

# How

to become a member  
of Security  
Operation  
Center's  
team



Submitted by:  
Eng. Abdulrahim Abdullah Alamoudi

SECURITY OPERATIONS CENTER  
مركز العمليات الأمنية

SOC

2022



## عن الكاتب

المهندس / عبدالرحيم عبدالله عبدالرحيم العمودي

حصل على بكالوريوس هندسة حاسب من جامعة الطائف، وماجستير في إدارة الاعمال مسار نظم معلومات إدارية من كليات الشرق العربي في مدينة الرياض، حاصل على عدة دورات في مجال تقنية المعلومات وامن المعلومات والإدارة.



| الفهرس |  |
|--------|--|
| Page   | العنوان  |
| 1      | المقدمة  |
| 2      | الفصل الأول/ مقدمة شاملة عن الشبكات- Networks .  |
| 13     | الفصل الثاني/ مقدمة شاملة عن أمن المعلومات- Information security .   |
| 21     | الفصل الثالث/ بعض التقنيات المستخدمة في مركز عمليات امن المعلومات –<br>. SOC Technologies<br>.Security incident and event management (SIEM) -<br>.Data loss prevention (DLP) -<br>.Intrusion detection system (IPS) -<br>.User behavioral analytics (UBA) -<br>.Endpoint detection and response (EDR) -<br>.Firewalls -  |
| 24     | الفصل الرابع/ . Splunk<br>.Splunk Overview -<br>.Basic Searching in Splunk -<br>.Creating Reports in Splunk Enterprise -<br>.Create Dashboards in Splunk Enterprise -<br>.Creating Alerts in Splunk -  |
| 26     | الفصل الخامس/ Anti-Virus<br>.Antivirus Software Example -<br>.Symantec Endpoint Protection -<br>.Symantec Endpoint Protection Console Overview -<br>.How to Create SEP Client Package -<br>.Symantec Endpoint Protection Home Page Overview -<br>.Symantec Endpoint Protection Monitors Overview -<br>.Symantec Endpoint Protection Reports Overview -<br>.Symantec Endpoint Protection Clients Overview - |
| 29     | الفصل السادس/ منهجية الاستجابة للحوادث السيبرانية.<br>- إطار الاستجابة للحوادث من NIST.<br>- أشياء لا يجب عملها أثناء الاستجابة للحوادث السيبرانية.<br>- أبرز الحوادث السيبرانية الشائعة وطرق التعامل معها.  |
| 35     | المراجع  |



## شكر وتقدير

أحمد الله تعالى أولاً وآخرًا على الفضل العظيم الذي منحني إياه، ثم أنقدم بالشكر لمن فضلهمَا لا ينقطع علىي والدي الحبيبين على كل جهودهم، ويسري أن أوجه الشكر الجزيل لكل من نصحني أو أرشدني أو ساهم لو بشيء قليل أو وجهني في إعداد هذا الكتاب في أي مرحلة من المراحل التي مررت بها، وأسأل الله أن يكون هذا الكتاب في صحيفة اعمالهم جميعاً، وأن يجزيهم تعالى خير الجزاء والحمد لله رب العالمين.



## المقدمة

### بسم الله الرحمن الرحيم

مع تزايد المخاطر الأمنية وتحديداً مخاطر أمن المعلومات والأمن السيبراني، بدأت المنظمات في اتخاذ قرارات مهمة بشأن تأمين أنظمة تكنولوجيا المعلومات لديهم، من خلال التركيز على التأثير البشري بدلاً من التأثير التكنولوجي على الفحص وتقليل التهديدات. يقوم أعضاء الفريق الأمني بمراقبة وتحليل التهديدات المعروفة لدراسة المخاطر الناشئة بشكل مستمر. يمكن لأنظمة التكنولوجيا، مثل جدران الحماية، أن تمنع الهجمات الأساسية، لكن التحليل البشري يمكن أن يوقف الحوادث الكبرى ويتوعدتها قبل حدوثها، وذلك بتزويد فريق SOC بأحدث التقنيات، لتحسين القرارات آلية الدفاع. يقوم المركز بجمع جميع البيانات من داخل المنظمة مع ربطها بالمعلومات الواردة من مصادر خارجية، مثل موجز الأخبار وتقارير الحوادث ومحركات التهديدات وتبيهات نقاط الضعف، والتي توفر نظرة ثاقبة ل نقاط الضعف وتساعد في مواكبة التهديدات السيبرانية المتطرفة.

ولكي يكون أداء الفريق الأمني مناسب لهذه المهمة يجب ان تكون لديهم معلومات مهمة عن كيفية تكوين الشبكة وطرق نقل البيانات وطرق حماية البيانات وقدرة على تحليها.

### ما هو مركز العمليات الأمنية (SOC)؟

هو مركز عمليات مخصص للمراقبة والتصدي للهجمات السيبرانية 24 ساعة طوال الأسبوع والتحقق بشكل مسبق من أي تهديد يواجه المنظمة. هذه الخدمة تقدم من قبل خبراء في الأمن السيبراني وباستخدام أحدث التقنيات ل توفير الحماية للمنظمة، لتحقيق أعلى المعايير الأمنية.

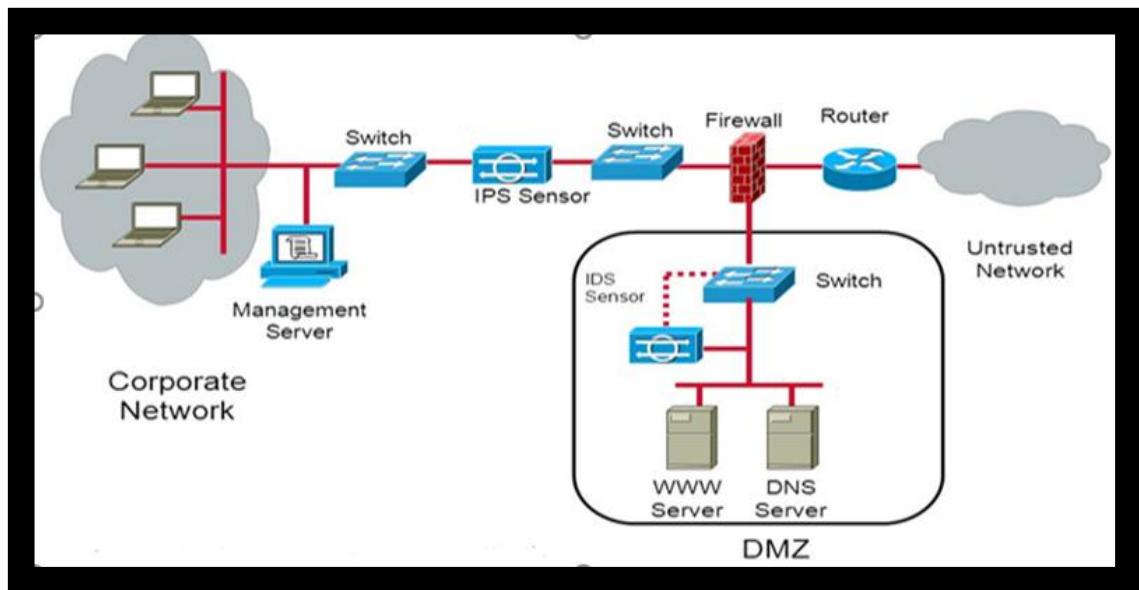
وفي هذا الكتاب سوف تحصل على المعلومات الالزمة لتصبح محترف في امن المعلومات ولكي تكون عضو في فريق مركز العمليات الأمنية، سوف يتم ذكر جميع المعلومات المهمة في مجال الشبكات و المجال امن المعلومات وتحليلها وشرح بعض الأدوات المستخدمة والبرامج المهمة لفريق مركز العمليات الأمنية (SOC).



## الفصل الأول/مقدمة شاملة عن الشبكات - Networks

في نهاية هذا الفصل سوف تستطيع تمييز مكونات الشبكة داخل المنظمة ومعرفة المصطلحات المهمة المستخدمة في مجال الشبكات لكي تساعدك في تحليل الهجمات داخل المنظمة.

- الشكل التالي يبين بعض مكونات الشبكة المهمة في كل منظمة.



### What is a Network?

It is 2 or more devices that are linked needs to

sharing information between them.

Also called (Computer Network).

الشبكات: هي عبارة عن جهاز حاسوب أو مجموعة من الأجهزة المتصلة مع بعضها البعض بواسطة أسلاك التوصيل أو الكابلات ومن الممكن أن تكون متصلة بشكل لاسلكي لمشاركة الموارد والملفات المختلفة.

### أنواع الشبكات – Network Types

|   |  |
|---|--|
| LAN (Local Area Network): some users in different rooms/department connected using a router and some switches.  | LAN: هي شبكة تتكون من بعض المستخدمين في غرفة او اقسام مختلفة متصلون باستخدام Router وبعض Switches. |
| MAN (Metropolitan Area Network): is consisting of a computer network across an entire city or a small region. This type of network is large than a LAN. | MAN: تتكون من شبكة كمبيوتر في مدينة بأكملها أو منطقة صغيرة. هذا النوع من الشبكات أكبر من شبكة LAN. |



|   |  |
|---|--|
| WAN (Wide Area Network): A LAN connects with other LAN's using telephone lines and radio waves. It is mostly limited to organization. | WAN : تتصل شبكة LAN بشبكات LAN الأخرى باستخدام خطوط الهاتف وموجات الراديو.<br>يقتصر استخدامها في الغالب على المنظمات والشركات. |
| PAN (Personal Area Network): is a computer network formed around a person. It generally consists of a computer or mobile.             | PAN : هي شبكة كمبيوتر تكون حول شخص واحد (شخصية).<br>ت تكون بشكل عام من جهاز كمبيوتر أو هاتف محمول.                             |

| مكونات الشبكة – Network Components  |  |
|---|--|
| <b>Routers:</b>   |  |
| Network devices that connect different network domains and routes the IP packets to its correct destinations. | هو جهاز يستخدم للتوصيل بين الاجهزة في الشبكات المختلفة.<br>- يعمل في الطبقة الثالثة.<br>- يتعامل مع الـ IP Address<br>- يستخدم الـ Packets<br>- يستخدم في شبكات الـ WAN  |
| <b>Switches:</b>  |  |
| Network devices that connect 2 or more devices in one network domain.   | هو جهاز يستخدم للتوصيل بين الاجهزة في الشبكات المتماثلة.<br>- يعمل في الطبقة الثانية.<br>- يتعامل مع الـ MAC Address<br>- يستخدم الـ Frames<br>- يستخدم في شبكات الـ LAN<br>- يوجد طبعا switches ت العمل في الطبقة الثالثة.  |
| <b>Firewalls:</b>   |  |
| Firewalls protects you from the internet Apply some restrictions to your local network.                       | جدار الحماية هو الجهاز الذي تقوم الشركات أو المؤسسات بوضعه لضمان حماية أمن برامجها وملفاتها من الاختراق والسرقة من الجهات الخارجية، بحيث يتم وضع هذا الجهاز تحديداً بين كل من الشبكة الداخلية للمنظمة وشبكة الإنترنت، بحيث يتم تحديد الجهات غير المرغوب بها والتي تتسلل إلى شبكة الكمبيوتر الداخلية الخاصة بالمنظمة، ثم تنبيه المشرف عن النظام بذلك. |



## IDS:

An Intrusion Detection System (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system.

يراقب نظام كشف التسلل (IDS) حركة مرور الشبكة ويراقب النشاط المريب وبنية النظام أو مسؤول الشبكة. في بعض الحالات، قد تستجيب IDS أيضًا لحركة المرور الشاذة أو الخبيثة من خلال اتخاذ إجراء مثل حظر المستخدم أو عنوان IP المصدر من الوصول إلى الشبكة.

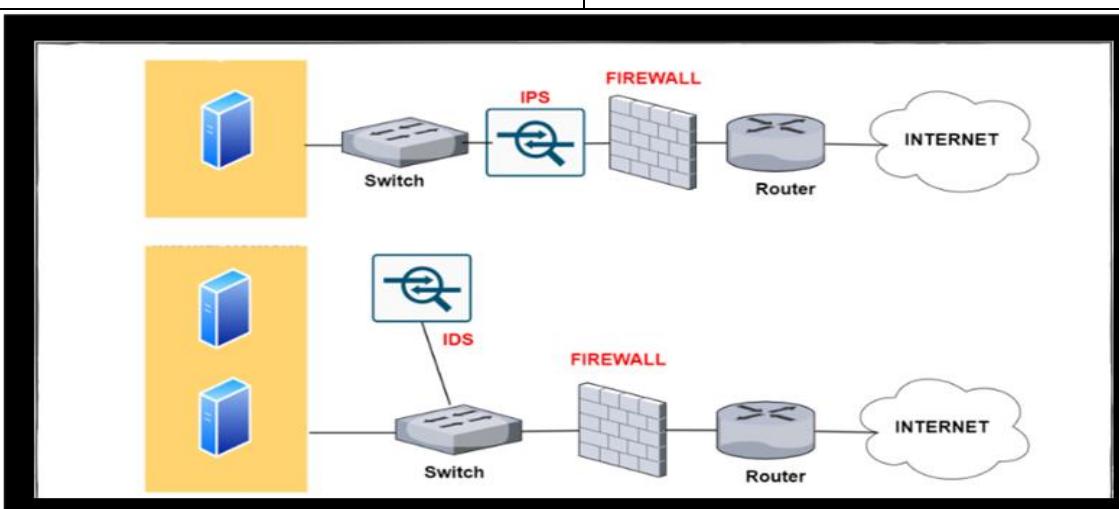
## IPS:

Intrusion Prevention Systems (IPS) Do deep packet inspection (DPI) Try to spot attacks.

يقوم بكشف المهاجمات والحرص على توقيفها سواء بقطع الاتصال ب IP الذي يحاول المهاجم علينا عن طريق وضع access list.

## Next-Generation Firewalls:

(NGFW): FW+ IPS



## Access Points (AP):

Like switches, Access Points are the (wireless) destination for a host to communicate with other hosts.

Access Points هي الوجهة اللاسلكية للمضيف للتواصل مع المضيفين الآخرين، مثل ال Switches.

## Wireless Controllers:

A central management point for multiple Access Points (APs).

هي عبارة عن نقطة إدارة مركزية لنقاط وصول متعددة (multiple Access Points).



## Servers:

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network.

السيفر أو الخادم هو عبارة عن جهاز حاسوب له مواصفات خاصة وحجم خاص قادر على العمل لمدة تصل إلى عام دون الحاجة إلى إيقاف تشغيله والخادم له مواصفات جبارة لكي يقوم بعمل المهام المطلوبة منه والقدرة على تحمل العمل لفترة طويلة ويتم تخصيص هذا الجهاز للقيام بمهام محددة لخدمة باقي الأجهزة المتصلة بنفس الشبكة او الاتصال به عن بعد وان كانت ليست على نفس الشبكة المتصل بها الخادم.

## Virtual Machines:

A Virtual Machine (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps. One or more virtual “guest” machines run on a physical “host” machine. Each virtual machine runs its own operating system and functions separately from the other VMs, even when they are all running on the same host.

استخدم البرامج بدلاً من الحاسوب الفعلي لتشغيل البرامج ونشر التطبيقات. يعمل جهاز افتراضي واحد أو أكثر على جهاز "مضيف" فعلي واحد. يقوم كل جهاز افتراضي بتشغيل نظام التشغيل الخاص به ويعمل بشكل منفصل عن الأجهزة الافتراضية الأخرى، حتى عندما تعمل جميعها على نفس المضيف.

## Network Architecture Models:

### A- The Open Systems Interconnection model (OSI model):

It is a conceptual framework used to describe the functions of a networking system.

- ISO هو نموذج نظري، تم عمله بواسطة منظمة الأيزو يوضح كيفية انتقال البيانات من المرسل للمستقبل.
- الطبقات الثلاث الأولى مخصوصة لنقل البيانات وبياناتها وتبادلها.
- الطبقة الرابعة تعمل كواجهة بين الطبقات السفلية والعلوية.
- الطبقات الثلاث الأخيرة مخصوصة لتطبيقات وبرامج المستخدم.
- ترتيب الطبقات من الأسفل للأعلى كما في الجدول التالي.

### B- The Transmission Communication Protocol/Internet Protocol Model (TCP/IP Model):

Helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them.

TCP/IP Model هي لغة متفق عليها بين مستخدمي الإنترنت للاتصال والتواصل فيما بينهم وبين الأجهزة المستخدمة لدخول الإنترنت.

الصورة التالية تبين الفرق بينهما:



| TCP/IP MODEL         | OSI MODEL          | PROTOCOLS       |
|----------------------|--------------------|-----------------|
| Application Layer    | Application Layer  | FTP,HTTP,Telnet |
|                      | Presentation Layer | JPEG,MPEG       |
|                      | Session Layer      | NFS,SQL,PAP     |
| Transport Layer      | Transport Layer    | TCP,UDP         |
| Network Layer        | Network Layer      | IPv4,IPv6       |
|                      | Data Link Layer    | ARP,CDP,STP     |
| Network Access Layer | Physical Layer     | Ethernet,Wi-Fi  |

### Media Access Control Address (MAC Address):

- The MAC address unique numbers, identifies that device from every other globally .
  - The MAC address is a 12-digit hexadecimal number that is most often displayed with a colon or hyphen separating every two digits (an octet), making it easier to read .
  - The ID is assigned to vendors by the IEEE and "burned into" the network circuit at the time of manufacture.
- الـ MAC Address هو العنوان الفيزيائي لكرت الشبكة ويكون وحيد لا يتشابه مع آخر وهو قابل للتغيير ويستخدم من قبل ال switch .12 digit hexadecimal number -

### IP Address:

الـ IP address هو العنوان الذي يأخذه الحاسب للاتصال بالشبكة أو الإنترنت وهو قابل للتغيير ويستخدم من قبل ال router .

### Internet Protocol Version 4 (IPv4):

1. Address Size: 32-bit address.
  2. Binary [0/1]
  3. Number of addresses:  $2^{32}$ .
  4. Example: 192.0.1.1
- يتكون من أربع اقسام وكل قسم يسمى أوكتت ويتوافق ما بين (0-255).
- يبلغ عدد العناوين ما يزيد عن 4 مليارات عنوان.
- يوجد 5 أنواع من الكلاسات من (A,B,C,D,E) .
- هو البروتوكول الأكثر استخداماً في تبادل البيانات بين مختلف أنواع الشبكات.



| Address Class | RANGE                               | Default Subnet Mask              |
|---------------|-------------------------------------|----------------------------------|
| <b>A</b>      | <b>1.0.0.0 to 126.255.255.255</b>   | <b>255.0.0.0</b>                 |
| <b>B</b>      | <b>128.0.0.0 to 191.255.255.255</b> | <b>255.255.0.0</b>               |
| <b>C</b>      | <b>192.0.0.0 to 223.255.255.255</b> | <b>255.255.255.0</b>             |
| <b>D</b>      | <b>224.0.0.0 to 239.255.255.255</b> | <b>Reserved for Multicasting</b> |
| <b>E</b>      | <b>240.0.0.0 to 254.255.255.255</b> | <b>Experimental</b>              |

**Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.**

### Internet Protocol Version 6 (IPv6):

- 128-bit address.
- Hexadecimal [0-9] [A-F].
- Number of addresses:  $2^{128}$ .
- Example: 2002:db8::8a3f:362:7897

مع انتشار الانترنت والتوزع الكبير في الاجهزة، أدرك القائمون على الانترنت انه خلال سنوات سوف تتجاوز عدد الاجهزه ٤ ميليار مما يتسبب في مشكلة في التواصل بين الاجهزه وأصبح لابد من وجود نظام عنونه جديد يستوعب هذا الكم المتزايد من العنوانين.

- يمثل 128 بت.

الميزة التي تفرقه عن الا ipv4 يقوم بزيادة حجم العنوان من 32 بت إلى 128 بت.

### Transmission Communication Protocol & User Datagram Protocol:

**TCP:** is extremely reliable and is used for everything from surfing the web (HTTP), sending emails (SMTP), and transferring files (FTP).

TCP is used in situations where it's necessary that all data being sent by one device is received by another completely intact.

**UDP:** is less reliable than TCP, and faster than TCP.

UDP is used for situations where some data loss is acceptable, like live video/audio, or where speed is a critical factor like online gaming.

**TCP**: ينقل البيانات للطرف الآخر وبشكل موثوق، ولكنه بطيء يقوم بإرسال البيانات دفعة واحدة وبعد التتحقق من استلامها يرسل دفعة أخرى. - مثل إرسال بريد إلكتروني.

**UDP**: ينقل البيانات للطرف الآخر بشكل سريع لكنه غير موثوق حيث يقوم بتقسيم الرسالة المراد ارسالها الى وحدات مما يسرع وصول البيانات. - مثل إرسال البيانات في الراديو أو التلفاز أو كاميرات المراقب.



- الان سوف نقوم بشرح بعض المصطلحات والاختصارات المهمة المستخدمة في مجال عمل تقنية المعلومات وخصوصاً مجال

الشبكات:

### Domain:

It is the domain that is created within the organization or company, which includes all Users, Computers, Groups, and resources for the place such as Server Print, Server File, and so on.

هو المجال الذي يتم إنشاؤه داخل المؤسسة أو الشركة والذي يضم جميع الـ Resources Groups والـ Computers وـ File Server وـ Print Server وـ ونكذا.

أي جهاز كمبيوتر يحتوي على (Windows Server) يسمى Active Directory domain ولكن عند تفعيل الـ domain عليه يسمى .Domain Controller

### Domain Controller:

A domain controller is a type of computer server that responds to security authentication requests and verifies users on the domain of a computer network. The controller is a gatekeeper for allowing host access to domain resources. It also enforces security policies, stores a user's account information, and authenticates users for a domain.

وحدة التحكم بال المجال هي كمبيوتر خادم يستجيب لطلبات مصادقة الأمان داخل مجال شبكة الكمبيوتر. إنه خادم شبكة مسؤول عن السماح للمضيف بالوصول إلى موارد المجال. إنه يصادق المستخدمين ويخزن معلومات حساب المستخدم ويفرض سياسة أمنية لمجال ما.

### Active Directory (AD):

Active Directory (AD) is a directory service that runs on Microsoft Windows Server. The main function of Active Directory is to enable administrators to manage permissions and control access to network resources.

هو عبارة عن قاعدة بيانات لكل موارد الشبكة والخدمات والمستخدمين بحيث يمكن من خلاله عمل تحكم مركزي بكل هذه الأجزاء في الشبكة والتحكم بصلاحيات المصادقة والتغويض (authentication and authorization)

### ADFS (Active Directory Federation Services):

Active Directory Federation Services is a feature and web service in the Windows Server Operating System that allows sharing of identity information outside a company's network. It authenticates users with their usernames and passwords. Users can access some applications (Microsoft Office apps, etc.) without being prompted to provide login credentials again.

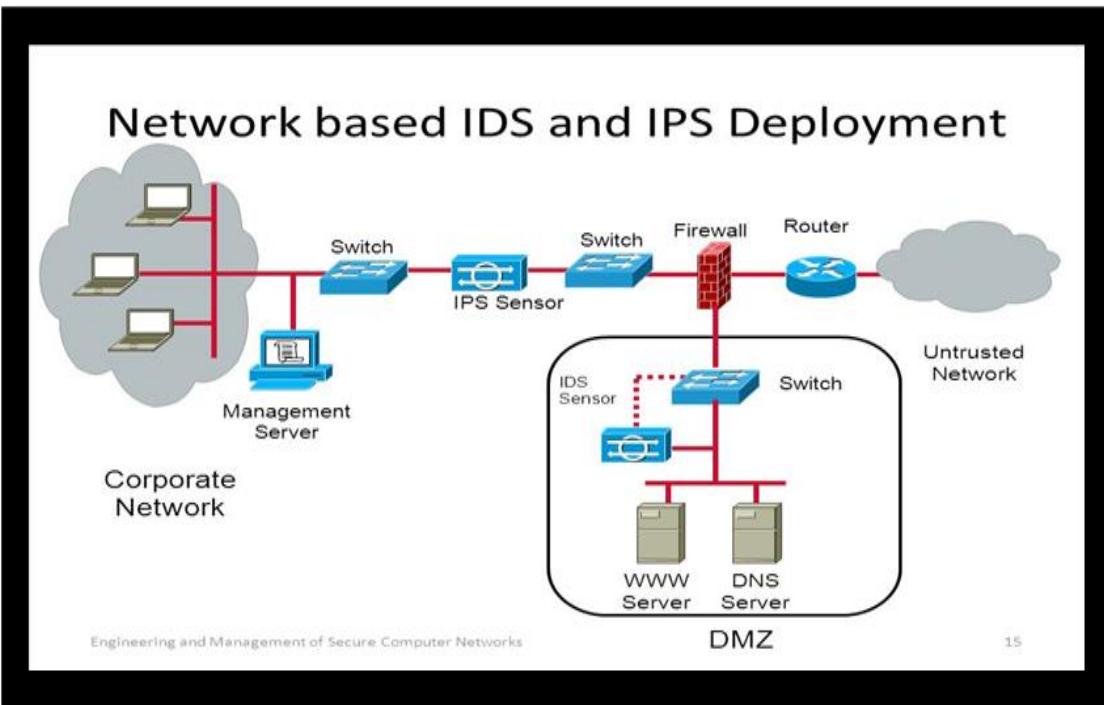
ميزة وخدمة ويب في نظام تشغيل Windows Server يسمح بمشاركة معلومات الهوية خارج شبكة الشركة. يصادق المستخدمين بأسماء وكلمات المرور الخاصة بهم. يمكن للمستخدمين الوصول إلى بعض التطبيقات (مثل تطبيقات Microsoft Office) دون مطالبتك بتقديم بيانات اعتماد تسجيل الدخول مرة أخرى.



## DMZ:

De-Militarized Zone, which is a sub-network, typically between the protected internal network protected by Firewalls and an "untrusted" external network, such as the Internet.

منطقة منزوعة السلاح هو اختصار نوع ثالث من شبكات الإنترنت أي وقع في مستوى وسط بين الشبكات الداخلية والخارجية. هي منطقة ليست مؤمنة بشكل كلي كما هي الحال في الشبكة الداخلية ولا هي مكشوفة بشكل صريح كما في شبكة الإنترنت الخارجية، ويتم اللجوء إلى استخدامها في بعض الحالات أبرزها عند الحاجة إلى تمكين المستخدمين في الشبكة الخارجية من الوصول إلى بعض الخدمات المحلية مثل FTP أو Web Server، حيث في حالة توفير مثل هذه الخدمات في الشبكة الداخلية قد يعرض الشبكة بالكامل للخطر لهذا السبب، يتم وضع هذه الخدمات في شبكة ثلاثة منفصلة عن الشبكة الداخلية لحماية الشبكة الداخلية.



## Power over Ethernet (PoE):

Carrying Power over 2 pairs of Copper Cables (enough to power up some network devices).

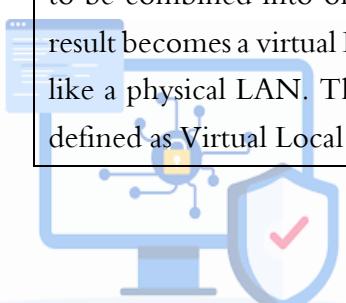
خاصية استقبال الطاقة من خلال كابل الشبكة دون الحاجة لتوصيل تيار كهربائي للجهاز مثل بعض أجهزة التلفون (الستنترال).

## What is VLAN?

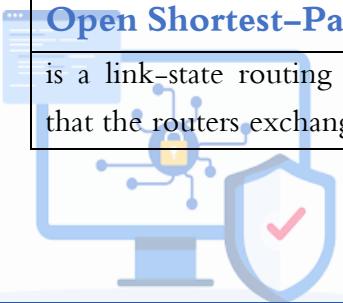
VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

هي اختصار لـ Virtual Local Area Network وتعني الشبكة المحلية الوهمية وسميت بذلك لأنها في الواقع عندما تنظر إلى بنيتها تظهر وكأنها شبكة واحدة، ولكن في الحقيقة تكون أكثر من شبكة. تعمل في الطبقة الثانية Data Link Layer والطبقة الثالثة Network Layer.

حيث إن الـ Switch يقوم بتقسيم الشبكة الواحدة إلى عدة شبكات كل منها منفصلة عن الأخرى أي لا يمكن لأجهزة شبكة افراضية الاتصال



|   |   |
|---|---|
|   | بأجهزة شبكة افتراضية أخرى مع أئم مرتبطين بـ Switch وتستخدم لتنظيم الشبكات.  |
| <b>Dynamic Host-Configuration Protocol (DHCP):</b>  |   |
| is a protocol that automatically provides an Internet Protocol (IP) host with its IP address.   | فائدة: يعمل على توزيع الـ IP للعديد من الأجهزة بشكل أوتوماتيكي.   |
| <b>What's a DNS?</b>  |   |
| Domain Name System: resolve a URL to an IP Address and an IP Address to a URL its works on UDP port 53.   | يعمل على ترجمة أسماء النطاقات إلى عناوين فائدته تسهيل الوصول إلى الموقع بكتابة اسمها بدلاً من كتابة عنوان الـ IP الخاص بها.   |
| <b>Network Address Translation (NAT):</b>   |   |
| Private IP address or local address are translated into the public IP address.  | هو عملية تحويل الـ IP من Private إلى Public بغرض الخروج إلى الإنترنت.<br>الغرض من الـ NAT هو التغلب على مشكلة عدم توفر العناوين الكافية من الـ IPv4 حيث يتم استخدام IP Public واحد من أكثر من جهاز. |
| <b>Application Programming Interface (API):</b>   |   |
| The transformers that are transforming everything from The Application to the controllers, and from the controllers to The Application.   | وهي خدمة تُقدمها المواقع أو البرمجيات الخاصة بالشركات الكبرى لتسهيل إضافة بعض من ميزاتها لبرامج أخرى.<br>هي خدمة تسمح للم المنتجات والخدمات التقنية للتواصل مع بعضها.                               |
| <b>ISP:</b>   |   |
| Internet service provider.  | مزود خدمة الانترنت.   |
| <b>What is port security:</b>   |   |
| By using port security, users can limit the number of MAC addresses that can be learned to a port, set static MAC addresses, and set penalties for that port if it is used by an unauthorized user. | هي عملية حماية الأجهزة المتصلة على المنفذ عن طريق ربط الـ mac address للجهاز الذي سيتم توصيله بالمنفذ ملن توصيل أي جهاز غير معروف على الشبكة.   |
| <b>Spanning Tree Protocol (STP):</b>  |   |
| It is a protocol that works to avoid the occurrence of loop between the switches by sending Bridge Protocol Data Unit (BPDU) with a duration of 2-20 seconds.                                       | هو بروتوكول يعمل على تجنب حصول الـ loop بين الـ switches عن طريق ارسال ما يسمى Bridge Protocol Data Unit (BPDU) ومدته من 20 ثانية.  |
| <b>Open Shortest-Path First (OSPF):</b>   |   |
| is a link-state routing protocol, which means that the routers exchange topology information  | هو بروتوكول توجيه حالة الارتباط، يعني أن أجهزة التوجيه تتبادل معلومات الميكل مع أقرب جيرانها. لذلك، في بروتوكول توجيه حالة الارتباط، يتم  |



|   |  |
|---|--|
| <p>with their nearest neighbors. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.</p> | <p>تحديد عنوان القفزة التالية التي يتم إعادة توجيه البيانات إليها عن طريق اختيار أفضل مسار من طرف إلى طرف إلى الوجهة النهائية.</p> |
|---|--|

### Port Address Translation (PAT):

|  |  |
|--|--|
| <p>Private IP addresses are translated into the public IP address via Port numbers. PAT also uses IPv4 address but with port number.</p> | <p>يتم تحويل عنوان المرسل ورقم منفذه (Source IP address and Port number) لأن العنوان الخارجي (public IP) مثل عدة عناوين داخلية، ويتم تغيير رقم المنفذ (layer 4 source port) لتمييز تبعية البيانات المرسلة كون ستصبح هذه البيانات (number) كأنها من مصدر واحد عنوانه (public IP) مع أنها قادمة من مصادر مختلفة قبل عملية التغيير (NAT) فيستخدم أرقام منافذ مختلفة لكل (private IP).</p> |
|--|--|

### Remote Desktop Protocol (RDP) :

|   |  |
|---|--|
| <p>The Remote Desktop Protocol (RDP) is a protocol, or technical standard, for using a desktop computer remotely.</p> | <p>سطح المكتب البعيد، خاصية الدخول على الجهاز عن بعد لتسليط التحكم به عبر حاسوبك الشخصي من خارج العمل.</p> |
|---|--|

### Azure RMS:

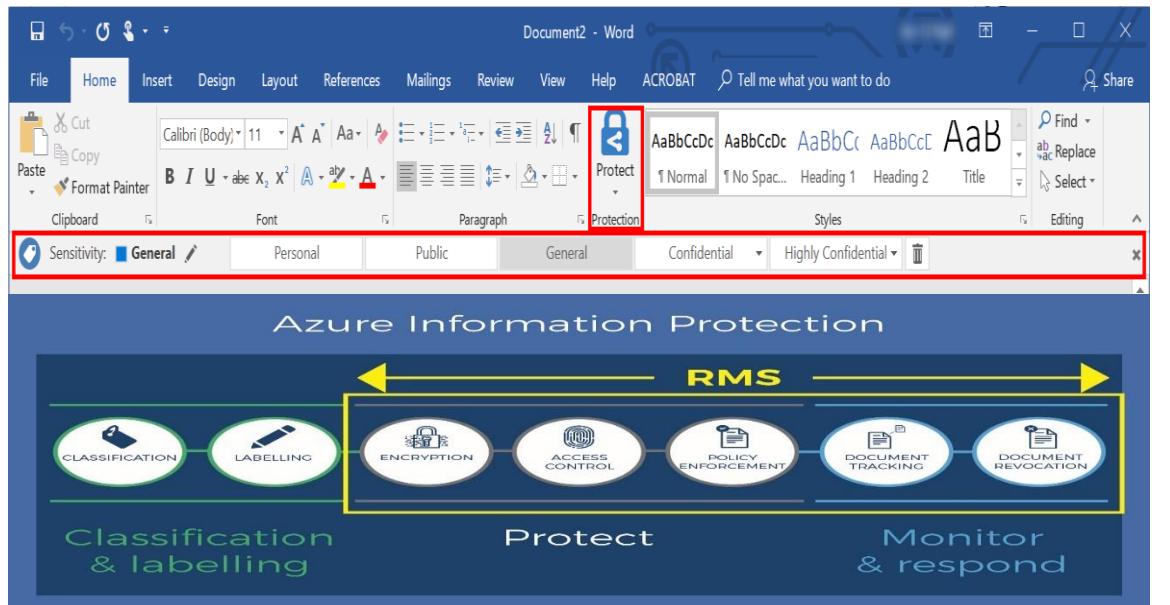
|   |  |
|---|--|
| <p>Azure Rights Management (Azure RMS) is the cloud-based protection technology used by Azure Information Protection.</p> <p>Azure RMS helps to protect files and emails across multiple devices, including phones, tablets, and PCs by using encryption, identity, and authorization policies.</p> | <p>هي تقنية الحماية المستندة إلى السحابة المستخدمة بواسطة AIP. تساعد في حماية الملفات ورسائل البريد الإلكتروني علىأجهزة متعددة، بما في ذلك الهواتف والأجهزة اللوحية وأجهزة الكمبيوتر الشخصية باستخدام سياسات التشفير والهوية والتفويض.</p> |
|---|--|

### Azure Information Protection (AIP):

|  |  |
|--|--|
| <p>Azure Information Protection (AIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content.</p> <p>AIP is part of the Microsoft Information Protection (MIP) solution and extends the labeling and classification functionality provided by Microsoft 365.</p> | <p>هو حل قائم على السحابة يمكن المؤسسات من اكتشاف المستندات ورسائل البريد الإلكتروني وتصنيفها وحمايتها من خلال تطبيق تسميات على المحتوى.</p> <p>يعد AIP جزءاً من حل حماية معلومات (MIP)، وهو يوسع وظائف وضع العلامات والتصنيف التي يوفرها Microsoft 365.</p> |
|--|--|



AIP:



- الان سوف نقوم بذكر اهم البروتوكولات مع ذكر رقم المنفذ المستخدم وذلك يساعدك في حماية الشبكة من خلال اغلاق المنافذ غير المستخدمة او غير المرغوبة:

| يستخدم | رقم المنفذ | الاسم  | البروتوكول   |
|--------|------------|--|--------------|
| TCP    | 20 – 21    | File transfer protocol   | FTP          |
| TCP    | 22         | Secure File Transfer Protocol                                    | SFTP         |
| TCP    | 22         | Secure Shell   | SSH          |
| TCP    | 3389       | Remote Desktop Protocol  | RDP          |
| UDP    | 53         | Domain Name Service  | DNS          |
| TCP    | 23         | Telnet   | Telnet       |
| TCP    | 25         | Simple Mail Transfer Protocol                                    | SMTP         |
| UDP    | 67 – 68    | Dynamic Host Configuration Protocol                              | DHCP         |
| TCP    | 80/8080    | Hypertext Transfer Protocol                                      | HTTP         |
| TCP    | 443        | Hypertext Transfer Protocol Secure                               | HTTPS        |
| TCP    | 143        | Internet Message Access Protocol                                 | IMPA         |
|        | 445        | Microsoft-DS (Directory Services) Active Directory, file sharing | File sharing |

## الفصل الثاني / أمن المعلومات-Information security

في نهاية هذا الفصل سوف تستطيع معرفة المصطلحات المهمة المستخدمة في مجال امن المعلومات ومعرفة أنواع المهاجمات وطريقة منعها لكي تساعدك في تحليل ومنع المهاجمات داخل المنظمة.

### What Is Information Security?

Information Security: is a set of tools and practices that you can use to protect your digital and analog information. It uses tools like authentication and permissions to restrict unauthorized users from accessing private information. These measures help you prevent harms related to information theft, modification, or loss.

هي مجموعة من الأدوات والمارسات التي يمكنك استخدامها لحماية معلوماتك الرقمية. يستخدم أدوات مثل المصادقة والأذونات لتقييد المستخدمين غير المصرح لهم من الوصول إلى المعلومات الخاصة. تساعدك هذه الإجراءات على منع الأضرار المتعلقة بسرقة المعلومات أو التعديل عليها أو ضياعها.

### Goals of Information security- أهداف أمن المعلومات:

#### CIA

**1- Confidentiality**: information must only be available to authorized parties .

**2-Integrity**: information must remain consistent, trustworthy, and accurate .

**3-Availability**: information must remain accessible to authorized parties, even during failures (with minimal or no disruption).

- 1- الخصوصية: منع غير المصرح لهم بالوصول والدخول على الشبكة.
- 2- السلامة: منع التعديل على البيانات الموجودة على الشبكة من قبل الأشخاص غير المصرح لهم.
- 3- الاتاحة: ان تكون الشبكة متاحة اي مقاومة لهجمات حجب الخدمة ان يكون 99% طوال العام متاحة.

### Identify and Authentication:

Identify: ترمز الى اسم المستخدم.

Authentication: ترمز الى كلمة السر.

### Authentication, Authorization, and Accounting (AAA):

AAA: is a model for access control.

هو نموذج للتحكم في الوصول

### Threat Types:

1 -Internal Threats.

1- تهديدات من داخل المنظمة.

2- External Threats.

2- تهديدات خارجية.



## Malware:

Malware (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals, or conducts virtually any behavior an attacker wants.

البرامج الضارة هي ملف أو رمز، يتم تسليمها عادةً عبر شبكة، والذي يصيب أو يستكشف أو يسرق أو يمارس أي سلوك يريد المهاجم تقويّاً.

## Malware types and methods:

**Viruses:** A Virus is a malicious executable code attached to another executable file. A virus needs a host program to run.

الفيروس هو جزء من كود كمبيوتر يدخل نفسه في كود برنامج مستقل آخر، ثم يجبر ذلك البرنامج على اتخاذ إجراءات ضارة ونشر نفسه على جهاز الضحية.

**Worm:** Standalone malware which replicates itself to spread to other computers.

الدودة هي جزء مستقل من البرامج الضارة التي تستنسخ نفسها وتنتشر من كمبيوتر إلى آخر.

**Ransomware:** is a flavor of malware that encrypts your hard drive's files and demands a payment, usually in Bitcoin, in exchange for the decryption key.

برامج الفدية هي جزء من البرامج الضارة التي تقوم بتشифر ملفات محرك الأقراص الثابتة وتطلب الدفع مقابل استعادة البيانات والحصول على مفتاح فك التشفير.

**Petya:** are ransomware. Without the decryption key, it's mathematically impossible for victims to regain access to their files

بيتيا، هي برامج الفدية. بدون مفتاح فك التشفير، من المستحيل رياضياً على الضحايا استعادة الوصول إلى ملفاتهم.

**Scareware:** is a sort of shadow version of ransomware; it claims to have taken control of your computer and demands a ransom but is just using tricks like browser redirect loops to make it seem as if it's done more damage than it really has, and unlike ransomware can be relatively easily disabled.

Scareware تعتبر نوعاً من نسخة الظل من برامج الفدية؛ يزعم أنه سيطر على جهاز الكمبيوتر الخاص بك ويطلب فدية ، ولكنه في الواقع يستخدم حيلاً مثل حلقات إعادة توجيه المتصفح لجعل الأمر يبدو كما لو أنه تسبب في ضرر أكبر مما حدث بالفعل ، وعلى عكس برامج الفدية يمكن تعطيلها بسهولة نسبياً.

**Crypto – Malware:** A crypto malware is a type of malware that allows threat actors to use someone else's computer or server to mine for cryptocurrencies.

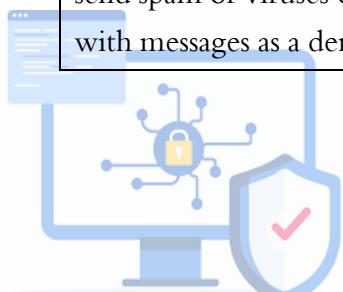
البرامج الضارة المشفرة هي نوع من البرامج الضارة التي تسمح للجهات الفاعلة بالتهديف باستخدام كمبيوتر أو خادم شخص آخر للتعدّين من أجل العملات المشفرة.

**Trojan Horse:** A trojan is a program that cannot reproduce itself but masquerades as something the user wants and tricks them into activating it so it can do its damage and spread.

حصان طروادة هو برنامج لا يمكنه إعادة إنتاج نفسه، ولكنه يتذكر كشيء يريد المستخدم وبخدعه لتنشيطه حتى يمكن من إحداث ضرره وانتشاره.



|  |  |
|--|--|
| <p><b>RATs:</b> A remote access Trojan (RAT) is a program used by the intruders to take complete control of the victim's computer for the purpose of performing various malicious activities. They operate in a stealth mode and are usually rather small to avoid detection.</p>    | <p>(RAT) هو برنامج يستخدمه المتسلين للسيطرة الكاملة على كمبيوتر الضحية بغضّن تنفيذ أنشطة ضارة مختلفة. تعمل في وضع التخفي وعادة ما تكون صغيرة نوعاً ما لتجنب الكشف عنها.</p>  |
| <p><b>Rootkit:</b> A rootkit is, a program or, more often, a collection of software tools that gives a threat actor remote access to and control over a computer or other system.</p>  | <p>المذور الخفية عبارة عن برنامج أو في أغلب الأحيان مجموعة من أدوات البرامج التي تتيح لممثل التهديد الوصول عن بعد إلى جهاز كمبيوتر أو نظام آخر والتحكم فيهما.</p>  |
| <p><b>Keylogger:</b> A keylogger is a specific kind of spyware that records all the keystrokes a user makes—great for stealing passwords.</p>  | <p>برنامج تسجيل المفاتيح هو نوع معين من برامج التجسس التي تسجل جميع ضغطات المفاتيح التي يقوم بها المستخدم. وهي رائعة لسرقة كلمات المرور.</p>   |
| <p><b>Adware:</b> Adware is malware that forces your browser to redirect to web advertisements, which often themselves seek to download further, even more malicious software.</p>   | <p>هي برنامج ضارة يجبر متصفحك على إعادة التوجيه إلى إعلانات الويب، والتي غالباً ما تسعى هي نفسها إلى تنزيل المزيد من البرامج الضارة.</p>   |
| <p><b>Spyware:</b> Spyware is malware used for the purpose of secretly gathering data on an unsuspecting user. it spies on your behavior as you use your computer, and on the data, you send and receive, usually with the purpose of sending that information to a third party.</p> | <p>برامج التجسس هي برامج ضارة تستخدم لغرض جمع البيانات سرّاً على المستخدم. إنه يتتجسس على سلوكك أثناء استخدامك لجهاز الكمبيوتر الخاص بك، وعلى البيانات التي ترسلها وتتلقاها، عادة بغرض إرسال تلك المعلومات إلى طرف ثالث.</p> |
| <p><b>Bots:</b> Bots, or Internet robots, while they may be utilized to perform repetitive jobs, such as indexing a search engine, they often come in the form of malware. Malware bots are used to gain total control over a computer.</p>  | <p>الروبوتات، أو روبوتات الإنترنت، على الرغم من إمكانية استخدامها لأداء مهام متكررة، مثل فهرسة محرك بحث، إلا أنها تأتي غالباً في شكل برنامج ضارة. تُستخدم روبوتات البرامج الضارة للسيطرة الكاملة على جهاز الكمبيوتر.</p>     |
| <p><b>Botnet:</b> A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack.</p>  | <p>الروبوتات عبارة عن عدد من أجهزة الكمبيوتر المختربة المستخدمة لإنشاء وإرسال بريد عشوائي أو فيروسات أو إغراق الشبكة بالرسائل كهجوم لرفض الخدمة.</p>   |



|   |  |
|---|--|
| <p><b>Logic Bombs:</b> logic bomb is a computer program often hidden within another seemingly innocuous program that is designed to perform usually malicious actions (such as deleting files) when certain conditions have been met.</p> | <p>القنبلة المنطقية هي برنامج كمبيوتر غالباً ما يتم إخفاؤه داخل برنامج آخر يبدو أنه غير ضار مصمم لأداء أعمال ضارة عادةً (مثل حذف الملفات) عند استيفاء شروط معينة.</p>  |
| <p><b>Malvertising:</b> is the use of online advertising to spread malware. It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.</p>                       | <p>استخدام الإعلانات عبر الإنترنت لنشر البرامج الضارة. يتضمن ذلك عادةً ضخ إعلانات ضارة أو محملة بالبرمجيات الخبيثة في شبكات إعلانات وصفحات ويب شرعية عبر الإنترنت.</p> |
| <p><b>Backdoors:</b> A backdoor is any method that allows someone to remotely access your device without your permission or knowledge</p>   | <p>الباب الخلفي هو أي طريقة تسمح لشخص ما بالوصول إلى جهازك عن بعد دون إذنك أو علمك</p>   |

## EMAIL ATTACKS:

|   |  |
|---|--|
| <p><b>Spam:</b> Spam (also known as junk mail) is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.</p>                                 | <p>البريد العشوائي (المعروف أيضاً باسم البريد غير الهام) هو بريد إلكتروني غير مرغوب فيه. يعد البريد العشوائي وسيلة إعلانية، ومع ذلك، يمكن للبريد العشوائي إرسال روابط ضارة أو برامج ضارة أو محتوى مخادع.</p>     |
| <p><b>Adware:</b> Adware is unwanted software designed to throw advertisements up on your screen, most often within a web browser. Some adware also monitors your behavior online so it can target you with specific ads.</p> | <p>Adware عبارة عن برنامج غير مرغوب فيه مصمم لعرض الإعلانات على شاشتك، وغالباً ما يتم ذلك داخل مستعرض ويب. تراقب بعض برامج الإعلانات المتسللة أيضاً سلوكك عبر الإنترنت حتى تتمكن من استهدافك بإعلانات محددة.</p> |
| <p><b>Pharming:</b> is the impersonation of an authorized website in an effort to deceive users into entering their credentials. Pharming misdirects users to a fake website that appears to be official.</p>                 | <p>هو انتقال هوية موقع ويب مصريح به في محاولة لخداع المستخدمين لإدخال بيانات اعتمادهم.</p>   |
| <p><b>Phishing:</b> A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.</p>  | <p>عبارة عن شخص يبدو أنه جدير بالثقة يطلب معلومات حساسة مثل أرقام بطاقات الائتمان أو معرفات تسجيل الدخول أو كلمات المرور عبر البريد الإلكتروني.</p>  |



|  |  |
|--|--|
| <b>Vishing:</b> is phishing using voice communication technology.  | هو عبارة عن التصيد باستخدام تقنية الاتصال الصوتي.                            |
| <b>Smishing:</b> is phishing using a text or SMS messaging on mobile phones.   | هو عملية تصيد احتيالي باستخدام الرسائل النصية على الهاتف المحمول.            |
| <b>Spear Phishing:</b> is phishing the cybercriminals target specific people through emails.                             | هو عملية تصيد احتيالي يستهدف أشخاصاً معينين من خلال رسائل البريد الإلكتروني. |
| <b>Whaling:</b> is a phishing attack that targets high profile targets within an organization such as senior executives. | هو هجوم تصيد يستهدف أهدافاً بارزة داخل المنظمة مثل كبار المديرين.            |

## WIRELESS AND MOBILE ATTACKS:

|   |   |
|---|---|
| <b>War driving:</b> is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection.  | هي طريقة يستخدمها المهاجمون للعثور على نقاط الوصول أيهما كانوا. مع توفر اتصال واي فاي مجاني.  |
| <b>WEP attack:</b> Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security. WEP uses a key for encryption. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks. | هو بروتوكول أمان حاول توفير شبكة محلية لاسلكية بنفس مستوى الأمان. يستخدم WEP مفتاحاً للتشифر. نظرًا لأن الجميع يستخدمون نفس المفتاح، فإن المجرم لديه حق الوصول إلى كمية كبيرة من حركة المرور للهجمات التحليلية. |
| <b>WPA attack:</b> Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and an authorized user.   | جاء الوصول الخفي بتقنية (WPA) ثم Wi-Fi WPA2 كبروتوكولات محسنة لتحل محل WEP . WPA2 عرضة للهجوم لأن مجرمي الإنترنت يمكنهم تحليل الحزم التي تنتقل بين نقطة الوصول والمستخدم المرخص له.                             |
| <b>Bluejacking:</b> is used for sending unauthorized messages to another Bluetooth device   | يُستخدم لإرسال رسائل غير مصرح بها إلى جهاز Bluetooth آخر.   |
| <b>Bluesnarfing:</b> is a way of stealing information using an unsecured Bluetooth connection. Hackers exploit vulnerabilities in Bluetooth technology to get access to contacts, messages, pictures, videos, and passwords.  | هي طريقة لسرقة المعلومات باستخدام اتصال Bluetooth غير آمن. يستغل المتسلين نقاط الضعف في تقنية Bluetooth للوصول إلى جهات الاتصال والرسائل والصور ومقاطع الفيديو وكلمات المرور.                                   |

|  |   |
|--|---|
| <b>RF Jamming:</b> consists of radio signals maliciously emitted to disrupt legitimate communications. Jamming attacks are a big threat to any type of wireless network.                                   | يتكون من إشارات لاسلكية تبعث بشكل ضار لتعطيل الاتصالات المشروعة. مثل هجمات التشویش تهدىءاً كبيراً لأي نوع من الشبكات اللاسلكية.   |
| <b>Rogue Access Points:</b> A rogue AP is a Wi-Fi Access Point that is set up by an attacker for the purpose of sniffing wireless network traffic to gain unauthorized access to your network environment. | نقطة الوصول المارقة هي نقطة وصول لشبكة Wi-Fi تم إعدادها بواسطة مهاجم بغرض التعرف على حركة مرور الشبكة اللاسلكية في محاولة للوصول غير المصرح به إلى بيئة الشبكة الخاصة بك. |

### APPLICATION ATTACKS:

|  |  |
|--|--|
| <b>Cross Site Scripting (XSS):</b> A code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.  | هجوم إدخال رمز يسمح للمهاجم بتنفيذ جافا سكريبت ضار في متصفح مستخدم آخر.  |
| <b>Code Injection:</b> is the malicious injection or introduction of code into an application. The code introduced or injected is capable of compromising database integrity and/or compromising privacy properties, security and even data correctness. | هو الحقن الخبيث أو إدخال التعليمات البرمجية في أحد التطبيقات. الشفرة التي تم إدخالها أو حقنها قادرة على المساومة على تكامل قاعدة البيانات أو المساومة على خصائص الخصوصية والأمان وحق صحة البيانات. |

### OTHER ATTACKS:

|  |  |
|--|--|
| <b>Social Engineering:</b> Social engineering manipulates people into performing actions or divulging confidential information. used of deception to gain information, commit fraud, or access computer systems. | تلاعب الهندسة الاجتماعية بالناس في أداء الإجراءات أو إفشاء المعلومات السرية. استخدام الخداع للحصول على معلومات أو ارتكاب عملية احتيال أو الوصول إلى أنظمة الحاسوب. |
| <b>Denial of Service (DOS) Attack:</b> Any attack where the attackers attempt to prevent the authorized users from accessing the service.  | أي هجوم يحاول فيه المهاجمون منع المستخدمين المصرح لهم من الوصول إلى الخدمة.  |
| <b>Distributed Denial-of-Service (DDOS):</b> is a type of attack where multiple systems are used to launch DOS attack on one targeted system.  | هو نوع من الهجوم حيث يتم استخدام أنظمة متعددة لشن هجوم DOS على نظام مستهدف واحد.   |
| <b>Man-in-the-Middle Attack:</b> This attack intercepts and relays messages between two  | يقوم هذا الهجوم باعتراض ونقل الرسائل بين طرفين يتواصلان مباشرة مع بعضهما البعض.  |



|   |  |
|---|--|
| parties who are communicating directly with each other.   |  |
| <b>Sniffing:</b> is the process of monitoring and capturing all the packets passing through a given network using sniffing tools  | هي عملية مراقبة والتقط جمجمة الحزم التي تمر عبر شبكة معينة باستخدام أدوات الاستئثار.   |
| <b>Zero-day Attacks:</b> A vulnerability in a system or device that has been disclosed but is not yet patched.  | ثغرة أمنية في نظام أو جهاز تم الكشف عنها، ولكن لم يتم تصحيحها بعد.   |
| <b>SQL injection:</b> A very common exploited web application vulnerability that allows malicious hacker to steal and alter data in website's database.   | ثغرة شائعة جدًا في تطبيقات الويب يتم استغلالها والتي تسمح للمتسلل الضار بسرقة البيانات وتعديلها في قاعدة بيانات موقع الويب.  |
| <b>Spoofing:</b> is the act of disguising a communication from an unknown source as being from a known, trusted source  | هي عملية تقويه اتصال من مصدر غير معروف على أنه من مصدر معروف وموثوق  |
| <b>ARP poisoning:</b> Also called as ARP Spoofing is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer or server on the network. It is used to do a Man-in-the-Middle attack.              | يرسل المهاجم رسائل ARP مزيفة عبر شبكة منطقة محلية (LAN) لربط عنوان MAC الخاص بالهاجم بعنوان IP لجهاز كمبيوتر أو خادم شرعي على الشبكة.  |
| <b>DNS Poisoning:</b> Also called as DNS Spoofing Type of cyberattack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones. This is done by introducing corrupt (poisoned) DNS data into DNS Resolver's Cache. | هو الهجوم الإلكتروني الذي يستغل نقاط الضعف في نظام اسم المجال (DNS) لتحويل حركة مرور الإنترنت بعيداً عن الخوادم الشرعية ونحو الخوادم المزيفة. يتم ذلك عن طريق إدخال بيانات DNS التالفة (المسمومة) في ذاكرة التخزين المؤقت لخادم DNS. |
| <b>Pass-the-hash</b> is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying hash of a user's password, instead of requiring the associated plaintext password as is normally the case.  | هي تقنية قرصنة تسمح للمهاجم بالصادقة على خادم أو خدمة بعيدة باستخدام التجزئة الأساسية لكلمة مرور المستخدم، بدلاً من طلب كلمة المرور ذات النص العادي كما هو الحال عادةً.  |
| <b>Scanning:</b> is a method for discovering exploitable communication channels .   | هي طريقة لاكتشاف قنوات الاتصال القابلة للاستغلال. البحث عن المنافذ المفتوحة البحث عن نقاط الضعف المعروفة.  |



|   |   |
|---|---|
| Scanning for open ports Scanning for known vulnerabilities.   |   |
| <b>Watering Hole Attacks:</b> is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware. Eventually, some member of the targeted group will become infected.                                    | هي عبارة عن إستراتيجية هجوم على الكمبيوتر يقوم فيها المهاجم بتخمين أو ملاحظة موقع الويب التي تستخدمها المؤسسة غالباً والقيام بإصابة واحد أو أكثر منها ببرامج ضارة. ثم سيصاب بعض أعضاء المجموعة المستهدفة بالعدوى.   |
| <b>Domain Hijacking:</b> is the act of changing the registration of a domain name without the permission of its original registrant, or by abuse of privileges on domain hosting and registrar software systems.  | اختطاف المجال هو عملية تغيير تسجيل اسم المجال دون إذن من المسجل الأصلي، أو عن طريق إساءة استخدام الامتيازات على استضافة المجال وأنظمة برامج المسجل.   |
| <b>Cryptographic Attacks:</b> is a method for circumventing the security of a cryptographic system by finding a weakness in a code, cipher, cryptographic protocol, or key management scheme.   | هي طريقة للتحايل على أمان نظام تشفير من خلال إيجاد نقطة ضعف في رمز، أو تشفير، أو بروتوكول تشفير، أو نظام إدارة مفتاح.   |
| <b>Evil Twins:</b> is a spoofing cyberattack that works by tricking users into connecting to a fake Wi-Fi access point that mimics a legitimate network. Once a user is connected to an “evil twin” network, hackers can access everything from their network traffic to private login credentials. | هجوم التوأم الشرير هو هجوم إلكتروني مخادع يعمل عن طريق خداع المستخدمين للاتصال بنقطة وصول Wi-Fi مزيفة تحاكي شبكة شرعية. بمجرد اتصال المستخدم بشبكة "التوأم الشرير"، يمكن للقراصنة الوصول إلى كل شيء من حركة مرور الشبكة الخاصة بهم إلى بيانات اعتماد تسجيل الدخول الخاصة. |



### الفصل الثالث/ بعض التقنيات المستخدمة في مركز عمليات امن المعلومات – SOC Technologies

#### Security incident and event management (SIEM)

Security incident and event management (SIEM) is the process of identifying, monitoring, recording, and analyzing security events or incidents within a real-time IT environment. It provides a comprehensive and centralized view of the security scenario of an IT infrastructure.

##### How Does SIEM Work?

SIEM software works by collecting log and event data produced from applications, devices, networks, infrastructure, and systems to draw analysis and provide a holistic view of an organization's information technology (IT).

##### Top SIEM tools:

- 1 -Splunk.
- 2 -IBM.
- 3 -Exabeam.
- 4 -LogRhythm.
- 5 -Microsoft.
- 6 -Rapid7.
- 7 -RSA.
- 8 -Securonix.
- 9 -FireEye.

Splunk, it was one of the first software vendors to discover gold in log file analysis. Splunk Enterprise Security draws on the company's mature data analytics and visualization capabilities to deliver a SIEM solution integrated with threat intelligence and available in the cloud or on prem. IDC maintains that Splunk has the largest SIEM market share.

إدارة الأحداث والحوادث الأمنية (SIEM) هي عملية تحديد ورصد وتسجيل وتحليل الأحداث أو الحوادث الأمنية داخل بيئة تكنولوجيا المعلومات في الوقت الفعلي. يوفر رؤية شاملة ومركبة لسيناريو الأمان للبنية التحتية لتكنولوجيا المعلومات.

##### كيف يعمل SIEM؟

يعمل برنامج SIEM من خلال جمع بيانات السجل والأحداث الناجمة عن التطبيقات والأجهزة والشبكات والبنية التحتية والأنظمة لرسم التحليل وتقديم نظرة شاملة لتقنية المعلومات الخاصة بالمؤسسة (IT).

##### أفضل أدوات SIEM:

- .Splunk -1
- .IBM -2
- .Exabeam -3
- .LogRhythm -4
- .Microsoft -5
- .Rapid7 -6
- .RSA -7
- .Securonix -8
- .FireEye -9

Splunk ، كان أحد بائعي البرامج الأوائل الذين اكتشفوا الذهب في تحليل ملف السجل. يعتمد Splunk Enterprise Security على Splunk Enterprise Security وقدرات التصور لتقديم حل SIEM مدمج مع معلومات التهديدات ومتاح في السحابة أو في مكان العمل. تؤكد IDC أن Splunk لديها أكبر حصة في سوق SIEM.

- سوف يتم شرح Splunk بشكل كامل في الفصل الرابع.



## Data loss prevention (DLP)

DLP strategies incorporate tools and practices that protect data from loss or modification. This includes categorizing data, backing up data, and monitoring how data is shared across and outside an organization. For example, you can use DLP solutions to scan outgoing emails to determine if sensitive information is being inappropriately shared.

تتضمن استراتيجيات DLP الأدوات والممارسات التي تحمي البيانات من الضياع أو التعديل. يتضمن ذلك تصنيف البيانات ونسخهااحتياطياً ومراقبة كيفية مشاركة البيانات عبر المؤسسة وخارجها. على سبيل المثال، يمكنك استخدام حلول منع فقدان البيانات (DLP) لفحص رسائل البريد الإلكتروني الصادرة لتحديد ما إذا كانت المعلومات الحساسة تتم مشاركتها بشكل غير لائق.

## Intrusion detection system (IPS)

Intrusion Prevention Systems (IPS) Do deep packet inspection (DPI) Try to spot attacks.

يقوم بكشف المهاجمات والحرص على ايقافها سواء بقطع الاتصال ب IP الذي يحاول الهجوم علينا عن طريق وضع access list.

## User behavioral analytics (UBA)

User behavior analytics (UBA) is a cybersecurity process about detection of insider threats, targeted attacks, and financial fraud that tracks a system's users. UBA looks at patterns of human behavior, and then analyzes them to detect anomalies that indicate potential threats.

Security systems provide so much information that it's tough to uncover information that truly indicates a potential for real attack . Analytics tools help make sense of the vast amount of data that SIEM, IDS/IPS, system logs, and other tools gather.

تحليلات سلوك المستخدم (UBA) هي عملية للأمن السيبراني تتعلق باكتشاف التهديدات الداخلية والمهاجمات المستهدفة والاحتيال المالي الذي يتبع مستخدمو النظام. تنظر UBA في أنماط السلوك البشري، ثم تحللها لاكتشاف الانحرافات التي تشير إلى التهديدات الخاطئة.

توفر أنظمة الأمان الكثير من المعلومات بحيث يصعب الكشف عن المعلومات التي تشير حفّاً إلى احتيال وقوع هجوم حقيقي.

تساعد أدوات التحليلات في فهم الكم الهائل من البيانات التي تجمعهاIDS / IPS وسجلات النظام والأدوات الأخرى SIEM.

## Endpoint detection and response (EDR)

EDR cybersecurity solutions enable you to monitor endpoint activity, identify suspicious activity, and automatically respond to threats. These solutions are intended to improve the visibility of endpoint devices and can be used to prevent threats from entering your networks or information from leaving. EDR solutions rely on continuous endpoint data collection, detection engines, and event logging.

تتيح لك حلول الأمن السيبراني EDR مراقبة نشاط نقطة النهاية وتحديد النشاط المشبوه والاستجابة تلقائياً للتهديدات. تهدف هذه الحلول إلى تحسين رؤية أجهزة نقطة النهاية ويمكن استخدامها لمنع التهديدات من دخول شبكاتك أو معلوماتك من المغادرة. تعتمد حلول EDR على التجميع المستمر لبيانات نقطة النهاية ومحركات الكشف وتسجيل الأحداث.



## Firewalls:

Firewalls are a layer of protection that you can apply to networks or applications.

These tools enable you to filter traffic and report traffic data to monitoring and detection systems.

Firewalls often use established lists of approved or unapproved traffic and policies determining the rate or volume of traffic allowed.

تعد جدران الحماية طبقة حماية يمكنك تطبيقها على الشبكات أو التطبيقات.

تتيح لك هذه الأدوات تصفية حركة المرور والإبلاغ عن بيانات حركة المرور لأنظمة المراقبة والكشف.

غالباً ما تستخدم جدران الحماية قوائم ثابتة لحركة المرور المعتمدة أو غير المعتمدة والسياسات التي تحدد معدل أو حجم حركة المرور المسموح بها.



## الفصل الرابع / Splunk

### Splunk:

Splunk is an advanced, scalable, and effective technology that indexes, and searches log files stored in a system. It analyzes the machine-generated data to provide operational intelligence. The main advantage of using Splunk is that it does not need any database to store its data, as it extensively makes use of its indexes to store the data.

Splunk هي تقنية متقدمة وقابلة للتطوير وفعالة تقوم بفهرسة ملفات السجل المخزنة في النظام والبحث فيها. يقوم بتحليل البيانات التي تم إنشاؤها بواسطة الآلة لتقديم تجارب تشغيلية. الميزة الرئيسية لاستخدام Splunk هي أنه لا يحتاج إلى أي قاعدة بيانات لتخزين بياناته، لأنه يستخدم على نطاق واسع فهارسه لتخزين البيانات.

### Splunk Overview:

Splunk Overview. (Splunk)



### Basic Searching in Splunk:

In this video we demonstrate how to perform basic searches, use the timeline and time range picker, and use fields in the Splunk Search & Reporting app.



### Creating Reports in Splunk Enterprise:

In this video We show you how to create reports to share with your users that can be scheduled to run automatically. Saving you time and letting you go home on time.



### **Create Dashboards in Splunk Enterprise:**

In this view we show you how to create a dashboard, giving you a single pane of glass into your machine data.



### **Creating Alerts in Splunk:**

This video will show you how to create alerts in Splunk Enterprise and settings to use to keep them from driving your users or yourself crazy.



## الفصل الخامس / Anti-Virus

### Anti-Virus:

Software that is created specifically to help detect, prevent, and remove malware (malicious software).

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

تُعرف برامج مكافحة الفيروسات بأنها مجموعة البرامج التي صُممت خصيصاً للكشف عن الفيروسات وإزالتها من أجهزة الكمبيوتر، بالإضافة إلى قدرتها على حماية أجهزة الكمبيوتر من مجموعة متنوعة من التهديدات كبرامج التجسس وبرامج أحصنة طروادة وغيرها من البرامج التي تعرف بالفيروسات.

### Antivirus Software Examples

- 1- Symantec.
- 2- Norton.
- 3- Panda.
- 4- McAfee.
- 5- avast.
- 6- AVG.
- 7- KASPERSKY.

### Symantec Endpoint Protection:

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities .

Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your client computers against known and unknown threats, such as viruses, worms, Trojan horses, and adware .

Symantec Endpoint Protection provides protection against even the most sophisticated attacks that evade traditional security

هو حل خادم العميل الذي يحمي أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر المكتبية والخوادم في شبكتك من البرامج الضارة والمخاطر ونقاط الضعف.

يجمع Symantec Endpoint Protection بين الحماية من الفيروسات والحماية المتقدمة من التهديدات لتؤمن أجهزة الكمبيوتر العميلة بشكل استباقي ضد التهديدات المعروفة وغير المعروفة، مثل الفيروسات والدودان وأحصنة طروادة وبرامج الإعلانات المتسللة.

يوفر Symantec Endpoint Protection الحماية ضد أكثر المجموعات تعقيداً التي تتهرب من إجراءات الأمان التقليدية، مثل أدوات Zero-day وهجمات rootkits وبرامج التجسس التي تتغير.



measures, such as rootkits, zero-day attacks, and spyware that mutates.

### Symantec Endpoint Protection Console Overview:

This video about Symantec Endpoint Protection Manager Console Over View, where will learn how to use SEPM Console. (Mr. Harvansh Singh)



### How to Create SEP Client Package:

This video about how to create a SEP client package in Symantec Endpoint Protection Manager. (Mr. Harvansh Singh).



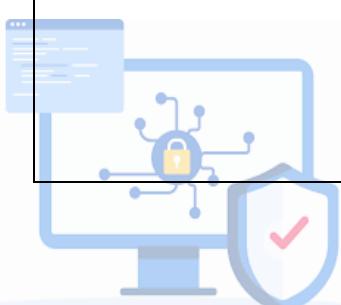
### Symantec Endpoint Protection Home Page Overview:

This video about home Page overview. (Mr. Harvansh Singh).



### Symantec Endpoint Protection Monitors Overview:

This video about Monitors Page overview. (Mr. Harvansh Singh).



### **Symantec Endpoint Protection Reports Overview:**

This video about, Overview for Reports in Symantec Manager. (Mr. Harvansh Singh).



### **Symantec Endpoint Protection Clients Overview:**

This video about Clients Overview. (Mr. Harvansh Singh).



## **الفصل السادس / منهجية الاستجابة للحوادث السيبرانية:** " دليل الاستجابة للحوادث السيبرانية، ثامر الشمرى، 2022 ."

عدم وجود إطار وخطة للاستجابة للحوادث الأمنية لدى المنظمات والشركات يؤدي إلى تفاقم الضرر الحال وتوسيع دائرة العوّق من ورائه، بسبب الملل والقرارات المتعجلة وغير مدروسة التي يتم اتخاذها حال اكتشاف الحادثة الأمنية.

### **إطار الاستجابة للحوادث من NIST**

#### **1- الاستعداد:**

إنشاء وتأسيس إطار إدارة الحوادث الازمة، ووضع سياسات وإجراءات الاستجابة للحوادث، توظيف وتدريب مسؤولي الاستجابة للحوادث، الحصول على الأدوات والبرامج الازمة، إنشاء أو استخدام برنامج تتبع للحوادث الأمنية، وضع سياسات وإجراءات للتقارير المتعلقة بالحوادث الأمنية، تحديد سياسات وإجراءات وعمليات وأدوات الكشف عن الحوادث الأمنية.

#### **2- الاكتشاف والتحليل:**

توعية الموظفين بضرورة الإبلاغ عن الاختراقات الأمنية وعمليات الخداع والتصيد من خلال تعريفهم بما وبأيّواعها، ووضع الإجراءات والسياسات المناسبة لذلك والمراقبة الأمنية.

#### **3- الاحتواء والقضاء والاستعادة:**

- حصر الأصول التقنية المصابة وتحديدها.
- اخذ نسخة رقمية للأجهزة المصابة والبدء بتحليلها.
- تحليل البرمجيات والملفات الضارة.
- حصر مؤشر الاختراق.
- حجب مؤشرات الاختراق من الشبكة.
- التأكيد من خلو الشبكة من مؤشرات الاختراق.
- عزل الأنظمة المصابة.
- إعادة تعيين الأنظمة المصابة.
- تفعيل خطة التعافي.

#### **4- ماذا بعد الحادثة؟**

ويتم التركيز هنا على ما تم تعلمه من الحادثة لتحقيق هدفين:

الأول: تطوير قدرة الاستجابة للحوادث.

الثاني: منع حصول الاختراق نفسه مرة أخرى.

وذلك من خلال الإجابة على الأسئلة التالية:

- ما الذي حدث فعلياً؟ من خلال تعرير زمني مفصل عن الحادثة وما تم ومتى تم خلال عملية الاستجابة لها.
- ما هي الإجراءات التي فشلت أو لم تصل بكفاءتها إلى مستوى الحادثة؟
- هل تم ارتكاب أية أخطاء منعت أو أثرت على عملية الاستجابة للحادثة؟
- هل يجب علينا مراجعة السياسات، والإجراءات، وتحسينها، وتطويرها؟
- كيف كان من الممكن منع حصول هذه الحادثة؟ وكيف منع حدوثها مستقبلاً؟



### **أشياء لا يجب عملها أثناء الاستجابة للحوادث السيبرانية:**

- عدم إيقاف الأنظمة المصابة، بل يفضل عرطاً عن الشبكة بعد التحليل الأولي للحادثة.
- عند أخذ نسخة كاملة من النظام لا يجب العبث بها وإنما يتم أخذ نسخة إضافية لأجل التحليل.
- التأكد بعد أخذ نسخة من الذاكرة العشوائية RAM بعد وجود تشفير على مستوى القرص الصلب وفي حال وجوده يجب عمل نسخة للنظام قبل إيقاف تشغيله.
- استخدام حسابات مدراء الأنظمة للاستجابة للحادثة يادي إلى استغلالها من قبل المهاجم.
- تشغيل برمجيات على الأنظمة المصابة غير مخصصة للاستجابة للحوادث.
- استرجاع نسخة احتياطية من النظام المصاب مما يسبب في عودة المهاجم بعد عملية التعافي، بل يجب فحص والتأكد من سلامة النسخة الاحتياطية من وجود أي برمجيات ضارة.

### **أبرز الحوادث السيبرانية الشائعة وطرق التعامل معها:**

#### **1- تسريب البيانات :Information Leakage**

تسريب البيانات هو عبارة عن نقل بيانات من المنظمة إلى جهة خارجية غير مصرح لها الإطلاع عليها.

الخطوات:

##### **- الاستعداد:**

- تصنيف البيانات داخل المنظمة.
- تجهيز خطة الاستجابة للبيانات المسروقة.
- الاشتراك في خدمات استخبارات التهديد (Threat Intelligence) لمعرفة أي تسريب لبيانات المنظمة.
- تطبيق برمجيات امنية لمنع حدوث تسرب لبيانات.

##### **- الاكتشاف والتحليل:**

- تحديد سبب التسرب هل حدث من الداخل أو طرف ثالث.
- البحث من خلال محركات البحث أو قواعد بيانات خارجية لاي تسرب بيانات.
- أداة منع تسرب البيانات تساعد في اكتشاف سبب التسرب (DLP).

##### **- الاحتواء والازالة والتعافي:**

- تعليق حساب الموظف بعد التأكيد ان التسرب حدث من خالله.
- عزل الجهاز لعمل تحليلات جنائية رقمية على النظام.
- إعادة تعيين كلمات السر للحسابات التي ظهرت في التسرب.
- التواصل مع الموقع الإلكتروني الذي تم كشف البيانات فيه لحذف البيانات فوراً.
- تخليل البيانات المسروقة واتخاذ اللازم لجعلها عديمة الفائدة.

#### **2- البريد التصيدي : (Phishing)**

التتكر على هيئة جهة جديدة بالثقة عن طريق رسائل بريد الكتروني للحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور او تفاصيل بطاقة الائتمان وذلك لأسباب ونوايا ضارة.



- في حال المستخدم استقبل الرسالة وتفاعل مع البريد الإلكتروني التصيدي بالضغط على الرابط او فتح الرفق عليه اتباع الارشادات أدناه:

الاجراء:

- عزل النظام عن الشبكة.
  - تغيير كلمات السر الخاصة بالمستخدم وكذلك أي كلمات سر مستخدمة أو محفوظة بالنظام.
  - فحص الملفات او الروابط المتضمنة بالبريد من خلال معمل خاص لفحص الفيروسات ومعزول عن الشبكة الداخلية والعمل على استخراج مؤشرات الاختراق IOCs.
  - التحليل من خلال مركز السجلات المركزية (SEIM) من اتصالات مشبوهة أنشئت من قبل نظامه او أجهزة أخرى داخل النظام.
  - التأكيد من عدم وجود أي حالات تصيد مشابهه في البريد الالكتروني للمستخدمين الآخرين من خلال إدارة بوابة البريد الالكتروني وفي حال وجود مستقبلين آخرين يتم ارسال تنبيه أمني بعدم التجاوب مع البلاغ.
  - حجب مصدر الرسالة وكذلك الروابط الضارة من خلال أنظمة الحماية.
  - فحص النظام من خلال برامجيات الحماية والتأكد من خلوها من برامجيات الضارة.
  - استعادة النظام المصايب للشبكة بعد التأكيد من خلوها من الأنشطة الضارة
- في حال ان المستخدم استقبل الرسالة ولم يتفاعل مع البريد الالكتروني عليك اتباع الارشادات التالية:
- فحص الملفات او الروابط المتضمنة بالبريد من خلال معمل خاص لفحص الفيروسات ومعزول عن الشبكة الداخلية واستخراج مؤشرات الاختراق IOCs.
  - التأكيد من ان المستخدمين لم يقوموا بالتفاعل سواء القيام بفتح الرابط الضار او الملفات المرفقة او بالرد على المرسل وتستطيع التحقق من ذلك من خلال مركز السجلات (SEIM) او إدارة البوابة الالكترونية للبريد.
  - التأكيد من عدم وجود أي حالات تصيد مشابهه في البريد الالكتروني للمستخدمين الآخرين من خلال إدارة بوابة البريد الالكتروني وفي حال وجود مستقبلين آخرين يتم ارسال تنبيه أمني بعدم التجاوب والبلاغ.
  - حجب مصدر الرسالة وكذلك الروابط الضارة من خلال أنظمة الحماية.
- البريد المزعج او الاقتحامي (Spam): 3

يتم حجب مصدر الرسالة من قبل برامج الحماية او من خلال إدارة بوابة الالكترونية للبريد.



المراجع:

- .1 دليل الاستجابة للحوادث السيبرانية، ثامر الشمري، 2022.
  - .2 تكنولوجيا أمنية المعلومات وأنظمة الحماية، علاء حسين الحمامي، سعد عبدالعزيز العاني، 2007.
  - .3 احتراف إنشاء وادارة الشبكات ضمور، قصي نايل، 2015.
- /https://www.gispp.org/2022/03/04/email-security-email-attacks-types .4  
https://www.splunk.com/en\_us/about-splunk.html. .5
- https://www.broadcom.com/products/cyber-security/endpoint .6  
/https://docs.microsoft.com/en-us .7
- https://www.exabeam.com/security-operations-center/security-operations- .8  
/center-roles-and-responsibilities  
/https://byjus.com/govt-exams/computer-virus .9
- /https://www.imperva.com/learn/data-security/data-loss-prevention-dlp .10
- https://www.techopedia.com/definition/4097/security-incident-and-event- .11  
management-siem  
.CCNA .12  
.Security+ .13





## Certificates

