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

إدارة التحقيقات في الجرائم المعلوماتية

فكرة الدورة

تتسم الجرائم المعلوماتية بالتغير المستمر في الأساليب والأدوات، وتشمل نطاقًا واسعًا من الأفعال مثل الاختراق، إساءة استخدام الأنظمة، الاحتيال الرقمي، سرقة البيانات، وتعطيل الخدمات. ويحتاج التعامل معها إلى منهجية تحقيق تجمع بين الفهم الأمني، والتحليل الفني، والإجراءات المنضبطة لحفظ الأدلة الرقمية وإدارة ملف القضية.

يقدم هذا البرنامج التدريبي من AINFCT إطارًا عمليًا لإدارة التحقيقات في الجرائم المعلوماتية، بدءًا من تلقي البلاغ وتحديد نطاق الحادث، مرورًا بجمع الأدلة من الأجهزة والشبكات والحسابات، وتحليل المؤشرات الرقمية، وانتهاءً بتوثيق النتائج وعرضها بصورة مهنية. كما يركز البرنامج على التنسيق بين فرق التحقيق، والأمن السيبراني، والجهات القانونية ذات العلاقة.

يساعد البرنامج المشاركين على بناء مسار تحقيق واضح وقابل للتتبع، ويعزز قدرتهم على التعامل مع الأدلة الرقمية بكفاءة تحافظ على سلامتها وقيمتها المهنية.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- فهم أنواع الجرائم المعلوماتية ومؤشراتها.
- تحديد نطاق التحقيق الرقمي بدقة.
- جمع الأدلة الرقمية وفق إجراءات سليمة.
- تحليل الأنظمة والحسابات والسجلات الرقمية.
- إدارة سلسلة الحيازة بوضوح.
- إعداد تقارير تحقيق مهنية ومترابطة.

منهجية الدورة

- عروض تفاعلية حول مفاهيم التحقيق الرقمي.
- تمارين تحليل على سجلات ومؤشرات رقمية مبسطة.
- دراسات حالة لجرائم معلوماتية شائعة.
- نقاشات جماعية حول سلسلة الحيازة والتوثيق.
- نماذج عملية لإعداد تقارير التحقيق.

أثر الدورة على المنظمة

يمكن تعزيز فاعلية التحقيقات الرقمية المؤسسية من خلال:

- تعزيز جاهزية المؤسسة للتحقيقات المعلوماتية.
- تحسين موثوقية الأدلة الرقمية المستخدمة.
- رفع كفاءة التنسيق بين الفرق المختصة.
- دعم الاستجابة المنهجية للحوادث السيبرانية.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على تطوير مهارات تحقيق رقمية منهجية من خلال:

- تصنيف الجرائم المعلوماتية وفق طبيعتها.
- تحديد مصادر الأدلة الرقمية المهمة.
- تحليل السجلات والمؤشرات الفنية الأساسية.
- توثيق نتائج التحقيق بلغة مهنية.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج العاملين في التحقيقات الأمنية والجرائم الإلكترونية، والفرق الفنية المرتبطة بالأمن السيبراني. كما يفيد المشرفين الذين يحتاجون إلى فهم منهجي لإدارة قضايا ذات طبيعة معلوماتية.

- ضباط وأفراد التحقيقات الجنائية والرقمية.
- العاملون في وحدات مكافحة الجرائم المعلوماتية.
- مختصو الأمن السيبراني والاستجابة للحوادث.
- محللو الأدلة الرقمية والسجلات الأمنية.
- المشرفون على إدارة قضايا تقنية وأمنية.

موضوعات الدورة

اليوم الأول: مدخل إلى الجرائم المعلوماتية والتحقيق الرقمي

- مفهوم الجريمة المعلوماتية ونطاقها العملي.
- الفرق بين الحادث السيبراني والجريمة المعلوماتية.
- أنواع الجرائم المرتبطة بالأنظمة والبيانات والحسابات.
- الأدوار الرئيسية في فرق التحقيق الرقمي.
- مبادئ النزاهة والسرية والحياد في التحقيق.
- التحديات المرتبطة بالاختصاص والبيئة التقنية.

اليوم الثاني: إدارة البلاغ وتحديد نطاق التحقيق

- استقبال البلاغات وتوثيق المعلومات الأولية.
- تحديد الأصول الرقمية والأطراف المتأثرة.
- تقدير مستوى الخطورة والأولوية التشغيلية.
- رسم نطاق التحقيق وحدود الوصول إلى البيانات.
- إعداد خطة تحقيق أولية قابلة للتنفيذ.
- التنسيق مع فرق الأمن السيبراني والدعم القانوني.

اليوم الثالث: جمع الأدلة الرقمية وسلسلة الحيازة

- مصادر الأدلة من الأجهزة، الشبكات، والخدمات السحابية.
- إجراءات العزل والحفظ الأولي للأصول الرقمية.
- توثيق زمن الحصول على الدليل ومصدره.
- إدارة سلسلة الحيازة للأدلة الرقمية.
- التعامل مع السجلات والملفات والبيانات الوصفية.
- الاسترشاد بمتطلبات ISO/IEC 27037 في الجمع.

اليوم الرابع: تحليل الأدلة وبناء التسلسل الزمني

- تحليل سجلات الدخول والأحداث الأمنية.
- قراءة مؤشرات الاختراق وسوء الاستخدام.
- ربط الأدلة الرقمية بالأشخاص والأنظمة.
- بناء التسلسل الزمني للأنشطة المشبوهة.
- تقييم الفرضيات الفنية في ضوء الأدلة.
- الاستفادة من مبادئ ISO/IEC 27042 في التحليل.

اليوم الخامس: التقرير الفني وإدارة ملف القضية

- تنظيم الأدلة والنتائج داخل ملف التحقيق.
- صياغة التقرير الفني بلغة واضحة ومحايدة.
- عرض النتائج للقيادات والجهات المختصة.
- تحديد الثغرات والإجراءات التصحيحية بعد التحقيق.
- تمرين تطبيقي على حالة جريمة معلوماتية.
- مراجعة الدروس المستفادة وتحسين إجراءات التحقيق.

course_daily_schedule

يمتد البرنامج على خمسة أيام تدريبية، بواقع أربع ساعات يوميًا. يبدأ كل يوم بتأطير معرفي لموضوع اليوم، ثم ينتقل إلى تطبيقات عملية ونقاشات تحليلية. ويُختتم البرنامج بتمرين متكامل يساعد المشاركين على إدارة بلاغ جريمة معلوماتية، وجمع أدلته، وتحليلها، وإعداد تقرير مهني.

course_assessment

يعتمد تقييم المشاركين على التفاعل داخل الجلسات، وتنفيذ تمارين جمع وتحليل الأدلة، والمشاركة في دراسة حالة تطبيقية، وإعداد مخرجات تقرير تحقيق مختصر في اليوم الأخير. يحصل المشاركون الذين يستكملون متطلبات الحضور والمشاركة

على شهادة إتمام أو حضور صادرة من AINFCT.

course_key_competencies

- التحقيقات المعلوماتية.
- جمع الأدلة الرقمية.
- تحليل السجلات الأمنية.
- إدارة سلسلة الحيازة.
- بناء التسلسل الزمني.
- إعداد التقارير الفنية.

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