QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1986

دورة الاستجابة لحوادث الأمن السيبراني وإدارتها

العمليات الأمنية والاستجابة للحوادث
تقنية المعلومات والأمن السيبراني

المدة
5 أيام

طريقة التقديم
حضوري

شركة كويست ترينينج

quest-training.com

نظرة عامة على الدورة

تقدم دورة الاستجابة لحوادث الأمن السيبراني وإدارتها إطاراً عملياً ومنظماً لتحديد الحوادث السيبرانية وتحليلها واحتوائها وإدارتها والتعافي منها. وتركز الدورة على تطوير القدرات المؤسسية اللازمة للاستجابة للحوادث الأمنية بكفاءة، مع الحد من تأثيراتها على العمليات والخدمات والبيانات والتكاليف والسمعة المؤسسية.

يتناول البرنامج دورة الاستجابة للحوادث بشكل متكامل، بدءاً من الاستعداد والتعرف على الحادث، مروراً بالفرز والتقييم والتحليل والاحتواء والقضاء على التهديد والتعافي، وصولاً إلى المراجعة بعد الحادث واستخلاص الدروس المستفادة. كما يركز على اتخاذ القرارات بصورة منظمة، وتحديد المسؤوليات، والتصعيد، وحفظ الأدلة، وتوثيق الحوادث، والتنسيق بين الفرق الفنية وأطراف الأعمال.

ويتناول البرنامج أيضاً الجوانب الإدارية والتنظيمية لإدارة الحوادث السيبرانية، بما يشمل تصنيف الحوادث وتقييم مستوى الخطورة وتحديد أولويات الاستجابة والاتصالات وإدارة التصعيد واستمرارية الأعمال والاعتبارات التنظيمية ومشاركة الإدارة التنفيذية. ويتعلم المشاركون كيفية تنسيق جهود الأمن السيبراني وتقنية المعلومات والمخاطر والالتزام والشؤون القانونية والاتصال والإدارة أثناء الحوادث المعقدة.

ومن خلال السيناريوهات الواقعية وتمارين التحقيق ومحاكاة الحوادث والتطبيقات العملية، يطور المشاركون القدرة على إدارة الحادث منذ اكتشافه الأولي وحتى معالجته وإغلاقه واستخلاص الدروس منه. كما تركز الدورة على التحسين المستمر لمساعدة المؤسسات على تعزيز إجراءات الاستجابة وتحديد نقاط الضعف المتكررة وتحسين الجاهزية وبناء مرونة سيبرانية أكثر فاعلية.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح مبادئ ومراحل وأهداف الاستجابة لحوادث الأمن السيبراني.
- إنشاء عمليات فعالة للاستجابة للحوادث تتوافق مع المخاطر المؤسسية.

- تحديد الحوادث السيبرانية وتصنيفها وفق مستوى الخطورة والتأثير.
- تطبيق أساليب منظمة لفرز الحوادث وتقييمها الأولي.
- تحليل الحوادث الأمنية وتحديد أولويات الاستجابة المناسبة.
- تنسيق عمليات احتواء الحوادث والقضاء على التهديد والتعافي.
- تحديد الأدوار والمسؤوليات وإجراءات التصعيد بوضوح.
- تطبيق الممارسات المناسبة لحفظ الأدلة وتوثيق الحوادث.
- إدارة الاتصالات بين الفرق الفنية وأطراف الأعمال.
- تقييم التأثيرات التشغيلية والمالية والتنظيمية والسمعية للحوادث السيبرانية.
- تنسيق الاستجابة للحوادث مع استمرارية الأعمال والتعافي من الكوارث.
- إدارة الحوادث عالية التأثير التي تتطلب تدخلاً تنفيذياً أو استجابة على مستوى الأزمة.
- تقييم فعالية الاستجابة للحوادث من خلال التمارين والمراجعات اللاحقة.
- تحديد الأسباب الجذرية ونقاط الضعف المتكررة بعد الحوادث الأمنية.
- تطوير إجراءات تصحيحية ووقائية للحد من مخاطر الحوادث المستقبلية.
- تعزيز نضج إدارة الحوادث السيبرانية والمرونة المؤسسية.

الفئة المستهدفة

تستهدف الدورة مديري الأمن السيبراني ومتخصصي الاستجابة للحوادث ومحللي الأمن ومتخصصي عمليات الأمن ومتخصصي أمن المعلومات ومتخصصي اكتشاف التهديدات ومهندسي الأمن ومتخصصي تقنية المعلومات المسؤولين عن تحديد الحوادث السيبرانية أو الاستجابة لها.

كما تناسب متخصصي المخاطر والالتزام واستمرارية الأعمال والرقابة الداخلية والشؤون القانونية والخصوصية وإدارة الأزمات ومديري التقنية ومتخصصي الاتصال والقيادات التنفيذية المشاركين في إدارة الحوادث السيبرانية أو

الاستجابة للأزمات المؤسسية.

وتعد الدورة مناسبة بصورة خاصة للجهات الحكومية والوزارات والمصارف والمؤسسات المالية وشركات النفط والغاز وشركات الاتصالات ومشغلي البنية التحتية الحيوية والمؤسسات التقنية والشركات متعددة الجنسيات والمؤسسات الكبرى التي تسعى إلى تعزيز قدراتها في إدارة الحوادث السيبرانية والمرونة المؤسسية.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- تقييم مستوى جاهزية المؤسسة لإدارة الحوادث السيبرانية.
- إنشاء عمليات منظمة لتحديد الحوادث وتقييمها وتصعيدها.
- تصنيف الحوادث وفق مستوى الخطورة وتأثيرها على الأعمال ودرجة الاستعجال.
- تنفيذ الفرز الأولي للحوادث وتحديد إجراءات الاستجابة المناسبة.
- تحليل المعلومات الفنية والسياقية لفهم نطاق الحادث.
- بناء التسلسل الزمني للحادث وتوثيق القرارات الرئيسية أثناء الاستجابة.
- تنسيق عمليات الاحتواء والقضاء على التهديد بين الفرق المعنية.
- دعم استعادة الأنظمة والخدمات المتضررة بصورة آمنة.
- حفظ الأدلة ذات الصلة وإدارة سجلات الحوادث بدقة.
- إيصال حالة الحادث بوضوح إلى الأطراف الفنية والتشغيلية والتنفيذية.
- تقييم الآثار التشغيلية والتنظيمية والمالية والسمعية للحادث.
- تنسيق الاستجابة السيبرانية مع متطلبات استمرارية الأعمال والتعافي.
- إدارة الحوادث المعقدة التي تشمل فرقاً متعددة وأولويات متنافسة.

- تنفيذ مراجعات ما بعد الحوادث وتحديد فرص التحسين.
- تطوير إجراءات تصحيحية استناداً إلى الأسباب الجذرية والدروس المستفادة.
- إعداد خارطة طريق عملية لتحسين قدرات الاستجابة للحوادث.
- المحاور التدريبية

محاور الدورة

اليوم الأول

أسس الاستجابة لحوادث الأمن السيبراني

- مبادئ وأهداف الاستجابة للحوادث.
- الحوادث السيبرانية والسيناريوهات الشائعة للهجمات.
- دورة حياة الاستجابة للحوادث.
- الاستعداد للحوادث والجاهزية المؤسسية.
- تحديد الحوادث والإبلاغ الأولي عنها.
- تصنيف الحوادث ومستويات الخطورة.
- تقييم نطاق الحادث وتأثيره ودرجة الاستعجال.
- أدوار ومسؤوليات فرق الاستجابة للحوادث.
- التنسيق بين عمليات الأمن والاستجابة للحوادث.
- معايير التصعيد وأولويات الاستجابة.
- سياسات وإجراءات الاستجابة للحوادث.
- التكامل مع إدارة المخاطر المؤسسية.

اليوم الأول — تابع

- التطبيق العملي: تقييم مجموعة من السيناريوهات السيبرانية وتصنيف الحوادث وتحديد مستوى خطورتها وأولويات التصعيد المناسبة.

اليوم الثاني

فرز الحوادث وتحليلها والتحقيق فيها

- التقييم والفرز الأولي للحوادث.
- جمع معلومات الحادث والتحقق منها.
- بناء التسلسل الزمني للحادث.
- تحليل التنبيهات والأدلة الأمنية المتاحة.
- تحديد مؤشرات الاختراق.
- تحديد نطاق الحادث والأصول المتأثرة.
- التحقيق في الحسابات وبيانات الاعتماد المخترقة.
- تحليل أنشطة الأجهزة والشبكات والتطبيقات.
- حفظ الأدلة وتوثيقها.
- بناء فرضيات التحقيق والتحقق منها.
- تنسيق أنشطة التحقيق الفني.
- تحديد الحالات التي تنتقل من حدث أمني إلى حادث مؤكد.
- التطبيق العملي: التحقيق في حادث سيبراني افتراضي وبناء تسلسله الزمني وتحديد الأصول المتأثرة وتحليل الأدلة وتحديد الاستجابة المطلوبة.

اليوم الثالث

الاحتواء والقضاء على التهديد والتعافي

- مبادئ احتواء الحوادث السيبرانية.
- استراتيجيات الاحتواء قصيرة وطويلة الأجل.
- عزل الأنظمة والحسابات المتأثرة.
- إدارة بيانات الاعتماد والوصول المخترق.
- إزالة المكونات الخبيثة وآليات الاستمرارية.
- معالجة الثغرات والأسباب الجذرية.
- الاستعادة الآمنة للأنظمة.
- التحقق من نجاح عملية التعافي ومراقبتها.
- تنسيق التعافي التقني والتشغيلي.
- إدارة الاعتماديات والخدمات الحيوية.
- إعادة الأنظمة إلى التشغيل الطبيعي.
- التحقق الأمني بعد التعافي.
- التطبيق العملي: تطوير وتنفيذ خطة استجابة لحالة اختراق افتراضية تشمل الاحتواء والقضاء على التهديد والتعافي والتحقق وإعادة الخدمات الحيوية إلى العمل.

اليوم الرابع

إدارة الحوادث والاتصالات والاستجابة للأزمات السيبرانية

- إدارة الحوادث السيبرانية على المستوى المؤسسي.
- هياكل إدارة الحوادث والمسؤوليات.
- التنسيق بين الأمن السيبراني وتقنية المعلومات والمخاطر والشؤون القانونية والالتزام والاتصال.

اليوم الرابع — تابع

- التصعيد للإدارة التنفيذية واتخاذ القرارات.
- تقييم تأثير الحادث على الأعمال.
- حماية الخدمات والعمليات الحيوية.
- الاتصالات الداخلية والخارجية أثناء الحوادث.
- التواصل مع الأطراف المعنية والعملاء.
- الاعتبارات التنظيمية والخصوصية والالتزام.
- إدارة المخاطر التشغيلية والسمعة المؤسسية.
- تصعيد الأزمات والإحاطات التنفيذية.
- إدارة سجلات القرارات والحوادث.
- التطبيق العملي: تنفيذ محاكاة لإدارة حادث سيبراني تتضمن تعطل العمليات وتسرب معلومات حساسة وتصعيداً للإدارة التنفيذية واتصالات مع الأطراف المعنية وتعدد أولويات الاستجابة.

اليوم الخامس

إدارة ما بعد الحادث والتمارين والتحسين المستمر

- مبادئ المراجعة بعد الحوادث.
- تحليل الأسباب الجذرية والدروس المستفادة.
- تقييم أداء الاستجابة للحوادث.
- تحديد الفجوات في الأفراد والعمليات والتقنية والحوكمة.
- الإجراءات التصحيحية والوقائية.
- تحديث سياسات وإجراءات الاستجابة للحوادث.
- اختبار قدرات الاستجابة للحوادث.
- تصميم التمارين المكتبية والمحاكاة.

اليوم الخامس — تابع

- قياس الجاهزية ومستوى النضج.
- مؤشرات أداء الاستجابة للحوادث.
- بناء إطار للتحسين المستمر.
- إعداد خارطة طريق لنضج الاستجابة لحوادث الأمن السيبراني.
- الورشة الختامية: تنفيذ محاكاة متكاملة للاستجابة لحادث سيبراني تبدأ من الاكتشاف والفرز الأولي، مروراً بالتحقيق والاحتواء والقضاء على التهديد والتعافي والاتصالات التنفيذية، وصولاً إلى المراجعة بعد الحادث، ثم إعداد خارطة طريق ذات أولويات لتحسين قدرات الاستجابة والجاهزية والمرونة السيبرانية.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/cybersecurity-incident-response-management-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440