# English

Title Slide

"Enhancing Cybersecurity Through Analyst Expertise with Incribo's Synthetic Cyber Dataset"

Self introduction

Data analyst | Security Data Analyst

Capable in data analytics. Familiar with SQL, Python, and Tableau for transforming data into simple graphs. Developing skills in cybersecurity analysis to ensure data integrity and protection against basic threats for informed decision-making.

**skills**

* Python
* SQL
* Excel
* Power BI
* Google Analytics
* Splunk
* Splunk Phantom
* Wireshark
* Tenable Nessus
* Autopsy

education

* Cisco Certified Support Technician (CCST) Cybersecurity
* Pearson VUE Information Technology Specialist
* Google Advanced Data Analytics Professional Certificate
* Google Cybersecurity Professional Certificate
* IBM Data Analytics with Excel and R Professional Certificate
* Google Analytics Certi􀀁cation

Scenario

* **About the Company:**

Incribo, a company specializing in tailored synthetic data generation for cybersecurity needs, utilizes synthetic network attack datasets to assist organizations in identifying and mitigating cybersecurity threats

* **Problem Statement:**

The escalating cyber threat landscape necessitates robust security measures to protect sensitive data and critical infrastructure. Synthetic network datasets, meticulously crafted to mimic real-world network traffic patterns, offer a valuable tool for enhancing cybersecurity posture. Incribo's synthetic network attack datasets provide organizations with a safe and controlled environment to test their security systems, identify vulnerabilities, and develop effective mitigation strategies.

Proposed Solution

* **Strategy:**

Utilize the synthetic dataset to extract actionable insights and support  
strategic cybersecurity decisions.

* **Deliverables:**

1. **Business Task Statement:** Clearly define the cybersecurity  
   objectives and tasks.
2. **Data Sources Description:** Outline the sources and relevance of  
   data used.
3. **Data Cleaning Documentation:** Detail the cleaning processes to  
   ensure data integrity.
4. **Analysis Summary:** Present the analysis methods and findings.
5. **Visualizations and Key Findings:** Highlight critical insights  
   through visual data representation.
6. **Top Recommendations:** Provide prioritized recommendations based on  
   the analysis.

**Ask**

- - - Task:- -

Explicitly state the importance of Incribo's synthetic cyber dataset in identifying and mitigating cybersecurity threats, demonstrating the analyst's expertise in data interpretation and strategy formulation.

Prepare

* **Data Sources:**

The data used requires rigorous cleaning and adheres to ROCCC (Relevant,  
Original, Comprehensive, Consistent, and Correct) standards, ensuring  
high- quality input for analysis.

* **Data Cleaning:**

The analyst utilized Python in Jupyter Notebook for efficient data  
cleaning and manipulation. Each step was meticulously documented to  
ensure reproducibility and transparency, demonstrating the analyst's  
technical proficiency.

Process:

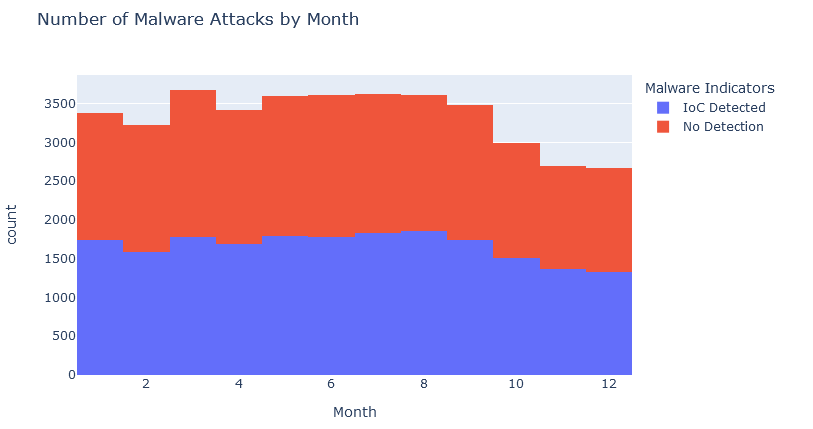
Data Analysis:

* Scrutinized network traffic volume trends to identify potential threats, such as DDoS attacks and credential stuffing attempts.
* Conducted targeted mitigation efforts by concentrating on potential attackers and prioritizing threat response.
* Performed trend analysis to forecast potential escalation points and anomalous authentication patterns, informing patching and mitigation strategies.

Analysis

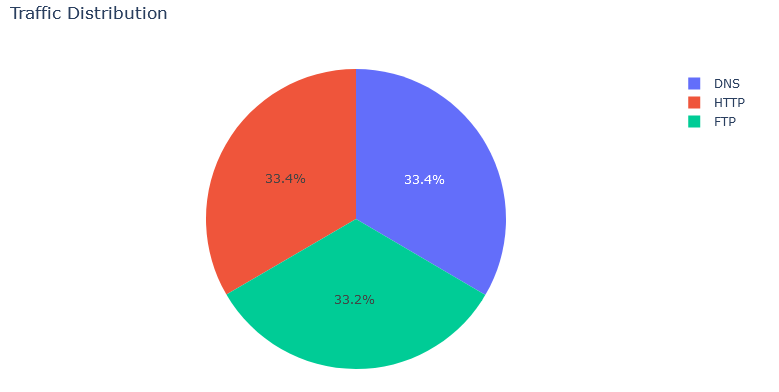
1. Network Traffic Volume Over Time:

Malicious software attacks exhibited significant fluctuations over 12 months, with peak activity during February, April, and June. This underscores the need for heightened vigilance during these periods.



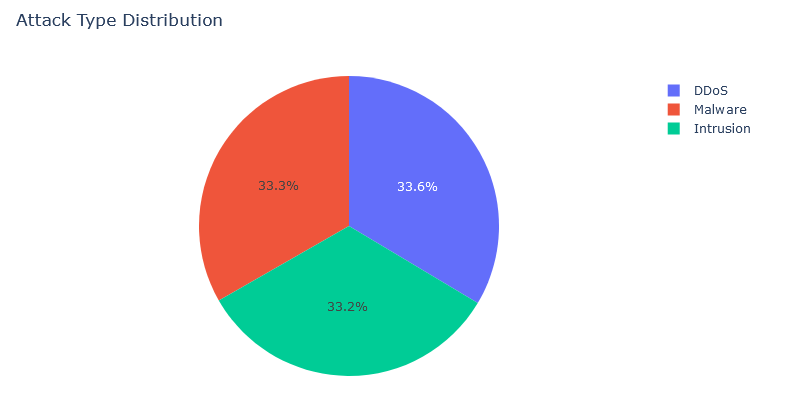
1. Top Sources of Malicious Traffic:

Traffic distribution across DNS (33.4%), HTTP (33.4%), and FTP (33.2%) protocols was relatively even. Organizations should monitor traffic across all these protocols to detect anomalies.



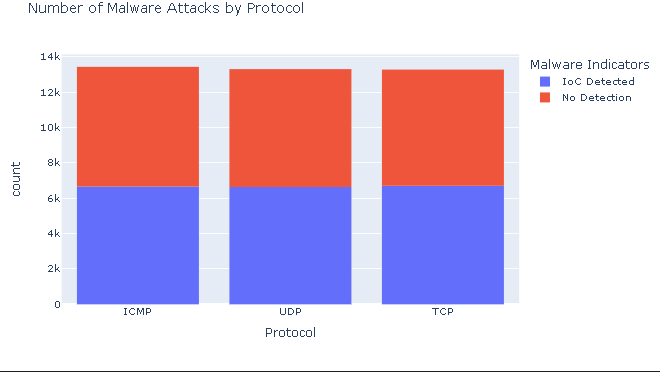
1. Types of Detected Threats:

DDoS (33.6%), Malware (33.3%), and Intrusion (33.2%) emerged as the most prevalent threat types. This necessitates a comprehensive security strategy encompassing all three threat categories.



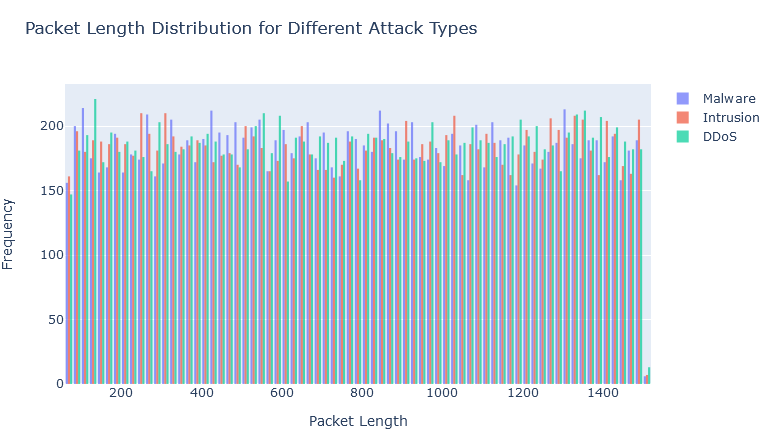
4: User Authentication Attempts

TCP protocol accounted for the highest volume of authentication attempts, followed by UDP and ICMP. Monitoring authentication attempts across these protocols can reveal suspicious activities.



5. Vulnerability Status by System and Severity:

Data packet lengths varied significantly across different attack types (Malware, Intrusion, DDoS). This variation can be utilized for anomaly detection and signature-based protection.



Share:

DDoS Attack Detection:

Abnormal spikes in traffic volume and specific packet characteristics indicate DDoS attacks. Prompt deployment of DDoS mitigation tools and notification of the IT security team are essential.

Credential Stuffing:

Multiple login attempts from diverse IP addresses within a short timeframe suggest password injection attacks. Implementing Multi-Factor Authentication (MFA) and account lockouts after multiple failed attempts is recommended.

Insider Threats:

Unusual patterns of internal employee access to sensitive data raise concerns about potential insider threats. Thorough investigations and implementation of least privilege access controls are warranted.

Act:

Recommendations:

* Continuous Monitoring: Consistently monitor and update visualizations to capture real- time changes in network behavior and the threat landscape.
* Collaborative Analysis: Foster collaboration between analysts and stakeholders to interpret visual insights and implement effective security measures.
* Adaptive Strategies: Develop adaptive strategies based on evolving threat trends and insights derived from visualizations.

Understanding Patterns:

* Pattern Recognition:
  + Threat Detection: Identified patterns indicative of potential threats, such as DDoS attacks and credential stuffing attempts.
  + Targeted Strategies: Developed targeted strategies for vulnerability management and incident response based on the identified patterns.
* Outcome Improvement:
  + Demonstrated how understanding these patterns enhances incident response and overall cybersecurity outcomes, reinforcing the value of the analyst's expertise.

Thoughts on class

This course delved into the intersection of AI, information security, and data analysis, equipping me with the skills to leverage these tools for enhanced cybersecurity. Synthetic network data proved invaluable for training AI models, simulating cyberattacks, and conducting vulnerability assessments. AI-powered threat detection, automated incident response, and proactive vulnerability assessment emerged as key takeaways. By incorporating hands-on experience, real-world case studies, and expert insights, future courses can further empower participants to safeguard our digital landscape.

AI, data analysis, and synthetic network data are crucial for modern cybersecurity.

AI-powered threat detection, automated incident response, and proactive vulnerability assessment are essential.

Hands-on experience, real-world case studies, and expert insights enhance learning.

# 中

標題幻燈片

"通過分析Incribo 合成網路數據集增強網路安全"

**自我介紹**

**資訊安全分析師 | 數據分析師**

* 具有數據分析能力。熟悉 SQL、Python 和 Tableau 將資料轉換為簡單圖表。培養網路安全分析技能，以確保資料完整性並防範基本威脅，從而做出明智的決策。

**技能**

* Python
* SQL
* Excel
* Power BI
* Google Analytics
* Splunk
* Splunk Phantom
* Wireshark
* Tenable Nessus
* Autopsy

教育

* Cisco CCST 思科認證技術人員原廠國際認證
* Pearson VUE ITS 資訊科技專家國際專業認證
* Google Advanced Data Analytics Professional Certificate
* Google Cybersecurity Professional Certificate
* IBM Data Analytics with Excel and R Professional Certificate
* Google Analytics (分析) 個人認證

- 策略:

利用合成數據集提取可行動的洞見,支援網路安全決策。

- 交付成果:

1. 業務任務說明:明確定義網路安全目標和任務。

2. 數據來源描述:概述數據源及其相關性。

3. 數據清洗文檔:詳細說明確保數據完整性的清洗過程。

4. 分析摘要:呈現分析方法和發現。

5. 可視化和關鍵發現:通過視覺數據呈現突出關鍵洞見。

6. 主要建議:根據分析提供優先次序的建議。

任務:

展示Incribo合成網路攻擊數據集在識別和緩解網路安全威脅方面的重要性,展示分析師在數據解讀和戰略制定方面的專業能力。

準備

- 數據來源:

所用數據需經過嚴格清洗,符合ROCCC (相關性、原創性、全面性、一致性和正確性)標準,確保高質量的分析輸入。

- 數據清洗:

分析師使用Jupyter Notebook中的Python進行高效的數據清洗和處理。每個步驟都有詳細記錄,確保可重複性和透明度,體現分析師的技術熟練度。

過程:

數據分析:

- 檢查網路流量量趨勢,以識別潛在的威脅,如DDoS攻擊和密碼注入嘗試。

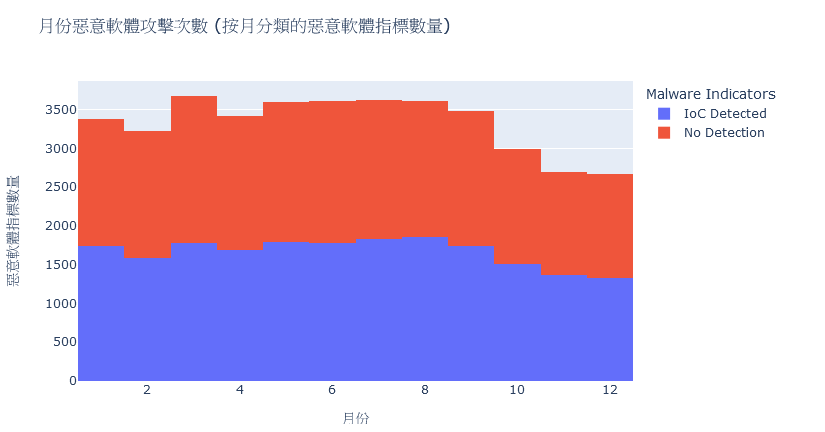
- 集中應對潛在攻擊者,優先處理威脅響應,採取針對性緩解措施。

- 進行趨勢分析,預測潛在的升級點和異常認證模式,為修補和緩解制定策略。

分析

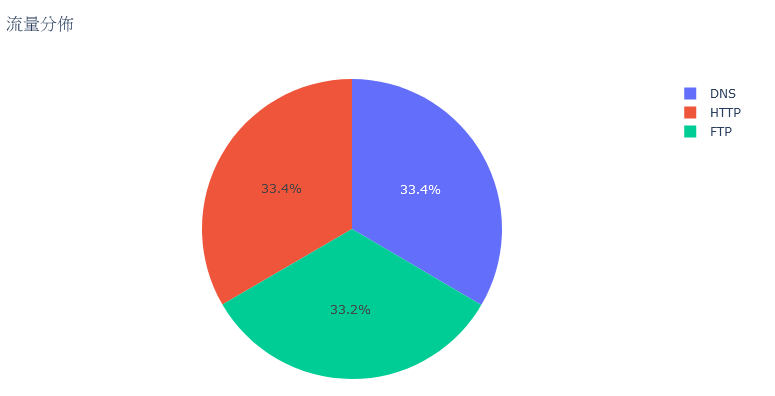
1. 隨時間變化的網路流量:

惡意軟體攻擊在 12 個月內出現明顯波動，2 月、4 月和 6 月是攻擊高峰期。這強調了在此期間需要提高警惕。



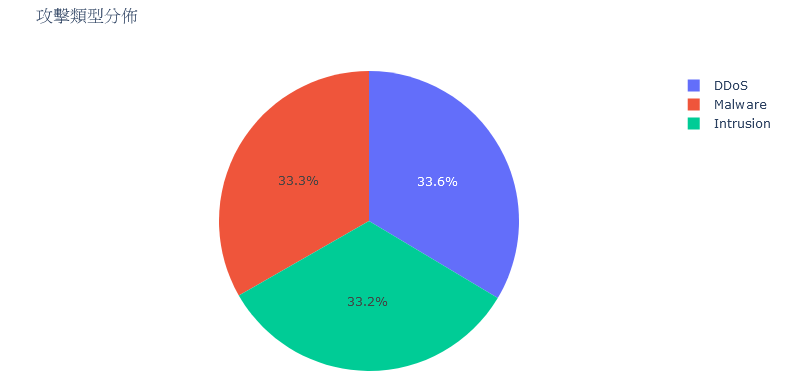
2. 惡意流量的主要源頭:

DNS（33.4%）、HTTP（33.4%）和 FTP（33.2%）協議的流量分佈相對均勻。組織應監控所有這些協定的流量以檢測異常。



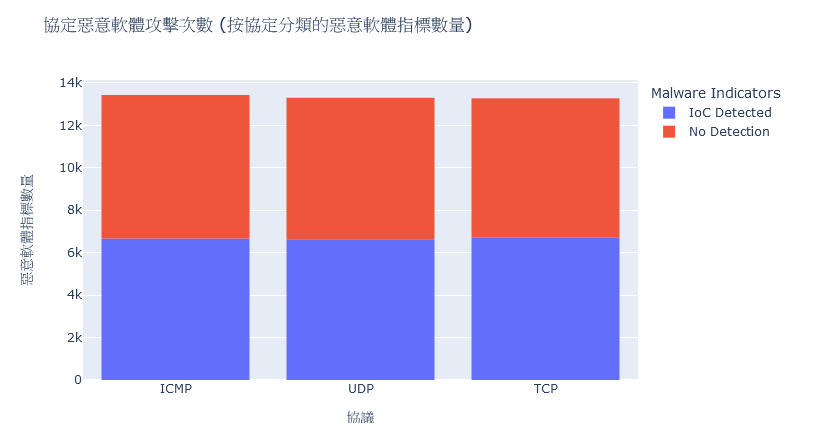
3. 檢測到的威脅類型:

DDoS（33.6%）、惡意軟體（33.3%）和入侵（33.2%）成為最普遍的威脅類型。這需要一個全面的安全性原則，涵蓋所有三個威脅類別。



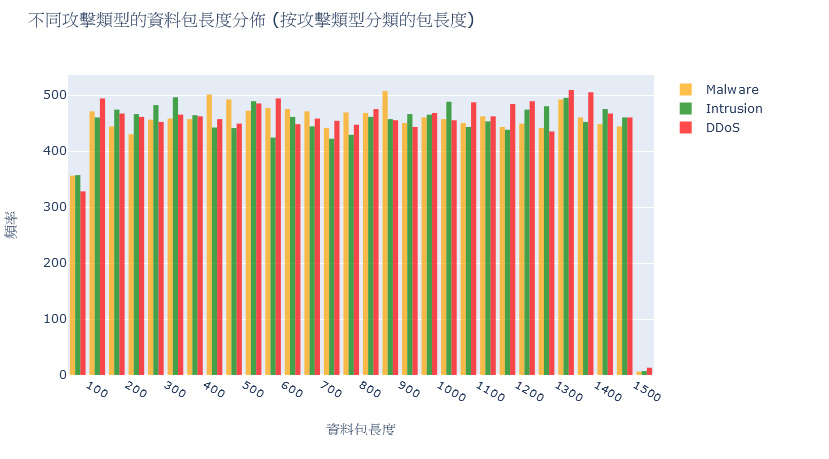
4. 用戶認證嘗試:

TCP 協議的驗證嘗試數量最多，其次是 UDP 和 ICMP。監控這些協議的驗證嘗試可以揭示可疑活動。



5. 按系統和嚴重性劃分的漏洞狀況:

不同攻擊類型（惡意軟體、入侵、DDoS）的資料包長度差異很大。這種差異可用於異常檢測和基於簽名的保護。



分享:

DDoS攻擊:

當流量異常激增和特定資料包特徵表明 DDoS 攻擊。立即部署 DDoS 緩解工具並通知 IT 安全團隊至關重要。

密碼注入:

在短時間內從不同 IP 位址進行多次登錄嘗試表明密碼注入攻擊。建議實施多因素身份驗證（MFA）並在多次失敗嘗試後鎖定帳戶。

內部威脅:

內部員工對敏感性資料的異常訪問模式引發了對潛在內部威脅的擔憂。需要進行徹底調查並實施最小特權存取控制。

行動:

1. 建議:

持續監控

1. 風險評估和管控  
   定期對網路系統、關鍵資產進行全面評估,識別存在的漏洞和風險點。針對高風險領域,制定詳細的補救措施和應急預案。同時識別關鍵業務流程和系統依賴關係,以便在發生事故時進行有效響應。
2. 安全運維和應急響應  
   建立標準化的安全運維流程,包括系統修補、備份恢復、日誌審核等。對發生的安全事件進行根源分析,制定有效的修復方案。同時保持與執法部門的緊密溝通,在發生重大安全事故時獲得支援。

協作分析

1. 身份和訪問管理  
   嚴格管控對內部系統和資源的訪問權限,避免權限濫用或內部人員威脅。可以採用基於角色的訪問控制、雙因素認證等手段。同時檢視第三方服務供應商的身份驗證機制,防範供應鏈安全風險。
2. 加密和密鑰管理  
   對重要數據和通訊進行全生命週期的加密保護,杜絕資訊外洩。部署統一的密鑰管理平台,確保密鑰的安全生成、存儲和使用。密鑰更新頻率、長度等參數要根據實際需求進行設定和調整。

適應性策略

1. 威脅情報收集與分析  
   瞭解當前網路安全領域的最新動態和趨勢非常重要。可以訂閱安全情報服務,收集來自政府、安全廠商等多方面的資訊。通過數據挖掘和分析,識別潛在的威脅因子,預判未來可能出現的攻擊模式。
2. 持續安全培訓與演練  
   不斷提升員工的安全意識和應急技能,使其成為網路安全建設的重要一環。定期開展滲透測試、惡意郵件演習等,檢驗現有防護措施的有效性。並根據演練結果優化應急預案,持續提升整體安全防護能力。

2. 理解模式:

- 模式識別:

o 威脅檢測:識別出DDoS攻擊和密碼注入等潛在威脅的特徵模式。

o 針對性策略:根據識別的模式制定針對性的漏洞管理和事件響應策略。

- 提高成果:

o 展示如何通過理解這些模式來提高事件響應和整體網路安全成果。

課程心得

事實證明，合成網路資料對於訓練人工智慧模型、類比網路攻擊和進行漏洞評估非常有價值。人工智慧驅動的威脅檢測、自動事件回應和前瞻性漏洞評估成為主要收穫。通過結合實踐經驗、真實案例研究和專家見解，未來的課程可以進一步增強參與者保護數位環境的能力。

人工智慧、資料分析和合成網路資料對現代網路安全至關重要。

人工智慧驅動的威脅檢測、自動事件響應和主動漏洞評估至關重要。

實踐經驗、真實案例研究和專家見解可增強學習效果。