Developing Job-Ready Cybersecurity Capabilities using NICE Framework

2025

تطويرقدرات الأمن السيبراني الجاهزة للوظيفة باستخدام إطار عمل NICE

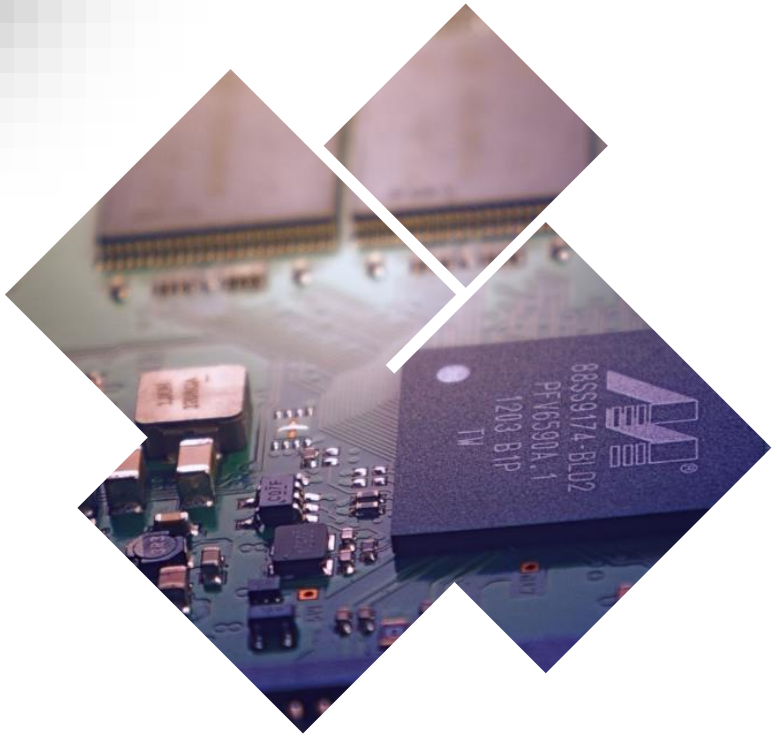
د. عبدالرحمن مثنى
خبير الأمن السيبراني
Certified Ethical Hacker C|EH
OIC-CERT Professional member

اليمن - صنعاء

16 صفر 1446هـ

10-08-2025

المواضيع



1. مشهد التهديدات السيبرانية
2. التحديات والفرص في الأمن السيبراني
3. نظرة عامة على إطار عمل NICE
4. إستخدام NICE في التوظيف

مشهد التهديدات السيبرانية

التحديات والفرص في مجال الأمن السيبراني

التحديات

- نقص عدد المتخصصين بالأمن السيبراني
- غياب تنوع الكفاءات في الأمن السيبراني
- ضعف المسارات المهنية
- هجرة الكفاءات وصعوبة الإحتفاظ بهم

الفرص

- الطلب العالمي الكبير على مهارات الأمن السيبراني
- إمكانية دعم التحول الرقمي المحلي من خلال الكفاءات الوطنية
- تعزيز الاقتصاد الوطني من خلال فرص العمل في المجال السيبراني

نظرة عامة على إطار عمل NICE

د. عبدالرحمن مثنى

إطار عمل NICE

إطار عمل القوى العاملة في الأمن السيبراني (NICE) تم تطويره بواسطة المعهد الوطني للمقاييس والتكنولوجيا الأمريكي NIST. يحدد:

- 5 مجالات عمل
- 41 دوراً وظيفياً
- 11 كفاءة أساسية
- المهام والمعارف والمهارات المطلوبة (TKS) للأدوار الوظيفية

مكونات إطار العمل NICE

- 942 المهام
- 631 قواعد المعرفة
- 538 المهارات
- 11 الكفاءات
- 41 الوظائف
- 5 فئات الوظائف

مكونات إطار العمل NICE

المعرفة مجموعة من المفاهيم التي يُمكن استرجاعها من الذاكرة. تُحدّد بيانات المعرفة ما يعرفه المتعلم

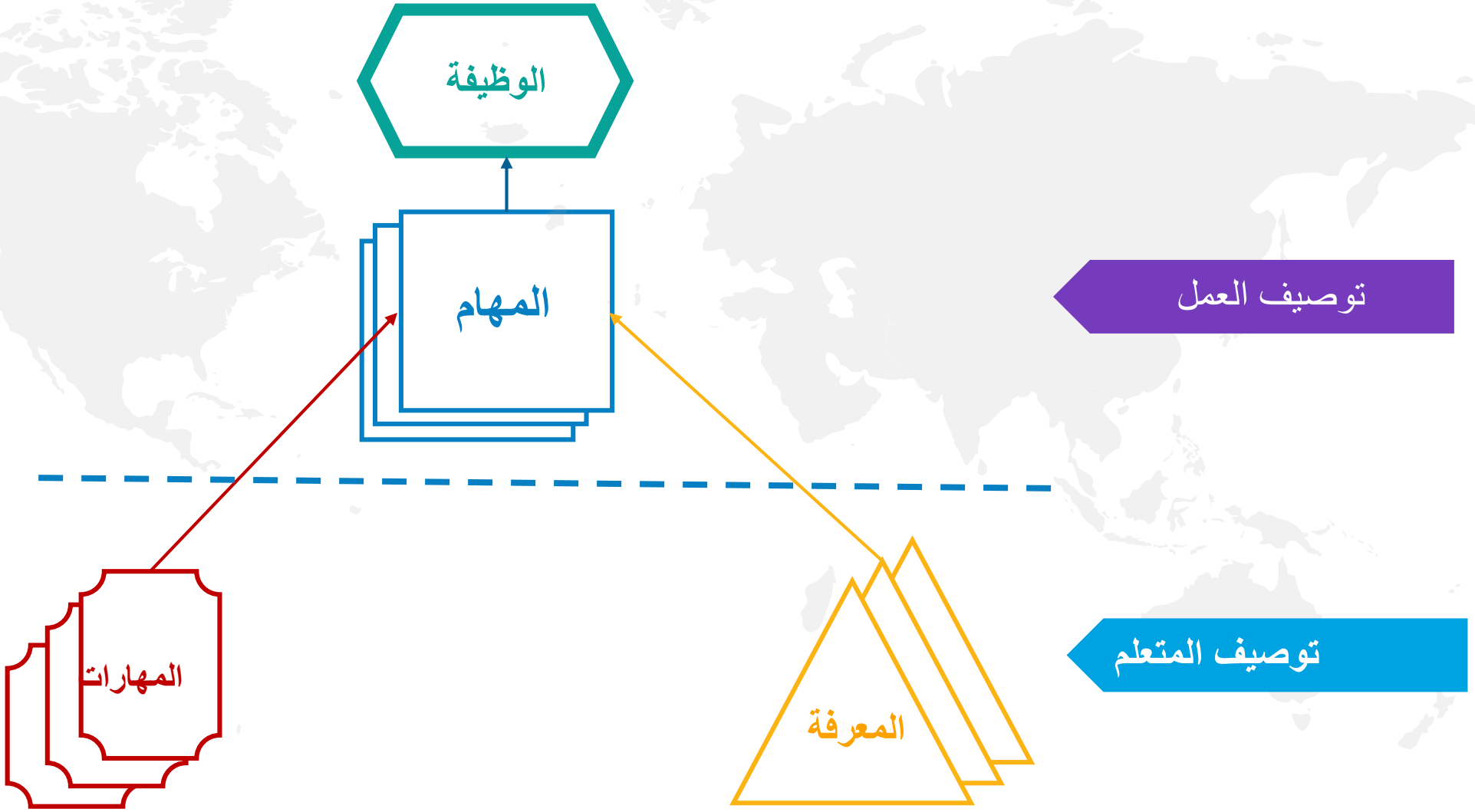
المهارة القدرة على أداء فعل مُلاحظ. تُحدّد بيانات المهارة ما يُمكن للمتعلم القيام به.

المهمة العمل المطلوب إنجازه، وتتضمن بيانات المعرفة والمهارات المرتبطة بها والتي تُمثّل قدرة المتعلم على أداء المهمة

الكفاءة مجموعة من بيانات المعرفة والمهارات ذات الصلة التي ترتبط بقدرة الفرد على أداء المهام في مجال مُعيّن

الوظيفة مجموعة من الأعمال التي يكون فرد أو فريق مسؤولاً عنها أو مُحاسباً عليها. وهي تتألف من مجموعة من المهام التي تُحدد العمل المطلوب إنجازه.

المهام والمعارف والمهارات



فئات الوظائف في الأمن السيبراني

- الإشراف والحوكمة
- التصميم والتطوير
- التنفيذ والتشغيل
- الحماية والدفاع
- التحريات

الوظائف/أدوار العمل في إطار NICE

الإشراف والحوكمة	التصميم والتطوير	التنفيذ والتشغيل	الحمايه والدفاع	التحريات
أمن إدارة الإتصالات	هندسة الأمن السيبراني	تحليل البيانات	الأمن السيبراني الدفاعي	التحقيق في الجرائم السيبرانية
سياسة وتخطيط الأمن السيبراني	هندسة المؤسسات	إدارة قواعد البيانات	التحليل الجنائي الرقمي	تحليل الأدلة الرقمية
إدارة القوى العاملة في مجال الأمن السيبراني	تطوير البرمجيات الآمنة	إدارة المعرفة	الاستجابة للحوادث	
تطوير مناهج الأمن السيبراني	تطوير الأنظمة الآمنة	عمليات الشبكة	دعم البنية التحتية	
تعليم الأمن السيبراني	تقييم أمن البرمجيات	إدارة الأنظمة	تحليل التهديدات	
الاستشارات القانونية السيبرانية	تخطيط متطلبات الأنظمة	تحليل أمن الأنظمة	تحليل التهديدات الداخلية	
قيادة الأمن السيبراني التنفيذية	البحث والتطوير التكنولوجي	الدعم الفني	تحليل الثغرات الأمنية	
الامتثال للخصوصية	اختبار وتقييم الأنظمة			
إدارة دعم المنتجات	التكنولوجيا التشغيلية للأمن السيبراني			
إدارة البرامج				
إدارة المشاريع الآمنة				
تقييم الرقابة الأمنية				
تفويض الأنظمة				
إدارة أمن الأنظمة				
إدارة توثيق التكنولوجيا				
تدقيق برامج التكنولوجيا				

أمثلة لبعض الأدوار الوظيفية في إطار عمل NICE

التحليل الجنائي الرقمي

الفئة :الحماية والدفاع

المسؤول عن تحليل الأدلة الرقمية من حوادث أمن الكمبيوتر لاستخلاص معلومات مفيدة لدعم التخفيف من ثغرات النظام والشبكة.

- المهام (46)
- المعارف (94)
- المهارات (46)

سياسة وتخطيط الأمن السيبراني

الفئة :الإشراف والحوكمة

المسؤول عن تطوير وصيانة خطط الأمن السيبراني والاستراتيجيات والسياسات لدعم ومواءمة مبادرات الأمن السيبراني التنظيمية والامتثال التنظيمي.

- المهام (25)
- المعارف (34)
- المهارات (9)

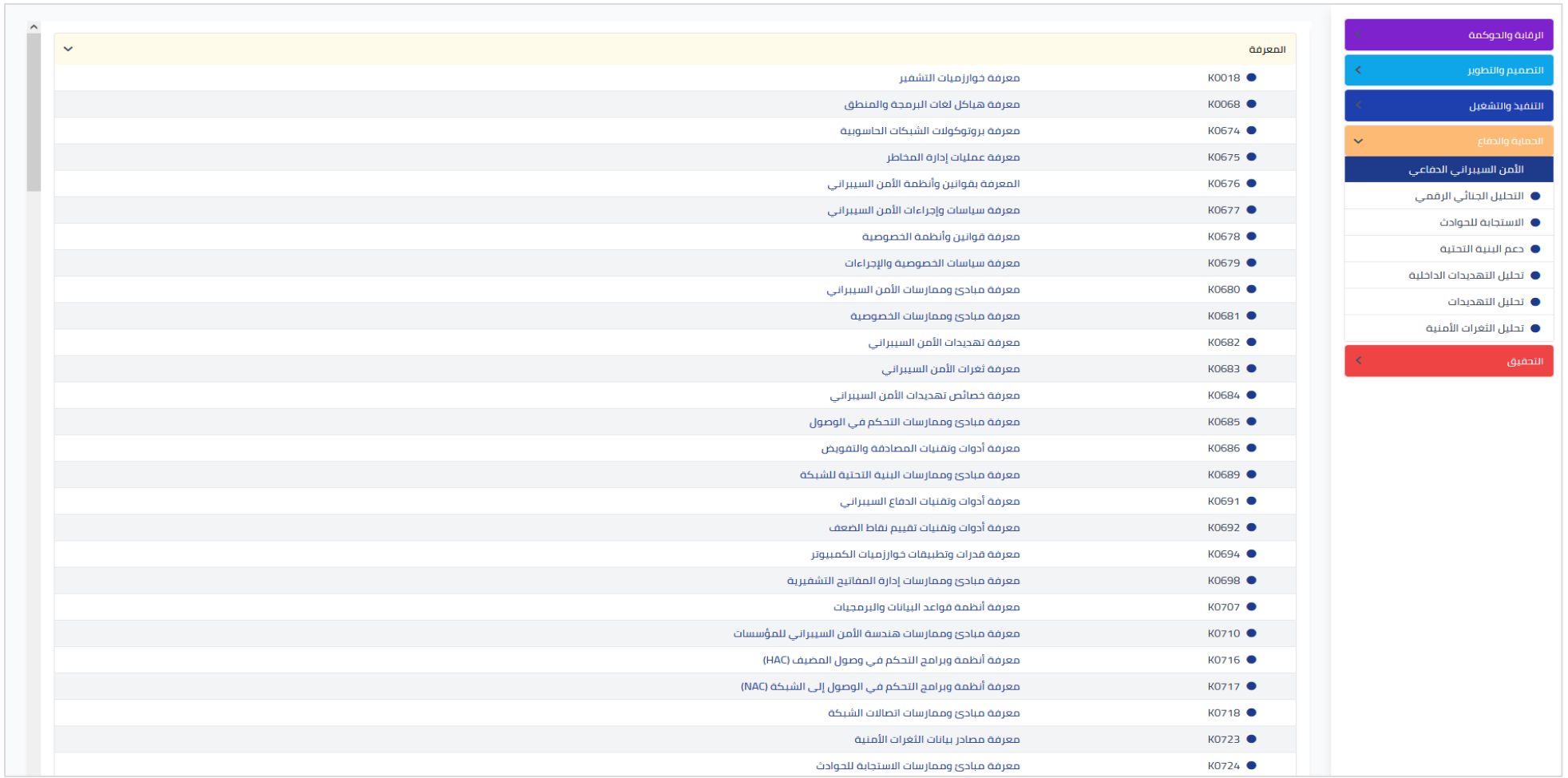
محلل الدفاع السيبراني

الفئة :الحماية والدفاع

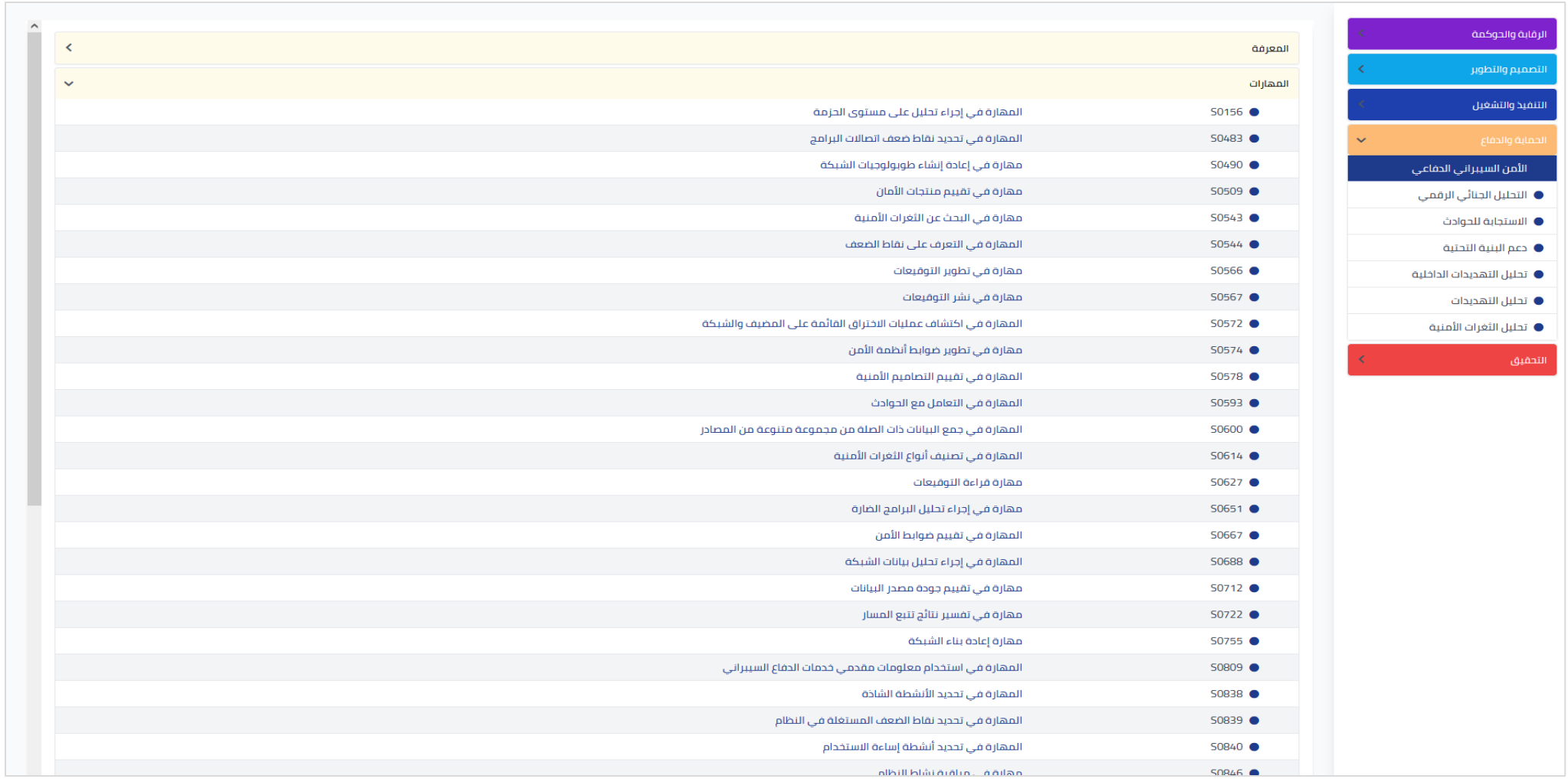
المسؤول عن تحليل البيانات التي تم جمعها من أدوات الحماية المختلفة للتخفيف من المخاطر.

- المهام (43)
- المعارف (125)
- المهارات (39)

البيانات المعرفية المطلوبة لوظيفة "محلل الدفاع السيبراني" (125)



المهارات المطلوبة لوظيفة "محلل الدفاع السيبراني" (39)



المعرفة

المهارات

S0156	المهارة في إجراء تحليل على مستوى الحزمة
S0483	المهارة في تحديد نقاط ضعف اتصالات البرامج
S0490	مهارة في إعادة إنشاء طوبولوجيات الشبكة
S0509	مهارة في تقييم منتجات الأمان
S0543	مهارة في البحث عن الثغرات الأمنية
S0544	المهارة في التعرف على نقاط الضعف
S0566	مهارة في تطوير التوقيعات
S0567	مهارة في نشر التوقيعات
S0572	المهارة في اكتشاف عمليات الاختراق القائمة على المضيف والشبكة
S0574	مهارة في تطوير ضوابط أنظمة الأمن
S0578	المهارة في تقييم التصاميم الأمنية
S0593	المهارة في التعامل مع الحوادث
S0600	المهارة في جمع البيانات ذات الصلة من مجموعة متنوعة من المصادر
S0614	المهارة في تصنيف أنواع الثغرات الأمنية
S0627	مهارة قراءة التوقيعات
S0651	مهارة في إجراء تحليل البرامج الضارة
S0667	المهارة في تقييم ضوابط الأمن
S0688	المهارة في إجراء تحليل بيانات الشبكة
S0712	مهارة في تقييم جودة مصدر البيانات
S0722	مهارة في تفسير نتائج تتبع المسار
S0755	مهارة إعادة بناء الشبكة
S0809	المهارة في استخدام معلومات مقدمي خدمات الدفاع السيبراني
S0838	المهارة في تحديد الأنشطة الشاذة
S0839	المهارة في تحديد نقاط الضعف المستغلة في النظام
S0840	المهارة في تحديد أنشطة إساءة الاستخدام
S0846	مهارة في ... مراقبة نشاط النظام

الرقابة والحوكمة

التصميم والتطوير

التنفيذ والتشغيل

الحماية والدفاع

الأمن السيبراني الدفاعي

- التحليل الجنائي الرقمي
- الاستجابة للحوادث
- دعم البنية التحتية
- تحليل التهديدات الداخلية
- تحليل التهديدات
- تحليل الثغرات الأمنية

التحقيق

المهام المطلوبة لوظيفة "محلل الدفاع السيبراني" (43)

المعرفة	
المهارات	
المهام والقدرات	
T0020	تطوير محتوى لأدوات الدفاع السيبراني
T0164	إجراء تحليل اتجاهات الدفاع السيبراني وإعداد التقارير عنها
T0292	يوصي بتصحيحات ثغرات بيئة الحوسبة
T0299	تحديد أنشطة تعيين الشبكة وبصمة نظام التشغيل (OS)
T1020	تحديد التأثيرات التشغيلية والسلامة الناجمة عن ثغرات الأمن السيبراني
T1021	مراجعة هيكل إعداد التقارير لمقدمي خدمات الدفاع السيبراني
T1084	تحديد نشاط الشبكة الشاذ
T1085	تحديد التهديدات المحتملة لموارد الشبكة
T1112	التحقق من صحة تنبيهات الشبكة
T1119	أوصي باستراتيجيات معالجة الثغرات الأمنية
T1176	تحديد ما إذا كانت المنتجات التي تدعم الأمن السيبراني تقلل المخاطر المحددة إلى مستويات مقبولة
T1177	تحديد ما إذا كانت تقنيات التحكم الأمني تقلل من المخاطر المحددة إلى مستويات مقبولة
T1241	وثّق حوادث الأمن السيبراني
T1242	تصعيد الحوادث التي قد تسبب تأثيرًا مستمرًا وفوريًا على البيئة
T1254	تحديد فعالية الهجوم الذي تم رصده
T1266	أوصي باستراتيجيات التخفيف من المخاطر
T1278	يوصي بتعديلات النظام
T1290	إبلاغ تقارير الأحداث والأنشطة اليومية للشبكة
T1299	تحديد أسباب تنبيهات الشبكة
T1347	اكتشف هجمات واختراقات الأمن السيبراني
T1348	التمييز بين هجمات واختراقات الأمن السيبراني الحميدة والضارة المحتملة
T1349	إبلاغ تنبيهات هجمات الأمن السيبراني والاختراقات
T1350	إجراء مراقبة مستمرة لنشاط النظام
T1351	تحديد تأثير النشاط الضار على الأنظمة والمعلومات

الرقابة والحوكمة
التصميم والتطوير
التنفيذ والتشغيل
الحماية والدفاع
الأمن السيبراني الدفاعي
التحليل الجنائي الرقمي
الاستجابة للحوادث
دعم البنية التحتية
تحليل التهديدات الداخلية
تحليل التهديدات
تحليل الثغرات الأمنية
التحقيق

فوائد وآثار تطبيق إطارNICE على المستوى الوطني

موائمة التعليم والتدريب والتوصيف الوظيفي مع معايير عالمية

قبول عالمي ومصداقية عالية للمخرجات

04

مسارات تعلم واضحة

تخطيط جيد للقدرات والكفاءات

03

لغة موحدة بين جميع الأطراف المعنية

التنسيق بين القطاعات

02

تنظيم الوظائف في القطاعين العام والخاص

01

تحديد واضح للأدوار الوظيفية

د. عبدالرحمن مثنى

إعتماد إطار عمل NICE عالمياً

- الولايات المتحدة: اعتماد NICE للوظائف الفيدرالية في الأمن السيبراني
- الإتحاد الأوروبي: اعتماد NICE لبناء القدرات في الأمن السيبراني لدول الإتحاد
- دول أخرى مثل كندا وكوريا الجنوبية وأستراليا وغيرها

من يمكنه الإستفادة من إطار عمل NICE

مقدمو خدمات التعليم والتدريب والإعتماد

03

تطوير دورات وبرامج تعليمية متوائمة مع إطار عمل NICE

إجراء تقييمات قائمة على الأداء

المتعلمون, الطلاب, الباحثون عن عمل, والموظفون

02

التعرّف على مختلف أدوار العمل

تطوير المعرفة والمهارات في تخصص محدد

تطبيق ما تعلموه وإثبات قدراتهم

أصحاب العمل

01

تتبع قدرات القوى العاملة

إنشاء توصيفات الوظائف

تطوير الموظفين

توفير مسارات مهنية

إستخدام NICE في التوظيف

التحديات الشائعة للقوى العاملة في الأمن السيبراني

- إحتياجات القوى العاملة غير واضحة
- العمل دون توصيف واضح ومفصل للوظائف في مجال الأمن السيبراني
- البحث عن موظفين بأهداف غير واقعية

هل لدينا الأشخاص
المناسبين في فريق الأمن
السيبراني الخاص بنا؟

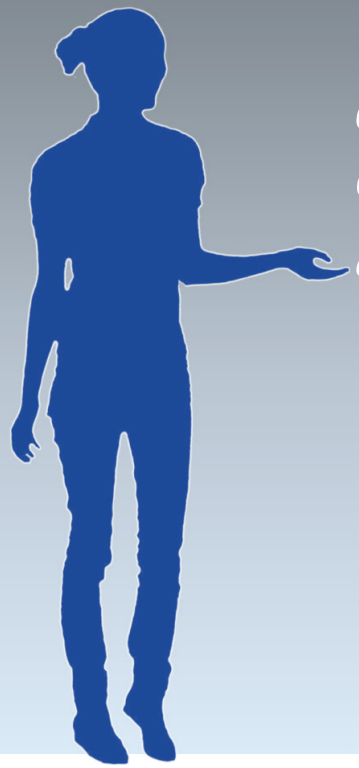
الحل: إجراء تقييم للفريق باستخدام إطار عمل NICE

1. حدّد أدوار العمل المطلوبة
2. قيّم موظفي الأمن السيبراني الحاليين في مجالات الكفاءة المطلوبة
3. حدّد الفجوات وقم توفير التدريب اللازم

كيف يمكننا التأكد من توظيف المتقدم المناسب؟

الحل: إستخدم إطار عمل NICE للقيام بالمهام التالية:

1. تحديد الكفاءات والأدوارالوظيفية التي سيتولى الموظف الجديد مسؤوليتها
2. توصيف الوظائف
3. تقييم المرشحين من حيث المعرفة والمهارات اللازمة



أرغب في الانتقال إلى دور جديد في مجال الأمن السيبراني في مؤسستي، ولكنني أريد التأكد من إستعدادي.

الحل: طوّر مهاراتك وأعد تطويرها مع إطارعمل NICE

1. إستخدام أدوار العمل ذات الصلة في تحديد المسار الوظيفي
2. تحديد إحتياجات المؤسسة بشكل واضح
3. تحديد مواطن القوة والضعف، ثم التركيز على المجالات التي تحتاج إلى تحسين

شكراً