BLACKBIRD FOR TRAINING

أمن الحوسبة السحابية للقادة



أمن الحوسبة السحابية للقادة

مقدمة

يشهد العالم تحولاً متسارعاً نحو الاعتماد على الحوسبة السحابية كركيزة أساسية للعمليات المؤسسية. ومع هذا التحول، تتزايد المخاطر المرتبطة بحماية البيانات، إدارة الوصول، وضمان استمرارية الأعمال. لم يعد أمن الحوسبة السحابية مسألة تقنية بحتة، بل أصبح مسؤولية قيادية تتطلب فهماً استراتيجياً عميقاً وقدرة على اتخاذ قرارات مدروسة.

تقدم دورة أمن الحوسبة السحابية للقادة إطاراً عملياً يركز على تمكين القيادات من فهم المخاطر السحابية وإدارتها بفعالية. كما تساعدهم على مواءمة ضوابط الحماية مع الأهداف المؤسسية، وضمان التوازن بين الابتكار الرقمي وإدارة المخاطر.

تكمن الفائدة العملية لهذه الدورة في تمكين المشاركين من بناء رؤية واضحة لأمن السحابة، وتحليل بيئة التهديدات، ووضع خطط حوكمة فعالة تعزز الثقة في البيئة الرقمية وتحمي الأصول المؤسسية.

أهداف الدورة

تهدف دورة أمن الحوسبة السحابية للقادة إلى تمكين المشاركين من:

- فهم نماذج الحوسبة السحابية ومسؤولياتها المشتركة.
- تحليل المخاطر المرتبطة بالبيئات السحابية.
- تصميم إطار حوكمة لأمن السحابة.
- تقييم ضوابط الحماية وإدارة الامتثال.
- إدارة العلاقة مع مزودي الخدمات السحابية.
- بناء مؤشرات لقياس فعالية الأمن السحابي.
- دعم اتخاذ القرار في مشاريع التحول الرقمي.
- تعزيز ثقافة الوعي الأمني داخل المؤسسة.
- التعامل مع الحوادث السحابية بقدرة قيادية.
- تطوير خطة تحسين مستمرة لأمن السحابة.



محاور الدورة

اليوم الأول: المفاهيم الأساسية لأمن الحوسبة السحابية

- نماذج تقديم الخدمات السحابية.
- توزيع المسؤوليات بين المؤسسة ومزود الخدمة.
- أبرز التهديدات السحابية.
- تحليل المخاطر الاستراتيجية.
- مبادئ الحوكمة السحابية.
- تمرين عملي لتحليل سيناريو تهديد.

اليوم الثاني: إدارة المخاطر والامتثال

- تقييم المخاطر السحابية.
- ضوابط حماية البيانات.
- إدارة الهوية والصلاحيات.
- الامتثال للمتطلبات التنظيمية.
- مراجعة سياسات الأمن المؤسسي.
- دراسة حالة تطبيقية.

اليوم الثالث: القيادة والحوكمة السحابية

- بناء إطار حوكمة متكامل.
- تحديد الأدوار والمسؤوليات.
- إدارة التعاقدات مع مزودي الخدمات.
- قياس نضج أمن السحابة.
- إعداد تقارير للإدارة العليا.
- تمرين عملي على إعداد خطة حوكمة.



اليوم الرابع: الاستجابة للحوادث في البيئة السحابية

- آليات كشف الحوادث.
- إدارة فرق الاستجابة.
- التواصل أثناء الأزمات.
- تحليل الحوادث واستخلاص الدروس.
- تحسين خطط الاستجابة المستقبلية.
- سيناريو تطبيقي متكامل.

اليوم الخامس: التخطيط الاستراتيجي والتحسين المستمر

- تقييم جاهزية المؤسسة للتحول السحابي.
- تحليل الفجوات الأمنية.
- إعداد خطة تطوير مستدامة.
- مراجعة شاملة للمفاهيم.
- مناقشة سيناريوهات قيادية.
- تقييم ختامي للأداء.

لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات!

- تعزيز القدرة على قيادة التحول السحابي بأمان.
- تحسين إدارة المخاطر الرقمية.
- دعم القرارات الاستثمارية في البنية السحابية.
- تعزيز الامتثال وحماية البيانات.
- تحسين التنسيق بين الفرق التقنية والإدارية.
- رفع مستوى الجاهزية للتعامل مع الحوادث.
- تطوير رؤية استراتيجية شاملة لأمن السحابة.
- بناء ثقة مؤسسية في البيئة الرقمية.

الخاتمة

تمثل دورة أمن الحوسبة السحابية للقادة إطاراً عملياً يعزز قدرة القيادات على إدارة المخاطر الرقمية المرتبطة بالتحول السحابي. فهي تجمع بين الحوكمة، إدارة المخاطر، الاستجابة للحوادث، والتخطيط الاستراتيجي ضمن منظومة متكاملة تدعم الاستقرار المؤسسي.



من خلال هذا المسار التدريبي، يكتسب المشاركون أدوات تحليلية ومنهجية تساعدهم على اتخاذ قرارات مبنية على فهم عميق للتهديدات والفرص، وتحقيق توازن فعال بين الابتكار والحماية. كما تسهم الدورة في ترسيخ ثقافة أمنية مستدامة داخل المؤسسة تعزز قدرتها على مواجهة التحديات المستقبلية بثقة وكفاءة.

إن الاستثمار في تطوير مهارات القيادة في أمن الحوسبة السحابية يعد خطوة استراتيجية تدعم استدامة الأداء وتحمي الأصول الرقمية في بيئة تتسم بالتغير المستمر.

