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

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

بوسطن

(للشخص الواحد) € ٥٧٠٠

Ref: #CYB1141_266614

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

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

القطاعات والصناعات المستهدفة:

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

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

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

منهجية الدورة التدريبية:

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

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.

للحوادث الوحدة الرابعة: إدارة المخاطر الأمنية والاستجابة

- 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.

السيبرانية الوحدة الخامسة: الوعي الأمني وبناء المرونة

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

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:

السيبراني لا السيبرانية المتزايدة، كيف يمكن للمؤسسات المصرفية في ظل التطور المتسارع للتقنيات المالية والتهديدات

سيبرانية تمكنها من مواجهة التحديات يقتصر على الامتثال التنظيمي، بل يمتد ليشمل بناء أن تتبنى نهجًا استباقيًا للأمن

المستقبلية والابتكار بأمان؟ ثقافة مرونة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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