



احتراف الأمن للشبكة ونقطة النهاية والسحابة | دورة تدريبية
SEC410



AGILE LEADERS
Training Center

احتراف الأمن للشبكة ونقطة النهاية والسحابة | دورة تدريبية SEC410

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 أمن أنظمة التشغيل، التحكم في الوصول، عمليات الأمن، والاستجابة للحوادث. تتوافق الدورة مباشرة مع شهادة GSEC Essentials Security GIAC.

الجمهور المستهدف:

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

الأقسام 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 أمن نقطة النهاية وضوابط وصول المستخدمين
- تحليل حركة مرور الشبكة وتأمين البروتوكولات الشائعة
- الاستجابة للحوادث باستخدام أدوات SIEM وأساليب الكشف
- إدارة منصات السحابة Azure/AWS بشكل أمن باستخدام أفضل الممارسات
- التحضير لاجتياز اختبار شهادة GSEC GIAC



منهجية التدريب:

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

أدوات الدورة:

- Linux لنظام النواير سطر واجهة, Wireshark, PowerShell
- نموذج اختبار تدريبي J GSEC
- قوالب التكوين الأمن
- سيناريوهات تحليل أحداث SIEM
- عرض توضيحي لأدوات التشفير

محتوى الدورة:

اليوم الأول: أساسيات الأمن السيبراني والتشفير

- الموضوع 1: مقدمة في الأمن السيبراني ونظرة عامة على GSEC GIAC
- 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: نهج المصادقة واليات التحكم في الوصول
- الموضوع 6: إدارة الهوية وأمان كلمات المرور
- تأهل ومراجعة: مختبر أدوات التشفير وسيناريوهات التحكم في الوصول

اليوم الثاني: أمن الشبكات والدفاع عن البروتوكولات

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

اليوم الثالث: أمن نقطة النهاية وأنظمة التشغيل Linux و Windows

- الموضوع 1: أساسيات أمان Windows: سياسات المجموعة GPOs وحقوق المستخدمين
- الموضوع 2: مبادئ أمان Linux: النذونات، sudo، والسجلات
- الموضوع 3: تقنيات التكوين الأمن وتعزيز
- الموضوع 4: مفاهيم الكشف والاستجابة لنقطة النهاية EDR
- الموضوع 5: الأمن لهام Bash و PowerShell
- الموضوع 6: أساسيات أمان الأجهزة المحمولة MDM، BYOD
- تأهل ومراجعة: تمارين تعزيز أمان أنظمة التشغيل وتحقق الوصول



اليوم الرابع: عمليات الأمن وأساسيات السحابة

- الموضوع 1: مقدمة إلى SIEM وتقنيات تحليل السجلات
- الموضوع 2: مبادئ أمن السحابة والمسؤولية 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 البيانات الافتراضية وأعباء عمل السحابة
- تأهل 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 بالدور 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 التحلل، SOC، أمن السحابة
- الموضوع 6: قائمة مراجعة، أسئلة شائعة، وجاهزية الشهادة
- تأهل 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. تهتد مدة الدورة الإجمالية لخمس أيام، بإجمالي حوالي 20-25 ساعة من التعليم الموجب.

لماذا يعد فهم نموذج المسؤولية المشتركة أمراً 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 حرجية، مثل تخزين البيانات غير المحمي أو أدوار IAM غير الممنوعة، مما يجعل من الضروري للمتعلمين استيعاب هذا المفهوم مبكراً 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 نهجاً عملياً وواقعياً 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 حقاً. بدلاً من الاعتماد فقط على المفاهيم النظرية، تدمج SEC410 عروضاً 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 تماماً مع إطار عمل شهادة GSEC GIAC، مما يساعد المشاركين ليس فقط على فهم مفاهيم الأمن ولكن أيضاً على تطبيقها في سيناريوهات الاختبار والتحديات المتعلقة بالوظيفة. كما تتميز بسد الفجوة بين أمن تقنية المعلومات التقليدي وبيئات السحابة الحديثة، وتقدم محتوى محدثاً حول AWS وAzure ومخاطر المحاكاة الافتراضية.

فئات الدورات التدريبية

الدورات التدريبية في مجال البيئة والاستدامة	دورات إدارة الجودة وتطوير العمليات
دورات إدارة و تحليل البيانات ودورات علم البيانات	دورات إدارة و تطوير الموارد البشرية
دورات الذهن السيرياني ودورات تقنية المعلومات	دورات الاتصال الجماهيري و السياسات والعلاقات العامة
دورات التدريب القانوني والهشتريات والتعاقدات	دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات
دورات الحوكمة وإدارة المخاطر والامتثال	دورات السكرتارية و إدارة المكاتب
دورات الصحة والسلامة والذهن المهني	دورات الصيانة ودورات المجالات الهندسية المتنوعة
دورات المحاسبة و التهويل و دورات الإدارة المالية	دورات المهارات الشخصية وتطوير الذات
دورات في مجالات القيادة والإدارة	دورات معتمدة من قبل هيئات دولية
دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقية	



مدن التدريب

أهستردام هولندا	أكرا غانا	أثينا اليونان
الدار البيضاء المغرب	الجبيل المملكة العربية السعودية	استنبول تركيا
القاهرة مصر	الرياض المملكة العربية السعودية	الدوحة قطر
باريس فرنسا	الهناوة مملكة البحرين	الكويت الكويت
براغ جمهورية التشيك	بانكوك تايلند	باكو أذربيجان
بورتو البرتغال	برلين ألمانيا	برشلونة إسبانيا
تورنتو كندا	تيليسي جورجيا	بوكيت تايلاند
جوهانسبرغ جنوب افريقيا	جنيف سويسرا	جاكرتا جمهورية اندونيسيا
زنجار تنزانيا	روما إيطاليا	حلي الإمارات العربية المتحدة
سيول كوريا الجنوبية	سنغافورة سنغافورة	سان دييغو الولايات المتحدة الأمريكية
طرابزون تركيا	شيكاغو الولايات المتحدة الأمريكية	شرم الشيخ مصر
عمان المملكة الأردنية الهاشمية	طوكيو اليابان	طشقند أوزبكستان
فيينا النمسا	فرانكفورت ألمانيا	عن بعد منصة زووم

مدن التدريب

لانكاوي ماليزيا	كيب تاون جنوب افريقيا	كوالالمبور ماليزيا
هاربيا اسبانيا	لندن المملكة المتحدة	لشبونة البرتغال
هونتر سويسرا	مسقط سلطنة عمان	مدريد اسبانيا
نيروبي كينيا	هيونج المانيا	ميلان ايطاليا
		نيويورك الولايات المتحدة الأمريكية