# الأكاديمية العربية الدولية


## الأكاديمية العربية الدولية

## المقررات الجامعية

www.aiacademy.info | care@aiacademy.info

# أساسيات الأمن السيبراني

إعداد
حسن الحسين

# ملخص المحاور

السياسات الخاصة في أمن المعلومات
الهجوم
التحكم التقني
التحكم الإداري

تقييم الثغرات
الهندسة الإجتماعية
حماية البيانات
الجدار الناري
التشفير
الضوابط المادية
المعايير

أساسيات الحماية

الهندسة الإجتماعية

السرية والتشفير

خدمات التحقق وكيفية الإستخدام الامن للحسابات

ادارة المخاطر والثغرات، الفرق بين انواع البرمجيات الخبيثة والثغرات

حماية الأجهزة الملموسة

اساسيات حماية الشبكات

VPNs الجدار الناري وبرمجيات حماية البيانات و

الحماية وسياسة الخصوصية في التطبيقات والانظمة وأخيراً أهم الطرق المتبعة للحد من الإختراقات وتسريب البيانات

CIA

Cyber Security Fundamentals • Free

CSF

السياسات الخاصة في أمن المعلومات

نموذج مصمم لتوجيه السياسات الخاصة بأمن المعلومات داخل المنظمة. ويشار اليها ايضا AIC لتجنب الالتباس مع وكالة الاستخبارات المركزية.


- Confidentiality - السرية
- Integrity - النزاهة
- Availability - التوفر


# ماهو CIA

| Confidentiality (CIA)<br>السرية | Integrity (CIA)<br>النزاهة | Availability (CIA)<br>التوفر |
|---|---|---|
| **Encryption - التشفير**<br><br>إدارة عملية الدخول:<br>• Identification - Username<br>• Authentication - Password<br>• Authorization - Permissions<br><br>**Steganography - اخفاء البيانات**<br><br>• الرسائل الخفية داخل المواقع<br>• الرسائل الخفية داخل الملفات والصور | **التأكد من عدم العبث بالبيانات**<br><br>التشفير<br>إنشاء كود مشتق من خلال خوارزمية، إذا تم تغيير البيانات ، فسيتم تغيير الكود في المستقبل أيضًا<br><br>**Digital Signatures, Certificates, and Non-Repudiation**<br>إرسال توقيع رقمي فريد، بتوضيح من أرسل الرسالة ومن يسمح للمستلم بقراءتها<br><br>**PKI - Public Key Infrastructure**<br>تمكن التوقيعات والشهادات للعمل من خلال الحفاظ مفاتيح التشفير وإدارة الشهادات | **ضمان إمكانية استرداد البيانات عند الحاجة إليها**<br><br>• أي فشل SPOF يتوقف النظام بأكمله عن العمل<br>• Disk Redundancy تكرار القرص<br>• Server Redundancy تكرار الخوادم<br>• Load Balancing - توزيع الحمل<br>• Site Redundancies - الزيادات في الموقع<br>• Backups - النسخ الاحتياطية<br>• Alternate Power - الطاقة البديلة<br>• Cooling Systems - تبريد النظام<br>• Patching - الترقيع |

# Authentication Services خدمات المصادقة

خدمات المصادقة هي آلية مماثلة لاستخدام كلمات المرور في أنظمة مشاركة الوقت، المصادقة هي عملية التعرف على هوية المستخدم.
تتم مقارنة بيانات المستخدم المقدمة بتلك الموجودة في ملف في قاعدة بيانات لمعلومات المستخدم المصرح له على نظام تشغيل محلي أو داخل خادم مصادقة.

**Ownership**
Access card with photo

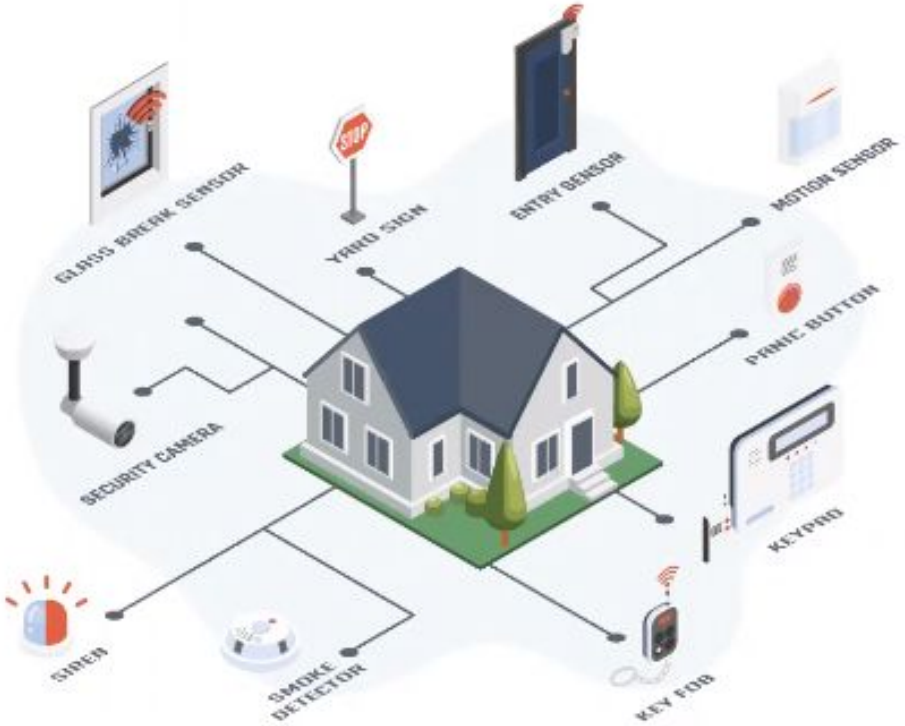

**Knowledge**
User name and password

**Biometrics**
Iris recognition

## أنواع الخدمات :

1. Kerberos
2. Asymmetric Encryption Key
3. LDAP and Secure LDAP - Lightweight Directory Access Protocol
4. SSO - Single Sign On
5. RAS - Remote Access Service Authentication

# Control Implementation - طرق التحكم




تقسم التحكم إلى ثلاث أقسام:

1. Technical Controls - التحكم التقني

إدارة التقنيات المستخدمة

2. Management Controls - التحكم الإداري

استخدم الأساليب الإدارية

3. Operational Controls - تحكم العمليات

يتم تنفيذه من قبل الناس في العمليات اليومية

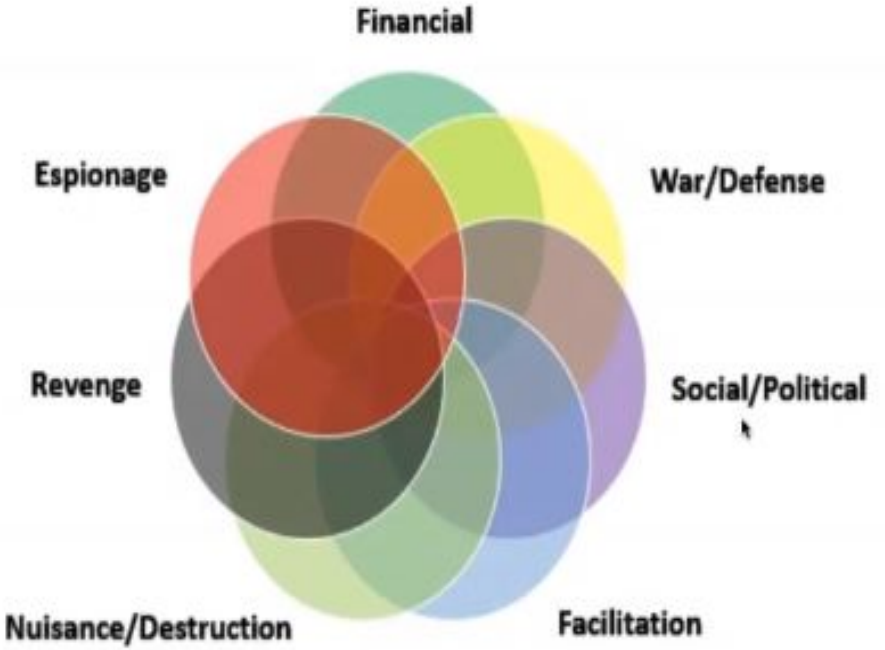
**Attack**
**الـهجوم**

Cyber Security Fundamentals • Free

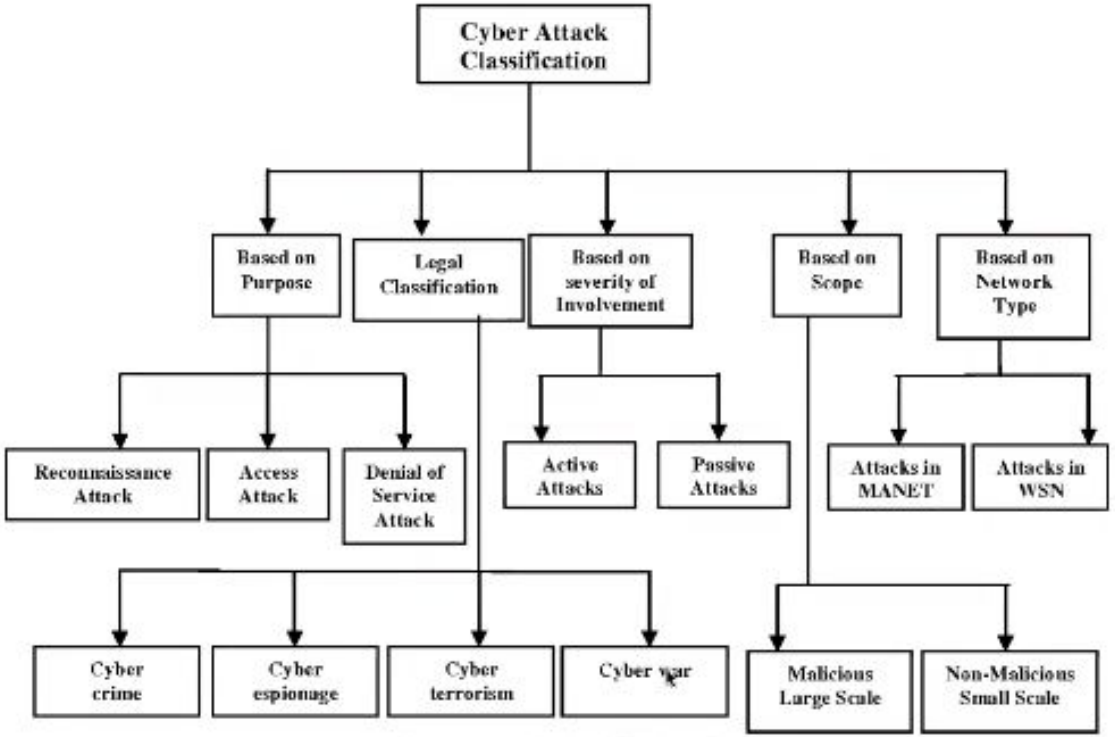
CSF

**Attacks** = Motivate + Method + Vulnerability

**الهجوم** = الهدف + الطريقة + الثغرة



# Attack Classifications

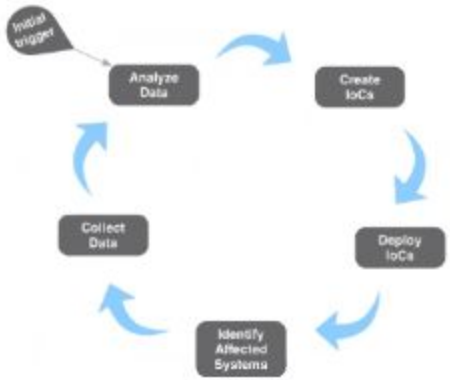


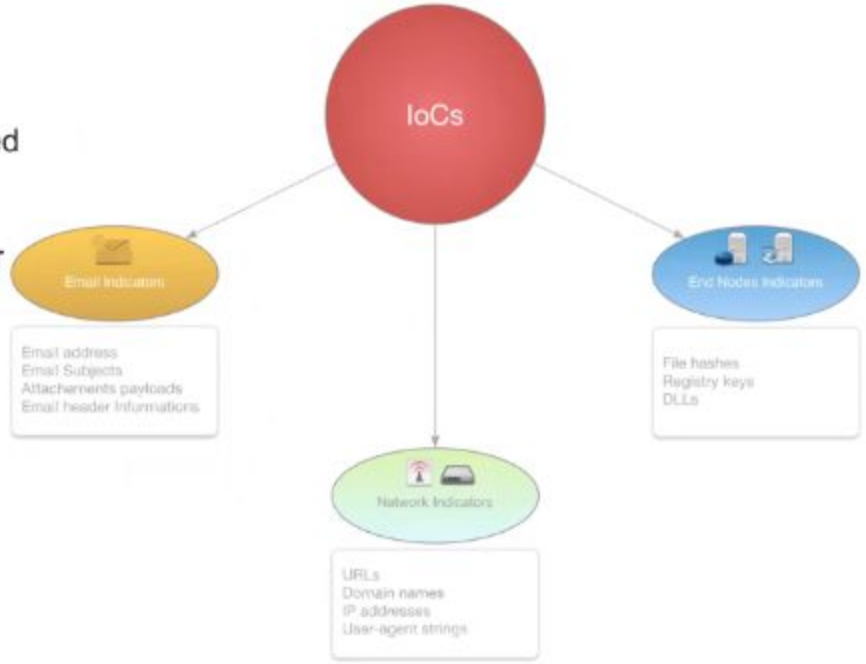

https://www.airitilibrary.com/Publication/alDetailedMesh?DocID=18163548-201309-201309100001-201309100001-390-396

# Indicators of compromise (IOCs)

Forensic evidence of potential intrusions on a host system or network.

Data that indicates a system may have been infiltrated by a cyber threat. They provide cybersecurity teams with crucial knowledge after a data breach or another breach in security




علامات تدل على الإختراق

# IOCs vs IOAs


IOCs
Malware, Signatures, Exploits, Vulnerabilities, IP Addresses
REACTIVE INDICATORS OF COMPROMISE
VS
PROACTIVE INDICATORS OF ATTACK
IOAs
Code Execution, Persistance, Stealth, Command Control, Lateral Movement

# Hacker Types


مجرم

دفاع

مبتدء

هجومي
مفيد

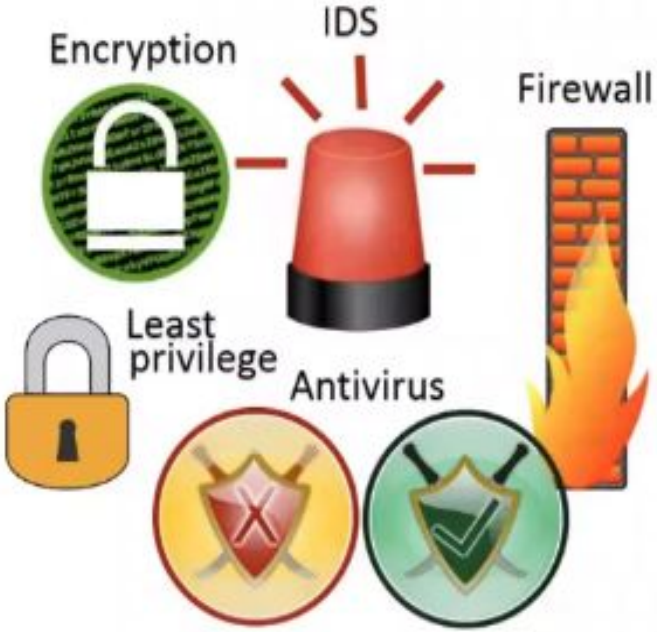
# Hacking Steps

# التحكم التقني
# Technical Controls

Cyber Security Fundamentals • Free

CSF

# Technical Controls الضوابط التقنية




## تثبيت التقنيات بواسطة مسؤول الحماية التلقائية وتقليل من الثغرات الأمنية

- **Encryption** - التشفير
- **Antivirus Software** - برامج حماية البرمجيات الخبيثة والفيروسات
- **IDSs- Intrusion Detection Software** - برامج كشف التسلل
  - رصد وتقرير عمليات الدخول الى الخوادم
- **Firewalls** - الجدار الناري
  - تقييد حركة مرور الإدخال / الإخراج إلى خادم أو مضيف
- **Least Privilege** - إدارة الإمتيازات
  - السماح فقط لكل مستخدم بالحد الأدنى من الامتيازات التي يحتاجها للحد من المخاطر في حالة حدوث خطأ ما
- **Motion detectors** - نظام كشف التحركات
  - أنظمة إخماد الحرائق وغيرها من الأجهزة

# التحكم الإداري
# Management Controls

Cyber Security Fundamentals • Free

CSF

# Threat VS Risk VS Vulnerability

Threat تهديد

Vulnerability ثغرة

Risk - خطر

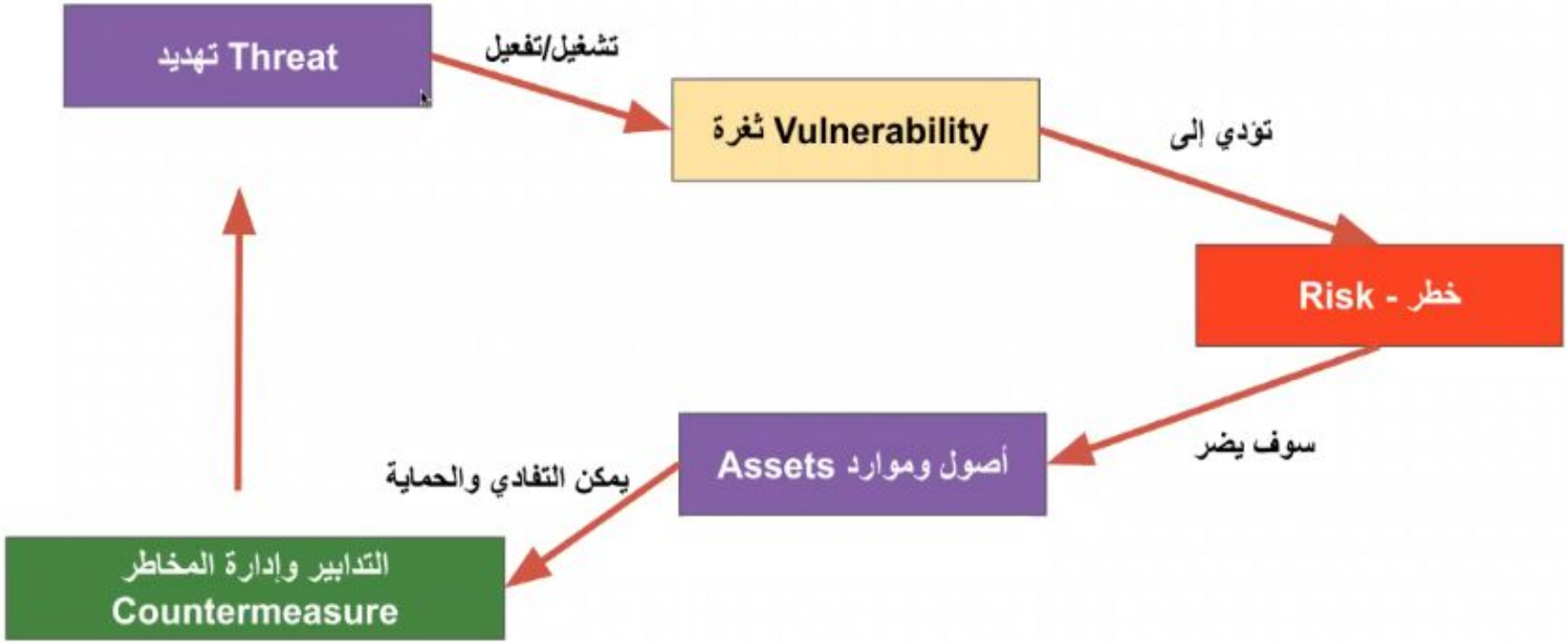
# Threat VS Risk VS Vulnerability

Threat تهديد

Vulnerability ثغرة

Risk - خطر

# Threat VS Risk VS Vulnerability



# Management Controls - التحكم الإداري

تُعرف أيضًا باسم الضوابط الإدارية ، وهي تستخدم التخطيط والتقييم لتقليل المخاطر.

1. تقييم المخاطر - Risk Assessment
   - Quantitative Assessment - التقييم الكمي ( يستخدم قيم التكلفة والأصول لتحديد تكلفة حماية القيمة للأصول )
   - Qualitative Assessment - التقييم النوعي ( تصنيف المخاطر على أساس الاحتمالية والتأثير )


2. تقييم الضعف - Vulnerability Assessment

تُستخدم لاكتشاف نقاط الضعف للمساعدة في تحديد أولويات تنفيذ الضوابط الأمنية

3. اختبارات الاختراق - Penetration Tests

محاولات لاستغلال الثغرات لتحديد مدى سهولة القيام بذلك ، وما هي التأثيرات الفعلية

# Assessment Types - أنواع التقييم

تنقسم أنواع التقييم للمخاطر والتهديدات الى ثلاث اقسام: (Risks, Threats, and Vulnerabilities)


1. المخاطر - Risks

تقييم المخاطر احتمالية الخسارة أو الضرر وعواقبه (التكلفة)

2. التهديدات - Threats

مصادر أو دوافع الأشخاص والأشياء التي يمكن أن تسبب الخسارة أو الضرر

3. نقاط الضعف - Vulnerabilities

ضعف أو ثغرة في النظام يمكن استغلاله للدخول على النظام.

# Threats and Threat Vectors - التهديدات ونواقل التهديد

تنقسم التهديدات الى عدة اقسام، تحديد نوع التهديد:

1. التهديدات الطبيعية مثل ( الحرائق - الزلازل - الفيضانات .... )
2. التهديدات البشرية الخبيثة ( السرقة - استياء الموظف وما إلى ذلك - ..... )
3. التهديدات البشرية العرضية ( الغير مقصودة )
4. التهديدات البيئية ( انقطاع التيار الكهربائي على المدى الطويل - انسكاب المواد الكيميائية - .... )
5. التهديد الخبيث من الداخل ( شخص لديه وصول إلى الموارد الداخلية ويسعى إلى استغلالها - الامتيازات )

# Managing Risk - إدارة المخاطر


تنقسم أنواع إدارة المخاطر Managing Risk إلى

1. التهديدات وناقل التهديد - Threats and Threat Vectors
2. تقييمات التهديد - Threat Assessments
3. إدارة المخاطر - Risk Management
4. تقييم المخاطر - Risk Assessment

# تقييم التهديدات - Threat Assessments

## ماهو Threat Assessments تقييم التهديدات:

تقييم التهديد هو عملية تحديد مصداقية وخطورة التهديدات و احتمال أن يصبح التهديد حقيقة واقعة. تقييم التهديد يحدد ما مدى احتمالية وجود أشياء معينة ، وما الذي يسبب أكبر ضرر؟ ونقاط الضعف مثل

- عدم التحديث
- الإعدادات الافتراضية
- عدم وجود حماية من البرامج الضارة
- عدم وجود جدار ناري
- عدم وجود سياسات تنظيمية

# Risk Management - إدارة المخاطر

إدارة المخاطر الأمنية وسيلة لفهم طبيعة التهديدات الأمنية وتفاعلها على المستوى الفردي أو التنظيمي أو المجتمعي. عملية إدارة المخاطر تندرج تحت سياق إدارة المخاطر الأمنية.


| | |
|---|---|
| Risk Avoidance<br>تجنب المخاطر | لا تشارك في نشاط غير آمن وإذا تطلب منك أمر ما لفتح منافذ غير آمنة أسأل نفسك لو الأمر يستحق المجازفة |
| Risk Transference<br>تحول المخاطر | هل يمكنك مشاركة المخاطرة مع طرف آخر أو عرضها لهم ؟ |
| Risk Acceptance<br>قبول المخاطر | هل ستكون حماية الجهاز أكثر تكلفة مما يستحقه الجهاز؟<br>ما هي التكلفة الحقيقية للخسارة مقابل تكلفة الحماية ؟ |
| Risk Mitigation<br>تخفيف المخاطر | تقليل المخاطر باستخدام أحدث التقنيات |
| Risk Deterrence<br>ردع المخاطر | تصعيب أمان النظام لجعلك هدف غير جذاب |

# Risk Management - إدارة المخاطر

1
**Identification -**
التحقق من الهوية

2
**Assessment -**
التقييم

3
**Mitigation -**
تخفيف الخطر

4
**Prevention -**
الوقاية والحماية

# تقييم المخاطر - Risk Assessment

## ماهو Risk Assessment تقييم المخاطر:

تقييم المخاطر هي جزء من عملية إدارة المخاطر في العديد من المنظمات في جميع أنحاء العالم. وهي تقييم التهديدات ونقاط الضعف لموارد وعمليات المنظمة وهو جزء مهم من عمل الفريق الأمني و يجب السيطرة على كل نقطة ضعف و إزالة المخاطر أو تخفيفها أو تخصيصها أو قبولها ، ولكن لا يمكن تجاهلها.

## الخطوات:

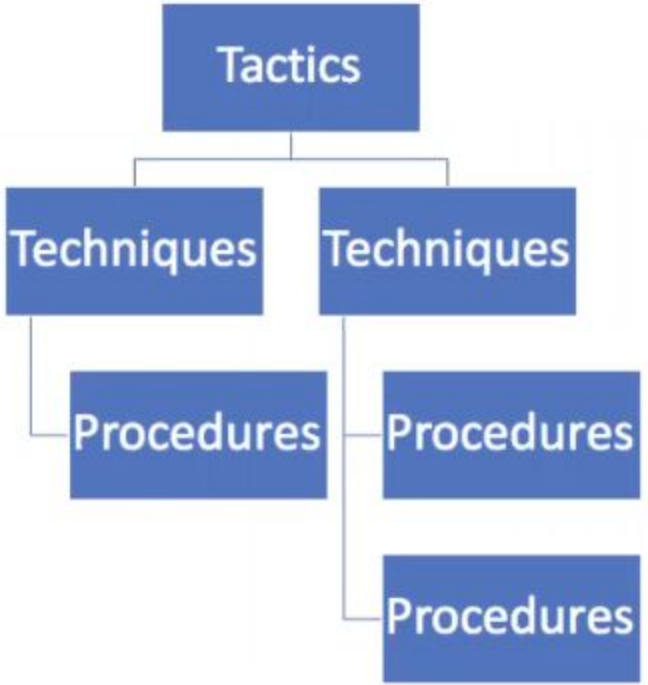
1. تحديد الموارد والتهديدات وتوثيقها
2. تحديد درجة المخاطر المرتبطة بكل أصل وإجراء
3. تقييم المخاطر الكمية
4. تقييم المخاطر النوعي
5. تقييم الضعف
6. توثيق التقييم

# Risk Assessment - تقييم المخاطر

| Quantitative Risk Assessment<br>تقييم المخاطر الكمية | Qualitative Risk Assessment<br>تقييم المخاطر النوعية | Documenting the Assessment<br>توثيق المخاطر | Metrics to Assess Risk<br>معايير متبعة للتقييم |
|---|---|---|---|
| القيمة النقدية المحددة للأصول مقابل التكلفة المحددة لتخفيف الضوابط<br><br>1- توقع الخسارة الفردية - SLE Single Loss Expectancy<br><br>2- توقع معدل الحدوث بالسنة ARO Annual Rate of Occurrence<br><br>3- توقع الخسارة السنوية ALE Annual Loss Expectancy | الحكم على أساس الاحتمالية والتأثير<br><br>1- هل الاحتمالية واضحة؟<br><br>2- التأثير يشمل فقدان السرية أو النزاهة أو توافر بيانات النظام<br><br>3- الاستعانة بمجموعة من الخبراء لتحديد المخاطر والتأثير<br><br>4- تعيين أرقام على مقياس من 1 إلى 10 لتسهيل عملية التقييم مخاطرة | تقديم تقرير يتضمن المخاطر والحلول الموصى بها<br><br>1- للإدارة إمكانية مراجعة هذه التقارير لاتخاذ القرارات النهائية<br><br>2- التقرير النهائي يوثق المخاطر التي تم قبولها للتخفيف من حدتها<br><br>3- احرص على عدم تسريب هذا التقرير | Mean Time Between Failure (MTBF)<br>متوسط الساعات بين حالات الخطأ<br><br>Mean Time to Failure (MTTF)<br>الفترة الزمنية التي يكون فيها الجهاز بالخدمة قبل حدوث الخلل<br><br>Mean Time to Recover (MTTR)<br>متوسط طول الوقت لاستعادة ملف النظام |

# Tactics, Techniques, and Procedures (TTPs)

Tactics, Techniques, and Procedures (TTPs) are the behaviors, methods, tools and strategies that cyber threat actors and hackers use to plan and execute cyber attacks on business networks. In short, they are the why and how of cyber attacks that provide information to businesses on how to respond to breaches and prevent future breaches from similar threat actors.


مجموعة من الطرق التي تحدد السلوك والادوات التي يستخدمها المخترق لفهم طريقة عمله لتقليل الخطر

# Cyber Kill Chain

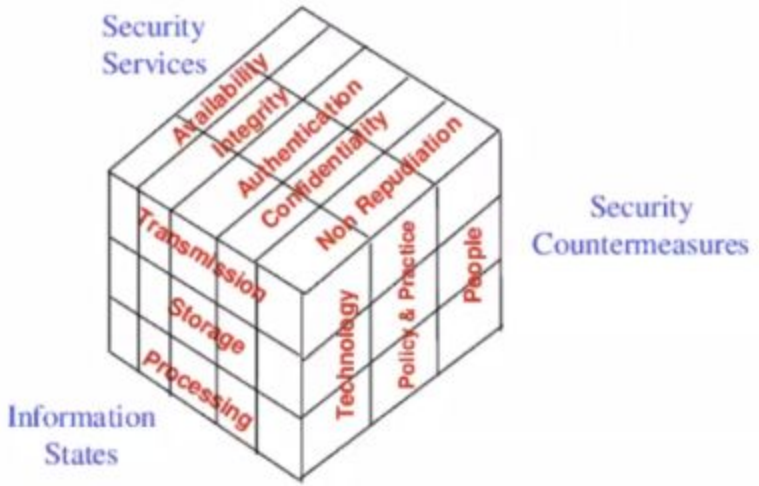
A series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).


فهم العمليات التي يقوم فيها المخترق لتلافيها والحماية وهي لفهم الاختراقات التي يتم استخدامها وتلافيها

# Information Assurance (IA)

The practice of assuring information and managing risks related to the *use, processing, storage, and transmission of information.*

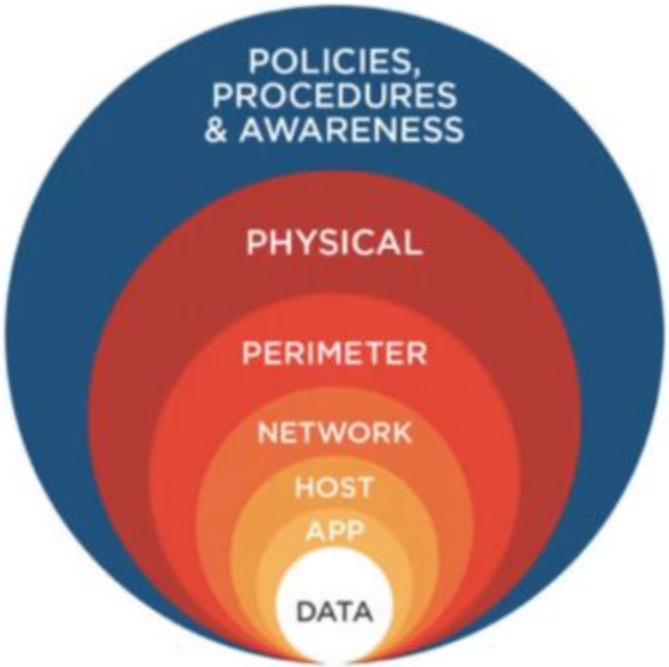
Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data




هي التاكد للاستخدام من سلامة البيانات والتحقق منها وعدم الانكار في الاستلام والسرية يجب توفرها لحماية الداتا

# Defense in Depth (DiD)

An information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within




طبقات الحماية لتفعيل الحماية من الاختراقات والتصعيب عليه في حال اخترق احدى الطبقات وكل طبقة مختلفة وحمايتها الخاصة

# Defense in Depth (DiD)

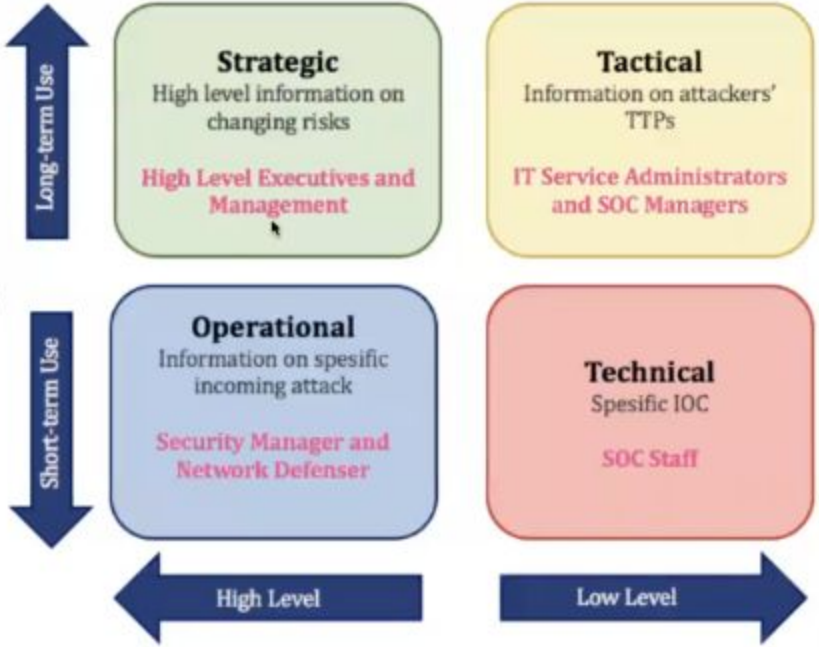

توفير طبقات الحماية

# Cyber Threat Intelligence - CTI

A collection and analysis of information about current and potential attacks that threaten the safety of an organization or its assets.

The benefit of threat intelligence is that it's a proactive security measure, preventing data breaches and saving you the financial costs of cleaning up after an incident.

Its purpose is to give companies an in-depth understanding of the threats that pose the greatest risk to their infrastructure and tell them what they can do to protect their business




تجميع المعلومات لحل المشاكل التقنية ومعالجة الاختراق لحماية الاصول

# Incident management (IcM)

An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions.

The activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.


الخطر

ادارات المخاطر


تسجيلها

ترتيبها

الاهمية

حل المشكلة

# Operational Controls التحكم العمليات

الممارسات والعمليات التي ينفذها الأشخاص وفقًا لخطة الأمان الشاملة.

- التوعية والتدريب ( يمنع الهندسة الاجتماعية ، التوعية حول استخدام كلمات المرور )
- التكوين/التهيئة وإدارة التغيير ( كل نظام يبدأ في الأساس على الأمان وأن التغييرات لا تبطل ميزات الأمان )
- التخطيط للطوارئ - يقلل التأثير الكلي إذا حدث خطأ ما من خلال التجهيز لخطط الطوارئ البديلة
- حماية الوسائط - لا تفقد الأقراص الصلبة بسبب رخص ثمنها
- الحماية المادية والبيئية - الكاميرات وأقفال الأبواب وأنظمة التكييف

# تقييم الثغرات
# Vulnerability Assessment

Cyber Security Fundamentals • Free

CSF

# Vulnerability Assessment - تقييم الضعف

خلال هذه العملية يتم مسح وفحص نقاط الضعف والمنافذ، تحديد الموارد والمخاطر، إعطاء الأولوية للعوامل التي سوف يتم استخدامها للتخفيف من المخاطر

## Vulnerability Scanning - فحص الضعف

تحديد نقاط الضعف

تحديد الخطأ في إعدادات التهيئة

- Open Ports
- Weak Passwords
- Default accounts and pass
- Sensitive Data - DLP
- Security and Configuration Errors

اختبارات الضوابط الأمنية بشكل سلبي

يحدد نقص الضوابط الأمنية

## Other Assessments - تقييمات أخرى

- التحقق من وجود مخاطر الهندسة الاجتماعية
- التحقق من وعي الموظفين
- مراجعة الكود (الملفات المصدرية)
- مراجعة هجوم السطح
- مراجعة الهيكلية للنظام
- مراجعة تصميم النظام

# Vulnerability Assessment - تقييم الضعف

| Credentialed v.s Non-credentialed | Penetration Testing | White, Black, Gray Box | Obtaining Consent | Passive v.s Active Tools | Continuous Monitoring |
|---|---|---|---|---|---|
| يمكن تشغيل أنواع متعددة من الفحص أسماء المستخدمين لمعرفة المخاطر على مستويات مختلفة من وصول المستخدمين | -محاولة استغلال الثغرات الأمنية لإكتشاف الثغرات<br>-التحقق من التهديدات<br>-تجاوز الضوابط الأمنية<br>-اختبار الضوابط الأمنية<br>-استغلال الثغرات<br>-تجربة حقن قواعد البيانات SQL | -القبعة البيضاء<br>-القبعة السوداء<br>-القبعة الرمادية | - لا تختبر اختراق الانظمة بدون موافقة خطية (عقد)<br>- استخدم وثيقة rules of" "engagement | - فحص الثغرات الأمنية PASSIVE<br>- عملية الاختراق ACTIVE | المراقبة المستمرة |

# الهندسة الإجتماعية
# Social Engineering, Malware

Cyber Security Fundamentals

CSF

# الهندسة الإجتماعية

## معنى الهندسة الإجتماعية ؟

**فن التلاعب بالأشخاص لأداء أفعال أو الإقرار بمعلومات حساسة. يتم بواسطة الإغراء والخداع، تشجيع الآخرين على إفشاء المعلومات الحساسة، انتحال شخصية شخص ما،**


- **بيانات الاتصال**
- **البريد الإلكتروني**
- **المعلومات البنكية**
- **الأصدقاء والعلاقات**
- **العمل**

# خطوات الهندسة الإجتماعية

- **الوصول الجهة المستهدفة**

( الموقع, الموظفين, نبذة عن الجهة المستهدفة وغيرها)

- **اختيار أضحية معينة**

البحث عن الشخص الضعيف المحبط المتردد

- **بناء علاقة**

يتم بناء علاقة مع الموظف لبناء الثقة المتبادلة

- **استغلال العلاقة**

يتم استغلال العلاقة لجمع البيانات الحساسة مثل بيانات المالية والتقنيات المستخدمة حاليا في جهة العمل

# كيف يتم استغلال الضحية عبر الهندسة الإجتماعية


- الهاتف
- البحث في المهملات
- الإقناع (استغلال عواطف الضحية )
- الهندسة الاجتماعية المعاكسة (Identity Theft)
- استغلال الشائعات
- استغلال المواضيع الساخنة
- استغلال موضوع الأمن الرقمي وضعف الخبرة التقنية للضحية
- استغلال السمعة الجيدة لتطبيقات معينة
- اصطياد كلمات السرّ Passwords Phishing
- خيانة الثقة

# البرمجيات الخبيثة

## البرمجيات الخبيثة - Malware

البرامج الضارة (بالإنجليزية: Malware) (وهي اختصار لكلمتين هما (بالإنجليزية: malicious software). البرمجيات الخبيثة عُبارة عن برمجيات تم تصميمها من أجل تدمير و إتلاف الحاسوب الخاص بك وتتضمن الفيروسات العادية, Trojans, Worms, Rootkits يتم تثبيتها في نظام الضحية لجمع بيانات الضحية مثل كلمات المرور واسم المستخدم والبريد الإلكتروني.


Adware


Ransomware


Trojan


Computer Viruses


Spear Phishing


Scareware


Worms


Rootkits


Spyware


Keyloggers


Bots

# البرمجيات الخبيثة

| Virus - الفيروس | Worm - الدودة | Ransomware - فيروس الفدية | Trojan Horse - حصان طروادة | Phishing Website - الإصطياد |
|---|---|---|---|---|
| نوع من أنواع البرامج الخبيثة وهو برنامج يقوم بعملية نسخ ذاتية وتكاثر داخل الجهاز بهدف تعطيل او حذف الملفات بدون إذن الضحية. ويمكن إصابة الفيروس بالجهاز اما ان يكون مدمج مع صورة، ملف صوتي او فيديو او برنامج، او عبر تحميلها بدون علم الضحية | دودة الحاسوب هدفها سرقة بيانات بعض المستخدمين أثناء تصفحهم للإنترنت. تنتشر بسبب الثغرات في نُظم التشغيل, و بُناءً على ذلك, يُفَضل تحميل و تنصيب التحديثات المُختَلفة لنظام التشغيل في أسرع وقت مُمكن. | برنامج خبيث يقيد الوصول إلى نظام التشغيل أو تشفر جميع البيانات المخزنة على جهاز الكمبيوتر، ويطالب بدفع فدية مالية من أجل التمكين من الوصول للملفات. | هي شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته. | محاولة الحصول على البيانات الشخصية لغرض سرقة الهوية، اما عن طريق بريد الكتروني او رسالة نصية وهمية تظهر بمظهر الرسائل الحقيقية الرسمية. تهدف لسرقة كلمات المرور، ارقام الحسابات البنكية، رقم الهوية الوطنية. |

# الحماية من البرمجيات الخبيثة

- Anti-Malware on Mail Servers
- Anti-Malware on All Systems
- Boundaries or Firewalls
- Antivirus Software
  - Signature-Based Detection
  - Behaviour-Based Detection
  - Checking File Integrity
  - Pop-up blockers o Spam Filters
  - Anti-Spyware

# حماية البيانات
# Protecting Data

Cyber Security Fundamentals

CSF

# حماية البيانات

- الحفاظ على البيانات المحفوظة على محرك الأقراص الثابتة ( الهارديسك ) ، سواء كان ذلك محرك أقراص فلاش أو نسخًا احتياطية
- الحفاظ على البيانات أثناء النقل عبر الشبكات ومنع فقدان البيانات
- تشفير البيانات باستخدام IPsec أو SSH أو SFTP
- احرص على تشفير البيانات المخزنة واحتفظ بها مشفرة عند إرسالها
- تشفير الأقراص الصلبة
- تشفير محتويات قواعد البيانات
- تشفير الأجهزة
- تفعيل خدمات المصادقة Authentication

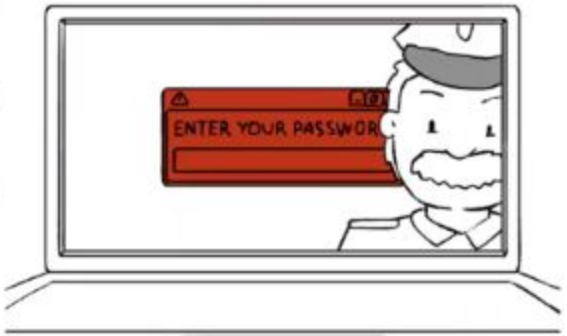
# حماية كلمات المرور والبريد الالكتروني

## حماية كلمة المرور

- عدم استخدام المعلومات الشخصية في كلمات السر
- استخدام كلمات سر معقدة ارقام وحروف ورموز
- عدم استخدام نفس كلمة السر لجميع الحسابات
- تغيير كلمة السر بين فترة و فترة
- حساب الادمن لابد أن يتغير كل شهر

## حماية البريد الإلكتروني

- إنشاء كلمة مرور قوية
- استخدام كلمات مرور مختلفة وعدم تكرارها
- استخدام التحقق الثنائي
- عدم فتح المرفقات دون التأكد من مصدرها
- عدم مشاركة كلمات السر
- معرفة ايميلات التصيد




شرح تنبئ كلمات السر في نظام الاختراق

الجدار الناري، خدمات

Firewall, IDs, VPNs, Honeypot

Cyber Security Fundamentals • Free

CSF

# الجدار الناري - Firewall

## Firewall:

عبارة عن نظام مصمم لمنع الدخول الغير مصرح به للشبكة الخاصة. الجدار الناري له نوعان قد يكون عبارة عن برنامج او جهاز او كلاهما.

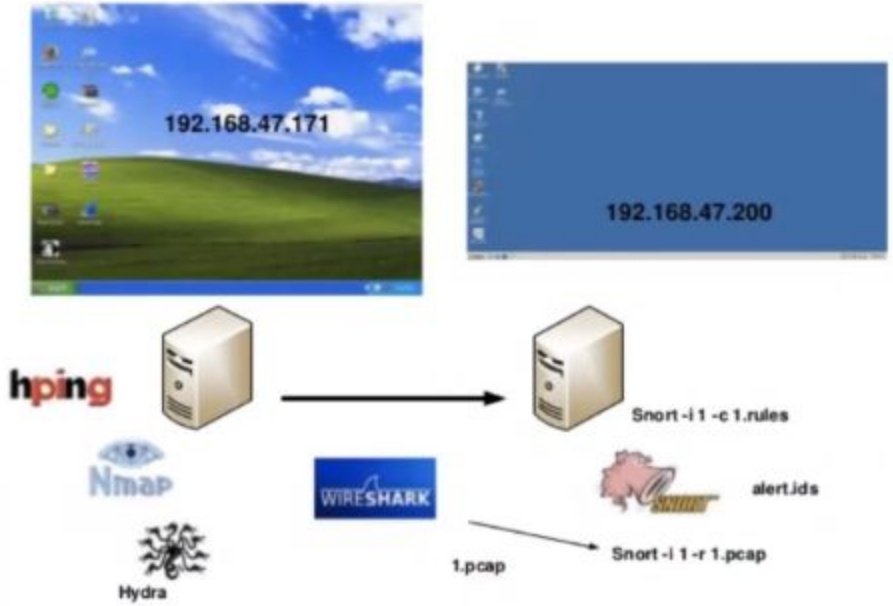
# أنواع Firewall - الجدار الناري

| | | | |
|---|---|---|---|
| Circuit Level Gateways |  | Packet Filters |  |
| Stateful Multilayer Inspection Firewalls |  | Application Level Gateways |  |

## ماهو IDS ؟

**Intrusion Detection System**

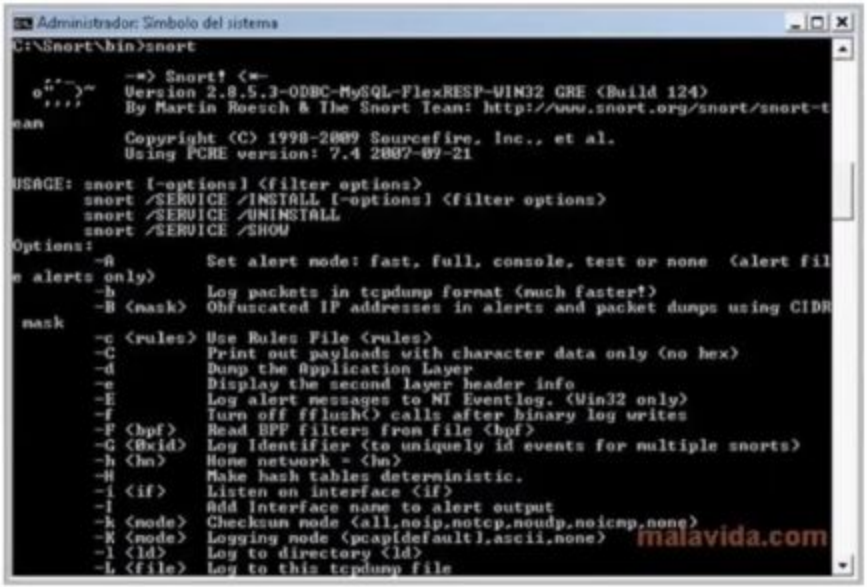
نظام حماية يشبه مضاد الفيروسات الموجود على أجهزتنا يقوم بتحليل كل Traffic عبر الشبكة. الهدف من IDS هو تحليل الـ Traffic وتحذيرنا في حالة كان هناك خطر محتمل أو هجمة محتملة تستهدف جهازنا أو شبكتنا.




## أهميته في عالم الانترنت؟

- كشف الثغرات الموجودة في أنظمة الحماية
- أرشفة كل أنواع التهديدات التى تحدث للشبكة
- تحديد الأخطاء التي وقع فيها مسؤولين الحماية وتصحيحها

# IDs - Intrusion Detection Tool: Snort

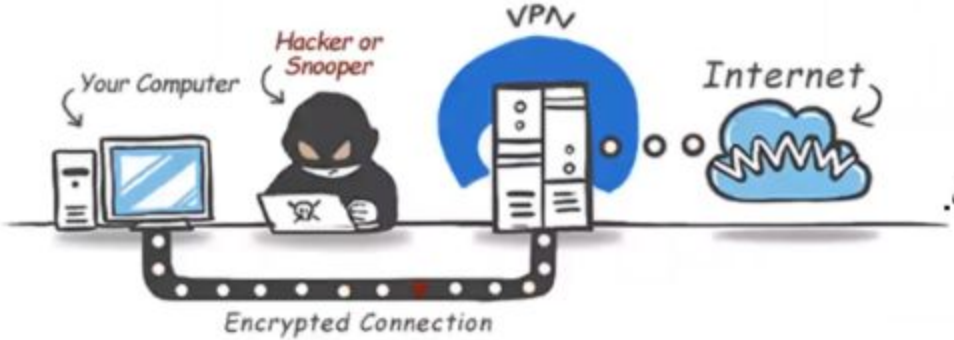



- نظام مفتوح المصدر للتعرف على الشبكات المصابة او المخترقة.
  وتحليل بيانات الإتصال و حزم البيانات في الشبكة بشكل مباشر وحي
- إمكانية تحليل البروتوكولات ومحتوى البحث والتطابق وتستخدم ايضا للتعرف على الهجمات مثل: buffer overflows, stealth port scan, CGI attacks
- مرونة في الاستخدام وسهولة في شرح كيفية جمع الإتصالات او عبور والتعرف على الآلة والهيكلة
- يستخدم سنورت Snort:
  - اشتمام حزم لبيانات مثل tcpdump
  - packet logger
  - نظام لمنع الشبكات من الإختراق او التلاعب

# VPNs

## ماهو تعريف VPN ؟

الـ **VPN** هي عبارة عن توصيل شبكتين أو جهازين عن طريق الإنترنت، حيث تقوم بتشفير البيانات لحمايتها من السرقة وإخفاء هوية المستخدم.




## مميزات VPN ؟

- لن تستطيع الشركة المزودة لخدمة الإنترنت التطفل على بياناتك.
- تصفح الإنترنت بأكثر أماناً وسرية.
- منع تتبع المخترقين والمتطفلين.
- تشفير جميع البيانات التي تستخدمها على الإنترنت.

# Honeypot - المصيدة

نظام مصادر معلوماتية متخصصة لإصطياد وجذب المستخدمين الذين يحاولون اختراق شبكة الشركة

لا تحتوي على تصاريح لنشاطاتها ولا تحتوي على حماية واي اتصال بها يكون عبارة عن هجوم

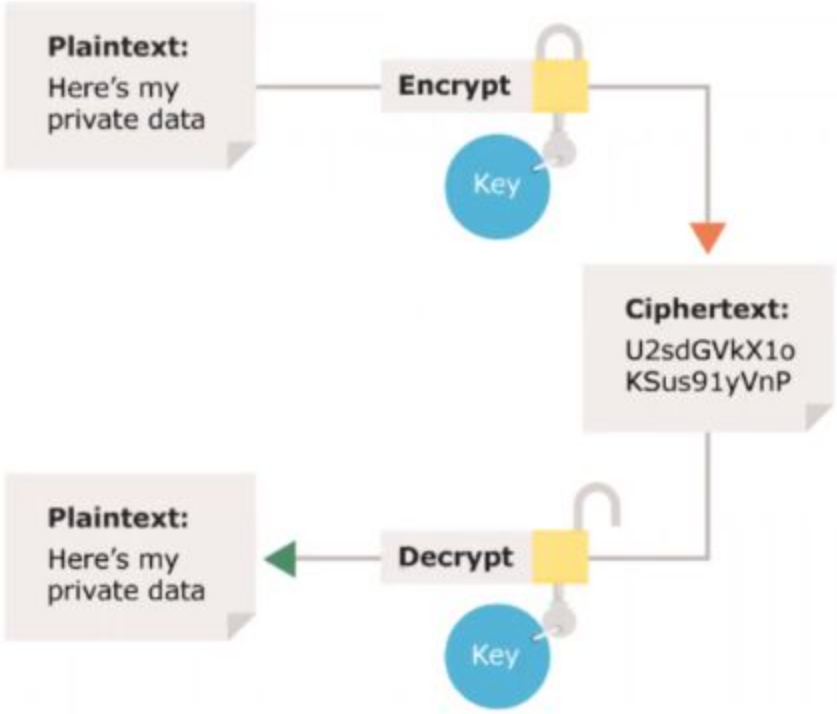
هي منفذ لمحاولة دخول او لمتابعة المخترق و ضربات الكيبورد الخاصة بالمخترق.

# التشفير
# Encryption

Cyber Security Fundamentals

CSF

# التشفير




## معنى التشفير ؟

يعرف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة.

أهداف التشفير:

1. السرية
Confidentiality

2. المصادقة (التحقق)
Authentication

3. السلامة
Integrity

4. عدم الإنكار
Non-repudiation

# الضوابط المادية
# Physical Controls

Cyber Security Fundamentals • Free

CSF

# الأمن المادي

الأمن المادي هو حماية الأشخاص والممتلكات والأصول المادية من الإجراءات والأحداث التي يمكن أن تسبب ضررًا أو خسارة وذلك يشمل حمايتها من الحرائق والكوارث الطبيعية والسطو والتخريب

# الضوابط المادية Physical Controls

- Perimeter - المحيط
  - ( الإحاطة سياج كبير مثل الجيش )
- Building - البناء
  - ( أربعة جدران وباب كبير مغلق )
- Secure Work Areas - مناطق العمل الآمنة
  - ( لا تدع الناس الذين ليس من المفترض أن يكونوا هناك )
- Server and Network Rooms - غرف الخوادم والشبكات
  - يسمح لموظفي التقنية فقط بالدخول واستخدم أقفالا
- Hardware - العتاد
  - أكثر اقفالاً

# Physical Controls الضوابط المادية

- **Doors - الابواب**
  - أقفال بالتشفير
  - بطاقات التعريف الشخصية
  - البصمة
  - ID شارات الهوية الشخصية
  - Tailgating - الملاحقة
  - قوائم وسجلات الأحداث والدخول
  - الأقفال أقفال كمبيوتر محمول والخزائن وقفل والخزائن
  - سياسة المجموعات
  - تحديد امتيازات الدخول Least Privilege

# حماية الأجهزة

- تحديث الجهاز
- استخدام الجدار الناري
- تثبيت برامج ضد الفيروسات
- استخدام برامج ضد التجسس
- استخدام كلمات سر معقدة
- تجاهل البريد العشوائي

- إغلاق الكمبيوتر في حين عدم استخدامه
- عدم فتح أي مرفقات بدون التأكد من مصدرها
- تشفير الملفات المهمة
- استخدام الاتصال الآمن


# Standards
# المعايير

Cyber Security Fundamentals

CSF

# ISO 27001

ISO/IEC 27001 is an international standard on how to manage information security.
It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure.


المعيار الامني كمسابقات الايزو للحمياية وتوفير الحماية لجميع ادوات الشركة وتحصل على شهاداتها في توفير الامان

# General Data Protection Regulation
# GDPR

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business.



حماية البيانات على النظام الاوربي وكيف تحمي بيانات المواطنين وكيف تخزنها وتعالجها الطرق القانونية لحماية المستخدمين في اوربا

# Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. It was launched on September 7, 2006, to manage PCI security standards and improve account security throughout the transaction process. An independent body created by Visa, MasterCard, American Express, Discover, and JCB, the PCI Security Standards Council (PCI SSC) administers and manages the PCI DSS.


توفير الحماية للبنوك وهي اساسيات حماية البنوك

# Health Insurance Portability and Accountability Act
# HIPAA

It modernized the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addressed some limitations on healthcare insurance coverage.[3] It generally prohibits healthcare providers and healthcare businesses, called covered entities, from disclosing protected information to anyone other than a patient and the patient's authorized representatives without their consent. With limited exceptions, it does not restrict patients from receiving information about themselves.


معيار حماية بيانات المرضة الطبية في امريكا والمستخدمين المرضا

إعداد المدرب " حسن الحسين