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

ادارة التحقيقات في جرائم الابتزاز الإلكتروني

فكرة الدورة

أصبحت جرائم الابتزاز الإلكتروني من التحديات الأمنية المتزايدة نتيجة توسع استخدام المنصات الرقمية، وتنوع أساليب الجناة في الاستدراج، والتهديد، واستغلال البيانات الشخصية. وتتطلب مواجهة هذا النوع من الجرائم فهمًا منهجيًا لطبيعة السلوك الإجرامي الرقمي، ومهارة في استقبال البلاغات، وتوثيق الوقائع، وتحليل الأدلة الإلكترونية دون الإضرار بسلامتها.

يركز هذا البرنامج التدريبي من AINFCT على بناء قدرات المشاركين في إدارة تحقيقات الابتزاز الإلكتروني وفق خطوات عملية تبدأ من التقييم الأولي للبلاغ، وتمر بجمع المعلومات الرقمية، وتحليل الحسابات والمنصات، وحفظ الأدلة، وتنتهي بإعداد ملف تحقيق واضح وقابل للمراجعة. كما يراعي البرنامج الجوانب الإنسانية والأمنية المرتبطة بحماية الضحية وسرية المعلومات.

يوفر البرنامج محتوى مهنيًا متوازنًا يجمع بين التحقيق الجنائي الرقمي وإدارة الحالة، بما يدعم جودة الاستجابة، ويعزز قدرة الفرق المختصة على التعامل مع الوقائع الحساسة بكفاءة وثقة.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- فهم أنماط جرائم الابتزاز الإلكتروني الحديثة.
- استقبال بلاغات الابتزاز وتقييم درجة الخطورة.
- جمع الأدلة الرقمية مع الحفاظ على سلامتها.
- تحليل الحسابات والمنصات المرتبطة بالجريمة.
- توثيق نتائج التحقيق بصورة مهنية.
- حماية الضحية وسرية المعلومات الحساسة.

منهجية الدورة

- عروض تفاعلية مدعومة بأمثلة تحقيق رقمية.
- سيناريوهات تطبيقية لبلاغات ابتزاز إلكتروني.
- تمارين على حفظ الأدلة وبناء التسلسل الزمني.
- نقاشات موجهة حول حماية الضحايا وسرية البيانات.
- نماذج عملية لتوثيق الوقائع وملفات التحقيق.

أثر الدورة على المنظمة

يمكن تعزيز فاعلية التحقيقات الرقمية المؤسسية من خلال:

- رفع جودة التعامل مع بلاغات الابتزاز الإلكتروني.
- تحسين سلامة الأدلة الرقمية المقبولة للتحقيق.
- تعزيز الاستجابة المؤسسية للحوادث الحساسة.
- دعم التنسيق بين الجهات الفنية والتحقيقية.

أثر الدورة على المتدربين

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

- تمييز مؤشرات الابتزاز الإلكتروني الشائعة.
- إدارة البلاغات الرقمية بطريقة منظمة.
- حفظ الأدلة الإلكترونية وفق إجراءات سليمة.
- إعداد تقارير تحقيق واضحة ومترابطة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج العاملين في المجالات الأمنية والتحقيقية الذين يتعاملون مع بلاغات الابتزاز والتهديدات الرقمية. كما يفيد الفرق الفنية الداعمة للتحقيقات الرقمية وحماية المعلومات.

- ضباط وأفراد التحقيقات الجنائية والرقمية.
- العاملون في وحدات مكافحة الجرائم الإلكترونية.
- موظفو مراكز البلاغات والاستجابة الأمنية.
- محللو الأدلة الرقمية والدعم الفني الأمني.
- المشرفون على إدارة القضايا ذات الطابع الرقمي.

موضوعات الدورة

اليوم الأول: طبيعة جرائم الابتزاز الإلكتروني

- مفهوم الابتزاز الإلكتروني ومراحله السلوكية.
- أنماط التهديد والاستدراج والاستغلال الرقمي.
- الفئات الأكثر تعرضًا ومؤشرات الخطورة.
- الفرق بين الابتزاز، الاحتيال، التشهير، والتهديد.
- التحديات القانونية والفنية في إثبات الجريمة.
- أهمية السرية وحماية الضحية منذ البلاغ الأول.

اليوم الثاني: استقبال البلاغات وتقييم الحالة

- إجراءات المقابلة الأولية مع المبلّغ أو الضحية.
- تحديد المعلومات الأساسية دون تعريض الأدلة للخطر.
- تصنيف مستوى الخطورة والاستعجال الأمني.
- التعامل مع المحتوى الحساس والمواد الشخصية.
- تحديد الحسابات، المنصات، القنوات، والأطراف المرتبطة.
- إعداد خطة أولية لإدارة الحالة والتحقيق.

اليوم الثالث: جمع الأدلة الرقمية وحفظها

- مبادئ سلسلة الحيازة للأدلة الرقمية.
- توثيق الرسائل، الحسابات، الروابط، وبيانات الاتصال.
- استخدام لقطات الشاشة بطريقة قابلة للمراجعة.
- حفظ الملفات والبيانات الوصفية دون تعديل.
- تجنب الأخطاء التي تضعف موثوقية الدليل.
- الاسترشاد بمنهجيات ISO/IEC 27037 في الحفظ.

اليوم الرابع: التحليل الرقمي وبناء مسار التحقيق

- تحليل أنماط التواصل والتهديدات المتكررة.
- ربط الحسابات والأرقام والمعرّفات الرقمية.
- قراءة المؤشرات الفنية الداعمة لتحديد المصدر.
- التعامل مع الحسابات الوهمية والوسائط المتعددة.
- بناء التسلسل الزمني للواقعة الرقمية.
- صياغة فرضيات التحقيق ومراجعتها بالأدلة.

اليوم الخامس: إعداد ملف التحقيق والإجراءات اللاحقة

- تنظيم ملف القضية والمواد الرقمية الداعمة.
- كتابة ملخص تحقيق واضح ومترابط.
- عرض النتائج الفنية بلغة مفهومة للجهات المعنية.
- حماية الضحية أثناء المتابعة والإحالة.
- تمرين تطبيقي على سيناريو ابتزاز إلكتروني.
- استخلاص الدروس وتحسين إجراءات الاستجابة.

course_daily_schedule

يمتد البرنامج على خمسة أيام تدريبية، بواقع أربع ساعات يوميًا. يتضمن كل يوم عرضًا للمفاهيم الأساسية، ثم تطبيقات عملية على سيناريوهات واقعية، مع نقاشات موجهة وتمارين قصيرة تساعد المشاركين على الانتقال من فهم طبيعة الجريمة إلى إدارة البلاغ، وحفظ الأدلة، وتحليلها، وإعداد ملف التحقيق النهائي.

course_assessment

يعتمد تقييم المشاركين على المشاركة في المناقشات، وتنفيذ تمارين حفظ الأدلة، وتحليل سيناريو تدريبي لجريمة ابتزاز إلكتروني، وإعداد مخرجات تحقيق مختصرة في اليوم الأخير. يحصل المشاركون الذين يستكملون متطلبات الحضور

والمشاركة على شهادة إتمام أو حضور صادرة من AINFCT.

course_key_competencies

- تحقيقات الابتزاز الإلكتروني.
- إدارة البلاغات الحساسة.
- حفظ الأدلة الرقمية.
- تحليل الحسابات الرقمية.
- توثيق الوقائع الإلكترونية.
- حماية الضحايا رقمياً.

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