تدريب وحدة أمان الأجهزة (HSM): payShield 10K و أساس PCI DSS

22 – 26 مارس 2027

القاهرة

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

تدريب وحدة أمان الأجهزة (HSM): payShield 10K و أساس PCI DSS

المرجع: 103600517_81340 **التاريخ:** 22 – 26 مارس 2027 **المكان:** القاهرة **الرسوم:** Euro 4100

نظرة عامة على الدورة:

دورة تدريب وحدة أمان الأجهزة HSM: payShield 10K و PCI DSS هي برنامج مؤسسي شامل مصمم لبناء الخبرة العملية والتشغيلية في تأمين بيئات الدفع باستخدام وحدات أمان الأجهزة. تجمع هذه الدورة بين تدريب payShield HSM، وتدريب وحدة أمان الأجهزة، وتدريب PCI HSM في رحلة تعليمية منظمة تغطي الإعدادات والعمليات والامتثال.

سيكتسب المشاركون فهمًا راسخًا لمفاهيم تدريب payShield 10K، بما في ذلك تركيب وتشغيل HSM، وإعدادات payShield، وإدارة دورة حياة مفاتيح HSM. تؤكد الدورة على تدريب إدارة المفاتيح التشفيرية بما يتماشى مع متطلبات PCI DSS و PCI PTS HSM، مما يمكّن المشاركين من إدارة المفاتيح الحساسة بأمان طوال دورة حياتها.

باستخدام سيناريوهات تشغيلية واقعية مستوحاة من الوثائق الرسمية مثل دليل مستخدم تركيب payShield 10K، والأسئلة الفنية المتكررة حول PCI PTS HSM، وسياسة أمان payShield، تركز الدورة على تكامل المضيف الآمن، وإعدادات TLS لـ HSM، ومراقبة وتسجيل HSM، والنسخ الاحتياطي والاستعادة لـ HSM. بنهاية الدورة، سيكون المشاركون مستعدين لتشغيل بيئات HSM للدفع بثقة مع دعم عمليات التدقيق والامتثال التنظيمي.

الجمهور المستهدف:

- مهندسو أمن الدفع
- مسؤولو ومشغلو HSM
- مهندسو البنية التحتية لتكنولوجيا المعلومات المصرفية
- مهندسو أنظمة الدفع
- مسؤولو أمن المعلومات
- متخصصو الامتثال والتدقيق لمعيار PCI
- متخصصو التشفير وإدارة المفاتيح

AGILE LEADERS
Training Center

الاقسام المستهدفة:

- أمن المعلومات والأمن السيبراني
- البنية التحتية لتكنولوجيا المعلومات والعمليات
- أنظمة الدفع ومعالجة البطاقات
- إدارة المخاطر والامتثال
- التدقيق الداخلي والحوكمة
- الخدمات المصرفية الرقمية وعمليات التكنولوجيا المالية

تدعم هذه الدورة مبادرات التدريب على أمن الدفع وتعزز القدرات المؤسسية في التدريب على أمن HSM، والتدريب على إدارة مفاتيح HSM، وعمليات أنظمة الدفع الآمنة.

القطاعات المستهدفة:

- الخدمات المصرفية والمالية
- معالجو الدفع ومستحوذو البطاقات
- شركات التكنولوجيا المالية ومقدمو المحافظ الرقمية
- مصدرو البطاقات ومشغلو محولات الدفع
- منصات الدفع الحكومية
- عمليات الدفع في التجزئة والتجارة الإلكترونية

أهداف الدورة:

بنهاية هذه الدورة، سيتمكن المشاركون من:

- إجراء تركيب وتشغيل آمن لـ HSM بما يتماشى مع معايير payShield
- تكوين وإدارة بيئات payShield 10K HSM بفعالية
- تطبيق مبادئ إدارة دورة حياة مفاتيح HSM من الإنشاء إلى إيقاف التشغيل
- تطبيق أفضل ممارسات تدريب إدارة المفاتيح التشفيرية لأنظمة الدفع
- تكوين مضيف payShield الآمن والاتصال القائم على TLS
- مراقبة وتدقيق وتسجيل أنشطة HSM في البيئات التي تتطلب الامتثال
- إعداد بيئات HSM لعمليات تدقيق الامتثال لمعايير PCI DSS و PCI HSM
- تنفيذ إجراءات النسخ الاحتياطي والاستعادة لـ HSM وإيقاف التشغيل المتحكم به

منهجية التدريب:

تستخدم هذه الدورة منهجية تدريب مختلطة وعملية المنحى مصممة للمحترفين الذين يديرون بيئات دفع حية. يتم الجمع بين الجولات الفنية بقيادة المدرب وسيناريوهات الإعداد الموجهة وتمارين حل المشكلات القائمة على المجموعات التي تعكس تحديات تشغيلية حقيقية.

يحلل المشاركون سير عمل إعدادات payShield، ويؤدون تمارين دورة حياة المفاتيح، ويفسرون ضوابط الامتثال المستمدة من معايير PCI HSM. تناقش الحالات العملية المخاطر المتعلقة بضعف مراقبة وتسجيل HSM، والإعداد غير الصحيح لـ TLS، وممارسات التعامل مع المفاتيح غير الفعالة.

تعزز جلسات المراجعة التفاعلية الجاهزية للتدقيق، بينما تساعد أنشطة التفكير المشاركين على ترجمة مفاهيم تدريب أمان HSM إلى إجراءات تشغيلية قابلة للتنفيذ. يبقى التركيز على التعلم التطبيقي، مما يضمن أن يكتسب المشاركون رؤى عملية بدلاً من التعليمات المعتمدة على الأدوات.

AGILE LEADERS
Training Center

أدوات الدورة:

- قوائم مراجعة إعدادات payShield
- نماذج مرجعية لدورة حياة مفاتيح HSM
- قوالب جاهزية تدقيق PCI HSM
- نماذج سير عمل المراقبة والتسجيل
- رسوم بيانية لعمليات إدارة المفاتيح الآمنة
- كتيبات النشر وإيقاف التشغيل

ملاحظة: لا يتم توفير الأدوات ماديًا. تقدم الدورة رؤى وأطر عمل وأمثلة واقعية للأدوات ذات الصلة بموضوعات التدريب.

محتوى الدورة:

اليوم الأول: أنظمة الدفع وأسس HSM

- **الموضوع 1:** أساسيات أنظمة الدفع وتدفقات المعاملات الآمنة
- **الموضوع 2:** دور وحدات أمان الأجهزة في أمن الدفع
- **الموضوع 3:** نظرة عامة على بنية وقدرات payShield HSM
- **الموضوع 4:** معلومات منتج payShield 10K ومكونات الأجهزة
- **الموضوع 5:** أساسيات المنتج، نطاقات الأمان، وحالات التشغيل
- **الموضوع 6:** حالات استخدام HSM في الخدمات المصرفية، والتحويل، ومعالجة البطاقات
- **تفكير ومراجعة:** مخاطر بيئة الدفع ومواءمة قيمة HSM

AGILE LEADERS
Training Center

اليوم الثاني: تركيب، إعداد، وإدارة payShield

- **الموضوع 1:** دورة حياة تركيب وتشغيل HSM
- **الموضوع 2:** تشغيل البطاقة الذكية وأدوار المسؤولين
- **الموضوع 3:** جولة في payShield Manager وإدارة الجهاز
- **الموضوع 4:** إدارة مجموعات أمان payShield وضوابط الوصول
- **الموضوع 5:** تسلسل تشغيل payShield والتهيئة الآمنة
- **الموضوع 6:** إعداد Syslog عن بعد وإدارة إعدادات NTP
- **تفكير ومراجعة:** ضوابط الإعداد والجاهزية التشغيلية

اليوم الثالث: المفاتيح، التشفير، وعمليات payShield TMD

- **الموضوع 1:** مبادئ إدارة المفاتيح التشفيرية لوحدات HSM للدفع
- **الموضوع 2:** إنشاء المفتاح الرئيسي المحلي وتصميم التسلسل الهرمي للمفاتيح
- **الموضوع 3:** إدارة مفتاح المنطقة الرئيسي ومفتاح رقم التعريف الشخصي للمنطقة
- **الموضوع 4:** أدوار المسؤول المعتمد والتحكم في الأوامر الحساسة
- **الموضوع 5:** تشغيل payShield TMD وتصميم الوضع الموثوق
- **الموضوع 6:** إنشاء، تقسيم، وإعادة إنشاء مكونات المفاتيح
- **تفكير ومراجعة:** منع اختراق المفاتيح ومخاطر المطلعين

AGILE LEADERS
Training Center

اليوم الرابع: تكامل المضيف، المراقبة، والضوابط التشغيلية

- **الموضوع 1:** إعداد مضيف payShield ونماذج الاتصال
- **الموضوع 2:** تمكين اتصال المضيف عبر TLS ومعالجة الشهادات
- **الموضوع 3:** إجراءات التدقيق والمراقبة والفحص الصحي
- **الموضوع 4:** تركيب وإعداد payShield Monitor
- **الموضوع 5:** إعداد SNMPv3 وتسجيل الجهاز الآمن
- **الموضوع 6:** تسجيل HSM، التنبيهات، والرؤية التشغيلية
- **تفكير ومراجعة:** فعالية المراقبة واكتشاف الحوادث

اليوم الخامس: الامتثال، الصيانة، وإغلاق دورة حياة HSM

- **الموضوع 1:** متطلبات شهادة PCI DSS و PCI HSM
- **الموضوع 2:** التحضير لتدقيقات HSM وتقييمات الامتثال
- **الموضوع 3:** حفظ الإعدادات، النسخ الاحتياطي، وتخطيط الاستعادة
- **الموضوع 4:** صيانة payShield وإجراءات ترقية البرامج الثابتة
- **الموضوع 5:** إيقاف تشغيل HSM الآمن وتصفير المفاتيح
- **الموضوع 6:** حالات استخدام HSM المتقدمة وأفضل الممارسات التشغيلية
- **تفكير ومراجعة:** حوكمة دورة حياة HSM الشاملة والدروس المستفادة

الأسئلة الشائعة:

ما هي المؤهلات أو المتطلبات المسبقة المحددة المطلوبة للمشاركين قبل التسجيل في الدورة؟

يتوقع من المشاركين أن يكون لديهم فهم أساسي لتكنولوجيا المعلومات، أو الأمن السيبراني، أو أنظمة الدفع. بينما تعتبر الخبرة المسبقة في وحدات أمان الأجهزة أو التشفير مفيدة، إلا أنها ليست إلزامية، حيث تبني الدورة المعرفة العملية من المفاهيم الأساسية إلى الممارسات التشغيلية المتقدمة.

AGILE LEADERS
Training Center

كم مدة كل جلسة يومية، وما هي المدة الإجمالية للدورة؟

يتم تنظيم كل يوم تدريبي عادةً ليدوم ما بين 4 إلى 5 ساعات، ويجمع بين الجولات الفنية والتمارين العملية. يتم تقديم الدورة على مدار أسبوع، مما ينتج عنه حوالي 20 إلى 25 ساعة من التدريب العملي والمركز.

كيف تختلف هذه الدورة عن دورات وحدات أمان الأجهزة الأخرى:

تتجاوز هذه الدورة التدريب العام على أمان HSM من خلال التركيز بشكل خاص على تدريب payShield 10K ضمن بيئات الدفع الحقيقية. فهي تدمج سياسات أمان البائع ومعايير PCI في تجربة تعليمية منظمة واحدة تركز على التنفيذ التشغيلي بدلاً من التشفير النظري.

يكتسب المشاركون فهمًا واضحًا لكيفية تأثير إعدادات payShield، وإدارة دورة حياة مفاتيح HSM، وتكامل المضيف، والمراقبة بشكل مباشر على نتائج الامتثال والجاهزية للتدقيق. تربط الدورة الإجراءات الفنية بالآثار المترتبة على الحوكمة والمخاطر، مما يمكن المشاركين من إدارة بيئات HSM بثقة ودقة وتوافق تنظيمي.