QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1945

دورة أساسيات الأمن السيبراني وإدارة أمن المعلومات

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 أساسيات الأمن السيبراني وإدارة أمن المعلومات أساساً متكاملاً وعملياً في مبادئ الأمن السيبراني وإدارة أمن المعلومات والحوكمة الأمنية وإجراءات الحماية المؤسسية. وتهدف الدورة إلى تمكين المشاركين من فهم بيئة الأمن السيبراني الحديثة واكتساب المعرفة اللازمة لحماية المعلومات والأنظمة والشبكات والتطبيقات والخدمات الرقمية داخل المؤسسات.

يتعرف المشاركون على المبادئ الأساسية لأمن المعلومات، بما في ذلك السرية والسلامة والتوافر، إلى جانب التهديدات السيبرانية الشائعة ومسارات الهجوم والثغرات والضوابط الأمنية وإدارة الهوية والوصول وحماية البيانات وأمن الشبكات ونقاط النهاية والمراقبة الأمنية.

كما تقدم الدورة الجانب الإداري لأمن المعلومات، من خلال تناول حوكمة الأمن السيبراني والسياسات الأمنية وتقييم المخاطر وتحديد المسؤوليات وإدارة الحوادث واستمرارية الأعمال والتوعية الأمنية والامتثال وقياس الأداء. ويتعلم المشاركون كيفية تكامل الضوابط التقنية والتنظيمية للحد من المخاطر السيبرانية ودعم أهداف الأعمال.

ومن خلال التمارين العملية وسيناريوهات التهديدات وأنشطة تقييم المخاطر ومراجعة الضوابط الأمنية ومحاكاة الاستجابة للحوادث وورش تطوير السياسات، يطور المشاركون فهماً عملياً لكيفية تطبيق ممارسات فعالة لأمن المعلومات والمساهمة في تعزيز الوضع الأمني للمؤسسة.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح المفاهيم الأساسية للأمن السيبراني وأمن المعلومات.
- تحليل التهديدات السيبرانية والثغرات وأساليب الهجوم الشائعة.
- تطبيق مبادئ السرية والسلامة والتوافر في حماية المعلومات.
- تحديد أصول المعلومات والموارد التقنية الحيوية.

- تقييم المخاطر السيبرانية الأساسية ومستوى تعرض المؤسسة.
- تطبيق الضوابط الأمنية الأساسية لحماية المعلومات والأنظمة.
- تعزيز ممارسات إدارة الهوية والمصادقة والتحكم في الوصول.
- تطبيق إجراءات مناسبة لحماية البيانات والمعلومات.
- فهم أساسيات أمن الشبكات ونقاط النهاية والتطبيقات والحوسبة السحابية.
- تطوير وتطبيق السياسات والإجراءات الأساسية لأمن المعلومات.
- فهم عمليات إدارة الحوادث السيبرانية والاستجابة لها.
- دعم استمرارية الأعمال والمرونة المتعلقة بأمن المعلومات.
- تعزيز الوعي الأمني والسلوكيات المسؤولة في مجال الأمن السيبراني.
- فهم مبادئ حوكمة الأمن السيبراني والامتثال والمساءلة.
- بناء أساس عملي للتحسين المستمر للأمن السيبراني.

الفئة المستهدفة

تستهدف الدورة المتخصصين في تقنية المعلومات والأمن السيبراني وأمن المعلومات، ومسؤولي الأنظمة والشبكات، وفرق الدعم التقني، والمتخصصين المسؤولين عن حماية المعلومات والموارد التقنية داخل المؤسسات.

كما تناسب المديرين والمشرفين ومتخصصي المخاطر والالتزام والمدققين الداخليين ومتخصصي استمرارية الأعمال والحوكمة والموظفين الذين يحتاجون إلى فهم عملي لمبادئ الأمن السيبراني وإدارة أمن المعلومات.

وتكتسب الدورة أهمية خاصة للمؤسسات التي تسعى إلى بناء أساس موحد للمعرفة بالأمن السيبراني لدى الفرق التقنية وغير التقنية، وتعزيز الوعي الأمني، وتحسين الضوابط الأساسية، وتطوير ممارسات أكثر فعالية لإدارة أمن المعلومات.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- شرح المفاهيم والأهداف الأساسية للأمن السيبراني.
- توضيح المبادئ الأساسية لأمن المعلومات.
- تحديد التهديدات السيبرانية وأساليب الهجوم الشائعة.
- التعرف على الثغرات ونقاط الضعف الأمنية الشائعة.
- تحديد أصول المعلومات الحيوية داخل المؤسسة.
- تنفيذ عملية أساسية لتحديد وتقييم مخاطر الأمن السيبراني.
- تطبيق الضوابط الأمنية وإجراءات الحماية الأساسية.
- شرح مبادئ إدارة الهوية والمصادقة والتفويض والتحكم في الوصول.
- تطبيق ممارسات أساسية لحماية البيانات والشبكات ونقاط النهاية والتطبيقات.
- فهم أساسيات أمن الحوسبة السحابية والوصول عن بُعد.
- تطوير سياسات وإجراءات أساسية لأمن المعلومات.
- التعرف على الحوادث السيبرانية والمساهمة في أنشطة الاستجابة المناسبة.
- فهم اعتبارات استمرارية الأعمال والتعافي من الكوارث.
- دعم مبادرات التوعية الأمنية وبناء الثقافة السيبرانية.
- فهم مبادئ حوكمة الأمن السيبراني والامتثال والمساءلة.
- المساهمة في التحسين المستمر لمستوى الأمن السيبراني المؤسسي.
- المحاور التدريبية

محاور الدورة

اليوم الأول

أساسيات الأمن السيبراني وأمن المعلومات

- مفهوم الأمن السيبراني وأمن المعلومات.
- دور الأمن السيبراني في المؤسسات الحديثة.
- السرية والسلامة والتوافر.
- أصول المعلومات والموارد التقنية.
- التهديدات السيبرانية والجهات المهاجمة.
- مسارات الهجوم وتقنيات الاختراق الشائعة.
- البرمجيات الخبيثة وبرمجيات الفدية والتصيد الاحتيالي والهندسة الاجتماعية.
- سرقة بيانات الاعتماد والهجمات القائمة على الهوية.
- التهديدات الداخلية والمخاطر المرتبطة بالعامل البشري.
- مفهوم الثغرات ونقاط الضعف الأمنية.
- مبادئ الأمن السيبراني والمسؤوليات المؤسسية.
- التطبيق العملي: تحديد أصول المعلومات الحيوية والتهديدات والثغرات والآثار الأمنية المحتملة داخل مؤسسة افتراضية.

اليوم الثاني

الضوابط الأمنية وحماية الهوية والبيانات والتقنيات

- مفهوم الضوابط الأمنية وأهدافها.
- الضوابط الوقائية والكاشفة والتصحيحية والتعويضية.
- أساسيات إدارة الهوية والوصول.

اليوم الثاني — تابع

- المصادقة والتفويض.
- أمن كلمات المرور والمصادقة متعددة العوامل.
- مبدأ أقل صلاحية وحوكمة الوصول.
- تصنيف المعلومات وحماية البيانات.
- التشفير والتعامل الآمن مع المعلومات.
- أساسيات أمن الشبكات.
- أمن نقاط النهاية والأجهزة.
- أساسيات أمن التطبيقات.
- أمن الحوسبة السحابية والوصول عن بُعد.
- التطبيق العملي: تقييم الضوابط الأمنية الأساسية في مؤسسة افتراضية وتحديد فرص تحسين حماية الهوية والبيانات والشبكات ونقاط النهاية والتطبيقات.

اليوم الثالث

إدارة المخاطر والسياسات الأمنية

- أساسيات إدارة مخاطر الأمن السيبراني.
- تحديد الأصول والتهديدات والثغرات والمخاطر.
- تقييم احتمالية المخاطر والأثر على الأعمال.
- منهجيات تقييم المخاطر الأساسية.
- معالجة المخاطر والحد منها.
- السياسات والمعايير والإجراءات والإرشادات الأمنية.
- سياسات الاستخدام المقبول وأمن المعلومات.
- سياسات التحكم في الوصول وكلمات المرور.

اليوم الثالث — تابع

- سياسات حماية البيانات وتصنيف المعلومات.
- سياسات إدارة الثغرات والتحديثات الأمنية.
- متطلبات التوعية الأمنية.
- الأدوار والمسؤوليات والمساءلة الأمنية.
- التطبيق العملي: تنفيذ تقييم أساسي لمخاطر الأمن السيبراني وإعداد مجموعة من سياسات أمن المعلومات ومتطلبات الضوابط لمؤسسة افتراضية.

اليوم الرابع

إدارة الحوادث والمراقبة والمرونة المؤسسية

- مفهوم الحوادث السيبرانية.
- الأنواع الشائعة للحوادث الأمنية.
- اكتشاف الحوادث وتحديدها.
- الإبلاغ عن الحوادث وآليات التصعيد.
- دورة حياة الاستجابة للحوادث.
- مفاهيم الاحتواء والمعالجة والتعافي.
- أساسيات المراقبة الأمنية وتسجيل الأحداث.
- التعرف على الأنشطة المشبوهة والمؤشرات الأمنية.
- استمرارية الأعمال والتعافي من الكوارث.
- أمن المعلومات أثناء الاضطرابات التشغيلية.
- اعتبارات أمن الأطراف الثالثة وسلاسل التوريد.
- الوعي الأمني والعوامل البشرية.

اليوم الرابع — تابع

- التطبيق العملي: المشاركة في محاكاة لحادث سيبراني، وتحديد طبيعة الحادث وأثره، ووضع أولويات الاستجابة وإجراءات الاحتواء والتعافي.

اليوم الخامس

إدارة أمن المعلومات والحوكمة والتحسين المستمر

- أساسيات حوكمة أمن المعلومات.
- مسؤوليات الإدارة والمساءلة الأمنية.
- الامتثال السيبراني والمتطلبات الرقابية.
- أنظمة إدارة أمن المعلومات.
- أهداف أمن المعلومات وقياس الأداء.
- مؤشرات الأمن السيبراني والتقارير الإدارية.
- المراجعات الأمنية الداخلية وتقييم الضوابط.
- تحديد الفجوات الأمنية والإجراءات التصحيحية.
- التوعية الأمنية والثقافة المؤسسية.
- المراقبة والتحسين المستمر.
- مواءمة أمن المعلومات مع أهداف الأعمال.
- بناء برنامج مستدام لتحسين الأمن السيبراني.
- الورشة الختامية: إعداد إطار متكامل لأساسيات الأمن السيبراني وإدارة أمن المعلومات يشمل أصول المعلومات والتهديدات والثغرات وتقييم المخاطر والضوابط الأمنية والهوية والوصول وحماية البيانات والسياسات وإدارة الحوادث والمرونة والحوكمة والتوعية وقياس الأداء والتحسين المستمر.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/cybersecurity-fundamentals-information-security-management-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440