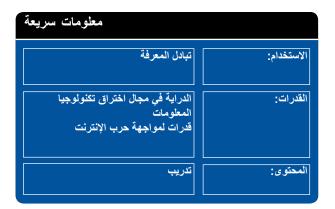
FINTRAINING



يقوم FinAdvisory بتحويل حصة تدريب فردية إلى برنامج تدريب واستشارات محترف من شأنه أن يبني أو يعزز قدرات فريق عمل اختراق تكنولوجيا المعلومات. إن حصص التدريب مكيفة تماماً وفقاً لمتطلبات المستخدم النهائي والتحديات التشغيلية التي يواجهها.

ومن أجل ضمان قابلية الاستخدام الكامل لهذه الدراية المكتسبة، يتم توفير دعم تشغيلي داخل البلاد في خلال البرنامج.

إن الوعي الأمني ضروري لأي حكومة للحفاظ على أمن تكنولوجيا المعلومات والتمكن من تجنب التهديدات التي تطال البنى التحتية لتكنولوجيا المعلومات والتي قد تؤدي إلى فقدان السرية وإلى نقص في البيانات وتوفرها.

من جهة أخرى، إن مواضيع مثل حرب الإنترنت والاعتراض الناشط وتجميع المعلومات الاستخباراتية عبر اختراق تكنولوجيا المعلومات، قد أصبحت أكثر أهمية في الحياة اليومية وهي تحتم على الحكومة تشكيل فرق عمل متخصصة في مجال اختراق تكنولوجيا المعلومات لمواجهة هذه التحديات الجديدة.

يتولى إعطاء حصص FinTraining خبراء عالميون في مجال اختراق تكنولوجيا المعلومات وذلك بطريقة عملية تركز على العمليات الواقعية وعلى ما يتعين على المستخدم النهائي أن يقوم به للتمكن من مواجهة التحديات اليومية التي تعترضه.

برنامج FinAdvisory

- برنامج كامل للاستشارات والتدريب على اختراق تكنولوجيا المعلومات
- تشكيل وتدريب منظم فلريق عمل اختراق تكنولوجيا المعلومات
 - تقييم كامل لأعضاء الفريق
 - حصص تدريب عملية تركز على العمليات الواقعية
 - استشارات تشغيلية داخل البلاد

للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.

أمثلة عن مواضيع حصص التدريب

- تحديد مواصفات المواقع الإلكترونية المستهدفة والأشخاص المستهدفين.
 - تعقب البريد الإلكتروني المجهول
 - ولوج عن بعد إلى حسابات البريد الإلكتروني
 - تقييم أمن خوادم الوب وخدمات الوب
 - استغلال البرمجيات عمليا
 - اختراق تكنولوجيا المعلومات السلكيا (الشبكة اللاسلكية/ مراقب ٨٠٢,١١
 - هجمات على البنى التحتية الأساسية
 - سلب البيانات واعتمادات المستخدم على الشبكات
- مراقبة نقاط الاتصال اللاسلكي ومقاهي الإنترنت وشبكات الفنادق.
- اعتراض الاتصالات وتسجيلها (بروتوكول الصوت عبر الإنترنت VoIP وDECT)
 - استعادة كلمات المرور

