

# دورة C|CT في المهارات الأساسية لفني الأمن السيبراني



## دورة C|CT في المهارات الأساسية لفني الأمن السيبراني

المرجع: 223969\_751 التاريخ: 27 سبتمبر – 1 أكتوبر 2027 المكان: أديس أبابا الرسوم: Euro 6000

### نظرة عامة

دورة C|CT في المهارات الأساسية لفني الأمن السيبراني دورة تأسيسية لمدة أسبوع للفنيين المبتدئين وموظفي الدعم التقني والمحليين الجدد ومديري الشبكات والراغبين في الانتقال المهني، ويعود المشاركون منها بدفتر عمليات فني الأمن السيبراني. يبني المشاركون مهارات فني الأمن السيبراني عبر خرائط الأنظمة والشبكات ومراجعة الحسابات والتحقق من التهيئة وتسجيل الثغرات وفرز الحركة والسجلات وتذاكر الحوادث وفحوص التعافي. تطور أجايل للتدريب الممارسة التأسيسية لفني الأمن السيبراني.

### الفئة المستهدفة

- وظائف الدعم التقني المسؤولة عن أجهزة المستخدمين ومعالجة مشكلات الوصول
- وظائف إدارة الشبكات المسؤولة عن الاتصال والتهيئة ورؤية حركة البيانات
- وظائف الأمن المبتدئة المسؤولة عن مراقبة الأحداث وتصعيد النشاط المشتبه به
- وظائف تشغيل الأنظمة المسؤولة عن الحسابات والخدمات والتحديثات والنسخ الاحتياطي
- المتعلمون في بداية المسار المهني المستعدون لتنفيذ مهام أمنية تحت الإشراف

تفترض الدورة أن المشاركين يستطيعون التعامل مع أنظمة التشغيل الشائعة والشبكات الأساسية، وتستبعد الاستغلال المتقدم وتطوير البرمجيات الضارة والاختساب الجنائي والتحضير للشهادات والتدريب على الاختبارات.

### الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تحتاج إلى مهام أمنية تأسيسية متسقة.

- الدعم التقني وعمليات الخدمات
- إدارة الشبكات والأنظمة
- العمليات الأمنية ودعم الحوادث
- الخدمات المالية والرعاية الصحية
- التجزئة والخدمات اللوجستية والرقمية



## أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق حدود مهام الفني والتصعيد
- بناء خرائط الأنظمة والشبكات والحسابات والبيانات
- استخدام قوائم التهيئة الآمنة ومراجعة الوصول
- تحليل أدلة الثغرات وحركة البيانات والسجلات
- ترتيب تذاكر الحوادث ودعم الاحتواء
- تقييم فحوص التعافي وتسليمات الفني

## جدول الدورة

### اليوم 1: تأسيس مهام الفني

- خريطة المهام والمعارف والمهارات وفق NICE Framework
- مصفوفة مسؤوليات فني الأمن السيراني والتصعيد
- ورقة جرد الأصول والخدمات والبيانات
- مخطط بنية الشبكة وحدود الثقة
- خط أساس حسابات نظام التشغيل وخدماته

### اليوم 2: حماية الأنظمة والوصول

- قائمة مراجعة دورة حياة حساب المستخدم
- سجل منح الصلاحيات واستثناءات الوصول
- ورقة التحقق من التهيئة الآمنة للأجهزة الطرفية
- لوحة متابعة حالة التصحيحات والتحديثات
- سجل حماية النسخ الاحتياطي وجاهزية الاستعادة



### اليوم 3: تسجيل الثغرات وأدلة الشبكة

- ورقة التحقق من نتيجة الثغرة
- شبكة أولوية التعرض والمعالجة
- دليل ملاحظة تدفق الحزم والبروتوكولات
- سجل مراجعة قواعد الجدار الناري وتغييراتها
- سجل التقاط أدلة شذوذ الشبكة

### اليوم 4: فرز السجلات والحوادث

- مصفوفة تغطية مصادر السجلات الأمنية
- مراجعة أحداث المصادقة والإدارة
- شجرة قرار فرز التنبيه ودرجة الثقة
- نموذج تصنيف تذكرة الحادث وتصعيدها
- قائمة دعم الاحتواء ومعالجة الأدلة

### اليوم 5: ممارسة عمليات الفني

- تمرين: رسم الأصول والحسابات وحدود الشبكة
- تمرين: التحقق من تهيئة الأجهزة والوصول
- تمرين: ترتيب الثغرات وحالات شذوذ الشبكة
- تمرين: فرز السجلات وإعداد تسليم الحادث
- المشروع الختامي: دفتر عمليات فني الأمن السيبراني

### التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الرعاية الصحية والخدمات المالية والتجزئة والخدمات اللوجستية والرقمية.

- نشاط مقترح: رسم خدمة وأجهزتها وحساباتها وبياناتها ومسارات شبكتها ومالكي التصعيد.
- نشاط مقترح: التحقق من إعدادات الأجهزة والصلاحيات والتحديثات وجاهزية النسخ الاحتياطي.
- نشاط مقترح: تحليل سجلات الثغرات وملاحظات الحزم وسجلات المصادقة والأحداث الإدارية.
- نشاط مقترح: تصنيف تذكرة حادث وتسجيل دعم الاحتواء وإعداد تسليم التعافي.



## الأسئلة الشائعة

### لمن تناسب دورة C|CT التأسيسية لفني الأمن السيبراني، وماذا تفترض؟

تناسب الفنيين المبتدئين وموظفي الدعم والمحليين الجدد ومديري الشبكات والراغبين في الانتقال المهني، وتفترض القدرة على التعامل مع أنظمة التشغيل والشبكات الأساسية.

### كيف تختلف دورة فني الأمن السيبراني عن تدريب اختبار الاختراق؟

تنمي دورة فني الأمن السيبراني مهارات العمليات الدفاعية ومعالجة الأدلة والتصعيد تحت الإشراف، بينما يركز اختبار الاختراق على اكتشاف نقاط الضعف والاستغلال المصريح به.

### كيف يستخدم فنيو الأمن السيبراني السجلات لفرز الحوادث؟

يقارن فنيو الأمن السيبراني أحداث المصادقة والإدارة والشبكة والتطبيق والنظام، ويحددون الانحرافات ويسجلون الأدلة ويقدمون الثقة ويصعدون وفق معايير محددة.

### كيف يرتب فنيو الأمن السيبراني نتائج الثغرات؟

يجمع فنيو الأمن السيبراني بين الأصل المتأثر والتعرض والاستغلال الملحوظ وأهمية الأعمال والمعالجة المتاحة وأدلة التحقق لدعم ترتيب الأولويات.

### ماذا يتضمن دفتر عمليات فني الأمن السيبراني؟

يتضمن دفتر عمليات فني الأمن السيبراني خرائط الأصول ومراجعات الحسابات وفحوص التهيئة وسجلات الثغرات وملاحظات الحركة وقرارات السجلات وتذاكر الحوادث وفحوص التعافي وملاحظات التسليم.

## الخاتمة

يعود المشاركون بدفتر عمليات فني الأمن السيبراني الذي ينظم المهام والأدلة التأسيسية. يحول الدفتر المعالجة غير المنظمة إلى حماية وملاحظة وفرز وتصعيد ودعم تعاف يمكن تتبعه. ويساعد الفنيين على تطبيق فحوص متسقة وتوثيق القرارات وتسليم العمل للفرق المتخصصة بسياق قابل للاستخدام.