QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1939

دورة إدارة الوصول المميز وأمن الهوية

إدارة الهوية والوصول
تقنية المعلومات والأمن السيبراني

المدة
5 أيام

طريقة التقديم
حضوري

شركة كويست ترينينج

quest-training.com

نظرة عامة على الدورة

تقدم دورة إدارة الوصول المميز وأمن الهوية إطاراً متكاملاً وعملياً لحماية الهويات ذات الصلاحيات العالية والحسابات الإدارية وعمليات الوصول الحساسة ضمن بيئات تقنية المعلومات الحديثة. وتركز الدورة على الحد من المخاطر المرتبطة بالصلاحيات المفرطة، واختراق بيانات اعتماد المسؤولين، والوصول الإداري غير المصرح به، والأنشطة الإدارية غير الخاضعة للرقابة على الأنظمة والبيانات الحيوية.

تتناول الدورة دور إدارة الوصول المميز باعتبارها أحد المكونات الأساسية لأمن الهوية وبنى انعدام الثقة. ويستكشف المشاركون أساليب اكتشاف الحسابات ذات الصلاحيات العالية وتصنيفها، وحماية بيانات الاعتماد، وإدارة خزائن كلمات المرور، ومراقبة الجلسات الإدارية، والوصول المؤقت عند الحاجة، وتطبيق مبدأ أقل صلاحية، ورفع الصلاحيات بشكل مضبوط، وإجراءات طلب الوصول والموافقة عليه، إلى جانب المراقبة والتدقيق.

كما تغطي الدورة إدارة الوصول المميز في البنية التحتية المحلية والبيئات السحابية والهجينة وقواعد البيانات والتطبيقات وأجهزة الشبكات ونقاط النهاية والأنظمة الموزعة. وسيتعلم المشاركون كيفية تحديد الحسابات المميزة وهويات الخدمات، ووضع الضوابط المناسبة، وإدارة الوصول الطارئ، وتعزيز الإجراءات الإدارية دون التأثير غير الضروري على العمليات التشغيلية المشروعة.

ومن خلال تمارين تصميم البنية الأمنية، وتقييمات الوصول المميز، وسيناريوهات الهجمات، ومحاكاة ضوابط الوصول، وورش الحوكمة العملية، سيتمكن المشاركون من تصميم وتطوير برامج إدارة الوصول المميز بما يتوافق مع المخاطر المؤسسية ومتطلبات الأمن السيبراني والامتثال ومبادئ انعدام الثقة.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- تحليل دور إدارة الوصول المميز في تعزيز أمن الهوية المؤسسية.
- تحديد وتصنيف الحسابات والهويات وبيانات الاعتماد ومسارات الوصول ذات الصلاحيات العالية.

- تقييم المخاطر المرتبطة بالحسابات المميزة والوصول الإداري.
- تصميم استراتيجية متكاملة لإدارة الوصول المميز تتوافق مع أهداف أمن المؤسسة.
- تطبيق مبادئ أقل صلاحية والوصول المؤقت القائم على الحاجة.
- تطوير ممارسات آمنة لإدارة بيانات اعتماد الحسابات المميزة وتخزينها وتغييرها.
- تصميم إجراءات فعالة لطلب الوصول المميز والموافقة عليه ومنحه.
- تطبيق ضوابط مراقبة الجلسات الإدارية وتسجيلها ومراجعتها.
- تعزيز حماية حسابات الخدمات والهويات الآلية وغير البشرية.
- إدارة الوصول المميز في البيئات المحلية والسحابية والهجينة والعمل عن بُعد.
- اكتشاف الأنشطة الإدارية المشبوهة ومؤشرات اختراق بيانات الاعتماد.
- وضع ضوابط فعالة للوصول الطارئ والحسابات الاحتياطية للحالات الحرجة.
- تطوير سياسات ومعايير وإجراءات حوكمة إدارة الوصول المميز.
- تحديد مؤشرات قياس أداء وفعالية ضوابط الوصول المميز.
- إعداد خارطة طريق عملية لتنفيذ برنامج إدارة الوصول المميز وتطويره بصورة مستمرة.

الفئة المستهدفة

تستهدف الدورة المتخصصين في الأمن السيبراني، ومتخصصي إدارة الهوية والوصول، ومهندسي أمن المعلومات، ومديري تقنية المعلومات، ومديري البنية التحتية، ومسؤولي الأنظمة والشبكات، ومتخصصي أمن الحوسبة السحابية، والمتخصصين التقنيين المسؤولين عن الوصول الإداري وأمن الأنظمة المؤسسية.

كما تناسب فرق عمليات الأمن السيبراني، ومتخصصي المخاطر والالتزام، والمدققين الداخليين، ومتخصصي الحوكمة، ومهندسي المؤسسات، ومسؤولي الحسابات المميزة، وصناع القرار المسؤولين عن أمن الهوية وحوكمة الوصول والتحول السيبراني ومبادرات انعدام الثقة.

وتكتسب الدورة أهمية خاصة للمنظمات التي تسعى إلى تقليل مخاطر سرقة بيانات الاعتماد، وتصعيد الصلاحيات، والتهديدات الداخلية، والأنشطة الإدارية غير المصرح بها، واختراق الأنظمة والبنية التحتية الحيوية.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- شرح مبادئ وبنية إدارة الوصول المميز.
- تحديد الهويات ذات الصلاحيات العالية ومسارات الوصول الحساسة داخل المؤسسة.
- تنفيذ تقييم منهجي لمخاطر الوصول المميز.
- تصنيف الحسابات المميزة وفق مستوى المخاطر والوظيفة ومستوى الصلاحيات.
- تصميم نماذج الوصول وفق مبدأ أقل صلاحية والوصول المؤقت.
- تطبيق ممارسات آمنة لتخزين بيانات الاعتماد وتغييرها وإدارتها.
- إنشاء إجراءات فعالة لطلبات الوصول المميز والموافقات المرتبطة بها.
- تطبيق آليات مراقبة الجلسات الإدارية وتسجيلها وتدقيقها.
- حماية حسابات الخدمات والهويات غير البشرية ذات الصلاحيات العالية.
- إدارة الوصول المميز عبر البيئات السحابية والهجينة.
- اكتشاف وتحليل الأنشطة المشبوهة المرتبطة بالحسابات المميزة.
- تصميم إجراءات الوصول الطارئ والحسابات الاحتياطية.
- تطوير إطار حوكمة وسياسات ومعايير لإدارة الوصول المميز.
- إعداد مؤشرات الأداء والتقارير الإدارية الخاصة بأمن الوصول المميز.
- تقييم مستوى نضج إدارة الوصول المميز وتحديد فجوات الضوابط.

- إعداد خارطة طريق مرحلية لتنفيذ برنامج إدارة الوصول المميز وتطويره.
- المحاور التدريبية

محاور الدورة

اليوم الأول

مخاطر الوصول المميز وأساسيات أمن الهوية

- مفهوم الوصول المميز والحسابات الإدارية.
- العلاقة بين إدارة الوصول المميز وإدارة الهوية والأمن السيبراني ونموذج انعدام الثقة.
- الحسابات المميزة ومصادر التهديد داخل المؤسسة.
- أنواع الهويات والحسابات ذات الصلاحيات العالية.
- الهويات البشرية وحسابات الخدمات والتطبيقات والأنظمة والأجهزة والبيئات السحابية.
- مخاطر تصعيد الصلاحيات وسرقة بيانات الاعتماد.
- التهديدات الداخلية والأنشطة الإدارية غير المصرح بها.
- تحديد الأنظمة الحيوية ومسارات الوصول عالية الخطورة.
- اكتشاف وحصر الحسابات المميزة.
- تقييم مستوى نضج أمن الوصول المميز.
- التطبيق العملي: تنفيذ تقييم للوصول المميز في مؤسسة افتراضية وتحديد الهويات والأنظمة ومسارات الوصول عالية المخاطر.

اليوم الثاني

إدارة بيانات الاعتماد وتطبيق مبدأ أقل صلاحية

- مبادئ أقل صلاحية.
- تصنيف الحسابات المميزة وترتيب أولويات المخاطر.
- حماية بيانات الاعتماد وإدارة كلمات المرور الآمنة.
- خزائن بيانات الاعتماد وتغيير كلمات المرور بصورة دورية.
- إدارة الحسابات الإدارية المشتركة والعامة.
- الوصول المؤقت والمحدد زمنياً إلى الصلاحيات.
- رفع الصلاحيات والتحكم في الوصول الإداري.
- إجراءات طلب الوصول والموافقة عليه.
- الحد من الصلاحيات الإدارية الدائمة.
- إدارة الاستثناءات المتعلقة بالوصول المميز.
- مواءمة الصلاحيات مع المتطلبات التشغيلية واحتياجات الأعمال.
- التطبيق العملي: تصميم نموذج متكامل لإدارة بيانات اعتماد الحسابات المميزة يشمل الاكتشاف والتصنيف والحفظ الآمن والتغيير والموافقة ورفع الصلاحيات وإنهاء الوصول.

اليوم الثالث

بنية إدارة الوصول المميز والضوابط التقنية

- مكونات بنية إدارة الوصول المميز في المؤسسات.
- اكتشاف الحسابات المميزة وإدارتها وإدخالها ضمن منظومة الحماية.
- خزائن بيانات الاعتماد والمستودعات الآمنة.
- إدارة الجلسات الإدارية المميزة.

اليوم الثالث — تابع

- تسجيل الجلسات ومراقبتها.
- الوصول المميز إلى التطبيقات وقواعد البيانات.
- إدارة الوصول إلى أجهزة الشبكات والبنية التحتية.
- إدارة الصلاحيات على الخوادم ونقاط النهاية.
- الوصول المميز في البيئات السحابية والهجينة.
- إدارة حسابات الخدمات والهويات الآلية.
- التكامل بين إدارة الوصول المميز ومنصات الهوية والأنظمة الأمنية وعمليات الأمن السيبراني.
- التطبيق العملي: تصميم بنية لإدارة الوصول المميز لمؤسسة هجينة تشمل الخوادم وقواعد البيانات وأجهزة الشبكات والمنصات السحابية والتطبيقات ونقاط النهاية والمستخدمين الإداريين.

اليوم الرابع

المراقبة واكتشاف التهديدات والاستجابة للحوادث

- مراقبة أنشطة الوصول المميز.
- تحديد السلوك الإداري غير الطبيعي.
- اكتشاف مؤشرات اختراق بيانات اعتماد الحسابات المميزة.
- مؤشرات تصعيد الصلاحيات غير المصرح به.
- تحليل الجلسات المشبوهة وأنماط الوصول غير المعتادة.
- تحليل سلوك المستخدم والكيان في الأنشطة ذات الصلاحيات العالية.
- ربط الأحداث الأمنية والتحقيق في الأنشطة المشبوهة.
- الاستجابة لحوادث اختراق الحسابات المميزة.
- إجراءات الوصول الطارئ والحسابات الاحتياطية.
- إلغاء الصلاحيات واستعادة السيطرة على الحسابات المخترقة.

اليوم الرابع — تابع

- التكامل بين إدارة الوصول المميز وعمليات الأمن السيبراني والاستجابة للحوادث.
- التطبيق العملي: التحقيق في سيناريو محاكاة لاختراق حساب مميز يتضمن سرقة بيانات الاعتماد، ورفع الصلاحيات، وجلسات إدارية مشبوهة، والوصول غير المصرح به إلى أنظمة حيوية.

اليوم الخامس

الحوكمة والامتثال والقياس وتنفيذ برنامج إدارة الوصول المميز

- تطوير إطار حوكمة إدارة الوصول المميز.
- تحديد الملكية والمسؤوليات والمساءلة.
- سياسات ومعايير وإجراءات إدارة الوصول المميز.
- مراجعة واعتماد الحسابات والصلاحيات بصورة دورية.
- الفصل بين المهام والضوابط الإدارية.
- متطلبات التدقيق والأدلة الرقابية.
- مؤشرات مخاطر وأداء إدارة الوصول المميز.
- قياس فعالية الضوابط ومستوى النضج.
- بناء نموذج التشغيل المستهدف لإدارة الوصول المميز.
- ترتيب أولويات مبادرات إدارة الوصول المميز وفق المخاطر والأثر المؤسسي.
- إدارة مخاطر التنفيذ والتغيير المؤسسي.
- التحسين المستمر وتطوير قدرات إدارة الوصول المميز.
- الورشة الختامية: إعداد استراتيجية متكاملة لإدارة الوصول المميز وأمن الهوية تشمل اكتشاف الهويات المميزة، وتقييم المخاطر، وأقل صلاحية، وحماية بيانات الاعتماد، والوصول المؤقت، وإدارة الجلسات، والوصول السحابي والهجين، والمراقبة، والاستجابة للحوادث، والحوكمة، والامتثال، وقياس الأداء، وتقييم النضج، وخارطة طريق التنفيذ.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/privileged-access-management-pam-identity-security-training-course

الموقع الإلكتروني: https://quest-training.com

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440