

# التحضير لاختبار CompTIA Security+ SY0-701

AGILE LEADERS
Training Center

21 – 25 يونيو 2027

بورتو

AGILE LEADERS
Training Center

# التحضير لاختبار CompTIA Security+ SY0-701

المرجع: 109399_103600442 التاريخ: 21 – 25 يونيو 2027 المكان: بورتو الرسوم: Euro 5700

AGILE LEADERS
Training Center

## نظرة عامة على الدورة

تم تصميم دورة التحضير لاختبار CompTIA Security+ SY0-701 لمساعدة المشاركين على تطوير المهارات والمعارف الأساسية اللازمة اجتياز اختبار شهادة CompTIA Security+ بنجاح. تغطي هذه الدورة التدريبية موضوعات حيوية تشمل الضوابط الأمنية، التهديدات والثغرات الأمنية، أمن الشبكات، إدارة المخاطر، والاستجابة للحوادث السيبرانية. ستقوم هذه الدورة بتزويد المتعلمين برؤى واقعية لتطبيقها في تأمين الأنظمة وإدارة المخاطر داخل المؤسسات المختلفة. سواء كنت تستعد لاختبار SY0-701 أو ترغب في تعزيز مسيرتك المهنية في مجال الأمن السيبراني، فإن هذا التدريب يوفر الفهم الشامل الضروري لاجتياز الاختبار وتأمين دور مهني في تكنولوجيا المعلومات. تعلم أهداف اختبار CompTIA Security+، عمليات الأمان، إدارة الثغرات، وغيرها الكثير. أتقن اختبارات التدريب ومواد الدراسة الخاصة بـ Security+ SY0-701 للتحضير للشهادة، واستعرض أهم نصائح شهادة CompTIA Security+ وأسئلة الاختبار الأساسية.

## الفئة المستهدفة

- محترفو تكنولوجيا المعلومات
- مسؤولو الأمان السيبراني
- مسؤولو الشبكات
- مسؤولو الأنظمة
- أي شخص يتطلع إلى اجتياز اختبار CompTIA Security+ SY0-701

## الإدارات المستهدفة

- قسم أامن تكنولوجيا المعلومات
- قسم أمن الشبكات
- قسم إدارة المخاطر
- قسم الامتثال والحوكمة
- قسم الاستجابة للحوادث وعمليات الأمن السيبراني

## القطاعات المستهدفة

- تكنولوجيا المعلومات
- الخدمات المالية
- قطاع الرعاية الصحية
- الحكومة والدفاع
- قطاع التعليم
- مزودو الحوسبة السحابية والشركات التقنية الناشئة

AGILE LEADERS
Training Center

## أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تحديد وتلخيص الوضع الأمني لبيئة المؤسسة والتوصية بالحلول الأمنية المناسبة.
- مناقشة ووصف طرق مراقبة وتأمين البيئات السحابية والأجهزة المحمولة وإنترنت الأشياء.
- التعرف على مبادئ الحوكمة والامتثال وإدارة المخاطر وشرحها.
- تصنيف وتحليل الحوادث الأمنية وتطبيق تقنيات التخفيف والاستجابة بفعالية للأحداث السيبرانية.

## محاور الدورة

AGILE LEADERS
Training Center

## اليوم الأول

- الموضوع الأول: التعرف على أهداف اختبار CompTIA Security+ SY0-701 ومناقشتها
- الموضوع الثاني: شرح مفاهيم الأمان العامة ثالوث السرية والسلامة والتوفر
- الموضوع الثالث: تلخيص إدارة المخاطر وأطر الحوكمة
- الموضوع الرابع: تحديد أنواع الضوابط الأمنية الوقائية، التكتيكية، التصحيحية، التعويضية
- الموضوع الخامس: مناقشة طرق المصادقة والتحكم في الوصول
- الموضوع السادس: وصف عمليات الأمان وفهم الاستجابة للحوادث
- التأمل والمراجعة: مراجعة المفاهيم الرئيسية لليوم الأول وتطبيق التحضير للاختبار على سيناريوهات واقعية.

## اليوم الثاني

- الموضوع الأول: تحديد أنواع هجمات البرمجيات الخبيثة برامج الفدية، طروادة، الديدان
- الموضوع الثاني: شرح هجمات الهندسة الاجتماعية التصيد الاحتيالي، التصيد عبر الرسائل القصيرة والصوتية
- الموضوع الثالث: تلخيص متجهات التهديد وأسطح الهجوم البريد الإلكتروني، الشبكات اللاسلكية، وسائط التخزين القابلة للإزالة
- الموضوع الرابع: مناقشة أساسيات التشفير التشفير، التجزئة، البنية التحتية للمفاتيح العامة
- الموضوع الخامس: وصف إدارة الثغرات الأمنية التحديد، التحليل، التخفيف
- الموضوع السادس: التعرف على أدوات الأمان لاكتشاف التهديدات والاستجابة للحوادث
- التأمل والمراجعة: تحليل دراسات الحالة وتقنيات تخفيف التهديدات باستخدام أسئلة التدريب لـ Security+.

## اليوم الثالث

- الموضوع الأول: مناقشة هندسة أمن الشبكات جدران الحماية، الشبكات الخاصة الافتراضية، أنظمة كشف ومنع التسلل
- الموضوع الثاني: شرح الأمان السحابي والبيئات الهجينة
- الموضوع الثالث: تلخيص هندسة الثقة المعدومة  بادئ التصميم الآمن
- الموضوع الرابع: تحديد البروتوكولات التشفيرية والبنية التحتية للمفاتيح العامة وإدارة المفاتيح
- الموضوع الخامس: وصف تأمين الأجهزة المحمولة وإنترنت الأشياء
- الموضوع السادس: مناقشة ضوابط الأمان المادية والبيئية
- التأمل والمراجعة: مراجعة هندسة الأمان والبروتوكولات عبر محاكاة أسئلة اختبار CompTIA Security+.

## اليوم الرابع

- الموضوع الأول: شرح الحوكمة وإدارة المخاطر والامتثال
- الموضوع الثاني: تحديد سياسات أمن المعلومات والإجراءات القياسية
- الموضوع الثالث: تلخيص برامج التوعية والتدريب الأمني للموظفين
- الموضوع الرابع: مناقشة تقييم المخاطر وتحليل التأثير على الأعمال
- الموضوع الخامس: وصف استمرارية الأعمال والتعافي من الكوارث
- الموضوع السادس: التعرف على اعتبارات الخصوصية وحماية البيانات
- التأمل والمراجعة: تطبيق أطر الحوكمة وإدارة المخاطر على سيناريوهات الامتثال التنظيمي.

## اليوم الخامس

- الموضوع الأول: تلخيص مفاهيم الطب الشرعي الرقمي والاستجابة للحوادث
- الموضوع الثاني: مناقشة جمع الأدلة وتحليلها وسلسلة الحيازة
- الموضوع الثالث: وصف عمليات اختبار الاستخراق وتقييم الضعف
- الموضوع الرابع: إجراء اختبار محاكاة شامل ومراجعة أسئلة اختبار CompTIA Security+ SY0-701
- الموضوع الخامس: استعراض نصائح وإرشادات يوم الاختبار لضمان النجاح
- الموضوع السادس: التخطيط للمسار الوظيفي المستقبلي في مجال الأمن السيبراني
- التأمل والمراجعة: إجراء اختبار تجريبي نهائي ومناقشة الإجابات لتحقيق الاستعداد التام لاجتياز الشهادة.

## الأسئلة الشائعة

AGILE LEADERS
Training Center

### ما هي متطلبات الدخول لحضور هذه الدورة؟

يوصح بأن يكون لدى المشاركين خبرة أساسية في شبكات الحاسوب وأنظمة التشغيل، ورغم ذلك تم تصميم الدورة لتغطية المفاهيم بأسلوب منظم وشامل يناسب التحضير لاختبار CompTIA Security+ SY0-701.

### هل تغطي هذه الدورة أحدث أهداف اختبار CompTIA Security+؟

نعم، تغطي الدورة بالكامل أحدث إصدار من أهداف اختبار SY0-701 مع توفير المواد التدريبية واختبارات الممارسة اللازمة.

### كيف تساعدني هذه الدورة في اجتياز الاختبار؟

من خلال الجمع بين الشرح النظري، ودراسات الحالة الواقعية، وحل أسئلة التدريب والمحاكاة المستمرة، مما يضمن اكتساب المعرفة والمهارة المطلوبة لاجتياز الاختبار والحصول على شهادة CompTIA Security+.

### هل تمنح الدورة شهادة إتمام؟

نعم، يحصل المشاركون على شهادة إتمام رسمية تثبت حضورهم للدورة وتأهيلهم لاجتياز اختبار CompTIA Security+ SY0-701.