ICDL Arabia

الأمن الرقمي
(الجيش والشرطة)

الغرض

يهدف هذا المستند إلى تقديم التفاصيل حول منهج ECDL / ICDL أساسيات الإنترنت. يصف المنهج، من خلال مخرجات التعلم، المعرفة والمهارات التي يجب أن يمتلكها المرشح للحصول على شهادة ECDL/ICDL أساسيات الإنترنت. كذلك يقوم المنهج بتقديم أساسا للاختبار النظري والعملي في هذه الوحدة.

إخلاء المسؤولية

بالرغم من أخذ كل عناية من قبل مؤسسة ECDL في إعداد هذا المنشور، لا يتم إعطاء أي ضمان من مؤسسة ECDL، بصفتها الناشر، حول اكتمال المعلومات الواردة فيه، ولن تتحمل مؤسسة ECDL أية مسؤولية عن أية أخطاء، سهو، عدم دقة، خسارة أو ضرر من أي نوع تنشأ بموجب هذه المعلومات أو أية تعليمات واردة في هذا المنشور. يجوز إجراء تغييرات من قبل مؤسسة ECDL حسب تقديرها الخاص وفي أي وقت ودون إشعار مسبق.

الفئة	مجموعة املهارات	موضوع املهمة
الحماية	تحديد المخاطر	تحديد السمات الرئيسية لأمن المعلومات الضرورية للعمليات العسكرية وأنظمة إنفاذ القانون. تحديد أنواع المعلومات الحساسة الموجودة في الأنظمة العسكرية وأنظمة إنفاذ القانون. فهم لماذا يجب أن يتم وضع علامات أمان على المستندات الحساسة التي يتم الاحتفاظ بها في الأنظمة العسكرية وأنظمة إنفاذ القانون . فهم مخاطر الحرب الإلكترونية. التعرف على المكاسب الإجرامية في الحصول على معلومات حساسة في الأنظمة العسكرية وأنظمة إنفاذ القانون. إدراك الطرق التي يستخدمها المجرمون للحصول على البيانات من الأنظمة الآمنة. تحديد الاستخدامات الإجرامية للمعلومات العسكرية الحساسة وأنظمة إنفاذ القانون. التعرف على برامج ضارة محددة يمكن استخدامها لاختراق الأنظمة العسكرية أو أنظمة إنفاذ القانون.
	المعلومات الشخصية	إدراك مدى أهمية وقيمة المعلومات الشخصية للأفراد العسكريين وموظفي أنظمة إنفاذ القانون بالنسبة لمجرمي الإنترنت. إدراك مدى أهمية وقيمة المعلومات العائلية للأفراد العسكريين وموظفي أنظمة إنفاذ القانون بالنسبة لمجرمي الإنترنت. التعرف على الطرق التي يمكن بها استغلال حسابات وسائل التواصل الاجتماعي للحصول على معلومات شخصية. التعرف على كيفية استغلال المعلومات التشغيلية من حسابات وسائل التواصل الاجتماعي. فهم كيفية استغلال بيانات الموقع الجغرافي المستمدة من الصور عبر الإنترنت. تحديد كيف يمكن استغلال المعلومات الشخصية والآراء المنشورة في منتديات الدردشة عبر الإنترنت.

موضوع املهمة	مجموعة املهارات	الفئة
مقدمة للبصمة الرقمية. فهم كيف يمكن للبصمة الرقمية الخاصة بالموظفين العسكريين وموظفي أنظمة إنفاذ القانون أن تضع هؤلاء الأفراد وأفراد أسرهم ، ووحداتهم الرسمية في خطر. فهم الأنشطة التي يمكنها أن تترك بصمة رقمية عبر الإنترنت. تحديد طرق لتقليل البصمة الرقمية.	البصمة الرقمية	
فهم مفهوم مصادقة المستخدم. إدراك المخاطر المرتبطة بالاستخدام غير المصرح به للأنظمة العسكرية وأنظمة إنفاذ القانون. معرفة كيفية إنشاء كلمات مرور فعالة مناسبة للاستخدام العسكري وأنظمة إنفاذ القانون. فهم مبادئ أمان كلمة المرور الخاصة بالأنظمة العسكرية وأنظمة إنفاذ القانون. التعرف على أهمية امتيازات إدارة الوصول عند استخدام الأنظمة العسكرية وأنظمة إنفاذ القانون. فهم أهمية "المصادقة الثنائية" عند استخدام الأنظمة العسكرية الحساسة وأنظمة إنفاذ القانون. فهم أهمية استخدام مقاييس المصادقة الحيوية في وصول الموظفين وإدارة المحتجزين ، وأثناء استخدام الأنظمة العسكرية الحساسة وأنظمة إنفاذ القانون. إدراك أن الملفات الفرعية الحساسة والوثائق المحددة يجب أيضًا أن تكون محمية بكلمة مرور على الأنظمة العسكرية وأنظمة إنفاذ القانون.	المصادقة	

موضوع املهمة	مجموعة املهارات	الفئة
فهم لماذا يجب على جميع الأنظمة العسكرية وأنظمة أنظمة إنفاذ القانون الحصول على أحدث برامج مكافحة الفيروسات. فهم تهديدات الفيروسات المرتبطة بوسائط التخزين المتنقلة. إدراك متطلبات استخدام وسائط التخزين متنقلة محمية لنقل المعلومات الحساسة. إدراك الحاجة لفحص الفيروسات للتحقق من جميع وسائط التخزين المتنقلة قبل توصيلها بالأنظمة العسكرية وأنظمة إنفاذ القانون. فهم خطورة الفيروسات المنقولة عبر البريد الإلكتروني. تحديد طرق فحص مرفقات البريد الإلكتروني للبحث عن الفيروسات.	مكافحة الفيروسات	
فهم مفهوم التجسس الإلكتروني ، وعلاقته ببرامج التجسس. فهم المخاطر المرتبطة بالتجسس على الأنظمة العسكرية وأنظمة إنفاذ القانون. إدراك الفترات الزمنية التي يمكن أن تبقى فيها برامج التجسس نشطة في الأنظمة دون أن يتم اكتشافها. فهم أهمية مواكبة تهديدات برامج التجسس الجديدة. التعرف على برامج التجسس الشائعة. التعرف على برامج مكافحة التجسس الشائعة. إدراك كيفية تحديد ما إذا كانت برامج التجسس قيد التشغيل.	مكافحة برامج التجسس	
فهم المخاطر المرتبطة بفيروس الفدية على الأنظمة العسكرية وأنظمة إنفاذ القانون. التعرف على أنواع مختلفة من فيروسات الفدية. التعرف على العديد من الأدوات المتخصصة في اكتشاف و مكافحة فيروسات الفدية الخاصة بالاستخدام العسكري.	مكافحة فيروس الفدية	

الفئة	مجموعة املهارات	موضوع املهمة
	الإنترنت المظلم	فهم تعريف الإنترنت المظلم. تعرف على كيفية عمل الإنترنت المظلم ولماذا يصعب تتبع المعلومات التي يتم تبادلها عن طريق. إدراك الاستخدام الإيجابي والسلبي للإنترنت المظلم. تحديد البرنامج المستخدم لتصفح وتبادل المعلومات على الإنترنت المظلم.
الحماية	البريد الإلكتروني	تحديد متطلبات المرشحات المرتفعة للرسائل الاقتحامية (SPAM) في حسابات البريد الإلكتروني العسكرية وأنظمة إنفاذ القانون. إدراك كيفية ضبط مرشحات الرسائل الاقتحامية على مستوى مناسب. تحديد كيفية وضع علامة على المرسل على أنه "موثوق به" لضمان تصفية البريد بشكل صحيح. إدراك المخاطر المرتبطة باستخدام البريد الإلكتروني الشخصي في الأنظمة العسكرية وأنظمة إنفاذ القانون. تحديد الاستخدامات المقبولة للبريد الإلكتروني في الأنظمة العسكرية وأنظمة إنفاذ القانون. فهم خطر سرقة المعلومات من خلال التصيد الاحتيالي.
	الاتصال اللاسلكي	فهم تقنيات الاتصال اللاسلكي الشائعة المستخدمة في المؤسسات العسكرية وأنظمة إنفاذ القانون - على سبيل المثال ، أجهزة الكمبيوتر القابلة للارتداء ، والكاميرا ت المرفقة بالجسم وما إلى ذلك. فهم الثغرات الأمنية الخاصة بالشبكات اللاسلكية. إدراك كيفية تعرض الشبكات اللاسلكية داخل المنشآت العسكرية وأنظمة إنفاذ القانون لخطر الجريمة الإلكترونية. إدراك الطرق المستخدمة من قبل مجرمي الإنترنت لاستغلال الشبكات اللاسلكية. تحديد كيفية تأمين الشبكات اللاسلكية المستخدمة في أغراض عسكرية وأنظمة إنفاذ القانون بشكل أفضل. فهم كيف يمكن استغلال الأجهزة الشخصية التي تستخدم تقنية الاتصال اللاسلكي في المنشآت العسكرية وأنظمة إنفاذ القانون.

موضوع املهمة	مجموعة املهارات	الفئة
تحديد منصات مختلفة من وسائل التواصل الاجتماعي.	وسائل التواصل الاجتماعي	
فهم عرض النطاق الترددي لساعات العمل والمشكلات السرية المرتبطة باستخدام الموظفين لوسائل التواصل الاجتماعي.		
إدراك المخاطر الشائعة التي تتشابه مع مختلف وسائط التواصل الاجتماعي.		
فهم أهمية الالتزام بسياسة وسائل التواصل الاجتماعي.		
فهم المخاطر المرتبطة بالاستخدام غير الملائم لوسائل التواصل الاجتماعي التي يمكن أن تؤثر على سمعة المؤسسات.		
فهم المخاطر المرتبطة بالاستخدام غير الملائم لوسائل التواصل الاجتماعي التي يمكن أن تؤثر على أمن التشغيل.		
فهم المخاطر المرتبطة بالاستخدام غير الملائم لوسائل التواصل الاجتماعي التي يمكن أن تؤثر على الأمن الشخصي.		
إدراك الطرق المستخدمة لاستهداف الأفراد العسكريين وموظفي أنظمة إنفاذ القانون للهندسة الاجتماعية من خلال وسائل التواصل الاجتماعي.		
إدراك الطرق المستخدمة لاستهداف الأفراد العسكريين وموظفي أنظمة إنفاذ القانون لسرقة الهوية من خلال وسائل التواصل الاجتماعي.		
إدراك كيفية استخدام المجرمين للملفات الشخصية المزيفة للعسكريين وأنظمة إنفاذ القانون على وسائل التواصل الاجتماعي لتحقيق أغراض إجرامية.		
إدراك متطلبات الأمان المادي لحماية الأنظمة العسكرية وأنظمة إنفاذ القانون.	الأمان المادي	
تحديد التحكم المادي لمتطلبات الوصول إلى الأنظمة التي تحتوي على معلومات عسكرية حساسة وأنظمة إنفاذ القانون.		
فهم مفهوم الفصل بين الأنظمة الحساسة وغير الحساسة في بيئة عسكرية أو أنظمة إنفاذ القانون.		
إدراك خطر إزالة المعلومات الحساسة من الأنظمة العسكرية وأنظمة إنفاذ القانون.		

موضوع املهمة	مجموعة املهارات	الفئة
فهم الحاجة إلى تشفير البيانات الحساسة الموجودة في الأنظمة العسكرية وأنظمة إنفاذ القانون. إدراك المخاطر المرتبطة باستخدام أجهزة الوسائط المتنقلة غير المشفرة لعمليات نقل البيانات الحساسة.	التشفير	
فهم كيف يمكن للمجرمين استخدام خدمات المراسلة المستندة إلى التشفير لتسريب وتبادل المعلومات الحساسة بطريقة لا يمكن تعقبها.		
فهم سبب أهمية وجود سياسة للتخلص الآمن من البيانات الموجودة في الأنظمة العسكرية وأنظمة إنفاذ القانون.	التدمير	
إدراك كيفية إزالة البيانات من نظام قبل التخلص منها.		
إدراك كيفية التأكد من أن جميع البيانات قد تمت إزالتها بشكل فعال من نظام قبل التخلص منها.		
إدراك مخاطر استخدام خدمات فرم الملفات السحابية.		
فهم خطر سرقة المعلومات عن طريق (التصيّد الصوتي) أو (التصيد عبر الرسائل النصية القصيرة).	المنزل/الهاتف المتحرك	
فهم المخاطر المرتبطة باستخدام الأجهزة الشخصية والمتنقلة في الأعمال العسكرية وأنظمة إنفاذ القانون.		
تحديد خطر نقل المعلومات بين الأنظمة الشخصية والعسكرية أو أنظمة إنفاذ القانون.		
فهم لماذا يجب مراقبة استخدام الأنظمة العسكرية أو أنظمة إنفاذ القانون في المنزل لأغراض المراجعة.		
العسكرية التي تربط الطائرات IoTمقدمة لشبكات إنترنت الأشياء وأنظمة الأسلحة والمركبات البرية والقوات.	إنترنت الأشياء	
فهم مخاطر الأدوات والآلات والمركبات المتصلة بالإنترنت التي يتم اختراقها أو التلاعب بها أو تعطيلها.		
تحديد أنواع مختلفة من التهديدات الشائعة المرتبطة بإنترنت الأشياء.		

الفئة	مجموعة املهارات	موضوع املهمة
التطبيق	شكل التواجد على الإنترنت	إدراك إعدادات الخصوصية التي تزيد من الأمان الشخصي والعائلي عند استخدام وسائل التواصل الاجتماعي. فهم لماذا يجب استخدام حسابات التواصل الاجتماعي المعتمدة فقط من قبل المؤسسات للتفاعل مع الجمهور. فهم مخاطر استخدام ميزة الفيديو المباشر على قنوات وسائل التواصل الاجتماعي. فهم كيفية إزالة المعلومات الموقع الجغرافي من الصور المنشورة على وسائل التواصل الاجتماعي.
	أفضل الأمثلة التطبيقية	فهم أهمية البقاء على اطلاع على أحدث المعلومات حول أحدث التهديدات عبر الإنترنت. تحديد بروتوكولات نظام إدارة أمن المعلومات المقبولة دوليا والمحددة للهيئات العسكرية وأنظمة إنفاذ القانون. فهم أهمية إخفاء هوية المستخدم عند استخدام الأنظمة العسكرية وأنظمة إنفاذ القانون لأغراض البحث. إدراك كيفية إجراء البحث عبر الإنترنت مع إخفاء هوية المستخدم. إدراك خطورة البيانات المخزنة مؤقتًا وملفات تعريف الارتباط عند استخدام الأنظمة العسكرية وأنظمة إنفاذ القانون. فهم خطر الإعلانات المنبثقة وكيفية إزالتها من الأنظمة العسكرية وأنظمة إنفاذ القانون. إدراك أهمية شهادات أمن الموقع. فهم سبب عدم إمكانية الوصول إلى المواقع غير الآمنة من الأنظمة العسكرية وأنظمة إنفاذ القانون. إدراك كيفية الاستخدام البريد الإلكتروني بأمان.

موضوع املهمة	مجموعة املهارات	الفئة
فهم سبب عدم تنزيل البرامج غير المعتمدة على الأنظمة العسكرية وأنظمة إنفاذ القانون.	البرامج والتطبيقات	
فهم سبب عدم تنزيل البرامج الشخصية على الأنظمة العسكرية وأنظمة إنفاذ القانون.		
إدراك المخاطر المرتبطة بتنزيل التطبيقات غير المعتمدة على الأنظمة العسكرية وأنظمة إنفاذ القانون.		
تحديد ميزات عملية تنظيمية للموافقة على البرامج والتطبيقات		
إدراك الآثار الأمنية المرتبطة بإصدارات قديمة وغير معتمدة من البرامج.		
فهم متطلبات فحص الأفراد الذين لديهم إمكانية الوصول إلى الأنظمة العسكرية وأنظمة إنفاذ القانون.	المتطلبات الواجبة	
فهم لماذا يجب أن يقتصر الوصول إلى الأنظمة العسكرية وأنظمة إنفاذ القانون الحساسة على الموظفين المعتمدين.		
فهم كيفية إجراء اختبارات الخلفية المرتبطة بجهات الاتصال عبر الإنترنت		
إدراك كيفية تتبع بروتوكول عنوان الإنترنت المرتبط بجهة اتصال عبر الإنترنت.		
إدراك اختبار اختراق الشبكات.		
فهم متطلبات الاختبار المنتظم لاختراق الشبكات في الأنظمة العسكرية وأنظمة إنفاذ القانون.		
فهم سبب أهمية إجراء نسخ احتياطي للأنشطة العسكرية وأنظمة إنفاذ القانون.	النسخ الاحتياطي	
تحديد الطرق المناسبة للنسخ الاحتياطي للمعلومات العسكرية وأنظمة إنفاذ القانون الحساسة.		
فهم مخاطر النسخ الاحتياطي للمعلومات السرية على الخوادم التي تعتمد على الخدمات السحابية.		

الفئة	مجموعة املهارات	موضوع املهمة
الدعم	سياسة الأمن الرقمي	فهم الحاجة إلى سياسة لأمن الإنترنت داخل المؤسسات العسكرية وأنظمة إنفاذ القانون.
		تحديد الميزات الرئيسية لسياسة الأمان الإلكتروني الفعال.
		فهم أهمية الوعي التنظيمي لسياسة الأمن الإلكتروني وضرورته داخل المنظمات العسكرية وأنظمة إنفاذ القانون.
		فهم أهمية تدقيق الالتزام بالسياسة الأمنية على الإنترنت.
	الطورائ والاستمرارية	فهم المصطلحات الطورائ والاستمرارية في سياق نظم تكنولوجيا المعلومات.
		إدراك الحاجة إلى استراتيجيات الطوارئ والاستمرارية في حالة حدوث هجوم على الإنترنت.
		فهم لماذا يجب على جميع الأفراد العسكريين وموظفي أنظمة إنفاذ القانون أن يكونوا قادرين على تنفيذ خطط الطوارئ والاستمرارية بفعالية في حالة حدوث هجوم على الإنترنت ، وأن يقوموا بإصلاح الخسائر الناتجة عن الهجوم.
	الاستجابة للحوادث	فهم مدى أهمية آلية الاستجابة للحوادث ضد الهجمات الإلكترونية.
		فهم السمات الأساسية للاستجابة للحوادث فيما يتعلق بالهجوم الإلكتروني.
		إدراك الحاجة إلى خطة استجابة للحادث الإلكتروني.
		تحديد السمات الرئيسية لخطة الاستجابة الفعالة للحوادث الإلكترونية.
	الثقافة	فهم فوائد ثقافة الأمن الرقمي الفعال داخل المؤسسات العسكرية وأنظمة إنفاذ القانون
		التعرف على أهمية ثقافة تبادل المعلومات والتعرف على أحدث التهديدات الإلكترونية وأفضل الممارسات لرعاية مجموعة مشتركة من المعرفة داخل المؤسسات العسكرية وأنظمة إنفاذ القانون.
		فهم مفهوم البلطجة الإلكترونية.
		إدراك كيفية تهديد البلطجة الإلكترونية للأمن داخل المؤسسات العسكرية وأنظمة إنفاذ القانون.