QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1937

دورة أمن الهوية وإدارة الوصول وفق نموذج انعدام الثقة

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 أمن الهوية وإدارة الوصول وفق نموذج انعدام الثقة إطاراً عملياً وشاملاً لتصميم وتنفيذ وإدارة أمن الهوية والوصول ضمن بنية أمنية قائمة على مبدأ انعدام الثقة. وتركز الدورة على مبدأ التحقق المستمر من المستخدمين والأجهزة والتطبيقات وطلبات الوصول، بدلاً من الاعتماد على نماذج الحماية التقليدية القائمة على حدود الشبكة والثقة الضمنية.

يتعرف المشاركون على الدور المحوري للهوية باعتبارها أحد أهم ضوابط الأمن السيبراني، مع التركيز على المصادقة والتفويض وإدارة دورة حياة الهوية والوصول المميز وسياسات الوصول التكيفية والمصادقة متعددة العوامل وثقة الأجهزة والوصول إلى التطبيقات والمراقبة المستمرة. كما توضح الدورة كيفية تقليل مخاطر الوصول غير المصرح به وسرقة بيانات الاعتماد والحركة الجانبية والصلاحيات المفرطة.

وتتناول الدورة تطبيق مبادئ انعدام الثقة في البيئات السحابية والهجينة والمحلية وبيئات العمل عن بُعد والبيئات الموزعة. ويتعلم المشاركون كيفية تقييم مخاطر الهوية، وتطبيق مبدأ أقل قدر من الصلاحيات، وحماية الحسابات المميزة، وتصميم سياسات وصول تعتمد على الهوية والجهاز والموقع والسلوك ومستوى المخاطر.

ومن خلال السيناريوهات العملية وتمارين تصميم البنية الأمنية وتقييمات الوصول ومحاكاة الضوابط الأمنية ودراسات حالات الحوادث، يطور المشاركون القدرة على بناء استراتيجيات متكاملة لأمن الهوية وإدارة الوصول تتوافق مع مبادئ انعدام الثقة، مع التركيز على الحوكمة والمراقبة وإدارة المخاطر والامتثال واكتشاف تهديدات الهوية والتحسين المستمر.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- تحليل مبادئ وأهداف أمن الهوية وإدارة الوصول وفق نموذج انعدام الثقة.
- تقييم مخاطر الهوية والوصول المرتبطة بالمستخدمين والأجهزة والتطبيقات والموارد.

- تصميم ضوابط أمنية تتمحور حول الهوية وفق مبادئ انعدام الثقة.
- تطبيق مبدأ أقل قدر من الصلاحيات ومبدأ الحاجة إلى المعرفة.
- تعزيز آليات المصادقة والتفويض والتحقق من الوصول.
- تطبيق أساليب المصادقة متعددة العوامل والمصادقة القائمة على المخاطر.
- تطوير عمليات فعالة لإدارة دورة حياة الهوية والوصول.
- حماية الحسابات المميزة والهويات الإدارية عالية الصلاحيات.
- تصميم سياسات وصول تكيفية تعتمد على الهوية والجهاز والموقع والسلوك والمخاطر.
- دمج أمن الهوية مع أمن السحابة والأجهزة والتطبيقات والشبكات والبيانات.
- اكتشاف التهديدات القائمة على الهوية والأنشطة المشبوهة المتعلقة بالوصول.
- إنشاء آليات فعالة لحوكمة الهوية ومراجعة الصلاحيات.
- تقييم بنى أمن الهوية وفق نموذج انعدام الثقة وتحديد الفجوات الأمنية.
- تطوير أولويات عملية وخارطة طريق لتطبيق أمن الهوية وفق نموذج انعدام الثقة.
- وضع مؤشرات لقياس فعالية أمن الهوية وإدارة الوصول.

الفئة المستهدفة

تستهدف الدورة مديري الأمن السيبراني، ومتخصصي أمن المعلومات، ومسؤولي الهوية وإدارة الوصول، ومهندسي الأمن، ومديري البنية التحتية وتقنية المعلومات، ومسؤولي الشبكات والأنظمة، ومتخصصي أمن الحوسبة السحابية، والمهنيين المسؤولين عن حماية الهويات والوصول إلى الموارد المؤسسية.

كما تناسب متخصصي المخاطر والالتزام والحوكمة الأمنية، والمدققين الداخليين، ومهندسي المؤسسات، وفرق عمليات الأمن السيبراني، ومسؤولي البيئات السحابية، وصناع القرار التقني المشاركين في مبادرات انعدام الثقة وأمن الهوية والتحول السيبراني.

وتعد الدورة مناسبة بشكل خاص للمنظمات التي تعتمد البيئات الهجينة والسحابية، وتدعم العمل عن بُعد، وتدير صلاحيات إدارية ومميزة، أو تسعى إلى تعزيز الحماية من سرقة بيانات الاعتماد والوصول غير المصرح به والتهديدات الداخلية والهجمات القائمة على الهوية.

مخرجات التعلم

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح المبادئ الأساسية لبنية انعدام الثقة وأمن الهوية.
- تحديد الهويات والموارد والتطبيقات والأجهزة وعلاقات الوصول بينها.
- تقييم مخاطر الهوية والوصول باستخدام منهجيات قائمة على المخاطر.
- تصميم بنى آمنة للمصادقة والتفويض.
- تطبيق مبدأ أقل قدر من الصلاحيات في البيئات المؤسسية.
- تقييم استراتيجيات المصادقة متعددة العوامل والمصادقة التكيفية.
- إنشاء عمليات فعالة لتوفير الهويات وإدارة دورة حياتها.
- تطبيق ضوابط متقدمة لحماية الهويات والحسابات ذات الصلاحيات المرتفعة.
- تصميم سياسات وصول مشروطة وتكيفية وفق مستوى المخاطر والسياق.
- دمج ضوابط الهوية مع أمن الأجهزة والسحابة والتطبيقات والشبكات والبيانات.
- تحديد مؤشرات اختراق الهوية والسلوكيات غير الطبيعية في عمليات الوصول.
- دعم عمليات اكتشاف الحوادث المرتبطة بالهوية والتحقيق فيها والاستجابة لها.
- إنشاء آليات فعالة لمراجعة الوصول والحوكمة والمراقبة والتدقيق.
- تقييم مستوى نضج أمن الهوية وفق نموذج انعدام الثقة وتحديد فرص التحسين.

- تطوير خارطة طريق مرحلية لتطبيق أمن الهوية وإدارة الوصول وفق نموذج انعدام الثقة.
- تحديد مؤشرات أداء وأمن مناسبة لقياس فعالية الضوابط المطبقة.
- المحاور التدريبية

محاور الدورة

اليوم الأول

مبادئ انعدام الثقة وأمن الهوية

- الانتقال من أمن حدود الشبكة إلى نموذج انعدام الثقة.
- المبادئ الأساسية والأهداف الأمنية لنموذج انعدام الثقة.
- الهوية باعتبارها محوراً رئيسياً للأمن السيبراني.
- المستخدمون والأجهزة والتطبيقات وأعباء العمل والموارد كعناصر أمنية.
- التحقق المستمر واتخاذ قرارات الوصول بناءً على الأدلة.
- مبدأ أقل قدر من الصلاحيات والحاجة إلى المعرفة.
- تهديدات الهوية والهجمات القائمة على بيانات الاعتماد.
- أسطح الهجوم المرتبطة بالهوية في البيئات السحابية والهجينة.
- تحديد علاقات الهوية والوصول والموارد.
- تقييم جاهزية المنظمة لتطبيق أمن الهوية وفق نموذج انعدام الثقة.
- تطبيق عملي: إجراء تقييم لأمن الهوية وفق نموذج انعدام الثقة في منظمة هجينة وتحديد أبرز المخاطر والفجوات الأمنية.

اليوم الثاني

المصادقة والتفويض والوصول التكيفي

- أساسيات المصادقة والتفويض.
- حماية كلمات المرور وبيانات الاعتماد.
- استراتيجيات المصادقة متعددة العوامل.
- المصادقة القوية وأساليب مقاومة التصيد الاحتيالي.
- الدخول الموحد ومفاهيم اتحاد الهوية.
- التحكم في الوصول القائم على الأدوار والسمات.
- قرارات الوصول المشروطة والقائمة على المخاطر.
- هوية الأجهزة ومستوى الثقة بها.
- الوصول القائم على السياق والهوية والجهاز والموقع والسلوك والمخاطر.
- تصميم سياسات وصول آمنة للسيناريوهات عالية المخاطر.
- تطبيق عملي: تصميم إطار للتحكم التكيفي في الوصول للموظفين والمسؤولين والمقاولين والمستخدمين عن بُعد وفق مستويات المخاطر المختلفة.

اليوم الثالث

دورة حياة الهوية والوصول المميز والحوكمة

- إدارة دورة حياة الهوية من الانضمام إلى إنهاء الخدمة.
- توفير الهويات وإلغاء الصلاحيات.
- إدارة انتقالات الموظفين وتغير أدوارهم.
- تصميم الأدوار وحقوق الوصول.
- تطبيق مبدأ أقل قدر من الصلاحيات.

اليوم الثالث — تابع

- حماية الحسابات ذات الصلاحيات المميزة.
- حماية الهويات الإدارية.
- مبادئ إدارة الوصول المميز.
- المراجعة الدورية للصلاحيات واعتماد حقوق الوصول.
- فصل المهام ومخاطر الصلاحيات المفرطة.
- حوكمة الهوية وتحديد المسؤوليات.
- تطبيق عملي: تطوير نموذج لإدارة دورة حياة الهوية والوصول المميز بهدف تقليل الصلاحيات المفرطة وتعزيز الرقابة على الحسابات الإدارية.

اليوم الرابع

تكامل انعدام الثقة والمراقبة واكتشاف تهديدات الهوية

- دمج أمن الهوية مع حماية الأجهزة.
- تأمين الوصول إلى التطبيقات والبيئات السحابية.
- تكامل أمن الهوية مع الشبكات والبيانات.
- بيانات المراقبة الأمنية المتعلقة بالهوية والوصول.
- اكتشاف أنماط المصادقة والوصول غير الطبيعية.
- سيناريوهات سرقة بيانات الاعتماد واختراق الحسابات.
- الحركة الجانبية القائمة على اختراق الهوية.
- مخاطر التهديدات الداخلية والحسابات المخترقة.
- التحقيق في الأنشطة المشبوهة المرتبطة بالهوية والاستجابة لها.
- الأتمتة الأمنية والتحقق المستمر.
- تعزيز مرونة الهوية وقدرات الاستعادة.

اليوم الرابع — تابع

- تطبيق عملي: تحليل حادثة افتراضية لاختراق هوية تتضمن مصادقة مشبوهة وتصعيداً للصلاحيات ووصولاً غير مصرح به، ثم إعداد خطة للتحقيق والاستجابة.

اليوم الخامس

بنية أمن الهوية والحوكمة وخارطة التنفيذ

- تصميم بنية مؤسسية لأمن الهوية وفق نموذج انعدام الثقة.
- دمج أمن الهوية في البيئات الهجينة ومتعددة السحابات.
- سياسات حوكمة الهوية والأمن.
- الضوابط الأمنية ومتطلبات الامتثال والتدقيق.
- التقييم المستمر لقرارات الوصول ومراقبتها.
- قياس مستوى نضج أمن الهوية وفق نموذج انعدام الثقة.
- مؤشرات الأداء والأمن الرئيسية.
- تحديد فجوات التنفيذ والاعتماديات التقنية.
- ترتيب مبادرات أمن الهوية وفق مستوى المخاطر والأثر المؤسسي.
- بناء خارطة طريق مرحلية لتطبيق انعدام الثقة.
- التحسين المستمر وتحسين الضوابط الأمنية.
- ورشة ختامية: تصميم استراتيجية متكاملة لأمن الهوية وإدارة الوصول وفق نموذج انعدام الثقة، تشمل بنية الهوية، والمصادقة، والتفويض، وأقل قدر من الصلاحيات، والوصول المميز، والوصول التكيفي، وإدارة دورة حياة الهوية، والمراقبة، واكتشاف التهديدات، والحوكمة، وتقييم النضج، ومؤشرات الأمن، والأولويات، وخارطة طريق التنفيذ.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة: https://quest-training.com/courses/zero-trust-identity-access-security-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440