الدورة التدريبية: الأمن السيبراني الاستراتيجي لمدراء التقنية

#CS3979

الدورة التدريبية: الأمن السيبراني الاستراتيجي لمدراء التقنية

مقدمة الدورة التدريبية / لمحة عامة:

تقدم الدورة التدريبية في الأمن السيبراني الاستراتيجي للقيادات التقنية: من الحماية إلى الريادة رؤية متكاملة لتحديات العصر الرقمي، حيث صُممت خصيصاً لتمكين رؤساء التكنولوجيا من قيادة تحول أمني استباقي. يستفيد المشاركون من منهجية "من الصفر إلى الواحد" التي تدمج بين الأسس النظرية وتطبيقات إدارة المخاطر السيبرانية في القطاعات الحيوية. يسلط البرنامج الضوء على أحدث استراتيجيات الدفاع ضد التهديدات الإلكترونية المعقدة، مع التركيز على حوكمة الأمن السيبراني وفقاً للمعايير العالمية. يشمل المحتوى تحليلات لحالات دراسية حقيقية في قطاعات البنوك والرعاية الصحية، مستنداً إلى أبحاث الخبير العالمي بروس شناير(Bruce Schneier) في تصميم أنظمة الحماية الذكية. يقدم BIG BEN Training Center هذه الدورة التفاعلية التي تركز على تطوير سياسات أمنية متكاملة قابلة للتطبيق الفوري، مع تحديثات حول التشريعات المحلية والدولية المؤثرة على بيئة العمل.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- رؤساء أقسام التكنولوجيا.
- المدراء التنفيذيون للمعلومات.
- قادة فرق الأمن السيبراني.
- مسؤولو حوكمة تقنية المعلومات.
- مدراء إدارة المخاطر المؤسسية.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- قطاع الرعاية الصحية.
- شركات الطاقة والبنية التحتية.
- قطاع الاتصالات وتكنولوجيا المعلومات.
- الهيئات الحكومية والجهات شبه الحكومية.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- أقسام الأمن السيبراني.
- إدارة المخاطر والامتثال.
- التخطيط الاستراتيجي المؤسسي.
- شؤون الحوكمة والرقابة.

أهداف الدورة التدريبية:

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

- تحليل التهديدات السيبرانية الناشئة وتأثيرها على الاستقرار المؤسسي.
- تصميم استراتيجيات حوكمة أمنية متوافقة مع التشريعات المحلية والدولية.
- قيادة فرق الأمن السيبراني في إدارة الحوادث الإلكترونية المعقدة.
- تطوير سياسات أمن المعلومات القابلة للتطبيق في القطاعات الحيوية.
- تقييم البنى التحتية الأمنية واقتراح تحسينات استباقية.

منهجية الدورة التدريبية:

تعتمد الدورة على منهجية تفاعلية تجمع بين المحاضرات الأكاديمية وورش العمل التطبيقية، مع التركيز على دراسات الحالة الواقعية من قطاعات متنوعة مثل البنوك والرعاية الصحية. يشمل البرنامج جلسات عصف ذهني جماعي لتحليل سيناريوهات إدارة المخاطر السيبرانية، وتصميم خطط الاستجابة للحوادث. يتم تنفيذ تمارين محاكاة لإدارة الأزمات الإلكترونية، مع تقديم تغذية راجعة فورية من خبراء .BIG BEN Training Center كما تتضمن الجلسات مناقشات حول تحديثات التشريعات الأمنية العالمية وتأثيرها على استراتيجيات الدفاع السيبراني، مع تطبيقات عملية على سياسات حوكمة أمن المعلومات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات القيادة الأمنية في العصر الرقمي

- مقدمة في التهديدات السيبرانية المتطورة للقطاعات الاستراتيجية.
- أدوار رؤساء التكنولوجيا في بناء الثقافة الأمنية.
- الإطار التشريعي الدولي للأمن السيبراني.
- تحليل مسؤوليات القيادة أثناء الأزمات الإلكترونية.
- دراسة حالة: اختراق البنى التحتية الحيوية.
- التحديات الأخلاقية في إدارة البيانات الحساسة.
- تحديثات لوائح NIST و.ISO 27001

الوحدة الثانية: استراتيجيات حوكمة وإدارة المخاطر

- تصميم أنظمة حوكمة الأمن السيبراني.
- تقنيات تقييم الثغرات في الشبكات المعقدة.
- آليات رصد التهديدات الداخلية والخارجية.
- دمج إدارة المخاطر مع التخطيط المؤسسي.
- دراسة حالة: قطاع الرعاية الصحية.
- معايير تقارير الامتثال التنظيمي.
- ورشة عمل: تطوير مؤشرات أداء رئيسية أمنية.

الوحدة الثالثة: الدفاع المتقدم ضد التهديدات الإلكترونية

- أحدث أدوات كشف التسلل والاستجابة.
- استراتيجيات التخفيف من هجمات التصيد والبرمجيات الخبيثة.
- تأمين أنظمة الذكاء الاصطناعي وإنترنت الأشياء.
- الاستعداد لهجمات ransomware المتطورة.
- محاكاة إدارة حادث اختراق شامل.
- تقييم فعالية حلول الأمن السحابي.
- التحديثات الأمنية للأنظمة الوراثية.

الوحدة الرابعة: سياسات الأمن وبناء القدرات المؤسسية

- تصميم سياسات أمن المعلومات القابلة للتطبيق.
- آليات تدريب فرق العمل على الوعي الأمني.
- معايير حماية البيانات الشخصية والخصوصية.
- إدارة الوصول الهوياتي المتقدم.
- دراسة حالة: القطاع المالي.
- نماذج نضج القدرات الأمنية.
- ورشة: صياغة وثائق سياسات أمنية.

الوحدة الخامسة: التخطيط الاستراتيجي واستشراف المستقبل

- دمج الأمن السيبراني في التخطيط المؤسسي.
- قياس العائد على الاستثمار في مبادرات الأمن.
- استشراف اتجاهات التهديدات السيبرانية المستقبلية.
- الاستعداد لتحديات الأمن في التحول الرقمي.
- بناء شراكات مع جهات الاستجابة للحوادث.
- دراسة حالة: الهيئات الحكومية.
- تطوير خطة تحول أمني لمدة 3 سنوات.

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 موازنة متطلبات الابتكار التكنولوجي مع تشديد إجراءات الأمن السيبراني دون إعاقة النمو المؤسسي؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تركز الدورة على البعد الاستراتيجي الفريد في تعامل القيادات التقنية مع التحديات الأمنية، متجاوزةً الأدوات التقنية إلى آليات صنع القرار المعقدة. من خلال منهجية "من الصفر إلى الواحد"، تقدم رؤى عملية في تحويل الأمن السيبراني من وظيفة دعم إلى محرك ريادة مؤسسية، مع استشراف تحديات مثل الذكاء الاصطناعي والتشريعات الناشئة. تعتمد على دراسات حالة من قطاعات حيوية كالبنوك والرعاية الصحية، مع تحديثات حول معايير حوكمة الأمن العالمية. يدمج المحتوى بين الأطر الأكاديمية الرصينة وتطبيقات إدارة المخاطر السيبرانية في السيناريوهات الواقعية، مما يمكّن القيادات من تطوير سياسات أمنية متكاملة قابلة للتنفيذ الفوري في بيئاتهم المؤسسية.