دورة التحضير لاختبار GSEC: أساسيات أمن المعلومات

GIAC

11 – 15 يناير 2027

أديس أبابا

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة التحضير لاختبار GSEC: أساسيات أمن المعلومات GIAC

المرجع: 93_223311 **التاريخ:** 11 – 15 يناير 2027 **المكان:** أديس أبابا **الرسوم:** Euro 4500

نظرة عامة

تقدم دورة التحضير لاختبار GSEC: أساسيات أمن المعلومات GIAC مسارا منهجيا لتغطية مجالات أمن المعلومات وبناء القدرات الدفاعية في البيئات المؤسسية الحديثة. يكتسب المشاركون خبرات عملية في أساسيات التحكم في الوصول وتطبيق خوارزميات التشفير وتصليب أنظمة التشغيل في بيئات Linux وWindowsg، وإدارة عمليات أمن السحابة على منصتي AWS وAzureg. يتناول المنهج تصميم البنية التحتية الشبكية الدفاعية وتطبيق أنظمة SIEM وفحص الثغرات وإجراءات الاستجابة للحوادث السيبرانية. يحلل المتدربون مسارات التهديدات وقوائم مراجعة أدلة الدراسة لترسيخ الكفاءة التقنية. تقدم هذه الدورة بواسطة أجايل للتدريب.

الفئة المستهدفة

- المتخصصون في أمن المعلومات الساعون لبناء مهارات تقنية أساسية في العمليات الدفاعية.
- مسؤولو الشبكات والأنظمة المكلفون بتأمين البنية التحتية وإعداد ضوابط الوصول.
- مشرفو الأمن وإداريو العمليات وفرق الدعم الفني المشرفة على التدابير الوقائية.
- محللو الأدلة الجنائية الرقمية ومختبرو الاختراق والمدققون الباحثون عن معرفة منظمة بالضوابط الأمنية.
- محللو الأمن المبتدئون الذين يستعدون لتولي مسؤوليات مهنية في الأمن السيبراني.

الإدارات والقطاعات المستهدفة

يخدم هذا البرنامج الكوادر الأمنية والشبكية وفرق الأنظمة في القطاعات الحيوية التي تتطلب معايير أمان موثوقة.

- فرق تقنية المعلومات والأمن السيبراني في قطاع البنوك والخدمات المالية
- مراكز عمليات الشبكة في قطاع الاتصالات والتجارة الإلكترونية
- مراكز العمليات الأمنية في المستشفيات ومنظومات الرعاية الصحية
- إدارات المخاطر والامتثال في قطاع الطاقة والمرافق الخدمية
- وحدات التدقيق الداخلي والعمليات التقنية في الهيئات الحكومية ومؤسسات الدفاع

أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تطبيق المفاهيم الأمنية الأساسية المتوافقة مع منهج اختبار GIAC Security Essentials.
- تحليل وحماية بروتوكولات الشبكات وخدمات التوجيه والاتصالات الشبكية عبر الويب.
- تنفيذ أساسيات التحكم في الوصول وسياسات إدارة كلمات المرور عبر الأدلة المؤسسية.
- نشر تقنيات التشفير المتماثل والمفتاح العام ودوال التجزئة وبروتوكولات تبادل المفاتيح.
- إجراء فحص الثغرات والتقييمات المنهجية باستخدام أدوات الفحص المعتمدة.
- تصليب أنظمة التشغيل Linux وWindowsg بالاعتماد على الضوابط الإدارية وكائنات نهج المجموعة.
- إعداد مسارات تطبيق SIEM وقواعد ربط السجلات لتشخيص الأنشطة والتهديدات الأمنية.
- تقييم عمليات أمن السحابة في منصتي AWS وAzureg بجانب نماذج مخاطر المحاكاة الافتراضية.

جدول الدورة

اليوم 1: أسس الأمن السيبراني وتقنيات التشفير

- هيكل منهج شهادة GIAC Security Essentials ومخطط المجالات المعرفية
- ثالوث أمن المعلومات CIA: نماذج تطبيق السرية والسلامة والتوافر
- مصطلحات ومفاهيم التشفير والخوارزميات المتماثلة بما في ذلك خوارزمية AES
- تشفير المفتاح العام وخوارزميات RSA وECC وآليات توزيع المفاتيح
- التحقق من سلامة البيانات بالتشفير عبر دوال التجزئة ورمز HMAC
- أساسيات التحكم في الوصول وسياسات إدارة كلمات المرور
- جلسة مراجعة: أوليات التشفير ونماذج التحقق من الهوية

اليوم 2: بنية الشبكات الدفاعية وأمن السحابة

- مبادئ الدفاع المتعمق وتحديد أولويات الضوابط الأمنية الحيوية
- تصميم البنية التحتية الشبكية الدفاعية: تجزئة الشبكة وحماية الحدود
- تحليل وحماية بروتوكولات الشبكة: بروتوكولات TCP/IP وDNS وSSL/TLS وIPSecg
- أمن اتصالات الويب وضوابط الخوادم الوكيلة وتقنيات معالجة ثغرات المتصفحات
- عمليات أمن السحابة عبر بيئات البنية التحتية في AWS وAzureg
- الضوابط الأمنية للحوسبة الافتراضية وإدارة مخاطر برمجيات Hypervisor
- جلسة مراجعة: تحليل حركة مرور الشبكة وسيناريوهات التهيئة السحابية

اليوم 3: تصليب أنظمة التشغيل في بيئات Linuxg Windows

- أساسيات بيئة Linux: أذونات نظام الملفات وإعداد سطر الأوامر وصلاحيات المستخدم الخارق
- تأمين وتصليب توزيعات خوادم Linux ضد الوصول غير المصرح به
- أمن نظام التشغيل Windows: توزيع حقوق المستخدمين وكائنات نهج المجموعة GPO
- سياسات التدقيق في Windows وبنية سجلات الأحداث والجاهزية للتحليل الجنائي
- استخدام نصوص PowerShell لأتمتة التدقيق الإداري والتهيئة الأمنية
- استراتيجيات حماية الأجهزة الطرفية وأمن الأجهزة المحمولة في المؤسسات
- جلسة مراجعة: إجراءات تدقيق أنظمة التشغيل وإنفاذ السياسات

اليوم 4: رصد التهديدات وإدارة الثغرات والاستجابة للحوادث

- تطبيق أنظمة SIEM وتجميع السجلات مركزيا وربط التنبيهات الأمنية
- مراحل دورة حياة الاستجابة للحوادث واستراتيجيات منع فقدان البيانات DLP
- مسارات فحص الثغرات باستخدام أدوات مثل OpenVASg Nessus
- منهجيات اختبار الاختراق ومراحل الاستطلاع والاستغلال
- تقنيات الحد من الاستغلال والتدابير الدفاعية على مستوى الأجهزة المضيفة
- تحليل السجلات والتمثيل المرئي للبيانات باستخدام Kibanag Elasticsearch
- جلسة مراجعة: مسارات رصد التهديدات وتحديد أولويات المعالجة

اليوم 5: استراتيجيات التحضير للاختبار وأطر الضوابط الأمنية

- تحليل الاختبارات التجريبية لشهادة GIAC GSEC ومنهجية تفكيك الأسئلة
- مواءمة المهارات الأمنية التقنية مع متطلبات الوظائف المبتدئة في الأمن السيبراني
- تدقيق تكوينات أمان الأجهزة الطرفية وفق معايير الامتثال المعتمدة
- استكمال قوائم مراجعة دليل الدراسة واستراتيجيات إدارة وقت الاختبار
- مواءمة الامتثال التنظيمي ومطابقة الضوابط وتقييم السيناريوهات
- تخطيط المسار المهني في مجالات تحليل الأمن والعمليات الأمنية
- جلسة مراجعة: التقييم التقني النهائي ومراجعة الجاهزية للاختبار

التمارين التطبيقية

ينفذ المشاركون أنشطة عملية لمعالجة التحديات التشغيلية وبناء خطط التنفيذ الدفاعي.

- إعداد عمليات التجزئة التشفيرية والتشفير المتماثل للملفات.
- فحص حزم البيانات عبر الشبكة لرصد بيانات الاعتماد غير المشفرة والأنشطة المشبوهة للبروتوكولات.
- تطبيق حدود صلاحيات المستخدمين وسياسات التدقيق على منصات Linux وWindowsg.
- تحليل لوحات تنبيهات SIEM الافتراضية لفرز الحوادث الأمنية والتعامل معها.

الأسئلة الشائعة

ما المؤهلات أو المتطلبات المسبقة المطلوبة للمشاركة في هذه الدورة؟

لا توجد متطلبات مسبقة رسمية للتسجيل. تعد المعرفة الأساسية بأنظمة تقنية المعلومات ومفاهيم الشبكات مفيدة ولكنها ليست إلزامية، حيث صممت هذه الدورة لتكون نقطة انطلاق عملية في مجال الأمن السيبراني.

ما مدة جلسات التدريب اليومية وما هو إجمالي الساعات المخصصة للدورة؟

تستغرق الجلسة اليومية ما بين 4 إلى 5 ساعات تشمل التمارين التطبيقية وفترات الاستراحة، ويمتد البرنامج التدريبي على مدار أسبوع بإجمالي يتراوح بين 20 إلى 25 ساعة من التدريب المباشر.

ما سبب أهمية أمن نظام Linux في اختبار شهادة GIAC GSEC؟

يتضمن اختبار GIAC GSEC أهدافا تركز على الإدارة الآمنة لنظام Linux والتعامل بكفاءة مع سطر الأوامر. ويعد فهم أساسيات Linux ضروريا لإدارة الخوادم الطرفية وضبط صلاحيات الوصول وتحليل سجلات النظام أثناء العمليات الأمنية.

الخاتمة

يوفر هذا البرنامج التدريبي الممتد لخمسة أيام إعدادا منهجيا للممارسين الأمنيين الراغبين في إتقان مفاهيم أمن المعلومات الأساسية. يكتسب المشاركون مهارات عملية في تصليب أنظمة التشغيل وحماية بروتوكولات الشبكة وإدارة مخاطر السحابة، إلى جانب استراتيجيات منظمة للتحضير للاختبار تعزز الموقف الأمني للمؤسسات.