คำชี้แจงเกี่ยวกับบันทึกการตรวจสอบและ SIEM ของ ProcessMind

วันที่มีผลบังคับใช้: 12 พฤศจิกายน 2026

คำชี้แจงนี้อธิบายวิธีที่ ProcessMind B.V. บันทึกการดำเนินการด้านความปลอดภัยและการดูแลระบบที่กระทำต่อข้อมูลลูกค้า ("บันทึกการตรวจสอบ") คำชี้แจงนี้เป็นเอกสารเพิ่มเติมจากมาตรการรักษาความปลอดภัย ภาคผนวกการประมวลผลข้อมูล ข้อตกลงกับลูกค้า และรายการผู้ประมวลผลช่วง

---

1. ขอบเขต

1.1 บันทึกการตรวจสอบหนึ่งชุด ProcessMind จัดทำบันทึกการตรวจสอบชุดเดียวสำหรับการดำเนินการด้านความปลอดภัยและการดูแลระบบที่กระทำต่อข้อมูลลูกค้าและบริการ ProcessMind บันทึกการตรวจสอบนี้แยกจากบันทึกการปฏิบัติการ (แอปพลิเคชัน) บันทึกการเข้าถึง HTTP และฟีดกิจกรรมของผลิตภัณฑ์ โดยบันทึกแต่ละประเภทมีวัตถุประสงค์ต่างกัน และไม่ได้แสดงเป็นบันทึกการตรวจสอบ

1.2 สิ่งที่บันทึกนี้ไม่ใช่ บันทึกการตรวจสอบไม่ใช่บันทึกการอ่านข้อมูลลูกค้าทุกครั้ง และไม่ใช่ประวัติการเปลี่ยนแปลงของผลิตภัณฑ์สำหรับแบบจำลองกระบวนการ แผนภาพ เอกสาร หรือการจำลอง สิ่งเหล่านั้นบันทึกไว้ในประวัติการเปลี่ยนแปลงกระบวนการซึ่งเข้าถึงได้ภายในผลิตภัณฑ์

---

2. ข้อมูลที่บันทึกการตรวจสอบแต่ละรายการมี

2.1 ฟิลด์ แต่ละรายการมีฟิลด์ตามรายการด้านล่าง ชุดฟิลด์กำหนดตายตัวตามสคีมาของรายการ: รายการไม่สามารถเพิ่มฟิลด์ที่ไม่มีอยู่ในรายการนี้ได้ และการดำเนินการไม่สามารถเพิ่มฟิลด์ที่ไม่ได้ระบุไว้ในทะเบียนได้

- *schemaVersion* (ตัวเลข): เวอร์ชันสคีมาของรายการ ปัจจุบันคือ 1
- *eventId* (สตริง): ตัวระบุรายการที่ไม่ซ้ำกัน รายการใหม่ใช้ ULID ส่วนแถวที่ย้ายมาจากที่เก็บข้อมูลเดิมจะคง UUID ไว้
- *occurredAt*, *ingestedAt* (การประทับเวลา): เวลาที่การดำเนินการเกิดขึ้น และเวลาที่ผู้เขียนบันทึกการตรวจสอบจัดเก็บรายการ ทั้งสองเวลาเป็น UTC
- *eventClass* (enum): security, auth, admin, data, api, ai หรือ platform
- *action* (enum): รหัสหนึ่งรายการจากทะเบียนการดำเนินการแบบปิดที่ผ่านการตรวจทานแล้ว เช่น auth.login.blocked หรือ api.key.revoked

- *outcome* (enum): success, failure, denied หรือ error
- *severity* (enum): info, notice, warning หรือ critical ซึ่งกำหนดจากผลลัพธ์ การดำเนินการที่สำเร็จใช้ค่าเริ่มต้นของทะเบียน (info เว้นแต่จะระบุเป็นอย่างอื่น) ความล้มเหลวบันทึกเป็น notice และ denied หรือ error บันทึกเป็น warning
- *actor* (ออบเจ็กต์): ผู้ดำเนินการ type (user, apiKey, service, system หรือ anonymous), id, email, displayName และ onBehalfOf พร้อม onBehalfOfEmail ในกรณีที่การดำเนินการทำในนามบัญชีอื่น
- *actorContext* (ออบเจ็กต์): เซสชันที่ใช้ดำเนินการ sessionId, authMethod (oidc, password, loginToken, apiKey หรือ none) และแฟล็กเซสชันการสนับสนุน
- *organizationId*, *tenantId* (ตัวระบุ อาจเป็นค่าว่าง): องค์กรและสภาพแวดล้อมที่การดำเนินการนั้นเกี่ยวข้อง ค่าเป็นค่าว่างสำหรับรายการที่ไม่เกี่ยวข้องกับลูกค้ารายใด หรืออยู่เหนือระดับสภาพแวดล้อม
- *resource* (ออบเจ็กต์ อาจเป็นค่าว่าง): ออบเจ็กต์ที่ได้รับผลกระทบ type, id และ name โดย type เป็นหนึ่งใน apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant หรือ user
- *source* (ออบเจ็กต์): แหล่งที่มาของรายการ service (api, externalApi, superadminApi, worker, cron หรือ webSocket), function และ version
- *stage*, *region* (สตริง): ระยะการติดตั้งใช้งานที่สร้างรายการ (เช่น prod) และ AWS region (eu-central-1 สำหรับรายการของลูกค้า)
- *correlation* (ออบเจ็กต์): requestId, traceId และ parentEventId ซึ่งเชื่อมโยงรายการกับคำขอที่ทำให้เกิดรายการนั้น และกับรายการก่อนหน้าในโฟลว์เดียวกัน
- *network* (ออบเจ็กต์ อาจเป็นค่าว่าง): sourceIp และ userAgent บันทึกเฉพาะการดำเนินการที่รายการในทะเบียนกำหนดให้บันทึก ได้แก่ การลงชื่อเข้าใช้ การตัดสินใจเกี่ยวกับการเข้าถึง การเปลี่ยนแปลงด้านการดูแลระบบและการตั้งค่า การอัปโหลด ดาวน์โหลด และส่งออกข้อมูล การเปลี่ยนแปลง API key และการเปลี่ยนแปลงนโยบาย AI
- *detail* (ออบเจ็กต์): เพย์โหลดเฉพาะของการดำเนินการ ซึ่งตรวจสอบความถูกต้องตามสคีมาของการดำเนินการนั้น ค่าเป็นชนิดพื้นฐานเท่านั้น (string, number, boolean, null) เพื่อให้ยังสามารถสืบค้นและปกปิดข้อมูลในรายการได้

2.2 คำศัพท์แบบปิด การดำเนินการมาจากรายการรหัสการดำเนินการที่กำหนดตายตัวและผ่านการตรวจทานแล้ว โดยไม่มีข้อความอิสระในบันทึกการตรวจสอบ การดำเนินการแต่ละรายการยัง

ระบุฟิลด์เพิ่มเติมที่อาจมีได้ด้วย ดังนั้นรายการจึงไม่สามารถเพิ่มเนื้อหาประเภทใหม่โดยไม่มีการแจ้งให้ทราบ

---

3. การดำเนินการที่มีการบันทึก

3.1 รายการที่บันทึกในปัจจุบัน ProcessMind บันทึกการดำเนินการต่าง ๆ ซึ่งรวมถึง:

- **การยืนยันตัวตน:** การลงชื่อเข้าใช้ที่สำเร็จและล้มเหลว การลงชื่อเข้าใช้ที่ถูกบล็อก (บัญชีถูกล็อก โดเมนไม่ได้รับอนุญาต อีเมลของผู้ให้บริการที่ยังไม่ได้ยืนยัน) การลงชื่อออก การออกและส่งต่อ login token
- **การอนุญาต:** การปฏิเสธการเข้าถึง รวมถึงข้อมูลรับรอง external API, scope และสถานะ tenant ที่ถูกปฏิเสธทุกรายการ ตลอดจนการปฏิเสธ origin (CORS)
- **การเข้าถึงเพื่อสนับสนุน:** การเริ่มเซสชันสนับสนุนของ ProcessMind ในบัญชีลูกค้า โดยระบุทั้งผู้ปฏิบัติงานและบัญชีที่ได้รับผลกระทบ
- **ข้อมูลรับรอง API:** การสร้าง การเปลี่ยน scope และการเพิกถอน API key รวมถึง scope ที่ได้รับอนุญาต
- **การดูแลบัญชีและบทบาท:** การสร้างผู้ใช้ การเชิญ การแก้ไขโปรไฟล์ผู้ดูแลระบบ การลบ การให้และเพิกถอนบทบาท และการเปลี่ยนแปลงการเป็นสมาชิก tenant หรือองค์กร
- **วงจรชีวิตองค์กร:** การสร้าง การลบ การกู้คืน การกำหนดเวลาและยกเลิกการลบ และการลบข้อมูลเสร็จสมบูรณ์
- **การอัปโหลด ดาวน์โหลด และส่งออกข้อมูล:** การอัปโหลด ดาวน์โหลด และลบ artifact การอัปโหลดและปรับปรุงข้อมูลแบบตาราง การดาวน์โหลดข้อมูลส่งออก การลบตารางข้อมูล และการสร้าง เปลี่ยนแปลง และลบ webhook (connection)
- **สถานะการเรียกเก็บเงิน:** การเปลี่ยนแผน การระงับและกู้คืนบริการเนื่องจากการชำระเงิน และการยกเลิกการสมัครใช้บริการ
- **คอนโซลผู้ให้บริการของ ProcessMind:** การเรียกใช้คำสั่งค้นหาที่มีสิทธิพิเศษ การดูแลผู้ใช้และองค์กร การเปลี่ยนแปลงการตั้งค่าและฟีเจอร์ คำขอซิงโครไนซ์การเรียกเก็บเงิน และการย้ายข้อมูล
- **การดำเนินการด้านการดูแลระบบและการทำลายข้อมูลโดยงานตามกำหนดเวลาของ ProcessMind:** การลบ tenant องค์กร ผู้ใช้ และ lead การกวาดล้างตามระยะเวลาเก็บรักษา และความล้มเหลวของ pipeline
- **ความถูกต้องสมบูรณ์ของบันทึกการตรวจสอบ:** ความล้มเหลวของกระบวนการเขียนบันทึกการตรวจสอบเอง

3.2 การแก้ไขในเวิร์กสเปซ การแก้ไขภายในเวิร์กสเปซ (แบบจำลองกระบวนการ เอกสาร การจำลอง แดชบอร์ด ความคิดเห็น และบุ๊กมาร์ก) จะบันทึกไว้ในประวัติการเปลี่ยนแปลงกระบวนการของผลิตภัณฑ์ ไม่ใช่ในบันทึกการตรวจสอบ บันทึกการตรวจสอบระบุว่าใครอัปโหลด ดาวน์โหลด ส่งออก หรือลบข้อมูล ส่วนประวัติการเปลี่ยนแปลงระบุว่ามีการเปลี่ยนแปลงอะไรภายในแบบจำลอง คุณสามารถขอรายการรหัสการดำเนินการที่บันทึกในปัจจุบันจาก ProcessMind ได้

---

4. สิ่งที่ไม่มีการบันทึกไม่ว่าในกรณีใด

ไม่มีการเขียนรหัสผ่าน โทเค็นการยืนยันตัวตน ค่า API key คุกกี้ ส่วนหัวการอนุญาต เนื้อหาคำขอหรือคำตอบ เนื้อหาไฟล์ URL ที่ลงนามล่วงหน้า และพรอมป์ต์หรือผลลัพธ์จาก AI ลงในบันทึกการตรวจสอบ บันทึกการตรวจสอบอาจมีข้อมูลส่วนบุคคลที่จำเป็นต่อการระบุผู้ดำเนินการ ได้แก่ ที่อยู่อีเมลของผู้ดำเนินการ และที่อยู่ IP ต้นทางกับ user agent สำหรับการดำเนินการที่รายการในทะเบียนกำหนดให้บันทึก (การลงชื่อเข้าใช้ การตัดสินใจเกี่ยวกับการเข้าถึง การเปลี่ยนแปลงด้านการดูแลระบบและการตั้งค่า การเคลื่อนย้ายข้อมูล การเปลี่ยนแปลง API key และนโยบาย AI) ฟิลด์ที่อนุญาตกำหนดไว้สำหรับการดำเนินการแต่ละรายการ และมีการตรวจทานเมื่อเพิ่มการดำเนินการ

---

5. ความถูกต้องสมบูรณ์

5.1 เพิ่มรายการได้เท่านั้น บันทึกการตรวจสอบอนุญาตให้เพิ่มรายการได้เท่านั้น ไม่มีบทบาทของแอปพลิเคชันใดมีสิทธิ์แก้ไขหรือลบข้อมูลในบันทึก และข้อจำกัดของฐานข้อมูลปฏิเสธการดำเนินการทั้งสองอย่าง

5.2 ผู้เขียนรายการเพียงรายเดียว รายการเขียนโดยองค์ประกอบเดียว ซึ่งตรวจสอบความถูกต้องของรหัสการดำเนินการและเพย์โหลดก่อนเขียน รายการที่ไม่ผ่านการตรวจสอบจะถูกปฏิเสธและรายงาน แทนที่จะเขียนเพียงบางส่วน

5.3 การจัดการความล้มเหลว ความล้มเหลวในการเขียนบันทึกการตรวจสอบจะไม่ทำให้การดำเนินการทางธุรกิจที่บันทึกไว้นั้นล้มเหลว โดยจะบันทึกความล้มเหลวผ่านช่องทางการปฏิบัติการที่มีการแจ้งเตือน และเก็บสำเนารองของรายการนั้นไว้เพื่อให้สามารถกู้คืนได้

---

6. ระยะเวลาเก็บรักษาและสถานที่จัดเก็บ

6.1 ระยะเวลาเก็บรักษา บันทึกการตรวจสอบจะเก็บรักษาไว้อย่างน้อยสิบ (10) ปีนับจากวันที่เกิดเหตุการณ์

6.2 สถานที่จัดเก็บและการเข้ารหัส บันทึกการตรวจสอบจัดเก็บไว้ในสหภาพยุโรป (แฟรงก์เฟิร์ต ประเทศเยอรมนี `eu-central-1`) และเข้ารหัสขณะจัดเก็บโดยใช้ AWS KMS key ที่ลูกค้าจัดการ นอกจากนี้ ยังมีการเขียนสำเนาปัจจุบันไปยังกลุ่มบันทึก Amazon CloudWatch ที่ควบคุมการเข้าถึง เพื่อให้สามารถตรวจสอบเหตุการณ์ได้ในขณะที่กำลังเกิดขึ้น

6.3 ไม่มีการจำลองข้อมูลข้ามภูมิภาค ไม่มีการจำลองบันทึกการตรวจสอบไปนอกสหภาพยุโรป

---

7. การเข้าถึงบันทึกการตรวจสอบ

7.1 สิทธิ์ในการเข้าถึง บันทึกการตรวจสอบภายในแอปรวมอยู่ในแผน Process Architecture และแผนที่สูงกว่า ผู้ดูแลองค์กรอ่านข้อมูลได้ทั้งองค์กร ส่วนผู้ดูแลที่จำกัดขอบเขตไว้ที่ tenant อ่านข้อมูลได้เฉพาะ tenant ของตน ขอบเขตดังกล่าวกำหนดจากเซสชันที่ผ่านการยืนยันตัวตนและตรวจสอบก่อนดำเนินการค้นหา ดังนั้นคำขอจึงไม่สามารถขยายขอบเขตไปยัง tenant หรือองค์กรอื่นได้

7.2 บุคลากรของ ProcessMind บุคลากรของ ProcessMind เข้าถึงบันทึกการตรวจสอบเฉพาะเพื่อการสนับสนุน การตอบสนองต่อเหตุการณ์ หรือการปฏิบัติตามข้อผูกพันทางกฎหมาย โดยยึดหลักการเข้าถึงเท่าที่จำเป็น การเข้าถึงข้ามลูกค้าจำกัดไว้เฉพาะบทบาทสนับสนุนที่กำหนดไว้โดยเฉพาะ และการเข้าถึงดังกล่าวถือเป็นการดำเนินการด้านการดูแลระบบที่มีการบันทึกไว้ด้วย

7.3 วิธีขอรับบันทึก ผู้ดูแลองค์กรและ tenant สามารถอ่านบันทึกการตรวจสอบของตนได้ในบันทึกการตรวจสอบภายในแอป และดึงหรือส่งออกผ่าน external API สำหรับคำขอขนาดใหญ่หรือคำขอที่ต้องการความช่วยเหลือ ฝ่ายสนับสนุนของ ProcessMind จะจัดส่งบันทึกในรูปแบบ CSV หรือ JSON สำหรับองค์กร tenant และช่วงเวลาที่ระบุ โดยตั้งเป้าดำเนินการคำขอมาตรฐานภายในห้า (5) วันทำการ

---

8. การลบบันทึกการตรวจสอบ

8.1 เมื่อมีคำขอ เมื่อได้รับคำขอเป็นลายลักษณ์อักษรที่ผ่านการตรวจสอบแล้ว ProcessMind จะลบบันทึกการตรวจสอบที่เป็นขององค์กรลูกค้าออกจากที่เก็บบันทึกการตรวจสอบ และยืนยันการ

ลบเป็นลายลักษณ์อักษร ไม่สามารถแก้ไขสำเนา CloudWatch สำหรับการปฏิบัติการทีละรายการได้ โดยสำเนาดังกล่าวจะหมดอายุตามระยะเวลาเก็บรักษาของตนเอง

8.2 ข้อมูลที่เก็บรักษาไว้ บันทึกที่ระบุว่ามีการลบข้อมูลแล้ว (ตัวระบุองค์กร วันที่ ผู้ร้องขอ เหตุผล และจำนวนรายการที่ลบ) จะเก็บรักษาไว้เป็นบันทึกการตรวจสอบระดับแพลตฟอร์ม และไม่มีข้อมูลลูกค้า คำขอให้ลบข้อมูลของลูกค้าจะไม่มีผลต่อรายการที่ไม่เกี่ยวข้องกับลูกค้ารายใด (เหตุการณ์ของแพลตฟอร์ม ProcessMind)

8.3 คำขอลบข้อมูลส่วนบุคคล ในกรณีที่คำขอเกี่ยวข้องกับบุคคลภายในองค์กรลูกค้าที่ยังคงใช้งานอยู่ จะเก็บรักษาบันทึกด้านความปลอดภัยไว้เพื่อการก่อตั้ง การใช้ หรือการต่อสู้สิทธิเรียกร้องทางกฎหมาย ตามที่มาตรา 17(3)(b) และ (e) ของ GDPR อนุญาต โดยบันทึกฐานดังกล่าวไว้ในบันทึกกิจกรรมการประมวลผลและใน[นโยบายความเป็นส่วนตัว]

---

9. การผสานรวมและส่งออก SIEM

9.1 ความพร้อมให้บริการ คลังบันทึกการตรวจสอบที่แก้ไขไม่ได้เป็นตัวเลือกสำหรับ Enterprise ซึ่งเปิดใช้งานให้แก่องค์กรลูกค้าเมื่อมีคำขอ โดยจะเขียนออบเจ็กต์ NDJSON ที่บีบอัดรายวันไว้ภายใต้ prefix เฉพาะของแต่ละองค์กรในบักเก็ต S3 ที่ล็อกออบเจ็กต์ (WORM) พร้อม manifest และการกระทบยอดทุกคืน

9.2 วิธีส่งข้อมูลในปัจจุบัน ปัจจุบัน ProcessMind ไม่มีตัวเชื่อมต่อ SIEM แบบเนทีฟหรือฟีดแบบ push การส่งข้อมูลเป็นแบบดึงข้อมูลจากสามช่องทาง ได้แก่ read API (`GET /v1/tenant/{tenantId}/audit`) งานส่งออกที่มีขอบเขตจำกัด (สร้างงานด้วย `POST /v1/tenant/{tenantId}/audit/exports` และรับผลลัพธ์จากการเรียกสถานะ ซึ่งส่งคืน URL ดาวน์โหลดที่ใช้ได้ในช่วงเวลาสั้น ๆ) และในกรณีที่ใช้คลังข้อมูล Enterprise จะเป็นออบเจ็กต์รายวันภายใต้ prefix ขององค์กรนั้นในบักเก็ตที่ล็อกออบเจ็กต์ ซึ่ง SIEM ของลูกค้าจะอ่านผ่านการจัดเตรียมสิทธิ์เข้าถึง ProcessMind ไม่ได้ส่งบันทึกไปยังสถานที่ที่ลูกค้าเลือกตามกำหนดเวลาของ ProcessMind เอง

9.3 การตรวจติดตามของ ProcessMind เอง การตรวจติดตามความปลอดภัยของ ProcessMind ใช้บันทึกชุดเดียวกัน ได้แก่ ความล้มเหลวในการเขียนบันทึกการตรวจสอบ การเพิ่มขึ้นอย่างรวดเร็วของความล้มเหลวในการยืนยันตัวตน การเปลี่ยนแปลงสิทธิพิเศษ และการดำเนินการด้านการดูแลระบบที่ทำลายข้อมูล ซึ่งจะทำให้เกิดการแจ้งเตือนภายใน

---

10. หลักฐานที่ลูกค้าสามารถขอได้

เมื่อมีคำขอ และอยู่ภายใต้ข้อกำหนดการรักษาความลับในกรณีที่เกี่ยวข้อง ProcessMind จะจัดเตรียมคำชี้แจงนี้ มาตรการรักษาความปลอดภัย ภาคผนวกการประมวลผลข้อมูล รายการผู้ประมวลผลช่วง ตัวอย่างบันทึกการตรวจสอบที่ปกปิดข้อมูลแล้ว และขั้นตอนที่ใช้สำหรับคำขอเข้าถึงและลบข้อมูล

---

11. ข้อจำกัด

เพื่อป้องกันข้อสงสัย ProcessMind ยืนยันว่ามีที่เก็บบันทึกการตรวจสอบแบบเพิ่มรายการได้เท่านั้นสำหรับทุกองค์กร และในกรณีที่เปิดใช้สิทธิ์เข้าถึงคลังบันทึกการตรวจสอบ จะมีสำเนาที่ล็อกออบเจ็กต์ (WORM) พร้อมการกระทบยอด manifest ทุกคืน ปัจจุบัน ProcessMind ไม่ได้ยืนยันว่ามี hash chain ตัวเชื่อมต่อ SIEM แบบ push ตามเวลาจริงที่เป็นเนทีฟ การปกปิดข้อมูลในบันทึกการตรวจสอบแยกตามผู้ใช้ การรับรอง ISO 27001 หรือ SOC 2 ที่ครอบคลุมการควบคุมนี้ หรือการครอบคลุมการอ่านข้อมูลลูกค้าทุกครั้ง ลูกค้าสามารถอ่านและส่งออกข้อมูลด้วยตนเองผ่านบันทึกการตรวจสอบภายในแอปและ external API