المتقدمة الدورة التدريبية: الاستجابة للحوادث الأمنية والتعافي من الكوارث السيبرانية

اغسطس ٢٠٢٦ ٢٨ - ٢٤

كوالالمبور

(للشخص الواحد) € ٥٢٠٠

Ref: #SM7664_329237

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الاستجابة للحوادث الوحدة الأولى: الإدارة الاستراتيجية لبرامج

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

الجنائية الرقمية الوحدة الثانية: التحليل المتقدم للحوادث والأدلة

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

الهجمات المعقدة الوحدة الثالثة: استراتيجيات الاحتواء والقضاء على

- 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.

السيبرانية واستمرارية الأعمال الوحدة الرابعة: التعافي المتقدم من الكوارث

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

والتوجهات المستقبلية الوحدة الخامسة: إدارة الأزمات والدروس المستفادة

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

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 ٢٠٢٥- 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:

يكفي لتتجاوز مجرد وسرعتها، كيف يمكن للمؤسسات أن تطور برامج استجابة في عصر يزداد فيه تعقيد الهجمات السيبرانية

والتحسين الأمني المستدام؟ الرد على التهديدات، لتصبح محركًا للتعلم المستمر للحوادث تكون ديناميكية بما

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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