الدورة التدريبية: إدارة الأمن السيبراني المتقدمة للمؤسسات

#SM8832

الدورة التدريبية: إدارة الأمن السيبراني المتقدمة للمؤسسات

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التطور المتسارع للتهديدات السيبرانية، لم تعد إدارة الأمن السيبراني مجرد مهمة تقنية، بل أصبحت ركيزة أساسية لاستمرارية الأعمال وسلامة المعلومات في المؤسسات. تتجاوز هذه الدورة المفاهيم الأساسية لتقدم رؤى عميقة واستراتيجيات متقدمة لإدارة الأمن السيبراني بشكل فعال وشامل. من خلال استكشاف أحدث التحديات والحلول، سيتعلم المشاركون كيفية بناء دفاعات سيبرانية قوية، وإدارة المخاطر بكفاءة، وتطبيق أفضل الممارسات الدولية. تركز الدورة على الجوانب العملية والتطبيقية، مستندة إلى أطر عمل معترف بها عالميًا مثل إطار عمل المعهد الوطني للمعايير والتقنية (NIST Cybersecurity Framework)، وتستلهم من أعمال خبراء بارزين في هذا المجال، مثل الدكتور Howard Schmidt Howard Schmidt الذي كان مستشار الأمن السيبراني الخاص بالبيت الأبيض. يقدم BIG BEN Training Center هذه الدورة المصممة خصيصًا لتزويد القادة والمتخصصين بالمعرفة والمهارات اللازمة لقيادة مبادرات الأمن السيبراني بنجاح، وضمان حماية الأصول الرقمية للمؤسسات في بيئة متغيرة باستمرار. سيتناول المشاركون تحليل التهديدات السيبرانية الناشئة، وتطوير استراتيجيات الاستجابة للحوادث، وإدارة الامتثال للوائح الأمن السيبراني، بالإضافة إلى تعزيز ثقافة الأمن السيبراني داخل مؤسساتهم.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو تقنية المعلومات.
- مديرو الأمن السيبراني.
- مسؤولو أمن المعلومات.
- متخصصو الامتثال والمخاطر.
- مستشارين الأمن السيبراني.
- مديرو المشاريع التقنية.
- القادة وصناع القرار في المؤسسات.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الرعاية الصحية.
- شركات الطاقة والمرافق.
- قطاع الاتصالات.
- القطاعات الحكومية وما في حكمها.
- شركات التكنولوجيا والبرمجيات.
- المؤسسات التعليمية والبحثية.
- شركات الصناعات التحويلية.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة الأمن السيبراني.
- إدارة المخاطر والامتثال.
- القسم القانوني.
- الإدارة العليا.
- قسم الموارد البشرية (فيما يتعلق بوعي الموظفين بالأمن السيبراني).
- إدارة العمليات التشغيلية.

أهداف الدورة التدريبية:

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

- تطوير استراتيجيات شاملة لإدارة الأمن السيبراني.
- تقييم المخاطر السيبرانية وتحديد أولوياتها بشكل فعال.
- تصميم وتنفيذ سياسات وإجراءات أمن المعلومات.
- إدارة الاستجابة للحوادث الأمنية والتعافي منها.
- ضمان الامتثال للمعايير واللوائح الدولية للأمن السيبراني.
- بناء فرق عمل قوية في مجال الأمن السيبراني.
- تطبيق أحدث التقنيات والحلول الأمنية.
- تعزيز الوعي بالأمن السيبراني في جميع مستويات المؤسسة.

منهجية الدورة التدريبية:

تتبنى هذه الدورة التدريبية منهجية تفاعلية وتطبيقية تهدف إلى تمكين المشاركين من اكتساب فهم عميق ومهارات عملية في إدارة الأمن السيبراني. تعتمد المنهجية على مزيج من المحاضرات التفاعلية التي يقدمها خبراء متخصصون، يليها نقاشات جماعية مفتوحة لتشجيع تبادل الخبرات والمعارف بين المشاركين. تُقدم دراسات حالة واقعية من بيئات عمل مختلفة، مما يتيح للمتدربين تحليل التحديات الأمنية الفعلية وتطبيق الحلول المناسبة. يتم التركيز بشكل كبير على التمارين العملية وورش العمل، حيث يقوم المشاركون بتطبيق المفاهيم النظرية على سيناريوهات محاكاة، مثل تقييم نقاط الضعف، وتطوير خطط الاستجابة للحوادث، وإعداد تقارير المخاطر. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتطوير حلول مبتكرة للمشكلات المعقدة. يتم توفير تغذية راجعة مستمرة وفردية لضمان تطور المهارات. تهدف هذه المنهجية إلى بناء قدرات قوية لدى المتدربين ليصبحوا قادة فعالين في مجال إدارة الأمن السيبراني، قادرين على مواجهة التحديات الأمنية المعاصرة بثقة وكفاءة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أسس ومفاهيم إدارة الأمن السيبراني في المؤسسات

- مقدمة إلى إدارة الأمن السيبراني وأهميتها.
- فهم التهديدات السيبرانية المتزايدة وأنواع الهجمات.
- مبادئ الأمن السيبراني: السرية، التكاملية، التوافر.
- نماذج وأطر عمل الأمن السيبراني (مثل NIST، ISO 27001).
- تطوير رؤية واستراتيجية الأمن السيبراني للمؤسسة.
- مؤشرات الأداء الرئيسية (KPIs) للأمن السيبراني.
- تكامل الأمن السيبراني مع استراتيجية الأعمال.

الوحدة الثانية: تقييم وإدارة المخاطر السيبرانية

- مفهوم المخاطر السيبرانية وعناصرها.
- منهجيات تقييم المخاطر (Qualitative and Quantitative).
- تحديد الأصول الحساسة وتقييم قيمتها.
- تحليل الثغرات ونقاط الضعف.
- تطوير استراتيجيات تخفيف المخاطر والتحكم فيها.
- إدارة مخاطر الجهات الخارجية وسلاسل التوريد.
- مراقبة المخاطر السيبرانية والإبلاغ عنها.

الوحدة الثالثة: حوكمة الأمن السيبراني والامتثال

- أهمية حوكمة الأمن السيبراني في المؤسسات.
- بناء هيكل حوكمة فعال للأمن السيبراني.
- دور اللجان التنفيذية ومجلس الإدارة في الأمن السيبراني.
- الامتثال للوائح والقوانين المحلية والدولية (مثل GDPR، CCPA).
- تطوير سياسات وإجراءات الأمن السيبراني.
- إدارة التدقيق والامتثال الداخلي والخارجي.
- المسؤولية القانونية والأخلاقية في الأمن السيبراني.

الوحدة الرابعة: الاستجابة للحوادث والتعافي من الكوارث

- مراحل دورة حياة الاستجابة للحوادث السيبرانية.
- تطوير خطة الاستجابة للحوادث (IRP).
- فرق الاستجابة للحوادث الأمنية (CSIRT/CERT).
- تقنيات التحقيق الجنائي الرقمي.
- إدارة الاتصالات أثناء الحوادث.
- خطط التعافي من الكوارث واستمرارية الأعمال.
- التدريبات والمحاكاة لاختبار خطط الاستجابة.

الوحدة الخامسة: تقنيات متقدمة وإدارة الأمن التشغيلي

- أمن الشبكات والخوادم المتقدم.
- أمن تطبيقات الويب وقواعد البيانات.
- إدارة الهوية والوصول (IAM).
- أمن الحوسبة السحابية (Cloud Security).
- الذكاء الاصطناعي وتعلم الآلة في الأمن السيبراني.
- أمن إنترنت الأشياء (IoT Security) وأنظمة التحكم الصناعي (ICS).
- التهديدات الداخلية وكيفية إدارتها.

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:

كيف يمكن للمؤسسات تحقيق التوازن بين الابتكار التكنولوجي المتسارع والحفاظ على مستوى عالٍ من الأمن السيبراني في بيئة التهديدات المتطورة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العميق على الجوانب الإدارية والاستراتيجية للأمن السيبراني، متجاوزةً مجرد الجوانب التقنية. نقدم للمشاركين رؤى شاملة حول كيفية دمج الأمن السيبراني كجزء لا يتجزأ من استراتيجية العمل الكلية، وليس كمجرد وظيفة دعم. تعتمد الدورة على منهجية تطبيقية تعزز الفهم النظري بالخبرة العملية، من خلال تحليل دراسات حالة معقدة وورش عمل تفاعلية تحاكي سيناريوهات التهديدات الحقيقية. بدلاً من التركيز على الأدوات والبرامج المحددة، نركز على المفاهيم الجوهرية والمنهجيات القابلة للتطبيق في أي بيئة تكنولوجية. كما يضمن فريق المدربين، من ذوي الخبرة الأكاديمية والعملية الطويلة في مجال إدارة الأمن السيبراني، تقديم محتوى عالي الجودة ومعاصر. يهدف BIG BEN Training Center من خلال هذه الدورة إلى إعداد قادة قادرين على مواجهة التحديات السيبرانية المعقدة، وقيادة فرقهم بفعالية لحماية الأصول الرقمية وضمان استمرارية الأعمال في عالم دائم التغير.