



An Integrated Framework for Privacy-Preserving Based Anomaly Detection for Cyber-Physical Systems

Presented by Miles Grant

Authors

01

Marwa Keshk

Commonwealth Scientific and
Industrial Research
Organisation, Australia

02

Elena Sitnikova

Flinders University

03

Nour Moustafa

University of New South Wales:
Canberra

04

Jiankun Hu

University of New South Wales:
Canberra

05

Ibrahim Khalil

RMIT University

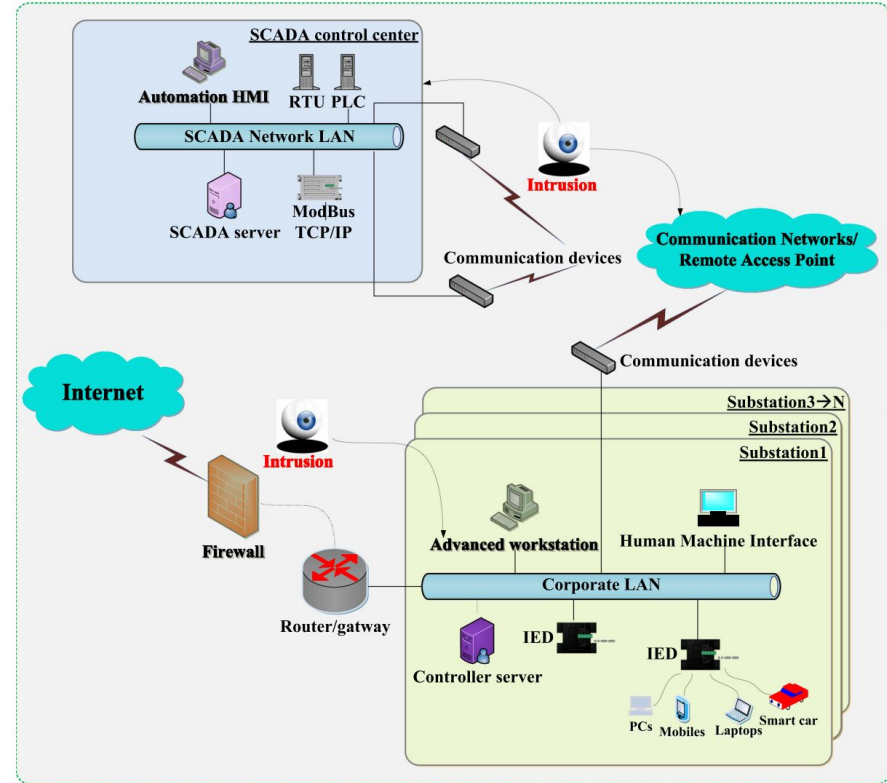
01

BACKGROUND



Background

- SCADA – Supervisory Control and Data Acquisition
- SCADA systems are responsible for controlling and monitoring cyber-physical systems
- SCADA systems are an obvious target for attacking critical infrastructure like power grids or pipelines



Privacy Preservation in CPSs

- Privacy preservation is “the process of protecting original information against being published or revealed by unauthorised users”
- Generalization, transformation, aggregation
- Intrusion Detection Systems (IDS)
 - Misuse vs Nomaly-based

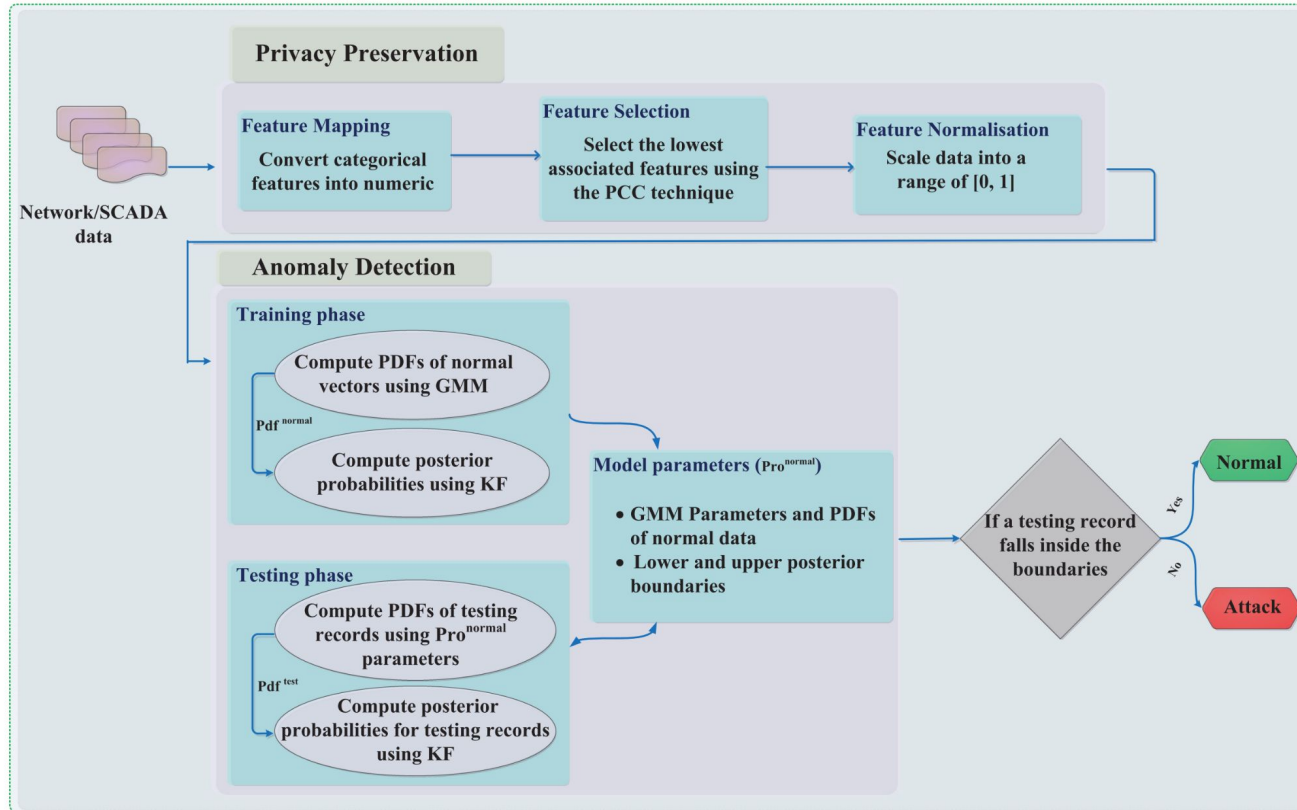


02

FRAMEWORK



Proposed Framework



Data Pre-Processing

- Mapping categorical features to numeric values
- Removing irrelevant features using PCC technique
- Normalizing features to values between 0 and 1
- This process minimizes data leaks and obscures features

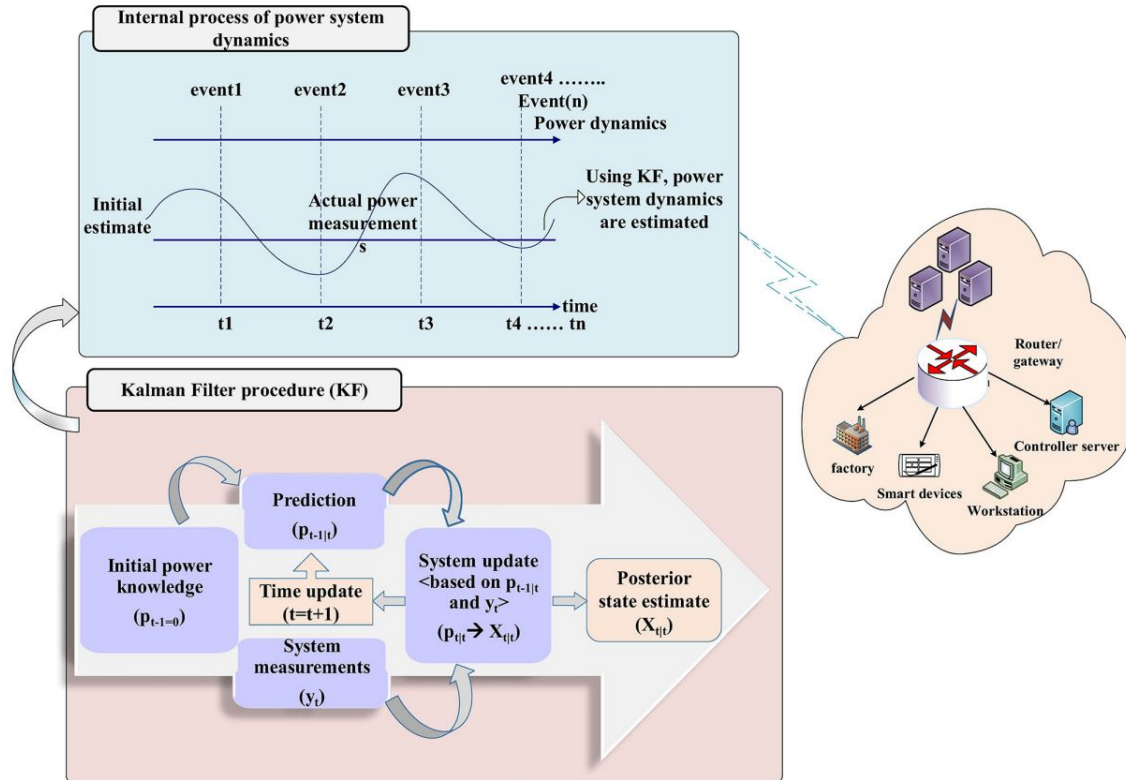


Anomaly Detection

- Gaussian Mixture Model
 - Probabilistic model for handling and representing multivariate data
- Kalman Filter
 - Commonly used algorithm for detecting outliers and anomalies in a dataset



Power System State Estimation with KF



| ct_dst_sport_ltm | dwin | ct_dst_src_ltm | Service | Service_Num | Label |
|------------------|------|----------------|----------|-------------|--------|
| 1 | 0 | 2 | smtp | 1 | Normal |
| 2 | 0 | 3 | dns | 2 | Normal |
| 3 | 0 | 4 | http | 3 | Normal |
| 6 | 0 | 3 | ftp-data | 5 | Normal |
| 3 | 0 | 1 | ssh | 4 | Normal |
| 4 | 0 | 5 | http | 3 | Normal |
| 5 | 255 | 6 | smtp | 1 | Attack |
| 8 | 255 | 5 | http | 3 | Attack |
| 9 | 255 | 2 | ssh | 4 | Attack |

B) Transformed and selected data

| ct | dst | sport | ltn | dwin | ct | dst | src | ltn | Service | Num |
|-------|-----|-------|-----|------|----|-----|-----|-----|---------|------|
| 0 | | | | 0 | | | 0.2 | | | 0 |
| 0.125 | | | | 0 | | | 0.4 | | | 0.25 |
| 0.25 | | | | 0 | | | 0.6 | | | 0.5 |
| 0.25 | | | | 0 | | | 0 | | | 0.75 |
| 0.625 | | | | 0 | | | 0.4 | | | 1 |
| 0.375 | | | | 0 | | | 0.8 | | | 0.5 |
| 0.5 | | | | 1 | | | 1 | | | 0 |
| 0.875 | | | | 1 | | | 0.8 | | | 0.5 |
| 1 | | | | 1 | | | 0.2 | | | 0.75 |

C) Parameters of GMM for the features of training set in B

| | ct_dst_sport_ltm | dwin | ct_dst_src_ltm | Service_Num |
|----------|------------------|------|----------------|-------------|
| Mean | 0.25 | 0 | 0.32 | 0.5 |
| Variance | 0.055 | 0 | 0.052 | 0.156 |
| Weight | 0.25 | 0.25 | 0.25 | 0.25 |


PCC for ranking features



D) PDFs for the feature vectors in B using the parameters in C

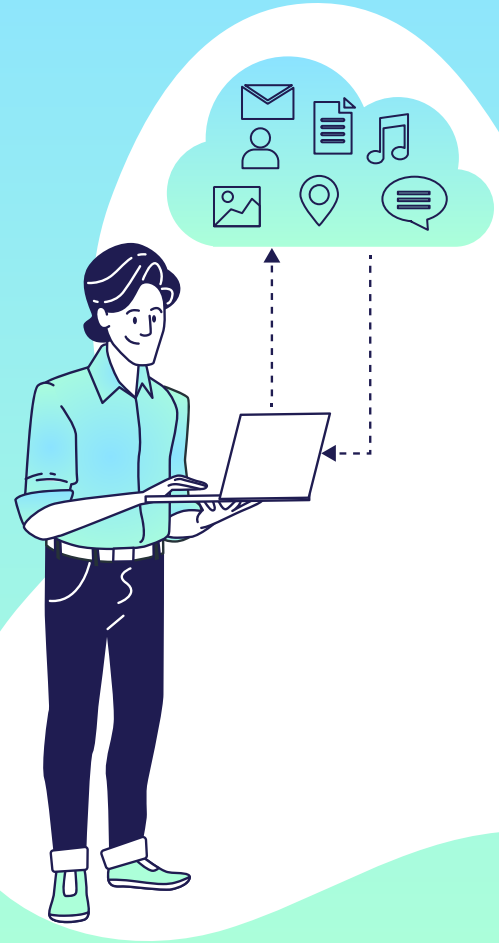
| PDFs |
|-------|
| 0.746 |
| 0.998 |
| 0.895 |
| 0.808 |
| 0.653 |
| 0.680 |
| 0.370 |
| 0.322 |
| 0.600 |

E) Posterior using Kalman Filter

| | | |
|-------|---|-------------------------------|
| 0.438 | | Normal training boundaries |
| 0.448 | Lower | 0.438 |
| 0.787 | Upper | 0.825 |
| 0.854 | | |
| 0.825 | | |
| | | Detection for testing records |
| 0.448 |  | Normal |
| 0.415 | | Attack |
| 0.384 | | Attack |
| 0.346 | | Attack |
| | | |

03

RESULTS



Datasets and Evaluation

- The researchers used two public benchmark datasets to evaluate their PPAD-CPS algorithm
 - Power System
 - UNSW-NB15
- Mixtures of normal, attack, and natural event data



Privacy Preservation Evaluation

- PPAD-CPS well outperforms several relevant privacy-preserving anomaly detection methods in terms of e privacy level (P_{index}), the dissimilarity level (DISS) and the information loss (IL).

TABLE 3
Comparison of Performances of Four Methods for Privacy Preservation and PPAD-CPS Framework on Both Datasets

| Privacy method | Power data | UNSW-NB15 | Power data | UNSW-NB15 | Power data | UNSW-NB15 |
|-----------------|-----------------|--------------|--------------|--------------|--------------|--------------|
| | $P_{index}(\%)$ | | $DISS(\%)$ | | $IL(\%)$ | |
| SDP | 27.83 | 32.67 | 42.31 | 52.90 | 35.87 | 42.72 |
| RDP | 43.56 | 46.16 | 52.45 | 54.61 | 57.41 | 59.16 |
| PPFSCADA | 51.33 | 58.89 | 49.73 | 58.75 | 52.14 | 56.43 |
| PCA-DR | 57.78 | 62.34 | 67.29 | 69.87 | 72.19 | 74.50 |
| PPAD-CPS | 67.43 | 81.35 | 68.87 | 73.52 | 75.20 | 79.16 |

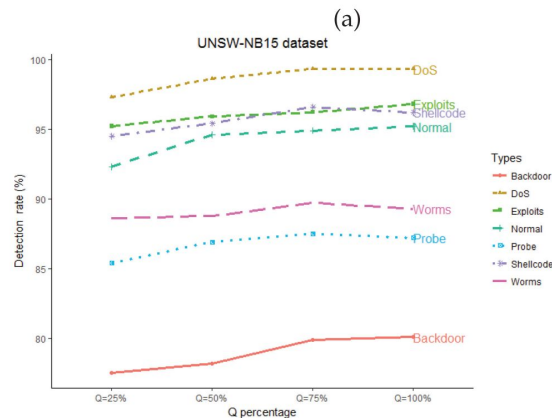
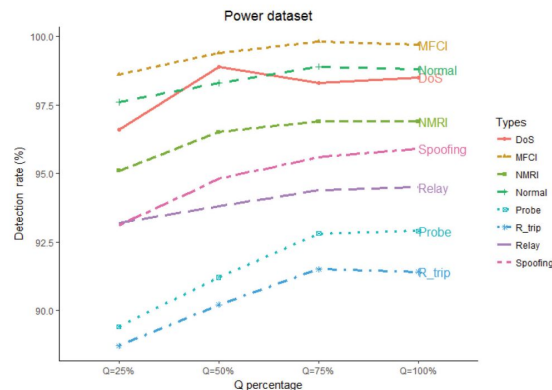
Performance on Different Attack Types

TABLE 5
DR (%) by Attack Class for Different Q Values of
Power System Dataset

| Class type | Power System data (Q) | | | |
|-------------|-----------------------|-------|-------|-------|
| | 25% | 50% | 75% | 100% |
| Normal | 97.63 | 98.32 | 98.90 | 98.86 |
| Probe | 89.40 | 91.26 | 92.83 | 92.91 |
| NMRI | 95.14 | 96.54 | 96.94 | 96.92 |
| Relay | 93.23 | 93.85 | 94.42 | 94.57 |
| Remote trip | 88.72 | 90.29 | 91.56 | 91.40 |
| Spoofing | 93.14 | 94.85 | 95.67 | 95.98 |
| MFCI | 98.60 | 99.42 | 99.82 | 99.73 |
| DoS | 96.68 | 98.90 | 98.36 | 98.57 |

TABLE 6
DR (%) by Attack Class for Different Q Values of
UNSW-NB15 Dataset

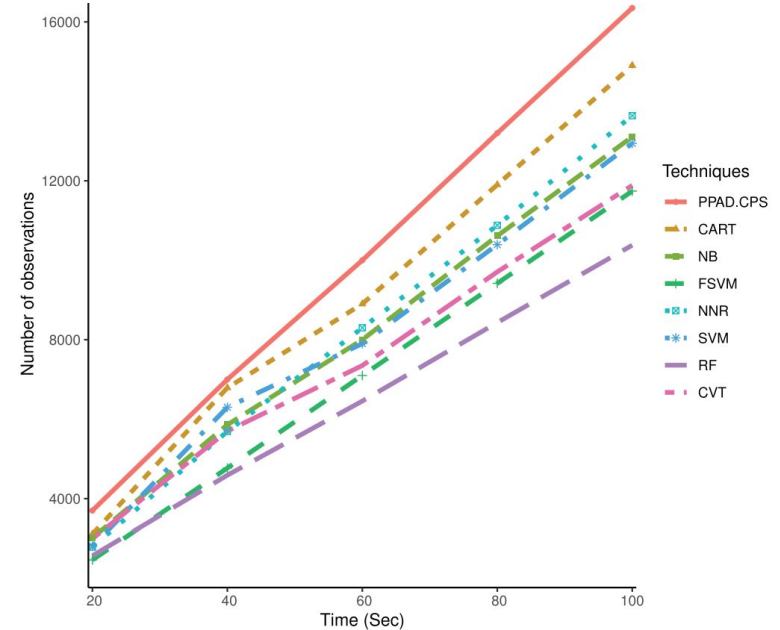
| Class type | UNSW-NB15 data (Q) | | | |
|------------|--------------------|-------|-------|-------|
| | 25% | 50% | 75% | 100% |
| Normal | 92.29 | 94.61 | 94.90 | 95.48 |
| Probe | 85.43 | 86.92 | 87.54 | 87.23 |
| Backdoor | 77.58 | 78.23 | 79.98 | 80.12 |
| DoS | 97.31 | 98.69 | 99.35 | 99.34 |
| Exploits | 95.24 | 95.93 | 96.23 | 96.56 |
| Shellcode | 94.59 | 95.40 | 96.67 | 96.28 |
| Worms | 88.63 | 88.88 | 89.72 | 89.37 |



Comparison of Performances

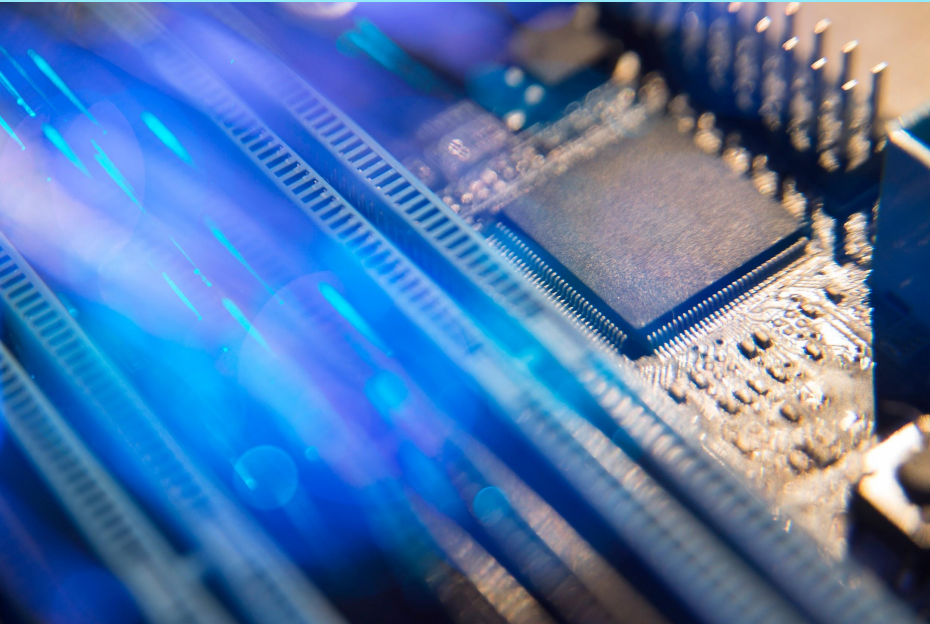
TABLE 7
Comparison of Performances of Seven Techniques
and PPAD-CPS Framework on Both Datasets

| | Datasets | | | |
|-----------|--------------|---------|-----------|---------|
| | Power System | | UNSW-NB15 | |
| Technique | DR (%) | FPR (%) | DR (%) | FPR (%) |
| CVT | 95.35 | 4.62 | 90.25 | 9.32 |
| RF | 92.26 | 7.49 | 89.76 | 10.15 |
| SVM | 91.80 | 7.68 | 90.57 | 8.72 |
| NNR | 89.42 | 9.27 | 85.68 | 10.51 |
| FSVM | 95.44 | 3.98 | 91.73 | 8.48 |
| NB | 81.95 | 16.23 | 75.01 | 24.36 |
| CART | 95.92 | 4.61 | 92.34 | 7.42 |
| PPAD-CPS | 96.26 | 3.52 | 93.71 | 6.75 |



Thanks for Listening!

Questions?



Discussion

How does privacy preservation improve the security of CPSs?

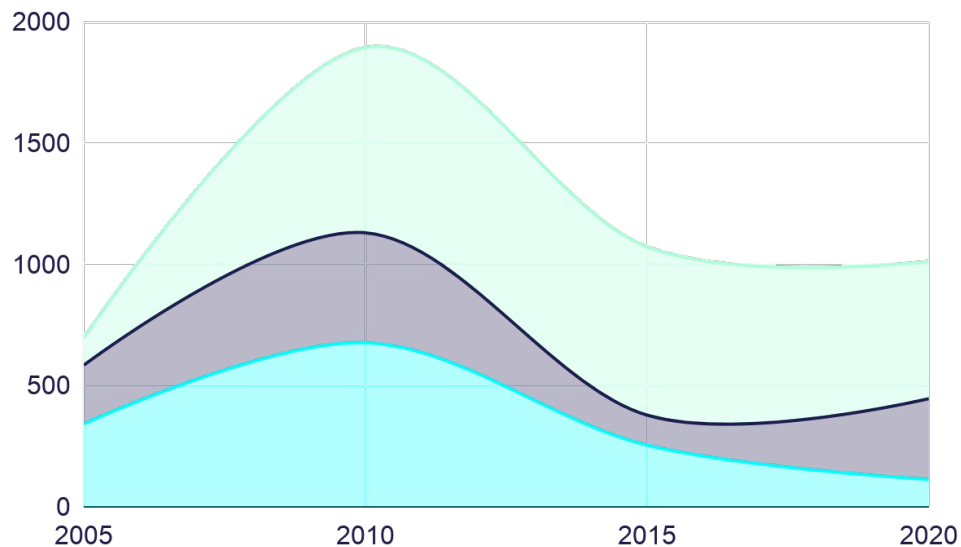
What information could still be leaked by CPSs using this algorithm?

OUR COMPANY



Mercury is the closest planet to the Sun and the smallest one in the Solar System—it's only a bit larger than the Moon

MARKET TRENDS

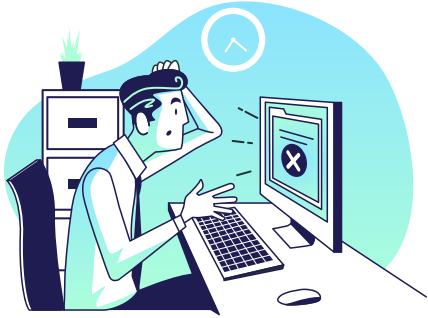


- Mars
- Saturn
- Venus

Edit this!

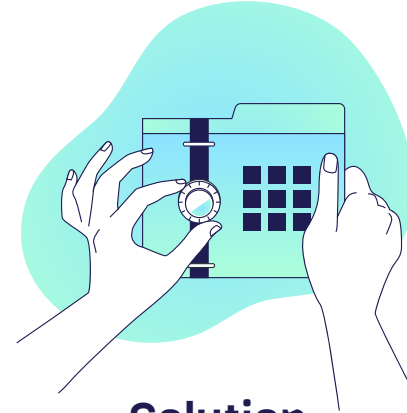
To modify this graph, click on it, follow the link, change the data and paste the resulting graph here

PROBLEM VS. SOLUTION



Problem

Mercury is the closest planet to the Sun and the smallest one in the Solar System—it's only a bit larger than the Moon



Solution

Venus has a beautiful name and is the second planet from the Sun. It's terribly hot and its atmosphere is poisonous

COMPETITORS



Mars

Despite being red, Mars is actually a cold place full of iron oxide



Jupiter

It's a gas giant and the biggest planet in the Solar System



Saturn

Saturn is a gas giant, composed mostly of hydrogen and helium

COMPETITIVE ADVANTAGE



Them

Mercury is the closest planet to the Sun and the smallest one in the Solar System

Us

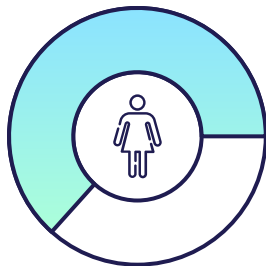
Jupiter is, the biggest planet in the Solar System and the fourth-brightest object in the sky

TARGET

60%

Women

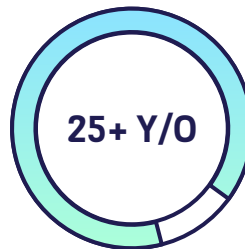
Saturn is a gas giant
and has rings



\$50K - \$60K

Average spend per customer

Mercury is the smallest planet in
the Solar System

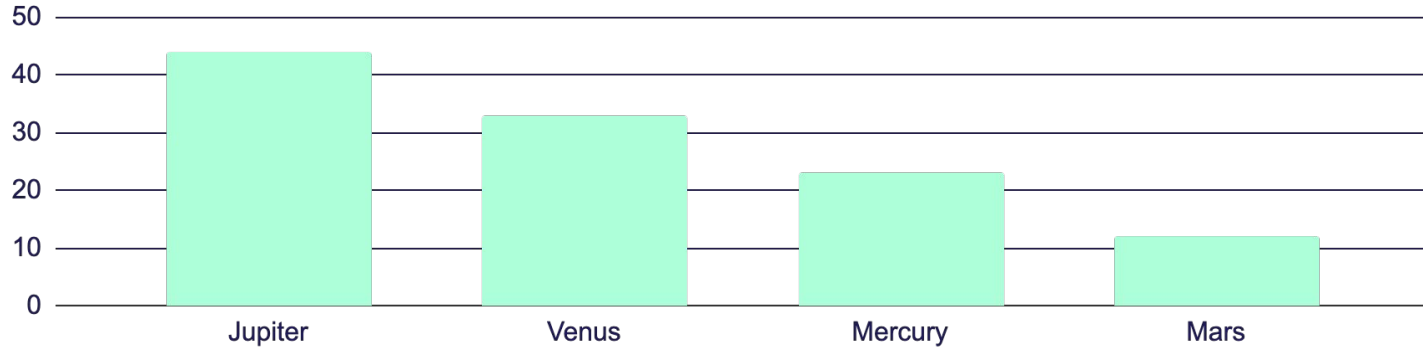


MARKET SIZE



MARKET SHARE

To modify this graph, click on it, follow the link, change the data and paste the new graph here



Jupiter

Jupiter is the biggest planet of them all

Mercury

Mercury is the closest planet to the Sun

Venus

Venus is the second planet from the Sun

Mars

Despite being red, Mars is a cold place

COMPETITION ANALYSIS

| Jupiter | Mercury | Venus | Mars |
|---------|---------|-------|------|
| Yes | No | Yes | No |
| Yes | No | Yes | Yes |
| No | Yes | No | Yes |



OUR SERVICES

Mercury

Mercury is the closest planet to the Sun

Venus

Venus is the second planet from the Sun

Mars

Despite being red, Mars is actually a cold place

Jupiter

It's the biggest planet in the Solar System

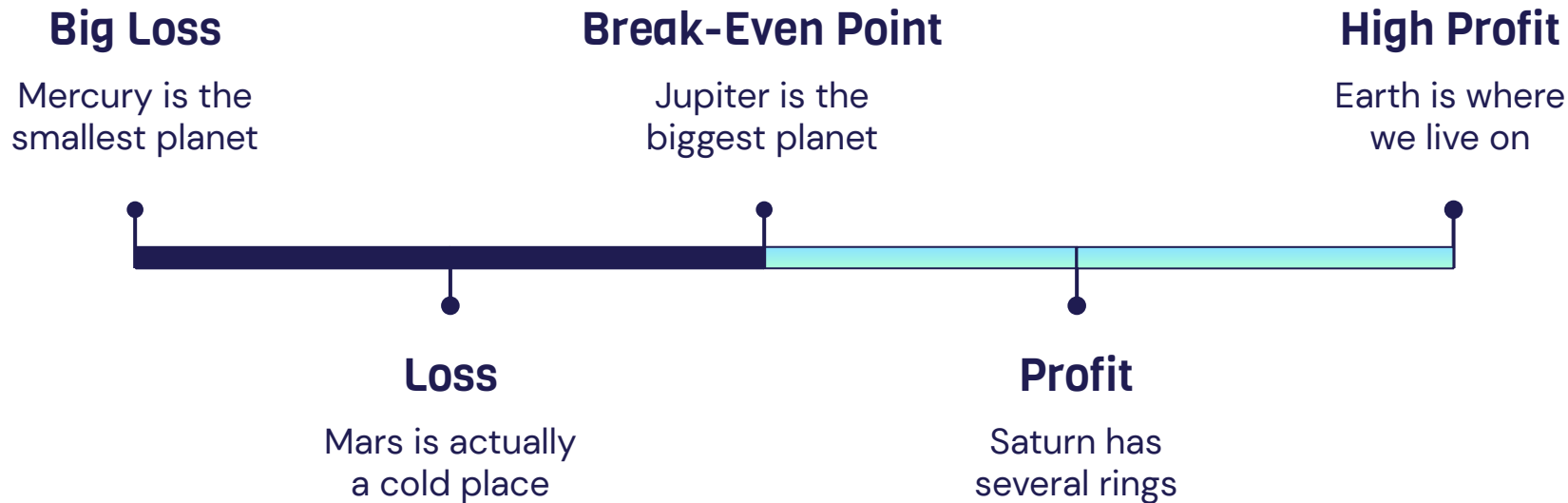
Saturn

Saturn is composed of hydrogen and helium

Neptune

Neptune is the farthest planet from the Sun

BREAK-EVEN ANALYSIS



OUR PLANS

BASIC

\$19.99

- Service 1
- Service 2
- Service 3

START

STANDARD

\$25.99

- Service 1
- Service 2
- Service 3

START

PREMIUM

\$30.99

- Service 1
- Service 2
- Service 3

START

SALES AND DISTRIBUTION



ADVERTISING AND PROMOTION



Advertising

Jupiter is a gas giant and the biggest planet in the Solar System



PR

Venus has a beautiful name and is the second planet from the Sun



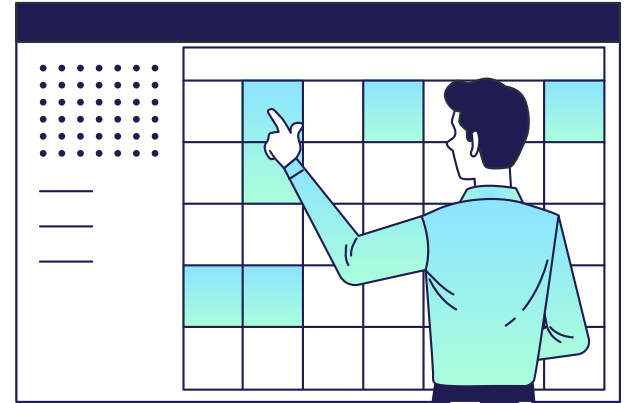
Online

Despite being red, Mars is actually a cold place full of iron oxide dust

04

MANAGEMENT PLAN

You could enter a subtitle
here if you need it



OUR TEAM

Albert Clifford

You can replace the image on the screen with your own

Joey Patterson

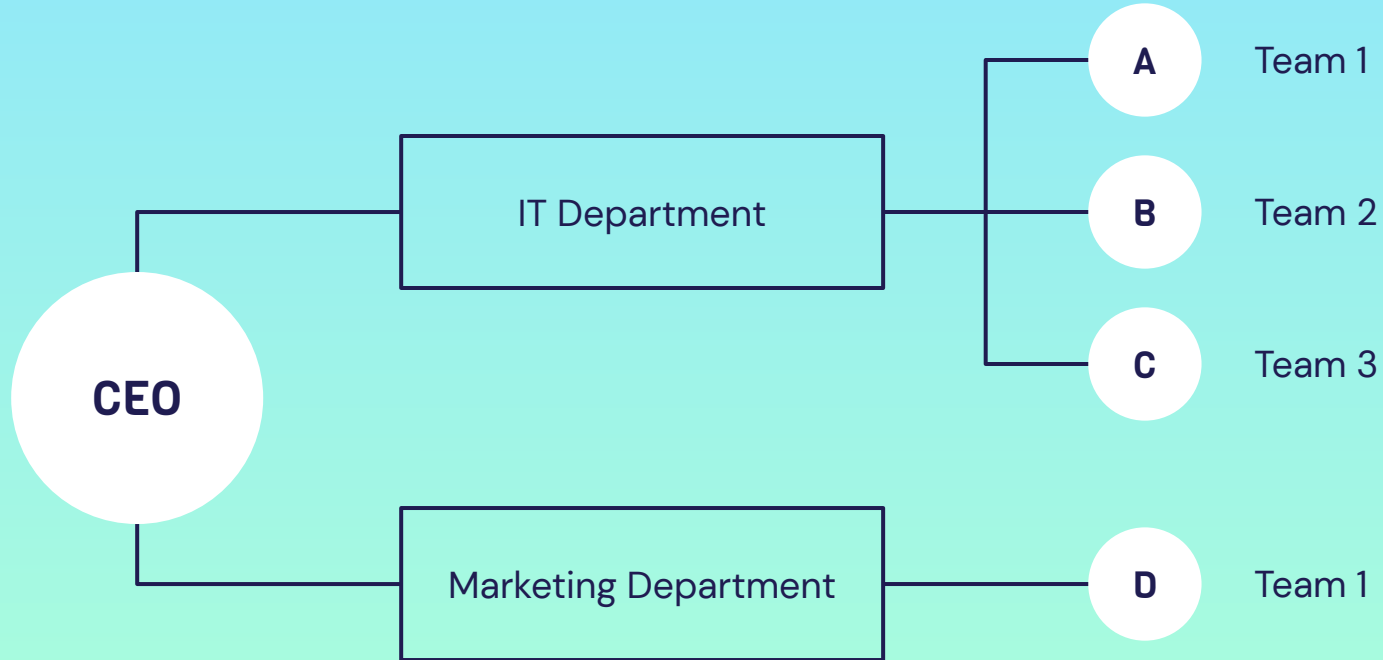
You can replace the image on the screen with your own

Laura Doe

You can replace the image on the screen with your own



ORGANIZATIONAL CHART



OUR PARTNERS

This is a list of partners

- Here you can talk about your partners
- Here you can talk about your partners
- Here you can talk about your partners
- Here you can talk about your partners

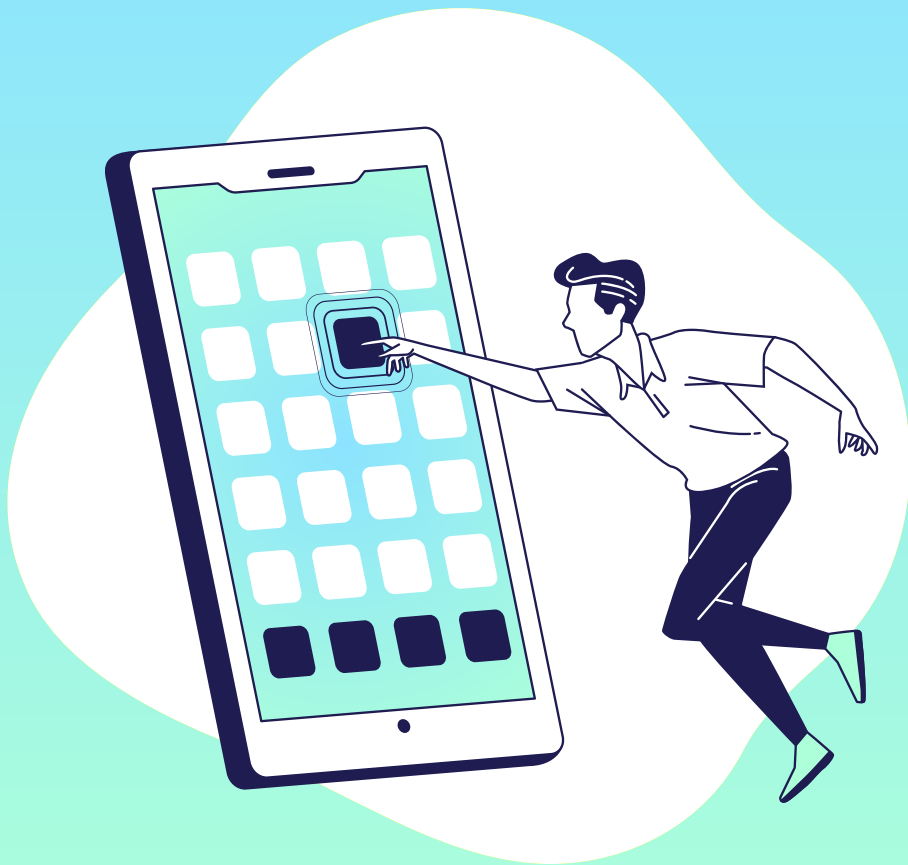


OUR EXPANSION



● Mercury is the smallest planet

○ Venus has a beautiful name



05 OPERATING PLAN

You could enter a subtitle
here if you need it

OUR PROCESS



Week 1

Mercury is the
smallest planet



Week 2

Mars is actually
a cold place



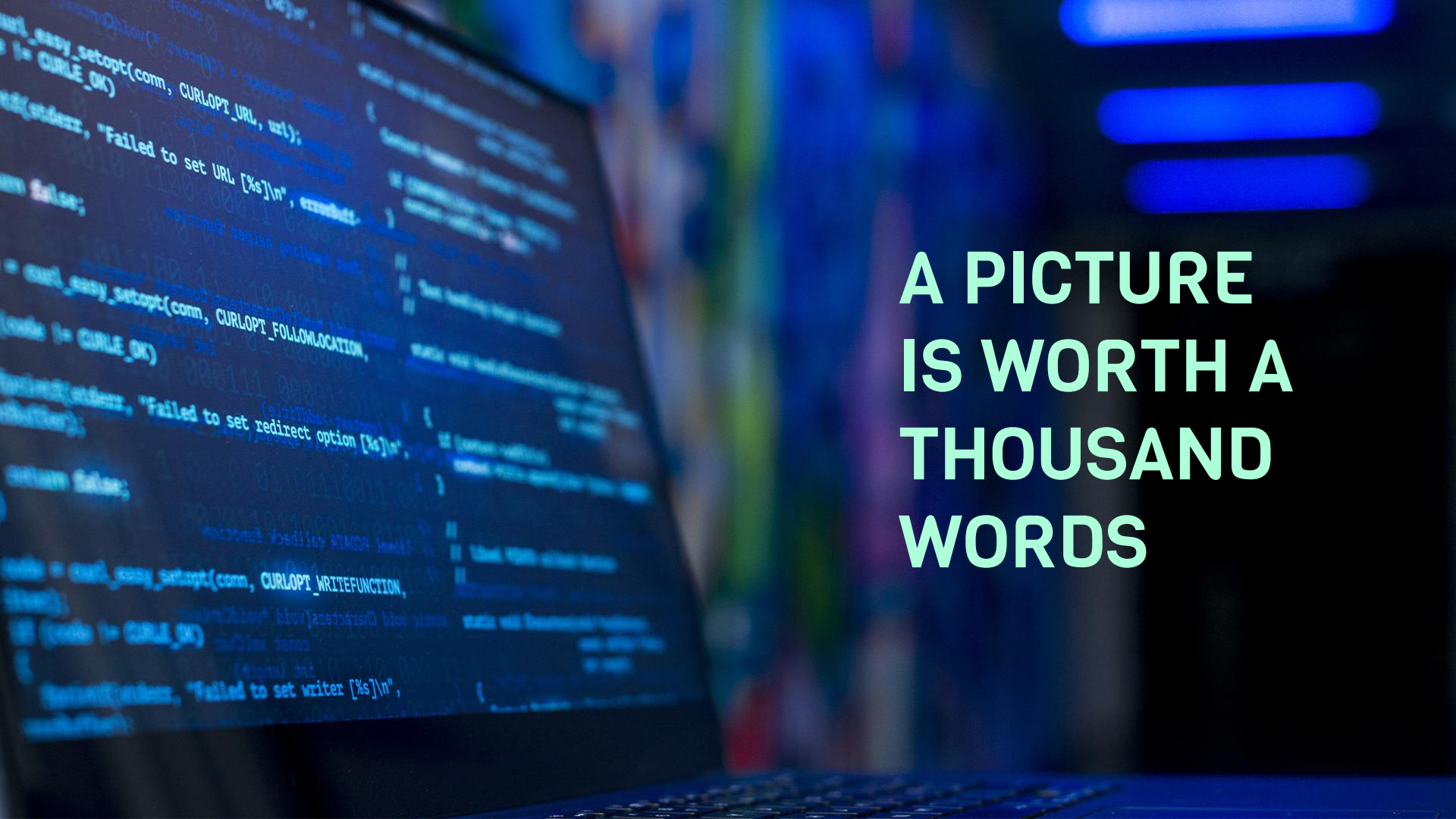
Week 3

Saturn has
several rings



Week 4

Earth is where
we live on



A PICTURE
IS WORTH A
THOUSAND
WORDS

06

FINANCIAL PLAN

You could enter a subtitle
here if you need it



PREDICTED GROW

Mercury

Mercury is the
smallest planet



Mars

Mars is actually
a cold place



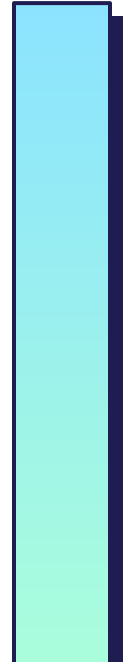
Saturn

Saturn has
several rings



Earth

Earth is where
we live on



BALANCE SHEET



THANKS!

Do you have any questions?

youremail@freepik.com

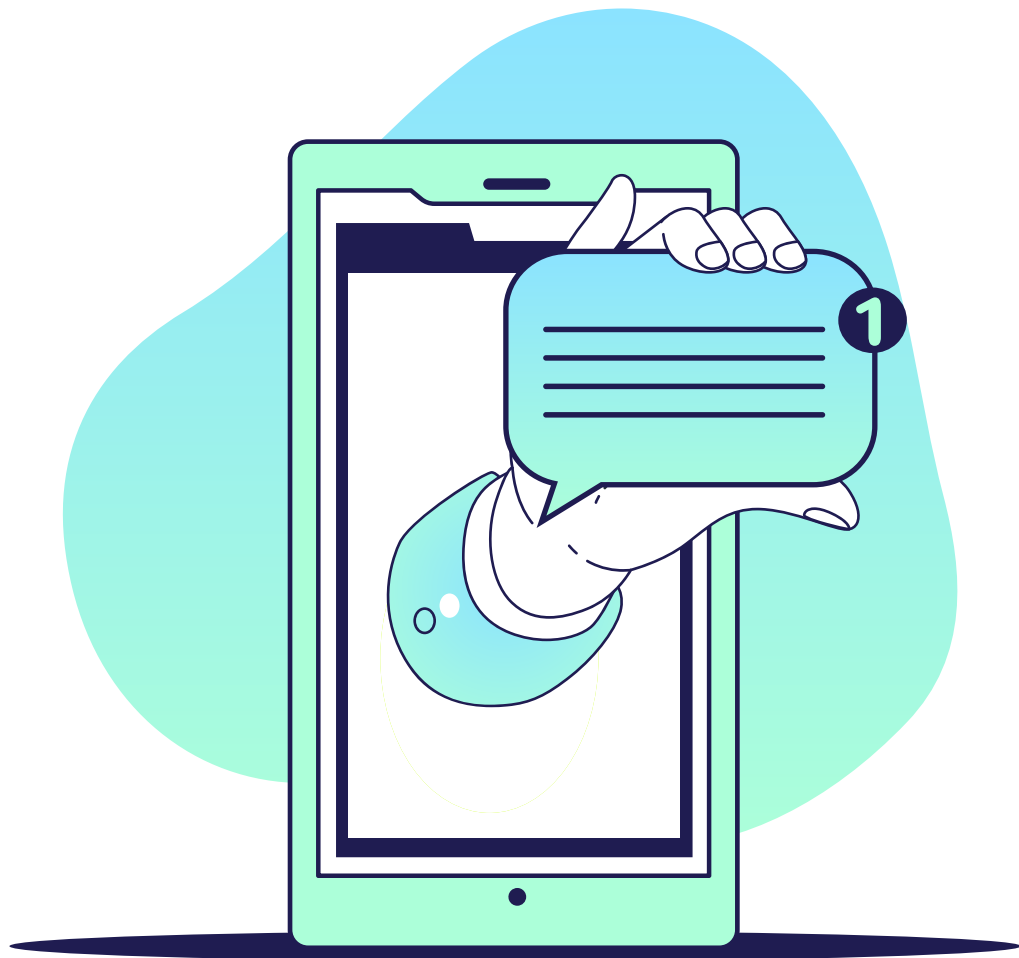
+91 620 421 838

yourcompany.com



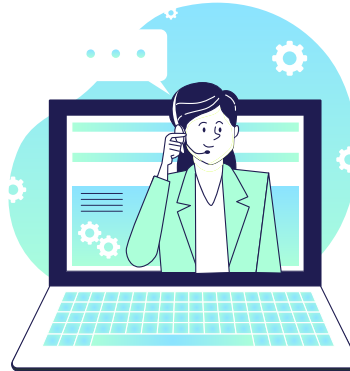
CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories

Please keep this slide for attribution.



ALTERNATIVE RESOURCES

Find more illustrations like these
on **Stories by Freepik**



RESOURCES

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

VECTORS:

Find more illustrations like these on **Stories by Freepik**

- No data concept illustration
- Secure data concept illustration
- Image upload concept illustration
- Credit card concept illustration
- Profile pic concept illustration
- Cloud hosting concept illustration
- Collaboration concept illustration
- Checklist concept illustration
- Transfer files concept illustration
- Organizing projects concept illustration
- Connecting teams concept illustration
- Meeting concept illustration
- Mobile apps concept illustration
- Concept illustration
- New message concept illustration
- Mission impossible concept illustration
- Alert concept illustration
- Secure server concept illustration

RESOURCES

- Active support concept illustration
- Safe concept illustration
- Logotype
- Login concept illustration
- Security concept illustration

PHOTOS:

- Motherboard with optical fiber cables
- Hacking concept

Instructions for use

In order to use this template, you must credit [Slidesgo](#) by keeping the **Thanks** slide.

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 Slidesgo School:

<https://slidesgo.com/faqs> and <https://slidesgo.com/slidesgo-school>

Fonts & colors used

This presentation has been made using the following fonts:

Viga

(<https://fonts.google.com/specimen/Viga>)

DM Sans

(<https://fonts.google.com/specimen/DM+Sans>)

#acffd9

#1f1c51

#8be3ff

Stories by Freepik

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

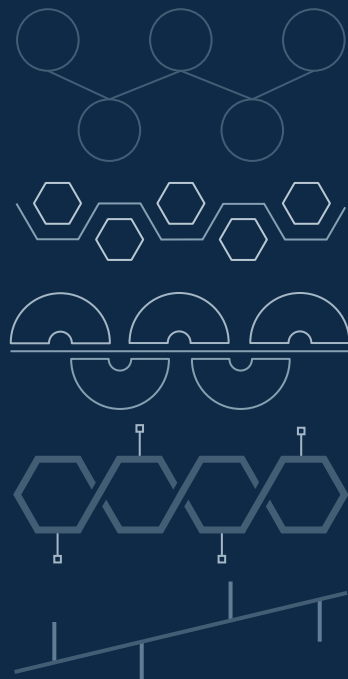
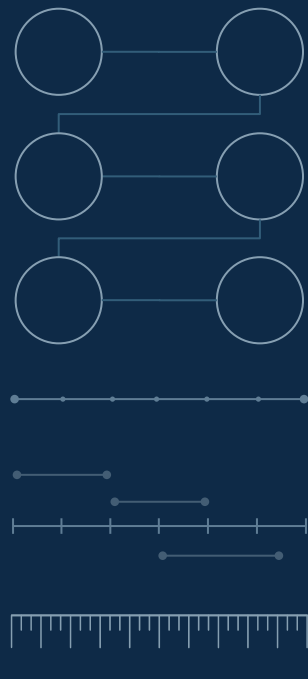
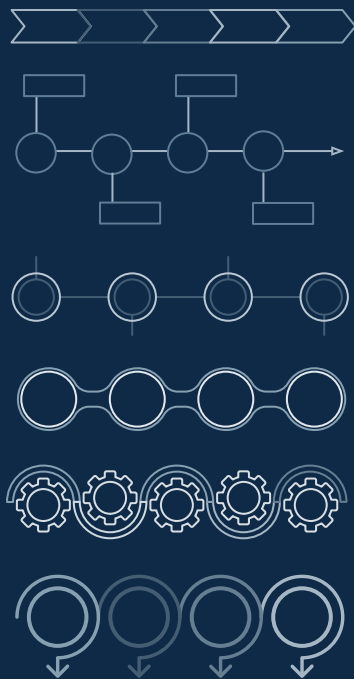
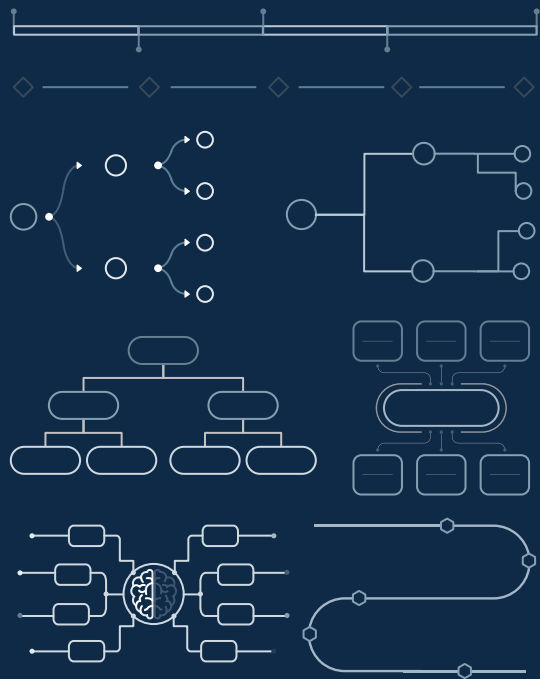
Use our editable graphic resources...

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.







| | | | | | | |
|--|--|--|--|--|--|--|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | |
|--|--|
| | |
| | |
| | |

| | | | | |
|--|--|--|--|--|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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

| | | | |
|--|--|--|--|
| | | | |
| | | | |
| | | | |

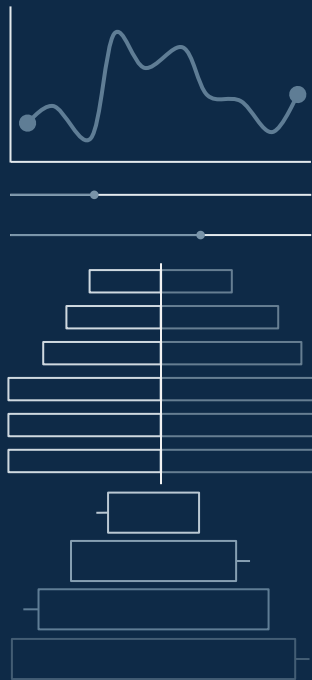
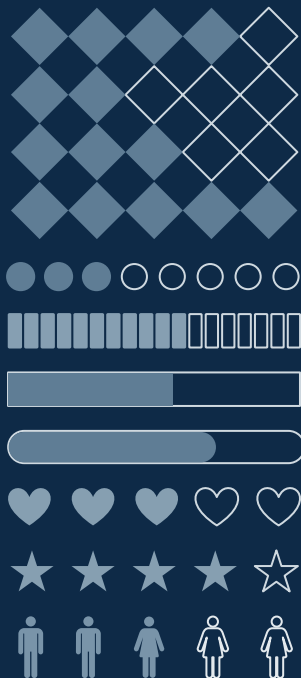
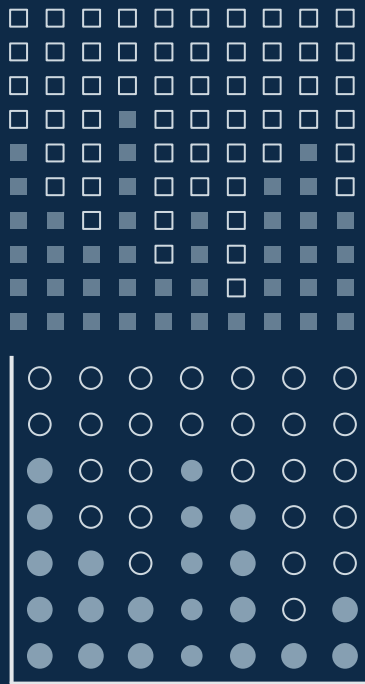
| | | | | |
|--|--|--|--|--|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | | |
|--|--|--|--|
| | | | |
| | | | |
| | | | |

| | | | |
|--|--|--|--|
| | | | |
| | | | |
| | | | |

| | | | | |
|---------|---------|----------|-------|-------|
| | 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



