COMPTIA SECURITY +

1. مفاهيم الأمن العامة

- **إيه هو؟:** أساسيات حماية المعلومات.
- **المهم:**
- **CIA Triad:**
  - Confidentiality (السرية): حماية البيانات من الوصول غير المصرح به (مثل التشفير).
  - Integrity (النزاهة): التأكد إن البيانات ماتتغيرش (مثل Hashing).
  - Availability (التوفر): ضمان استمرارية الخدمات (مثل النسخ الاحتياطي).
- **Controls:**
  - Preventive: منع الهجمات (مثل Firewall).
  - Detective: كشف الهجمات (مثل IDS).
  - Corrective: إصلاح الضرر (مثل النسخ الاحتياطي).
- **Authentication (AAA):**
  - Authentication: التحقق من الهوية (مثل كلمة السر أو MFA).
  - Authorization: تحديد الصلاحيات.
  - Accounting: تسجيل الأنشطة.
- **التشفير:**
  - Symmetric: مفتاح واحد (مثل AES).
  - Asymmetric: مفتاحين (Public وPrivate، مثل RSA).
- **نصيحة:** افهم الـ CIA Triad كويس لأنها أساس كل حاجة.

2. التهديدات والثغرات

- **إيه هو؟**: فهم الهجمات والثغرات وطرق الحماية.
- **المهم:**
  - **أنواع الهجمات:**
    - **Social Engineering**: مثل Phishing (خداع المستخدمين).
    - **DDoS**: إغراق الخادم بطلبات.
    - **Malware**: فيروسات، Ransomware، Spyware.
  - **الثغرات:**
    - في التطبيقات (مثل SQL Injection).
    - في الأجهزة (مثل عدم تحديث النظام).
    - في السحابة (مثل سوء إعدادات).
  - **الحماية:**
    - تحديث الأنظمة (Patching).
    - استخدام Firewalls وAntivirus.
    - Network Segmentation (تقسيم الشبكة).
- **نصيحة**: جرب أدوات زي Wireshark لفهم الهجمات.

3. هندسة الأمن

- **إيه هو؟**: تصميم شبكات وأنظمة آمنة.
- **المهم:**
  - **Secure Network Design**:
    - VLANs: تقسيم الشبكة للأمان.
    - DMZ: منطقة عازلة للخوادم العامة.
  - **Cloud Security**: حماية البيانات في السحابة (مثل AWS أو Azure).
  - **Zero Trust**: تحقق من كل اتصال، حتى داخل الشبكة.
- **نصيحة**: افهم إزاي DMZ بتحمي الخوادم.

4. عمليات الأمن

- **إيه هو؟**: إدارة الأمن اليومي والاستجابة للحوادث.
- **المهم:**
  - **Identity Management:**
    - إدارة حسابات المستخدمين (مثل Single Sign-On).
    - التحقق متعدد العوامل (MFA).
  - **Monitoring:**
    - استخدام SIEM لمراقبة Logs.
    - كشف التسلل (IDS/IPS).
  - **Incident Response:**
    - خطوات: الكشف، الاحتواء، الإصلاح، الاستعادة.
- **نصيحة:** جرب TryHackMe لفهم الـ Incident Response.

5. إدارة برامج الأمن

- **إيه هو؟**: إدارة المخاطر والامتثال.
- **المهم:**
  - **القوانين:**
    - GDPR: حماية بيانات العملاء في أوروبا.
    - HIPAA: حماية بيانات الصحة.
    - PCI-DSS: أمان الدفعات الإلكترونية.
  - **Risk Management**: تحديد المخاطر وتقليلها.
  - **Security Awareness**: تدريب الموظفين على تجنب Phishing.
- **نصيحة:** راجع أمثلة قوانين زي GDPR.