DSA
اكاديمية المهارات الرقمية
DIGITAL SKILLS ACADEMY

دبلومة
الأمن السيبراني

دبلومة الأمن السيبراني

Cybersecurity Diploma

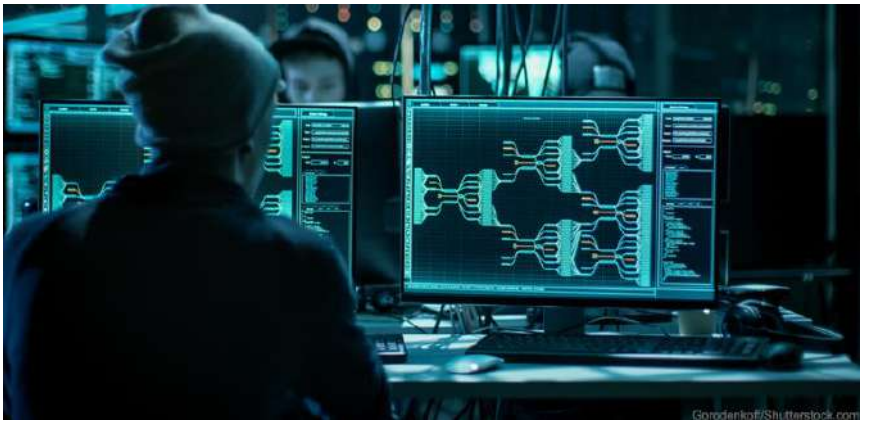
أحد أقوى الدبلومات وأكثرها طلباً، والمصنف ضمن المهن المستقبلية للعقد الجديد

ما هو الامن السيبراني ؟

السايبر 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 تواجد تخصص الأمن السيبراني، وهو الأمن الخاص لكل شي في هذا العالم الافتراضي

خبير الأمن السيبراني

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 أوصافًا للهجمات الشائعة وطرق تكوين أنظمة التشغيل والخوادم وأجهزة التوجيه وجدران الحماية والبريد الإلكتروني. سيمكن 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:

البرامج	عدد الساعات	المدة بالأسبوع
Introduction to Networks	16	1
Network Security	16	1
Cryptography for Computer Networks	14	1
Network Security Monitoring	14	1
Ethical Hacking and Network Defense	24	2
Computer Forensics	18	2
Advanced Ethical Hacking	18	2
المجموع	120	10

أهداف دبلومة الأمن السيبراني

- 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 جنائيًا
- التمكن من الفهم الجيد لآلية الاختراق
- التمكن من فهم الجانب الأخلاقي ونقاط الضعف في الهندسة الاجتماعي

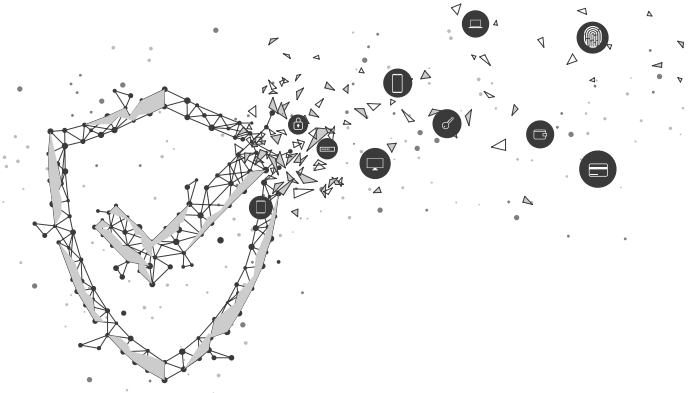
أهم مسميات الوظائف في الأمن السيبراني

يعتبر خبير الأمن السيبراني مطلوب في كل الجهات الحكومية، والخاصة او حتى المستخدمين الأفراد، وتوجد قله وندرة 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 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
- خبير طوارئ
- محلل الاختراقات الأمنية
- محلل البرمجيات الخبيثة



البرامج المقدمة في الدبلومة

اسم البرنامج: Introduction to Network

هذا القسم موجه للمتدربين الذين يرغبون في الدخول على مجال الشبكات، حيث أنه يغطي كافة اساسيات 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

اسم البرنامج: Network Security

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: Cryptography for Computer Networks

يعبتر الحفاظ على أمن المعلومات الشغل الشاغل للعالم اليوم، وأصبح من يملك المعلومات هو من يملك زمام القوة الاقتصادية والعسكرية، لذلك من أهم مجالات الأمن السيبراني هو حماية البيانات من التسريب او الوقوع في ايدي الخطأ، في هذا القسم سنغطي مفهوم تشفير البيانات، طرق وانواع التشفير، نقاط قوة وضعف كل نوع من هذه الانواع الى جانب الاساليب المتبعة من قبل الهاكرز لكسر التشفير.

موضوعات دروس البرنامج	
الدرس الأول	Encryption
الدرس الثاني	Randomness
الدرس الثالث	Cryptographic Security
الدرس الرابع	Block Ciphers
الدرس الخامس	Stream Ciphers
الدرس السادس	Hash Functions
الدرس السابع	Keyed Hashing
الدرس الثامن	Authenticated Encryption
الدرس التاسع	Hard Problems
الدرس العاشر	RSA
الدرس الحادي عشر	Diffie-Hellman
الدرس الثاني عشر	Elliptic Curves
الدرس الثالث عشر	TLS

اسم البرنامج: Network Security Monitoring

الجريمة السيبرانية تحتاج من الهاكر ساعات وأحيانا اسابيع وحتى أشهر لتنفيذها، لذلك أحد اهم طرق حماية الشبكة هي مراقبتها بشكل مستمر والتحرك مباشرة عند محاولة اي هاكر لبدء عملية سيبرانية ومحاولة امساكه قبل حصوله على مراده، في هذا القسم سنغطي أحد اهم وأشهر البرامج المستخدمة لهذا الغرض، سنتعرف على طريقة تركيبه وعمله، وكيفية استخدامه لمراقبة الشبكات بشكل كامل من مكان واحد، بالإضافة الى طرق استخدامه للامساك باي محاولة اختراق. يؤهل هذا القسم المتدرب للتقدم لامتحان شهادة Splunk Fundamentals 1.

موضوعات دروس البرنامج	
What is Machine Data	الدرس الأول
What is Splunk	الدرس الثاني
Installing Splunk	الدرس الثالث
Getting Data In	الدرس الرابع
Basic Searching	الدرس الخامس
Using Fields	الدرس السادس
Best Practices	الدرس السابع
SPL Fundamentals	الدرس الثامن
Transforming Commands	الدرس التاسع
Reports and Dashboards	الدرس العاشر
Pivot and Datasets	الدرس الحادي عشر
Lookups	الدرس الثاني عشر
Scheduled Reports and Alerts	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: Computer Forensics

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

يؤهل هذا القسم المتدرب
للحصول على شهادة

C|HFI™
Computer Hacking Forensic INVESTIGATOR

اسم البرنامج: Advanced Ethical Hacking

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

اسم البرنامج: Advanced Ethical Hacking

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: 9 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


C|EH
E|CSA
EC-Council
C|HFI
C|SA
L|PT


Security+
CompTIA
Get IT Certified
A+
CERTIFIED
Network+
CERTIFIED


TEKNOLOJI AKADEMI


CISCO
CISCO CERTIFIED CCNA SECURITY
CISCO CERTIFIED CCNA


OFFENSIVE
security


OFFENSIVE
security
OSWP
OFFENSIVE
security
OSCP