



دبلومة الأمن السيبراني

دبلومة الأمن السيبراني

Cybersecurity Diploma

أحد أقوى الدبلومات وأكثرها طلباً، والمصنف ضمن المهن المستقبلية للعقد الجديد

ما هو الامن السيبراني ؟

الساير سبايس Cyber Space هو مصطلح يشمل كل ما يحتويه الفضاء الالكتروني من أنظمة معلومات بشقيه الهارد وير والسوفت وير، كالحواسيب الجوالات، السيرفرات، أنظمة تشغيل، الشبكات، البرمجيات: ومع العدد الكبير من الأجهزة المرتبطة بالشبكة ومستخدميها، وخاصة مع دخول مفهوم انترنت الأشياء، أصبح الحفاظ على أمن المعلومة أهم من المعلومة نفسها، وأضحى الهاجس الأمني الشغل الشاغل للعالم اليوم، لذا كان من المهم تواجده تخصص الأمن السيبراني، وهو الأمن الخاص لكل شيء في هذا العالم الافتراضي



خبير الأمن السيبراني هو الشخص الذي يعمل على حماية أنظمة المعلومات من الهجمات الرقمية. التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية.



يتضمن هذا الدبلوم تعليمات في التدابير التي يجب اتخاذها لاكتشاف ومنع أخطاء ونقاط الضعف في الشبكة، ويتضمن أوصافاً للهجمات الشائعة وطرق تكوين أنظمة التشغيل والخوادم وأجهزة التوجيه وجدران الحماية والبريد الإلكتروني. سيتمكن هذا الدبلوم صاحبه من الدخول في سوق العمل كمهندس أمن شبكات كما تؤهله للحصول على عدة شهادات معتمدة ومطلوبة في هذا المجال.

المحاور العلمية

المحاور التي يتضمنها الدبلوم هي:

إدارة الشبكات

أمن الشبكات

آليات الاختراق ومكافحتها

وذلك من خلال البرامج التالية:

المدة بالأسبوع	عدد الساعات	البرامج
1	16	Introduction to Networks
1	16	Network Security
1	14	Certified Network Defender
1	14	Web App Penetration Testing
2	24	Ethical Hacking and Network Defense
2	18	Computer Forensics
2	18	Advanced Ethical Hacking
10	120	المجموع



- اعداد الخبراء في مجال أمن المعلومات
- اعداد الخبراء في مجال مكافحة القرصنة والاختراق
- اعداد المتخصصين في جرائم أمن المعلومات
- التمكن من تحليل المشكلات الأمنية في أنظمة المعلومات
- التمكن من حل مشكلات الأمان في أنظمة المعلومات
- التمكن من تأمين البنية التحتية لتكنولوجيا المعلومات
- التمكن من حماية البيانات والمعلومات
- التمكن من تصميم البرمجيات الآمنة وتطويرها واختبارها وتقييمها
- التمكن من تطوير السياسات والإجراءات لإدارة مخاطر أمن المؤسسة
- التمكن من تقييم الدور البشري في أنظمة الأمن
- التمكن من تفسير الحوادث الأمنية والتحقيق فيها جنائياً
- التمكن من الفهم الجيد لآلية الاختراق
- التمكن من فهم الجانب الأخلاقي ونقاط الضعف في الهندسة الاجتماعي

أهم مسميات الوظائف في الأمن السيبراني

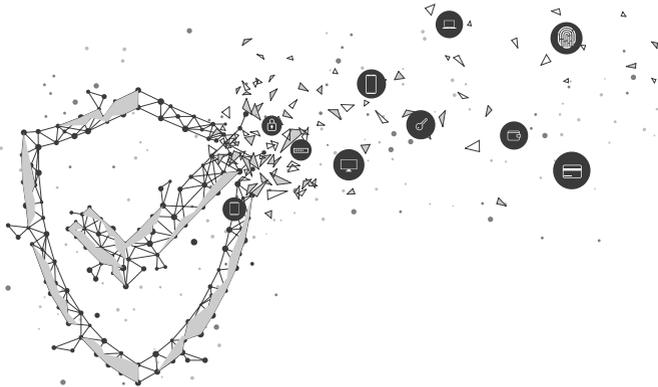


يعتبر خبير الأمن السيبراني مطلوب في كل الجهات الحكومية، والخاصة او حتى المستخدمين الأفراد، وتوجد قلة ونادرة في المتخصصين ولذلك فهو يعتبر من التخصصات المهمة والمطلوبة بقوة في السوق التقني العالمي والمحلي، وصاحب المهارة يستطيع الاختيار بين العروض بسهولة نظرا لكثرة الطلب وقلة المتخصصين.
لذا ينصح بالدخول في مجال الأمن السيبراني في هذه الفترة نظرا للحاجة الكبيرة في سوق العمل

مجالات العمل

- خبير طوارئ
- محلل الاختراقات الأمنية
- محلل البرمجيات الخبيثة

- خبير أمن معلومات
- خبير اختبار اختراق أنظمة المعلومات
- مدير قسم أمن المعلومات
- محقق جرائم حاسوبية / جرائم أمن معلومات
- خبير أدلة جنائية في أمن المعلومات
- ضابط حماية البيانات
- محلل أمني
- مهندس أمني
- مهندس أمن شبكات
- مطور برامج الأمن الذكية



البرامج المقدمة في الدبلومة

اسم البرنامج: Introduction to Network



هذا القسم موجه للمتدربين الذين يرغبون في الدخول على مجال الشبكات، حيث أنه يغطي كافة أساسيات الشبكات من مكونات الشبكة وطرق وصلها والتعامل مع أنواع متعددة من أجهزة الشبكة والاختلافات فيما بينها. يعد هذا القسم مدخل لدبلومة الأمن السيبراني كما أنه يؤهل المتدرب للتقدم على شهادة Network+.

موضوعات دروس البرنامج	
Introducing Computer Networks	الدرس الأول
Dissecting the OSI Model	الدرس الثاني
Identifying Network Components	الدرس الثالث
Understanding Ethernet	الدرس الرابع
Working with IP Addresses	الدرس الخامس
Routing Traffic	الدرس السادس
Introducing Wide-Area Networks	الدرس السابع
Connecting Wirelessly	الدرس الثامن
Using Command-Line Utilities	الدرس التاسع
Managing and securing a Network	الدرس العاشر
Troubleshooting Network Issues	الدرس الحادي عشر

تعد شبكات الانترنت المدخل الرئيسي للهاكرز لتنفيذ مخططاتهم، لذلك في هذا القسم سنتعرف على عالم الجرائم السيبرانية، والمخاطر التي تهدد الشركات والمؤسسات والأفراد من هذه الجرائم، بالإضافة الى التعرف على اهم الاجهزة التي يمكن اضافتها للشبكة لحمايتها من الاختراقات، واهمية هذه الاجهزة، وطرق تعريفها والاستفادة منها، الى جانب تعلم بعض الأساليب المتبعة عالميا لتقليل خطر واحتمالية اختراق الشبكة. يؤهل هذا القسم المتدرب للتقدم لامتحان شهادة Security+.



موضوعات دروس البرنامج

Mastering Security Basics	الدرس الأول
Exploring Control Types and Methods	الدرس الثاني
Understanding Basic Network Security	الدرس الثالث
Securing Your Network	الدرس الرابع
Securing Hosts and Data	الدرس الخامس
Understanding Malware and Social Engineering	الدرس السادس
Identifying Advanced Attacks	الدرس السابع
Managing Risk	الدرس الثامن
Preparing for Business Continuity	الدرس التاسع
Understanding Cryptography	الدرس العاشر
Exploring Operational Security	الدرس الحادي عشر

اسم البرنامج: Certified Network Defender(CND)



تعتمد الشركات الحكومية والخاصة الكبيرة او الصغيرة على الشبكات للتواصل فيما بينها في ربط البيانات وتخزين البيانات الهامة. يُعتبر إختراق الشبكات من أخطر التهديدات لاي جهة ومن أهم الأسباب لسرقة البيانات او إتلافها. هذه القسم تحضرك لأختبار شهادة Certified Network Defender. سوف تتدرب بشكل تطبيقي على مفهوم الشبكات وطرق حمايه والكشف والاستجابة والتنبؤ. وكيفية رفع مستوى الأمان والحماية للشبكات في الأجهزة والبرمجيات لإنشاء نظام دفاع قوي وفعال لجميع أجهزة الشبكة

موضوعات دروس البرنامج	
Network Attacks and Defense Strategies	الدرس الأول
Administrative Network Security	الدرس الثاني
Technical Network Security	الدرس الثالث
Network Perimeter Security	الدرس الرابع
Endpoint Security-Windows,Linux Systems	الدرس الخامس
Endpoint Security- Mobile Devices	الدرس السادس
Endpoint Security-IoT Devices	الدرس السابع
Administrative Application Security	الدرس الثامن
Data Security	الدرس التاسع
Enterprise Virtual,Cloud and Wireless Network Security	الدرس العاشر
Network Traffic,Logs Monitoring and Analysis	الدرس الحادي عشر
Business Continuity and Disaster Recovery	الدرس الثاني عشر
Threat Assessment with Attack Surface Analysis	الدرس الثالث عشر

اسم البرنامج: Ethical Hacking and Network Defense



أفضل وسيلة للدفاع هي الهجوم، في هذا القسم سنتعرف على أبرز الأساليب والاستراتيجيات التي يستخدمها الهاكر لإتمام عملية الاختراق، كيف يقوم بتطبيقها وما المعلومات التي يحصل عليها، سيتم تطبيق هذه الأساليب في بيئة افتراضية بشكل قانوني، كما سيتم تعلم طرق الدفاع ضد كل نوع من أنواع هذه الأساليب. يؤهل هذا القسم المتدرب للتقدم لامتحان شهادة CEH.

موضوعات دروس البرنامج	
Ethical Hacking Overview	الدرس الأول
TCP/IP Concepts Review	الدرس الثاني
Network and Computer Attacks	الدرس الثالث
Footprinting and Social Engineering	الدرس الرابع
Port Scanning	الدرس الخامس
Enumeration	الدرس السادس
Programming for Security Professionals	الدرس السابع
Desktop and Server OS Vulnerabilites	الدرس الثامن
Embedded Operating Systems: The Hidden Threat	الدرس التاسع
Hacking Web Servers	الدرس العاشر
Hacking Wireless Networks	الدرس الحادي عشر
Cryptography	الدرس الثاني عشر
Network Protection Systems	الدرس الثالث عشر

اسم البرنامج: Web App Penetration Testing and Bug Bounty

تلعب مواقع الويب دورًا حيويًا في كل مؤسسة حديثة، ولكن إذا لم تختبر مؤسستك مواقع الويب الخاصة بها وتأمينها بشكل صحيح وفعال، فيمكن للهاكرز اختراق موقع الويب وإتلاف وظائف الأعمال وحتى سرقة البيانات، ويركز الهاكر بشكل متزايد على هذه الأهداف عالية القيمة لأنها موجهة للجمهور بشكل مباشر، سيتعرف الطلاب على نقاط ضعف مواقع الويب الشائعة، وكذلك كيفية التعرف عليها وإستغلالها بقصد إظهار التأثير المحتمل على الاعمال في حال تم اختراقها من قبل الهاكرز ، وأيضًا كيفية توثيق نقاط الضعف وإبلاغ المؤسسة

موضوعات دروس البرنامج	
Introduction To Web App Penetration Testing	الدرس الأول
Core Defense Mechanisms and Web Application Technologies	الدرس الثاني
Mapping the Application	الدرس الثالث
Bypassing Client-Side Controls	الدرس الرابع
Attacking Authentication	الدرس الخامس
Attacking Session Management	الدرس السادس
Attacking Access Controls	الدرس السابع
Attacking Data Stores	الدرس الثامن
Attacking Back-End Components	الدرس التاسع
Attacking Application Logic	الدرس العاشر
Attacking Users: Cross-Site Scripting	الدرس الحادي عشر
Attacking Users: Other Techniques	الدرس الثاني عشر
Reporting & Managing a Bug Bounty Program	الدرس الثالث عشر

الجريمة في الماضي كانت تتطلب من مرتكبها حركة وقوة جسدية ومعدات خاصة وقدرة على الاختباء وغيرها، اما الهاكر اليوم يحتاج جهاز كمبيوتر وانترنت فقط لسرقة بنك في بلد اخرى. لهذا السبب ظهر الاحتياج لمفهوم الادلة الالكترونية للجرائم الالكترونية computer forensic. في هذا القسم سنغطي كيفية الحصول على دلائل الكترونية على حدوث جريمة سيبرانية، وكيفية تحليل هذه الدلائل لمعرفة معلومات على الجريمة من حيث وقت حصولها طريقة ارتكابها، المعلومات التي تم تسريبها، الاجهزة التي تم اختراقها، تسلسل احداث الجريمة، الى جانب محاولة اتباع المكان الذي نفذت منه الجريمة.

موضوعات دروس البرنامج	
Real-World Incidents	الدرس الأول
IR Management Handbook	الدرس الثاني
Pre-Incident Preparation	الدرس الثالث
Getting the Investigation Started on the Right Foot	الدرس الرابع
Initial Development of Leads	الدرس الخامس
Discovering the Scope of the Incident	الدرس السادس
Live Data Collection	الدرس السابع
Forensic Duplication	الدرس الثامن
Network Evidence	الدرس التاسع
Enterprise Services	الدرس العاشر
Analysis Methodology	الدرس الحادي عشر
Investigating Windows Systems (Part 1 of 3)	الدرس الثاني عشر
Investigating Windows Systems (Part 2 of 3)	الدرس الثالث عشر
Investigating Windows Systems (Part 3 of 3)	الدرس الرابع عشر
Investigating Mac OS X Systems	الدرس الخامس عشر
Investigating Applications	الدرس السادس عشر
Malware Triage	الدرس السابع عشر
Report Writing	الدرس الثامن عشر
Remediation Introduction	الدرس التاسع عشر

يؤهل هذا القسم المتدرب
للحصول على شهادة





العالم السيبراني يتطور بشكل سريع ويومي، وأنواع جديدة من الهجوم يتم تطويرها من قبل الهاكر لتفادي طرق الدفاع المعروفة، هذه الأنواع أكثر تعقيدا وفاعلية، في هذا القسم سنغوص أعمق في طرق متطورة من الاختراق وكيفية استغلال هذه الاختراقات في المستقبل من قبل الهاكر، الى جانب كيفية تجاوز الهاكر لبعض اساليب الدفاع المعتمدة. يؤهل هذا القسم المتدرب للتقدم لامتحان شهادة OSCP.

موضوعات دروس البرنامج

Using Kali Linux	الدرس الأول
Programming	الدرس الثاني
Using the Metasploit Framework	الدرس الثالث
Information Gathering	الدرس الرابع
Finding Vulnerabilities and Exploiting Domains	الدرس الخامس
Capturing Traffic	الدرس السادس
Exploitation	الدرس السابع
Password Attacks	الدرس الثامن
Client-Side Exploitation	الدرس التاسع
Social Engineering	الدرس العاشر
Bypassing Antivirus Applications	الدرس الحادي عشر
Post Exploitation Part 1	الدرس الثاني عشر
Post Exploitation Part 2	الدرس الثالث عشر

المدة الزمنية: 10 أسابيع 

عدد الساعات: 120 ساعة 

الرسوم: \$1000 

اللغة: العربية 

المدرسون 

نخبة من الخبراء والمتميزين وحملة الدكتوراه

المستوى المطلوب والخبرات السابقة 

لا يُشترط اي خبرات سابقة، فقط معرفة باستخدام الحاسب



00905013519000

00905352522205

00902124266620

digitalskillsa.com

sales@digitalskillsa.com