

دورة استراتيجية الدفاع السيبراني والتحقق منها بمساعدة الذكاء الاصطناعي

31 يناير – 4 فبراير 2027

لانكاوي

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة استراتيجية الدفاع السيبراني والتحقق منها بمساعدة الذكاء الاصطناعي

المرجع: 275_123567 **التاريخ:** 31 يناير – 4 فبراير 2027 **المكان:** لانكاوي **الرسوم:** Euro 6000

نظرة عامة

دورة استراتيجية الدفاع السيبراني والتحقق منها بمساعدة الذكاء الاصطناعي هي دورة تأسيسية لمدة أسبوع لمحللي عمليات الأمن وفرق الدفاع والاستجابة للحوادث وصيد التهديدات والهندسة والمخاطر، ويعود المشاركون منها بخطة استراتيجية الدفاع السيبراني والتحقق منها بمساعدة الذكاء الاصطناعي. تربط الدورة الدفاع السيبراني بمساعدة الذكاء الاصطناعي بمعلومات التهديدات، وتدعم كشف التهديدات بالذكاء الاصطناعي عبر هندسة الكشف السيبراني وفرز التنبيهات والاختبارات الهجومية والمقاييس. تقدم أجايل للتدريب دورة في استراتيجية الدفاع السيبراني بالذكاء الاصطناعي.

الفئة المستهدفة

- فرق عمليات الأمن المسؤولة عن مراقبة الإشارات وفرز التنبيهات
- فرق الدفاع السيبراني المسؤولة عن التغطية والكشف والاستجابة
- فرق الاستجابة للحوادث المسؤولة عن التحقق من الأدلة واختيار الإجراءات
- فرق صيد التهديدات المسؤولة عن الفرضيات والتحقيق الاستباقي
- فرق هندسة الأمن المسؤولة عن قواعد الكشف وجودة البيانات
- فرق المخاطر المسؤولة عن الضوابط والقياس والتصعيد

تفترض الدورة ممارسة المشاركين لمهام الأمن أو المخاطر أو الاستجابة، ولا تتناول حوكمة المخاطر غير التقنية أو إعداد المنصات أو اختبار الاختراق أو اعتماد الاستجابة للحوادث.

الإدارات والقطاعات المستهدفة

تدعم الدورة فرق الدفاع السيبراني والتحليلات الأمنية في قطاعات تعتمد على الخدمات الرقمية والعمليات الحرجة.

- مراكز العمليات الأمنية وفرق الاستجابة للحوادث
- إدارات هندسة الأمن ومعلومات التهديدات
- وظائف المخاطر التقنية وضمان الضوابط
- جهات المالية والرعاية الصحية والخدمات المهنية
- جهات الطاقة والتصنيع والبنية التحتية
- جهات الحكومة والتعليم والقطاع غير الربحي

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة سيكون المشاركون قادرين على:

- تطبيق نطاق دفاع يربط جهات التهديد بالأصول والأثر
- استخدام MITRE ATT&CK وATLAS لمواءمة التغطية
- بناء فرضيات الإشارات وقواعد الكشف وسماتها
- تحليل ثقة التنبيهات والأدلة وأخطاء الكشف
- تقييم الاستجابة والمخاطر والضوابط والاختبارات الهجومية
- بناء خطة دفاع قابلة للتحقق ومقاييس للانحراف

جدول الدورة

اليوم 1: سياق التهديد ونطاق الدفاع

- لوحة مهمة الدفاع السيبراني ونطاقه
- خريطة جهات التهديد والأصول والأثر
- ورقة مواءمة MITRE ATT&CK وATLAS
- مصفوفة حالات استخدام الدفاع المدعوم بالذكاء الاصطناعي
- سجل متطلبات الدفاع وقيوده

اليوم 2: الإشارات وهندسة الكشف

- قائمة معلومات التهديدات وإشاراتها
- فرضية كشف السلوك والشذوذ
- قائمة التحقق من مصدر البيانات وجودتها
- بطاقة تصميم قاعدة الكشف وسماتها
- خريطة التغطية والفجوات والنقاط العمياء

AGILE LEADERS
Training Center

اليوم 3: فرز التنبيهات والاستجابة

- مصفوفة ثقة التنبيه وأولويته
- قائمة التحقق البشري والأدلة
- سجل الإيجابيات الكاذبة وحالات الكشف الفائتة
- شجرة قرار دليل الاستجابة
- حلقة التغذية الراجعة من الكشف إلى الاستجابة

اليوم 4: التحقق الهجومي والضمان

- خريطة سيناريو تهديد الذكاء الاصطناعي ومسار الهجوم
- خطة الاختبار والمحاكاة الهجومية
- مراجعة مراوغة النماذج وتسميمها والتلاعب بها
- سجل مخاطر دفاع الذكاء الاصطناعي وضوابطه
- بطاقة أداء الدفاع وانحرافه

اليوم 5: ممارسة استراتيجية الدفاع السيبراني

- تمرين مقترح: رسم التهديدات وأولويات الدفاع
- تمرين مقترح: تصميم الإشارات ومنطق الكشف
- تمرين مقترح: فرز التنبيهات واختيار الاستجابات
- تمرين مقترح: التحقق من الدفاعات بسيناريوهات هجومية
- المشروع الختامي: خطة استراتيجية الدفاع السيبراني والتحقق منها بمساعدة الذكاء الاصطناعي

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة تحول بيانات الدفاع إلى قرارات كشف واستجابة واختبار قابلة للتتبع.

- نشاط مقترح: رسم جهات التهديد والأصول والأثر ومواءمة MITRE ATT&CK وATLAS مع التغطية
- نشاط مقترح: صياغة فرضية سلوكية وتحديد مصادر البيانات وقاعدة الكشف وسماتها
- نشاط مقترح: فرز تنبيهات متباينة الثقة وتوثيق الأدلة والاستجابة والتغذية الراجعة
- نشاط مقترح: تشغيل سيناريو هجومي وتقييم المراوغة والتسميم والضوابط والانحراف

AGILE LEADERS
Training Center

الأسئلة الشائعة

لمن تناسب دورة استراتيجية الدفاع السيبراني بمساعدة الذكاء الاصطناعي؟

تناسب الدورة محللي عمليات الأمن وفرق الدفاع والاستجابة وصيد التهديدات والهندسة والمخاطر. وتفترض ممارسة مهام أمنية أو رقابية ولا تتطلب خبرة في بناء نماذج الذكاء الاصطناعي.

كيف يختلف الدفاع السيبراني بمساعدة الذكاء الاصطناعي عن تدريب المخاطر السيبرانية غير التقني؟

يركز الدفاع السيبراني بمساعدة الذكاء الاصطناعي على الإشارات والكشف والتنبيهات والأدلة والاستجابة والاختبار، بينما يركز تدريب المخاطر غير التقني على الحوكمة والشهية والإشراف واستمرارية الأعمال.

كيف يدعم الذكاء الاصطناعي كشف التهديدات السيبرانية؟

يدعم الذكاء الاصطناعي كشف التهديدات عبر تحليل السلوك والشذوذ وربط الإشارات وترتيب التنبيهات، مع بقاء جودة البيانات والتحقق البشري وقياس أخطاء الكشف ضرورية.

لماذا يجب اختبار دفاعات الذكاء الاصطناعي بطريقة هجومية؟

يكشف الاختبار الهجومي مسارات المراوغة والتسميم والتلاعب والنقاط العمياء قبل الاعتماد على الدفاع، ويساعد الفرق على توثيق الضوابط والفجوات وإجراءات المعالجة.

ماذا تتضمن خطة استراتيجية الدفاع السيبراني والتحقق منها بمساعدة الذكاء الاصطناعي؟

تتضمن الخطة نطاق الدفاع وخرائط التهديد والتغطية وفرضيات الكشف ومصادر البيانات وقواعد الفرز وأدلة الاستجابة والسيناريوهات الهجومية والضوابط ومقاييس الأداء والانحراف.

الخاتمة

يعود المشاركون بخطة استراتيجية الدفاع السيبراني والتحقق منها بمساعدة الذكاء الاصطناعي تربط التهديدات والإشارات والكشف والتنبيهات والاستجابة والاختبارات. تجعل الخطة فرضيات الدفاع والأدلة والفجوات والضوابط ظاهرة لفرق الأمن والمخاطر. وتدعم مراجعة الأداء والانحراف وتحسين قرارات الكشف والاستجابة في العمل.