BLACKBIRD FOR TRAINING

دورة إدارة الحوادث الإلكترونية القيادية



دورة إدارة الحوادث الإلكترونية القيادية

مقدمة

تتناول هذه الدورة منهجًا متكاملاً لإدارة الحوادث الإلكترونية داخل المؤسسات وفق إطار منظم يعتمد على التخطيط المسبق، وسرعة الاستجابة، والتحليل الدقيق بعد انتهاء الحادث.

تركز على بناء نظام واضح لإدارة الأزمات التقنية بما يضمن حماية الأصول الرقمية، وتقليل الخسائر، والحفاظ على استمرارية العمليات.

كما توضح العلاقة بين إدارة الحوادث، وإدارة المخاطر، واستمرارية الأعمال، والحوكمة المؤسسية.

تستهدف القيادات التنفيذية، ومديري الإدارات، ومسؤولي أمن المعلومات، ومشرفي الأنظمة التقنية، إضافة إلى المختصين في إدارة المشاريع والرقابة والامتثال.

وتلائم محتوياتها قطاعات متعددة تشمل البنوك، والطاقة، والاتصالات، والجهات الحكومية، والمؤسسات الصناعية والخدمية.

تتمثل الفائدة العملية في تمكين المشاركين من إعداد خطة استجابة واضحة، وتنظيم فرق التعامل مع الحوادث، وتحليل الأسباب الجذرية للمشكلات التقنية، وتطوير إجراءات تمنع تكرارها مستقبلاً.

كما تساعد على تقليل زمن التعطل، وتحسين جودة اتخاذ القرار أثناء الأزمات، وتعزيز التنسيق بين الإدارات المختلفة.

أهداف الدورة

تهدف الدورة إلى تحقيق نتائج عملية قابلة للتطبيق كما يلي:



- التعرف على المفاهيم الأساسية لإدارة الحوادث الإلكترونية.
- فهم المراحل المتتابعة لدورة حياة الحادث.
- تطبيق منهجيات تصنيف الحوادث وفق مستوى الخطورة والتأثير.
- تحليل الأثر التشغيلي والمالي للحوادث.
- إعداد خطة استجابة متكاملة للحوادث الإلكترونية.
- تحديد الأدوار والمسؤوليات داخل فرق الاستجابة.
- تنظيم عملية التواصل الداخلي أثناء الأزمات.
- التعامل مع الجهات الرقابية عند الحاجة.
- قياس أداء فرق الاستجابة من خلال مؤشرات واضحة.
- إعداد تقارير تحليلية بعد انتهاء الحادث.
- تطوير خطط تحسين مستمرة بناءً على نتائج المراجعة.
- تعزيز التكامل بين إدارة الحوادث وإدارة استمرارية الأعمال.

محاور الدورة

اليوم الأول: الأسس التنظيمية لإدارة الحوادث الإلكترونية

- تعريف الحوادث الإلكترونية وأنواعها المختلفة.
- استعراض مراحل إدارة الحادث خطوة بخطوة.
- تحديد مسؤوليات الإدارات المعنية بالاستجابة.
- صياغة سياسة داخلية واضحة لإدارة الحوادث.
- تقييم مستوى الجاهزية المؤسسية.
- تنفيذ تمرين لتحديد نقاط القوة والضعف الحالية.

اليوم الثاني: الاكتشاف المبكر وتصنيف الحوادث

- وسائل اكتشاف الحوادث التقنية مبكرًا.
- آليات الإبلاغ الداخلي عن الحوادث.
- معايير تصنيف الحوادث حسب مستوى التأثير.
- تقييم حجم الضرر المحتمل على العمليات.
- تحديد أولويات المعالجة وفق أهداف المؤسسة.
- دراسة حالة تطبيقية لتحليل حادث واقعي.



اليوم الثالث: إدارة الاستجابة والتنسيق أثناء الأزمة

- تنظيم مركز إدارة الأزمة.
- توزيع المهام بين الفرق التقنية والإدارية.
- إدارة الاتصال الداخلي والخارجي بوضوح.
- التعامل مع الأطراف المتأثرة بالحادث.
- تقليل زمن الاحتواء والسيطرة على الحادث.
- تنفيذ محاكاة عملية لحادث افتراضي.

اليوم الرابع: التحليل والتحقيق في الحوادث

- جمع الأدلة الرقمية بطريقة منظمة.
- تحليل السبب الجذري للحادث.
- مراجعة الإجراءات المتخذة أثناء الأزمة.
- تحديد نقاط الضعف في الأنظمة والسياسات.
- إعداد تقرير شامل للحادث يتضمن التوصيات.
- تطبيق تمرين تحليلي على سيناريو معقد.

اليوم الخامس: التقييم النهائي والتحسين المستدام

- مراجعة شاملة لجميع مراحل إدارة الحادث.
- قياس فعالية خطة الاستجابة.
- تطوير خطة تحسين مستمرة.
- تحديث السياسات والإجراءات الداخلية.
- عرض نتائج التمارين التطبيقية.
- تقييم المشاركين من خلال دراسة حالة ختامية.



لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات!

- تعزيز قدرة المؤسسة على التعامل مع الحوادث الإلكترونية.
- تقليل الخسائر الناتجة عن التوقف التشغيلي.
- تحسين سرعة اتخاذ القرار أثناء الأزمات.
- رفع مستوى التنسيق بين الإدارات المختلفة.
- تطوير مهارات التحليل واتخاذ القرار المبني على البيانات.
- دعم الامتثال للمتطلبات التنظيمية.
- تقليل احتمالية تكرار الحوادث.
- تعزيز استمرارية الأعمال في الظروف الحرجة.

الخاتمة

تمثل إدارة الحوادث الإلكترونية عنصرًا أساسيًا في حماية المؤسسات من المخاطر التقنية المتزايدة.

تقدم هذه الدورة إطارًا عمليًا ومنظمًا للتعامل مع الحوادث بدءًا من الاكتشاف المبكر وحتى التقييم والتحسين بعد الإغلاق.

كما تسهم في تنظيم فرق العمل، وتوضيح المسؤوليات، وتحسين آليات اتخاذ القرار أثناء الأزمات.

يساعد تطبيق المفاهيم التي تغطيها الدورة على تقليل الخسائر التشغيلية، وتحسين سرعة الاستجابة، وتعزيز جاهزية المؤسسة أمام التهديدات الرقمية.

وتعد إدارة الحوادث منهجًا استراتيجيًا يساهم في رفع مستوى الحوكمة التقنية وتحسين الأداء المؤسسي بصورة مستدامة.

