QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1943

دورة تهديدات الأمن السيبراني والثغرات وتقييم المخاطر

الأمن السيبراني وأمن المعلومات
تقنية المعلومات والأمن السيبراني

المدة
5 أيام

طريقة التقديم
حضوري

شركة كويست ترينينج

quest-training.com

نظرة عامة على الدورة

تقدم دورة تهديدات الأمن السيبراني والثغرات وتقييم المخاطر إطاراً متكاملاً وعملياً لتحديد وتحليل وتقييم وإدارة التهديدات والثغرات والمخاطر السيبرانية في بيئات المؤسسات الحديثة. وتهدف الدورة إلى تمكين المشاركين من فهم كيفية ظهور التهديدات السيبرانية، وكيفية استغلال نقاط الضعف، وكيف يمكن للمؤسسات تقييم المخاطر وترتيب أولوياتها بصورة منهجية.

يتعرف المشاركون على مشهد التهديدات السيبرانية المتطور، بما يشمل البرمجيات الخبيثة، وبرمجيات الفدية، والتصيد الاحتيالي، والهندسة الاجتماعية، وهجمات سرقة بيانات الاعتماد، والتهديدات الداخلية، ومخاطر سلسلة التوريد، واستغلال الثغرات البرمجية، ومخاطر الحوسبة السحابية، والهجمات المتقدمة والموجهة. كما تركز الدورة على فهم سطح الهجوم وتحديد نقاط الضعف في التطبيقات والشبكات ونقاط النهاية والهويات والبيانات والمنصات السحابية والبنية التحتية الحيوية.

تقدم الدورة منهجيات منظمة لتقييم مخاطر الأمن السيبراني من خلال الربط بين تحديد الأصول وتحليل التهديدات وتقييم الثغرات وتقدير احتمالية الحدوث وتحليل أثر الأعمال وترتيب المخاطر. ويتعلم المشاركون كيفية تحويل النتائج الفنية المتعلقة بالأمن إلى معلومات واضحة عن المخاطر المؤسسية تساعد الإدارة في اتخاذ القرارات وتحديد أولويات الاستثمار ومبادرات تحسين الأمن السيبراني.

ومن خلال تمارين تقييم المخاطر وتحليل سيناريوهات التهديدات وورش تقييم الثغرات وتصنيف المخاطر وتقييم سطح الهجوم وتخطيط إجراءات المعالجة، يطور المشاركون القدرات اللازمة لتحديد المخاطر السيبرانية ذات الأولوية، واقتراح الضوابط المناسبة، والتواصل الفعال بشأن المخاطر، وإنشاء عملية مستمرة لتقييم التهديدات والثغرات والمخاطر السيبرانية.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- تحليل مشهد التهديدات السيبرانية الحديثة وأنماط الهجمات المتطورة.

- تحديد أصول المعلومات والأنظمة والتطبيقات والهويات والبنية التحتية الحيوية.
- تقييم أسطح الهجوم ونقاط التعرض داخل المؤسسة.
- تحديد الثغرات ونقاط الضعف السيبرانية الشائعة والناشئة.
- تقييم التهديدات وفق احتمالية الحدوث والقدرات والدوافع والأثر المحتمل.
- تنفيذ تقييمات منهجية لمخاطر الأمن السيبراني.
- تطبيق الأساليب النوعية والكمية في تحليل المخاطر السيبرانية.
- ترتيب أولويات الثغرات والمخاطر وفق أثر الأعمال وقابلية الاستغلال.
- تحليل العلاقة بين التهديدات والثغرات والأصول والنتائج المؤسسية.
- تطوير استراتيجيات معالجة المخاطر والحد من آثارها.
- تقييم الضوابط الأمنية وقدرتها على خفض المخاطر المحددة.
- إنشاء سجلات لمخاطر الأمن السيبراني وتحديد ملكية المخاطر.
- التواصل الفعال بشأن المخاطر السيبرانية مع الأطراف الفنية والتنفيذية.
- تطوير مؤشرات للمخاطر السيبرانية وآليات المراقبة المستمرة.
- بناء برنامج مستدام لتقييم التهديدات والثغرات والمخاطر السيبرانية.

الفئة المستهدفة

تستهدف الدورة المتخصصين في الأمن السيبراني وأمن المعلومات، ومحللي الأمن، ومتخصصي إدارة الثغرات، ومديري المخاطر، ومديري تقنية المعلومات، ومهندسي الأمن، وفرق عمليات الأمن السيبراني، والمتخصصين التقنيين المسؤولين عن تحديد مخاطر الأمن السيبراني أو إدارتها.

كما تناسب المتخصصين في الحوكمة والمخاطر والالتزام، والمدققين الداخليين، ومتخصصي استمرارية الأعمال، وإدارة المخاطر المؤسسية، وفرق أمن البنية التحتية والحوسبة السحابية، ومتخصصي أمن التطبيقات، والمديرين

المسؤولين عن حوكمة الأمن السيبراني واتخاذ القرارات القائمة على المخاطر.

وتكتسب الدورة أهمية خاصة للمؤسسات التي تسعى إلى تحسين فهمها للتهديدات السيبرانية، وتعزيز إدارة الثغرات، وإنشاء عمليات منظمة لتقييم المخاطر، وترتيب أولويات الاستثمارات الأمنية وفق أثر الأعمال ومستوى المخاطر المؤسسية.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- شرح أهم التهديدات السيبرانية وتقنيات الهجوم الحديثة.
- تحديد أصول المؤسسة والاعتماديات الحيوية للعمليات المؤسسية.
- رسم أسطح الهجوم عبر الشبكات والتطبيقات ونقاط النهاية والهويات والبيئات السحابية والبيانات.
- تحديد الثغرات وتقييم قابليتها للاستغلال وتأثيرها المحتمل.
- تحليل الجهات المهاجمة ومسارات الهجوم والدوافع والقدرات.
- تنفيذ تقييمات منظمة لمخاطر الأمن السيبراني.
- تحديد احتمالية حدوث المخاطر والأثر المحتمل على الأعمال.
- ترتيب أولويات المخاطر والثغرات وفق مستوى الخطورة والسياق المؤسسي.
- إعداد سجلات شاملة لمخاطر الأمن السيبراني.
- تصميم خطط مناسبة لمعالجة المخاطر والحد منها.
- تقييم الضوابط الأمنية القائمة وتحديد فجوات الحماية.
- تحديد ملكية المخاطر والمسؤوليات وآليات التصعيد.
- تقديم معلومات المخاطر السيبرانية للإدارة وصناع القرار بصورة واضحة.

- تطوير مؤشرات للمخاطر وآليات للمراقبة المستمرة.
- إنشاء عملية قابلة للتكرار لتقييم التهديدات والثغرات والمخاطر السيبرانية.
- المحاور التدريبية

محاور الدورة

اليوم الأول

مشهد التهديدات السيبرانية وسطح الهجوم

- فهم مشهد التهديدات السيبرانية الحديثة.
- التهديدات السيبرانية والجهات المهاجمة ودوافع الهجمات.
- تقنيات الهجوم السيبراني ومسارات الاختراق الشائعة.
- البرمجيات الخبيثة وبرمجيات الفدية والتصيد الاحتيالي والهندسة الاجتماعية.
- سرقة بيانات الاعتماد والهجمات القائمة على الهوية.
- التهديدات الداخلية وسلوكيات المستخدمين الخبيثة أو غير الآمنة.
- تهديدات سلسلة التوريد والأطراف الثالثة.
- الهجمات المتقدمة والموجهة.
- تهديدات البيئات السحابية والعمل عن بُعد والبيئات الهجينة.
- تحديد أسطح الهجوم داخل المؤسسة.
- الأصول الحيوية والخدمات المؤسسية والاعتماديات التقنية.
- التطبيق العملي: إعداد خريطة لسطح الهجوم في مؤسسة افتراضية وتحديد مصادر التهديد والأصول المكشوفة والاعتماديات الأمنية الحيوية.

اليوم الثاني

تحديد الثغرات وتقييم نقاط الضعف الأمنية

- مفهوم الثغرات ونقاط الضعف في الأمن السيبراني.
- أنواع الثغرات في التطبيقات والأنظمة والشبكات ونقاط النهاية.
- أخطاء الإعداد ونقاط الضعف الأمنية الشائعة.
- الثغرات البرمجية وإدارة التحديثات الأمنية.
- ثغرات التطبيقات وتطبيقات الويب.
- ثغرات الشبكات والبنية التحتية.
- ثغرات الهوية وإدارة الوصول.
- نقاط الضعف في أمن الحوسبة السحابية.
- نقاط الضعف المتعلقة بحماية البيانات والمعلومات.
- عمليات اكتشاف وتقييم الثغرات.
- تحديد مستوى خطورة الثغرات وقابليتها للاستغلال.
- التمييز بين الثغرة التقنية والمخاطر المؤسسية الناتجة عنها.
- التطبيق العملي: تنفيذ تقييم للثغرات في بيئة تقنية افتراضية وتحديد نقاط الضعف وتصنيفها وترتيب أولويات معالجتها.

اليوم الثالث

تقييم وتحليل مخاطر الأمن السيبراني

- مبادئ إدارة مخاطر الأمن السيبراني.
- العلاقة بين الأصول والتهديدات والثغرات والنتائج المحتملة.
- تحديد معايير تقييم مخاطر الأمن السيبراني.

اليوم الثالث — تابع

- منهجيات التقييم النوعي للمخاطر.
- مفاهيم التقييم الكمي للمخاطر السيبرانية.
- تقييم احتمالية الحدوث والأثر.
- تحليل أثر المخاطر على الأعمال والعمليات.
- نماذج تصنيف وتقييم المخاطر.
- التحليل القائم على التهديدات والثغرات.
- تحديد المخاطر المترابطة والمخاطر ذات الأثر المتسلسل.
- تطوير سيناريوهات مخاطر الأمن السيبراني.
- إعداد وإدارة سجلات المخاطر السيبرانية.
- التطبيق العملي: تنفيذ تقييم متكامل لمخاطر الأمن السيبراني في مؤسسة افتراضية وإعداد سجل مخاطر مرتب حسب الأولوية.

اليوم الرابع

معالجة المخاطر والحد من التهديدات والضوابط الأمنية

- استراتيجيات معالجة مخاطر الأمن السيبراني.
- تجنب المخاطر وتقليلها ونقلها وقبولها.
- اختيار الضوابط الأمنية المناسبة.
- الضوابط الوقائية والكاشفة والتصحيحية والتعويضية.
- ضوابط أمن الهوية وإدارة الوصول.
- ضوابط أمن الشبكات ونقاط النهاية.
- ضوابط إدارة الثغرات والتحديثات الأمنية.
- ضوابط حماية البيانات والتشفير.

اليوم الرابع — تابع

- ضوابط المراقبة الأمنية والاستجابة للحوادث.
- ضوابط أمن الحوسبة السحابية والأطراف الثالثة.
- إعداد خطط الحد من المخاطر.
- متابعة المعالجة والمخاطر المتبقية.
- التطبيق العملي: إعداد خطة لمعالجة المخاطر السيبرانية ذات الأولوية واختيار الضوابط المناسبة لخفض احتمالية حدوثها وأثرها ومستوى التعرض المتبقي.

اليوم الخامس

حوكمة المخاطر والمراقبة والتقييم المستمر

- إنشاء إطار لحوكمة مخاطر الأمن السيبراني.
- تحديد ملكية المخاطر والمسؤوليات والمساءلة.
- آليات إعداد تقارير المخاطر وتصعيدها.
- شهية المخاطر وحدود التحمل المؤسسية.
- مؤشرات المخاطر الرئيسية ومؤشرات الأداء الأمني.
- المراقبة المستمرة للتهديدات والثغرات.
- متابعة التغيرات في مشهد التهديدات السيبرانية.
- إعادة تقييم المخاطر بعد التغييرات التقنية أو المؤسسية.
- التواصل التنفيذي وإعداد تقارير المخاطر السيبرانية.
- دمج مخاطر الأمن السيبراني مع إدارة المخاطر المؤسسية.
- بناء برنامج مستدام لإدارة الثغرات والمخاطر.
- التحسين المستمر لعمليات تقييم مخاطر الأمن السيبراني.

اليوم الخامس — تابع

- الورشة الختامية: إعداد إطار متكامل لتهديدات الأمن السيبراني والثغرات وتقييم المخاطر يشمل تحديد الأصول، وتحليل التهديدات، وتقييم سطح الهجوم، واكتشاف الثغرات، وتصنيف المخاطر، وترتيب الأولويات، والمعالجة، والضوابط الأمنية، والمخاطر المتبقية، والحوكمة، وإعداد التقارير، والمراقبة المستمرة، والتحسين.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/cybersecurity-threats-vulnerabilities-risk-assessment-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440