로그, 방치된 데이터에서 비즈니스의 블랙박스로

대한민국 컴플라이언스 기준
AWS 로그 라이프사이클 관리 전략

우리는 로그를 ‘모으고’ 있을까, ‘관리’하고 있을까?

“로그를 관리해야 하는데 어떤 로그를 관리해야 하는지 정의가 되어 있지 않다.”

현실

- 주요정보통신기반시설 기술적 취약점 분석 평가 항목에 ‘로그의 정기적 검토 및 보고’, ‘정책에 따른 시스템 로깅 설정’이 있지만, 시스템별 로그 보관 정책 및 표준 수립이 어렵다.
- 로그 관리 지침이 별도로 존재하지 않고, 개발보안가이드나 시스템운영지침 내에 일부 내용만 포함되어 있다.

로그는 보안 사고의 '블랙박스'이자, 컴플라이언스의 '증거'입니다.

리스크 (Risks)

침해 사고 분석 불가: 사고 발생 시 원인 분석(Forensic)이 불가능하여 대응 및 복구가 지연됨

법적 제재: 법적 보존 연한 미준수로 인한 과태료 부과 위험

내부 통제 실패: 중요 시스템 접근 기록 부재로 내부 정보 유출 및 부정 행위 추적 불가

목표 (Goals)

가시성 확보: 모든 AWS 서비스에 대한 행위를 추적하여 이상 징후를 조기 탐지

무결성 보장: 로그의 위변조를 원천적으로 방지하여 증거 능력을 확보

규제 준수: 국내 주요 보안 법규(ISMS-P 등) 요구사항을 완벽히 만족

우리가 반드시 지켜야 할 기준: 법은 타협의 대상이 아니다.

ISMS-P 인증 기준 (2.9.4 로그 및 접속기록 관리)

시스템, 네트워크, 보안시스템의 이벤트 및 감사 로그 관리 요구.

특히 개인정보처리시스템 접속기록(접속자 계정, 일시, IP, 수행업무 등)의 상세 기록을 요구.

개인정보보호법 (제29조 안전조치의무)

개인정보처리시스템 접속 기록을 최소 1년 이상 보관.

보관된 접속 기록을 월 1회 이상 점검할 의무.

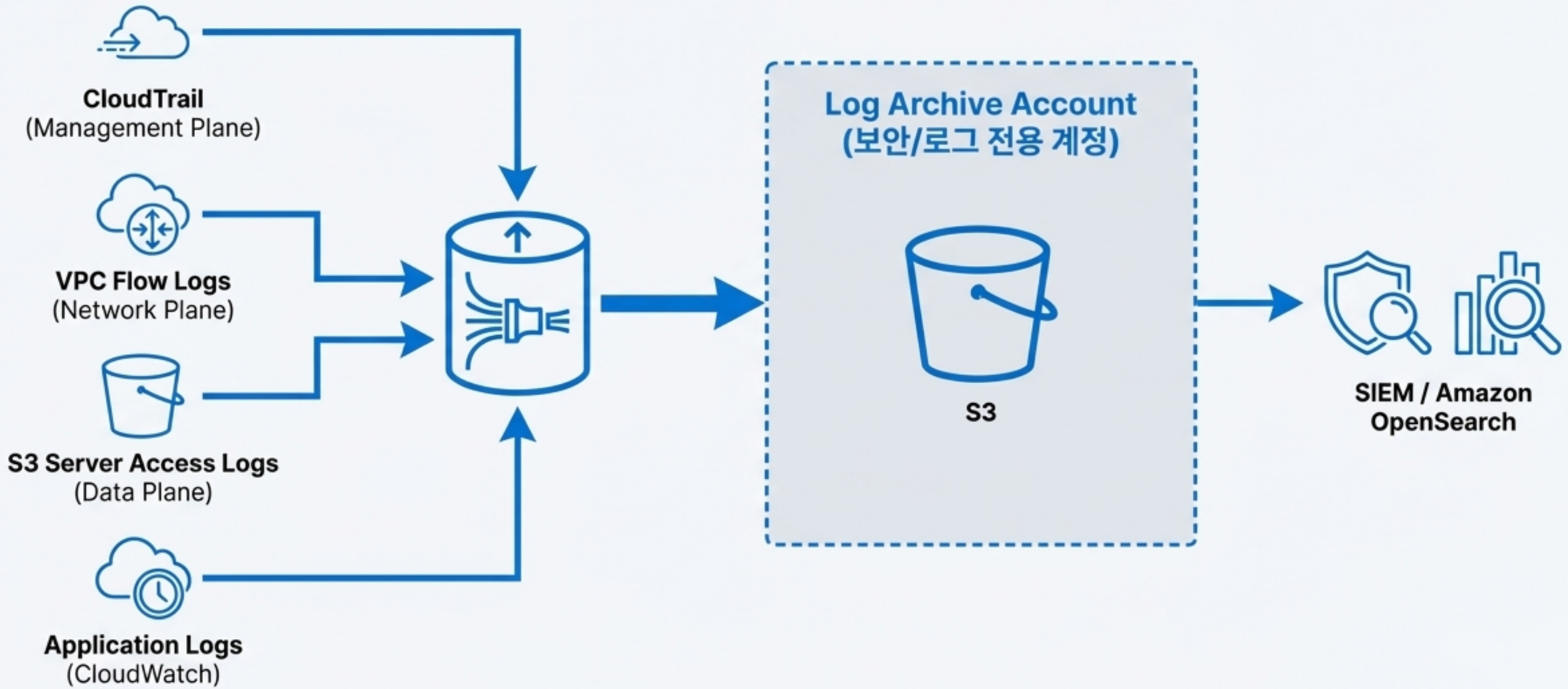
통신비밀보호법

인터넷 로그 기록 등 통신사실확인자료에 대한 법적 보존 기간 준수 의무.

그래서, 얼마나 보관해야 하는가?

로그 분류	주요 법적 근거	최소 보관 기간
개인정보처리시스템 접속기록	개인정보 보호법 제29조	1년 이상 (5만명 이상 정보주체 또는 고유식별/민감정보 처리 시 2년 이상)
통신 사실 확인 자료 (네트워크/웹 로그)	통신비밀보호법 제15조의2	3개월 이상
전자금융거래 기록	전자금융거래법 제22조	5년
보안시스템 및 감사 로그	정보통신망법, 개인정보 보호법	최소 6개월 이상 권고
시스템/네트워크 이벤트 로그	ISMS-P 인증 기준	6개월 이상 권장

중앙 집중형 로깅: 모든 흔적을 한 곳으로



5단계 로그 라이프사이클: 완벽한 통제를 위한 실행 계획

1. 생성 (Generation)

2. 수집 (Collection)

3. 이용 및 모니터링 (Use & Monitoring)

4. 저장 및 보존 (Storage & Retention)

5. 파기 (Destruction)

1단계. 생성: 빠짐없이 남겨라

로깅 활성화는 선택이 아닌 필수 (Default On).

Key Settings

- 모든 AWS 리전(Region)에 CloudTrail 활성화.
- 핵심 VPC의 Flow Logs 활성화 (허용/거부 트래픽 모두 로깅).
- ELB, CloudFront 등 모든 엣지 서비스의 로깅 활성화.

👮 행동 수칙 1

- 모든 EC2/Container는 Golden Image를 통해 부팅 시 로그 에이전트 실행을 보장.
- 애플리케이션 로그는 '누가(Who), 언제(When), 무엇을(What), 어디서(Where)'를 식별할 수 있는 정보를 반드시 포함 (민감정보 삭제, 개인정보 해싱 필수).
- 로그 포맷은 JSON 형태로 표준화하고, 환경(운영/개발)별로 로그 레벨 정의.

2단계. 수집: 안전하게 한곳으로 모아라

실시간성 확보 및 전송 구간 보안.

Key Technologies

- 로그 전송은 AWS PrivateLink를 통한 내부망 전송을 우선하여 인터넷 노출 최소화.
- 모든 로그는 생성된 계정이 아닌, 격리된 Log Archive 전용 계정으로 중앙 집중화.

👮 행동 수칙 2

- 운영 계정(Prod) 내에 로그를 장기 보관하지 말고, 즉시 보안/로그 전용 계정(Log Archive)의 S3로 전송.
- 로그 전송 시 반드시 TLS 암호화를 적용하여 데이터 가로채기 방지.
- 로그 수집 파이프라인(Kinesis, Firehose)의 장애 발생 시 즉시 알림(Alert)을 설정하여 '로그 유실' 방지.

3단계. 이용 & 모니터링: 보고, 분석하고, 대응하라

이상 징후의 조기 탐지 및 신속한 대응.

Key Technologies

- **Amazon GuardDuty**: 🗣️ 머신러닝 기반의 지능형 위협 탐지.
- **CloudWatch Alarms**: 'Unauthorized', 'Login Failed' 등 특정 로그 패턴 매칭 시 자동 경보.
- **SIEM 연동**: 외부 보안 정보 이벤트 관리 시스템과 연동하여 심층 상관 분석 수행.

👮 행동 수칙 3

- **월 1회 이상** 주요 시스템 접속 기록 및 권한 변경 이력을 점검하고 보고서 작성 (ISMS-P 증적 확보).
- Root 계정 사용, 로그 파이프라인 변경 등 회사가 정의한 **고위험 이벤트**는 Slack/SNS 등 메신저로 실시간 알림 구성.
- 디버깅 목적 외 프로덕션 로그 데이터에 대한 임의 접근을 금지하고, 접근 시 반드시 사유 기록.

4단계. 저장 & 보존: 위변조 불가능하게 보관하라

무결성(Integrity) 및 가용성(Availability) 보장.

Key Technologies

- **S3 Object Lock (WORM):** Write Once, Read Many 설정으로 지정된 보존 기간 동안 삭제/수정 원천 차단.
- **KMS 기반 서버 측 암호화 (SSE-KMS):** 저장된 모든 로그 파일을 암호화.
- **CloudTrail Log File Validation:** 로그 파일의 무결성 검증 기능 활성화.

👮 행동 수칙 4

- 로그가 저장된 S3 버킷에 **MFA Delete** 기능을 활성화하여 실수나 악의적 삭제 방지.
- 로그 저장소에 대한 접근 권한은 '최소 권한의 원칙'을 적용하며, **사전 승인 없이는 수정/삭제 권한을 절대 부여하지 않음.**

5단계. 파기: 기한이 지나면 확실하게 지워라

개인정보 목적 달성 후 파기 의무 준수 및 스토리지 비용 최적화.

Key Technologies

- **S3 Lifecycle Policy**: 법적 보존 기한이 만료된 객체를 자동으로 영구 삭제.
- **S3 Glacier Transition**: 장기 보관이 필요하지만 즉시 접근할 필요 없는 로그는 저비용 스토리지로 이동 후 파기.

👮 행동 수칙 5

- 법적 보존 기한(에: 2년)이 도래한 로그는 S3 Lifecycle 정책에 의해 **자동으로 파기**되도록 구성.
- 파기된 로그에 대해 **'언제, 어떤 로그가, 어떤 정책에 의해 파기되었는지'** 시스템 기록(메타데이터)을 남겨 사후 증빙.
- 수사나 감사 등으로 법적 보존(Legal Hold)이 필요한 경우, 해당 로그의 파기 정책을 일시 중지하는 프로세스 마련.

핵심 요약: 혼돈에서 통제로

- **정의하고 자동화하라 (Define & Automate):** 단순히 로그를 수집하지 말고, 명확한 정책으로 전체 라이프사이클을 정의하고 자동화하십시오.
- **중앙화하고 격리하라 (Centralize & Isolate):** 모든 로그를 보안 전용 계정으로 중앙화하여 무결성을 보장하고 통제권을 확보하십시오.
- **준수하고 대응하라 (Comply & Respond):** 관리되는 로그를 컴플라이언스 증거로 활용함과 동시에, 보안 위협을 탐지하고 대응하는 능동적 도구로 사용하십시오.