CONCEPT

حماية الأجهزة الطرفية والكشف والاستجابة EDR:
تقوية الأجهزة وفرز التنبيهات وعزل المضيف

14 – 18 يونيو 2027

لندن - فندق أربع نجوم في وسط لندن



حماية الأجهزة الطرفية والكشف والاستجابة EDR: تقوية الأجهزة وفرز التنبيهات وعزل المضيف

المرجع: 902_21166 **التاريخ:** 14 – 18 يونيو 2027 **المكان:** لندن - فندق أربع نجوم في وسط لندن **الرسوم:** SAR 25300

مقدمة:

تضعف حماية الأجهزة الطرفية بصمت حين تغادر الحواسيب المحمولة المكتب دون تحديثات، وتنتشر صلاحيات المسؤول المحلي، وتخرج البيانات على وحدات USB، وتتراكم تنبيهات EDR دون قرار واضح بعزل الجهاز أو تركه. تقدم هذه الدورة من كور كونسبت لمسؤولي الأنظمة منهجا محايدا تجاه الموردين لتأمين الحواسيب المحمولة والمكتبية والخوادم والأجهزة المحمولة: خطوط أساس التقوية، ودورة التحديثات، وقوائم السماح بالتطبيقات، والتحكم في الأجهزة، وتشفير الأقراص، وفرز بيانات القياس في EDR، وصولا إلى عزل المضيف المخترق وتسليم حالة موثقة إلى مركز العمليات الأمنية. ويبني المشاركون خط أساس لأمن الأجهزة الطرفية ودليل تعامل مع تنبيهات EDR لمنظمة افتراضية.

أهداف الدورة:

- رسم سطح الهجوم على الحواسيب المحمولة والمكتبية والخوادم والأجهزة المحمولة في المنظمة وترتيب درجة التعرض حسب مجموعات الأجهزة
- ضبط خط أساس للإعداد الآمن مستمد من معايير التقوية المتوافق عليها والتحقق منه مع توثيق الاستثناءات
- تشغيل دورة للتحديثات ومعالجة الثغرات على الأجهزة الطرفية ترتب الإصلاحات حسب قابلية الاستغلال وأهمية الأصل
- فرض قوائم السماح بالتطبيقات والتحكم في الأجهزة وتشفير الأقراص وتقليص صلاحيات المسؤول المحلي على مجموعات الأجهزة
- فرز تنبيهات EDR من بيانات العمليات والملفات والسجل والاتصالات الشبكية ثم عزل الجهاز ومعالجته وتسليم الحوادث المؤكدة إلى مركز العمليات الأمنية
- إعداد خط أساس لأمن الأجهزة الطرفية ودليل تعامل مع تنبيهات EDR يتضمن السياسات والاستثناءات ومؤشرات التغطية لمنظمة افتراضية

الفئة المستهدفة:

- وظائف إدارة الأجهزة الطرفية والمكتبية التي تجهز الحواسيب المحمولة ومحطات العمل وتضبطها وتصونها
- وظائف إدارة الخوادم المسؤولة عن تغطية الوكلاء والتقوية وحالة التحديثات على مضيفات Windows وLinux
- وظائف عمليات أمن تقنية المعلومات التي تدير وحدات تحكم حماية الأجهزة الطرفية وسياساتها وطلبات الاستثناء
- وظائف إدارة الأجهزة المحمولة التي تسجل الهواتف الذكية والأجهزة اللوحية وتقيدها وتمسح بياناتها عن بعد
- وظائف دعم البنية التحتية التي تستجيب أولا حين يطلق وكيل الجهاز الطرفي تنبيه كشف

محاور الدورة:

اليوم 1: سطح الهجوم على الأجهزة الطرفية وطبقات الحماية

- أنواع الأجهزة الطرفية في الجرد: الحواسيب المحمولة والمكتبية والخوادم والأجهزة المحمولة وأسطح المكتب الافتراضية
- مسارات الوصول الأولي: حمولات التصيد والمتصفحات المستغلة وبيانات الاعتماد المسروقة ووسائط USB
- طبقات EPP وEDR وXDR: المنع والكشف والربط بين المجالات
- تحليل فجوات تغطية الوكلاء: الأجهزة غير المدارة وغير المتصلة وأنظمة التشغيل غير المدعومة
- بطاقة تقييم التعرض لأسطول أجهزة مختلط

اليوم 2: خطوط أساس التقوية والإعداد الآمن ودورة التحديثات

- معايير التقوية المتوافق عليها: ملفات المستويات والضوابط المقيمة والقيم الموصى بها
- سجل الانحراف عن خط الأساس: المبرر التشغيلي والضوابط التعويضية وتاريخ الانتهاء
- فحص انحراف الإعدادات وتقارير المطابقة لكل مجموعة أجهزة
- تخطيط إدارة التحديثات في المنظمة: التحديد والترتيب والنشر والتحقق
- ترتيب أولوية الثغرات حسب توفر أدوات الاستغلال وأهمية الأصل ودرجة التعرض

اليوم 3: التحكم في التطبيقات والأجهزة والتشفير والصلاحيات

- قواعد السماح بالتطبيقات: طرق الناشر والمسار والبصمة مع الإطلاق بوضع التدقيق
- سياسة التحكم في الأجهزة لوحدات تخزين USB والطابعات Bluetooth والوسائط القابلة للإزالة
- نشر تشفير القرص الكامل وحفظ مفاتيح الاسترداد وإجراء فقدان الحاسوب المحمول
- إزالة صلاحيات المسؤول المحلي والرفع المؤقت عند الحاجة وتدوير كلمات مرور الحسابات المحلية
- تسجيل الأجهزة المحمولة وقواعد الامتثال والفصل بالحاويات والمسح عن بعد

اليوم 4: بيانات القياس في EDR وفرز التنبيهات والعزل والمعالجة

- مصادر بيانات القياس في EDR: شجرة العمليات وأسطر الأوامر وكتابة الملفات والسجل والاتصالات الشبكية
- ورقة فرز التنبيهات: أحكام الإيجابي الصحيح والإيجابي غير الضار والإيجابي الكاذب
- عزل المضيف وإنهاء العمليات وحجر الملفات وإزالة آليات البقاء
- حزمة التصعيد إلى مركز العمليات الأمنية: تسلسل الأحداث والمؤشرات والمضيفات المتأثرة والإجراءات المتخذة
- إدارة أمن الأجهزة الطرفية على نطاق واسع: توارث السياسات ومجموعات الأجهزة والاستثناءات والضبط

اليوم 5: تطبيق مخبري: خط أساس أمن الأجهزة الطرفية ودليل تنبيهات EDR

- إحاطة المنظمة الافتراضية: أسطول الأجهزة ووحدات الأعمال والضوابط الحالية
- تطبيق مخبري: بناء خط أساس لتقوية محطات العمل والخوادم مع سجل الانحراف
- تطبيق مخبري: فرز ثلاثة تنبيهات EDR متدرجة من سرقة بيانات الاعتماد إلى تمهيد لبرمجية فدية
- مجموعة مؤشرات أمن الأجهزة الطرفية: تغطية الوكلاء وزمن التحديث ومطابقة خط الأساس ومدة بقاء المهاجم
- عرض خط أساس أمن الأجهزة الطرفية ودليل تنبيهات EDR ومراجعته من المشاركين

المهارات التي ستكتسبها:

- رسم سطح الهجوم على الأجهزة الطرفية
- بناء خطوط أساس الإعداد الآمن
- ترتيب أولوية تحديثات الأجهزة
- إدارة قوائم السماح بالتطبيقات
- ضبط الوسائط القابلة للإزالة
- تقليص الصلاحيات المميزة
- فرز تنبيهات EDR
- احتواء المضيف المخترق

لماذا تحضر هذه الدورة:

- العودة بخط أساس لأمن الأجهزة الطرفية ودليل تعامل مع تنبيهات EDR جرى بناؤهما في تطبيق مخبري على منظمة افتراضية
- الحكم خلال دقائق على ما إذا كان تنبيه EDR يستدعي العزل أو المعالجة أو الإغلاق مع توثيق السبب
- خفض عدد الأجهزة التي تعمل بصلاحيات مسؤول محلي أو أقراص غير مشفرة أو منافذ USB مفتوحة
- مقارنة ممارسات حماية الأجهزة مع مسؤولين من أساطيل أجهزة في المصارف والرعاية الصحية والطاقة والخدمات الحكومية

الخاتمة:

تبدأ معظم الاختراقات من الأجهزة الطرفية، وعليها تسجل آثارها أيضا. تنتقل الدورة من رسم سطح الهجوم وطبقات EPP وEDR وXDR، إلى خطوط أساس التقوية ومعالجة الانحرافات ودورة التحديثات، ثم إلى قوائم السماح بالتطبيقات والتحكم في الأجهزة وتشفير الأقراص والصلاحيات المحلية وتسجيل الأجهزة المحمولة، وصولا إلى بيانات القياس في EDR وفرز التنبيهات والعزل والتصعيد إلى مركز العمليات الأمنية. ويطبق المشاركون كل ضابط في اليوم الأخير داخل المختبر ليخرجوا بخط أساس لأمن الأجهزة الطرفية ودليل تنبيهات EDR مع مؤشرات للتغطية والمطابقة.