

تسليم 1 لمقرر قضايا بحثية 1

إعداد: عبدالله نصر الدين
الرقم الاكاديمي: 251001251

تسليم 1



تحليل تقنيات الاختراق الحديثة للشركات الكبرى

تسليم ورقة بحثية 1

المرجع الرئيسي: "التقنيات الحديثة المعتمدة على البيانات والذكاء الاصطناعي"
الرابط: SDAIA.GOV.SA



SCAN ME

إعداد
عبدالله نصرالدين



- الأمن السيبراني يشكل تحدياً رئيسياً للشركات الكبرى بسبب تطور تقنيات الهجوم باستمرار.
- رغم التطورات الكبيرة في أنظمة الحماية، لا تزال الشركات تواجه تهديدات متزايدة من الهجمات المتقدمة.
- الهدف من هذه الدراسة هو تحليل أحدث أساليب الاختراق وكيفية تعزيز وسائل الحماية لمواجهتها بفعالية.

تسليم

01

مشكلة الدراسة

- ✓ على الرغم من التطور الكبير في تقنيات الأمن السيبراني، لا تزال الشركات والمؤسسات عرضة للهجمات الإلكترونية.
- ✓ تزايد أساليب الهجمات، مثل الهندسة الاجتماعية والاختراقات المتطورة، يجعل الأنظمة التقليدية غير كافية.
- ✓ الهجمات من نوع Zero-day تمثل تهديدًا حقيقيًا، حيث يتم استغلال ثغرات لم يتم اكتشافها بعد، مما يصعب مواجهتها بالطرق التقليدية.

السؤال البحثي الرئيسي:

ما هي نقاط الضعف في أنظمة الأمن السيبراني التي يستغلها المخترقون، وما الحلول التكنولوجية والاستراتيجية الأكثر كفاءة في التصدي لها؟

تسليم

01

أهمية الدراسة

- ✓ اقتصاديًا: الخسائر الناتجة عن الهجمات الإلكترونية تصل إلى مليارات الدولارات سنويًا، مما يؤثر على استقرار الأسواق العالمية.
- ✓ تقنيًا: تطوير استراتيجيات فعالة للأمن السيبراني يتطلب تحليل تكتيكات الهجمات الحديثة وفهم أنماطها المتغيرة.
- ✓ أمنيًا: تعزيز قدرة الشركات على التنبؤ بالهجمات السيبرانية والتصدي لها بفعالية قبل وقوعها.

أهداف الدراسة

🎯 تحليل التقنيات الحديثة المستخدمة في الهجمات السيبرانية.

🎯 دراسة الثغرات الأمنية الشائعة التي يستغلها المخترقون.

🎯 اقتراح حلول مبتكرة لتحسين الأمن السيبراني في الشركات الكبرى.

✓ الهندسة الاجتماعية: استغلال العامل البشري لخداع المستخدمين. [Al Arabiya](#)

✓ هجمات Zero-day: استغلال ثغرات لم يتم اكتشافها بعد من قبل الشركات. [Kaspersky](#)

✓ هجمات الفدية: عندما تصبح بياناتك رهينة من قبل المخترقين. [CyberSec Training & Consulting UK](#)

مفاهيم وتعريفات الدراسة

الدراسات السابقة

الدراسة	الموضوع الأساسي	النتائج
Sensors (2023)	الهجمات العكسية على الذكاء الاصطناعي	يمكن خداع أنظمة الذكاء الاصطناعي بسهولة عبر بيانات زائفة Kaspersky .
(2025) كاسبرسكي	تحليل الاختراقات في الشركات	91% من الشركات تعرضت لهجمات، أبرزها الهندسة الاجتماعية والتصيد Kaspersky .

✓ الهجمات السيبرانية تعتمد بشكل أساسي على ثغرات Zero-day والهندسة الاجتماعية.

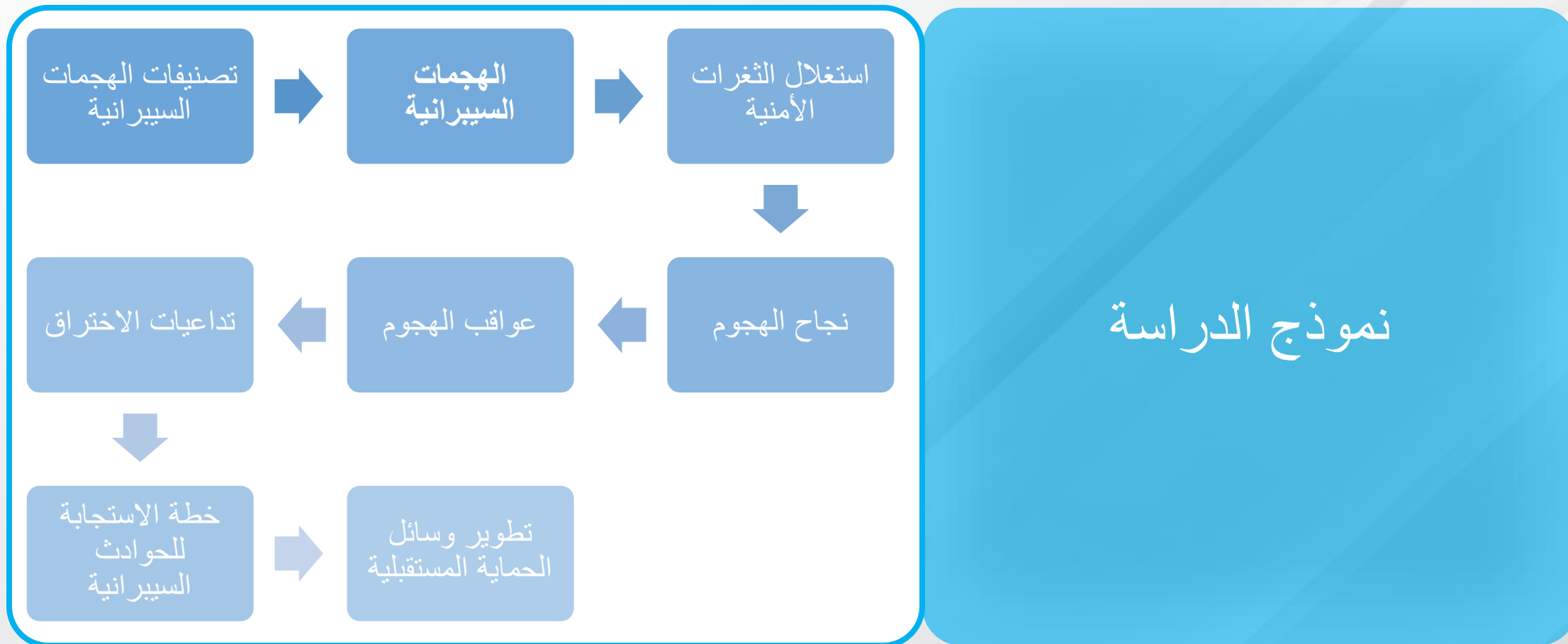
✓ معظم الشركات غير قادرة على اكتشاف الهجمات قبل حدوثها.

✓ استخدام الذكاء الاصطناعي يمكن أن يساعد في تقليل مخاطر الاختراقات.



تسليم
01

فرضيات الدراسة

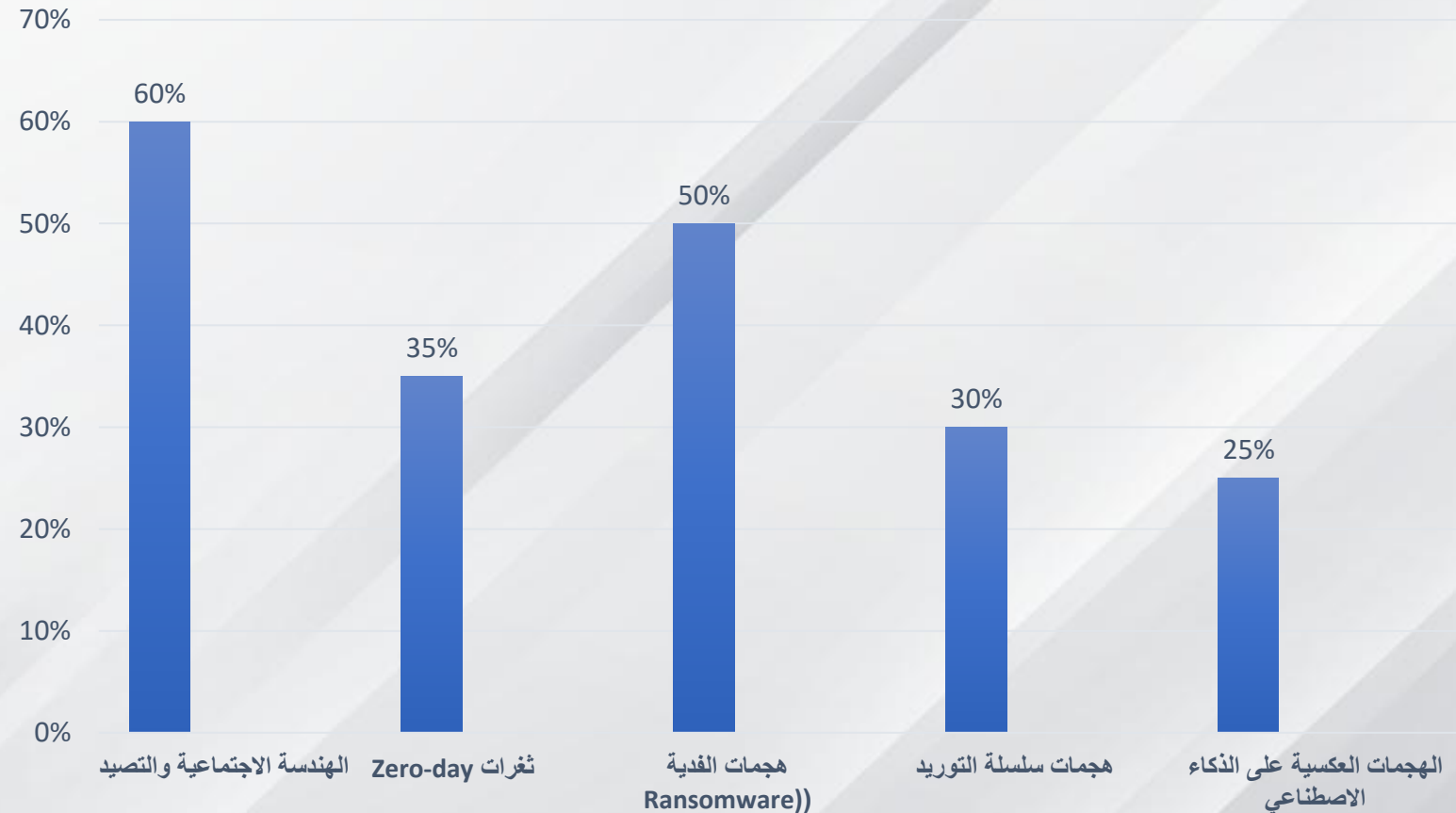


التحليل الإحصائي

تحليل أنواع الهجمات السيبرانية ونسب انتشارها

تسليم

01



- ✓ تدريب الموظفين على كشف محاولات التصيد الاحتيالي.
- ✓ تحديث الأنظمة الأمنية باستمرار لسد الثغرات المكتشفة.
- ✓ استخدام الذكاء الاصطناعي لتحليل الأنماط المشبوهة.
- ✓ تطبيق نموذج "Zero Trust Security" لمنع الوصول غير المصرح به..

الحلول والتوصيات

مناقشة النتائج والتوصيات

- ✓ لماذا تنجح هذه الهجمات؟
- ✓ كيف يمكن تحسين الحماية؟
- ✓ ما هي الخطوات المستقبلية للحد من هذه الهجمات؟

- Kaspersky. (2025). Network Security Incidents Dominate with 91% of Companies Targeted by Adversaries. Retrieved from [Kaspersky](#)
- MDPI. (2023). Adversarial Attacks on AI Security Systems. Retrieved from [MDPI](#) Sensors Journal
- FBI. (2016). Business E-mail Compromise: The 3.1 Billion Dollar Scam. Retrieved from IC3 [FBI](#)
- Kaspersky. (2023). Understanding Zero-Day Exploits. Retrieved from [Kaspersky](#) Resource Center
- CISA. (2023). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. Retrieved from [CISA](#)
- CISA. (2020). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. Retrieved from [CISA](#)

المراجع الأكاديمية



Thank You