

أنظمة تكنولوجيا المعلومات: إدارة الهوية والوصول

UK Training

**PARTNER**



## أنظمة تكنولوجيا المعلومات: إدارة الهوية والوصول

### مقدمة

هذه الدورة التدريبية تتضمن مناقشات جماعية ودراسات حالة وعمل نقابي. كما تتضمن تمارين عملية ولعب النرد التي تسمح لجميع المشاركين باستخدام المعرفة التي اكتسبوها لإظهار مهاراتهم في إدارة الهوية والوصول.

### أهداف الدورة

- توضيح إطار عمل هندسة إدارة الوصول والهوية ومناقشة مخاطر النهران المرتبطة بخيارات النشر المتنوعة الخاصة به.
- مناقش النيات المختلفة لإنشاء مصادقة قوية على سبيل المثال OTP ، المصادقة القائمة على الشهادة ، مصادقة الجهاز ، إلخ.
- شرح مبادئ البنية التحتية العامة الرئيسية وسلطات إصدار الشهادات ، وإثبات قيمتها في التخفيف من المخاطر الأمنية التي تواجه المجتمعات الحديثة.
- شرح آليات التحكم في الوصول الأكثر شهرة وأدوار معايير oauth و OATH و SAML و OpenID في مجال IAM وتطبيق مفاهيم SSO الموحدة.
- إظهار بناء IAM باستخدام أدوات صناعية مختارة ودراسات حالة عملية مثل جواز السفر الإلكتروني وبوابة الحدود ، والخدمات المصرفية عبر الهاتف المحمول ، ومخطط EMV ، وخدمات الحركة الإلكترونية.

### محاور الدورة

#### اليوم الأول: مقدمة ومبادئ أمن المعلومات

- نظرة عامة على إدارة الهوية والوصول IAM.
- سمات أمن المعلومات.
- السرية.
- التكامل.
- التوفر.
- عدم الاتصال.
- المسؤولية.
- القابلية للتدوين.
- التشفير المتماثل وغير المتماثل.
- التجزئة والتوقيع الرقمي.
- إدارة المفاتيح.

#### اليوم الثاني: البنية التحتية للمفتاح العام PKI

- الهندسة المعمارية: هيئة إصدار الشهادات والتسجيل.
- إدارة دورة الحياة.
- أنواع الشهادات وأنهاط الاستخدام.
- التشفير.
- توقيع إلكتروني.
- شهادة العميل.
- شهادة خادم SSL.
- شهادة تستند إلى السمة.
- دراسات الحالة مثل حماية البريد الإلكتروني والخدمات المصرفية عبر الهاتف المحمول وتوقيع المستندات.

PARTNER



### اليوم الثالث: تحديد الهوية والمصادقة

- نظرة عامة على التعريف والتحقق والمصادقة.
- آليات تحديد الهوية والتوثيق.
- كلمة السر لمرة واحدة.
- البصمات.
- التوقيع الإلكتروني.
- البطاقة ذكية.
- الرموز اللينة.
- جهاز محمول.
- المصادقة على أساس المخاطر.
- تصعيد المصادقة.
- تسجيل الدخول النحادي وتسجيل الدخول النحادي الموحد.
- SAML و BrowserID و OpenID و OATH.
- إطار معماري وأدوات صناعية.
- دور الحوسبة الموثوق به في ضمان الهوية.
- المخاطر الأمنية المرتبطة بالآليات التي تمت مناقشتها.

### اليوم الرابع: صلاحية التحكم صلاحية الدخول

- مبادئ الترخيص.
- مخططات التحكم في الوصول.
- بروتوكول OAuth.
- إدارة حقوق المؤسسات وإدارة الحقوق الرقمية.
- إدارة الحساب المميز.
- الحوكمة والامتثال.

### اليوم الخامس: إطار IAM وحالات الاستخدام

- إطار عمل IAM للهندسة المعمارية.
- نظام صدى IAM.
- السحابية والحوسبة IAM.
- حالات استخدام توضيحية.
- أمن الحدود.
- جواز السفر الإلكتروني.
- الهوية الوطنية.
- الخدمات المصرفية الإلكترونية.
- نظام الصحة الإلكترونية.

UK Training

**PARTNER**



## Blackbird Training Clients



UK Training  
**PARTNER**



## البرامج التدريبية

إدارة المشافي  
القطاع العام  
ورشات عمل خاصة  
النفط والغاز  
هندسة الاتصالات  
تكنولوجيا المعلومات  
الصحة والسلامة  
القانون وإدارة العقود  
الجهازك و السلامة  
الطيران والصلاح الجوية  
الإدارة العليا

## البرامج التقنية/البرامج الإدارية

المهارات الاحترافية  
الهالية والمحاسبة والهيرانية  
الإعلام والعلاقات العامة  
إدارة المشاريع  
الهوراد البشرية  
تدقيق الحسابات وضمان الجودة  
التسويق والمبيعات وخدمة العملاء  
السكرتارية وإدارة المكاتب  
سلسلة التوريد والخدمات اللوجستية  
الإدارة والقيادة  
الرشاقة والارتقاء



BLACKBIRD  
FOR TRAINING



International House 185 Tower Bridge  
Road London SE1 2UF United Kingdom



+44 7401 1773 35  
+44 7480 775526



Sales@blackbird-training.com



www.blackbird-training.com

UK Training

**PARTNER**

