

مقدمة في الأمان السيبراني



مدخل إلى الأمان السيبراني
والشبكات وأنظمة التشغيل

مقدمة في الأمان السيبراني

مدخل إلى الأمان السيبراني و الشبكات و أنظمة التشغيل

هذه المادة هي نتاج عدة أشهر من البحث كان الدافع وراءها الحيرة التي واجهتها حينما قررت الدخول في مجال الأمان السيبراني حيث لم أجد مرجعاً واضحاً يتطرق الى هذا الموضوع بشمولية كاملة.

إذا كنت تريده تطوير الكتب أو لديك ملاحظات او اسئلة فراسلني على :



الفهرس

3	المقدمة
5	نظرة عامة عن الأمن السيبراني
5.....	الأمن السيبراني تقنياً.....
6	أقسام مجال الأمن السيبراني الرئيسية
6	كيف أبدأ في مجال الأمن السيبراني
7	المرحلة الأولى
7.....	برمجة
8	أنظمة تشغيل
8.....	مصادر عربية لتعلم نظام التشغيل GNU/Linux
8.....	الشبكات
10.....	المرحلة الثانية
11.....	المرحلة الثالثة
12.....	ادارة Administration
12.....	نبذة عن التخصص
13.....	من أقسام التخصص
13.....	من المسميات الوظيفية التابعة للتخصص
13.....	أدوات وخرائط (MAPs & Tools)
15.....	شهادات و دورات
17.....	Digital Forensic / Incident Response (DFIR) التحليل الجنائي الرقمي و الإستجابة للحوادث
17.....	نبذة تعريفية عن التحليل الجنائي الرقمي
18.....	نبذة تعريفية عن الاستجابة للحوادث
18.....	أقسام التخصص + بعض التفاصيل
20.....	أدوات ، معامل ، الالات (Machines , Labs , Tools)
21.....	شهادات و دورات
22.....	Applications Security (AppSec) أمن التطبيقات
22.....	نبذة تعريفية عن التخصص
23.....	أقسام التخصص
23.....	ادوات ، معامل ، (Lab , Tools)
23.....	شهادات و دورات
24.....	Penetration testing (pen Testing) اختبار الإختراق
24.....	نبذة تعريفية عن التخصص
25.....	أقسام التخصص
25.....	أدوات ، معامل ، الالات (Tools , Labs , Machines)
26.....	شهادات و دورات
27.....	Malware Analysis / Reverse Engineering (RE) تحليل البرامج الخبيثة والهندسة العكسية

27.....	نبذة تعريفية عن البرمجيات الخبيثة
27.....	نبذة تعريفية عن الهندسة العكسية
28.....	نبذة تعريفية عن التخصص (الهندسة العكسية وتحليل البرامج الخبيثة)
29.....	كيف تتم هندسة البرمجيات الخبيثة عكسيا ؟
30.....	مواضيع وتقنيات ستساعدك في احتراف المجال
30.....	أدوات ، معامل ، الالات (Machines , Labs , Tools)
31.....	شهادات و دورات
32.....	بعض المقالات المقيدة في مجال الأمن السيبراني
32.....	بعض المواقع والأدوات المقيدة في مجال الأمن السيبراني
33.....	السميات الوظيفية في مجال أمن المعلومات والأمن السيبراني (وفق إطار سيف)
41.....	أسماء بعض الشهادات والدورات والشركات التي تقدمها
42.....	Beginner / Foundational مبتدئ / تأسيسي
42.....	INTERMEDIATE متوسط
43.....	ADVANCED متقدم
44.....	EXPERT خبير
44.....	بعض مسارات عدد من الشركات المتخصصة في الأمن السيبراني ونظم التشغيل والشبكات
44.....	CompTIA
45.....	Microsoft
46.....	CISCO
47.....	eLearnSecurity & ine
48.....	OFFENSIVE security
49.....	EC-COUNCIL
50.....	SANS & GIAC
51.....	Red Hat
52.....	mile2
53.....	(ISC)^2
54.....	ISACA
55.....	AWS
56.....	الخاتمة

المقدمة

بسم الله الرحمن الرحيم

هذه المادة موجة للمتخصصين في المجال التقني أو من يريد دخول مجال الأمن السيبراني من الناحية التقنية لا الإدارية أو الأكاديمية أو غيرها، إنما هو لمن يريد أن يتخصص في الناحية الفنية التطبيقية في مجال الأمن السيبراني حيث أنه يحتوي على دراسة الأمور الفنية و إرشادات لكيفية البدء في بعض التخصصات في الأمن السيبراني وكيفية الوصول إلى مدخل الشخص بمقدمة يسيرة مناسبة للمبتدئين .. أما التخصصات الإدارية مثل الحكومة و إدارة المخاطر و ما إلى ذلك.. فهذه التخصصات لم يتم التطرق لها بشكل مباشر و إنما تم ذكر بعض الأمور عنها.

تنويه : مجل محتويات هذه المادة هو مما جمع أو ترجم من مقالات موجودة .. و هو نتاج بحث و ليس من تأليفه، و ما كتبته بنفسه قليل إذا ما تم مقارنته بالمنقول و المترجم .. و هذه المادة هي خلاصة تساؤلات و بحوث و إستشارات امتدت إلى ما يقارب **عدة أشهر**.

تنويه : ستحتاج منك قراءة هذه المادة و الإطلاع على محتوياتها من (مقالات و مقاطع فيديو و صور) إلى عدة أيام .. لكن اقترح أن تأخذ تصور عام عن الماده ثم تبدأ فيها من البداية و تأخذ وقتاً في **القراءة و البحث و التعلم**.

بذل القائم على هذا العمل أقصى جهوده لتحقيق مستوى عالٍ من الجودة، إلا أنه لا يتحمل أي مسؤولية و لا يوفر أي ضمانات صريحة أو ضمنية تجاه ما قد ينجم عن استخدام أو سوء استخدام ما ورد في هذه المادة.

هذا كان اجتهادي فإن أصبت فمن الله و إن أخطأت فمن نفسي و الشيطان.

و الله ولي التوفيق



يخضع هذا الكتاب لرخصة المشاع البداعي (creative commons) نسب المصنف ، غير تجاري ، الترخيص بالمثل 4.0 دولي (CC BY-NC-SA 4.0) لك مطلق الحرية في:

- المشاركة — نسخ وتوزيع ونقل العمل لأي وسط أو شكل.
- التعديل — المزج، التحويل، والإضافة على العمل.

بموجب الشروط التالية:

نسب المصنف — يجب عليك نسب العمل لصاحبها بطريقة مناسبة، وتوفير رابط للترخيص، وبيان إذا ما قد أجريت أي تعديلات على العمل. يمكنك القيام بهذا بأي طريقة مناسبة، ولكن على ألا يتم ذلك بطريقة توحى بأن المؤلف أو المرخص مؤيد لك أو لعملك.



غير تجاري — لا يمكنك استخدام هذا العمل لأغراض تجارية.



الترخيص بالمثل — إذا قمت بأي تعديل، تغيير، أو إضافة على هذا العمل، فيجب عليك توزيع العمل الناتج بنفس شروط ترخيص العمل الأصلي.



منع القيود الإضافية — يجب عليك ألا تطبق أي شروط قانونية أو تدابير تكنولوجية تقييد الآخرين من ممارسة الصالحيات التي تسمح بها الرخصة.



This work is licensed under the Creative Commons License.
Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

To view a copy of this license, visit

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

أهلا بك.. أتمنى أن تكون هذه المادة خفيفةً عليك ..
و لكن قبل أن ننطلق في المسار التقني ..
أريد إثراء معلوماتك قليلاً عن الأمن السيبراني ..

ألم تتسائل ما هو الأمن السيبراني؟... و ما فائدته و ما تاريخه؟... و ما هي أبعاده السياسية؟..
.. و كيف أستفيد منه (؟؟) و الكثيير الكثير من الأسئلة التي سنجيب عليها في هذه المادة
بإذن الله.

مفهوم الأمن السيبراني و تاريخه و علاقته بالسياسة تاريخياً في [هذا المقال](#) استمتع يا صديقي

أتمنى بأن المقال لم يكن طويلاً عليك ﴿ .. دعنا لا نطيل الحديث و نبدأ في القسم الآخر..

الأمن السيبراني تقنياً..

قد يعتقد الكثير بأن تخصص أمن المعلومات هو فقط للمخترقين و الإختراقات مثل الأفلام التي كلها إثارة .. لكن يجب أن تعلم أن هذا التخصص كبير جداً و يندرج تحته العديد من التخصصات مثل : اختبار الإختراق و التحليل الجنائي الرقمي.. و سوف نتعرف في هذه المادة على بعض التخصصات المندرجة تحت تخصص الأمن السيبراني

نبدأ هنا > بعرض شرائح عن "[مفهوم الأمن السيبراني و عناصر أمن المعلومات و أنواع الهجمات و البرمجيات الخبيثة و التشفير](#)" .. من اعداد د.أيمن الحربي ([الاطلاع عليه مهم](#))

كما أريد أن أضيف إلى معلوماتك أن الأمن السيبراني ليس كياناً قائماً بذاته، و إنما هو عبارة عن مجموعة من الإجراءات و العمليات التي تستخدم لحماية أشياء كالشبكات و البرمجيات و أنظمة التشغيل و غيرها.. و بهذا نعرف أنه من البديهي أن يكون تعلم الأمن السيبراني مرحلة ثانية بعد دراسة أحد مجالات الحاسوب (مثل : علوم الحاسوب ، هندسة الحاسوب ...) و هذا يدعونا للحديث عن المسارات التقنية للأمن السيبراني من حيث وظائفها.

ينقسم مجال الأمن السيبراني إلى ثلات مسارات رئيسية

> ويشمل اختبار الإختراق بأنواعه (Pen Test) 

> ويشمل أمن الشبكات & إدارة الأنظمة و الخوادم و قواعد البيانات (Network Security & Administration) 

> ويشمل التحليل الجنائي الرقمي و الاستجابة للحوادث & تحليل البرمجيات الخبيثة و الهندسة العكسية (Digital Forensic / Incident Response (DFIR) & Malware Analysis / Reverse Engineering) 

هناك أكثر من منهجية لمساعدة المبتدئين في الدخول إلى مجال الأمن السيبراني، احرص دائمًا على اختيار المنهجية القائمة على الأساس السليم و من الأمثلة على ذلك؛ سلسلة مقاطع على اليوتيوب للمهندس Muhammad Alharneel < إبدأ بالمقاطع الثاني وأولاً

في هذه المادة، سنعتمد منهجية المراحل الثلاث:-

 **المرحلة الأولى** : أساسيات علوم الحاسوب

 **المرحلة الثانية** : أساسيات الأمن السيبراني

 **المرحلة الثالثة** : التخصص في أحد مسارات الأمن السيبراني

لكن قبل أن نبدأ يجب التنويه على أن اللغة الإنجليزية مهمة جداً في المجال التقني عموماً و في مجال الأمن السيبراني خصوصاً، لإحتياج المبتدئ في المجال إلى كتابة التقارير و القراءة والبحث في الأنترنت و ما إلى ذلك من أمور مهمة.

من المصادر الجيدة لتعلم اللغة الإنجليزية أكاديمية [English Place](#)



عزيزي المبتدئ: الشهادات هي مجرد جسر عبر للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تخرج نفسك (**لا تجمع شهادات بدون معرفة**)



التفاصيل المتعلقة بـ اي شهادة او دورة لن يتم ذكرها في هذه المادة، و يمكن لمن يرغب معرفتها وضع اسم الشهادة/الدورة في محركات البحث و الحصول على العديد من النتائج.



المرحلة الأولى : أساسيات علوم الحاسوب الأساسية

إذا كانت مهارتك في استخدام الكمبيوتر ضعيفة، فيجب عليك تعلم أساسيات الحاسوب، لأن تدرس محتوى تعليمي مخصص للمبتدئين (مثل دوره: A+) قبل أن تبدأ في أي شيء آخر.



البرمجة؛ مثل لغات : PHP , JS , Python , C , C++ , Java (قد تحتاج إلى أكثر من لغة و قد لا تحتاج إلى أيٍ منها !!)

- **أساسيات بعض أنظمة التشغيل الدارجة (Linux & Windows)** مثل كورسات:

MCSA , Linux+

- **أساسيات الشبكات؛ مثل كورسات :** Network+ , CCNA , CND

بعض الشهادات المذكورة حتى الآن ليس لها قيمة تذكر في سوق العمل كشهادة احترافية و إنما تم ذكرها للفائدة الكبيرة الموجودة في مناهجها، كاحتواها على أساسيات و تدرج مناسب للمبتدئين، لكن **هذا كله لا يفيد إذا لم يصح بتطبيق عمل !!**



البرمجة :-

قد تتسائل .. لماذا أحتاج إلى تعلم البرمجة في مجال الأمن السيبراني؟ و هل من الممكن العمل في المجال دون تعلمها؟ إن كان الأمر كذلك، فلأي لغة أتعلم؟ ستجد جواباً لهذه التساؤلات في مقال: "[البرمجة وأهميتها في أمن المعلومات](#)" للأستاذ تكناوي.

لمن يرغب في البدء في تعلم البرمجة، تحتوي منصة يوتوب والعديد من المنصات الأخرى على محتوى رائع ([باللغة الإنجليزية](#)) لكن المحتوى العربي فيها متواضع. إذا كان المتعلم لا يجيد اللغة الإنجليزية، فمنصة [فلاكس كورسز](#) تقدم محتوى (يعد من الأفضل في الساحة العربية حتى تاريخ هذه المادة).

يقسم المختصون في مجال الأمن السيبراني حسب حاجتهم إلى البرمجة إلى ثلاثة أقسام :

1. **مستخدمي الأدوات:** هؤلاء لا يحتاجون إلى تعلم البرمجة، فقط يحتاجون إلى إتقان كيفية استخدام الأدوات.
2. **معدلي الأدوات:** هؤلاء يحتاجون معرفة جيدة أو متوسطة في البرمجة، تمكنهم من التلاعب بالنصوص البرمجية لتنوافق مع حاجتهم.
3. **صانعي الأدوات:** هؤلاء يحتاجون معرفة ممتازة في البرمجة، لإنشاء أدوات جديدة لأهداف محددة.

أنظمة التشغيل :-

ما هي أنظمة التشغيل؟ موقع سلامتك ويكي فصل في الشرح عن أنظمة التشغيل و تاريخها وبعض أنواعها في بطريقة ممیز جداً <> [هنا](#)

لكن قد يتطرق إلى ذلك سؤال.. أي نظام تشغيل هو الأفضل؟ وقد يفيدك النقاش [هذا](#) في الإجابة عن سؤالك.. وإذا أردت معرفة سبب انتشار نظام ويندوز، فإليك النقاش [التالي](#)..

ولكن لا تنسى أنه من الممكن أن تستخدم أكثر من نظام تشغيل في كمبيوتر واحد بعده طرق مختلفة.. لأنك غالباً ستحتاج إلى معرفة استخدام وإدارة أكثر من نظام في مجال الأمن السيبراني.

مصادر عربية لتعلم نظام التشغيل GNU/Linux

مدونة أخونا أبو تيم

من ممكن أن تتعلم استخدام وإدارة سيرفرات GNU/Linux في [فلاكس كورسز](#) (مدفع لكن أنصح به) من المهم أن تتعلم [shell scripting](#) وهذه [دورة](#) مقدمة من الأستاذ : عبدالمحبوب الحميد

 **تتويه :** يعد التمكّن من استخدام وإدارة نظام GNU/Linux من أهم الأمور التي يحتاجها المتخصص في مجال الأمن السيبراني. في بداية التعلم، يفضل البدء باستخدام التوزيعات البسيطة المناسبة للمبتدئين قبل الانتقال إلى توزيعات GNU/Linux الإحترافية مثل (Kali أو parrot).

* بالرغم من أهمية تعلم نظام GNU/Linux إلا أنه في بعض الحالات القليلة قد يكفي المتخصص بنظام ويندوز ☺

الشبكات :-

في هذه الروابط، ستتجد إجابة هذا السؤال "من أين أبدأ وكيف أبدأ في مجال الشبكات؟" (بعض المعلومات في هذا المقطع غير محدث) المقاطع : [4](#) [3](#) [2](#) [1](#) سلسلة مهمة جداً، يشكر عليها المهندس عادل الحميدي، في هذه المرحلة، يكفي فقط الاطلاع على هذه الشهادات الموجودة في المقاطع السابقة للبدء في المجال، ينصح بشدة مشاهدة أحد دورات [Network+](#) و [CCNA](#) في اليوتيوب مع التطبيق في أحد برامج المحاكاة مثل: [Packet Tracer](#) (قد يكون أكثر مناسبة للمبتدئين) أو [Gns3](#) أو حتى [eve-ng](#) (ابحث في اليوتيوب عن طريقة استخدام البرنامج) و من الممكن أن تساعدك سلسلة الفيديوهات [هذه](#) على [الممارسة العملية](#).

إن كان لديك القدرة المادية فبإمكانك بناء المعمل الخاص بك (Switch + Router + Firewall)

بعض المصادر المفيدة للبدء في دراسة الشبكات :-

 [قناة المهندس](#) : حسن صالح مفيدة جداً في مجال الشبكات.

 [ملخص أساسيات الشبكات](#) من إعداد : ماتركس.

 [شرح عرض](#) تحتوي على بعض المعلومات عن بروتوكول الـ **HTTP** وأهميته في عالم الويب من إعداد : هيتمان العربي.



هذه فقط بعض الأساسيات و لا تغنى عن باقي العلوم الموجودة في مجال الحاسوب عموماً مثل التشغيل و الخوارزميات و هيكلة البيانات و قواعد البيانات و ما إلى ذلك من أمور لا يتسع المجال لذكرها و لذا اكتفيت بذكر الأشياء التي لابد من تعلمها (**برمجة ، أنظمة تشغيل ، شبكات**).



بعض الشهادات المذكورة حتى الآن ليس لها قيمة تذكر في سوق العمل كشهادة احترافية و إنما تم ذكرها للفائدة الكبيرة الموجودة في مناهجها، كاحتواها على أساسيات و تدرج مناسب للمبتدئين، لكن **هذا كله لا يفيد إذا لم يصاحب بتطبيق عملي !!**

المرحلة الثانية : أساسيات الأمن السيبراني

من المهم قبل التخصص في أحد مجالات الأمن السيبراني أن تأخذ بعض الدورات العامة لتكون ملماً بالمفاهيم الأساسية التي توسيع معرفتك و تيسر لك التقدم مستقبلاً بإذن الله.. مثل كورسات : **GSEC** , **Security+** , **CSCU** ، أو حتى

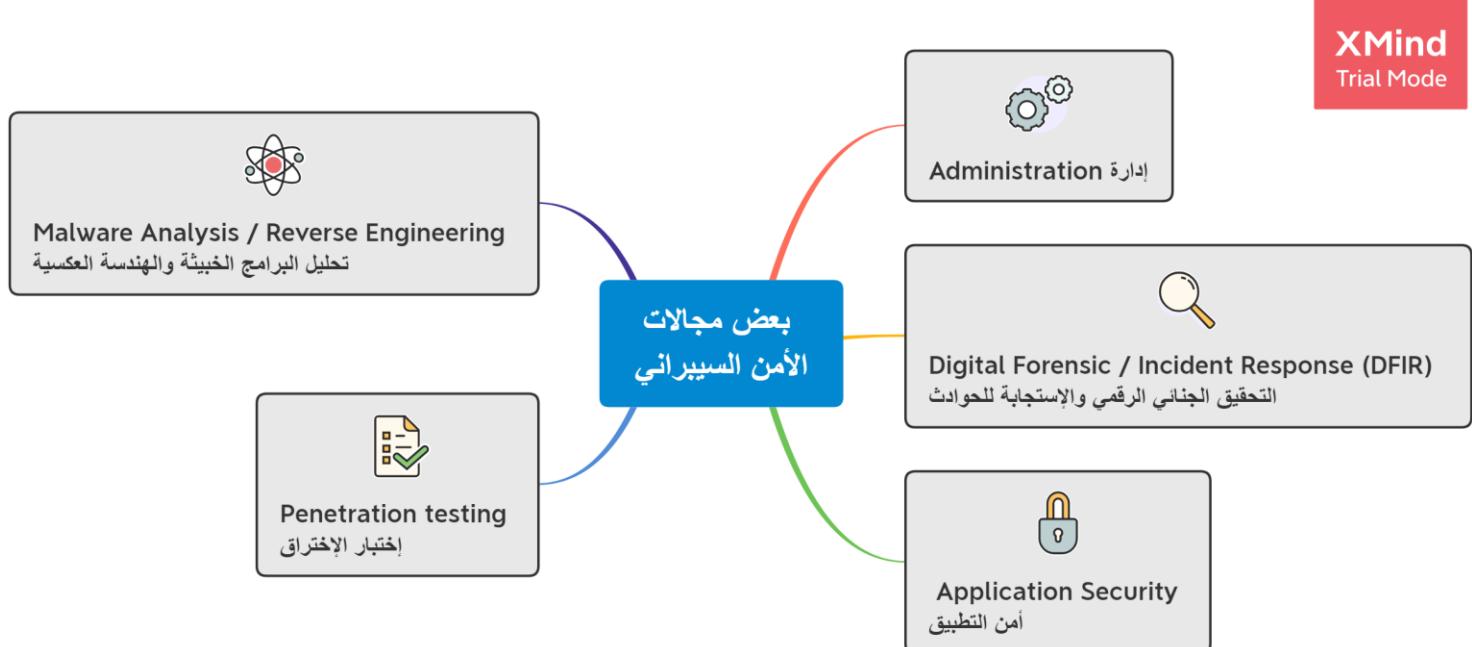
إذا كنت في هذه المرحلة **تبحث عن وظيفة** سريعة في المجال، فمن الممكن أن تكون الشهادات التالية مفيدة لك : **C|EH** و **CISSP** و **CISM** ، نظراً للاهتمام الذي توليه بعض أقسام الموارد البشرية في بعض الشركات بهذه الشهادات.

من المهارات التي يحتاجها المبتدئ والمتمرس في مجال الأمن السيبراني: **مهارات البحث** كيف و أين و عما تبحث و متى يجب أن توقف البحث، فمثلاً، مختبر الإختراق يجمع المعلومات عن الهدف و بقدر جمعه تتعدد سهولة الإختراق أو حتى إمكانيته، أيضاً، باستخدام مهارات البحث يكون المحلول الجنائي الرقمي قادر على الوصول إلى تفاصيل قد يعجز عن الوصول إليها إن لم يتقن هذه المهارة.



المرحلة الثالثة : التخصص في أحد تخصصات الأمن السيبراني

(هذه ليست جميع التخصصات و لكن المشهور منها، يمكن الاطلاع على تلخيص إطار سيف صفحة 34 أو [إطار سيف السعودي](#) للمزيد من التفاصيل)



الحقيقة أن كل تخصص يستحق كتاباً خاصاً به و لكن المقام لا يسمح بالإطالة لذا سنأخذ نبذة عن كل تخصص بشكل مختصر



في هذه المرحلة (المرحلة الثالثة) بعض الروابط و الشروحات ستكون باللغة الإنجليزية لشح المراجع العربية، و هنا يتبيّن لنا ضرورة أن يكون الفرد قادرًا على ممارسة اللغة الإنجليزية في هذه المرحلة من التخصص.



في الفترة التي ستحتاجها لتعلم الأساسيات من الممكن أن تكون قادرًا على تحديد المجال المناسب لك (و إن لم يكن أحد الخمس مجالات السابق ذكرها)



(إداره)



5 | 4 | 3 | 2 | 1

مستوى الصعوبة

مسؤول الأمن (**security administrator**) هو الشخص المسؤول عن فريق الأمن السيبراني. وعادة ما يكون مسؤولاً عن تثبيت وإدارة وصيانة الحلول الأمنية للمؤسسات.

يقوم مسؤول الأمن أيضاً بكتابة وثائق سياسات الأمان والتدريب حول الإجراءات الأمنية للزملاء، كما أنه مسؤول عن النظام بشكل عام.

عندما يقوم مسؤولي الشبكة والأنظمة بإعداد النظام وصيانته، يتراجع مسؤولي الأمان خطوة إلى الوراء للحصول على رؤية شاملة للأمان. بدلاً من التركيز على الأجهزة والبرامج، فإنهم يعملون للدفاع عن النظام ككل و الحفاظ عليه آمناً من التهديدات.

قد يكون من مهام مسؤول الأمن الأعمال التالية:

- الدفاع عن الأنظمة ضد الوصول غير المصرح به و التعديل و التدمير.
- مسح و تقييم الشبكة بحثاً عن نقاط الضعف.
- مراقبة حركة مرور الشبكة بحثاً عن نشاط غير عادي.
- تكوين و دعم أدوات الأمان مثل جدران الحماية و برامج مكافحة الفيروسات و أنظمة إدارة الترفيق.
- تنفيذ سياسات أمن الشبكة و أمن التطبيقات و التحكم في الوصول و حماية بيانات الشركة.
- تدريب زملائه الموظفين على الإجراءات الأمنية و رفع وعيهم الأمني.
- تطوير و تحديث الأعمال و بروتوكولات التعافي من الكوارث باستمرار.

المراجع : مدونة موقع CompTIA

من أقسام التخصص :-

إدارة أنظمة التشغيل:

- لينكس.
- ويندوز.
- إدارة الشبكات.
- إدارة السيرفرات.
- إدارة قواعد البيانات.

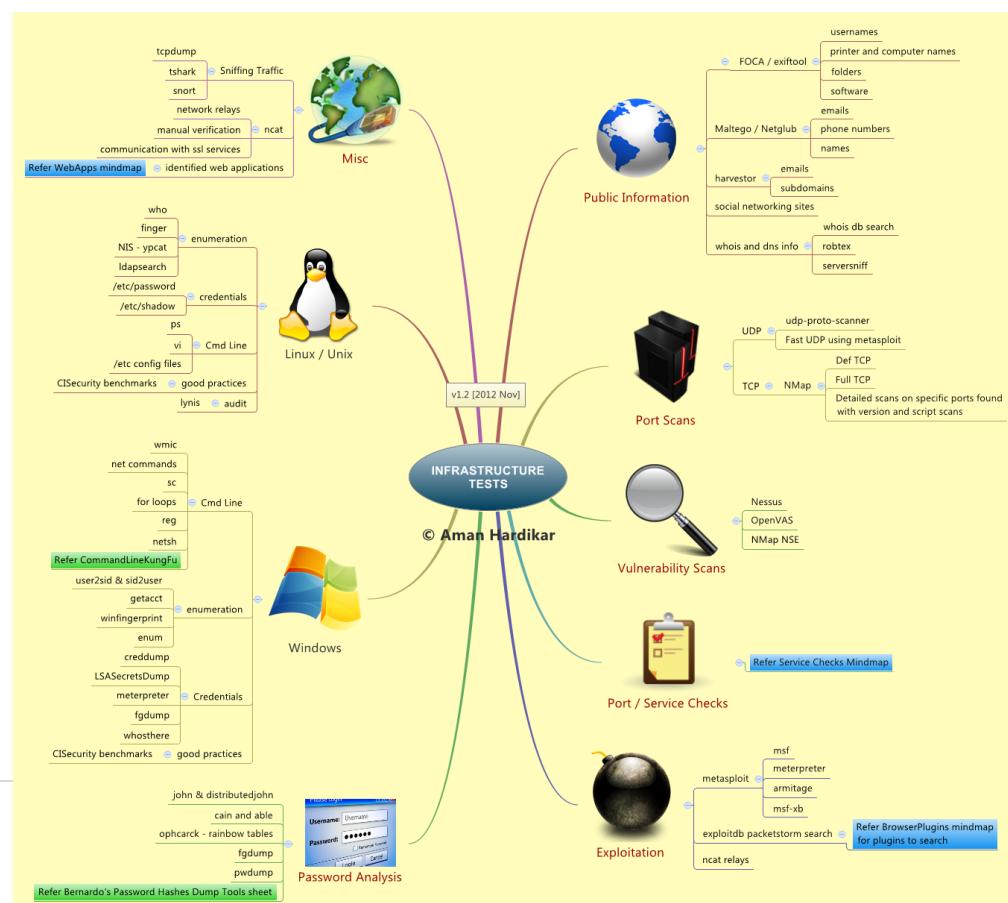
و غيرها..

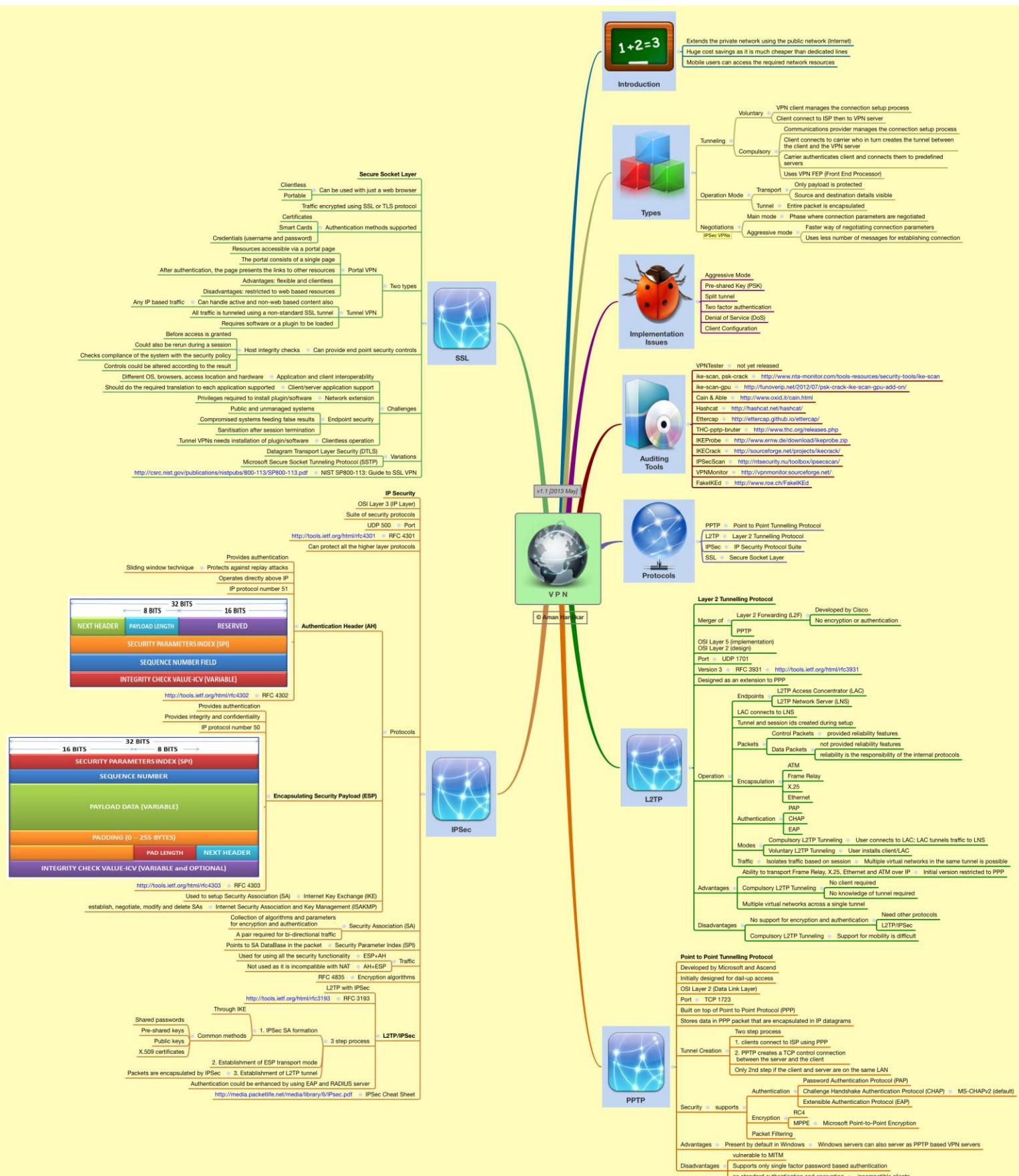
من المسميات الوظيفية التابعة للتخصص:-

- Security manager
- مدير أمن المعلومات -
- Information security manager
- Network security administrator
- مسؤول أمن الشبكة -
- Systems security administrator
- ضابط أمن نظم المعلومات -
- Information systems security officer
- IT security administrator
- مسؤول أمن تكنولوجيا المعلومات -

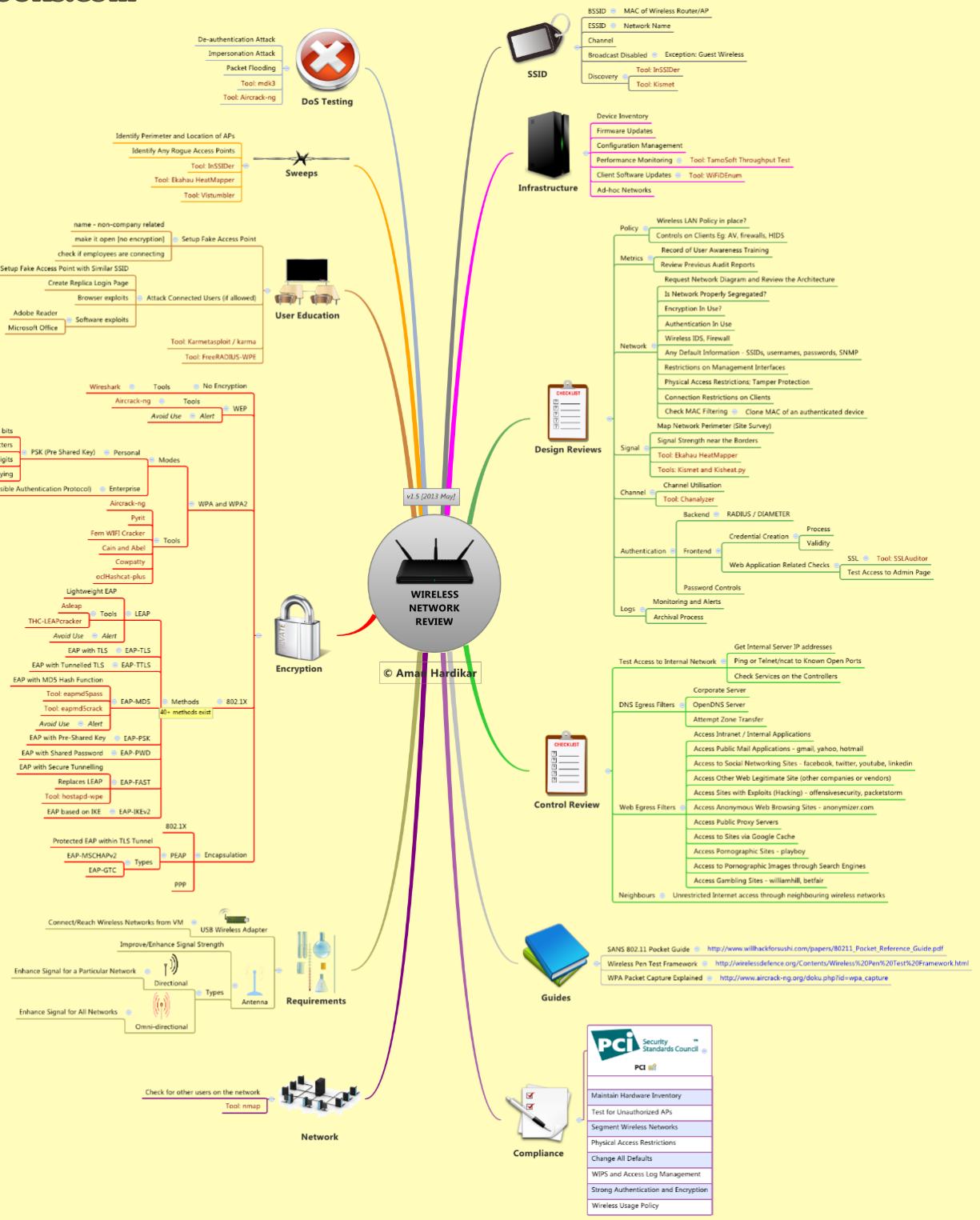
أدوات و خرائط (MAPs & Tools)

بعض الأدوات المهمة [هنا](#)





الصورة بجودة أعلى و الروابط في الصورة هنا



الصورة بجودة أعلى و الروابط في الصورة [هنا](#)

شهادات ودورات

عزيزي المبتدئ: الشهادات هي مجرد جسر عبر للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تخرج نفسك (لا تجمع شهادات بدون معرفة)



لينكس(GNU/Linux) : دورة [فليكس كورسز](#) ([ينصح بها للمعرفة العملية](#)) كما توجد دورة Linux+ لكن أغلب الشهادات في هذا المجال مقدمة من شركة RedHat ستجد خارطة شهادات الشركة في صفحة

52

ويندوز (Windows) : جميع الشهادات مقدمة من شركة Microsoft مثل شهادة MCSA و ستجد خارطة شهادات الشركة صفحة 46

الشبكات (Network) : (راجع [أساسيات الشبكات](#)) من الممكن أن تبدأ بدورة Network+ وبعد هذه المرحلة من الأفضل أن تبحث عن الشركة المقدمة لـ أجهزة/خدمات الشبكات في المنشأة التي تتوى العمل بها.. و تأخذ أحد مسارات التدريبية التي تقدمها تلك الشركة، من الأمثلة على الشركات: Cisco ، Juniper ، FireEye

لكن لو احترت أو لم تستطع معرفة أي المسارات أنساب لك، فمن الأفضل أن تأخذ دورات شركة Cisco حيث أنها الأكثر انتشاراً.. ولكن لا تقلق، فمهما كان المسار الذي أتبعته، ستجد أنك في الغالب ستكون على قدر عالي من الكفاءة التي تمكنت من التعامل مع معظم أنظمة باقي الشركات، حيث أن المفهوم العام واحد.. انظر إلى خارطة شهادات شركة Cisco في صفحة 47

مسار مقترن للشهادات:

اسم الشهادة المختصر	اسم الشهادة كامل	الشركة
CCNA	Cisco Certified Network Associate	Cisco
MCSA	Microsoft Certified Solutions Associate	Microsoft
MCSE	Microsoft Certified Solutions Expert	Microsoft
CCNP Enterprise	Cisco Certified Network Professional	Cisco
CCNP Security	Cisco Certified Network Professional Security	Cisco
RedHat		
Microsoft Azure		
AWS Certified Advanced Networking		
AWS Certified Security		



نبذة تعريفية عن التحليل الجنائي الرقمي:-

تعرف موسوعة [ويكيبيديا](#) التحليل الجنائي الرقمي (المعروف أحياناً باسم علم الطب الشرعي الرقمي) هو فرع من فروع علم التحليل الجنائي يشمل استرداد المواد الموجودة في الأجهزة الرقمية و التحقيق فيها ، و غالباً ما يتعلق بجرائم الكمبيوتر . تم استخدام مصطلح التحليل الجنائي الرقمي في الأصل كمرادف للتحليل الجنائي الحاسوبي و لكنه امتد ليشمل التحقيق في جميع الأجهزة القادرة على تخزين البيانات الرقمية . تعود جذورها إلى ثورة الحوسبة الشخصية في أواخر السبعينيات و أوائل الثمانينيات ، تطور النظام بطريقة عشوائية خلال التسعينيات ، و لم تظهر السياسات الوطنية إلا في أوائل القرن الحادي و العشرين.

نبذة تعريفية عن الإستجابة للحوادث:-

هي الممارسة المنظمة للإستجابة لحوادث الأمن السيبراني. يتم تنظيم هذه الممارسات في خطة محكمة تحدد الخطوات والأدوات التي يجب على المنظمة إتباعها خلال وقوع الحادث.

يمكن لهذه الخطة أن تختلف بين جهة وأخرى ، ولكنها على الأقل يجب أن تغطي 6 خطوات رئيسية:
 1- الإعداد 2- الإكتشاف 3- الإحتواء 4- الإستئصال 5- الإستعادة 6- الدروس المستفادة

يجب أن نضع في عين الاعتبار أن كل خطوة من هذه الخطوات تحتاج إلى أتمتها لذا يتم استخدام بعض الأدوات المختصة في التحليل الجنائي الرقمي لتساعدنا على جمع البيانات واستيعابها .. بينما تستخدم أدوات أخرى للوصول لأهداف أخرى مثل، إجراءات الإستجابة الفعلية .. كما يوجد أدوات أخرى أيضاً تساعد في تحقيقات تفصيلية معقدة في الحوادث الأمنية.

الجدير بالذكر هنا أن معظم الأدوات المجانية توفر حلاً لجزء فقط من عملية الإستجابة للحوادث ، لذا في الغالب ستحتاج إلى الجمع بين عدة أدوات للوصول إلى أفضل النتائج بالسرعة المطلوبة.

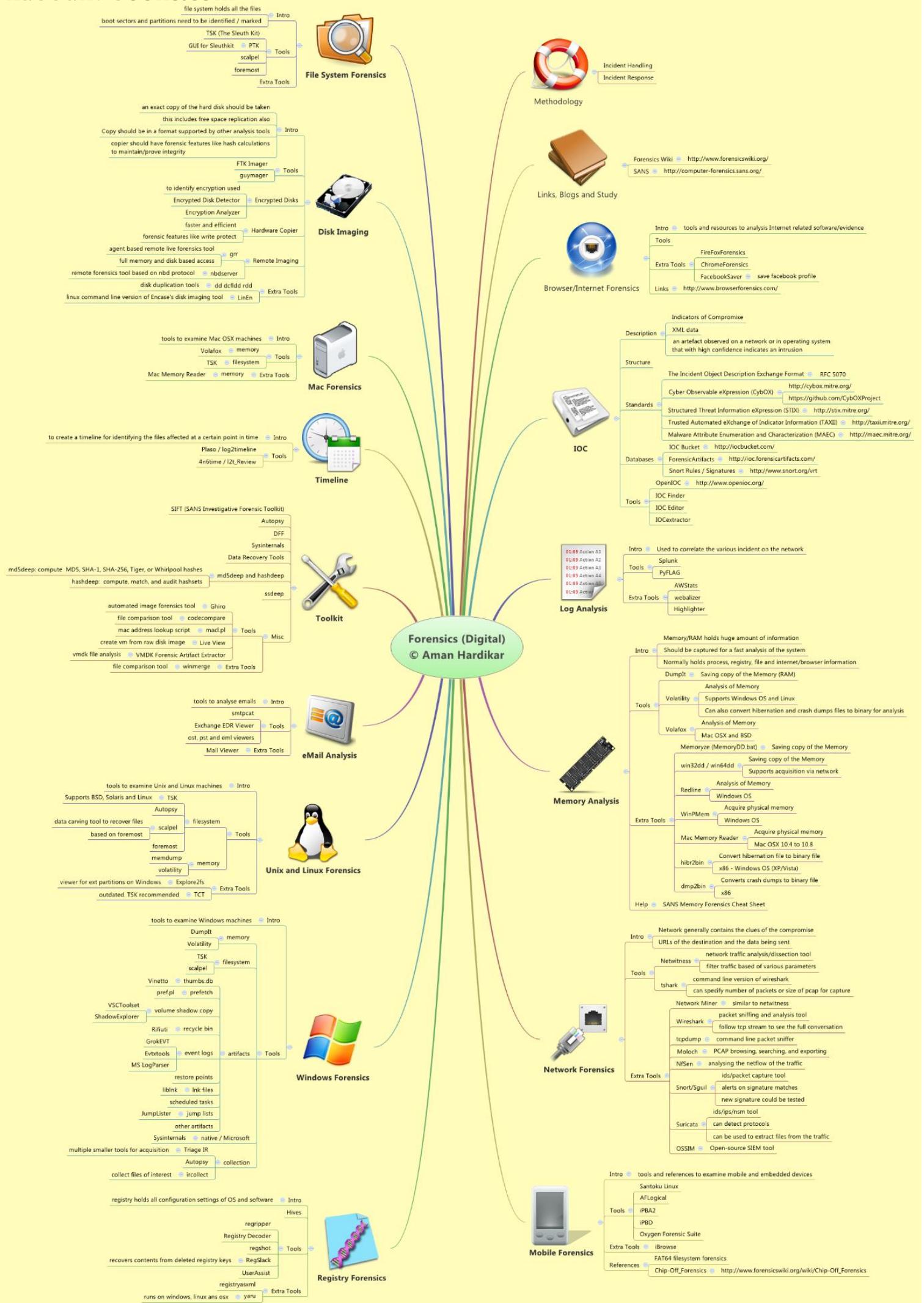
[للمزيد من التفاصيل](#)

أقسام التخصص + بعض التفاصيل

و التحليل الجنائي الرقمي له فروع كثيرة و نذكر منها:

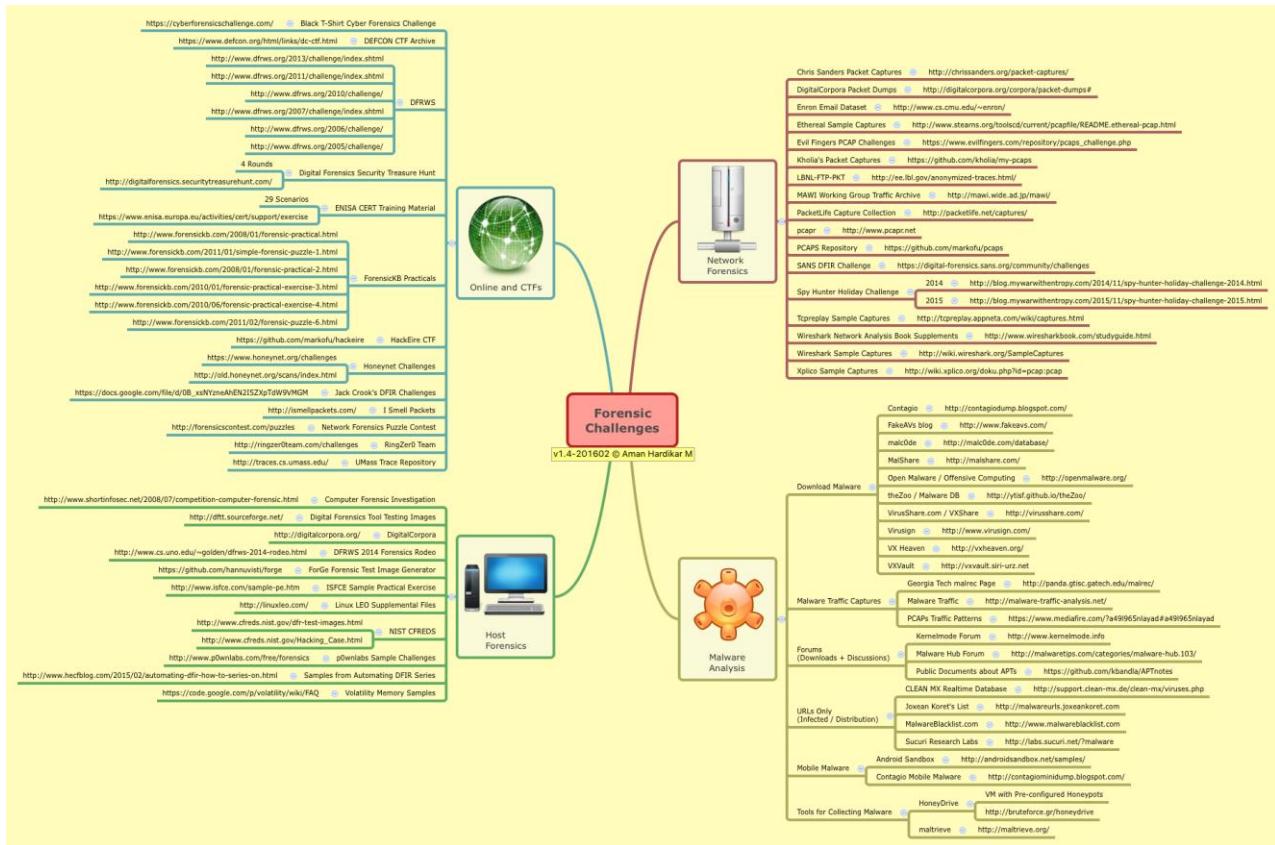
- التحليل الجنائي الرقمي لأجهزة الحاسوب.
- التحليل الجنائي الرقمي لقواعد البيانات.
- التحليل الجنائي الرقمي للشبكة.
- التحليل الجنائي الرقمي للويب.
- التحليل الجنائي الرقمي لأجهزة الجوال.

و المزيد من التفاصيل في الصورة التالية



أدوات ، معامل ، الالات (Machines , Labs , Tools)

توجد الكثير من الأدوات في الصورة السابقة



الصورة بجودة أعلى و الروابط في الصورة هنا

عزيزي المبتدئ: الشهادات هي مجرد جسر عبر للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تخرج نفسك (**لا تجمع شهادات بدون معرفة**)



اسم الشهادة المختصر	اسم الشهادة كامل	الشركة
CySA+	Cybersecurity Analyst	CompTIA
CEH	Certified Ethical Hacker	EC-Council
CHFI	Certified Forensic Hacking Investigator	EC-Council
GCIH	Certified Incident Handler	GIAC
GCIA	Certified Intrusion Analyst	GIAC
GCFA	Certified Forensic Analyst	GIAC
GCFE	Certified Forensic Examiner	GIAC
GREM	Reverse Engineering Malware	GIAC
GNFA	Network Forensic Analyst	GIAC
EnCE	Certified Examiner	EnCase
CCE	Certified Computer Examiner	
CFCE	Certified Forensic Computer Examiner	

المصدر

و من المهم أن تطلع على شهادات هذا التخصص في مسارات دورات الشركات خصوصا صفحه 48 eLearnSecurity

Applications Security (AppSec)

(أمن التطبيقات)



5 | 4 | 3 | 2 | 1

مستوى الصعوبة

نذة تعرفة عن التخصص :-

يعرف موقع "VMware" [أمن التطبيقات](#) بأنه: عملية تطوير و إضافة و اختبار ميزات الأمان داخل التطبيقات لتحسين الثغرات الأمنية ضد التهديدات مثل الوصول غير المصرح به و التعديل، كما يصف الإجراءات الأمنية على مستوى التطبيقات، و التي تهدف إلى منع سرقة أو اختطاف البيانات أو النصوص البرمجية داخل التطبيقات. تشمل العملية، احتمالات نشوء الثغرات الأمنية أثناء تطوير التطبيقات و تصميمها ، كما أنها تتضمن أنظمة و أساليب لحماية التطبيقات بعد نشرها .

قد يتضمن أمن التطبيقات: الأجهزة والبرامج و الإجراءات التي تحدد نقاط الضعف الأمنية أو تقللها. يعد جهاز التوجيه (و الذي من مهامه، منع أي شخص من عرض عنوان IP الخاص بجهاز الكمبيوتر من الإنترت) شكلاً من أشكال أمن تطبيقات الأجهزة. في العادة، تكون مقاييس الأمان على مستوى التطبيق مضمنة في البرنامج ، مثل جدار الحماية للتطبيق (و الذي من مهامه، تحديد الأنشطة المسموح بها والمحظورة بدقة). يمكن أن تستلزم الإجراءات أشياء مثل، العمليات الدورية لأمن التطبيقات و التي تتضمن بروتوكولات مثل الاختبار المنتظم.

أقسام التخصص:-

- أمن تطبيقات الويب.
- أمن تطبيقات الجوال.
- أمن تطبيقات سطح المكتب.
- و غيرها..

أدوات ، معامل ، (Lab , Tools)

معلم (يقدم الموقع خدمات اخرى)
بعض الادوات و الشروحات المفيدة

شهادات ودورات

عزيزي المبتدئ: الشهادات هي مجرد جسر عبور للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تخرج نفسك (**لا تجمع شهادات بدون معرفة**)



اسم الشهادة المختصر	اسم الشهادة الكامل	الشركة
GWEB	GIAC Certified Web Application Defender	GIAC
GWAPT	GIAC Web Application Penetration Tester	GIAC
OWASP (Open Web Application Security Project)		
WAPT	Web Application Penetration Testing	eLearnSecurity
WAPTX	Web Application Penetration Testing eXtreme	eLearnSecurity
Whitehat Security		
Veracode		

المصدر: شبكة نكرة



بعد مختبر الإختراق (**penetration tester, or pen tester**) ، من اصحاب القبعات البيضاء أو "مخترق أخلاقي". و على الرغم من أنه يجب عليه التفكير كمخترق غير أخلاقي (صاحب قبعة السوداء) ، فإن الهدف النهائي هو مساعدة المنظمات على تحسين ممارساتها الأمنية لمنع الأضرار، كالسرقة أو التدمير و يستهدف مختبر الإختراق أنظمة التشغيل و الأنظمة المضمنة و الهواتف و الحواسيب، كما يستهدف أيضا التقنيات الناشئة مثل، أنترنوت الأشياء (IoT) و غيرها.

بعض مسؤوليات مختبر الإختراق:-

- تطبيق الأدوات المناسبة لاختبار الإختراق.
- إجراء اختبارات الهندسة الإجتماعية و مراجعة الأمان المادي عندما يقتضي الامر.
- مواكبة أحدث طرق الإختبار و القرصنة.
- جمع البيانات و نشر منهجية الإختبار.
- تحديد وتقييم و إدارة نقاط الضعف.
- تقديم إقتراحات لتحسين الأمان و إعداد الإستجابات التقنية لأسئلة الأمان.

المرجع : مدونة موقع CompTIA

و أحب أن أنوه على جزئية عادةً ما يخطئ فيها الناس :-

PT ≠ vulnerable hunting & PT ≠ Red Teaming

ولكن تعني : **PT = penetration testing**

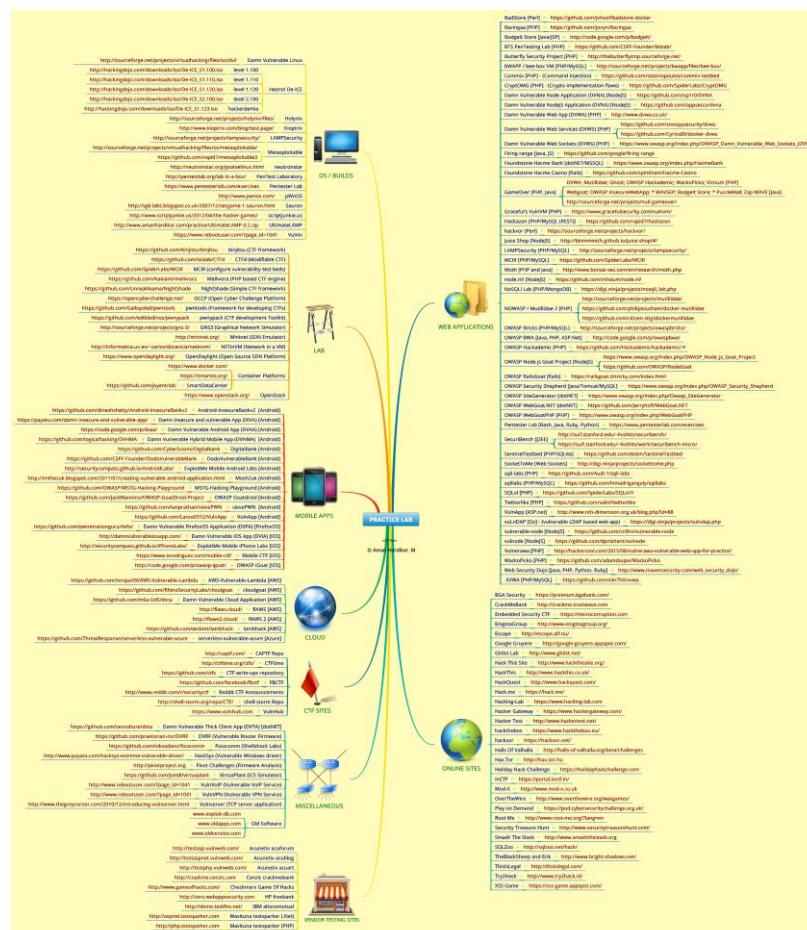
أقسام التخصص:-

- اختبار اختراق تطبيقات ويب.
 - اختبار اختراق تطبيقات جوال.
 - اختبار اختراق الشبكات.
 - اختبار اختراق أنظمة تشغيل.

و غيرها..

أدوات ، معامل ، الالآت (Machines , Labs , Tools)

من المهم الاطلاع على [هذا الكتيب](#) (قد تحتاج إلى تحميله لرؤيه بعض الصور بوضوح) و [مجتمع incyber](#) (حيث يحتوي على ملفات و معلومات و أدوات و شروحات و العديد من الأشياء عن : ... كلاهما من إعداد الاستاذ: مالك الدوسري (PenTest , BugBounty , SOC



الصورة بحودة أعلى، والروابط في الصورة هنا

شهادات و دورات

عزيزي المبتدئ: الشهادات هي مجرد جسر عبور للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تخرج نفسك (**لا تجمع شهادات بدون معرفة**)



اسم الشهادة المختصر	اسم الشهادة الكامل	الشركة
	OSCP	Offensive Security
	OSCE	Offensive Security
PTP	Penetration Testing Professional	eLearnSecurity
GPEN	GIAC Certified Penetration Tester	GIAC
GXPN	GIAC Exploit Researcher and Advanced Penetration Tester	GIAC
CoreLan Team		

المصدر: شبكة نكرة

أو يمكنك إتباع مسار أحد الشركات المذكورة في آخر هذا المحتوى مثل **eLearnSecurity**



5 | 4 | 3 | 2 | 1

مستوى الصعوبة

البرمجيات الخبيثة :

البرمجيات الخبيثة (Malicious Software) و هي برامج أو ملفات صممت بطريقة معينة لتلحق الضرر بالبرامج والأنظمة، بل وقد يصل ضررها إلى أجزاء الكمبيوتر، وهذا لا شك له تداعيات خطيرة منها الاقتصادي والسياسي والبيئي وغيرها.

هناك أنواع كثيرة من البرمجيات الضارة تختلف سلوكياتها وأهدافها ومدى الضرر الذي يمكن أن تسببه، من الأمثلة على هذا : الديدان ، الفيروسات ، أحصنة طروادة ، فيروسات الفدية ، برامج التجسس ، برمجيات الإعلانات ، الجذور الخفية وأنواع أخرى..

يمكن لبرنامج ضار وحيد القيام بعدة مهام، مثل: سرقة البيانات أو حذفها أو تشفيرها أو التعديل عليها أو حتى إضافة الأنظمة إلى شبكة روبوت (botnet) و مراقبتها دون علم المستخدم بذلك.

و للمزيد عن البرمجيات الخبيثة إليك هذا [المقال](#) (أو مجموعة المقالات إن أحببت التفصيل في كل نوع)

الهندسة العكسية :

الهندسة العكسية (Reverse engineering – وتسمى أيضا backwards engineering أو back engineering) وهي العملية التي يتم من خلالها تفكيك شيء اصطناعي للكشف عن تصميماته أو هندسته المعمارية أو برمجته أو من أجل المعرفة.

كما يمكن تطبيق الهندسة العكسية في مجالات هندسة الكمبيوتر و الهندسة الميكانيكية و الهندسة الإلكترونية و هندسة البرمجيات و الهندسة الكيميائية و بيولوجيا الأنظمة.

[المصدر](#)

لتبسيط الفكرة دعنا نفترض أنتي أعطيت متذوق حلويات قطعة من الكعك و طلبت منه اكتشاف مكوناتها (زيت ، بيض ، دقيق ، سكر ...) فتحليله لطعم الكعك ومحاولته اكتشاف الوصفة (دون علم مسبق) يعد هندسة عكسية (ولو أن الكعك ليس شيء علمي ولا هندي ☺)

لا أحد يمكنه تغطية جميع الجوانب في هذا المجال لأنه يمكن تطبيقه على عدد كبير جداً من العلوم و هذا يتخطى حدود معرفة الإنسان الواحد ولكن بإمكان مجتمع أو دولة مثل الصين مثلاً أن يبرع في كثير من مجالاته وقد فعلوا

لتتعرف أكثر عن الهندسة العكسية انظر هذا المقال في [ويكيبيديا](#) أو هذا المقال في موقع "Engineering 360"

و [هنا](#) شرائح عرض عن الهندسة العكسية للبرمجيات و [هنا](#) شرح للشرائح (بالعربي)

بما أن المقام لا يتسع للتفصيل في المجال فسأقتصر هنا على الحديث عن "[تحليل البرمجيات الخبيثة](#)" و [هندستها عكسياً](#)"

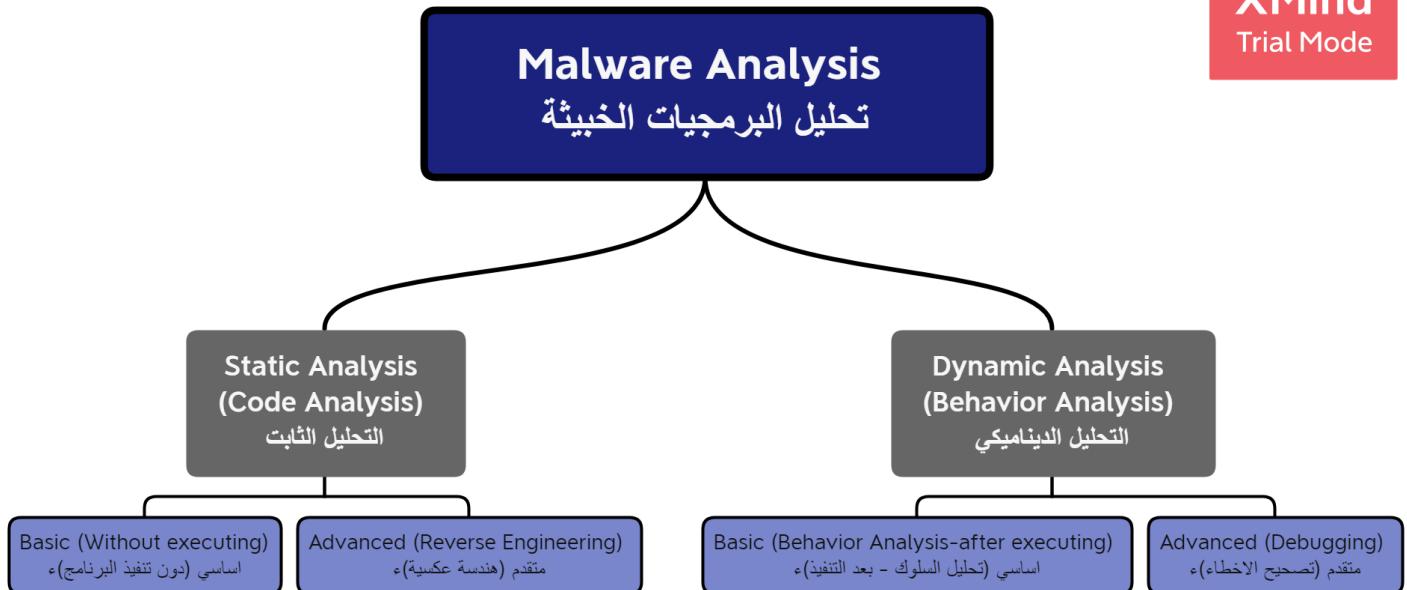
نبذة تعريفية عن التخصص ([الهندسة العكسية و تحليل البرامج الخبيثة](#))

هو فن تshireح البرمجيات الخبيثة لفهم كيفية عملها أو لرصدها أو لتعطيلها أو للتخلص منها لتصدي لها مستقبلاً. يتطلب العمل في هذا المجال معرفة واسعة في مجال تقنية المعلومات عموماً ومن الشركات التي تهتم في هذا المجال، شركات برامج الحماية مثل : كاسبرسکای ، نورتن و غيرها ..

حتى لا نطيل .. هذا مقطع عظيم جداً بعنوان : "[Malware Analysis](#)" للمهندس وجدي عصام .. تكلم فيه عن الطرق و المراحل و الأدوات و البرامج و البيئات الإفراضية لتحليل البرمجيات الخبيثة (رابط المكتبة المذكور في الفيديو و الموجودة على Github تجده مع الأدوات بالأسف)

نظرأً لضيق الوقت، اضطرّ المهندس وجدي إلى الاختصار و عدم الحديث بشكل مفصل عن تحليل البرمجيات الضارة و هندستها عكسياً و عن التحليل الجنائي للذاكرة و أتمتت هذه العمليات.

ليكون فهم الموضوع أسهل .. هذه خارطة ذهنية لمساعدتك على فهم تفاصيل الموضوع ..



مصادر : [مقال](#) و [مرجع](#) و [مقال](#)

[مقال عن "Basic Static Analysis"](#) و من الجيد قراءة [هذا الكتاب](#)

كيف تتم هندسة البرمجيات الخبيثة عكسياً؟

سابقاً كان الموضوع معقد ويحتاج إلى عدد من المختصين .. لكن مع تطور العلوم التقنية أصبح بإمكان شخص واحد بإستعمال الأدوات الجاهزة و لغات التجميع "Assembly languages" أداء دور كل هؤلاء المختصين

و كما ترى في الصورة التالية :

فإن عملية ترجمة الكود البرمجي "Compilation" تتم من الأعلى إلى الأسفل (من لغة يفهمها الإنسان مثل: java , python أو C إلى لغة الكود الثنائي 0 ، 1 ("Binary"))

و حيث أنه يتم عادةً كتابة الكود بلغة مثل C ثم تترجم "compiled" بالطريقة المذكورة سابقاً

فحينها لا يمكن فهم الكود وسنحتاج إلى إعادة إعادتها إلى لغة يمكن للأنسان فهمها، ويمكن عمل ذلك عن طريق أداة تسمى "Decompiler" ولكن في الغالب لن تتفق معنا هذه العملية أو سيكون من الأفضل استعمال أداة تسمى "Disassembler". هناك عدة أسباب لاستخدام هذه الأداة، منها.. تسهيل فهم البرنامج أو استعادة الـ "source code" و أسباب أخرى.. و بما أننا سنستخدم في الغالب أداة الـ "disassembler" فسنحتاج إلى معرفة لغات التجميع (تسمى عملية إرجاع الكود من اللغة الثنائية إلى لغات التجميع "Disassembly" و إرجاع الكود إلى لغة مثل java أو C تسمى ("decompilation"))

المصادر: [Malware Analysis and Detection Using Reverse Engineering Technique](#) ، [malwarebytes labs](#)

و في الخاتم إليك بعض المواضيع و التقنيات التي ستساعدك في احتراف هذا المجال :

Principles and Fundamental Concepts:

- Assembly languages and program compilation
- Binary code and ELF/PE data representations
- Static binary analysis and disassembly
- Dynamic execution analysis

Attacks and Existing Malware:

- Malware behavior (e.g., control flow hijacking)
- Anti-reverse engineering and obfuscation
- Return-oriented programming
- Web-based malware and social engineering

Analyses and Security Defenses:

- Symbolic execution and taint tracking
- Runtime memory forensics
- Behavioral detection signatures
- Security hardening (ASLR, DEP, and CFI)

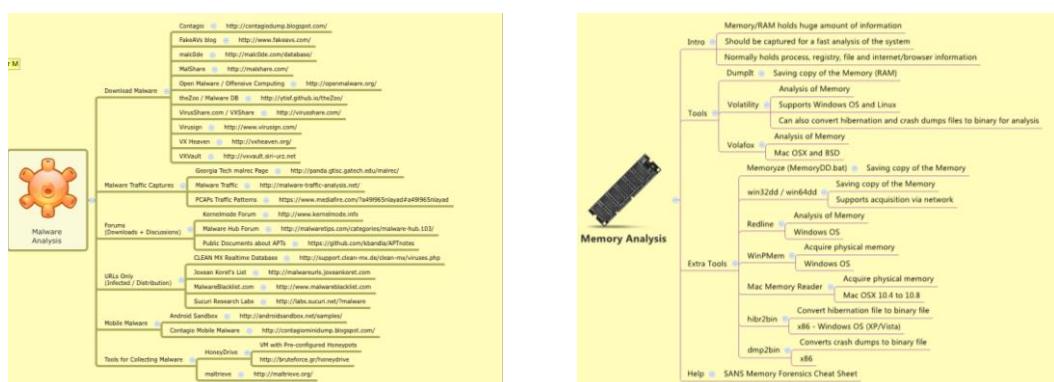
أدوات ، معامل ، الالات (Machines , Labs , Tools)

المكتبة المذكورة في شرح المهندس [هنا](#)

بعض الأدوات و المصادر [هنا](#)

بعض المراجع للهندسة العسكرية [هنا](#)

طريقة إنشاء معمل خاص [هنا](#)



الصورة بجودة أعلى و الروابط في الصورة [هنا](#)

شهادات و دورات

[هنا](#) دورة عبارة عن جزئين الهندسة العكسية 101 و 102 (مفيدة جداً و فيها معامل)

" Hacking — Best OF Reverse Engineering " [هنا](#) سلسلة من المقالات بعنوان

" Practical Malware Analysis " [هنا](#) سلسلة أخرى بعنوان

الشهادات

Reverse Engineering Malware (**GREM**) GIAC

Reverse Engineering Professional (**REP**) eLearnSecurity

الشهادتين في الأعلى لم أجل غيرهما و بحسب ما وصلت إليه من نتائج بعد البحث فهذا المجال تحديداً **يعتمد على المهارات أكثر من الشهادات**.

بعض المقالات المفيدة في مجال الأمن السيبراني:

- مقالة على موقع [نواتي](#) بعنوان "[كيف تصبح هكر أخلاقي](#)"
- مقالة بعنوان "[كتبيك الفريق الأحمر والأزرق والأرجواني](#)"
- مقالة بعنوان "[How to became a hacker](#)"
- مقالة بعنوان "[How Every Operating System Keeps You Safe](#)" و ترجمت و اختصرت.. [هنا](#)
- مقالة بعنوان "[ما هو Bug Bounty](#)"

بعض المواقع والأدوات المفيدة في مجال الأمن السيبراني:

- [مقطع](#) > يحتوي على عدة مواقع وأدوات.
- [hackerEnv](#) > منصة عربية سعودية من إبداع مجموعة من الشباب.
- [Nakerah Network](#)
- [Pentester Academy](#)
- [vuln hub](#)
- [reversing.kr](#)
- [w3challs](#)
- [I.O](#)
- [hacksplaining](#)
- [alf.nu](#)
- [hacker 101 ctf](#)
- [hack.me](#)
- [pentestit](#)
- [OverTheWire](#)
- [hellbound hackers](#)
- [root me](#)
- [komodo](#)
- [attack defense](#)

- بعض الكتب عن الشبكات وانظمة التشغيل وأشياء اخرى رفعتها على [Google Drive](#) [هنا](#)
- الكثير من الكتب و الفيديوهات و الكورسات بهذا المستودع الضخم [The-Art-of-Hacking](#) لمختلف التخصصات في مجال الأمن السيبراني.
- أكثر من **400** كتاب متاحة للتنزيل **مجاناً** من سبرنجر [Springer Text books](#)

قناتي على اليوتيوب (تحتوي على مجموعة من المقاطع المفيدة في مجال التقنية عموماً)



السميات الوظيفية في مجال أمن المعلومات و الأمن السيبراني : (وفق إطار سيف)

معمارية الأمن السيبراني والبحث والتطوير

تنفيذ اعمال التصميم والمعمارية والبحوث والتطوير في مجال الأمن السيبراني.

أ- معمارية الأمن السيبراني

تصميم أنظمة الأمن السيبراني ومكوناته التابعة لنظم وشبكات تقنية المعلومات، والإشراف على تطويرها وتنفيذها.

1- مصمم معمارية الأمن السيبراني

تصميم نظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها

2- أخصائي الحوسبة السحابية الأمينة

تصميم نظم الحوسبة السحابية الأمينة وتنفيذها وتشغيلها، مع تطوير سياسات السحابة الأمينة.

ب- البحث والتطوير في الأمن السيبراني

القيام بأعمال البحث والتطوير في مجال الأمن السيبراني.

1. أخصائي تطوير أمن النظم

تصميم أمن نظم المعلومات وتطويره وختباره وتقييمه في كافة مراحل تطوير تلك النظم.

2. مطور الأمن السيبراني

تطوير برمجيات الأمن السيبراني وتطبيقاته ونظمها ومنتجاته.

3. مقيم البرمجيات الأمينة

تقييم أمن تطبيقات الحاسوب وبرمجياته وشفراته أو برامجه، مع تقديم نتائج قابلة للتطبيق.

4. باحث الأمن السيبراني

إجراء الأبحاث العلمية في مجال الأمن السيبراني.

5. أخصائي علم البيانات للأمن السيبراني

استخدام نماذج رياضية ومنهجيات وعمليات علمية لتصميم وتنفيذ خوارزميات وأنظمة لاستخلاص استنتاجات و المعارف الأمن السيبراني من مصادر متعددة لمجموعة بيانات واسعة النطاق.

6. أخصائي الذكاء الاصطناعي للأمن السيبراني

استخدام نماذج الذكاء الاصطناعي وتقنياته (شاملاً أساليب التعلم الآلي) لتصميم وتنفيذ خوارزميات وأنظمة لأتمتة وتحسين كفاءة وفعالية مهام الأمن السيبراني.

القيادة وتطوير الكوادر

قيادة وتطوير فرق عمل الأمن السيبراني وأعمالها ، وتطوير كوادر الأمن السيبراني.

أ- القيادة

الإشراف على فرق الأمن السيبراني وأعمالها، وإدارتها وقيادتها.

1. رئيس إدارة الأمن السيبراني

إدارة أعمال الأمن السيبراني داخل المنظمة، ووضع الرؤية والتوجّه بشأن الأمن السيبراني، والاستراتيجيات والموارد والأنشطة ذات العلاقة وتقديم المرئيات لقيادة المنظمة حيال أساليب الإدارة الفعالة لمخاطر الأمن السيبراني للمنظمة.

2. مدير الأمن السيبراني

إدارة الأمن السيبراني للوظائف والنظم المعلوماتية داخل المنظمة .قيادة الأمن السيبراني سواء على مستوى فريق أو وحدة أو وظيفة على المستوى المؤسسي.

3. مستشار الأمن السيبراني

تقديم الرأي والمشورة لقيادة المنظمة وقادة وفرق الأمن السيبراني في مواضيع الأمن السيبراني.

ب- تطوير الكوادر

تطبيق معارف ومهارات الأمن السيبراني ومنهجيات تعليم وتطوير الموارد البشرية لتطوير مهارات كوادر الأمن السيبراني وإدارتها والحفاظ عليها وتحسينها.

1. مدير الموارد البشرية للأمن السيبراني

تطوير الخطط والاستراتيجيات والإرشادات داخل المنظمة لدعم تطوير كوادر الأمن السيبراني وإدارتها.

2. مطور المناهج التعليمية للأمن السيبراني

تطوير وتحفيظ وتنسيق وتقييم برامج التعليم والتدريب للأمن السيبراني والمناهج ومحتوياتها وطرقها وأساليب تقديمها، حسب الاحتياجات التعليمية.

3. مدرب الأمن السيبراني

تعليم الأفراد وتدريبهم وتطويرهم واختبارهم في موضوعات الأمن السيبراني.

الحكومة والمخاطر والالتزام والقوانين

تطوير سياسات الأمن السيبراني للمنظمة، وحكومة هيكل الأمن السيبراني وعملياته، وإدارة مخاطر الأمن السيبراني، وضمان الالتزام بمتطلبات إدارة المخاطر والأمن السيبراني للمنظمة والمتطلبات القانونية ذات الصلة.

أ- الحكومة والمخاطر والالتزام

حكومة هيكل الأمن السيبراني وعملياته، وإدارة مخاطر الأمن السيبراني، وضمان تلبية متطلبات إدارة المخاطر والأمن السيبراني للمنظمة لكافه ظُنوم وتقنيات المعلومات. وكذلك تطوير سياسات الأمن السيبراني داخل المنظمة وتحديثها.

1. أخصائي مخاطر الأمن السيبراني

تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها وإدارتها لحماية أصولها المعلوماتية والتقنية وفقاً لسياسات وإجراءات المنظمة، وكذلك القوانين والأنظمة ذات العلاقة.

2. أخصائي الالتزام في الأمن السيبراني

ضمان التزام برنامج الأمن السيبراني للمنظمة بمتطلبات السياسات والمعايير المعتمد بها.

3. أخصائي سياسات الأمن السيبراني

تطوير سياسات الأمن السيبراني وتحديثها، لدعم متطلبات الأمن السيبراني بالمنظمة ومواعيدها.

4. مقيم ضوابط الأمن السيبراني

تحليل ضوابط الأمن السيبراني وتقييم فاعليتها.

5. مدقق الأمن السيبراني

تصميم عمليات التدقيق للأمن السيبراني وتنفيذها وإدارتها بهدف تقييم مدى التزام المنظمة بمتطلبات السياسات والمعايير والضوابط المعتمد بها، وإعداد تقارير التدقيق وتقديمها للأطراف ذات الصلاحية.

بـ- القوانين وحماية البيانات

ضمان التزام المنظمة بقوانين وتنظيمات الأمان السيبراني وحماية البيانات.

1. أخصائي قانون الأمان السيبراني

تقديم الخدمات القانونية بشأن الموضوعات ذات الصلة بالقوانين والأنظمة السيبرانية.

2. أخصائي الخصوصية وحماية البيانات

دراسة هيكلة البيانات الشخصية وقوانين وأنظمة الخصوصية المعمول بها، مع تحليل مخاطر الخصوصية، وتطوير برنامج المنظمة للمواءمة مع ضوابط الخصوصية وحماية البيانات والسياسات الداخلية، والإشراف على تنفيذها، مع دعم استجابة المنظمة لحوادث الخصوصية أو حماية البيانات.

الحماية والدفاع



تحديد تهديدات وثغرات نظم وشبكات تقنية المعلومات، وتحليلها ومراقبتها والتعامل معها وإدارتها، واستخدام التدابير الدفاعية، والمعلومات التي تم الحصول عليها من مصادر متعددة، للإبلاغ عن الأحداث والاستجابة لحوادث.

أـ- الدفاع

استخدام أدوات المراقبة والتحليل لتحديد الأحداث وتحليلها والكشف عن حوادث الأمان السيبراني.

1. محل دفاع الأمان السيبراني

استخدام البيانات التي تم استخلاصها من مجموعة أدوات الدفاع السيبراني لتحليل الأحداث الواقعة داخل المنظمة بهدف الكشف عن التهديدات والتعامل معها

2. أخصائي البنية التحتية للأمن السيبراني

فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية وتشغيلها والإشراف عليها.

3. أخصائي الأمان السيبراني

تقديم الدعم العام للأمن السيبراني، والمساعدة في مهام الأمان السيبراني.

بـ- الحماية

استخدام أدوات المراقبة والتحليل لتحديد الأحداث وتحليلها والكشف عن حوادث الأمان السيبراني.

- 1. أخصائي التشفير**
تطوير أنظمة التشفير وخوارزمياته، وتقيمها وتحليلها وتحديد نقاط ضعفها وسبل تحسينها.
- 2. أخصائي إدارة الهوية والوصول**
إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق أنظمة وعمليات التعريف والتوثيق والتصريح.
- 3. محل أمن النظم**
تطوير أمن النظم واختباره وصيانته، وتحليل أمن العمليات والأنظمة المدمجة.

ت-تقييم الثغرات

اختبار نظم وشبكات تقنية المعلومات، وتقيم التهديدات والثغرات.

- 1. أخصائي تقييم الثغرات**
تقيم ثغرات النظم والشبكات، وتحديد مواطن انحرافها عن الإعدادات المقبولة أو السياسات المعمول بها، وقياس فاعلية البنية الدفاعية متعددة الطبقات ضد الثغرات المعروفة.
- 2. أخصائي اختبار الإختراقات**
أداء محاولات اختراق مصرح لها لأنظمة الحاسوب أو الشبكات والمنشآت المادية باستخدام أساليب تهديد واقعية لتقيم حالتها الأمنية وكشف الثغرات المحتملة.

ثـ- الاستجابة للحوادث

مباشرة الحوادث السيبرانية وتحليلها والاستجابة لها.

1. أخصائي استجابة للحوادث السيبرانية

مباشرة الحوادث المتعلقة بالأمن السيبراني وتحليلها والاستجابة لها.

2. أخصائي التحليل الجنائي الرقمي

جمع الأدلة الرقمية وتحليلها، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النظم والشبكات.

3. أخصائي تحقيقات الجرائم السيبرانية

تعريف الأدلة وجمعها وفحصها والحفظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة.

4. أخصائي الهندسة العكسية للبرمجيات الضارة

تحليل البرمجيات الضارة (عن طريق تفكيكها وإعادتها إلى صيغة برمجية مفهومة)، وفهم طريقة عملها وتأثيرها وغرضها، وتقديم توصيات للوقاية منها والاستجابة للحوادث الناتجة عنها.

جـ- إدارة التهديدات

جمع وتحليل المعلومات عن التهديدات والبحث عن التهديدات غير المكتشفة، وتقديم رؤى قابلة للتطبيق لدعم عمليات اتخاذ القرار في الأمن السيبراني.

1. محلل معلومات التهديدات السيبرانية

جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والإجراءات المتبعة، لاستبطاط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية والتنبؤ بها، وحماية النظم والشبكات من التهديدات السيبرانية.

2. أخصائي اكتشاف التهديدات السيبرانية

البحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنظم، وتحديد مؤشرات الإختراق، وتقديم التوصيات للتعامل معها.



تنفيذ أعمال الأمان السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية.

أ- أنظمة التحكم الصناعي والتقنيات التشغيلية

القيام بأعمال الأمان السيبراني المتعلقة بالحكومة وإدارة المخاطر، ومتابعة الالتزام، والتصميم والتطوير، والتشغيل والإشراف، والحماية والدفاع في نظم التقنيات التشغيلية التي تشمل نظم التحكم الصناعي، ونظم التحكم الإشرافي وحيازة البيانات

1. مصمم معمارية الأمان السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية تصميم نظم وشبكات الأمان السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها.

2. أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتشغيلها والإشراف عليها.

3. محلل دفاع الأمان السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية استخدام البيانات، التي تم جمعها من مجموعة متنوعة من أدوات الأمان السيبراني لتحليل الأحداث الواقعية في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية بهدف الكشف عن تهديدات الأمان السيبراني والتعامل معها.

4. أخصائي مخاطر الأمان السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية تحديد مخاطر الأمان السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتقديرها وإدارتها، مع تقييم وتحليل فاعلية ضوابط الأمان السيبراني القائمة، وتقديم الملاحظات والتوصيات بناء على تلك التقييمات.

5. أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية مباشرةً على حادث الأمان السيبراني وتحليلها والاستجابة لها في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية.

[المراجع إطار سيف السعودي](#)

من الممكن أن تساعدك الصورة التالية في تطوير مسيرتك المهنية : (ليس لها علاقة بطار سيف) (يسار)

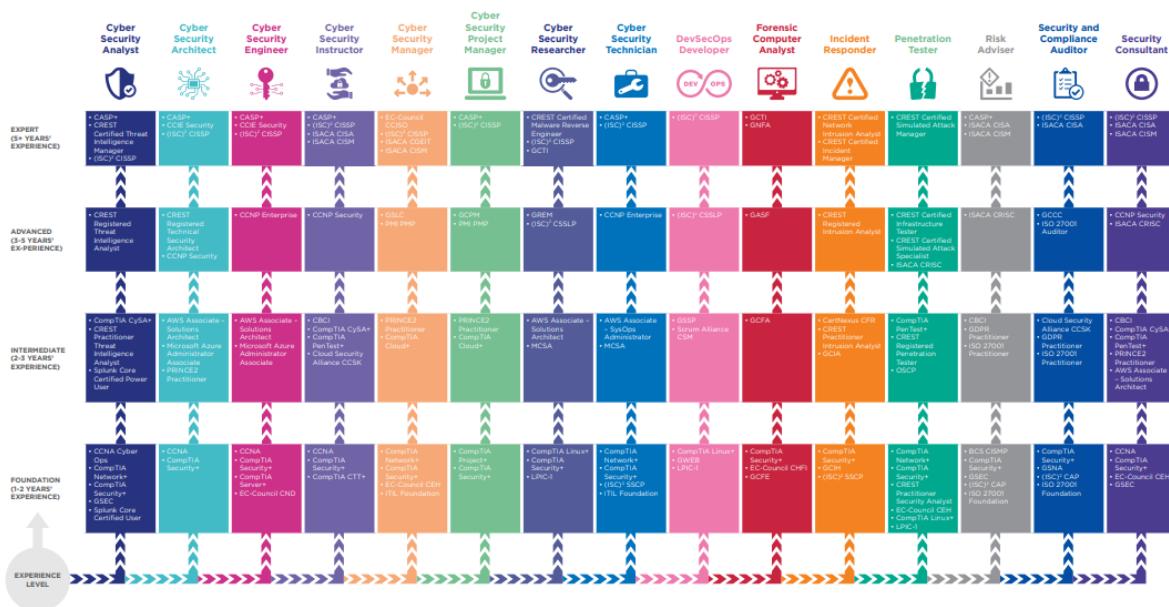
A GUIDE TO CYBER SECURITY CAREER DEVELOPMENT



[Looking to upskill your knowledge and climb up the Cyber Security ladder?](#)

Confused by the industry certifications landscape and trying to decide which one is right for you?

Check out our handy guide to Cyber Security Professional Certifications currently available in Scotland (as of June 2019).



أسماء بعض الشهادات والدورات والشركات التي تقدمها

مقسمة حسب مستوى الخبرة (للمزيد راجع قسم الشركات في الاسفل)

يوجد العديد من الشركات لم يتم وضعها في الجدول تجدها في قسم الشركات أسفل الصفحة .. مثل :
RedHat و Offensive Security و eLeanSecurity والمزيد



الشركة	الاسم كامل	اسم الشهادة/الدورة
Beginner / Foundational مبتدئ / تأسيسي		
CompTIA.	A+	

INTERMEDIATE متوسط		
Network+		CompTIA.
Security+		CompTIA.
Server+		CompTIA.
CCNA	Cisco Certified Network Associate	
C EH	Certified Ethical Hacker	
C HFI	EC Council Certified Incident Handler	
GCIH	GIAC Certified Incident Handler	

GISP	GIAC Information Security Professional	
GSEC	GIAC Security Essentials	
MCSA	Microsoft Certified Solutions Associate	

ADVANCED

مُتَقدِّم

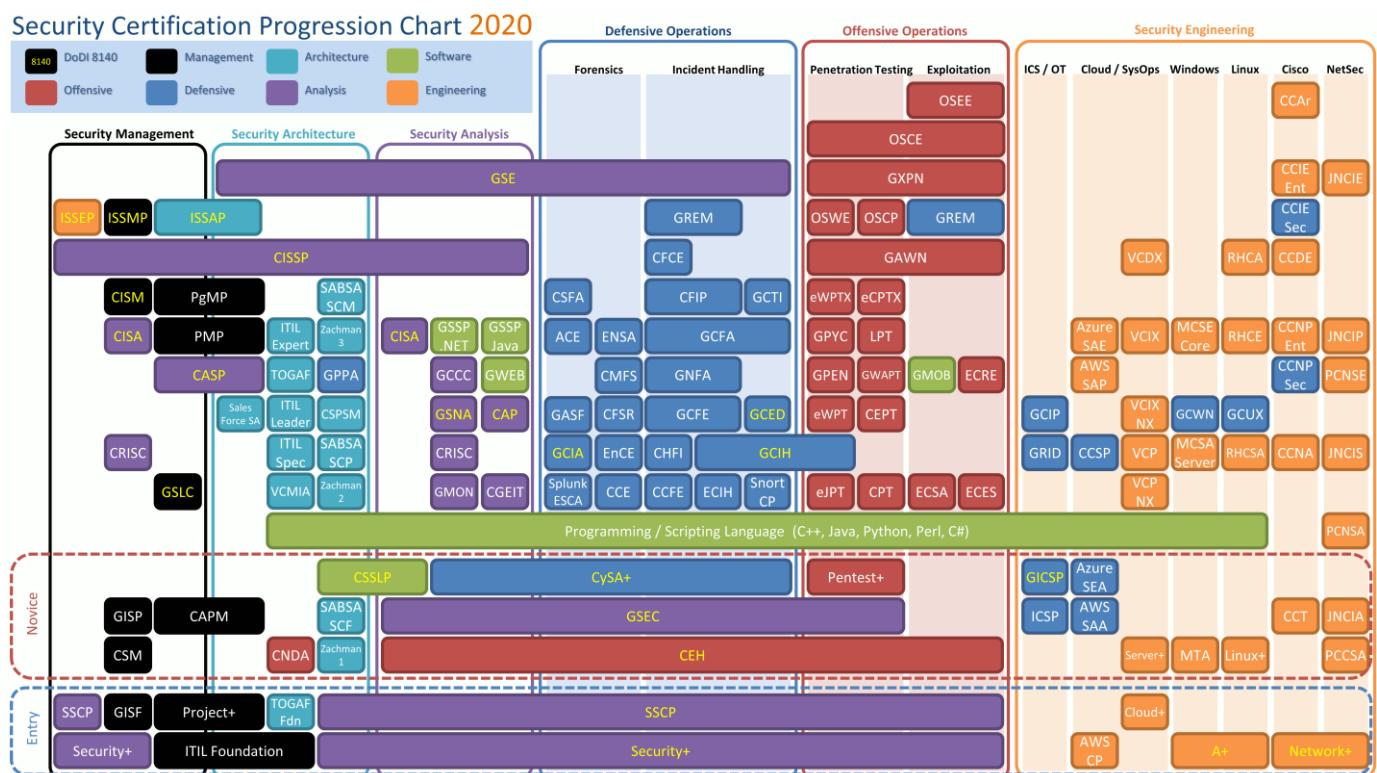
CSA+(CySA+)	Cyber Security Analyst+	CompTIA.
Pen Test+		CompTIA.
CCDP	Cisco Certified Design Professional	
CCNP	Cisco Certified Network Professional	
CISA	Certified Information Systems Auditor	
CSSLP	Certified secure software lifecycle professional	
MCSE Core Infrastructure	Microsoft Certified Solutions Expert	
GSLC	GIAC Security Leadership Certification	
GCED	GIAC Certified Enterprise Defender	

EXPERT

خیر

CASP+	CompTIA Advanced Security Practitioner	
CCIE	Cisco Certified Internetwork Expert	
SCYBER	Cisco Cybersecurity Specialist	
CGEIT	Certified in the Governance of Enterprise IT	 <small>Trust in, and value from, information systems</small>
CISM	Certified Information Security Manager	 <small>Trust in, and value from, information systems</small>
CISSP	Certified Information Systems Security Professional	

من الممكن أن تكون الصورة التالية مفيدة و أكثر ترتيب من الجداول السابقة :

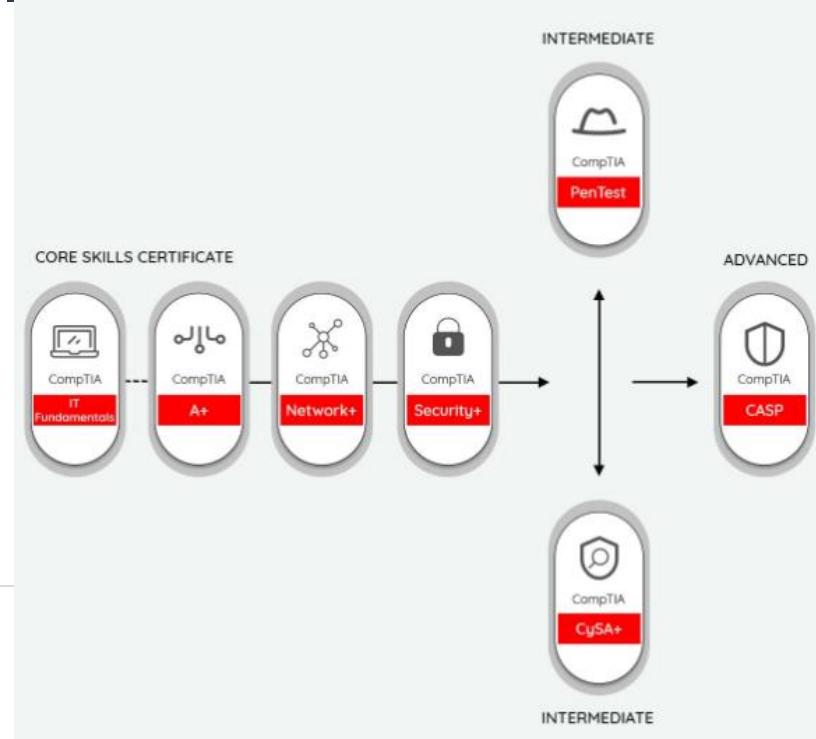
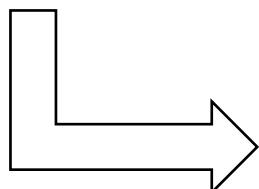


بعض مسارات عدد من الشركات المتخصصة في الأمن السيبراني ونظم التشغيل والشبكات.

ComptIA®

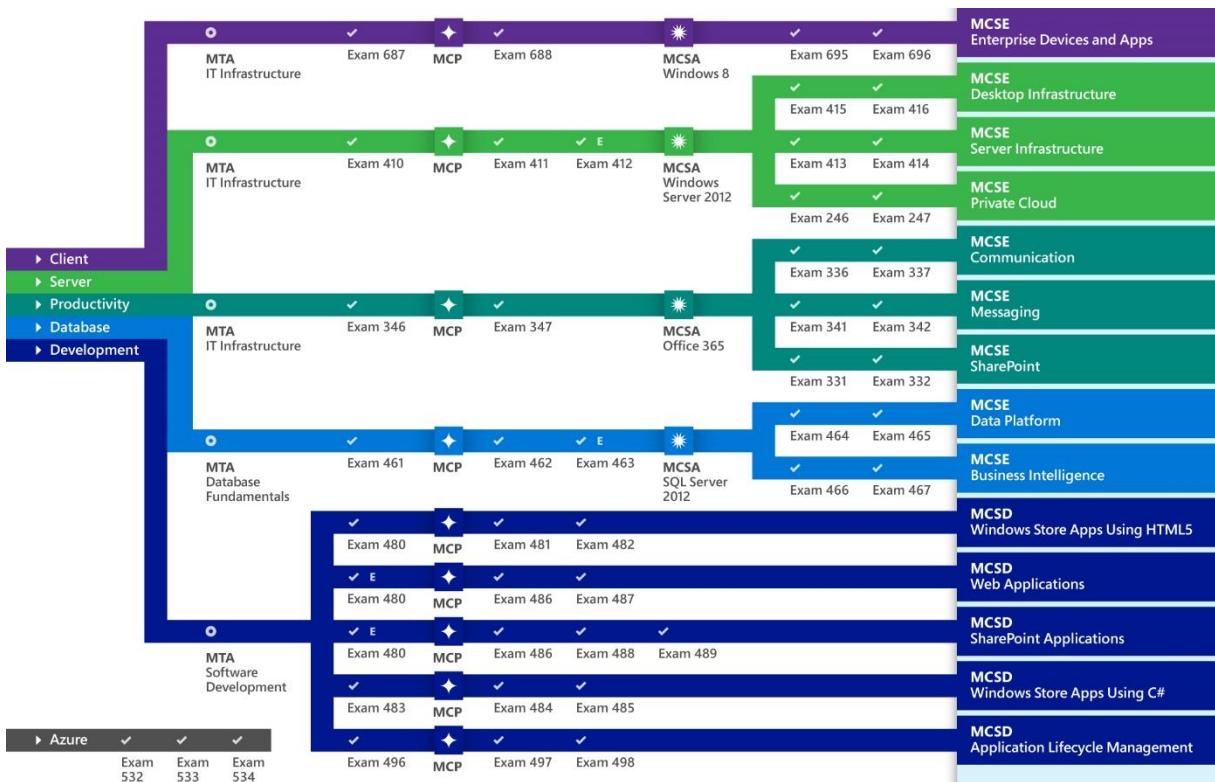


مسار
الأمن
السيبراني





Microsoft



Role-based

Technical skills required to perform a job



Apps & Infra



Data & AI



Modern Workplace



Business Applications

Azure Solutions Architect

Expert

Azure DevOps Engineer

Microsoft 365 Enterprise Administrator

Associate

Azure Administrator

Azure Data Scientist

Microsoft 365 Modern Desktop Administrator

Dynamics 365 for Sales Functional Consultant

Dynamics 365 for Customer Service Functional Consultant

Azure Developer

Azure AI Engineer

Microsoft 365 Teamwork Administrator

Dynamics 365 for Marketing Functional Consultant

Dynamics 365 for Field Service Functional Consultant

Azure Security Engineer

Azure Data Engineer

Microsoft 365 Messaging Administrator

Dynamics 365 for Finance and Operations, Financials Functional Consultant

Microsoft 365 Security Administrator

Dynamics 365 for Finance and Operations, Manufacturing Functional Consultant

Dynamics 365 for Finance and Operations, Supply Chain Management Functional Consultant

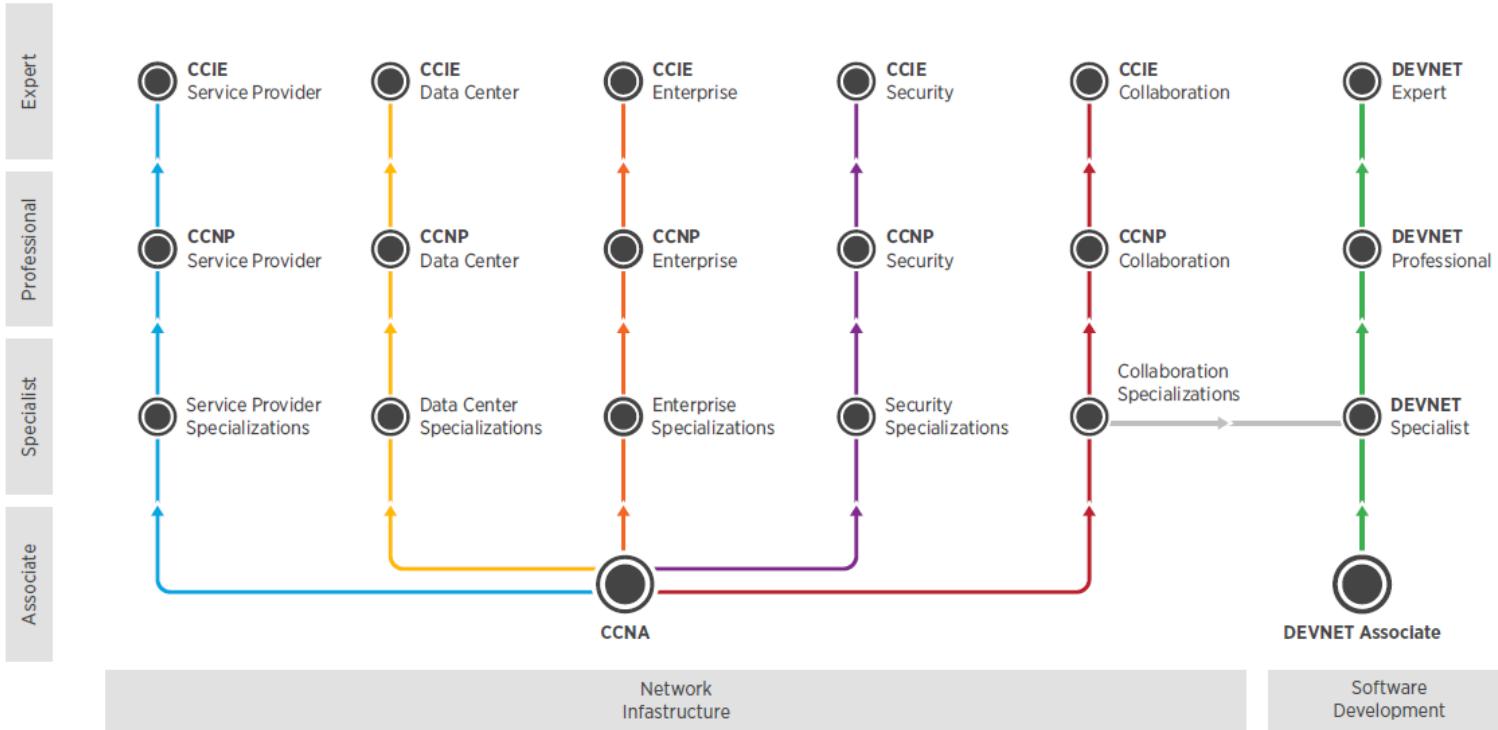
Fundamentals

Foundational understanding of technology

Azure Fundamentals

Microsoft 365 Fundamentals

Dynamics 365 Fundamentals



Core Exam	• Implementing and Operating Cisco Enterprise Network Core Technologies	• Implementing and Operating Cisco Security Core Technologies	• Implementing and Operating Cisco Service Provider Network Core Technologies	• Implementing and Operating Cisco Collaboration Core Technologies	• Implementing and Operating Cisco Data Center Core Technologies	• Developing Applications using Cisco Core Platforms & APIs
	+ 1 of the below	+ 1 of the below	+ 1 of the below	+ 1 of the below	+ 1 of the below	+ 1 of the below
Concentration Exams One Exam Earns 'Specialist'	<ul style="list-style-type: none"> Implementing Cisco Enterprise Advanced Routing and Services Designing Cisco Enterprise Wireless Networks Implementing Cisco Enterprise Wireless Networks Designing Cisco Enterprise Networks Implementing Cisco SD-WAN Solutions Automating and Programming Cisco Enterprise Solutions 	<ul style="list-style-type: none"> Securing Networks with Cisco Firepower Implementing Secure Solutions with Virtual Private Networks Securing Email with Cisco Security Appliances Securing the Web with Cisco Web Security Appliance Implementing and Configuring Cisco Identity Services Engine Automating and Programming Cisco Security Solutions 	<ul style="list-style-type: none"> Implementing Cisco Service Provider Advanced Routing Solutions Implementing Cisco Collaboration Applications Implementing Cisco Advanced Call Control and Mobility Services Implementing Cisco Collaboration Cloud and Edge Solutions Automating and Programming Cisco Service Provider Solutions 	<ul style="list-style-type: none"> Implementing Cisco Storage Area Networking Implementing Cisco Application Centric Infrastructure Designing Cisco Data Center Infrastructure Troubleshooting Cisco Data Center Infrastructure Automating and Programming Cisco Data Center Solutions 	<ul style="list-style-type: none"> Implementing DevOps Solutions and Practices using Cisco Platforms Developing Solutions using Cisco IoT & Edge Platforms Developing Applications for Cisco Webex and Webex Devices Automating and Programming Cisco Enterprise Solutions Automating and Programming Cisco Security Solutions Automating and Programming Cisco Service Provider Solutions Automating and Programming Cisco Collaboration Solutions Automating and Programming Cisco Data Center Solutions 	
One Exam						

Associate Level

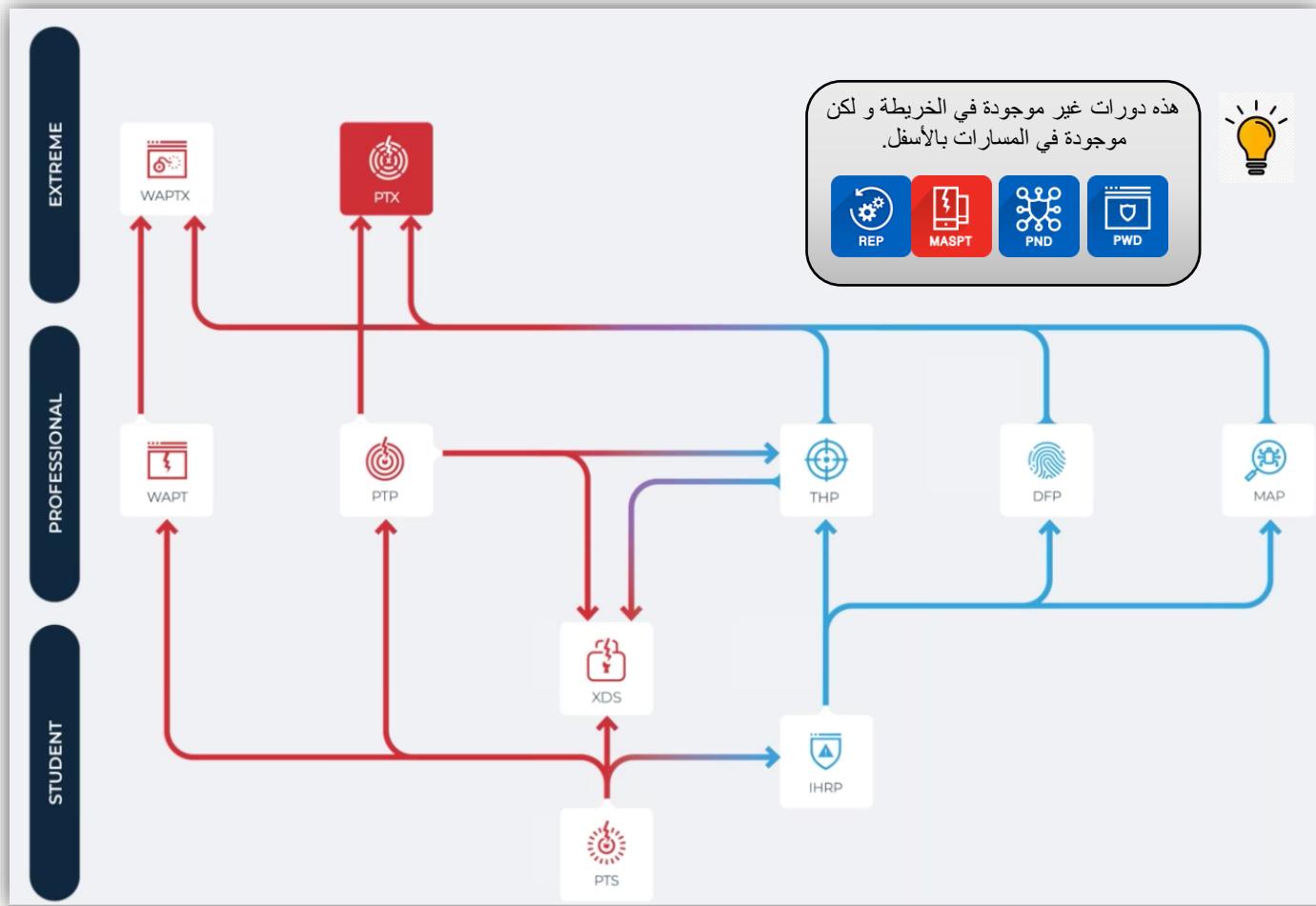
Specialist Level

Professional Level

Expert Level

Engineering**Software**

دورات شركة eLearnSecurity يتم أخذها في موقع ine (مسار الأمان السيبراني) و يتم أخذ الشهادة عليها بعد الاختبار في [موقع الشركة](#)



NETWORK PENTESTER



PURPLE TEAM MEMBER



ENTERPRISE DEFENDER



غير موجودة في أي مسار

WEB APPLICATION PENTESTER



ADVANCED PENTESTER



INCIDENT RESPONDER



يقم موقع ine دوره PTS مجاناً (لكن لديك وصول محدود للمعامل)

ممكن الحصول على الدورة عبر التسجيل في الموقع [هنا](#) ثم تأكيد تفعيل الحساب عبر رسالة البريد الإلكتروني التي ستصلك بعد التسجيل

الآن انت جاهز للبدأ كل ما عليك هو التوجه [لصفحة الدورة](#) وتسجيل الدخول ثم زيداً التعلم ☺

OFFENSIVE SECURITY®



COURSES AND CERTIFICATIONS

Offensive Security certifications are the most well-recognized and respected in the industry. Courses focus on real-world skills and applicability, preparing you for real-life challenges. Online, live, and in-house courses available.

OVERVIEW AND PRICING

START HERE

ADVANCED FOR WEB

ADVANCED FOR PENTEST

NETWORK SECURITY

EXPERT LEVEL FOR EXPLOIT DEVELOPERS

PENETRATION TESTING WITH KALI LINUX (PWK)

ADVANCED WEB ATTACKS & EXPLOITATION (AWAE)

EVASION TECHNIQUES AND BREACHING DEFENSES (PEN-300)

WIRELESS ATTACKS (WIFU)

ADVANCED WINDOWS EXPLOITATION (AWE)



EVERYTHING STARTS WITH PWK

Penetration Testing with Kali Linux (PWK) is a self-paced online course. Students learn the latest ethical hacking tools and techniques to become effective penetration testers. Learning materials include:

- A course guide
- Video lectures
- Active student forums
- Access to a virtual penetration testing lab

Students learn to conduct a penetration test from start to finish and practice techniques safely and legally. The course offers hands-on experience within a target-rich, diverse, and vulnerable network environment.

To earn the coveted OSCP certification, students must complete PWK and pass a 24-hour exam.

FREE RESOURCES: Offensive Security also provides free, open source courses that focus on introductory topics. Check out [Kali Linux Revealed](#) and [Metasploit Unleashed](#).

للمزيد من المعلومات عن
التدريب والشهادات :
[موقع الشركة](#)

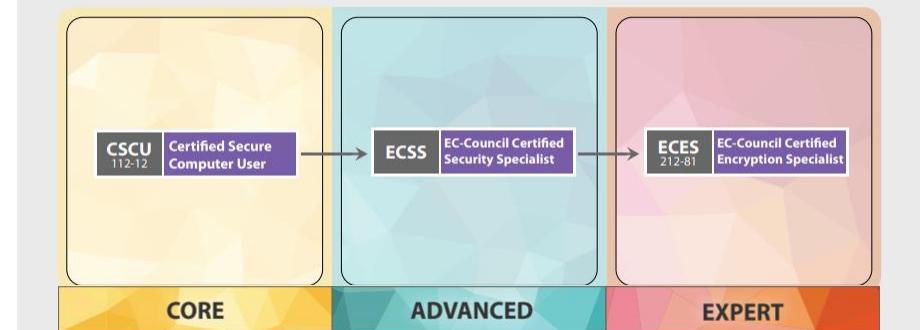
Penetration Testing		
Course	Description	
PEN-200	Penetration Testing with Kali Linux	\$999+
	PEN-200 is our foundational penetration testing course. Students learn the latest tools and techniques, and practice them in a virtual lab.	EARN YOUR OSCP
PEN-210	Offensive Security Wireless Attacks	\$450
	PEN-210 trains students to audit, compromise, and secure wireless devices. Get greater insight into the wireless security field with topics like packet interaction and complex WPA attack techniques.	EARN YOUR OSWP
PEN-300	Evasion Techniques and Breaching Defenses	\$1299+
	Take your penetration testing skills to the next level. PEN-300 teaches advanced penetration techniques, including bypassing security mechanisms and evading defenses.	EARN YOUR OSEP

Penetration Testing	Web Application	Exploit Development
Course	Description	
WEB-300	Advanced Web Attacks and Exploitation	\$999+
	Specialize in web application security with WEB-300. From XSS attacks to advanced SQL injections, learn how to exploit and secure web apps using white box pentesting methods.	EARN YOUR OSWE

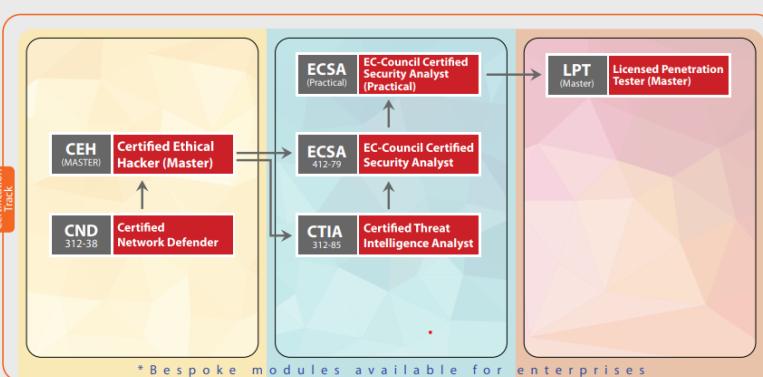
Penetration Testing	Web Application	Exploit Development
Course	Description	
EXP-401	Advanced Windows Exploitation	
	EXP-401 is the most difficult course offered by Offensive Security. Tackle advanced topics such as DEP and ASLR evasion, heap spraying, function pointer overwrites, and more.	EARN YOUR OSEE



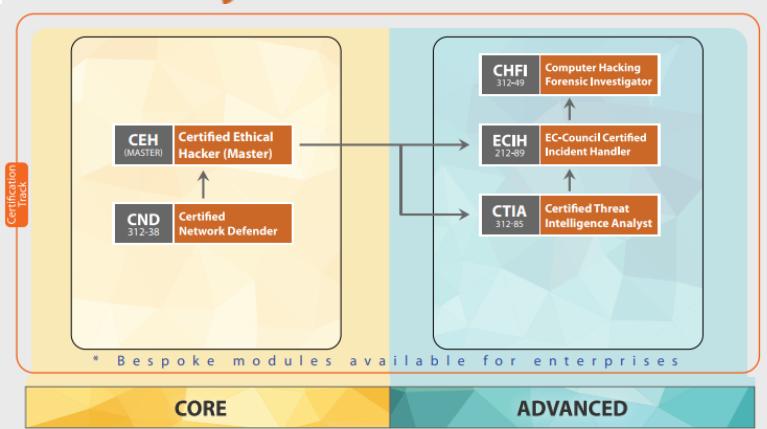
Foundation Track



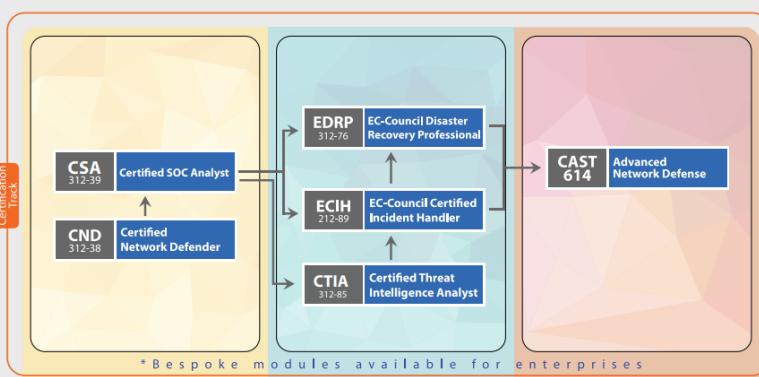
Vulnerability Assessment & Penetration Testing (VAPT)



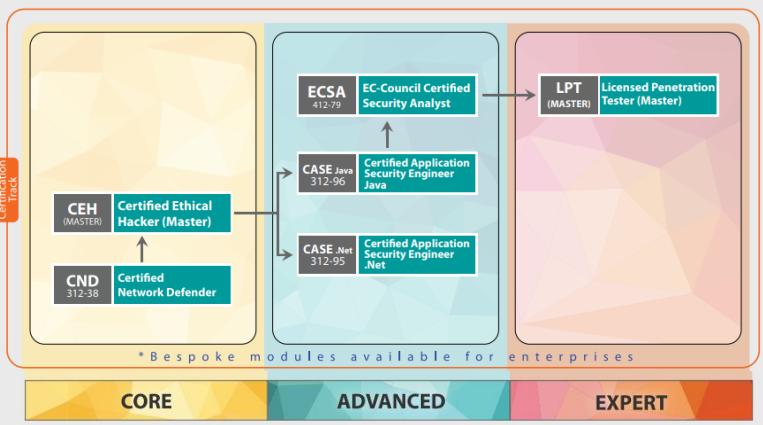
Cyber Forensics



Network Defense and Operations



Software Security



Governance



للمزيد من المعلومات عن التدريب و الشهادات : [ملف من الشركة](#)



قامت شركة SANS المعروفة بالتدريب في مجال الأمن السيبراني بتشكيل برنامج "شهادة ضمان المعلومات العالمية" (GIAC) ليصبح جهة الاعتماد التي تقدم شهادات للدورات التدريبية الخاصة بها

DIGITAL BADGES

ANNOUNCING GIAC'S NEW DIGITAL BADGE PROGRAM!

TO LEARN MORE ABOUT THIS ONE-CLICK VERIFICATION, DIGITAL REPRESENTATION OF YOUR GIAC CERTIFICATION, VISIT THE LINK IN THIS POST!

للمزيد من المعلومات عن التدريب والشهادات: [موقع الشركة](#)



1. BASELINE SKILLS

- Core Techniques** - Prevent, Defend, Maintain
2 COURSES
- Every Security Professional Should Know**
 - Security Essentials SEC401
 - Hacker Techniques SEC504

2. FOCUS JOB ROLES

- Monitoring & Detection** + Intrusion Detection, Monitoring Over Time
2 COURSES
- Penetration Testing** + Vulnerability Analysis, Ethical Hacking
3 COURSES
- Incident Response & Threat Hunting** + Host & Network Forensics
3 COURSES

3. CRUCIAL SKILLS, SPECIALIZED ROLES

- Cyber Defense Operations** + Harden Specific Defenses
9 COURSES
- Specialized Penetration Testing** + Focused Techniques & Areas
9 COURSES
- Threat Intel & Forensics** + Specialized Investigative Skills
7 COURSES
- Cloud Security** + Design, Develop, Procure & Deploy
5 COURSES
- Industrial Control Systems** +
4 COURSES

Security Management + Managing Technical Security Operations
2 COURSES

Advanced Management + Advanced Leadership, Audit, Legal
5 COURSES

Introduction to Cyber Security SEC301

CISSP® Training MGT414



Red Hat

للمزيد من المعلومات عن التدريب و الشهادات: [موقع الشركة](#)



LEARN MORE AT WWW.REDHAT.COM/TRAINING

Training and certification paths



للمزيد من المعلومات عن التدريب و الشهادات: [موقع الشركة](#)



New to
cybersecurity?

START HERE ►►►

CYBERSECURITY FOUNDATIONS CERTIFICATIONS - 100 LEVEL COURSES

CSA1&2™

Security Awareness 1 & 2

CHT™

Hardware Systems Technician

COST™

Operating Systems Technician

CNP™

Network Principles

CSP™

Security Principles

mile2 Cybersecurity Certifications

ROLE-BASED CERTIFICATIONS		INTERMEDIATE - 200 LEVEL COURSES	SPECIALIZATION - 300 LEVEL COURSES	ADVANCED - 400 LEVEL COURSES	
MANAGEMENT	IS Management & Leadership	C)ISSM™ Information Systems Security Manager	C)ISSO™ Information Systems Security Officer ISCAP™ IS Certification and Accreditation Professional	IS20™	IS20 Controls
	Healthcare	C)ISSM™ Information Systems Security Manager	C)ISSO™ Information Systems Security Officer	C)SLO™	Security Leadership Officer
RECOVERY	Incident Handling	C)ISSM™ Information Systems Security Manager	C)ISSO™ Information Systems Security Officer	C)IHE™	Incident Handling Engineer
	Forensics & Investigations	C)DFE™ Digital Forensics Examiner	C)NFE™ Networks Forensics Examiner C)CSA™ Cyber Security Analyst	C)VFE™	Virtualization Forensics Examiner
PREVENTION	Disaster Recovery	C)ISSM™ Information Systems Security Manager	C)ISSO™ Information Systems Security Officer	C)DRE™	Disaster Recovery Engineer
	Penetration Testing & Ethical Hacking	C)PEH™ Professional Ethical Hacker	C)PTE™ Penetration Testing Engineer	C)PTC™	Penetration Testing Consultant
	Application & Secure Coding	C)PEH™ Professional Ethical Hacker	C)PTE™ Penetration Testing Engineer	C)PSH™	Powershell Hacker
	Cloud Security & Virtualization	C)VE™ Virtualization Engineer	C)VSE™ Virtualization Security Engineer	C)SWAE™	Secure Web Application Engineer
	Auditing	C)ISSM™ Information Systems Security Manager	C)ISSO™ Information Systems Security Officer	C)CSO™	Cloud Security Officer
				C)ISSA™ C)ISMS-LA™ C)ISMS-LI™	Information Systems Security Auditor IS Management Systems Lead Auditor IS Management Systems Lead Implementer

CYBER WARFARE

RED vs BLUE



ELECTIVES

C)VA™ Certified Vulnerability Assessor

C)ISRM™ Certified Information Systems Risk Manager



Accreditations

NICCS



*Includes Cyber Range Labs

www.mile2.com

Phone: 813-920-6799

Toll Free: 800-816-4532

Email: information@mile2.com

للمزيد من المعلومات عن التدريب والشهادات: [موقع الشركة](#)



INSPIRING A SAFE AND SECURE CYBER WORLD.

CISSP - Certified Information Systems Security Professional



Summary:

The most-esteemed cybersecurity certification in the world. The CISSP recognizes information security leaders who understand cybersecurity strategy, as well as hands-on implementation. It shows you have the knowledge and experience to design, develop and manage the overall security posture of an organization. Are you

SSCP - Systems Security Certified Practitioner



Summary:

A global IT security certification. The SSCP recognizes your hands-on, technical abilities and practical experience. It shows you have the skills to implement, monitor and administer IT infrastructure using information security policies and procedures — ensuring the confidentiality, integrity and availability of data.

CCSP - Certified Cloud Security Professional



Summary:

The premier cloud security certification. One of the hottest certifications on the market today. The CCSP recognizes IT and information security leaders who have the knowledge and competency to apply best practices to cloud security architecture, design, operations and service orchestration. It shows you're on the forefront of

CAP - Certified Authorization Professional



Summary:

An information security certification aligning with the Risk Management Framework (RMF). The CAP recognizes your knowledge, skills and abilities to authorize and maintain information systems within the RMF. It proves you know how to formalize processes to assess risk and establish security documentation.

CSSLP - Certified Secure Software Lifecycle Professional



Summary:

A global, vendor-neutral certification to recognize those with leading software and application security skills. The CSSLP recognizes your expertise and ability to incorporate security practices — authentication, authorization and auditing — into each phase of the SDLC.

HCISPP - HealthCare Information Security and Privacy Practitioner



Summary:

A global healthcare security certification. It bridges healthcare information security and privacy like no other certification! The HCISPP recognizes your knowledge and ability to successfully implement, manage or assess security and privacy controls for healthcare and patient information. It proves you have a strong foundation in healthcare risk, security and privacy, and you understand important healthcare regulations.

CISSP - ISSAP - Information Systems Security Architecture Professional



Summary:

Elite, specialized credentials that build upon the CISSP. These are optional pursuits for CISSPs who wish to prove their subject matter mastery. The CISSP Concentrations recognize your evolving expertise in information security architecture, engineering or management. As a CISSP-ISSAP, you prove your expertise developing, designing and analyzing security solutions. You also excel at giving risk-based guidance to senior management in order to meet organizational goals.

CISSP - ISSEP - Information Systems Security Engineering Professional



Summary:

Elite, specialized credentials that build upon the CISSP. These are optional pursuits for CISSPs who wish to prove their subject matter mastery. The CISSP Concentrations recognize your evolving expertise in information security architecture, engineering or management. As a CISSP-ISSEP, you show your keen ability to practically apply systems engineering principles and processes to develop secure systems.

CISSP - ISSMP - Information Systems Security Management Professional



Summary:

Elite, specialized credentials that build upon the CISSP. These are optional pursuits for CISSPs who wish to prove their subject matter mastery. The CISSP Concentrations recognize your evolving expertise in information security architecture, engineering or management. As a CISSP-ISSMP, you excel at establishing, presenting and governing information security programs. You also demonstrate deep management and leadership skills.

Associate of (ISC)² - Associate of (ISC)²



Summary:

A unique designation to validate your skills and rapidly advance toward certification. The Associate of (ISC)² proves your knowledge in cybersecurity.



CISA - Certified Information Systems Auditor

The CISA certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems. The recent quarterly IT Skills and Certifications Pay Index (ITSCPI) from Foote Partners ranked CISA among the most sought-after and highest-paying IT certifications. This certification is a must have for entry to mid-career IT professionals looking for leverage in career growth.



CRISC - Certified in Risk and Information Systems Control

ISACA's Certified in Risk and Information Systems Control™ (CRISC®) certification indicates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls. Gain instant recognition and credibility with CRISC and boost your career! If you are a mid-career IT professional with a focus on IT and cyber risk and control, CRISC can get you the leverage you need to grow in your career.



CISM - Certified Information Security Manager

ISACA's Certified Information Security Manager® (CISM®) certification indicates expertise in information security governance, program development and management, incident management and risk management. If you are a mid-career IT professional aspiring to senior management roles in IT security and control, CISM can get you the visibility you need.



CGEIT - Certified in the Governance of Enterprise IT

ISACA's Certified in the Governance of Enterprise IT® (CGEIT®) is unique and framework agnostic. It is the only IT governance certification that can give you the mindset to assess, design, implement and manage enterprise IT governance systems aligned with overall business goals. Get visibility at the executive level with CGEIT!



CSX-P - Cybersecurity Practitioner Certification

CSX®-P remains the first and only comprehensive performance certification testing one's ability to perform globally validated cybersecurity skills spanning five security functions – Identify, Protect, Detect, Respond, and Recover – derived from the [NIST Cybersecurity Framework](#). CSX-P requires that candidates demonstrate critical cybersecurity skills in a live, proctored, virtual environment that assesses their analytical ability to identify assets and resolve network and host cybersecurity issues by applying the foundational cybersecurity knowledge and skills required of an evolving cyber first responder. For more information, see the [CSX-P Exam Content Outline](#).



CDPSE - Certified Data Privacy Solutions Engineer

Modern privacy laws and regulations require organizations to implement privacy by design and by default into IT systems, networks, and applications. To do so, privacy professionals must partner with software developers, system and network engineers, application and database administrators, and project managers to build data privacy and protection measures into new and existing technology environments.



Available AWS Certifications

aws certified
Updated May 2019

Professional

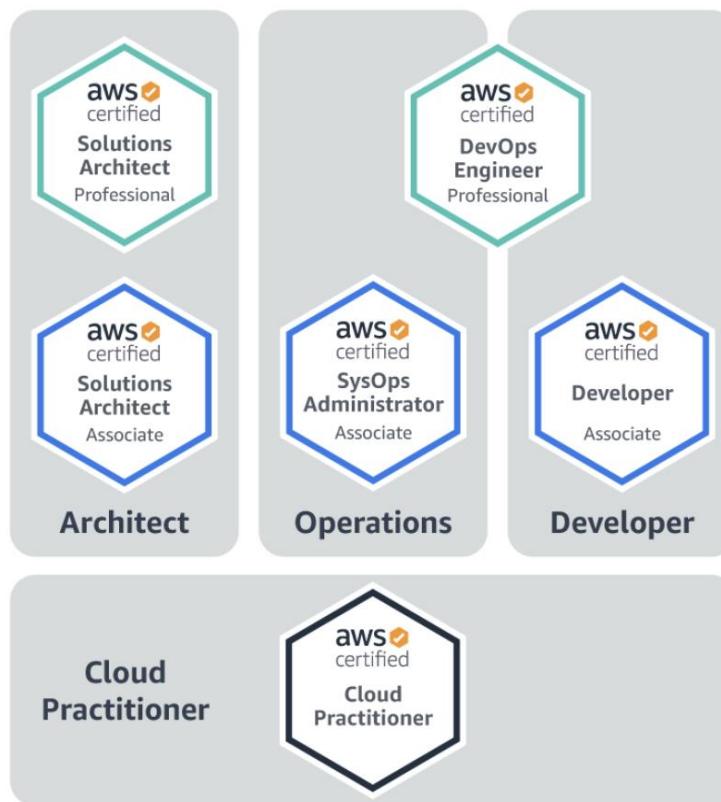
Two years of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud

Associate

One year of experience solving problems and implementing solutions using the AWS Cloud

Foundational

Six months of fundamental AWS Cloud and industry knowledge



Specialty

Technical AWS Cloud experience in the Specialty domain as specified in the **exam guide**



الخاتمة

أخيراً: لا تتردد في تعلم شيء معين (شبكات ، برمجة ، أنظمة تشغيل ، الإنجليزية ، ..) لأن التردد سيضيع وقتك و جهلك **ولكن شخص وقتاً معيناً (أسبوعين مثلاً) للبحث والاستفسار و شاور أهل الخبرة ثم صل الإستخاراة **و أبداً فوراً** بعد إنتهاء تلك المدة حتى لو لم تكن مستعداً تماماً .. لأنك مهما ارتكبت من الأخطاء في البداية فإنك مع الوقت سوف تصحح مسارك بنفسك وتلاحظ أن الأخطاء ستقل تدريجياً و هذا أفضل بكثير من إضاعة الوقت في التردد.**

"**و مُشَتَّتُ الْعَزَمَاتِ يُنْفِقُ عُمَراً *** حَيْرَانَ لَا ظَفَرٌ وَ لَا إِخْفَاقٌ**"



في الختام، أرغب في النتوصيه على أن الموضوع يحتاج إلى طويل و صبر و إجتهاد، لذا فإياك أن تيأس و تستسلم أمام الصعاب و سترى نتائج عظيمة بإذن الله

تم بحمد الله في : 1442/05/21 الموافق 2021/01/15

آخر تحديث : لا يوجد