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

Incident Response and Forensics Training

فكرة الدورة

أصبحت الحوادث السيبرانية جزءاً أساسياً من واقع المؤسسات الرقمية، حيث تتنوع مصادرها بين البرمجيات الخبيثة، والهجمات الموجهة، وسوء استخدام الصلاحيات، وتسرب البيانات، والاختراقات المعقدة للبنية التحتية. لذلك لا تكفي الضوابط الوقائية وحدها، بل تحتاج المؤسسات إلى قدرة منظمة على الاكتشاف، والتحليل، والاحتواء، والتعافي، والتعلم من الحوادث.

يركز هذا البرنامج التدريبي من AINFCT على بناء فهم عملي متكامل لدورة حياة الاستجابة للحوادث والتحقيقات الرقمية، مع إبراز العلاقة بين فرق الأمن، والعمليات التقنية، والحوكمة، والاتصال، وحفظ الأدلة الرقمية. ويتناول البرنامج مراحل الاستعداد، والرصد، والتحليل، والتصنيف، والاحتواء، والاستئصال، والتعافي، إضافة إلى مبادئ التحقيق الجنائي الرقمي وتحليل السجلات والذاكرة والشبكات ونقاط النهاية.

يوفر البرنامج قيمة مهنية واضحة من خلال تحويل مفاهيم الاستجابة والتحقيق إلى إجراءات قابلة للتطبيق داخل بيئات العمل، بما يدعم سرعة القرار، ودقة التوثيق، وتقليل أثر الحوادث على الأعمال.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تفسير دورة حياة الاستجابة للحوادث السيبرانية.
- تصنيف الحوادث وفق الأثر والأولوية التشغيلية.
- تطبيق إجراءات الاحتواء والاستئصال والتعافي.
- إدارة الأدلة الرقمية وفق ممارسات سليمة.
- تحليل السجلات والمؤشرات الداعمة للتحقيق.
- توثيق الدروس المستفادة وتحسين الجاهزية.

منهجية الدورة

- عروض تطبيقية تربط المفاهيم بالإجراءات التشغيلية.
- سيناريوهات حوادث واقعية لتحليل القرارات.
- تمارين جماعية على التصنيف والتصعيد والتوثيق.
- نماذج عملية لقوائم التحقق وتقارير الحوادث.
- مناقشات موجهة حول تحسين الجاهزية المؤسسية.

أثر الدورة على المنظمة

يمكن رفع جاهزية المؤسسة للتعامل مع الحوادث السيبرانية من خلال:

- تقليل زمن اكتشاف الحوادث ومعالجتها.
- تحسين تنسيق الفرق أثناء الاستجابة.
- تعزيز جودة التوثيق وحفظ الأدلة.
- دعم التحسين المستمر بعد الحوادث.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم أدوار الاستجابة والتحقيق الرقمي.
- تحليل الحوادث بمنهجية منظمة.
- استخدام مؤشرات الاختراق بفاعلية.
- صياغة تقارير حوادث مهنية.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المختصين الذين يشاركون في اكتشاف الحوادث السيبرانية وتحليلها والاستجابة لها داخل بيئات تقنية أو مؤسسية. كما يفيد العاملين في الأمن السيبراني الذين يحتاجون إلى فهم عملي للتحقيقات الرقمية وحفظ الأدلة.

- محللو الأمن السيبراني ومراكز العمليات الأمنية.
- مسؤولو الاستجابة للحوادث والتحقيقات الرقمية.
- مسؤولو الشبكات والأنظمة والبنية التحتية.
- مختصو إدارة المخاطر والامتثال الأمني.
- مديرو فرق تقنية المعلومات والأمن التشغيلي.

موضوعات الدورة

اليوم الأول: مدخل إلى الاستجابة للحوادث والتحقيقات الرقمية

- مفهوم الحادث السيبراني وأنواعه الشائعة.
- العلاقة بين الأمن الوقائي والاستجابة الفعالة.
- أدوار فرق الاستجابة ومسؤولياتها الأساسية.
- مبادئ التنسيق بين التقنية والإدارة والشؤون القانونية.
- مخرجات الاستجابة الناجحة ومؤشرات النضج.

اليوم الثاني: الحوكمة والسياسات وخطط الاستجابة

- عناصر سياسة الاستجابة للحوادث.
- بناء خطة استجابة قابلة للتفعيل.
- تحديد مستويات التصعيد والمسؤوليات.
- متطلبات الاتصال الداخلي والخارجي أثناء الحوادث.
- اختبار الخطط وتحديثها بشكل دوري.

اليوم الثالث: الاستعداد والجاهزية التشغيلية

- تجهيز الأدوات والموارد والفرق المعنية.
- بناء قوائم التحقق وقنوات الاتصال.
- إدارة الأصول الحرجة ومصادر السجلات.
- التدريب والتمارين المكتبية والسيناريوهات.
- قياس جاهزية الاستجابة قبل وقوع الحوادث.

اليوم الرابع: الاكتشاف والرصد وجمع المؤشرات

- مصادر التنبيهات الأمنية داخل المؤسسة.
- مؤشرات الاختراق ومؤشرات الهجوم.
- تحليل السلوك غير الطبيعي في الأنظمة.

- تجميع السجلات من الشبكات ونقاط النهاية.
- تمييز الحوادث الحقيقية عن الإنذارات الكاذبة.

اليوم الخامس: الفرز الأولي وتصنيف الحوادث

- أساليب التحقق الأولي من التنبيهات.
- تصنيف الحوادث حسب النوع والخطورة.
- تقدير الأثر التشغيلي والأمني.
- تحديد الأولويات ومستويات التصعيد.
- توثيق القرارات الأولية أثناء الفرز.

اليوم السادس: التحليل الفني للحوادث

- تحليل التسلسل الزمني للحادث.
- ربط الأحداث بين مصادر متعددة.
- فهم أساليب المهاجمين وتقنياتهم.
- استخدام القرائن الفنية في دعم القرار.
- تحديد نطاق التأثر والأنظمة المتضررة.

اليوم السابع: الاحتواء قصير وطويل المدى

- اختيار استراتيجية الاحتواء المناسبة.
- عزل الأنظمة المتأثرة دون تعطيل مفرط.
- حماية الأدلة أثناء إجراءات الاحتواء.
- ضبط الحسابات والصلاحيات المعرضة للخطر.
- موازنة الاستمرارية التشغيلية مع السيطرة الأمنية.

اليوم الثامن: الاستئصال والتعافي

- إزالة مسببات الحادث من البيئة.
- معالجة الثغرات والإعدادات الضعيفة.
- استعادة الخدمات والأنظمة بأمان.

- التحقق من عدم عودة النشاط الخبيث.
- إدارة المراقبة المكثفة بعد التعافي.

اليوم التاسع: التحقيقات الرقمية ومبادئ الأدلة

- مفهوم الدليل الرقمي وخصائصه.
- سلسلة الحيازة وحفظ سلامة الأدلة.
- إجراءات جمع الأدلة من الأنظمة.
- الاعتبارات القانونية والتنظيمية للتحقيق.
- توثيق الأدلة بطريقة قابلة للمراجعة.

اليوم العاشر: تحليل السجلات والأحداث

- أنواع السجلات الأمنية والتشغيلية.
- تحليل سجلات الدخول والصلاحيات.
- ربط أحداث الجدران النارية والأنظمة.
- اكتشاف الأنماط المشبوهة في السجلات.
- إعداد تسلسل زمني للحادث من السجلات.

اليوم الحادي عشر: تحليل نقاط النهاية والذاكرة

- مؤشرات الإصابة على أجهزة المستخدمين والخوادم.
- جمع الأدلة من نقاط النهاية.
- مفاهيم تحليل الذاكرة الحية.
- تتبع العمليات والملفات والاتصالات النشطة.
- تحديد البرمجيات الخبيثة والسلوكيات المرتبطة.

اليوم الثاني عشر: تحليل الشبكات والاتصالات

- فهم حركة الشبكة أثناء الحوادث.
- استخدام سجلات الشبكة في التحقيق.
- تحليل الاتصالات الخارجية المشبوهة.

- تحديد قنوات القيادة والسيطرة.
- ربط بيانات الشبكة بمؤشرات الاختراق.

اليوم الثالث عشر: تقارير الحوادث والاتصال المهني

- هيكل تقرير الحادث الأمني.
- صياغة الملخص التنفيذي والفني.
- عرض الأدلة والنتائج دون افتراضات غير مثبتة.
- إدارة الرسائل لأصحاب المصلحة.
- توثيق الإجراءات والقرارات خلال الاستجابة.

اليوم الرابع عشر: الدروس المستفادة والتحسين المستمر

- إجراء مراجعة ما بعد الحادث.
- تحليل الأسباب الجذرية والثغرات التنظيمية.
- تحويل النتائج إلى إجراءات تحسين.
- تحديث السياسات والضوابط وخطط الاستجابة.
- بناء مؤشرات أداء لقياس فعالية الاستجابة.

اليوم الخامس عشر: تطبيق متكامل ومحاكاة حادث

- تنفيذ سيناريو حادث من الاكتشاف إلى التعافي.
- توزيع الأدوار داخل فريق الاستجابة.
- تحليل الأدلة والسجلات والمؤشرات.
- إعداد تقرير حادث مختصر ومهني.
- مراجعة الأداء واستخلاص فرص التحسين.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة مركزة لما سبق، ثم عرض المفاهيم الرئيسية، يلي ذلك تطبيق أو نقاش موجه حول سيناريو مهني، وينتهي اليوم بخلاصة عملية تربط الموضوعات بإجراءات الاستجابة والتحقيق داخل بيئة العمل. يتم توزيع الوقت بما يوازن بين الشرح، والتحليل، والتمارين، والمراجعة.

course_assessment

يعتمد التقييم على المشاركة الفعالة، وتمارين تحليل الحوادث، ومناقشات السيناريوهات، وجودة التوثيق العملي خلال الأنشطة التدريبية. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- إدارة الاستجابة للحوادث.
- التحليل والتحقيق الرقمي.
- تصنيف الحوادث وتحديد الأولويات.
- حفظ الأدلة الرقمية.
- تحليل السجلات والمؤشرات.
- إعداد تقارير الحوادث.
- (REFERENCES USED)

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