الدورة التدريبية: الأمن في القطاع المالي والمصرفي: حماية الأصول والمعاملات الرقمية

#SM6641

الدورة التدريبية: الأمن في القطاع المالي والمصرفي: حماية الأصول والمعاملات الرقمية

مقدمة الدورة التدريبية / لمحة عامة:

يُعد الأمن في القطاع المالي والمصرفي: حماية الأصول والمعاملات الرقمية تحديًا حيويًا ومحوريًا في عصر يتزايد فيه الاعتماد على التقنيات الرقمية. تواجه المؤسسات المالية والمصرفية تهديدات سيبرانية متطورة ومتجددة تستهدف أصولها ومعاملاتها الحيوية وبيانات عملائها. هذه الدورة التدريبية الشاملة مصممة لتزويد المهنيين في هذا القطاع بالمعارف والمهارات المتقدمة اللازمة لتصميم، وتنفيذ، وإدارة استراتيجيات أمنية قوية تحمي الأصول المالية والمعاملات الرقمية. سنتعمق في تحليل المخاطر، تطبيق أطر الحوكمة والامتثال (مثل PCI DSS وISO 27001)، وتطوير خطط استجابة فعالة للحوادث. تستند الدورة إلى أعمال خبراء أكاديميين بارزين في مجال الأمن المالي والسيبراني، مثل البروفيسور Ross Anderson Ross Anderson، الذي يُعرف بإسهاماته القيمة في أمن النظم المالية. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين العاملين في القطاع المالي من بناء دفاعات متينة، وضمان سلامة الأنظمة، وتعزيز ثقة العملاء من خلال حماية بياناتهم ومعاملاتهم الرقمية بفعالية. سيركز التدريب على الجوانب التطبيقية والعملية، مع تقديم دراسات حالة واقعية وتمارين محاكاة، لمساعدة المشاركين على تطبيق المفاهيم النظرية في بيئات عملهم المعقدة، وتعزيز قدراتهم على مواجهة التحديات الأمنية ببراعة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو أمن المعلومات في البنوك والمؤسسات المالية.
- متخصصو الامتثال والمخاطر.
- مدققو الأمن الداخلي والخارجي.
- مهندسو الأمن السيبراني.
- مطورو الأنظمة المصرفية.
- مديرو العمليات المالية.
- مسؤولو حماية البيانات.

القطاعات والصناعات المستهدفة:

- البنوك التجارية والاستثمارية.
- شركات التأمين.
- شركات الدفع الإلكتروني والتقنيات المالية (FinTech).
- صناديق الاستثمار وإدارة الأصول.
- الجهات التنظيمية المالية.
- شركات الوساطة المالية.
- القطاع الحكومي وما في حكمها (فيما يتعلق بالقطاع المالي).

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- قسم الامتثال والحوكمة.
- إدارة المخاطر.
- العمليات المصرفية والمالية.
- القسم القانوني.
- التدقيق الداخلي.
- قسم تقنية المعلومات.

أهداف الدورة التدريبية:

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

- فهم التهديدات الأمنية الفريدة التي تواجه القطاع المالي.
- تطبيق أطر الحوكمة والامتثال الرئيسية (مثل PCI DSS، ISO 27001).
- تأمين الأنظمة المصرفية والتطبيقات المالية.
- حماية بيانات العملاء والمعاملات الرقمية.
- إدارة المخاطر السيبرانية في البيئات المالية.
- تطوير خطط استجابة للحوادث المالية والتعافي من الكوارث.
- تعزيز الوعي الأمني بين الموظفين والعملاء.
- التعامل مع عمليات الاحتيال المالي والغسل.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وتطبيقية مكثفة، تهدف إلى بناء قدرات احترافية في مجال الأمن في القطاع المالي والمصرفي: حماية الأصول والمعاملات الرقمية. تبدأ المنهجية بمحاضرات متعمقة يقدمها خبراء أمنيون وماليون متخصصون، يليها جلسات نقاش حيوية تتيح تبادل الخبرات والتحديات الفريدة للقطاع. تركز الدورة بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المشاركون بتحليل سيناريوهات هجمات مالية معقدة، واختراقات للبيانات المصرفية، وعمليات احتيال، وتطوير استراتيجيات للحماية والاستجابة. تتضمن المنهجية ورش عمل تطبيقية وتمارين محاكاة لسيناريوهات أمنية مالية، مثل تأمين أنظمة الدفع، وتقييم مخاطر المعاملات، وتنفيذ ضوابط الامتثال. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتعزيز التفكير النقدي وقدرات حل المشكلات تحت الضغط. يتم تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات والخبرة العملية اللازمة لحماية الأصول والمعاملات الرقمية بفعالية وكفاءة عالية، مما يعزز الثقة والأمان في النظام المالي.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: المشهد الأمني للقطاع المالي والمصرفي

- تحديات الأمن السيبراني الفريدة للقطاع المالي.
- التهديدات الشائعة (هجمات APT، الاحتيال المالي، غسيل الأموال).
- أهمية حماية البيانات المالية والشخصية.
- مفاهيم الأمن السيبراني المتقدمة في البيئة المصرفية.
- التقنيات الحديثة ودورها في تعزيز الأمن المالي.
- دور الذكاء الاصطناعي في الكشف عن الاحتيال.
- التطورات التنظيمية والقانونية في الأمن المالي.

الوحدة الثانية: أطر الحوكمة والامتثال في القطاع المالي

- مقدمة إلى أطر الامتثال الرئيسية (PCI DSS، GDPR، ISO 27001).
- متطلبات البنوك المركزية والجهات التنظيمية.
- تنفيذ ضوابط الامتثال وتدقيقها.
- إدارة المخاطر القانونية والتنظيمية.
- التقارير الدورية ومتطلبات الشفافية.
- أهمية الامتثال في بناء الثقة والسمعة.
- التعامل مع الدقيقات الخارجية والداخلية.

الوحدة الثالثة: تأمين الأنظمة والتطبيقات والمعاملات المصرفية

- أمن البنية التحتية المصرفية (الشبكات، الخوادم، قواعد البيانات).
- تأمين تطبيقات الخدمات المصرفية عبر الإنترنت والموبايل.
- حماية أنظمة الدفع الإلكتروني (SWIFT، بطاقات الائتمان).
- تشفير البيانات وحماية المفاتيح.
- التحقق متعدد العوامل (MFA) والتحكم في الوصول.
- أمن المعاملات الرقمية والتعامل مع العملات المشفرة.
- إدارة الثغرات الأمنية في الأنظمة المصرفية.

الوحدة الرابعة: إدارة مخاطر الاحتيال وغسيل الأموال

- فهم آليات الاحتيال المالي وأنواعه.
- تقنيات الكشف عن الاحتيال ومنعه.
- مكافحة غسيل الأموال (AML) وتمويل الإرهاب (CFT).
- دور تحليلات البيانات والذكاء الاصطناعي في مكافحة الاحتيال.
- الامتثال لمتطلبات "اعرف عميلك" (KYC).
- التعامل مع التحقيقات في الاحتيال.
- التوعية الداخلية والخارجية بمخاطر الاحتيال.

الوحدة الخامسة: الاستجابة للحوادث والتعافي في البيئة المالية

- تخطيط الاستجابة للحوادث الأمنية في القطاع المالي.
- إدارة الأزمات السيبرانية ذات التأثير المالي.
- تقنيات الأدلة الجنائية الرقمية للحوادث المالية.
- خطط التعافي من الكوارث المالية واستمرارية الأعمال.
- التعامل مع خروقات البيانات المالية والإبلاغ عنها.
- التواصل مع الجهات التنظيمية والعملاء أثناء الحوادث.
- الدروس المستفادة والتحسين المستمر للأمن المالي.

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 التوسع المستمر للخدمات المالية الرقمية والتهديدات السيبرانية المتجددة، كيف يمكن للمؤسسات المالية أن توازن بين الابتكار وتقديم خدمات جديدة وبين الحفاظ على أعلى مستويات الأمن والثقة للعملاء؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على الأمن في القطاع المالي والمصرفي: حماية الأصول والمعاملات الرقمية، مما يميزها عن الدورات الأمنية العامة. نحن نقدم رؤى متخصصة حول التحديات الأمنية الفريدة التي تواجه هذا القطاع الحيوي، مع التركيز على أطر الحوكمة والامتثال الصارمة. تعتمد الدورة على منهجية تطبيقية مكثفة، تتضمن دراسات حالة واقعية من القطاع المالي وتمارين محاكاة متخصصة، مما يمنح المشاركين خبرة عملية لا تقدر بثمن في بيئة تدريبية آمنة. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث التهديدات والحلول الأمنية المصممة خصيصًا للقطاع المالي. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا خبراء قادرين على حماية الأصول والمعاملات الرقمية، وتعزيز ثقة العملاء، وضمان استمرارية الأعمال المالية في مواجهة أي تحدٍ أمني.