الدورة التدريبية: الاستجابة للحوادث الأمنية والتعافي من الكوارث السيبرانية المتقدمة

#SM7664

الدورة التدريبية: الاستجابة للحوادث الأمنية والتعافي من الكوارث السيبرانية المتقدمة

مقدمة الدورة التدريبية / لمحة عامة:

في ظل المشهد السيبراني المعقد والمتغير باستمرار، أصبحت الاستجابة للحوادث الأمنية والتعافي من الكوارث السيبرانية المتقدمة من المهارات الحيوية لضمان مرونة واستمرارية الأعمال. هذه الدورة التدريبية المتخصصة مصممة لتزويد المشاركين بالمعرفة والمهارات المتقدمة اللازمة لتطوير، وتنفيذ، وإدارة برامج استجابة شاملة للحوادث الأمنية، وخطط تعاف قوية من الكوارث السيبرانية. سنغوص بعمق في منهجيات التعامل مع الهجمات المعقدة، تحليل الأدلة الجنائية الرقمية، واستعادة الأنظمة والبيانات بكفاءة عالية. تستمد الدورة محتواها من خبرات أكاديميين وباحثين بارزين في مجال الأمن السيبراني وإدارة الأزمات، مثل البروفيسور Dorothy Denning Dorothy Denning، التي تُعد من الشخصيات المؤثرة في أمن المعلومات. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من بناء قدرات استباقية وفعالة لمواجهة التهديدات السيبرانية المتطورة، وتقليل الأثر السلبي للحوادث، وضمان التعافي السريع والكامل للمؤسسة. سيركز التدريب على الجوانب التطبيقية المتقدمة، مع تقديم سيناريوهات واقعية وتمارين محاكاة مكثفة، لإعداد المشاركين للتعامل مع أصعب التحديات الأمنية بثقة وخبرة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- قادة فرق الاستجابة للحوادث (CSIRT/CERT).
- مديرو الأمن السيبراني.
- خبراء الأدلة الجنائية الرقمية.
- مسؤولو التعافي من الكوارث واستمرارية الأعمال.
- كبار محللي الأمن السيبراني.
- مديرو تقنية المعلومات.
- الاستشاريون في الأمن السيبراني.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- القطاع الحكومي والدفاع.
- البنى التحتية الحيوية.
- شركات الاتصالات ومزودو الخدمات.
- الرعاية الصحية.
- شركات التكنولوجيا والبرمجيات.
- المؤسسات الكبيرة ومتعددة الجنسيات.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- فرق الاستجابة للحوادث الأمنية.
- إدارة تقنية المعلومات.
- إدارة المخاطر.
- إدارة استمرارية الأعمال والتعافي من الكوارث.
- قسم التدقيق الأمني.
- العمليات الأمنية (SOC).

أهداف الدورة التدريبية:

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

- تطوير وإدارة برنامج استجابة شامل للحوادث الأمنية.
- إجراء تحليل متقدم للحوادث الأمنية وتحديد نطاقها.
- التعامل مع الهجمات السيبرانية المعقدة والمستمرة (APTs).
- تنفيذ تقنيات متقدمة لجمع الأدلة الجنائية الرقمية وتحليلها.
- تصميم وتنفيذ خطط تعاف فعالة من الكوارث السيبرانية.
- إدارة الأزمات السيبرانية والتواصل الاستراتيجي.
- تقييم وتحسين أداء برامج الاستجابة والتعافي باستمرار.
- تطبيق الإطار القانوني والتنظيمي المتعلق بالاستجابة للحوادث.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وعملية متقدمة، تهدف إلى بناء قدرات احترافية في مجال الاستجابة للحوادث الأمنية والتعافي من الكوارث السيبرانية المتقدمة. تبدأ المنهجية بمحاضرات متعمقة يقدمها خبراء رواد في الأمن السيبراني، يليها نقاشات جماعية تحليلية لحالات واقعية معقدة. تركز الدورة بشكل مكثف على دراسات الحالة المتقدمة وتمارين المحاكاة التفاعلية، حيث يقوم المشاركون بتولي أدوار قيادية في سيناريوهات هجمات سيبرانية معقدة، وتطبيق منهجيات متقدمة لاكتشاف التهديدات، واحتوائها، والقضاء عليها، واستعادة الأنظمة. تتضمن المنهجية ورش عمل تطبيقية لاستخدام أدوات متخصصة في تحليل الأدلة الجنائية الرقمية وتخطيط التعافي من الكوارث. يشجع BIG BEN Training Center العمل الجماعي وتبادل الخبرات بين المشاركين لتعزيز الابتكار والقدرة على حل المشكلات تحت الضغط. يتم تقديم تغذية راجعة فردية ومفصلة لضمان تطوير أقصى إمكانات كل متدرب. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات والخبرة القيادية اللازمة لإدارة الأزمات السيبرانية بنجاح وضمان مرونة الأعمال في مواجهة أي تهديد.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: الإدارة الاستراتيجية لبرامج الاستجابة للحوادث

- تطوير استراتيجية الاستجابة للحوادث على مستوى المؤسسة.
- بناء وتأهيل فرق الاستجابة للحوادث السيبرانية المتقدمة.
- دمج الاستجابة للحوادث مع إدارة المخاطر والحوكمة.
- قياس أداء برامج الاستجابة للحوادث.
- المتطلبات القانونية والتنظيمية للاستجابة للحوادث.
- التخطيط المسبق للسيناريوهات المعقدة.
- التعاون مع الأطراف الخارجية (إنفاذ القانون، الموردين).

الوحدة الثانية: التحليل المتقدم للحوادث والأدلة الجنائية الرقمية

- تقنيات متقدمة لاكتشاف التهديدات المستمرة (APTs).
- تحليل البرمجيات الخبيثة المتقدمة.
- جمع وتحليل الأدلة من الأنظمة المختلفة (الشبكة، المضيفات، السحابة).
- أدوات ومنهجيات الأدلة الجنائية الرقمية.
- تحليل السجلات (Logs) والبيانات الكبيرة (Big Data) لتحديد الحوادث.
- تتبع المهاجمين وتقنياتهم.
- إعداد تقارير الأدلة الجنائية للاستخدام القانوني.

الوحدة الثالثة: استراتيجيات الاحتواء والقضاء على الهجمات المعقدة

- احتواء الهجمات المستمرة والمعقدة.
- تقنيات الإزالة المتقدمة للتهديدات الخفية.
- إدارة التصحيحات والثغرات الأمنية في سياق الحوادث.
- التعامل مع هجمات الفدية وتشفير البيانات.
- استعادة الأنظمة المتضررة بشكل آمن.
- أتمتة عمليات الاحتواء والإزالة.
- تأمين نقاط الضعف لمنع تكرار الهجوم.

الوحدة الرابعة: التعافي المتقدم من الكوارث السيبرانية واستمرارية الأعمال

- تصميم خطط تعافٍ متقدمة للكوارث الرقمية.
- استراتيجيات النسخ الاحتياطي والاستعادة للأنظمة الكبيرة والمعقدة.
- اختبار خطط التعافي من الكوارث على نطاق واسع.
- إدارة سلسلة التوريد في سياق التعافي من الكوارث.
- التعافي من الهجمات التي تستهدف البنية التحتية الحرجة.
- التخطيط للتعافي في بيئات الحوسبة السحابية.
- تقييم مرونة الأعمال بعد الكوارث.

الوحدة الخامسة: إدارة الأزمات والدروس المستفادة والتوجهات المستقبلية

- إدارة الأزمات السيبرانية على مستوى الإدارة العليا.
- استراتيجيات التواصل أثناء الأزمات مع الجمهور وأصحاب المصلحة.
- الدروس المستفادة من الحوادث والكوارث لتحسين الأمن.
- بناء ثقافة المرونة السيبرانية داخل المؤسسة.
- التوجهات المستقبلية في التهديدات والاستجابة للحوادث.
- الذكاء الاصطناعي والتعلم الآلي في الاستجابة للحوادث.
- التخطيط الاستباقي لمستقبل الأمن السيبراني.

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 عصر يزداد فيه تعقيد الهجمات السيبرانية وسرعتها، كيف يمكن للمؤسسات أن تطور برامج استجابة للحوادث تكون ديناميكية بما يكفي لتتجاوز مجرد الرد على التهديدات، لتصبح محركًا للتعلم المستمر والتحسين الأمني المستدام؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتقديمها لمستوى متقدم وشامل في الاستجابة للحوادث الأمنية والتعافي من الكوارث السيبرانية المتقدمة، مما يميزها عن الدورات الأساسية أو المتخصصة في جانب واحد. نحن نركز على تمكين المشاركين من قيادة وإدارة برامج استجابة معقدة، مع التركيز على التعامل مع التهديدات المتقدمة وتحليل الأدلة الجنائية بمهارة عالية. تعتمد الدورة على منهجية تطبيقية مكثفة، تتضمن تمارين محاكاة واقعية ودراسات حالة متقدمة، مما يوفر للمتدربين خبرة عملية لا تقدر بثمن في بيئة تدريبية آمنة. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث الابتكارات والاستراتيجيات في مجال الأمن السيبراني. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا قادة قادرين على مواجهة أصعب التحديات الأمنية، وضمان استمرارية الأعمال وحمايتها من الكوارث السيبرانية بفعالية استثنائية.