International Federation of Biosafety Associations

شهادة مهنية في الأمن السيبراني البيولوجي
محتوى الاختبار وبعض النماذج من الأسئلة والمراجع

تُثبت الشهادة المهنية في الأمن السيبراني البيولوجي، الممنوحة من قبل الفيدرالية الدولية لجمعيات السلامة البيولوجية (IFBA)، أن الأشخاص الحاصلين عليها يمتلكون كفاءات في مواجهة مخاطر الأمن السيبراني داخل المختبرات البيولوجية. يشمل ذلك مواجهة مخاطر تكنولوجيا المعلومات (IT)، ومخاطر تكنولوجيا التشغيل (OT) بهدف حماية البحوث البيولوجية الحساسة، والبيانات، وقواعد البيانات، ومرافق المختبرات، والمعدات من الوصول غير المصرح به، والسرقة، والتلاعب، أو أية أشكال أخرى من إساءة الاستخدام.

إن الشهادة المهنية في الأمن السيبراني البيولوجي تهم فئة واسعة من المهنيين العاملين داخل وحول المختبرات البيولوجية، ومختبرات التكنولوجيا الحيوية، والمختبرات البحثية والصيدلانية، على غرار مديري ومستشاري إدارة المخاطر البيولوجية، وضباط السلامة البيولوجية، وجميع العاملين في المختبرات من باحثين وتقنيين، والعاملين في مجال تكنولوجيا المعلومات والأمن السيبراني، وعمال الصيانة، وأفراد الأمن، والكوادر الإدارية.

لأغراض هذه الشهادة، يُعرَّف الأمن السيبراني البيولوجي بأنه "حماية المعلومات القيمة، والبيانات، وقواعد البيانات، والمعدات، والمرافق من سوء الاستخدام، والاستغلال، والأضرار، والاضطرابات التي قد تنشأ عند تقاطع المختبرات البيولوجية والمرافق المرتبطة بعلوم الحياة مع العوالم الرقمية.

يتكون الهيكل المعرفي (BOK) أدناه من خمس مجالات، تتضمن خمسة وأربعين نشاطًا معرفيًا، يعرف الكفاءات المطلوبة للحصول على شهادة مهنية في الأمن السيبراني البيولوجي. محتوى الاختبار مبني على هذا الهيكل المعرفي (BOK)، وكل سؤال في الاختبار مرتبط بأحد هذه المجالات.

المجال أ ـ مفاهيم الأمن السيبراني البيولوجي

1. وصف مجال الأمن السيبراني البيولوجي الناشئ عند تقاطع الأمن السيبراني، والأمن السيبراني المادي، وإدارة الجودة، والسلامة البيولوجية، والأمن البيولوجي.
2. وصف التهديدات والثغرات (نقاط الضعف) المرتبطة بالأمن السيبراني البيولوجي في العديد من القطاعات المتميزة في مجالات علوم الحياة، والعلوم الطبية الحيوية، والتكنولوجيا الحيوية، وعلم البيولوجيا التركيبية، والجوانب الأخرى من الاقتصاد الحيوي.
3. تحديد الطرق التي تُشكل بها ثغرات الأمن السيبراني البيولوجي في المختبرات البيولوجية مخاطر على سلامة المواد البيولوجية والبيانات الرقمية المرتبطة بها، وعلى عمال المختبرات والمجتمع المحيط والحيوانات والبيئة.
4. فهم كيف تزيد أجهزة ومعدات الشبكات من الثغرات ومن مخاطر الأمن السيبراني البيولوجي، وكذلك فهم كيفية التقليل من هذه المخاطر، مثل: فصل الأجهزة الأقل أمانًا عن الشبكة، وإزالة أجهزة إنترنت الأشياء غير الحيوية أو غير الآمنة.
5. معرفة كيفية تحديد وتقييم وتقليل المخاطر، وكيفية الاستجابة للتهديدات والمخاطر والحوادث المتعلقة بالأمن السيبراني البيولوجي، الناشئة عن الأصول المرتبطة بالمكونات الرقمية والمعدات المتصلة بالشبكة، والأجهزة، وأنظمة المرافق في المختبرات البيولوجية.
6. فهم أدوار ومسؤوليات موظفي الأمن السيبراني البيولوجي الرئيسيين مثل (مسؤولي السلامة البيولوجية، وعلماء المختبرات، وموظفي صيانة المرافق، وموظفي تكنولوجيا المعلومات، والإداريين، وأفراد الأمن) وأهمية التواصل المنتظم بينهم.
7. معرفة كيفية تطوير وتنفيذ برامج تدريبية على الأمن السيبراني البيولوجي وتعزيز الوعي به، وتشجيع الممارسات الشخصية الجيدة للأمن السيبراني في بيئة العمل داخل المختبر.
8. الإلمام وفهم كيفية تطوير/تحديث السياسات التنظيمية وإجراءات التشغيل القياسية بما يتماشى مع أفضل الممارسات المتعلقة بالأمن السيبراني البيولوجي.

المجال ب ـ أساسيات الأمن السيبراني

9. فهم الخيارات والامكانيات المتاحة للخصم لإجراء مراقبة مادية وسيبرانية لمنشأة لأهداف قد تكون خفية أو غير مباشرة أو غير متوقعة، وكيفية تقليل هذه المخاطر المحتملة.
10. فهم تكتيكات وتقنيات الاختراق التي يمكن أن يستخدمها الخصم للوصول إلى البيانات والأنظمة واستغلالها، مثل: الهندسة الاجتماعية، واستغلال يوم الصفر (zero-day)، واختراق سلسلة توريد البرمجيات، والشبكات، والتخزين السحابي، والمستخدمين، والبريد الإلكتروني، وتطبيقات الويب، وبوابات الوصول عن بعد، والأجهزة المحمولة.
11. تعريف المصطلحات :تكنولوجيا المعلومات (IT) والتكنولوجيا التشغيلية (OT) وإنترنت الأشياء.(IoT)

12. وصف الفئات الثلاث الشائعة للمصادقة متعددة العوامل (أي المعرفة والحيازة والسمات البيولوجية).
13. فهم مبادئ التحكم في الوصول مثل: الخصوصية وفقًا للتصميم، وحماية البيانات وفقًا للتصميم، وسياسة الاستخدام المقبول، وحسابات المستخدمين ذات الصلاحيات الأدنى، وتكوين حسابات المستخدمين وأذونات الأمان في بيئات متعددة، وإدارة الحقوق الرقمية.
14. فهم المبادئ الأساسية لإدارة تحديد الهوية وصلاحيات الوصول. على سبيل المثال: إدارة أذونات الأفراد والمجموعات، وتهيئة الوحدات التنظيمية والعناصر المرتبطة بها.
15. فهم مبادئ الحماية المادية، مثل وضع ضوابط التحكم في الوصول المادي، وحماية الوسائط، مثل تعقيم الوسائط أو إتلافها بشكل صحيح.
16. فهم مبادئ حماية النظام والاتصالات، مثل مراقبة أجهزة الحدود الخارجية والداخلية، وتنفيذ الشبكات الفرعية.
17. فهم مبادئ نزاهة النظام والمعلومات، على سبيل المثال: تحديد المشكلات التي قد تواجه النظام، تطبيق التواقيع الأمنية سواء على مستوى الشبكة أو الأجهزة المضيفة، وكذلك إجراء عمليات المسح الدورية للكشف عن الفيروسات ومكافحتها.

المجال ج - مخاطر تكنولوجيا المعلومات (IT) في المختبرات البيولوجية

18. وصف الأنواع المختلفة للبيانات المُخزنة والمُنقولة عبر منصات ومعدات تكنولوجيا المعلومات في المختبرات البيولوجية، والتي يمكن أن تشكل تدفق بيانات مهم للخصوم.
19. فهم كيف تؤثر ثغرات البيانات سلبًا على إدارة الجودة من خلال فقدان السرية (أي فقدان البيانات)، وفقدان التوفر (أي تعطيل التشغيل)، وفقدان النزاهة (أي التغيير غير المصرح به في البيانات).
20. وصف كيفية حدوث تسريب للبيانات من قِبَل أطراف داخلية وخارجية، وبيان كيفية استخدام تقنيات تشفير قواعد البيانات لتأمين المعلومات في قواعد البيانات البيولوجية.
21. وصف الطرق التي يمكن من خلالها استغلال المعدات المخبرية المتصلة بالشبكة عن بُعد/رقميًا للإخلال بنزاهة البحث، وتغيير التسلسلات الجينومية، والتلاعب بخصائص العوامل البيولوجية، وإنتاج منتجات بيولوجية ضارة.

22. وصف كيفية استخدام المناطق المنزوعة السلاح (DMZ)، ومناطق الثقة (Trust Zones) لتعزيز أمن المعدات المخبرية المتصلة بالشبكة والبنية التحتية.
23. وصف كيفية استغلال خوارزميات التشفير في استخدامات كلمات المرور، والمصادقة متعددة العوامل، والشبكة الخاصة الافتراضية، وتشفير البيانات سواء المخزنة أو المنقولة، وكيف يمكن دمج ذلك في سياسة الأمن السيبراني البيولوجي للمختبر.
24. فهم أهمية إجراء التقييمات الدورية للثغرات الأمنية، واختبارات الاختراق المحددة النطاق للشبكات والتطبيقات، والتي يمكن من خلالها تحديد الثغرات وتخفيف حدتها.
25. معرفة كيفية تقليل الثغرات الأمنية السيبرانية البيولوجية التي تظهر عند استخدام الأجهزة الشخصية للوصول إلى الأنظمة ذات الصلة بالمختبرات، مثل: الحواسيب والهواتف الشخصية المحمولة.
26. فهم الثغرات ونقاط الضعف المرتبطة باستخدام تقنيات ومعدات الطيف اللاسلكي المتصلة بالإنترنت، وكيف يمكن للأجهزة اللاسلكية أن تزيد من سطح الهجوم، وتوفر متجهات هجوم جديدة للخصوم.
27. وصف نوعية الثغرات ونقاط الضعف والمعلومات الحساسة التي يمكن الكشف عنها للخصوم من خلال وثائق التحكم الإداري، مثل: إجراءات الاستجابة للطوارئ، وخطط برامج الأمن/السلامة، ووثائق الميزانية والتخطيط، ووثائق العقود، ومخططات الطوابق، والرسومات التخطيطية للمختبرات، وغرف الدعم، والمساحات الميكانيكية.
28. وصف طرق تقييد الكشف عن المعلومات الحساسة، وثغرات المرافق لمقاولي صيانة المرافق الخارجيين، ومقدمي خدمات المعدات، والموردين.
29. فهم الثغرات ونقاط الضعف الأمنية السيبرانية المرتبطة بأنظمة جرد مسببات الأمراض المتصلة بالشبكة، وأنظمة إدارة معلومات المختبرات.
30. معرفة كيفية تحديد وتخفيف الثغرات في الأنشطة المتعلقة بالمختبر، والتي يقوم بها العاملون، والتي قد تؤدي إلى تسرب المعلومات الحساسة، مثل: المشاركة الشرعية للبيانات لأغراض البحث أو التدريس، أو لأغراض تجارية.

المجال د ـ مخاطر تكنولوجيا التشغيل (OT) في المختبرات البيولوجية

31. فهم كيف أن الابتكار التكنولوجي في "المختبرات الذكية" عرضة للثغرات الأمنية السيبرانية. (المختبرات الذكية هي المختبرات المزودة بأجهزة متصلة بالشبكة قادرة على المراقبة والتحكم عن بُعد، بالإضافة إلى المفاتيح الذكية).
32. فهم الثغرات الأمنية السيبرانية المرتبطة باستخدام دفتر الملاحظات الإلكتروني، والمساعد الصوتي الشخصي الافتراضي الذي يعمل بالأوامر الصوتية في المختبرات.
33. فهم كيفية تعرض أنظمة أتمتة المباني المتصلة بالشبكة، وبرمجيات إدارة الطاقة، لثغرات الأمن السيبراني.
34. وصف الطرق التي يمكن من خلالها استغلال نظام التحكم في الوصول المادي للمختبر عن بُعد/ رقميًا للإخلال بالأمن.
35. وصف الطرق التي يمكن من خلالها استغلال نظام أتمتة المباني في مختبر الاحتواء البيولوجي عن بُعد/رقميًا لتعريض السلامة البيولوجية، والاحتواء، وسلامة الحياة، وسلامة المواد البيولوجية، والبيانات للخطر.
36. وصف الطرق التي يمكن من خلالها استغلال أنظمة ومعدات إزالة التلوث في المختبر البيولوجي عن بُعد/رقميًا، لتعريض السلامة البيولوجية والاحتواء البيولوجي للخطر.
37. وصف الطرق التي يمكن من خلالها استغلال غرف إيواء الحيوانات وأنظمة الأقفاص الخاصة بالاحتواء عن بُعد/رقميًا، والتأثيرات المحتملة لمثل هذا الاختراق.
38. فهم مخاطر الأمن السيبراني المحتملة التي قد تُعرض سلسلة التوريد الخاصة بالمختبر للخطر، وفهم كيفية تقليل هذه المخاطر وعكس تأثيرها في حال اكتشافها.

المجال ي - الاستعداد والاستجابة لحوادث الأمن السيبراني البيولوجي

39. معرفة كيفية إجراء جولة شاملة في المنشأة بهدف تطوير خطة لتخفيف تهديدات الأمن السيبراني البيولوجي والاستجابة للحوادث.
40. وصف كيفية تطوير خطة شاملة للتخفيف من تهديدات الأمن السيبراني البيولوجي، والاستجابة للحوادث، وخطة التواصل من أجل تقليل الأضرار، واحتواء التهديدات، والحفاظ على السلامة البيولوجية والأمن البيولوجي.
41. فهم الأدوار والمسؤوليات لأفراد الفريق الرئيسيين في الاستجابة لحوادث الأمن السيبراني البيولوجي، سواء داخل المؤسسة أو من المتخصصين الخارجيين.
42. المعرفة المسبقة بمكان الحصول على مساعدة إضافية خارجية موثوقة ومختبرة لتحديد حوادث الأمن السيبراني البيولوجي، والاستجابة لها، والتعافي منها.

43. معرفة متى وكيفية إشراك سلطات تنفيذ القانون التي قد تكون مطلوبة للاستجابة، والتحقيق، وجمع الأدلة الإثباتية، وإجراء المقابلات.
44. معرفة قنوات الاتصال والطريقة والجهة التي يتم الإبلاغ إليها عن حوادث الأمن السيبراني البيولوجي المحتملة والمكتشفة.
45. معرفة كيفية إجراء تمارين منتظمة لفريق الاستجابة لحوادث الأمن السيبراني البيولوجي، بما في ذلك تمارين الطاولة (tabletop).

مخطط الاختبار:

الجدول التالي يوضح عدد الأسئلة المتضمنة في الاختبار من كل مجال:

مخطط الاختبار **شهادة مهنية في الأمن السيبراني البيولوجي** **النسبة المئوية للنجاح هي 70%**	
المجال	**عدد الأسئلة**
المجال أ - مفاهيم الأمن السيبراني البيولوجي	19
المجال ب - أساسيات الأمن السيبراني	18
المجال ج - مخاطر تكنولوجيا المعلومات (IT) في المختبرات البيولوجية	28
المجال د - مخاطر تكنولوجيا التشغيل (OT) في المختبرات البيولوجية	12
المجال ي - الاستعداد والاستجابة لحوادث الأمن السيبراني البيولوجي	13

عينة من الأسئلة:

لجعل طبيعة وشكل أسئلة الاختبار مألوفة لدى المترشحين، فيما يلي بعض الأمثلة للأسئلة. تُشير علامة النجمة (*) إلى الإجابة الصحيحة.

1. ما هو السيناريو الذي يمثل بشكل أفضل أشد المخاوف المتعلقة بالأمن السيبراني البيولوجي في بيئة المختبرات البيولوجية الحالية؟
   أ. دخول أفراد غير مصرح لهم إلى المختبر بسبب ضعف تأمينه وسرقتهم لمسببات الأمراض من مجمدات المختبر.
   ب. إمكانية اختراق معدات المختبر وأجهزة إنترنت الأشياء (IoT) المتصلة بالإنترنت والوصول إلى بيانات المختبر السرية وتعديلها. *
   ج. إمكانية بيع معلومات وبيانات علمية مسجلة في ملكية المختبر من طرف باحثي المختبر إلى مؤسسة بحثية منافسة.
   د. يمكن أن تُعالج مواد النفايات بطريقة غير ملائمة قبل خروجها من المختبر للتخلص منها خارج الموقع.

2. أكمل العبارة التالية: استخدام _____ للتحقق من هوية مستخدم الشبكة هو مثال على المصادقة المتعددة العوامل لتقليل احتمالية الهجوم السيبراني.
   أ. اسم المستخدم وكلمة المرور.
   ب. سؤال الأمان ورمز PIN .
   ج. رمز مكون من 4 أرقام يُرسل مرة واحدة عبر الرسائل النصية القصيرة SMS *
   د. مسح البصمة والتعرف على الوجه.

3. يقوم قسم تكنولوجيا المعلومات بتطوير سياسة وإجراءات بشأن الموظفين الذين يجلبون أجهزتهم الشخصية (BYOD) إلى المختبر. ما هو الخيار الصحيح؟
   أ. سياسة "أحضر جهازك الخاص (BYOD)" في المختبر مقبولة، ولا تتطلب إجراءات خاصة إذا لم تُستخدم الأجهزة للوصول إلى معلومات وبيانات المختبر الحساسة.

ب. يجب حظر سياسة "أحضر جهازك الخاص (BYOD)" بالنظر إلى التحديات الأمنية السيبرانية الخاصة والمستوى العالي من المخاطر في جميع بيئات المختبرات التي تتعامل مع العوامل البيولوجية.

ج. الإجراءات الأمنية السيبرانية المطبقة حاليًا لتأمين الأجهزة وبيانات المختبر عادةً ما تكون كافية لتوفير حماية فعالة لنظام "أحضر جهازك الخاص (BYOD)" أيضًا.

د. يجب تطبيق سياسات وإجراءات محددة تتناول المخاطر الفريدة لتكنولوجيا المعلومات المرتبطة بنظام "أحضر جهازك الخاص (BYOD)" ، بما في ذلك المخاطر التي تهدد المؤسسة وخصوصية الموظفين.*

4. قد يتم تصميم البنية التحتية لمختبرات الاحتواء البيولوجي باستخدام معدات وأنظمة معرضة لهجمات سيبرانية.

أكمل العبارة التالية: بالنظر إلى الأمن السيبراني وأنظمة الاحتواء في المباني، يجب على مديري المرافق:

أ. التواصل بانتظام مع قسم تكنولوجيا المعلومات والموردين لتطبيق حلول الأمن السيبراني على البنية التحتية القائمة وعقود الخدمة والصيانة والتركيبات الجديدة. *

ب. الاعتماد على قسم تكنولوجيا المعلومات، الذي يمتلك الخبرة والمسؤولية لتطوير وتبني سياسات وإجراءات الأمن السيبراني لبنية المختبر وأنظمة المبنى.

ج. الاعتماد على الموردين المسؤولين عن ضمان أمان أنظمة المبنى، والمعدات، والموظفين المختصين بالخدمة، والتزامهم بأفضل ممارسات الأمن السيبراني.

د. التعاون مع مديري المختبرات لإجراء فحص دوري لثغرات الأمن السيبراني واختبارات اختراق لأنظمة الاحتواء في المبنى، على الأقل مرة واحدة شهريًا.

5. أكمل العبارة التالية:

عند تطوير خطة استجابة لحادث أمن سيبراني لمختبر بيولوجي، يجب على المؤسسة

أ. اعداد وتطوير تعليمات "خطوة بخطوة" لجميع الموظفين للتعامل مع كل حادث محتمل قد يؤثر سلباً على المؤسسة .

ب. التركيز على الاستعداد بشكل عام في جميع أنحاء المؤسسة وبشكل أكبر على كيفية التعامل مع الحوادث التي تستخدم متجهات الهجوم الشائعة. *

ج. التقييد الصارم لمشاركة المعلومات حول جميع جوانب الخطة داخل المؤسسة، لتقليل احتمالية الهجمات السيبرانية من التهديدات الداخلية.

د. وضع إجراءات مكتوبة للتعامل مع الحوادث المتعددة على أساس الأسبقية "من يأتي أولا يُخدم أولا "لتوفير الوقت للمسؤولين عن التعامل مع الحوادث.

المراجع:

إلى جانب الإلمام بالمصطلحات والمبادئ الأساسية للأمن السيبراني، فيما يلي قائمة ببعض المصادر الموصى بها للاستعداد للامتحان، على سبيل المثال لا الحصر:

Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience, Daniel S. Schabacker et al, Frontiers in Bioengineering and Biotechnology, 29 March 2019.

Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape, Lauren C. Richardson et al, Frontiers in Bioengineering and Biotechnology, 06 June 2019.

Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy, Randall S. Murch et al, Frontiers in Bioengineering and Biotechnology, 05 April 2018.

Cyberbiosecurity Implications for the Laboratory of the Future, J. Craig Reed & Nicolas Dunaway, Frontiers in Bioengineering and Biotechnology, 21 August 2019.

Cyberbiosecurity: From Naïve Trust to Risk Awareness, Jean Peccoud et al, Trends in Biotechnology, January, 2018.

Cybersecurity Incident Response Exercise Guidance, Larry G. Wlosinski et al, ISACA Journal, Vol 1, January 2022.

Information technology - Security techniques - Guidelines for Cybersecurity, International Standards Organization. ISO/IEC 27032:2012.

Facing the 202 Pandemic: What does Cyberbiosecurity Want us to Know to Safeguard the future? Siguna Meuller, Biosafety & Health, February, 2021.

Computer Security Incident Handling Guide, US National Institute of Standards & Technology NIST, 2012.

Cyberthreats to Biotechnology, US Dept. Health & Human Services, 2021.

Guidelines for Media Sanitation, US National Institute of Standards & Technology, 2014.

Framework for Improving Critical Infrastructure Cybersecurity, US National Institute of Standards & Technology, 2018.

Mobile Device Best Practices, US National Security Agency, 2020.

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, US National Institute of Standards & Technology, 2019.