



تخطيط المسار الوظيفي في مجالات الأمن السيبراني

Career Path Planning in the Cybersecurity Field

الكاتبة: دلال بنت ناصر الحارثي

مقدمة:

مع تزايد التوجه للتحويل الرقمي في كثير من جهات العمل عالمياً ومحلياً، تزداد أهمية الأمن السيبراني لحماية بيانات وأصول الجهات من أي مخاطر سيبرانية. خاصة في ظل أزمة كوفيد-19، والتي تزايد معها اعتمادنا بشكل مكثف على الانترنت، حيث أصبحنا نعمل ونتعلم ونتسوق ونقوم بكافة أمور حياتنا عن بعد، ما نتج عنه زيادة التهديدات السيبرانية، وزيادة الطلب على وظائف الأمن السيبراني المختلفة.

كيف أبدأ في مجال الأمن السيبراني؟ سؤال يتبادر لذهن الكثيرين. هذه الوثيقة، تجيب بشكل فيه جزء من التفصيل عن هذا السؤال. الهدف من هذا المقال هو إثراء المحتوى العربي في مجال الأمن السيبراني، وتقديم الدعم للمهتمين بتعلم الأمن السيبراني أو بالعمل فيه، من خلال إيضاح الصورة الكبرى لوظائف الأمن السيبراني المختلفة. في بقية أجزاء هذا المقال، سأستعرض أبرز مجالات الأمن السيبراني، طبيعة العمل والأدوات المستخدمة في كل مجال، بالإضافة إلى أبرز الشهادات المهنية التي ينصح بها للاستعداد الأمثل للمنافسة على وظائف الأمن السيبراني المختلفة.

كل ما ورد في هذه الوثيقة هو نتاج سنوات طويلة من عملي في مجال الأمن السيبراني في شركات عالمية، ونتاج دراستي الأكاديمية في مرحلتي الماجستير والدكتوراه بجامعة كاليفورنيا إرفاين، وأبحاثي العلمية المنشورة في هذا المجال، وتجربتي في التحكيم العلمي لأبحاث المختصين والأكاديميين في المجال في مؤتمري WICyS 2020 and GHC 2020 وغيرها. ومعسكر الأمن السيبراني المكثف CyberSecurity Bootcamp والذي كنت جزءاً منه لمدة 8 أشهر. أضعها بين يديكم هنا للفائدة، ولنشر العلم، علها تضيء الطريق، وتساعد المهتمين في التغلب على عوائق الطريق.

بعد قراءة هذا المقال، سيكون لدى القاري تصور شمولي لوظائف الأمن السيبراني، يساعده في اختيار مساره الأقرب لاهتماماته وقدراته. الوظائف التي تم استعراضها هنا هي في مجال (1) الاستجابة للحوادث السيبرانية Incident Response، (2) التحقيق الجنائي الرقمي Digital Forensics، (3) أمن الخدمات السحابية Cloud Security، (4) إدارة أمن المعلومات والحوادث Security Information and Event Management (SIEMs)، (5) الاختراق الأخلاقي واختبار الاختراق Penetration Testing and Ethical Hacking، (6) أمن الشبكات Network Security، و (7) سياسات الأمن السيبراني Cybersecurity Policies.



أولاً: الاستجابة للحوادث السيبرانية Incident Response:

هناك الكثير من الحوادث السيبرانية التي من الممكن أن تحدث في أي جهة عمل، دون استثناء، مثل هجمات حجب الخدمات (DoS) أو Denial of Service (DDoS)، سرقة أو ضياع الأجهزة Physical Theft، تسريب البيانات Data Breaches، أو هجمات الهندسة الاجتماعية Social Engineering والتي تتمثل في بريد التصيد Phishing أو مكالمات التصيد Vishing أو انتحال الشخصية Impersonation، أو غير ذلك.

بالمقابل، كموظفين في قسم الاستجابة للحوادث السيبرانية في الجهة، لدينا العديد من الأدوات التي تساعدنا في اكتشاف هذه الحوادث السيبرانية، والتصدي لها، مثل جدر الحماية Firewalls، برامج مكافحة الفيروسات Anti-Virus، نظم منع الاختراقات Intrusion Prevention Systems، وغير ذلك. عندما تفشل هذه الأدوات في كشف التهديدات السيبرانية والتصدي لها، يأتي دور فريق الاستجابة للحوادث الأمنية للتحقيق في هذه الحادثة، وأسبابها، وطرق علاجها، وتقنيات التفاعلي المستقبلي لمثل هذه الحوادث. بعض الجهات لديها فريقين لهذا الغرض، فريق المراقبة Monitoring Team وفريق الاستجابة للحوادث الأمنية Incident Response Team، والبعض الآخر يدمج المهمتين في فريق واحد تحت مسمى فريق الاستجابة للحوادث الأمنية.

يقوم فريق الاستجابة للحوادث السيبرانية بـ (1) التجهيز Preparation أو الإعداد للتحقيق في هذه الحادثة من خلال إعداد خطة محكمة لذلك. يحتاجون لإتمام عملهم لمراجعة خريطة/مخطط الشبكة Network Map، وكتابة خطة لمتابعة الحادثة، مع كتابة أسماء وبيانات الأشخاص المسؤولين عن عن عمليات المراقبة والاستجابة لهذه الحادثة. بعد ذلك، تبدأ عملية (2) الكشف والتحليل Detection and Analysis، من خلال مراجعة سجلات/ملفات الشبكة Network Logs وتنبيهات برامج الكشف عن الفيروسات Intrusion Prevention System (IPS) و Intrusion Detection System (IDS). لعل أحد الأمثلة عليها Snort والذي أصبح متضمناً داخل أكثر برامج مكافحة الفيروسات الجديدة Next Generation Anti-Virus. في هذه الخطوة أيضاً يتم مراقبة حركة مرور الشبكة عن كثب Network Traffic Anomalies، كما يتم تحديد درجة أولوية وخطورة هذه الحادثة، سواءً أكانت قليلة الخطورة Low Risk، متوسطة الخطورة Medium Risk، أو بالغة الخطورة High Risk. بعد أن تتم عملية التحليل، يأتي دور (3) الاحتواء والقضاء على الملفات الخبيثة Containment, Eradication, and Recovery. يتم ذلك من خلال عزل الأجهزة المصابة عن بقية الشبكة Isolation، تعطيل حساباتهم على الشبكة Disabling the Breached User Accounts، وحذف الملفات الخبيثة والملفات المصابة. يتم هنا أيضاً تحديد نوع الهجمة السيبرانية، وطريقة تنفيذها، ونوع الثغرة Vulnerability التي استهدفتها. يتم أيضاً مراقبة الشبكة بعد القضاء على الفيروس للتأكد من أنها سليمة تماماً من آثار الحادثة السيبرانية، كما يتم استعادة الملفات على هذه الأجهزة من النسخ الاحتياطية Backups. بعد ذلك، تأتي الخطوة الرابعة والأخيرة، وهي (4) ما بعد الحادثة السيبرانية Post Incident، والتي تتمثل في كتابة تقرير يحتوي الدروس المكتسبة من هذه الحادثة، كما يتطلب الأمر عقد اجتماعات لإعادة تقييم خطة الاستجابة للحوادث الأمنية التي تمت كتابتها في الخطوة الأولى، كما يتم هنا تحديث لتنبيهات الأنظمة System Alerts للتأكد من استلامنا لتنبيهات في حال حدوث حوادث مماثلة مستقبلاً.



لكن، هنالك أسئلة هامة هنا ينبغي لفريق الاستجابة للحوادث الأمنية التفكير فيه والتحقق منه. كيف يمكن التأكد من خلو النسخ الاحتياطية من وجود الفيروسات أو الملفات الخبيثة، قبل أن يتم عمل استعادة الملفات منها؟ ماذا لو كانت مصابة بالفيروس، ولم يتم اكتشاف ذلك بعد؟ ماذا لو تم اكتشاف الفيروس وتم تشفير كل هذه الملفات؟ هل يوجد لدى الجهة خطة حكيمة لإدارة النسخ الاحتياطية؟ متى يتم عمل هذه النسخ الاحتياطية؟ هل يتم استخدام الخدمات السحابية لذلك والتي توفر لنا خاصية الاحتفاظ بنسخ كثيرة Versioning والرجوع لأي نقطة إن احتجنا ذلك؟ هل يوجد هنالك نسخة خارج شبكة الانترنت Offline Copy؟ هل هذه النسخة محمية ومشفرة؟ أين يتم الاحتفاظ بمفاتيح فك التشفير؟ هل يتم استخدام أدوات إدارة كلمات المرور والمفاتيح الهامة Secret Management Tools؟ من يمتلك صلاحية الوصول إليها؟

عطفاً على الأسئلة أعلاه، قد يتم استلام تنبيهات خاطئة عن وجود مخاطر سيبرانية أو ملفات خبيثة في الأنظمة والشبكات. كيف يمكننا التأكد من أن هذا التنبيه هو صحيح أو خاطيء؟ على سبيل المثال، قد يتم تنبيهنا عن وجود ملف خطير اسمه Trojan في الشبكة، لكن قد لا يكون هذا فيروساً، ففي عالم طب الأسنان، يسمى النظام المستخدم لديهم بـ Trojan! بالتالي، يمكن التحقق من ذلك من خلال مقارنة الـ Hashing لهذا الملف، حيث أنه من المعروف أن الـ Hashing لا يتغير إلا بتغيير محتوى الملف، لا بتغيير البيانات الإضافية عن الملف Metadata.


للتعرف عن قرب عن طريقة العمل في هذا النوع من الوظائف، يمكن التدريب عملياً باستخدام أجهزة افتراضية يتم تحميلها على الجهاز باستخدام Virtual Box مثلاً. يمكن الاستعانة بموقعي Malware Traffic Analysis والذي يحتوي العديد من التدريبات في هذا النطاق، وموقع Virus Total لمقارنة الـ Hashing لهذه الملفات.

رابط الموقع

<https://www.malware-traffic-analysis.net/>



Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community

FILE	URL	SEARCH
<div></div> <p>By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.</p>		



رابط الموقع

<https://www.virustotal.com/gui/home/upload>

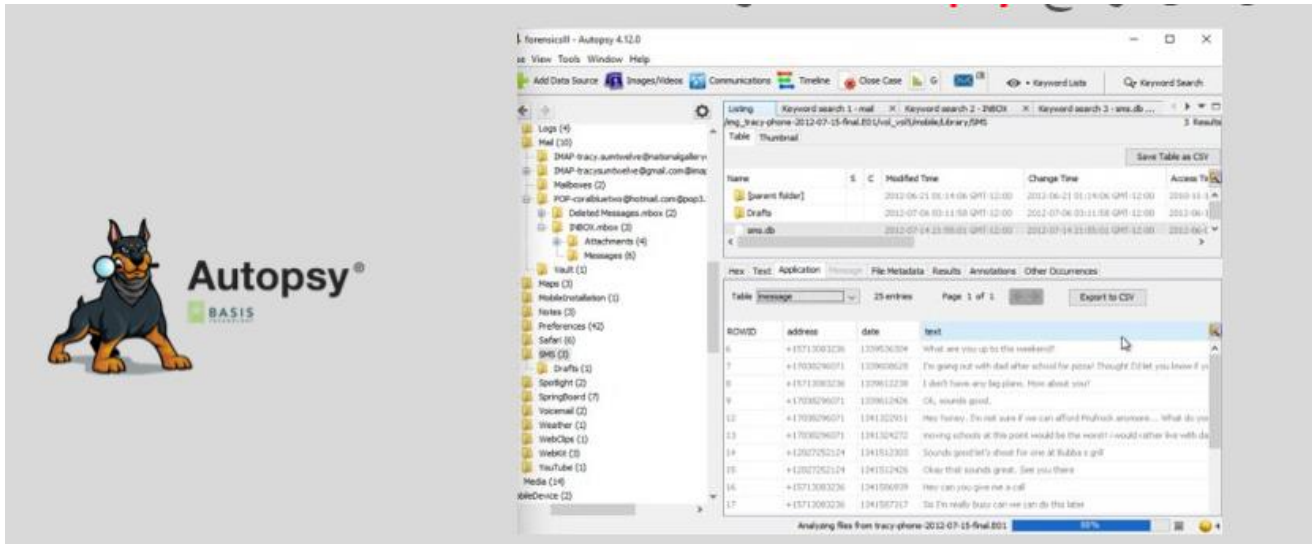
هناك بعض المسميات الوظيفية في هذا المجال، مثل محلل عمليات الأمن السيبراني، محلل مركز عمليات الأمن السيبراني، وغير ذلك.

ثانياً: التحقيق الجنائي الرقمي Digital Forensics:

هناك عدة أنواع للتحقيق الجنائي الرقمي، تختلف باختلاف الوسيط الذي يتم التحقيق فيه، مثلاً لدينا Disk Forensics, Memory Forensics, Network Forensics, Email Forensics, Mobile Forensics, Cloud Forensics, Software Forensics, and Drone Forensics.

منهجية التحقيق الجنائي الرقمي تتمثل في (1) جمع الأدلة Collection، وهي مرحلة، يتم من خلالها اتخاذ قرارات حول ما يتم جمعة من بيانات، وما أفضل البيانات التي تدعم "القضية". ينبغي هنا جمع كافة الأدلة والتأكد من قبولها من المحكمة. بعد ذلك، يأتي دور (2) الحفاظ على الأدلة Preserving Evidence. في هذه الخطوة، ينبغي التأكد من أن العمل لا يتم على النسخ الأصلية من الأدلة، بل على نسخة إضافية منها Read Only Master Copy، للحفاظ على هذه الأدلة، وعدم المساس بها. بعد ذلك يتم البدء بخطوة (3) التحليل Analysis، والتي تسمى بـ Dead Analysis، من خلال تحليل كافة الأدلة وتدوين وقت التحليل، وتاريخه، والبرامج المستخدمة في التحليل، والنتائج المتوصل إليها. بعد إتمام المراحل الثلاثة السابقة، يأتي دور (4) كتابة وتقديم التقرير Reporting. هذا التقرير ينبغي أن يحتوي على الخطوات والاختبارات التي تم عملها، وقت وجود هذه الأدلة، والخاتمة المتوصل إليها والنتائج التي وجدت في هذه القضية.

للتعرف عن قرب عن طريقة العمل في هذا النوع من الوظائف، يمكن التطبيق العملي باستخدام برنامج Autopsy وهو أحد أدوات كالي لينكس Kali Linux.



هناك أيضاً تمرين يمكن من خلاله تحميل الملفات والتطبيق لأغراض تعليمية، متاح على هذا الموقع:



<https://digitalcorpora.org/corpora/scenarios/national-gallery-dc-2012-attack>

يمكن تحميل الأدلة، والعمل على تحليلها من خلال أداة Autopsy.

← → ↻ 🏠 ⓘ <https://digitalcorpora.org/corpora/scenarios/national-gallery-dc-2012-attack>

📁 Farmers 📁 FI 📁 Dalal

📁 Robbers

Evidence

The seized evidence has been processed for you by the ingest team of the crime laboratory. You have been provided with the following data:

- Carry's phone on 2012-07-15 [ZIP] [FTK Logical Dump]
- Carry's tablet on 2012-07-16 [E01] [TAR]
- Email messages generated by the spyware installed on Tracy's Macbook Air and that were periodically emailed to Joe [ZIP]
- Tracy's phone on 2012-07-15 (encase) [L01] [ZIP]
- Tracy's phone on 2012-07-15 (other extraction tools) [E01] [tar]
- Tracy's external hard drive [E01]
- Tracy's home computer [E01] [E02]
- Exterior Network Packet Dumps
 - exterior 2012-07-06 [exterior-2012-07-06.pcap](#)
 - exterior 2012-07-09 [exterior-2012-07-09.pcap](#)
 - exterior 2012-07-10 [exterior-2012-07-10.pcap](#)
 - exterior 2012-07-12 [exterior-2012-07-12.txt](#)
- Interior Network Packet Dumps
 - interior 2012-07-06 [interior-2012-07-06.pcap](#)
 - interior 2012-07-09 [interior-2012-07-09.pcap](#)
 - interior 2012-07-10 [interior-2012-07-10.pcap](#)
 - interior 2012-07-12 [interior-2012-07-12.txt](#)

ثالثاً: أمن الخدمات السحابية Cloud Security Engineer:

من أبرز مزودي الخدمات السحابية، مرتبة حسب قوتها في سوق الخدمات السحابية عالمياً Amazon Web Service (AWS)، Microsoft Azure، و Google Cloud Platform (GCP).



للتعرف عن قرب عن طريقة العمل في هذا النوع من الوظائف، ينصح بالتطبيق العملي على أحد هذه المواقع أعلاه. وبشكل عام، إذا تم التعلم على AWS مثلاً، يمكن للشخص فهم الحوسبة السحابية والعمل بالتالي على أي موقع آخر مثل Azure أو GCP. لذلك يقال، The Cloud is the Cloud! No matter what platform you're using. قد يكون الاختلاف بين مزودي الخدمات السحابية هو في مسمى الخدمات فقط Service Names. الموقع التالي يوضح الفرق بين مسميات الخدمات في AWS and Azure.

<https://docs.microsoft.com/en-us/azure/architecture/aws-professional/services>

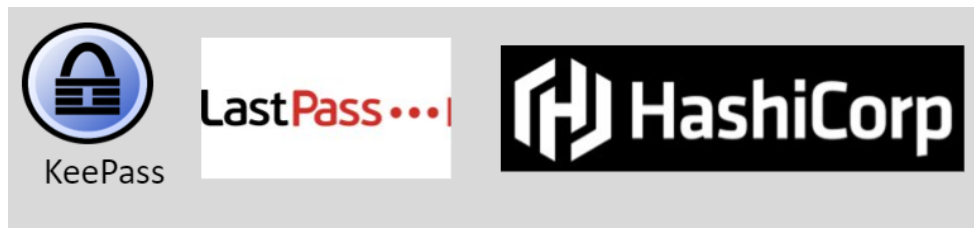
- by title
- view
- Services comparison
- for GCP Professionals
- : Azure Well-Architected
- rk
- atterns
- gies
- achine Learning
- ics
- hain
- jte
- ners
- ases
- per Tools
- is
- availability
- ad PDF

AI and machine learning

AWS service	Azure service	Description
SageMaker	Machine Learning	A cloud service to train, deploy, automate, and manage machine learning models.
Alexa Skills Kit	Bot Framework	Build and connect intelligent bots that interact with your users using text/SMS, Skype, Teams, Slack, Office 365 mail, Twitter, and other popular services.
Lex	Speech Services	API capable of converting speech to text, understanding intent, and converting text back to speech for natural responsiveness.
Lex	Language Understanding (LUIS)	Allows your applications to understand user commands contextually.
Polly, Transcribe	Speech Services	Enables both Speech to Text, and Text into Speech capabilities.
Rekognition	Cognitive Services	Computer Vision : Extract information from images to categorize and process visual data.

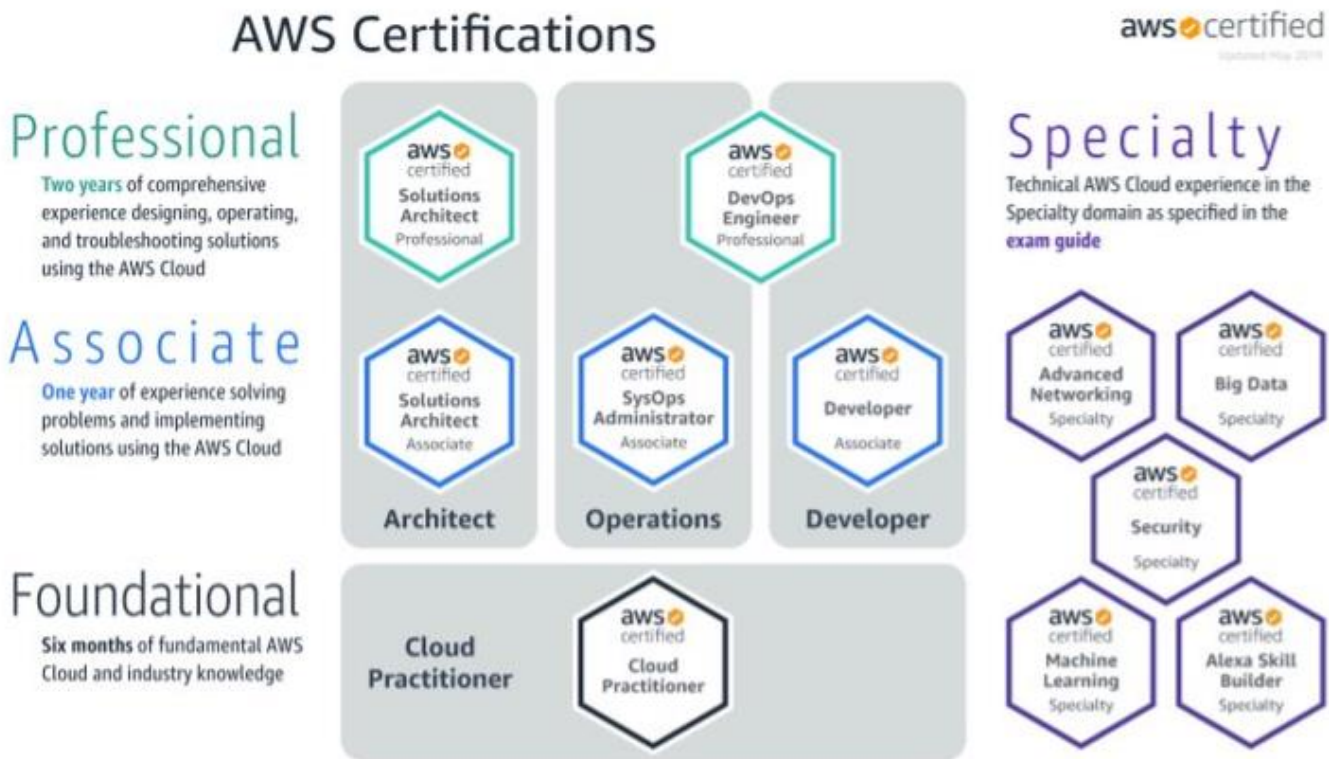
[Face](#): Detect, identify, and analyze faces in photos

يتركز عمل فريق أمن الخدمات السحابية حول (1) العمل ضمن فريق متكامل يسمى بـ Cloud Center of Excellence (CCoE)، والذي يحتوي العديد من الفرق الأخرى أيضاً مثل فريق البنية التحتية Infrastructure Team، فريق الـ Architecture، وفريق المطورين Developers Team. يقوم فريق أمن الخدمات السحابية أيضاً بـ (2) توزيع الأدوار والمسؤوليات والمعروف بـ IAM Roles and Responsibility، و(3) أتمتة عمليات الأمن السيبراني من خلال أكواد Python or Lambda Functions، و(4) إدارة كلمات المرور لحسابات الكلاود جميعها، من خلال أدوات Secret Managemt Tools مثل KeePass, LastPass, and HashiCorp.



إضافة للأدوار المذكورة أعلاه، يقوم فريق أمن الخدمات السحابية بالتأكد من امتثال جميع حسابات الكلاود لسياسات ومعايير الأمن السيبراني، من خلال استخدام بعض الأدوات مثل Prisma Cloud، والمعروفة سابقاً باسم RedLock قبل أن تمتلكها بالو ألتو وتغير اسمها. بخطوات بسيطة يمكن إدراج حساب الكلاود في هذه الأداة، والتي تقوم بمقارنة جميع الخدمات الموجودة في هذا الحساب مع سياسات ومعايير الأمن السيبراني للتأكد من خلوها من أي ثغرات أمنية Vulnerabilities or Insecure Configuration.

الصور الثلاثة التالية، توضح الشهادات المهنية التي ينصح بها للاستعداد الأمثل لمثل هذا النوع من الوظائف



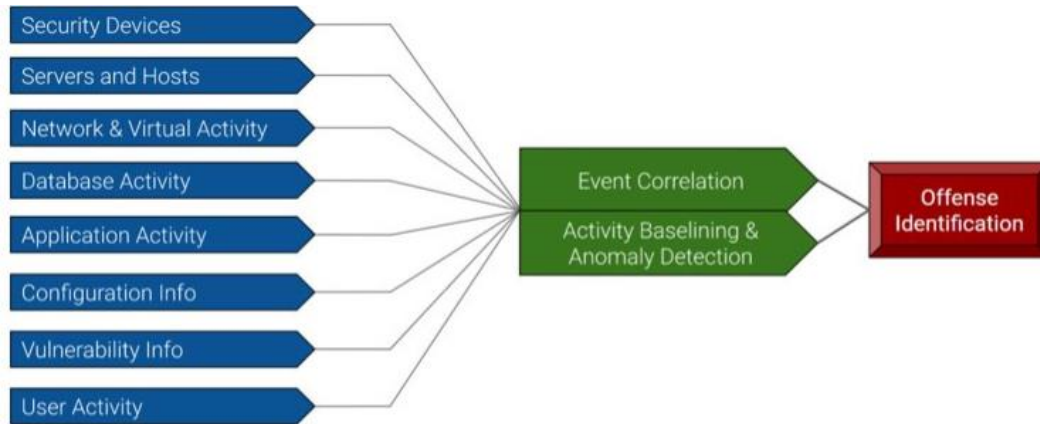




رابعاً: إدارة أمن المعلومات والحوادث (SIEMs) Security Information and Event Management:

تحتوي البنية التحتية لتكنولوجيا المعلومات على العديد من الأنظمة والبرامج، مثل Host Systems, Product Applications, Network Devices, Firewalls. من الصعب على جهات العمل الحصول على رؤية كاملة لشبكاتها، مما يجعل اكتشاف السلوك المشبوه أكثر صعوبة. لذلك، يتم استخدام أنظمة الـ SIEMs لمراقبة السلوك المشبوه وحركة المرور غير العادية على الشبكة، مما يسمح لفريق الأمن السيبراني بالكشف عن الأنشطة المشبوهة.

يمكن تشبيه أنظمة الـ SIEMs بأنها مثل محرك البحث Google لمنظمتك. حيث أننا نتمكن من خلالها من البحث عن أي معلومات/بيانات مهما كان نوعها ومكانها وامتدادها، وتحليل هذه المعلومات/البيانات.

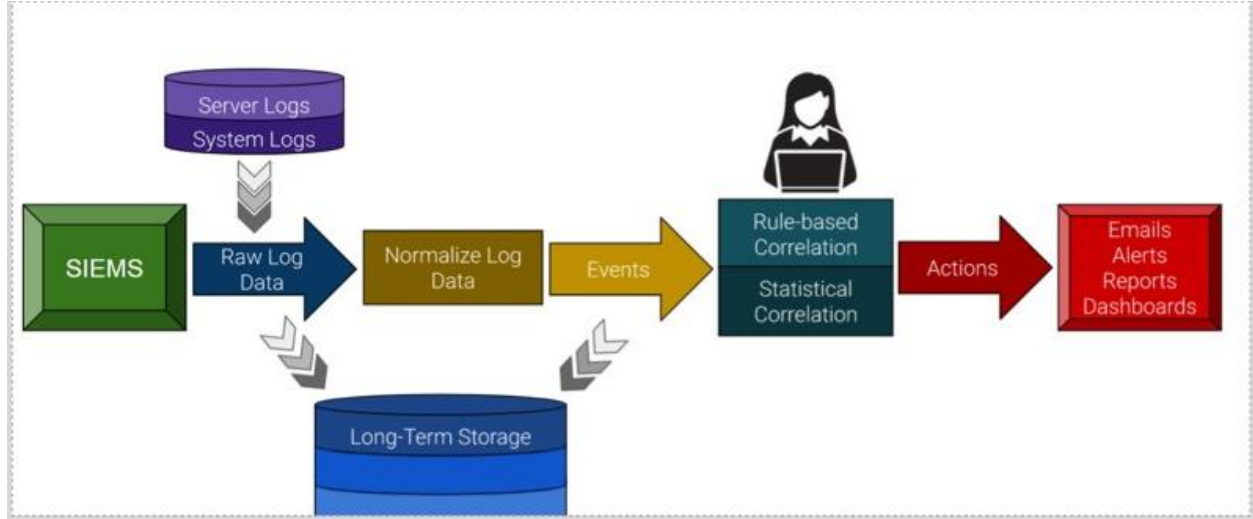


تعد Splunk الأداة الأشهر في هذا المجال، والأعلى سعراً أيضاً، ولكن هنالك العديد من الخيارات المنافسة أيضاً والتي يوضحها الشكل التالي.

Top SIEM Vendors								
..... Best Very Good ... Good . Fair								
	Threats Blocked	Sources Ingested	Performance	Value	Implementation	Management	Support	Scalability
splunk > ES
LogRhythm
ALIEN VAULT
MICRO FOCUS ArcSight
MICRO FOCUS Sentinel
McAfee ESM
Trustwave SIEM
IBM QRadar
RSA NetWitness
solarwind LEM

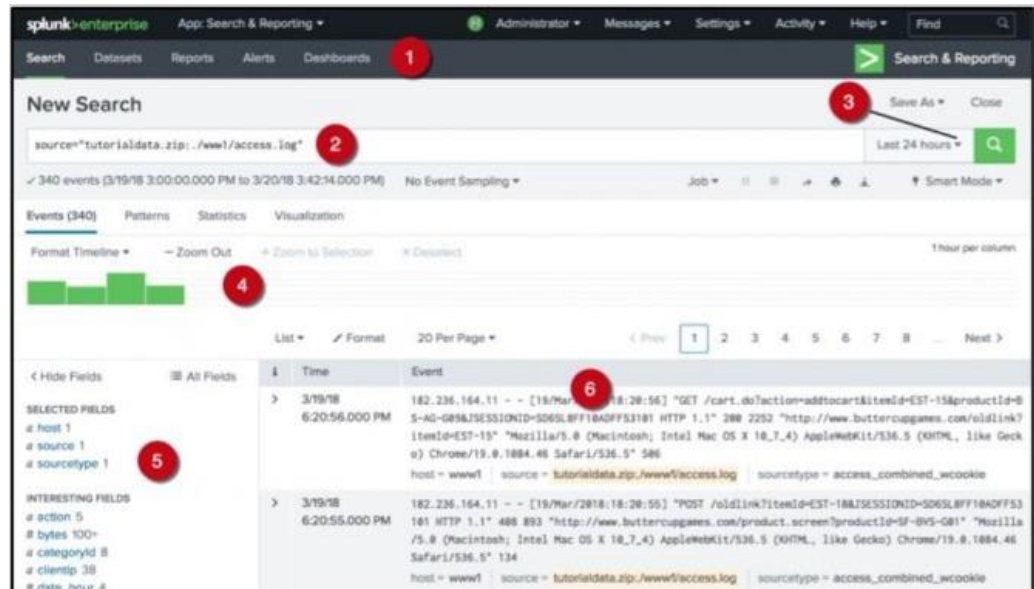
بعض الجهات تختار من هذه الخيارات، بينما البعض الآخر يقوم بتطوير نظام الـ SIEM الخاص به. تارقت مثلاً، قاموا بتطوير نظام SIEM خاص بهم، أطلقوا عليه اسم (ECHO) Events Correlation and Hunting Operations، وتم استخدامه لديهم بنجاح منذ بداية 2018.

فكرة أنظمة الـ SIEMs تتركز حول أربعة نقاط محورية، هي Logs, Events, Analysis, and Response. وتعطينا إنذارات في حال حصول أي حادثة سيبرانية مثلاً، أو في حال محاولة الدخول بكلمات مرور خاطئة لأحد حسابات الموظفين، أو في حالة وجود أي محاولة لعمل Privileged Access Abuse، أو لو كان هنالك أي نشاط من أحد الحسابات التي تم تعطيلها.



للتعرف عن قرب عن طريقة العمل في هذا النوع من الوظائف، يمكن ببساطة إنشاء حساب مجاني في Splunk، والتدرب العملي عليه. ما يميز Splunk، أن لديهم وثائق وشروحات مكتوبة ومرئية كثيرة ومفصلة، يمكن اتباعها خطوة بخطوة، والحصول على نتائج باهرة. كما يمكن التعلم على اللغة الخاصة بـ Splunk والتي تعرف بـ SPL. هنالك دليل مكتوب ومجاني أيضاً على موقع Splunk لهذه اللغة.

الصورة التالية توضح أجزاء الشاشة الرئيسية لـ Splunk.





في التالي، شرح لمحتويات الصورة أعلاه.

1. يسمى الجزء رقم (1) بـ Application Bar، والذي يحتوي على المحتويات الرئيسة Datasets, Reports, Alerts, and Dashboards.
2. يطلق على المحتوى رقم (2) اسم Search Bar، والذي يتم من خلاله البحث والاستعلام باستخدام لغة Splunk وهي Unix Pipeline and SQL Standard. تعد هذه اللغة مزيج بين Query.
3. يسمى ذلك بـ Time Range Picker للاستعلام مثلاً عن النتائج التي حصلت في آخر 24 ساعة، أو آخر أسبوع، أو كل النتائج المتاحة.
4. الجزء الرابع في الصورة يوضح Timeline بمعنى متى كان هنالك Spikes in Activities ومتى كان الخادم خارج الخدمة Server Downtime.
5. يمكن من خلال الجزء الذي يحمل الرقم (5) اختيار الأشياء التي أرغب بالبحث فيها Selected/Interesting Fields.
6. أما في الجزء رقم (6)، والمسمى بـ Event Viewer، يتم استعراض الأحداث/النتائج. الأحدث يأتي أولاً، ويتم عمل Highlight للأمر التي تتطابق مع جملة البحث التي تم كتابتها في الجزء رقم (2).

جدير بالذكر هنا، أنه يمكن تغذية Splunk بالبيانات من خلال رفعها Uploading أو من خلال إعادة توجيهها باستخدام Splunk Forwarder. يمكن التدرب على ذلك بشكل عملي من خلال (1) تحميل Splunk Enterprise على AWS Instance مثلاً، أو على جهازك المحلي أو جهاز افتراضي، و(2) تحميل Splunk Forwarder على جهاز آخر. الخطوات للقيام بذلك موجودة بالتفصيل على موقع Splunk.

خامساً: الاختراق الأخلاقي واختبار الاختراق Penetration Testing and Ethical Hacking:

من المهم في هذا النوع من الوظائف أن يكون الشخص مطلع على أحدث الثغرات التي تصدرها OWASP كل 3-4 سنوات. الصورة التالية توضح آخر قائمتين تم نشرهم من قبل OWASP، والتي توضح أن Injection لا زال التهديد الأكبر منذ 2013 وحتى الآن.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

ماذا نعني بـ Injection؟ يعني ذلك ببساطة أن يقوم المستخدم بخداع الخادم من خلال إدخال أوامر معينة، بدلاً من إدخال مدخلات عادية. يتزايد خطر هذا الهجوم السيبراني في مواقع الانترنت التي تكون مرتبطة بقاعدة بيانات، وتتطلب مدخلات من المستخدم مثل "اسم المستخدم" و"كلمة المرور". تسمى هذه المواقع بـ Database Driven Website. تكون هذه المواقع مستهدفة من قبل المخترقين، للحصول على معلومات غير مصرح لهم بالحصول عليها، وهنا يأتي دور مختبري الاختراق أو المخترقين الأخلاقيين للتأكد من خلو هذه المواقع من أي ثغرات أمنية. الصورة التالية توضح مفهوم الـ Injection بشكل عملي.

Hello, Mnemosyne!

Name

Mnemosyne

Submit

Attackers can submit malicious HTML instead of "expected" input, causing the web application to behave in unexpected ways.

In this example, a user added an HTML element that causes JavaScript to execute when the user passes their mouse over the name Mnemosyne.

Hello, Mnemosyne!

hacked

OK

Name

Mnemosyne

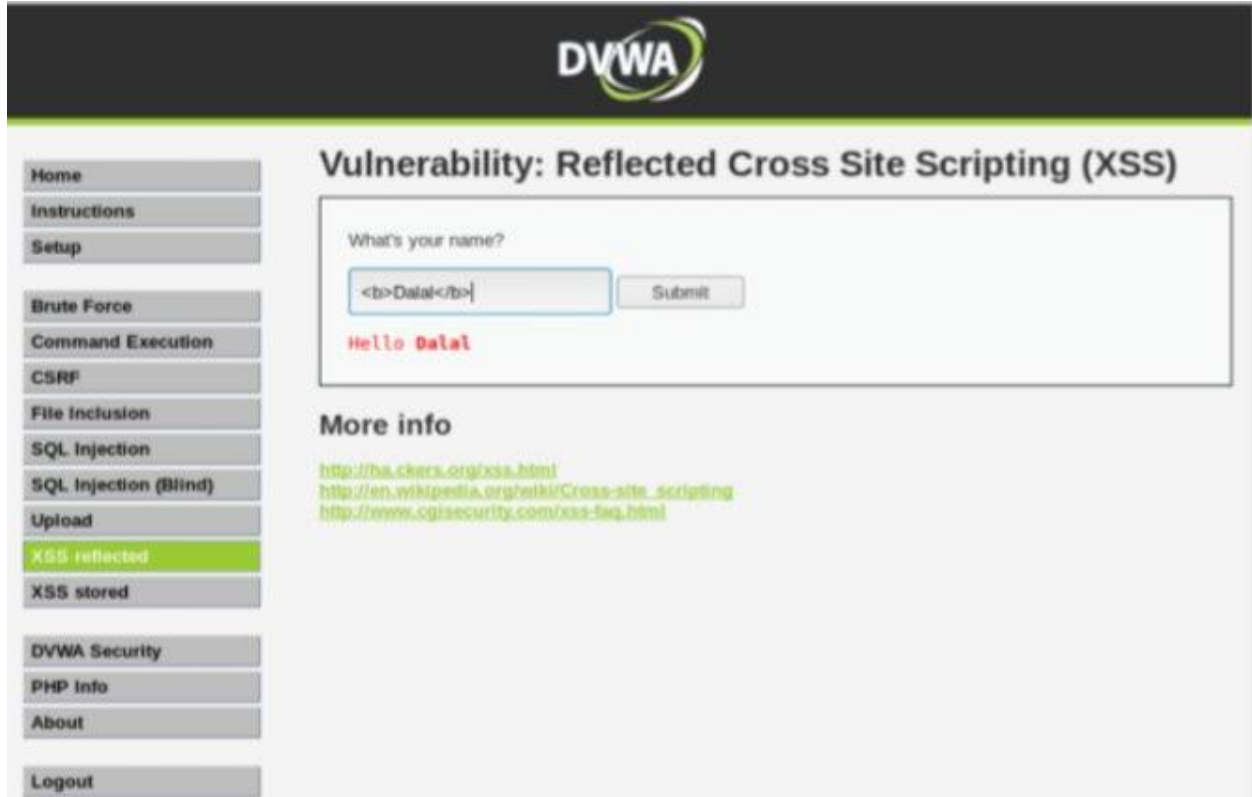
Submit

في مثل هذا النوع من الوظائف، يُطلب منك أن تقدم تقرير يشرح (1) الأدوات التي استخدمتها في عملية الاختراق الأخلاقي، (2) النتائج التي توصلت إليها، و(3) التوصيات التي تنصح بها لسد الثغرات الأمنية والتصدي لمخاطر الهجمات السيبرانية. لكن قبل البدء في أي من ذلك، ينبغي حصولك على موافقة مكتوبة Written Approval من الجهة قبل البدء في عملية الاختراق الأخلاقي. جدير بالذكر هنا أن هنالك العديد من النماذج المتاحة على شبكة الانترنت لهذه التقارير، والتي يمكن الاستئناس بها. يوجد أحد هذه النماذج على الرابط التالي:

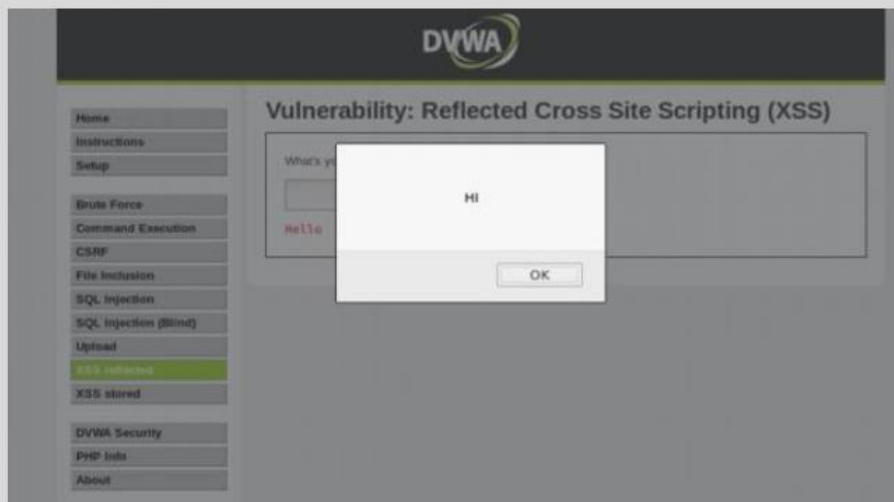
<https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>



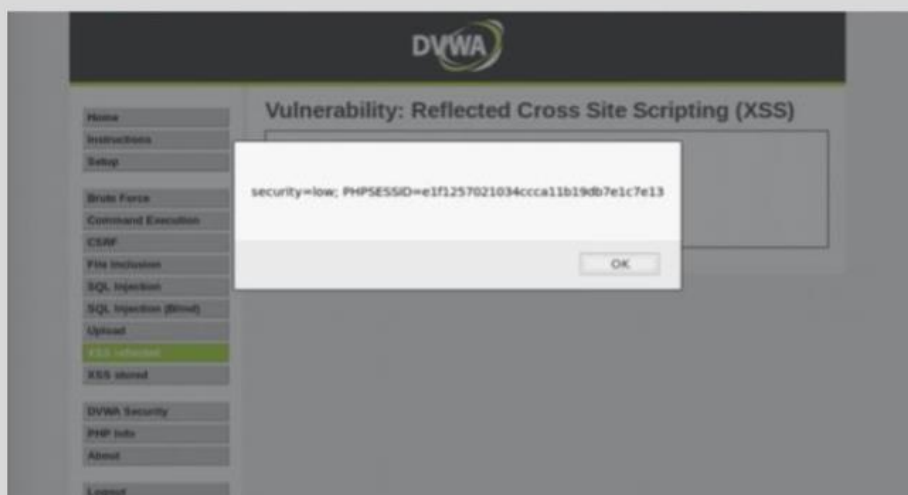
للتعرف عن قرب عن طريقة العمل في هذا النوع من الوظائف، يمكن التدريب عملياً على Damn Vulnerable Web Application (DVWA). الصور التالية، توضح تطبيق عملي على ذلك من خلال الجهاز الافتراضي .Metasploitable2



What if I typed `<script>alert("HI")</script>`



What if I typed `<Script>alert(document.cookie)</script>`



لعل الحل الأمثل لتقوية مستوى الأمن لصفحات الانترنت من النوع Database Driven Websites هو الـ Input Validation. بمعنى، أن يتم منع إدخال الكلمة التالية على سبيل المثال Script سواء أكانت Capital or Small أو كانت مزيج بين Capital and Small. ينبغي أيضاً التأكد من الطول المسموح لاسم المستخدم وكلمة المرور مثلاً، وحجب أي مدخل إذا كان أطول من ذلك.



لمزيد من التطبيق العملي، يمكن استخدام Burp Suite وهو أحد أدوات كالي لينكس Kali Linux.

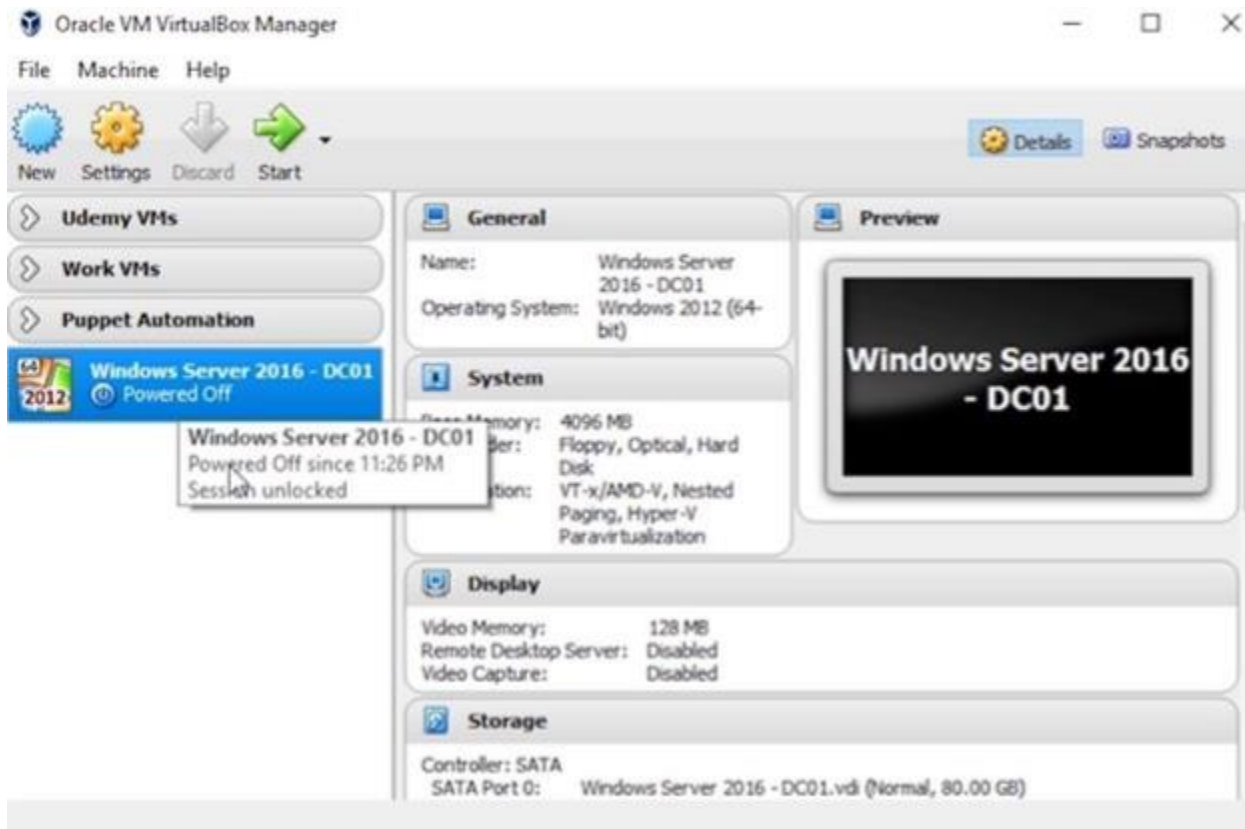


ينصح بالحصول على شهادة Certified Ethical Hacker (CEH) للاستعداد الأمثل لهذا النوع من الوظائف.

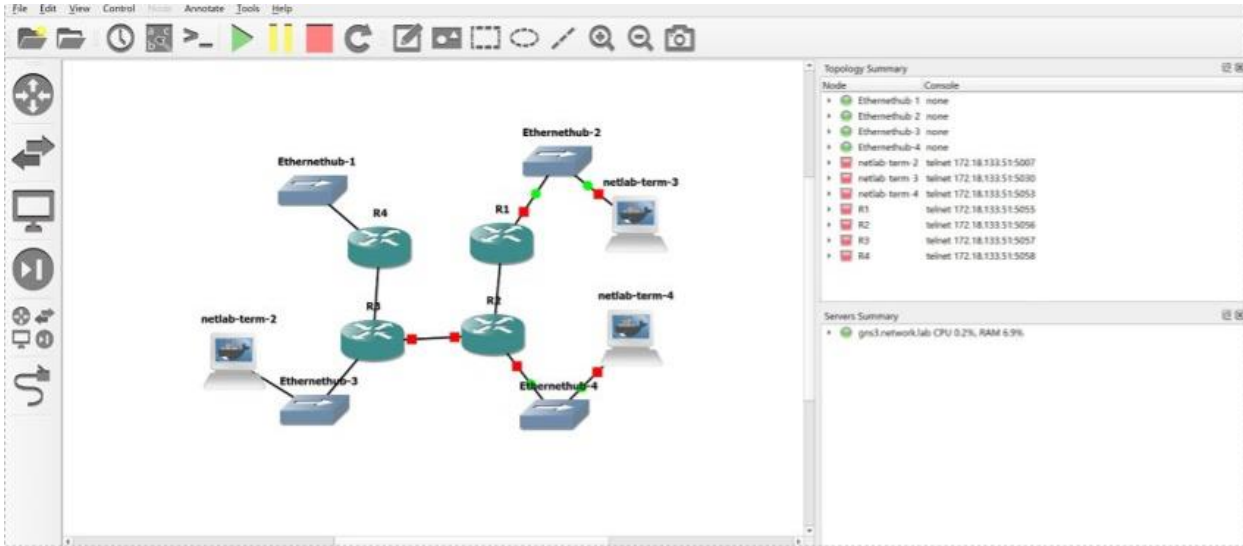
سادساً: أمن الشبكات Network Security:

يقال بأن الأمن السيبراني، والشبكات، جزء واحد لا يتجزأ. ومن خلال خبرتي العملية والأكاديمية، أثني على هذا القول، فالخبرة في أساسيات الشبكات، هي أمر أساسي وجوهري للعمل في أي من مجالات الأمن السيبراني المختلفة.

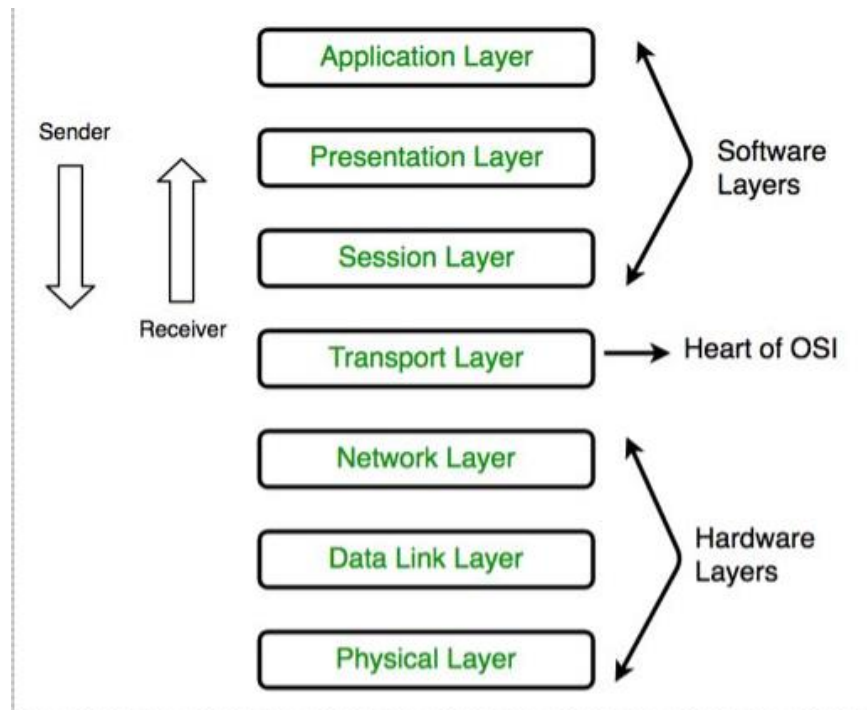
في السابق، كان تعلم أمن الشبكات أمراً صعباً ومكلفاً للغاية. يحتاج الشخص إلى شراء العديد من الأجهزة الفيزيائية، وقضاء وقت طويل في التعلم عليها. الآن، أصبح كل شيء مختلفاً، وأصبحت عملية التعلم متاحة بشكل مجاني، وافتراضي. يمكن لأي شخص أن يقوم من خلال Virtual Box أو VMWare بتحميل Microsoft Server 2016 و Microsoft 10 على سبيل المثال، والتطبيق العملي عليها وبناء شبكة الخادم-العميل Client-Server Network بكل سهولة.



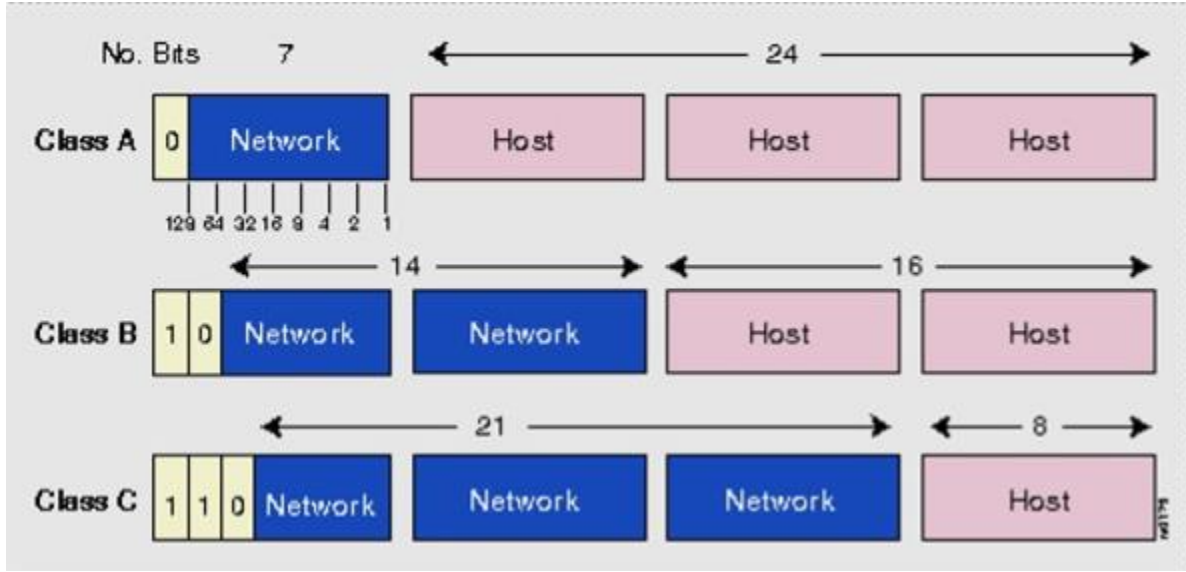
يمكن أيضاً الاستعانة بـ GNS3 والذي يمكن بناء شبكة متكاملة وإضافة الـ Switches, Routers, Firewall افتراضي ومحاكاة عمل الشبكة بشكل احترافي ومجاني.



ينبغي على مختصي الأمن السيبراني أيضاً الإلمام الكامل بـ OSI Layers ومعرفة طريقة تطبيقها على أرض الواقع.



كما ينبغي الإلمام بمعنى (IP) Internet Protocol، وتصنيفات/خصائص الشبكة المختلفة والتي يمكن التعرف عليها بمجرد معرفة الـ IP.



كما أنه من المهم معرفة طريقة استخدام العنوان الفيزيائي MAC Address، وحفظ الـ Ports الهامة والتي يتم استخدامها باستمرار، وطريقة عمل الـ Domain Name Service (DNS)، والفرق بين TCP and UDP، على سبيل المثال. القراءة بكثف عن المفاهيم التي أوردتها هنا، قد تكون نقطة انطلاق هامة للاستزادة في علم أمن الشبكات.

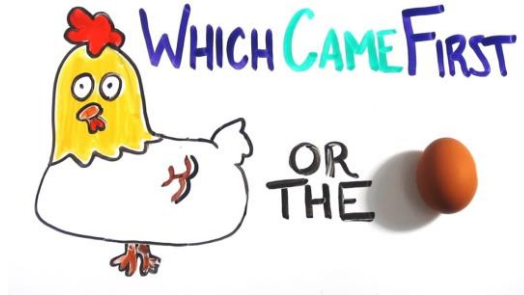
للتعرف عن قرب عن طريقة العمل في هذا النوع من الوظائف، يمكن القراءة عن مفاهيم الشبكات التي أوردتها، والتطبيق العملي من خلال الأدوات التي وضحتها. كما أن هنالك بعض الشهادات التي ينصح بها في هذا المجال مثل CCNA and CompTIA Network+.

سابعاً: سياسات الأمن السيبراني Cybersecurity Policies:

هنالك الكثير من المعايير لسياسات الأمن السيبراني، لعل من أبرزها معيار NIST والمعمول به في أمريكا، ومعيار ISO والمعمول به في أوروبا والشرق الأوسط. هنالك أيضاً معايير أخرى شهيرة في هذا المجال مثل، CIS Benchmark، GDPR، PCI DSS v3.2، CSA CCM v3.0.1، HITRUS CSF v9.3، PIPEDA، CCPA 2018، HIPPA، SOC2. قراءة هذه الوثائق بنتمعن والإلمام بها، فهي خير مصدر لمعرفة أفضل الممارسات في عالم الأمن السيبراني Best Practices.

في جهات العمل، يقع على فريق (GRC) Governance, Risk, and Compliance مسؤولية (1) تطوير/مراجعة سياسات الأمن السيبراني، (2) نشر سياسات الأمن السيبراني Publishing، (3) التأكد من امتثال الموظفين لسياسات الأمن السيبراني Compliance، (4) التأكد من وعي الموظفين بسياسات الأمن السيبراني Awareness، و(5) التأكد من فرض تطبيق سياسات الأمن السيبراني Enforcement من خلال ترجمة هذه السياسات المكتوبة إلى خطوات تقنية داخل الأنظمة.

الخطوتين (2) و(3) أعلاه، يمثلان تحدي أمام موظفي قسم GRC، إذ يطلب منهم في كثير من الأحيان عدم نشر السياسات قبل التأكد من أن الموظفين سيتمثلون بها، ولكن كيف يمكن قياس امتثال الموظفين للسياسات قبل نشرها؟ أيهما يأتي أولاً، نشر السياسات أم الامتثال بها؟!



لعل من أبرز السياسات الواجب تضمينها لضمان أمن المعلومات سياسة استخدام الانترنت والتواصل الاجتماعي، سياسة استخدام بريد العمل، سياسة الاتصال عن بعد والاتصال بـ Wireless، سياسة استخدام أجهزة الشركة (لابتوب.. الخ)، سياسة استخدام أجهزة التخزين، سياسة تحميل البرامج، سياسة الوصول للمعلومات والأنظمة، سياسات كلمات المرور، سياسة استخدام الأجهزة الشخصية BYOD، سياسة مشاركة المعلومات مع الموظفين داخل القسم ومع الموظفين في أقسام أخرى داخل المنظمة ومع الشركاء ومع العامة، سياسة التوعية بالأمن السيبراني، سياسة التشفير، سياسة أمن التطبيقات، سياسة أمن الخوادم، سياسة أمن الشبكات، سياسة تصنيف البيانات، وسياسة استمرارية الأعمال وإدارة الكوارث. السؤال هنا، كيف يمكن فرض تطبيق هذه السياسات؟

سأستعين هنا ببعض الأمثلة العملية للإجابة على هذا السؤال. مثلاً، لفرض تطبيق سياسة استخدام الانترنت والتواصل الاجتماعي، ينبغي حجب المواقع التي قد تشكل تهديداً على بيانات المنظمة. فلنفترض أننا حجبنا اليوتيوب، واحتاج أحد الموظفين لاستخدامه لأغراض العمل. في هذه الحالة، ينبغي أن يكون لدينا آلية لـ Proxy Exception، يقوم الموظف بتقديم طلبه، مع المبررات والتواريخ التي يحتاجها فيها.

مثال آخر لفرض تطبيق سياسة الوصول للمعلومات والأنظمة، ينبغي أن يكون الوصول مبني على مبدأ الامتيازات الأقل Least Privileges بحيث يمكن للموظف الوصول للمعلومات، واستخدام الأنظمة، بما يمكنه من أداء عمله فقط، دون زيادة أو نقصان، وهذا من التحديات التي تواجه مختصي الأمن السيبراني في الجهات.

لفرض تطبيق سياسات كلمات المرور، ينبغي أن يكون هنالك سياسات واضحة لكلمات المرور. مثلاً، كم خانة يجب أن تكون؟ هل يجب أن تحتوي على رموز وأرقام وحروف؟ متى يجبر المستخدم على تغييرها؟ هل يسمح له بإعادة استخدام كلمات المرور السابقة؟ ماذا عن فرض تطبيق معيار التحقق الثنائي MFA؟

لفرض تطبيق سياسة استخدام الأجهزة الشخصية لأغراض العمل (Bring Your Own Device (BYOD، ينبغي أن يكون هنالك آلية لطلب استخدام الأجهزة الشخصية للعمل. في إحدى الجهات التي عملت بها في أمريكا، طلبت إضافة بريد العمل لجوالي الشخصي. بعد اجتياز طلبي للموافقات اللازمة، طلب مني تحميل برنامج الـ SSO، وتغيير كلمة المرور لجهازي! ثم يتم تجزئة ملفات الجوال إلى قسمين، قسم يحتوي الملفات الشخصية، وقسم آخر يحتوي الملفات الخاصة بالعمل. لماذا؟ لأن الجهة تقوم بمسح كل البيانات التي تتعلق بالشركة مباشرة في حال ترك الموظف لعمله لأي سبب من الأسباب.

لفرض تطبيق سياسة مشاركة المعلومات، ينبغي استخدام بعض الأدوات التي تساعدنا في ذلك. مثلاً، فلنفترض أن الموظفين يتشاركون ملفاتهم من خلال Box، أو غيرها من أدوات المشاركة. يمكن استخدام الأدوات التي تمكننا من التأكد من عدم مشاركة الملفات مع بريد شخصي، عدم تخزينها على USB، وعدم تحميلها على الجهاز، لعل من أبرزها أداة Prisma SaaS، والمعروفة بـ Aperture سابقاً قبل أن تمتلكها بالو ألثو وتغير اسمها. الأداة تقوم بعمل Flag عند إرسال الملفات لبريد شخصي أو تحميلها على الجهاز، وتعتبرها Incident. كما يمكن تعطيل إمكانية استخدام الـ USB على أجهزة العمل لمنع تحميل الملفات.

لفرض تطبيق سياسات التوعية بالأمن السيبراني، ينبغي أن يكون هنالك آليات لقياس وعي الموظفين بالأمن السيبراني. كما ينبغي وجود برامج إلزامية للتوعية بذلك. من الممكن أيضاً عمل محاكاة لبريد التصيد مثلاً، وتصميم برامج توعية بشكل ذكي يمكن من خلالها التأكد من أن الموظف يشاهد الفيديو، ويفهمه، ويقرأ السياسة كاملة، ويفهمها.

لفرض تطبيق سياسة استمرارية الأعمال وإدارة الكوارث Disaster Recovery and Business Continuity، النقطة الأهم هي أن يكون لدينا آلية حكيمة للنسخ الاحتياطية. كم مرة يتم حفظ البيانات؟ أين يتم حفظها؟ هل يتم تشفير البيانات المحفوظة؟ أين يتم الاحتفاظ بمفاتيح فك التشفير؟ هل يتم استخدام Secret Management Tools؟ هل هنالك نسخة Offline؟ من يمتلك صلاحية الوصول إليها؟

للتعرف عن قرب عن طريقة العمل في هذا النوع من الوظائف، يمكن البدء بقراءة وثائق هذه المعايير، والمتوفر غالباً على شبكة الانترنت، كما ينصح بالاطلاع على موقعي SANS والهيئة الوطنية للأمن السيبراني National Cybersecurity Authority (NCA)، إذ يحتوي هذين الموقعين على قوالب جاهزة ومجانية يمكن البدء منها، مع أهمية تحويلها لتناسب توجهات ورؤية واستراتيجية جهة العمل.



Search Google or type a URL

Fi Dalal



[Find Training](#) [Online Training](#) [In Person Training](#) [Programs](#) [Resources](#) [Vendor](#) [About](#)

[Home](#) > [Policies](#)

Security Policy Templates

In collaboration with information security subject-matter experts and leaders who volunteered their security policy know-how and time, SANS has developed and posted here a set of security policy templates for your use. To contribute your expertise to this project, or to report any issues you find with these free templates, contact us at policies@sans.org.

Filters:

Categories

- ☐ Application Security
- ☐ General
- ☐ Server Security
- ☐ Network Security
- ☐ Retired

10 per page

Acceptable Encryption Policy	+
Acceptable Use Policy	+
Acquisition Assessment Policy	+
Analog/ISDN Line Security Policy	+



خاتمة:

في ختام هذا المقال، قد يكون دليلك الأمثل للتعرف على طبيعة العمل في كل وظيفة من وظائف الأمن السيبراني، والأدوات التي يتم استخدامها، والشهادات/المؤهلات المطلوبة، هو إعلانات الوظائف. لقد كانت هذه سياستي في تعلم الأمن السيبراني، والتي تمكنت من خلالها من تعلم الكثير عن مجالات الأمن السيبراني، والعمل في فريق أمن الخدمات السحابية في كبرى الشركات المالية في لوس أنجلوس، بالإضافة للعمل كمستشارة للأمن السيبراني في شركة مالية كبرى في زوريك. جرب الاطلاع على هذه الإعلانات، كخطوة أولى بعد قراءة مقالي هذا، للاستعداد الأمثل للعمل في وظائف الأمن السيبراني المختلفة.

وفيما يتعلق بالشهادات المهنية في هذا المجال، ينصح بالاطلاع على الرابط التالي:

<https://secureninja.com/government/nice-framework-secure-ninja-alignment.html>

الرابط أعلاه يوضح الشهادات المهنية الأساسية لكل مسمى وظيفي في مجال الأمن السيبراني. ستجد أن شهادة CompTIA Security+ هي الشهادة الأساسية Core Certificate في جميع المسميات الوظيفية دون استثناء. من هذا المنطلق، أنصح وبشدة بالبداية بالاستعداد لهذه الشهادة الهامة. متمنية للجميع التوفيق والسداد.