الدورة التدريبية CyberOps Associate (CA) v1.0 Scope and Sequence

آخر تحديث شهر، يوم، سنة

مقدمة

تواجه المؤسسات الحالية تحديًا في الكشف سريعًا عن الاختراقات للأمن السيبراني والاستجابة بفعالية للحوادث الأمنية. تراقب فرق من الأشخاص العاملين في مراكز عمليات الأمن (SOCs) بشكل يقظ أنظمة الأمان، لحماية مؤسساتها عن طريق اكتشاف ثغرات الأمن السيبراني وتهديداته، والاستجابة لها. وتعمل CyberOps Associate على إعداد المرشحين لبدء مسار مهني للعمل كمحللي أمن سيبراني بمستوى مساعدين داخل مراكز العمليات الأمنية.

الجمهور المستهدف

تم تصميم الدورة التدريبية CyberOps Associate لطلاب Cisco Networking Academy® الذين يسعون لاكتساب المهارات الموجّهة مهنيًا للمحلل الأمني من مستوى المبتدئين. ويشمل الطلاب المستهدفون الأفرادَ المُسجلين في برامج شهادات التكنولوجيا في المؤسسات التعليمية العالية ومحترفي تكنولوجيا المعلومات الذين يرغبون في ممارسة مهنة في مركز عمليات الأمان (SOC). يتعرض المتعلّمون في هذه الدورة التدريبية لجميع المعارف الأساسية المطلوبة لاكتشاف تهديدات الأمن السيبراني الأساسية وتحليلها وتصعيدها باستخدام الشائع من الأدوات مفتوحة المصدر.

المتطلبات الأساسية

يجب أن يمتلك طلاب الدورة التدريبية CyberOps Associate المهارات والمعارف التالية:

- مهارات تصفُّح الكمبيوتر الشخصي والإنترنت
- المفاهيم الأساسية لنظامي التشغيل Windows وLinux
- الفهم الأساسي لشبكات الكمبيوتر
- فهم نظامي الأعداد الثنائي والسداسي العشري
- التعرّف على برنامج محاكي الشبكات Packet Tracer من Cisco

الشهادة المستهدفة

تتماشى هذه الدورة التدريبية مع شهادة CyberOps Associate (CBROPS) المعتمدة من Cisco. يحتاج المرشحون إلى اجتياز اختبار 200-201 CBROPS للحصول على شهادة CyberOps Associate المعتمدة من Cisco. يقيس اختبار CBROPS مستوى معرفة المرشح ومهاراته المتعلقة بمفاهيم الأمان ومراقبة الأمان والتحليل المستند إلى المضيف وتحليل اختراق الشبكة والسياسات والإجراءات الأمنية.

وصف الدورة التدريبية

تتضمن الدورة التدريبية العديد من الميزات لمساعدة الطلاب في استيعاب هذه المفاهيم:

- وتتألف الدورة التدريبية من ثماني وعشرين (28) وحدة. وتتألف كل وحدة من موضوعات.
- تركز الوحدات على التفكير النقدي، وحل المشكلات، والتعاون، والتطبيق العملي للمهارات.
- وتحتوي كل وحدة على طريقة ما لممارسة الفهم وتقييمه، كتمرين معملي مثلاً أو نشاط من برنامج Packet Tracer. وتوفر هذه الأنشطة على مستوى الوحدة ملاحظات وهي مصممة للإشارة إلى إتقان الدارِس للمهارات المطلوبة للدورة التدريبية. يمكن أن يتأكد الدارِسون من استيعابهم جيدًا قبل خوض اختبار أو امتحان سريع يُقيَّم بالدرجات.
- قد تحتوي بعض المواضيع على اختبار تفاعلي بعنوان "تحقّق من استيعابك"، أو طريقة أخرى لتقييم الاستيعاب، كتمرين معملي مثلاً أو نموذج من برنامج محاكي الشبكات Packet Tracer. تم تصميم هذه التقييمات على مستوى الموضوع لإعلام المتعلّمين إذا كان لديهم استيعاب جيد لمحتوى الموضوع، أو إذا كانوا بحاجة إلى مراجعته قبل المتابعة. يمكن أن يتأكد المتعلّمون من استيعابهم جيدًا قبل خوض اختبار أو امتحان سريع يُقيَّم بالدرجات. لا تؤثر الاختبارات السريعة بعنوان "تحقّق من استيعابك" على التقدير العام للمتعلّم.

- يعمل المحتوى الغني بالوسائط المتعددة، بما يشمل الأنشطة التفاعلية ومقاطع الفيديو والاختبارات السريعة، على معالجة مجموعة متنوعة من أساليب التعلم ويساعد على تحفيز عملية التعلم وزيادة القدرة على الاحتفاظ بالمعرفة المكتسبة.
- تحاكي البيئات الظاهرية سيناريوهات تهديد الأمن السيبراني في العالم الحقيقي، وتخلق فرصًا لمراقبة الأمان وتحليله وحلّ مشاكله.
- وتساعد التمارين المعملية العملية الطلاب على تطوير التفكير النقدي ومهارات حل المشاكل المعقدة.
- توفِّر التقييمات الابتكارية ملاحظات فورية لدعم تقييم المعارف والمهارات المكتسبة.
- يتم شرح المفاهيم الفنية باستخدام لغة تناسب الدارِسين من جميع المستويات، وتعمل الأنشطة التفاعلية المُضمَّنة على تجزئة قراءة المحتوى وتساعد على تعزيز الفهم.
- لا يُشجّع المنهج الدراسي الطلاب على التفكير في تعليم إضافي لتكنولوجيا المعلومات فقط، لكنه يركِّز أيضًا على المهارات التطبيقية والخبرة العملية.
- تم تصميم أنشطة برنامج Packet Tracer من Cisco للاستخدام مع برنامج Packet Tracer الإصدار 7.3.0 أو الإصدارات الأحدث.

أهداف الدورة التدريبية

تغطي الدورة التدريبية CyberOps Associate الإصدار 1.0 المعرفة والمهارات اللازمة للتعامل بنجاح مع المهام والواجبات والمسؤوليات الخاصة بمحلل أمن سيبراني بمستوى مساعد يعمل في مركز عمليات أمنية (SOC).

عقب الانتهاء من الدورة التدريبية *CyberOps Associate v1.0*، سيكون بمقدور الطلاب إنجاز المهام التالية:

- تثبيت الأجهزة الظاهرية لإنشاء بيئة آمنة لتنفيذ أحداث تهديد الأمن السيبراني وتحليلها.
- شرح دور محلل عمليات الأمن السيبراني في المؤسسة.
- شرح ميزات نظام التشغيل Windows وخصائصه اللازمة لدعم تحليلات الأمن السيبراني.
- شرح ميزات نظام التشغيل Linux وخصائصه.
- تحليل تشغيل بروتوكولات الشبكة وخدماتها.
- شرح تشغيل البنية التحتية للشبكة.
- تصنيف الأنواع المختلفة من الهجمات التي تتعرض لها الشبكة.
- استخدام أدوات مراقبة الشبكة لتحديد الهجمات التي تتعرض لها بروتوكولات الشبكة وخدماتها.
- شرح كيفية منع الوصول الضار إلى شبكات الكمبيوتر والبيئات المضيفة والبيانات.
- شرح آثار التشفير على مراقبة أمان الشبكة.
- شرح كيفية إجراء التحقيقات في حالات الثغرات الأمنية لنقطة النهاية والهجمات عليها.
- تقييم تنبيهات أمان الشبكة.
- تحليل بيانات اختراق الشبكة لتحديد الأجهزة المضيفة التي تم اختراقها.
- تطبيق نماذج الاستجابة للحوادث لإدارة حوادث أمان الشبكة.

متطلبات المعدات المعملية

لا تتطلب هذه الدورة أي معدات مادية بخلاف كمبيوتر شخصي معملي خاص بالطالب. فإنه يستخدم العديد من الأجهزة الافتراضية (VMs) لإنشاء تجربة معملية.

حِزمة المعدات الأساسية:

- أجهزة الكمبيوتر الشخصي - الحد الأدنى من متطلبات النظام
  - CPU وحدة المعالجة المركزية: Intel Pentium 4، بسرعة 2.53 جيجاهرتز أو ما يعادلها مع دعم المحاكاة الظاهرية
  - أنظمة التشغيل، مثل Microsoft Windows وLinux وMac OS
  - معالج 64 بت
  - ذاكرة الوصول العشوائي: 8 جيجابايت
  - سعة التخزين: 40 جيجابايت من مساحة القرص الفارغة
  - دقة العرض: 1024 × 768

- خطوط اللغة التي تدعم ترميز Unicode (إذا تم العرض بلغات أخرى غير اللغة الإنجليزية)
- أحدث برامج تشغيل بطاقة الفيديو وتحديثات نظام التشغيل

- اتصال بالإنترنت للتمارين المعملية وأجهزة الكمبيوتر الشخصية للطلاب

برامج الكمبيوتر الشخصي للطالب:

- Oracle VM VirtualBox Manager (الإصدار 6.1 أو إصدار أحدث)
- CyberOps Workstation VM
  - قابل للتنزيل من الدورة التدريبية
  - يتطلب 1 جيجابايت من ذاكرة الوصول العشوائي و20 جيجابايت من مساحة القرص
- Security Onion VM
  - قابل للتنزيل من الدورة التدريبية
  - يتطلب 4 جيجابايت من ذاكرة الوصول العشوائي (الحد الأدنى) و8 جيجابايت من ذاكرة الوصول العشوائي (المُوصى به بشدة) و20 جيجابايت من مساحة القرص

المخطط التفصيلي لدورة CyberOps Associate

مُدرج أدناه مجموعة الوحدات الحالية والكفاءات المرتبطة بها موضحةً لهذه الدورة التدريبية. كل وحدة هي وحدة متكاملة للتعلّم تتألف من المحتوى والأنشطة والتقييمات التي تستهدف مجموعة محددة من الكفاءات. يعتمد حجم الوحدة على عمق المعرفة والمهارة اللازمة لإتقان الكفاءة. تعتبر بعض الوحدات تأسيسية، والتي تعمل الأدوات المقدَّمة فيها، ولكن لا يتم تقييم الطالب فيها، على تمكين تعلّم المفاهيم التي تمت تغطيتها في اختبار شهادة CBROPS.

الجدول 1. مخطط الدورة التدريبية CyberOps Associate v1.0

الوحدة/الموضوعات	الأهداف/الأغراض
الوحدة 1. الخطر	**شرح سبب تعرض الشبكات والبيانات للهجوم.**
1.0 مقدمة	مقدمة موجزة للدورة التدريبية والوحدة الأولى.
1.1 قصص الحرب	توضيح ميزات حوادث الأمن السيبراني.
1.2 الجهات القائمة بالتهديدات	شرح دوافع الجهات القائمة بالتهديدات التي تقف وراء حوادث أمنية محددة.
1.3 تأثير التهديدات	شرح التأثير المحتمل للهجمات الأمنية التي تتعرض لها الشبكة.
1.4 ملخص الخطر	ملخص موجز واختبار الوحدة.
الوحدة 2. المقاتلون المشاركون في الحرب على الجرائم الإلكترونية	**شرح كيفية الاستعداد للعمل في مجال عمليات الأمن السيبراني.**
2.0 مقدمة	مقدمة إلى الوحدة.
2.1 مركز العمليات الأمنية الحديثة	شرح مهمة مركز عمليات الأمان.
2.2 أن تصبح مدافعًا	وصف الموارد المتاحة للإعداد لمهنة في عمليات الأمن السيبراني.
2.3 المقاتلون المشاركون في الحرب على موجز الجرائم الإلكترونية	ملخص موجز واختبار الوحدة.
الوحدة 3. نظام التشغيل Windows	**شرح ميزات الأمان في نظام التشغيل Windows.**
3.0 المقدمة	مقدمة للوحدة.
3.1 محفوظات نظام التشغيل Windows	وصف تاريخ نظام التشغيل Windows.

الوحدة/الموضوعات	الأهداف/الأغراض
3.2 البنية التحتية لنظام التشغيل Windows وعملياته	شرح البنية التحتية لنظام التشغيل Windows وكيفية تشغيله.
3.3 تكوين Windows ومراقبته	شرح كيفية تكوين نظام التشغيل Windows ومراقبته.
3.4 أمان Windows	شرح كيف يمكن الحفاظ على أمان Windows.
3.5 ملخص نظام التشغيل Windows	ملخص موجز واختبار الوحدة.
الوحدة 4. نظرة عامة على نظام التشغيل Linux	**تنفيذ الأمان الأساسي لنظام التشغيل Linux.**
4.0 المقدمة	مقدمة للوحدة.
4.1 أساسيات Linux	شرح سبب أهمية مهارات Linux لمراقبة أمان الشبكة وتنفيذ التحقيقات المتعلقة به.
4.2 العمل في Linux Shell	استخدام واجهة Linux الأساسية لمعالجة الملفات النصية.
4.3 خوادم Linux وعملاؤه	شرح كيفية عمل شبكات العميل-الخادم.
4.4 إدارة الخادم الأساسي	شرح كيفية تحديد مسؤول Linux لموقع ملفات سجل الأمان ومعالجتها.
4.5 نظام ملفات Linux	إدارة نظام ملفات Linux وأذوناته.
4.6 العمل مع واجهة المستخدم الرسومية لنظام التشغيل Linux	شرح المكونات الأساسية لواجهة المستخدم الرسومية لنظام التشغيل Linux.
4.7 العمل على بيئة مضيفة تعمل بنظام التشغيل Linux	استخدام أدوات الكشف عن البرامج الضارة على بيئة مضيفة تعمل بنظام التشغيل Linux.
4.8 ملخص أساسيات نظام التشغيل Linux	ملخص موجز واختبار الوحدة.
الوحدة 5. بروتوكولات الشبكة	**شرح كيفية تمكين البروتوكولات لعمليات الشبكة.**
5.0 المقدمة	مقدمة للوحدة.
5.1 عملية اتصال الشبكة	شرح العمليات الأساسية للاتصالات الشبكية بالبيانات.
5.2 بروتوكولات الاتصال	شرح كيفية تمكين البروتوكولات لعمليات الشبكة.
5.3 تضمين البيانات	شرح كيف يسمح تضمين البيانات بنقل البيانات عبر الشبكة.
5.4 ملخص بروتوكولات الشبكة	ملخص موجز واختبار الوحدة.
الوحدة 6. بروتوكول الإنترنت (IP) والإيثرنت	**شرح مدة قدرة بروتوكولات الإنترنت والإيثرنت على دعم اتصالات الشبكة.**
6.0 مقدمة	مقدمة للوحدة.
6.1 الإيثرنت	شرح كيفية دعم الإيثرنت لاتصالات الشبكة.
6.2 IPv4	شرح كيفية دعم بروتوكول IPv4 لاتصالات الشبكة.
6.3 أساسيات تحديد عناوين IP	شرح كيفية تمكين عناوين IP لاتصال الشبكة.
6.4 أنواع عناوين IPv4	شرح أنواع عناوين IPv4 التي تمكّن اتصال الشبكة.
6.5 البوابة الافتراضية	شرح كيفية تمكين البوابة الافتراضية لاتصال الشبكة.
6.6 طول بادئة IPv6	شرح كيفية دعم بروتوكول IPv6 لاتصالات الشبكة.

الوحدة/الموضوعات	الأهداف/الأغراض
6.7 ملخص الإيثرنت وبروتوكول IP	ملخص موجز واختبار الوحدة.
الوحدة 7. مبادئ أمان الشبكة	**التحقق من صحة الاتصال**
7.0 المقدمة	مقدمة للوحدة.
7.1 ICMP	شرح كيفية استخدام ICMP لاختبار اتصال الشبكة.
7.2 الأداتان المساعدتان Ping وTraceroute	استخدم أدوات Windows وPing وTraceroute للتحقق من صحة اتصال الشبكة.
7.3 ملخص التحقق من الاتصال	ملخص موجز واختبار الوحدة.
الوحدة 8. بروتوكول تحليل العناوين	**تحليل وحدات بيانات البروتوكول (PDUs) الخاصة ببروتوكول تحليل العناوين على شبكة ما.**
8.0 المقدمة	مقدمة للوحدة.
8.1 MAC وIP	مقارنة أدوار عنوان MAC وعنوان IP.
8.2 ARP (بروتوكول تحليل العناوين)	تحليل ARP (بروتوكول تحليل العناوين) من خلال فحص إطارات الإيثرنت.
8.3 مشاكل ARP (بروتوكول تحليل العناوين)	شرح مدى تأثير طلبات ARP (بروتوكول تحليل العناوين) على أداء الشبكة والبيئة المضيفة.
8.4 ملخص بروتوكول تحليل العنوان	ملخص موجز واختبار الوحدة.
الوحدة 9. طبقة النقل	**شرح كيفية دعم بروتوكولات طبقة النقل لوظائف الشبكة.**
9.0 المقدمة	مقدمة للوحدة.
9.1 خصائص طبقة النقل	شرح كيفية دعم بروتوكولات طبقة النقل لاتصال الشبكة.
9.2 إنشاء جلسة عمل طبقة النقل	شرح كيفية إنشاء طبقة النقل لجلسات عمل الاتصالات.
9.3 موثوقية طبقة النقل	شرح كيفية قيام إنشاء طبقة النقل لاتصالات موثوقة.
9.4 ملخص طبقة النقل	ملخص موجز واختبار الوحدة.
الوحدة 10. خدمات الشبكة	**شرح كيفية تمكين خدمات الشبكة لوظائف الشبكة.**
10.0 المقدمة	مقدمة للوحدة.
10.1 DHCP	شرح كيفية تمكين خدمات DHCP لوظائف الشبكة.
10.2 DNS	شرح كيفية تمكين خدمات DNS لوظائف الشبكة.
10.3 NAT	شرح كيفية تمكين خدمات NAT لوظائف الشبكة.
10.4 خدمات نقل الملفات ومشاركتها	شرح كيفية تمكين خدمات نقل الملفات ومشاركتها لوظائف الشبكة.
10.5 البريد الإلكتروني	شرح كيفية تمكين خدمات البريد الإلكتروني لوظائف الشبكة.
10.6 HTTP	شرح كيفية تمكين خدمات HTTP لوظائف الشبكة.
10.7 ملخص خدمات الشبكة	ملخص موجز واختبار الوحدة.

الوحدة/الموضوعات	الأهداف/الأغراض
الوحدة 11. أجهزة اتصالات الشبكة	**شرح كيفية تمكين أجهزة الشبكة لاتصال الشبكة السلكي واللاسلكي.**
11.0 المقدمة	مقدمة للوحدة.
11.1 أجهزة الشبكة	شرح كيفية تمكين أجهزة الشبكة لاتصال الشبكة.
11.2 الاتصالات اللاسلكية	شرح كيفية تمكين الأجهزة اللاسلكية لاتصال الشبكة.
11.3 ملخص أجهزة اتصالات الشبكة	ملخص موجز واختبار الوحدة.
الوحدة 12. البنية التحتية لأمان الشبكة	**شرح كيفية استخدام أجهزة الشبكة وخدماتها لتعزيز أمان الشبكة.**
12.0 مقدمة	مقدمة للوحدة.
12.1 هياكل الشبكة	شرح مدى تأثير تصميمات الشبكة على تدفق حركة مرور البيانات عبر الشبكة.
12.2 أجهزة الأمان	شرح كيفية استخدام الأجهزة المتخصصة لتعزيز أمان الشبكة.
12.3 خدمات الأمان	شرح مدى قدرة خدمات الشبكة على تعزيز أمان الشبكة.
12.4 ملخص البنية التحتية لأمان الشبكة	ملخص موجز لهذه الوحدة.
الوحدة 13. المهاجمون وأدواتهم	**شرح كيفية تعرض الشبكات للهجوم.**
13.0 مقدمة	مقدمة للوحدة.
13.1 مَن الذي يهاجم شبكتنا؟	شرح مدى تطور تهديدات الشبكات.
13.2 أدوات القائمين بالتهديدات	وصف الأنواع المختلفة من أدوات الهجوم التي يستخدمها القائمون بالتهديدات.
13.3 ملخص المهاجمين وأدواتهم	ملخص موجز واختبار الوحدة.
الوحدة 14. التهديدات والهجمات الشائعة	**شرح الأنواع المختلفة من التهديدات والهجمات.**
14.0 مقدمة	مقدمة للوحدة.
14.1 البرامج الضارة	وصف أنواع البرامج الضارة.
14.2 الهجمات الشائعة على الشبكة – الاستطلاع والوصول والهندسة الاجتماعية	شرح هجمات الاستطلاع والوصول والهندسة الاجتماعية.
14.3 الهجمات على الشبكة – رفض الخدمة وتجاوزات سعة المخزن المؤقت والتهرب	شرح هجمات رفض الخدمة وتجاوزات سعة المخزن المؤقت والتهرب.
14.4 ملخص التهديدات والهجمات الشائعة	ملخص موجز واختبار الوحدة.
الوحدة 15. مراقبة تشغيل الشبكة	**شرح مراقبة حركة مرور بيانات الشبكة.**
15.0 مقدمة	مقدمة للوحدة.
15.1 مقدمة إلى مراقبة الشبكة	شرح أهمية مراقبة الشبكة
15.2 مقدمة إلى أدوات مراقبة الشبكة	شرح كيفية تنفيذ مراقبة الشبكة.
15.3 ملخص مراقبة الشبكة والأدوات	ملخص موجز واختبار الوحدة.

الوحدة/الموضوعات	الأهداف/الأغراض
الوحدة 16. مهاجمة الأساس	**شرح كيفية تمكين الثغرات الأمنية في TCP/IP لهجمات الشبكة.**
16.0 مقدمة	مقدمة للوحدة.
16.1 تفاصيل وحدات PDU لبروتوكول IP	شرح بنية عنوان IPv4 وIPv6.
16.2 الثغرات الأمنية في IP	شرح كيفية تمكين الثغرات الأمنية في IP لهجمات الشبكة.
16.3 الثغرات الأمنية في TCP وUDP	شرح كيفية تمكين الثغرات الأمنية في TCP وUDP لهجمات الشبكة.
16.4 ملخص مهاجمة المؤسسة	ملخص موجز واختبار الوحدة.
الوحدة 17. مهاجمة ما نقوم به	**شرح مدى تعرض تطبيقات الشبكات وخدماتها الشائعة لخطورة الهجوم.**
17.0 مقدمة	مقدمة للوحدة.
17.1 خدمات IP	شرح الثغرات الأمنية في خدمة IP.
17.2 خدمات المؤسسة	شرح كيفية تمكين الثغرات الأمنية في تطبيق الشبكة لهجمات الشبكة.
17.3 ملخص مهاجمة ما نفعله	ملخص موجز واختبار الوحدة.
الوحدة 18. فهم الدفاع	**شرح النُهُج الخاصة بالدفاع عن أمان الشبكة.**
18.0 مقدمة	مقدمة للوحدة.
18.1 الدفاع المتعمق	شرح كيفية استخدام استراتيجية الدفاع المتعمق لحماية الشبكات.
18.2 سياسات الأمان ولوائحه ومعاييره	شرح سياسات الأمان ولوائحه ومعاييره.
18.3 ملخص فهم الدفاع	ملخص موجز واختبار الوحدة.
الوحدة 19. التحكم بالوصول	**شرح التحكم بالوصول كطريقة لحماية الشبكة.**
19.0 مقدمة	مقدمة للوحدة.
19.1 مفاهيم التحكم بالوصول	شرح كيفية حماية التحكم بالوصول لبيانات الشبكة.
19.2 استخدام AAA (المصادقة والتفويض والمحاسبة) وتشغيلها	شرح كيفية استخدام AAA (المصادقة والتفويض والمحاسبة) للتحكم بالوصول إلى الشبكة.
19.3 ملخص التحكم بالوصول	ملخص موجز واختبار الوحدة.
الوحدة 20. التحليل الذكي للتهديدات	**استخدام مصادر متنوعة للتحليل الذكي لتحديد موقع التهديدات الأمنية الحالية.**
20.0 مقدمة	مقدمة للوحدة.
20.1 مصادر المعلومات	وصف مصادر المعلومات المُستخدمة لنقل التهديدات المستجدة لأمان الشبكة.
20.2 خدمات التحليل الذكي للتهديدات	وصف العديد من خدمات التحليل الذكي للتهديدات.
20.3 ملخص ذكاء التهديدات	ملخص موجز واختبار الوحدة.
الوحدة 21. التشفير	**شرح كيفية دعم البنية التحتية للمفتاح العمومي لأمان الشبكة.**
21.0 مقدمة	مقدمة للوحدة.

الوحدة/الموضوعات	الأهداف/الأغراض
21.1 التكامل والأصالة	شرح دور التشفير في ضمان تكامل البيانات وأصالتها.
21.2 السرية	شرح كيفية تعزيز نُهُج التشفير لسرية البيانات.
21.3 تشفير المفتاح العمومي	شرح تشفير المفتاح العمومي.
21.4 المراجع المُصدَّقة ونظام توثيق البنية التحتية للمفتاح العمومي (PKI)	شرح كيفية عمل البنية التحتية للمفتاح العمومي.
21.5 التطبيقات وآثار التشفير	شرح مدى تأثير استخدام التشفير على عمليات الأمن السيبراني.
21.6 ملخص التشفير	ملخص موجز لهذه الوحدة.
الوحدة 22. حماية نقطة النهاية	**شرح كيفية إنشاء موقع ويب لتحليل البرامج الضارة لتقرير لتحليل البرامج الضارة.**
22.0 مقدمة	مقدمة للوحدة.
22.1 حماية مكافح البرامج الضارة	شرح طرق التخفيف من حدة البرامج الضارة.
22.2 منع الاقتحام المستند إلى البيئة المضيفة	شرح إدخالات سجل IPS/IDS المستندة إلى البيئة المضيفة.
22.3 أمان التطبيق	شرح كيفية استخدام وضع الحماية لتحليل البرامج الضارة.
22.4 ملخص حماية نقطة النهاية	ملخص موجز واختبار الوحدة.
الوحدة 23. تقييم الثغرات الأمنية في نقاط النهاية	**شرح كيفية تقييم الثغرات الأمنية في نقاط النهاية وإدارتها.**
23.0 مقدمة	مقدمة للوحدة.
23.1 جمع معلومات الشبكة والخادم	شرح قيمة جمع معلومات الشبكة والخادم.
23.2 نظام تسجيل درجات الثغرات الأمنية الشائعة (CVSS)	شرح كيفية استخدام تقارير CVSS لوصف الثغرات الأمنية.
23.3 الإدارة الآمنة للجهاز	شرح كيفية استخدام تقنيات إدارة الآمنة للجهاز لحماية البيانات والأصول.
23.4 أنظمة إدارة أمان المعلومات	شرح كيفية استخدام أنظمة إدارة أمان المعلومات لحماية الأصول.
23.5 ملخص تقييم الثغرات الأمنية في نقاط النهاية	ملخص موجز واختبار الوحدة.
الوحدة 24. التقنيات والبروتوكولات	**شرح مدى تأثير تقنيات الأمان على مراقبة الأمان.**
24.0 مقدمة	مقدمة للوحدة.
24.1 بروتوكولات المراقبة الشائعة	شرح سلوك بروتوكولات الشبكة الشائعة في سياق مراقبة الأمان.
24.2 تقنيات الأمان	شرح مدى تأثير تقنيات الأمان على القدرة على مراقبة بروتوكولات الشبكة الشائعة.
24.3 ملخص التقنيات والبروتوكولات	ملخص موجز واختبار الوحدة.
الوحدة 25. بيانات أمان الشبكة	**شرح أنواع بيانات أمان الشبكة المُستخدمة في مراقبة الأمان.**
25.0 مقدمة	مقدمة للوحدة.
25.1 أنواع بيانات الأمان	وصف أنواع البيانات المُستخدمة في مراقبة الأمان.
25.2 سجلات الأجهزة الطرفية	وصف عناصر ملف سجل الجهاز الطرفي.

الوحدة/الموضوعات	الأهداف/الأغراض
25.3 سجلات الشبكة	وصف عناصر ملف سجل جهاز الشبكة.
25.4 ملخص بيانات أمان الشبكة	ملخص موجز واختبار الوحدة.
الوحدة 26. تقييم التنبيهات	**شرح عملية تقييم التنبيهات.**
26.0 مقدمة	مقدمة للوحدة.
26.1 مصدر التنبيهات	تحديد بنية التنبيهات.
26.2 نظرة عامة على تقييم التنبيهات	شرح كيفية تصنيف التنبيهات.
26.3 ملخص تنبيهات التقييم	ملخص موجز واختبار الوحدة.
الوحدة 27. العمل مع بيانات أمان الشبكة	**ترجمة البيانات لتحديد مصدر التنبيه.**
27.0 مقدمة	مقدمة للوحدة.
27.1 منصة البيانات المشتركة	شرح كيفية تحضير البيانات لاستخدامها في نظام مراقبة أمان الشبكة (NSM).
27.2 تقصّي بيانات الشبكة	استخدام أدوات Security Onion لتقصّي أحداث أمان الشبكة.
27.3 تعزيز عمل محلل الأمن السيبراني	وصف أدوات مراقبة الشبكة التي تعزز إدارة سير العمل.
27.4 العمل مع ملخص بيانات أمان الشبكة	ملخص موجز واختبار الوحدة.
الوحدة 28. التحليلات القضائية الرقمية وتحليل الحوادث والاستجابة لها	**شرح كيفية استجابة CyberOps Associate لحوادث الأمن السيبراني.**
28.0 مقدمة	مقدمة للوحدة.
28.1 التعامل مع الأدلة وعزو الهجوم	شرح دور عمليات التحليلات القضائية الرقمية.
28.2 إطار عمل Cyber Kill Chain	تحديد الخطوات الواردة في إطار عمل Cyber Kill Chain.
28.3 النموذج الماسي لتحليل الاقتحام	تصنيف حدث اقتحام باستخدام أداة Diamond Model.
28.4 الاستجابة للحوادث	تطبيق إجراءات التعامل مع حوادث NIST 800-61r2 على سيناريو حادث معين.
28.5 ملخص التحليلات القضائية الرقمية، وتحليل الحوادث والاستجابة لها	ملخص موجز لهذه الوحدة.
28.6 استعد لامتحانك وابدأ مسارك المهني!	إعداد الشهادة وقسائم الخصم والموارد المهنية الأخرى.

المقرات الرئيسية بالأمريكتين
Cisco Systems. Inc
San Jose. CA

المقر الرئيسي بدول آسيا المطلة على المحيط الهادئ
Cisco Systems (USA) Pad Ltd.
سنغافورة

المقرات الرئيسية في أوروبا
Cisco Systems International BV Amsterdam،
هولندا

يوجد لدى Cisco أكثر من 200 مكتب في العالم. تتوفر قائمة بالعناوين وأرقام الهواتف وأرقام الفاكسات على موقع الويب الخاصة بشركة Cisco على العنوان **www.cisco.com/go/offices**.