الدورة التدريبية: الاستجابة للحوادث السيبرانية ـ خطة الطوارئ للمؤسسات

#CYB5052

الدورة التدريبية: الاستجابة للحوادث السيبرانية ـ خطة الطوارئ للمؤسسات

مقدمة الدورة التدريبية / لمحة عامة:

في عالم يزداد فيه تعقيد التهديدات السيبرانية، لم يعد السؤال هو "هل ستتعرض مؤسستك لهجوم؟" بل "متى ستتعرض؟". تُعد الاستجابة للحوادث السيبرانية عنصرًا حاسمًا في مرونة الأعمال واستمرارية العمليات لأي مؤسسة. تقدم هذه الدورة التدريبية المتخصصة خطة طوارئ شاملة للمؤسسات، مزودة المهنيين بالمعرفة والمهارات اللازمة لإدارة الحوادث الأمنية بفعالية، من الاكتشاف الأولي وحتى التعافي الكامل. سنتعمق في مراحل الاستجابة للحوادث، التحقيق الجنائي الرقمي، واستراتيجيات التواصل أثناء الأزمات. سيتعلم المشاركون كيفية بناء فريق استجابة للحوادث (CSIRT)، ووضع سياسات وإجراءات الاستجابة للحوادث، والامتثال للمعايير الدولية ذات الصلة. تهدف الدورة إلى تمكين المؤسسات من تقليل الأضرار الناجمة عن الهجمات السيبرانية، وحماية سمعتها، واستعادة العمليات بسرعة. يستند المحتوى إلى أحدث الأطر المعيارية، مثل NIST Special Publication 800–61، وإسهامات خبراء أكاديميين بارزين مثل البروفيسور يوجين سبافورد (Eugene Spafford)، المعروف بأعماله الرائدة في أمن المعلومات والتحقيق في الحوادث. يقدم BIG BEN Training Center هذه الدورة لمساعدة المؤسسات على بناء قدرات استجابة سيبرانية قوية وفعالة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصو الأمن السيبراني.
- مديرو تكنولوجيا المعلومات وأنظمة المعلومات.
- أعضاء فرق الاستجابة للحوادث الأمنية (CSIRT).
- مديرو المخاطر والامتثال.
- مدققو أمن المعلومات.
- أي مسؤول عن الأمن التشغيلي واستمرارية الأعمال.

القطاعات والصناعات المستهدفة:

- القطاع الحكومي والهيئات العامة وما في حكمها لـأمن البنية التحتية الوطنية.
- القطاع المالي والمصرفي لحماية الأنظمة المصرفية من الهجمات.
- قطاع الاتصالات والتكنولوجيا.
- الرعاية الصحية لحماية بيانات المرضى الحساسة.
- قطاع الطاقة والمرافق الحيوية.
- شركات تطوير البرمجيات.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة تكنولوجيا المعلومات.
- إدارة المخاطر والامتثال.
- الإدارة القانونية (للتشاور بشأن الجوانب القانونية للحوادث).
- إدارة العمليات واستمرارية الأعمال.
- العلاقات العامة (للتواصل أثناء الأزمات).

أهداف الدورة التدريبية:

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

- فهم مراحل دورة حياة الاستجابة للحوادث السيبرانية.
- القدرة على إنشاء وتطوير خطة استجابة للحوادث فعالة.
- تحديد علامات الاختراق (Indicators of Compromise) واكتشاف الحوادث.
- إجراء التحقيق الجنائي الرقمي الأساسي وجمع الأدلة.
- تطبيق استراتيجيات احتواء الحوادث والتخفيف من آثارها.
- وضع خطط التعافي وإعادة البناء بعد الحوادث.
- التواصل الفعال أثناء الأزمات الأمنية داخليًا وخارجيًا.

منهجية الدورة التدريبية:

تتبنى هذه الدورة التدريبية منهجية عملية ومكثفة تركز على التطبيق المباشر لمفاهيم الاستجابة للحوادث السيبرانية. سيتمكن المشاركون من خلال ورش العمل التفاعلية وتمارين المحاكاة الواقعية من تجربة سيناريوهات حوادث أمنية مختلفة، من اختراق البيانات إلى هجمات برامج الفدية. تتضمن المنهجية دراسات حالة تفصيلية لحوادث سيبرانية كبرى، مع تحليل كيفية استجابة المؤسسات لها وما يمكن تعلمه. سيتم التركيز على الأدوات والتقنيات المستخدمة في التحقيق الجنائي الرقمي وإدارة الأدلة. يقدم BIG BEN Training Center بيئة تعليمية محفزة، تمكن المشاركين من بناء خطط استجابة للطوارئ قابلة للتنفيذ. يتم تشجيع العمل الجماعي والنقاشات لتبادل الخبرات وتطوير حلول جماعية لتحديات الاستجابة للحوادث.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الاستجابة للحوادث ودورة الحياة

- مقدمة إلى الاستجابة للحوادث السيبرانية.
- أهمية خطة الاستجابة للطوارئ.
- مراحل دورة حياة الاستجابة للحوادث (الإعداد، الاكتشاف والتحليل، الاحتواء، الاستئصال، التعافي، الدروس المستفادة).
- بناء فريق الاستجابة للحوادث الأمنية (CSIRT).
- الأدوار والمسؤوليات في فريق الاستجابة.
- تطوير سياسات وإجراءات الاستجابة للحوادث.
- مفاهيم المرونة السيبرانية.

الوحدة الثانية: الاكتشاف والتحليل للتهديدات السيبرانية

- مصادر اكتشاف الحوادث الأمنية.
- علامات الاختراق (Indicators of Compromise – IoCs).
- أدوات اكتشاف التهديدات (SIEM, EDR).
- تحليل سجلات الأحداث (Logs Analysis).
- تقنيات تحليل البرمجيات الخبيثة (Malware Analysis) الأساسية.
- تحليل حركة مرور الشبكة.
- التصنيف الأولي للحوادث.

الوحدة الثالثة: الاحتواء والاستئصال والتعافي من الحوادث

- استراتيجيات احتواء الحوادث الأمنية.
- إجراءات عزل الأنظمة المصابة.
- خطوات الاستئصال وإزالة التهديد.
- التعافي وإعادة بناء الأنظمة المتأثرة.
- فحص الثغرات الأمنية بعد الحادث.
- استعادة البيانات من النسخ الاحتياطية.
- إجراءات ما بعد الحادث.

الوحدة الرابعة: التحقيق الجنائي الرقمي وجمع الأدلة

- أساسيات التحقيق الجنائي الرقمي (Digital Forensics).
- مبادئ الحفاظ على الأدلة الرقمية.
- أدوات جمع الأدلة وتحليلها.
- تحليل الذاكرة (Memory Forensics).
- تحليل الأقراص الصلبة (Disk Forensics).
- تقرير التحقيق الجنائي.
- الجوانب القانونية لجمع الأدلة.

الوحدة الخامسة: التواصل وإدارة الأزمات والدروس المستفادة

- استراتيجيات التواصل الفعال أثناء الأزمات الأمنية.
- التواصل مع أصحاب المصلحة الداخليين والخارجيين.
- العلاقات العامة في حالة اختراق البيانات.
- الامتثال للمتطلبات التنظيمية للإبلاغ عن الحوادث.
- الدروس المستفادة من الحوادث الأمنية.
- تحديث خطة الاستجابة للحوادث بناءً على الخبرة.
- إدارة سمعة المؤسسة بعد الحوادث.

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 المستمر للتهديدات السيبرانية، وكيف يمكن للمؤسسات أن تضمن أن خطة الاستجابة للحوادث الخاصة بها ليست مجرد وثيقة، بل هي نظام حي يتطور ويتكيف مع التهديدات الجديدة، مما يحول كل حادث إلى فرصة لتعزيز مرونتها السيبرانية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل والعملي على الاستجابة للحوادث السيبرانية، وتقديم خطة طوارئ متكاملة للمؤسسات. بدلاً من مجرد عرض المفاهيم، نغوص في التطبيق العملي لمراحل الاستجابة، من الاكتشاف إلى التعافي. نركز على التحقيق الجنائي الرقمي وجمع الأدلة، وهي مهارات حاسمة للتعامل مع أي حادث أمني. تتضمن الدورة محاكاة لسيناريوهات حوادث حقيقية، مما يمنح المشاركين خبرة عملية لا تقدر بثمن في اتخاذ القرارات تحت الضغط. إنها ليست مجرد دورة نظرية، بل هي تدريب عملي يهدف إلى بناء فرق استجابة للحوادث قادرة على حماية المؤسسات وتقليل الأضرار في مواجهة التهديدات السيبرانية المتطورة.