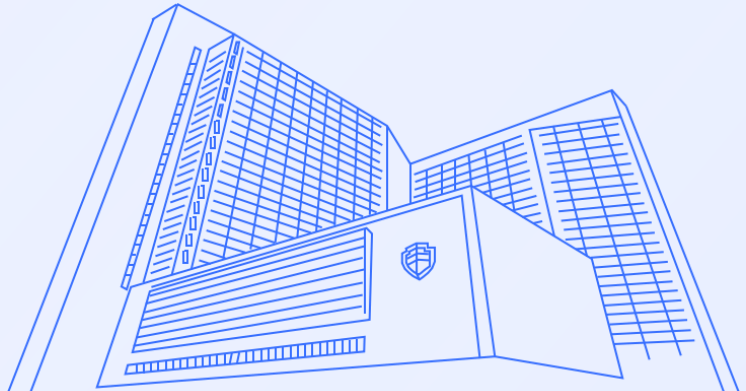
国家金融监督管理总局
National Financial Regulatory Administration

推动数字化转型　实现高质量发展

《银行业保险业数字化转型的指导意见》解读

主讲人：刘宏健



出台背景

“十四五”规划

激活数据要素潜能

加快建设数字经济

2022年制定指导意见

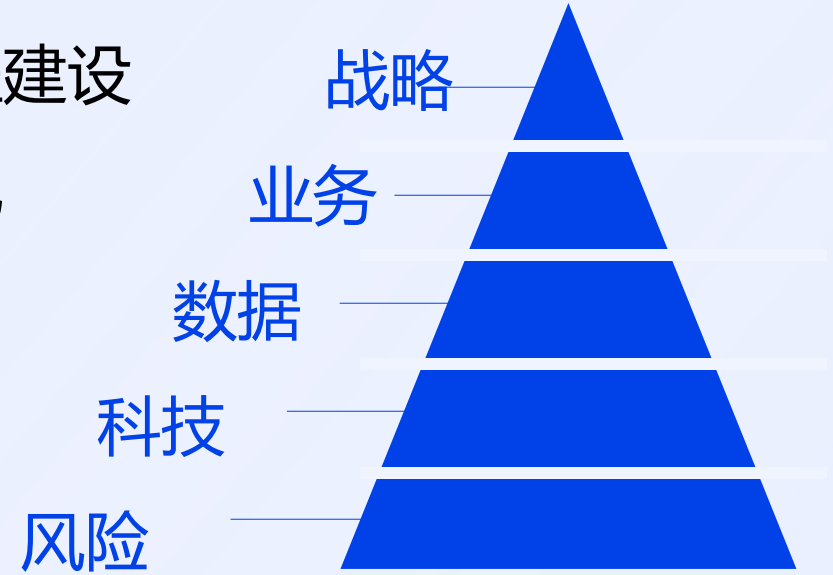
战略规划与组织流程建设

业务经营管理数字化

数据能力建设

科技能力建设

风险防范



战略规划与组织流程建设

◆ 战略规划

董事会主导

纳入整体发展战略

◆ 组织架构

高管层统筹

跨部门协同

纳入考评机制

◆ 人才队伍

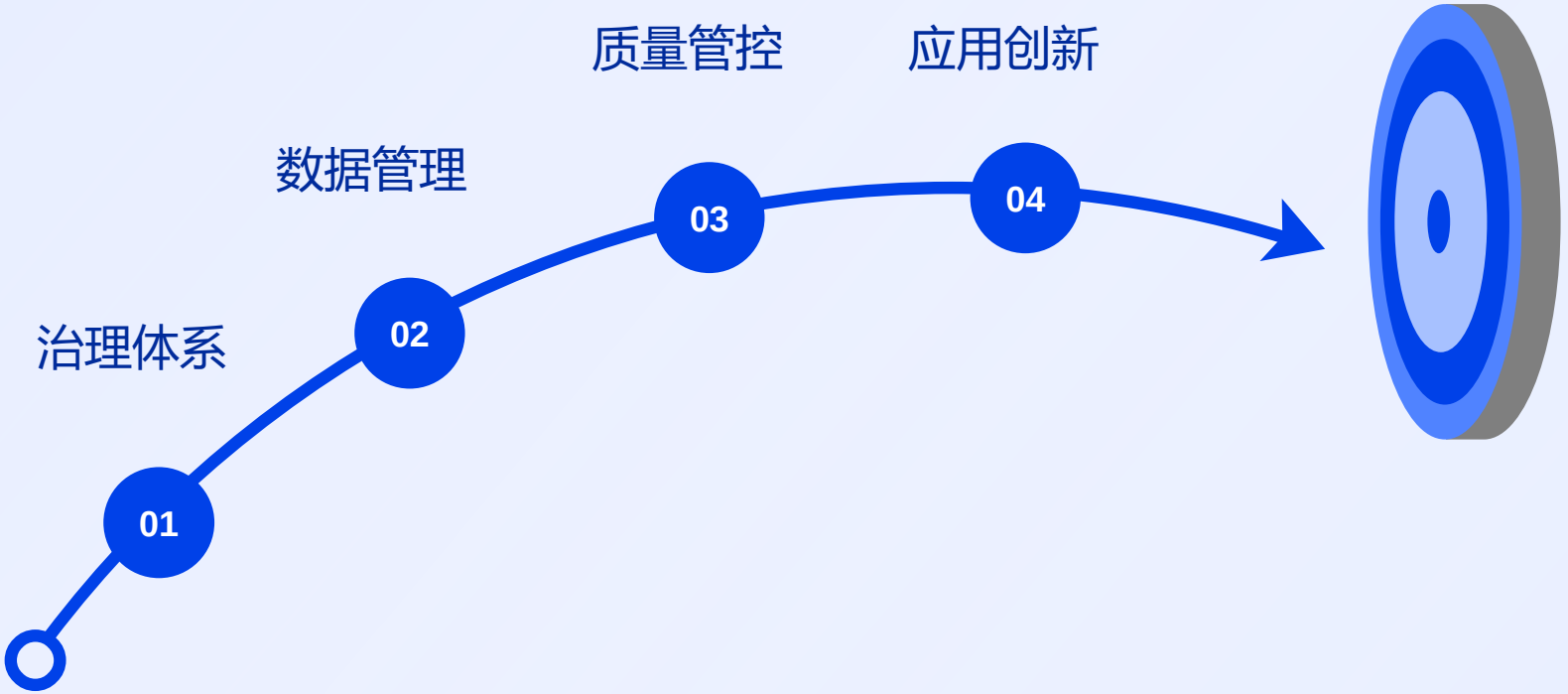
科技背景

复合型人才

业务经营管理数字化


产业
金融
战略性新兴产业
先进制造业和新型基础设施建设
个人
金融
营销服务转型
老年、残障、少数民族服务
交易
运营
市场交易、运营服务、数字化风控

数据能力建设



科技能力建设

◆ 技术可控

技术研发

核心技术自主可控

◆ 敏捷转型

前端敏态

后端稳态

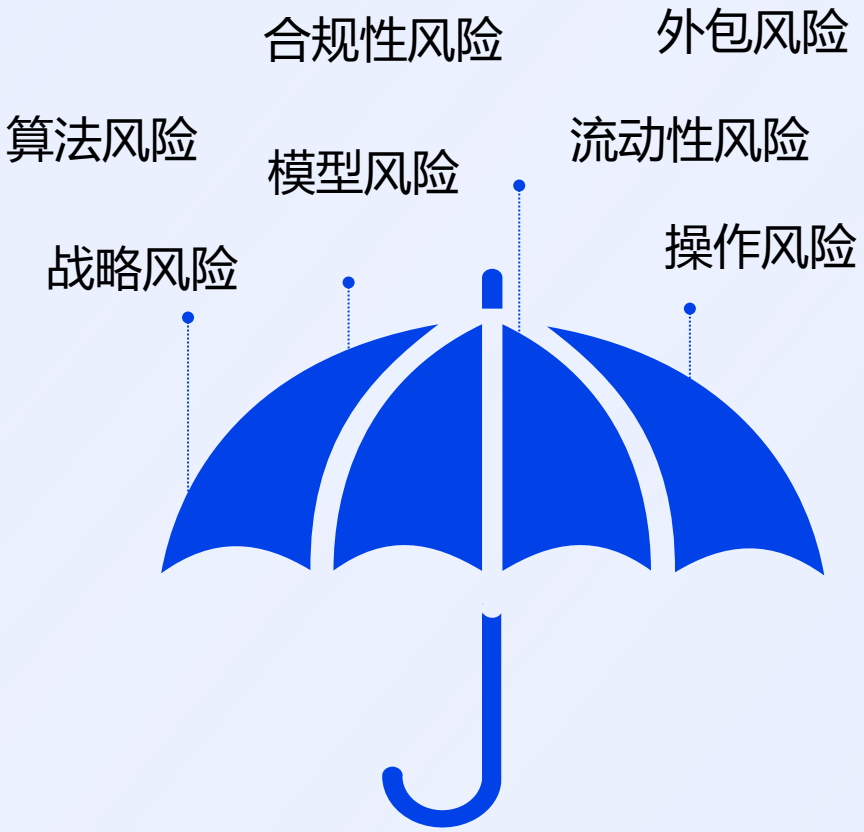
◆ 夯实科技基础

大数据中心

分布式架构

风险防范

- 业务合规
- 算法公平
- 隐私保护



行业影响

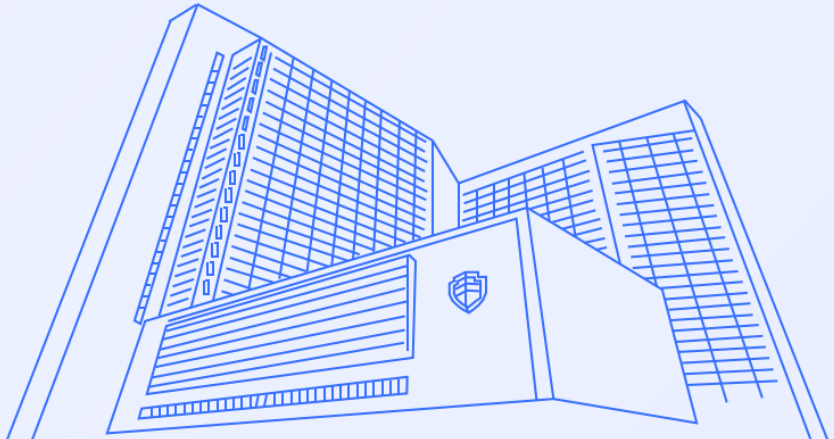
- 明确转型方向
- 推动资源投入
- 促进生态合作
- 强化风险意识
- 加速行业发展

银行业保险业数字化转型

必答题·任重道远·未来可期

国家金融监督管理总局
National Financial Regulatory Administration

谢谢
THANK YOU



ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

葡語國家 / 地區保險監管專員協會研討會

《數位營運韌性法》

Ana Moitinho Byrne

澳門

2025年5月12日

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

Ana Moitinho Byrne

葡萄牙保險監察及退休基金局

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

- 背景
- 歐洲金融業數位營運韌性
- 《數位營運韌性法》
- 主要挑戰
- 總結

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

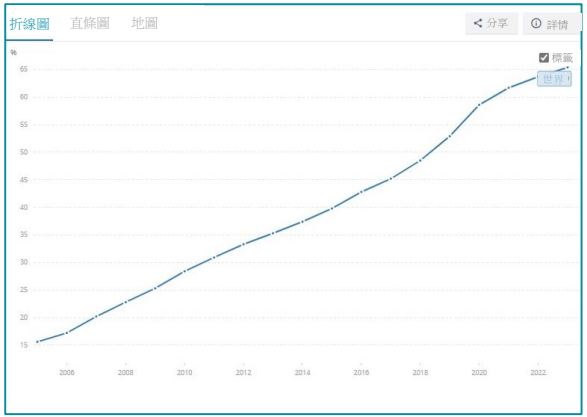
- 背景
- 歐洲金融業數位營運韌性
- 《數位營運韌性法》
- 主要挑戰
- 總結

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

背景

對資訊及通訊科技的依賴程度日益提高

互聯網用戶（佔人口比例）
（2005-2023）



來源：https://data.worldbank.org

- 約55億人能夠上網*
- 超過160億台聯網設備（包括智能手機和電腦）**
- 新業態——如電商
- 在線服務簽約
- 在線身份認證
- 電子支付

* www.statista.com ， 2025年2月
** www.iot-analytics.com，2024年

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

背景

金融業數位化進程日益加快

雲服務

人工智能

區塊鏈

分散式帳本

大數據

加密資產

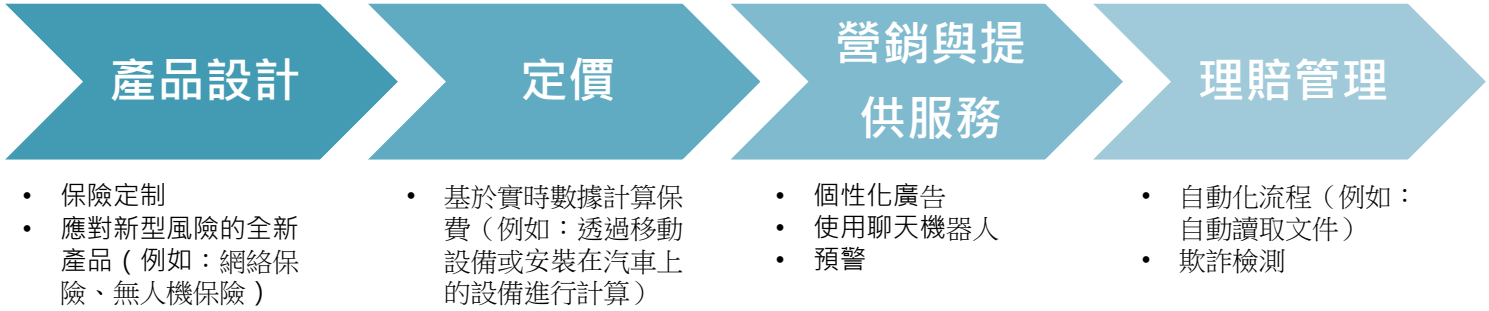
來源：http://www.atlantichub.com/

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

背景

價值鏈碎片化

- 科技公司提供的金融服務（例如：保險）
- 支撐提供金融服務的數位化技術解決方案

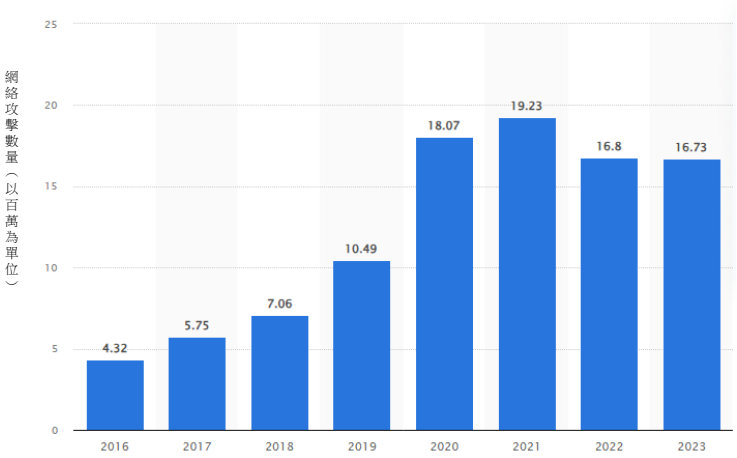


ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

背景

資訊及通訊科技相關風險顯著增加

- 2025年，每天發生2200起網絡攻擊（即每39秒一起）



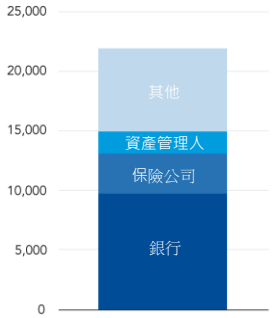
來源：www.statista.com

有吸引力的目標

在過去 20 年中，金融業遭受了超過 20,000 起網絡攻擊，造成 120 億美元的損失。

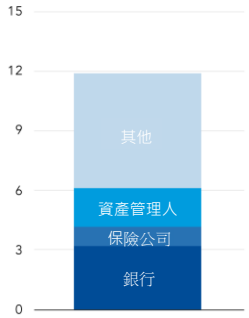
金融業網絡安全事件

（2004-2023年間的數字）



金融業損失

（以十億美元為單位，2004-2023年）



來源：Advisen網絡損失數據和國際貨幣基金組織工作人員統計。 **國際貨幣基金組織**

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

背景

出現應對相關風險的措施

表一：按管轄區劃分的公開信息摘要

管轄區	國家策略	法規/方針							監管實務							未來計劃
		金融市場基建	交易場所	銀行	保險公司	證券商	資產管理人	養老金基金	金融市場基建	交易場所	銀行	保險公司	證券商	資產管理人	養老金基金	
阿根廷		■		■							■					✓
澳洲	✓	■	■	■	■	■	■	■	■		■					✓
巴西	✓	■	■	■	■	■	■							■		✓
加拿大	✓	■	■	■	■	■	■									
中國	✓	■	■	■	■	■	■			■	■		■	■		✓
歐盟	✓	■	■	■	■	■					■					✓
法國	✓	■	■	■	■	■	■	■	■		■	■				✓
德國	✓	■	■	■	■	■	■	■								✓
香港	✓	■		■	■	■	■		■		■		■	■		✓
印度	✓	■	■	■	■						■					✓
印尼		■		■		■	■		■		■		■			
意大利	✓	■	■	■	■		■		■	■						✓
日本	✓	■	■	■	■	■	■		■	■	■	■	■			
韓國		■	■	■	■		■		■	■	■	■		■		
墨西哥		■	■	■	■	■	■	■	■	■	■	■	■	■		✓
荷蘭	✓	■		■								■	■	■	■	✓
俄羅斯	✓	■	■	■							■					✓
沙特阿拉伯		■		■	■											✓
新加坡	✓	■	■	■	■	■	■		■	■	■	■	■	■		✓
南非	✓			■												✓
西班牙	✓	■	■	■												✓
瑞士	✓	■	■	■	■	■	■									
土耳其	✓	■	■	■		■	■	■	■	■	■		■	■	■	
英國	✓	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
美國	✓	■	■	■	■	■	■	■	■	■	■	■	■	■	■	✓
總數	20	24	19	24	18	16	17	7	12	9	16	8	9	10	4	18

■ 管轄範圍

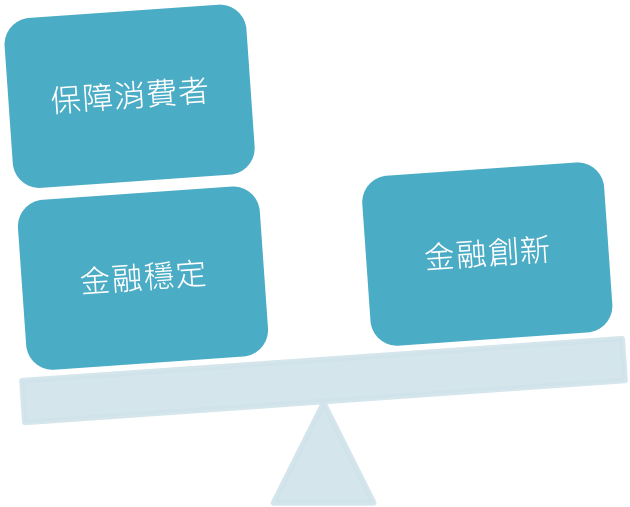
空白表示未覆蓋

來源：金融穩定委員會，《公開發布的網絡安全法規、方針及監管實務滙總》，2017

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

背景

需要平衡技術的風險與回報



ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

- 背景
- 歐洲金融業數位營運韌性
- 《數位營運韌性法》
- 主要挑戰
- 總結

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

歐洲金融業數位營運韌性

歐盟數位融資戰略（歐盟委員會，2020）

“融資的未來是數位化”

- 數位創新**趨勢**
- 數位融資作為**戰略目標**
- **優先事項**，以充分利用金融業數位化帶來的益處，同時預防相關風險
  - 消除數位金融服務單一市場的**碎片化**
  - 調整歐盟監管框架，**促進數位創新**
  - 建立歐洲金融數據空間，推動**基於數據的創新**
  - 應對數位轉型帶來的挑戰和風險，包括提升金融系統的**數位營運韌性**

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

歐洲金融業數位營運韌性

歐洲網絡安全法律法規框架

- **<u>保險業</u>方面：**
  - 《償付能力(Solvency) II——運營風險管理的一般要求》（2009）
  - 《關於外判予雲計算服務提供商的指引》（歐洲保險和職業養老金管理局，2020年2月）
  - 《關於資訊及通訊科技安全和治理的指引》（歐洲保險和職業養老金管理局，2020年10月）
- **<u>金融業</u>方面：**
  - 數位金融一攬子計劃（歐盟委員會，2020）
    - 數位融資戰略
    - 數位營運韌性一攬子計劃——《數位營運韌性法》

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

歐洲金融業數位營運韌性

歐盟第2554/2022號法規（《數位營運韌性法》）

- **統一現有規則：** 資訊及通訊科技風險管理， 資訊及通訊科技相關事件通報
- **新規則：**數位營運韌性測試， 資訊及通訊科技服務提供商的風險管理，信息共享
- **實施日期：**自2025年1月17日起

歐盟第2556/2022號指令（《數位營運韌性指令》）

- **修訂金融子部門框架指令：**確保與《數位營運韌性法》在數位營運韌性要求的應用上保持一致；為制定實施技術標準和監管技術標準提供法律依據

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

- 背景
- 歐洲金融業數位營運韌性
- 《數位營運韌性法》
- 主要挑戰
- 總結

《數位營運韌性法》

《數位營運韌性法》的目標

- 為歐盟金融業建立**統一的數位營運韌性框架**
- 確保金融機構能夠**抵禦**、**應對**資訊及通訊科技事件或重大網絡威脅並從中**恢復**過來
- 為**消費者**提供保障並確保**金融穩定**

《數位營運韌性法》

網絡安全與數位營運韌性

“數位營運韌性”是指金融機構建立、保證及重新評估其營運完整性和可靠性的能力——透過直接或間接使用資訊及通訊科技第三方服務提供商提供之服務，確保為達到以下目的所需之全方位資訊及通訊科技的能力：1) 保障金融機構所使用之網絡及信息系統的安全；2) 確保即使出現動蕩，金融服務的持續提供及其服務質素。

《數位營運韌性法》

《數位營運韌性法》的適用範圍

涵蓋20類金融機構，包括：

- 保險及再保險公司
- 職業養老金計劃機構
- 保險中介、再保險中介及附屬保險中介

根據適度原則：

- 根據金融機構的規模、整體風險狀況，以及其服務、活動及營運的性質、規模和複雜程度，開展落實及監管。

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

《數位營運韌性法》

主要支柱

金融機構

資訊及通訊科技風險管理

- 治理要求
- 與資訊及通訊科技相關風險管理的職能
  - 識別
  - 保護及預防
  - 檢測
  - 應對及恢復
  - 學習及演變
  - 溝通

與資訊及通訊科技相關的嚴重事件

- 管理
- 分類
- 溝通

數位營運韌性測試

- 資訊及通訊科技領域系統及工具測試
- 滲透測試(TLPT)

第三方資訊及通訊科技風險管理

- 信息登記
- 與資訊及通訊科技第三方服務提供商簽訂的合同協議

ICT CTPP*

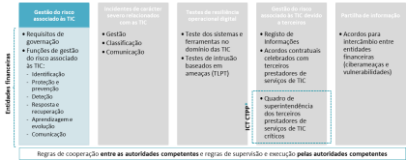
- 關鍵資訊及通訊科技第三方服務提供商監督架構

信息共享

- 金融機構間的交流協議（網絡威脅與漏洞）

權限當局之間的合作規則以及**權限當局**監督和執行規則

* ICT CTPP = 關鍵資訊及通訊科技第三方服務提供商



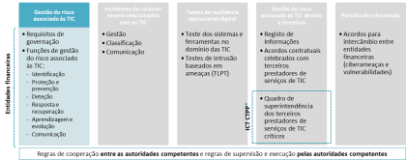
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

《數位營運韌性法》

《數位營運韌性法》是進步，而非革命

資訊及通訊科技風險管理

- 對於歐盟金融機構而言，與資訊及通訊科技風險相關的大部分要求並不陌生
  - 資訊及通訊科技策略
  - 信息安全政策與措施
  - 物理安全與邏輯安全
  - 簽訂資訊及通訊科技相關服務合同前的措施（例如：雲計算）



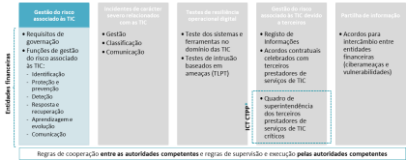
《數位營運韌性法》

網絡安全人人有責

資訊及通訊科技風險管理

- 資訊及通訊科技風險管理包括：
  - 明確劃分資訊及通訊科技領域內的職能及職責
  - 任命負責人，例如負責監控與資訊及通訊科技第三方服務提供商簽訂的協議
- 但……
  - 行政管理機關成員對資訊及通訊科技風險承擔最終責任

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES



《數位營運韌性法》

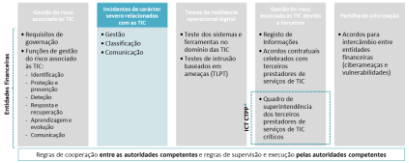
人類：從最脆弱的一環到最強大的防禦

資訊及通訊科技風險管理

- 2024年，71%的網絡攻擊源自員工帳戶（例如：通過網絡釣魚竊取憑證）*
- 《數位營運韌性法》包括：
  - 資訊及通訊科技安全意識計劃
  - 數位營運韌性培訓
  - 所有員工須具備資訊及通訊科技相關能力

*來源：IBM X-Force，2024

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES



《數位營運韌性法》

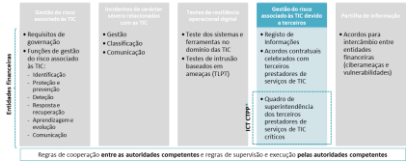
“有兩類公司：一類是已經遭受網絡攻擊的公司，另一類是遭受了網絡攻擊而不知的公司”

——引自思科系統公司前首席執行官John Chambers

與資訊及通訊科技相關的嚴重事件

- 金融機構必須記錄與資訊及通訊科技相關的所有事件，並將嚴重事件以及嚴重網絡威脅通報給監管機構：
  - **初步通報**：應在認定為嚴重事件起計的4小時內盡早通報，但最遲不得超過自知悉相關事件起的24小時
  - **中期報告**：在初步通報後的72小時內提交
  - **最終報告**：在提交最後一份中期報告後的一個月內提交

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES



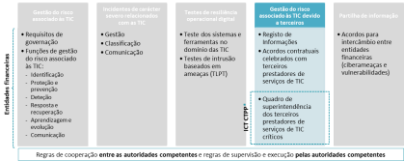
《數位營運韌性法》

網絡安全生態系統

第三方資訊及通訊科技風險管理

- 管理與**資訊及通訊科技第三方服務提供商相關的風險**是《數位營運韌性法》的主要支柱之一
  - 金融業以及其他行業實體之間的高度**互聯互通**，可能會對金融穩定構成風險
- 在《數位營運韌性法》的框架範圍內，歐盟識別並指定出對歐洲金融業而言最為**關鍵**的資訊及通訊科技第三方服務提供商
  - 相關實體（不受金融系統監管的實體）受歐洲監管當局協調之**監督架構**的約束

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES



《數位營運韌性法》

監督架構

聯合委員會
- **由歐洲監管機構（成員）、歐盟委員會及歐洲系統性風險委員會（觀察員）構成**
- **每年更新第三方服務提供商名單**
- 每年向歐洲議會、歐盟理事會和歐盟委員會報告監督架構的工作進展

監督論壇
- 構成：歐洲監管機構主席、一名權限當局（國家主管機關）的高層代表和一名觀察員、歐洲監管機構執行董事、其他相關當局、歐盟網絡與資訊安全局、歐洲中央銀行、歐洲系統性風險委員會、歐盟網絡安全局及歐盟委員會
- 聯合委員會下屬小組委員會
- 準備聯合委員會的立場提案
- 定期討論與資訊及通訊科技相關的風險和漏洞，採取共同措施監測風險
- 討論由首席監督員給予第三方服務提供商的建議

監督委員會
- 批准指定之第三方服務提供商、首席監督員的任命及監督活動報告（三個監督委員會）
- 批准首席監督員就監管第三方服務提供商作出之行為與決定（首席監督員監督委員會）

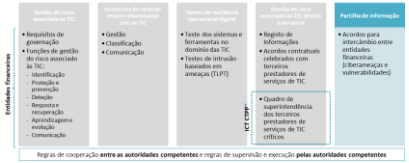
主要監管機構（首席監督員）
- 一個歐洲監管機構（歐洲銀行業管理局、歐洲證券及市場管理局、歐洲保險和職業養老金管理局），取決於第三方服務提供商在不同行業的活動
- 落實對第三方服務提供商的監管

聯合監管網絡
- 由首席監督員組成，可諮詢歐洲中央銀行及歐盟網絡安全局
- 協調首席監督員的活動（監管協議）

聯合審查小組
- 由歐洲監管機構人員、權限當局及歐盟網絡與資訊安全局（自願參加）組成
- 在第三方服務提供商的一般調查和現場檢查中為首席監督員提供支援

來源：歐洲監管機構

歐洲監管機構法規的治理架構　《數位營運韌性法》引入的治理架構　《數位營運韌性法》引入的職能



《數位營運韌性法》

“了解你的對手”

信息共享

- **金融機構**之間
  - 網絡攻擊
  - 策略、技巧和程序
- 涉及**公共實體**
  - 創建信息共享平台
- 向**權限當局**通報加入信息共享協議的情況

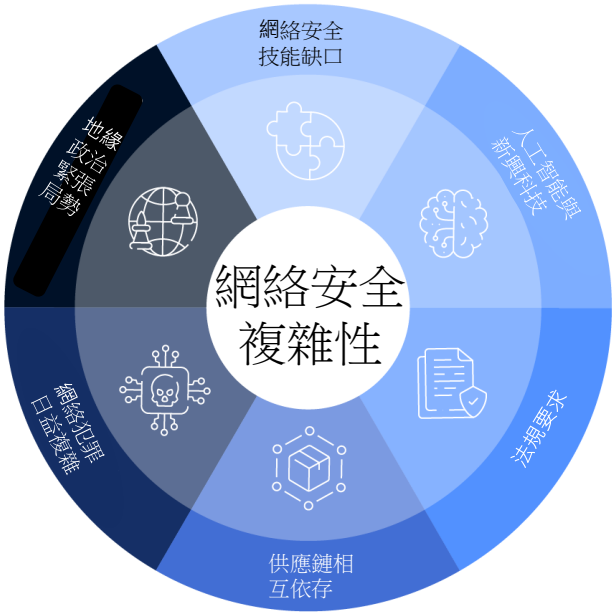
ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

- 背景
- 歐洲金融業數位營運韌性
- 《數位營運韌性法》
- 主要挑戰
- 總結

主要挑戰

全球層面

- 網絡攻擊數量**不斷增長**
- 網絡攻擊**日益複雜**
- 各行各業之間高度**相互依存**及**互聯互通**
- 缺乏網絡安全**專家**



來源：世界經濟論壇《2025年全球網絡安全展望》

主要挑戰

對於《數位營運韌性法》涵蓋的金融機構而言：

- 技術要求高度詳細
- 開發/調整信息系統，以滿足新要求
- 專業人力資源不足

對於監管機構而言：

- 監管金融領域外的風險
- 開發/調整信息系統，以滿足新要求

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

- 背景
- 歐洲金融業數位營運韌性
- 《數位營運韌性法》
- 主要挑戰
- 總結

AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

總結

“知彼知己，百戰不殆。”

——孫武《孫子兵法》

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

謝謝！

生成式人工智慧在金融行業的機遇與應用

2025.05.09

Garry Sien

Chief Solutions Architect, Global Financial Services Solutions
Alibaba Cloud Intelligence International

What an incredible year!

1. AI beats humans on some tasks, but not on all.

AI has surpassed human performance on several benchmarks, including some in image classification, visual reasoning, and English understanding. Yet it trails behind on more complex tasks like competition-level mathematics, visual commonsense reasoning and planning.

2. Industry continues to dominate frontier AI research.

In 2023, industry produced 51 notable machine learning models, while academia contributed only 15. There were also 21 notable models resulting from industry-academia collaborations in 2023, a new high.

3. Frontier models get way more expensive.

According to AI Index estimates, the training costs of state-of-the-art AI models have reached unprecedented levels. For example, OpenAI's GPT-4 used an estimated $78 million worth of compute to train, while Google's Gemini Ultra cost $191 million for compute.

4. The United States leads China, the EU, and the U.K. as the leading source of top AI models.

In 2023, 61 notable AI models originated from U.S.-based institutions, far outpacing the European Union's 21 and China's 15.

5. Robust and standardized evaluations for LLM responsibility are seriously lacking.

New research from the AI Index reveals a significant lack of standardization in responsible AI reporting. Leading developers, including OpenAI, Google, and Anthropic, primarily test their models against different responsible AI benchmarks. This practice complicates efforts to systematically compare the risks and limitations of top AI models.

6. Generative AI investment skyrockets.

Despite a decline in overall AI private investment last year, funding for generative AI surged, nearly octupling from 2022 to reach $25.2 billion. Major players in the generative AI space, including OpenAI, Anthropic, Hugging Face, and Inflection, reported substantial fundraising rounds.

7. The data is in: AI makes workers more productive and leads to higher quality work.

In 2023, several studies assessed AI's impact on labor, suggesting that AI enables workers to complete tasks more quickly and to improve the quality of their output. These studies also demonstrated AI's potential to bridge the skill gap between low- and high-skilled workers. Still other studies caution that using AI without proper oversight can lead to diminished performance.

8. Scientific progress accelerates even further, thanks to AI.

In 2022, AI began to advance scientific discovery. 2023, however, saw the launch of even more significant science-related AI applications—from AlphaDev, which makes algorithmic sorting more efficient, to GNoME, which facilitates the process of materials discovery.

9. The number of AI regulations in the United States sharply increases.

The number of AI-related regulations in the U.S. has risen significantly in the past year and over the last five years. In 2023, there were 25 AI-related regulations, up from just one in 2016. Last year alone, the total number of AI-related regulations grew by 56.3%.

Source: Artificial Intelligence Index Report 2024

Is AI Still Artificial?

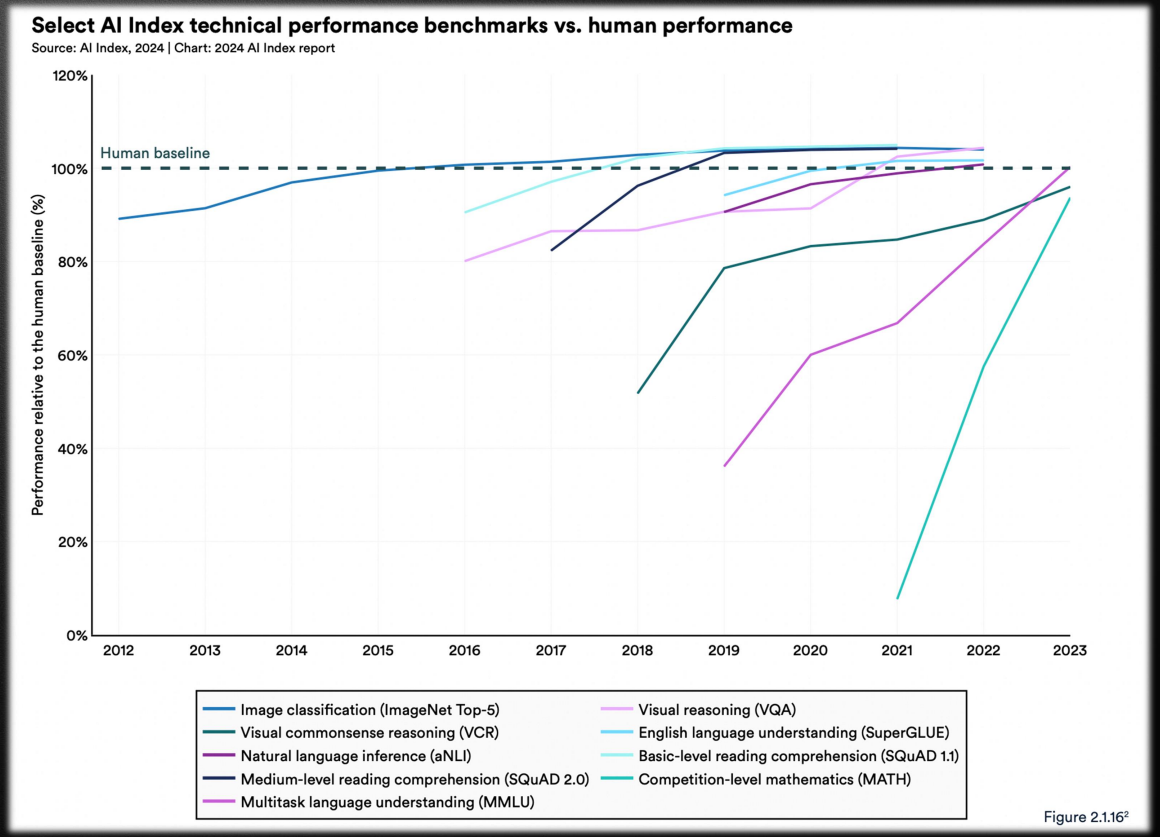


Figure 2.1.16[2]

Over the years, AI has surpassed human baselines on a handful of benchmarks, such as **image classification** in 2015, **basic reading comprehension** in 2017, **visual reasoning** in 2020, and **natural language inference** in 2021. As of 2023, there are still some task categories where AI fails to exceed human ability.

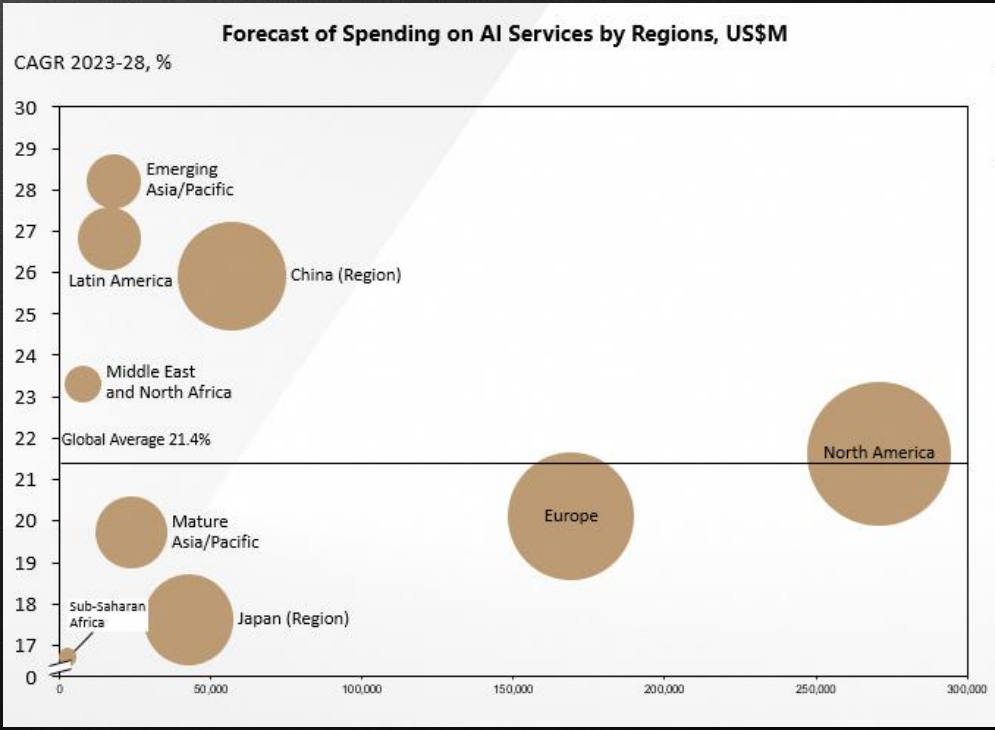
Source: Artificial Intelligence Index Report 2024

Is AI Still Artificial?

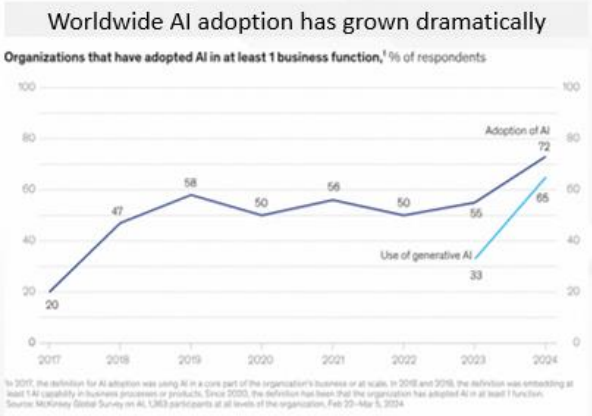
Artificial Intelligence Index Report 2024

The Adoption of AI services Worldwide

The world is investing big on AI



- **North America** is no doubt the largest market with the largest projected spending (US$270B) on AI services by 2028, but the market is growing moderately.
- **Greater China,** including Mainland China, Hong Kong Macau and Taiwan, is among **leaders in the spending growths.**

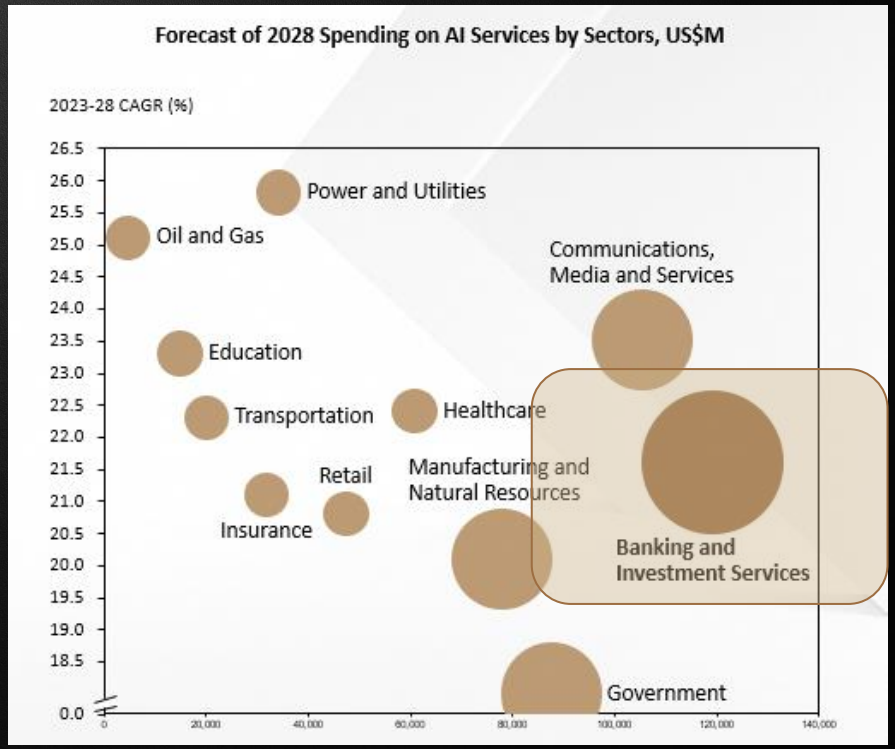


Source: Gartner

Disclaimer: Charts created by Alibaba based on Gartner research. Source: Gartner, Inc., Forecast Analysis: Artificial Intelligence Services, Worldwide, 27 August 2024.

The Adoption of AI services Worldwide

The world is investing big on AI



Source: Gartner

Disclaimer: Charts created by Alibaba based on Gartner research. Source: Gartner, Inc., Forecast Analysis: Artificial Intelligence Services, Worldwide, 27 August 2024.

Alibaba Cloud

AI Is Never New to Us

Alibaba Cloud

3 billion

Snap-n-Buy based on Image Search

Image Search

Over tens of millions of unique visitors, performing real-time searches on more than **3 billion product images**

10 M/day

Orders Delivered by AGV

Smart Logistics

Covering **147 cities,** delivering over **tens of millions** of shipping orders every day.

98 %

Alibaba Intelligent Customer Service

Intelligent Customer Services

Intelligent customer service handles **98%** of the services on Taobao, equivalent to 700,000 human customer service representatives.

160 B/day

Alibaba Vision AI Requests

Visual Identification

Alibaba's visual intelligence system is accessed over **160 billion times** per day

40 M

Households Connected to Tmall Genie

Smart Home

Tmall Genie is connected to **40 million households** and links to **460 million terminals**, with over **8 billion interactions** monthly.

1.3 B/day

Alibaba Translation Requests

Real-time Translation

With a daily usage of over **1.3 billion times**, it is the world's first live real-time translation broadcast, supporting 214 languages

Alibaba Cloud

Alibaba Cloud is investing, with unprecedented intensity, in the research and development of AI technology and the building of its global infrastructure

Alibaba Group CEO Eddie Wu
At 2024 Apsara Conference in Hangzhou

Alibaba Group announced plans to invest at least RMB 380 billion (US $53 billion) over the next three years to advance its cloud computing and AI infrastructure, reinforcing its commitment to long-term technological innovation. The investment, which exceeds Alibaba's total AI and cloud spending over the past decade, underscores the company's focus on AI-driven growth and its role as a leading global cloud provider.

Transforming Alibaba Businesses

Tongyi LLM Foundation Model

×

TMALL · Alibaba Cloud · DingTalk · Taobao · Alibaba.com · AliExpress · Lazada · trendyol · CAINIAO · Damai · LingYang · 1688 · TMALL GLOBAL · TMALL GENIE · Fliggy · Quark · YOUKU

"The most significant opportunity for AI lies beyond smartphone screens; AI will take over the digital realm and transform the physical world."

Source: : Alibaba Group CEO Eddie Wu Speaks At The 2024 Apsara Conference In Hangzhou

Alibaba Cloud's Journey on Developing Gen AI Foundation Models

Providing a broad range of models with different sizes, flexible choice between performance and cost

Qwen2.5-0.5B · Qwen2.5-1.5B · Qwen2.5-3B · Qwen2.5-7B · Qwen2.5-14B · Qwen2.5-32B · Qwen2.5-72B

TOP 1
Download in 2024 open-source model

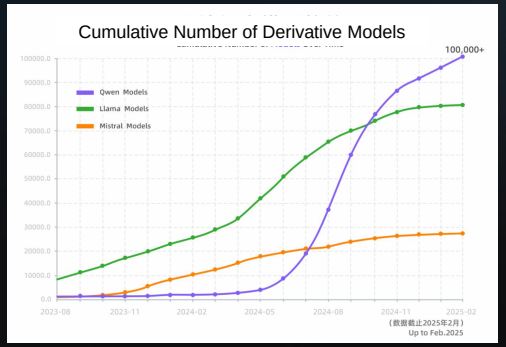
200 million
Cumulative # of Model Downloads

100K
Cumulative # of Derivative Models

All top 10 LLMs on Hugging Face Open LLM Leaderboard are based on Qwen architecture (also 19 out of top 20)

Rank	Type	Model	Average	IFEval	BBH	MATH	GPQA	MUSR	MMLU-P...	Architect...	CO_2 Cost
1	🔶	MaziyarPanahi/calme-3.2-instruct-78b	52.08 %	80.63 %	62.61 %	40.33 %	20.36 %	38.53 %	70.03 %	Qwen2ForCau...	66.01 kg
2	💬	MaziyarPanahi/calme-3.1-instruct-78b	51.29 %	81.36 %	62.41 %	39.27 %	19.46 %	36.50 %	68.72 %	Qwen2ForCau...	64.44 kg
3	💬	dfurman/CalmeRys-78B-Orpo-v0.1	51.23 %	81.63 %	61.92 %	40.63 %	20.02 %	36.37 %	66.80 %	Qwen2ForCau...	25.99 kg
4	💬	MaziyarPanahi/calme-2.4-rys-78b	50.77 %	80.11 %	62.16 %	40.71 %	20.36 %	34.57 %	66.69 %	Qwen2ForCau...	25.95 kg
5	🔶	huihui-ai/Qwen2.5-72B-Instruct-abliterated	48.11 %	85.93 %	60.49 %	60.12 %	19.35 %	12.34 %	50.41 %	Qwen2ForCau...	76.77 kg
6	💬	Qwen/Qwen2.5-72B-Instruct	47.98 %	86.38 %	61.87 %	59.82 %	16.67 %	11.74 %	51.40 %	Qwen2ForCau...	47.65 kg
7	💬	MaziyarPanahi/calme-2.1-qwen2.5-72b	47.86 %	86.62 %	61.66 %	59.14 %	15.10 %	13.30 %	51.32 %	Qwen2ForCau...	29.50 kg
8	🔶	newsbang/Homer-v1.0-Qwen2.5-72B	47.46 %	76.28 %	62.27 %	49.02 %	22.15 %	17.90 %	57.17 %	Qwen2ForCau...	29.55 kg
9	💬	ehristoforu/qwen2.5-test-32b-it	47.37 %	78.89 %	58.28 %	59.74 %	15.21 %	19.13 %	52.95 %	Qwen2ForCau...	29.54 kg
10	🔶	Saxo/Linkbricks-Horizon-AI-Avengers-V1-32B	47.34 %	79.72 %	57.63 %	60.27 %	14.99 %	18.16 %	53.25 %	Qwen2ForCau...	7.95 kg

Qwen open-source LLMs are widely used by top researchers & industrial leaders



Alibaba Cloud

Core Business of FSI

- Risk Management -


Alibaba Cloud
AI Democratization Accelerates AI-Driven Innovation and Application in “Real Business Scenarios”

SEA has potential to have the largest market share migration, as customers move toward digital – Is Fintech and AI the Answer?

Alibaba Cloud

75%

of bill payments will be done through mobile channels, up from 18% in 2019

70%

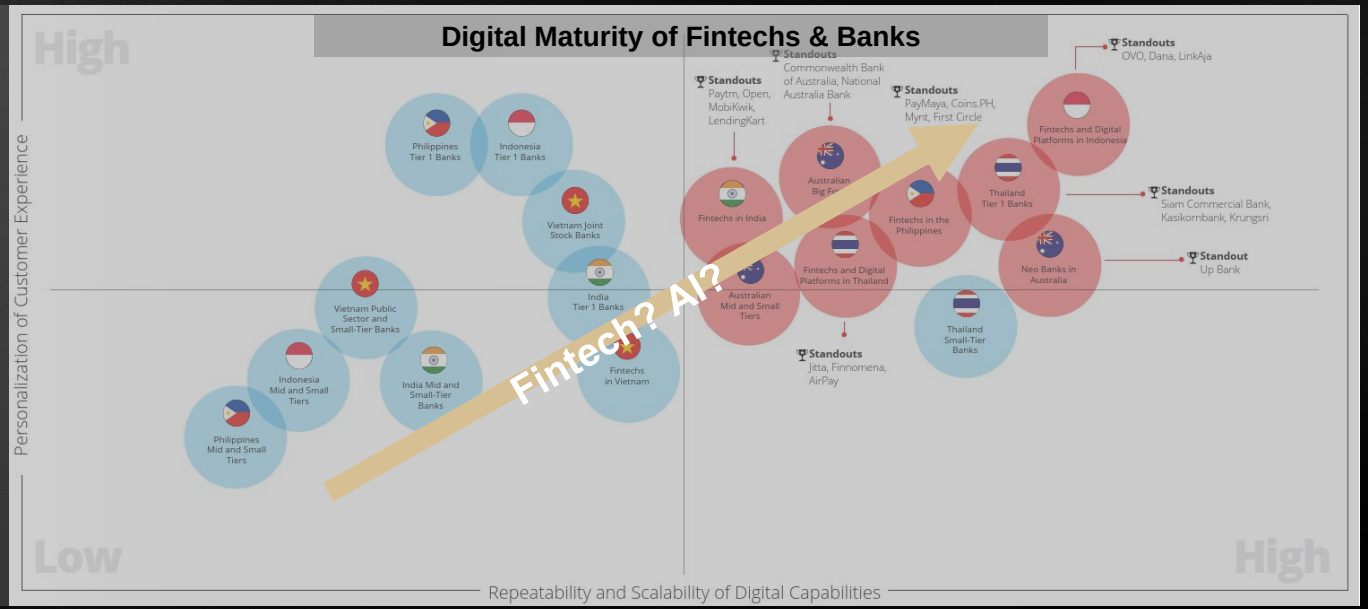
of customers who are active on digital apps believe they do not have options for “value add” banking products

60%

of bankable customers are willing to shift to other players that are more digital

Trends to watch for in H2’24:

Increasing investor attention on less traditional fintech markets,… such as **SEA**.
(IDC)



Source: Source: IDC - Fintech and Digital Banking 2025 Asia Pacific

Let's talk about *AI in FSI*

The adoption of AI and GenAI will accelerate, with primary near-term use cases related to ***Productivity, Sales and Marketing and Risk Management/ Fraud Prevention***

"For fintechs in particular, given that their "digital first" cost structures are heavily weighted toward areas where GenAI is delivering huge gains —coding, customer support, and digital marketing—the impact is likely to be even more pronounced in the near term."

-- BCG

"AI continued to grow on the radar of both fintech investors and fintechs, following a trend seen broadly both across APAC and globally. During H1'24, the AI focus came predominantly from traditional financial institutions looking to leverage AI to drive operational improvements and efficiencies. Fintechs in the region have also enhanced the emphasis of any AI components of their solutions and Offerings…"

-- KPMG

"Generative AI's impact on the banking industry will be significant, delivering benefits beyond existing applications of AI in areas such as marketing. As our colleagues have written, this technology could generate an additional $200 billion to $340 billion annually in value, arising from around 2.8 to 4.7 percent increase in the productivity of banking's annual revenues—if the use cases are fully implemented. For fintech, we expect a commensurate impact, if not more, given the already high exposure to tech."

-- McKinsey

"Ongoing GenAI media coverage and available products (e.g., ChatGPT, Bard and Gemini) continue to accelerate finance executives' commitment to exploring this technology within finance. As a percentage of budget, finance plans to spend significantly more on GenAI than all other functions except HR and customer service in 2024, according to the Gartner Generative AI 2024 Planning Survey"

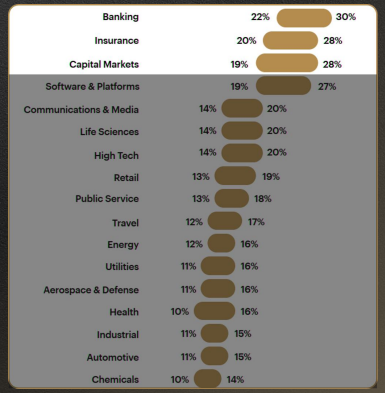
-- Gartner

What Does It Mean To Financial Services

AI may not change What FSI Does, but transforming How FSI Does Business

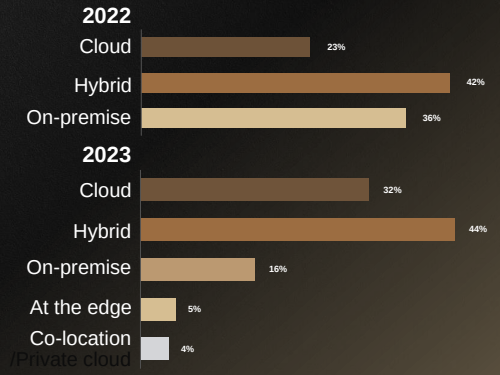
Value to FSI

FSI can improve their productivity by up to 30% by adopting generative AI



Going Cloud for AI

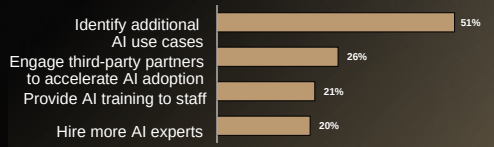
Deployment type of AI Projects/Workloads
(% of FSI survey respondents)



FSI Investing

Deployment type of AI Projects/Workloads
(% of FSI survey respondents)

Areas to invest in AI in the future
(% of FSI respondents)



Source: Banking Top 10 Trends for 2024 (Accenture), State of AI in Financial Services (Nvidia 2022,2023, 2024)

Alibaba Cloud

Make AI Work For FSI

Alibaba Cloud

Make AI Work For You

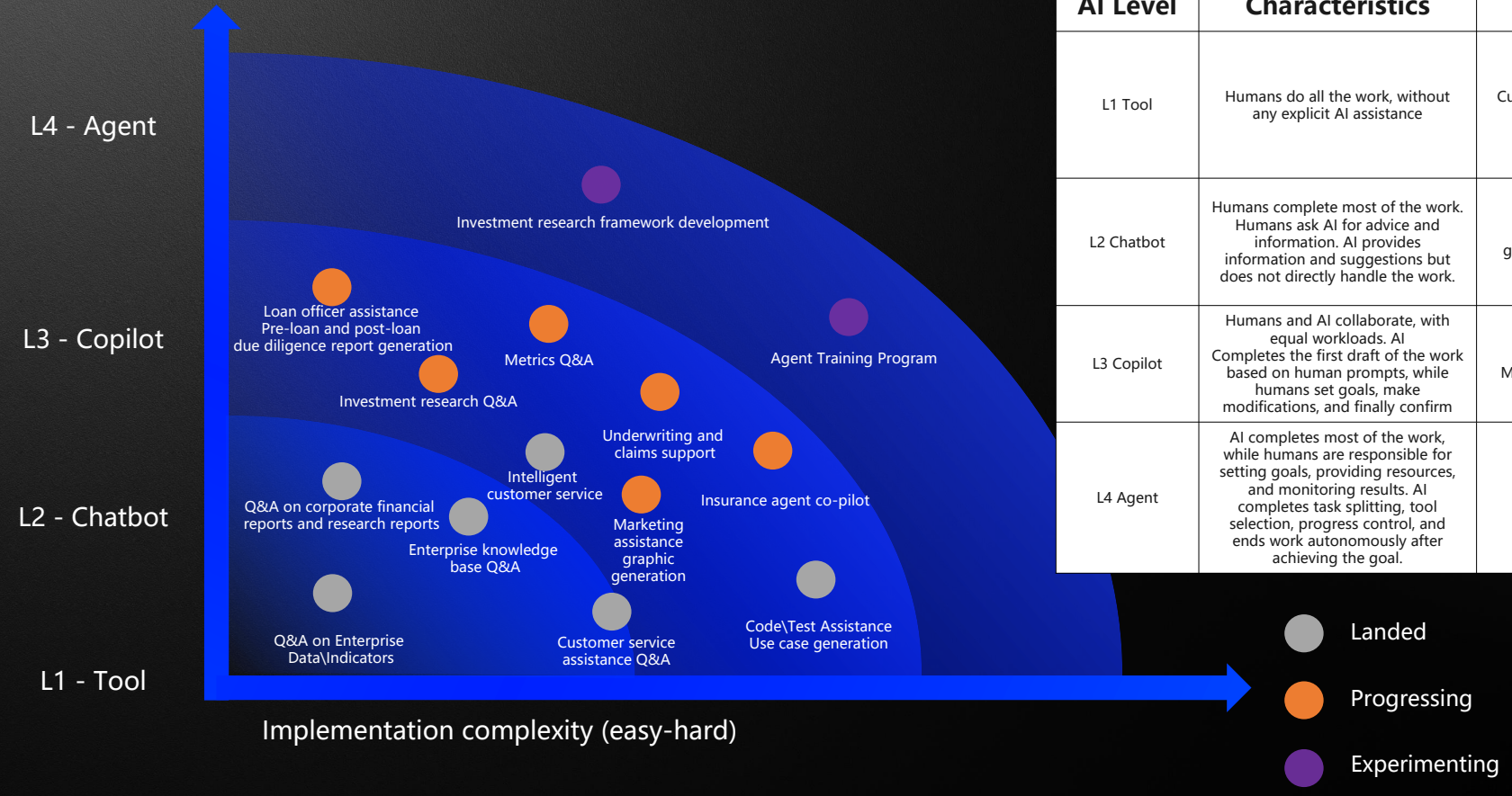
Artificial + Intelligence

Made Or Produced By Human Beings Rather Than Occurring Naturally, Especially As A Copy Of Something Natural.

The Ability To Acquire And Apply Knowledge And Skills.

AI accelerates new knowledge acquisition by helping us to overcome the “cold start”

Where Are We Today? It Varies!



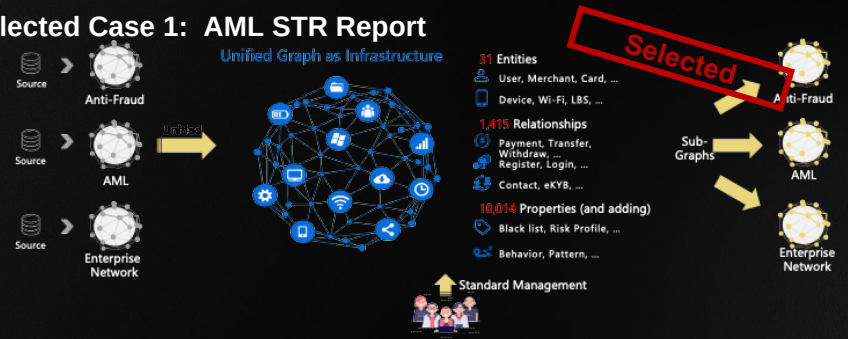
AI Level	Characteristics	Example
L1 Tool	Humans do all the work, without any explicit AI assistance	Currently, most software products
L2 Chatbot	Humans complete most of the work. Humans ask AI for advice and information. AI provides information and suggestions but does not directly handle the work.	Chatbots like first generation of ChatGPT
L3 Copilot	Humans and AI collaborate, with equal workloads. AI Completes the first draft of the work based on human prompts, while humans set goals, make modifications, and finally confirm	GitHub Copilot, Midjourney, Jasper, etc.
L4 Agent	AI completes most of the work, while humans are responsible for setting goals, providing resources, and monitoring results. AI completes task splitting, tool selection, progress control, and ends work autonomously after achieving the goal.	AutoGPT, etc.

HKMA Generative AI Sandbox – Accelerate AI Adoption for Banking Industry

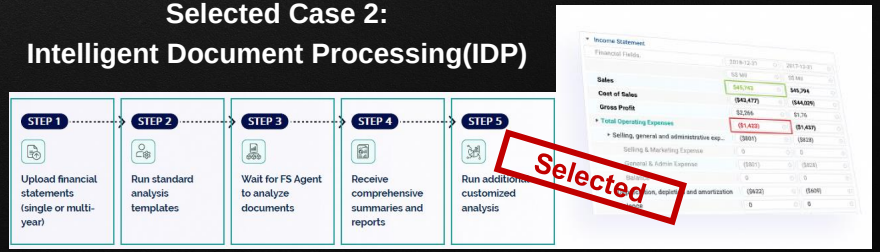
Alibaba Cloud is selected to be one of the four HKMA GenAI Sandbox Technology Partners

Theme	Example Use Cases
Risk Management	• AI-assisted financing approval • AI-powered AML Suspicious Transaction Reporting (STR) • Enhanced Know Your Customer (KYC) with unstructured data
Anti-Fraud Measures	• Intelligent assistant for fraud investigator • Protection against fraudulent account openings
Customer Experience	• AI advisor for financial knowledge and updates • Banking chatbot with AI-enhanced interactivity

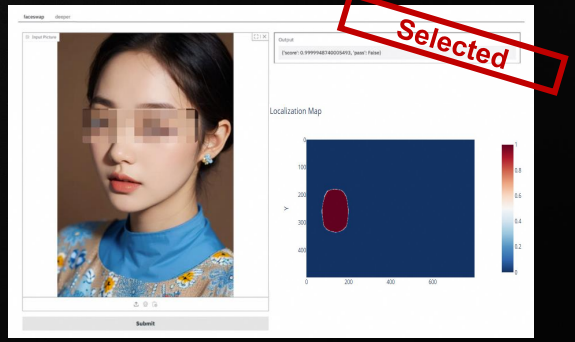
Selected Case 1: AML STR Report



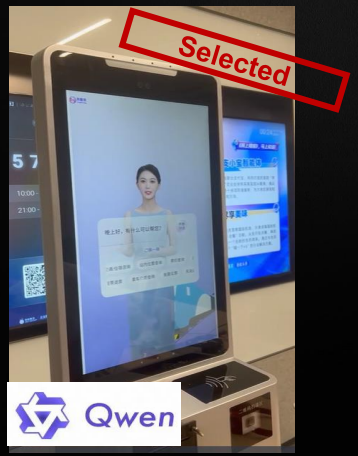
Selected Case 2: Intelligent Document Processing(IDP)



Selected Case 3: Anti-Deepfake

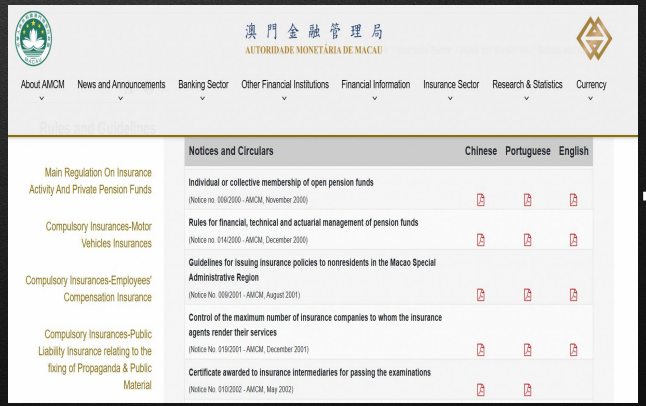


Selected Case 4: Digital Avatar + LLM



Simplify Understand of Regulatory and Compliance Requirements with LLM

Regulatory Requirements



LLM + =

In a few seconds, key regulatory requirements can be summarised!

Insurance：Bank B being registered with the Insurance Authority as a licensed insurance agency

- Insurance Authority audit rights **(summarised by IA regulations)**: the Insurance Authority (IA) of Hong Kong can **audit insurance agents for outsourcing management**. The IA has the power to regulate and supervise the insurance industry in Hong Kong, including insurance agents, and to **conduct audits of insurance agents** to ensure that they comply with relevant regulations and guidelines. Outsourcing is a common practice in the insurance industry, and insurance agents in Hong Kong are required to comply with certain rules and guidelines when outsourcing business activities to service providers. For example, the IA's Code of Conduct for Licensed Insurance Agents requires insurance agents to ensure that their outsourcing arrangements do not compromise their ability to comply with regulatory requirements or to protect the interests of their clients. Insurance agents are also required to maintain appropriate records and documentation related to outsourcing arrangements. **During an audit, the IA may review an insurance agent's outsourcing policies and procedures, as well as its documentation and records related to outsourcing arrangements**. The IA may also review an insurance agent's due diligence on service providers, performance monitoring, and risk management processes related to outsourcing. If the IA identifies any non-compliance issues during an audit, it may take enforcement action against the insurance agent. Enforcement action may include fines, suspension or revocation of licenses, or other penalties, depending on the severity of the non-compliance. Overall, insurance agents in Hong Kong are expected to comply with relevant regulations and guidelines related to outsourcing management, **and the IA may conduct audits to ensure compliance and to protect the interests of policyholders**.

Simplify Understand of Regulatory and Compliance Requirements with LLM

"General Disclosure of Aspect B4 of Appendix C2 of the ESG Code: Information on
(b) compliance with relevant laws and regulations that have a significant impact on the issuer relating to preventing child and forced labour."

Preventing child and forced labour

Alibaba 2024 ESG report
Expected result: complied
Real result: complied

Lenovo 2022 Social value report
Expected result: complied
Real result: complied

Accelerate Regulatory Reporting Generation

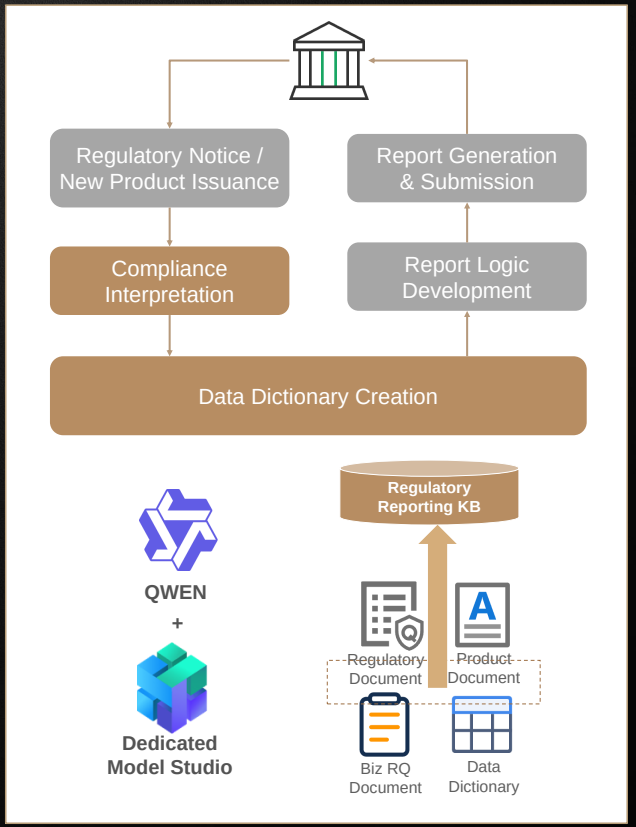
Background: Leveraging LLM to generate Data Dictionary based on regulatory policy or product change, highly improve the efficiency of regulatory reporting update process.

Business Pain Points

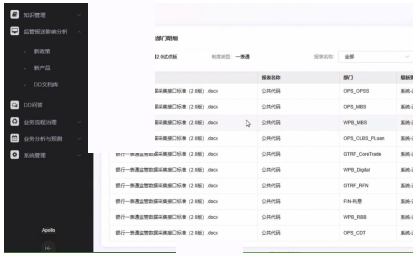
Complexity
- 4 local regulators & 135 affiliates
- 48 branches, including 12 Rural Banks
- 50+ NEW regulatory requirements each year

Volume
- More than 50 IT services related to regulatory reporting
- 774+ regulatory reports generated per month
- Over 80 million data records submitted to regulators monthly

Cost
- $14.5 million project cost per year

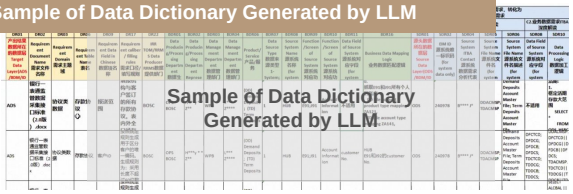


Import Regulatory Update Documents



Chatbot for New Data Dictionary Report Generation

Sample of Data Dictionary Generated by LLM

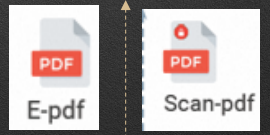


Banker's Agent for Financial Reports Analysis and Credit Proposal Generation

Alibaba Cloud

User Interaction

Standard Analysis



Upload:
Financial Statement

Create:
New Analysis Task

Free-style Analysis

Process of Analysis

S1: Business Summary

- What the company does
- Who its customers are
- Industry in which it operates
- Recent major events

S2: Executive Summary

- Company director list
- Executive earning structure
- Directors' plan to minimize debt and increase profitability

S3: Management View

- View on financial condition
- View on changes of economic environment
- View on company outlook

S4: Risk Factor

- Company litigation and legal cases
- Company outstanding debts and insolvency risk
- Company unexpected / extraordinary events
- Company faced market risk information
- Company faced credit risk information
- Company faced liquidity risk information
- Potential risk highlight

S5: Stockholder Information

- Stockholder list
- Dividend policies and activities
- Share issuance
- Share buyback

S6: Financial Data Analysis

- **Balance sheet performance**
  - 17 standard financial fields
  - Statement-specific
  - non-standard financial fields
  - Current ratio
  - Working capital
  - Return on equity (ROE)
  - Return on assets (ROA)
  - Debt-to-equity ratio
- **Income statement performance**
  - 9 standard financial fields
  - Statement-specific non-standard financial fields
  - Gross margin
  - Net profit margin
- **Cash-flow performance**
  - Net cash flows from operating activities (CFO)
  - Net cash flows from investing activities (CFI)
  - Net cash flows from financing activities (CFF)
  - Ending cash balance

Free-style Question for Document Content

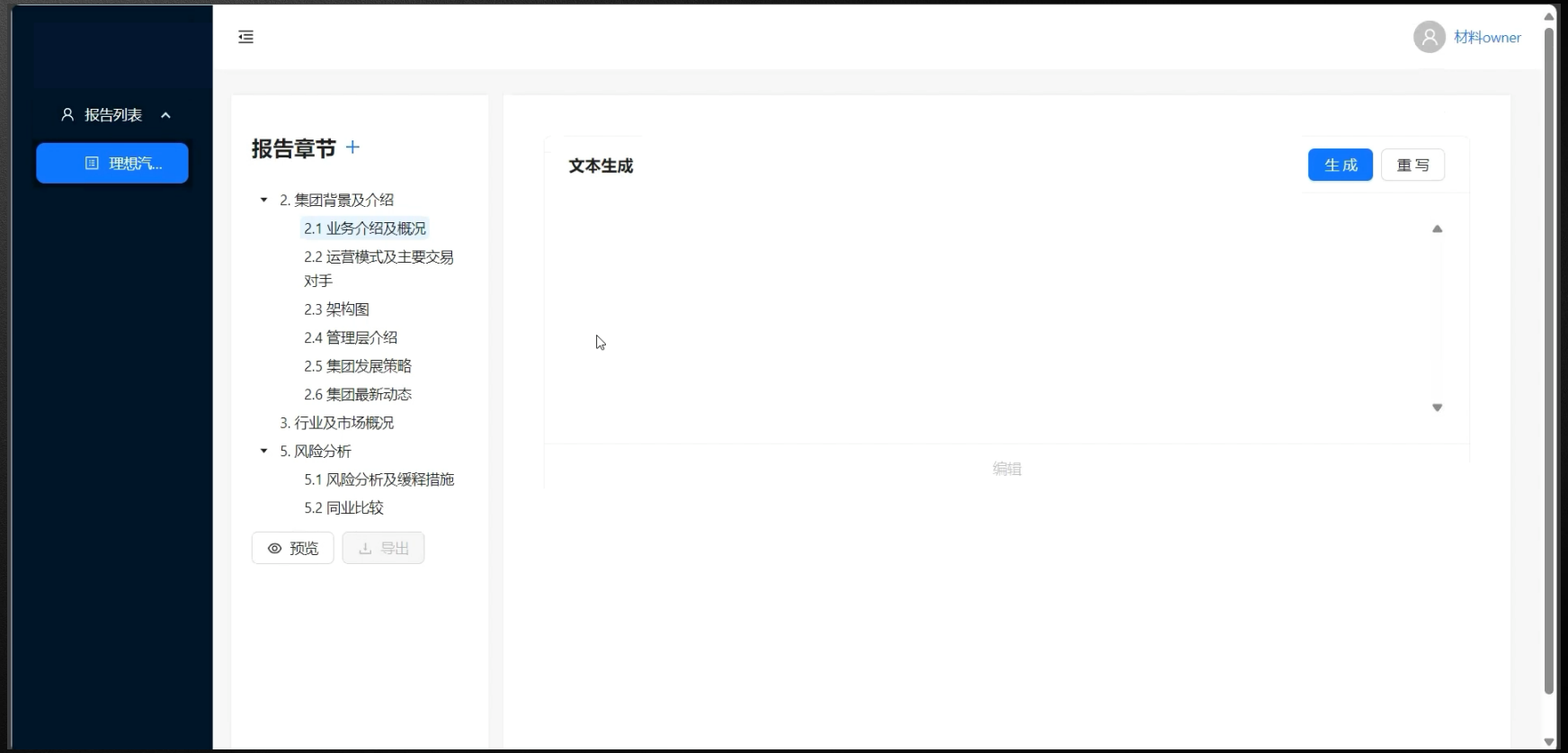
Free-style Question for Standard Analysis

Report

Auto-generated Editable Memo

- **S1**
  - Analysis points
- **S2**
  - Analysis points
- **S3**
  - Analysis points
- **S4**
  - Analysis points
  - Model summary
- **S5**
  - Analysis points
- **S6**
  - Analysis points
  - Model summary of sub-section
  - Model summary of entire-section
- **S7: Recent News**
  - Company news
  - Industry news
- **S8: Self Analysis**
  - Free-style analysis outcome

Banker's Agent for Financial Reports Analysis and Credit Proposal Generation



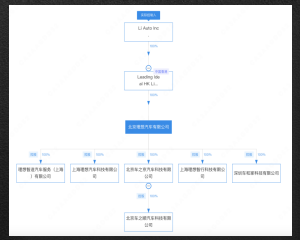
Banker's Agent for Financial Reports Analysis and Credit Proposal Generation

Alibaba Cloud

Multiple Data Source Integration & Processing

1. Various types of websites: HKEX, CADA, car owner's home, etc.

2, pictures.
(Company Organization Chart)



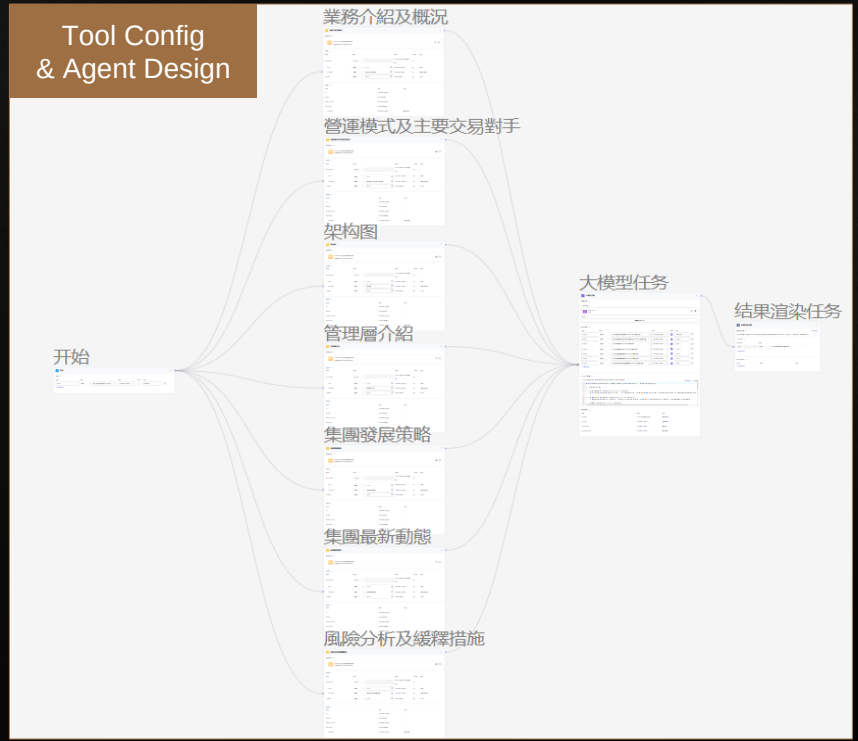
3. PDF text
(Annual Report)

4, Tables & Structured Data
(Ideal sales by model)

车型	销量	所属级别	占该厂商销量份额	在级别中排名	时间	厂商
理想L6	25393	SUV	47.28%	4	2024.09	理想
理想L7	12731	SUV	23.70%	25	2024.09	理想
理想L9	7597	SUV	14.14%	39	2024.09	理想
理想L8	6592	SUV	13.24%	44	2024.09	理想
理想MEGA	654	MPV	1.64%	30	2024.09	理想
理想L6	24897	SUV	51.74%	4	2024.08	理想
理想L7	10307	SUV	21.42%	28	2024.08	理想
理想L9	6696	SUV	13.91%	39	2024.08	理想
理想L8	5476	SUV	11.38%	49	2024.08	理想
理想MEGA	746	MPV	1.55%	31	2024.08	理想

Built-in tools: AutoDoc, AutoBI configuration & Agent Orchestration

Tool Config & Agent Design



Banker's Agent for Financial Reports Analysis and Credit Proposal Generation

Scenario	Sub-Tasks	Models
AutoDoc (Documentation Q & A)	Document Parsing	OCR, Framework recognition, table extraction, reading order analysis
	Query overwrite	Qwen2.5-14B-OpentrekQuery
	Recall & Sort	Qwen2.5-1.5B
	Document Summary	Qwen2.5-72B
AutoBi (Data Report)	Query overwrite	Qwen2.5-14B-OpentrekQuery
	Mate & Value Recall	Qwen2.5-14B-OpentrekBI
	NL2SQL	Qwen2.5-72B
	Data summary	Qwen2.5-72B
	Icon generation	Qwen2.5-14B-Opentrek Chart
AI Writing (Summary Report)	Intent recognition	Qwen2.5-72B
	Report Summary	Qwen2.5-72B

Re-define Sales, Service and Training with Digital Avatar

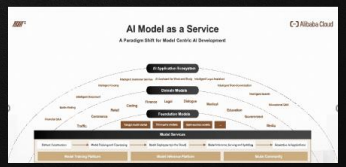
Q&A
Digital Avatar

+

LLM

+

Speech AI

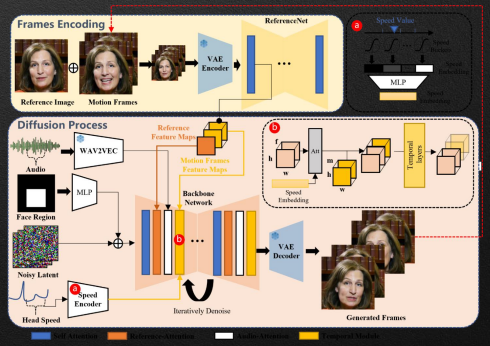


=

In a few hours, an entire new customer service and training experience is complete!

Accelerate Product Development with Coding Copilot (For Non-Coders!)

Digital Avatar Model

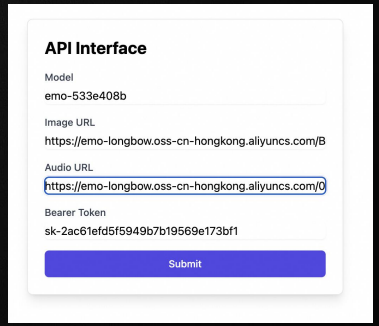


Coding Copilot

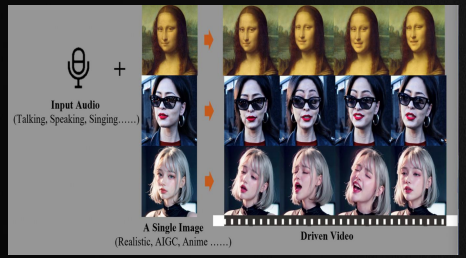
- **Authoring code:** 2x faster
- **Adding comments:** 10x faster
- **Reading code:** 5x faster
- **Getting help:** 2x faster

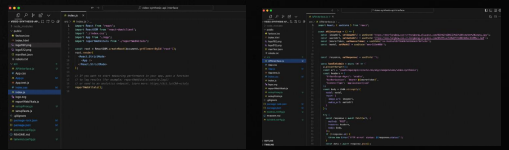
=

In A Few Days, A Digital Avatar Service That Can Generate New Videos!



+





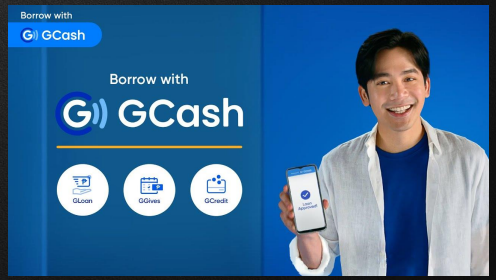
In an Alibaba Group Ecosystem company, 30% of coding copilot code that are accepted by developers, and overall, about 10% of the code copilot code that are adopted in the final codebases.

Accelerate Advertisement and Image/Video Generation with Content AI (For non-marketers!)

Models

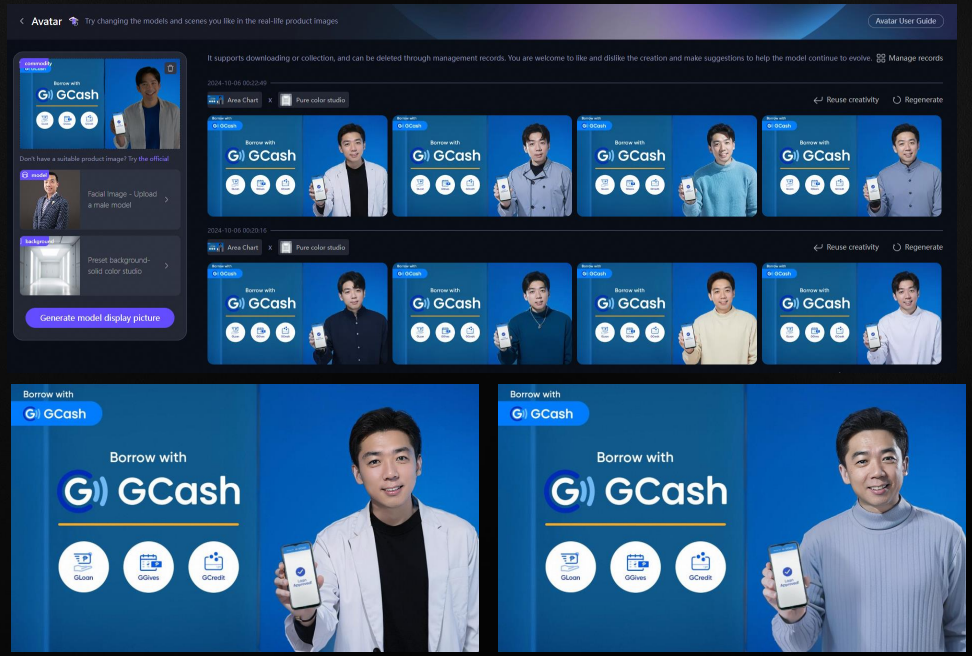
+

Original Advertisement



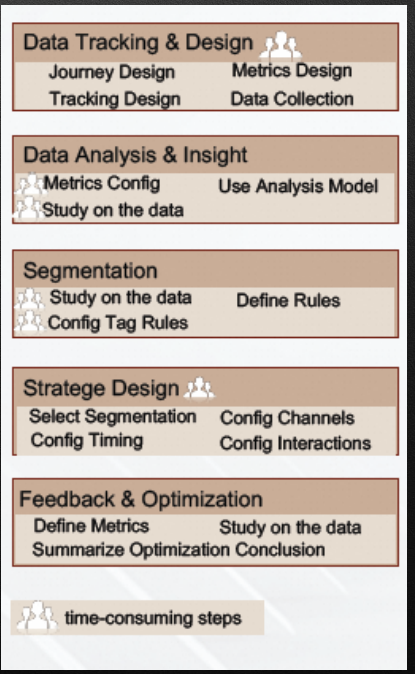
=

In a few seconds, an portfolio of advertisements are generated!



Achieve Hyper-Personalisation with Digital Marketing AI-Workbench

Rule Based



+

AI-Enhanced Tagging and Insights

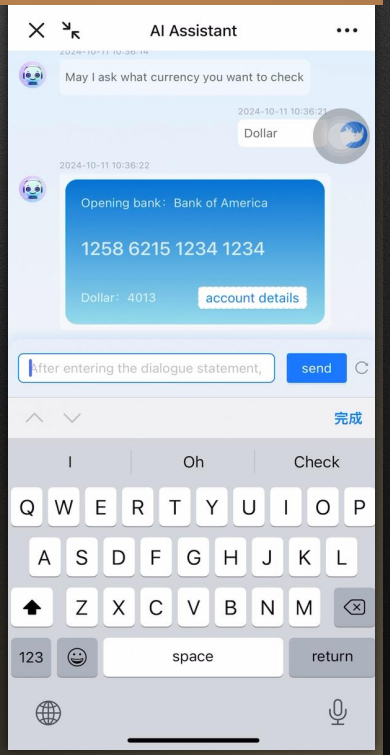
- AI Tracking
- AI Data Insight
- AI Segmentation

=

Significant time-savings on defining and executing on Marketing Strategies!

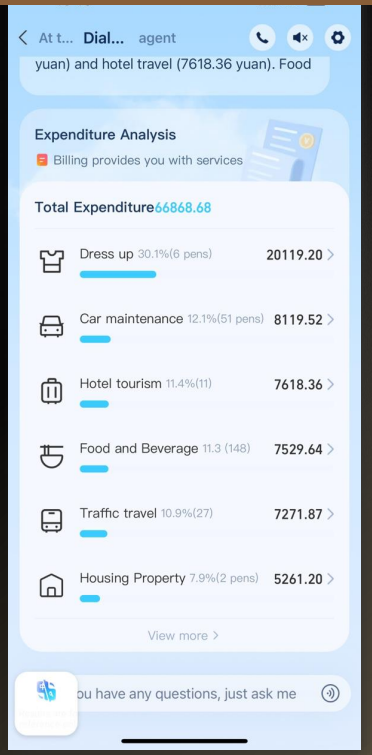
Mobile AI Agent – Seamless Experience Out of the Box

Transfer



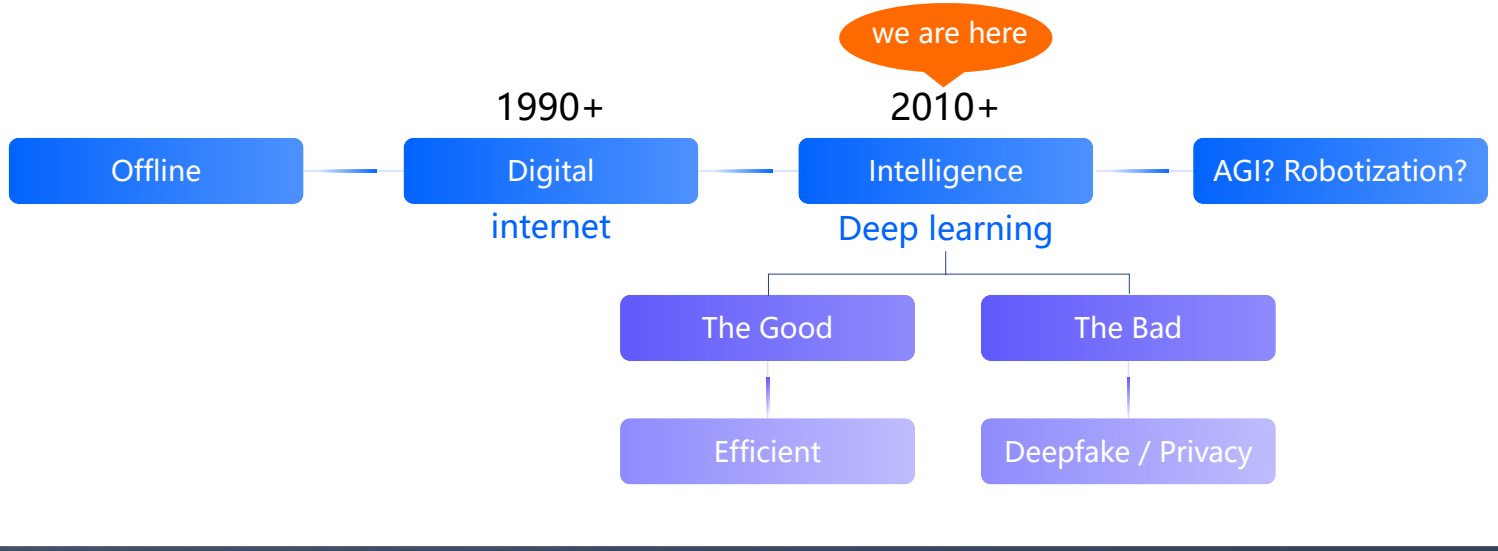
Industry/Field	Scenarios	Scenario Description
Bank	Query Balance	Debit Card Balance Query
	Personal Deposit Certificate	Issuance of Personal Deposit Certificate
	Modify mobile phone number	Handle mobile phone number modification business
	Transfers	Quickly identify the contact person according to the user's historical habits, or guide the entry of new contact information, and directly call the transfer transaction after completing the security verification.
	Transaction Details Query	Query Mobile Banking Transaction Details
	Credit Card Repayment	Handling Credit Card Repayment Transactions
	Quota Adjustment	Adjust credit card limit
	Query Bill	Query Credit Card Bills
	Bill Installment	Handle credit installment
Insurance	Insurance options	Insurance Product recommend: Help me recommend medical insurance.
	Claims	Commercial Insurance Claims Application
	Product comparison	Formatting Comparison of Insurance Products
	Policy Query	Policy Covered Amount Query
	Claim progress query	Insurance claim progress query
Securities	Application for Account Opening	Securities Account Opening Application
	Account Query	Securities account status
Fund	Fund recommend	recommend financial products based on user risk tolerance
	KYC-Risk Assessment	The user welcome interface displays interactive information such as customer-related assets and to-do information.
	Management scale	Company/Market Fund Management Size Change
	Application for Account Opening	Fund Account Opening Application
	Monthly Position Report	Fund monthly position information progress, earnings, market conditions, opportunity analysis, etc.
	Zhou Dou Focus	Fund weekly position information progress, earnings, market conditions, opportunity analysis, etc.
	Chance for after-hours chat	Fund daily market interpretation, point of view display,
	Position Analysis	Position Analysis, Configuration Recommendations, Strategy Portfolio, recommend of Interest
	Fund Morning Post	Fund Morning Post recommend, Allocation Recommendations

Budget Management



The Ethical Dilemma of AI – How Does The Risk Landscape Change?

- The transformation from digital-driven to intelligence-driven is unstoppable.
- With AI generated content booming these years, there are the good and the bad.



Do You Know Who Is Watching You?

Smart Glasses

+

5 Established Technology

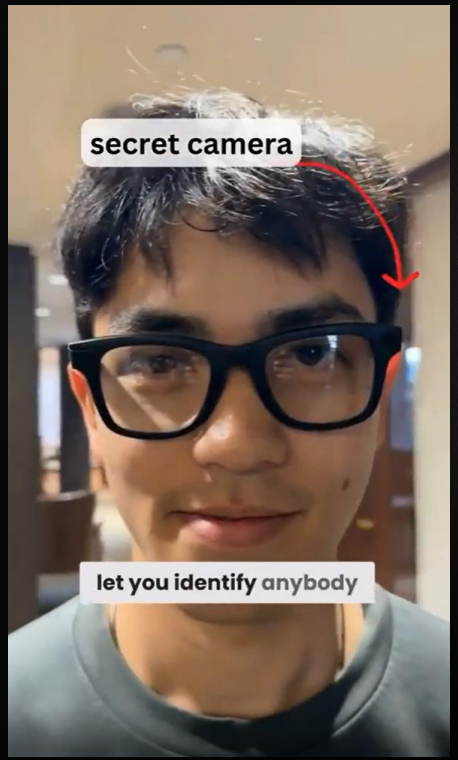
I-XRAY: The AI Glasses That Reveal Anyone's Personal Details—Home Address, Name, Phone Number, and More—Just from Looking at Them

Builders: AnhPhu Nguyen & Caine Ardayfio
Special thanks to Pavan Pandurangi, Alyssa Suh, Matthew Fisher, Jake Lewin, and Aida Baradari for contributing to the project.

1. Pimeyes (Face → URLs)
2. FireCrawl (URLs → Scraped Data)
3. LLMs (Scraped Data → Name + Personal Details)
4. FastPeopleSearch (Name → Home Address, Phone #, Relative's Names)

=

Identify (or Verify?)



Source: I-XRAY: The AI Glasses That Reveal Anyone's Personal Details—Home Address, Name, Phone Number, and More—Just from Looking at Them

Do You Know Who Is Calling You?

Most trending type of fraud in 2023

×10 increase in the number of deepfakes detected worldwide from 2022 to 2023 (our internal statistics)

Finance Employee Defrauded for $25M by Deepfake CFO

The Hong Kong-based worker was tricked by a multi-person video conference where everyone else was fake.

Published Feb. 5, 2024

Is Deepfake Is Real? Yes, Thanks to Popularity of Gen AI

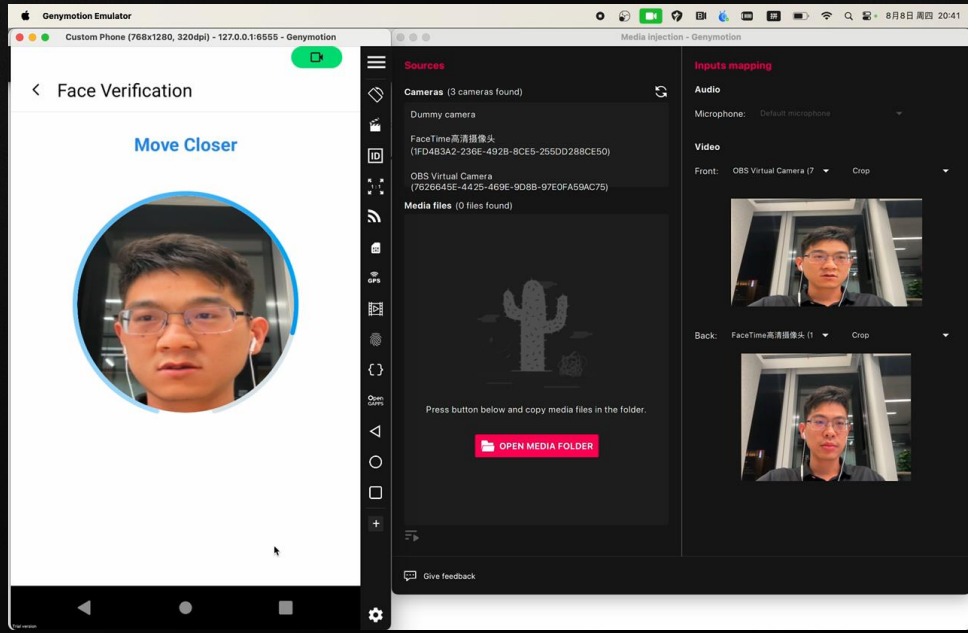
Alibaba Cloud

Deepfake Photos

Philippines black market
Genuine Deepfake attacks

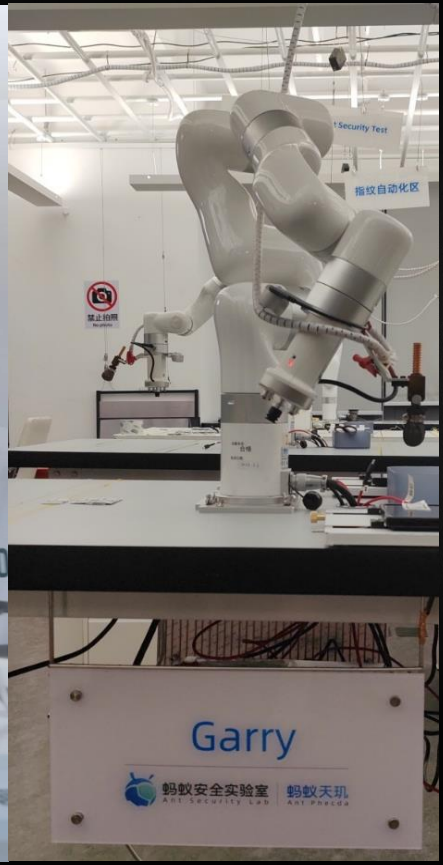
Hijacking Tools

In a few seconds, a new fake account is opened!



Using AI To Fight AI-Induced Identity Fraud

Alibaba Cloud



Using AI To Rethink About Anti-Money Laundering

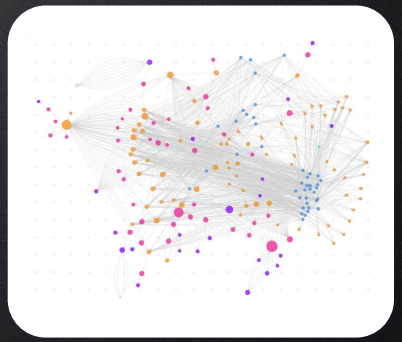
Alibaba Cloud

Traditional Solution Result

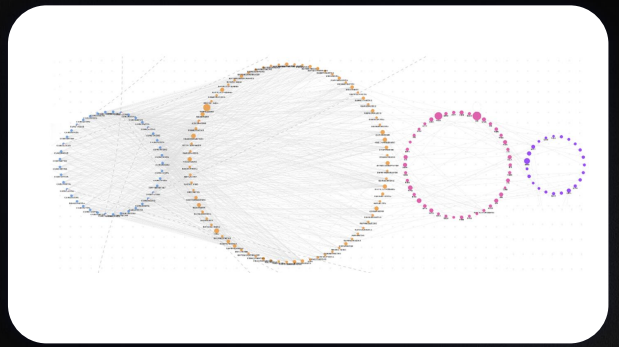
Our Solution Result

Complex Group Risk

- Obscured internal structure
- Extended group size
- Poor Signal-Noise-Ratio

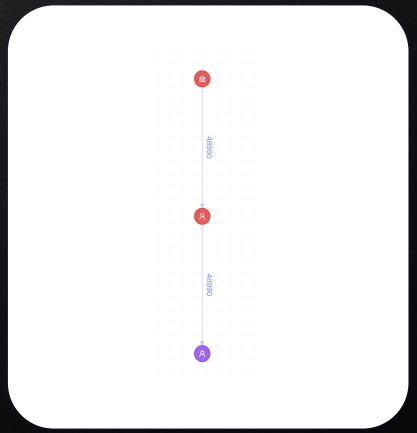


Graph Restructure Engine

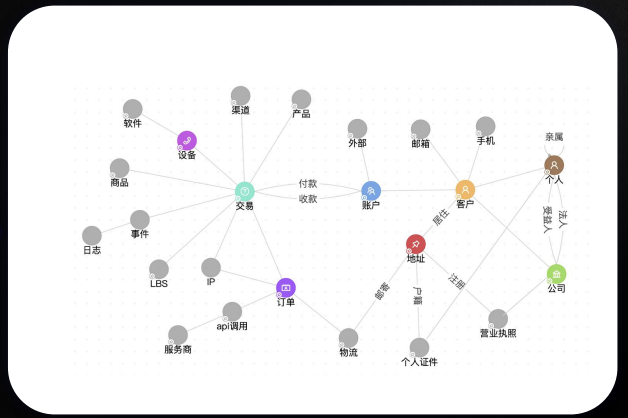


Highly Concealed Risk

- Few risk trace
- Severer risk type

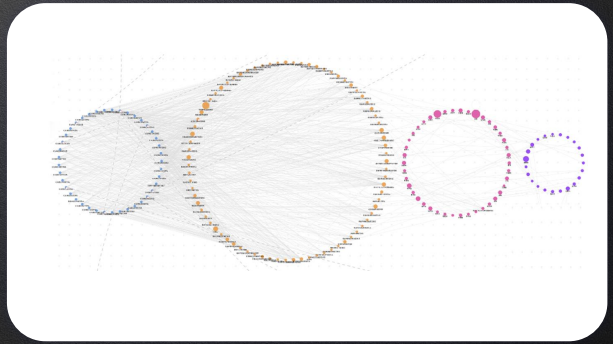


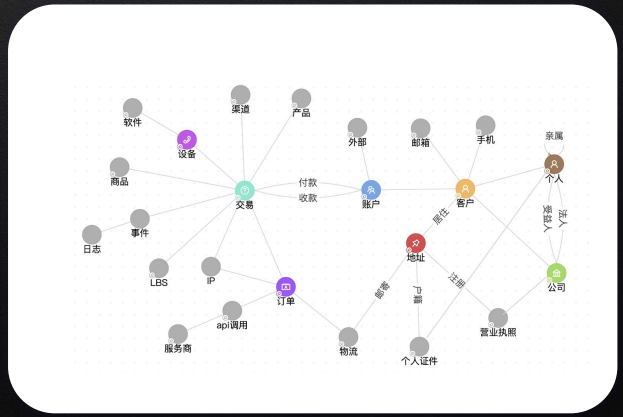
Generative Detection Engine



Using AI To Rethink About Anti-Money Laundering

Suspicious Transactions Report Generation





AML insights into STR reports

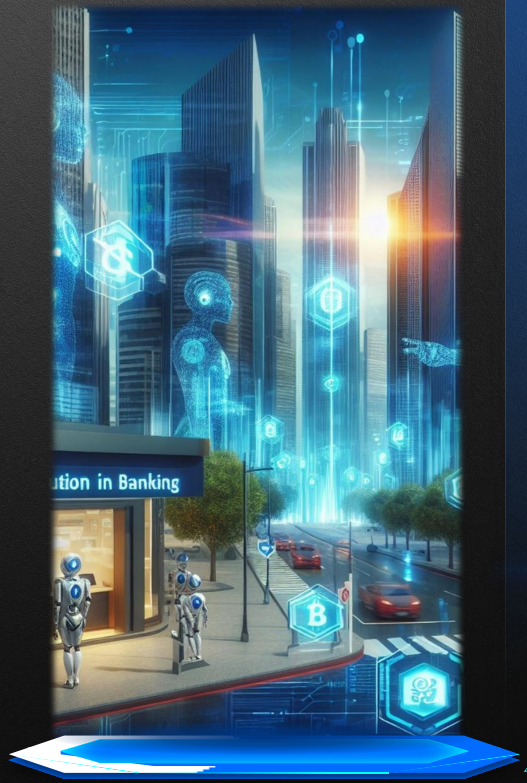
IDA7400880_2024-04-11T00_00_00 - Notepad

File Edit Format View Help

```
--- Customer's background ---
Name: KDBY KDQYW NOY ("KDBY KDQYW NOY")
Gender: Male
Date of Birth / Age: 01 Jan 1984, 39
Nationality / ID Type: DJ / Passport
Occupation: Management Personnel
Relationship with our Bank since: 12 Dec 2018
Account maintained with our Bank: AT, CA, AP, SA, EG, HB, IA
Purpose and reason for opening account: N/A
Source of fund / wealth: N/A
Anticipated turnover and no. of transaction/year: N/A
Any previous STR to JFIU: 630/24
Online search: Nil

--- Triggering event ---
SAS alerts - Large Total Cash Transactions

The customer, IDA7400880, triggered an investigation due to a large
total amount of cash transactions exceeding HKD 608,785 over a
period of 3 business days.

--- Transaction Summary ---
Transaction review period (from 08 Apr 2024 to 11 Apr 2024)

There were totaling 23 counts of debit transactions totaling
equivalent to HKD608,785 and 1 count of credit transaction totaling
equivalent to HKD1400.

Major debit transactions:
- 16 counts of ATM cash withdrawals totaling HKD216,500 with
transaction amount range from HKD500 to HKD160,185.
- 4 counts of teller cash withdrawals totaling HKD203,000 with
transaction amount range from HKD1400 to HKD203,000.

--- Additional Information ---
```

Ln 1, Col 1 | 100% | Unix (LF) | UTF-8

Embrace the AI-Powered Future



Predictive AI and Generative AI is reshaping the finance industry with innovative applications that create value for both financial institutions and their customers.

- Marketing
- Productivity
- Risk Management

However, AI also poses some challenges and opportunities for the finance industry, such as ethical issues, regulatory compliance, talent development, and competitive advantage.

Is important for the finance industry to embrace AI as a strategic tools and a catalyst for innovation.


Alibaba Cloud
THANK YOU

網絡威脅形勢之最新動態及網絡管理的重要性

HACK A DAY 2

Securing identity

顏國定

PwC 合夥人，網絡安全與隱私領域

Dark Lab 聯合創辦人

2025 年 5 月

pwc

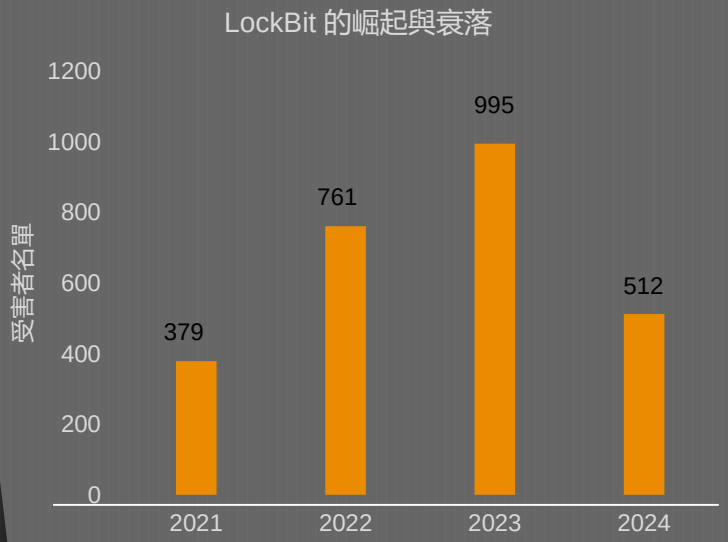
2024年勒索軟體形勢出現動盪，在執法行動打擊及詐騙性撤退事件後，其行為變得更難以預測。

Fabian Wosar
@fwosar

Since people continue to fall for the ALPHV/BlackCat cover up: ALPHV/BlackCat did not get seized. They are exit scamming their affiliates. It is blatantly obvious when you check the source code of the new takedown notice. You will see code like this.

```
c="THIS%20WEBSITE%20HAS%20BE
tion has been taken in coor
```

資料來源：Dark Lab，2021年8月至2024年10月期間之威脅情報監測，基於專有洞察、開放來源情報及暗網監控。



↑30%
活躍的勒索軟體威脅組織

↑42
2024年出現了新的專用洩漏網站

27
2024年解散的勒索軟體組織

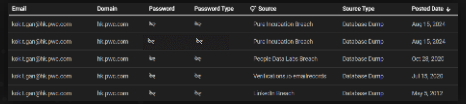
Dark Lab

威脅行為者正在迅速適應，通過多樣化其策略並探索替代手段來增加成功的機會。這些行為者不斷改進他們的技術和方法，以應對新的安全措施和技術進步

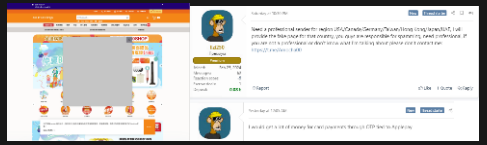
跳過加密；重點在於數據盜竊
單一勒索回歸，直接在洩漏網站上出售受害者的數據

採用生成式人工智能於社會工程
加速創建高度逼真的深偽和網絡釣魚攻擊

增加對雲端和 SaaS 憑證的攻擊
針對暴露的配置文件中的機密和 API 密鑰



數據銷售顯著增加
特別是洩漏的憑證，這些憑證不僅涉及受害者本人，還延伸到他們的第三方



假冒短信的增加
不僅僅是個人身份信息（PII）和信用數據，還試圖竊取有效的憑證、會話和受害者的元數據

資料來源：Dark Lab，基於專有洞察、開放來源情報及暗網監控的威脅情報監測

我的身份

- 創辦人
- Dark Lab
- Hack A Day
- 馬來西亞人
- 父親
- 酒愛好者

Dark Lab

這引出了當今價值連城的問題：
我們應如何定義並保護「身份」？

“**身份**是指一項或一組能夠**唯一識別使用者**的**屬性**。”

2024年澳門網絡威脅概況：聚焦「身份」的新挑戰

CII: 關鍵基礎設施

2024年1月

Ivanti Pulse Secure Vulnerabilities

受影響的澳門CII (9間) :
能源, 政府, 酒店業, 電信業, 金融服務, 教育及醫療保健

2024年2月

Fortinet SSL VPN RCE Vulnerability

受影響的澳門CII :
政府

2024年4月

Command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software

受影響的澳門CII (8間):
政府, 電信業, 醫療保健, 建築, 零售

2024年7月

Improper Authentication vulnerability in Progress MOVEit Transfer

受影響的澳門CII :
酒店業

2024年12月

Sophos Firewall Pre-Auth SQL Injection Vulnerability Allows RCE

受影響的澳門CII :
酒店業

2024年1月

Updated for exploited zero-days in Ivanti VPN

受影響的澳門CII (9間) :
能源, 政府, 酒店業, 電信業, 金融服務, 教育及醫療保健

2024年2月

Another Ivanti Connect Secure Authentication Bypass Vulnerability

受影響的澳門CII (17間):
政府, 酒店業, 電信業, 金融服務, 教育及醫療保健

2024年6月

Progress MOVEit Transfer Authentication Bypass Vulnerability

受影響的澳門CII :
酒店業

2024年9月

Critical Security Flaw Found in GitLab Pipeline Execution

受影響的澳門CII :
教育

2025年1月

Zero-Day Actively Exploited Ivanti Connect Secure VPN Vulnerabilities Lead to RCE and Privilege Escalation (CVE-2025-0282 and CVE-2025-0283)

受影響的澳門CII (17間):
能源, 政府, 酒店業, 電信業, 金融服務, 教育, 媒體及醫療保健

影響 勒索軟件 數據外洩 服務拒絕攻擊 財務損失

Dark Lab

經驗教訓總結 (Summary of Lesson Learnt)

威脅行為者在攻擊中變得更加有意圖和資源豐富

他們專注於濫用有效身份來繞過防禦措施

CVE 的武器化

CVE（公共漏洞和暴露）越來越多地被用來攻擊身份驗證系統和繞過保護身份的控制措施

利用洩漏的憑證作為攻擊向量

針對更廣泛的攻擊面，例如無意中暴露的非生產或管理服務

網絡釣魚攻擊的演變

捕獲有效會話 (Sessions) 並冒充受害者身份，同時其他攻擊則冒充受信任的品牌 (Brands)

CVE 的利用越來越集中於獲取有效身份並繞過身份安全

HACK A DAY 2
Securing identity

資料來源：Dark Lab，2023年1月1日至9月期間之威脅情報監測，基於專有洞察及開放來源情報

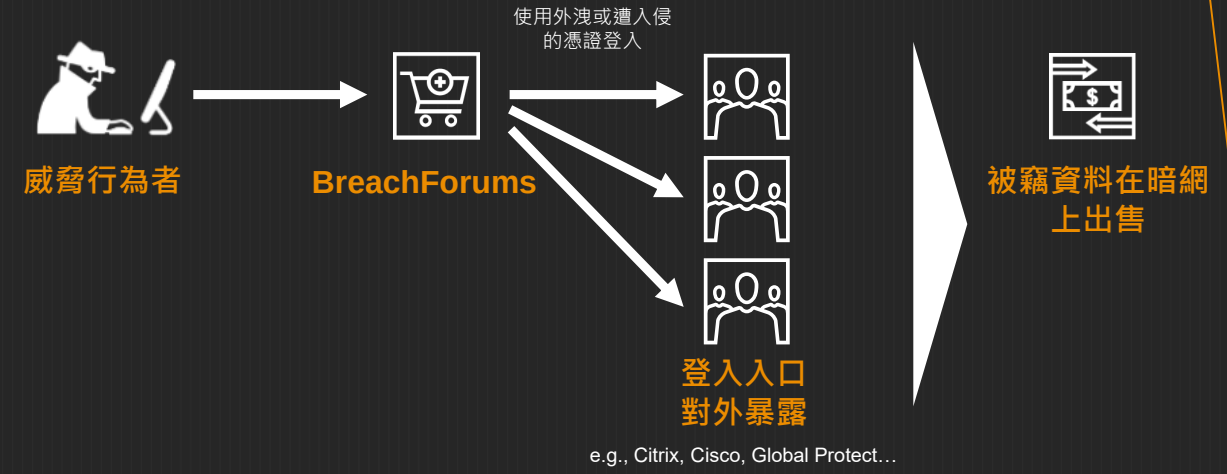
↑ 57% 利用 CVE 進行身份盜竊

↑ 11% 利用 CVE 繞過身份安全控制

最常被攻擊的技術：

- SSLVPN
- 防火牆
- 移動設備管理（MDM）
- 無意暴露的公共雲資產/服務
- 未加固的第三方託管服務

網絡犯罪生態系正日益有意識地將「身份」武器化



資料來源：PwC Dark Lab · 2023年1月1日至2024年10月10日之威脅情報監測，基於專有洞察、開放來源情報及暗網監控

37% 在針對香港及澳門的資訊竊取惡意程式（InfoStealer）感染事件中

174% 於每次存取銷售的平均價格中

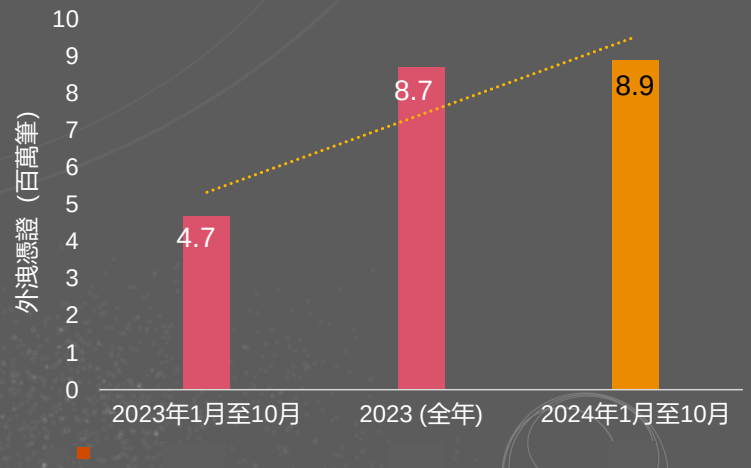
2023 **US$ 1583** 2024 **US$ 4339**

1238% 最高價掛售價格

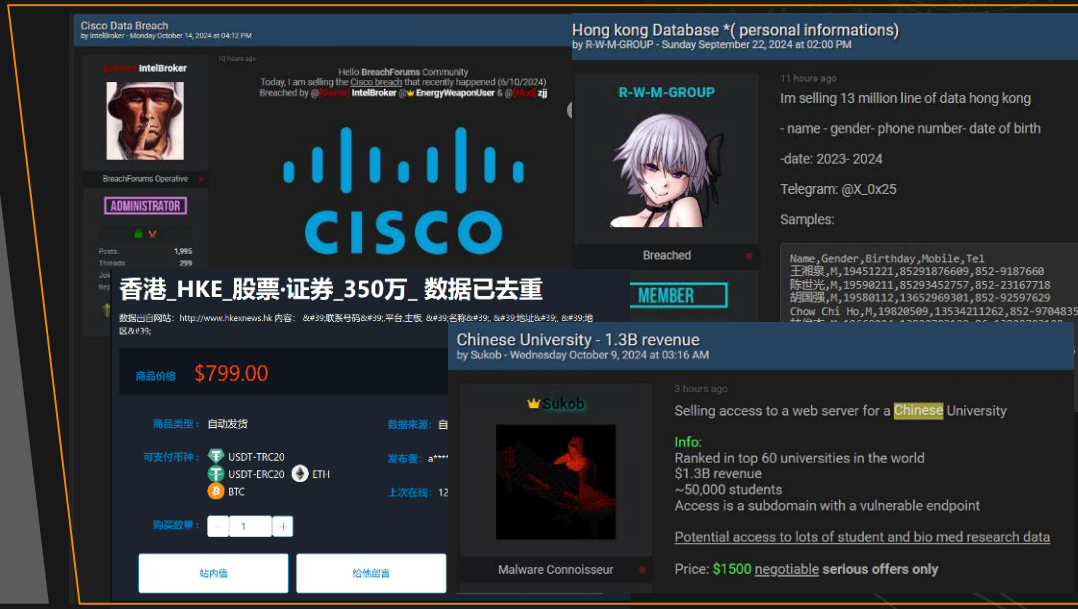
2023 **US$ 74.8K** 2024 **US$ 1 MIL**

Dark Lab

網絡威脅格局的宏觀和微觀變化顯著促成了暗網上洩漏憑證的增加



資料來源：Dark Lab，2023年1月1日至2024年10月22日之威脅情報監測，基於專有洞察、開放來源情報及暗網監控



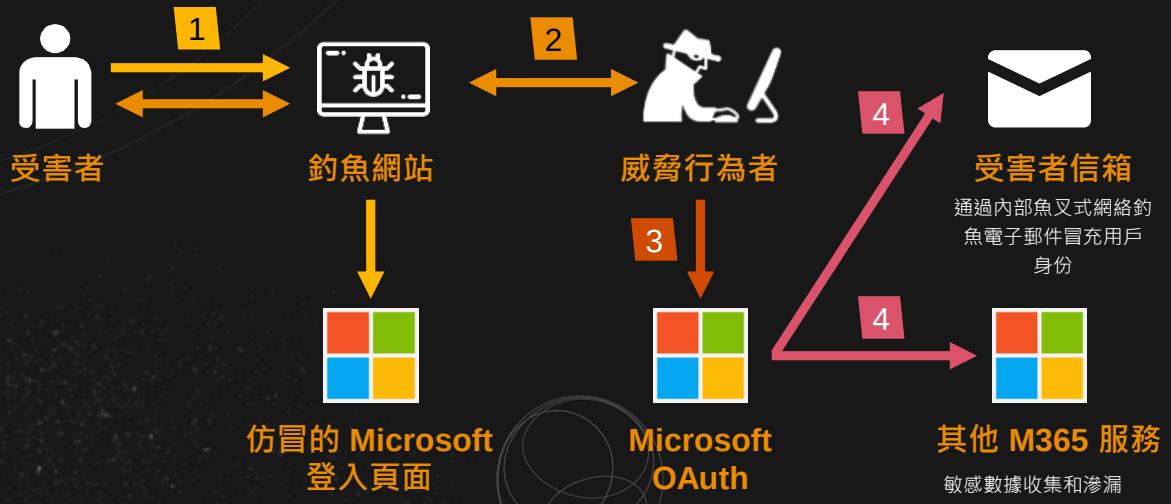
資訊竊取惡意程式（InfoStealer）的使用日益普遍，這類工具專門設計用來從受感染系統中竊取憑證。

資料來源：PwC Dark Lab 專有洞察

Dark Lab

中間人攻擊 (AiTM) 網絡釣魚活動持續存在，冒充受信任的品牌以進行攻擊

HACK A DAY 2
Securing identity



1 釣魚網站重定向
受害者訪問釣魚網站後被重定向到官方的 M365 登錄頁面。

2 身份驗證
受害者在 M365 入口網站上使用多因素驗證 (MFA) 進行合法登錄。威脅行為者捕獲憑據和令牌。

3 持續性
威脅行為者請求主刷新令牌 (PRT) 以註冊自己的設備進行 M365 的單一登錄 (SSO)。

4 影響
訪問並收集 M365 服務中的數據，並通過內部魚叉式網絡釣魚冒充受害者。

我們該如何預防和偵測這些攻擊？
關鍵在於如何保護「身份」！

預防措施

實施**條件式存取政策**以限制未經授權的存取

- 限制僅可在簽發憑證的裝置上使用該憑證
- 啟用憑證保護機制
- 僅允許從已加入 Entra ID 的混合裝置，或受 MDM/MAM 解決方案管理的裝置登入
- 強制採用多層次強化驗證機制
- 將 Outlook on the Web (OWA) 的工作階段時限限制為 1 小時

偵測機制

偵測並監控**異常活動**

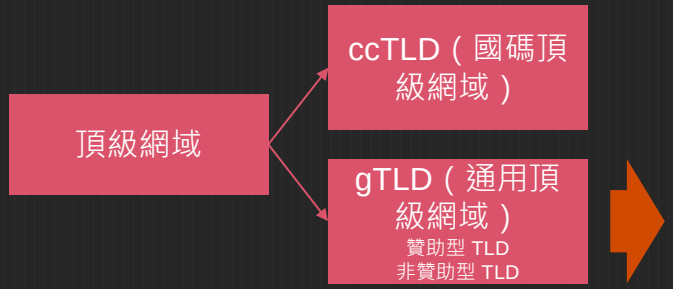
- 監察 Entra ID 中短時間內來自兩個以上國家的存取行為
- 檢視 Entra ID 中標記為「高風險」的登入紀錄
- 監控敏感帳戶是否被指派臨時存取通行碼（Temporary Access Pass）
- 監察大量使用者從同一裝置登入的情況
- 關注特定使用者事件（例如：註冊安全資訊、開始安全資訊註冊等）

向使用者發送裝置註冊通知

我們追蹤網域的方式——它們是如何開始的？

網域在網絡犯罪分子所使用的基礎設施中扮演關鍵角色。

Dark Lab 提出的問題是：威脅行為者是如何「培養」他們的網域?



我們的分析從網域「誕生」之時開始，也就是自註冊起便開始追蹤，並持續觀察其整個生命週期。因此，我們針對通用頂級網域（gTLD）進行調查，所依據的資料來自公開可獲取的數據來源，包括：

- 資料推送（Data Feeds）
  - 新註冊網域（Newly Registered Domains）
- 原始 DNS 紀錄
- WHOIS
- 群眾外包數據（Crowd-sourced Data）
  - 如: VirusTotal, URLScan, CriminalIP, Shodan
- 來自 Dark Lab 網絡威脅行動團隊的資料

我們追蹤網域的方式——它們是如何開始的？

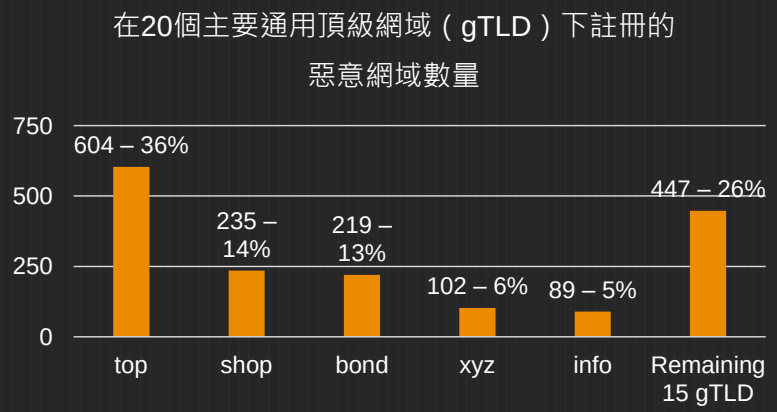
我們會回溯檢視那些被判定為可疑或惡意的網域之歷史活動與註冊情況。

- 原始 DNS 紀錄
- 資料推送（Data Feeds）
  新註冊網域（Newly Registered Domains）
- WHOIS
- 群眾外包數據（Crowd-sourced Data）
  如:VirusTotal, URLScan, CriminalIP,Shodan
- 來自 Dark Lab 網絡威脅行動團隊的資料

方法與結果

網域相似性分析	新註冊網域透過拼寫錯誤（Typo-squatting）或仿冒知名企業名稱，意圖進行冒充或詐騙，例如透過釣魚網站誘騙受害者。
DNS 紀錄分析	透過已知的惡意 IP 位址或網段，識別與指揮控制（Command-and-Control, C2）基礎設施相關聯的網域。
WHOIS 紀錄分析	透過開放來源情報（OSINT），辨識登記資訊中可疑的名稱或電子郵件地址，以發現潛在的惡意網域。
網站架構	託管內容明顯模仿知名網站的網域，顯示其具有冒充意圖的行為。
開放來源情報（OSINT）	由資安社群透過群眾情報平台（如 VirusTotal、Urlhaus）提交的判定結果，用於識別惡意或可疑網域。

我們從針對2025年1月某一天、20個主要通用頂級網域（gTLD）新註冊網域的研究中，獲得了哪些洞察？



資料來源：PwC Dark Lab · 2025年1月針對20個主要通用頂級網域（gTLD）單日的新註冊網域進行的威脅情報分析，基於開放來源情報。其餘 gTLD 包括：.online（87）、.xin（60）、.sbs（58）、.click（42）、.org（38）、.net（38）、.vip（29）、.icu（24）、.site（21）、.cyou（18）、.pro（11）、.store（9）、.biz（7）、.club（2）、以及 .asia（2）

釣魚

垃圾郵件

惡意程式

C2

APT

相關的活動

70,000 每日新註冊網域數量

2,800 在被標示為惡意的70,000個新註冊網域中

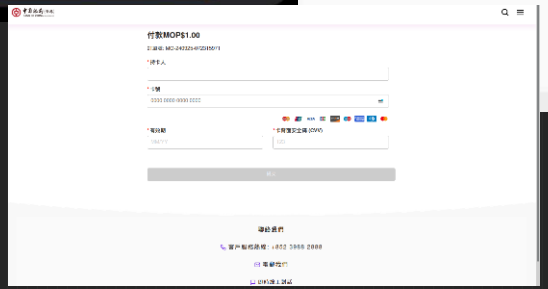
74% 前五大通用頂級網域（gTLD）占了大部分

Dark Lab

新註冊惡意網域範例：

Phishing | Spam | Malware | C2

新註冊網域通常被用於簡訊詐騙中，用以重新導向並誘騙受害者輸入敏感資訊（例如憑證、個人身份資料等），其手法多透過冒充知名機構來進行。



- 冒充中銀獎賞平台以針對澳門及香港地區
- 誘騙受害者提供信用卡資訊、信用卡一次性密碼（OTP）及個人身份資料，例如姓名、地址、電郵及電話號碼等。

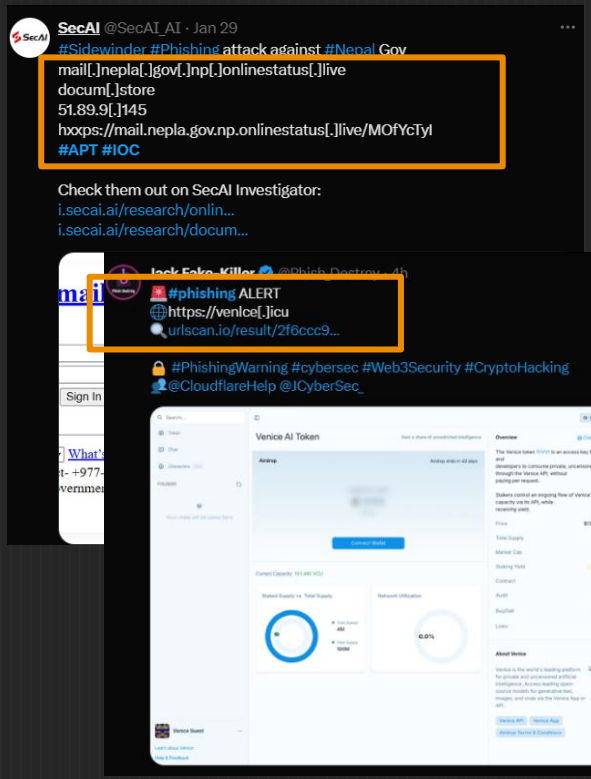
- 冒充「全城消費大獎賞」活動以針對澳門及香港地區
- 誘騙受害者提供信用卡資訊、信用卡一次性密碼（OTP）及個人身份資料，例如姓名、地址、電郵及電話號碼等。

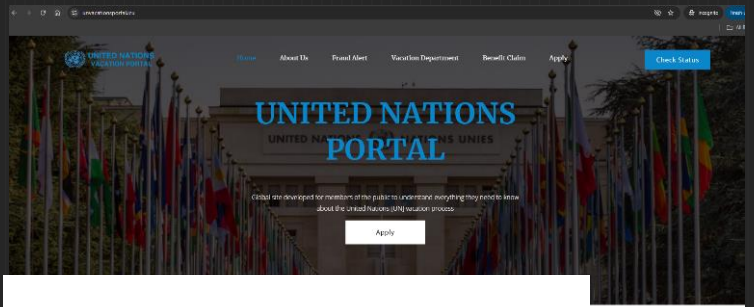
Dark Lab

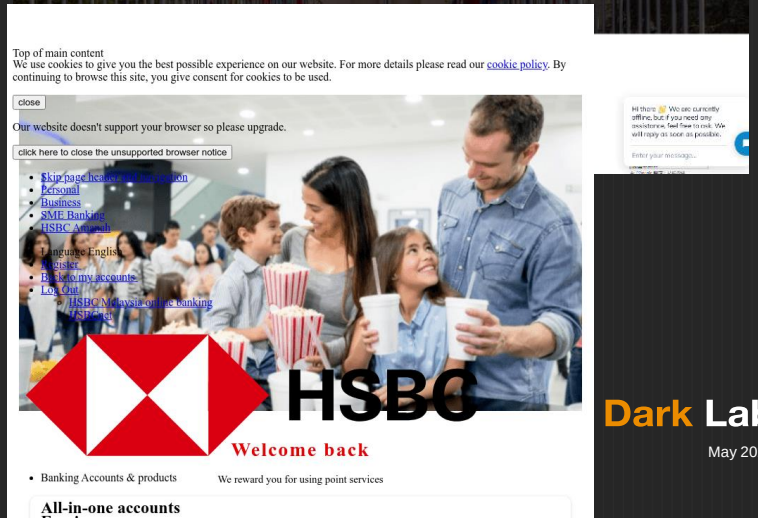
新註冊惡意網域範例 (續):

Phishing | Spam | Malware | C2

除了簡訊外，新註冊網域亦廣泛用於電子郵件中，透過冒充知名機構進行重新導向與誘騙，誘使受害者提供敏感資訊（例如憑證、個人身份資料等）。







新註冊惡意網域範例 (續):

Phishing | Spam | Malware | C2

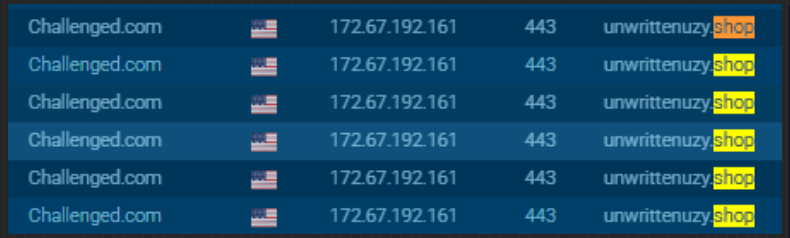
近年來，社交媒體與即時通訊平台已成為謀取財務利益的熱門攻擊目標，原因之一是註冊相似網域的成本低廉，助長了冒充與詐騙行為的氾濫。

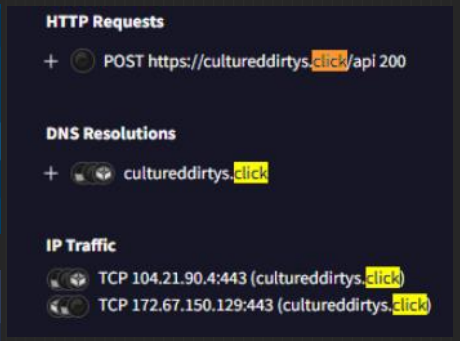
Dark Lab

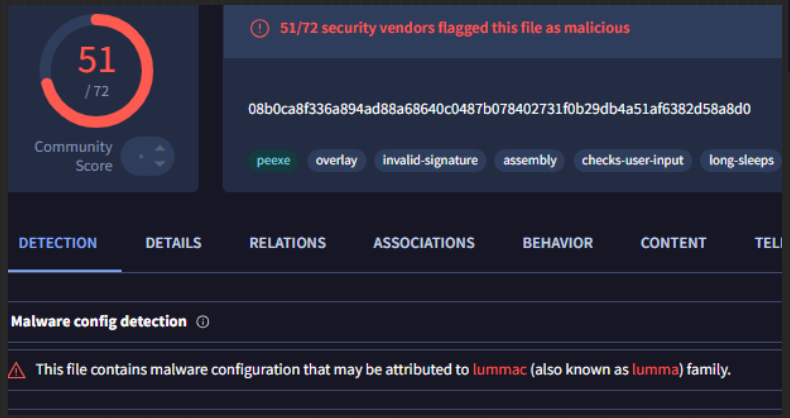
新註冊惡意網域範例 (續):

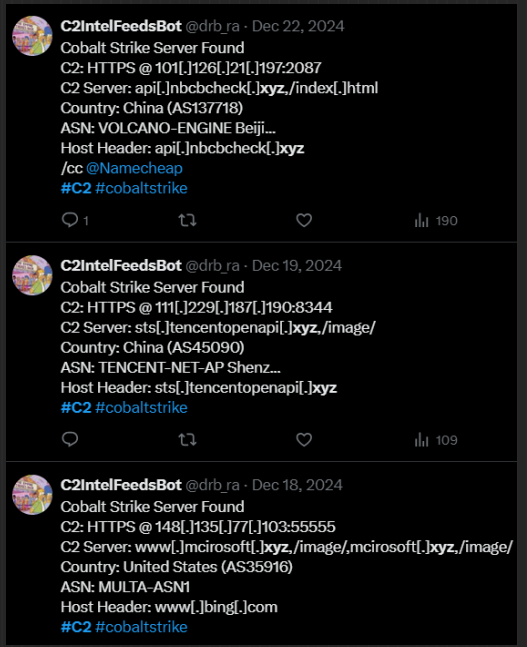
Phishing | Spam | Malware | C2

威脅行為者利用資訊竊取程式（如 Lumma）或架設指揮控制（C2）伺服器時，常會註冊新網域，以便向毫無戒心的使用者散播惡意程式，或維持對受害者系統的持續性控制與通訊。









Dark Lab

這種情況為何會發生？

通用頂級網域（gTLD）缺乏主動治理機制

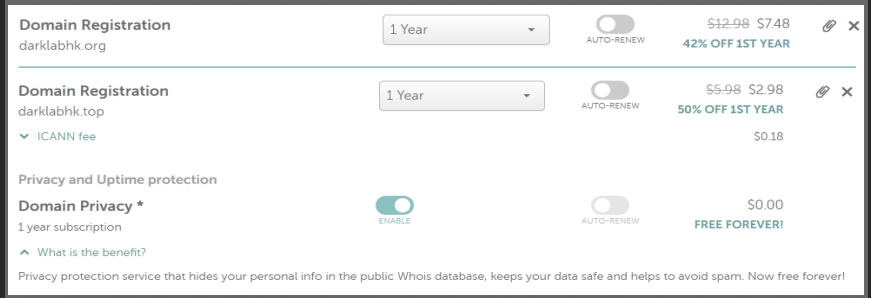
根據 ICANN 指出，註冊商主要依賴**社群回報濫用行為**，才會識別並下架惡意網域

然而，目前缺乏一套**主動、定期且可量化的監測機制**，能即時標示可疑網域。

此問題同樣延伸至**國碼頂級網域（ccTLD）**，情況亦不容忽視**!**

註冊程序過於簡便，加上成本低廉，使得大量註冊網域變得非常容易；

惡意行為者得以**低成本大量**註冊可疑網域



此外，由於網域隱私保護機制，僅需提供有限的 WHOIS 聯絡資訊，且**缺乏對註冊人資料的有效驗證**，進一步助長了此類濫用行為的發生。

如何有效提升頂級網域（TLD）治理與防護能力？

加強跨境協作以提升頂級網域（TLD）治理與防護能力

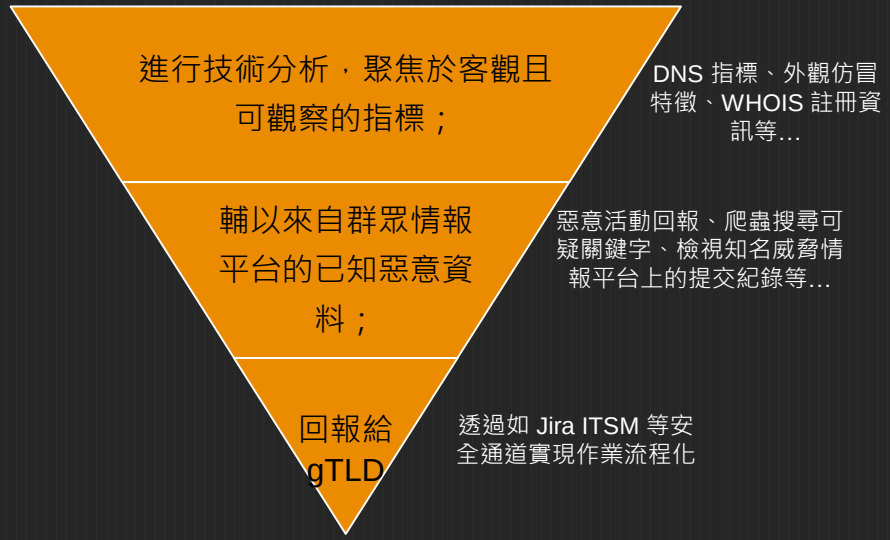
- 加強跨境協作機制，推動 gTLD 與 ccTLD 註冊機構之間的資訊共享與聯防聯控;
- 建立統一的惡意網域通報及應對框架，提升不同司法管轄區間的聯動效率;
- 鼓勵註冊商與國際執法機構、資安團體（如 CERT、ISAC）建立長期合作關係;
- 支援跨境資料分析與威脅情報交換，提升對仿冒及釣魚網域的偵測與回應能力;
- 推動制定國際網域濫用治理準則，協助提升各地註冊流程與驗證機制的標準化與透明度;

冒充政府及國際組織

Dark Lab

我們設計了一套主動監測機制，並正與 .top 網域合作進行概念驗證（PoC），以作為後續擴展推行的基礎。

定期從 gTLD 註冊管理機構接收區域檔（Zone File）



由 gTLD 註冊管理機構執行下架，或將相關資訊分享予執法機關及潛在受害者

自2024年 Hack A Day 起正式展開合作，致力加強香港網絡空間的韌性

Source: https://www.pwchk.com/en/press-room/press-releases/pr-111124.html

Dark Lab

謝謝

pwc.com