

تدريب أمن أجهزة الدفع والتقنية المالية والمدفوعات الرقمية

10 – 14 مايو 2027

القاهرة

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

تدريب أمن أجهزة الدفع والتقنية المالية والمدفوعات الرقمية

المرجع: 84332_103600689 **التاريخ:** 10 – 14 مايو 2027 **المكان:** القاهرة **الرسوم:** 4100 Euro

نظرة عامة على الدورة:

تطور دورة تدريب أمن أجهزة الدفع والتقنية المالية والمدفوعات الرقمية القدرات التقنية والتشغيلية اللازمة لتأمين بيئات البطاقات الحديثة ونقاط البيع والأجهزة المحمولة والمدفوعات الرقمية. يستكشف المشاركون أجهزة الدفع، والتجار، وجهات الاستحواذ، وجهات الاصدار، شبكات الدفع، وبوابات الدفع، واجهات برمجة التطبيقات، منصات التقنية المالية، المحافظ الرقمية، وتقنيات الدفع اللاتلامسي. تجمع الدورة التدريبية بين تدريب أمن أجهزة الدفع، تدريب أمن نقاط البيع، تدريب أمن المدفوعات الرقمية، وتدريب أمن التقنية المالية مع الإدارة العملية لمخاطر الدفع. تشمل المجالات الرئيسية الأمن المادي والمنطقي لأجهزة الدفع، دمج نقاط البيع، أامن الاتصالات، التشفير، إدارة المفاتيح، تهديدات المدفوعات المحمولة، الاحتيال الرقمي، حماية النقاط الطرفية، أمن بوابات الدفع، أامن واجهات برمجة تطبيقات الدفع، المرونة التشغيلية، والاعتماد على الأطراف الثالثة. سيعمل المشاركون على تطوير قدرات عمليّة لتعزيز أمن أجهزة الدفع، أمن البطاقات ونقاط البيع، أمن الدفع الإلكتروني، وعمليات الدفع الرقمي الآمنة.

AGILE LEADERS
Training Center

الجمهور المستهدف:

- مديرو ومخصصو نظم الدفع
- مسؤولو أجهزة الدفع ونقاط البيع
- محترفو الأمن السيبراني
- محللو أمن المعلومات
- محترفو التقنية المالية
- أخصائيو الخدمات المصرفية الرقمية
- مديرو عمليات البطاقات
- أخصائيو عمليات الدفع
- محترفو مخاطر الاحتيال والوقاية من الاحتيال
- مسؤولو مخاطر تكنولوجيا المعلومات والمخاطر التكنولوجية
- مهندسو أمن المدفوعات
- محترفو أمن الشبكات والبنية التحتية
- أخصائيو استحواذ التجار
- فرق بوابات الدفع واجهات برمجة التطبيقات
- فرق المحافظ الرقمية والمدفوعات المحمولة
- محترفو الامتثال ومخاطر الدفع
- محترفو استمرارية الأعمال والمرونة التشغيلية

AGILE LEADERS
Training Center

الأقسام المستهدفة:

- نظم الدفع والمدفوعات الرقمية
- عمليات البطاقات واستحواذ التجار
- أمن المعلومات والأمن السيبراني
- التقنية المالية والخدمات المصرفية الرقمية
- بنية تكنولوجيا المعلومات وأمن الشبكات
- الوقاية من الاحتيال والجرائم المالية
- المخاطر التكنولوجية والمخاطر التشغيلية
- إدارة نقاط البيع وأجهزة الدفع
- معالجة وتحويل المدفوعات
- القنوات الرقمية والخدمات المصرفية عبر الهاتف المحمول
- إدارة بوابات الدفع واجهات برمجة التطبيقات
- استمرارية الأعمال والمرونة التشغيلية
- الامتثال وأمن المدفوعات
- خدمات التجار

AGILE LEADERS
Training Center

القطاعات المستهدفة:

- البنوك والمؤسسات المالية
- شركات التقنية المالية
- مزودو خدمات الدفع
- جهات اصدار واستحواذ البطاقات
- شركات معالجة المدفوعات
- مؤسسات الأموال الإلكترونية
- البنوك الرقمية
- القطاع التجاري والتجارة الإلكترونية
- الاتصالات ومزودو المدفوعات المحمولة
- مزودو بوابات الدفع
- مزودو خدمات التجار
- مزودو تكنولوجيا الحوسبة السحابية
- منصات الدفع الحكومية
- النقل وأنظمة الدفع الذكية
- قطاع الضيافة وعمليات التجزئة عالية الحجم

أهداف الدورة:

بنهاية هذه الدورة التدريبية، سيكون المشاركون قادرين على:

- رسم تدفقات معاملات البطاقات، نقاط البيع، المحافظ المحمولة، المدفوعات اللاتلامسية، بوابات الدفع، والمعاملات الرقمية.
- شرح أدوار التجار، وجهات الاستحواذ، وجهات الإصدار، الجهات المعالجة، شبكات الدفع، البوابات، ومزودي التقنية المالية.
- تقييم أمن أجهزة الدفع عبر المجالات المادية والمنطقة ومجالات التكامل والاتصالات ودورة الحياة.
- تحديد عمليات العبث بالأجهزة، البرمجيات الخبيثة، التعديل غير المصرح به، الواجهات غير الآمنة، وتعرض بيانات الدفع للخطر.
- تطبيق مبادئ إدارة مخاطر نقاط البيع وإدارة مخاطر أجهزة الدفع.
- تقييم التهديدات ضد المدفوعات التي تتطلب حضور البطاقة، والتي لا تتطلب حضور البطاقة، والمدفوعات المحمولة واللاتلامسية.
- فحص برمجيات نقاط البيع الخبيثة، هجمات الوسيط، إعادة التشغيل، التصيد الاحتيالي، الهندسة الاجتماعية، واختراق الأجهزة.
- فهم التشفير، المفاتيح التشفيرية، الترميز، حماية أرقام التعريف الشخصية، والتعامل الآمن مع بيانات الدفع.
- تقييم مخاطر أمن بوابات الدفع وأمن واجهات برمجة تطبيقات الدفع.
- تقييم المحافظ الرقمية، تقنية الاتصال القريب المدى، رموز الاستجابة السريعة، المدفوعات القائمة على الترميز، المصادقة على الأجهزة، وتقنيات الدفع اللاتلامسي.
- التمييز بين الاحتيال في المدفوعات التي تتطلب حضور البطاقة، والتي لا تتطلب حضور البطاقة، البطاقات المزيفة، البطاقات المفقودة والمسروقة، والاحتيال الرقمي.
- تطوير ضوابط الوقاية من احتيال الدفع والوقاية من احتيال البطاقات.
- تقييم الاعتماد على الأطراف الثالثة، السحابة، الاتصالات، الجهات المعالجة، ومزودي التكنولوجيا.
- تعزيز أمن النقاط الطرفية، الاستجابة للحوادث، استمرارية الأعمال، التكرار، ومرونة نظم الدفع.
- تطوير استراتيجيات أمنية متعددة الطبقات لأنظمة الدفع الآمنة وبيئات التقنية المالية الحديثة.

منهجية التدريب:

تستخدم الدورة جلسات يقودها مدربون، تحليل تدفقات المدفوعات، دراسات حالة للأمن السيبراني، تمارين جماعية، أنشطة رسم الخرائط التهديدية، سيناريوهات الاحتيال، مناقشات الاستجابة للحوادث، وورش العمل التفاعلية. يفحص المشاركون نقاط ضعف أجهزة نقاط البيع، الأمن السيبراني للمدفوعات الرقمية، أمن مدفوعات البطاقات، مخاطر المحافظ المحمولة، أمن بوابات الدفع، أمن واجهات برمجة تطبيقات الدفع، احتيال المدفوعات، والتهديدات السيبرانية للتقنية المالية. تشمل الأنشطة العملية تحديد أسطح هجوم نظم الدفع، تقييم الضوابط الأمنية، تقييم مخاطر الأجهزة، تحليل تدفقات المعاملات، مراجعة الحوادث السيبرانية، وتطوير استراتيجيات التخفيف. يعزز العمل الجماعي عملية صنع القرار حول إدارة مخاطر نقاط البيع، إدارة مخاطر أجهزة الدفع، الاعتماد على الأطراف الثالثة، المرونة التشغيلية، وبنية الدفع الآمنة. تعزز جلسات التأمل والتعقيب تطبيق مفاهيم تدريب أمن نظم الدفع على الخدمات المصرفية، التقنية المالية، استحواذ التجار، المدفوعات الرقمية، وبيئات معالجة المدفوعات.

AGILE LEADERS
Training Center

أدوات الدورة:

- منظومة الدفع وخرائط تدفق المعاملات
- قوائم مراجعة أمن نقاط البيع وأجهزة الدفع
- رسم خريطة سطح الهجوم لأجهزة الدفع
- أمثلة على ضوابط الأمن المادي والمنطقي
- اعتبارات أمن تكامل نقاط البيع
- قوائم مراجعة أمن اتصالات وواجهات الدفع
- إطار مخاطر دورة حياة أجهزة الدفع
- أمثلة على نماذج تهديدات المدفوعات الرقمية
- قوالب نماذج تهديدات المحافظ المحمولة
- أمثلة مراجعة مخاطر واجهات برمجة تطبيقات وبوابات الدفع
- مصفوفات تحليل احتيال البطاقات
- مكتبة سيناريوهات احتيال المدفوعات
- أمثلة تصنيف الحوادث السيبرانية
- مصفوفة مخاطر الأطراف الثالثة ومزودي الخدمات الحيوية
- قائمة مراجعة مرونة نظم الدفع
- قوالب سيناريوهات استمرارية الأعمال وانقطاع الخدمة
- إطار مراجعة هندسة الدفع الآمن
- أمثلة سجل مخاطر الأمن السيبراني للمدفوعات

ملاحظة: لا توفر الدورة برمجيات تجارية، أجهزة نقاط البيع، منصات الأمن السيبراني، نظم الدفع، أو الأدوات المرخصة. توفر الدورة رؤى مهنية وأمثلة على الأدوات، الأطر، قوائم المراجعة، والتقنيات ذات الصلة بالدورة.

AGILE LEADERS
Training Center

محتوى الدورة:

اليوم الأول: التقنية المالية والمدفوعات الرقمية ومنظومات الدفع الحديثة

- **الموضوع 1:** مشهد التقنية المالية، التمويل الرقمي وتطور المدفوعات
- **الموضوع 2:** منظومة المدفوعات الرقمية: التجار، مزودو خدمات الدفع، جهات الاستحواذ، جهات الإصدار وشبكات الدفع
- **الموضوع 3:** معالجة مدفوعات البطاقات: تدفقات التفويض، المقاصة والتسوية
- **الموضوع 4:** تكنولوجيا المدفوعات الرقمية: البطاقات، نقاط البيع، المحافظ الرقمية، رموز الاستجابة السريعة والمدفوعات اللاتلامسية
- **الموضوع 5:** بوابات الدفع، واجهات برمجة تطبيقات الدفع ونماذج دمج التقنية المالية
- **الموضوع 6:** الأمن السيبراني، المخاطر التشغيلية والثقة في نظم الدفع الآمنة
- **المراجعة والتأمل:** رسم خريطة الاعتمادات الأمنية للتقنية المالية والمدفوعات الرقمية

اليوم الثاني: البنية الأمنية لأجهزة الدفع ونقاط البيع والبطاقات

- **الموضوع 1:** هندسة أجهزة الدفع وأمن نقاط التفاعل
- **الموضوع 2:** الأمن المادي: العبث بالأجهزة، تعديل الأجهزة وتعريض البيانات الحساسة للخطر
- **الموضوع 3:** الأمن المنطقي: البرمجيات الثابتة، التطبيقات، المصادقة وضوابط الوصول
- **الموضوع 4:** تكامل أجهزة نقاط البيع ومكونات الدفع الآمن
- **الموضوع 5:** اتصالات الدفع، الواجهات، البروتوكولات ومخاطر التعرض عبر الشبكات
- **الموضوع 6:** أمن دورة حياة الأجهزة، النشر، تحميل المفاتيح وإدارة الأجهزة
- **المراجعة والتأمل:** تقييم أمن أجهزة الدفع عبر دورة حياة الجهاز

AGILE LEADERS
Training Center

اليوم الثالث: الأمن السيبراني لأجهزة الدفع وإدارة تهديدات نقاط البيع

- **الموضوع 1:** مشهد تهديدات الأمن السيبراني لأجهزة الدفع وأسطح الهجوم
- **الموضوع 2:** البرمجيات الخبيثة لنقاط البيع، اختراق الأجهزة والتعديل غير المصرح به
- **الموضوع 3:** هجمات الوسيط، هجمات إعادة الإرسال وهجمات اتصالات الدفع
- **الموضوع 4:** إدارة مخاطر أجهزة الدفع وإدارة مخاطر نقاط البيع
- **الموضوع 5:** الإعداد الآمن، التحكم في الوصول وحماية نقاط نهاية الدفع
- **الموضوع 6:** الاكتشاف، المراقبة والاستجابة لحوادث أمن أجهزة الدفع
- **المراجعة والتأمل:** بناء نموذج دفاعي متعدد الطبقات للأمن السيبراني لنقاط البيع

اليوم الرابع: أمن المدفوعات المحمولة واللاتلامسية والبطاقات والمدفوعات الرقمية

- **الموضوع 1:** أمن المدفوعات المحمولة وهندسة المحافظ الرقمية
- **الموضوع 2:** أمن تقنية الاتصال قريب المدى، رموز الاستجابة السريعة والمدفوعات اللاتلامسية
- **الموضوع 3:** الترميز، الرموز التشفيرية وحماية بيانات حاملي البطاقات
- **الموضوع 4:** مصادقة المستخدم، مصادقة الأجهزة والعناصر الآمنة
- **الموضوع 5:** الاحتيال في معاملات حضور البطاقة ومعاملات عدم حضور البطاقة وأنماط الهجوم المرتبطة بها
- **الموضوع 6:** استراتيجيات الوقاية من احتيال المدفوعات والوقاية من احتيال البطاقات
- **المراجعة والتأمل:** ربط ضوابط أمن بطاقات الدفع والمدفوعات المحمولة واللاتلامسية

اليوم الخامس: استراتيجية أمن المدفوعات والمرونة والمخاطر السيبرانية الناشئة

- **الموضوع 1:** حوكمة الأمن السيبراني لنظم الدفع واستراتيجية الأمن
- **الموضوع 2:** أمن بوابات الدفع وأمن واجهات برمجة تطبيقات الدفع
- **الموضوع 3:** مخاطر الأطراف الثالثة، الحوسبة السحابية ومزودو الخدمات الحيوية
- **الموضوع 4:** الاستجابة للحوادث السيبرانية، انقطاع خدمات الدفع والمرونة التشغيلية
- **الموضوع 5:** التكرار التشغيلي، استمرارية الأعمال وترتيبات الدفع البديلة
- **الموضوع 6:** تهديدات التقنية المالية الناشئة، الاحتيال الرقمي وأمن المدفوعات المستقبلي
- **المراجعة والتأمل:** تصميم بيئة مدفوعات رقمية آمنة ومرنة

الأسئلة الشائعة:

ما المؤهلات أو المتطلبات المسبقة التي يحتاجها المشاركون قبل الالتحاق بالدورة؟

لا توجد مؤهلات رسمية مطلوبة في الأمن السيبراني أو صناعة المدفوعات. يُفضل أن يكون لدى المشاركين خبرة عملية في مجال الخدمات المصرفية، المدفوعات، تكنولوجيا المعلومات، الأمن السيبراني، التقنية المالية، عمليات البطاقات، نظم نقاط البيع، إدارة الاحتيال، مخاطر التكنولوجيا، استحواذ التجار أو القنوات الرقمية. تعد الإلمامة الأساسية بالمدفوعات الإلكترونية، شبكات الحاسوب، معالجة المدفوعات أو مصطلحات أمن المعلومات أمراً مفيداً. ولا تتطلب الدورة خبرة متقدمة في البرمجة أو التشفير.

ما مدة الجلسة التدريبية اليومية، وما إجمالي عدد الساعات المطلوبة لإكمال الدورة؟

تستغرق الجلسة التدريبية اليومية عادةً ما بين 4 إلى 5 ساعات، بما في ذلك الاستراحات والأنشطة التفاعلية. تمتد الدورة على مدار أسبوع، بإجمالي يتراوح تقريباً بين 20 و25 ساعة تدريبية.

هل الأمن السيبراني لأجهزة الدفع هو نفسه الامتثال لمعيار أمن بيانات صناعة بطاقات الدفع؟

لا. يغطي الأمن السيبراني لأجهزة الدفع الأمن المادي والمنطقي للأجهزة، تكامل نقاط البيع، الاتصالات، المدفوعات المحمولة واللاتلامسية، الاحتيال، بوابات الدفع، واجهات برمجة التطبيقات، حماية نقاط النهاية، مخاطر الأطراف الثالثة، الحوادث السيبرانية والمرونة التشغيلية. وتشكل متطلبات معيار أمن بيانات صناعة بطاقات الدفع PCI DSS جزءاً مهماً من أمن المدفوعات، لكنها لا تمثل كامل منظومة الأمن السيبراني للمدفوعات.

AGILE LEADERS
Training Center

ما الذي يميز هذه الدورة عن غيرها من دورات الأمن السيبراني لأجهزة الدفع؟

تدمج دورة أمن أجهزة الدفع والتقنية المالية والمدفوعات الرقمية الأمن السيبراني للأجهزة، التقنية المالية، أمن البطاقات، أمن نقاط البيع، المدفوعات المحمولة، التقنيات اللاتلامسية، احتيال المدفوعات، بوابات الدفع، واجهات برمجة التطبيقات والمرونة التشغيلية ضمن برنامج تدريبي مؤسسي متكامل.

وبدلاً من التعامل مع تدريب أمن نقاط البيع أو أمن أجهزة الدفع باعتبارهما موضوعين تقنيين منفصلين، تتبع الدورة منظومة معاملات الدفع كاملة، بدءاً من العملاء والأجهزة، مروراً بالتجار وبوابات الدفع والجهات المعالجة وجهات الاستحواذ وشبكات الدفع، وصولاً إلى جهات الإصدار.

يتعامل المشاركون مع الأمن المادي والمنطقي للأجهزة، الاتصالات الآمنة، المحافظ المحمولة، الترميز، احتيال البطاقات، أمن بوابات الدفع، أمن واجهات برمجة التطبيقات، مخاطر الأطراف الثالثة، الحوادث السيبرانية، استمرارية الأعمال والمرونة التشغيلية.

ويربط هذا النهج المتكامل بين الضوابط التقنية للأمن السيبراني وتدريب أمن المدفوعات الرقمية، والأمن السيبراني للتقنية المالية، والوقاية من احتيال المدفوعات، والوقاية من احتيال البطاقات، وأمن نظم الدفع، بما يدعم التطبيق العملي في بيئات المدفوعات الحديثة.