دورة الدفاع المتقدم عن شبكات المؤسسات

31 مايو – 4 يونيو 2027

مدريد

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة الدفاع المتقدم عن شبكات المؤسسات

المرجع: 1651_221961 **التاريخ:** 31 مايو – 4 يونيو 2027 **المكان:** مدريد **الرسوم:** Euro 5700

نظرة عامة

دورة الدفاع المتقدم عن شبكات المؤسسات هي برنامج مهني لمدة أسبوع لممارسي أمن الشبكات ومراكز العمليات والاستجابة للحوادث والبنية والهندسة الأمنية، ويغادر المشاركون بخطة لتحسين الدفاع الشبكي. تعالج الدورة الفجوات بين البنية والقياسات والكشف والصيد والاستجابة عبر تحليل مناطق الثقة وإدارة الأجهزة وتحليل الحركة والكشف القائم على التهديد والتحقق المصرح به. تطور أجايل للتدريب القدرة التطبيقية في الدفاع المتقدم عن شبكات المؤسسات.

الفئة المستهدفة

- فرق أمن الشبكات المسؤولة عن البنية والضوابط الدفاعية
- فرق مراكز العمليات المسؤولة عن المراقبة والتحقيق
- وظائف الاستجابة للحوادث المسؤولة عن الاحتواء والأدلة
- فرق البنية التحتية المسؤولة عن تشغيل أجهزة الشبكة بأمان
- مهندسو الكشف المسؤولون عن التحليلات والتغطية
- فرق الضمان الأمني المسؤولة عن التحقق من فعالية الدفاعات

تفترض الدورة أن المشاركين يفسرون بروتوكولات الشبكات والعنونة والتوجيه والضوابط والسجلات، ولا تتناول نشاطا هجوميا ضد أنظمة الإنتاج أو أنظمة الغير.

الإدارات والقطاعات المستهدفة

تخدم الدورة المؤسسات التي تشغل شبكات حرجة عبر البيئات المحلية والسحابية والعمل عن بعد والشركاء.

- عمليات الأمن السيبراني والهندسة والبنية والاستجابة
- عمليات الشبكات والبنية التحتية والسحابة والمنصات
- المصارف والتأمين والاتصالات والتقنية
- الطاقة والمرافق والتصنيع والخدمات اللوجستية
- الرعاية الصحية والتعليم والتجزئة والخدمات المهنية
- الحوكمة والمخاطر والضمان والخدمات الأمنية المدارة

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تحليل الأصول ومناطق الثقة والتدفقات ومسارات الهجوم
- بناء التقسيم وضوابط الشبكة الواعية بالهوية
- استخدام قياسات الحزم والتدفقات وDNS والوكيل والجدار الناري
- تطبيق هندسة كشف تهديدات الشبكات وصيدها
- تشخيص الاختراقات وترتيب إجراءات الاحتواء
- تقييم التغطية الدفاعية عبر تحقق مصرح به

جدول الدورة

اليوم 1: البنية الدفاعية والتعرض

- نتائج NIST CSF 2.0 للدفاع عن الشبكات
- الأصول والخدمات والاعتماديات وتدفقات البيانات
- مناطق الثقة والحدود ومسارات الهجوم
- أمن أجهزة الشبكة ومستوى الإدارة
- خريطة الوضع الحالي للدفاع الشبكي

اليوم 2: التقسيم والثقة الصفرية

- تقسيم الشبكات وعزلها وإنفاذ السياسات
- مبادئ دفاع الشبكات بالثقة الصفرية
- الهوية ووضع الجهاز والوصول إلى الموارد
- مسارات العمل عن بعد والسحابة والشركاء والإدارة
- بنية الضوابط ومراجعة الاستثناءات

AGILE LEADERS
Training Center

اليوم 3: القياسات وهندسة الكشف

- الحزم والتدفقات وDNS والوكيل والجدار وسجلات الأجهزة
- جودة القياسات والوقت والسياق والاستبقاء
- تقنيات أجهزة الشبكة في MITRE ATT&CK
- هندسة كشف تهديدات الشبكات ومنطق التحليلات
- خريطة التغطية وبيانات الاختبار والضبط

اليوم 4: صيد التهديدات والاستجابة

- فرضيات صيد تهديدات شبكات المؤسسات
- الخطوط الأساسية والشذوذ والقنوات المشفرة
- الوصول إلى بيانات الاعتماد والاكتشاف والحركة الجانبية
- القيادة والتحكم والإخراج والأثر
- الاحتواء والأدلة والتعافي والتصعيد

اليوم 5: التحقق والمشروع الختامي

- محاكاة الخصم المصرح بها وضوابط السلامة
- سيناريوهات الفريق البنفسجي والتحقق من الكشف
- فعالية الضوابط والفجوات وأولويات المخاطر
- المقاييس والحوكمة وقائمة التحسين
- المشروع الختامي: خطة تحسين الدفاع الشبكي

التمارين التطبيقية

تستخدم الأنشطة المقترحة أدلة من مختبر مصرح به لربط البنية بالكشف والاستجابة.

- نشاط مقترح: رسم مناطق الثقة والتدفقات الحرجة ومسارات الهجوم المحتملة
- نشاط مقترح: تحليل أدلة الحزم والتدفقات في سيناريو اختراق
- نشاط مقترح: كتابة تحليل كشف شبكي قائم على معلومات التهديد وضبطه
- نشاط مقترح: التحقق من الكشف والاحتواء في تمرين فريق بنفسجي منضبط

AGILE LEADERS
Training Center

الأسئلة الشائعة

لمن تناسب دورة الدفاع المتقدم عن شبكات المؤسسات وما متطلباتها؟

تناسب ممارسي الشبكات ومراكز العمليات والاستجابة والبنية وهندسة الكشف والضمان ذوي الخبرة، وتفترض معرفة عملية بالبروتوكولات والتوجيه وضوابط الوصول والسجلات.

كيف يختلف الدفاع المتقدم عن شبكات المؤسسات عن دورة عامة في الأمن السيبراني؟

يركز الدفاع الشبكي المتقدم على التدفقات وحدود الثقة وأمن الأجهزة والقياسات ومنطق الكشف والصيد والاستجابة والتحقق، بينما تغطي الدورات العامة نطاقا أوسع من الحوكمة والهوية والتطبيقات والبيانات والتوعية.

هل تلغي الثقة الصفرية الحاجة إلى تقسيم الشبكات؟

لا. تزيل الثقة الصفرية الثقة الضمنية المرتبطة بالموقع وتحمي الموارد بقرارات وصول سياقية مستمرة، بينما يظل التقسيم مفيدا لتقليل التعرض وإنفاذ سياسات الاتصال.

كيف يستخدم الدفاع الشبكي القائم على معلومات التهديد إطار MITRE ATT&CK؟

يستخدم المدافعون ATT&CK كلغة مشتركة لتحديد سلوك الخصوم وربط القياسات والكشوف وتصميم فرضيات الصيد واختبار التغطية وكشف الفجوات وترتيب التحسينات.

هل تسمح دورة الدفاع المتقدم عن الشبكات باختبار أنظمة خارجية؟

لا. تتطلب التمارين تفويضا صريحا ونطاقا محددا وبيئة معزولة أو معتمدة وضوابط سلامة وشروط توقف. ولا تمنح الدورة شهادة CAST أو تأييدا أو إذنا باستهداف الأنظمة.

الخاتمة

يعود المشاركون بخطة تحسين الدفاع الشبكي التي تربط التدفقات الحرجة ومناطق الثقة والتقسيم وأمن الأجهزة والقياسات وتغطية ATT&CK وهندسة الكشف والصيد والاحتواء والتحقق والمقاييس والحوكمة. تجعل الخطة الافتراضات والفجوات الدفاعية مرئية. وتساعد الفرق على ترتيب التحسينات واختبار إنتاج الضوابط لأدلة قابلة للاستخدام ضد تهديدات الشبكة.