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:

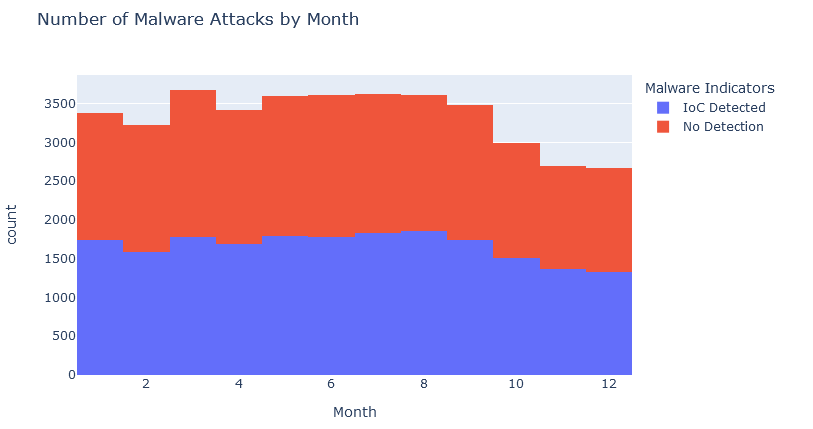
Data Analysis:

* 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

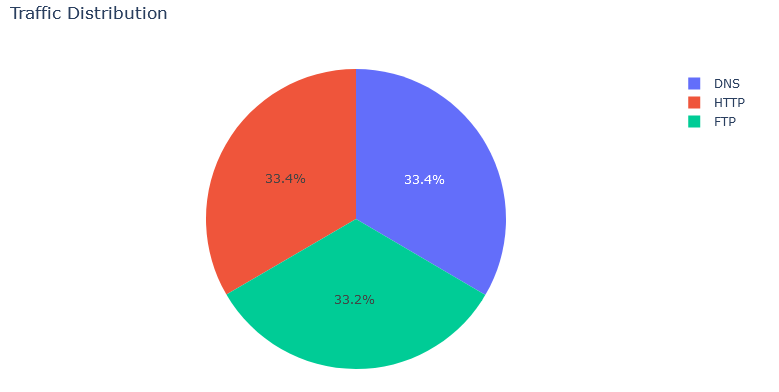
1. Network Traffic Volume Over Time:

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.



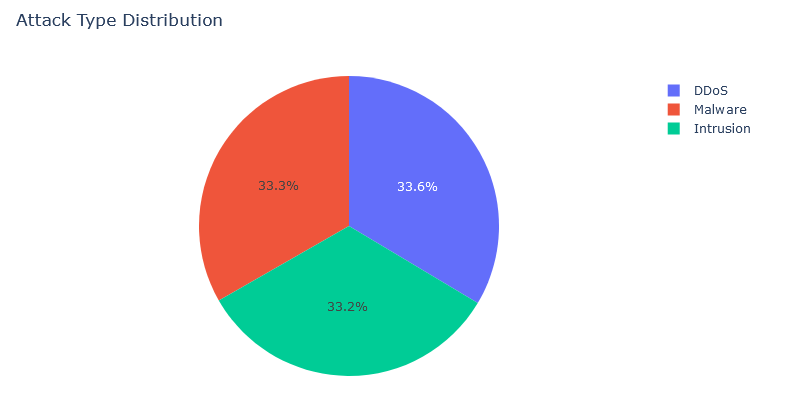
1. Top Sources of Malicious Traffic:

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.



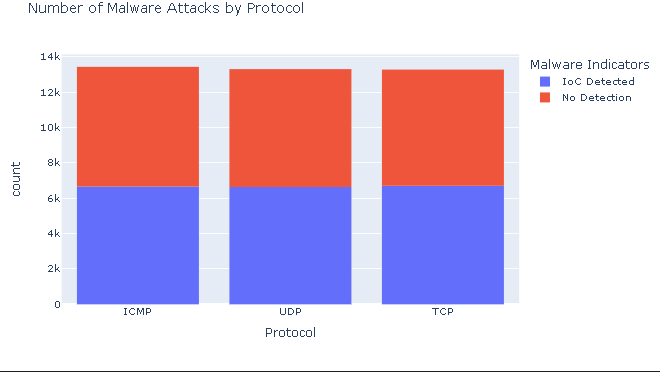
1. Types of Detected Threats:

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.



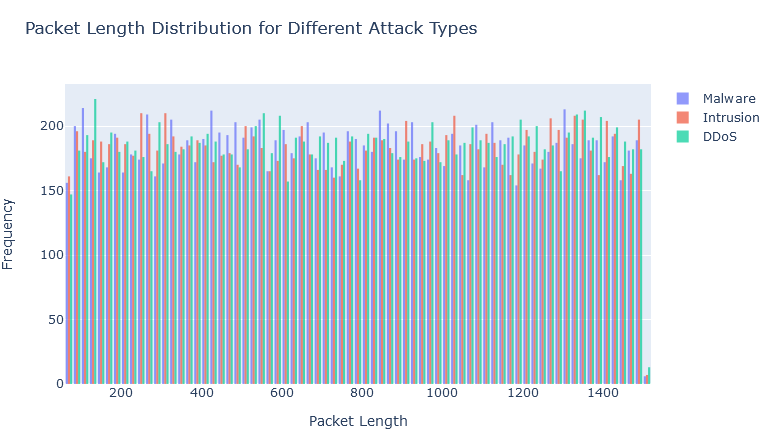
4: User Authentication Attempts

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.