المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

Cybersecurity Leadership and Governance Training

فكرة الدورة

أصبحت القيادة السيبرانية عنصرًا أساسيًا في حماية القيمة المؤسسية واستمرارية الأعمال، خصوصًا مع تصاعد الهجمات الرقمية وتوسع الاعتماد على الخدمات السحابية وسلاسل التوريد التقنية. لم تعد إدارة الأمن السيبراني مسؤولية فنية فقط، بل أصبحت مجالًا حوكميًا يتطلب قرارات استراتيجية، أدوارًا واضحة، سياسات فعالة، ومؤشرات تقيس النضج والمخاطر والجاهزية.

يركز هذا البرنامج التدريبي من AINFCT على تطوير قدرات المشاركين في قيادة الأمن السيبراني ضمن إطار حوكمي متكامل. يتناول البرنامج بناء الاستراتيجية، إدارة المخاطر، السياسات، الامتثال، إدارة الأطراف الثالثة، تقارير الأمن السيبراني للإدارة العليا، وتنسيق الاستجابة للحوادث من منظور قيادي. كما يربط البرنامج بين ممارسات ISO/IEC 27001 وNIST Cybersecurity Framework وCOBIT بما يدعم النضج المؤسسي.

- يوفر البرنامج قيمة عملية متقدمة عبر تحويل متطلبات الأمن السيبراني إلى قرارات حوكمة قابلة للتنفيذ والمتابعة.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تطوير استراتيجية أمن سيبراني مؤسسية.
- تطبيق حوكمة فعالة للأمن السيبراني.
- إدارة مخاطر الأمن السيبراني المؤسسية.
- مواءمة الامتثال مع المتطلبات التنظيمية.
- قيادة الاستجابة للحوادث السيبرانية.
- تقديم تقارير أمنية للإدارة العليا.

منهجية الدورة

- شرح تفاعلي للأطر والمفاهيم القيادية.
- تحليل حالات حوكمة أمن سيبراني.
- تمارين على المخاطر والتقارير التنفيذية.
- مناقشات موجهة حول القرارات السيبرانية.
- تطبيق عملي لبناء خارطة طريق.

أثر الدورة على المنظمة

يمكن تعزيز نضج الأمن السيبراني المؤسسي من خلال:

- تحسين حوكمة القرارات السيبرانية.
- رفع جاهزية إدارة المخاطر.
- تعزيز الامتثال للضوابط التنظيمية.
- توحيد تقارير الأمن السيبراني.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- قيادة مبادرات الأمن السيبراني بفعالية.
- تفسير المخاطر بلغة إدارية.
- تصميم سياسات أمنية قابلة للتطبيق.
- إدارة أصحاب المصلحة أثناء الأزمات.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج القيادات والمتخصصين المعنيين بحوكمة الأمن السيبراني وإدارة المخاطر التقنية. كما يفيد المشاركين الذين يحتاجون إلى ربط القرارات الأمنية بالأهداف المؤسسية والامتثال.

- مدراء الأمن السيبراني وتقنية المعلومات.
- مسؤولو الحوكمة والمخاطر والامتثال.
- مدراء التحول الرقمي والبنية التقنية.
- أعضاء لجان الأمن السيبراني.
- مستشارو التدقيق والرقابة التقنية.

موضوعات الدورة

اليوم الأول: مدخل قيادي إلى الأمن السيبراني

- الدور الاستراتيجي للأمن السيبراني في المؤسسة.
- الفصل بين الإدارة الفنية والحوكمة القيادية.
- التهديدات السيبرانية وتأثيرها على الأعمال.
- الأمن السيبراني كمسؤولية مشتركة.
- مؤشرات النضج القيادي للأمن السيبراني.

اليوم الثاني: أطر حوكمة الأمن السيبراني

- مفهوم الحوكمة في سياق الأمن السيبراني.
- الأدوار والمسؤوليات بين الإدارة والفرق الفنية.
- مبادئ COBIT لحوكمة التقنية والمعلومات.
- العلاقة بين الحوكمة والامتثال والمخاطر.
- بناء نموذج حوكمة قابل للتطبيق.

اليوم الثالث: استراتيجية الأمن السيبراني

- تحديد الرؤية والأولويات السيبرانية.
- ربط الاستراتيجية السيبرانية بأهداف الأعمال.
- بناء خارطة طريق أمنية متعددة المراحل.
- إدارة الاستثمارات الأمنية ومبرراتها.
- قياس تقدم الاستراتيجية ومراجعتها.

اليوم الرابع: إدارة مخاطر الأمن السيبراني

- مفاهيم المخاطر والتهديدات والثغرات.
- تحديد شهية المخاطر السيبرانية.
- تصنيف الأصول والخدمات الحرجة.

- تقييم المخاطر باستخدام منهجيات مهنية.
- تحويل نتائج المخاطر إلى قرارات.

اليوم الخامس: نظام إدارة أمن المعلومات ISMS

- مبادئ نظام إدارة أمن المعلومات.
- متطلبات ISO/IEC 27001 الأساسية.
- نطاق النظام والسياسات والإجراءات.
- التدقيق الداخلي والتحسين المستمر.
- علاقة ISMS بحوكمة الأمن السيبراني.

اليوم السادس: السياسات والضوابط الأمنية

- هيكل السياسات الأمنية المؤسسية.
- تصميم ضوابط أمنية قابلة للقياس.
- ضوابط الوصول والهوية والصلاحيات.
- الضوابط السلوكية والتوعوية للموظفين.
- مراجعة السياسات وتحديثها دوريًا.

اليوم السابع: الامتثال والمتطلبات التنظيمية

- تحليل متطلبات الامتثال السيبراني.
- مواءمة الضوابط مع القوانين والمعايير.
- إدارة أدلة الامتثال والتوثيق.
- التعامل مع المراجعات والتدقيق الخارجي.
- قياس فجوات الامتثال وخطط المعالجة.

اليوم الثامن: إدارة الأطراف الثالثة والموردين

- مخاطر الموردين وسلاسل التوريد الرقمية.
- متطلبات الأمن في العقود التقنية.
- تقييم أمن الموردين قبل التعاقد.

- متابعة التزامات الموردين الأمنية.
- إدارة مخاطر الخدمات السحابية الخارجية.

اليوم التاسع: قيادة برنامج التوعية الأمنية

- دور الثقافة المؤسسية في الأمن السيبراني.
- تصميم رسائل توعوية موجهة للمخاطر.
- بناء حملات توعية قابلة للقياس.
- إدارة سلوكيات المستخدمين عالية الخطورة.
- قياس أثر التوعية على تقليل المخاطر.

اليوم العاشر: مقاييس الأمن السيبراني والتقارير

- مؤشرات الأداء والمخاطر السيبرانية.
- تصميم لوحات متابعة أمنية للإدارة.
- عرض المخاطر بلغة غير فنية.
- تفسير اتجاهات الحوادث والضوابط.
- إعداد تقارير تنفيذية مختصرة.

اليوم الحادي عشر: إدارة الحوادث السيبرانية

- مراحل الاستعداد والاستجابة للحوادث.
- دور القيادة أثناء الحوادث الحرجة.
- تصعيد الحوادث واتخاذ القرار السريع.
- التواصل الداخلي والخارجي أثناء الأزمة.
- دروس ما بعد الحوادث والتحسين.

اليوم الثاني عشر: استمرارية الأعمال والتعافي

- العلاقة بين الأمن السيبراني والاستمرارية.
- تحديد الخدمات والأصول الحرجة.
- متطلبات التعافي من الهجمات السيبرانية.

- سيناريوهات انقطاع الخدمات الرقمية.
- اختبار الجاهزية والتحسين الدوري.

اليوم الثالث عشر: الحوكمة السحابية والتحول الرقمي

- مخاطر الأمن في البيئات السحابية.
- توزيع المسؤوليات في الخدمات السحابية.
- حوكمة الهوية والبيانات في السحابة.
- تأمين مبادرات التحول الرقمي.
- متابعة الامتثال السحابي والتشغيلي.

اليوم الرابع عشر: إدارة أصحاب المصلحة واللجان

- تشكيل لجان الأمن السيبراني الفعالة.
- إدارة العلاقة مع الإدارة العليا.
- بناء توافق بين الأمن والأعمال.
- تقديم قرارات استثمارية أمنية واضحة.
- إدارة مقاومة التغيير الأمني.

اليوم الخامس عشر: تطبيق قيادي متكامل

- تحليل حالة حوكمة أمن سيبراني.
- بناء خارطة طريق أمنية مختصرة.
- تحديد مؤشرات ومخاطر رئيسية.
- إعداد تقرير تنفيذي للإدارة العليا.
- عرض المخرجات ومناقشة التحسينات.

course_daily_schedule

يمتد البرنامج لمدة 15 يومًا تدريبيًا، بواقع 4 ساعات يوميًا. يجمع كل يوم بين العرض التفاعلي، المناقشة، تحليل الحالات، والتمارين التطبيقية. يتم تخصيص الجزء الأخير من البرنامج لتطبيق متكامل يساعد المشاركين على بناء خارطة طريق حوكمة أمن سيبراني وتقديمها بمنظور قيادي.

course_assessment

يتم تقييم المشاركين من خلال التفاعل في الجلسات، تحليل الحالات، التمارين التطبيقية، وجودة المخرجات النهائية. وفي نهاية البرنامج، يحصل المشاركون على شهادة حضور أو إتمام صادرة عن AINFCT وفق متطلبات المشاركة المعتمدة.

course_key_competencies

- قيادة الأمن السيبراني.
- حوكمة الأمن السيبراني.
- إدارة المخاطر السيبرانية.
- إدارة الامتثال الأمني.
- التقارير التنفيذية الأمنية.
- إدارة الحوادث والأزمات.

مكتب القاهرة الرئيسي

القاهرة، جمهورية مصر العربية

7 شارع وهران، الطيران، مدينة نصر

+201152466358

info@ainfct.com

ainfct.com

رقم التسجيل الضريبي: 472920235

مكتب مدريد الفرعي

مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد

training@ainfct.com
ainfct.com