إدارة أمن المعلومات (الأمن السيبراني)

المقدمة

تتضمن هذه الدورة التدريبية مزيجاً من التطبيقات العملية والعروض المرئية التوضيحية، إلى جانب نماذج حقيقية من البرمجيات الخبيثة وأدوات الاختراق الأخلاقي وغير الأخلاقي. كما يحصل المشاركون على أحدث الدراسات والمقالات المتعلقة بالمجال.
كجزء من البرنامج، سيقوم المتدربون بإجراء تحليل للمخاطر استناداً إلى معيار ISO 27001، وذلك لتحديد التهديدات الأمنية المحتملة، سواء المباشرة أو غير المباشرة، والوقوف على الثغرات التي قد تعرّض المنظمة للخطر.
كما سيُمنح المشاركون أدوات معرفية متقدمة حول كيفية معالجة التهديدات الإلكترونية، من خلال أفضل الممارسات التقنية والاستراتيجية لحماية الأصول الحيوية في المؤسسات. وتتضمن الدورة توزيع مواد داعمة تشمل كتيبات توعوية حول الابتزاز الإلكتروني، هجمات حجب الخدمة (DoS/DDoS)، وأساليب التحقيق الرقمي الجنائي.

الفئات المستهدفة

- العاملون في أقسام تكنولوجيا المعلومات، الأمن السيبراني، والتدقيق الداخلي
- مدراء المواقع الإلكترونية والبنى التحتية الرقمية
- كل من لديه خبرة أساسية في الإنترنت، أمن الشبكات، أو نظم المعلومات
- أي شخص يرغب في تطوير كفاءاته ومهاراته ضمن بيئة الأمن الرقمي

الأهداف التدريبية

بنهاية الدورة سيكون المشاركون قادرين على:
- تنفيذ معايير أمن المعلومات على مستوى المؤسسة والأصول الحساسة
- التعرف على أنماط التهديدات الشائعة مثل الفيروسات، البرمجيات الخبيثة، الشفرات النشطة، والهجمات المستمرة المتقدمة (APT)، وتحديد استراتيجيات التخفيف منها
- تأسيس وإدارة فرق أمن إلكتروني فعالة، وتطبيق إطار فرق الاستجابة للحوادث (CSIRT) مع الأدوات المطلوبة لحلول آمنة وفعّالة من حيث التكلفة
- استخدام تقنيات البرمجة اللغوية العصبية (NLP) للتأثير على سلوك الموظفين نحو ممارسات آمنة
- تقييم أمان بروتوكولات الشبكات اللاسلكية وكشف الثغرات المحتملة داخل المؤسسات أو في الأماكن العامة
- توضيح تطبيقات اختبار الاختراق والقرصنة الأخلاقية لتعزيز الدفاعات الأمنية
- تحليل التهديدات السيبرانية الحديثة، الذكاء من المصادر المفتوحة (OSINT)، والتطورات في الذكاء الاصطناعي

الكفاءات المستهدفة

- حوكمة أمن المعلومات
- تحليل وتقييم نقاط الضعف
- تطبيق ضوابط الأمن الإلكتروني الفعالة

• تطوير سياسات وإجراءات الأمن المعلوماتي
• التحقيقات الجنائية الرقمية
• القرصنة الأخلاقية والاختراقات من طرف القراصنة ذوي النوايا الخبيثة

محتوى الدورة

الوحدة الأولى: التكيّف مع المعايير الحديثة وأدوات الامتثال

• أطر أمن المعلومات المعتمدة (مثل ISO 27001 / PCI-DSS)
• المعايير الدولية ISO / IEC 27001
• دليل PAS 555
• إطار COBIT لحوكمة تكنولوجيا المعلومات

الوحدة الثانية: المعايير التنظيمية والتشريعية القادمة

• تطورات ISO / IEC 2017
• تشريعات حماية الخصوصية ضمن الاتحاد الأوروبي
• المتطلبات الحكومية المحلية والدولية الخاصة بالوصول إلى البيانات

الوحدة الثالثة: الأسس التقنية لأمن تكنولوجيا المعلومات

• هيكلة الأنظمة الأمنية في المؤسسة
• الدفاعات الخارجية والداخلية
• تصفية المحتوى عبر الإنترنت
• أنظمة منع التسلل (IPS) وكشفه (IDS)
• الجدران النارية متعددة الطبقات
• مفاهيم قانون التأمين الرقمي
• دورة حياة تطوير البرمجيات الآمن (SDL)
• تقييم أمان التطبيقات الداخلية
• تأمين الشبكات اللاسلكية (WiFi)
• حماية بروتوكولات VoIP
• المخاطر المتعلقة بالحوكمة والامتثال (GRC)
• أنظمة إدارة الحوادث الأمنية (SIEM)
• أمان بيئة الحوسبة السحابية
• إدارة الطرف الثالث ومتطلبات الالتزام

الوحدة الرابعة: تعزيز قدرات الحماية والتصدي

• بناء الوعي الأمني لدى الموظفين باستخدام تقنيات NLP

- نشر برامج التوعية الأمنية الفعالة
- تنفيذ اختبارات اختراق احترافية
- فهم أخلاقيات الاختراق الأمني
- أساليب مكافحة الفيروسات والبرمجيات الخبيثة والتهديدات المعقدة
- نشر فرق الاستجابة للحوادث (CSIRT) مع الأدوات والمنهجيات المناسبة
- إدارة الاستجابة الأولية للأحداث، وتوثيق الأدلة الرقمية
- مقدمة في الطب الشرعي الرقمي وأدوات التحقيق
- أمن أنظمة التحكم الصناعية (SCADA)
- معالجة انتهاكات البيانات والامتثال للتشريعات المحلية والدولية

الوحدة الخامسة: تأسيس فرق أمن سيبراني فعّالة

- تصميم وإدارة مركز عمليات أمن المعلومات (SOC)
- بناء الهيكل الأمني الداخلي في المؤسسة
- تنفيذ فرق الاستجابة لحوادث أمن المعلومات (CSIRT)
- استخدام أدوات SIEM لرصد وتحليل التهديدات
- تقييم مخاطر الأجهزة الطرفية المحمولة والقابلة للإزالة (USB/CD وغيرها)
- التعامل مع هجمات إدخال الشفرات الضارة وتطبيق إجراءات الوقاية

الوحدة السادسة: التهديدات المتقدمة وأدوات التحليل

- تحليل الجرائم السيبرانية داخل شبكة الإنترنت المظلم (Darknet/Dark Web)
- فهم بيئة الجرائم الرقمية المخفية
- استخدام الهندسة الاجتماعية لاختبار جاهزية الأفراد
- تحليل مصادر المعلومات من البيانات المفتوحة (OSINT)
- استخدام تقنيات الذكاء الاصطناعي للتنبؤ بالتهديدات
- أدوات الأمان مفتوحة المصدر والتجارية
- استخدام التشفير في حماية المعلومات
- تطبيق الشبكات الخاصة الافتراضية (VPN) لتعزيز الخصوصية