ProcessMind Denetim Günlüğü ve SIEM Beyanı

Yürürlük tarihi: 12 Kasım 2026

Bu beyan, ProcessMind B.V.'nin Müşteri Verileri üzerinde gerçekleştirilen güvenlikle ilgili ve idari işlemleri nasıl kaydettiğini ("denetim günlüğü") açıklar. Bu beyan, Güvenlik Önlemleri, Veri İşleme Eki, Müşteri Sözleşmesi ve Alt İşleyenler Listesi'ni tamamlar.

---

1. Kapsam

1.1 Tek bir denetim günlüğü. ProcessMind, Müşteri Verileri ve ProcessMind Hizmeti üzerinde gerçekleştirilen güvenlikle ilgili ve idari işlemler için tek bir denetim günlüğü tutar. Denetim günlüğü; operasyonel (uygulama) kaydından, HTTP erişim kaydından ve ürünün etkinlik akışından ayrıdır; bu akışlar farklı amaçlara hizmet eder ve denetim izi olarak sunulmaz.

1.2 Ne olmadığı. Denetim günlüğü, Müşteri Verilerinin her okunmasının kaydı değildir ve süreç modelleri, diyagramlar, belgeler veya simülasyonlar için ürünün değişiklik geçmişi değildir. Bunlar, ürün içinde bulunan süreç değişiklik geçmişine kaydedilir.

---

2. Her denetim kaydının içeriği

2.1 Alanlar. Her kayıt aşağıdaki alanları içerir. Alan kümesi kayıt şemasıyla sabitlenmiştir: bir kayda bu listede bulunmayan bir alan eklenemez ve bir işlem, kayıt defterinde beyan etmediği bir alanı ekleyemez.

- *schemaVersion* (sayı): kayıt şeması sürümü; şu anda 1.
- *eventId* (dize): benzersiz kayıt tanımlayıcısı. Yeni kayıtlar ULID kullanır; önceki depodan taşınan satırlarda UUID korunur.
- *occurredAt*, *ingestedAt* (zaman damgaları): işlemin gerçekleştiği zaman ve denetim yazıcısının kaydı depoladığı zaman. Her ikisi de UTC cinsindendir.

- *eventClass* (enum): security, auth, admin, data, api, ai veya platform.
- *action* (enum): kapalı ve gözden geçirilmiş işlem kayıt defterinden bir kod; örneğin auth.login.blocked veya api.key.revoked.
- *outcome* (enum): success, failure, denied veya error.
- *severity* (enum): info, notice, warning veya critical; sonuçtan türetilir. Başarılı bir işlem, kayıt defterindeki varsayılan değeri kullanır (işlem aksini belirtmedikçe info); başarısızlık notice, denied veya error ise warning olarak kaydedilir.
- *actor* (nesne): işlemi yapan kişi. type (user, apiKey, service, system veya anonymous), id, email, displayName ve işlem başka bir hesap adına yürütüldüğünde onBehalfOf ile onBehalfOfEmail.
- *actorContext* (nesne): işlemi gerçekleştiren oturum. sessionId, authMethod (oidc, password, loginToken, apiKey veya none) ve destek oturumu işareti.
- *organizationId*, *tenantId* (tanımlayıcılar, null olabilir): işlemin ait olduğu kuruluş ve ortam. Müşteriyle ilgili olmayan veya ortamın üzerinde yer alan kayıtlar için null.
- *resource* (nesne, null olabilir): etkilenen nesne. type, id ve name; type şu değerlerden biridir: apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant veya user.
- *source* (nesne): kaydın oluşturulduğu yer. service (api, externalApi, superadminApi, worker, cron veya webSocket), function ve version.
- *stage*, *region* (dizeler): kaydı oluşturan dağıtım aşaması (örneğin prod) ve AWS bölgesi (müşteri kayıtları için eu-central-1).
- *correlation* (nesne): kaydı, buna neden olan istekle ve aynı akışta öncesinde yer alan kayıtlarla ilişkilendiren requestId, traceId ve parentEventId.
- *network* (nesne, null olabilir): sourceIp ve userAgent. Yalnızca kayıt defteri girdisinde bu alanların kullanılmasına izin verilen işlemler için yakalanır: oturum açma, erişim kararları, idari işlemler ve ayar

değişiklikleri, veri yüklemeleri, indirmeler ve dışa aktarımlar, API anahtarı değişiklikleri ve AI politikası değişiklikleri.
- *detail* (nesne): işlemin kendi yükü; ilgili işlemin şemasına göre doğrulanır. Değerler yalnızca ilkel türlerden oluşur (string, number, boolean, null); böylece kayıt sorgulanabilir ve hassas bilgilerden arındırılabilir.

2.2 Kapalı bir sözlük. İşlemler, sabit ve gözden geçirilmiş işlem kodları listesinden seçilir; denetim kaydında serbest metin mesajı bulunmaz. Her işlem ayrıca taşıyabileceği ek alanları beyan eder; böylece bir kayda fark edilmeden yeni bir içerik türü eklenemez.

---

3. Hangi işlemler kaydedilir

3.1 Şu anda kaydedilenler. ProcessMind, diğerlerinin yanı sıra aşağıdakileri kaydeder:

- **Kimlik doğrulama:** başarılı ve başarısız oturum açma, engellenen oturum açma (kilitli hesap, izin verilmeyen etki alanı, doğrulanmamış sağlayıcı e-postası), oturum kapatma, oturum açma belirteci oluşturma ve devretme.
- **Yetkilendirme:** her reddedilen harici API kimlik bilgisi, kapsam ve kiracı durumu ile kaynak (CORS) retleri dahil olmak üzere erişim retleri.
- **Destek erişimi:** bir ProcessMind destek oturumunun müşteri hesabında başlatılması; hem operatörün hem de etkilenen hesabın belirtilmesi.
- **API kimlik bilgileri:** API anahtarlarının oluşturulması, kapsamının değiştirilmesi ve iptal edilmesi; verilen kapsamlar dahil.
- **Hesap ve rol yönetimi:** kullanıcı oluşturma, davet etme, yönetici profillerini düzenleme, silme, rol verme ve iptal etme ile kiracı veya kuruluş üyeliği değişiklikleri.
- **Kuruluş yaşam döngüsü:** oluşturma, silme, geri yükleme, silme planlama ve iptal etme ile silme işleminin tamamlanması.

- **Veri yükleme, indirme ve dışa aktarma:** artifact yükleme, indirme ve silme; tablo verisi yükleme ve güncelleme; dışa aktarımları indirme; veri tablosu silme ve webhook (bağlantı) oluşturma, değiştirme ve silme.
- **Faturalandırma durumu:** plan değişiklikleri, ödemeye bağlı askıya alma ve yeniden etkinleştirme ile abonelik iptali.
- **ProcessMind'in sağlayıcı konsolu:** ayrıcalıklı sorgu yürütme, kullanıcı ve kuruluş yönetimi, ayar ve özellik değişiklikleri, faturalandırma senkronizasyonu istekleri ve geçişler.
- **ProcessMind'in zamanlanmış işleri tarafından gerçekleştirilen idari ve yıkıcı işlemler:** kiracı, kuruluş, kullanıcı ve lead silme işlemleri, saklama süresi taramaları ve işlem hattı hataları.
- **Denetim günlüğü bütünlüğü:** denetim günlüğünün kendi yazma yolundaki hatalar.

3.2 Çalışma alanı düzenlemeleri. Bir çalışma alanındaki düzenlemeler (süreç modelleri, belgeler, simülasyonlar, panolar, yorumlar ve yer işaretleri) denetim günlüğüne değil, ürünün kendi süreç değişiklik geçmişine kaydedilir. Denetim günlüğü, verileri kimin yüklediğini, indirdiğini, dışa aktardığını veya sildiğini kaydeder; değişiklik geçmişi ise bir modelde nelerin değiştiğini kaydeder. Kaydedilen işlem kodlarının güncel listesi ProcessMind'den talep üzerine edinilebilir.

---

4. Hiçbir zaman kaydedilmeyenler

Parolalar, kimlik doğrulama belirteçleri, API anahtarı değerleri, çerezler, yetkilendirme başlıkları, istek veya yanıt gövdeleri, dosya içerikleri, önceden imzalanmış URL'ler ve AI istemleri veya tamamlamaları denetim günlüğüne hiçbir zaman yazılmaz. Denetim kayıtları, ilişkilendirme için gerekli kişisel verileri içerebilir: işlemi gerçekleştiren kişinin e-posta adresi ve kayıt defteri girdisinde bu alanların kullanılmasına izin verilen işlemler için kaynak IP adresi ile kullanıcı aracısı (oturum açma, erişim kararları, idari işlemler ve ayar değişiklikleri, veri aktarımı, API anahtarı ve AI politikası değişiklikleri).

İzin verilen alanlar her işlem için tanımlanır ve işlem eklendiğinde gözden geçirilir.

---

5. Bütünlük

5.1 Yalnızca eklemeli. Denetim günlüğüne yalnızca kayıt eklenebilir. Hiçbir uygulama rolünün bu günlük üzerinde güncelleme veya silme ayrıcalığı yoktur ve bir veritabanı kısıtlaması her iki işlemi de reddeder.

5.2 Tek yazıcı. Kayıtlar, yazılmadan önce işlem kodunu ve yükünü doğrulayan tek bir bileşen tarafından yazılır. Doğrulamadan geçmeyen bir kayıt kısmen yazılmak yerine reddedilir ve bildirilir.

5.3 Hata yönetimi. Başarısız bir denetim yazma işlemi, tanımladığı iş işleminin başarısız olmasına hiçbir zaman neden olmaz. Hata, alarm üreten bir operasyonel yolda kaydedilir ve kurtarılabilmesi için kaydın kendisi ikincil bir kopyada saklanır.

---

6. Saklama ve konum

6.1 Saklama. Denetim kayıtları, olay tarihinden itibaren en az on (10) yıl saklanır.

6.2 Konum ve şifreleme. Denetim kayıtları Avrupa Birliği'nde (Frankfurt, Almanya, `eu-central-1`) saklanır ve bekleme hâlindeyken müşteri tarafından yönetilen bir AWS KMS anahtarıyla şifrelenir. Ayrıca, bir olay meydana gelirken incelenebilmesi için canlı bir kopya erişim denetimli bir Amazon CloudWatch günlük grubuna yazılır.

6.3 Bölgeler arası çoğaltma yoktur. Denetim kayıtları Avrupa Birliği dışına çoğaltılmaz.

---

7. Denetim kayıtlarına erişim

7.1 Erişim yetkisi. Uygulama içi denetim günlüğü, Process Architecture planına ve üzerindeki planlara dahildir. Kuruluş yöneticisi kuruluşun tamamını okuyabilir; kiracı kapsamındaki yönetici kendi kiracısını okuyabilir. Kapsam, kimliği doğrulanmış oturumdan türetilir ve sorgudan önce denetlenir; bu nedenle bir istek kapsamı başka bir kiracıya veya kuruluşa genişletemez.

7.2 ProcessMind personeli. ProcessMind personeli denetim kayıtlarına yalnızca destek, olay müdahalesi veya yasal bir yükümlülük amacıyla ve bilmesi gerekenler ilkesi uyarınca erişir. Müşteriler arası erişim, özel bir destek rolüyle sınırlandırılmıştır ve bu tür erişimlerin kendisi de idari işlem olarak kaydedilir.

7.3 Kayıtların edinilmesi. Kuruluş ve kiracı yöneticileri, denetim kayıtlarını uygulama içi denetim günlüğünde okuyabilir ve harici API aracılığıyla alabilir veya dışa aktarabilir. Daha kapsamlı veya destekli bir talep için ProcessMind destek ekibi, belirtilen kuruluş, kiracı ve zaman aralığına ait kayıtları CSV veya JSON biçiminde sağlar; standart talepler için hedef süre beş (5) iş günüdür.

---

8. Denetim kayıtlarının silinmesi

8.1 Talep üzerine. Doğrulanmış yazılı bir talep üzerine ProcessMind, müşteri kuruluşuna ait denetim kayıtlarını denetim deposundan siler ve silme işlemini yazılı olarak teyit eder. Operasyonel CloudWatch kopyası kayıt bazında düzenlenemez; kendi saklama süresi sonunda sona erer.

8.2 Saklananlar. Silme işleminin gerçekleştiğine ilişkin kayıt (kuruluş tanımlayıcısı, tarih, talep sahibi, gerekçe ve silinen kayıt sayısı), platform düzeyinde bir denetim kaydı olarak saklanır ve Müşteri Verisi içermez. Hiçbir müşteriye ait olmayan kayıtlar (ProcessMind platform olayları), müşteri tarafından yapılan silme talebinden etkilenmez.

8.3 Bireysel silme talepleri. Talep, faal olmaya devam eden bir müşterinin bünyesindeki bir kişiyle ilgiliyse, güvenlik kaydı GDPR'nin 17(3)(b) ve (e) maddelerinin izin verdiği şekilde hukuki taleplerin oluşturulması, ileri sürülmesi veya savunulması amacıyla saklanır; bu dayanak, işleme faaliyetleri kayıtlarında ve Gizlilik Politikası'nda belirtilir.

---

9. SIEM entegrasyonu ve dışa aktarma

9.1 Kullanılabilirlik. Değiştirilemez denetim arşivi, talep üzerine müşteri kuruluşu için etkinleştirilen bir Enterprise seçeneğidir. Arşiv, kuruluş başına bir önek altında Object-Locked (WORM) bir S3 bucket'ına günlük sıkıştırılmış NDJSON nesneleri yazar; bir manifest ve gece mutabakatı da içerir.

9.2 Mevcut teslim yöntemi. ProcessMind şu anda yerel bir SIEM bağlayıcısı veya push akışı sunmamaktadır. Teslim alma, üç arayüz üzerinden pull yöntemiyle yapılır: okuma API'si (`GET /v1/tenant/{tenantId}/audit`), sınırlandırılmış dışa aktarma işi (`POST /v1/tenant/{tenantId}/audit/exports` ile oluşturulur ve kısa süreli bir indirme URL'si döndüren durum çağrısından sonuç alınır) ve Enterprise arşiviyle, müşterinin SIEM'inin bir erişim düzenlemesi aracılığıyla okuduğu, Object-Locked bucket'ta kuruluşun kendi öneki altındaki günlük nesneler. ProcessMind, kayıtları müşterinin seçtiği bir konuma kendi belirlediği bir takvime göre teslim etmez.

9.3 ProcessMind'in kendi izlemesi. ProcessMind'in güvenlik izlemesi aynı kayıtları kullanır: denetim yazma hataları, kimlik doğrulama hatalarında ani artışlar, ayrıcalık değişiklikleri ve yıkıcı idari işlemler dahili alarmları tetikler.

---

10. Müşterilere sunulan kanıtlar

Talep üzerine ve uygulanabildiği durumlarda gizlilik yükümlülüğü kapsamında ProcessMind bu beyanı, Güvenlik Önlemleri'ni, Veri İşleme Eki'ni, Alt İşleyenler Listesi'ni, denetim kayıtlarının hassas bilgilerden arındırılmış bir örneğini ve erişim ile silme talepleri için kullanılan prosedürü sağlar.

11. Sınırlamalar

Her türlü tereddüdü gidermek üzere ProcessMind, her kuruluş için yalnızca eklemeli bir denetim deposu ve denetim arşivi yetkisi etkinleştirildiğinde gece manifest mutabakatı yapılan Object-Locked (WORM) bir kopya bulunduğunu beyan eder. ProcessMind şu anda hash zinciri, yerel gerçek zamanlı SIEM push bağlayıcısı, denetim kayıtlarının kullanıcı bazında hassas bilgilerden arındırılması, bu denetimi kapsayan ISO 27001 veya SOC 2 tasdiki ya da Müşteri Verilerinin her okunmasını kapsama iddiasında bulunmamaktadır. Müşteriler, uygulama içi denetim günlüğü ve harici API aracılığıyla kendi kendilerine okuma ve dışa aktarma işlemlerini gerçekleştirebilir.