دورة إدارة مخاطر الاحتيال الرقمي وضوابطه

8 – 12 مارس 2027

القاهرة

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة إدارة مخاطر الاحتيال الرقمي وضوابطه

المرجع: 1243_191798 **التاريخ:** 8 – 12 مارس 2027 **المكان:** القاهرة **الرسوم:** Euro 4100

نظرة عامة

تقدم دورة إدارة مخاطر الاحتيال الرقمي وضوابطه برنامجا متقدما لمدة أسبوع للمتخصصين المسؤولين عن مخاطر الاحتيال في الهويات الرقمية ورحلات العملاء والحسابات والأجهزة والمدفوعات والمنصات والخدمات المتصلة. يربط المشاركون بين أنماط الاحتيال ومعلومات التهديد ورسم الرحلات وإثبات الهوية والمصادقة ومراقبة المعاملات وإشارات الأجهزة والسلوك وعمليات القضايا والتحقيقات والخصوصية وحماية العملاء والمعالجة والأطراف الثالثة واختبار الضوابط.

يبني كل مشارك دليل مخاطر وضوابط الاحتيال الرقمي لخدمة مختارة. ويضم الدليل نموذج التهديد وخريطة مخاطر الرحلة وهندسة الضوابط وفهرس الإشارات وسيناريوهات الكشف ومسار التنبيهات والقضايا وحدود التحقيق وضمانات الخصوصية وتصميم دعم المتضررين ولوحة الأداء وقائمة التحسين. تقدم أجايل للتدريب إدارة الاحتيال الرقمي كنظام تشغيل مستمر الاختبار يجمع الأفراد والعمليات والبيانات والتقنية والحوكمة.

الفئة المستهدفة

- فرق مخاطر الاحتيال واستراتيجيته وعملياته والجرائم المالية
- قادة الخدمات المصرفية الرقمية والمدفوعات والتجارة والمنصات ورحلات العملاء
- فرق الهوية والوصول والمصادقة والأمن السيبراني ومعلومات التهديد
- مختصو تحليل البيانات ومخاطر النماذج وعلوم القرار والمراقبة
- فرق الامتثال والخصوصية والقانون والتدقيق والمخاطر التشغيلية
- فرق التحقيق والنزاعات واسترداد المدفوعات والشكاوى وحماية العملاء
- فرق المنتجات والهندسة وإدارة الموردين وضمان الأطراف الثالثة

تفترض الدورة مسؤولية عن قرارات الاحتيال أو الخدمات الرقمية. ولا تقدم تعليما للاختراق ولا استشارة قانونية ولا صلاحية إنفاذ ولا تستبدل المراجعة الفنية والخصوصية والتحقيقات والمتطلبات التنظيمية.

AGILE LEADERS
Training Center

أهداف الدورة

- رسم تعرض الاحتيال عبر الهويات والأجهزة والحسابات والمعاملات والقنوات والأطراف الثالثة
- تمييز الاختراق والهندسة الاجتماعية والتلاعب بالمدفوعات واحتيال الهوية والإساءة الداخلية
- تصميم ضوابط متعددة الطبقات للمنع والكشف والاستجابة والتعافي
- تعزيز إثبات الهوية والمصادقة واستعادة الحساب ومعالجة المتضررين
- تحويل البيانات وإشارات التهديد إلى سيناريوهات كشف قابلة للتفسير
- حوكمة القضايا والأدلة والخصوصية والإحالات والاستجابة المشتركة
- قياس فعالية الضوابط وأثرها في العميل والتنبيهات الخاطئة والخسائر
- اختبار الضوابط وتحسينها باستمرار مع تغير الأساليب والتقنية

المنتج التطبيقي

يبني المشاركون دليل مخاطر وضوابط الاحتيال الرقمي الذي يتضمن:

- خريطة الخدمة الرقمية ورحلة العميل
- أنماط الاحتيال ونموذج التهديد
- هندسة ضوابط الهوية والحساب
- فهرس الإشارات ومصادر البيانات
- مكتبة سيناريوهات الكشف والحدود
- مسار التنبيه والقضية والتصعيد والإحالة
- ضمانات الخصوصية والعدالة ومعالجة العملاء
- لوحة أداء الضوابط
- قائمة تحسين لمدة تسعين يوما

اليوم 1: مشهد الاحتيال الرقمي ومخاطر الرحلة

- المنظومات الرقمية وحدود الثقة والتبعيات ونقاط التعرض
- الجهات المحتالة ودوافعها وقدراتها وتعاونها وخدمات الاحتيال المنظمة
- الهندسة الاجتماعية وانتحال الشخصية والتصيد واختراق البريد والاحتيال في المدفوعات المصرح بها
- الاستيلاء على الحساب والهوية الاصطناعية واحتيال الطلبات والحسابات الوسيطة والإساءة الداخلية
- رسم التعرض عبر التهيئة والدخول وتغيير الحساب والدفع والدعم والاستعادة والإغلاق

ورشة تطبيقية: إعداد خريطة رحلة تربط الجهات والأساليب والفرص والعواقب والضوابط.

AGILE LEADERS
Training Center

اليوم 2: الهوية الرقمية والمصادقة وحماية الحساب

- مخاطر إثبات الهوية والأدلة والمصادر الموثوقة وقرارات التحقق
- أنماط الهوية المسروقة والمختلقة والاصطناعية والمعدلة والمخترقة
- مستويات المصادقة وربط الجهاز والقياسات الحيوية ومفاتيح المرور والتحقق الإضافي
- تبديل الشرائح وعناوين الشبكات المشبوهة وعمر الجهاز والحساب وأحداث التغيير
- مخاطر الخصوصية وسهولة الوصول والتحيز واحتكاك العميل وفشل التحقق والتظلم

ورشة تطبيقية: تصميم هندسة ضوابط للهوية والحساب بمستويات ضمان واستثناءات وضوابط تعويضية.

اليوم 3: الإشارات والكشف وتحليلات الاحتيال

- إشارات المعاملات والأجهزة والشبكات والسلوك والهوية والعملاء والتهديد
- قواعد الكشف والسيناريوهات والدرجات والنماذج والحدود والسرعة والروابط
- المؤشرات الاستباقية وجودة البيانات وانحراف الخصائص وحدود النماذج وقابلية التفسير
- أولوية التنبيهات والنتائج الخاطئة والقدرة والطوابير ومستويات الخدمة
- اختبار تغطية الكشف أمام الأنماط وتكيف الجهات المحتالة

ورشة تطبيقية: إنشاء فهرس إشارات ومكتبة كشف بمنطق واضح ومصدر بيانات وحدود ومالك واختبار.

اليوم 4: القضايا والتحقيق والاستجابة وحماية العملاء

- إثراء التنبيه والفرز وإنشاء القضية والخطورة والملكية والتصعيد
- سلامة الأدلة والتسلسل الزمني وضبط الوصول والتوثيق وسجلات القرار
- حدود العمل بين الاحتيال والأمن السيبراني والامتثال والخصوصية والقانون والموارد البشرية
- تعليق المعاملات وتقييد الحساب والتحقق الإضافي والتواصل والتدخل المتناسب
- دعم المتضررين والشكاوى والنزاعات وقرارات التعويض والمعالجة

ورشة تطبيقية: تصميم مسار قضية واستجابة لحادث استيلاء على حساب واحتيال مدفوعات منسق.

AGILE LEADERS
Training Center

اليوم 5: الحوكمة وفعالية الضوابط والتكيف

- شهية مخاطر الاحتيال والملكية واللجان والصلاحيات والتصعيد والتقارير
- تبعيات الهوية والمدفوعات والبيانات والسحابة والمنصات والعمليات الخارجية
- مؤشرات محاولات الاحتيال والخسائر الممنوعة وجودة الكشف ونتائج القضايا وأثر العميل
- اختبار الضوابط وإعادة تشغيل السيناريوهات ونتائج الاختبارات ودروس الحوادث
- مراقبة التهديد والتقييم المستمر وحوكمة التغيير وقائمة التحسين

المشروع الختامي: عرض دليل المخاطر والضوابط أمام لجنة حوكمة احتيال محاكية.

أساليب التدريب

- حالات احتيال رقمي ورسم تهديدات رحلة العميل
- ورش الهوية والإشارات والكشف وتصميم الضوابط
- محاكاة التنبيهات والقضايا والاستجابة والمعالجة
- تمارين اختبار الضوابط وقياس الأداء
- مراجعة جماعية للأدلة وقوائم التحسين

مخرجات الدورة

يغادر المشاركون وهم قادرون على ربط أساليب الاحتيال الرقمي بضوابط متعددة الطبقات وإشارات قابلة للاستخدام وقرارات مسؤولة واستجابة متناسبة وأداء قابل للقياس. كما يمكنهم تحسين الحماية مع مراعاة الخصوصية والعدالة واحتكاك العميل والمعالجة.

أسئلة شائعة

هل هذه دورة أمن سيبراني؟

لا، تعالج مخاطر الاحتيال وضوابطه في الخدمات الرقمية وتتقاطع مع الأمن عندما يجمع الحدث الاختراق والاحتيال.

هل تعلم الاختراق الهجومي؟

لا، تدرس الأساليب لأغراض التقييم الدفاعي والكشف والاستجابة والحوكمة فقط.

هل تقتصر على المصارف؟

لا، تنطبق على المدفوعات والتقنية المالية والتجارة والمنصات والاتصالات والخدمات الحكومية.

ما المنتج الذي سأعده؟

ستنجز دليل مخاطر وضوابط يشمل الرحلات والتهديدات والهوية والإشارات والكشف والقضايا والمعالجة والمؤشرات والتحسين.