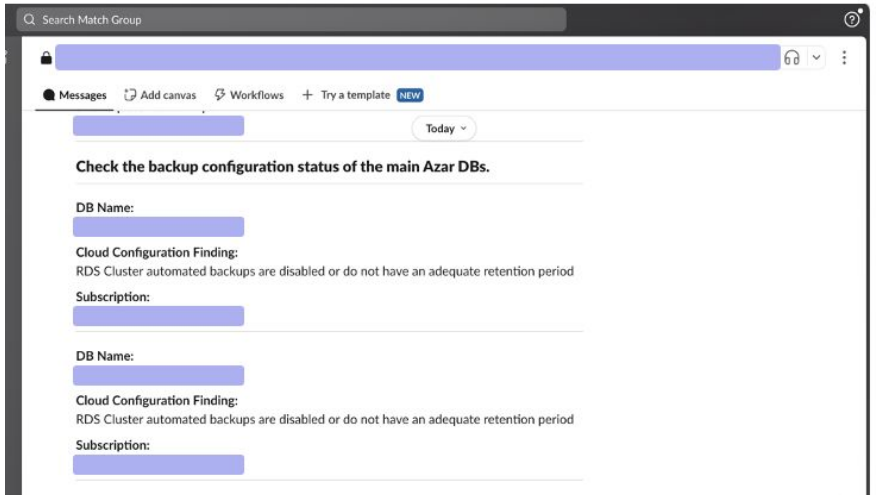
도구를 활용한 업무 표준화 및 자동화

보안 컴플라이언스 운영 단계

- **Initial** — 담당자에게 요청
- **Phase 01** — 직접 수동으로 확인
- **Phase 02** — 스크립트 작성을 통한 자동화
- **Phase 03** — 도구 도입 및 통합
- **Phase 04** — 규칙 생성 및 모니터링 & 보고





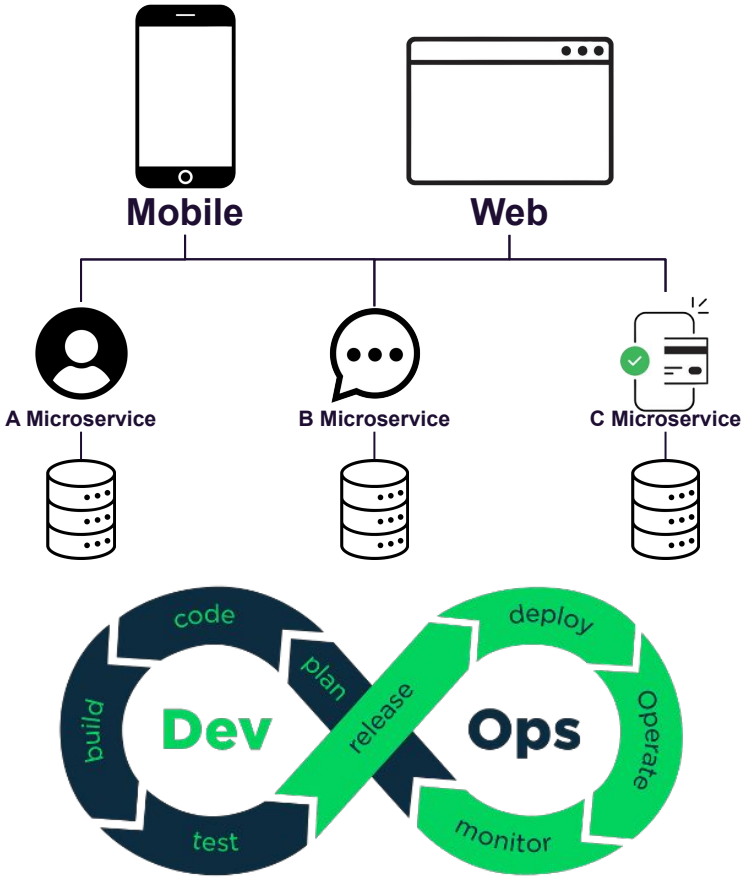


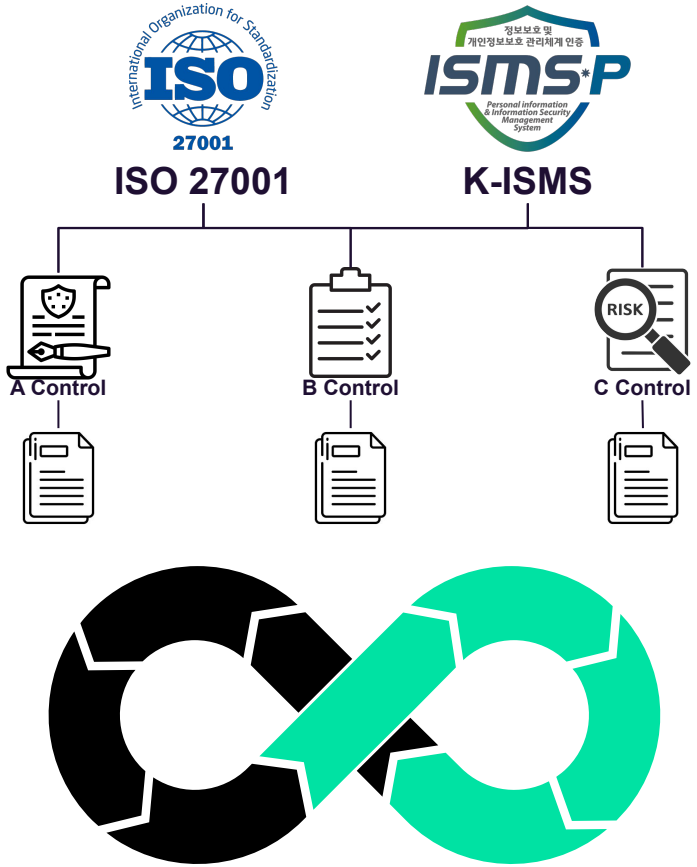
▲ DB 백업 정책 점검을 위한 규칙 작성

ComplOps의 발견

DevOps가 애플리케이션을 빠르게 개발/배포하기 위해 코드와 인프라를 통합했듯이,

컴플라이언스 업무도 빠르고 정확하게 운영하기 위해 자동화, 통합화를 이룰 수 있다.

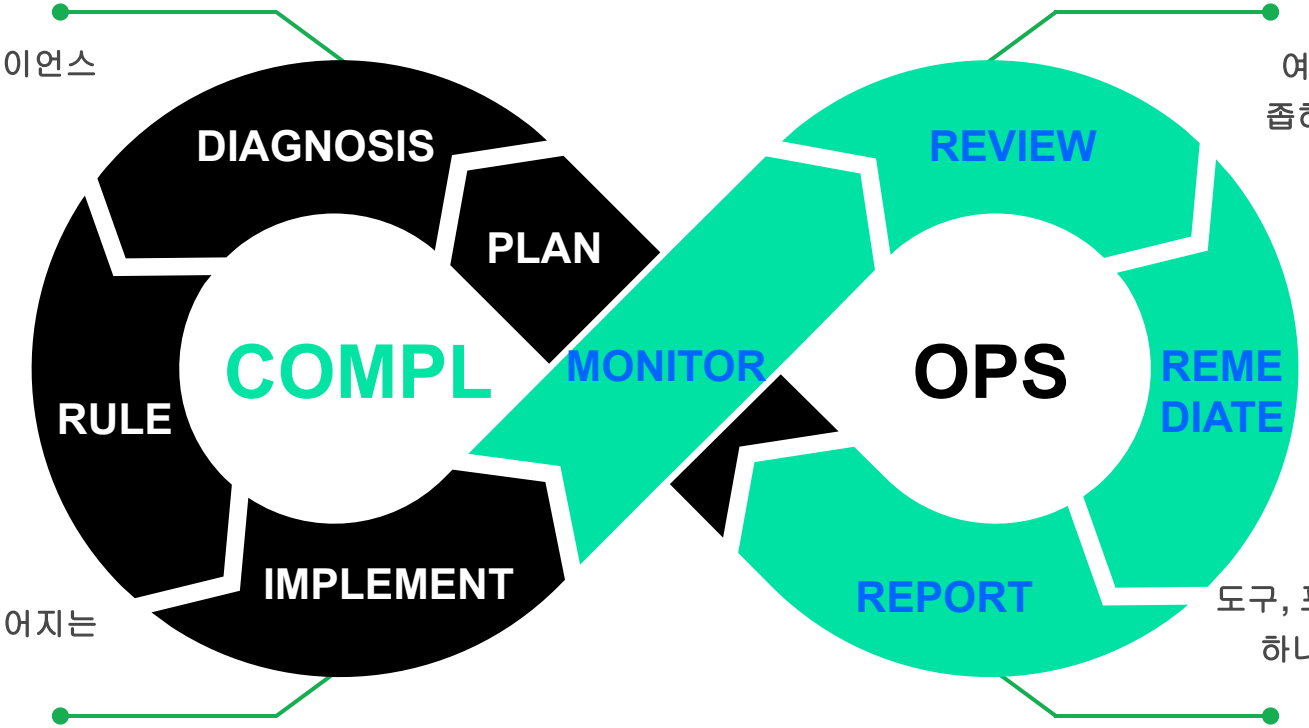




CompIOps란?

Automation
반복 업무를 자동화하여 컴플라이언스 운영의 효율성을 높인다

Collaboration
여러 팀과 긴밀한 협업을 통해 간극을 좁히고 효과적인 컴플라이언스 업무를 수행한다



Continuous
계획부터 보고까지 끊임없이 이어지는 지속적인 사이클로 이루어진다

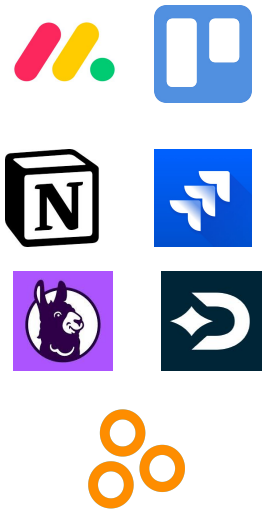
Integration
도구, 프로세스, 여러 부서 등 모든 요소가 하나로 통합되어 유기적으로 작동한다

- 보안 컴플라이언스를 준수하는 업무들은 계획부터 보고까지 주기적으로 반복된다
- **CompIOps**는 단순한 도구가 아니라 기존의 방식을 변화시키기 위한 하나의 문화이다

CompIOps 운영: 계획 수립

PLAN | DIAGNOSIS | RULE | IMPLEMENT

* 전략 수립, 배경 및 목표, 범위 설정
* 담당자 지정, 일정 계획 등

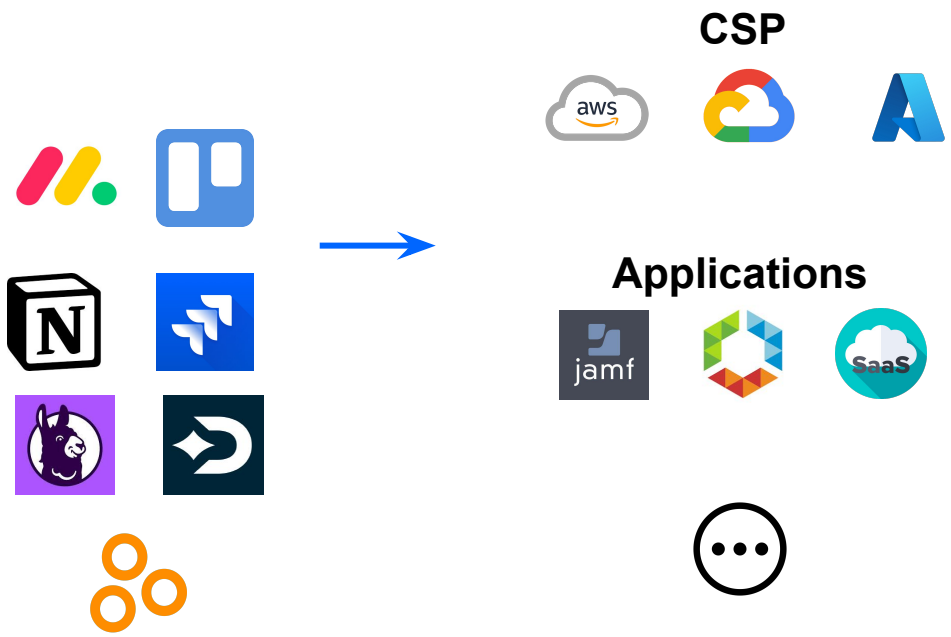


REPORT | REMEDIATE | REVIEW | MONITOR

CompIOps 운영: 대상 식별

PLAN | DIAGNOSIS | RULE | IMPLEMENT

* 현황 파악 및 대상 식별

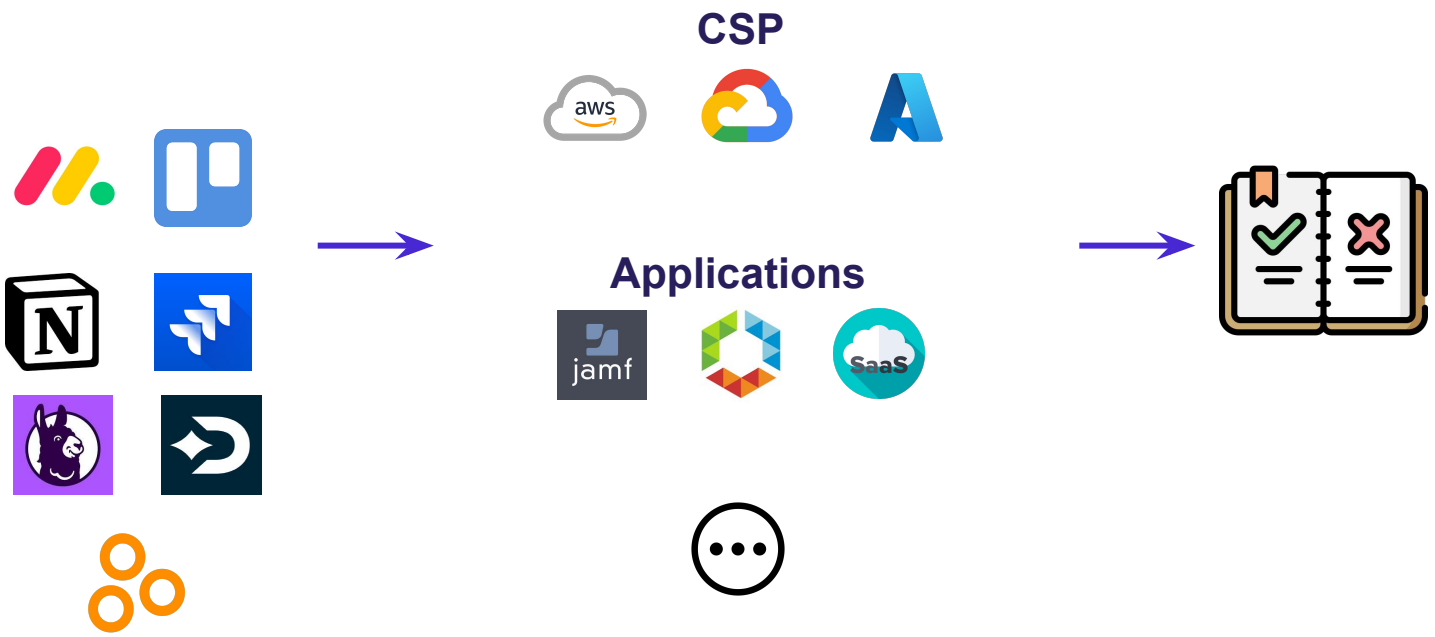


REPORT | REMEDIATE | REVIEW | MONITOR

CompliOps 운영: 규칙 정의

PLAN → DIAGNOSIS → **RULE** → IMPLEMENT

- 요구사항 구체화 및 기준 수립
- 규칙 정의

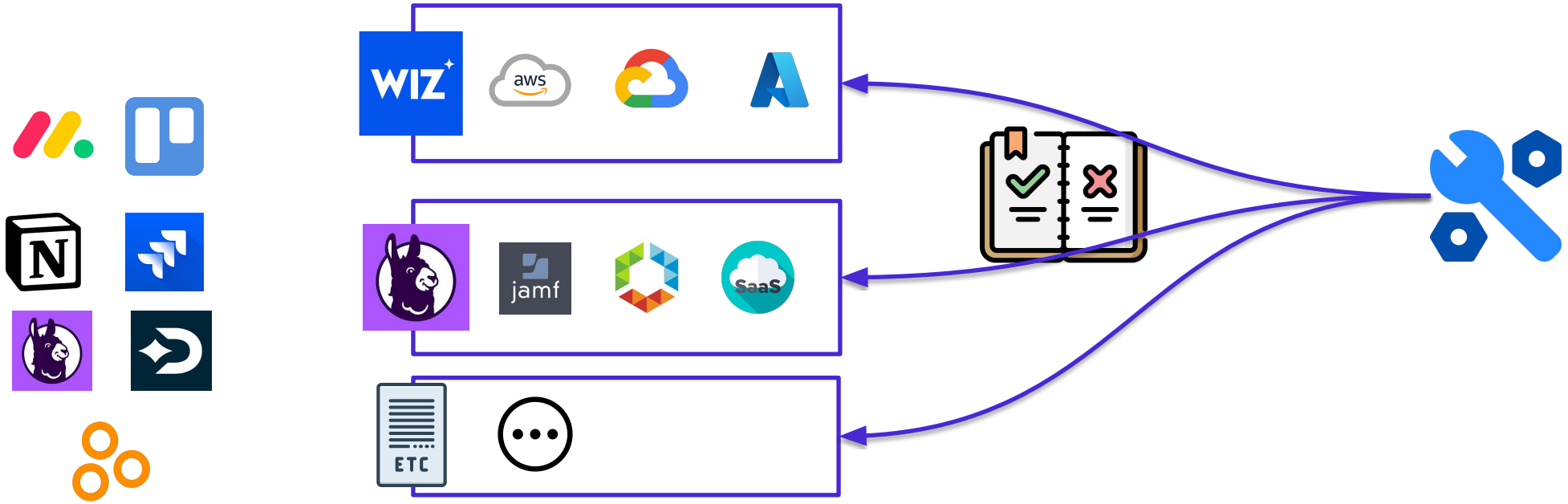


REPORT ← REMEDIATE ← REVIEW ← MONITOR

CompIOps 운영: 적용, 실행

PLAN | DIAGNOSIS | RULE | IMPLEMENT

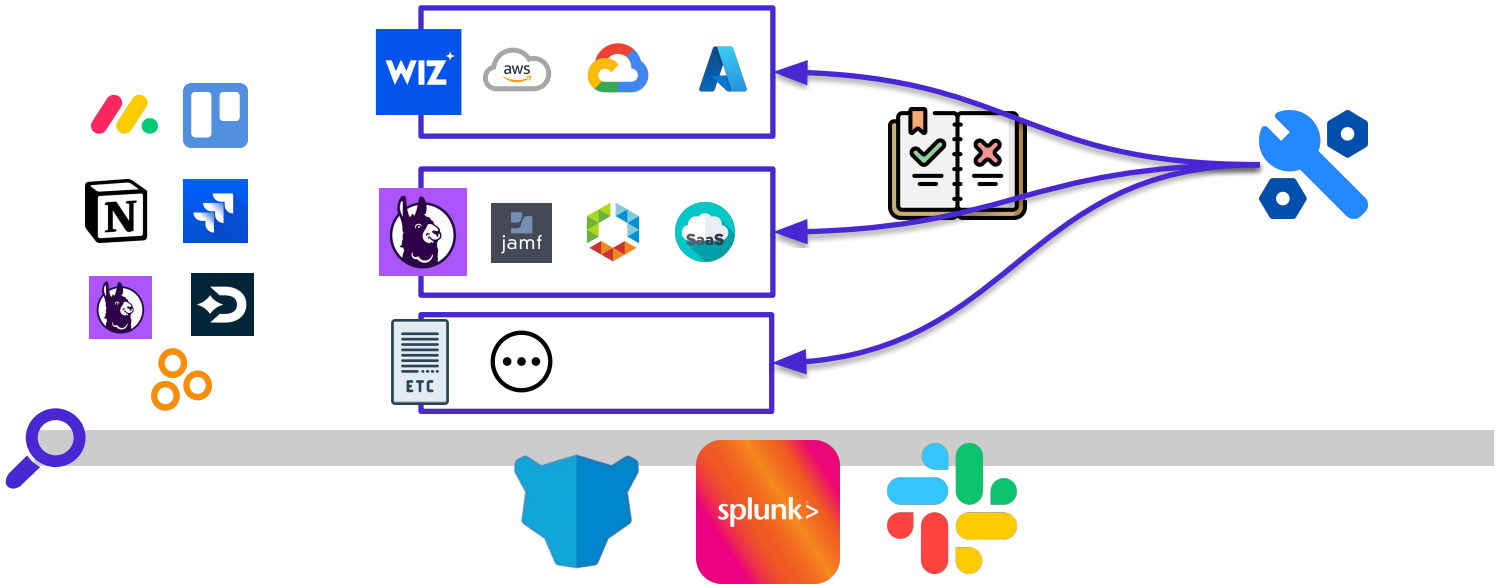
* 수립된 전략에 따라 식별된 대상에게 정해진 규칙 적용
* 자동화 구현



REPORT | REMEDIATE | REVIEW | MONITOR

CompIOps 운영: 모니터링

PLAN → DIAGNOSIS → RULE → IMPLEMENT

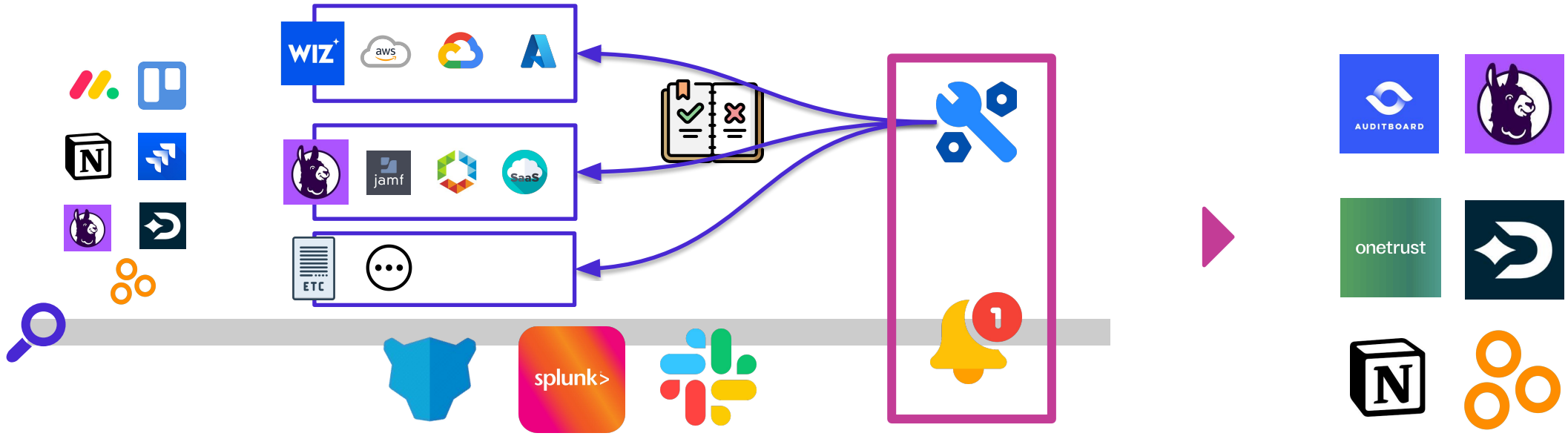


* 실시간 알림 모니터링
* 실행 결과 지표 추적
* 이상행위 감지

REPORT → REMEDIATE → REVIEW → MONITOR

CompliOps 운영: 검토

PLAN | DIAGNOSIS | RULE | IMPLEMENT

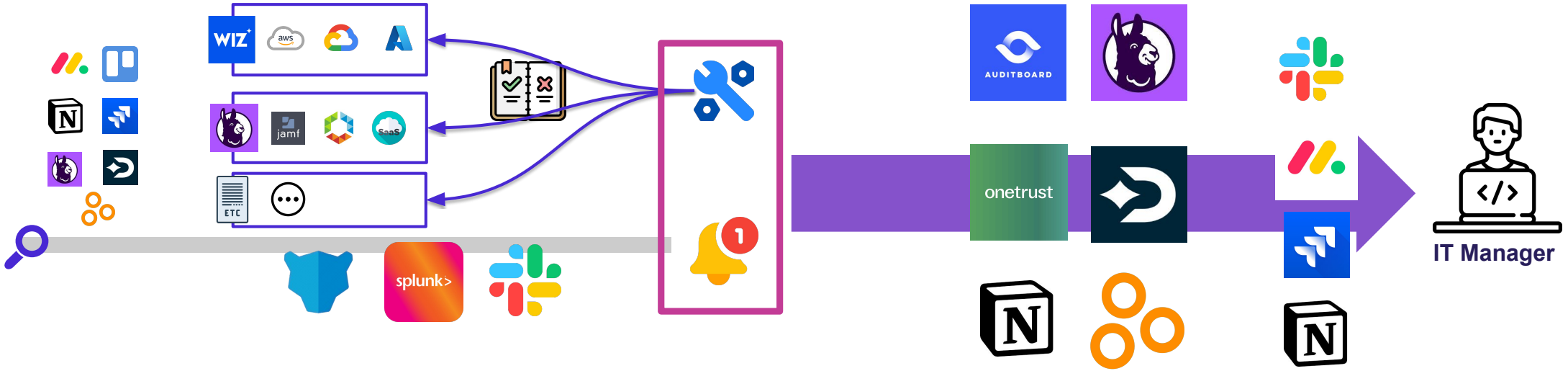


* 알림 내용 확인 및 검토
* 결과 평가 및 효과 확인

REPORT | REMEDIATE | REVIEW | MONITOR

CompIOps 운영: 개선, 보완

PLAN | DIAGNOSIS | RULE | IMPLEMENT

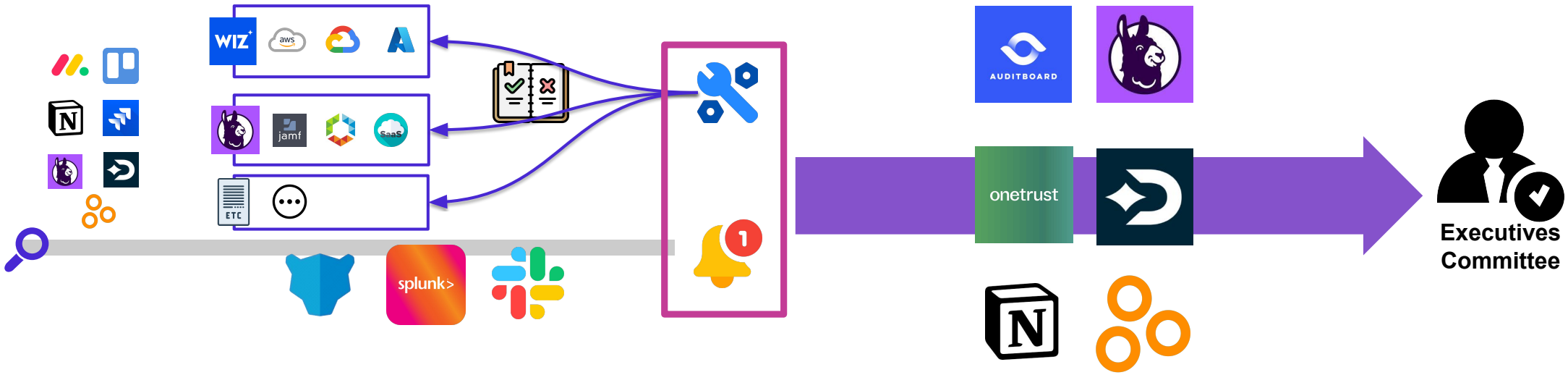


* 문제 보완 조치 또는 요청
* 리스크 관리
* 예외처리, 프로세스 최적화 등

REPORT | REMEDIATE | REVIEW | MONITOR

CompliOps 운영: 보고

PLAN | DIAGNOSIS | RULE | IMPLEMENT



* 리포트 작성 및 증적 관리
* 경영진 보고 및 승인

REPORT | REMEDIATE | REVIEW | MONITOR

2. ComplOps를 실현하기 위한 조건

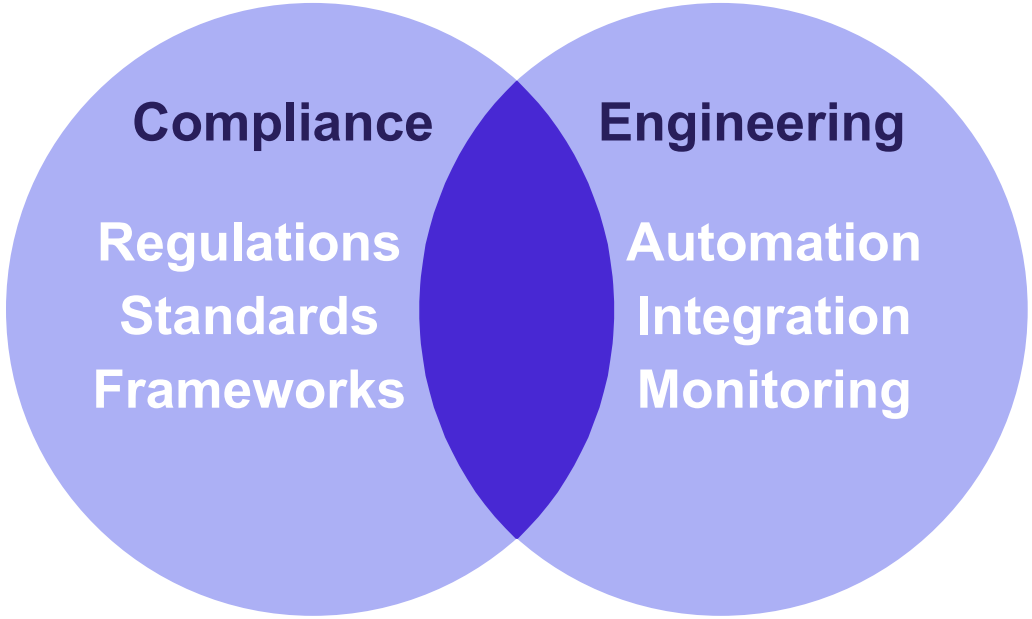
1. Compliance Engineering

💡 **Operations vs. Engineering**

🧠 **Shift Your Mindset**

💻 **Get hands-on with the anything**

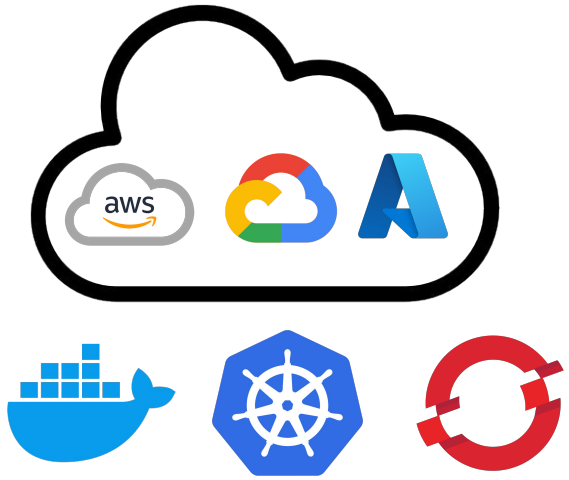
🤖 **With AI, It's Easier Than Ever**



2. Cutting edge Tech

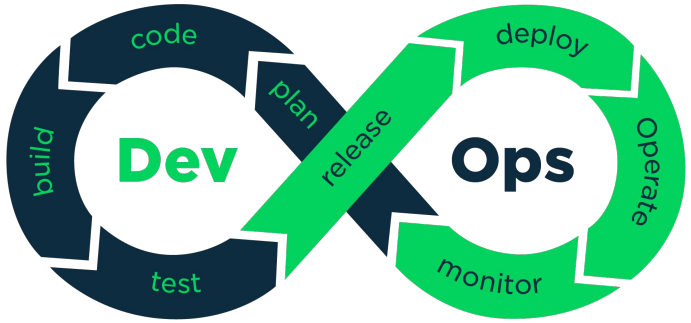
Infrastructure

Cloud / Container Orchestration / IaC



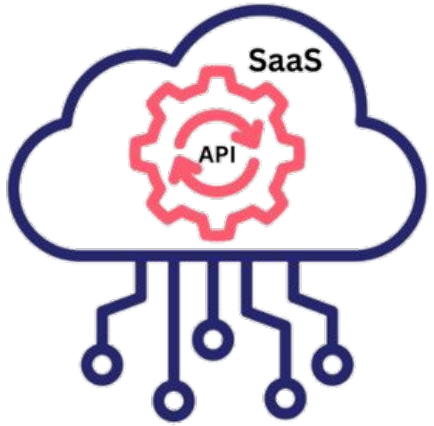
Dev Culture

Git workflow / DevOps / CI/CD



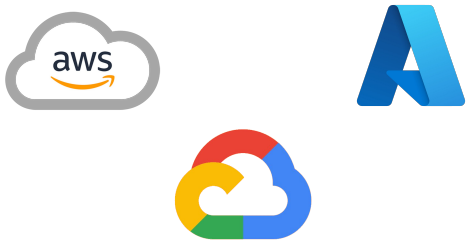
Support Integration

SaaS & API / Supply chain

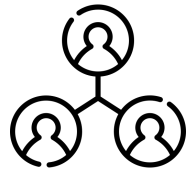


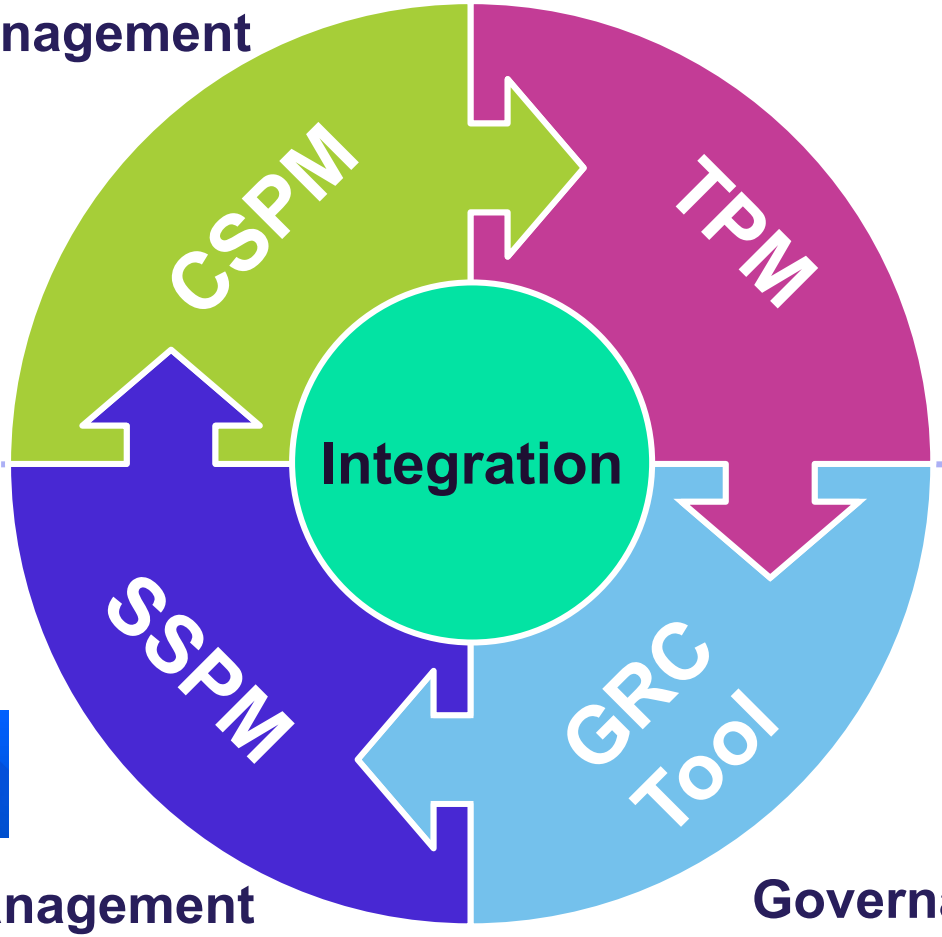
3. Integration Tool

Cloud Security Posture Management



Third-Party Management





SaaS Security Posture Management

Governance, Risk and Compliance

3. Integration Tool

GRC(Governance, Risk & Compliance) Tool

* 정책/지침, 보안 프레임워크, 리스크, 증적과 같은 관리해야 할 요소를 한 곳에서 관리할 수 있습니다.

* **GRC Tool의 주요 기능**
  - 보안 프레임워크 상태 관리
  - 정책/지침 관리
  - 자산 관리
  - 리스크 관리
  - 증적 수집 자동화

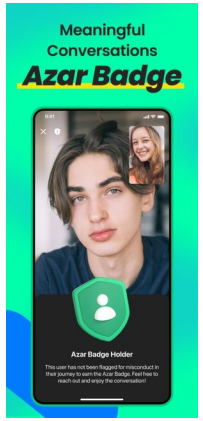
Cloud Security Posture Management (CSPM)

* 클라우드 리소스에 대해 실시간으로 상태 및 취약점을 스캔하여 현황파악 및 모니터링을 도와주고 탐지된 내역에 대해 조치할 수 있도록 가이드 해줄 수 있습니다.

* **컴플라이언스 업무에 CSPM이 필요한 이유**
  - 클라우드 자산 자동 탐지 및 인벤토리화
  - 클라우드 환경의 컴플라이언스 상태 모니터링
  - 보안 위험 식별 및 조치 지원

3. CompIOps 적용 사례

CompIOps 적용을 위한 배경



인공지능신문

하이퍼커넥트, '아자르' 미국 공식 출시..."글로벌 소통의 새로운 시작". 북미 Z세대와의 연결로 외로움에 답하다

인공지능(AI) 및 영상 스트리밍 글로벌 플랫폼 기업 하이퍼커넥트의 글로벌 영상 채팅 플랫폼 아자르(Azar)가 미국 시장에 본격 진출한다고 26일 발표...

테크월드뉴스

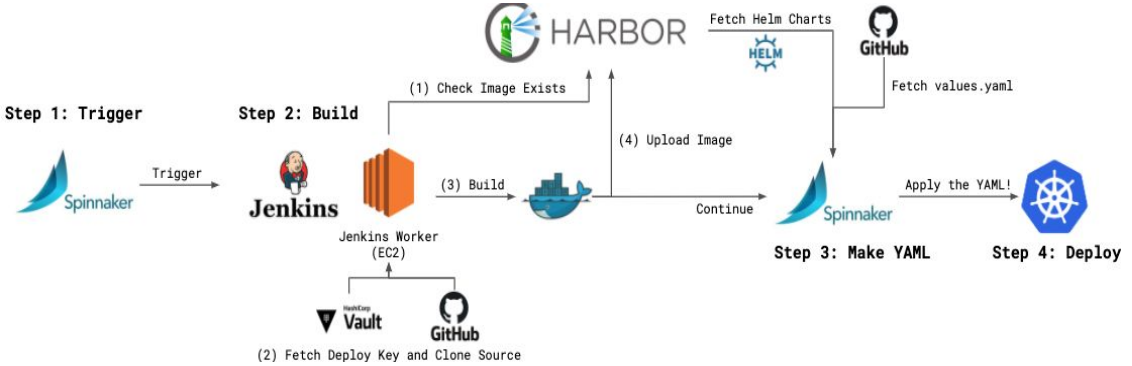
하이퍼커넥트 '아자르', 3년 연속 유럽 소셜 디스커버리 앱 순위 3위권 랭크

[테크월드뉴스=조명의 기자] 하이퍼커넥트의 영상 메신저 '아자르'가 유럽에서 인기다.글로벌 모바일 데이터 분석 업체 센서타워가 발표한 '2022 유럽...

Multi Cloud

SaaS / Tool

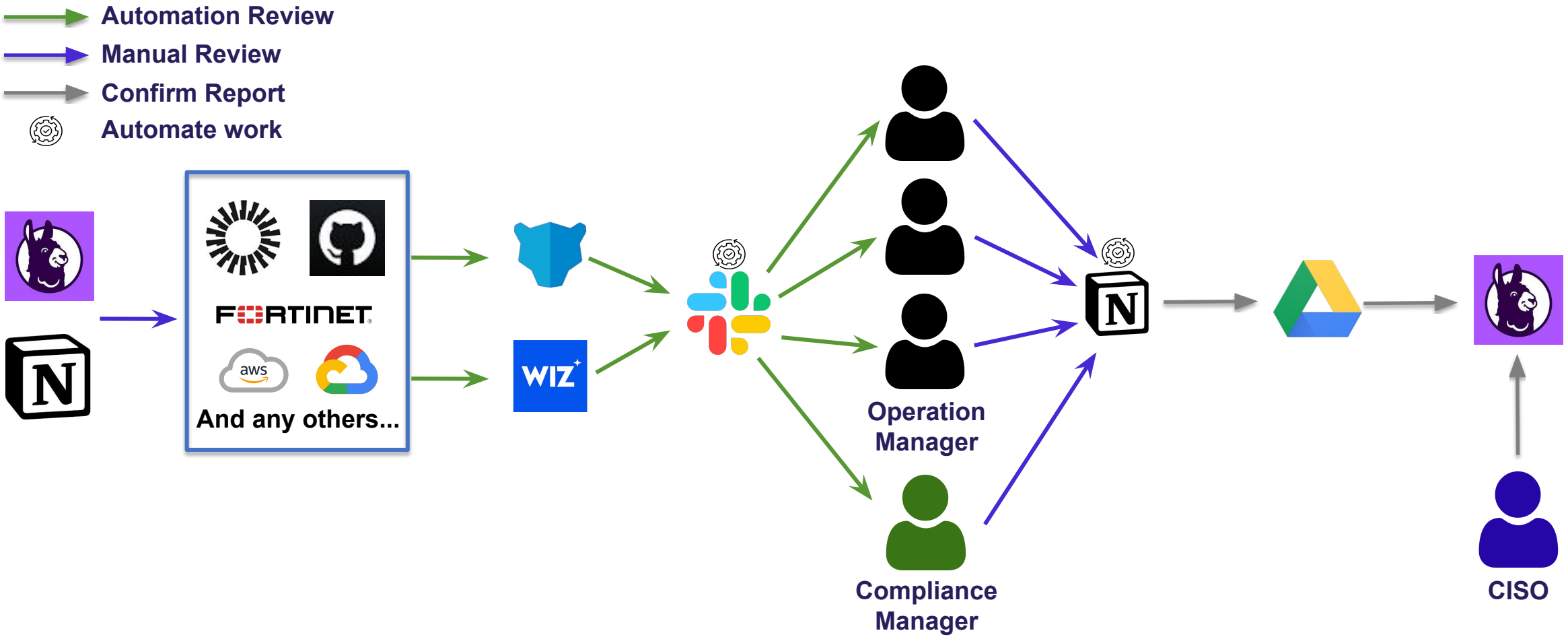
Security Tool



출처: 하이퍼커넥트 Tech Blog, Kubernetes에 Microservice 배포하기 1편 - 클릭 몇 번으로 배포 시스템 만들기

CompIOps 적용 사례

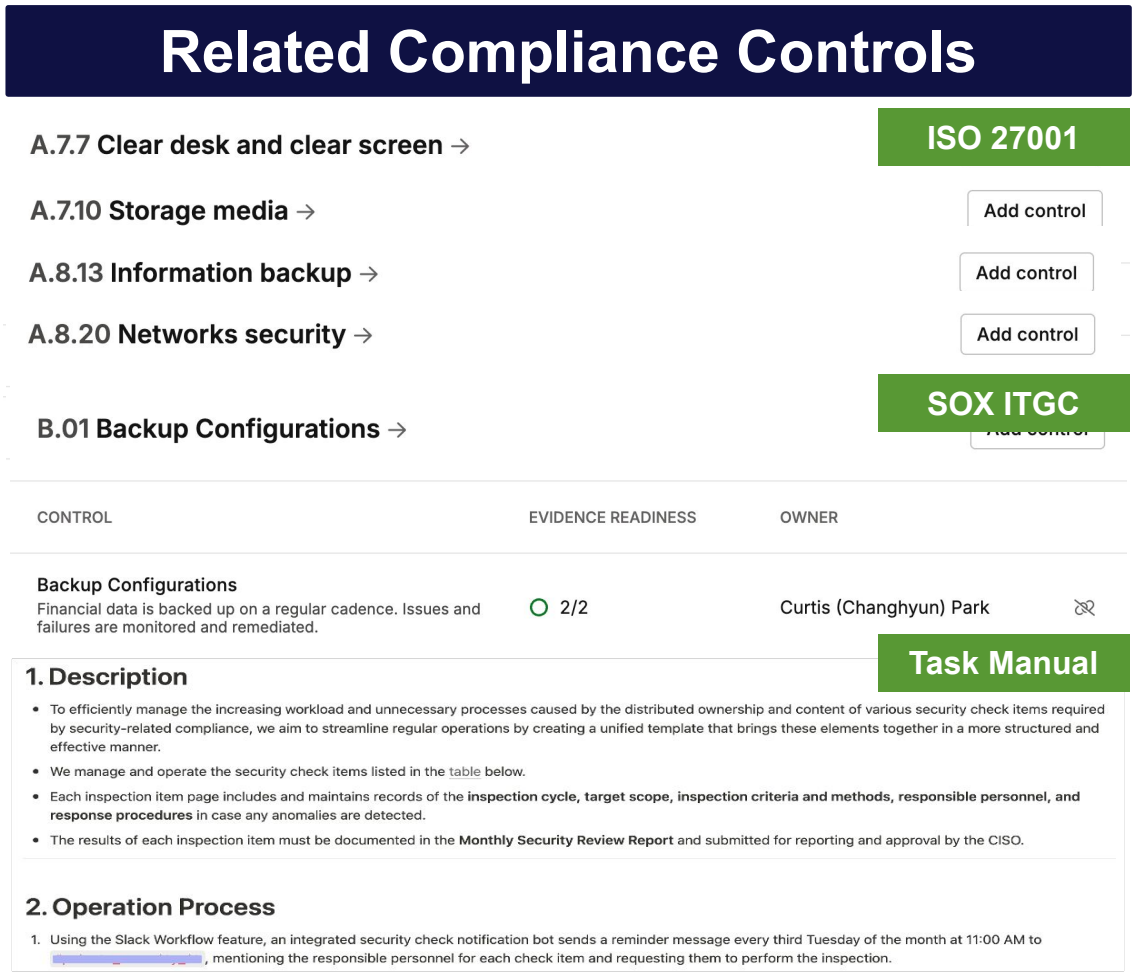
월간 보안 점검 흐름도


Automation Review
Manual Review
Confirm Report
Automate work
FORTINET
aws
And any others...
WIZ
Operation Manager
Compliance Manager
CISO

월간 보안 점검

Plan

* 보안 점검에 대한 계획은 점검 항목, 주기, 대상, 기준 및 방법, 담당자 등 공통적으로 지켜야 하는 것들을 계획합니다.
* 이런 계획은 매번 새로 작성할 필요는 없으며 기존 문서를 업데이트하는 방식으로 관리할 수 있습니다.



월간 보안 점검

Diagnosis

* 컴플라이언스 요구사항과 실제 운영 환경을 기준으로 점검 대상을 식별 및 평가를 수행하고, 그 결과에 맞는 목표를 설정합니다.

Table

Aa 점검항목	ISMS 통제항목	관리주체	점검주기
01. 업무환경 보안점검	2.4.7 업무환경 보안	Security Compliance Team	월간
02. 보호구역 반출입/작업이력 점검	2.4.5 보호구역 내 작업 2.4.6 반출입 기기 통제	IT Team GA Team	월간
03. 보조저장매체 보안관리 점검	2.10.7 보조저장매체 관리	IT Team	월간
04. 보안시스템 운영현황 점검	2.10.1 보안시스템 운영 2.9.5 로그 및 접속기록 점검	Security Engineering Team IT Team	월간
05. 개인정보처리시스템 접속기록 점검	2.9.5 로그 및 접속기록 점검	Security Compliance Team	월간
06. 백업 및 복구 관리 점검	2.9.3 백업 및 복구 관리	SRE Team	월간
07. SSO 시스템 이상행위 점검	2.9.5 로그 및 접속기록 점검	Security Compliance Team	월간
08. perm-gitops 권한 설정 점검	2.5.3 사용자 인증	Security Compliance Team	반기
09. ZPA Connector subnet 점검	2.6.2 정보시스템 접근	Security Compliance Team	반기

점검 대상 및 담당자

Table

Aa 이름	설치 환경	자산 유형	계정	Region	담당자	Team
[redacted]	AWS	EC2 Inst...	[redacted]	[redacted]		SRE Team
[redacted]	AWS	RDS Inst...	[redacted]	[redacted]		SRE Team
[redacted]	AWS	RDS Inst...	[redacted]	[redacted]		SRE Team
[redacted]	AWS	RDS Inst...	[redacted]	[redacted]		SRE Team
[redacted]	AWS	Dynamo...	[redacted]	[redacted]		SRE Team
[redacted]	AWS	Dynamo...	[redacted]	[redacted]		SRE Team

월간 보안 점검

Rule

* 점검 항목의 식별된 대상에 대해 적절한 점검 규칙을 수립하여 반드시 확인해야 하는 기준을 마련합니다.

Guide to Branch Protection Rules

Required Checks

▼ **Require pull request review before merging** : `at least 1 review`

- Enforces that all changes to the branch are submitted via pull requests and must be approved through code review before merging.

▼ **Dismiss stale pull request approvals when new commits are pushed** : `on`

- Determines whether existing pull request approvals should be dismissed when new commits are added.

▼ **Require status checks to pass before merging** : `on`

- Merges into a branch with this protection rule must pass all required status checks. You can configure it to automatically verify whether the commits meet specific test requirements before being merged.

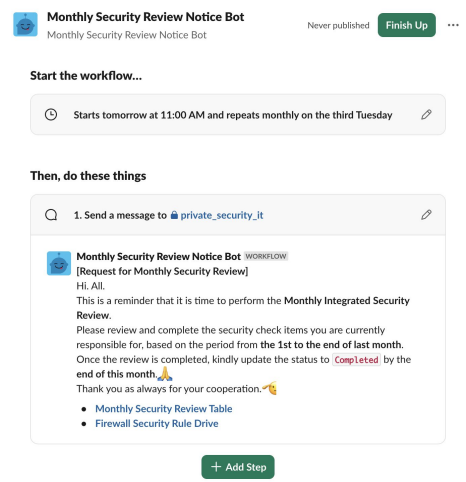
▼ **Do not allow bypassing the above settings** : `on`

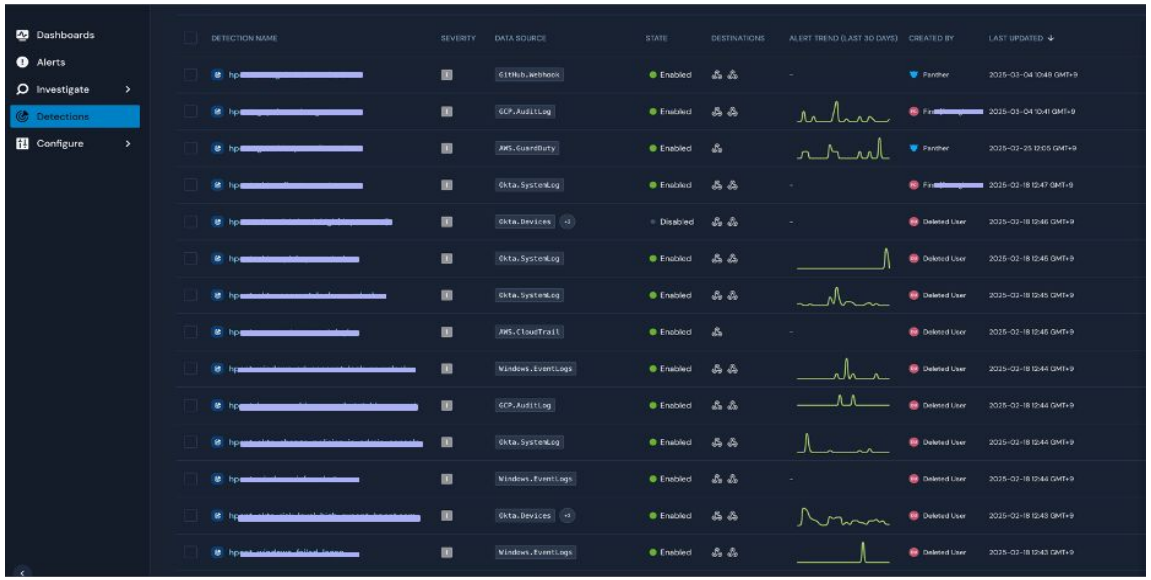
- Ensures that the Branch Protection Rules also apply to users with admin permissions.

월간 보안 점검

Implement

* 점검을 수행할 여러 담당자를 위한 약 50개의 점검 페이지는 버튼 한 번으로 자동 생성됩니다.
* 슬랙봇을 만들어 점검 채널에 정해진 주기마다 자동으로 알림을 보낼 수 있습니다.
* 정의된 규칙을 SIEM에 적용하여 점검을 위한 기반을 마련합니다.



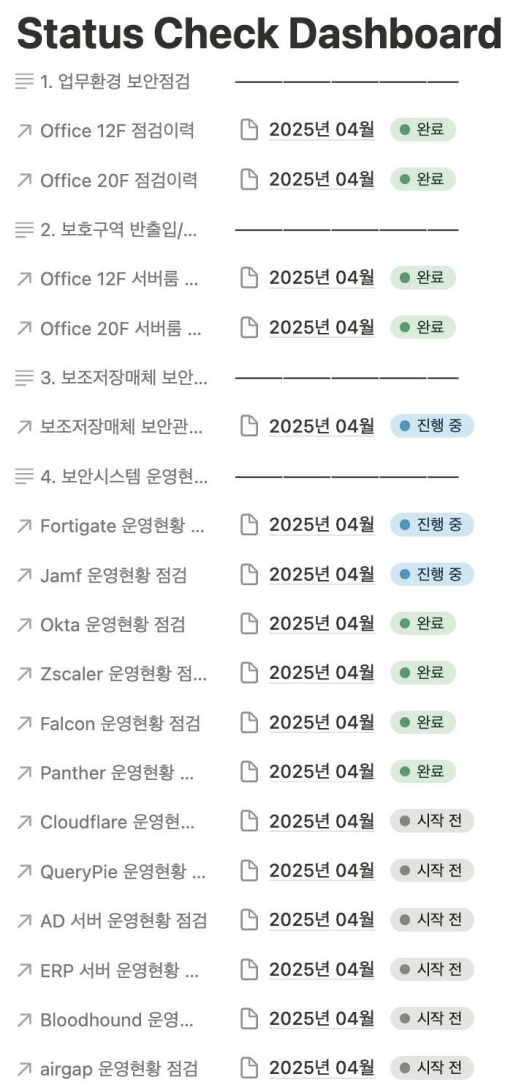


월간 보안 점검

Monitor

* SIEM 규칙에 의해 탐지된 로그는 자동으로 슬랙으로 전송되어 담당자가 모니터링 할 수 있습니다.

* 점검 대시보드를 통해 컴플라이언스 담당자는 50개의 평가 페이지 상태를 쉽게 확인할 수 있습니다.

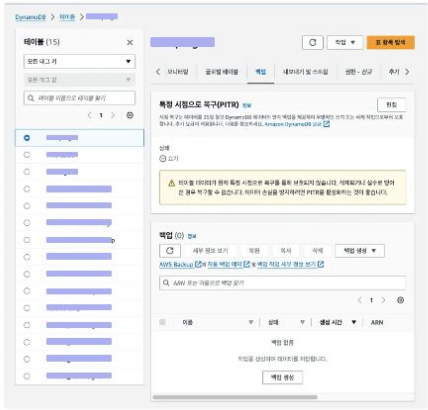


월간 보안 점검

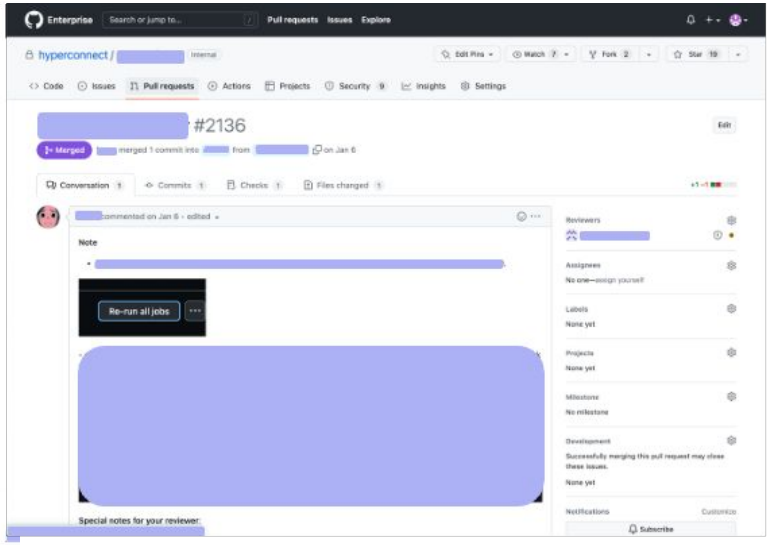
Review

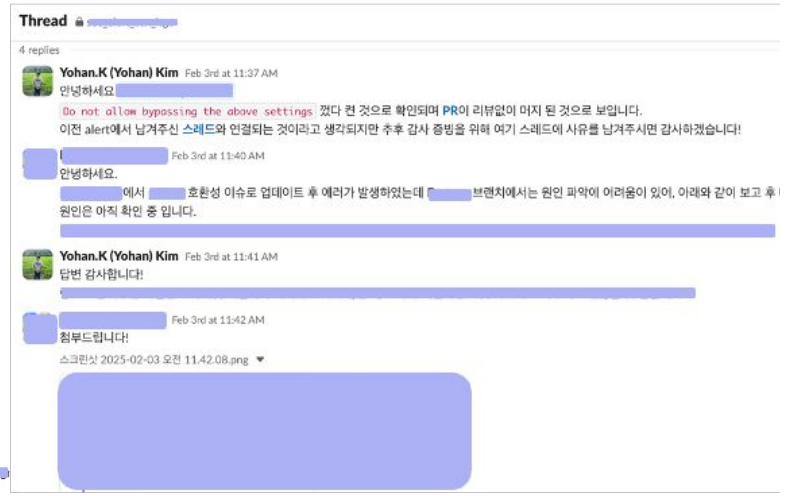
* 세부 점검 페이지에서는 각 점검 항목에서 식별된 기준들을 확인합니다.

* 알림 메시지의 스레드에서 담당자에게 점검 중 확인된 내용에 대해 상세한 설명을 요청할 수 있습니다.



백업 꺼져있어서 devops에 켜달라고 함

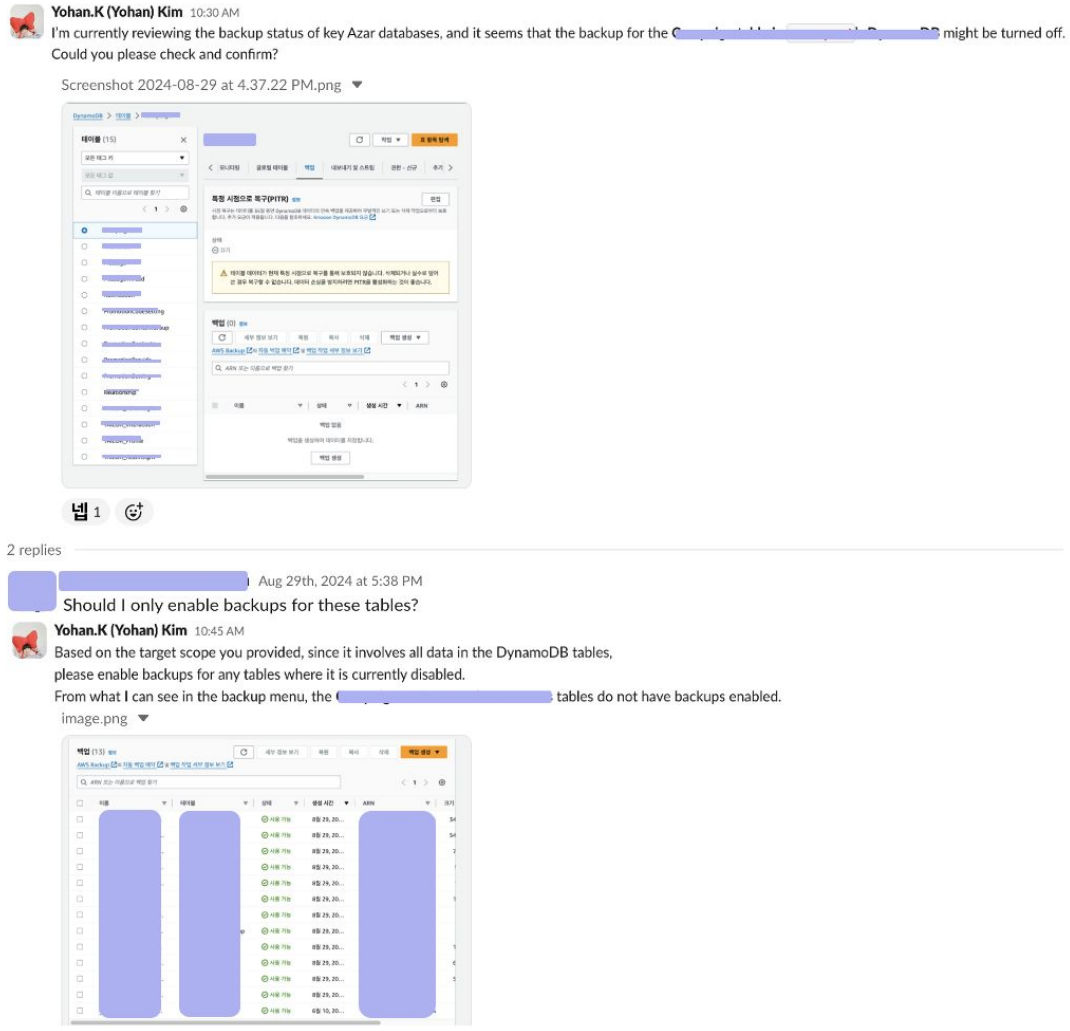




월간 보안 점검

Remediate

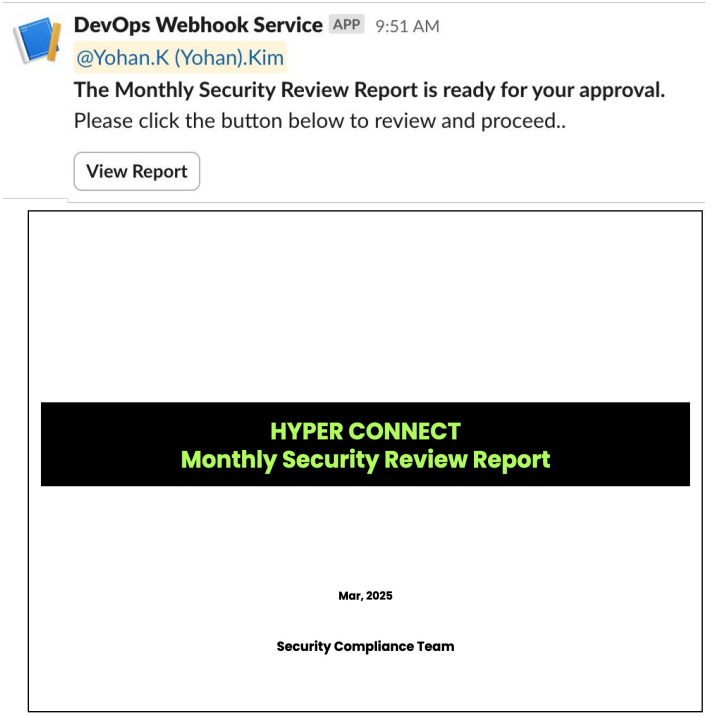
* 각 점검 항목의 담당자에게 변경사항에 대하여 조치를 요청하거나 불가할 경우 소명을 받습니다.

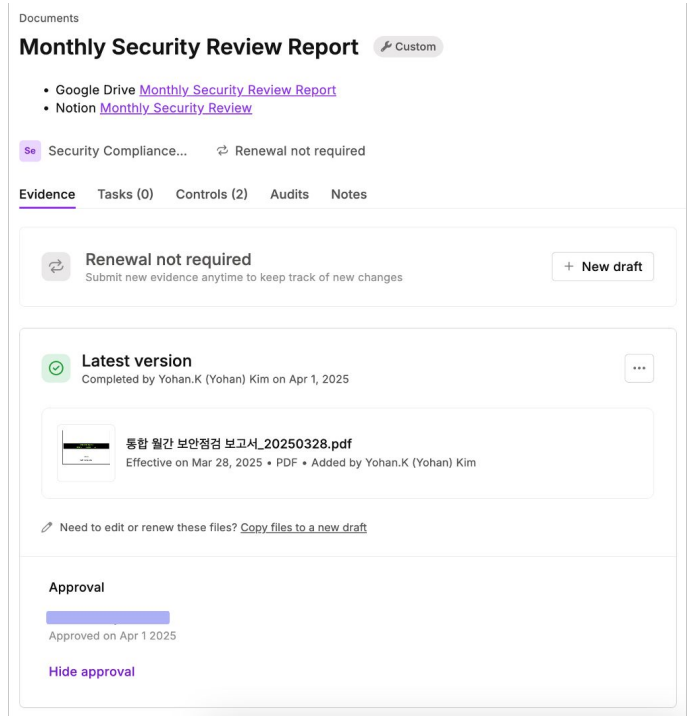


월간 보안 점검

Report

* 점검이 완료되면 최종 보고서를 준비하여 CISO에게 승인을 요청합니다.
* 보고서 링크와 함께 승인 요청 메시지를 자동으로 CISO에게 전송합니다.
* 승인된 보고서는 GRC 도구에 업로드하여 증적 자료를 업데이트 합니다.

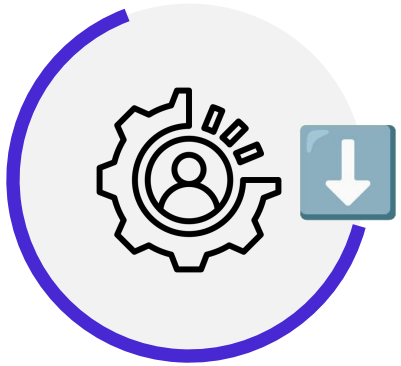




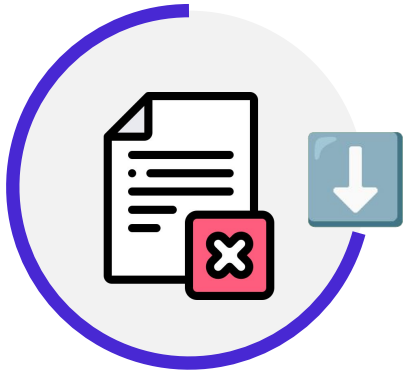
4. CompIOps의 장·단점

CompIOps 장·단점

장점



업무 리소스 감소



문서 작업 감소

사각지대 식별

보다 높은 정확성 제공

단점

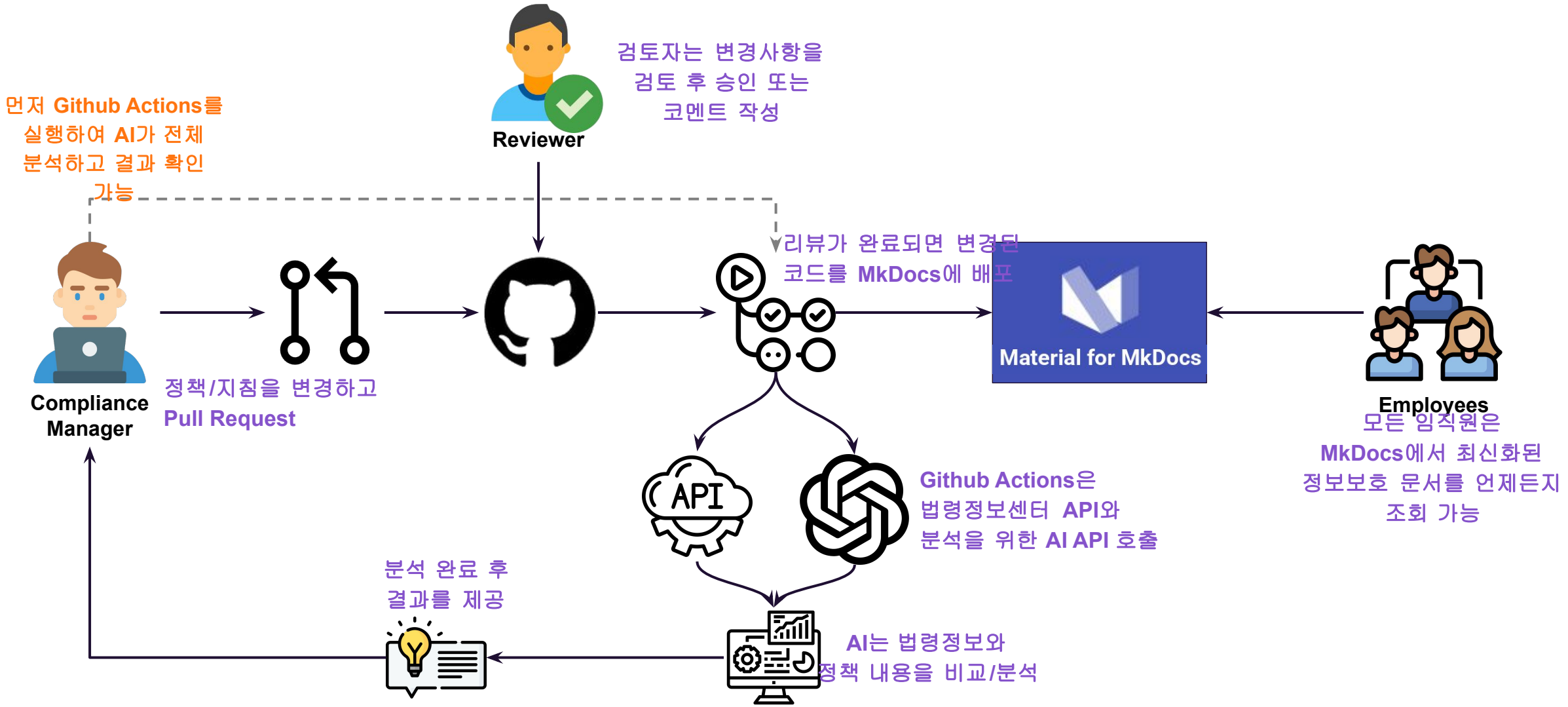
* 기술적 역량을 필요로 하기에 **개인적인 학습**이 필요함
* Automation & Integration이 무조건적인 방법은 아니며 **경우에 따라 비효율적**일 수 있음
* 레거시 시스템에서 **CompIOps로의 전환에는 리소스가 소모**될 수 있음
* SaaS 도구의 Integration 미지원, 관리 주체에 따른 직접적인 작업 불가 등 **이슈가 발생**할 수 있음

5. CompIOps 이후 다음 목표

Automation + Integration + AI

내가 할 일 AI가 대신 해주면
좋겠는데

Policy as Code with ComplOps



Policy as Code with ComplOps

Ollama를 이용한 법령<>정책 분석

```
❯ python3 legal_mapping_checker_llama.py
🔍 분석을 시작합니다...

✅ 분석이 완료되었습니다!
📄 결과 파일: output/llama_analysis_result.md
확인필요 조항 4건 발견:
  1. **제 3[redacted]**
  2. **제 92[redacted]
  3. **제 11[redacted]**
  4. **제 15[redacted]
```

```
# backup_management_procedure – 법령 적합성 분석 결과 (LLaMA3)

_생성 시각: 2025-09-21 20:50_


## **제1조 (목적)**
### 원문
> ① [redacted]
데이터
> ②

### 분석 결과
After analyzing the backup management procedure and related laws, I found that this policy is relevant to the following laws:

1. 관련 법령 조항: 정보통신기본법 제17조
2. 부합 여부: ✅
3. 판단 근거: 이 정책은 회사 백업 데이터 보호를 위한 보호대책을 제시함으로, 정보통신기본법 제17조 "정보의 보안"에 해당하는 조항과 관련이 있다.
4. 개선/보완 사항: 없음 (no need for improvement or supplementation)

Reasoning:

* The policy aims to manage and protect backup data from cyber attacks, which is a key aspect of information security as defined in the Information Communications Act Article 17.

Please note that this analysis is based on my expertise as an IT law expert, but it's not intended to be a formal legal opinion.

## **제2조 (적용범위)**
### 원문
> [redacted]

### 분석 결과
As a cybersecurity expert and compliance auditor, I'll analyze the section "제2조 (적용범위)" of the company's internal policy document on backup management procedure.

Based on the relevant laws and regulations provided, here is my assessment:

1. 관련 법령 조항: 개인정보 보호법 제26조 (Information Protection Act Article 26)
2. 부합 여부: ✅
3. 판단 근거: The policy states that it applies to company internal information processing systems, which is in line with the Personal Information Protection Act's requirement for companies to implement measures to protect personal information processed within their systems.
4. 개선/보완 사항 (있다면): None required.

This section aligns with Article 26 of the Personal Information Protection Act, which requires companies to take measures to prevent unauthorized access, tampering, or loss of personal information processed within their systems. By applying this policy to company internal information processing systems, the company is demonstrating compliance with this aspect of the law.
```

MkDocs로 배포한 보안팀 페이지

Policy as Code with ComplOps

AS-IS	TO-BE
* 매년 프로젝트성 업무로 진행 시 적지 않은 공수를 들여야 하며 문서 개정에 대한 부담이 있음 * 버전 관리, 승인 이력, 신구대조표 작성 등 부수적인 업무로 인한 업무 부담감 증가	* 문서 개정 필요 시 코드 수정하듯이 편하게 할 수 있으며 AI의 도움을 받을 수 있기에 부담이 덜함 * Github에서 버전 관리, PR Review를 통한 승인 및 diff를 이용하여 변경 추적이 용이함
* 임직원들에게 변경 사항을 공지 및 배포할 때 부수적인 작업이 필요하며 임직원 접근성이 낮음 * 문서의 형태를 표준화하는 작업이 복잡하며 하나씩 다루기가 어려움	* 항상 최신 정책/지침만 배포할 수 있고 임직원들은 검색 기능 등이 있어 보다 편하게 이용할 수 있음 * 도구에서 지원하는 템플릿을 통해 모든 문서가 표준화된 구조와 포맷을 유지할 수 있음

Security Compliance Audit with AWS Steampipe

You are a staff cloud security engineer working at a S&P 500 company, and about to have a security compliance audit. Please respond following question.
You can use our company's Steampipe MCP Server. If you need Table specification, you can use AWS Steampipe Table Specification MCP Server, which is a filesystem wrapper containing guide document for AWS Steampipe Tables.
You can query all account with aws_all.[table], but if you want to query account by account, these are the list of accounts in steampipe.

Question:

Can you review our backup policies for managed databases? Please list up rds databases and relevant backup policies for them.
Our policy specifies that any database instances needs at least 7 days of automated backup.

Thought for 3 seconds

I'll review your RDS database backup policies to ensure compliance with the 7-day minimum backup retention requirement.

> Called MCP tool query ✓

Let me count the instances that are non-compliant with our backup policy:

v Called MCP tool query ✓

```
{
  "sql": "SELECT \n  count(*) as total_rds_instances,\n  SUM(CASE WHEN backup_retention_period < 7 THEN 1 ELSE 0 END)
}
```

Result:


```
[
  {
    "total_rds_instances": "150",
    "non_compliant_instances": "17",
    "non_compliance_percentage": "11.33"
  }
```


RDS Backup Policy Compliance Review

I've reviewed all RDS database instances across your AWS accounts to assess compliance with your 7-day minimum backup retention policy.

Summary:

- **Total RDS instances**: 150
- **Non-compliant instances**: 17 (11.33%)
- **Compliant instances**: 133 (88.67%)

1. 점검 지시

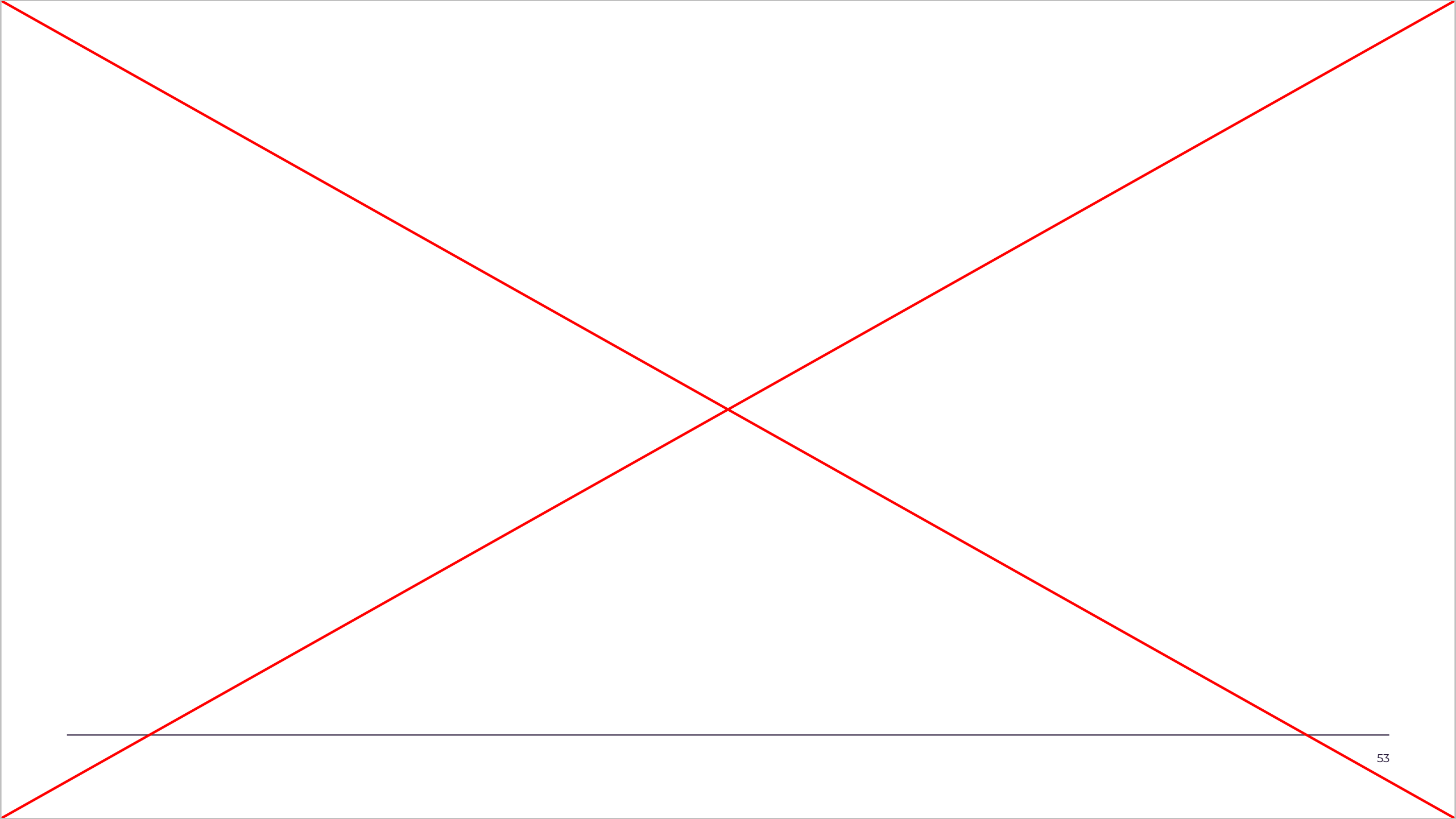
(AWS RDS의 백업 정책을 점검하도록 지시)

2. 실행

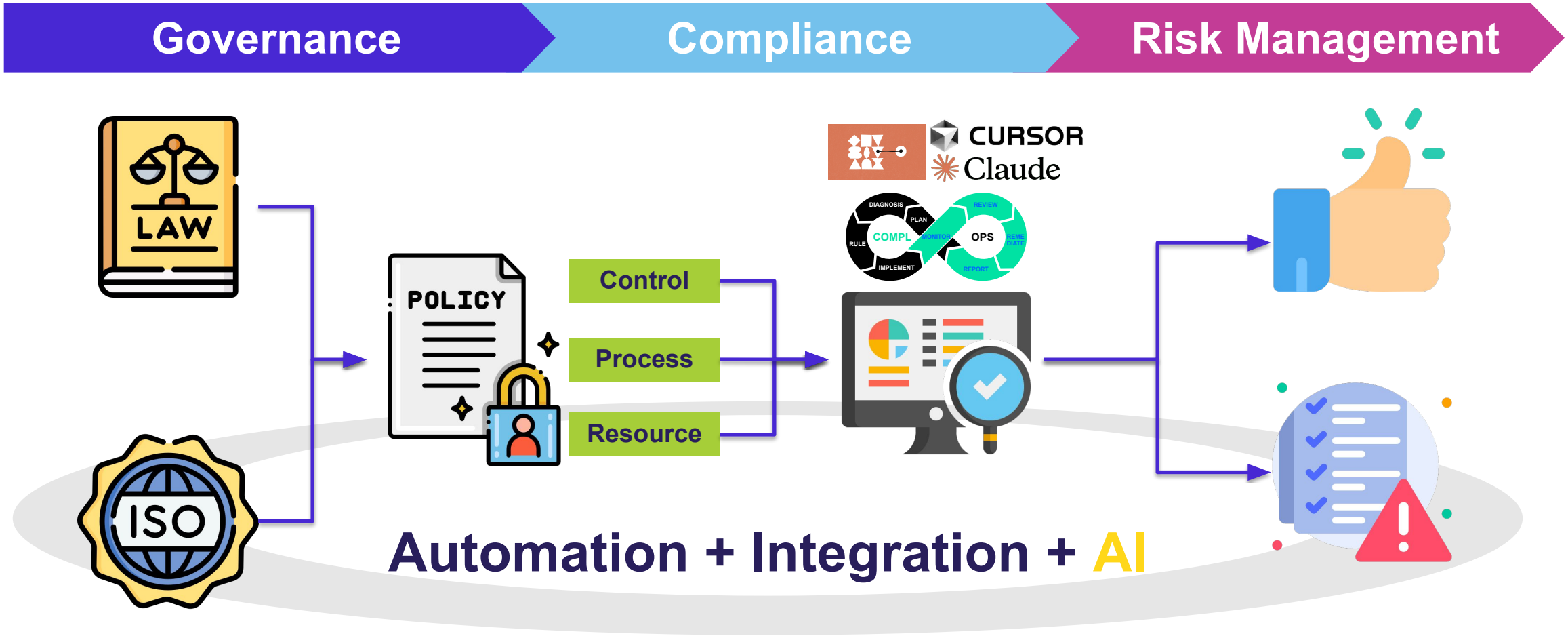
(Steampipe Query를 이용하여 점검 실행)

3. 결과 요약

(전체 RDS 중 요건 충족/미충족 결과)



GRCOps의 실현


Governance
Compliance
Risk Management
LAW
ISO
POLICY
Control
Process
Resource
CURSOR
Claude
DIAGNOSIS
PLAN
REVIEW
RULE
COMPL
MONITOR
OPS
IMPLEMENT
REPORT
Automation + Integration + AI

감사합니다