BLACKBIRD FOR TRAINING

أمن وإدارة إنترنت الأشياء

October 2027 15 – 11

ليون (فرنسا)



أمن وإدارة إنترنت الأشياء

المرجع: 204705_3255298 **التاريخ:** 11 – 15 October 2027 **المكان:** ليون (فرنسا) **الرسوم:** GBP 5900

مقدمة

يشهد العالم تطورًا متسارعًا في تقنيات إنترنت الأشياء، التي أصبحت جزءًا أساسيًا من البنية الرقمية في المؤسسات الصناعية والتجارية والخدمية.

تتيح هذه التقنية الربط الذكي بين الأجهزة والأنظمة لتمكين التحليل الفوري واتخاذ القرارات المستندة إلى البيانات.

إلا أن هذا التوسع الكبير في الاتصال الرقمي أدى إلى ظهور تحديات جديدة تتعلق بالأمن السيبراني، وحماية البيانات، وإدارة الأجهزة المتصلة بكفاءة عالية.

تقدم دورة أمن وإدارة إنترنت الأشياء إطارًا متكاملاً لفهم التهديدات الأمنية المرتبطة بهذا المجال، وتطبيق أفضل الممارسات في تصميم وإدارة أنظمة إنترنت الأشياء الآمنة.

وتركز الدورة على الجوانب التقنية والتنظيمية التي تضمن التشغيل المستدام والموثوق للأجهزة المتصلة ضمن بيئات عمل متعددة.

أهداف الدورة

بنهاية هذه الدورة سيتمكن المشاركون من:

- فهم البنية الأساسية لإنترنت الأشياء ومكوناته الرئيسية.
- تحديد التحديات الأمنية المرتبطة بالأجهزة والاتصالات والبيانات.
- تطبيق أفضل الممارسات لحماية شبكات إنترنت الأشياء.
- تنفيذ آليات التشفير والتحقق من الهوية في الأنظمة الذكية.
- إدارة دورة حياة الأجهزة المتصلة من التسجيل حتى الصيانة والتحديث.
- تحليل الحوادث الأمنية والاستجابة الفعّالة لها.
- تصميم خطط حوكمة وأمن تتناسب مع متطلبات إنترنت الأشياء المؤسسية.
- ربط أنظمة إنترنت الأشياء بالبنية التحتية الرقمية للمؤسسات بشكل آمن ومستدام.



محاور الدورة

اليوم الأول: المفاهيم الأساسية لإنترنت الأشياء

- مقدمة حول تطور تقنيات إنترنت الأشياء.
- مكونات النظام الذكي الأجهزة، المستشعرات، المنصات السحابية.
- بنية الاتصال بين الأجهزة وأنواع البروتوكولات المستخدمة.
- مفاهيم المعالجة الموزعة والذكاء الطرفي.
- تحليل العلاقة بين البيانات والاتصال في بيئات التشغيل.
- تمرين عملي حول تتبع تدفق البيانات في نظام إنترنت الأشياء.

اليوم الثاني: المخاطر الأمنية في إنترنت الأشياء

- التهديدات الشائعة في الأجهزة المتصلة.
- الهجمات القائمة على البروتوكولات وأنظمة التحكم.
- دراسة حالات لاختراقات واقعية وتأثيرها.
- المفاهيم الأساسية للأمن الوقائي والاستجابة للحوادث.
- إعداد استراتيجيات حماية متعددة الطبقات.
- تمرين عملي لمحاكاة هجوم وتحليل الثغرات الأمنية.

اليوم الثالث: إدارة الهوية والتحكم في الوصول

- التعرف على أساليب التحقق والمصادقة في أنظمة إنترنت الأشياء.
- إدارة مفاتيح التشفير وتوزيع الصلاحيات.
- بناء سياسات وصول آمنة للأجهزة والمستخدمين.
- التعامل مع البيانات الحساسة وخصوصية المعلومات.
- تطبيق أنظمة إدارة الهوية الرقمية IAM.
- تمرين عملي لتصميم نظام مصادقة متكامل للأجهزة.



اليوم الرابع: حوكمة وإنفاذ سياسات الأمن

- بناء إطار الحوكمة الأمنية لأنظمة إنترنت الأشياء.
- وضع معايير الامتثال والتنظيم داخل المؤسسات.
- أدوات المراقبة والإدارة المركزية للأجهزة.
- تحليل المخاطر ووضع خطط استمرارية الأعمال.
- مؤشرات الأداء لقياس فعالية الأمن والإدارة.
- تمرين عملي على تصميم لوحة مراقبة أمنية للأجهزة المتصلة.

اليوم الخامس: الاستجابة للحوادث والتحسين المستمر

- إجراءات الاستجابة الفورية للحوادث الأمنية.
- تحليل الأدلة الرقمية وتحديد مصدر الهجمات.
- تطوير خطط التعافي من الأزمات.
- مراجعة استراتيجيات الأمن وتحديثها بشكل دوري.
- تطبيق تقنيات الذكاء الاصطناعي في كشف الأنماط السلوكية المشبوهة.
- تمرين ختامي لمحاكاة إدارة حادث أمني حقيقي وتحليله.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب معرفة متعمقة حول أمن الأجهزة المتصلة وإدارة البيانات.
- تطوير مهارات عملية في تحليل الثغرات والتعامل مع الهجمات.
- تعزيز قدرات التخطيط الأمني والتشغيلي ضمن بيئات رقمية متكاملة.
- تحسين الأداء المؤسسي عبر إدارة ذكية للأجهزة المتصلة.
- تعلم كيفية تطبيق ضوابط الحوكمة والسياسات الأمنية بفاعلية.
- القدرة على ربط الأمن السيبراني بعمليات إنترنت الأشياء التشغيلية.
- فهم أحدث الاتجاهات في الذكاء الاصطناعي وتحليل البيانات ضمن هذا المجال.
- بناء استراتيجية متكاملة لإدارة الأصول الرقمية وإنترنت الأشياء بمرونة وأمان.

الخاتمة

إن أمن وإدارة إنترنت الأشياء يمثلان أحد أهم محاور التحول الرقمي الحديث، حيث يتقاطع الأمان مع الكفاءة التشغيلية لضمان استمرارية الأعمال وحماية البيانات.



هذه الدورة تمنح المشاركين القدرة على بناء أنظمة ذكية وآمنة، مع فهم شامل لكيفية إدارة وتعزيز الأداء في بيئات إنترنت الأشياء المتقدمة.

باتت المؤسسات اليوم تعتمد على الاتصال الذكي في كل تفاصيل أعمالها، مما يجعل امتلاك المعرفة المتعمقة في أمن وإدارة هذه الأنظمة عنصرًا أساسيًا في تحقيق النجاح الرقمي والاستدامة المستقبلية.

