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

الأساليب الاحتيالية في اختراق شبكات البنوك وكيفية الوقاية منها

فكرة الدورة

تتعرض شبكات البنوك والمؤسسات المالية لمحاولات احتيال إلكتروني متزايدة تستهدف الأنظمة، بيانات العملاء، قنوات الدفع، والبنية التشغيلية الداعمة للخدمات المصرفية. وتتنوع هذه المحاولات بين التصيد، الهندسة الاجتماعية، البرمجيات الخبيثة، استغلال الثغرات، إساءة استخدام الصلاحيات، والهجمات المركبة التي تجمع بين الجانب التقني والسلوكي.

يركز هذا البرنامج التدريبي من AINFCT على تمكين المشاركين من فهم الأساليب الاحتيالية المستخدمة في اختراق الشبكات المصرفية، وتحليل نقاط الضعف الشائعة، وربط مؤشرات الاختراق بإجراءات الوقاية والاستجابة. كما يتناول البرنامج الضوابط الفنية والتنظيمية المرتبطة بحماية الشبكات، إدارة الوصول، المراقبة الأمنية، الاستجابة للحوادث، والتوعية الداخلية.

ويقدم البرنامج قيمة عملية للمشاركين من خلال ربط مفاهيم الأمن السيبراني بسياق العمل المصرفي، بما يساعد على تقليل فرص الاختراق، تعزيز الجاهزية التشغيلية، وتحسين قدرة الفرق على اكتشاف التهديدات والتعامل معها بفعالية.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تحديد أساليب الاحتيال المستخدمة في اختراق الشبكات المصرفية.
- تحليل مؤشرات الاختراق والأنشطة غير الاعتيادية.
- تطبيق ضوابط الوقاية الفنية والإجرائية.
- تقييم مخاطر الوصول والصلاحيات داخل الشبكات.
- دعم الاستجابة الأولية للحوادث السيبرانية.
- تعزيز الوعي الأمني لدى فرق العمل المصرفية.

منهجية الدورة

- عروض فنية مبسطة تربط الهجمات السيبرانية بسياق العمل المصرفي.
- مناقشات جماعية حول حالات احتيال واختراق واقعية.
- تمارين تحليل مؤشرات اختراق وسجلات أمنية افتراضية.
- سيناريوهات محاكاة للتعامل مع بلاغات وحوادث أمنية.
- تطبيقات عملية لإعداد قوائم تحقق وقائية قابلة للاستخدام.

أثر الدورة على المنظمة

يمكن تعزيز حماية الشبكات المصرفية وتقليل التعرض للاحتيال من خلال:

- خفض احتمالات الاختراق الناتجة عن الثغرات الشائعة.
- تحسين جاهزية المراقبة والاستجابة للحوادث.
- تعزيز الالتزام بضوابط الأمن السيبراني المصرفي.
- حماية بيانات العملاء والعمليات المصرفية الحساسة.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على تطوير قدراتهم في رصد الاحتيال السيبراني من خلال:

- فهم أنماط الهجمات الموجهة للبنوك.
- قراءة مؤشرات الاختراق ضمن بيئات الشبكات.
- تطبيق إجراءات الوقاية قبل التصعيد الفني.
- التعامل المنضبط مع البلاغات والحوادث الأمنية.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج العاملين في البنوك والمؤسسات المالية ممن يتعاملون مع الشبكات، الأنظمة، العمليات الرقمية، الرقابة، أو إدارة المخاطر، ويحتاجون إلى فهم عملي لأساليب الاحتيال السيبراني والوقاية منها.

- موظفو تقنية المعلومات وأمن المعلومات في البنوك.
- مسؤولو الشبكات والدعم الفني والعمليات الرقمية.
- موظفو المخاطر التشغيلية والامتثال والرقابة الداخلية.
- مشرفو الفروع والعمليات المصرفية الرقمية.
- فرق خدمة العملاء المعنية ببلاغات الاحتيال الإلكتروني.

موضوعات الدورة

اليوم الأول: طبيعة الاحتيال السيبراني في البيئة المصرفية

- مفهوم الاحتيال الإلكتروني وعلاقته باختراق شبكات البنوك.
- أبرز الأصول المصرفية المستهدفة داخل الشبكات والأنظمة.
- مسارات الهجوم من الاستطلاع إلى الوصول غير المصرح.
- الفرق بين الخطأ التشغيلي، الاحتيال، والاختراق المتعمد.
- مؤشرات الخطر المرتبطة بسلوك المستخدمين والأنظمة.
- أثر الحوادث السيبرانية على الثقة والامتثال واستمرارية الأعمال.

اليوم الثاني: أساليب الاختراق والاحتيال الشائعة

- التصيد الإلكتروني واستهداف الموظفين والعملاء.
- الهندسة الاجتماعية واستغلال الثقة داخل بيئة العمل.
- البرمجيات الخبيثة وبرمجيات الفدية في الشبكات المصرفية.
- سرقة بيانات الاعتماد واستغلال كلمات المرور الضعيفة.
- استغلال الثغرات في التطبيقات والخدمات المتصلة بالشبكة.
- الاحتيال عبر القنوات الرقمية وأنظمة الدفع والتحويل.

اليوم الثالث: نقاط الضعف ومؤشرات الاختراق

- تحليل نقاط الضعف في الشبكات والأجهزة والخوادم.
- مخاطر الصلاحيات الزائدة والحسابات المشتركة.
- مؤشرات الاختراق في السجلات الأمنية وحركة الشبكة.
- أنماط الاتصال غير الاعتيادية ومحاولات الدخول المتكررة.
- مخاطر الموردين والربط الخارجي مع الأنظمة المصرفية.
- استخدام قوائم التحقق في مراجعة الضوابط الأساسية.

اليوم الرابع: ضوابط الوقاية والحماية المصرفية

- مبادئ الدفاع متعدد الطبقات في حماية الشبكات.
- إدارة الهوية والوصول والمصادقة متعددة العوامل.
- تقسيم الشبكات وعزل الأنظمة الحساسة.
- التحديثات الأمنية وإدارة الثغرات والتصحيحات.
- التوعية الأمنية للموظفين ضد الاحتيال والهندسة الاجتماعية.
- مراقبة الأنظمة والتنبيهات الأمنية وآليات التصعيد.

اليوم الخامس: الاستجابة للحوادث والتحسين المستمر

- خطوات التعامل الأولي مع بلاغات الاختراق والاحتيال.
- احتواء الحوادث وتقليل أثرها على العمليات المصرفية.
- توثيق الحوادث وحفظ الأدلة الرقمية الأولية.
- التنسيق بين فرق الأمن، التقنية، المخاطر، والامتثال.
- مراجعة الدروس المستفادة وتحسين الضوابط الوقائية.
- تطبيق عملي على سيناريو اختراق شبكة مصرفية.

course_daily_schedule

يمتد البرنامج لمدة 5 أيام تدريبية، بواقع 4 ساعات تدريبية يوميًا. يتضمن كل يوم شرحًا تفاعليًا، مناقشات تطبيقية، تمارين تحليل، وسيناريوهات عملية ترتبط بأساليب الاحتيال واختراق الشبكات المصرفية. ويتم توزيع الوقت بما يوازن بين المفاهيم الفنية، تحليل المخاطر، تطبيق الضوابط، ومراجعة إجراءات الاستجابة والتحسين.

course_assessment

يتم تقييم المشاركين من خلال المشاركة في النقاشات، تحليل السيناريوهات، تنفيذ التمارين العملية، وتطبيق قوائم التحقق الخاصة بالوقاية والاستجابة. ويحصل المشاركون في نهاية البرنامج على شهادة حضور أو إتمام صادرة عن AINFCT وفق

متطلبات المشاركة المعتمدة.

course_key_competencies

- الوعي بالاحتيال السيبراني.
- تحليل مؤشرات الاختراق.
- حماية الشبكات المصرفية.
- إدارة الوصول والصلاحيات.
- الاستجابة للحوادث الأمنية.
- الرقابة الوقائية.

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