

只允許 很酷的 DLL

貝坦 betan @B33F H4CK1NG



要上嗎.....??



betan貝坦

我是考慮欸

被迫上崗

自願

誒...真的假的?



B33F504P

我發表讀書會!?



良好慣例



Supermarket Together

最多可以16人一起遊玩的
模擬超市遊戲

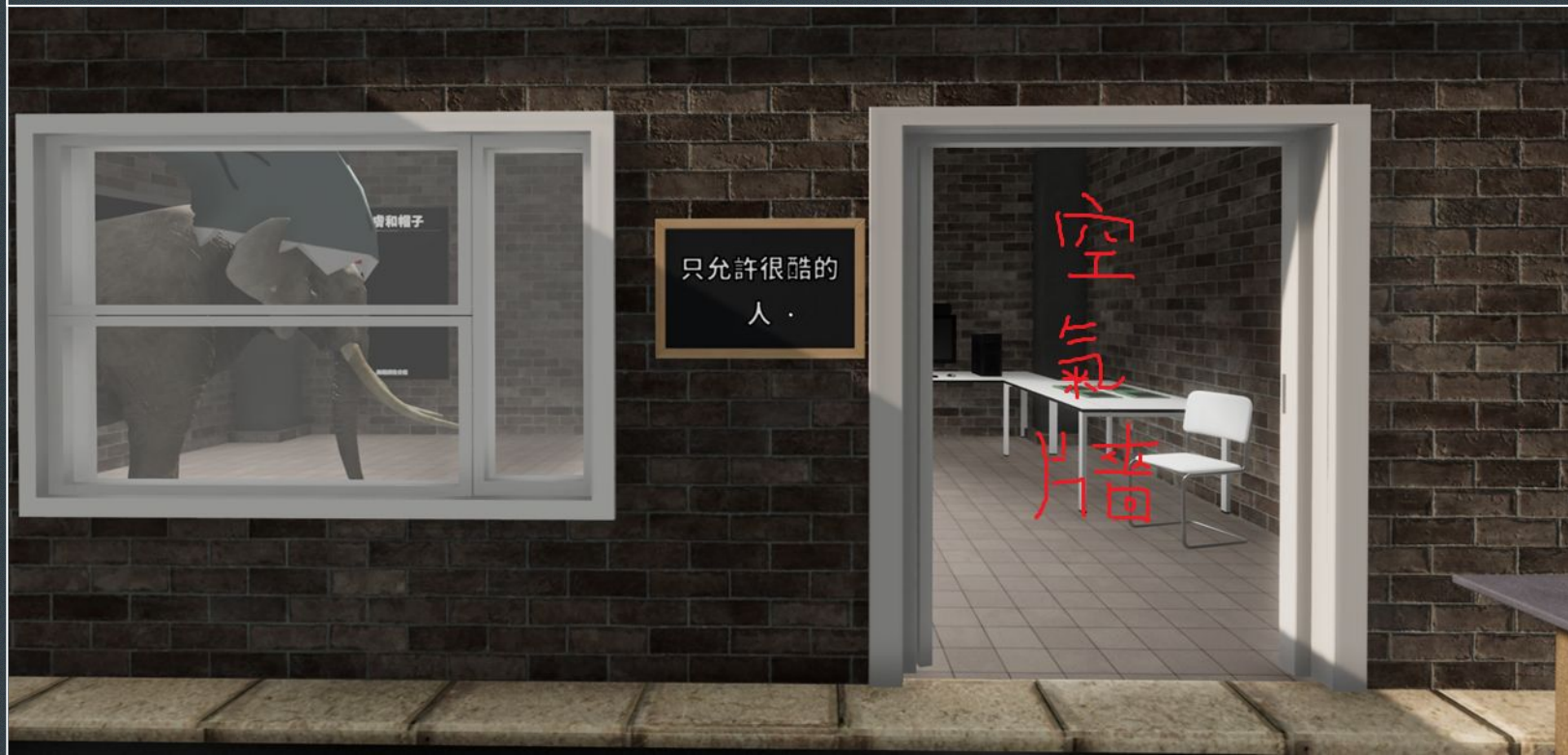
超市、、一起、、強大、、



SupermarketTogether.exe



SupermarketTogether.exe



官方預期解(?)

沒學資安的下場就是這樣..

÷ ≥ ↓↑

> ↺ ∫



BUG!!

CE啟動!

學資安的下場就是這樣

÷ ≥ ↓↑

> ↺ ∞

有興趣的話歡迎去複習下列影片

基本使用方法



如何找座標



Teleporting Through Walls with Cheat Engine - "No Way Out" [PicoCTF...



順利找到座標值

\$0005000 .00

1 08:00 lvl 1
週一

商店關門的時候，時間過得比較慢。

第一步是放置一些家具。按 [TAB] 開啟

Cheat Engine 7.5

File Edit Table D3D Mono Help

000059A4-Supermarket Together

Found: 11

Address	Value	Prev...	First
C3F356B4E4	-1.90...	2.1...	2.2...
C3F356BBE4	-1.90...	2.1...	2.2...
C3F356BC04	-1.90...	2.1...	2.2...
C3F356C0E4	-1.90...	2.1...	2.2...
29B22B147D8	-1.90...	2.1...	2.2...
29B22B1480C	2.125...	2.1...	2.2...
29B22B14840	2.125...	2.1...	2.2...
29B22B14874	2.125...	2.1...	2.2...
29B22B148A8	2.146...	2.1...	2.2...
29B22BEDB1C	-1.90...	2.1...	2.2...
29E45B2E5D0	2.080...	2.1...	2.2...

New Scan Next Scan Undo Scan

Value: 2.15 and 2.17

Scan Type: Value between... Value Type: Float

Memory Scan Options

Start: 0000000000000000 Stop: 00007fffffffffffffff

Writeable CopyOnWrite Active memory only Fast Scan: 4 Alignment: Last Digits

Pause the game while scanning

Memory View

Active	Description	Address	Type	Value
☒	No description	29B22BEDB1C	Float	-1.905949235

Advanced Options

Table E

Active	Description	Address	Type	Value
☒	No description	29B22BEDB1C	Float	-1.905949235

順利找到座標值

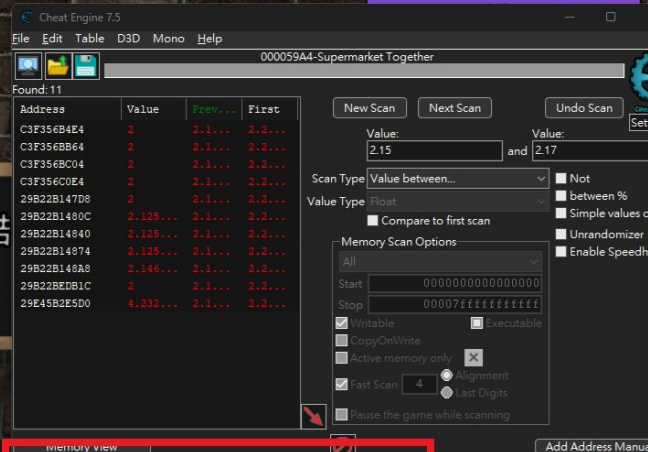
\$0005000.00

1 08:00 lvl 1
週一

商店關門的時候，時間過得比較慢。

第一步是放置一些家具。按 [TAB] 開啟

只允許很酷
人



Active	Description	Address	Type	Value
☒	No description	29822BEDB1C	Float	2

Active	Description	Address	Type	Value
☒	No description	29822BEDB1C	Float	2

成功進入房間內

\$0005000.00

1 08:00 週一

商店關門的時候，時間過得比較慢。
第一步是放置一些家具，按 [TAB] 開啟建構器

Cheat Engine 7.5

File Edit Table D3D Mono Help

000059A4-Supermarket Together

Found: 11

Address	Value	Prev...	First
C3F356B4E4	2.5	2.1...	2.2...
C3F356BB64	2.5	2.1...	2.2...
C3F356BC04	2.5	2.1...	2.2...
C3F356C0E4	2.5	2.1...	2.2...
29B22B147D8	2.5	2.1...	2.2...
29B22B1480C	2.5	2.1...	2.2...
29B22B14840	2.125...	2.1...	2.2...
29B22B14874	2.125...	2.1...	2.2...
29B22B148A8	2.146...	2.1...	2.2...
29B22BEDB1C	2.5	2.1...	2.2...
29E45B2E5D0	-1.14...	2.1...	2.2...

New Scan Next Scan Undo Scan

Value: 2.15 and Value: 2.17

Scan Type Value between... ☐ Not

Value Type Float ☐ between %

☐ Compare to first scan ☐ Simple values only

☐ Unrandomizer ☐ Enable Speedhack

Memory Scan Options

Start: 0000000000000000

Stop: 00007fffffffffffffff

☒ Writable ☐ CopyOnWrite ☐ Active memory only ☒ Fast Scan 4 Alignment Last Digits

☐ Pause the game while scanning

Memory View

Add Address Manually

Memory view				
Active	Description	Address	Type	Value
☒	No description	29B22BEDB1C	Float	2.5

來回切換也太麻煩

- 每次變更都需要切出去、變更值、切回來
- 明顯停頓



那來把這部分寫成 DLL 吧



把外掛寫成DLL



單純使用CE改參數



What's DLL?

- Dynamic Link Library (動態連結庫)
- 魔法師的魔導書
- 多種類型
 - 系統
 - 函式庫
 - 應用程式
 - 注入型

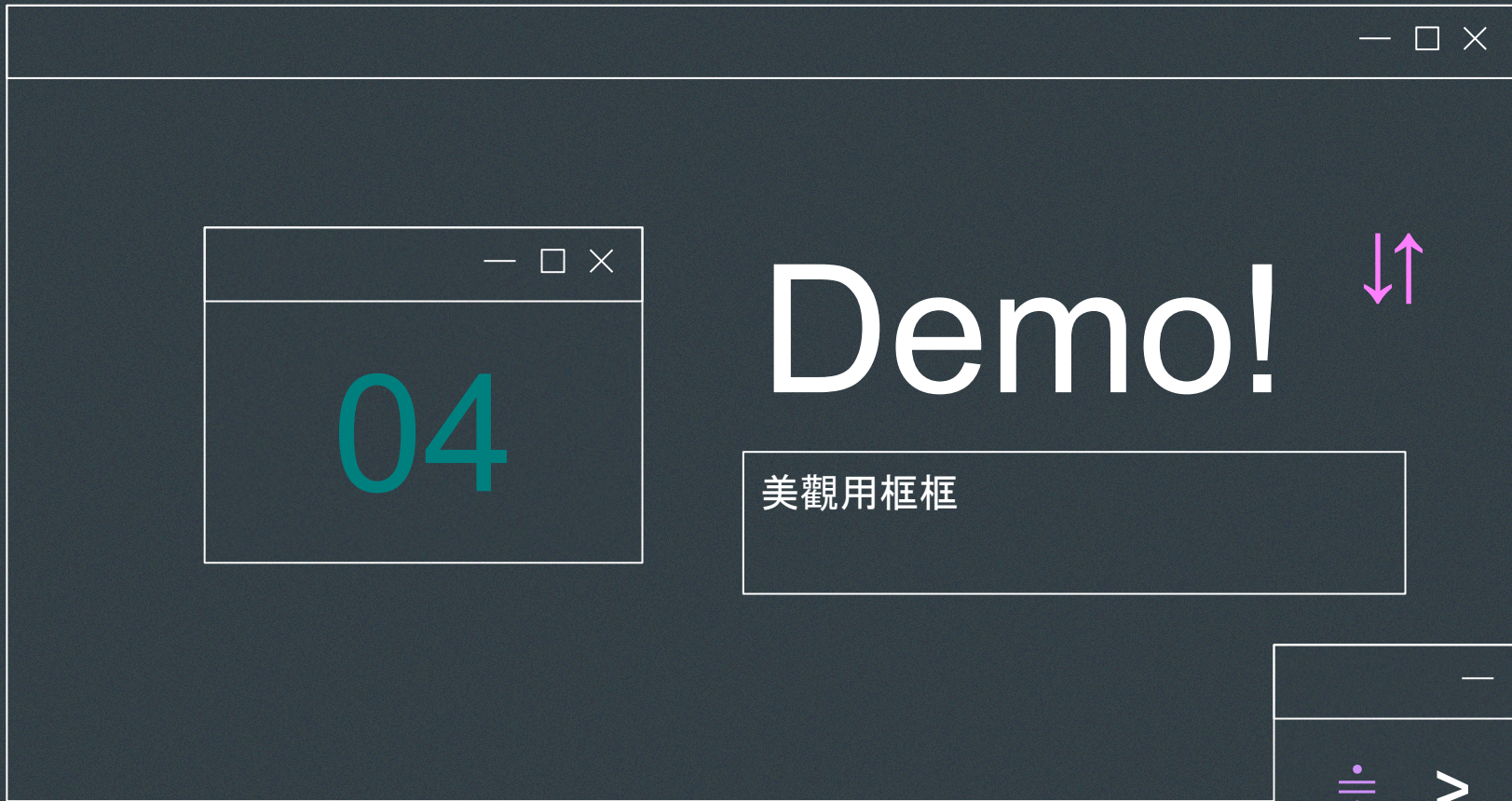


Principais fatores do lucro

	Descrição	Exemplo
A situação	Você precisa fornecer uma descrição neutra com fatos com os quais você sabe que seu público concorda	Nossa empresa vende seus produtos nos EUA há 10 anos, com um crescimento de lucro anual acima de 10%
A complicação	A complicação é uma mudança desejada da situação atual	Com uma participação de mercado já acima de 40%, o crescimento dos lucros será limitado nos Estados Unidos
A pergunta	A pergunta que resulta implicitamente da complicação	Devemos entrar no mercado europeu agora mesmo?

官方預期解.mp4





— □ ×

04

Demo!



美觀用框框

— □ ×

÷

≥

↔

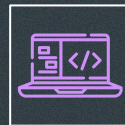
[illegible]

Planejamento estratégico do projeto



Missão

Vênus tem um nome bonito e temperaturas muito altas



Visão

Júpiter é um gigante gasoso e o maior planeta de todos



Objetivos

Apesar de ser vermelho, Marte é um lugar muito frio



Iniciativas chave

Saturno é um gigante gasoso composto de hidrogênio e hélio

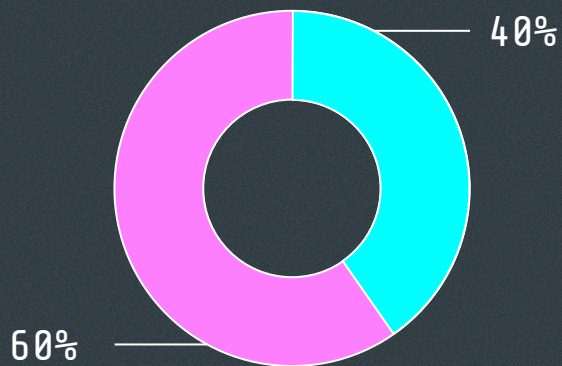
Principais fatores do lucro

	Descrição	Exemplo
A situação	Você precisa fornecer uma descrição neutra com fatos com os quais você sabe que seu público concorda	Nossa empresa vende seus produtos nos EUA há 10 anos, com um crescimento de lucro anual acima de 10%
A complicação	A complicação é uma mudança desejada da situação atual	Com uma participação de mercado já acima de 40%, o crescimento dos lucros será limitado nos Estados Unidos
A pergunta	A pergunta que resulta implicitamente da complicação	Devemos entrar no mercado europeu agora mesmo?

Palavras
incríveis



Modelo financeiro

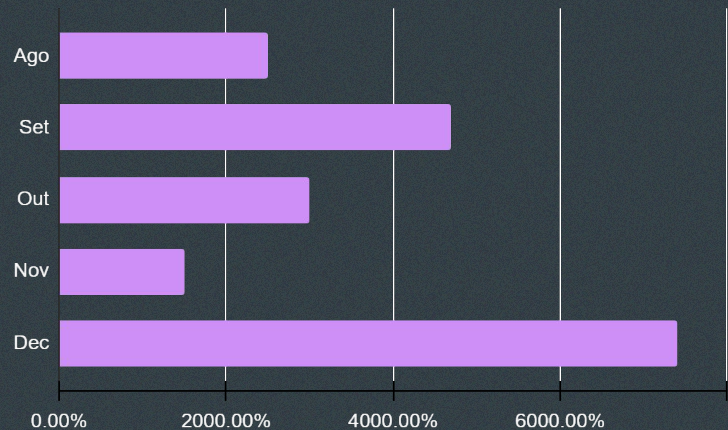


■ **Vênus**

Vênus é o
segundo planeta
a partir do Sol

■ **Marte**

Apesar de ser
vermelho, Marte
é um lugar frio



■ **Vênus**

* Siga o link no gráfico para modificar seus dados e, em seguida, cole os novos dados aqui. Para obter mais informações, [clique aqui](#)

Proposta de consultoria

Serviços

Mercúrio é o planeta
mais próximo do Sol

Taxas

Vênus é o segundo
planeta a partir do Sol

Faturas

Apesar de ser vermelho,
Marte é um lugar frio

Despesas

Júpiter é o maior
planeta de todos

Materiais

Saturno é composto de
hidrogênio e hélio

Termos

Netuno é o planeta mais
distante do Sol

Caso de negócios

1

Mercúrio é o planeta
mais próximo do Sol

2

Júpiter é o maior
planeta de todos

3

Vênus é o segundo
planeta a partir do Sol

Nome da
empresa

Logotipo
da
empresa

XX/XX/XX

4

Saturno é composto de
hidrogênio e hélio

5

Apesar de ser vermelho,
Marte é um planeta frio

6

Netuno é o planeta mais
distante do Sol

Implementar e gerenciar o progresso

Gerenciar o progresso

Progresso		Estado			Link
		Para fazer	Em prog	Feito	
Vênus	0%				www.seulink aqui.com
Marte	35%				www.seulink aqui.com
Netuno	0%				www.seulink aqui.com
Júpiter	50%				www.seulink aqui.com
Terra	100%				www.seulink aqui.com
Ceres	90%				www.seulink aqui.com



489.300 \$

Números grandes chamam a atenção do público



20.000 \$

Marte é realmente um lugar frio

15.000 \$

Vênus tem um nome bonito

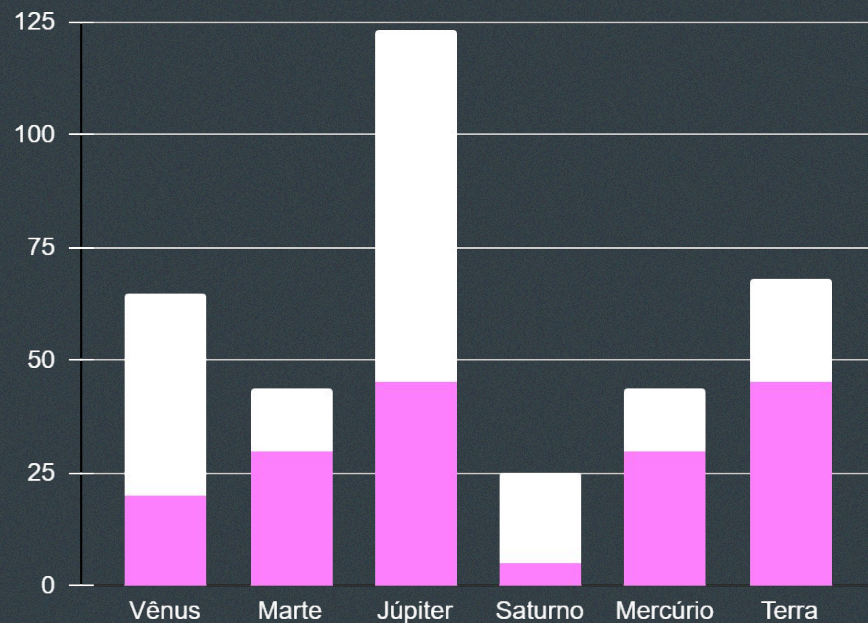
10.000 \$

Mercúrio é un planeta pequeno

45.000 \$

Saturno tem vários anéis

Sobre os termos do acordo



Vênus

Vênus é o segundo planeta a partir do Sol

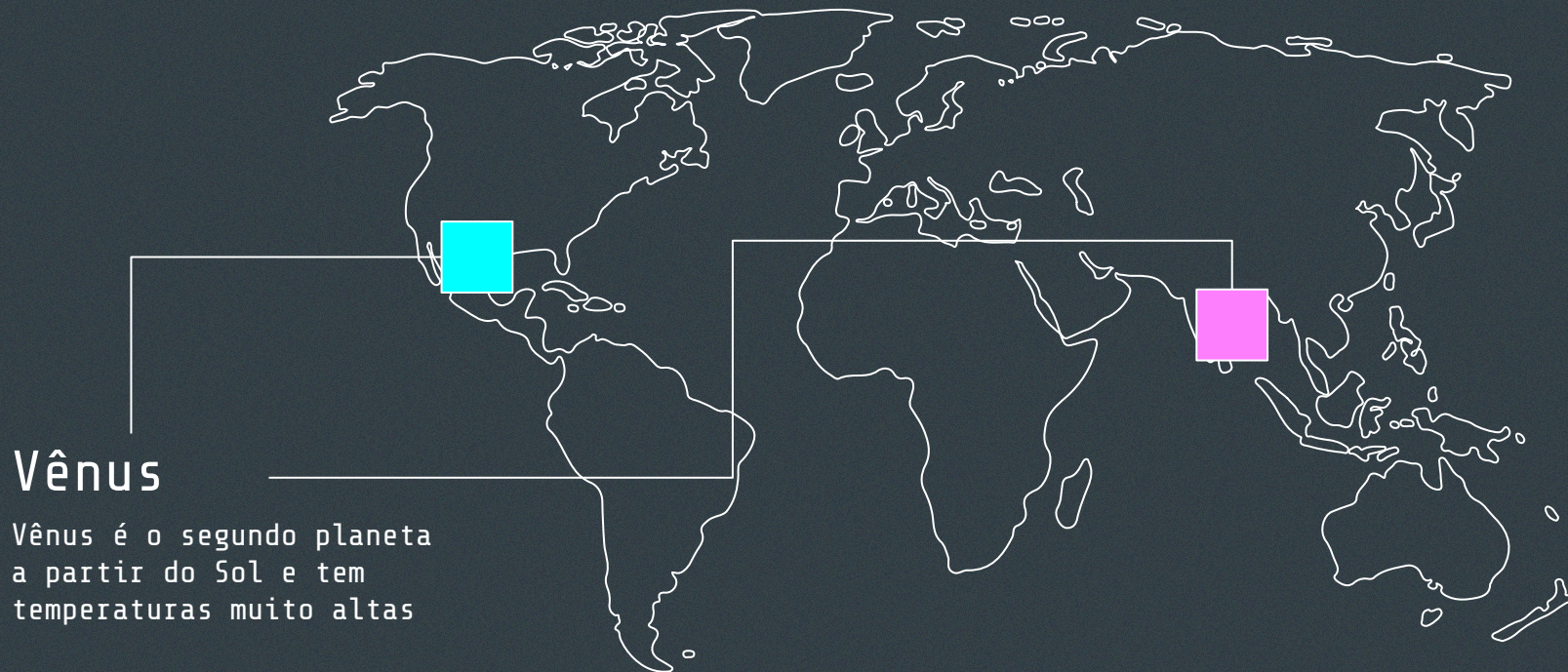


Marte

Apesar de ser vermelho, Marte é um lugar frio

* Siga o link no gráfico para modificar seus dados e, em seguida, cole os novos dados aqui. Para obter mais informações, [clique aqui](#)

Alianças estratégicas



Vênus

Vênus é o segundo planeta
a partir do Sol e tem
temperaturas muito altas

Respostas e argumentos

Escreva sua pergunta

Escreva sua resposta

Saturno

Saturno é um gigante gasoso e tem vários anéis. É composto de hidrogênio e hélio. Recebeu seu nome em homenagem ao deus romano da riqueza e da agricultura

Vênus

Vênus tem um nome bonito e é o segundo planeta a partir do Sol. É terrivelmente quente, ainda mais quente que Mercúrio, e sua atmosfera é venenosa

Marte

Apesar de ser vermelho, Marte é, na verdade, um lugar muito frio. Ele está repleto de poeira de óxido de ferro, que é o que dá ao planeta seu tom avermelhado

10 principais perguntas sobre planos de negócios

1

Qual é a sua situação?

2

Qual é sua visão?

3

Como você pode alcançar sua visão?

4

O que você oferece?

5

Qual é o tamanho do mercado?

6

Quem são os principais participantes?

7

Como fazer a diferença?

8

Qual é o seu plano de marketing?

9

Qual é a sua economia?

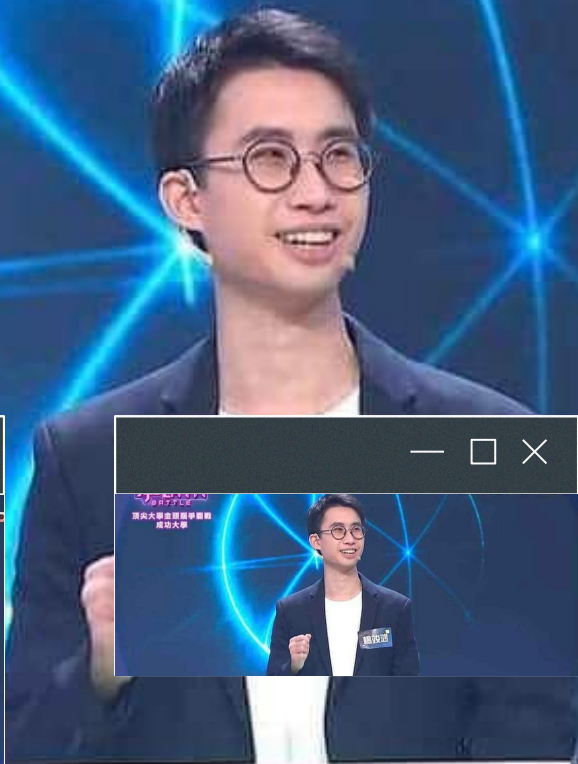
10

O que você precisa para começar?

拜託ATM
BATTLE

頂尖大學金頭腦爭霸戰
成功大學

T/BS 歡樂台 HD



我們是做好駭客

THANKS



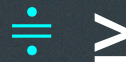
!

https://betan423.github.io/posts/005_2024hitcon/
<https://github.com/Betan423/SupermarkerTogether-dll>



CRÉDITOS: Este modelo de apresentação foi criado pela Slidesgo, e inclui ícones do Flaticon e imagens da Freepik

Por favor, mantenha este slide para atribuição



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:

Share Tech Mono

(<https://fonts.google.com/specimen/Share+Tech+Mono>)

#ffffff

#2f3b42

#ce90f7

#00ffff

#fd7ffd

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



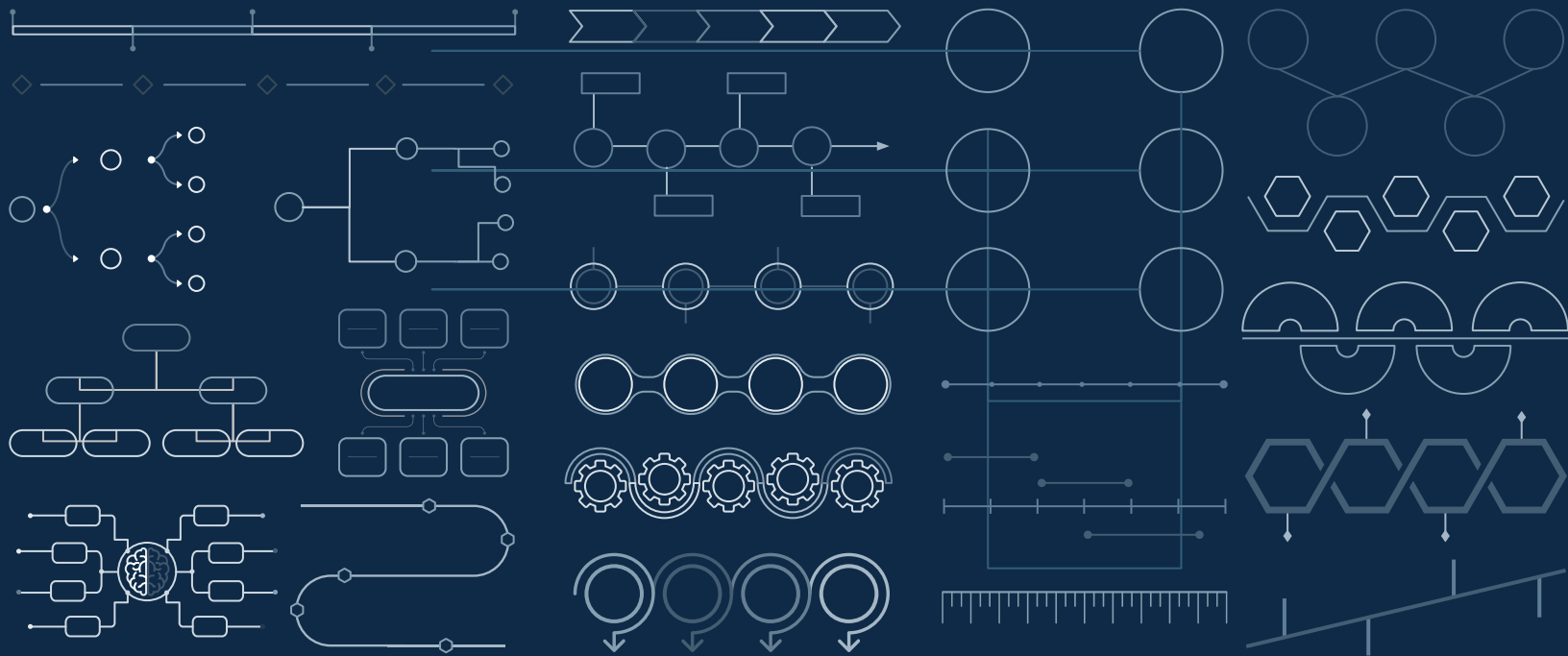
Cuate

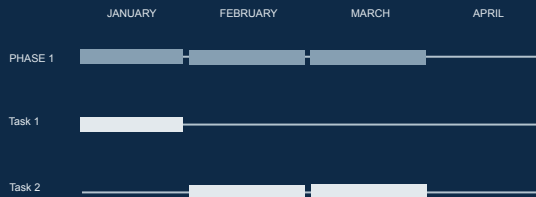
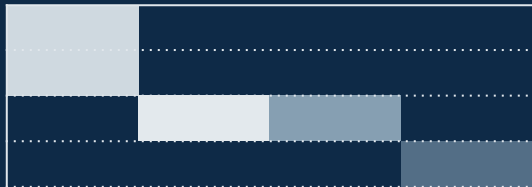
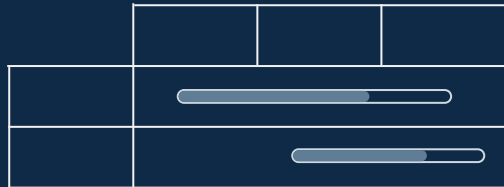
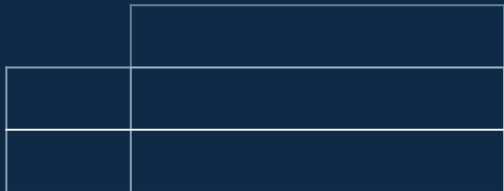
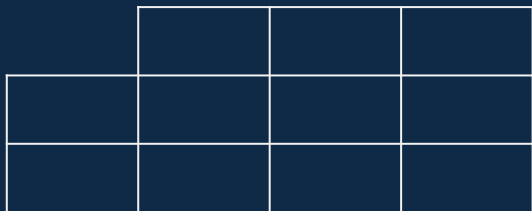
Use our editable graphic resources...

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](#).











...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



