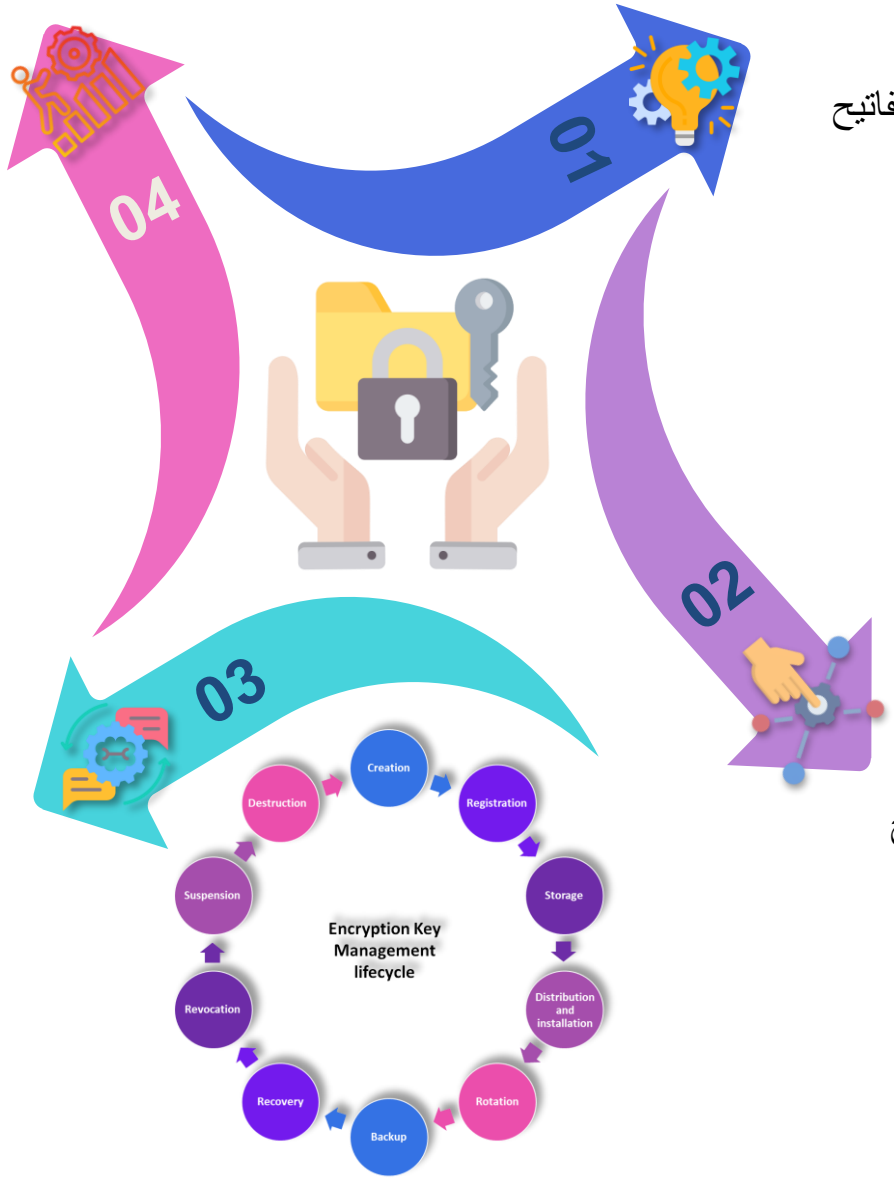
Encryption Key Management

مفهوم إدارة مفاتيح التشفير

- إدارة مفاتيح التشفير هي عملية إنشاء، توزيع، وتخزين مفاتيح التشفيربطريقة آمنة لضمان حماية البيانات المشفرة ومنع الوصول غير المصرح به

آلية العمل

- يتم إنشاء مفاتيح تشفير جديدة لحماية البيانات، وتخزينها في أماكن آمنة، وتوزيعها فقط على المستخدمين المصرح لهم للوصول إلى البيانات المشفرة



المزايا والتحديات

- **المزايا**: تضمن حماية البيانات حتى في حالة وقوعها في أيدي غير مصرح لهم
- **التحديات**: يتطلب إدارة دقيقة للمفاتيح، وإذا تم فقدان المفتاح، قد يصبح من المستحيل استعادة البيانات المشفرة

الاستخدامات العملية

- تُستخدم في المؤسسات التي تتعامل مع كميات كبيرة من البيانات الحساسة، مثل البنوك، لضمان أمان البيانات المشفرة أثناء النقلوالتخزين

Threat Intelligence

مفهوم استخبارات التهديدات

- عملية جمع وتحليل البيانات حول التهديدات الأمنية المتوقعة لاتخاذ التدابير الوقائية

آلية العمل

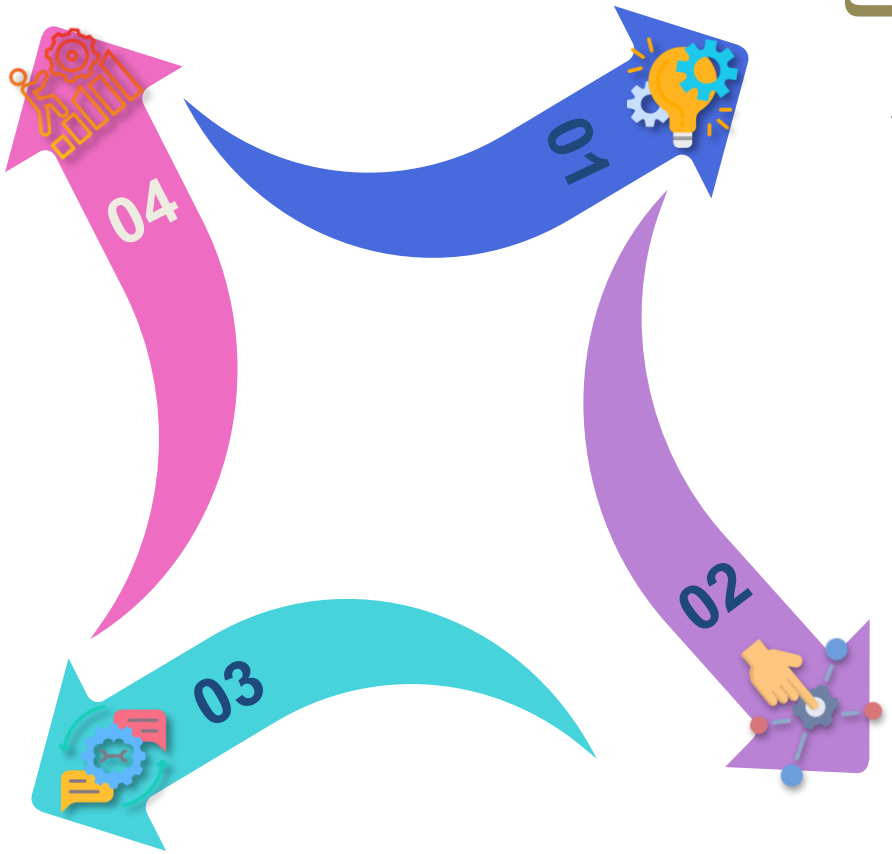
- تعتمد على مصادر متعددة مثل سجلات الشبكة وقواعد بيانات التهديدات

الاستخدامات العملية

- تستخدمها الشركات لتحسين استراتيجيات الحماية

المزايا والتحديات

- **المزايا**: تساعد في الاستجابة بشكل أسرع للهجمات
- **التحديات**: يتطلب وقتًا وموارد لتحليل البيانات بكفاءة



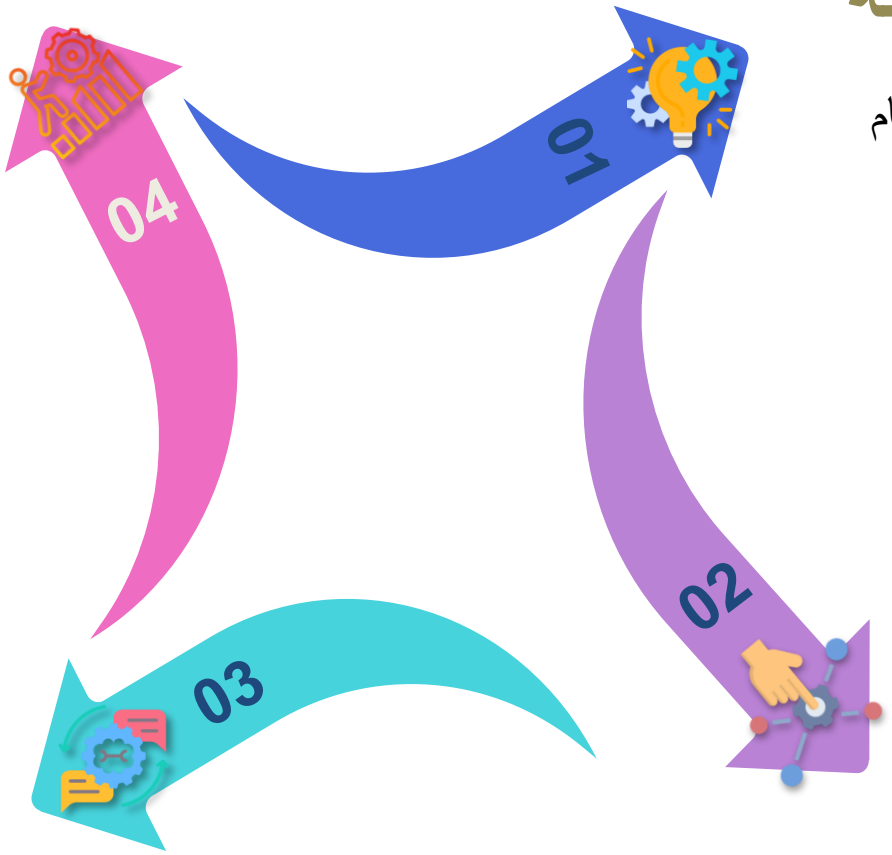
Sandboxing

مفهوم تقنية البيئة المعزولة

- آلية لعزل الملفات أو التطبيقات المشبوهة عن النظام الأساسي لفحص نشاطها دون تأثير على البيانات

آلية العمل

- يتم تشغيل الملف المشبوه داخل بيئة افتراضية مغلقة لفحص سلوكه



المزايا والتحديات

- **المزايا**: يحمي النظام من البرامج الضارة خلال عملية التحليل
- **التحديات**: قد يستهلك موارد زائدة عند تحليل تطبيقات كبيرة

الاستخدامات العملية

- يستخدم في مختبرات تحليل البرمجيات الخبيثة والشركات الأمنية

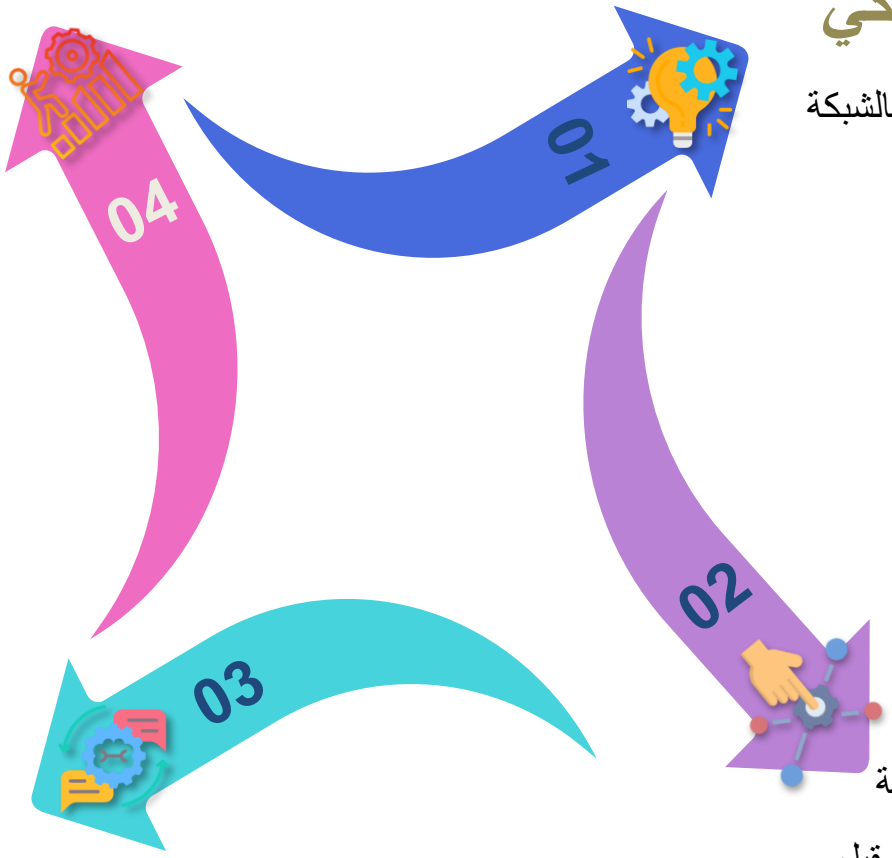
Network Access Control (NAC)

مفهوم التحكم في الوصول الشبكي

- تقنية تستخدم للتحكم في الأجهزة المصرح لها بالاتصال بالشبكة بناءً على معايير محددة مثل الهوية ومستوى الأمان

آلية العمل

- يتم التحقق من هوية الجهاز باستخدام قواعد مصادقة معينة (مثل الشهادات الرقمية أو تسجيل الدخول عبر المستخدم) قبل السماح بالاتصال



الاستخدامات العملية

- يستخدم بشكل واسع في الشبكات المؤسسية لحماية البيانات الحساسة وضمان أمان الشبكة

المزايا والتحديات

- **المزايا**: زيادة أمان الشبكة بمنع الأجهزة غير المصرح بها من الاتصال
- **التحديات**: يمكن أن يؤدي الإعداد السيئ إلى حظر الأجهزة المصرح بها أو زيادة التعقيد الإداري

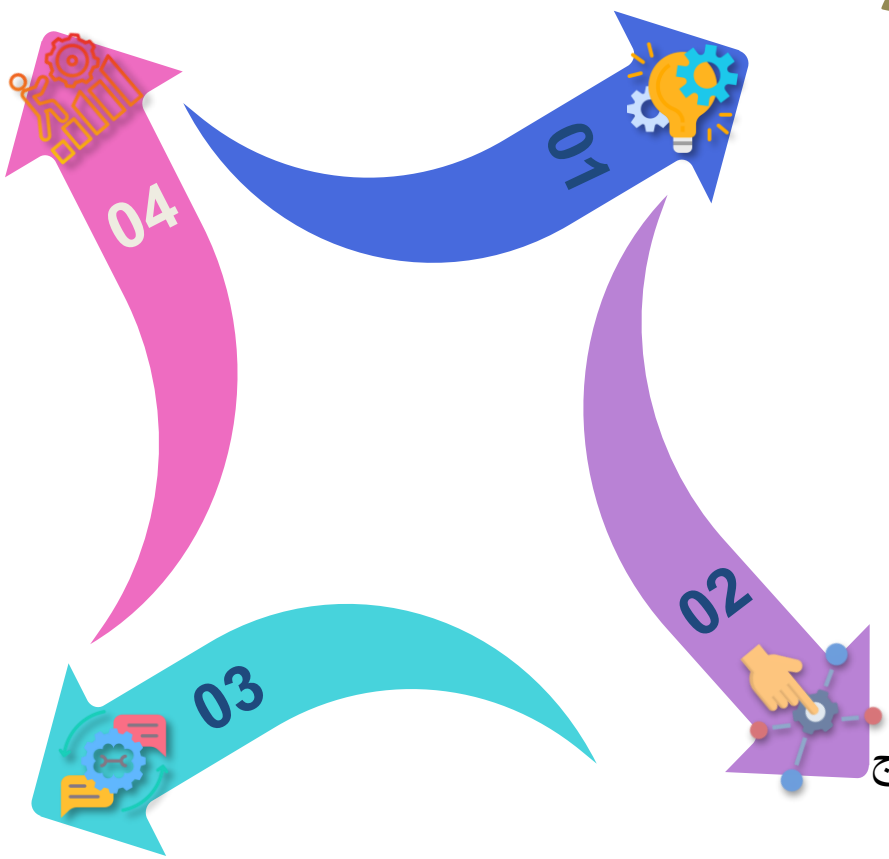
Honeypots

مفهوم الفخاخ الإلكترونية

• نظام أمني يتم إنشاؤه لجذب المهاجمين السيبرانيين ودراسة أساليبهم في الهجوم

آلية العمل

• يتم إعداد نظام وهمي يحتوي على ثغرات لاستدراج القراصنة وتسجيل أنشطتهم



المزايا والتحديات

• **المزايا**: يكشف عن أساليب المهاجمين ويتيح فرصة لتطوير تقنيات الدفاع

• **التحديات**: قد يصبح هدفًا إذا اكتشف المهاجمون أنه ليس نظامًا حقيقيًا

الاستخدامات العملية

• يستخدم في الأبحاث الأمنية واختبار الدفاعات الشبكية

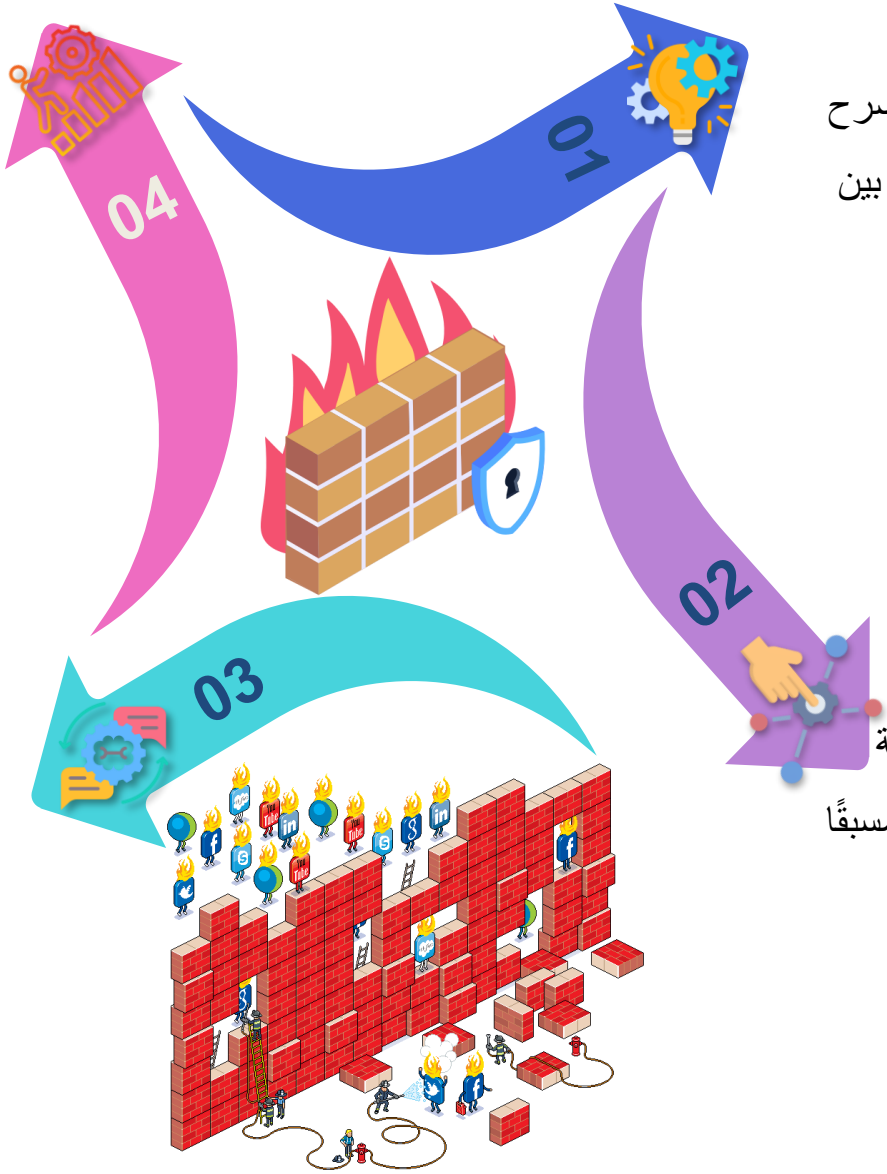
Firewall

مفهوم جدار الحماية

- جدار الحماية هو نظام أمني يقوم بمنع الوصول غير المصرح به إلى الشبكات عن طريق مراقبة وتصفية حركة المرور بين الشبكات الداخلية والخارجية

آلية العمل

- يقوم جدار الحماية بتحديد القواعد التي تسمح أو تمنع حركة المرور بناءً على مجموعة من السياسات الأمنية المحددة مسبقًا
- يُستخدم في الشركات والأجهزة الشخصية لحماية البيانات والأنظمة من التهديدات الخارجية



الاستخدامات العملية

- حماية الشبكات الداخلية للشركات من الهجمات الإلكترونية
- تصفية حركة المرور المشبوهة ومنعها من الوصول إلى الأنظمة الحساسة

المزايا والتحديات

- **المزايا**: يمنع الوصول غير المصرح به ويحافظ على أمان الشبكة
- **التحديات**: قد يكون من الصعب تحديث القواعد باستمرار لمواجهةالتهديدات الجديدة

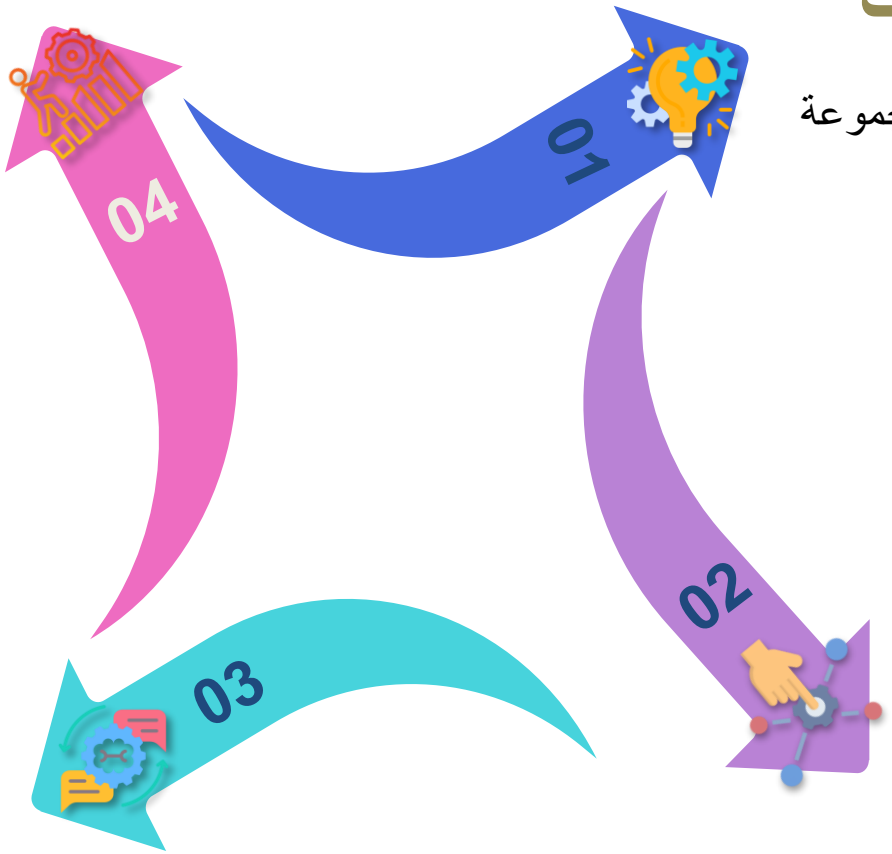
Packet Filtering

مفهوم تصفية حزم البيانات

- تقنية تراقب حركة البيانات في الشبكة بناءً على مجموعة من القواعد المحددة مسبقًا

آلية العمل

- يتم فحص كل حزمة بيانات باستخدام معايير مثل العنوان المصدر أو الوجهة والبروتوكول



الاستخدامات العملية

- تستخدم في أنظمة الجدران النارية لحماية الشبكات الداخلية

المزايا والتحديات

- **المزايا**: تمنع نقل الحزم الضارة أو غير المصرح بها
- **التحديات**: قد يؤدي الإعداد غير الصحيح إلى حجب البيانات السليمة

Zero Trust Network Architecture (ZTNA)

مفهوم مبدأ عدم الثقة

- إطار أمني يُلزم بعدم الثقة بأي جهاز أو مستخدم، حتى لو كان داخل الشبكة، ويتطلب التحقق المستمر

آلية العمل

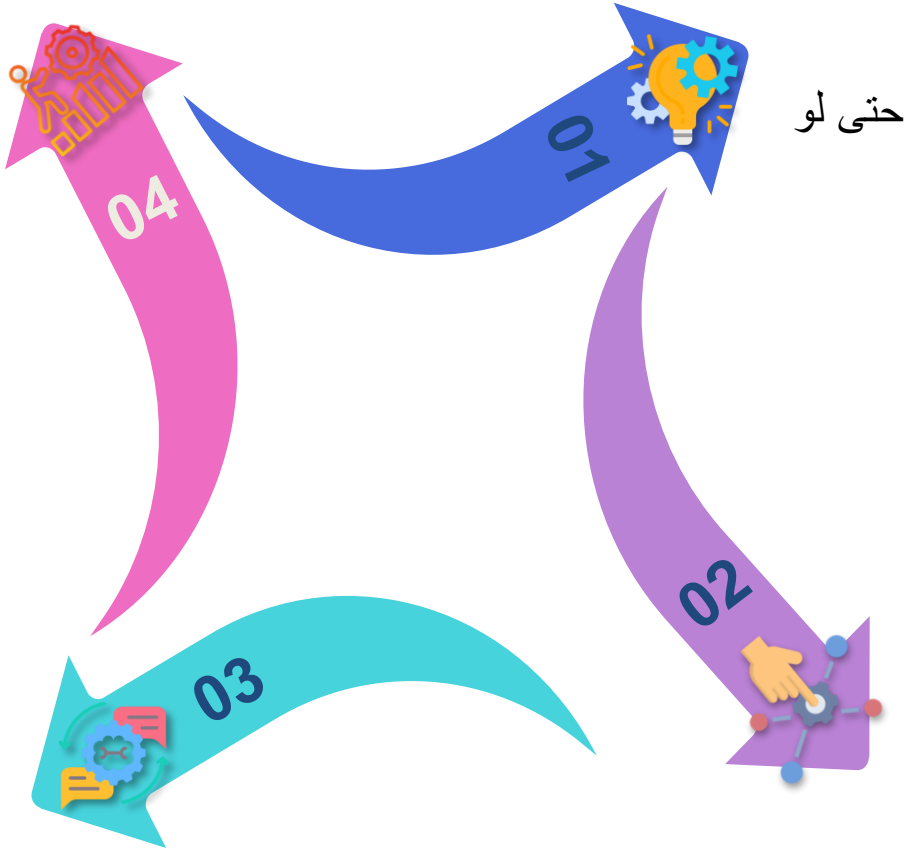
- يتم فرض سياسات أمان دقيقة ومستمرة للتحقق من هوية المستخدم والجهاز مع مراقبة البيانات

الاستخدامات العملية

- مناسب للشركات التي تعمل في بيئات مختلطة أو تعتمد على السحابة

المزايا والتحديات

- **المزايا**: تقليل مخاطر الهجمات الداخلية
- **التحديات**: يتطلب استثمارات في التقنية والتدريب لضمان التنفيذ الناجح



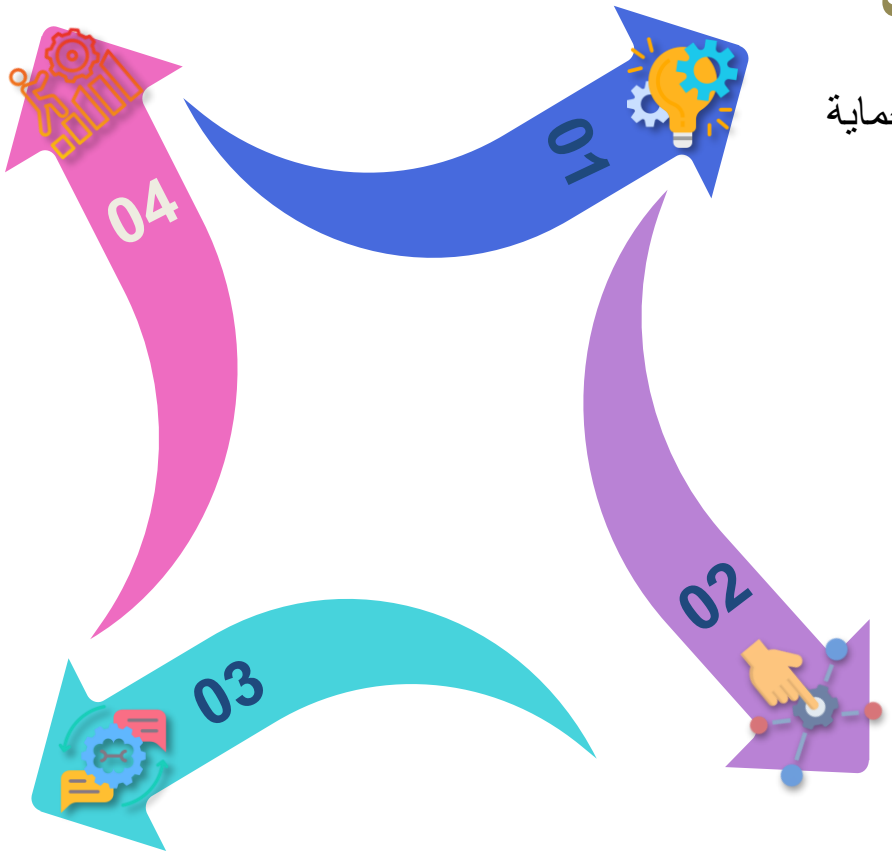
Data Loss Prevention (DLP)

مفهوم منع فقدان البيانات

- مجموعة من السياسات والتقنيات التي تهدف إلى حماية البيانات الحساسة من التسرب أو الفقدان

آلية العمل

- يتم مراقبة البيانات أثناء النقل أو الاستخدام أو التخزين، وتطبيق سياسات تحدد ما إذا كان يمكن نسخها أو مشاركتها



المزايا والتحديات

- **المزايا**: حماية البيانات الحساسة والامتثال للوائح القانونية
- **التحديات**: قد يؤدي إلى قيود في الاستخدام المشروع للبيانات أو أخطاء في التصنيف

الاستخدامات العملية

- يستخدم في البنوك والشركات التي تتعامل مع بيانات العملاء الحساسة

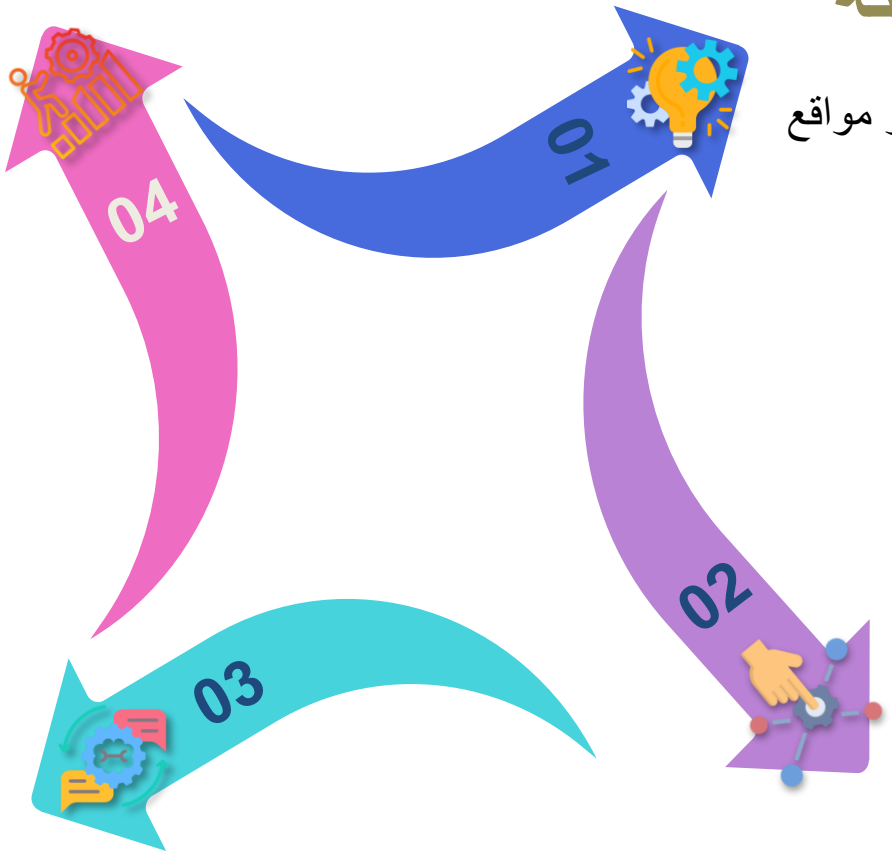
Secure Web Gateway (SWG)

مفهوم البوابة الشبكية الآمنة

• أداة تحمي المستخدمين من الوصول إلى محتوى أو مواقع ضارة أثناء تصفح الإنترنت

آلية العمل

• مراقبة حركة المرور على الإنترنت وتحليلها، وحظر البرامج الضارة أو المواقع المشبوهة



المزايا والتحديات

• **المزايا**: زيادة الأمان أثناء الاتصال بالإنترنت

• **التحديات**: قد يبطئ الأداء في حال زيادة الفلترة

الاستخدامات العملية

• يستخدم في المؤسسات التي تعتمد بشكل كبير على الإنترنت في أعمالها اليومية

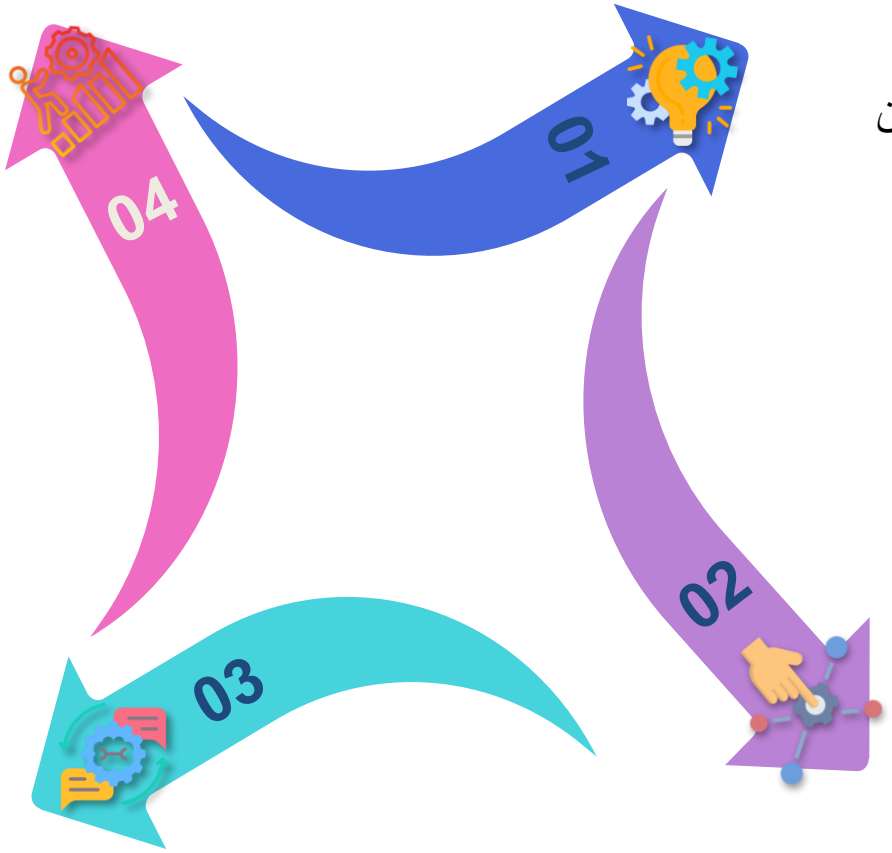
Microsegmentation

مفهوم التقسيم الجزئي

- تقنية تُستخدم لتقسيم الشبكة إلى أجزاء صغيرة يمكن التحكم بها بشكل مستقل

آلية العمل

- يتم إنشاء سياسات أمان منفصلة لكل جزء في الشبكة بناءً على التطبيقات أو المستخدمين



المزايا والتحديات

- **المزايا**: تحسين الأمان عن طريق الحد من انتشار التهديدات بين مكونات الشبكة
- **التحديات**: قد يتطلب إدارة مكثفة وإعادة هيكلة الشبكة

الاستخدامات العملية

- مناسب لمراكز البيانات والبنى التحتية السحابية التي تحتوي على تطبيقات متعددة

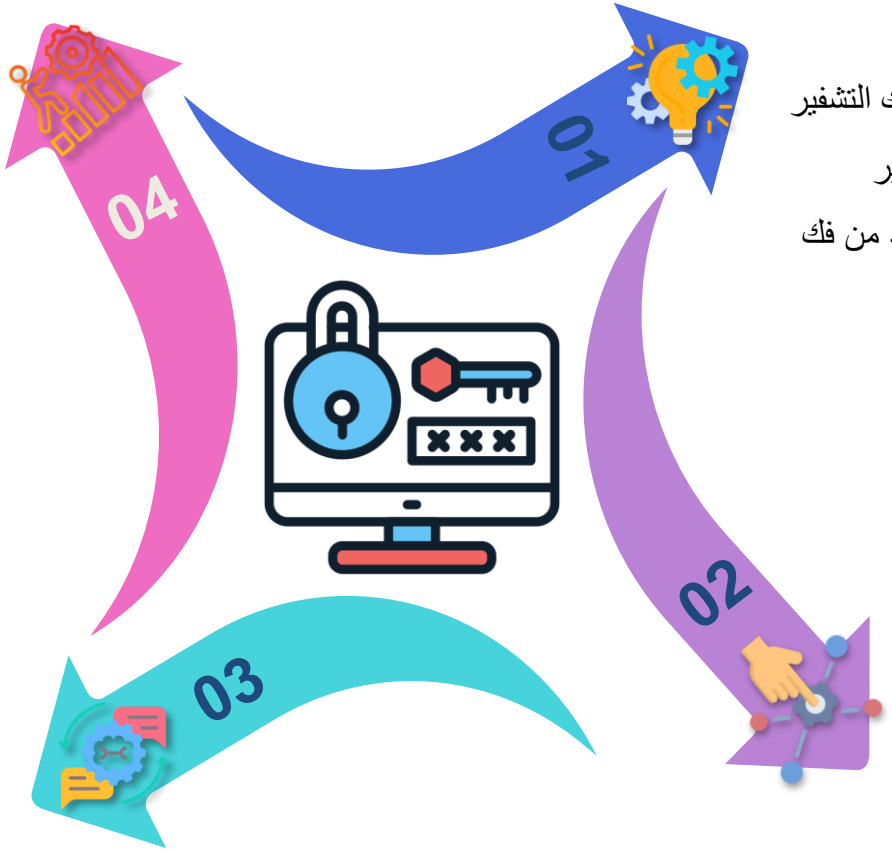
Asymmetric encryption

مفهوم التشفير غير المتماثل

- التشفير غير المتماثل يعتمد على مفتاحين: عام للتشفير وخاص لفك التشفير
- **المفتاح العام** يُستخدم لتشفير الرسالة، و**المفتاح الخاص** لفك التشفير
- هذه العملية تضمن أن حتى لو تم اعتراض الرسالة، لن يتمكن أحد من فك تشفيرها سوى الشخص الذي يمتلك المفتاح الخاص

المزايا والتحديات

- **المزايا**:
- يوفر أمانًا عاليًا، حيث يمكن فك تشفير البيانات فقط باستخدام **المفتاح الخاص**
- **التحديات**:
- يتطلب موارد حاسوبية كبيرة وقد يكون إدارة المفاتيح معقدًا

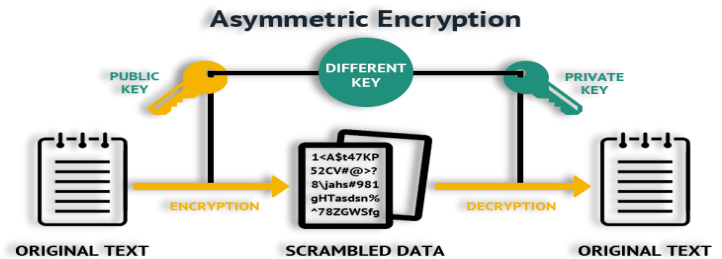


آلية العمل

- يقوم المرسل بتشفير الرسالة باستخدام **المفتاح العام** للمستلم
- المستلم يستخدم **المفتاح الخاص** لفك التشفير وقراءة الرسالة
- يضمن التشفير غير المتماثل أمان البيانات ويمنع أي جهة أخرى من الوصول إلى محتواها

الاستخدامات العملية

- تأمين المعاملات البنكية عبر الإنترنت
- البروتوكولات الأمنية: يعتمد العديد من بروتوكولات الأمان على التشفير غيرالمتماثل لتأمين الاتصال بين المتصفحات والخوادم
- التوقيعات الرقمية لتأكيد هوية المرسل



Two-factor Authentication (2FA)

مفهوم المصادقة الثنائية

- المصادقة الثنائية هي إجراء أمني يُستخدم لتأكيد هوية المستخدم عن طريق الجمع بين كلمة المرور ووسيلة تحقق إضافية (مثل رمز يُرسل إلى الهاتف المحمول)

المزايا والتحديات

- **المزايا**: يعزز الأمان بشكل كبير لأنه يتطلب خطوة إضافية بعد كلمة المرور
- **التحديات**: قد يكون مزعجًا للمستخدمين في بعض الأحيان بسبب الحاجة إلى إدخال رمز التحقق في كل مرة

آلية العمل

- بعد إدخال كلمة المرور، يطلب النظام من المستخدم إدخال رمز تحقق إضافي يُرسل إلى هاتفه أو يتم توليده عبر تطبيق مخصص لضمان أن الشخص الذي يحاول الوصول هو المالك الشرعي للحساب

الاستخدامات العملية

- تُستخدم المصادقة الثنائية بشكل شائع في الحسابات البنكية، البريد الإلكتروني، ومنصات التواصل الاجتماعي لتأمين الحسابات الشخصية

Digital Signatures

مفهوم التوقيعات الرقمية

• التوقيع الرقمي هو تقنية تشفير تستخدم للتحقق من صحة وسلامة المستندات أو الرسائل الرقمية، والتأكد من أن مصدرها أصلي وغير معدّل

المزايا والتحديات

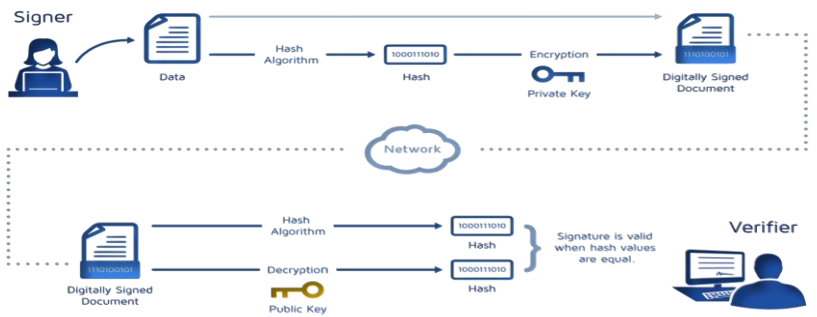
• **المزايا**: يضمن التحقق من هوية المرسل وسلامة المستندات• **التحديات**: يعتمد على الثقة المتبادلة وإدارة المفاتيح الرقمية بشكل آمن

آلية العمل

• يقوم المرسل بإنشاء توقيع رقمي باستخدام المفتاح الخاص. عندما يتلقى المستلم الرسالة أو المستند، يقوم باستخدام المفتاح العام للتحقق من صحة التوقيع

الاستخدامات العملية

• يُستخدم التوقيع الرقمي على نطاق واسع في المعاملات المالية والعقود القانونية الرقمية لضمان صحة المستندات وعدم العبث بها



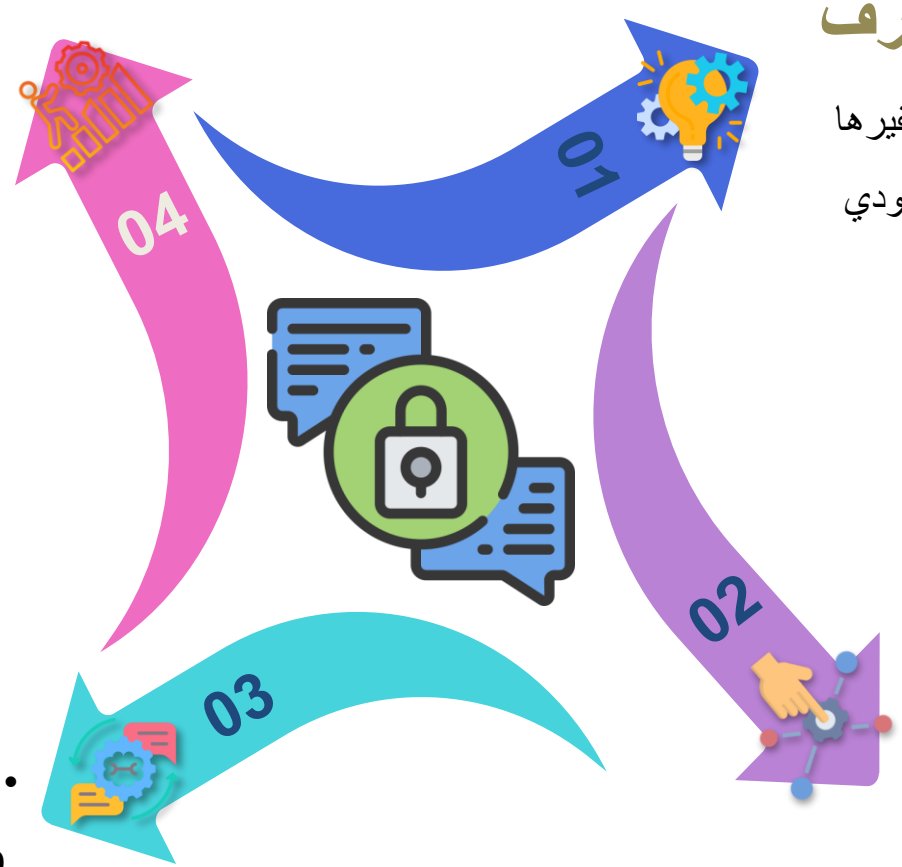
End-to-End Encryption

مفهوم التشفير من طرف إلى طرف

- هو نوع من التشفير يضمن أن الرسالة أو البيانات يتم تشفيرها من المرسل وفك تشفيرها فقط من قبل المستقبل. حتى مزودي الخدمة لا يمكنهم قراءة أو اعتراض المحتوى

المزايا والتحديات

- **المزايا**: يضمن سرية كاملة للمحادثات ويمنع أي جهة ثالثة من اعتراضها
- **التحديات**: إذا تم فقدان المفتاح الخاص، لا يمكن استعادة الرسائل

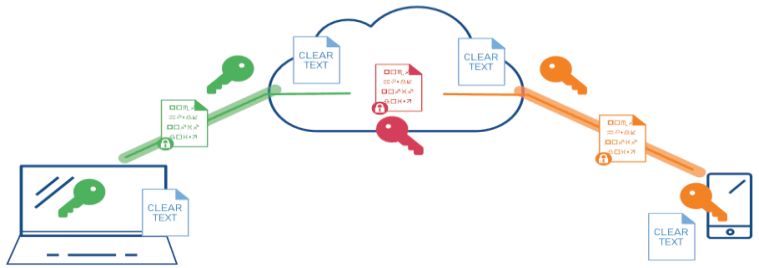


آلية العمل

- يتم تشفير الرسالة باستخدام مفتاح المرسل وفك تشفيرها فقط عند وصولها إلى المستقبل باستخدام مفتاحه الخاص

الاستخدامات العملية

- يُستخدم بشكل شائع في تطبيقات المراسلة مثل **WhatsApp** لتأمين الاتصالات بين المستخدمين



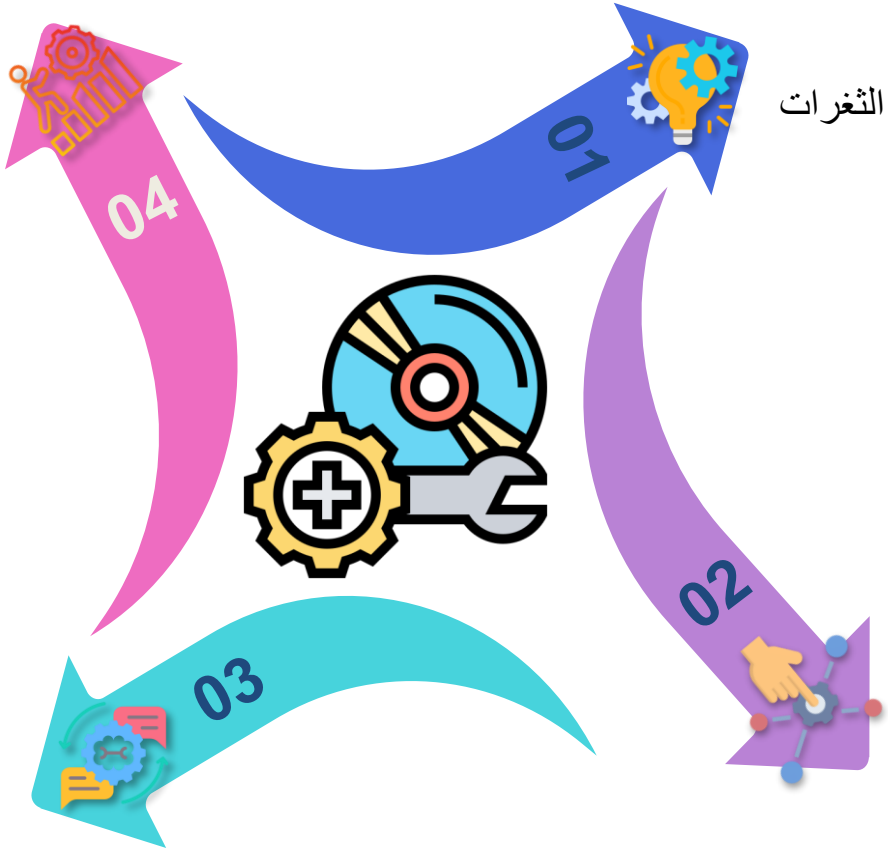
Security Patches

مفهوم التحديثات الأمنية

- التحديثات الأمنية هي ترقيات برمجية تهدف إلى تصحيح الثغرات الأمنية التي يتم اكتشافها في الأنظمة أو البرامج

المزايا والتحديات

- **المزايا**: تمنع الهجمات الإلكترونية التي تستغل الثغرات المعروفة في الأنظمة
- **التحديات**: قد يتم تأجيل تثبيت التحديثات من قبل المستخدمين، مما يترك الأنظمة عرضة للهجمات



آلية العمل

- يقوم المطورون بإصدار تحديثات تصحيحية تعمل على سد الثغرات وتحسين أمان النظام. يجب على المستخدمين تثبيت هذه التحديثات فور توفرها

الاستخدامات العملية

- تُستخدم في جميع الأجهزة والأنظمة لضمان حماية البيانات والمستخدمين من التهديدات المستجدة

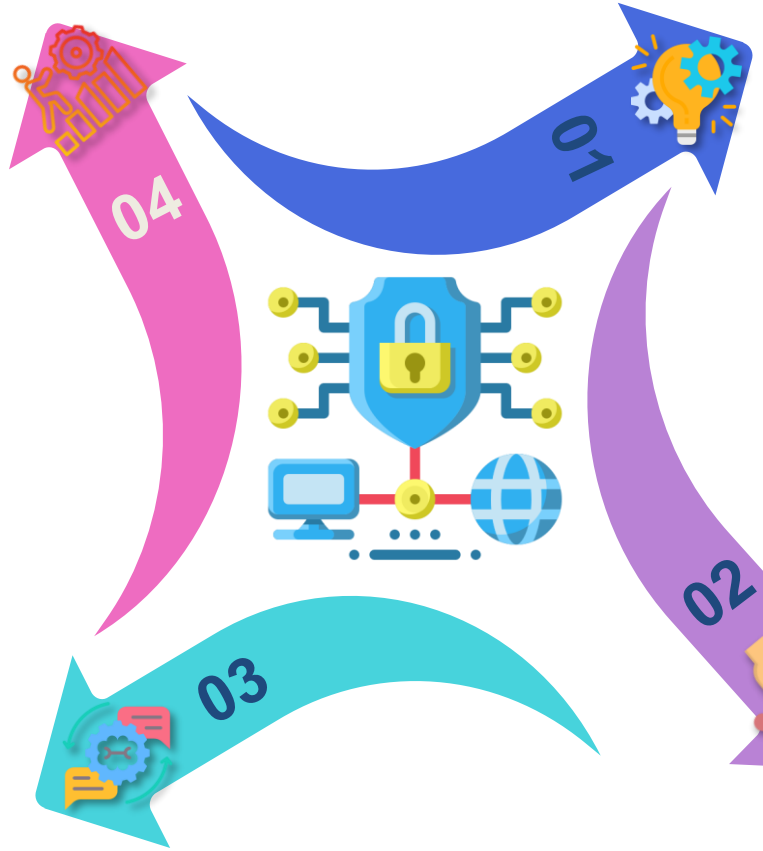
Virtual Private Network (VPN)

مفهوم VPN

- الشبكة الافتراضية الخاصة هي أداة تستخدم لإنشاء اتصال آمن ومشفر بين جهاز المستخدم وخادم آخر عبر الإنترنت. يتم توجيه حركة المرور عبر نفق مشفر لضمان الخصوصية وحماية البيانات أثناء التصفح

آلية العمل

- يقوم المستخدم بالاتصال بخادم الشبكة الافتراضية الخاصة مما يخفي العنوان الخاص به ويؤمن نقل البيانات
- يتم تشفير جميع البيانات المرسلة والمستلمة بين VPN الجهاز وخادم مما يضمن عدم تمكن الجهات الخارجية من اعتراض البيانات



المزايا والتحديات

- **المزايا**: يحمي الخصوصية ويمنع تتبع النشاط عبر الإنترنت
- **التحديات**: يعتمد على قوة الاتصال وسرعة الإنترنت، وقد يؤدي إلى بطء في التصفح

الاستخدامات العملية

- **التصفح الآمن**: يستخدمه الأفراد والشركات لتصفح الإنترنت بشكل آمن ومجهول
- **الوصول إلى المحتوى المحظور**: يمكن للمستخدمين تجاوز القيودالجغرافية للوصول إلى محتوى محظور في بلدانهم

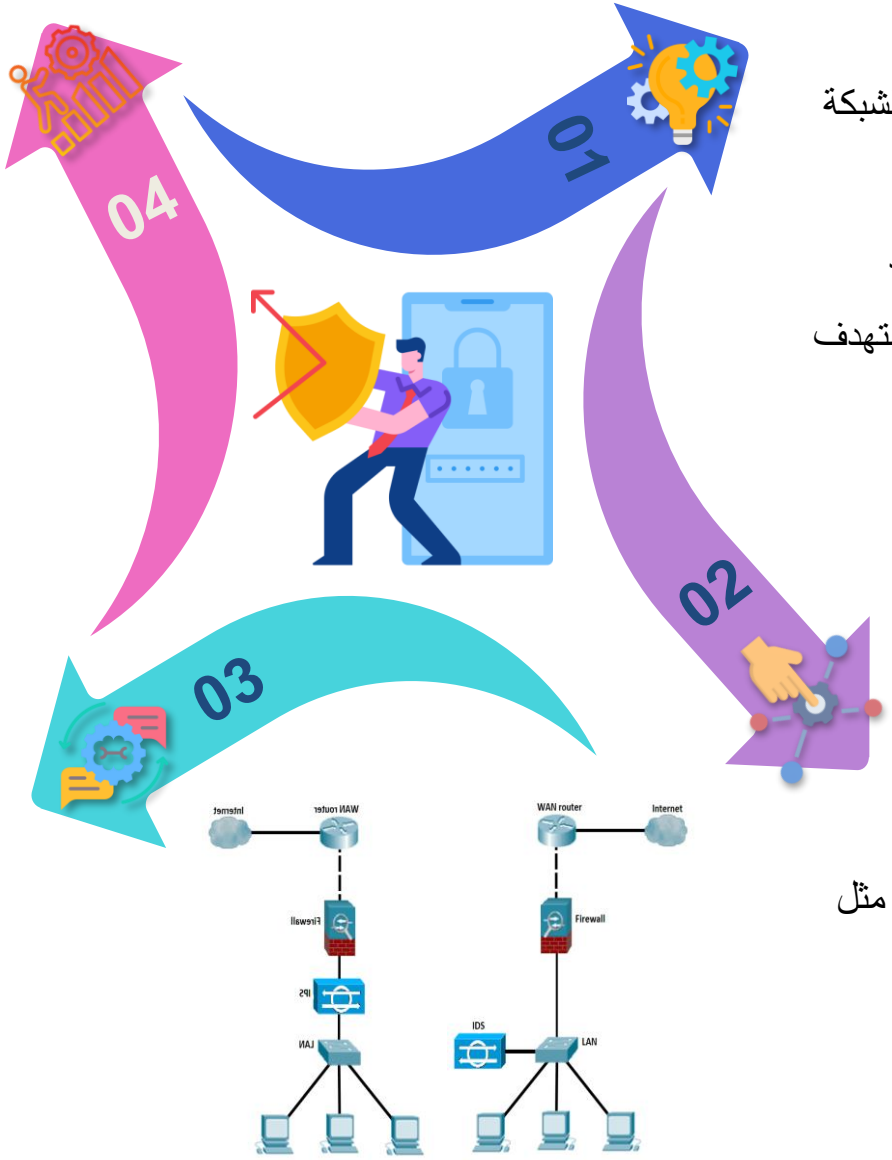
IDS/IPS Intrusion Detection System/Intrusion Prevention Syste

مفهوم IDS/IPS

- **نظام كشف التطفل:** هو نظام يقوم بمراقبة حركة مرور الشبكة لاكتشاف أي نشاط مشبوه أو محاولات اختراق
- **نظام منع التطفل:** هو نظام يقوم بمنع التهديدات تلقائيًا بعد اكتشافها، ويقوم بعرقلة النشاطات غير المشروعة التي تستهدف الشبكة

آلية العمل

- **نظام كشف التطفل:** يراقب حركة المرور ويقوم بتنبيه المسؤولين عند اكتشاف أي محاولة اختراق
- **نظام منع التطفل:** يقوم باتخاذ إجراء فوري لمنع التهديد، مثل قطع الاتصال أو منع الوصول إلى النظام



المزايا والتحديات

- **المزايا:** يوفر حماية استباقية، حيث يقوم بمنع التهديدات قبل أن تصل إلى النظام
- **التحديات:** قد يؤدي إلى تحذيرات كاذبة ويحتاج إلى ضبط دقيق لتجنب إيقاف حركة المرور الشرعية

الاستخدامات العملية

- يُستخدمان في المؤسسات الكبيرة لضمان اكتشاف التهديدات مبكرًا ومنع الاختراقات، خاصة في البيئات الحساسة مثل الشبكات البنكية أو الحكومية

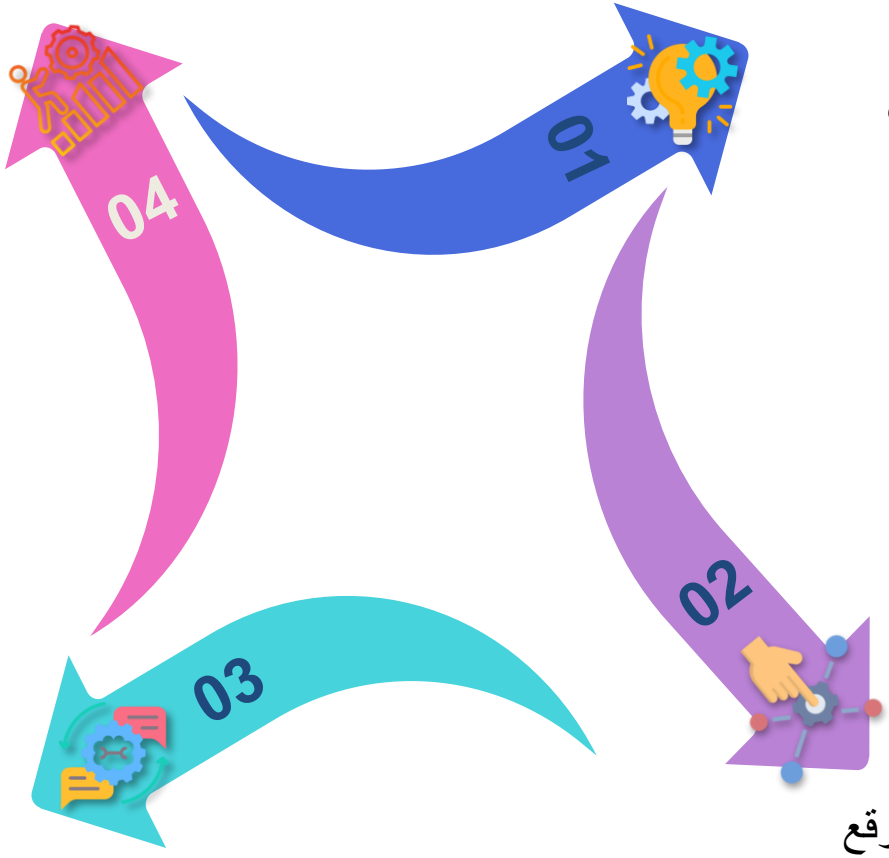
Load Balancing

مفهوم توازن الأحمال

- تقنية لتوزيع حركة البيانات على عدة خوادم لتجنب الضغط وتحسين الأداء

آلية العمل

- يحدد الخادم الأنسب بناءً على الحمل الحالي أو الموقع الجغرافي



المزايا والتحديات

- **المزايا**: يقلل من الأعطال ويزيد من كفاءة الشبكة
- **التحديات**: يتطلب تكلفة إضافية لشراء معدات وبرمجيات التوزيع

الاستخدامات العملية

- شائع في الشبكات عالية الحركة مثل مواقع التجارة الإلكترونية

References

NIST

- NIST Cybersecurity Framework (CSF)
- NIST Incident Response Lifecycle
- NIST Special Publication 800-53
- NIST Guidelines on Security and Privacy Controls

ISO/IEC

- ISO/IEC 27001 Information Security Management

Google

- Google Cybersecurity Certificate

EC-Council

- CEH Certification - EC-Council

Recommendation

- الهيئة الوطنية للأمن السيبراني
- المعجم العربي للأمن السيبراني