التدريبية: حماية بيانات الشركات - الدليل
الشامل للمديرين التنفيذيين الدورة

يونيو ٢٠٢٦ ٠٥ - ٠١

كوالالمبور

(للشخص الواحد) € ٥٢٠٠

Ref: #CYB3888_266249

مقدمة الدورة التدريبية / لمحة عامة:

للمؤسسات ليس الشركات تمثل أولوية قصوى للمديرين التنفيذيين في ظل التطور الرقمي المتسارع، أصبحت حماية بيانات واستمرارية الأعمال. هذه الدورة مجرد قضية تقنية، بل هو جزء لا يتجزأ من الحوكمة الذين يدركون أن الأمن السيبراني الرقمية. ستتناول العميقة والاستراتيجيات الفعالة لتعزيز الأمن التدريبية مصممة خصيصًا لتزويد القادة بالمعرفة المؤسسية والامتثال التنظيمي للبيانات. سيكتشف الدورة أطر عمل الأمن السيبراني، إدارة المخاطر السيبراني للشركات وحماية الأصول الدورة مؤسساتهم، وكيفية تقييم الثغرات الأمنية، ووضع خطط المشاركون كيف يمكنهم بناء ثقافة أمنية قوية داخل الأمنية، التهديدات السيبرانية أساسية لأي مدير تنفيذي يسعى لضمان أمن المعلومات الاستجابة للحوادث السيبرانية. تُعد هذه والأطر المعيارية، مع الإشارة إلى مساهمات المتزايدة. يستند المحتوى إلى أحدث الممارسات الحساسة لشركته في مواجهة كبيرة في شميدت (Howard Schmidt)، الذي كان مستشار الأمن خبراء بارزين في هذا المجال، مثل البروفيسور هوارد العالمية تمكين القادة من Training Center استراتيجيات الأمن السيبراني. يقدم BIG BEN السيبراني للرئيس الأمريكي وله إسهامات وتحقيق مرونة سيبرانية عالية. اتخاذ قرارات مستنيرة بشأن أمن البيانات المؤسسية هذه الدورة بهدف

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- المديرون التنفيذيون في مختلف القطاعات.
- أعضاء مجالس الإدارة والقيادات العليا.
- مديرو تكنولوجيا المعلومات ومديرو الأمن السيبراني.
- المسؤولون عن الامتثال وحوكمة البيانات.
- الأمن السيبراني. مديرو المخاطر الذين يرغبون في فهم أعمق لمخاطر
- السيبراني. المستشارون الإداريون المتخصصون في استشارات الأمن

القطاعات والصناعات المستهدفة:

- المالية. القطاع المالي والمصرفي لحماية بيانات العملاء
- الأنظمة التشغيلية. قطاع الطاقة والبنية التحتية الحيوية لتأمين
- الرعاية الصحية لحماية البيانات الصحية السرية.
- تعتمد على البيانات الضخمة. الاتصالات والتكنولوجيا نظرًا لطبيعة أعمالها التي
- المعلومات السيادية. القطاع الحكومي والهيئات العامة وما في حكمها لأمن
- التشغيلية والملكية الفكرية. الصناعات التحويلية التي تعتمد على البيانات

الأقسام المؤسسية المستهدفة:

- الأمن السيبراني. الإدارة العليا ومجلس الإدارة لوضع استراتيجيات
- الأمنية. إدارة تقنية المعلومات والأمن لتنفيذ السياسات
- السيبرانية. إدارة المخاطر والامتثال لتقييم المخاطر
- للقوانين. الإدارة القانونية لوضع السياسات والامتثال
- للموظفين. إدارة الموارد البشرية لتطوير الوعي الأمني

أهداف الدورة التدريبية:

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

- على الشركات. فهم المشهد الحالي للتهديدات السيبرانية وتأثيرها
- ومواجهة التحديات الأمنية. تطوير استراتيجيات فعالة لحماية بيانات الشركات
- وتطبيقها. التعرف على أطر عمل الأمن السيبراني الرائدة
- منها. القدرة على تقييم المخاطر الأمنية ووضع خطط للتخفيف
- فهم أهمية الحوكمة الأمنية والامتثال التنظيمي.
- بناء ثقافة أمنية قوية داخل المؤسسة.
- الأزمات. وضع خطط الاستجابة للحوادث السيبرانية وإدارة

منهجية الدورة التدريبية:

المفتوحة، ودراسات نحو الحلول، تضع المديرين التنفيذيين في قلب عملية تتبنى هذه الدورة منهجية تدريبية تفاعلية وموجهة التعامل معها، وتمارين المحاكاة التي تحاكي الحالة الواقعية التي تستعرض اختراقات البيانات التعلم. نركز على المناقشات الجماعي من تحليل أمثلة على حوادث الأمن السيبراني، وتطوير سيناريوهات الهجمات السيبرانية. سيتمكن المشاركون وكيفية توفر الدورة بيئة داعمة للأسئلة لتبادل الخبرات وتطوير حلول جماعية للتحديات خطط استجابة عملية. يتم تشجيع العمل يلتزم BIG BEN Training Center بتقديم والنقاشات حول أفضل الممارسات في الأمن السيبراني الأمنية المشتركة. يتم العملي، مما يضمن أن يكتسب القادة الأدوات والمعرفة محتوى عالي الجودة يجمع بين النظرية والتطبيق المؤسسي. الشاملة لضمان استمرارية الأعمال. التركيز على كيفية دمج الأمن السيبراني في اللازمة لتعزيز مرونة مؤسساتهم السيبرانية. استراتيجية العمل

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

وتحديات الأعمال الوحدة الأولى: المشهد العام للأمن السيبراني

- تعريف الأمن السيبراني من منظور تنفيذي.
- التهديدات السيبرانية الحديثة التي تواجه الشركات.
- تأثير اختراقات البيانات على سمعة الأعمال وقيمتها.
- الأمن السيبراني كجزء من استراتيجية الأعمال.
- المخاطر السيبرانية على المستوى التنظيمي.
- دور القيادة في الحوكمة السيبرانية.
- أهمية تقييم المخاطر السيبرانية.

الممارسات الوحدة الثانية: أطر عمل الأمن السيبراني وأفضل

- (مثل NIST و.(ISO ٢٧٠٠١ نظرة عامة على أطر عمل الأمن السيبراني الرائدة
- تطبيق مبادئ الأمن السيبراني في بيئة الشركات.
- إدارة الثغرات الأمنية على مستوى المؤسسة.
- التحكم في الوصول وأمن الهوية.
- أمن سلسلة التوريد.
- أمن التطبيقات والبرمجيات.
- الامتثال لمعايير الأمن السيبراني.

الوحدة الثالثة: حماية البيانات وإدارة المخاطر

- تصنيف البيانات وحمايتها.
- سياسات حماية البيانات وخصوصية المعلومات.
- تقييم المخاطر السيبرانية وتحليلها.
- تخفيف المخاطر وبناء دفاعات سيبرانية قوية.
- النسخ الاحتياطي للبيانات وخطط التعافي من الكوارث.
- أمن البيانات في السحابة.
- حماية الملكية الفكرية الرقمية.

وإدارة الأزمات الوحدة الرابعة: الاستجابة للحوادث السيبرانية

- وضع خطة الاستجابة للحوادث السيبرانية.
- التعامل مع اختراقات البيانات والإبلاغ عنها.
- التحقيق الجنائي الرقمي الأساسي.
- التواصل أثناء الأزمات الأمنية.
- استمرارية الأعمال بعد الحوادث.
- إدارة سمعة الشركة في الأزمات.
- فرق الاستجابة للحوادث الأمنية.

الأمن السيبراني الوحدة الخامسة: القيادة، الثقافة، والامتثال في

- السيبراني. دور المدير التنفيذي في تعزيز ثقافة الأمن
- تدريب الموظفين على الوعي الأمني.
- و.(CCPA الامتثال للوائح حماية البيانات (مثل GDPR
- المتطلبات القانونية والتنظيمية للأمن السيبراني.
- إدارة أمن المعلومات كقيمة استراتيجية.
- التعاون مع خبراء الأمن السيبراني الخارجيين.
- الاستثمار في حلول 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 ٢٠-٢٥ 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:

الملحة للابتكار الرقمي وتصبح أكثر تعقيدًا، كيف يمكن للمديرين التنفيذيين في عالم تتطور فيه التهديدات السيبرانية باستمرار النمو المستدام للمؤسسة مع حماية أصولها الرقمية والحفاظ على أقصى درجات الأمن السيبراني، لضمان الموازنة بين الحاجة بشكل فعال؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

يواجهونها في حماية خصيصًا للمديرين التنفيذيين، مما يضمن أن المحتوى تتميز هذه الدورة بتركيزها الاستراتيجي الموجه في الاستراتيجية العامة للأعمال، بيانات شركاتهم. نحن نقدم رؤى عميقة حول كيفية دمج يلامس التحديات الفعلية التي مما الدورة على الحوكمة السيبرانية، إدارة المخاطر على بدلاً من التعامل معه كمجرد مشكلة تقنية. تركز الأمن السيبراني لاختراقات البيانات الشهيرة، مع يميزها عن الدورات التقنية البحتة. نقدم دراسات مستوى القيادة، والامتثال التنظيمي للبيانات، بل إلى يوفر دروسًا قيمة قابلة للتطبيق. هذه الدورة لا تحليل كيفية استجابة الشركات الرائدة لها، مما حالة حقيقية للمؤسسة وتعزيز تمكينهم من اتخاذ قرارات استراتيجية مستنيرة تساهم تهدف فقط إلى تزويد المشاركين بالمعلومات، مرونتها ضد الهجمات المستقبلية. في تقوية الدفاعات السيبرانية