الدورة التدريبية: الأمن السيبراني في القطاع المالي - امتثال وحماية الأنظمة المصرفية



16 - 20 نوفمبر 2026
كيب تاون
4600 € (للشخص الواحد)
Ref: #CYB1141_421221

مقدمة الدورة التدريبية / لمحة عامة:

يمثل الأمن السيبراني في القطاع المالي تحديًا بالغ الأهمية نظرًا للحساسية الشديدة للبيانات المالية واعتماد القطاع المتزايد على الأنظمة الرقمية. هذه الدورة التدريبية المتقدمة مصممة خصيصًا للمتخصصين والعاملين في المؤسسات المالية، بهدف تعزيز فهمهم العميق لمخاطر الأمن السيبراني المصرفي وكيفية حماية الأنظمة المصرفية الحيوية. سنتناول في هذه الدورة أطر الامتثال المالي، أمن المعاملات الإلكترونية، والتعامل مع الاحتيال المالي السيبراني. سيكتسب المشاركون الخبرة اللازمة لتطبيق أفضل الممارسات الأمنية، وتطوير استراتيجيات حماية البيانات المصرفية، وضمان الامتثال للوائح المالية الصارمة. تهدف الدورة إلى تزويد المشاركين بالقدرة على تحديد الثغرات الأمنية في الأنظمة المالية، وتطبيق حلول الأمن السيبراني المتقدمة. يستند المحتوى إلى أحدث التطورات في مجال الأمن السيبراني المصرفي، مع الاستفادة من خبرات أكاديميين بارزين مثل البروفيسور آلان بوجون (Alan Paller)، مؤسس SANS Institute، الذي له إسهامات كبيرة في تدريب الأمن السيبراني وتطوير القوى العاملة الأمنية. يقدم BIG BEN Training Center هذه الدورة لتمكين المتخصصين في القطاع المالي من بناء دفاعات سيبرانية قوية ومواجهة التهديدات المالية السيبرانية بفعالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصو الأمن السيبراني في البنوك والمؤسسات المالية.
- مديرو المخاطر والامتثال في القطاع المالي.
- مدققو الأنظمة المالية ومديرو التدقيق الداخلي.
- أخصائيو تقنية المعلومات العاملون في البنوك.
- مديرو العمليات المالية والمسؤولون عن أمن البيانات المصرفية.
- المستشارون القانونيون المتخصصون في التشريعات المالية والأمن السيبراني.

القطاعات والصناعات المستهدفة:

- البنوك التجارية والمؤسسات المصرفية المركزية.
- شركات الاستثمار وإدارة الأصول.
- شركات التأمين والخدمات المالية غير المصرفية.
- شركات التكنولوجيا المالية (FinTech) لأمن الابتكار المالي.
- الهيئات الحكومية وما في حكمها، خاصة تلك المعنية بالرقابة المالية والتنظيم المصرفي.
- شركات المدفوعات الإلكترونية ومعالجة المعاملات.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني وإدارة أمن المعلومات.
- إدارة المخاطر والامتثال التنظيمي.
- إدارة تقنية المعلومات والعمليات المصرفية.
- إدارة التدقيق الداخلي والخارجي.
- إدارة الشؤون القانونية والمراجعة.

أهداف الدورة التدريبية:

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

- فهم المشهد المعقد للتهديدات السيبرانية التي تواجه القطاع المالي.
- التعرف على أطر الامتثال الأمني والمتطلبات التنظيمية المصرفية.
- تطبيق استراتيجيات فعالة لحماية الأنظمة المصرفية وبيانات العملاء.
- القدرة على تقييم الثغرات الأمنية وإدارة المخاطر السيبرانية المالية.
- فهم آليات الاحتيال المالي السيبراني وكيفية الوقاية منه.
- بناء برامج توعية أمنية قوية داخل المؤسسات المالية.
- وضع خطط الاستجابة للحوادث الأمنية المصرفية وإدارة الأزمات.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية متقدمة تجمع بين الشرح الأكاديمي المتعمق والتطبيق العملي المكثف، مع التركيز بشكل خاص على السياق الفريد للقطاع المالي. تشمل المنهجية دراسات حالة واقعية لاختراقات مصرفية كبرى وكيفية معالجتها، مما يوفر للمشاركين رؤى عملية حول التحديات الأمنية في البنوك. سيتم تحليل أطر الامتثال المالي المعمول بها، مثل PCI DSS وSWIFT CSP، وكيفية تطبيقها بفعالية. تتضمن الدورة ورش عمل تفاعلية حول تقييم المخاطر السيبرانية للمؤسسات المالية، وتطوير خطط الاستجابة للحوادث المصرفية. يتم تشجيع المشاركة النشطة والنقاشات الموجهة لتبادل الخبرات بين المتخصصين. يقدم BIG BEN Training Center هذه الدورة لضمان أن يكتسب المشاركون فهمًا شاملاً للأمن السيبراني المصرفي والقدرة على تطبيق المعرفة المكتسبة لتعزيز المرونة السيبرانية لمؤسساتهم المالية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: التهديدات السيبرانية والسياق المالي

- المشهد الحالي للتهديدات السيبرانية في القطاع المالي.
- أنواع الهجمات السيبرانية المستهدفة للبنوك.
- تأثير الجرائم السيبرانية المالية على الاقتصاد.
- التهديدات الداخلية والخارجية للمؤسسات المالية.
- أمن البنية التحتية المصرفية الحيوية.
- الاحتيال المالي الرقمي.
- حماية الأصول المالية الرقمية.

الوحدة الثانية: أطر الامتثال الأمني واللوائح المصرفية

- أطر عمل الأمن السيبراني ذات الصلة بالقطاع المالي (مثل NIST CSF).
- الامتثال لـ PCI DSS وSWIFT CSP.
- قوانين حماية البيانات المالية (مثل GDPR وCCPA).
- اللوائح المصرفية المحلية والدولية المتعلقة بالأمن.
- حوكمة المخاطر الأمنية في المؤسسات المالية.
- التقارير الأمنية للجهات الرقابية.
- أخلاقيات الأمن السيبراني المالي.

الوحدة الثالثة: حماية الأنظمة المصرفية والبيانات الحساسة

- أمن الشبكات المصرفية.
- تشفير البيانات المالية ونقلها الآمن.
- أمن تطبيقات الخدمات المصرفية عبر الإنترنت.
- المصادقة القوية وإدارة الهوية والوصول.
- أمن السحابة في القطاع المالي.
- أمن المعاملات المصرفية الإلكترونية.
- التعافي من الكوارث وأمن استمرارية الأعمال.

الوحدة الرابعة: إدارة المخاطر الأمنية والاستجابة للحوادث

- تقييم المخاطر السيبرانية الخاصة بالقطاع المالي.
- تحليل الثغرات الأمنية في الأنظمة المصرفية.
- بناء فرق الاستجابة للحوادث الأمنية المصرفية.
- خطط الاستجابة للطوارئ السيبرانية.
- التحقيق في الحوادث الأمنية المالية.
- التعافي من الهجمات السيبرانية واستعادة الخدمات.
- التواصل الفعال أثناء الأزمات الأمنية.

الوحدة الخامسة: الوعي الأمني وبناء المرونة السيبرانية

- تطوير برامج الوعي الأمني للموظفين في المؤسسات المالية.
- محاكاة هجمات التصيد الاحتيالي لزيادة الوعي.
- أهمية الثقافة الأمنية في بيئة العمل المصرفي.
- التعاون مع الجهات الحكومية والخاصة في مجال الأمن السيبراني.
- الاستثمار في التقنيات الأمنية الحديثة.
- أمن البائعين الخارجيين في القطاع المالي.
- مستقبل الأمن السيبراني المصرفي.

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 ظل التطور المتسارع للتقنيات المالية والتهديدات السيبرانية المتزايدة، كيف يمكن للمؤسسات المصرفية أن تتبنى نهجًا استباقيًا للأمن السيبراني لا يقتصر على الامتثال التنظيمي، بل يمتد ليشمل بناء ثقافة مرونة سيبرانية تمكنها من مواجهة التحديات المستقبلية والابتكار بأمان؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص على الأمن السيبراني في القطاع المالي، مع تقديم رؤى عميقة ومفصلة تتجاوز المفاهيم العامة. نحن نغوص في التحديات الأمنية الفريدة التي تواجه البنوك والمؤسسات المالية، مع التركيز على أطر الامتثال التنظيمي الصارمة. بدلاً من مجرد سرد المعلومات، نقدم تحليلاً عمليًا لسيناريوهات الهجمات السيبرانية المصرفية وكيفية تطوير استراتيجيات دفاع فعالة. تركز الدورة على الجمع بين الجوانب التقنية والإدارية للأمن السيبراني، مما يجعلها مناسبة لمتخذي القرار والمهنيين التقنيين على حد سواء. إنها ليست مجرد دورة نظرية، بل هي تجربة تعليمية مكثفة تهدف إلى تمكين المشاركين من تطبيق أفضل الممارسات الأمنية لضمان حماية الأنظمة المصرفية وبيانات العملاء في بيئة مالية متغيرة.