



## دورة محلل التهديدات السيبرانية المبتدئ للملاحقة المتقدمة



**AGILE LEADERS**  
Training Center

## دورة محلل التهديدات السيبرانية المبتدئ للملاحقة المتقدمة

### نظرة عامة على الدورة

في المشهد السيبراني اليوم، تواجه المؤسسات تهديدات مستمرة تتطلب متخصصين ماهرين في الأمن السيبراني لتحديد المخاطر وتحليلها وتخفيفها بفعالية. صُممت دورة محلل التهديدات السيبرانية المبتدئ CCTA - الملاحقة المتقدمة للتهديدات لتزويد المشاركين بأحدث تقنيات وملاحقة التهديدات وأطر استخبارات التهديدات السيبرانية واستراتيجيات الاستجابة للحوادث.

تهزج هذه الدورة الشاملة لمحللي التهديدات السيبرانية بين المعرفة النظرية والمختبرات العملية، مما يوفر خبرة واقعية في ملاحقة التهديدات. سيتعلم المشاركون كيفية تطبيق أطر استخبارات التهديدات السيبرانية، وتطوير منهجيات تقييم المخاطر، وتعزيز الوضع الأمني لمؤسساتهم.

من خلال الحصول على شهادة محلل التهديدات السيبرانية من PECB، يثبت المحترفون خبرتهم في إدارة مخاطر الأمن السيبراني، والملاحقة المتقدمة للتهديدات، واكتشاف التهديدات السيبرانية. سواء كنت محللاً في مركز العمليات الأمنية SOC، أو مستجيباً للحوادث، أو مختبر اختراق، فإن هذه الدورة تقدم المهارات والمعرفة اللازمة للتفوق في استراتيجيات الدفاع السيبراني.

### الجمهور المستهدف

- متخصصو الأمن السيبراني محللو مركز العمليات الأمنية، المستجيبون للحوادث، مهندسو الأمن
- مديرو البنية التحتية لتقنية المعلومات
- مديرو ورؤساء الأمن
- المخترقون الأخلاقيون ومختبرو الاختراق
- متخصصو إدارة المخاطر
- المتخصصون الطموحون في مجال الأمن السيبراني

### الإدارات التنظيمية المستهدفة

- فرق مركز العمليات الأمنية SOC
- فرق الاستجابة للحوادث والتحقيق الجنائي الرقمي
- إدارات أمن وتقنية المعلومات والامتثال
- فرق استخبارات التهديدات وحوكمة الأمن السيبراني
- إدارات إدارة المخاطر والتحقيق

### القطاعات المستهدفة

- المؤسسات المالية وال مصرفية
- الرعاية الصحية والصناعات الدوائية
- الحكومة والدفاع
- الاتصالات وخدمات تقنية المعلومات
- التجارة الإلكترونية والتجزئة
- الطاقة والبنية التحتية الحيوية



## أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تحديد التهديدات السيبرانية وأطر الهجوم لتقييم المخاطر التنظيمية
- تطوير استراتيجيات استخبارات التهديدات السيبرانية للتنبؤ بالهجمات وتخفيفها
- تطبيق تقنيات وملاحقة التهديدات المتقدمة لاتخاذ تدابير أمنية استباقية
- تنفيذ خطط الاستجابة للحوادث وإدارتها لتقليل الحوادث السيبرانية
- استخدام تقنيات المراقبة السيبرانية لتعزيز اكتشاف التهديدات
- صياغة فرضيات وملاحقة التهديدات والتحقق منها باستخدام مناهج قائمة على البيانات
- إجراء تحقيقات جنائية سيبرانية لتحليل أنماط الهجوم
- تطبيق استراتيجيات التحسين المستمر للأمن السيبراني لتعزيز الدفاعات

## منهجية التدريب

يجمع هذا التدريب التفاعلي في مجال الأمن السيبراني بين:

- جلسات مباشرة يقودها خبراء مع دراسات حالة واقعية
- تدريب عملي على تحليل التهديدات السيبرانية باستخدام أدوات متقدمة
- سيناريوهات هجوم سيبراني محاكاة للاختبار جاهزية الاستجابة للحوادث
- أفضل ممارسات الصناعة للاهتمام والحوكمة في مجال الأمن السيبراني

## أدوات الدورة

- قوالب أطر الهجوم السيبراني للتطبيق في العالم الحقيقي
- الوصول إلى موارد الأمن السيبراني عبر الإنترنت للتعلم المستمر
- دراسات حالة في استخبارات التهديدات لفهم تكتيكات الخصوم

## جدول أعمال الدورة

### اليوم الأول: أسس تحليل التهديدات السيبرانية واستخباراتها

- الموضوع 1: مقدمة في تحليل التهديدات السيبرانية وأهداف الدورة التدريبية
- الموضوع 2: نظرة عامة على التهديدات السيبرانية - الأنواع والخصائص ونقلات الهجوم
- الموضوع 3: استخبارات التهديدات السيبرانية - النماذج والمصادر الرئيسية
- الموضوع 4: أطر التهديدات والهجمات السيبرانية CK&ATT MITRE, Chain Kill Cyber Martin Lockheed
- الموضوع 5: نهج التهديدات - تحديد وتقييم المخاطر المحتملة
- الموضوع 6: فهم دور محلي التهديدات السيبرانية في العمليات الأمنية
- تأمل ومراجعة: النقاط الرئيسية المستفادة من استخبارات التهديدات السيبرانية والنظر



## اليوم الثاني: استراتيجيات وملاحقة التهديدات وتخطيط الاستجابة للحوادث

- الموضوع 1: أساسيات خطط الاستجابة للحوادث وإدارتها
- الموضوع 2: أساسيات وملاحقة التهديدات - استراتيجيات الذهن الاستباقي
- الموضوع 3: إعداد برنامج لملاحقة التهديدات - تحديد الأهداف والغايات
- الموضوع 4: تنفيذ عملية وملاحقة التهديدات - التقنيات والمنهجيات
- الموضوع 5: اكتشاف الحوادث والاستجابة لها - دمج عمليات مركز العمليات الأمنية
- الموضوع 6: إدارة مخاطر الذهن السيبراني - تحديد ومعالجة نقاط الضعف
- تأمل ومراجعة: أفضل الممارسات لتنفيذ الاستجابة للحوادث وملاحقة التهديدات

## اليوم الثالث: الملاحقة المتقدمة للتهديدات والاستفادة من استخبارات التهديدات

- الموضوع 1: جمع البيانات وتحليلها لملاحقة التهديدات
- الموضوع 2: صياغة فرضيات وملاحقة التهديدات والتحقق منها
- الموضوع 3: تقنيات إعداد التقارير والتوثيق لملاحقة التهديدات السيبرانية
- الموضوع 4: أطر استخبارات التهديدات - التنفيذ العملي في المؤسسات
- الموضوع 5: تقنيات المراقبة السيبرانية - تعزيز الاكتشاف المستمر للتهديدات
- الموضوع 6: تدريب مركز العمليات الأمنية SOC - تحسين كفاءة الاستجابة للتهديدات
- تأمل ومراجعة: الدروس المستفادة من الملاحقة العملية للتهديدات والاستفادة من استخباراتها

## اليوم الرابع: ثقافة الذهن السيبراني والامتثال والتحسين المستمر

- الموضوع 1: مقاييس وملاحقة التهديدات - قياس الأداء والفعالية
- الموضوع 2: برامج التوعية والتدريب في مجال الذهن السيبراني - تعزيز الدفاعات التنظيمية
- الموضوع 3: الامتثال والحوكمة في الذهن السيبراني - النظر واللوائح
- الموضوع 4: التحقيق الجنائي السيبراني - تتبع وتحليل الحوادث السيبرانية
- الموضوع 5: التحسين المستمر في ملاحقة التهديدات السيبرانية - استراتيجيات الذهن التكييفية
- الموضوع 6: استراتيجيات تخفيف التهديدات السيبرانية - تقوية آليات الدفاع
- تأمل ومراجعة: استراتيجيات لتطوير ثقافة أمان سيبراني مرنة

## اليوم الخامس: التقييم العملي ومراجعة الدورة

- الموضوع 1: شهادة الاعتراف المهني في الذهن السيبراني - نظرة عامة على الاختبار والتحضير له
- الموضوع 2: المحاكاة النهائية لملاحقة التهديدات السيبرانية - دراسات حالة واقعية
- الموضوع 3: الاختراق الأخلاقي وملاحقة التهديدات - فهم منظور الخصم
- الموضوع 4: تدريب على اكتشاف تهديدات أمن الشبكات - تحديد التهديدات الخفية
- الموضوع 5: أفضل الممارسات لاستراتيجيات الدفاع السيبراني - دروس من خبراء الصناعة
- الموضوع 6: التطوير الوظيفي في تحليل التهديدات السيبرانية - الخطوات التالية للمحللين المبتدئين
- تأمل ومراجعة: مراجعة الدورة، النقاط الرئيسية المستفادة، والاستعداد للحصول على الشهادة

## الأسئلة الشائعة

ما هي المؤهلات أو المتطلبات المحددة اللازمة للمشاركين قبل التسجيل في الدورة؟

يجب أن يكون لدى المشاركين معرفة أساسية بالذهن السيبراني وإلمام بمبادئ أمن الشبكات. وعلى الرغم من أن الخبرة السابقة في تحليل التهديدات أو عمليات مركز العمليات الأمنية أو الاستجابة للحوادث مفيدة، إلا أنها ليست إلزامية.



كم تبلغ مدة الجلسة اليومية، وما هو إجمالي عدد ساعات الدورة؟

تستمر كل جلسة يومية من 4 إلى 5 ساعات، وتشمل مختبرات تفاعلية ومناقشات وتمارين عملية. تبلغ مدة الدورة الإجمالية من 20 إلى 25 ساعة على مدار خمسة أيام.

ما هي الأدوات التي سيستخدمها المشاركون خلال التمارين العملية لملاحقة التهديدات؟

سيستكشف المشاركون أدوات الازمن السيبراني مفتوحة المصدر لاكتشاف التهديدات والتحقيق الجنائي الرقمي وتحليل استخبارات التهديدات السيبرانية. ورغم عدم توفير برامج مملوكة، تقدم الدورة رؤى حول الأدوات الأمنية الرائدة في الصناعة.

بماذا تختلف هذه الدورة عن دورات محلي التهديدات السيبرانية الأخرى

تتميز دورة محلل التهديدات السيبرانية المعتمد CCTA - الملاحقة المتقدمة للتهديدات بما يلي:

- دمج أطر تحليل التهديدات السيبرانية الواقعية مع المختبرات العملية
- التركيز على تقنيات ملاحقة التهديدات الاستباقية، وليس فقط التدابير الأمنية التفاعلية
- تقديم تقنيات متقدمة للمراقبة السيبرانية من أجل الكشف المستمر عن التهديدات
- توفير تدريب يقوده خبراء من متخصصي الازمن السيبراني ذوي الخبرة في هذا المجال
- التوافق مع المعايير العالمية للائتمثال والحوكمة في مجال الازمن السيبراني

## فئات الدورات التدريبية

|                                                    |                                                     |
|----------------------------------------------------|-----------------------------------------------------|
| الدورات التدريبية في مجال البيئة والاستدامة        | دورات إدارة الجودة وتطوير العمليات                  |
| دورات إدارة و تحليل البيانات ودورات علم البيانات   | دورات إدارة و تطوير الموارد البشرية                 |
| دورات الذهن السيرياني ودورات تقنية المعلومات       | دورات الاتصال الجماهيري و السياسات والعلاقات العامة |
| دورات التدريب القانوني والهشتريات والتعاقدات       | دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات |
| دورات الحوكمة وإدارة المخاطر والامتثال             | دورات السكرتارية و إدارة المكاتب                    |
| دورات الصحة والسلامة والذهن المهني                 | دورات الصيانة ودورات المجالات الهندسية المتنوعة     |
| دورات المحاسبة و التهويل و دورات الإدارة المالية   | دورات المهارات الشخصية وتطوير الذات                 |
| دورات في مجالات القيادة والإدارة                   | دورات معتمدة من قبل هيئات دولية                     |
| دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقية |                                                     |



## معدن التدريب

|                                      |                                         |                                    |
|--------------------------------------|-----------------------------------------|------------------------------------|
| أكر<br>غانا                          | أثينا<br>اليونان                        | أبوظبي<br>الإمارات العربية المتحدة |
| الجبيل<br>المملكة العربية السعودية   | استنبول<br>تركيا                        | أهستردام<br>هولندا                 |
| الرياض<br>المملكة العربية السعودية   | الدوحة<br>قطر                           | الدار البيضاء<br>المغرب            |
| المنامة<br>مملكة البحرين             | الكويت<br>الكويت                        | القاهرة<br>مصر                     |
| بانكوك<br>تايلند                     | باكو<br>أذربيجان                        | باريس<br>فرنسا                     |
| برلين<br>ألمانيا                     | برشلونة<br>إسبانيا                      | براغ<br>جمهورية التشيك             |
| تيليسي<br>جورجيا                     | بوكيت<br>تايلاند                        | بورتو<br>البرتغال                  |
| جنيف<br>سويسرا                       | جاكارتا<br>جمهورية إندونيسيا            | تورنتو<br>كندا                     |
| روما<br>إيطاليا                      | دبي<br>الإمارات العربية المتحدة         | جوهانسبرغ<br>جنوب أفريقيا          |
| سنغافورة<br>سنغافورة                 | سان دييغو<br>الولايات المتحدة الأمريكية | زنجان<br>تنزانيا                   |
| شيكاغو<br>الولايات المتحدة الأمريكية | نهر الشيخ<br>مصر                        | سيول<br>كوريا الجنوبية             |
| طوكيو<br>اليابان                     | طشقند<br>أوزبكستان                      | طرابزون<br>تركيا                   |
| فرانكفورت<br>ألمانيا                 | عن بعد<br>منصة زووم                     | عمان<br>المملكة الأردنية الهاشمية  |



## مدن التدريب

|                          |                                       |                    |
|--------------------------|---------------------------------------|--------------------|
| كيب تاون<br>جنوب افريقيا | كوالالمبور<br>ماليزيا                 | فيينا<br>النمسا    |
| لندن<br>المملكة المتحدة  | لشبونة<br>البرتغال                    | لانكاوي<br>ماليزيا |
| مسقط<br>سلطنة عمان       | هدريد<br>اسبانيا                      | ماربيا<br>اسبانيا  |
| ميونخ<br>ألمانيا         | ميلان<br>إيطاليا                      | مونترو<br>سويسرا   |
|                          | نيويورك<br>الولايات المتحدة الأمريكية | نيروبي<br>كينيا    |