الدورة التدريبية: خبير أمن المعلومات والحوكمة الرقمية المتقدمة للمؤسسات



28 ديسمبر 2026 - 01 يناير 2027
بوسطن
7500 € (للشخص الواحد)
Ref: #IT4439_375613

مقدمة الدورة التدريبية / لمحة عامة:

في العصر الرقمي المتسارع، لم يعد أمن المعلومات مجرد تحدٍ تقني، بل أصبح ركيزة أساسية للحوكمة الرقمية وضمان استمرارية الأعمال وحماية الأصول الحيوية للمؤسسات. تتزايد التهديدات السيبرانية وتتطور باستمرار، مما يفرض على المؤسسات تبني استراتيجيات شاملة لأمن المعلومات تتوافق مع الأطر التنظيمية والمعايير العالمية. هذه الدورة التدريبية مصممة لتزويد المشاركين بالمعرفة والمهارات اللازمة ليصبحوا خبراء في مجال أمن المعلومات والحوكمة الرقمية، بدءاً من فهم المفاهيم الأساسية للأمن السيبراني وصولاً إلى تطبيق أفضل الممارسات في إدارة المخاطر والامتثال. سيتعمق المشاركون في تحليل الهجمات السيبرانية، وتطوير استراتيجيات الدفاع، وتطبيق أطر الحوكمة لضمان الشفافية والمساءلة في البيئة الرقمية. إن مفهوم "الأمن ليس غاية، بل عملية مستمرة" الذي طرحه البروفيسور هوارد شميدت (Howard Schmidt)، المستشار السابق للأمن السيبراني للرئيس الأمريكي، يؤكد على الطبيعة الديناميكية لهذا المجال. يلتزم BIG BEN Training Center بتقديم تدريب متكامل يجمع بين النظريات المتقدمة والتطبيقات العملية، لتمكين قادة الأمن والمختصين من بناء أنظمة دفاعية قوية، ووضع سياسات حوكمة رقمية فعالة، وحماية البيانات والمعلومات الحساسة من أي تهديدات محتملة، مما يعزز الثقة والامتثال المؤسسي في المشهد الرقمي المعقد.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء أمن المعلومات.
- متخصصو الأمن السيبراني.
- مسؤولو الامتثال والمخاطر.
- مدققو نظم المعلومات.
- مدراء تقنية المعلومات.
- المستشارون في مجال الأمن والحوكمة الرقمية.
- المحامون والمشرعون في القانون الرقمي.
- المهندسون والمطورون المعنيون بأمن الأنظمة.
- قادة الأعمال الذين يرغبون في فهم أعمق لأمن المعلومات.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- قطاع الاتصالات.
- القطاع الحكومي والعام.
- قطاع الرعاية الصحية.
- شركات التكنولوجيا والبرمجيات.
- شركات الطاقة والمرافق.
- قطاع التجزئة والتجارة الإلكترونية.
- شركات الاستشارات الأمنية.
- المؤسسات التعليمية والبحثية.

الأقسام المؤسسية المستهدفة:

- أقسام أمن المعلومات.
- أقسام تقنية المعلومات.
- أقسام إدارة المخاطر والامتثال.
- أقسام التدقيق الداخلي والخارجي.
- الأقسام القانونية.
- أقسام الحوكمة المؤسسية.
- أقسام تطوير الأعمال والمنتجات الرقمية.
- أقسام العمليات التشغيلية.

أهداف الدورة التدريبية:

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

- وضع استراتيجيات شاملة لأمن المعلومات تتوافق مع أهداف المؤسسة.
- تطبيق أطر الحوكمة الرقمية ومعايير الامتثال الدولية.
- تحديد وتقييم ومعالجة المخاطر الأمنية بشكل فعال.
- تطوير وتنفيذ سياسات وإجراءات الأمن السيبراني.
- إدارة حوادث الأمن والاستجابة لها بفعالية.
- فهم تحديات أمن الحوسبة السحابية والبيانات الضخمة.
- تطبيق مبادئ الخصوصية وحماية البيانات الشخصية.
- الاستفادة من تقنيات الذكاء الاصطناعي في تعزيز الأمن السيبراني.
- إعداد خطط التعافي من الكوارث واستمرارية الأعمال.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة التدريبية على منهجية تدريبية متطورة تجمع بين المعرفة النظرية العميقة والتطبيق العملي المكثف، لضمان بناء خبراء في أمن المعلومات والحوكمة الرقمية. تشمل المنهجية محاضرات تفاعلية يقدمها نخبة من الخبراء في مجال الأمن السيبراني، بالإضافة إلى ورش عمل مكثفة تركز على السيناريوهات الواقعية، حيث يقوم المشاركون بتطبيق المفاهيم المكتسبة لحل مشكلات أمنية معقدة. يتم التركيز على دراسات الحالة الفعلية التي تعرض لأحدث التهديدات السيبرانية وأفضل أساليب الدفاع، مما يمنح المشاركين رؤى عملية حول كيفية بناء نظم دفاعية مرنة. كما تتضمن الدورة جلسات محاكاة للهجمات السيبرانية والاستجابة للحوادث، لتدريب المشاركين على التعامل مع الأزمات الأمنية بفعالية. الهدف هو تزويد المشاركين بمهارات تحليلية ونقدية تمكنهم من صياغة استراتيجيات أمنية متكاملة، وإدارة المخاطر، وضمان الامتثال للمعايير التنظيمية، والمساهمة بفاعلية في حماية الأصول الرقمية لمؤسساتهم في ظل التحديات الأمنية المتزايدة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن المعلومات ومفاهيم الحوكمة الرقمية.

- مقدمة لأمن المعلومات والأمن السيبراني.
- مفاهيم ومبادئ الحوكمة الرقمية.
- أهمية أمن المعلومات والحوكمة في المؤسسات الحديثة.
- التهديدات والهجمات السيبرانية الشائعة.
- المخاطر الأمنية وتصنيفاتها.
- دور الإنسان في سلسلة الأمن السيبراني.
- أخلاقيات الأمن السيبراني.

الوحدة الثانية: استراتيجيات وتقنيات أمن المعلومات المتقدمة.

- أنظمة إدارة أمن المعلومات (ISMS) ومعيار ISO 27001.
- أمن الشبكات والاتصالات.
- أمن التطبيقات وقواعد البيانات.
- التشفير وإدارة المفاتيح.
- أنظمة كشف ومنع التسلل (IDS/IPS).
- أمن الحوسبة السحابية.
- أمن إنترنت الأشياء (IoT) والأنظمة التشغيلية (OT).

الوحدة الثالثة: إدارة المخاطر الأمنية والاستجابة للحوادث.

- منهجيات تقييم المخاطر الأمنية.
- تحليل الثغرات وإدارة نقاط الضعف.
- خطط الاستجابة للحوادث الأمنية.
- التحقيق الجنائي الرقمي (Digital Forensics).
- التعافي من الكوارث واستمرارية الأعمال.
- إدارة الأزمات الأمنية.
- فرق الاستجابة للطوارئ الحاسوبية (CSIRT).

الوحدة الرابعة: أطر الحوكمة الرقمية والامتثال التنظيمي.

- أطر الحوكمة الأمنية مثل NIST وCOBIT.
- الامتثال للوائح حماية البيانات (GDPR، CCPA).
- أمن المعلومات والقوانين المحلية والدولية.
- إدارة الهوية والوصول (IAM).
- التحكم في الوصول والأذونات.
- تدقيق أمن المعلومات وتقييم الامتثال.
- التقارير الأمنية والامتثال للجهات التنظيمية.

الوحدة الخامسة: مستقبل أمن المعلومات والاتجاهات الحديثة.

- الذكاء الاصطناعي والتعلم الآلي في الأمن السيبراني.
- أمن البلوك تشين والعملات الرقمية.
- التهديدات المتقدمة المستمرة (APTs).
- الأمن السلوكي (Behavioral Security).
- الخصوصية بال تصميم (Privacy by Design).
- العمليات الأمنية المدارة (Managed Security Services).
- التعاون الدولي في مكافحة الجريمة السيبرانية.

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:

في عالم تتسارع فيه وتيرة التهديدات السيبرانية وتتعقد أطر الحوكمة الرقمية، كيف يمكن للمؤسسات ضمان بناء مرونة أمنية مستدامة تتجاوز مجرد الامتثال وتصل إلى التنبؤ بالمخاطر والابتكار في الدفاع؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديمها رؤية شاملة وعميقة لمفاهيم أمن المعلومات والحوكمة الرقمية، متجاوزةً بذلك الدورات التي تركز على جانب واحد فقط. نحن لا نقدم مجرد معلومات حول الأدوات والتقنيات، بل نركز على تمكين المشاركين من صياغة استراتيجيات أمنية متكاملة وبناء أطر حوكمة فعالة تتلاءم مع التحديات الحالية والمستقبلية. ترتكز الدورة على دراسات حالة واقعية وتحليل معمق لسيناريوهات أمنية معقدة، مما يمنح المتدربين فهماً عملياً لكيفية تطبيق المفاهيم النظرية في بيئات العمل الحقيقية. كما نركز على دمج أحدث الاتجاهات مثل الذكاء الاصطناعي في الأمن السيبراني، وإدارة المخاطر المعقدة، وأهمية الامتثال للوائح الدولية. إن هذا المزيج الفريد من المعرفة الأكاديمية العميقة والتدريب العملي المكثف، بالإضافة إلى التركيز على التفكير الاستراتيجي في مجال الأمن، يضمن للمشاركين اكتساب مهارات قيادية تمكنهم من حماية الأصول الرقمية لمؤسساتهم بفاعلية وثقة.