

دورة إدارة بوابات API وواجهات برمجة التطبيقات: تصميم السياسات والأمن وتشغيل المنصة

28 يونيو – 2 يوليو 2027

جنييف





دورة إدارة بوابات API وواجهات برمجة التطبيقات: تصميم السياسات والأمن وتشغيل المنصة

المرجع: 290_20349 التاريخ: 28 يونيو - 2 يوليو 2027 المكان: جنيف الرسوم: GBP 5500

ملخص البرنامج

إدارة بوابات API وواجهات برمجة التطبيقات محور دورة تدريبية تمتد أسبوع بمسئول إداري لمعماري المؤسسات وقيادات المنصات والتكامل ورؤساء التسليم الرقمي، ويخرج منها كل مشارك بتصميم لبوابات API وإدارة الواجهات لمنظومة واجهات واحدة. فكثيرا ما تبني البوابات والسياسات فريقا بعد فريق دون ملكية واضحة. ويتدرج البرنامج من الأدوار ومواضع التركيب، مروراً بتشخيص المخاطر وحركة الطلبات، إلى تصميم السياسات والتشغيل، ثم إلى تصميم عملي. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في إدارة بوابات API وواجهات برمجة التطبيقات.

المبررات المؤسسية

حين تنشر فرق كثيرة واجهات دون سياسات مشتركة، تظهر الثغرات الأمنية وانقطاعات الخدمة الناجمة عن الحركة غير المضبوطة والجهد المكرر في وقت متأخر وبكلفة أعلى للتصحيح. أما القيادات التي تحدد موضع البوابة ومالك كل واجهة والسياسات المطبقة، فتتخلف التعرض وتحمي الخدمات المشتركة.

- التعرض الأمني للواجهات: يقل حين تطبق مراجعة المخاطر وسياسات موحدة للمصادقة والتحقق على كل واجهة.
- توافر الخدمة: يتحسن حين تحمي حدود الطلبات والحصص وفحوص السعة الخدمات الخلفية المشتركة.
- زمن التسليم: يقصر حين تحل المعايير المنشورة والفهرس وبوابة المطورين محل أعمال الإعداد المتكررة.

المبادئ والأساس المعرفي

- OWASP API Security Top 10 قائمة مخاطر أمن الواجهات: تنظم مخاطرها مراجعة التهديدات في الجلسة 2 ومجموعة السياسات في الجلسة 3.
- Little's Law قانون ليتل في الطوابير: تقوم عليه علاقة التزامن ومعدل الوصول وزمن الاستجابة في عمل السعة وحدود الطلبات في الجلستين 2 و3.
- Conway's Law قانون كونواي: يوجه ربطه بين هيكل المؤسسة وتصميم النظام ترتيبات الملكية والمراجعة في الجلسة 4.



المشاركون المستهدفون

- معماريو المؤسسات الذين يقررون كيف تعرض الواجهات وتؤمن وتعاد الاستفادة منها.
- قيادات المنصات التي تشغل خدمات البوابات والتكامل المشتركة لفرق كثيرة.
- قيادات التكامل التي تدير مستهلكي الواجهات من الشركاء والجهات الداخلية.
- رؤساء التسليم الرقمي الذين يرفعون معايير الواجهات عبر فرق المنتجات.

يخدم البرنامج المصارف وشركات الاتصالات والخدمات الحكومية وقطاع الخدمات اللوجستية.

مخرجات التعلم

1. سيكون المشاركون قادرين على التمييز بين دور البوابة ودور منصة الإدارة وتبرير خيار موضع التركيب.
2. سيكون المشاركون قادرين على تشخيص نقاط الضعف الأمنية في منظومة واجهات قياسا على قائمة مخاطر معتمدة.
3. سيكون المشاركون قادرين على تقييم أنماط الحركة وتحديد شرائح حدود الطلبات والحصص.
4. سيكون المشاركون قادرين على بناء سياسات المصادقة والتحقق وإدارة الإصدارات لمجموعة من الواجهات.
5. سيكون المشاركون قادرين على ترتيب أولويات مقاييس الرصد وأهداف مستوى الخدمة لتشغيل المنصة.
6. سيكون المشاركون قادرين على تبرير نموذج الملكية والحوكمة أمام راعي المنصة ومسؤول الأمن.

هيكل البرنامج

اليوم 1: أدوار إدارة بوابات API وواجهات برمجة التطبيقات ومواضع التركيب

ما الذي تؤديه البوابة، وما الذي تضيفه منصة الإدارة، وأين يوضع كل منهما؟

- جرد منظومة الواجهات وخريطة المستهلكين
- مصفوفة أدوار البوابة ومنصة الإدارة
- مقارنة خيارات موضع تركيب البوابة
- مخطط أولي لنموذج الملكية والتمويل
- مراجعة حالتين لمنصات من قطاعين

اليوم 2: تشخيص المخاطر وحركة الطلبات

أين تتعرض المنظومة للخطر، وكم حركة يجب أن تتحمل؟



- استعراض مخاطر OWASP API Security Top 10
- ورقة عمل نمذجة تهديدات الواجهات
- مراجعة فجوات مصادقة المستهلكين
- ملف الحركة وتقدير ذروة الحمل
- فحص السعة وفق Little's Law

اليوم 3: تصميم السياسات

أي السياسات يجب أن تحملها كل واجهة، وأيها يختلف باختلاف المستهلك؟

- مجموعة أنماط المصادقة والتفويض
- شرائح حدود الطلبات والحصص
- قواعد التحقق من الطلبات ومعالجة الأخطاء
- سياسة الإصدارات وإنهاء الدعم
- خطة محتوى بوابة المطورين

اليوم 4: تشغيل المنصة وحوكمتها

كيف تدار المنصة وتقاس وتبقى تحت المراجعة؟

- ورقة أهداف مستوى الخدمة
- تصميم السجلات والمقاييس والتنبيهات
- مسار الإصدار وضبط التغيير
- خريطة ملكية الفرق وفق Conway's Law
- اختصاصات لجنة مراجعة فهرس الواجهات

اليوم 5: تطبيق إدارة بوابات API وواجهات برمجة التطبيقات على منظومة واجهات واحدة

هل التصميم جاهز ليقره راعي المنصة ومسؤول الأمن؟

- تطبيق مصفوفة الأدوار من الجلسة 1 على المنظومة المختارة
- اختبار نتائج المخاطر من الجلسة 2 على واجهات نموذجية
- فحص سياسات الجلسة 3 مقابل احتياجات المستهلكين
- تطبيق خريطة الملكية من الجلسة 4 على القضايا المفتوحة
- إنجاز تصميم بوابات API وإدارة الواجهات



المنهجية

يقوم البرنامج على تمارين منظمة تعتمد منظومة واجهات مجهولة المصدر. يرسم المشاركون الواجهات ويراجعون المخاطر ويحددون شرائح الحركة ويصوغون السياسات في فرق صغيرة، ثم يدافعون عن تصميمهم أمام لجنة معمارية محاكاة. ولا يتطلب البرنامج أي برمجة.

- نشاط مقترح: تقييم عشر واجهات نموذجية قياسا على قائمة OWASP وترتيب الإصدارات.
- نشاط مقترح: تحديد شرائح الحصص لثلاث فئات من المستهلكين استنادا إلى ملف الحركة.
- نشاط مقترح: صياغة سياسة إشعار إنهاء الدعم لواجهة موجهة للشركاء.

المخرج الختامي

يعد كل مشارك تصميمًا لبوابات API وإدارة الواجهات لمنظومة واحدة. ويتضمن قرارا بالأدوار والموضع، وسجلا للمخاطر، ومجموعة سياسات بشرائح حدود الطلبات، وورقة أهداف مستوى الخدمة، وخريطة للملكية، وعملية لمراجعة الفهرس. ويستخدم لإحاطة الراعي ومسؤول الأمن وللتخطيط للمرحلة الأولى من التسليم.

الأسئلة الشائعة

هل يناسب إدارة بوابات API وواجهات برمجة التطبيقات المعماريين الذين لا يملكون خبرة عملية بالأدوات؟

نعم، فهو بمستوى إداري، ويفترض مسؤولية عن قرارات الواجهات أو المنصات، لا خبرة بمنتج بوابة بعينه أو بالبرمجة.

ما النماذج التي يقوم عليها إدارة بوابات API وواجهات برمجة التطبيقات؟

يقوم إدارة بوابات API وواجهات برمجة التطبيقات على 10 OWASP API Security Top للمخاطر، Little's Law للسعة، و Conway's لتصميم الملكية.

كيف يستخدم التصميم الناتج عن إدارة بوابات API وواجهات برمجة التطبيقات في العمل؟

يستخدم التصميم الناتج عن إدارة بوابات API وواجهات برمجة التطبيقات لإحاطة الراعي، ووضع سياسات مشتركة للواجهات، والتخطيط للمرحلة الأولى من تسليم المنصة.



بماذا يختلف إدارة بوابات API وواجهات برمجة التطبيقات عن دورة في أداة بعينها؟

يركز إدارة بوابات API وواجهات برمجة التطبيقات على الموضوع والسياسة والملكية والمقاييس التي تنطبق على أي منتج، بينما تركز دورة الأداة على إعداد منتج واحد.