التدريبية: الاستجابة للحوادث السيبرانية -
خطة الطوارئ للمؤسسات الدورة

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

شرم الشيخ

(للشخص الواحد) € ٤١٠٠

Ref: #CYB5052_564041

مقدمة الدورة التدريبية / لمحة عامة:

السيبرانية يعد السؤال هو "هل ستتعرض مؤسستك لهجوم؟" بل "متى في عالم يزداد فيه تعقيد التهديدات السيبرانية، لم لأي مؤسسة. تقدم هذه الدورة التدريبية عنصرًا حاسمًا في مرونة الأعمال واستمرارية ستتعرض؟". تُعد الاستجابة للحوادث الأولي وحتى المهنيين بالمعرفة والمهارات اللازمة لإدارة المتخصصة خطة طوارئ شاملة للمؤسسات، مزودة العمليات الجنائي الرقمي، واستراتيجيات التعافي الكامل. سنتعمق في مراحل الاستجابة الحوادث الأمنية بفعالية، من الاكتشاف بناء فريق استجابة للحوادث (CSIRT)، ووضع سياسات التواصل أثناء الأزمات. سيتعلم المشاركون كيفية للحوادث، التحقيق الهجمات السيبرانية، الدولية ذات الصلة. تهدف الدورة إلى تمكين المؤسسات وإجراءات الاستجابة للحوادث، والامتثال للمعايير إلى أحدث الأطر المعيارية، مثل NIST وحماية سمعتها، واستعادة العمليات بسرعة. يستند من تقليل الأضرار الناجمة عن (Eugene أكاديميين بارزين مثل البروفيسور يوجين سبافورد ، وإسهامات خبراء ٨٠٠-٦١ Special Publication المحتوى على Training Center أمن المعلومات والتحقيق في الحوادث. يقدم BIG BEN الرائدة في ، المعروف بأعماله (Spafford بناء قدرات استجابة سيبرانية قوية وفعالة. هذه الدورة لمساعدة المؤسسات

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

- البنية التحتية الوطنية. القطاع الحكومي والهيئات العامة وما في حكمها لـأمن
- من الهجمات. القطاع المالي والمصرفي لـحماية الأنظمة المصرفية
- 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.
- للحوادث). الإدارة القانونية (للتشاور بشأن الجوانب القانونية
- إدارة العمليات واستمرارية الأعمال.
- العلاقات العامة (للتواصل أثناء الأزمات).

أهداف الدورة التدريبية:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الحياة الوحدة الأولى: أساسيات الاستجابة للحوادث ودورة

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

السيبرانية الوحدة الثانية: الاكتشاف والتحليل للتهديدات

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

الحوادث الوحدة الثالثة: الاحتواء والاستئصال والتعافي من

- 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.

المستفادة الوحدة الخامسة: التواصل وإدارة الأزمات والدروس

- 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:

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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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