ProcessMind 감사 로그 및 SIEM 설명서

발효일: 2026년 11월 12일

이 설명서는 ProcessMind B.V.가 고객 데이터에 대해 수행된 보안 관련 조치 및 관리 조치(이하 "감사 로그")를 기록하는 방법을 설명합니다. 본 설명서는 보안 조치, 데이터 처리 부록, 고객 계약 및 하위 처리자 목록을 보완합니다.

---

1. 범위

1.1 단일 감사 로그. ProcessMind는 고객 데이터 및 ProcessMind 서비스에 대해 수행된 보안 관련 조치 및 관리 조치를 위한 단일 감사 로그를 유지합니다. 감사 로그는 운영(애플리케이션) 로깅, HTTP 액세스 로깅 및 제품의 활동 피드와 별개입니다. 이러한 데이터 스트림은 서로 다른 목적을 위해 사용되며 감사 추적 기록으로 간주되지 않습니다.

1.2 감사 로그가 아닌 것. 감사 로그는 고객 데이터에 대한 모든 읽기 작업을 기록하지 않으며, 프로세스 모델, 다이어그램, 문서 또는 시뮬레이션에 대한 제품의 변경 이력도 아닙니다. 이러한 항목은 제품 내에서 확인할 수 있는 프로세스 변경 이력에 기록됩니다.

---

2. 각 감사 기록에 포함되는 내용

2.1 필드. 각 기록에는 아래 필드가 포함됩니다. 필드 집합은 기록 스키마에 따라 고정됩니다. 즉, 목록에 없는 필드를 기록에 추가할 수 없으며, 작업은 레지스트리에 선언되지 않은 필드를 추가할 수 없습니다.

- *schemaVersion* (숫자): 기록 스키마 버전. 현재 버전은 1입니다.
- *eventId* (문자열): 고유한 기록 식별자입니다. 새 기록에는 ULID를 사용하며, 이전 저장소에서 마이그레이션된 행은 기존 UUID를 유지합니다.
- *occurredAt*, *ingestedAt* (타임스탬프): 작업이 발생한 시각과 감사 기록 작성기가 기록을 저장한 시각입니다. 두 시각 모두 UTC 기준입니다.
- *eventClass* (열거형): security, auth, admin, data, api, ai 또는 platform입니다.
- *action* (열거형): 검토를 거친 폐쇄형 작업 레지스트리의 코드 하나입니다. 예: auth.login.blocked 또는 api.key.revoked.
- *outcome* (열거형): success, failure, denied 또는 error입니다.

- *severity* (열거형): info, notice, warning 또는 critical이며, 결과에 따라 결정됩니다. 성공한 작업에는 레지스트리 기본값(info, 작업에 별도 지정이 없는 경우)이 사용되고, 실패는 notice로, 거부 또는 오류는 warning으로 기록됩니다.
- *actor* (객체): 작업을 수행한 주체입니다. type(user, apiKey, service, system 또는 anonymous), id, email, displayName 및 다른 계정을 대신하여 작업이 수행된 경우 onBehalfOf와 onBehalfOfEmail이 포함됩니다.
- *actorContext* (객체): 작업을 수행한 세션입니다. sessionId, authMethod(oidc, password, loginToken, apiKey 또는 none) 및 지원 세션 여부를 나타내는 플래그가 포함됩니다.
- *organizationId*, *tenantId* (식별자, null 허용): 작업이 속한 조직 및 환경입니다. 고객과 관련이 없거나 환경보다 상위 수준에 해당하는 기록에서는 null입니다.
- *resource* (객체, null 허용): 영향을 받은 객체입니다. type, id 및 name이 포함되며, type은 apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant 또는 user 중 하나입니다.
- *source* (객체): 기록이 생성된 위치입니다. service(api, externalApi, superadminApi, worker, cron 또는 webSocket), function 및 version이 포함됩니다.
- *stage*, *region* (문자열): 기록을 생성한 배포 단계(예: prod) 및 AWS 리전(고객 기록의 경우 eu-central-1)입니다.
- *correlation* (객체): 기록을 발생시킨 요청 및 동일한 흐름에서 그보다 앞선 기록과 연결하는 requestId, traceId 및 parentEventId입니다.
- *network* (객체, null 허용): sourceIp 및 userAgent입니다. 레지스트리 항목에서 수집을 허용한 작업에 한해 수집됩니다. 해당 작업은 로그인, 액세스 결정, 관리 및 설정 변경, 데이터 업로드, 다운로드 및 내보내기, API 키 변경 및 AI 정책 변경입니다.
- *detail* (객체): 해당 작업의 자체 페이로드이며, 해당 작업의 스키마에 따라 검증됩니다. 값은 기본형(string, number, boolean, null)만 허용되므로 기록을 계속 조회하고 삭제 처리할 수 있습니다.

2.2 폐쇄형 용어 체계. 작업은 고정되고 검토된 작업 코드 목록에서 선택되며, 감사 기록에는 자유 형식의 메시지가 없습니다. 각 작업은 포함할 수 있는 추가 필드도 선언하므로, 기록에 새로운 유형의 콘텐츠가 조용히 추가될 수 없습니다.

---

3. 기록되는 작업

3.1 현재 기록되는 항목. ProcessMind는 다음을 포함한 작업을 기록합니다.

- **인증:** 로그인 성공 및 실패, 차단된 로그인(계정 잠김, 허용되지 않은 도메인, 확인되지 않은 공급자 이메일), 로그아웃, 로그인 토큰 발급 및 전달.
- **권한 부여:** 거부된 모든 외부 API 자격 증명, 범위 및 테넌트 상태와 출처(CORS) 거부를 포함한 액세스 거부.
- **지원 액세스:** 고객 계정에서 ProcessMind 지원 세션이 시작된 사실. 운영자와 영향을 받는 계정이 모두 명시됩니다.
- **API 자격 증명:** API 키 생성, 범위 변경 및 폐기(부여된 범위 포함).
- **계정 및 역할 관리:** 사용자 생성, 초대, 관리자 프로필 수정, 삭제, 역할 부여 및 취소, 테넌트 또는 조직 멤버십 변경.
- **조직 수명 주기:** 생성, 삭제, 복원, 삭제 예약 및 취소, 삭제 완료.
- **데이터 업로드, 다운로드 및 내보내기:** 아티팩트 업로드, 다운로드 및 삭제, 표 형식 데이터 업로드 및 업데이트, 내보내기 다운로드, 데이터 테이블 삭제, 웹후크(연결) 생성, 변경 및 삭제.
- **결제 상태:** 요금제 변경, 결제에 따른 서비스 중단 및 복구, 구독 취소.
- **ProcessMind의 공급자 콘솔:** 권한이 필요한 쿼리 실행, 사용자 및 조직 관리, 설정 및 기능 변경, 결제 동기화 요청 및 마이그레이션.
- **ProcessMind의 예약 작업에 의한 관리 및 파괴적 조치:** 테넌트, 조직, 사용자 및 리드 삭제, 보존 기간에 따른 정리 작업, 파이프라인 실패.
- **감사 로그 무결성:** 감사 로그 자체의 쓰기 경로에서 발생한 실패.

3.2 워크스페이스 수정. 워크스페이스 내 수정(프로세스 모델, 문서, 시뮬레이션, 대시보드, 댓글 및 북마크)은 감사 로그가 아니라 제품 자체의 프로세스 변경 이력에 기록됩니다. 감사 로그에는 데이터를 업로드, 다운로드, 내보내기 또는 삭제한 사용자가 기록되고, 변경 이력에는 모델 내에서 변경된 내용이 기록됩니다. 현재 기록되는 작업 코드 목록은 요청 시 ProcessMind에서 제공받을 수 있습니다.

---

4. 기록되지 않는 항목

비밀번호, 인증 토큰, API 키 값, 쿠키, 권한 부여 헤더, 요청 또는 응답 본문, 파일 콘텐츠, 사전 서명된 URL, AI 프롬프트 또는 완성 결과는 감사 로그에 기록되지 않습니다. 감사 기록에는 귀속 확인에 필요한 개인정보가 포함될 수 있습니다. 즉, 작업자의 이메일 주소와 레지스트리

항목에서 수집을 허용한 작업(로그인, 액세스 결정, 관리 및 설정 변경, 데이터 이동, API 키 및 AI 정책 변경)의 출처 IP 주소 및 사용자 에이전트가 포함될 수 있습니다. 허용되는 필드는 작업별로 정의되며 작업이 추가될 때 검토됩니다.

---

5. 무결성

5.1 추가 전용. 감사 로그는 추가 전용입니다. 어떤 애플리케이션 역할에도 감사 로그를 업데이트하거나 삭제할 권한이 없으며, 데이터베이스 제약 조건이 두 작업을 모두 거부합니다.

5.2 단일 작성기. 기록은 단일 구성 요소가 작성하며, 이 구성 요소는 기록 전에 작업 코드와 페이로드를 검증합니다. 검증에 실패한 기록은 일부만 작성되는 대신 거부되고 보고됩니다.

5.3 실패 처리. 감사 기록 쓰기가 실패하더라도 해당 기록이 설명하는 업무 작업은 실패하지 않습니다. 실패는 경보가 설정된 운영 경로에 기록되며, 복구할 수 있도록 해당 기록 자체를 보조 사본에 보존합니다.

---

6. 보존 및 위치

6.1 보존. 감사 기록은 이벤트 발생일로부터 최소 10년간 보존됩니다.

6.2 위치 및 암호화. 감사 기록은 유럽연합(독일 프랑크푸르트, `eu-central-1`)에 저장되며, 고객이 관리하는 AWS KMS 키를 사용하여 저장 시 암호화됩니다. 또한 사고가 발생하는 동안 조사할 수 있도록 액세스가 통제된 Amazon CloudWatch 로그 그룹에 실시간 사본을 기록합니다.

6.3 리전 간 복제 없음. 감사 기록은 유럽연합 외부로 복제되지 않습니다.

---

7. 감사 기록에 대한 액세스

7.1 이용 자격. 앱 내 감사 로그는 Process Architecture 요금제 이상에 포함됩니다. 조직 관리자는 조직 전체의 기록을 읽을 수 있고, 테넌트 범위 관리자는 자신이 관리하는 테넌트의 기록을 읽을 수 있습니다. 범위는 인증된 세션을 기준으로 결정되고 쿼리 전에 확인되므로, 요청으로 다른 테넌트 또는 조직까지 범위를 확대할 수 없습니다.

7.2 ProcessMind 직원. ProcessMind 직원은 지원, 사고 대응 또는 법적 의무 이행을 위해 알아야 할 필요가 있는 경우에만 감사 기록에 액세스합니다. 고객 간 액세스는 전담 지원

역할로 제한되며, 그러한 액세스 자체도 관리 조치로 기록됩니다.

7.3 기록을 받는 방법. 조직 및 테넌트 관리자는 앱 내 감사 로그에서 감사 기록을 읽고 외부 API를 통해 가져오거나 내보낼 수 있습니다. 대량 요청 또는 지원이 필요한 요청의 경우 ProcessMind 지원팀은 지정된 조직, 테넌트 및 기간의 기록을 CSV 또는 JSON 형식으로 제공하며, 일반 요청은 영업일 기준 5일 이내 제공을 목표로 합니다.

---

8. 감사 기록 삭제

8.1 요청에 따른 삭제. 확인된 서면 요청을 받으면 ProcessMind는 감사 저장소에서 고객 조직에 속한 감사 기록을 삭제하고, 삭제 사실을 서면으로 확인합니다. 운영용 CloudWatch 사본은 기록별로 수정할 수 없으며 자체 보존 기간이 만료되면 삭제됩니다.

8.2 보존되는 정보. 삭제가 이루어졌다는 기록(조직 식별자, 날짜, 요청자, 사유 및 삭제된 기록 수)은 플랫폼 수준의 감사 기록으로 보존되며 고객 데이터를 포함하지 않습니다. 고객에게 속하지 않는 기록(ProcessMind 플랫폼 이벤트)은 고객의 삭제 요청에 영향을 받지 않습니다.

8.3 개인의 삭제 요청. 계속 운영 중인 고객 내 개인에 관한 요청의 경우, GDPR 제17조 제3항 (b) 및 (e)에 따라 허용되는 범위에서 법적 청구의 설정, 행사 또는 방어를 위해 보안 기록을 보존합니다. 해당 근거는 처리 활동 기록 및 개인정보 처리방침에 기록됩니다.

---

9. SIEM 통합 및 내보내기

9.1 이용 가능성. 변경 불가능한 감사 아카이브는 Enterprise 옵션이며, 요청 시 고객 조직에 활성화됩니다. 조직별 접두사가 지정된 Object-Locked(WORM) S3 버킷에 매일 압축된 NDJSON 객체를 기록하며, 매니페스트 및 야간 대조 작업을 포함합니다.

9.2 현재 제공 방식. ProcessMind는 현재 기본 SIEM 커넥터 또는 푸시 피드를 제공하지 않습니다. 제공 방식은 풀 방식이며 다음 세 가지 경로를 이용합니다. 읽기 API(`GET /v1/tenant/{tenantId}/audit`), 제한된 내보내기 작업(`POST /v1/tenant/{tenantId}/audit/exports`을 사용하여 생성하고, 단기간 유효한 다운로드 URL을 반환하는 상태 호출을 통해 결과를 가져옵니다), 그리고 Enterprise 아카이브를 사용하는 경우 고객의 SIEM이 액세스 계약을 통해 읽는 Object-Locked 버킷 내 조직별 접두사

아래의 일일 객체입니다. ProcessMind는 고객이 선택한 위치로 고객이 정한 일정에 따라 기록을 전송하지 않습니다.

9.3 ProcessMind 자체 모니터링. ProcessMind의 보안 모니터링은 동일한 기록을 사용합니다. 감사 기록 쓰기 실패, 인증 실패 급증, 권한 변경 및 파괴적인 관리 조치가 내부 경보를 발생시킵니다.

---

10. 고객에게 제공되는 증거

요청이 있는 경우, 해당되는 때에는 비밀유지 조건에 따라 ProcessMind는 본 설명서, 보안 조치, 데이터 처리 부록, 하위 처리자 목록, 삭제 처리된 감사 기록 샘플 및 액세스 및 삭제 요청에 사용되는 절차를 제공합니다.

---

11. 제한 사항

의문의 여지를 없애기 위해 명확히 하자면, ProcessMind는 모든 조직에 대해 추가 전용 감사 저장소를 제공하며, 감사 아카이브 이용 권한이 활성화된 경우 야간 매니페스트 대조가 이루어지는 Object-Locked(WORM) 사본을 제공합니다. ProcessMind는 현재 해시 체인, 기본 실시간 SIEM 푸시 커넥터, 사용자별 감사 기록 삭제 처리, 이 통제를 포함하는 ISO 27001 또는 SOC 2 인증, 또는 고객 데이터의 모든 읽기 작업에 대한 기록을 주장하지 않습니다. 고객은 앱 내 감사 로그 및 외부 API를 통해 직접 기록을 읽고 내보낼 수 있습니다.