



إدارة الهوية والوصول IAM: حوكمة الهويات والمصادقة وإدارة الصلاحيات المميزة



إدارة الهوية والوصول IAM: حوكمة الهويات والمصادقة وإدارة الصلاحيات المميزة

مقدمة:

لا تظهر إخفاقات إدارة الهوية والوصول IAM عادة في صورة حادث كبير، بل في حساب موظف غادر وبقي فعالاً، أو موظف انتقل واحتفظ بصلاحياته القديمة، أو كلمة مرور مشتركة لحساب مسؤول، أو مراجعة صلاحيات وقعت دون قراءة. وكل حالة منها توسع سطح الهجوم وتضعف أدلة التدقيق. تدرب هذه الدورة من كور كونسبت الممارسين على تشغيل إدارة الهوية والوصول بوصفها منظومة محكومة، من دورة حياة الهوية والاتحاد إلى قوة المصادقة وتصميم الأدوار واعتماد الصلاحيات وفصل المهام وإدارة الصلاحيات المميزة. ويبنى المشاركون تقييماً لضوابط الهوية والوصول وخارطة طريق لتحسينها في مؤسساتهم.

أهداف الدورة:

- رسم خريطة لمصادر الهوية والأدلة والتطبيقات ومسارات الوصول في المؤسسة ضمن بنية مرجعية لإدارة الهوية والوصول
- تشغيل إجراءات التعيين والانتقال والمغادرة مع ضوابط لمنح الحسابات وسحبها تترك أثراً قابلاً للتدقيق
- اختيار طرق المصادقة وخيارات المصادقة متعددة العوامل وبروتوكولات الاتحاد وفق مستويات ضمان المصادقة في NIST SP 800-63B
- تصميم نماذج وصول قائمة على الأدوار وعلى السمات مع قواعد فصل المهام ومصفوفة التراكيبات المتعارضة
- تنفيذ مراجعات الصلاحيات وحملات الاعتماد وضوابط الوصول المميزة، ومنها خزائن بيانات الاعتماد والرفع المؤقت للصلاحيات عند الحاجة وتسجيل الجلسات
- بناء تقييم لضوابط الهوية والوصول وخارطة طريق لتحسينها مع مؤشرات وأدلة تدقيق لبيئة المؤسسة

الفئة المستهدفة:

- العاملون المسؤولون عن إدارة حسابات المستخدمين وخدمات الأدلة ومسارات منح الحسابات
- العاملون المسؤولون عن تشغيل خدمات المصادقة والدخول الموحد والمصادقة متعددة العوامل
- العاملون المسؤولون عن مراجعة الصلاحيات وتنظيف الاستحقاقات وفحوص فصل المهام
- العاملون المسؤولون عن حسابات المسؤولين والخدمات والطوارئ وأدوات الوصول المميزة
- العاملون المسؤولون عن إعداد أدلة الهوية والوصول للتدقيق الداخلي والخارجي

محاوِر الدورة:

اليوم 1: أسس إدارة الهوية والوصول ودورة حياة الهوية وتقييم الوضع الحالي

- مكونات إدارة الهوية والوصول: التعريف والمصادقة والتفويض والمساءلة
- البنية المرجعية للهوية: المصادر الموثوقة والأدلة ومزود الهوية والتطبيقات المستهدفة
- رسم إجراءات التعيين والانتقال والمغادرة من سجل الموارد البشرية حتى حذف الحساب
- حصر أنواع الهويات: الموظفون والمتعاقدون وحسابات الخدمة وهويات الأجهزة
- نموذج تقييم نضج الوضع الحالي لإدارة الهوية وسجل الفجوات

اليوم 2: خدمات الأدلة والاتحاد ومعايير المصادقة

- خدمات الأدلة وتصميم مخطط LDAP للمجموعات والسمات والوحدات التنظيمية
- تأكيدات SAML لتبادل معلومات الهوية وإعداد الثقة بين مزود الهوية ومزود الخدمة
- مسارات التفويض في OAuth ورموز الهوية في OpenID Connect للدخول الموحد
- مستويات ضمان المصادقة AAL1 وAAL2 وAAL3 في NIST SP 800-63B
- خيارات المصادقة متعددة العوامل: كلمات المرور لمرة واحدة والإشعارات والمفاتيح التشفيرية والمصادقات المقاومة للتصيد

اليوم 3: نماذج الوصول ومنح الحسابات واعتماد الصلاحيات

- التحكم في الوصول القائم على الأدوار: استخراج الأدوار وهندستها والصلاحيات الأساسية عند التعيين
- سياسات التحكم في الوصول القائم على السمات باستخدام سمات المستخدم والموارد والسياق
- موصلات منح الحسابات الآلية ومسارات الطلب وسلاسل الموافقة
- تصميم حملات مراجعة الصلاحيات واعتمادها: النطاق والمراجعون وتتبع السحب
- بناء قواعد فصل المهام ومصفوفة التركيبات المتعارضة

اليوم 4: إدارة الصلاحيات المميزة والهوية في الثقة الصفيرية ومخاطر الهوية

- اكتشاف الحسابات المميزة: حسابات المسؤولين والخدمات والطوارئ والحسابات المشتركة
- خزائن بيانات الاعتماد المميزة وتدوير كلمات المرور وضوابط الاستعارة
- الرفع المؤقت للصلاحيات عند الحاجة وتطبيق أقل الصلاحيات وتسجيل الجلسات المميزة
- مبادئ الهوية في الثقة الصفيرية: التحقق المستمر وقرارات الوصول المبنية على السياق
- نظرة عامة على قدرات أدوات حوكمة الهوية وإدارتها ومعايير اختيارها

اليوم 5: دراسات حالة الهوية والمؤشرات وخارطة طريق الضوابط

- دراسة حالة: حسابات يتيمة وصلاحيات زائدة كشفها التدقيق في مؤسسة خدمات مالية
- دراسة حالة: إساءة استخدام بيانات اعتماد مميزة لدى فريق البنية التحتية في مقدم رعاية صحية
- المؤشرات الرئيسة للهوية: زمن سحب صلاحيات المغادرين ونسبة إكمال المراجعات وتغطية الحسابات المميزة
- ملف أدلة التدقيق: سجلات منح الحسابات وتوقيعات الاعتماد وسجلات الاستثناءات
- صياغة تقييم ضوابط الهوية والوصول وخارطة طريق التحسين ومناقشتها مع الزملاء

المهارات التي ستكتسبها:

- إدارة دورة حياة الهوية
- إعداد الدخول الموحد الاتحادي
- اختيار مستوى ضمان المصادقة
- هندسة الأدوار
- إدارة اعتماد الصلاحيات
- تحليل فصل المهام
- ضبط الحسابات المميزة
- إعداد أدلة تدقيق الهوية

لماذا تحضر هذه الدورة:

- العودة بتقييم لضوابط الهوية والوصول وخارطة طريق لتحسينها مبنية على أدلتك وتطبيقاتك وحساباتك المميزة
- سد فجوات حسابات المغادرين والمتنقلين والحسابات اليتيمة التي يكتشفها المدققون والمهاجمون أولاً
- تحويل مراجعات الصلاحيات من جداول موقعة إلى حملات تسحب الصلاحيات وتثبت ذلك
- مقارنة ممارسات الهوية والوصول المميز مع زملاء من قطاعات المال والصحة والطاقة والاتصالات والخدمات العامة

الخاتمة:

أصبحت الهوية الضابط الذي تعتمد عليه معظم ضوابط الأمن الأخرى. تنتقل الدورة من مكونات إدارة الهوية والوصول وإجراءات التعيين والانتقال والمغادرة، إلى خدمات الأدلة وبروتوكولات SAML وOpenID Connect وOAuth ومستويات ضمان المصادقة، ثم إلى الوصول القائم على الأدوار والسمات ومنح الحسابات واعتماد الصلاحيات وفصل المهام، ومنها إلى إدارة الصلاحيات المميزة والهوية في الثقة الصفريّة وأدوات الحوكمة. ويطبق اليوم الأخير دراسات حالة في التدقيق وإساءة استخدام بيانات الاعتماد، وينتج تقييمًا لضوابط الهوية والوصول وخارطة طريق لتحسينها.