احتراف الأمن للشبكة ونقطة النهاية والسحابة | دورة تدريبية SEC410

2 – 6 أغسطس 2027

القاهرة

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

احتراف الأمن للشبكة ونقطة النهاية والسحابة | دورة تدريبية SEC410

المرجع: 72_78883 **التاريخ:** 2 – 6 أغسطس 2027 **المكان:** القاهرة **الرسوم:** Euro 4100

نظرة عامة على الدورة:

توفر هذه الدورة معرفة تأسيسية ومهارات عملية أساسية للدفاع عن الأنظمة والشبكات. تغطي SEC410 النطاق الكامل للأمن السيبراني الحديث، مع التركيز على الأمن عبر بيئات الشبكة ونقطة النهاية والسحابة. سيطور المشاركون خبرة عملية في التشفير، تعزيز أمان أنظمة التشغيل، التحكم في الوصول، عمليات الأمن، والاستجابة للحوادث. تتوافق الدورة مباشرة مع شهادة GSEC GIAC Security Essentials.

الجمهور المستهدف:

- متخصصو أمن المعلومات
- مسؤولو الأنظمة والشبكات
- موظفو دعم تقنية المعلومات والمساعدة الفنية
- محللو مراكز العمليات الأمنية SOC المبتدئون
- مهندسو وفنيو الأمن

الاقسام المستهدفة:

- تقنية المعلومات والأمن السيبراني
- مراكز العمليات الأمنية SOC
- فرق السحابة والشبكات
- إدارة المخاطر والتدقيق
- الامتثال والبنية التحتية

أهداف الدورة:

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- فهم وتطبيق مبادئ الأمن السيبراني الأساسية واستراتيجيات الدفاع
- تأمين الاتصالات باستخدام أساليب وأدوات التشفير
- تطبيق تعزيز أمان نقطة النهاية وضوابط وصول المستخدمين
- تحليل حركة مرور الشبكة وتأمين البروتوكولات الشائعة
- الاستجابة للحوادث باستخدام أدوات SIEM وأساليب الكشف
- إدارة منصات السحابة AWS/Azure بشكل آمن باستخدام أفضل الممارسات
- التحضير لاجتياز اختبار شهادة GIAC GSEC

منهجية التدريب:

- جلسات بقيادة المدرب
- مختبرات عملية ومحاكاة
- نمذجة التهديدات والمراجعة القائمة على المجموعات
- دراسات حالة واقعية وتمارين النظافة السيبرانية
- اختبارات تدريبية ومراجعات للاختبار

أدوات الدورة:

- Wireshark, PowerShell, واجهة سطر الأوامر لنظام Linux
- نموذج اختبار تدريبي لـ GSEC
- قوالب التكوين الآمن
- سيناريوهات تحليل أحداث SIEM
- عرض توضيحي لأدوات التشفير

AGILE LEADERS
Training Center

محتوى الدورة:

اليوم الأول: أساسيات الأمن السيبراني والتشفير

- **الموضوع 1:** مقدمة في الأمن السيبراني ونظرة عامة على GIAC GSEC
- **الموضوع 2:** مفاهيم الأمن الأساسية: التهديدات، ثلاثية CIA، والضوابط
- **الموضوع 3:** مصطلحات التشفير، التشفير المتماثل وغير المتماثل
- **الموضوع 4:** التجزئة Hashing، HMAC، والشهادات الرقمية
- **الموضوع 5:** نماذج المصادقة وآليات التحكم في الوصول
- **الموضوع 6:** إدارة الهوية وأمان كلمات المرور
- **تأمل ومراجعة:** مختبر أدوات التشفير وسيناريوهات التحكم في الوصول

اليوم الثاني: أمن الشبكات والدفاع عن البروتوكولات

- **الموضوع 1:** أساسيات الشبكات: IP، TCP/UDP، والهجمات الشائعة
- **الموضوع 2:** نماذج الدفاع عن الشبكات: جدران الحماية، أنظمة كشف التسلل IDS، والثقة المعدومة
- **الموضوع 3:** البروتوكولات الآمنة: VPN، SSL/TLS، SSH، وDNSSEC
- **الموضوع 4:** أمن الويب والبريد الإلكتروني: HTTPS، الشهادات، SPF، DKIM
- **الموضوع 5:** التقاط الحزم وتحليل البروتوكولات مختبر Wireshark
- **الموضوع 6:** تجزئة الشبكة والهندسة المعمارية الآمنة
- **تأمل ومراجعة:** فحص حركة المرور وتعزيز أمان البروتوكولات

AGILE LEADERS
Training Center

اليوم الثالث: أمن نقطة النهاية وأنظمة التشغيل Windows و Linux

- **الموضوع 1:** أساسيات أمان Windows: سياسات المجموعة GPOs وحقوق المستخدمين
- **الموضوع 2:** مبادئ أمان Linux: الأذونات، sudo، والسجلات
- **الموضوع 3:** تقنيات التكوين الآمن والتعزيز
- **الموضوع 4:** مفاهيم الكشف والاستجابة لنقطة النهاية EDR
- **الموضوع 5:** PowerShell و Bash لمهام الأمن
- **الموضوع 6:** أساسيات أمان الأجهزة المحمولة MDM, BYOD
- **تأمل ومراجعة:** تمارين تعزيز أمان أنظمة التشغيل وتدقيق الوصول

اليوم الرابع: عمليات الأمن وأساسيات السحابة

- **الموضوع 1:** مقدمة إلى SIEM وتقنيات تحليل السجلات
- **الموضوع 2:** مبادئ أمان السحابة المسؤولية المشتركة، إدارة الهوية والوصول
- **الموضوع 3:** إجراءات المراقبة والاستجابة للحوادث
- **الموضوع 4:** إدارة الثغرات الأمنية واستراتيجية التصحيح
- **الموضوع 5:** أساسيات اختبار الاختراق ومنع الاستغلال
- **الموضوع 6:** تأمين البيئات الافتراضية وأعباء عمل السحابة
- **تأمل ومراجعة:** مختبر SIEM وعرض توضيحي لسوء تكوين السحابة

اليوم الخامس: التحضير لـ GSEC والجاهزية المهنية

- **الموضوع 1:** استراتيجية اختبار GSEC ومراجعة أسئلة التدريب
- **الموضوع 2:** ربط التعلم بالأدوار الوظيفية ومسارات الأمن السيبراني
- **الموضوع 3:** تطوير سياسات وضوابط أمن المؤسسات
- **الموضوع 4:** مختبر عملي نهائي: سيناريو الدفاع عن الشبكة ونقطة النهاية
- **الموضوع 5:** التخطيط الوظيفي: أدوار المحلل، SOC، أمن السحابة
- **الموضوع 6:** قائمة مراجعة، أسئلة شائعة، وجاهزية الشهادة
- **تأمل ومراجعة:** أسئلة وأجوبة، محاكاة الاختبار، واختتام الدورة

الأسئلة الشائعة:

ما هي المؤهلات أو المتطلبات المسبقة المحددة المطلوبة للمشاركين قبل التسجيل في الدورة؟

لا توجد متطلبات مسبقة رسمية. ومع ذلك، فإن الإلمام الأساسي بأنظمة تقنية المعلومات أو أنظمة التشغيل أو مفاهيم الشبكات مفيد. تم تصميم هذه الدورة كنقطة دخول عملية إلى الأمن السيبراني.

كم مدة كل جلسة يومية، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تُصمم كل جلسة يومية عادةً لتستمر حوالي 4-5 ساعات، بما في ذلك فترات الاستراحة. تمتد مدة الدورة الإجمالية لخمسة أيام، بإجمالي حوالي 20-25 ساعة من التعليم الموجه.

لماذا يعد فهم نموذج المسؤولية المشتركة أمرًا بالغ الأهمية في أمن السحابة؟

في بيئات السحابة مثل AWS أو Azure، تُقسم مسؤوليات الأمن بين مزود السحابة والعميل. يمكن أن يؤدي سوء فهم هذا النموذج إلى أخطاء تكوين حرجة، مثل تخزين البيانات غير المحمي أو أدوار IAM غير الآمنة، مما يجعل من الضروري للمتعلمين استيعاب هذا المفهوم مبكرًا في رحلتهم نحو أمن السحابة.

كيف تختلف هذه الدورة عن دورات أساسيات الأمن الأخرى:

على عكس دورات أساسيات الأمن السيبراني العامة، تقدم دورة SEC410: أساسيات الأمن - الشبكة، نقطة النهاية، والسحابة نهجًا عمليًا وواقعيًا للغاية لأساسيات الأمن. ما يميز هذه الدورة هو تركيزها المتوازن على أمن الشبكات، وحماية نقطة النهاية، والدفاعات القائمة على السحابة، مما يضمن بناء المشاركين لمجموعة مهارات شاملة حقًا. بدلاً من الاعتماد فقط على المفاهيم النظرية، تدمج SEC410 عروضًا توضيحية حية وتمارين موجهة قائمة على الأدوات باستخدام أدوات أمن حقيقية مثل Wireshark وPowerShell وتكوينات IAM السحابية.

بالإضافة إلى ذلك، تم تصميم هذه الدورة بما يتوافق تمامًا مع إطار عمل شهادة GIAC GSEC، مما يساعد المشاركين ليس فقط على فهم مفاهيم الأمن ولكن أيضًا على تطبيقها في سيناريوهات الاختبار والتحديات المتعلقة بالوظيفة. كما تتميز بسد الفجوة بين أمن تقنية المعلومات التقليدي وبيئات السحابة الحديثة، وتقدم محتوى محدثًا حول AWS Azureg ومخاطر المحاكاة الافتراضية.