MERCURY

تشفير البيانات في نظام حماية البيانات الشخصية

3 – 7 يناير 2027

اسطنبول (تركيا)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

تشفير البيانات في نظام حماية البيانات الشخصية

المرجع: 148528_120983 **التاريخ:** 3 – 7 يناير 2027 **المكان:** اسطنبول (تركيا) **الرسوم:** Euro 5500

مقدمة الدورة التدريبية: تشفير البيانات في نظام حماية البيانات الشخصية:

في ظل التطورات المتسارعة في عالم التكنولوجيا وتزايد حجم البيانات الرقمية، أصبح تشفير البيانات أداة ضرورية لضمان حماية الخصوصية. تعد هذه الدورة التدريبية في تشفير البيانات في نظام حماية البيانات الشخصية، مدخلاً شاملاً لفهم آليات وتقنيات التشفير ضمن إطار نظام حماية البيانات الشخصية.

تهدف دورة تشفير البيانات في نظام حماية البيانات الشخصية، إلى تزويد المشاركين بالمعرفة الأساسية والمتقدمة في كيفية تأمين البيانات الحساسة ضمن البيئات المؤسسية. كما تناقش أهمية التوافق مع اللوائح المحلية والدولية المتعلقة بالخصوصية وتخزين البيانات. من خلال منهجية تعليمية متكاملة، يتعلم المشاركون كيفية استخدام خوارزميات التشفير المختلفة وتطبيقها في نظم إدارة المعلومات.

تسلط الدورة التدريبية في تشفير البيانات في نظام حماية البيانات الشخصية، الضوء على التحديات الحالية في حماية البيانات الشخصية وطرق تجاوزها باستخدام أدوات التشفير الحديثة. في نهاية الدورة، سيكون المتدرب قادرًا على تطبيق أفضل الممارسات لتحقيق الأمان المعلوماتي في إطار الامتثال القانوني والتنظيمي.

الفئات المستهدفة:

تستهدف دورة تشفير البيانات في نظام حماية البيانات الشخصية، الفئات والمحترفين الذين يسعون لاكتساب المعرفة والمهارات:

- مسؤولو حماية البيانات في المؤسسات العامة والخاصة.
- موظفو تقنية المعلومات المسؤولون عن أمن المعلومات.
- المستشارون القانونيون المتخصصون في خصوصية البيانات.
- مطورو البرمجيات المهتمون بتأمين التطبيقات والأنظمة.
- مدراء المخاطر وإدارة الامتثال في الشركات.
- الأفراد الراغبون في بناء أساس معرفي في تشفير البيانات.
- مشرفو أمن الشبكات وحماية البنية التحتية الرقمية.
- العاملون في مجالات تحليل البيانات الضخمة والذكاء الاصطناعي.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

أهداف الدورة التدريبية:

في نهاية هذا البرنامج التدريبي في تشفير البيانات في نظام حماية البيانات الشخصية، سيكون المشاركون قادرين على:

- تحديد مفاهيم تشفير البيانات وتفسير أنواعها المختلفة.
- تحليل الفرق بين التشفير المتناظر وغير المتناظر واختيار الأنسب حسب السياق.
- تطبيق تقنيات التشفير في حماية قواعد البيانات وأنظمة الملفات.
- تقييم نقاط الضعف المحتملة في نظم التشفير وتصميم حلول فعالة لمعالجتها.
- إعداد وتنفيذ سياسات تشفير تتماشى مع نظام حماية البيانات الشخصية.
- قياس فعالية تقنيات التشفير المستخدمة في المؤسسات.
- تطوير إجراءات أمنية متقدمة تعتمد على التشفير لحماية البيانات الحساسة.
- استخدام أدوات تشفير مفتوحة المصدر وتقييم ملاءمتها للأهداف الأمنية.
- ربط التشفير بمتطلبات الامتثال القانوني للائحة العامة لحماية البيانات GDPR والقوانين المحلية.
- تعزيز القدرة على توثيق عمليات التشفير والاحتفاظ بسجلات لحالات الوصول والاستخدام.
- تدريب المشاركين على إجراء اختبارات الأمان للتأكد من فعالية التشفير.
- تصميم بنية أمنية معلوماتية تعتمد على التشفير كنقطة ارتكاز أساسية.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج تشفير البيانات في نظام حماية البيانات الشخصية:

- الإلمام بأساسيات وأدوات التشفير الحديثة.
- فهم العلاقة بين التشفير وحماية البيانات الشخصية.
- القدرة على تصميم استراتيجيات أمنية فعالة باستخدام التشفير.
- تحليل المخاطر وتطبيق سياسات أمنية مناسبة.
- التعامل مع خوارزميات التشفير بكفاءة.
- التكيف مع التغيرات التشريعية المرتبطة بحماية البيانات.
- تقييم أدوات وتقنيات التشفير من منظور أمني وتشغيلي.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

محتوى الدورة التدريبية:

الوحدة الأولى: أساسيات تشفير البيانات وحماية الخصوصية:

- تعريف التشفير وأهميته في حماية البيانات.
- الفرق بين التشفير والتعتيم وإخفاء البيانات.
- نظرة تاريخية على تقنيات التشفير وتطورها.
- التعرف على التشفير المتناظر Symmetric ومزاياه.
- التشفير غير المتناظر Asymmetric واستخداماته العملية.
- التطبيقات الشائعة للتشفير في الأعمال والمؤسسات.
- علاقة التشفير بنظام حماية البيانات الشخصية.
- مقدمة في تشريعات حماية الخصوصية مثل GDPR وCCPA.
- دور التشفير في ضمان الامتثال القانوني.

الوحدة الثانية: خوارزميات وتقنيات التشفير المتقدمة:

- خوارزمية AES وأمانها في الاستخدام المؤسسي.
- RSA كخوارزمية لتبادل المفاتيح بأمان.
- تشفير ECC: مزايا الكفاءة والأداء العالي.
- التجزئة Hashing ودورها في حماية السلامة الرقمية.
- خوارزميات SHA-2 و SHA-3 في أمن البيانات.
- بروتوكولات تشفير طبقة النقل TLS/SSL.
- استخدام التشفير في البريد الإلكتروني والتخزين السحابي.
- تطبيقات HMAC في التحقق من النزاهة.
- المقارنة بين خوارزميات التشفير من حيث الأداء والأمان.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

الوحدة الثالثة: تطبيق التشفير في نظام حماية البيانات الشخصية:

- تشفير البيانات أثناء النقل والتخزين.
- دمج التشفير في سياسات أمن المعلومات المؤسسية.
- حماية بيانات العملاء باستخدام تشفير القاعدة.
- التحكم في الوصول المشفر للملفات والسجلات.
- تشفير قواعد البيانات وتطبيقات الأعمال.
- استراتيجيات تشفير البريد الإلكتروني المهني.
- حماية الهوية الرقمية للمستخدمين بالتشفير.
- التشفير في أنظمة إدارة علاقات العملاء CRM.
- ربط التشفير مع أنظمة كشف التسلل والاستجابة للحوادث.

الوحدة الرابعة: التحديات والمخاطر في تنفيذ التشفير:

- ضعف المفاتيح السرية وسوء إدارتها.
- مخاطر الهندسة الاجتماعية واختراق التشفير.
- التأثيرات السلبية على الأداء التشغيلي للنظم.
- التوافق بين التشفير والتقنيات الأخرى.
- السيناريوهات الفعلية لفشل التشفير في المؤسسات.
- تحديات التوافق مع التشريعات المحلية والدولية.
- إدارة المفاتيح المشفرة وتدويرها الآمن.
- التعامل مع الحوادث الأمنية المرتبطة بفشل التشفير.
- قياس مؤشرات أداء نظام التشفير المؤسسي.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

الوحدة الخامسة: أفضل الممارسات لتطبيق آمن لتقنيات التشفير:

- إعداد سياسات تشفير واضحة ومحدثة.
- استخدام تقنيات التشفير المعتمدة والمُوصى بها.
- توثيق عمليات التشفير ومراجعتها بانتظام.
- تنفيذ اختبار الاختراق والتقييم الأمني.
- تدريب الفرق على استخدام أدوات التشفير.
- دمج التشفير في دورات حياة تطوير البرمجيات SDLC.
- تبني حلول أمنية هجينة تدعم التشفير والتوثيق.
- مراقبة استخدام التشفير وتحليل السجلات الأمنية.
- تعزيز الوعي المؤسسي بأهمية تشفير البيانات.

خلاصة وتوصيات الدورة التدريبية:

تقدم دورة تشفير البيانات في نظام حماية البيانات الشخصية، فهماً عميقًا لتقنيات التشفير ضمن إطار حماية البيانات الشخصية. كما تساعد المشاركين على تحويل المعارف النظرية إلى ممارسات فعلية في بيئة العمل. يُوصى المؤسسات بتطبيق التشفير كأحد الأعمدة الأساسية في استراتيجية أمن المعلومات. ويُنصح بتحديث استراتيجيات التشفير باستمرار لمواكبة التهديدات المتجددة.