

# دورة هندسة إدارة الهوية والوصول IAM: الدخول الموحد والربط الاتحادي وحوكمة الصلاحيات

2027 – 7 مايو

الدار البيضاء





## دورة هندسة إدارة الهوية والوصول IAM: الدخول الموحد والربط الاتحادي وحوكمة الصلاحيات

المرجع: 22261\_347 التاريخ: 3 - 7 مايو 2027 المكان: الدار البيضاء الرسوم: GBP 4000

### ملخص البرنامج

هندسة إدارة الهوية والوصول، بما فيها الدخول الموحد والربط الاتحادي والحوكمة، محور دورة تدريبية تمتد 5 أيام بمستوى إداري للمعماريين وقيادات الأمن ورؤساء المنصات الرقمية، ويخرج منها كل مشارك بحزمة بنية مستهدفة للهوية لمؤسسة واحدة. فمنظومات الهوية تتراكم مع الاستحواذات والمشاريع، فتتعدد مسارات الدخول وتبقى صلاحيات لا يراجعها أحد. ويتدرج البرنامج من مبادئ البروتوكولات وتشخيص المنظومة، مروراً بتصميم الدخول الموحد والربط الاتحادي، إلى حوكمة الوصول، ثم إلى حزمة بنية عملية. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في هندسة إدارة الهوية والوصول.

### المبررات المؤسسية

حين تبنى الهوية تطبيقاً تلو آخر، يحصل المستخدمون على صلاحيات تفوق حاجتهم، وتبقى حسابات المغادرين قائمة، ويستغرق جمع أدلة التدقيق أسابيع. أما القادة الذين يتفقون على تصميم دخول واحد وملكية واضحة ودورة حياة لكل حساب، فيخفضون التعرض ويجيبون عن أسئلة التأكيد بسرعة.

- التعرض للوصول غير المصرح به: ينخفض حين تكتشف الصلاحيات الخاملة واليتيمة والزائدة وتزال.
- جهد أدلة التدقيق: يقصر حين تترك مراجعات الوصول وموافقاته أثراً موحداً.
- احتكاك الدخول: يخف حين تشترك التطبيقات في تصميم دخول اتحادي واحد.

### المبادئ والأساس المعرفي

- OAuth 2.0 إطار تفويض الوصول: يستند إليه تفويض الصلاحيات الذي تراجع أنماطه في الجلستين 1 و3.
- OpenID Connect طبقة الهوية فوق OAuth 2.0: تشكل أنماط الدخول التي تصمم في الجلسة 3.
- SAML 2.0 معيار تبادل إقرارات الهوية: يوجه الربط الاتحادي مع الشركاء والتطبيقات القديمة في الجلسة 3.
- أقل قدر من الصلاحيات والتحكم بحسب الأدوار: يبينان تشخيص الصلاحيات في الجلسة 2 وقواعد الحوكمة في الجلسة 4.



## المشاركون المستهدفون

- المعماربيون المؤسسيون الذين يضعون التصميم المستهدف للهوية عبر التطبيقات والمنصات.
- قيادات الأمن التي تملك مخاطر الوصول والوصول ذا الامتياز وأدلة التدقيق.
- رؤساء المنصات الرقمية الذين يربطون تطبيقات العملاء والشركاء والموظفين.
- قيادات الحوكمة التي تدير مراجعات الوصول وعمليات الانضمام والانتقال والمغادرة.

يخدم البرنامج البنوك ومقدمي الرعاية الصحية والجهات العامة والمؤسسات القائمة على التقنية.

## مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم منظومة الهوية في ضوء أدوار OAuth 2.0 و OpenID Connect و SAML 2.0.
2. سيكون المشاركون قادرين على تشخيص الوصول اليتيم والزائد وذي الامتياز عبر التطبيقات.
3. سيكون المشاركون قادرين على بناء تصميم للدخول الموحد والربط الاتحادي للموظفين والعملاء والشركاء.
4. سيكون المشاركون قادرين على ترتيب قوة التوثيق وقواعد التحكم في الوصول بحسب المخاطر.
5. سيكون المشاركون قادرين على تصميم دورة حياة للانضمام والانتقال والمغادرة مع اعتماد الصلاحيات.
6. سيكون المشاركون قادرين على تبرير بنية مستهدفة وخارطة طريق للانتقال أمام جهة التصميم.

## هيكل البرنامج

### اليوم 1: مبادئ هندسة إدارة الهوية والوصول

ما القرارات التي يجب أن تحسمها هندسة إدارة الهوية والوصول، وأي بروتوكولات تحملها؟

- خريطة نطاقات الهوية وحدود الثقة
- مراجعة مسار التفويض في OAuth 2.0
- مراجعة نمط الدخول في OpenID Connect
- مراجعة تبادل الإقرارات في SAML 2.0
- الفصل بين هوية الموظفين والعملاء والشركاء

### اليوم 2: تشخيص منظومة الهوية ومخاطر الوصول

أين تحمل الحسابات والصلاحيات ومسارات الدخول مخاطر لا يملكها أحد؟



- جرد الحسابات والصلاحيات
- تقييم تعدد مزودي الهوية
- مراجعة الحسابات اليتيمة وذات الامتياز
- فحص قوة التوثيق ومستوى الثقة بالهوية
- تدقيق سجل طلبات الوصول وموافقاتها

### اليوم 3: تصميم الدخول الموحد والربط الاتحادي

كيف يربط المستخدمون والتطبيقات والشركاء بتصميم دخول واحد دون توسيع الثقة؟

- البنية المرجعية للدخول الموحد
- تصميم الثقة الاتحادية مع الشركاء
- مصفوفة سياسة التوثيق متعدد العوامل
- نموذج التحكم في الوصول بحسب الأدوار
- قواعد مدة الجلسات والرموز

### اليوم 4: حوكمة الوصول ودورة حياة الهوية

كيف يبقى الوصول صحيحا من الانضمام إلى المغادرة، ومن يثبت ذلك؟

- مسار الانضمام والانتقال والمغادرة
- تصميم حملة اعتماد الصلاحيات
- مجموعة قواعد الفصل بين المهام
- نمط الموافقة على الوصول ذي الامتياز
- حزمة أدلة تدقيق الهوية

### اليوم 5: تطبيق هندسة إدارة الهوية والوصول على مؤسسة واحدة

هل البنية المستهدفة جاهزة لتعتمدها جهة التصميم؟

- تطبيق الجرد من الجلسة 2 على المؤسسة المختارة
- اختبار تصميم الدخول من الجلسة 3 مقابل المخاطر
- ربط ضوابط دورة الحياة من الجلسة 4 بالأنظمة
- ترتيب خارطة طريق الانتقال
- إنجاز حزمة البنية المستهدفة للهوية



## المنهجية

يقوم البرنامج على تمارين منظمة تستند إلى منظومات هوية مجهولة المصدر من بيانات مصرفية وصحية، إذ يعمل المشاركون في فرق صغيرة، ويتتبعون مسارات الدخول، ويرتبون مخاطر الوصول، ويصوغون تصميمًا مستهدفًا كما يفعل مجلس المعمارية، دون كتابة أي شيفرة برمجية.

- نشاط مقترح: تتبع ثلاثة تطبيقات من الدخول إلى الصلاحية وحصر افتراضات الثقة فيها.
- نشاط مقترح: ترتيب مجموعة من الحسابات اليتيمة وذات الامتياز بحسب المخاطر.
- نشاط مقترح: صياغة مسار مغادرة يزيل الوصول من كل نظام.

## المخرج الختامي

يعد كل مشارك حزمة بنية مستهدفة للهوية لمؤسسة واحدة. وتضم ملخص جرد المنظومة، وتصميم الدخول الموحد والربط الاتحادي، وسياسة التوثيق، ونموذج دورة الحياة والاعتماد، وخارطة طريق مرحلية. وتستخدم الحزمة لإطلاع جهة التصميم وتخطيط الانتقال.

## الأسئلة الشائعة

### هل تناسب هندسة إدارة الهوية والوصول القادة الذين لا يكتبون شيفرة برمجية؟

نعم، فهندسة إدارة الهوية والوصول في هذا التدريب بمستوى إداري، وتفترض إلماما بمشهد التطبيقات لا بالبرمجة أو إدارة المنتجات.

### ما البروتوكولات التي تقوم عليها هندسة إدارة الهوية والوصول في هذا التدريب؟

تقوم هندسة إدارة الهوية والوصول على OAuth 2.0 و OpenID Connect و SAML 2.0 للدخول والربط الاتحادي، مع أقل قدر من الصلاحيات والتحكم بحسب الأدوار للحكومة.

### كيف تستخدم حزمة البنية الناتجة عن هندسة إدارة الهوية والوصول في العمل؟

تستخدم الحزمة الناتجة عن هندسة إدارة الهوية والوصول لإطلاع جهة التصميم وتوجيه فرق المنصات وترتيب انتقال التطبيقات.

### بماذا تختلف هندسة إدارة الهوية والوصول عن برنامج في استراتيجية الأمن السيبراني؟

تركز هندسة إدارة الهوية والوصول على كيفية توثيق المستخدمين والتطبيقات وما يحق لكل منهم الوصول إليه، بينما يركز برنامج استراتيجية الأمن السيبراني على سياسة التهديدات والضوابط في المؤسسة كلها.