التحضير لاختبار GSEC: أساسيات الأمن السيبراني من GIAC

6 – 10 سبتمبر 2027

دبي

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

التحضير لاختبار GSEC: أساسيات الأمن السيبراني من GIAC

المرجع: 93_79151 التاريخ: 6 – 10 سبتمبر 2027 المكان: دبي الرسوم: 4500 Euro

AGILE LEADERS
Training Center

نظرة عامة على الدورة

تقدم هذه الدورة التدريبية تعليماً متعمقاً يشمل المجالات الأساسية لأمن المعلومات، حيث تغطي مفاهيم الدفاع في العمق، أساسيات التحكم في الوصول، إدارة كلمات المرور، ومفاهيم وتقنيات التشفير. يتعرف المشاركون على أمن أنظمة ويندوز وليكسوس، العمليات السحابية في بيئتي أمازون ويب سيرفيسز ومايكروسوفت أزور، إضافة إلى تصميم الشبكات القابلة للدفاع والاستجابة للحوادث بفعالية. يوازن البرنامج بين المعرفة النظرية والتطبيق العملي لتمكين المتعلمين من اكتساب خبرة عملية باستخدام أدوات الأمن السيبراني الحرجة، وأنظمة إدارة معلومات وتنبيهات الأمان، وتقنيات التخفيف من الثغرات الأمنية، وحماية نقاط النهاية، وأمن الأجهزة المحمولة، وفحص الثغرات واختبار الاختراق.

الفئة المستهدفة

تستهدف هذه الدورة محترفي أمن المعلومات الجدد، خبراء الأمن السيبراني، مسؤولي الشبكات والأنظمة، مديري الأمان، موظفي العمليات، مهندسي ومشرفي تقنية المعلومات، مسؤولي الأمان، محلي الأدلة الجنائية الرقمية، مختبري الاختراق، والمدققين الداخليين والخارجيين.

الإدارات المستهدفة

تستفيد من هذه الدورة فرق تقنية المعلومات والأمن السيبراني، مراكز عمليات الشبكات، إدارات المخاطر والامتثال، أقسام التدقيق الداخلي، خدمات الأمان المدارة، ومراكز عمليات الأمان.

القطاعات المستهدفة

تعتبر هذه الدورة ذات قيمة عالية لكل من قطاع المالية والبنوك، الجهات الحكومية والدفاعية، قطاع الرعاية الصحية والمستشفيات، الطاقة والمرافق العامة، الاتصالات، التجارة الإلكترونية والقطاع التجزئة، إضافة إلى قطاع التعليم والأكاديميات.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- شرح ومناقشة المفاهيم الأمنية الأساسية من منظور أدلة التحضير لاختبارات شهادات أمن المعلومات.
- تحديد ووصف بروتوكولات وخدمات الشبكة المختلفة وتصنيفها من حيث الأمان.
- التعرف على أساسيات التحكم في الوصول وأفضل ممارسات إدارة كلمات المرور ومقارنتها.
- تلخيص أساسيات التشفير المستخدمة لتأمين الاتصالات واستخدام الخوارزميات المناسبة.
- مناقشة تقنيات فحص الثغرات واختبار الاختراق للمبتدئين وتوضيح آلية عملها.
- استعراض إدارة وتأمين أنظمة التشغيل وحملات الصلابة الرقمية لنظام لينكس.
- تحديد متطلبات تطبيق أنظمة مراقبة الأحداث الأمنية في سيناريوهات العمل الواقعية.
- توضيح استراتيجيات حماية نقاط النهاية وأمن الأجهزة المحمولة ووصف آليات عملها.
- تفسير أساليب التخفيف من الثغرات واستخدام أطر التحكم الأمنية الحرجة.
- شرح إدارة العمليات السحابية على منصتي أمازون ومايكروسوفت أزور بأمان.
- توصيف بنية الشبكات القابلة للدفاع وحماية اتصالات الويب بشكل فعلي.
- تلخيص تقنيات الاختبار التجريبي لاجتياز اختبار شهادة أساسيات الأمن السيبراني من المحاولة الأولى.

محاور الدورة

اليوم الأول: أساسيات الأمن السيبراني ومبادئ التشفير

- نظرة عامة على شهادة أساسيات الأمان ومخطط الاختبار
- ثلاثية أمن المعلومات: السرية، السلامة، والتوافر في التطبيق العملي
- مصطلحات ومفاهيم واستخدامات التشفير
- خوارزميات التشفير المتماثل والمفتاح العام
- دوال الهاش والسلامة التشفيرية
- أساسيات التحكم في الوصول وأفضل ممارسات إدارة كلمات المرور

اليوم الثاني: تصميم الشبكات الآمنة والبنية التحتية السحابية

- التدريب على الدفاع في العمق وأطر التحكم الأمنية الحرجة
- هندسة الشبكات الآمنة: التقسيم وطبقات البروتوكول
- بروتوكولات الإنترنت والاتصالات الآمنة
- أمن اتصالات الويب وتقنيات حماية المتصفح
- عمليات الأمان السحابي على المنصات الكبرى
- الافتراضية وأمن البيئات السحابية

اليوم الثالث: أمن أنظمة التشغيل ونقاط النهاية

- تأمين وإدارة أنظمة ويندوز بحسب أفضل الممارسات
- تقنيات الصلابة الإدارية والتأمين لنظام لينكس
- استراتيجيات حماية نقاط النهاية ومنع البرمجيات الخبيثة
- إدارة أمن الأجهزة المحمولة والأجهزة اللوحية
- رصد وتحليل سجلات الأحداث عبر أنظمة التشغيل
- أدوات الفحص والتدقيق المتقدمة لنقاط النهاية

اليوم الرابع: اختبار الاختراق وفحص الثغرات واستجابة الحوادث

- مفاهيم فحص الثغرات الأمنية وتقييم المخاطر
- منهجيات اختبار الاختراق للمبتدئين والفرق الزرقاء
- تطبيق تقنيات التخفيف من الثغرات وسد الثغرات المكتشفة
- مقدمة في الاستجابة للحوادث السيبرانية وتحليل الأدلة
- أنظمة إدارة معلومات الأمان والأحداث في سيناريوهات واقعية
- تطبيقات عملية على تحليل التنبيهات الأمنية

اليوم الخامس: التحضير للاختبار والمراجعة الشاملة

- استراتيجيات وتقنيات اجتياز الاختبار الدولي من المحاولة الأولى
- حل أسئلة تجريبية ومحاكاة بيئة الامتحان الفعلية
- استعراض قائمة التحقق لدليل المراجعة والملخصات النهائية
- مناقشة السيناريوهات العملية المعقدة والحلول المقترحة
- تقييم المهارات الفردية وتحديد نقاط القوة والضعف
- جلسة أسئلة وأجوبة ختامية وتوجيهات التطوير المهني

الأسئلة الشائعة

س: هل تتطلب هذه الدورة خبرة مسبقة متقدمة في تقنية المعلومات؟
ج: الدورة مصممة لتكون شاملة، ويفضل وجود خلفية أساسية في الشبكات وأنظمة التشغيل لتحقيق أقصى استفادة ممكنة.

س: كيف تساعد هذه الدورة في التحضير للامتحان الرسمي؟
ج: توفر الدورة تغطية كاملة لمخطط الاختبار، مع تدريبات عملية وأسئلة محاكاة مشابهة للاختبار الحقيقي.

س: هل تشمل الدورة تطبيقات عملية ونقاشات تفاعلية؟
ج: نعم، تعتمد الدورة على منهجية التعلم التجريبي وتتضمن ورش عمل وتطبيقات عملية على أدوات الأمن السيبراني.