



دورة أمن سلسلة توريد البرمجيات وحوكمة المصادر المفتوحة: قوائم مكونات البرمجيات SBOM ومخاطر الاعتماديات



دورة أمن سلسلة توريد البرمجيات وحوكمة المصادر المفتوحة: قوائم مكونات البرمجيات SBOM ومخاطر الاعتماديات

مقدمة:

دورة أمن سلسلة توريد البرمجيات وحوكمة المصادر المفتوحة تتناول قوائم مكونات البرمجيات SBOM ومخاطر الاعتماديات خلال 5 أيام، وتخطب العاملين في أمن التطبيقات وهندسة البناء والامثال للتراخيص ومشتريات التقنية، وتنتهي بخطة حوكمة سلسلة توريد البرمجيات لجهة حالة. فمعظم التطبيقات تبنى اليوم من حزم مفتوحة المصدر يطورها آخرون، ومع ذلك تعجز جهات كثيرة عن معرفة المكونات التي تشحنها، والتراخيص التي تحكمها، وهل تطالها ثغرة أعلن عنها للتو. ويعمل المشاركون في بناء البرمجيات أو تقييمها أو شرائها، ويتدربون في مختبرات تطبيقية على ملفات بيان حقيقية وقوائم مكونات وشهادات بناء. وتقدم كور كونسبت هذه الدورة في أمن سلسلة توريد البرمجيات.

أهداف الدورة:

- تصنيف تراخيص المصادر المفتوحة إلى متساهلة وحافطة للحقوق المتبادلة وتطبيق سياسة موافقة على الاعتماديات الجديدة
- تأسيس ميثاق مكتب برامج المصادر المفتوحة OSPO ومسار استقبال الطلبات وأدوار الحوكمة وفق ISO/IEC 5230 و ISO/IEC 18974g
- إنشاء قوائم مكونات البرمجيات SBOM والتحقق منها وتبادلها بصيغتي SPDX و CycloneDX للتطبيقات المطورة داخليا
- فرز نتائج تحليل مكونات البرمجيات وإصدار بيانات VEX توثق قابلية استغلال كل ثغرة في سياق كل منتج
- رفع سلامة البناء عبر إثبات مصدر البناء وفق SLSA والتوقيع بأدوات Sigstore والتحقق من المخرجات قبل النشر
- صياغة بنود تسليم قوائم المكونات والشهادات في عقود شراء البرمجيات وإعداد خطة حوكمة سلسلة توريد البرمجيات

الفئة المستهدفة:

- الموظفون المسؤولون عن اختبار أمن التطبيقات واستقبال الثغرات ومتابعة معالجتها
- الموظفون المسؤولون عن أنظمة البناء ومستودعات الحزم ومخرجات الإصدار
- الموظفون المسؤولون عن مراجعة تراخيص المصادر المفتوحة وإشعارات النسب والاعتماد القانوني
- الموظفون المسؤولون عن توريد البرمجيات واستبيانات الموردين والملاحق الفنية للعقود
- الموظفون المسؤولون عن الاستجابة الأمنية للمنتجات والإفصاح عن الثغرات للعملاء

محاورة الدورة:

اليوم 1: تهديدات سلسلة توريد البرمجيات وبيئة الاعتماديات مفتوحة المصدر

- مسارات الهجوم على سلسلة توريد البرمجيات من الشيفرة المصدرية إلى النشر
- مراجعة حالات خلط الاعتماديات وانتحال أسماء الحزم والحزم الخبيثة
- مخططات الاعتماديات غير المباشرة وكشف المكونات المخفية
- مؤشرات صحة المشاريع مفتوحة المصدر ومخاطر القائمين على صيانتها
- خط الأساس لنضج سلسلة التوريد في ممارسات المكونات الحالية

اليوم 2: تراخيص المصادر المفتوحة وحوكمة OSPO ومعايير البرامج

- عائلات التراخيص المتساهلة مقابل الحافظة للحقوق المتبادلة واشتراطات كل منها
- معرفات تراخيص SPDX وصياغة تعبيرات الترخيص المركبة
- متطلبات برنامج الامتثال للتراخيص وفق ISO/IEC 5230 خطوة بخطوة
- عناصر عملية ضمان أمن المصادر المفتوحة وفق ISO/IEC 18974
- تصميم ميثاق OSPO ومسار استقبال الطلبات وأدوار الموافقة

اليوم 3: إنشاء قوائم مكونات البرمجيات SBOM وتبادلها وتحليل المكونات

- الحقول الدنيا لقائمة SBOM ومعرفات المكونات مثل PURL
- مختبر إنتاج قوائم CycloneDX وSPDX من ملفات بيان البناء
- تقييم جودة قوائم المكونات والتحقق منها وفحوص تحويل الصيغ
- تحليل مكونات البرمجيات ومطابقتها مع الشغرات المعروفة
- توليد إشعارات النسب وتقارير التراخيص من بيانات SBOM

اليوم 4: قابلية استغلال الشغرات ومصدر البناء ومتطلبات الموردين

- قيم حالة VEX ومبرراتها في سياق المنتج
- سياسة تحديث الاعتماديات وثبيت الإصدارات وقواعد مراجعة ملفات القفل
- مستويات مسار البناء في SLSA ومحتوى شهادة مصدر البناء
- التوقيع دون مفاتيح دائمة في Sigstore وسجل الشفافية وخطوات التحقق
- بنود تسليم قوائم المكونات والشهادات في عقود البرمجيات

اليوم 5: مختبر إعداد خطة حوكمة سلسلة توريد البرمجيات

- موجز الجهة الحالية ومحفظة تطبيقاتها وتنوع مورديها
- مختبر حصر الاعتماديات وفرز التراخيص لتطبيق الحالة
- مختبر صياغة بيانات VEX لنتائج الثغرات في الحالة
- مستويات المصدر والتوقيع المستهدفة لأنظمة البناء في الحالة
- استكمال خطة حوكمة سلسلة توريد البرمجيات ومناقشتها مع النظراء

المهارات التي ستكتسبها:

- تصنيف تراخيص المصادر المفتوحة
- تصميم سياسات OSPO
- إعداد قوائم SBOM والتحقق منها
- فرز ثغرات المكونات
- كتابة بيانات VEX
- تقييم مصدر البناء
- التحقق من توقيع المخرجات
- صياغة بنود توريد البرمجيات

لماذا تحضر هذه الدورة:

- تسليم مسؤول الأمن والمستشار القانوني خطة حوكمة سلسلة توريد البرمجيات تحدد سياسة التراخيص وقواعد SBOM وممارسة VEX وأهداف سلامة البناء
- الحكم على قبول حزمة مفتوحة المصدر أو منتج مشتري في بيئة الإنتاج بقراءة قائمة مكوناته وترخيصه وأدلة مصدر بنائه
- تجنب نزاعات التراخيص والتحديات الفاتئة وعمليات البحث الطارئة في التطبيقات عند الإعلان عن ثغرة في مكتبة واسعة الانتشار
- توجيه المطورين ومهندسي البناء والمشتريين إلى مسار الاستقبال الموحد ونماذج قوائم المكونات وبنود العقود التي أعدت في المختبرات

الخاتمة:

بعد العودة إلى العمل يسلم المشاركون مسؤول الأمن والمستشار القانوني ومدير المشتريات خطة حوكمة سلسلة توريد البرمجيات للجهة الحالة. وتعتمد فرق الأمن عليها في ضبط ممارسة SBOM و VEX، ويستخدم مهندسو البناء أهداف المصدر والتوقيع فيها، يطبق المشترون بنود الموردين في صفقة البرمجيات التالية. وبعد أول إفصاح كبير عن ثغرة في اعتمادية أو أول عقد مورد يعالج وفق الخطة، تراجع الوحدة سرعة تحديد المنتجات المتأثرة وأسئلة التراخيص التي ظهرت ومدى تسليم الموردين قوائم مكونات صالحة للاستخدام.

الأسئلة الشائعة:

ما الذي يحتاجه المشاركون قبل دورة أمن سلسلة توريد البرمجيات؟

يحتاج المشاركون إلى خبرة عملية في بناء البرمجيات أو اختبارها أو تقييمها أو شرائها، وفهم لطريقة استخدام التطبيقات للحزم الخارجية. ويفيد الإلمام بسطر الأوامر في المختبرات. ولا تشترط الدورة خلفية قانونية، إذ تعرض التراخيص من زاوية الاشتراطات العملية.

بم تختلف دورة أمن سلسلة توريد البرمجيات عن دورات البرمجة الآمنة أو إدارة أصول البرمجيات؟

تحكم هذه الدورة المكونات التي لم يكتبها الفريق: تراخيص المصادر المفتوحة وقوائم SBOM وثغرات الاعتماديات وبيانات VEX ومصدر البناء. أما دورات البرمجة الآمنة فتعالج عيوب الشيفرة الداخلية، وتطابق دورات إدارة أصول البرمجيات حقوق التراخيص التجارية مع عمليات التثبيت.

لماذا تهتم قوائم SBOM في أمن سلسلة توريد البرمجيات وحوكمة المصادر المفتوحة؟

تسرد قائمة SBOM كل مكون داخل المنتج، فتتمكن الجهة من تحديد البرمجيات المتأثرة خلال ساعات عند الإعلان عن ثغرة في مكتبة، ومراجعة اشتراطات التراخيص قبل الإصدار، ومطالبة الموردين بالأدلة نفسها في العقود.

ماذا يعود به المشاركون من دورة أمن سلسلة توريد البرمجيات؟

يعود المشاركون بخطة حوكمة سلسلة توريد البرمجيات لجهة حالة، ومسار استقبال طلبات OSPO، ونماذج SBOM و VEX، وسياسة تحديث الاعتماديات، وبنود نموذجية للموردين يمكن تكييفها لتطبيقات جهته.