QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1983

# دورة تخطيط الاستجابة للحوادث وأدلة الاستجابة وإدارة الأزمات السيبرانية

**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 تخطيط الاستجابة للحوادث وأدلة الاستجابة وإدارة الأزمات السيبرانية إطاراً عملياً واستراتيجياً لإعداد المؤسسات لاكتشاف الحوادث السيبرانية والاستجابة لها واحتوائها والتعافي منها بفاعلية. وتركز الدورة على بناء قدرات منظمة للاستجابة للحوادث بما يضمن التنسيق الفعال بين فرق الأمن السيبراني وتقنية المعلومات والمخاطر والالتزام والإدارة التنفيذية عند مواجهة التهديدات والحوادث الأمنية المؤثرة.

يتناول البرنامج دورة الاستجابة للحوادث بشكل متكامل، بدءاً من الاستعداد والكشف والتحليل، مروراً بالاحتواء والقضاء على التهديد والتعافي، وصولاً إلى المراجعة والتحسين بعد الحادث. كما يتناول تصنيف الحوادث ومعايير التصعيد والأدوار والمسؤوليات وبروتوكولات الاتصال وحفظ الأدلة واتخاذ القرارات واستمرارية الأعمال والتنسيق بين الأطراف الفنية وغير الفنية.

ويركز البرنامج بصورة متقدمة على تطوير أدلة الاستجابة للحوادث واستخدامها بفاعلية. ويتعلم المشاركون كيفية تحويل المخاطر والسيناريوهات السيبرانية المحتملة إلى إجراءات استجابة واضحة وقابلة للتنفيذ، بما يشمل هجمات الفدية والتصيد الاحتيالي واختراق الحسابات والبرمجيات الخبيثة وتسرب البيانات وهجمات حجب الخدمة والتهديدات الداخلية والحوادث المرتبطة بمقدمي الخدمات والأطراف الثالثة.

كما تتناول الدورة إدارة الأزمات السيبرانية على المستوى المؤسسي والتنفيذي، بما في ذلك الحوادث التي تؤثر في استمرارية الأعمال والخدمات الحيوية والمعلومات الحساسة والالتزامات التنظيمية والسمعة المؤسسية. ومن خلال المحاكاة والتمارين المكتبية وتحليل السيناريوهات وورش بناء خطط الاستجابة، يطور المشاركون قدرات عملية تعزز جاهزية المؤسسة ومرونتها السيبرانية.

## أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح مبادئ ودورة حياة الاستجابة لحوادث الأمن السيبراني.
- تقييم مستوى جاهزية المؤسسة للتعامل مع الحوادث والأزمات السيبرانية.

- تطوير خطط منظمة للاستجابة للحوادث بما يتوافق مع المخاطر المؤسسية.
- تحديد مستويات خطورة الحوادث ومعايير التصعيد وأولويات الاستجابة.
- تحديد الأدوار والمسؤوليات بوضوح ضمن فرق الاستجابة للحوادث.
- تصميم أدلة استجابة عملية للسيناريوهات السيبرانية الشائعة.
- تطبيق إجراءات منظمة للكشف عن الحوادث وتحليلها واحتوائها والتعافي منها.
- تعزيز التنسيق بين الأمن السيبراني وتقنية المعلومات والمخاطر والشؤون القانونية والالتزام والاتصال والإدارة التنفيذية.
- تطوير إجراءات فعالة للاتصالات الداخلية والخارجية أثناء الحوادث السيبرانية.
- تقييم التأثيرات التشغيلية والتجارية عند التعامل مع الحوادث الأمنية الكبرى.
- تطبيق المبادئ المناسبة لحفظ الأدلة وتوثيق الحوادث.
- إدارة عملية اتخاذ القرار تحت الضغط أثناء الأزمات السيبرانية عالية التأثير.
- تطوير عمليات تصعيد الأزمات السيبرانية وإخطار الإدارة التنفيذية.
- تنفيذ تمارين مكتبية لاختبار قدرات الاستجابة للحوادث.
- تحديد نقاط الضعف في خطط الاستجابة وأدلة الإجراءات الحالية.
- إنشاء آليات للمراجعة بعد الحوادث والتحسين المستمر.

## الفئة المستهدفة

تستهدف الدورة مديري الأمن السيبراني، ومتخصصي عمليات الأمن، ومتخصصي الاستجابة للحوادث، ومتخصصي أمن المعلومات، ومديري تقنية المعلومات، ومهندسي الأمن، ومتخصصي إدارة التهديدات والثغرات، والعاملين في تطوير أو تشغيل قدرات الاستجابة للحوادث داخل المؤسسات.

كما تناسب المتخصصين في المخاطر والالتزام واستمرارية الأعمال والرقابة الداخلية والشؤون القانونية

والخصوصية والاتصال المؤسسي وإدارة الأزمات، إضافة إلى قادة التقنية والقيادات التنفيذية المشاركة في اتخاذ القرارات المتعلقة بالحوادث السيبرانية أو إدارة الأزمات المؤسسية.

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

## مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- تقييم مستوى نضج قدرات الاستجابة للحوادث في المؤسسة.
- تحديد الأنظمة الحيوية والأطراف المعنية والاعتماديات ومتطلبات الاستجابة.
- بناء خطة متكاملة للاستجابة للحوادث تتضمن مراحل واضحة ومسؤوليات محددة.
- تصنيف الحوادث السيبرانية وفق مستوى الخطورة والتأثير والأولوية.
- تحديد حدود التصعيد وصلاحيات اتخاذ القرارات.
- تطوير أدلة استجابة قابلة للتنفيذ للسيناريوهات السيبرانية ذات الأولوية.
- تنسيق أنشطة الاستجابة الفنية مع المتطلبات التشغيلية والتنفيذية.
- تنظيم الاتصالات أثناء الحوادث مع الأطراف الداخلية والخارجية.
- دعم حفظ الأدلة وتوثيق الحوادث بصورة دقيقة ومنظمة.
- تقييم التأثيرات التشغيلية والمالية والتنظيمية والسمعية للأزمات السيبرانية.
- تنسيق عمليات الاحتواء والقضاء على التهديد والتعافي.
- تنفيذ تمارين مكتبية منظمة وتقييم أداء الاستجابة.

- تحديد الفجوات في الخطط والإجراءات والأدوار والقدرات.
- تطوير إجراءات تصحيحية بعد الحوادث السيبرانية.
- إنشاء مؤشرات لقياس جاهزية وأداء الاستجابة للحوادث.
- إعداد خارطة طريق عملية لتحسين إدارة الأزمات السيبرانية والمرونة المؤسسية.
- المحاور التدريبية

## محاور الدورة

**اليوم الأول**

### أسس الاستجابة للحوادث والجاهزية السيبرانية

- مبادئ الاستجابة لحوادث الأمن السيبراني وأهدافها.
- دورة حياة الاستجابة للحوادث.
- أنواع الحوادث السيبرانية وتصنيفاتها ومستويات خطورتها.
- التعرف على التهديدات والحوادث الأمنية.
- تقييم جاهزية المؤسسة للاستجابة للحوادث.
- أدوار فرق الأمن وفرق الاستجابة للحوادث.
- مسؤوليات تقنية المعلومات والمخاطر والالتزام والشؤون القانونية والاتصال والإدارة.
- تصنيف الحوادث وتحديد أولوياتها.
- معايير التصعيد وحدود الإخطار.
- سياسات الاستجابة للحوادث وحوكمتها.
- التكامل مع استمرارية الأعمال والتعافي من الكوارث.
- بناء الجاهزية المؤسسية للاستجابة للحوادث.

اليوم الأول — تابع

- التطبيق العملي: تنفيذ تقييم لجاهزية الاستجابة للحوادث وتطوير إطار أولي لتصنيف الحوادث وتصعيدها.

**اليوم الثاني**

## تخطيط الاستجابة للحوادث وتطوير أدلة الاستجابة

- هيكل ومكونات خطة الاستجابة للحوادث.
- تحديد أدوار الاستجابة وصلاحيات اتخاذ القرار.
- إجراءات الاستجابة ومسارات العمل.
- تصميم أدلة استجابة عملية للحوادث السيبرانية.
- هيكل دليل الاستجابة ومحفزاته ونقاط القرار وإجراءات التنفيذ.
- الاستجابة لهجمات برمجيات الفدية.
- الاستجابة للتصيد الاحتيالي واختراق بيانات الاعتماد.
- الاستجابة للبرمجيات الخبيثة واختراق أجهزة المستخدمين.
- الاستجابة لتسرب البيانات والوصول غير المصرح به.
- الاستجابة لهجمات حجب الخدمة.
- الاستجابة للتهديدات الداخلية وحوادث الأطراف الثالثة.
- اختبار أدلة الاستجابة وتحديثها وإدارة إصداراتها.
- التطبيق العملي: تطوير دليل استجابة متكامل لسيناريو سيبراني مختار، يتضمن المحفزات والأدوار والإجراءات والتصعيد والاتصالات ومتطلبات التعافي.

اليوم الثالث

## التحقيق في الحوادث والاحتواء والتعافي

- اكتشاف الحوادث والتحقق منها والتحليل الأولي.
- بناء التسلسل الزمني للحادث.
- تحديد الأدلة وحفظها.
- توثيق الحوادث وإدارة سجلاتها.
- استراتيجيات احتواء الحوادث وتحديد أولويات الاستجابة.
- الاحتواء قصير الأجل وطويل الأجل.
- القضاء على التهديد وتحليل الأسباب الجذرية.
- استعادة الأنظمة والخدمات.
- التنسيق بين فرق التقنية وفرق الأعمال.
- إدارة الاعتماديات أثناء عملية التعافي.
- التحقق من أمن الأنظمة بعد الاستعادة.
- الدروس المستفادة والتحليل بعد الحادث.
- التطبيق العملي: تحليل حادث سيبراني افتراضي منذ اكتشافه وحتى احتوائه والتعافي منه، مع توثيق القرارات والأدلة والإجراءات والنتائج.

اليوم الرابع

## إدارة الأزمات السيبرانية والاستجابة التنفيذية

- الانتقال من الحادث السيبراني إلى الأزمة المؤسسية.
- تحديد الأزمات السيبرانية وآليات التصعيد.
- اتخاذ القرارات التنفيذية أثناء الحوادث الكبرى.

اليوم الرابع — تابع

- هياكل إدارة الأزمات والمسؤوليات.
- تقييم تأثير الحادث على الأعمال.
- حماية الخدمات الحيوية والعمليات التشغيلية.
- الاتصالات الداخلية والخارجية أثناء الأزمات.
- التواصل مع العملاء والشركاء والموردين والأطراف المعنية.
- الاعتبارات التنظيمية والقانونية ومتطلبات الخصوصية والالتزام.
- إدارة المخاطر الإعلامية والسمعة المؤسسية.
- إدارة عدم اليقين وتضارب المعلومات.
- إعداد الإحاطات التنفيذية وسجلات قرارات الأزمة.
- التطبيق العملي: تنفيذ محاكاة لأزمة سيبرانية على المستوى التنفيذي تتضمن تعطلاً في الأعمال وتسرب معلومات حساسة واتصالات مع الأطراف المعنية وتعدد أولويات الاستجابة.

**اليوم الخامس**

## التمارين المكتبية واختبار الاستجابة والتحسين المستمر

- مبادئ تصميم تمارين الاستجابة للحوادث.
- إعداد سيناريوهات التمارين المكتبية السيبرانية.
- اختبار خطط الاستجابة وأدلة الإجراءات.
- تقييم التنسيق بين الفرق وجودة اتخاذ القرار.
- قياس فعالية الاستجابة ومستوى الجاهزية.
- تحديد الفجوات في الأفراد والعمليات والتقنية والحوكمة.
- مؤشرات أداء وجاهزية الاستجابة للحوادث.
- إعداد تقارير ما بعد التمرين والإجراءات التصحيحية.

اليوم الخامس — تابع

- تحديث أدلة الاستجابة بناءً على الدروس المستفادة.
- التحسين المستمر ونضج قدرات الاستجابة.
- بناء قدرة مستدامة لإدارة الأزمات السيبرانية.
- إعداد خارطة طريق لتحسين الاستجابة للحوادث.
- الورشة الختامية: تنفيذ تمرين مكتبي متكامل لأزمة سيبرانية يبدأ من الاكتشاف الأولي للحادث، مروراً بالتصعيد التنفيذي والاحتواء والاتصالات وإدارة الأزمة والتعافي، وصولاً إلى المراجعة بعد الحادث، ثم إعداد خارطة طريق ذات أولويات لتحسين الجاهزية والاستجابة والمرونة السيبرانية.

## للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/incident-response-planning-playbooks-cyber-crisis-management-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440