Sentinel: AI-Powered Threat Intelligence - Team XGBoosted

Chan Ding Hao
Hoo Kai Sng
Lew Choon Hean
Yip Kai Men

TABLE OF CONTENTS

01

PROBLEM STATEMENT

Addressing the **pain points** of ISD personnel

ISD's Mission

1. Countering **Terrorism** and **Violent Extremism**
2. Guarding against **Espionage**
3. Contending with **Communalism**
4. **Cybersecurity** threats and risks

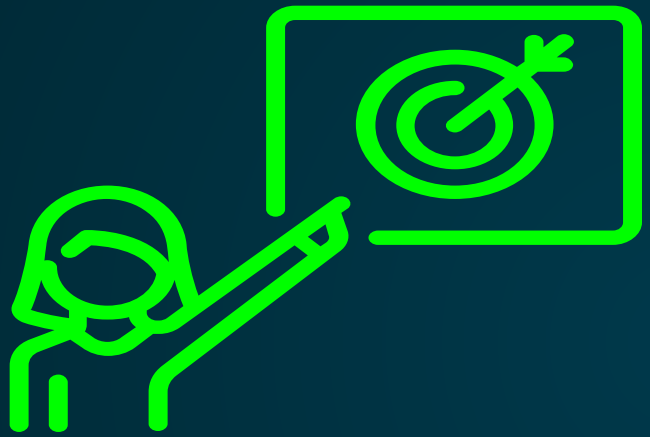
Abbreviated as TCCE

ISD

- ISD's mission to protect Singapore from **TCCE** threats shapes our approach to developing Sentinel
- Ensuring our solution extracts information in these key areas for effective threat detection and analysis

Source : https://www.mha.gov.sg/isd/keeping-threats-at-bay

User Personas



ISD Research Analyst

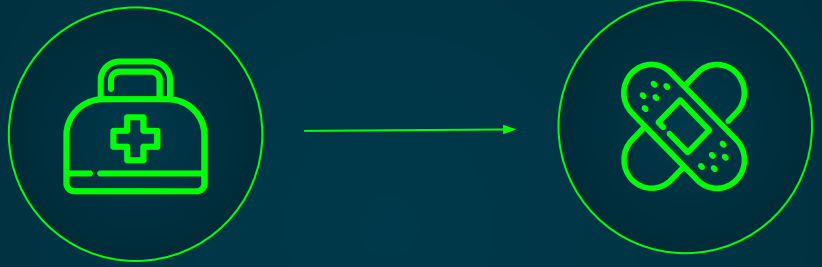
- Extracts and analyzes intelligence from security trends.
- Assesses policies to safeguard Singapore's security.
- ISD analysts need to analyse data that reflects the true security landscape.

Source :https://www.mha.gov.sg/isd/be-part-of-isd/career-opportunities

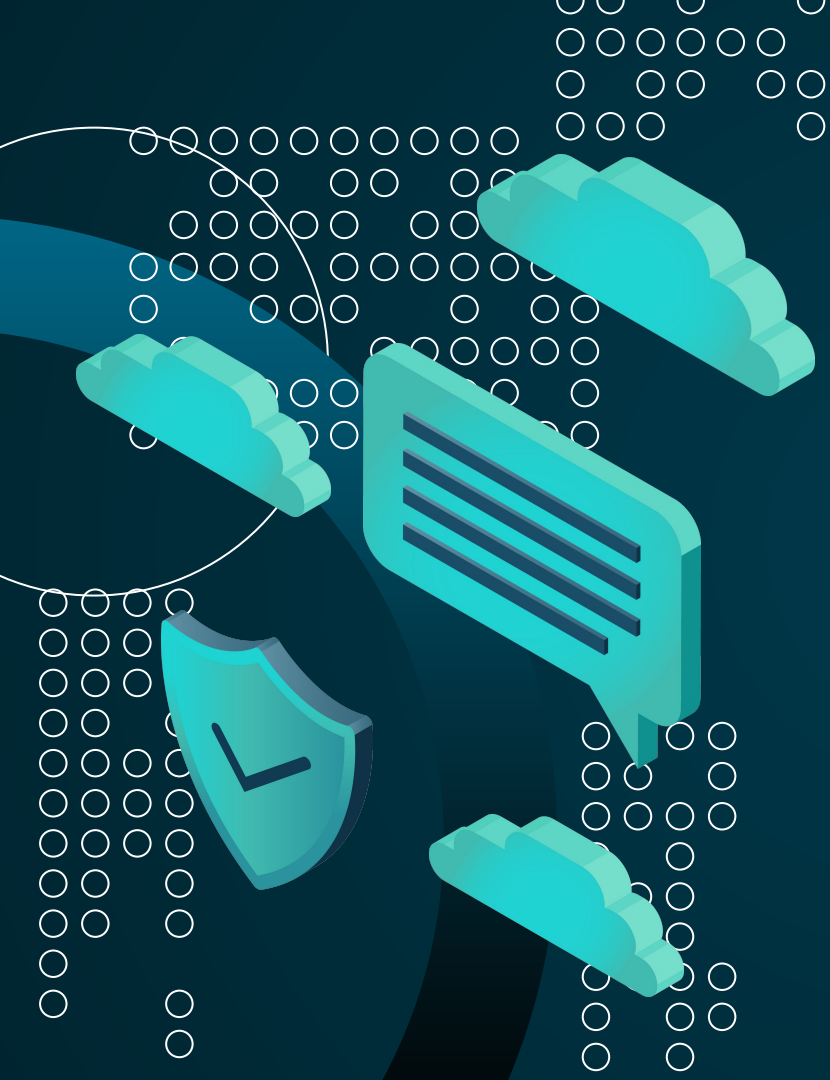
Pain Points : ISD Research Analyst

- Large volumes of unstructured data make manual analysis very **inefficient**.
- Extracting insights from text data manually is **slow and resource-intensive**.
- Manual processing increases the risk of **missing critical intelligence**.
- Threat identification requires rapid response, making **manual methods impractical**.

Triage

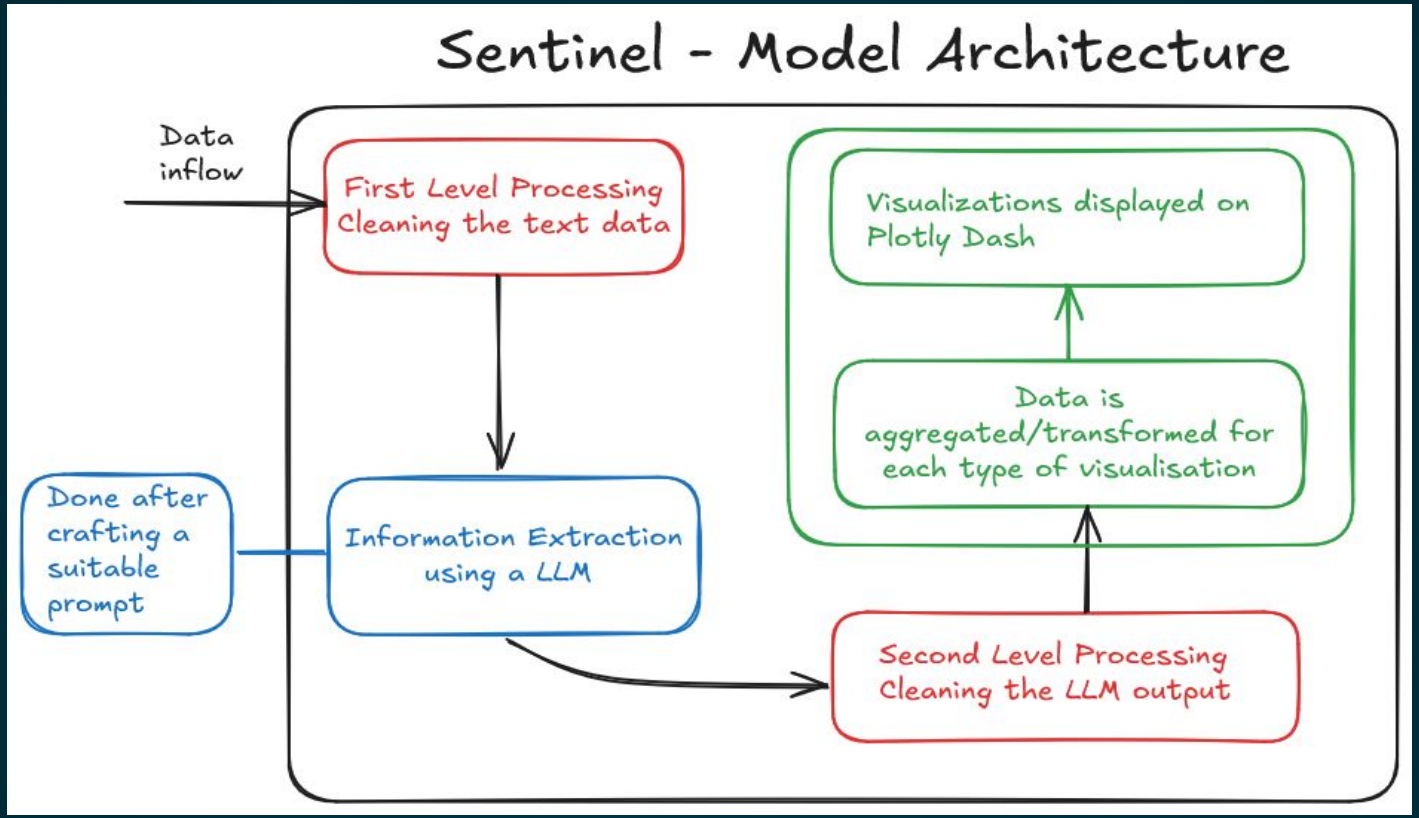


AI driven solution **resolves all pain points**



02

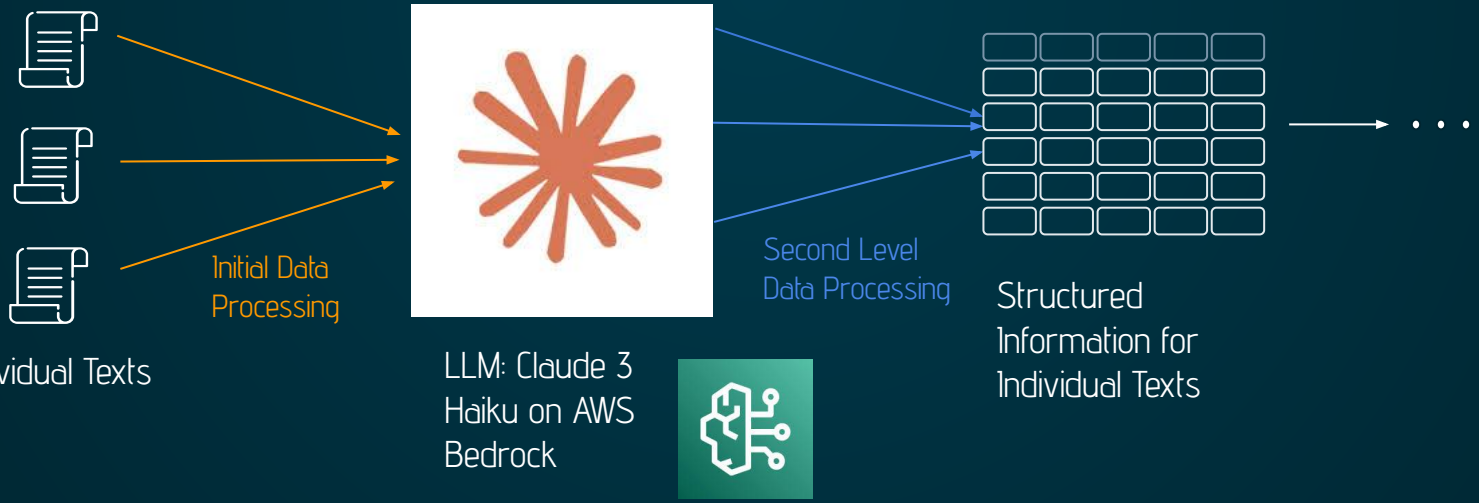
Solution


Sentinel - Model Architecture
Data inflow
First Level Processing Cleaning the text data
Visualizations displayed on Plotly Dash
Data is aggregated/transformed for each type of visualisation
Done after crafting a suitable prompt
Information Extraction using a LLM
Second Level Processing Cleaning the LLM output

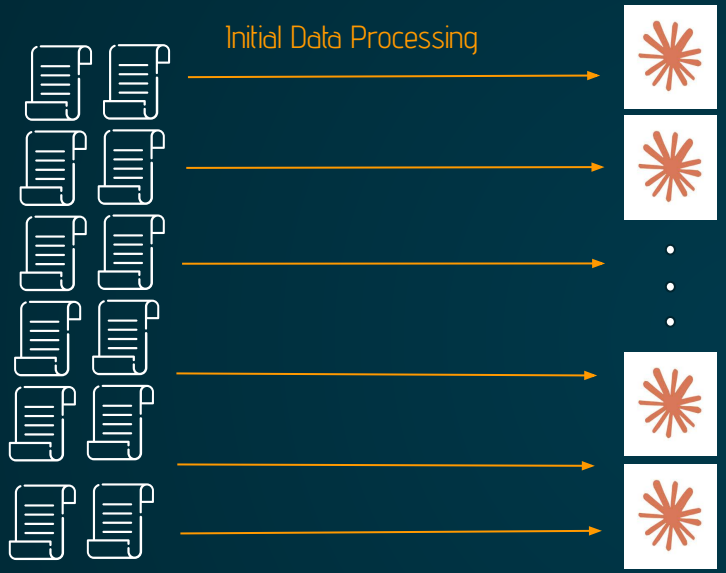
Extract Structured Data Using LLM

Prompt

You are an assistant helping Singapore's Internal Security Department (ISD) in categorizing texts into 0 to 4 critical areas of concern: Espionage, Terrorism and Violent Extremism, Cybersecurity, and Communalism. Return the data in the following JSON format ...



Scalability - Parallel Process



- Sentinel can be scaled
- Process larger amounts of data
- Multiple LLMs running at once

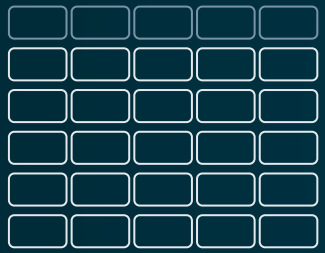
Scalability - Cost

Our costs for running the model during this hackathon on all texts (from AWS Cost Manager)

- Extremely cheap - US$0.55 for running all of the datathon text using LLM on AWS Bedrock
- Scaling with multiple models is cost effective

Aggregation / Transformation

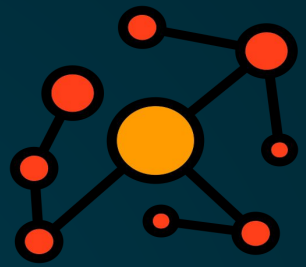
Terrrorism	Communalism	Cybersec	Espionage	Date
T	F	F	F	2022
F	T	T	F	2021
T	F	F	T	2024
F	T	F	T	2024
F	T	T	T	2024



Structured Information for Individual Texts

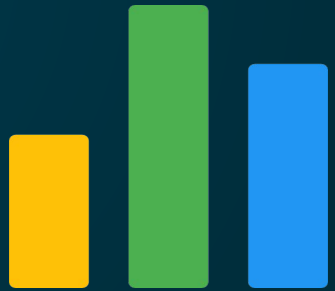
Data Transformation for Visualisations

Breadth First Search



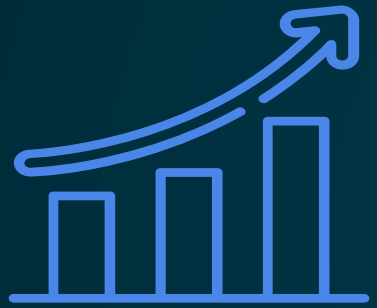
Network Graph

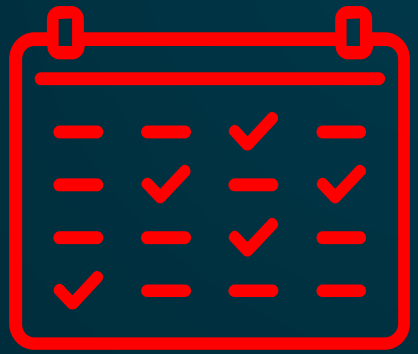
Aggregation



Bar Graph

Visualisations





Visualisation - Plotly Dash

Python framework for building interactive dashboards.

- Traditional Front End Tech Stack: JavaScript (JS), JS Framework (Node, React, etc), HTML, CSS, ...
- Plotly Tech Stack - Only Python
- Dynamic & interactive – supports real-time updates and user inputs.
- Open Source and Free

Visualisation - Cost

Comparison against other commonly used no code dashboarding tools

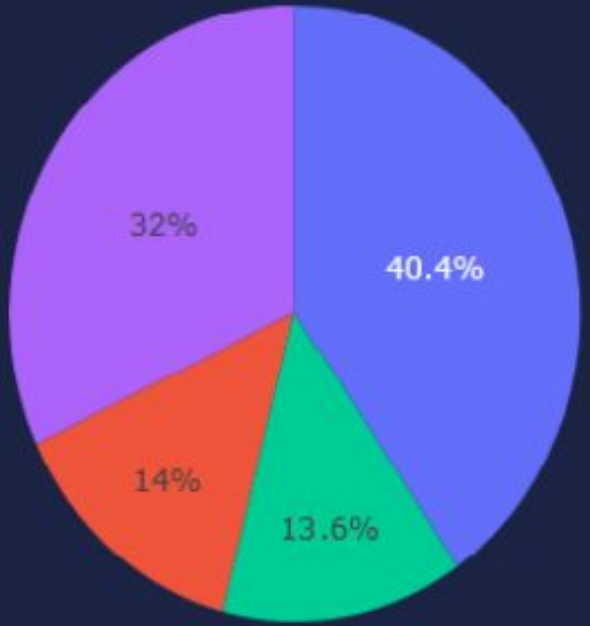
Visualisation Tool	Monthly Cost (US$ Per User)	Annual Cost (US$ Per User)
Plotly Dash	0	0
Tableau Enterprise	75	900
PowerBI Enterprise	24	288

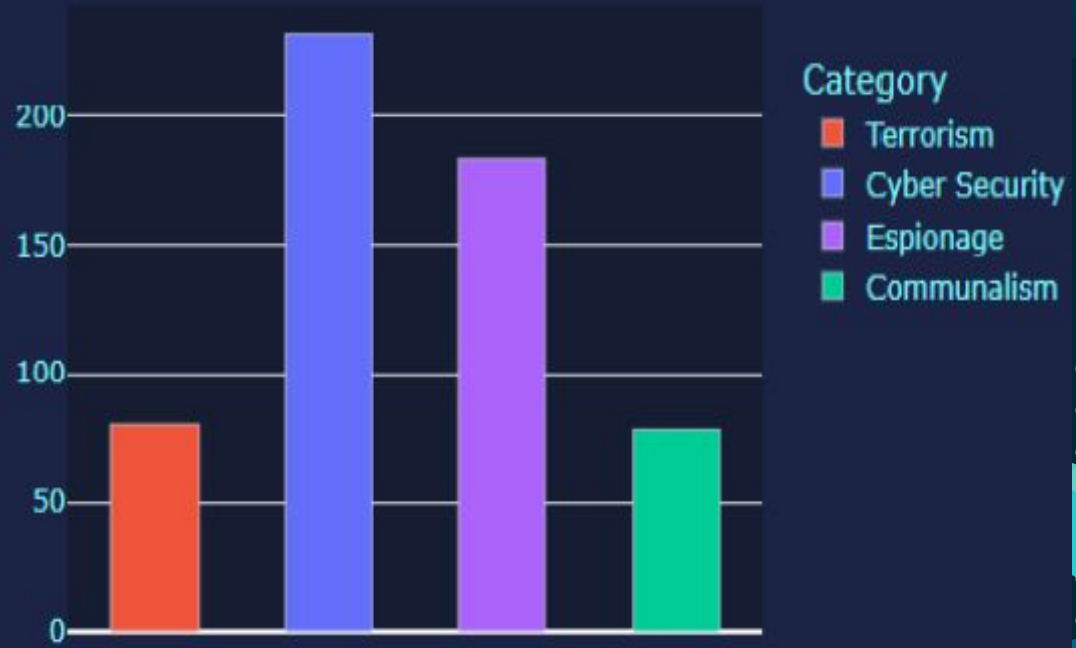
- Plotly Dash is free for many users
- Each unique user requires a product key that needs to be paid for
- Costs will scale for tools like Tableau and PowerBI

Sources :
www.tableau.com/pricing
www.microsoft.com/en-us/power-platform/products/power-bi/pricing

Geospatial Threat Heatmap

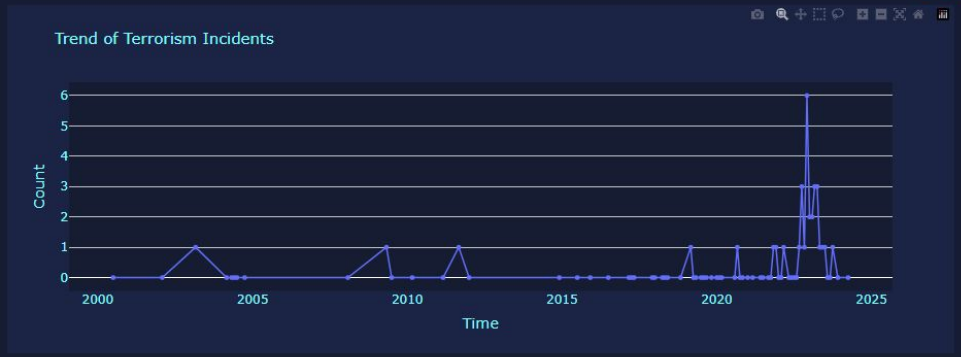
Geospatial Threat Heatmap

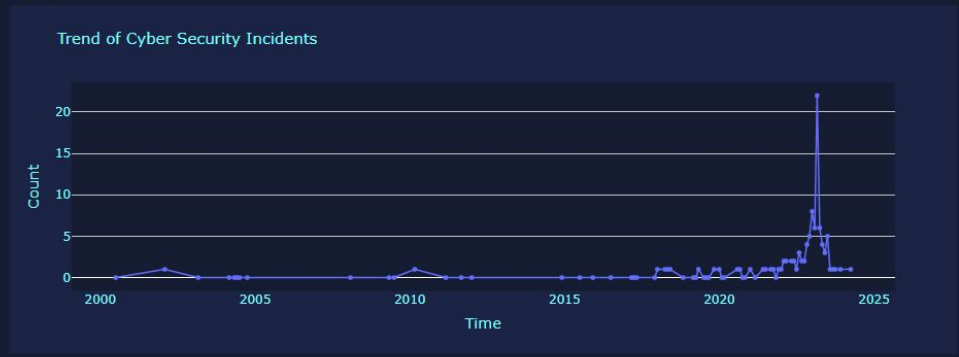

32%
40.4%
14%
13.6%

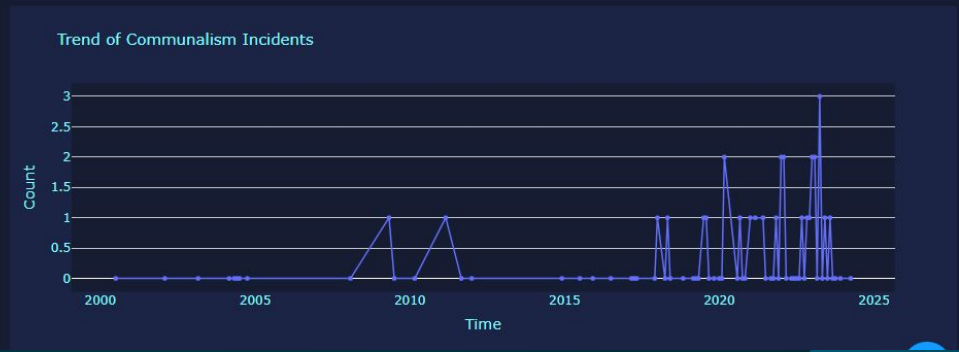

200
150
100
50
0
Category
Terrorism
Cyber Security
Espionage
Communalism

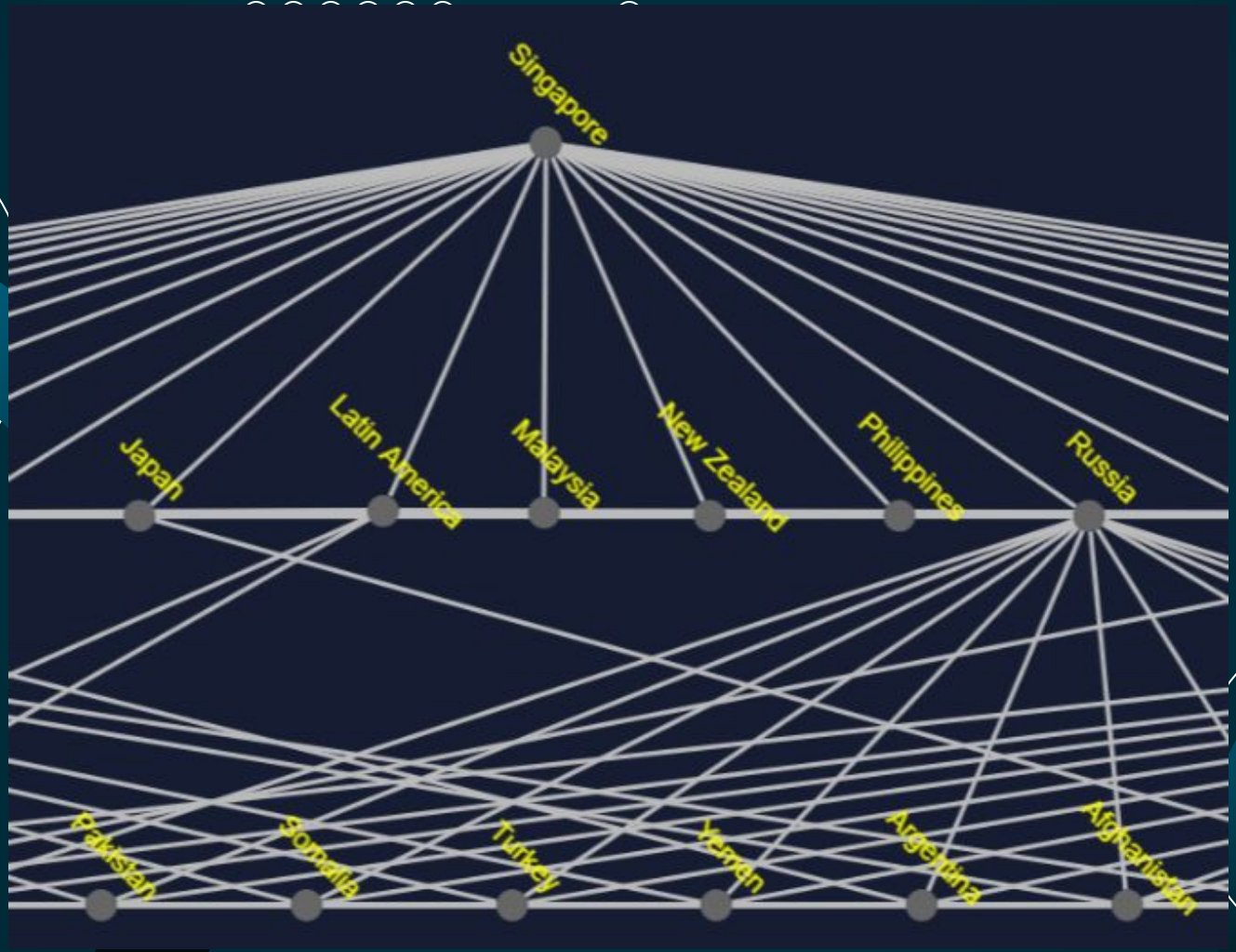
Trend Analysis Over Time

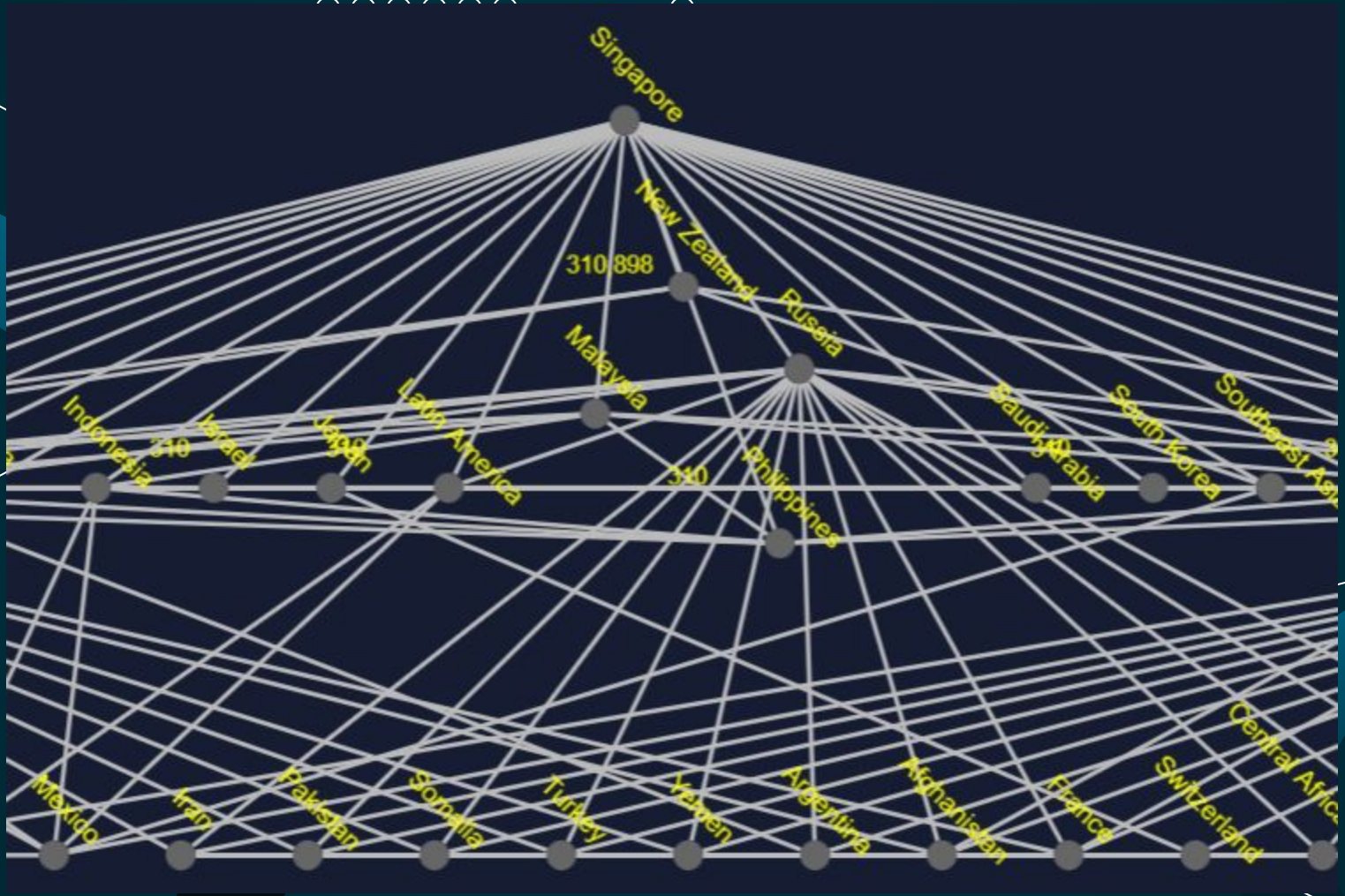
News Leaks








Singapore
Japan
Latin America
Malaysia
New Zealand
Philippines
Russia
Pakistan
Somalia
Turkey
Yemen
Argentina
Afghanistan


Singapore
New Zealand
310 898
Rusia
Malaysia
Latin America
Indonesia
Israel
Japan
310
310
Philippines
Saudi Arabia
South Korea
Mexico
Iran
Pakistan
Somalia
Turkey
Yemen
Argentina
Afghanistan
France
Switzerland

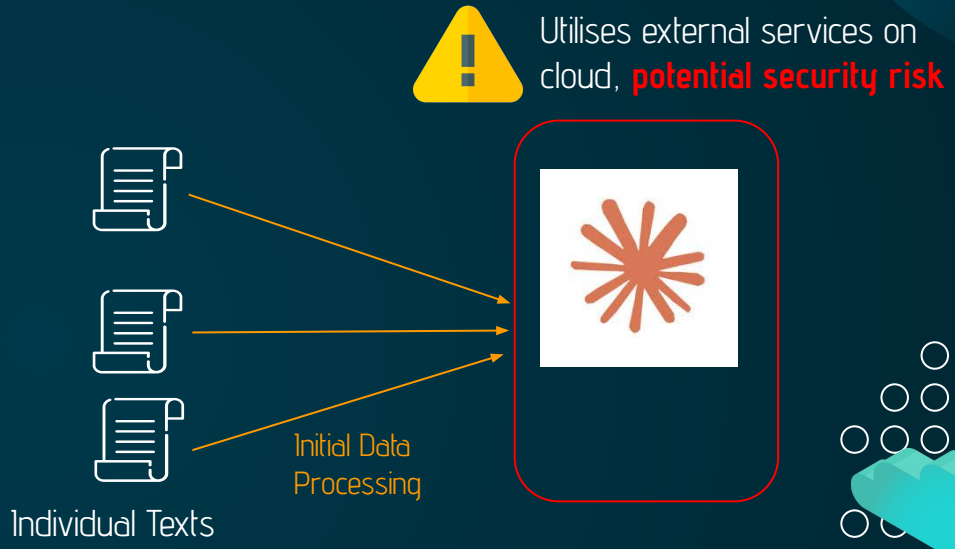
03

Future Improvements

Safety and Security

Part of the pipeline utilises AWS and Anthropic services. This comes with some risks.

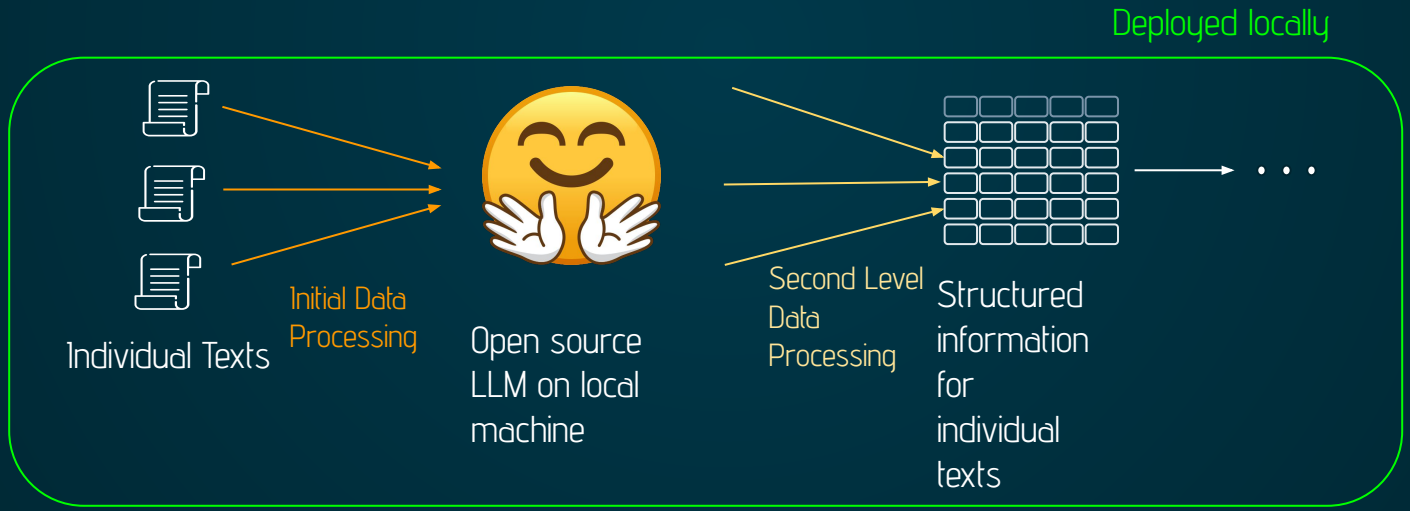
- Anthropic/AWS may utilise sensitive ISD documents for LLM training data.
- Reliance on AWS for service continuity is not ideal. Outages could happen that could disrupt monitoring.



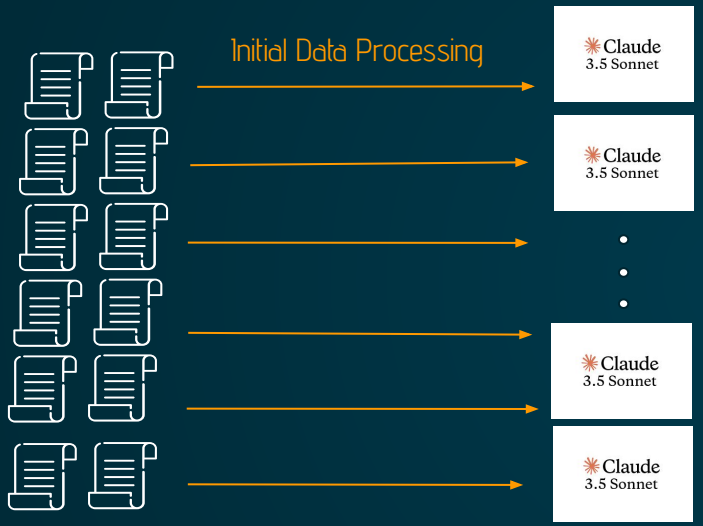
Resolving Safety Security Concerns

Solution? Deploy locally -

- LLMs can be downloaded onto a computer, e.g. Hugging Face
- Cannot use Anthropic models locally (Public endpoints/Not open-source)
- Scripts to process data can run on the same PC
- Plotly Dash can be deployed locally for secure access.

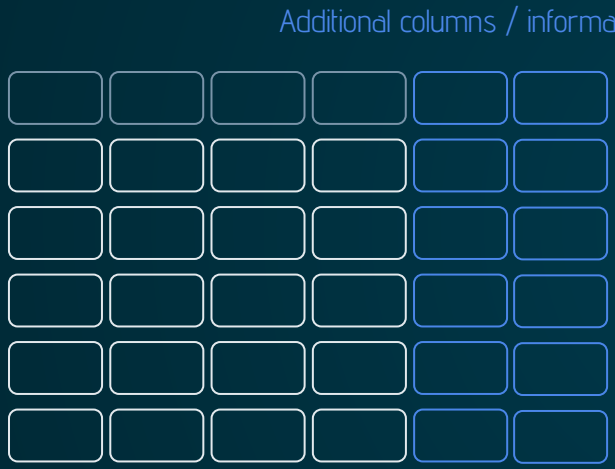


Upgrade LLM



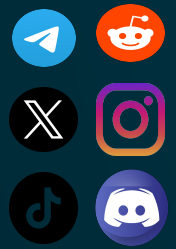
- Could consider more powerful models like Claude 3.5 Sonnet
- Better at extracting data
- Many options available - Hugging Face, DeepSeek R1 etc

Customizability



- Additional information can be requested from the LLM to augment existing analyses
- E.g. Risk score to Singapore - **1 (low)** to **5 (immediate danger)**
- Information can be highlighted in visualisations (e.g. edges on Network Graph) for immediate action.

Expand Data Sources



- Datathon only provided 2 data sources - News Excerpts and WikiLeaks Documents
- Include more news articles from multiple global sources.
- Include official government and company documents.
- Social Media monitoring dashboards to detect potential threats

04

Conclusion

Benefits of Sentinel

- Low Cost - US$0.55 for 1553 texts/documents
- Scalable - Solution can accommodate larger datasets
- Security - Entire pipeline can be ran in an isolated environment
- Reproducibility - All tools are open source, requires only a good understanding of Python

All pain points addressed

1. ~~Large volumes of unstructured data make manual analysis very inefficient~~.
2. ~~Extracting insights from text data manually is slow and resource-intensive~~.
3. ~~Manual processing increases the risk of missing critical intelligence~~.
4. ~~Threat identification requires rapid response, making manual methods impractical~~.

1. Leveraged LLM on AWS to parse large volumes of text, improving efficiency.
2. Enabled ISD Research Analysts to focus on higher-value tasks instead of manual text review.
3. Generated structured data from text and visualise data on a Dashboard enable quick identification of key intelligence.
4. Minimised missed critical insights with comprehensive data extraction.

THANK YOU!

Any questions?

References

1. https://www.mha.gov.sg/isd/keeping-threats-at-bay
2. https://www.mha.gov.sg/isd/be-part-of-isd/career-opportunities
3. Logos : https://www.flaticon.com/
4. www.tableau.com/pricing
5. www.microsoft.com/en-us/power-platform/products/power-bi/pricing

Resources

Did you like the resources on this template? Get them for free at our other websites:

PHOTOS:

- Close up programmer typing on keyboard
- Close up programmer sitting at desk
- Above view woman typing on laptop
- Cyber security concept with computer close up
- Close up programmer typing on keyboard
- Portrait of young woman with afro dreadlocks posing outside
- Medium shot smiley man sitting at desk

VECTORS:

- Cyber security instagram stories template

Instructions for use

If you have a free account, in order to use this template, you must credit **Slidesgo** by keeping the **Thanks** slide. Please refer to the next slide to read the instructions for premium users.

As a Free user, you are allowed to:

- Modify this template.
- Use it for both personal and commercial projects.

You are not allowed to:

- Sublicense, sell or rent any of Slidesgo Content (or a modified version of Slidesgo Content).
- Distribute Slidesgo Content unless it has been expressly authorized by Slidesgo.
- Include Slidesgo Content in an online or offline database or file.
- Offer Slidesgo templates (or modified versions of Slidesgo templates) for download.
- Acquire the copyright of Slidesgo Content.

For more information about editing slides, please read our FAQs or visit our blog:
https://slidesgo.com/faqs and **https://slidesgo.com/slidesgo-school**

Instructions for use (premium users)

As a Premium user, you can use this template without attributing **Slidesgo** or keeping the "**Thanks**" slide.

You are allowed to:

- Modify this template.
- Use it for both personal and commercial purposes.
- Hide or delete the “Thanks” slide and the mention to Slidesgo in the credits.
- Share this template in an editable format with people who are not part of your team.

You are not allowed to:

- Sublicense, sell or rent this Slidesgo Template (or a modified version of this Slidesgo Template).
- Distribute this Slidesgo Template (or a modified version of this Slidesgo Template) or include it in a database or in any other product or service that offers downloadable images, icons or presentations that may be subject to distribution or resale.
- Use any of the elements that are part of this Slidesgo Template in an isolated and separated way from this Template.
- Register any of the elements that are part of this template as a trademark or logo, or register it as a work in an intellectual property registry or similar.

For more information about editing slides, please read our FAQs or visit our blog:
https://slidesgo.com/faqs and **https://slidesgo.com/slidesgo-school**

Fonts & colors used

This presentation has been made using the following fonts:

Alumni Sans Pinstripe
(https://fonts.google.com/specimen/Alumni+Sans+Pinstripe)

Roboto Slab
(https://fonts.google.com/specimen/Advent+Pro)

Storyset

Create your Story with our illustrated concepts. Choose the style you like the most, edit its colors, pick the background and layers you want to show and bring them to life with the animator panel! It will boost your presentation. Check out **how it works**.

Pana

Amico

Bro

Rafiki

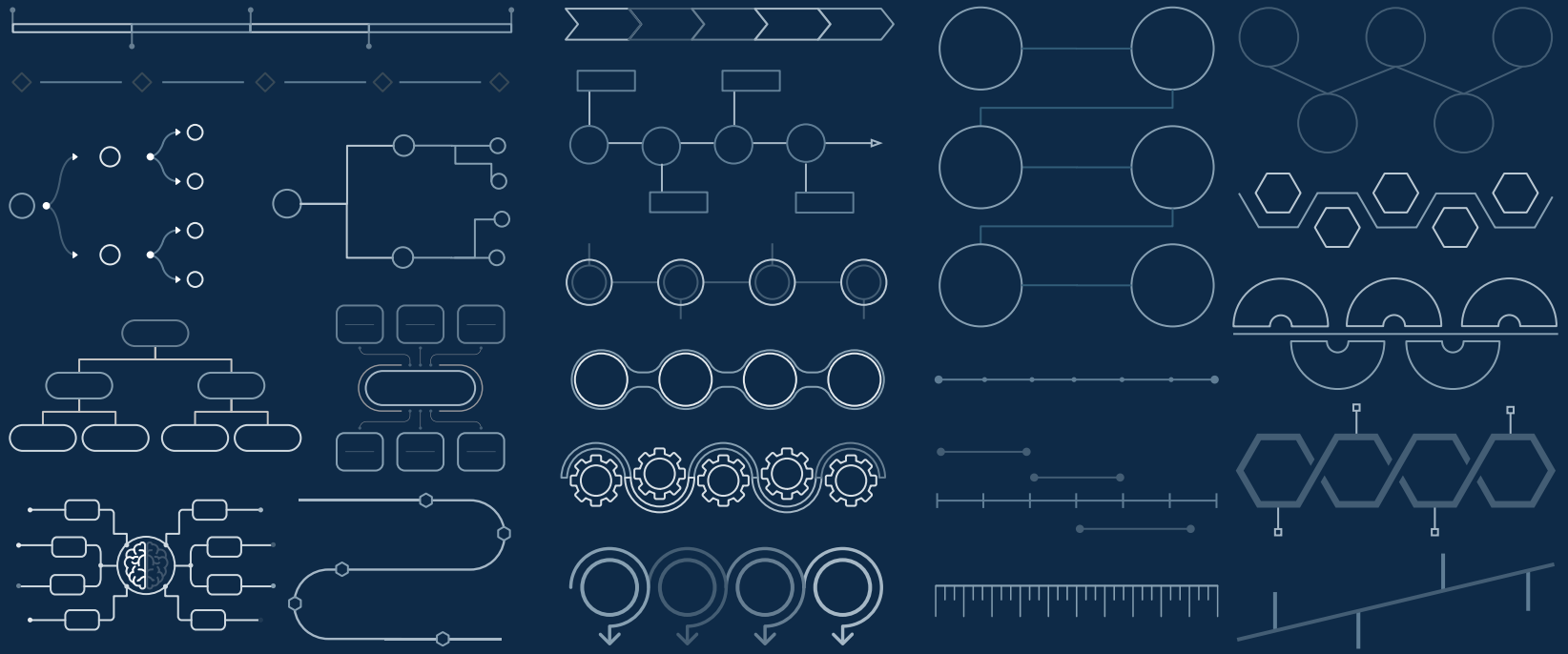
Cuate

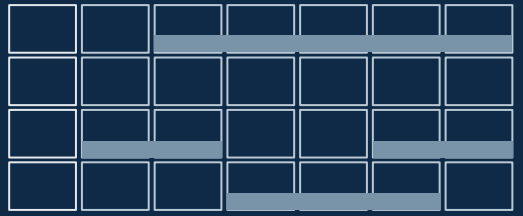
Use our editable graphic resources...

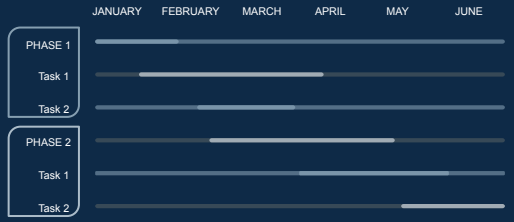
You can easily **resize** these resources without losing quality. To **change the color**, just ungroup the resource and click on the object you want to change. Then, click on the paint bucket and select the color you want. Group the resource again when you're done. You can also look for more **infographics** on Slidesgo.

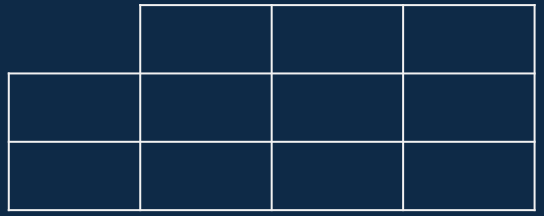


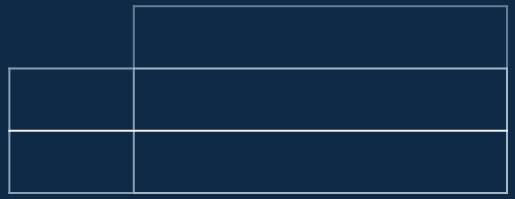


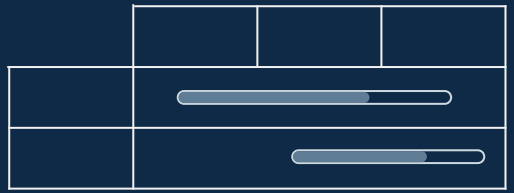



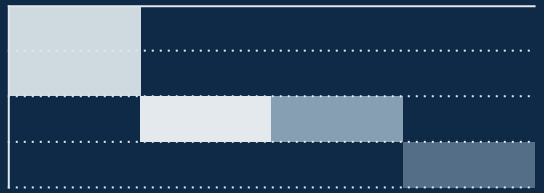


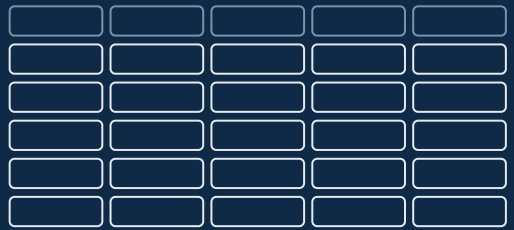

JANUARY
FEBRUARY
MARCH
APRIL
MAY
JUNE
PHASE 1
Task 1
Task 2
PHASE 2
Task 1
Task 2

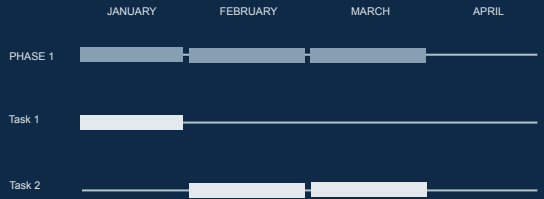


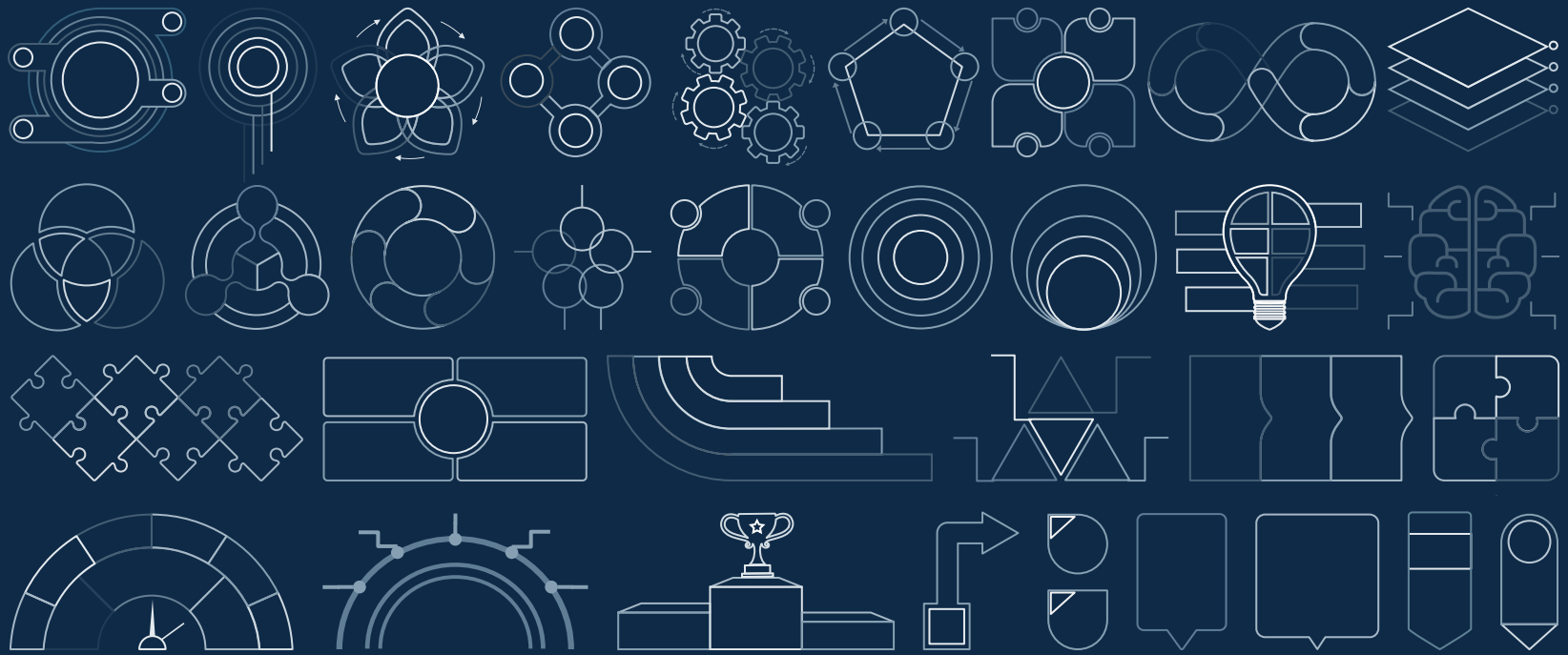


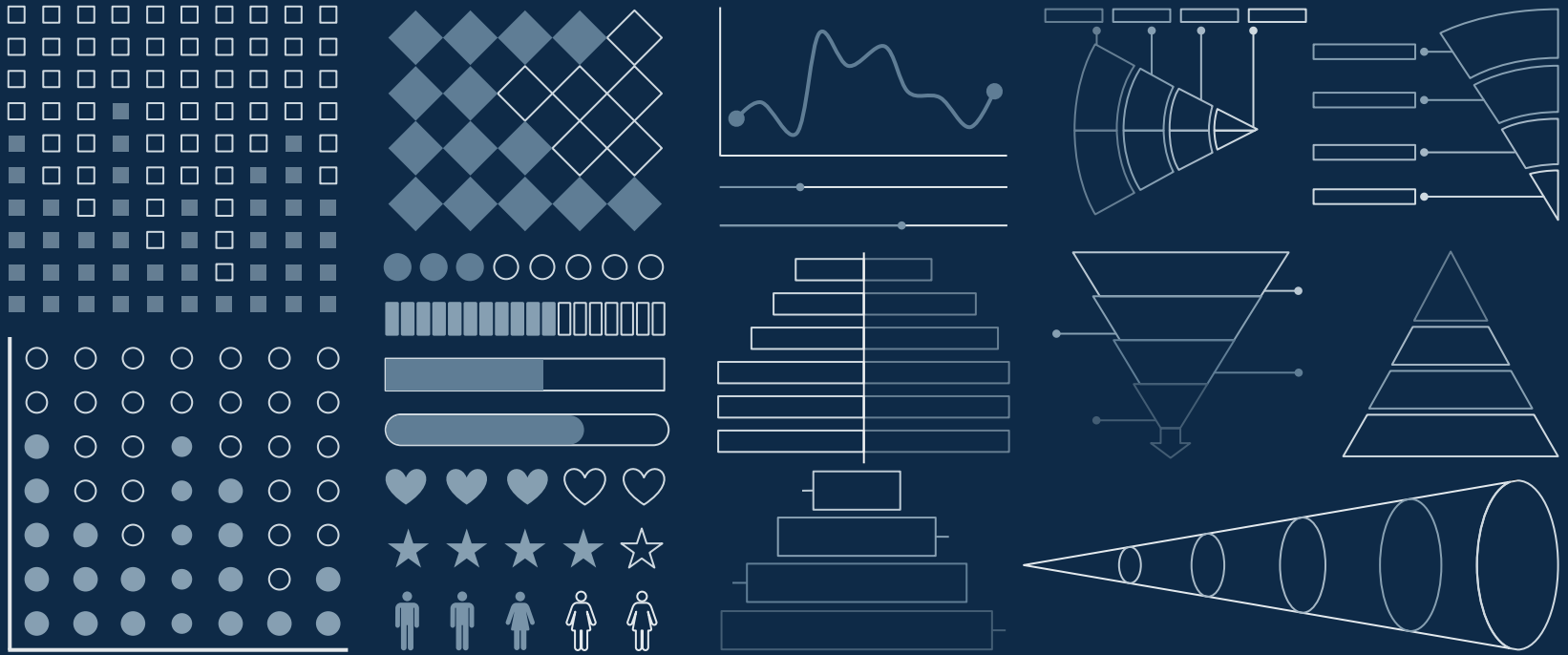







JANUARY
FEBRUARY
MARCH
APRIL
PHASE 1
Task 1
Task 2





...and our sets of editable icons

You can **resize** these icons without losing quality.
You can **change the stroke and fill color**; just select the icon and click on the **paint bucket/pen**.
In Google Slides, you can also use **Flaticon's extension**, allowing you to customize and add even more icons.

Educational Icons

Medical Icons

Business Icons

Teamwork Icons

Help & Support Icons

Avatar Icons

Creative Process Icons

Performing Arts Icons

Nature Icons

SEO & Marketing Icons


slidesgo