الدورة التدريبية: تطوير وتنفيذ سياسات الأمن السيبراني للشركات والمؤسسات

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

الدار البيضاء

(للشخص الواحد) € ٤١٠٠

Ref: #SM3355_576352

مقدمة الدورة التدريبية / لمحة عامة:

والمؤسسات. السيبراني العمود الفقري لحماية الأصول الرقمية في عصر التحول الرقمي المتسارع، أصبحت سياسات الأمن بالمعرفة والمهارات اللازمة لتطوير، هذه الدورة التدريبية المتخصصة مصممة لتزويد وضمان استمرارية الأعمال في الشركات حياة السياسة تتوافق مع أحدث المعايير والممارسات العالمية. تنفيذ، وصيانة سياسات أمن سيبراني قوية وفعالة المشاركين بالصياغة والاعتماد، وصولا إلى النشر والتوعية الأمنية، بدءًا من تحديد المتطلبات، مرورًا سنتناول من خلالها جميع مراحل دورة Matt Bishop Matt خبراء بارزين في مجال أمن المعلومات، مثل الدكتور والمراجعة الدورية. تستمد الدورة محتواها من خبرات تمكين المهنيين هذه الدورة Training Center مرجعًا في فهم أسس أمن الأنظمة. يقدمBIG BEN ، الذي تُعد أعمالBishop الأمني بين التهديدات السيبرانية المتزايدة، ويضمن الامتثال من بناء إطار عمل سياساتي متين يحمي المؤسسات من بهدف عملية تساعد المشاركين على الموظفين. سيركز التدريب على الجوانب العملية، مع للوائح التنظيمية، ويعزز ثقافة الوعي مؤسساتهم. ترجمة المفاهيم النظرية إلى واقع ملموس داخل تقديم أمثلة وتطبيقات

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديرو أمن المعلومات.
- مسؤولو الأمن السيبراني.
- خبراء الامتثال والحوكمة.
- مديرو تقنية المعلومات.
- مديرو المشاريع التقنية.
- مستشارو أمن المعلومات.
- المسؤولون عن وضع السياسات المؤسسية.

القطاعات والصناعات المستهدفة:

- قطاع الخدمات المالية.
- قطاع الرعاية الصحية.
- قطاع الاتصالات.
- القطاع الحكومي وما في حكمها.
- الصناعات التكنولوجية.
- شركات الطاقة.
- قطاع الخدمات الاستشارية.
- المؤسسات التعليمية.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- إدارة تقنية المعلومات.
- إدارة المخاطر والامتثال.
- القسم القانوني.
- إدارة الموارد البشرية.
- إدارة التدقيق الداخلي.
- الإدارة العليا.

أهداف الدورة التدريبية:

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

- المؤسسات. فهم أهمية سياسات الأمن السيبراني ودورها في حماية
- فعالة. تحديد المتطلبات الأساسية لتطوير سياسات أمنية
- صياغة سياسات وإجراءات أمن سيبراني واضحة وشاملة.
- تنفيذ آليات لضمان تطبيق السياسات الأمنية.
- مراجعة وتحديث السياسات الأمنية بشكل دوري.
- تعزيز الوعي بالسياسات الأمنية بين جميع الموظفين.
- ضمان الامتثال للوائح والمعايير الدولية والمحلية.
- قياس فعالية السياسات الأمنية وتحسينها المستمر.

منهجية الدورة التدريبية:

في مجال تطوير وتنفيذ وتطبيقية، تهدف إلى تزويد المشاركين بالمعرفة تعتمد هذه الدورة التدريبية على منهجية تفاعلية بمحاضرات تفصيلية يقدمها خبراء في أمن سياسات الأمن السيبراني للشركات والمؤسسات. تبدأ والخبرة العملية اللازمة المتدربون بتبادل التحديات والخبرات. تركز الدورة بشكل كبير المعلومات، تليها جلسات نقاش حيوية تسمح للمشاركين المنهجية تحسينات. تتضمن المنهجية ورش بتحليل سياسات أمنية قائمة، وتحديد نقاط القوة على دراسات الحالة الواقعية، حيث يقوم إجراءات تنفيذها، وتصميم برامج توعية عمل مكثفة حيث يمارس المشاركون صياغة سياسات أمنية والضعف فيها، واقتراح الجماعي والتعاون بين المتدربين لتطوير حلول مبتكرة العمل BIG BEN Training Center للموظفين. يشجع محددة، وتطوير مؤسساتهم وهم لضمان اكتساب المهارات المطلوبة. تهدف هذه المنهجية وعملية. يتم تقديم تغذية راجعة فردية ومستمرة قوية ومرنة تحمي أصولهم الرقمية مسلحون بالمعرفة والأدوات اللازمة لتطوير وتنفيذ إلى تمكين المشاركين من العودة إلى بفعالية. سياسات أمن سيبراني

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

وأهميتها الوحدة الأولى: أساسيات سياسات الأمن السيبراني

- البيانات. مفهوم سياسات الأمن السيبراني ودورها في حماية
- أهمية السياسات الأمنية في إطار الحوكمة والامتثال.
- التكاملية، التوافر. المفاهيم الأساسية لأمن المعلومات: السرية،
- الأمنية. العلاقة بين السياسات والإجراءات والمعايير
- أنواع السياسات الأمنية الشائعة.
- تحديد نطاق ومتطلبات السياسات الأمنية.
- قوية. أثر التهديدات السيبرانية على الحاجة إلى سياسات

الوحدة الثانية: مراحل تطوير سياسات الأمن السيبراني

- تحديد أصحاب المصلحة ودورهم في صياغة السياسات.
- جمع المتطلبات وتحليلها.
- المحتوى). صياغة مسودات السياسات الأمنية (اللغة، الهيكل،
- عمليات المراجعة والاعتماد للسياسات.
- أدوات وقوالب تطوير السياسات.
- تجنب الأخطاء الشائعة في صياغة السياسات.
- ربط السياسات بالأهداف الاستراتيجية للمؤسسة.

الوحدة الثالثة: تنفيذ ونشر سياسات الأمن السيبراني

- خطة نشر السياسات وتعميمها.
- برامج التوعية والتدريب على السياسات الأمنية.
- آليات فرض الالتزام بالسياسات.
- دمج السياسات في العمليات التشغيلية اليومية.
- أدوات إدارة السياسات الأمنية.
- التواصل الفعال حول السياسات الجديدة.
- إدارة الاستثناءات والانحرافات عن السياسات.

الدورية للسياسات الوحدة الرابعة: الامتثال والتدقيق والمراجعة

- ربط السياسات باللوائح والمعايير (مثل ISO ٢٧٠٠١، GDPR).
- إجراء التدقيقات الداخلية لضمان الامتثال.
- التحضير للتدقيقات الخارجية.
- مراجعة وتحديث السياسات الأمنية بشكل دوري.
- قياس فعالية السياسات وأثرها على الأمن.
- معالجة حالات عدم الامتثال.
- التحسين المستمر لدورة حياة السياسة.

وتطبيقات عملية الوحدة الخامسة: سياسات أمن سيبراني متقدمة

- سياسات أمن البيانات والخصوصية.
- سياسات الاستجابة للحوادث والتعافي من الكوارث.
- سياسات استخدام الأجهزة الشخصية (BYOD).
- سياسات الأمن السحابي وأمن تطبيقات الويب.
- سياسات أمن سلسلة التوريد.
- دراسات حالة عملية لتطوير وتنفيذ السياسات.
- تحديات مستقبلية في تطوير السياسات الأمنية.

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:

الجديدة والمتطورة، مع السيبراني الخاصة بها مرنة وقابلة للتكيف مع كيف يمكن للمؤسسات ضمان أن تظل سياسات الأمن

الحفاظ على فعاليتها وتوافقها مع الأهداف التجارية؟ التهديدات التكنولوجية

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

عن الدورات التي تكتفي تطوير وتنفيذ سياسات الأمن السيبراني للشركات تتميز هذه الدورة بتركيزها العملي والعميق على
السياسة بالكامل، بدءًا من التخطيط ووصولا بتقديم مفاهيم عامة. نقدم نهجًا شموليًا يغطي دورة والمؤسسات، مما يميزها
الدورة على أمثلة كيفية ترجمة المتطلبات التنظيمية والمخاطر إلى إلى المراجعة والتحسين المستمر، مع التركيز على حياة
فرصة لتطبيق المفاهيم النظرية عملية من الصناعات المختلفة ودراسات حالة واقعية، سياسات قابلة للتطبيق. تعتمد
من BIG BEN Training Center ، أن يكتسب في سياقات عملية. يضمن المحتوى الأكاديمي المتقدم، مما يمنح المشاركين
لا تهدف فقط إلى اللازمة لإنشاء وتنفيذ سياسات أمنية قوية تحمي المتدربون ليس فقط المعرفة، بل أيضًا المهارات المقدم
قادة قادرين على بناء بيئات رقمية آمنة تزويد المشاركين بالمعلومات، بل إلى تمكينهم مؤسساتهم بفعالية. هذه الدورة
ومرنة. ليصبحوا