التدريبية: الأمن السيبراني الاستراتيجي

لمدراء التقنية الدورة

يوليو ٢٠٢٦ ١٠ - ٠٦

كاليفورنيا

(للشخص الواحد) ٧٩٠٠ €

Ref: #CS3979_399526

مقدمة الدورة التدريبية / لمحة عامة:

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

لمن الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

منهجية الدورة التدريبية:

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

التدريبية) خريطة المحتوى التدريبي (محاور الدورة

الرقمي الوحدة الأولى: أساسيات القيادة الأمنية في العصر

- الاستراتيجية : مقدمة في التهديدات السيبرانية المتطورة للقطاعات
- أدوار رؤساء التكنولوجيا في بناء الثقافة الأمنية :
- الإطار التشريعي الدولي للأمن السيبراني :
- الإلكترونية : تحليل مسؤوليات القيادة أثناء الأزمات
- دراسة حالة: اختراق البنى التحتية الحيوية :
- التحديات الأخلاقية في إدارة البيانات الحساسة :
- تحديثات لوائح NIST و ISO ٢٧٠٠١

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
- الخبيثة: استراتيجيات التخفيف من هجمات التصيد والبرمجيات
- 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

المستقبل الوحدة الخامسة: التخطيط الاستراتيجي واستشراف

- 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 ٣ سنوات

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 :

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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