الدورة التدريبية: الاستجابة للحوادث الأمنية والتعافي من الكوارث الرقمية الشاملة

يوليو ٢٠٢٦ ٣٠ - ٢٦

عمان

(للشخص الواحد) € ٤١٠٠

Ref: #SM6871_74904

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

- 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.
- الاستجابة للحوادث. تطبيق أفضل الممارسات والمعايير العالمية في

منهجية الدورة التدريبية:

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

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 ٨٠٠-٦١).
- 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).

واستمرارية الأعمال الوحدة الرابعة: التخطيط للتعافي من الكوارث

- الأعمال (BC). مفاهيم التعافي من الكوارث (DR) واستمرارية
- 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.

الأزمات الوحدة الخامسة: اختبار الخطط وتحسينها وإدارة

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

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

عميق وشامل لضمان يمكن للمؤسسات أن توازن بين الاستجابة السريعة في ظل التطور المتسارع للتهديدات السيبرانية، كيف

التعافي الكامل ومنع تكرار الحوادث المستقبلية؟ للحوادث وضرورة إجراء تحليل

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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