MERCURY

التحكم المتقدم في تسريبات البيانات واستراتيجيات الدفاع والتحقيق والاستجابة

14 – 18 مارس 2027

المنامة (البحرين)



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

MERCURY

التحكم المتقدم في تسريبات البيانات واستراتيجيات الدفاع والتحقيق والاستجابة

المرجع: 151414_121050 **التاريخ:** 14 – 18 مارس 2027 **المكان:** المنامة (البحرين) **الرسوم:** Euro 5500

المقدمة:

في عالم اليوم الذي تحكمه البيانات، أصبحت حماية المعلومات أحد أهم أولويات المؤسسات على اختلاف أنواعها. ومع تزايد الحوادث المتعلقة بتسريب البيانات، سواء الناتجة عن هجمات إلكترونية معقدة أو أخطاء بشرية أو ضعف في النظم والسياسات، بات من الضروري امتلاك فهم شامل لمسببات التسريبات، وأساليب الوقاية منها، وآليات التعامل السريع والفعال عند حدوثها. تهدف هذه الدورة إلى تزويد المشاركين برؤية متقدمة وعملية حول جميع جوانب تسريب البيانات، من التحليل الفني إلى الاستجابة التنظيمية، لضمان تقوية دفاعات البيانات في مؤسساتهم.

الفئات المستهدفة:

- مدراء ومشرفو أمن المعلومات.
- مسؤولو الامتثال وحوكمة البيانات.
- مدراء تكنولوجيا المعلومات والتحول الرقمي.
- فرق الاستجابة للحوادث الأمنية.
- المهندسون والمحللون في مراكز عمليات الأمن SOC.
- مسؤولو حماية الخصوصية والبيانات الشخصية.
- خبراء إدارة المخاطر والامتثال.
- المستشارون في مجالات الأمن السيبراني والتحقيقات الرقمية.

الأهداف التدريبية:

في نهاية هذا البرنامج، سيكون المشاركون قادرين على:

- فهم السياقات المتقدمة لتسريبات البيانات وطرق حدوثها.
- التعرف على أبرز أنواع التسريبات والتهديدات المرتبطة بها.
- تصميم سياسات حماية متكاملة للبيانات.
- استخدام أدوات تحليل وتقييم مخاطر التسريب.
- تطبيق استراتيجيات الاستجابة السريعة والتعافي بعد التسريبات.
- تعزيز ثقافة الوعي الأمني ضمن بيئات العمل.
- تقييم مدى توافق البنية الأمنية مع أطر الحوكمة العالمية للبيانات.

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

MERCURY

الكفاءات المستهدفة:

- التحليل المتقدم لحوادث تسريب البيانات.
- تطوير السياسات والإجراءات الأمنية.
- القيادة في الاستجابة للحوادث.
- إدارة المخاطر السيبرانية.
- المعرفة بأطر الحوكمة والامتثال مثل GDPR، ISO 27001.
- استخدام أدوات المراقبة والكشف عن الاختراقات.
- التوعية والتدريب الأمني للموظفين.

محتوى الدورة:

الوحدة الأولى، مفاهيم تسريب البيانات وأنواعها وأسبابها المتقدمة:

- التعريف المتقدم لمفهوم تسريب البيانات وأنماطه التقنية والتنظيمية.
- الفروق الدقيقة بين التسريب والاختراق والضياع.
- أنواع التسريبات: عرضية، خبيثة، خارجية، داخلية.
- أسباب التسريبات:
  - الإهمال البشري.
  - نقاط الضعف التقنية.
  - سوء تصميم نظم التخزين.
  - ضعف التشفير أو غيابه.
  - الثغرات الناتجة عن الخدمات السحابية.
- أمثلة واقعية لحوادث تسريب عالمية وتحليلها الفني.

الوحدة الثانية، دورة حياة التسريب واستراتيجيات الوقاية منه:

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

- مراحل التسريب: من التسلل إلى الاستخراج إلى النشر.
- تحليل دورة الحياة باستخدام إطار MITRE ATT&CK.
- الاستراتيجيات الوقائية:
  - تصنيف البيانات الحساسة.
  - ضبط صلاحيات الوصول بدقة Least Privilege.
  - تقنيات تشفير البيانات في الراحة والحركة.
  - أدوات منع فقدان البيانات DLP Systems.
  - تقنيات مراقبة النشاطات المشبوهة.
- أهمية التدقيق الدوري والتقييم الأمني الاستباقي.

الوحدة الثالثة، بناء نظام استجابة وتحقيق فعال لحوادث التسريب:

- إعداد خطة الاستجابة لحوادث تسريب البيانات.
- أدوار ومسؤوليات فرق الطوارئ.
- آليات الكشف والاستجابة السريعة.
- أدوات التحقيق الجنائي الرقمي Digital Forensics.
- توثيق الحادث وتحليل أثره.
- تقنيات حفظ الأدلة الرقمية وتهيئتها للجهات القانونية.
- دراسات حالة لتسريبات وطرق التعامل معها داخليًا وخارجيًا.

الوحدة الرابعة، الأطر القانونية والتنظيمية لتسريبات البيانات:

- قوانين حماية البيانات حول العالم:
  - اللائحة العامة لحماية البيانات الأوروبية GDPR.
  - قانون خصوصية المستهلك في كاليفورنيا CCPA.
  - قانون حماية البيانات في الشرق الأوسط والخليج.
- الإبلاغ الإجباري عن الحوادث والتسريبات.
- تبعات عدم الامتثال والغرامات التنظيمية.
- التزامات الشركات تجاه العملاء والمؤسسات الأخرى.
- السياسات الداخلية للامتثال ومهام مسؤولي الخصوصية.
- التحديات القانونية المتعلقة بالتسريبات عبر الحدود.

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

MERCURY

الوحدة الخامسة، ثقافة الأمان السيبراني وتعزيز الوعي الداخلي:

- دور العنصر البشري في منع التسريبات.
- تصميم برامج توعية أمنية متقدمة للمستخدمين.
- اختبار محاكاة التسريبات والاختراقات Phishing Simulations.
- مؤشرات السلوك المريب التي يجب توعية الموظفين بها.
- بناء ثقافة أمنية مستدامة داخل المؤسسة.
- القياس والتحليل الدوري لمدى فعالية برامج الوعي.
- إدماج الأمن في العمليات اليومية Security by Design & Default.