



الدورة التدريبية في مبادئ الأمن السيبراني وحماية الأنظمة والاستجابة للحوادث



الدورة التدريبية في مبادئ الأمن السيبراني وحماية الأنظمة والاستجابة للحوادث

مقدمة:

دورة مبادئ الأمن السيبراني وحماية الأنظمة والاستجابة للحوادث مدتها 5 أيام، وتستهدف العاملين في الدعم الفني والبنية التحتية لتقنية المعلومات وموظفي الأمن المبتدئين، وينتهي فيها المشاركون بإعداد حزمة خط الأساس الأمني والاستجابة الأولية للحوادث. تخسر المنظمات الوقت والبيانات حين تطبق الضوابط الأساسية بشكل متفاوت، وتبقى الثغرات دون معالجة، وتدار الساعة الأولى من الحادثة دون إجراء واضح. يعمل المرشحون فعلاً في إدارة الأنظمة أو الشبكات أو حسابات المستخدمين دون تأهيل أمني منهجي، وتقدم الدورة بأسلوب المختبر العملي باستخدام أدوات فحص الثغرات وتحليل السجلات والتقاط حزم الشبكة. وتقدم كور كونسبت هذه الدورة في مبادئ الأمن السيبراني.

أهداف الدورة:

- شرح التهديدات الشائعة وأساليب الهجوم ومبادئ الأمن بمصطلحات MITRE ATT&CK و NIST CSF 2.0
- اختيار الضوابط الأمنية الأساسية للهويات والشبكات والأجهزة الطرفية وتطبيقات الويب وتطبيقها وفق CIS Controls v8.1
- تشغيل فحوص الثغرات وتفسير نتائجها وترتيب أولويات المعالجة بدرجات CVSS v4.0
- جمع سجلات الأجهزة الطرفية وحركة الشبكة وفحصها لرصد النشاط المشبوه
- فرز التنبيهات الأمنية وتنفيذ الاحتواء الأولي للحوادث وفق NIST SP 800-61 Rev. 3
- إعداد حزمة خط الأساس الأمني والاستجابة الأولية للحوادث للوحدة التي يعمل فيها المشاركون

الفئة المستهدفة:

- موظفو الدعم الفني والبنية التحتية المسؤولون عن الخوادم والأجهزة الطرفية وحسابات المستخدمين
- مسؤولو الأنظمة والشبكات المسؤولون عن الإعدادات والتحديثات الأمنية وصلاحيات الوصول
- موظفو الأمن والمراقبة المبتدئون الذين يراجعون التنبيهات ويصدون الحوادث
- الفنيون المنتقلون إلى العمل الأمني من التطوير أو التشغيل أو مكاتب الخدمة
- موظفو دعم الامتثال والتدقيق في تقنية المعلومات الذين يجمعون أدلة تشغيل الضوابط الأمنية

محاوِر الدورة:

اليوم 1: مشهد التهديدات ومبادئ الأمن وسياق الأصول

- مبادئ السرية والسلامة والتوافر ومفهوم الدفاع متعدد الطبقات
- أنواع الجهات المهددة ودوافعها وربطها بسطح الهجوم
- التصيد الاحتيالي وبرامج الفدية وسرقة بيانات الاعتماد في MITRE ATT&CK قاعدة معرفة أساليب المهاجمين
- وظائف NIST CSF 2.0 إطار الأمن السيبراني لتقييم الوضع الأمني للمنظمة
- حصر الأصول وتصنيف البيانات وفق CIS Controls v8.1 الضوابط الأمنية الحرجة

اليوم 2: الضوابط الأمنية وبنية الحماية

- مجموعات التطبيق في CIS Controls v8.1 واختيار الضمانات المناسبة
- إدارة الهويات والصلاحيات وفرض التحقق متعدد العوامل
- تقسيم الشبكة وقواعد جدران الحماية وتصميم الوصول الآمن عن بعد
- حماية الأجهزة الطرفية وخطوط أساس التحصين وسياسة التحديثات الأمنية
- مخاطر تطبيقات الويب في OWASP Top 10 قائمة أبرز مخاطر الويب ووسائل الحماية الأساسية

اليوم 3: إدارة الثغرات والمراقبة الأمنية

- اكتشاف الشبكة وحصر المنافذ المفتوحة بأداة Nmap
- فحص الثغرات بأداة OpenVAS Greenbone وتفسير النتائج
- تقييم الثغرات بنظام CVSS v4.0 نظام تقييم خطورة الثغرات لترتيب أولويات المعالجة
- جمع السجلات بعرض أحداث ويندوز وأداة Sysmon
- تحليل حركة المرور المشبوهة بالتقاط الحزم في Wireshark

اليوم 4: اكتشاف التهديدات والاستجابة للحوادث

- استعلامات البحث في نظام SIEM إدارة المعلومات والأحداث الأمنية لفرز التنبيهات وربطها
- تحديد مؤشرات الاختراق في السجلات والأجهزة الطرفية
- دورة حياة الاستجابة للحوادث والأدوار وفق NIST SP 800-61 Rev. 3 دليل التعامل مع الحوادث
- خطوات الاحتواء والإزالة والتعافي في حوادث برامج الفدية
- حفظ الأدلة وتوثيق تذاكر الحوادث

اليوم 5: المختبر العملي وحزمة خط الأساس الأمني والاستجابة الأولية

- مختبر فحص الثغرات وبناء قائمة أولويات المعالجة
- مختبر اكتشاف حادثة تصيد من ترويسات البريد والسجلات
- مختبر احتواء حادثة برامج فدية وفق قائمة تحقق للاستجابة
- مراجعة ما بعد الحادثة بنموذج الدروس المستفادة
- استكمال حزمة خط الأساس الأمني والاستجابة الأولية للحوادث

المهارات التي ستكتسبها:

- الوعي بمشهد التهديدات
- اختيار الضوابط الأمنية
- ترتيب أولويات معالجة الثغرات
- تحليل سجلات الأجهزة الطرفية
- تحليل حركة الشبكة
- فرز التنبيهات الأمنية
- احتواء الحوادث
- التوثيق الأمني

لماذا تحضر هذه الدورة:

- تسليم حزمة خط الأساس الأمني والاستجابة الأولية للحوادث إلى مدير تقنية المعلومات ومسؤول أمن المعلومات
- الحسم في ما إذا كان التنبيه أو نتيجة الفحص يستدعي احتواء فوريا أم تحديثا مجدولا أم تصعيدا إلى المختصين
- تفادي الثغرات غير المعالجة والصلاحيات الزائدة وبطء الاستجابة الأولى التي تحول الأحداث البسيطة إلى انقطاعات مكلفة
- توجيه الزملاء في الدعم الفني والتشغيل إلى الإبلاغ عن النشاط المشبوه واتباع قائمة الاستجابة الأولية

الخاتمة:

بعد العودة إلى العمل يعرض المشاركون حزمة خط الأساس الأمني والاستجابة الأولية للحوادث على مدير تقنية المعلومات ومسؤول أمن المعلومات، فيعتمدان عليها في تحديد الضوابط الأساسية التي تفرض أولا، والثغرات التي تعالج في دورة التحديث القادمة، ومن يتصرف في الساعة الأولى من الحادثة، وتستخدم فرق الدعم والتشغيل قوائم التحقق فيها للإبلاغ عن النشاط المشبوه واحتوائه بأسلوب موحد. وبعد أول تنبيه فعلي أو فحص مجدول تراجع الوحدة أزمته الاستجابة وتقدم المعالجة مقارنة بالحزمة، ثم تعدل قوائم التحقق التي لم تحقق المطلوب.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة مبادئ الأمن السيبراني والاستجابة للحوادث؟

يحتاج المشارك إلى إلمام بأنظمة التشغيل وحسابات المستخدمين وأساسيات الشبكات مثل عناوين IP والمنافذ، ولا يشترط عمل سابق في الأمن. وتساعد خبرة إدارة الخوادم أو الأجهزة الطرفية أو أجهزة الشبكة على التقدم بسرعة في تمارين المختبر.

بم تختلف دورة مبادئ الأمن السيبراني والاستجابة للحوادث عن دورات تعقب التهديدات المتقدمة؟

تبنى هذه الدورة الأساس: مبادئ الأمن والضوابط الرئيسية وفحص الثغرات وقراءة السجلات والاستجابة الأولية. أما دورات تعقب التهديدات والعمليات الأمنية المتقدمة فتفترض هذا الأساس، وتركز على ملاحقة المهاجمين وكتابة قواعد الاكتشاف وتبادل المعلومات داخل فريق مراقبة متمرس.

لماذا يعتمد اكتشاف التهديدات على مبادئ الأمن السيبراني مثل حصر الأصول وجمع السجلات؟

لأن الاكتشاف لا يعمل إلا على ما هو معروف ومسجل. فدون حصر الأصول تبقى الأجهزة المجهولة دون مراقبة، ودون سجلات مجمعة لا توجد أدلة يبحث فيها عند ظهور التنبيه. لذلك تحدد المبادئ الأساسية سرعة اكتشاف الحادثة واحتوائها.

ماذا يعود به المشارك من دورة مبادئ الأمن السيبراني والاستجابة للحوادث؟

يعود المشارك بحزمة خط الأساس الأمني والاستجابة الأولية للحوادث: قائمة ضوابط مرتبة حسب الأولوية، وقائمة لمعالجة الثغرات، وإجراء لمراجعة السجلات، وقائمة تحقق للاستجابة الأولية للحوادث الشائعة، جاهزة للمراجعة من مدير تقنية المعلومات ومسؤول الأمن.