JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة خصوصية بيانات الأجهزة المتصلة

4 – 8 أبريل 2027

عمّان

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة خصوصية بيانات الأجهزة المتصلة

المرجع: 3109_118008 **التاريخ:** 4 – 8 أبريل 2027 **المكان:** عمان **الرسوم:** GBP 4200

دورة خصوصية بيانات الأجهزة المتصلة دورة تدريبية مدتها أسبوع لمختصي الخصوصية ومالكي المنتجات وفرق أمن المعلومات الذين يحددون ما تجمعه الساعات الذكية وأجهزة المنازل الذكية والتطبيقات المرافقة من معلومات شخصية، ويعد كل مشارك فيها مراجعة خصوصية الأجهزة المتصلة لمنتج أو خدمة واحدة. فالمستشعرات تلتقط الموقع والصوت والسلوك دون توقف، وكل قرار تصميم يحمل اليوم أثرا قانونيا وأثرا على السمعة. وتضع جوبيتر برايم للتدريب خصوصية بيانات الأجهزة المتصلة في قلب قرارات المنتج.

لماذا تهم خصوصية بيانات الأجهزة المتصلة الآن

تتشكل خصوصية بيانات الأجهزة المتصلة اليوم بثلاث قوى. فالأجهزة تلتقط إشارات أدق، وكثيرا ما تعمل دون شاشة تشرح للمستخدم ما يجري. وتعتمد فرق المنتجات على منصات سحابية وموردي رقائق وشركاء تحليلات، فتنتقل المعلومات الشخصية بين أطراف عديدة قبل أن يقرأ أحد إشعارا. كما يسأل العملاء والجهات الرقابية بإلحاح متزايد عن معاملة الإعدادات الافتراضية وتحديثات البرامج الثابتة لمعلوماتهم. والمؤسسة التي تحسن التعامل مع ذلك تطلق منتجات يثق بها الناس وتخفض كلفة الحوادث، أما التي تسيء التعامل معه فتواجه سحب ميزات وخسارة شراكات وتحقيقات طويلة بموجب أنظمة حماية البيانات المعمول بها.

المستفيدون من خصوصية بيانات الأجهزة المتصلة

- مختصو الخصوصية الذين يقيمون ميزات الأجهزة الجديدة ويوجهون الجمع المشروع للمعلومات والإشعار بها
- مالكو المنتجات الذين يقررون المستشعرات وبيانات القياس عن بعد وأذونات التطبيق في كل إصدار
- فرق أمن المعلومات التي تحمي البرامج الثابتة للأجهزة وعمليات الاقتران والروابط السحابية
- فرق الموردين والشراكات التي تفاوض على حدود إعادة استخدام الموردين والمنصات لمعلومات الأجهزة
- فرق الاستجابة للحوادث التي تحقق في تسرب بيانات القياس أو سجلات الحسابات وتحتويه

ويستفيد فريق المنتج متعدد التخصصات أكثر من غيره حين يحضر أعضاؤه من الخصوصية والهندسة والأمن معا.

قدرات خصوصية بيانات الأجهزة المتصلة

يتتبع المشاركون ما يسجله كل مستشعر ويحددون ما لا ينبغي للجهاز الاحتفاظ به أبدا.

- رسم تدفقات المعلومات الشخصية من المستشعر إلى التطبيق إلى السحابة — اعتماد الإصدار لدى مالكي المنتجات
- تصميم الموافقة والإشعار للأجهزة بلا شاشة والأجهزة المشتركة — ثقة العملاء ومعالجة الشكاوى
- تحديد قواعد تقليل البيانات والاحتفاظ ببيانات القياس — قائمة الأعمال الهندسية وكلفة التخزين
- تقييم شروط المشاركة مع الموردين والمنصات — التفاوض على العقود مع الشركاء
- اختبار سيناريوهات الاختراق لمعلومات الأجهزة والحسابات — جاهزية فرق الأمن للحوادث
- إيصال مخاطر الخصوصية المتبقية إلى الرعاة — قرارات الإطلاق أو التأجيل

مصطلحات خصوصية بيانات الأجهزة المتصلة الأساسية

- القياس عن بعد — معلومات الاستخدام والحالة التي يرسلها الجهاز تلقائيا إلى الشركة المصنعة، وغالبا ما تتضمن معرفات مرتبطة بشخص.
- تقليل البيانات — جمع المعلومات الشخصية التي يحتاجها غرض محدد فقط والاحتفاظ بها وحدها.
- التطبيق المرافق — تطبيق الهاتف الذي يقترن بالجهاز ويحفظ حسابه وإعدادات الخصوصية فيه.
- إشعار الخصوصية — بيان واضح يخبر الناس بما يجمعه المنتج ولماذا ومع من يشاركه وإلى متى.
- معالج البيانات — طرف خارجي يتعامل مع المعلومات الشخصية نيابة عن المؤسسة ووفق تعليماتها الموثقة.
- الترميز المستعار — استبدال المعرفات المباشرة برموز بحيث لا تربط المعلومات بشخص دون تفاصيل محفوظة بشكل منفصل.

خصوصية بيانات الأجهزة المتصلة يوما بيوم

اليوم 1: الأجهزة والمستشعرات والمعلومات الشخصية

- جرد المستشعرات — ما يمكن لكل مكون أن يكشفه عن الأشخاص
- فئات المعلومات الشخصية — الإشارات التي تعد حساسة
- خريطة دورة حياة الجهاز — نقاط الخصوصية من الإعداد حتى التخلص منه
- مصفوفة توقعات أصحاب المصلحة — العملاء والشركاء والجهات الرقابية
- خيارات الأساس النظامي — مطابقة كل غرض للجهاز مع مسوغ معالجته

اليوم 2: تتبع التدفقات عبر التطبيقات والسحابة

- مخطط تدفق البيانات — محطات المستشعر والتطبيق والبوابة والسحابة
- تدقيق حقول القياس عن بعد — فصل احتياجات التشخيص عن التنميط
- مراجعة ربط المعرفات — مفاتيح الأجهزة والحسابات ورموز الإعلانات
- فحص النقل عبر الحدود — أماكن تخزين السجلات في المناطق السحابية
- قيد سجل مخاطر الخصوصية — تقدير الاحتمال والضرر لكل تدفق

اليوم 3: الموافقة والشفافية والإعدادات الافتراضية

- أنماط الإشعار بلا شاشة — الأضواء والتنبيهات الصوتية وبطاقات التطبيق
- تصميم الموافقة متعددة الطبقات — خيارات دقيقة للميزات الاختيارية
- الأجهزة المنزلية المشتركة — الضيوف والأطفال والمستخدمون الثانويون
- الإعدادات الافتراضية الحامية للخصوصية — ما يشحن قبل أي اختيار للمستخدم
- معالجة طلبات الحقوق — الوصول والحذف ونقل البيانات عبر التطبيقات

اليوم 4: التقليل والاحتفاظ والموردون والاختراقات

- خيارات المعالجة داخل الجهاز — إبقاء الإشارات الخام بعيدا عن السحابة
- تصميم جدول الاحتفاظ — محفزات حذف بيانات القياس والسجلات التقنية
- استبيان العناية الواجبة للموردين — شركاء الرقائق والمنصات والتحليلات
- بنود اتفاقية المعالجة — حدود إعادة الاستخدام وحقوق التدقيق
- دليل التعامل مع اختراق الأجهزة — الاحتواء والإخطار وإصلاحات البرامج الثابتة

اليوم 5: ممارسة مراجعة خصوصية الأجهزة المتصلة

- استعراض خريطة التدفق — تطبيق مخططات اليوم 2 على منتج مختار
- نقد رحلة الموافقة — اختبار أنماط اليوم 3 مع الزملاء
- قائمة فجوات الاحتفاظ والموردين — تطبيق ضوابط اليوم 4
- إحاطة المخاطر المتبقية — عرض الموازنات على رعاة الإطلاق
- مراجعة خصوصية الأجهزة المتصلة — استكمال الوثيقة النهائية وعرضها

تطبيق خصوصية بيانات الأجهزة المتصلة بعد الدورة

- إجراء تدقيق لحقول القياس عن بعد في منتج قائم واقتراح حقول تحذف أو تختصر في إصدار البرامج الثابتة التالي.
- قيادة نقد لرحلة الموافقة مع زملاء التصميم والهندسة.

أسئلة حول خصوصية بيانات الأجهزة المتصلة

ما خصوصية بيانات الأجهزة المتصلة ولماذا تهم الآن؟

خصوصية بيانات الأجهزة المتصلة هي ضبط طريقة جمع المستشعرات والتطبيقات والخدمات السحابية للمعلومات الشخصية ومشاركتها. وتهم الآن لأن الأجهزة تسجل إشارات أكثر خصوصية، بينما يتوقع العملاء والشركاء والجهات الرقابية خيارات واضحة.

ما الأدوار الأكثر استفادة من تدريب خصوصية بيانات الأجهزة المتصلة؟

يستفيد مختصو الخصوصية ومالكو المنتجات وفرق أمن المعلومات أكثر من غيرهم. كما يستفيد زملاء الموردين والاستجابة للحوادث.

كيف تختلف خصوصية بيانات الأجهزة المتصلة عن دورة عامة في حماية البيانات؟

تركز خصوصية بيانات الأجهزة المتصلة على العتاد والبرامج الثابتة والتطبيقات المرافقة بدلا من السجلات المكتبية. فتعمل على الإشعار بلا شاشة وبيانات القياس والمشاركة المنزلية وسلاسل الموردين، وهي موضوعات تتناولها الدورة العامة في حماية البيانات باختصار.

ماذا تعود به من تدريب خصوصية بيانات الأجهزة المتصلة؟

تعود بمراجعة خصوصية لمنتج أو خدمة حقيقية واحدة. وتضم خريطة تدفق وخيارات الموافقة وقواعد الاحتفاظ وشروط الموردين وخطة للتعامل مع الاختراق.

خصوصية بيانات الأجهزة المتصلة: الطريق إلى الأمام

توجه مراجعة خصوصية الأجهزة المتصلة أولا قرار إطلاق الإصدار التالي بمستشعراته وإعداداته الافتراضية الحالية أو تعديلها. ويستخدمها مالكو المنتجات والمهندسون وقادة الأمن للاتفاق على بيانات القياس التي تبقى، والشركاء الذين يتلقونها، ومدة الاحتفاظ بها. وبعد الإطلاق الأول تستحق نظرة الأسرة المشتركة مراجعة جديدة، لأن العملاء يتشاركون الأجهزة بطرق لم تخطط لها جلسات التصميم.