CYBERSECURITY GUIDE

يهدف هذا الدليل إلى تعزيز الوعي بأهمية حماية البيانات والحفاظ على الأمن السيبراني، من خلال تسليط الضوء على المخاطر المحتملة وطرق الوقاية منها بلغة مبسطة ومباشرة.

الفهرس

المقدمة 3
التهديدات الداخلية والخارجية 11
أنواع الهجمات السيبرانية 31
حساسية البيانات وجمع المعلومات 50
الهجمات المتقدمة 62
تحليل وتقييم شامل 75
الإجراءات الأمنية 86
الخاتمة 95
المصطلحات 97

1.المقدمة

1.1 ما هي التهديدات السيبرانية

تخيل معي، كل يوم إحنا متصلين بالشبكة، نستخدم الكمبيوتر، الموبايل، نفتح الإيميل أو نشارك بياناتنا عالإنترنت. بهالوقت، في مجموعة ناس أو برامج خبيثة ممكن تحاول توصل لبياناتنا أو تسبب لنا مشاكل بدون ما نحس. هالشي هو بالضبط اللي بنسميه تهديدات سيبرانية.

التهديدات السيبرانية ببساطة هي أي شي ممكن يضر أجهزتنا، بياناتنا، أو حتى سمعتنا الرقمية. ممكن تجي من خارج الشركة، زي هاكرز يحاولوا يخترقوا النظام، أو من داخل الشركة، زي موظف يستخدم صلاحياته بشكل خاطئ أو ينسى يتبع القواعد الأمنية.

ليش صارت التهديدات السيبرانية حساسة اليوم أكتر من أي وقت؟ لأن:

1. كل شي صار رقمي: بياناتنا كلها مخزنة إلكترونياً، ومن السهل الوصول إلها إذا ما كان فيه حماية.
2. الهجمات صارت أذكى: ما صارت مجرد فيروس بسيط، صار فيها هجمات معقدة، تقدر تتجنب الكشف وتسرق معلوماتك بدون ما تحس.
3. التأثير كبير: تهديد واحد ممكن يوقف شغل الشركة، يخرب سمعتها، أو يسرق معلومات حساسة تؤثر على الكل.

فببساطة، التهديدات السيبرانية مو بس مشكلة تقنية، هي مشكلة استراتيجية لكل شخص وكل مؤسسة. فهمها أول خطوة لتعرف كيف تحمي حالك ونظامك.

1.2 ليش صارت التهديدات السيبرانية حساسة

زمان كان موضوع الاختراقات والفيروسات إشي محدود، بس مع الوقت وتطور التكنولوجيا صار الموضوع حساس بشكل أكبر. ليش؟ خليني أحكي لك:

1. الاعتماد الكلي على التكنولوجيا

اليوم تقريبًا كل إشي بحياتنا مربوط بالإنترنت: البنوك، الشغل، الجامعات، حتى البيت الذكي. يعني إذا صار تهديد بسيط، ممكن يأثر على تفاصيل دقيقة بحياتنا اليومية.

2. القيمة الكبيرة للبيانات

البيانات صارت زي النفط، إلها قيمة تجارية وسياسية ضخمة. أي معلومة صغيرة – حتى إيميلك أو مكانك – ممكن تنباع أو تستغل بطرق ما بتخطر عبالك.

3. تطور الهجمات

الهاكرز ما عادوا أفراد لحالهم قاعدين بغرفة مظلمة. صار في جماعات منظمة، وبعضهم مدعومين من دول، وعندهم موارد وأدوات متطورة جدًا. يعني الهجمات صارت أذكى وأخطر.

4. السرعة بالتأثير

تهديد إلكتروني واحد ممكن خلال دقائق يخلي أنظمة شركة كاملة تتوقف، أو يعمل تشفير للملفات (زي Ransomware) ويشل الشغل كليًا.

5. الأثر الواسع

الموضوع ما بوقف عند الخسارة المالية. في أثر على السمعة، على ثقة العملاء، وعلى استمرارية العمل. عشان هيك صار الأمن السيبراني مش بس موضوع IT، صار جزء أساسي من إستراتيجية أي مؤسسة.

باختصار، التهديدات السيبرانية صارت حساسة لأنها بتلمس كل جوانب حياتنا ومؤسساتنا، من أبسط معلومة لحد أعقد نظام. عشان هيك الوعي فيها والتعامل معها صار ضرورة مش خيار.

1.3 أثر التهديدات على المؤسسات والمستخدمين

خلينا نكون واقعيين شوي: التهديدات السيبرانية مش إشي بعيد أو مجرد خبر بنسمع فيه. هي إلها أثر مباشر علينا كمستخدمين وعلى المؤسسات بشكل عام. والأثر هذا ممكن يكون صغير وبسيط، أو كبير يغير مجرى الشغل بالكامل.

أولاً: على المؤسسات

1. خسائر مالية

أي هجوم ممكن يوقف السيستم أو يسرّب بيانات حساسة، وهذا بخلي الشركة تدفع مبالغ ضخمة سواء لإصلاح الضرر أو تعويض العملاء.

2. ضياع السمعة

العملاء إذا حسّوا إنه بياناتهم مش آمنة، صعب يرجعوا يثقوا بالشركة. والسمعة أصعب إشي ترجع زي أول.

3. توقف العمل

هجمات زي الـ Ransomware ممكن توقف الشغل لساعات أو أيام، وهذا بيأثر على الإنتاجية ويعمل خسائر متراكمة.

4. **مشاكل قانونية**

إذا الشركة ما حمت بيانات العملاء بشكل كافي، ممكن تواجه قضايا أو غرامات من جهات رقابية.

ثانياً: على المستخدمين

1. سرقة البيانات الشخصية

زي الحسابات البنكية، الإيميلات، أو حتى ملفات خاصة.

2. الابتزاز الإلكتروني

ممكن حد يخترق صور أو ملفات خاصة ويستغلها للضغط على الشخص.

3. انتهاك الخصوصية

تخيل حياتك الرقمية مكشوفة لشخص غريب! شعور مزعج وخطير.

4. خسائر مالية شخصية

اختراق بطاقة بنكية أو سرقة كلمة مرور حساب التسوّق ممكن يخليك تخسر فلوسك بلحظة.

باختصار، أثر التهديدات السيبرانية مش بس "مشكلة تقنية"، هو إشي بيلمس المال، السمعة، الخصوصية، وحتى الراحة النفسية للمستخدمين. عشان هيك التعامل معها بذكاء صار جزء من نجاح أي مؤسسة وأمان أي فرد.

1.4 هدف الدليل والفئة المستهدفة

الهدف من هذا الدليل هو توفير مرجع شامل وبنفس الوقت عملي يساعد القارئ يفهم التهديدات السيبرانية بشكل واضح، ويعرف كيف يواجهها بخطوات مدروسة. إحنا ما بدنا مجرد معلومات نظرية، بدنا ندمج الشرح مع أمثلة واقعية وسيناريوهات ممكن تصير بأي مؤسسة أو حتى على مستوى الأفراد. هيك القارئ بطلع مش بس فاهم، بل كمان جاهز يطبق.

1. الأهداف الأساسية للدليل:

- رفع الوعي الأمني عند مختلف الفئات.
- شرح طبيعة التهديدات والثغرات بأسلوب مبسط وذكي.
- تقديم إجراءات دفاعية عملية قابلة للتطبيق.
- دعم المؤسسات باتخاذ قرارات مدروسة لحماية أصولها.

2. الفئة المستهدفة:

- **المختصين بأمن المعلومات:** الدليل رح يكون بمثابة مراجعة شاملة لأحدث التهديدات وأساليب الدفاع.
- **الإداريين وصنّاع القرار:** راح يساعدهم يفهموا ليش الأمن السيبراني مش مجرد تكاليف إضافية، بل استثمار ضروري بيحافظ على سمعة المؤسسة وبيمنع خسائر ضخمة.
- **الموظفين والمستخدمين داخل المؤسسة:** رح يتعلموا كيف يحافظوا على أمان بياناتهم ويتجنبوا الأخطاء البسيطة اللي ممكن تكلف الشركة كتير.
- **الطلاب والباحثين:** يعتبر مرجع أكاديمي مبسط يربط بين النظرية والتطبيق
- **المستخدم العادي:** راح يستفيد بفهم أساسيات الحماية وكيف يطبّقها على حياته اليومية مثل حماية حساباته وكلماته السرية.

2. التهديدات الداخلية والخارجية

2.1 التهديدات الداخلية (Inside Threats)

2.1.1 شو المقصود بالتهديد الداخلي؟

التهديد الداخلي هو أي خطر بيجي من داخل المؤسسة — من شخص، جهاز، أو عملية داخلية — بيقدر يسبب تسريب، تعديل، أو تلف للبيانات أو تعطيل للخدمات. المشكلة الأساسية إنه مصدر التهديد عنده معرفة وصلاحيات جوّا النظام، فلازم نتعامل معاه بحذر مختلف عن التهديد الخارجي.

2.1.2 أنواع التهديدات الداخلية

بنقسمها لثلاث فئات أساسية:

خبيث (Malicious insider)

موظف أو متعاقد عنده نية سيئة: يسرق بيانات، يعبث بالنظام أو يبيع معلومات. الدافع ممكن يكون انتقام، ربح مادي أو ضغوط خارجية.

غير مقصود / إهمال (Negligent insider)

خطأ بشري: تحميل ملف مصاب، مشاركة مستند في مكان غير آمن، استخدام كلمات سر ضعيفة أو إعادة استخدامها. النية مش سيئة بس الضرر كبير.

مخترق استغل صلاحيات داخلية (Compromised insider)

حساب موظف تم اختراقه عبر phishing أو credential stuffing، وبعدين المهاجم يستغل صلاحيات الحساب للعمل من الداخل.

2.1.3 أمثلة عملية (قريبة للواقع)

موظف HR ينسخ قاعدة بيانات الموظفين على USB ثم يفقدها أو يشاركها.

موظف خدمة عملاء يشارك تفاصيل حساسة عبر Slack بدون تشفير.

مهندس نظم ينزل أداة من موقع غير موثوق وتكون Trojan يسمح بالوصول الخارجي.

حساب مدير تم اختراقه فيرسل أوامر لتحويل مبالغ مالية داخل النظام.

2.1.4 تحليل الأثر (ليه الموضوع خطير؟)

- **صعوبة الاكتشاف:** لأن السلوك غالبًا يطابق سلوك موظف عادي، خصوصًا بالاول.
- **قوة الوصول:** insider عنده صلاحيات أو معرفة بتسلسل العمل، فضرره عادةً أكبر من outsider.
- **التبعات:** فقدان بيانات حساسة، غرامات قانونية، اضطراب بالعمل، تأثر سمعة الشركة.
- **التكلفة:** أحيانًا أعلى لأن التحقيق والتعافي يتطلبان وقت وتدخّل تقني وقانوني.

2.1.5 مؤشرات قد تدل على تهديد داخلي (Red Flags)

- تحميل أو نسخ ملفات غريبة أو بكميات كبيرة (خصوصًا في أوقات غير عمل).
- تسجيل دخول من أوقات/أماكن غير معتادة.
- تغيّر مفاجئ في سلوك الحساب (مثلاً الوصول لأدلة ما كان الموظف يحتاجها).
- حذف سجلات أو تعطيل logging.
- شكاوى من زملاء لوجود سلوك مشبوه أو تعليقات عن "ضغط" أو "ظلم" على موظف.

2.1.6 استراتيجيات عملية للوقاية والكشف (Technical + Organizational)

أ. ضوابط وصول وسياسات

- **مبدأ أقل الصلاحيات (Least Privilege):** لا تعطِ صلاحيات أكثر من الحاجة الوظيفية.
- **فصل المهام (Separation of Duties):** ما تخلي مهمة مالية كاملة بإيد شخص واحد.
- **مراجعات وصول دورية (Access Reviews):** راجع مَن يملك أي صلاحية كل فترة (شهري/ربع سنوي).

ب. مراقبة ورصد

- **Logging مركزي وSIEM:** سجّل كل الأنشطة المهمة وخلّي عندك نظام يجمع ويحلل السجلات.
- **UEBA (User & Entity Behavior Analytics):** يكتشف سلوك المستخدم الشاذ ويضبط تنبيهات.
- **EDR لنقاط النهاية:** يكشف ويحاصر البرمجيات الخبيثة على أجهزة الموظفين.

ج. سياسات وعمليات بشرية

- **تدريب وتوعية مستمرة:** دورات على التصيد، التعامل مع الملفات، وأمان البيانات.
- **سياسة استخدام الأجهزة (BYOD) واضحة:** امنع أو قيّد استخدام الأجهزة الشخصية للعمل.
- **إجراءات إنهاء الخدمة واضحة وفورية:** عند أي خروج لازم إلغاء صلاحيات فوراً واسترجاع الأجهزة.

د. حماية البيانات

- **DLP (Data Loss Prevention):** منع نقل بيانات حساسة عبر قنوات غير مصرّح بها.
- **تشفير البيانات:** تشفير البيانات المخزنة والمنقولة.
- **تقسيم الشبكة (Segmentation):** قلّل نطاق الأضرار بجعل الوصول مقيدًا.

هـ. الضوابط الإدارية والقانونية

- **عقود عمل واضحة:** بنود عقابية على التسريب، توصيف صلاحيات ومسؤوليات.
- **سياسة أمان معلومات موثقة:** يتبعها الجميع ويُطبّق عليها رقابة.
- **تحقيق داخلي واضح:** خطوات للتحقيق والاحتفاظ بالأدلة.

2.1.7 خطوات استجابة سريعة لو اكتُشف تهديد داخلي

- عزل الحساب/الجهاز فوراً لمنع مزيد من الضرر.
- التحقق من السجلات لفهم نطاق الضرر والوقت.
- استعادة البيانات من نسخ احتياطية إن لزم.
- تحقيق جنائي داخلي أو توظيف جهة خارجية إذا الضرر كبير.
- تطبيق إجراءات تأديبية وقانونية حسب النتائج.
- مراجعة الضوابط والإجراءات ومنع تكرار الحادث.

2.1.8 سيناريو تطبيقي كامل (Walkthrough)

المشهد: موظف محاسبة، "أحمد"، عنده صلاحية الوصول لقوائم الدفع. أحمد زعل بسبب رفض طلب ترقية، ونُشرت له رسالة يفكر يسرق بيانات العملاء.

الحدث: أحمد بنسخ ملفات العملاء على USB في المساء. بعد يومين، أحد المنافسين يعرض بيانات بعضها على الإنترنت.

كيف اكتشفنا؟ نظام DLP رصد عملية نسخ ملفات كبيرة إلى وسيلة تخزين خارجية ونبّه فريق الأمان. UEBA بين إن سلوك أحمد بوقت متأخر غير طبيعي.

إجراءات سريعة: عزل حساب أحمد، استرجاع النسخ الاحتياطية، فتح تحقيق داخلي، منع أحمد من الوصول، إشعار المتأثرين إن لزم، اتخاذ إجراءات قضائية/تأديبية.

النتائج المطلوبة: تقليل الضرر، استعادة البيانات، فرض عقوبات، تحسين سياسات الوصول، وإجراء تدريب إلزامي لكل الموظفين.

2.1.9 قائمة تحقق سريعة للمسؤولين (Quick Checklist)

- تطبيق مبدأ Least Privilege على كل الأنظمة.
- إجراء مراجعات صلاحيات دورية (رمز: شهري/ربع سنوي)
- نشر حلول Logging + SIEM + UEBA.
- تركيب EDR على كل نقاط النهاية.
- تفعيل DLP على بوابات النقل (Email, Cloud, USB controls).
- سياسات إنهاء الخدمة وإجراءاتها موثّقة ومطبقة فوراً.
- تدريب توعية دوري لكل الموظفين (Phishing simulations).
- تشفير قواعد البيانات والنسخ الاحتياطية.
- تفعيل MFA على كل حسابات الوصول الحرجة.
- تجربة خطة استجابة للحوادث داخلياً (Tabletop exercise).

الخلاصة السريعة

التهديد الداخلي خطر حقيقي ويمتاز بصعوبة اكتشافه وقوة تأثيره. الوقاية مش بس أدوات، لازم مزيج من تقنيات مراقبة ذكية، سياسات صارمة، وتدريب بشري واداري سليم. التحكم الجيد بالوصول ومتابعة السلوك وتطبيق إجراءات إنهاء الخدمة الفورية يقلل كثير من المخاطر.

2.2 التهديدات الخارجية (Outside Threats)

2.2.1 شو المقصود بالتهديد الخارجي؟

التهديد الخارجي هو أي هجوم أو محاولة اختراق بتيجي من خارج المؤسسة — من أفراد، مجموعات إجرامية، منافسين، أو حتى جهات مدعومة. الهدف عادة: اختراق النظام، سرقة أو تعديل بيانات، تعطيل خدمات، أو ابتزاز المؤسسة. المهاجم الخارجي ما عنده وصول داخلي كبداية، بس بيستخدم ثغرات تقنية أو خداع بشري للدخول.

2.2.2 أنواع التهديدات الخارجية الشائعة

1. البرمجيات الخبيثة (Malware & Ransomware) :-

برمجيات تخرب أو تشفر أو تسرق البيانات، أو تفتح بابًا خلفيًا للمهاجمين.

2. التصيد (Phishing / Spear-phishing / Business Email Compromise):-

رسائل مزيفة لخداع المستخدم للحصول على كلمات مرور أو دفع مبالغ.

3. هجمات الشبكة (DDoS, Man-in-the-Middle, Sniffing) :-

تعطيل خدمات أو اعتراض الاتصالات أو تعديل البيانات أثناء النقل.

4. استغلال الثغرات (Exploits, RCE, SQL Injection):-

مهاجم يستغل ثغرة برمجية للدخول وتنفيذ أوامر.

5. هجمات متقدمة ومستمرة (APT — Advanced Persistent Threats) :-

مجموعات منظمة تستهدف شركة محددة وتتسلل ببطء لجمع معلومات أو التجسس.

6. هجمات سلاسل التوريد (Supply Chain Attacks) :-

استهداف مزود خدمة أو مكتبة برمجية للوصول إلى عملاء المزود.

7. Credential Stuffing وBrute Force :-

محاولة دخول بحسابات مستخدمين عبر بيانات مسروقة أو تخمين كلمات المرور.

8. الهجمات الفيزيائية من الخارج

سرقة أجهزة، تركيب أجهزة تنصت على مداخل الشبكة، أو إدخال وسائط تخزين ملغمة.

2.2.3 أمثلة واقعية قريبة

- حملة Ransomware تخترق شبكة عبر بريد مرفق وتشفّر خوادم الإنتاج.
- هجوم Spear-phishing يستهدف المدير المالي برسالة مزيفة تؤدي لتحويل مبلغ كبير.
- مهاجم يستغل ثغرة في ويب أبلكيشن ويخرج قواعد بيانات العملاء.
- مجموعة APT تستغل مكتبة برمجية مفتوحة المصدر لتوزيع backdoor على عملاء المكتبة.

2.2.4 تحليل الأثر (ليش الموضوع خطير؟)

- **سرعة الانتشار والضرر:** بعض البرمجيات الخبيثة تنتشر بسرعة داخل الشبكة وتشفّر كل شي.
- **التكاليف المالية:** فدية، تكاليف استعادة، خسائر تشغيلية، غرامات قانونية.
- **تأثير السمعة:** فقدان ثقة العملاء والشركاء.
- **التأثير التشغيلي:** توقف خدمات حيوية، فقدان بيانات مهمة.
- **التعقيد التقني:** هجمات APT طويلة الأمد صعبة الاكتشاف وتحتاج خبرات خاصة للتحقيق.

2.2.5 مؤشرات قد تدل على تهديد خارجي (IOCs)

- زيادة مفاجئة في حركة البيانات الخارجة (Data exfiltration).
- اتصالات لشبكات أو عناوين IP مش مألوفة.
- ملفات مشفرة أو تغيرات مفاجئة في ملفات النظام.
- ظهور عمليات برمجية غير معروفة على الخوادم أو نقاط النهاية.
- رسائل خطأ متكررة أو محاولات تسجيل دخول كثيرة من عناوين مختلفة.
- ظهور عمليات مسح للشبكة (port scans) أو محاولات استغلال متكررة.

2.2.6 كيف نكشف ونحمي (Detection & Prevention)

أ. طبقة الشبكة والبنية التحتية

- **جدران نارية متقدمة (Next-Gen Firewalls):** فلترة الترافيك وتطبيق سياسات.
- **IDS/IPS:** لاكتشاف ومحاولة صد الأنماط الهجومية.
- **تجزئة الشبكة (Segmentation):** عزل الأنظمة الحساسة لتقليل نطاق الضرر.
- **DDoS Mitigation Services / CDN:** حماية مواقع الإنترنت وخدمات الواجهة.

ب. طبقة التطبيقات

WAF (Web Application Firewall): حماية تطبيقات الويب من SQLi، XSS، وغيرها.

Secure Coding & SAST/DAST: فحص الشيفرة والتطبيق لتقليل الثغرات قبل الإنتاج.

إدارة الثغرات (Vulnerability Scanning & Penetration Testing): فحص دوري وإصلاح سريع.

ج. طبقة المستخدم ونقاط النهاية

- **EDR (Endpoint Detection & Response):** كشف وسرعة استجابة للتهديدات على الأجهزة.
- **MFA (Multi-Factor Authentication):** تقليل خطر credential theft.
- **سياسة كلمات مرور قوية وإدارة الهوية (IAM):** التحكم بالوصول وإدارة الحسابات.
- **تدريب وتوعية على التصيد:** محاكاة هجمات ورفع وعي الموظفين.

د. بيانات ونسخ احتياطية

- **نسخ احتياطية منفصلة ومشفرة:** وتأكد من اختبار الاسترجاع دوريًا.
- تشفير البيانات أثناء النقل والتخزين (TLS, at-rest encryption).
- **DLP:** منع خروج البيانات الحساسة خارج المؤسسة.

هـ. استخبارات التهديدات (Threat Intelligence)

متابعة مؤشرات التهديدات الحديثة، قوائم IPs/IOCs، وتحميل تحديثات قواعد الدفاع.

2.2.7 استجابة الحوادث (IR — Incident Response) خطوة بخطوة

- **الإبلاغ الفوري:** أي شك بوجود اختراق يجب الإبلاغ فورًا للفريق الأمني.
- **العزل (Containment):** فصل الأجهزة المصابة أو تعطيل الحسابات المشتبه بها.
- **التشخيص وجمع الأدلة:** حفظ السجلات، صور الذاكرة (memory dumps)، وحفظ الأدلة بطريقة تحافظ على سلامتها.
- **التطهير (Eradication):** إزالة البرمجيات الخبيثة وإصلاح الثغرات المستغلة.
- **الاستعادة (Recovery):** استرجاع الأنظمة من النسخ الاحتياطية والتأكد من سلامة البيانات.
- **التقارير والتواصل:** إخطار الجهات الداخلية والخارجية (إذا مطلوب قانونيًا)، وإعلام المتضررين.
- **التعلّم والتحسين:** مراجعة الحادث، تحديث السياسات، وإجراء اختبارات لمنع تكراره.

2.2.8 سيناريو تطبيقي (Ransomware Walkthrough)

المشهد: موظف فتح ملحق إيميل من مصدر ظاهريًا رسمي. الملحق كان وثيقة Word مع ماكرو مخبأ. بعد فتحه، انتشر Ransomware في الشبكة.

العلامات الأولى: أجهزة تظهر رسائل تشفير، ملفات بامتداد غريب، طلب فدية يظهر على الشاشات.

الإجراءات الفورية:

1. فصل الشبكة وحجب الاتصالات الخارجية التي تستخدمها البرمجية.
2. تشغيل خطة الاستجابة: عزل الخوادم المصابة، إيقاف الخدمات المتأثرة.
3. التحقق من النسخ الاحتياطية وصلاحيتها لاستعادة البيانات.
4. إعلام الإدارة والجهات القانونية/التنظيمية إن لزم.

النتائج المرغوبة: استعادة بيانات من النسخ الاحتياطية، تعزيز سياسات البريد والتحميل، إجراء تدريب تصيد جديد، تركيب EDR وWAF، وتطبيق تحديثات عاجلة للبرنامج الذي استُغل.

2.2.9 قائمة تحقق سريعة للمسؤولين (Quick Checklist)

1. تطبيق MFA على جميع الحسابات الحساسة.
2. تفعيل نظم EDR وSIEM ومراقبة مستمرة.
3. تحديث دوري للبرمجيات/الأنظمة وباتش مانجمنت موثّق.
4. وجود نسخة احتياطية منفصلة ومختبرة (offline/immutable backups).
5. تركيب WAF للواجهات العامة وفحص التطبيقات.
6. سياسات مكافحة التصيد وتدريب دوري للموظفين (spear-phishing simulations).
7. خطة استجابة للحوادث (IR Plan) مختبرة عمليًا (Tabletop & Live drills).
8. اتفاقيات مع مزودين لخدمات DDoS/Threat Intelligence عند الحاجة.
9. اختبارات اختراق دورية وتقارير إدارة لمدى التهديد.
10. مراقبة الاتصالات الخارجية والـDNS لتحذير مبكر عن تسرب بيانات.

2.2.10 خلاصة سريعة

التهديدات الخارجية متنوعة وسريعة التطور — من هجوم بسيط بالـphishing لو شبكة منظمة تشن APT طويلة الأمد. الدفاع الفعال مبني على مبدأ الطبقات: حماية الشبكة، التطبيقات، نقاط النهاية، المستخدمين، والبيانات مع خطة استجابة جاهزة. الوقاية الأفضل دائمًا هي مزيج من تكنولوجيا صحيحة، سياسات واضحة، وتدريب بشري مستمر.

3. أنواع الهجمات السيبرانية(Cyber Attacks Types)

الهجمات السيبرانية صار لها دور كبير بتقويض أنظمة الشركات حول العالم. كل هجوم له أسلوبه، هدفه، ومدى تأثيره. لازم نفهم الأنواع حتى نقدر نتصدى لها بطريقة استراتيجية.

3.1 الهجمات البرمجية (Software Attacks)

3.1.1 شو المقصود بالهجمات البرمجية؟

الهجمات البرمجية هي أي هجوم يعتمد على استغلال ثغرات في البرامج أو النظام، أو استخدام برمجيات خبيثة للوصول للنظام، تعطيله، أو سرقة البيانات. المهاجم ما يحتاج يدخل جسدياً، بل يعتمد على البرمجيات نفسها.

3.1.2 أنواع الهجمات البرمجية وتقييمها

النوع	مدى الضرر	سهولة الاكتشاف	رأي مختصر
Ransomware	عالي جدًا، يمكن تشفير بيانات المؤسسة بالكامل	صعب الاكتشاف قبل التنفيذ	هجوم خطير على المؤسسات، خصوصًا بدون نسخ احتياطية؛ الأفراد أقل تأثيرًا لكنه قد يخسر ملفاتهم الشخصية
Trojan Horse	متوسط إلى عالي، يعتمد على الوظائف المخفية	صعب جدًا، غالبًا يعمل بصمت	يشكل تهديد خفي لكل من المؤسسات والأفراد، خصوصًا عند فتح ملفات مجهولة
Virus / Worm	متوسط إلى عالي، يمكن أن يعطل الشبكة	متوسط، أحيانًا يظهر فور تشغيله	تهديد كلاسيكي لكنه ما زال خطير على المؤسسات إذا انتشر سريعًا؛ الأفراد معرضون لإتلاف الملفات
Exploit Kits	عالي جدًا إذا استُغلت ثغرة مهمة	صعب، خصوصًا إذا استهدف ثغرة جديدة	خطير للمؤسسات التي تعتمد على تطبيقات ويب؛ الأفراد غالبًا يتأثرون عند استخدام برامج قديمة
Spyware / Keylogger	متوسط إلى عالي، سرقة بيانات حساسة	صعب جدًا، غالبًا يعمل خفي	خطر عالي على خصوصية الأفراد والمؤسسات، خصوصًا لو تم جمع بيانات مالية أو كلمات مرور

3.1.3 أمثلة عملية

موظف يفتح ملف Word من بريد مجهول => Ransomware يشفّر ملفات المكتب.

تنزيل برنامج مجاني من الإنترنت => يحتوي Trojan يفتح باب خلفي للمهاجمين.

فيروس ينتشر عبر الشبكة => يعطل الخوادم المشتركة.

مهاجم يستخدم Exploit Kit => يخترق تطبيق ويب ويخرج قاعدة بيانات العملاء.

برنامج Spyware على جهاز موظف => يجمع كلمات المرور والبيانات الحساسة دون علمه.

3.1.4 تحليل الأثر

- **المؤسسات:** الهجمات البرمجية يمكن أن تسبب توقف خدمات، خسارة مالية كبيرة، فقدان بيانات حساسة، وتأثير سلبي على السمعة.
- **الأفراد:** قد يفقدون بيانات شخصية، صور، مستندات مالية، أو كلمات مرور، لكن عادة التأثير المالي أقل من المؤسسات.
- **الاكتشاف:** صعب غالبًا قبل الهجوم، خصوصًا مع الهجمات المخفية مثل Trojans وSpyware.

3.1.5 استراتيجيات الدفاع والحماية

1. تحديث البرمجيات باستمرار (Patch Management).
2. تركيب برامج مضادة للفيروسات وEDR للكشف والتعامل مع البرمجيات الخبيثة.
3. مراقبة الشبكة لاكتشاف نشاط غير طبيعي (Network Monitoring).
4. نسخ احتياطية مشفرة ومنفصلة لضمان استعادة البيانات.
5. تقييد الصلاحيات بحيث الموظفين لا يقدروا يثبتوا برامج عشوائية.
6. تدريب الموظفين على التصيد وملفات البريد المشبوهة.

3.1.6 سيناريو عملي

المشهد: موظف يفتح مرفق إيميل مجهول، الملف يحتوي Trojan.

النتيجة: Trojan يفتح باب خلفي للمهاجمين => يبدأ بسرقة البيانات بشكل خفي.

الاستجابة:

1. فصل الجهاز المصاب عن الشبكة.
2. فحص الجهاز بـ EDR وبرامج مكافحة الفيروسات.
3. استعادة البيانات من النسخ الاحتياطية.
4. مراجعة سياسة البريد والملفات المرفقة وتدريب الموظفين على التصيد.

رأيي: الهجمات البرمجية من أخطر الأنواع لأنها تجمع بين سرعة الانتشار وسهولة استغلال الأخطاء البشرية أو التقنية، خصوصًا على مستوى المؤسسات. الأفراد أقل عرضة للخطر المالي، لكن الخصوصية الشخصية معرضة بشكل كبير.

3.2 الهجمات على الأجهزة (Hardware Attacks)

3.2.1 شو المقصود؟

الهجمات على الأجهزة هي أي محاولة لاستهداف مكونات الحاسوب أو الشبكة نفسها، سواء كانت أجهزة المستخدمين، الخوادم، أو معدات الشبكة. الهدف عادة: تعطيل الأجهزة، الوصول لنظام التشغيل، أو سرقة البيانات بشكل مباشر من الأجهزة.

3.2.2 أنواع الهجمات على الأجهزة وتقييمها

رأي مختصر	سهولة الاكتشاف	مدى الضرر	النوع
تهديد واقعي لكل المؤسسات والأفراد، خصوصًا عند استخدام وسائط غير معروفة	صعب، خصوصًا إذا الموظف غير واعي	متوسط إلى عالي، يعتمد على ما يحويه الفلاش	USB Malware
خطير جدًا على المؤسسات، خصوصًا الخوادم والمعدات الحيوية؛ الأفراد معرضون إذا استخدموا أجهزة قديمة أو غير محدثة	صعب جدًا، غالبًا صامت	عالي جدًا، يمكن التحكم بالجهاز بالكامل	Firmware Attack
عادة تهديد للمؤسسات الحساسة جدًا مثل البنوك أو مراكز البيانات؛ الأفراد نادرًا يتأثرون	صعب جدًا، يحتاج أدوات متخصصة	متوسط، يستهدف جمع معلومات حساسة من الأجهزة	Side-Channel Attack
خطر كبير على المؤسسات، خصوصًا إذا الأجهزة في أماكن غير مؤمنة؛ الأفراد معرضون إذا تركوا أجهزة دون حراسة	متوسط، يعتمد على المراقبة الفيزيائية	عالي جدًا، مثل تركيب أجهزة تنصت أو سرقة الجهاز	Physical Tampering

3.2.3 أمثلة عملية

- موظف يستخدم فلاش USB من مصدر مجهول => يدخل Malware على الشبكة.
- مهاجم يغيّر Firmware للراوتر => يسيطر على كل حركة الشبكة.
- مهاجم يستخدم Side-Channel Attack => يستخرج كلمات مرور من استهلاك الطاقة أو إشعاع الجهاز.
- شخص يسرق خادم أو يركب جهاز تنصت خلف الخوادم في غرفة غير مؤمنة.

3.2.4 تحليل الأثر

- **المؤسسات:** الهجمات على الأجهزة قد تسمح للمهاجم بالسيطرة على الشبكة بالكامل، تعطيل الأنظمة، أو سرقة بيانات حساسة.
- **الأفراد:** غالبًا تأثيره على الخصوصية والبيانات الشخصية، لكن أقل حدة من المؤسسات.
- **الاكتشاف:** غالبًا صعب قبل حدوث الضرر، خصوصًا مع Firmware و-Side Channel، لأن الهجمات غالبًا صامتة.

3.2.5 استراتيجيات الدفاع والحماية

- **تأمين الأجهزة مادياً:** خزانات، غرف خوادم مقفلة، كاميرات مراقبة.
- تحديث Firmware دوري واستخدام نسخ أصلية فقط.
- **مراقبة الأجهزة ونقاط النهاية:** استخدام EDR وتقنيات مراقبة الأداء غير الطبيعي.
- منع استخدام وسائط تخزين غير مصرح بها.
- **تقييد الوصول الفيزيائي:** فقط الأشخاص المخوّلين يمكنهم الوصول للأجهزة الحساسة.
- تدريب الموظفين على التعامل مع الأجهزة وملاحظة أي نشاط مشبوه.

3.2.6 سيناريو عملي

المشهد: مهاجم يضع فلاش USB معدي في مكتب موظف.

النتيجة: بمجرد تشغيل الفلاش، يدخل Malware على الشبكة ⟵ يبدأ بجمع البيانات سرًا.

الاستجابة:

1. فصل الأجهزة المصابة عن الشبكة فورًا.
2. فحص الأجهزة المصابة بـ EDR وبرامج مضادة للفيروسات.
3. منع استخدام وسائط USB غير معروفة مستقبلًا.
4. مراجعة سياسات الوصول الفيزيائي للأجهزة الحساسة.

رأيي: الهجمات على الأجهزة غالبًا أخطر لأنها تمنح المهاجم تحكمًا عميقًا في النظام، خصوصًا مع Firmware و Side-Channel. المؤسسات معرضة بشكل أكبر بسبب عدد الأجهزة وحساسية البيانات، بينما الأفراد غالبًا يتأثرون بالبيانات الشخصية أو الحواسيب المنزلية.

3.3 الهجمات النفسية (Social Engineering)

3.3.1 شو المقصود؟

الهجمات النفسية أو الهندسة الاجتماعية هي أساليب يعتمدها المهاجم لخداع البشر مش الأجهزة. بدل ما يحاول يخترق سيرفر مباشرة، بيستغل ثقة أو خطأ بشري ليحصّل معلومات، يفعل رابط خبيث، أو يخلّي الضحية تعمل إجراء يفتح للمهاجم باب للدخول. باختصار: بيهاجموا العقل قبل ما يهاجموا النظام.

3.3.2 أنواع الهجمات النفسية (الشائعة)

1. Phishing (التصيد العام) :-

إيميلات أو رسائل تبدو من جهة موثوقة (بنك، مزود خدمة) تطلب بيانات أو رابط.

2. Spear-phishing (التصيد المستهدف) :-

نفس الفكرة بس موجهة لشخص أو دور محدد (مثلاً المدير المالي) بمعلومات شخصية لتبدو أقنع.

3. Whaling :-

تصيد موجه لكبار المسؤولين (CEOs, CFOs) بهدف عمليات مالية كبيرة أو سرقة أسرار.

4. Pretexting :-

المهاجم يخلق قصة مقنعة (مثلاً موظف دعم أو محقق) ليحصل على معلومات.

5. Baiting :-

عرض "طعم" (مثلاً USB مجاني أو رابط مجاني) بحيث الضحية تنقر أو توصل جهازها للمهاجم.

6. Quid pro quo :-

عرض خدمة مقابل معلومات (مثلاً اتصال "دعم فني" يعرض حل مشكلة مقابل تنفيذ أو إعطاء بيانات).

7. Tailgating / Piggybacking :-

دخول شخص غير مصرح خلف موظف داخل المبنى أو غرفة سيرفرات.

8. Vishing / Smishing :-

هجمات عبر المكالمات الصوتية (vishing) أو رسائل SMS (smishing) لخداع الضحية.

3.3.3 أمثلة عملية

إيميل يبدو من البنك يطلب "تحديث معلومات الحساب" => دخل الضحية الرابط وأعطى بياناته.

رسالة موجهة لمدير الموارد البشرية باسم "مورد قانوني" تطلب ملفات الموظفين.

فلاش USB ملقى في مواقف السيارات يحمل ملفًا يفتح برنامج تشغيلي عند الاتصال.

مكالمة "من قسم الدعم" تطلب من الموظف تفعيل برنامج وصول عن بعد بحجة حل مشكلة عاجلة.

3.3.4 تحليل الأثر

- **المؤسسات:** الهندسة الاجتماعية ممكن تؤدي لاختراقات واسعة (حسابات المدير، تحويلات مالية، تسريب بيانات). غالبًا الهجوم البشري هو البوابة للأخطار التقنية الكبيرة.
- **الأفراد:** فقدان خصوصية، سرقة هوية، خسائر مالية مباشرة.
- **السبب في فعالية الهجمات:** البشر عرضة للثقة، الضغط الزمني، وعدم اليقظة، خصوصًا لو المهاجم استثمر معلومات شخصية أو ضغط عاطفي.

3.3.5 تقييم مدى الضرر وسهولة الاكتشاف (تقييمي الشخصي)

رأي مختصر	سهولة الاكتشاف	مدى الضرر للفرد	مدى الضرر للمؤسسة	النوع
هجوم شائع وفعال، الوقاية بالتدريب + تقنيات تصفية البريد.	سهل نسبيًا بعد حدوثه (لكن صعب قبله)	متوسط	متوسط - عالي	Phishing
خطر كبير على المدراء والبيانات الحساسة، يحتاج حماية خاصةMFA) ، تحقق ثنائي(	صعب جدًا	عالي (لو استهدف حسابات شخصية مهمة)	عالي جدًا	Spear-phishing / Whaling
يصعب كشفه لأن المهاجم يتكلم هاتفياً ويقنع الضحية؛ التدريب مهم.	صعب	متوسط - عالي	متوسط - عالي	Pretexting / Vishing
سهل التطبيق من المهاجم وفعال لو الموظفين غير واعين.	صعب قبل التنفيذ	متوسط	متوسط - عالي	Baiting (USB)
خطر فيزيائي حقيقي — أحيانًا يسهل تنفيذها داخل بيئة عمل مرنة.	متوسط	منخفض	عالي	Tailgating

رأيي: الهجمات النفسية هي "الثغرة الأسهل" للمهاجم. التكنولوجيا ممكن تحمي أجزاء كبيرة، لكن لو الإنسان خانق (غير مدرّب أو متسرّع) فالمهاجم يحصل على مفتاح النظام.
مؤسسات صغيرة ومتوسطة كثيرًا ما تتهاون بهالنوع؛ وهذا خروج خطير لأن الثمن كبير.

3.3.6 مؤشرات قد تدل على هجوم نفسي جاري أو ناجح

- موظف يفتح روابط أو مرفقات من مصادر غير معروفة.
- طلب مفاجئ لمعلومات حساسة من جهة تبدو داخلية لكن بصيغة غير معتادة.
- ضغط على موظف لاتخاذ إجراء سريع بدون توثيق.
- وجود وسائط USB مجهولة في المكاتب.
- ورود شكاوى عن مكالمات تطلب بيانات داخلية.

3.3.7 استراتيجيات كشف ووقاية عملية (Technical + إنساني)

أ. إجراءات تقنية

- **فلترة البريد (Email Filtering & Anti-Phishing):** حلول تصفية متقدمة تقلل وصول الرسائل المشبوهة.
- **MFA وIAM قوي:** تجعل سرقة كلمة المرور لوحدها غير كافية.
- DMARC / DKIM / SPF: تقي البريد من انتحال المرسل.
- **حظر تنفيذ الماكروز والبرمجيات من المرفقات:** منع تشغيل macros في ملفات Office إلا إذا موثوقة.
- **تقييد استخدام USB:** سياسات أو أدوات تمنع تركيب وسائط غير مرخّصة.

ب. إجراءات بشرية/إدارية

- **تدريب موظفين دوري (Awareness & Simulations):** محاكاة حملات phishing، تعليم كيفية التحقق من طلبات حساسة.
- **سياسات التحقق من الهوية (Verify Requests):** أي طلب لتحويل نقود أو إعطاء بيانات حساسة يتطلب خطوة تحقق ثانوية (call-back، تأكيد عبر قنوات رسمية).
- **تقارير سهلة للإبلاغ عن محاولات التصيد:** قناة سريعة للإبلاغ دون لوم، حتى لو كان الموظف وقع بالخطأ.
- **ثقافة الشك الحذر:** تشجيع الموظفين يسألوا "ليش هدا مطلوب الآن؟" بدل تنفيذ فوري.
- **تدريب فرق الاستقبال والأمن الفيزيائي:** لمنع tailgating والتعامل مع الزوار.

3.3.8 سيناريو تطبيقي (Spear-phishing يستهدف المدير المالي)

المشهد: المهاجم جمع معلومات عامة (OSINT) عن الشركة والمدير المالي عبر لينكدإن وموقع الشركة. بيلّس رسالة تبدو كإمضاء من مدير تنفيذي آخر، يطلب تحويل مبلغ لمورد طارئ.

العلامات: الرسالة فيها لغة استعجال، حساب المرسل قريب لكن مش مطابق تمامًا، الطلب يأتي خارج الإجراءات المالية المعتادة.

الإجراءات الوقائية المثالية:

- وجود سياسة "2 عيون" على أي تحويل مالي (شخصان يوافقان).
- التحقق عبر قنوات بديلة (اتصال هاتفي موثوق).
- استعمال MFA وأنظمة مراقبة التحويلات الغريبة.

لو فُعل الخطر:

عزل وتحليل الرسائل، فتح تحقيق، استرجاع الأموال إن أمكن، إشعار الإدارة والقانونية، وتحديث التدريب لكل الفريق.

3.3.9 قائمة تحقق سريعة للمؤسسة (Quick Checklist)

- تنفيذ حلول فلترة البريد وAnti-Phishing.
- تفعيل MFA على كل الحسابات الحساسة.
- سياسة تحقق ثانية على التحويلات المالية (Segregation of Duties).
- حظر تشغيل الماكروز بشكل افتراضي وفحص المرفقات.
- حظر أو تقييد USB/وسائط خارجية.
- جلسات تدريب ومحاكاة تصيد دورية للموظفين.
- قناة إبلاغ بسيطة عن محاولات التصيد (بدون عقاب للخطأ الأول).
- آموزش فرق الاستقبال والحراسة على منع tailgating.
- إنشاء Checklists لإجراءات الطوارئ عند الشك بتحويل أو طلب حساس.

3.3.10 الخلاصة + رأيي

الهجمات النفسية تعتمد على العنصر البشري — وده اللي بيخليها أخطر وأسهل تطبيقًا في كثير من الحالات. التكنولوجيا تعطينا أدوات دفاع قوية، لكن بدون تدريب وثقافة أمنية فعلية، راح تكون هالطبقة الدفاعية هشة.

رأيي العملي: الاستثمار في التدريب الواقعي (محاكاة هجمات)، سياسات تحقق صارمة، وآليات بسيطة للإبلاغ، يعطوا نتيجة أكبر أحيانًا من شراء حلول تقنية باهظة. خلي الناس تكون أول خط دفاع وليس نقطة ضعف.

4. حساسية البيانات وجمع المعلومات (OSINT)

4.1 شو المقصود بـ "حساسية البيانات" و"OSINT"؟

حساسية البيانات: يعني قديش المعلومة هادي حساسة لو انسرقت أو تغيرت — هل بتأثر على سمعة الشركة، على أموال العملاء، أو على سرية مشاريع؟ بيانات بسيطة زي منشورات عامة أقل حساسية، بينما قواعد بيانات العملاء أو مفاتيح التشفير حسّاسة جدًا.

OSINT (Open Source INTelligence): عبارة عن كل المعلومات المتاحة للعامة واللي المهاجم يقدر يجمعها بدون اختراق رسمي — من مواقع إنترنت، شبكات اجتماعية، سجلات DNS، مستودعات كود، إعلانات توظيف، وحتى مستندات PDF منشورة بالإنترنت. المهاجم الذكي يبني صورة عن المؤسسة من المصادر المفتوحة قبل ما يحاول الهجوم.

4.2 أنواع البيانات وحساسيتها (تصنيف مبسّط)

نقسم البيانات حسب الحساسية وتأثير التسرب:

1. البيانات الشخصية الحساسة (PII / PII الحساسة)

أمثلة: أرقام الهوية، أرقام جواز/جنسية، بيانات صحية.

حساسية: عالي جدًا — تسبب مشاكل قانونية وضرر للأفراد.

2. البيانات المالية

أمثلة: أرقام حسابات بنكية، سجلات دفعات، معلومات بطاقات.

حساسية: عالي جدًا — خسائر مالية مباشرة ومساءلة قانونية.

3. أسرار تجارية وملكية فكرية (IP)

أمثلة: تصميمات، خوارزميات، خطط منتجات.

حساسية: عالي — فقدان ميزة تنافسية.

4. صلاحيات الوصول وبيانات الاعتماد (Credentials / Keys)

أمثلة: كلمات مرور، مفاتيح API، شهادات TLS الخاصة.

حساسية: حرج جدًا — دخول مباشر للنظام.

5. معلومات بنية الشبكة والتكوين (Infra / Configs)

أمثلة: عناوين IP داخلية، ملفات configs، خرائط الشبكة.

حساسية: متوسط - عالي — تُسهل الاستهداف التقني.

6. بيانات عامة/تسويقية

أمثلة: الكتالوجات، الأخبار الصحفية.

حساسية: منخفضة — لكنها تُستخدم في هندسة اجتماعية.

7. سجلات ونسخ احتياطية

أمثلة: backup snapshots، logs كاملة.

حساسية: عالي — تحتوي بيانات مركبة قابلة للاستخراج.

4.3 كيف الهاكر يجمع المعلومات (OSINT) — مصادر وتقنيات

المهاجم بيركّب "بورتريه" عن المؤسسة من مصادر عامة، عادة بالخطوات التالية:

- المواقع الرسمية: صفحات "عنّا"، ملفات التعريف، PDFs، ملفات word/pdf قد تحتوي metadata.
- **الشبكات الاجتماعية:** LinkedIn (الموظفين والمناصب)، Facebook, Twitter — معلومات عن الأسماء، المناصب، الأحداث.
- **محركات البحث & Google Dorking:** العثور على ملفات مفتوحة، قواعد بيانات منسوخة، أو صفحات مؤرشفة.
- **مستودعات الكود (GitHub, GitLab):** مفاتيح مطروحة بالخطأ، ملفات config، أو تعليمات تشغيل تكشف التقنية المستخدمة.
- **WHOIS وDNS:** كشف سجلات النطاق، خوادم البريد، سجلات MX وSRV، subdomains.
- **Shodan / Censys:** كشف أجهزة متصلة بالإنترنت، خوادم، كاميرات، قواعد بيانات مكشوفة.
- **مواقع التسريب وPastebin:** قواعد بيانات مسروقة منشورة، كلمات مرور.
- **إعلانات الوظائف:** تكشف التقنيات المستخدمة، مزايا داخلية، أو بنية الفريق.
- **Certificates Transparency:** شهادات TLS تكشف أسماء نطاقات فرعية.

- الـ Metadata في الملفات (منشورات PDF/Word/Images) — قد تحتوي على أسماء المستخدمين أو المسارات.
- Dumpster diving وزيارات فيزيائية: مستندات مطبوعة، أو معلومات عن الشحن والتوريد.

المهاجم الذكي يجمع من كل هالمصادر ويبني سيناريوهات للهجوم — خاصة لعمل Spear-phishing أو لاكتشاف ثغرات في شبكتك.

4.4 أمثلة عملية لكيف OSINT يؤدي لاختراق

- إيجاد مطور نشر ملف config.json على GitHub يحتوي على مفتاح API — المهاجم يستخدم المفتاح للوصول لخدمات الشركة.
- عثور على إعلان وظيفي يذكر "نستخدم X tool على port 8080" — المهاجم يفحص هذا الـport ويجد واجهة إدارية غير محمية.
- جمع أسماء مدراء الموارد البشرية وبيانات عن موظفين — صنع رسالة Spear-phishing تبدو موثوقة وتؤدي لسرقة بيانات.
- Shodan يظهر قاعدة بيانات MongoDB مكشوفة على الإنترنت — المهاجم يستخرجها ويبيعها

4.5 تقييم الحساسية: مدى الضرر وسهولة الاكتشاف (تقييمي الشخصي)

نحط جدول مبسّط يوضح كل نوع بيانات: مدى الضرر لو انسرق، وسهولة اكتشاف التسريب.

نوع البيانات	مدى الضرر لو انسرق	سهولة اكتشاف التسريب	رأيي المختصر
مفاتيح / API Credentials	حرج جدًا	صعب (غالباً يُستَخدَم بدون كشف فوري)	أخطر أنواع البيانات لأن الاختراق يصير فورًا
بيانات مالية (حسابات/بطاقات)	عالي جدًا	متوسط (تظهر التعاملات لكن بعد وقوعها)	تستوجب حماية قانونية وتقنية مشددة
PIIحساسة	عالي جدًا	متوسط - قد يتكشف عبر شكاوى أو تجاوزات	له تبعات قانونية واجتماعية كبيرة
أسرار تجارية / IP	عالي	صعب (يُكشف عندما يستخدم المنافس أو يتسرب)	تأثير طويل المدى على تنافسية الشركة
تكوينات Infra/ info	متوسط - عالي	متوسط (يعتمد مراقبة الشبكة)	مفيد للمهاجم في مرحلة الاستطلاع — يجب تقليله
سجلاتBackup/	عالي	صعب (قد تظل مخفية لفترة)	تحتوي على تراكم من المعلومات الهامة
بيانات عامة/تسويقية	منخفض	سهل الاكتشاف	تُستخدم لهندسة اجتماعية أكثر مما تُسبب خسارة مادية مباشرة

4.6 تحليل المخاطر: شو الخطر الحقيقي على المؤسسة؟

OSINT ما هو اختراق مباشر لكن هو المرحلة الأولى لأي هجوم ناجح. أقل قدر من المعلومات يمكن أن يخفض تكلفة الهجوم ويزيد نجاحه.

المؤسسات اللي عندها بيانات حساسة مكشوفة معرضة لهجمات تصيد متقدمة واستغلالات تقنية مباشرًة.

عادة ما لا تُكتشف جمعيات OSINT إلا بعد وقوع حادث أكبر؛ لذلك الوقاية مبكرة أهم بكثير من الكشف بعد الضرر.

4.7 كيف ندافع؟ إجراءات عملية لتقليل خطر OSINT وتسريب البيانات

أ. إدارة البيانات وتقليل السطح المعرض (Data Minimization & Inventory)

- **جرد البيانات (Data Inventory):-** عرف كل أنواع البيانات وين مخزنة ومنو له وصول.
- **تصنيف البيانات (Data Classification):-** عرف شو حساس (Confidential/Restricted) وشو عام.
- **تقليل نشر المعلومات:** راجع ما يُنشر في الموقع، الوثائق، ملفات PDF، وحذف metadata قبل النشر.

ب. حماية الاعتماديات والمفاتيح

- **عدم وضع مفاتيح في الكود العام:** استخدم secret managers وبيئة CI/CD آمنة.
- **دوران المفاتيح (Key Rotation):** غيّر المفاتيح دورياً أو فور كشفها.
- **مراقبة الاستخدام:** رصد أنماط استعمال المفاتيح للكشف عن إساءة الاستخدام.

ج. تحصين الواجهة العامة

تقييد عرض الـsubdomains ورفض كشف معلومات داخلية.

تأمين بوابات الإدارة: لا تعرض واجهات إدارة علنياً — استخدم VPN أو IP allowlists.

فحص دوري بواسطة Shodan/Censys لمعرفة ما هو معروض على الإنترنت.

د. تقليل المعلومات على الشبكات الاجتماعية

- **سياسة نشر رسمية:** منو يقدر ينشر عن الشركة؟ شو المسموح؟
- **توعية الموظفين:** لا يشاركوا معلومات داخلية على لينكدإن أو تويتر.
- **مراجعة ملفات الموظفين العامة:** اطّلع على معلومات الموظفين المنشورة واطلب حذف ما يعرّض للخطر.

هـ. تقنيات وحلول

- **DLP (Data Loss Prevention):** منع خروج بيانات حساسة عبر البريد أو السحابة.
- **IAM + MFA:** تحكم صارم بصلاحيات الدخول ومنع إعادة استخدام الحسابات.
- **SIEM + UEBA:** رصد نشاطات مشبوهة وتحليل سلوك الاستخدام
- **Web Application Scanning & SAST/DAST:** فحص تطبيقات الويب لمنع كشف قواعد البيانات.
- **Secret Scanning (GitGuardian-like):** فحص مستودعات الكود لاكتشاف تسرب أسرار.
- **Threat Intelligence / Brand Monitoring:** مراقبة الشبكة العنكبوتية عن ذكر اسم الشركة أو تسريبات محتملة.

و. إدارة طرف ثالث (Third-party Risk)

- **تقييم موردي الخدمة:** هل شريكك يخزن بياناتك؟ كيف يحميها؟
- **شروط بالعقود:** بنود أمان، إشعار في حال وقوع تسريب، والتزام باتباع معايير.
- **فحص دوري لموردي التوريد:** Pen-test وsecurity audit.

ز. الحوكمة والقوانين

- **سياسات حفظ البيانات وحذفها:** لا تخزن بيانات لازم تتحذف بعد فترة.
- **الامتثال:** التزام بلوائح (GDPR-like أو قوانين محلية) وإجراءات إشعار الاختراق.

4.8 سيناريو عملي (من جمع OSINT للاختراق ثم الاستجابة)

السيناريو: مهاجم يريد سرقة بيانات رواتب شركة متوسطة.

جمع المعلومات (OSINT): يجمع أسماء موظفين من LinkedIn، يجد مستودع GitHub يحوي ملف deploy.sh بأمر يوضح وجود S3 bucket باسم company-backups

الاستكشاف التقني: يستخدم Shodan ليتأكد من أن بعض الـbuckets ليست مؤمنة.

استغلال: يجد أن الـS3 كان عامًا — يحمل نسخة احتياطية تحتوي على جدول رواتب.

هندسة اجتماعية: يرسل رسائل Spear-phishing لمدير الموارد البشرية بطلب "تأكيد" مع رابط يؤدي لملف مزيف لسرقة بيانات الدخول.

النتيجة: يحصل على بيانات الموظفين ويبدأ ببيعها أو ابتزاز الشركة.

إجراءات منع ومراقبة كانت تمنع الحادث:

- secret scanning يمنع مفاتيح في GitHub.
- سياسة نشر تمنع جعل S3 عامًا.
- DLP وSIEM يكتشفون تحميلًا غير معتاد من S3 أو حركة نقل بيانات كبيرة.
- تدريب HR على التحقق ثنائياً لأي طلب حساس.

4.9 قائمة تحقق سريعة لحماية الحساسية وOSINT (Quick Checklist)

- عمل جرد كامل للبيانات وحصر مكان تخزينها.
- تصنيف البيانات (Public / Internal / Confidential / Restricted).
- إزالة الـmetadata من الملفات قبل نشرها علنًا.
- منع نشر المفاتيح والكلمات السرية في الكود (secret manager).
- تفعيل DLP على بوابات البريد والسحابة.
- تفعيل IAM مع مبدأ Least Privilege وMFA.
- فحص دوري باستخدام Shodan/Censys وSecret Scanners.
- سياسة نشر موحدة وتوعية للموظفين عن OSINT.
- تحقق من إعدادات سحابات التخزين (S3, Azure Blob) للتأكد من عدم كونها عامة.

- اتفاقيات أمن مع الموردين وعمليات تدقيق دورية.
- خطة استجابة للحوادث تتضمن استجابة لتسريبات OSINT.

4.10 الخلاصة ورأيي

الـOSINT هو سلاح ذو حدين: للمهاجم، معلومات بسيطة من الإنترنت قد تفتح له الباب كله؛ وللمؤسسة، التنبّه لمصادر المعلومات المفتوحة وقدرية التحكم بها ممكن يمنع هجمات كبيرة.

رأيي العملي: الاستثمار في جرد البيانات، منع تسريبات المفاتيح، وفحص السطح الهجومي العام دوريًا يعطينا دفاعًا وقائيًا قوي — غالبًا أكثر فعالية من الإنفاق على كشف الاختراق لاحقًا.

5. الهجمات المتقدمة (Advanced Attacks)

الهجمات المتقدّمة مش زي الهجمات العادية — هاي غالبًا بتكون مخططة، متعدّدة المراحل، بتستهدف طبقات عميقة بالنظام (نظام التشغيل، النواة، الفيرموير، أو سلاسل التوريد)، وغالبًا هدفها البقاء طويلًا داخل بيئة الهدف لجمع معلومات مهمة أو تخريبها بهدوء. المهاجمين هون ممكن يكونوا مجموعات منظّمة (APTs) أو أطراف بدعم متقدّم. عشان كده الدفاع لازم يكون طبقي، تقني وإداري بنفس الوقت.

5.1 أنواع الهجمات المتقدمة وتعريفها

5.1.1 Kernel / Ring-0 Attacks (استغلال النواة)

شو هي؟ استغلال ثغرات في نواة نظام التشغيل (Kernel) للحصول على صلاحيات أعلى جداً (Ring-0) والتحكم الكامل بالنظام.

لماذا خطيرة؟ لأن أي كود شغّال في النواة يقدر يلغي آليات الحماية وحتى يخفي وجوده.

5.1.2 Rootkits

شو هي؟ مجموعة أدوات برمجية تُثبت نفسها لتخفي وجود برامج خبيثة أو نشاط المهاجم، وتمنع اكتشافه على مستوى النظام أو النواة.

لماذا خطيرة؟ بتعمل استمرارية للاختراق وتسهل جمع البيانات دون الكشف.

5.1.3 Firmware / BIOS Attacks

شو هي؟ تعديل أو استبدال الـ firmware (مثلاً BIOS/UEFI، firmware للراوتر، للـ SSD) لزرع كود يتحكّم بالجهاز قبل ما يشتغل نظام التشغيل.

لماذا خطيرة؟ لأنها تعمل تحت نظام التشغيل — إعادة تثبيت النظام غالبًا ما ما بتنهيها.

5.1.4 Supply-Chain Attacks (سلاسل التوريد)

شو هي؟ استهداف مورّد/مكتبة/أداة طرف ثالث لإدخال برمجية خبيثة ضمن المنتج اللي توزّع على عملاء كثيرين.

لماذا خطيرة؟ لأنها توصل المهاجم لكثير مؤسسات دفعة وحدة ومن الصعب توقعها.

5.1.5 APTs — Advanced Persistent Threats

شو هي؟ مجموعات من الهجمات طويلة الأمد، منظمة، تهدف للتجسس أو التخريب على هدف محدد (مثلاً حكومة أو شركة استراتيجية). تستخدم مخلوطات من Phishing, 0-day exploits, lateral movement, persistence.

لماذا خطيرة؟ لأنها إصرار وموارد ووقت — المهاجم يندمج داخل الشبكة ويعمل بصمت لسنوات أحيانًا.

5.1.6 Kernel-Level Rootkits و Hypervisor Attacks

هجمات تستهدف Virtualization layer أو hypervisor عشان يسيطر على آلات افتراضية متعددة — خطورتها عظيمة في بيئات السحابة.

5.2 أمثلة واقعية (مبسطة وقابلة للفهم)

- **Rootkit:** يخبّي نشاط المهاجم على سيرفر مهم بحيث الأدلة تختفي من السجلات.
- **Firmware malware:** يُصيب راوتر شركة ويوجه الترافيك لصالح المهاجم.
- **Supply-chain:** حزمة مكتبات فيها تروجان تُوزّع عبر تحديث رسمي لمئات الشركات.
- **APT:** مجموعة تستهدف شركة طاقة، تدخل عبر spear-phishing، تبني بوابات وصول طويلة المدى وتسرق خطط تشغيلية سنين.

5.3 تحليل الأثر (ليه الهجمات المتقدمة خطيرة؟)

- **قدرة البقاء (Persistence):** المهاجم يقدر يبقى شهور أو سنين بدون اكتشاف.
- **الاختفاء من الأدلة:** rootkits وتراكيب نواة بتخفي آثار الهجوم وتمنع الفحص التقليدي.
- **التحكم العميق:** الوصول إلى نواة أو فيرمور يعني تحكم كامل تقريبًا.

- **الانتشار على مستوى المؤسسة/السحابة:** خاصة لو كان الاستهداف لسلاسل التوريد أو الـhypervisor.
- **تعقيد الاستجابة:** يحتاج خبراء، أدوات متقدمة، وربما استبدال أجهزة مادية.

5.4 تقييم (مدى الضرر وسهولة الاكتشاف) — جدول ملخص وتقييمي

الأولوية للمعالجة	سهولة الاكتشاف	مدى الضرر	النوع
عاجل جدًا	صعب جدًا (قد يخبئ نفسه على مستوى النواة)	حرج جدًا / كارثي	Kernel / Ring-0 Exploit
عاجل جدًا	صعب جدًا (يصعب كشفه بالأدوات العادية)	حرج جدًا	Rootkits
عاجل جدًا	صعب جدًا - عادة لا يظهر في الفحص العادي	حرج جدًا	Firmware Attacks
عاجل جدًا	متوسط - يعتمد على كشف المصدر	حرج جدًا (موسّع النطاق)	Supply-Chain Attack
عاجل/طويل الأمد	متوسط إلى صعب (اكتشاف متأخر شائع)	عالي إلى حرج	APT(مراحل متعددة)
عاجل جدًا	صعب جدًا	حرج جدًا للسحابة	Hypervisor Attacks

رأيي المختصر: هالهجمات هي "الكابوس" للتشغيل المستمر — لأن تأثيرها طويل المدى وغالبًا يكلف تغيير بنية تحتية أو توريدات. اكتشافها متأخر في معظم الحالات، لذا الوقاية والتحصين المبكر مهم جدًا.

5.5 مؤشرات (IOCs) قد تدل على هجوم متقدم

- سجلات نظام مغيّبة أو معدّلة على مستوى low-level.
- تغيّر في firmware versions بدون توثيق.
- نشاط شبكي لا يفسّره تطبيق أو المستخدم (C2 traffic مموّه).
- وجود عمليات خفية في الذاكرة لا تظهر كملفات على القرص.
- فشل متكرر في التحديثات/بوت النظام أو سلوك boot غير طبيعي.
- استخدام أدوات إدارية بطرق غير معتادة أو من حسابات غير متوقعة.
- كشف مفاتيح API/شهادات مُسربة تُستخدم للوصول الداخلي.

5.6 استراتيجيات دفاع عمليّة وطبقيّة (Defense-in-Depth for Advanced Attacks)

أ. تقوية النواة والـOS

- تحديث النظام ونواة التشغيل باستمرار — لكن مع اختبار قبل البيئات الإنتاجية.
- استخدام تقنيات Hardening: kernel hardening (مثل grsecurity/PaX approached where possible)، إغلاق ميزات غير مستخدمة.
- تمكين صفحة وقف تنفيذ التعليمات (NX/DEP), ASLR لمنع استغلال الذاكرة بسهولة.

- Signed Kernel Modules — السماح فقط للـ modules الموقعة بالعمل.

ب. حماية الفيرموير ومراقبته

- Secure Boot / Measured Boot — التأكد من سلامة الـboot chain.
- تحديث Firmware عبر قنوات موثوقة ومؤمنة، مع تحقق من التواقيع الرقمية.
- استخدام HSM أو TPM لتخزين المفاتيح الحساسة.
- فحص تكامل الفيرموير دوريًا واستخدام أدوات كشف التغيّرات.

ج. كشف الجذور والبرمجيات الخفية

- EDR متقدّم + Memory Forensics — مراقبة الذاكرة وتحليل السلوك غير الاعتيادي.
- Integrity Monitoring: مراقبة تغيّرات في ملفات النظام والسجلات بنظام لا يُعدّل بسهولة.
- Periodic offline scans (boot from trusted media) لفحص الأجهزة المشكوك بها.

د. حماية سلسلة التوريد

- تحقق من توقيع البرمجيات والحزم قبل تثبيتها.
- Secret Scanning & Code Review لمنع مفاتيح مضمّنة في المستودعات.
- تقييم أمان الموردين: Security questionnaires، audits، وSLA's أمنية تضمن إشعار عن الاختراق.
- تقليل الاعتماد على مكتبات غير موثوقة واستخدام نسخة مؤمنة ومحكّمة.

هـ. شبكات وسحابة مؤمّنة

- Segmentation صارمة — عزل الأنظمة الحساسة حتى لو اخترق جزء.
- مبدأ الأقل صلاحية (Least Privilege) وJust-in-Time access للأذونات العالية.
- مراقبة Hypervisor/Cloud Control Plane واستخدام CSPM / Cloud-Threat detection.
- Immutable infrastructure وInfrastructure as Code مع مراجعات أمان قبل نشر التغييرات.

و. الاستعداد والقدرات التحليلية

- فريق IR جاهز + SOC متقدّم قادراً على memory forensics و malware reverse engineering.
- نُهج للتعامل مع 0-day: Sandbox، Isolation، وRapid patch testing.
- Threat Hunting دوري لاكتشاف أي نشاط بصمة منخفضة.

5.7 خطوات استجابة عملية (IR) لهجوم متقدم

- العزل الفوري للأجزاء المتأثرة (network segmentation, isolate hosts).
- جمع الأدلة بأمان (memory dumps, disk images, logs) مع الحفاظ على السلسلة الجنائية للأدلة.
- **التحليل العميق:** memory forensics, rootkit analysis, firmware analysis.
- **التواصل الداخلي/القانوني:** إشعار الإدارة، الفرق القانونية، والتعاون مع جهات خارجية متخصصة إن لزم.
- **إصلاح وبناء بديل:** في حالات الفيرموير أو rootkit قد يتطلب الأمر استبدال الأجهزة أو إعادة فلاش الفيرموير من مصدر موثوق.
- **استعادة بنظام منقّح:** إعادة الأنظمة بعد التأكد من خلوها، واختبار شامل.

- **بعد الحادث:** تقرير مفصّل، تحديث سياسات، وإجراء دروس مستفادة وتحسين الدفاعات.

5.8 سيناريو تطبيقي (Walkthrough — هجوم متقدم عبر سلسلة التوريد)

المشهد: مزوّد أدوات بناء (build tool) أصدر تحديثًا يحتوي على مكتبة ملوّثة تحمل backdoor. آلاف الشركات تستقبل التحديث تلقائيًا.

العملية:

1. المهاجم زرع backdoor في مكتبة الطرف الثالث.
2. تحديث المكتبة ينتشر لمئات المشاريع داخل الشركات.
3. المهاجم يستخدم backdoor للانتشار داخل شبكات عملاء محددين، يجمع بيانات حساسة ويثبت persistence عبر firmware لعدد من الخوادم.

اكتشاف الحادث: بالاكتشاف القليل في البداية عبر SIEM الذي رصد نشاط C2 غير اعتيادي من أجهزة مُحددة. بعد تهجّم Threat Hunting وتحليل الشيفرة، اكتشفوا المصدر هو التحديث.

الاستجابة:

1. إيقاف استخدام النسخ المتأثرة، استبدال الحزم، عمل مراجعة كاملة للـ dependencies.
2. فحص الأجهزة المشبوهة، استبدال أو فلاش الفيرموير المتضرر.
3. إشعار الموردين والعملاء المتأثرين، وتطبيق شروط أقوى على التزوّد.
4. الدروس: تحقق من توقيع الحزم، استخدام SBOM (Software Bill of Materials)، فحص التبعيات بانتظام، ووجود قدرة للسحب السريع (rollback) للتحديثات.

5.9 قائمة تحقق سريعة للحماية من الهجمات المتقدمة (Checklist)

- تفعيل Secure Boot وMeasured Boot على الأجهزة الحساسة.
- استخدام TPM/HSM لتخزين المفاتيح.
- فرض توقيع رقمي على Kernel modules والـfirmware.
- فحص تكامل الفيرموير دوريًا وإدارة تحديثات موثوقة.
- تنفيذ Segmentation وJust-in-Time access للأذونات الحرجة.
- استخدام EDR متقدّم مع قدرات memory forensics.
- Threat Hunting دوري وسياسات SIEM متقدّمة.
- تقييم ومراجعة سلسلة التوريد وطلب SBOM من الموردين.
- سياسة صارمة لإدارة الحزم المفتوحة المصدر وفحص السرّيات (secret scanning).
- تدريب فريق IR على rootkit/firmware analysis أو اتفاقيات مع فرق خارجية متخصصة.
- اختبار استعادة الأنظمة (disaster recovery) بما يشمل استبدال الأجهزة إن لزم.

5.10 الخلاصة ورأيي العملي

الهجمات المتقدمة هي تهديد من نوع آخر — مش بس لأنها تقنية قوية، لكن لأنها تخبئ نفسها تحت طبقات السيستم وتستفيد من أي ضعف في سلسلة التوريد أو في إجراءات النشر. الوقاية أفضل بكثير من الاستجابة هنا: تقوية عملية التطوير (DevSecOps)، توقيع كل مكوّن، فحص التبعيات، ووجود SIEM/EDR وفِرَق مختصة — هذول كلهم هم الفارق.

رأيي: المؤسسات الكبيرة والحساسة لازم تعتبر الهجمات المتقدمة تهديد وجودي — استثمار مبكر في hardening، مراقبة متقدمة، وتعاون مع خبراء خارجيين يوفر وقت ومال على المدى الطويل. القوة الحقيقية هون مش بس في شراء أدوات، بل في دمج الأمان داخل دورة حياة التطوير والإدارة اليومية.

6. تحليل وتقييم شامل

6.1 الهدف والطريقة بسرعة

الهدف: نحدّد أي مخاطر تشكل أعلى تهديد للمؤسسة، ليش، وإيش الخطوات العملية لترتيب أولويات المعالجة والحد من الضرر.

الطريقة (بمراحل بسيطة):

- جرد للأصول والبيانات (what we have).
- تحديد التهديدات والثغرات المرتبطة بكل أصل.
- تقييم الاحتمال (Likelihood) والتأثير (Impact) لكل نقطة.
- حساب المخاطر (Risk = Likelihood × Impact) وتحديد الأولويات.
- اختيار ضوابط مناسبة (Technical / Org / Physical).
- مراقبة وقياس فعالية الإجراءات (KPIs وMetrics).

6.2 تعريف مصفوفة التقييم (بسيطة ونستخدمها)

نستخدم مقياسين أساسيين لكل خطر:

الاحتمال (Likelihood):

- 1 = نادر
- 2 = ممكن
- 3 = محتمل
- 4 = متكرر
- 5 = شبه مؤكد

التأثير (Impact):

- 1 = بسيط (Minor)
- 2 = منخفض (Low)
- 3 = متوسط (Moderate)
- 4 = عالي (High)
- 5 = كارثي (Catastrophic)

المخاطرة = التأثير * الأحتمال (النطاق 1-25)

- 1–6 = منخفض (Green)
- 7–14 = متوسط (Yellow)
- 15–25 = عالي / عاجل (Red)

مثال: اذا اكتشفنا هجوم احتماله هو متكرر(4) وتأثيره عالي(4) فا المعادلة تصبح 4*4والناتج هو 25 (أي عالي /عاجل يجب اتخاذ اجراء عاجل وطارئ بشأن الهجوم)

6.3 مصفوفة نموذجية لمخاطر مُختارة (أمثلة عملية)

هذي أمثلة نموذجية — كل مؤسسة تحوّلها على بياناتها الفعلية بعد الجرد.

تصنيف الأولوية	Risk Score	Impact (1-5)	Likelihood (1-5)	تهديد / ثغرة
عالي - عاجل	20	5	4	Ransomwareعلى خوادم الإنتاج
عالي - عاجل	15	5	3	موظف غير راضٍ يسرّب بيانات حساسة
عالي - عاجل	16	4	4	Spear-phishingيستهدف الإدارة المالية
متوسط-عال	12	4	3	كشف مفاتيح API علىGitHub
متوسط	10	5	2	Firmware compromiseعلى الراوتر الرئيسي
متوسط	9	3	3	DDoSلموقع الشركة التسويقي
متوسط	10	2	5	كشف بيانات عامة مستخدمة للهندسة الاجتماعية

رأيي: عادةً الفدية، الهجمات التي تستهدف النواة/الفِرمور، والتصيد الموجَّه لطبقة الإدارة، هم اللي لازم يتعالَجوا أولًا لأنهم يجمعوا بين احتمال متوازن وتأثير كارثي.

6.4 تحليل الأسباب الجذرية (Root Cause Analysis) — أمثلة

لماذا تنتشر Ransomware؟ => ضعف في تحديث الأنظمة، صلاحيات زائدة، ضعف نسخ احتياطية أو اختبارات استرجاع.

لماذا نقع في Phishing؟ => وعي بشري ضعيف، فلترة بريد ضعيفة، ولا MFA على الحسابات الحيوية.

لماذا نكوّن سطح هجوم كبير عبر OSINT؟ => نشر بيانات غير ضرورية، مفاتيح مخفية في الكود، إعدادات سحابة عامة.

6.5 أولويات المعالجة (Prioritization & Roadmap)

نقسم العمل إلى ثلاث موجات زمنية: فوري (0–30 يوم)، قصير المدى (1–3 شهور)، متوسط/طويل المدى (3–12 شهر).

أ. فوري (0–30 يوم) — أشياء لازم تعملها الآن

1. تفعيل/فرض MFA على كل الحسابات الحرجة.
2. فحص النسخ الاحتياطية والتأكد من قابليّة الاستعادة (Restore test).
3. تطبيق تحديثات أمان حرجة على الخوادم والبنية التحتية.
4. إعداد فلتر بريد أساسي مع قواعد منع التصيد وفحص المرفقات.
5. فرض سياسة Least Privilege على حسابات مسؤولة.

ب. قصير المدى (1–3 شهور)

1. نشر EDR وSIEM وربط التنبيهات الأساسية.
2. تنفيذ محاكاة phishing وتدريب الموظفين.
3. إغلاق وتحصين واجهات الإدارة (WAF, VPN only, IP allowlist).
4. فحص المستودعات للكشف عن سرّيات (secret scanning).
5. تنفيذ سياسة إدارة التصحيحات (Patch Management) ووضع جدول زمني.

ج. متوسط/طويل المدى (3–12 شهر)

1. تنفيذ Network Segmentation وJust-in-Time access للأذونات الحرجة.
2. تطبيق Secure Boot / TPM وHardening في الأجهزة الحساسة.
3. تنفيذ برنامج إدارة ثغرات (Vulnerability Management Lifecycle).
4. تقييم سلسلة التوريد وطلب SBOM من الموردين.
5. بناء فريق IR أو التعاقد مع مزود خدمات استجابة للحوادث (MDR/SOC).
6. تنفيذ عمليات Threat Hunting دورية وتحسين SIEM rules.

6.6 اختيار الضوابط الممكنة لكل فئة خطر (مقترح مختصر)

Ransomware ⟶ Backups immutable + EDR + Patch mgmt + Network segmentation + User training.

Internal Data Leak ⟶ DLP + Least Privilege + Logging & UEBA + Exit procedures.

Phishing / BEC ⟶ Email filtering + MFA + User simulation + Policies for payments.

Supply Chain ⟶ SBOM + Package signing + Vendor security assessments + CI/CD hardening.

Firmware/Kernel attacks ⟶ Secure Boot + Firmware signing + Memory forensic capability + Replacement policy.

6.7 KPIs وMetrics لقياس التقدّم (مهم عشان تعرف إذا الكل فعّال)

MTTR (Mean Time To Recover) — متوسط وقت الاستعادة بعد حادث.

MTTD (Mean Time To Detect) — متوسط وقت الاكتشاف.

%patched systems (within X days) — نسبة الأنظمة المحدثة خلال 60/30 يوم.

Number of successful phishing clicks (per campaign) — نجاح المحاكاة.

Number of critical vulnerabilities (open >30 days) — الثغرات الحرجة المفتوحة.

Backup restore success rate (%) — نجاح اختبارات الاسترجاع.

Number of privileged accounts reviewed (monthly) — مراجعات الوصول.

False positive rate for SIEM alerts — جودة التنبيهات.

6.8 خطة مراقبة & تقرير للإدارة (Executive Summary format — موجز للإدارة)

الأهداف: تقليل احتمال الحوادث الكبيرة، تقليل مدة التعافي، حماية الأصول الحساسة.

الحالة الآن: (مثال) معرضين لـRansomware بسبب نسخ احتياطية غير معزولة ووجود حسابات بصلاحيات واسعة.

أولوية العمل: أولاً تنفيذ MFA، ثانياً نشر EDR، ثالثاً اختبار النسخ الاحتياطية، ورابعاً محاكاة phishing.

تكلفة تقريبية: (تعتمد على حجم المؤسسة) — نحتاج ميزانية لشراء أدوات EDR/SIEM + تدريب + موارد تنفيذ.

مقاييس النجاح خلال 90 يوم: خفض نسبة النقر على محاكاة phishing إلى <5%، تحديث 90% من الأنظمة الحرجة خلال 30 يوم، رفع نسبة النسخ الاحتياطية المختبرة إلى 100%.

6.9 أمثلة تطبيقية سريعة (كيف نحول التقييم لإجراءات عملية)

مثال A: لو (Ransomware) score = 20 ⟶ فورًا: منع الوصول الخارجي لبورتات RDP، تعطيل ماكروز في Office، تنفيذ offline immutable backups، إعلان حملة توعية.

مثال B: لو كشفنا مفتاح على GitHub (score=12) ⟶ إلغاء المفتاح، تدوير المفاتيح، فحص استخدامه، وفرض secret scanning على repos.

6.10 قائمة تحقق تنفيذية (Actionable Quick Plan)

- عمل Inventory للأصول والبيانات خلال 14 يوم.
- تفعيل MFA على الحسابات الحرجة فورًا.
- اختبار استرجاع النسخ الاحتياطية (restore test) خلال 7 أيام.
- نشر EDR على نقاط النهاية الحساسة خلال 30 يوم.
- إجراء حملة محاكاة Phishing + تدريب خلال 45 يوم.
- تنفيذ سياسة Patch Management وتحديث الأنظمة الحرجة خلال 30 يوم.
- تفعيل DLP للبوابات البريدية والسحابة خلال 60 يوم.
- إعداد SIEM وربط التنبيهات الحرجة خلال 90 يوم.
- وضع خطة IR مفصّلة واختبارها (Tabletop exercise) خلال 90 يوم.

6.11 الخلاصة والنصيحة العملية مني

التحليل والتقييم مش هدفه يُخيف الناس، هدفه يوجّه الجهد والموارد للمكان الصح. ابدأ بالأساسيات اللي تخفض المخاطر الكبيرة بسرعة: MFA، نسخ احتياطية قابلة للاستعادة، تحديث الأنظمة، وتدريب الموظفين. بعدين بنبني دفاعات أعقد (EDR, SIEM, segmentation).

نصيحتي: لا تنتظر حادث كبير عشان تشتري أدوات — اشتغل على جرد البيانات، سياسات الوصول، واختبارات الاسترجاع أولًا. هالأشياء عادةً تعطينا أكبر فائدة مقابل أقل تكلفة.

7. الإجراءات الأمنية (Security Measures / Controls)

7.1 مقدمة

الإجراءات الأمنية هي مجموعة من الخطوات والسياسات اللي بتساعد على حماية أنظمة المؤسسة من كل التهديدات اللي درسناها قبل. الهدف مش بس منع الهجمات، بل كمان تقليل الضرر وسرعة الاستجابة إذا صار أي حادث.

تنقسم الإجراءات الأمنية عادة لثلاث فئات:

- تقنية (Technical controls)
- مادية / بيئية (Physical / Environmental controls)
- بشرية / تنظيمية (Administrative / Human controls)

7.2 الإجراءات التقنية (Technical Controls)

الإجراء	الوصف	الفائدة
تحديثات الأنظمة والبرامج	تحديث الأنظمة، التطبيقات، السيرفرات بشكل دوري	يقلل الثغرات ويمنع استغلالها
EDR / Antivirus / Anti-malware	برامج كشف ومنع الهجمات على الأجهزة	كشف الفيروسات والهجمات قبل ما تسبب ضرر
Firewall / WAF	جدار حماية للشبكة والمواقع	منع الوصول غير المصرح به وحماية الشبكة
MFA (Multi-Factor Authentication)	تحقق متعدد العوامل للوصول للحسابات	يمنع الدخول الغير مصرح به حتى لو تم سرقة كلمة السر
DLP (Data Loss Prevention)	منع تسرب البيانات الحساسة	حماية المعلومات المهمة من السرقة أو التسريب
تشفير البيانات	تشفير الملفات والبريد والاتصالات	حتى لو تسربت البيانات تبقى غير قابلة للقراءة
Backup & Disaster Recovery	نسخ احتياطية ومخطط استعادة سريع	استرجاع البيانات بعد أي حادث بدون خسائر كبيرة
Monitoring / SIEM	متابعة النشاطات وتنبيه على أي سلوك مشبوه	كشف الهجمات مبكرًا وتحليلها

7.3 الإجراءات المادية / البيئية (Physical Controls)

الإجراء	الوصف	الفائدة
حماية مراكز البيانات	أقفال، كاميرات، مراقبة الدخول	منع الوصول الفيزيائي غير المصرح به
تحديد صلاحيات الوصول للأجهزة	أجهزة الحاسوب، السيرفرات، الشبكات	حماية الأجهزة الحساسة من العبث
حماية كهربائية \ UPS	مزود طاقة مستمر وأنظمة حماية من الصدمات	منع فقدان البيانات بسبب انقطاع الكهرباء
تخزين الوسائط الحساسة	خزن الأقراص الصلبة والنسخ الاحتياطية في مكان آمن	منع السرقة أو التلف الفيزيائي للبيانات

7.4 الإجراءات البشرية / التنظيمية (Administrative / Human Controls)

الفائدة	الوصف	الإجراء
تقليل الأخطاء البشرية، زيادة الوعي	محاكاةphishing ، حملات توعية	تدريب الموظفين على الأمن السيبراني
منع الاستخدام المفرط للحقوق وتأمين المعلومات	Least Privilege، مراجعة الصلاحيات	سياسات الوصول(Access Policies)
سرعة التعامل مع الحوادث وتقليل الضرر	خطة واضحة للاستجابة عند الهجوم	إجراءات الطوارئ والاستجابة للحوادث (Incident Response)
اكتشاف نقاط الضعف قبل استغلالها	تقييم دوري للأنظمة والبيانات	مراجعة الأصول والمخاطر بشكل دوري
حماية الحسابات من الدخول الغير مصرح به	طول معقدة، تغيير دوري	سياسات كلمات المرور

7.5 نصائح عملية للمؤسسات والأفراد

1. خلي كل شيء محدث: أنظمة، برامج، نسخ احتياطية.
2. اختبر النسخ الاحتياطية دائمًا (Restore Test).
3. فعّل MFA لكل الحسابات المهمة.
4. درب الموظفين على التعرف على رسائل البريد الاحتيالية.
5. استعمل تشفير للبيانات الحساسة داخل وخارج المؤسسة.
6. حدّد صلاحيات كل مستخدم وراجعها بشكل دوري.
7. ضع خطة طوارئ واضحة للتعامل مع أي حادث.

7.6 تقييم فاعلية الإجراءات الأمنية (Effectiveness Assessment)

لتقييم فاعلية كل إجراء، نستخدم ثلاثة محاور رئيسية:

- التحقق من التطبيق (Implementation Check): هل الإجراء مطبق فعليًا؟
- النتيجة (Outcome): هل الإجراء يقلل المخاطر أو يمنع الهجوم بنجاح؟
- المتابعة المستمرة (Continuous Monitoring): هل هناك مراجعة دورية وتحسينات مستمرة؟

يمكن استخدام مقياس رقمي (1–5) لتقييم كل إجراء:

درجة الفاعلية	النتيجة	فاعلية التطبيق	التحليل	الإجراء الأمني
4/5	يقلل اختراق الحسابات	مطبق على 80% من الحسابات	تحقق متعدد العوامل يمنع الدخول الغير مصرح به	MFAعلى الحسابات الحرجة
3/5	استرجاع بيانات محدود	مطبق لكن بدون اختبار دوري	نسخ احتياطية خارجية قابلة للاسترجاع	Backup & Restore
3/5	يحد من تسرب المعلومات بنسبة متوسطة	مطبق جزئيًا	منع تسرب البيانات الحساسة	DLPعلى البريد والسحابة
2/5	ثغرات لا تزال موجودة	متقطع	Patch Management دوري	تحديث الأنظمة والبرامج
4/5	انخفضت نسبة النقر على الرسائل الخبيثة	70%من الموظفين مدربين	محاكاة + توعية	تدريب الموظفين على Phishing

رأيي: الإجراءات اللي مطبقة جزئيًا أو بدون متابعة مستمرة غالبًا تكون ضعيفة رغم أهميتها، لذلك المراجعة الدورية مهمة جدًا لضمان نجاحها.

7.7 أمثلة عملية على تطبيق الإجراءات الأمنية (Practical Examples)

الحالة	الإجراء الأمني	التطبيق العملي	النتيجة المتوقعة
موظف يحاول فتح مرفق مشبوه	تدريب الموظفين + فلترة البريد	موظف يتلقى بريد phishing (نظام البريد يمنع الرسالة + الموظف يتعلم)	منع الإصابة بالبرمجيات الخبيثة
خادم إنتاج معرض للـRansomware	Backup & Disaster Recovery + Patch Management	عمل نسخ احتياطية Immutable +تحديث الأنظمة	عند الهجوم يمكن استرجاع البيانات بسرعة
كشف مفتاح API على GitHub	Secret Scanning + Access Policy	فحص المستودعات تلقائيًا(إلغاء المفتاح وتعويضه)	منع استغلال المفاتيح والتسريب
محاولة وصول غير مصرح به للبيانات الحساسة	DLP + Logging + Least Privilege	المستخدم حاول نسخ بيانات (النظام يمنع + سجل التهديد)	حماية البيانات الحساسة ورصد المخالفات
هجوم DDoS على موقع الشركة	Firewall/WAF + Anti-DDoS	تفعيل WAF + مراقبة الحركة	تقليل توقف الموقع وتأمين الخدمة

الخلاصة العملية:

- تقييم فاعلية الإجراءات الأمنية يساعد على تحديد نقاط القوة والضعف.
- المراجعة الدورية تجعل الإجراءات أكثر صلابة وواقعية ضد الهجمات.
- الأمثلة العملية توضح كيف كل إجراء يترجم إلى حماية حقيقية.
- الجمع بين التقنية + السياسات + التدريب البشري يعطي أفضل نتيجة ويقلل المخاطر بشكل كبير.

8. الخاتمة (Conclusion)

بعد ما غطينا كل جوانب الأمن السيبراني من التهديدات الداخلية والخارجية، الهجمات السيبرانية، حساسية البيانات، الهجمات المتقدمة، التحليل والتقييم، والإجراءات الأمنية، صار عندنا صورة واضحة لكيفية حماية المؤسسة ومستخدميها.

النقاط الرئيسية:

1. **الوعي هو خط الدفاع الأول:** تدريب الموظفين والتوعية الدورية يقلل الأخطاء البشرية ويزيد الحماية.
2. **التقنية مش كافية وحدها:** البرامج والتحديثات مهمة، لكن بدون سياسات واضحة ومراقبة مستمرة، المخاطر تبقى عالية.
3. **التقييم المستمر:** تحليل التهديدات ومراجعة الإجراءات بشكل دوري ضروري لضمان فاعلية الحماية.
4. **الاستجابة السريعة:** وجود خطة واضحة للحوادث تقلل الضرر وتسرّع التعافي.
5. **التكامل بين كل عناصر الأمن:** الجمع بين التقنية + الإجراءات المادية + التدريب البشري هو اللي يعطي أفضل النتائج.

رسالة ختامية للمستخدمين:

الأمن السيبراني مش مجرد إجراءات، هو ثقافة وسلوك يومي. كل خطوة صغيرة تقوم فيها— سواء تحديث نظامك، استخدام كلمات مرور قوية، أو توخي الحذر مع البريد الإلكتروني— تساهم بحماية المؤسسة وبياناتك الشخصية.

الهدف النهائي هو خلق بيئة رقمية آمنة ومرنة، بحيث كل مستخدم يعرف دوره ويقدر يتعامل مع أي تهديد بشكل ذكي وفعّال.

9. المصطلحات (Glossary)

المصطلح	التعريف / الشرح
Threat (تهديد)	أي شيء يمكن أن يضر بالنظام أو البيانات، سواء كان هجومًا خارجيًا أو خطأ داخلي.
Vulnerability (ثغرة)	نقطة ضعف في النظام أو البرنامج يمكن استغلالها للوصول غير المصرح به.
Malware (البرمجيات الخبيثة)	برامج ضارة مثل فيروسات، رانسوموير، Trojan، تستخدم لإتلاف أو سرقة البيانات.
Phishing (التصيد الاحتيالي)	محاولات احتيالية لخداع المستخدم للكشف عن معلومات حساسة.
Ransomware (البرمجيات الخبيثة المطالبة بفدية)	برنامج يقوم بتشفير البيانات ويطلب فدية لفك التشفير.
EDR (Endpoint Detection & Response)	نظام لمراقبة الأجهزة واكتشاف ومنع الهجمات على الأجهزة الطرفية.
MFA (Multi-Factor Authentication)	تحقق متعدد الخطوات لتأكيد هوية المستخدم قبل السماح بالدخول.
DLP (Data Loss Prevention)	تقنيات وسياسات لمنع تسرب المعلومات الحساسة خارج المؤسسة.
OSINT (Open Source Intelligence)	جمع معلومات من مصادر عامة مثل الإنترنت ووسائل التواصل لأغراض أمنية.

SIEM (Security Information and Event Management)	نظام لمراقبة وتحليل الأحداث الأمنية في الشبكة لتحديد التهديدات.
Patch Management	عملية تحديث الأنظمة والتطبيقات لسد الثغرات الأمنية.
Least Privilege	مبدأ منح المستخدمين أقل صلاحيات ممكنة لأداء مهامهم فقط.
Disaster Recovery Plan (خطة التعافي من الكوارث)	خطة لاسترجاع البيانات والخدمات بعد حدوث أي حادث أو هجوم.
Firmware Compromise	تعديل غير مصرح به لبرمجيات الأجهزة (Firmware) لزرع ثغرات أو backdoors.
Social Engineering (الهندسة الاجتماعية)	استخدام الخداع النفسي للحصول على معلومات حساسة من الأشخاص.
DDoS (Distributed Denial of Service)	هجوم يهدف لإيقاف الخدمة عن المستخدمين عبر زيادة الضغط على الشبكة أو الخادم.
Macro (ماكرو)	مجموعة أوامر مسجّلة ضمن برنامج مثل Excel أو Word تُنفذ بشكل تلقائي عند تشغيلها. أحيانًا تُستغل من قبل المخترقين لإدخال برمجيات خبيثة عند فتح الملف.