BLACKBIRD FOR TRAINING

الأمن المتقدم وإدارة مخاطر المستخدمين



الأمن المتقدم وإدارة مخاطر المستخدمين

المقدمة

تقدم هذه الدورة برنامجًا متقدمًا ومتخصصًا في أمن المستخدمين، مع التركيز على حماية المستخدمين والحسابات والهويات والصلاحيات من التهديدات السيبرانية الحديثة. وتتناول الدورة مخاطر العنصر البشري، وإدارة الهوية والوصول، وحماية الحسابات، والمصادقة المتقدمة، والهندسة الاجتماعية والتصيد الاحتيالي، والتهديدات الداخلية، ومراقبة سلوك المستخدمين، وإدارة مخاطر المستخدمين.

وتركز الدورة على الجانب العملي من خلال دراسة حالات وسيناريوهات واقعية تساعد المشاركين على تحديد مخاطر المستخدمين، واكتشاف الأنشطة المشبوهة، واتخاذ الإجراءات المناسبة لحماية الأنظمة والبيانات.

أهداف الدورة

بنهاية الدورة، سيتمكن المشاركون من:

- فهم المخاطر الأمنية المرتبطة بالمستخدمين والعنصر البشري.
- تقييم وتصنيف مخاطر المستخدمين والحسابات.
- تعزيز حماية الهوية والحسابات والصلاحيات.
- تطبيق مبادئ إدارة الهوية والوصول IAM.
- تطبيق المصادقة متعددة العوامل MFA ووسائل المصادقة الحديثة.
- تطبيق مبدأ الحد الأدنى من الصلاحيات Least Privilege.
- فهم وتطبيق مبادئ Zero Trust.
- اكتشاف وتحليل هجمات التصيد الاحتيالي والهندسة الاجتماعية.
- تحديد مؤشرات التهديدات الداخلية والسلوكيات غير الاعتيادية.
- مراقبة وتحليل الأنشطة الأمنية للمستخدمين.
- تطوير منهجيات فعالة لإدارة مخاطر المستخدمين.



المحاور التدريبية

اليوم الأول: إدارة أمن المستخدمين وتقييم المخاطر

1. دور المستخدم والعنصر البشري في الأمن السيبراني.
2. التهديدات الحديثة التي تستهدف المستخدمين.
3. تقييم مخاطر المستخدمين وتصنيف مستويات الخطورة.
4. إدارة الحسابات والهويات والصلاحيات.
5. دراسة حالة: تقييم مخاطر المستخدمين والحسابات داخل مؤسسة.

اليوم الثاني: الهوية والمصادقة والتحكم في الوصول

1. إدارة الهوية والوصول IAM.
2. المصادقة متعددة العوامل MFA.
3. حماية كلمات المرور والحسابات ووسائل المصادقة.
4. مبدأ الحد الأدنى من الصلاحيات Least Privilege.
5. .والتحكم الآمن في وصول المستخدمين Zero Trust

اليوم الثالث: التصيد الاحتيالي والهندسة الاجتماعية

1. التصيد الاحتيالي والتصيد الموجه Spear Phishing.
2. الهندسة الاجتماعية وأساليب استهداف المستخدمين.
3. الاستيلاء على الحسابات Business Email Compromiseg.
4. التعرف على الرسائل والروابط والاتصالات المشبوهة.
5. تحليل هجوم تصيد موجه واستجابة المستخدم والمؤسسة.

اليوم الرابع: التهديدات الداخلية ومراقبة سلوك المستخدم

1. التهديدات الداخلية ومصادر مخاطر المستخدمين.
2. تحديد السلوكيات غير الاعتيادية والمؤشرات عالية الخطورة.
3. مراقبة أنشطة المستخدمين وتحليل السلوك.
4. حماية البيانات ومنع الوصول أو الكشف غير المصرح به.
5. اكتشاف نشاط مستخدم غير اعتيادي وتحليل المخاطر.
6. دراسة حالة ختامية: تحليل مخاطر مستخدم ووضع إجراءات الحماية والاستجابة المناسبة.



لماذا تحضر هذه الدورة؟ — المكاسب والخسائر

المكاسب:

- تعزيز حماية المستخدمين والحسابات من التهديدات السيبرانية.
- تحسين إدارة الهوية والوصول والصلاحيات.
- رفع القدرة على اكتشاف التصيد والهندسة الاجتماعية.
- تحسين اكتشاف التهديدات الداخلية والسلوكيات المشبوهة.
- تعزيز مراقبة مخاطر المستخدمين.
- تطوير نهج مؤسسي متقدم لإدارة المخاطر البشرية.

الخسائر في حال عدم معالجة هذه المخاطر:

- زيادة مخاطر اختراق حسابات المستخدمين.
- الوصول غير المصرح به إلى الأنظمة والبيانات.
- ارتفاع التعرض لهجمات التصيد والهندسة الاجتماعية.
- صعوبة اكتشاف الأنشطة غير الاعتيادية للمستخدمين.
- زيادة مخاطر تسريب البيانات أو إساءة استخدام الصلاحيات.
- ارتفاع التأثير التشغيلي للحوادث الناتجة عن اختراق المستخدمين.

الخاتمة

تقدم هذه الدورة منهجًا متقدمًا وعمليًا لحماية المستخدمين وإدارة المخاطر المرتبطة بهم، مع التركيز على الهوية والوصول، والمصادقة، والهندسة الاجتماعية، والتصيد الاحتيالي، والتهديدات الداخلية، ومراقبة سلوك المستخدمين. ومن خلال الدراسات العملية والحالات التطبيقية، يكتسب المشاركون المعرفة والمهارات اللازمة لتحديد مخاطر المستخدمين وتعزيز حماية الحسابات والبيانات والأنظمة.

ملاحظة: بما أن الدورة أصبحت 4 أيام، حذفت موضوع الاستجابة للحوادث وإدارة مخاطر المستخدمين الخاص باليوم الخامس، ودمجت العناصر الضرورية منه بشكل مناسب ضمن الأيام الأربعة دون جعل الدورة تبدو ناقصة.

