

# دورة الانتقال إلى التشفير ما بعد الكمي: الجرد والمرونة التشفيرية وخارطة الطريق

12 – 16 يوليو 2027

طوكيو





## دورة الانتقال إلى التشفير ما بعد الكمي: الجرد والمرونة التشفيرية وخارطة الطريق

المرجع: 32612\_651 التاريخ: 12 - 16 يوليو 2027 المكان: طوكيو الرسوم: GBP 6900

### ملخص البرنامج

الانتقال إلى التشفير ما بعد الكمي محور دورة تدريبية تمتد أسبوع لقادة الأمن والمعمارية ومخاطر التقنية على المستوى الإداري، ويخرج منها كل مشارك بحزمة خارطة طريق للانتقال في منظمة واحدة. قد تفشل حمايات المفاتيح العامة التي تؤمن المدفوعات والهويات والسجلات المؤرشفة حين تظهر حواسيب كمية قادرة، ومع ذلك لا تعرف أغلب المنظمات أين توجد هذه الحميات. وينتقل البرنامج من التهديد الكمي إلى الجرد واختيار الخوارزميات والمرونة التشفيرية وترتيب الخطوات، ويطبق ذلك على منظمة يختارها المشارك. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في الانتقال إلى التشفير ما بعد الكمي لمجموعات من منظمات مختلفة.

### المبررات المؤسسية

يمكن فك تشفير البيانات المسروقة اليوم لاحقاً، فتتعرض المعلومات طويلة العمر قبل ظهور أي حاسوب كمي. ويمس استبدال التشفير التطبيقات والأجهزة والموردين والعقود، ولا يمكن إنجازه في اللحظة الأخيرة. أما البنوك والجهات الصحية ومشغلو الاتصالات التي تثبت جرداً وقواعد للخوارزميات وتسلسلاً للخطوات من الآن فتوزع العمل على سنوات وتجب المجالس والمدققين بالأدلة.

- تعرض البيانات طويلة العمر: ينخفض حين ترتب الأنظمة بحسب المدة التي يجب أن تبقى فيها بياناتها سرية.
- تجاوز كلفة الانتقال: ينخفض حين ترسم الاعتمادات المتبادلة وجدول الموردين قبل تمويل العمل.
- مخاطر إعادة العمل: تنخفض حين تتيح المرونة التشفيرية استبدال الخوارزميات دون إعادة تصميم كل نظام.

### المبادئ والأساس المعرفي

- NIST IR 8547 الانتقال إلى معايير التشفير ما بعد الكمي: يؤطر تخطيط الانتقال وترتيب خطواته في الجلستين 2 و4.
- FIPS 203 وFIPS 204 وFIPS 205: توفر معايير الخوارزميات ما بعد الكمية التي تقارن في الجلسة 3.
- ممارسات جرد الأنظمة التشفيرية: توجه اكتشاف الخوارزميات والمفاتيح والشهادات وتقييمها في الجلسة 2.
- مبادئ المرونة التشفيرية: تشكل أنماط التصميم القابلة للاستبدال في الجلسة 3.



## المشاركون المستهدفون

- قادة الأمن الذين يتولون سياسة التشفير ومخاطر تعرض البيانات طويلة العمر.
- معماريو المؤسسة والأمن الذين يصممون الأنظمة المعتمدة على تشفير المفاتيح العامة.
- مديرو مخاطر التقنية الذين يرفعون تقدم الانتقال إلى المجالس والمدققين.
- رؤساء البنية التحتية والمنصات الذين يديرون الشهادات والمفاتيح والأجهزة المطلوب تغييرها.
- مديرو المشتريات والموردين الذين يمسكون بتعهدات الموردين للمنتجات المحدثة.

يأتي المشاركون عادة من البنوك والجهات الصحية ومشغلي الاتصالات والجهات الحكومية الرقمية.

## مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم البيانات والأنظمة المعرضة على المدى الطويل لهجوم كمي مستقبلي.
2. سيكون المشاركون قادرين على بناء جرد للأنظمة التشفيرية يسجل الخوارزميات والمفاتيح والشهادات والمالكين.
3. سيكون المشاركون قادرين على ترتيب أولويات الأنظمة للانتقال بمصفوفة تقييم التعرض.
4. سيكون المشاركون قادرين على مقارنة الخوارزميات البديلة والأنماط الهجينة بحسب احتياجات الأداء والتوافق.
5. سيكون المشاركون قادرين على تصميم مبادئ للمرونة التشفيرية تتيح تغيير الخوارزميات لاحقاً.
6. سيكون المشاركون قادرين على تبرير خارطة طريق مرتبة للانتقال ومخاطرها المتبقية أمام مجلس الإدارة.

## هيكل البرنامج

### اليوم 1: أسس الانتقال إلى التشفير ما بعد الكمي

أي حمايات التشفير الحالية قد يكسرها حاسوب كمي، ومتى يصبح ذلك مهماً؟

- موجز الجدول الزمني للتهديد الكمي
- خريطة الاعتماد على المفاتيح العامة
- اختبار التعرض للجمع المسبق
- ورقة تصنيف عمر البيانات
- سجل مبادئ الانتقال

### اليوم 2: جرد الأنظمة التشفيرية وتشخيص التعرض

أين تستخدم الخوارزميات والمفاتيح والشهادات، وأي الأنظمة أشد تعرضاً؟



- نموذج جرد الأنظمة التشفيرية
- خطة اكتشاف الشهادات والمفاتيح
- جدول اعتماد الموردين وسلسلة الإمداد
- مصفوفة تقييم التعرض
- قائمة الأنظمة ذات الأولوية

### اليوم 3: اختيار الخوارزميات وتصميم المرونة التشفيرية

أي الخوارزميات البديلة والتصاميم تتيح التغيير القادم دون إعادة بناء جديدة؟

- جدول اختيار الخوارزميات المعتمدة
- نمط النشر الهجين
- مبادئ تصميم المرونة التشفيرية
- خطة اختبار الأداء والتوافق
- مخطط تغيير إدارة المفاتيح

### اليوم 4: خارطة الطريق والحوكمة وقرارات المخاطر

كيف يرتب الانتقال ويمول ويحكم عبر مالكين كثيرين؟

- خطة موجات الانتقال
- مخطط الاعتماد المتبادل والتسلسل
- خريطة أدوار الحوكمة
- سجل المخاطر المتبقية
- مخطط إحاطة المجلس

### اليوم 5: حزمة خارطة طريق الانتقال لمنظمة واحدة

هل يدعم الجرد واختيار الخوارزميات والتسلسل قرار انتقال واحد؟

- تطبيق مصفوفة تقييم التعرض من الجلسة 2
- اختبار جدول اختيار الخوارزميات المعتمدة من الجلسة 3
- مراجعة سجل المخاطر المتبقية من الجلسة 4
- فحص خطة موجات الانتقال من الجلسة 4
- إنجاز حزمة خارطة طريق الانتقال



## المنهجية

يقوم البرنامج على ورش البيانات اعتمادا على حالة مشتركة لبيئة مدفوعات وسجلات فيها تطبيقات قديمة ومجموعة شهادات وعدة موردين. يبني المشاركون كل مخرج على الحالة ببيانات جاهزة ثم ينفذونه مع منظمة يعرفونها، مع ملاحظات مكتوبة من الميسرين في كل جلسة.

- نشاط مقترح: تقييم عشرين نظاما من حيث التعرض والاتفاق على قائمة الأولويات.
- نشاط مقترح: مقارنة خيارين للخوارزميات بحسب أدلة الأداء والتوافق.
- نشاط مقترح: عرض تسلسل الانتقال أمام لجنة تمثيلية لمخاطر التقنية.

## المخرج الختامي

يعد كل مشارك حزمة خارطة طريق للانتقال في منظمة واحدة. وتضم الحزمة نموذجا للجرد ومصفوفة لتقييم التعرض وجدولاً لاختيار الخوارزميات وخطة لموجات الانتقال وسجلا للمخاطر المتبقية. وتستخدم الحزمة في العمل لبدء الجرد وإحاطة المجلس وتحديد متطلبات الموردين للمنتجات المحدثة.

## الأسئلة الشائعة

### هل يناسب تدريب الانتقال إلى التشفير ما بعد الكمي القادة من غير المتخصصين في التشفير؟

نعم، فالانتقال إلى التشفير ما بعد الكمي يدرس بالحالات والنماذج الجاهزة، ويفترض البرنامج مسؤولية عن الأمن أو المعمارية أو مخاطر التقنية دون خلفية رياضية في التشفير.

### على أي معايير يقوم تدريب الانتقال إلى التشفير ما بعد الكمي؟

يقوم تدريب الانتقال إلى التشفير ما بعد الكمي على NIST IR 8547 و FIPS 203 و FIPS 204 و FIPS 205، إضافة إلى ممارسات جرد الأنظمة التشفيرية ومبادئ المرونة التشفيرية.

### كيف تستخدم حزمة خارطة الطريق الناتجة عن تدريب الانتقال إلى التشفير ما بعد الكمي في العمل؟

تستخدم حزمة خارطة طريق الانتقال لبدء الجرد وإحاطة المجلس وتحديد متطلبات الموردين للمنتجات المحدثة.

### بماذا يختلف الانتقال إلى التشفير ما بعد الكمي عن تدريب الأمن السيبراني العام؟

يتيح الانتقال إلى التشفير ما بعد الكمي حول استبدال حمايات المفاتيح العامة بتسلسل مخطط، بينما يغطي تدريب الأمن السيبراني العام التهديدات والضوابط والاستجابة للحوادث في جميع الأنظمة.