الدورة التدريبية: الاستجابة للحوادث الأمنية والتعافي من الكوارث الرقمية الشاملة

#SM6871

الدورة التدريبية: الاستجابة للحوادث الأمنية والتعافي من الكوارث الرقمية الشاملة

مقدمة الدورة التدريبية / لمحة عامة:

في عالمنا الرقمي المتسارع، لم يعد السؤال "هل ستحدث حادثة أمنية؟" بل "متى ستحدث؟". لذا، أصبحت الاستجابة للحوادث الأمنية والتعافي من الكوارث الرقمية الشاملة من المهارات الأساسية لضمان استمرارية الأعمال وحماية الأصول الحيوية للمؤسسات. هذه الدورة التدريبية المتخصصة مصممة لتزويد المشاركين بالمعرفة والقدرات اللازمة لتطوير وتنفيذ خطط فعالة للاستجابة للحوادث الأمنية والتعافي من الكوارث، بدءًا من اكتشاف التهديد وحتى استعادة العمليات بالكامل. سنتناول منهجيات متقدمة لإدارة الأزمات السيبرانية، وتحليل الأدلة الجنائية الرقمية، وتنفيذ إجراءات التعافي. تستمد الدورة محتواها من خبرات أكاديميين وباحثين بارزين في مجال الأمن السيبراني وإدارة الأزمات، مثل البروفيسور Eugene H. Spafford Eugene H. Spafford، الذي يُعد من الرواد في مجال أمن الحاسوب. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من بناء فرق استجابة قوية، وتطوير خطط متكاملة، وتقليل الأثر السلبي لأي حادثة أمنية أو كارثة رقمية على المؤسسة. سيركز التدريب على الجوانب العملية والتطبيقية، مع تقديم سيناريوهات واقعية وتمارين محاكاة لضمان جاهزية المشاركين للتعامل مع التحديات الأمنية المعقدة بفعالية وثقة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو أمن المعلومات.
- فرق الاستجابة للحوادث الأمنية.
- محللو الأمن السيبراني.
- مديرو البنية التحتية لتقنية المعلومات.
- مسؤولو التعافي من الكوارث واستمرارية الأعمال.
- مدققو أمن المعلومات.
- مديرو المخاطر.

القطاعات والصناعات المستهدفة:

- القطاع الحكومي وما في حكمها.
- القطاع المصرفي والمالي.
- الاتصالات وتقنية المعلومات.
- الرعاية الصحية.
- التصنيع.
- الطاقة والمرافق.
- الخدمات الاستشارية الأمنية.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- إدارة تقنية المعلومات.
- إدارة المخاطر.
- العمليات.
- إدارة استمرارية الأعمال.
- التدقيق الداخلي.
- القسم القانوني.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم دورة حياة الاستجابة للحوادث الأمنية.
- تطوير خطط استجابة فعالة للحوادث السيبرانية.
- تحديد وتقييم الحوادث الأمنية فور وقوعها.
- تنفيذ إجراءات احتواء الحوادث والقضاء عليها.
- إجراء تحليل الأدلة الجنائية الرقمية الأساسية.
- وضع خطط شاملة للتعافي من الكوارث الرقمية.
- اختبار وتحسين خطط الاستجابة والتعافي باستمرار.
- تطبيق أفضل الممارسات والمعايير العالمية في الاستجابة للحوادث.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وتطبيقية مكثفة، تهدف إلى تزويد المشاركين بالمعرفة والخبرة العملية في مجال الاستجابة للحوادث الأمنية والتعافي من الكوارث الرقمية الشاملة. تبدأ المنهجية بمحاضرات تفصيلية يقدمها خبراء متخصصون، تليها جلسات نقاش حيوية لتبادل التحديات والخبرات. تركز الدورة بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المتدربون بتحليل سيناريوهات حوادث أمنية وكوارث رقمية معقدة، وتحديد مسارات الهجوم، وتقييم الأضرار المحتملة. تتضمن المنهجية ورش عمل تطبيقية وتمارين محاكاة عملية، حيث يتدرب المشاركون على إجراءات الاستجابة للحوادث، واستخدام أدوات تحليل الأدلة الجنائية، وتفعيل خطط التعافي من الكوارث. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتعزيز التفكير النقدي وقدرات اتخاذ القرار تحت الضغط. يتم تقديم تغذية راجعة فردية ومستمرة لضمان اكتساب المهارات المطلوبة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات اللازمة للتعامل مع أي طارئ أمني بثقة وكفاءة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الاستجابة للحوادث الأمنية

- مفهوم الحوادث الأمنية وأنواعها.
- دورة حياة الاستجابة للحوادث (التحضير، الاكتشاف والتحليل، الاحتواء، الإزالة، الاستعادة، الدروس المستفادة).
- أهمية فرق الاستجابة للحوادث (CSIRT/CERT).
- الأطر والمعايير الدولية للاستجابة للحوادث (مثل NIST SP 800-61).
- بناء فريق الاستجابة للحوادث وتحديد الأدوار والمسؤوليات.
- التحديات الشائعة في إدارة الحوادث الأمنية.
- أهمية التواصل الفعال أثناء الحوادث.

الوحدة الثانية: اكتشاف الحوادث وتحليلها واحتوائها

- أدوات وتقنيات اكتشاف الحوادث (SIEM، IDS/IPS).
- جمع الأدلة الرقمية وتحليلها.
- تقنيات تحليل البرمجيات الخبيثة.
- أساليب الاحتواء الفوري للحوادث.
- عزل الأنظمة المتأثرة.
- تتبع مصادر الهجوم.
- التحليل الجنائي الأساسي للبيانات.

الوحدة الثالثة: إزالة الحوادث والاستعادة والتتبع

- إجراءات إزالة التهديدات من الأنظمة.
- إعادة بناء الأنظمة المتأثرة.
- التحقق من خلو الأنظمة من التهديدات.
- توثيق الحادث ونتائجه.
- خطوات الاستعادة بعد الحادث.
- التعافي التشغيلي بعد الهجمات السيبرانية.
- التنسيق مع الأطراف الخارجية (القانون، السلطات).

الوحدة الرابعة: التخطيط للتعافي من الكوارث واستمرارية الأعمال

- مفاهيم التعافي من الكوارث (DR) واستمرارية الأعمال (BC).
- تحليل تأثير الأعمال (BIA).
- تقييم المخاطر في سياق التعافي من الكوارث.
- تطوير خطط التعافي من الكوارث (DRP).
- مواقع التعافي (الباردة، الدافئة، الساخنة).
- تقنيات النسخ الاحتياطي والاستعادة المتقدمة.
- التخطيط للاتصالات أثناء الكوارث.

الوحدة الخامسة: اختبار الخطط وتحسينها وإدارة الأزمات

- أنواع اختبارات خطط الاستجابة والتعافي (المحاكاة، التدريبات الجدولية).
- أهمية التحديث والمراجعة الدورية للخطط.
- مؤشرات الأداء الرئيسية لفعالية الاستجابة والتعافي.
- إدارة الأزمات السيبرانية والتواصل الاستراتيجي.
- الدروس المستفادة من الحوادث والكوارث.
- الامتثال للمعايير واللوائح في التعافي من الكوارث.
- التعامل مع التحديات المستقبلية في الاستجابة والتعافي.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20–25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور المتسارع للتهديدات السيبرانية، كيف يمكن للمؤسسات أن توازن بين الاستجابة السريعة للحوادث وضرورة إجراء تحليل عميق وشامل لضمان التعافي الكامل ومنع تكرار الحوادث المستقبلية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العملي والشمولي على الاستجابة للحوادث الأمنية والتعافي من الكوارث الرقمية الشاملة، مما يوفر للمشاركين فهماً عميقاً وإعداداً شاملاً للتعامل مع الطوارئ السيبرانية. لا تقتصر الدورة على المفاهيم النظرية، بل تركز على التطبيق العملي من خلال دراسات حالة واقعية وتمارين محاكاة مكثفة، مما يتيح للمتدربين تجربة سيناريوهات حقيقية وتطبيق المهارات المكتسبة مباشرة. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث المنهجيات والأدوات في مجال الاستجابة للحوادث وإدارة الكوارث. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا محترفين قادرين على حماية المؤسسات من التهديدات السيبرانية، وتقليل أوقات التوقف، وضمان استمرارية الأعمال في مواجهة أي تحدٍ رقمي.