BLACKBIRD FOR TRAINING

برنامج تدريب أمن مدفوعات فيزا



برنامج تدريب أمن مدفوعات فيزا

مقدمة

في عالم رقمي يزداد فيه الاعتماد على المدفوعات الإلكترونية، أصبحت قضايا أمان المعاملات المالية تحتل الصدارة في اهتمامات المؤسسات على اختلاف أنواعها.

تُعد شركة فيزا من أبرز اللاعبين في هذا المجال، حيث تقدم بنية تحتية عالمية متطورة تُمكن المؤسسات من معالجة ملايين المعاملات يومياً بأمان.

مع تزايد التهديدات السيبرانية، بات من الضروري فهم آليات أمن مدفوعات فيزا وآخر التحديثات في هذا المجال.

تم تصميم هذه الدورة المتخصصة لتلبية احتياجات المدراء التنفيذيين، قادة الفرق، والمسؤولين عن نظم الدفع والامتثال والحوكمة في المؤسسات الحكومية والخاصة في منطقة الشرق الأوسط وشمال إفريقيا.

سواء كنت من العاملين في القطاع المصرفي، النفط والغاز، الاتصالات، أو حتى إدارة المشاريع والتقنية، فإن هذه الدورة ستمنحك الأدوات العملية لفهم المخاطر وكيفية التعامل معها باستخدام معايير فيزا.

ستتعلم كيفية بناء نظام دفع آمن، وفهم التهديدات المستجدة، والامتثال لمعايير حماية البيانات، مما ينعكس مباشرة على أداء مؤسستك وسمعتها الرقمية.

أهداف الدورة

- التعرف على البنية التحتية لنظام مدفوعات فيزا وكيفية عمله.
- فهم المخاطر الأمنية الشائعة في بيئة المدفوعات الرقمية.
- تحليل الحوادث الأمنية الواقعية ودروسها المستفادة.
- تطبيق المعايير العالمية لأمن المعلومات في بوابات الدفع الإلكترونية.
- التعرف على أدوات فيزا الخاصة بالكشف المبكر والاستجابة للتهديدات.
- إعداد خطة أمن مدفوعات تتناسب مع بيئة مؤسستك.
- تقييم مستوى الامتثال لمعايير حماية بيانات البطاقات داخل المؤسسة.
- تطوير استراتيجيات دفاعية مستندة إلى البيانات وتحليل المخاطر.



محاور الدورة

اليوم الأول: مقدمة في أمن مدفوعات فيزا

- نظرة عامة على نظام فيزا العالمي للمدفوعات.
- مكونات بنية الدفع الإلكترونية ومراكز المعالجة.
- المبادئ الأساسية لأمن المدفوعات.
- التهديدات السيبرانية التقليدية مقابل التهديدات الحديثة.
- الإطار التنظيمي لأمان المدفوعات في منطقة الشرق الأوسط وشمال إفريقيا.
- دراسة حالة: تأثير خروقات البيانات على الشركات.

اليوم الثاني: فهم التهديدات الأمنية الحديثة

- هجمات البرمجيات الخبيثة على بوابات الدفع.
- سرقة البيانات من بطاقات الدفع ونقاط البيع.
- الاحتيال الإلكتروني والاحتيال عبر الهاتف المحمول.
- تحليل نماذج التهديدات في قطاع البنوك.
- التعرف على سلاسل الهجوم الرقمية.
- دراسة حالات فعلية لاختراق أنظمة مدفوعات.

اليوم الثالث: أدوات ومعايير فيزا للحماية

- نظرة تفصيلية على أدوات فيزا مثل إدارة المخاطر والتفويض المتقدم.
- التعرف على معايير حماية بيانات البطاقات: ما الذي يُطلب وكيف يُطبق.
- فحص أمان الشبكة والبنية التحتية.
- كيفية استخدام أنظمة الإنذار المبكر والاستجابة للحوادث.
- إدارة وتسجيل الأحداث الأمنية في المؤسسة.
- تمرين عملي على تحليل اختراق باستخدام أدوات حقيقية.



اليوم الرابع: بناء نظام أمان داخلي للمدفوعات

- تصميم خطة شاملة لأمن المدفوعات داخل المؤسسة.
- سياسات الوصول والتحكم في البيانات.
- تقسيم المهام والمسؤوليات بين الفرق الأمنية والتقنية.
- إدارة الأطراف الخارجية وشركاء الدفع بأمان.
- اعتماد تقنيات التشفير والتوثيق المتعدد.
- ورشة تطبيقية: بناء سيناريو واقعي لخطة أمنية.

اليوم الخامس: التقييم والامتثال والتحسين المستمر

- كيفية إجراء تقييم دوري لأمن المدفوعات.
- أدوات القياس والتحليل في أمن المعاملات.
- الامتثال لمتطلبات حماية بيانات البطاقات والتدقيق الدوري.
- إعداد تقارير للجهات الرقابية والمصارف المركزية.
- تطوير خطة استمرارية العمل في حالات الطوارئ.
- تمرين ختامي شامل يحاكي سيناريو اختراق واقعي.

لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات

- فهم عميق وشامل لنظام فيزا الأمني.
- تعزيز حماية بيانات العملاء والمؤسسة.
- رفع جاهزية المؤسسة لمواجهة الهجمات الرقمية.
- تحسين الامتثال للمعايير الدولية.
- الوصول إلى أدوات احترافية من فيزا.
- دعم استدامة العمليات المالية بأمان.
- تأهيل فريق العمل للتعامل مع المخاطر الإلكترونية.
- الحصول على شهادة معتمدة تعزز المسار المهني.



الخاتمة

مع تزايد الاعتماد على المدفوعات الرقمية في جميع القطاعات، يصبح أمن مدفوعات فيزا أكثر من مجرد التزام تنظيمي، بل عنصرًا استراتيجيًا لحماية سمعة المؤسسة وضمان استمراريتها.

من خلال هذه الدورة المكثفة، ستحصل على مزيج فريد من المعرفة النظرية والتطبيق العملي الذي يُمكّنك من تعزيز بنية الأمان في منظومة المدفوعات لديك.

المحتوى صُمم بعناية ليتماشى مع احتياجات المدراء التنفيذيين والموظفين التقنيين على حد سواء، ويغطي أحدث التهديدات والحلول المبتكرة المستخدمة عالميًا.

سواء كنت تسعى لتطوير مهاراتك أو لتأمين مؤسستك ضد التهديدات الرقمية، فإن هذه الدورة هي الخطوة الأمثل نحو تحقيق ذلك.

