PROFISSÃO: ETHICAL HACKER

DESMISTIFICANDO CYBER SECURITY

START

SIGN IN

EDUARDO VASCONCELOS

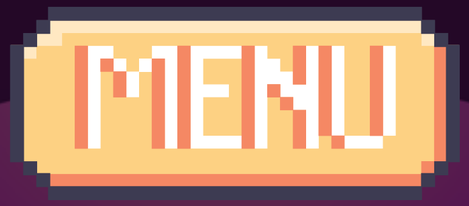
ENGENHEIRO DE SEGURANÇA MOBILE @ IFOOD

FORMAÇÃO

Mestrado em Computação (ongoing) @ ICMC-USP
Esp. Eng. Software @ IC-UNICAMP
Eng. Computação @ ICMC-USP
Eng. Eletrônica (visiting) @ Trinity College

EXPERIÊNCIA

Engenheiro de Segurança @ iFood
Analista de Segurança @ SiDi
Analista de Segurança @ Hacker Rangers
Estagiário de TI @ Embraer



Básico de Sec em “5” minutos a.k.a. Missão: Impossível

A TODO list perdida de um analista de segurança

A TODO list perdida de um engenheiro de segurança

Gostei! Por onde eu começo?

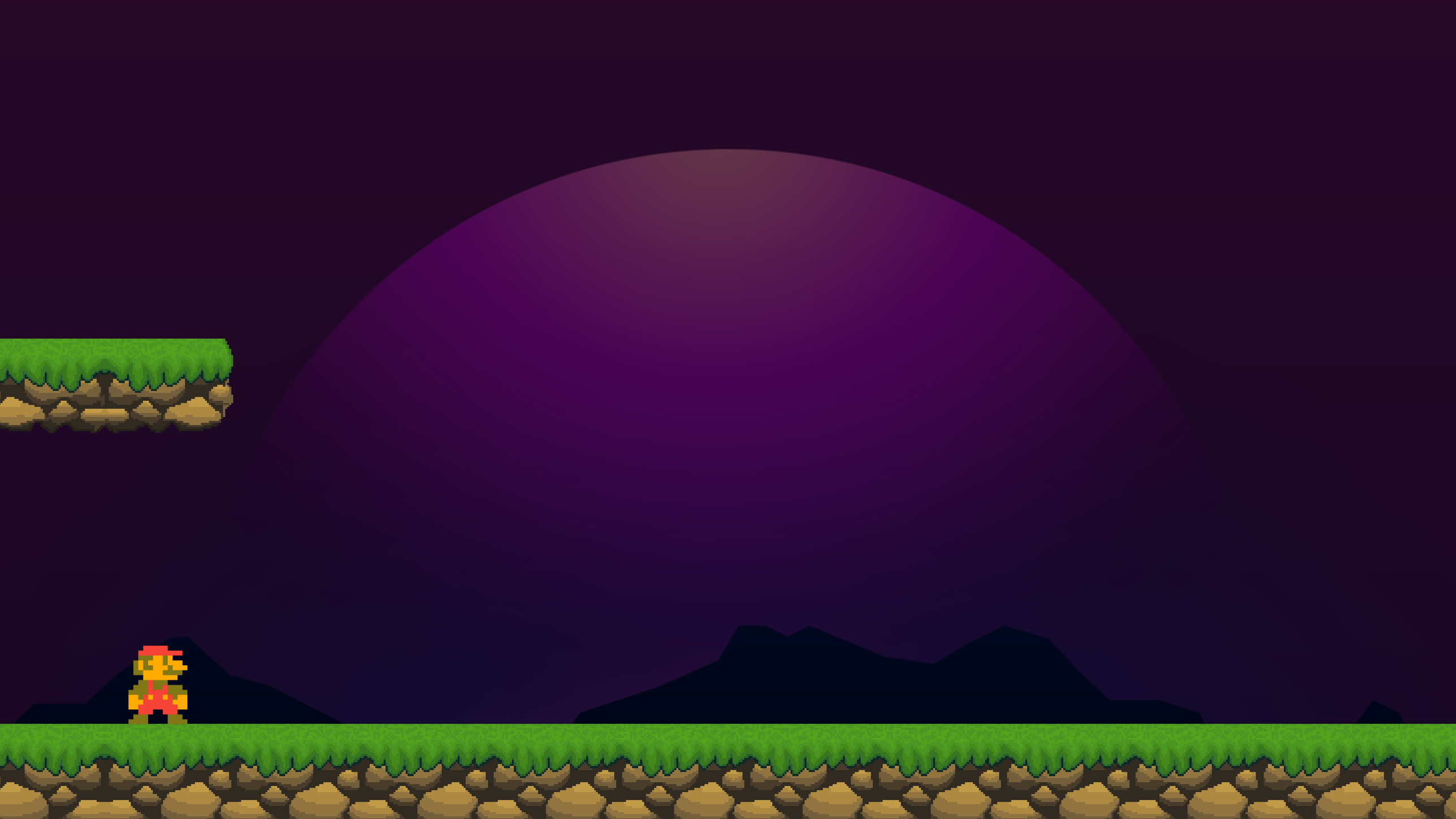
Dois dedos de juízo: não seja a vergonha da profission!

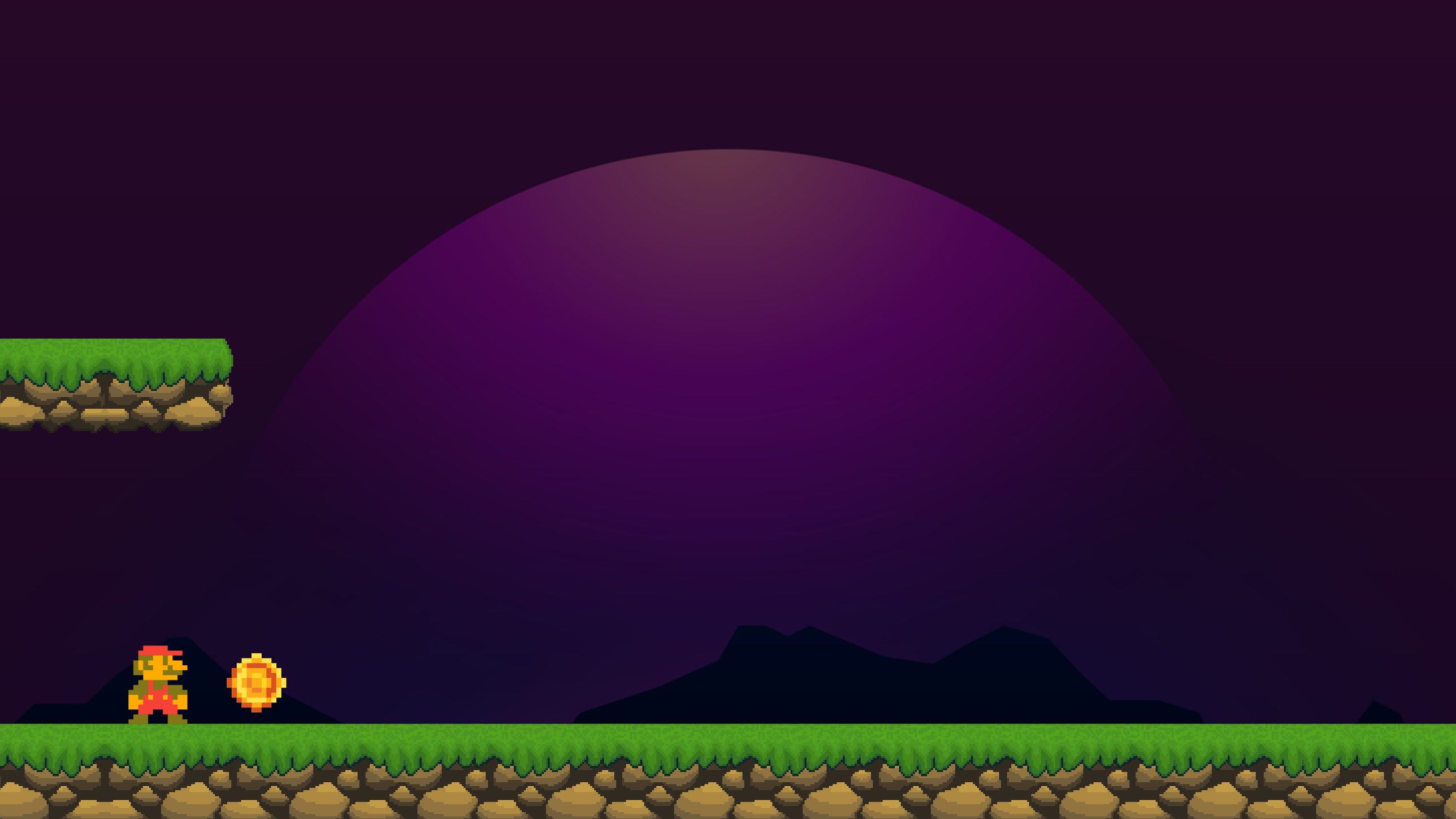
Não paramos por aqui

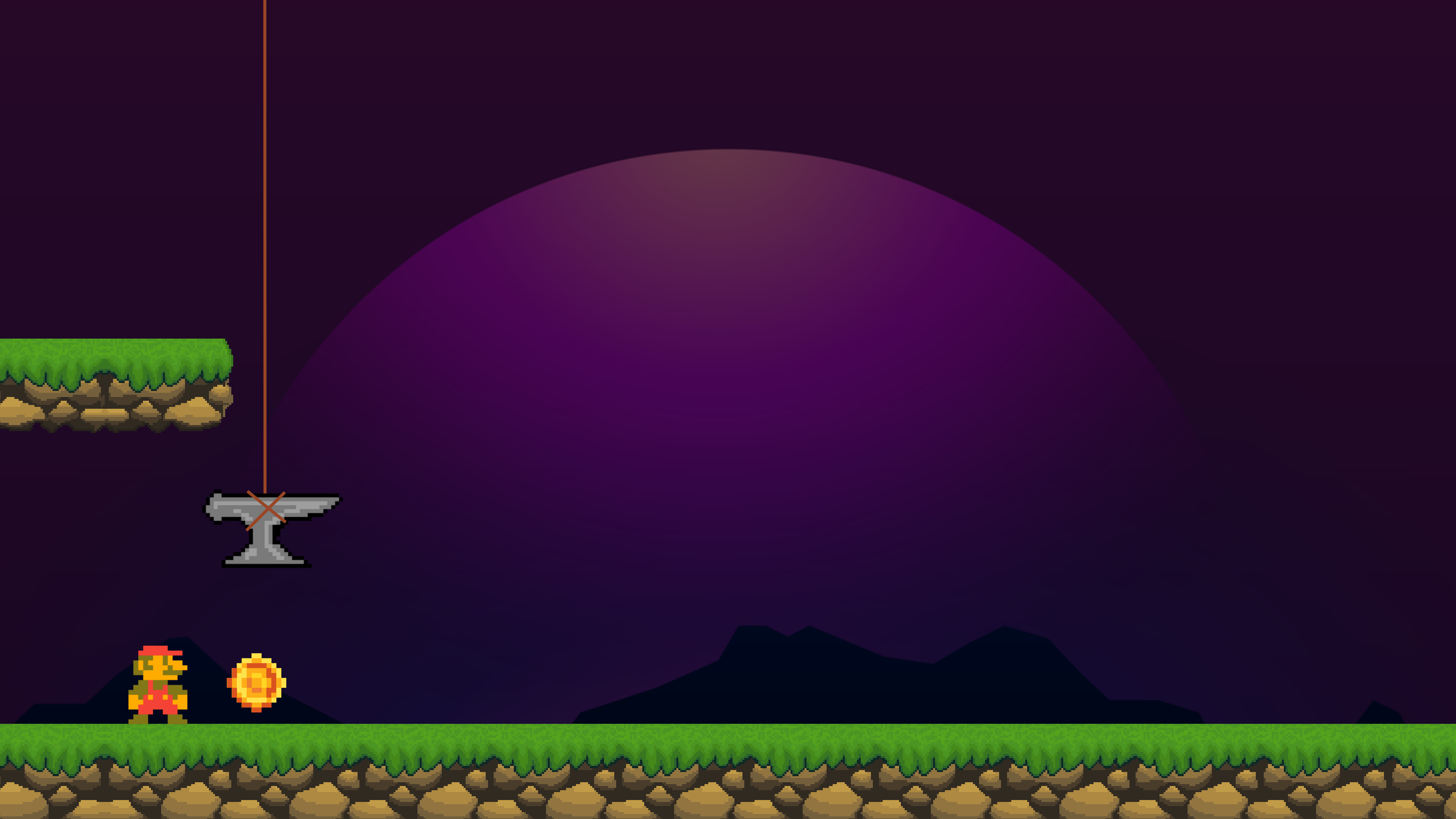
Q&A

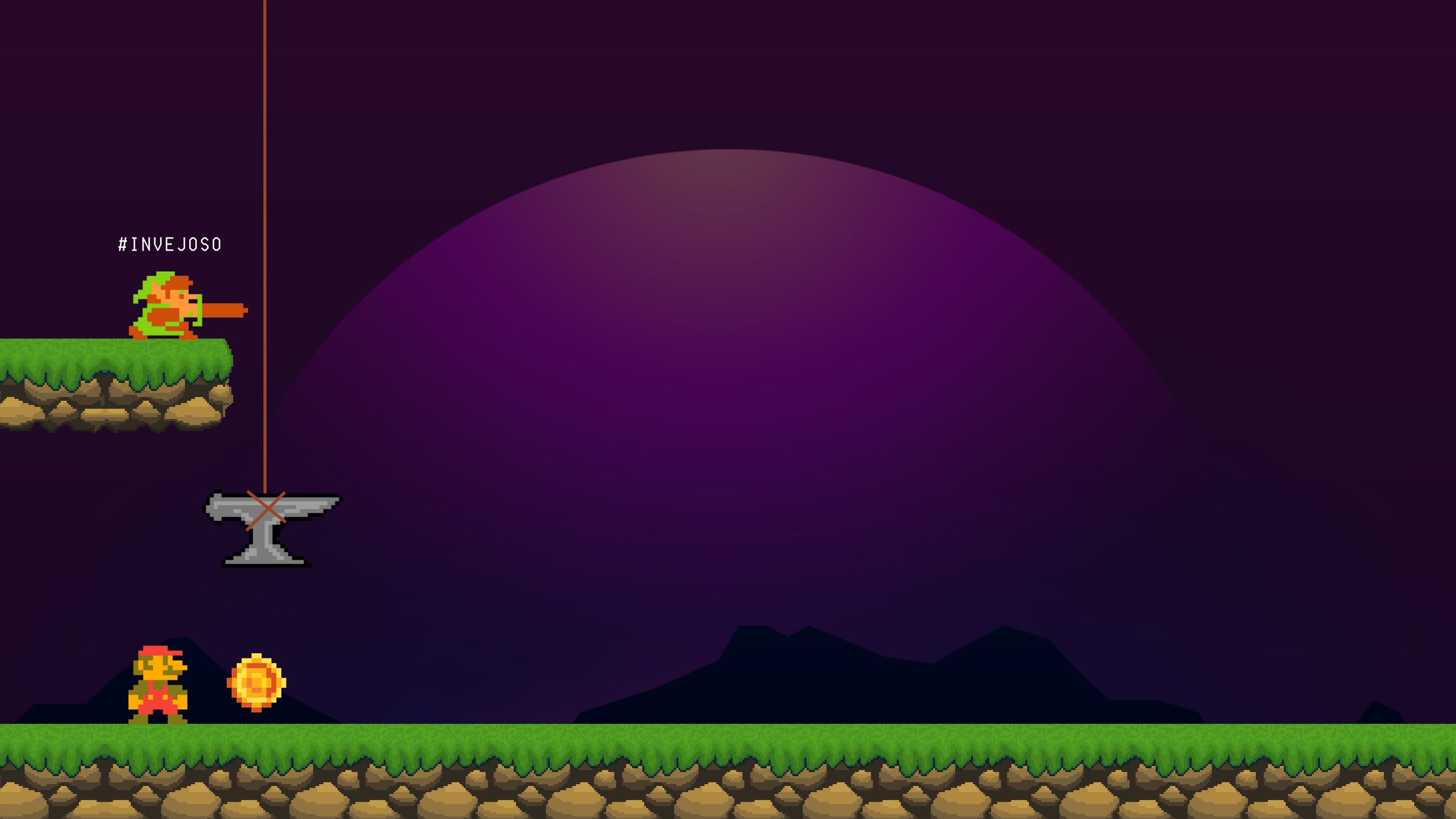
MENU

- Básico de Sec em “5” minutos a.k.a. Missão: Impossível
- A TODO list perdida de um analista de segurança
- A TODO list perdida de um engenheiro de segurança
- Gostei! Por onde eu começo?
- Dois dedos de juízo: não seja a vergonha da profission!
- Não paramos por aqui
- Q&A

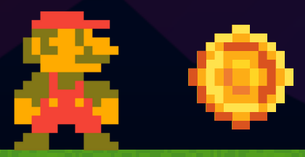







#INVEJOSO

#INVEJOSO



VULNERABILIDADE

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

EXPLORAÇÃO

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

ATAQUE

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

AMEAÇA

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

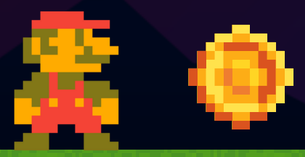
MITIGAÇÃO

MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

RISCO

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

#INVEJOSO



VULNERABILIDADE?

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

EXPLORAÇÃO

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

ATAQUE

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

AMEAÇA

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

MITIGAÇÃO

MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

RISCO

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

#INVEJOSO

VULNERABILIDADE

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

A MOEDA ESTÁ BEM DEBAIXO DA BIGORNA

EXPLORAÇÃO?

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

ATAQUE

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

AMEAÇA

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

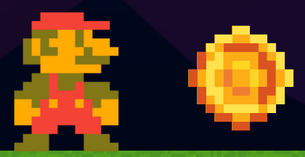
MITIGAÇÃO

MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

RISCO

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

#INVEJOSO



VULNERABILIDADE

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

A MOEDA ESTÁ BEM DEBAIXO DA BIGORNA

EXPLORAÇÃO

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

CORTAR A CORDA

ATAQUE

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

AMEAÇA?

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

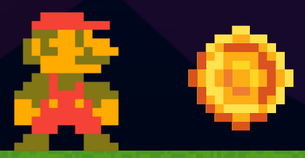
MITIGAÇÃO

MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

RISCO

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

#INVEJOSO



VULNERABILIDADE

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

A MOEDA ESTÁ BEM DEBAIXO DA BIGORNA

EXPLORAÇÃO

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

CORTAR A CORDA

ATAQUE?

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

AMEAÇA

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

O LINK PODE TENTAR CORTAR A CORDA

MITIGAÇÃO

MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

RISCO

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

#INVEJOSO

VULNERABILIDADE

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

A MOEDA ESTÁ BEM DEBAIXO DA BIGORNA

EXPLORAÇÃO

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

CORTAR A CORDA

ATAQUE

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

O LINK TENTOU CORTAR A CORDA

AMEAÇA

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

O LINK PODE TENTAR CORTAR A CORDA

MITIGAÇÃO

MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

RISCO?

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

#INVEJOSO

VULNERABILIDADE

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

A MOEDA ESTÁ BEM DEBAIXO DA BIGORNA

EXPLORAÇÃO

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

CORTAR A CORDA

ATAQUE

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

O LINK TENTOU CORTAR A CORDA

AMEAÇA

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

O LINK PODE TENTAR CORTAR A CORDA

MITIGAÇÃO?

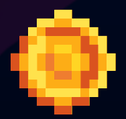
MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

RISCO

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

MOEDA--

#INVEJOSO



VULNERABILIDADE

FRAQUEZA QUE PODE SER ABUSADA/“EXPLORADA”

A MOEDA ESTÁ BEM DEBAIXO DA BIGORNA

EXPLORAÇÃO

MÉTODO QUE PODE SER USADO PARA ABUSAR DE/”EXPLORAR” UMA VULNERABILIDADE

CORTAR A CORDA

ATAQUE

TENTATIVA DE ABUSO, “EXPLORANDO” UMA VULNERABILIDADE

O LINK TENTOU CORTAR A CORDA

AMEAÇA

ATAQUE EM POTENCIAL (I.E. AINDA NO “CAMPO TEÓRICO”)

O LINK PODE TENTAR CORTAR A CORDA

MITIGAÇÃO

MEDIDA PARA REDUZIR A PLAUSIBILIDADE DE UMA AMEAÇA

MOVER A MOEDA UM POUQUINHO MAIS PRA LÁ

RISCO

PERDA EM POTENCIAL CASO UMA AMEAÇA SE CONCRETIZE

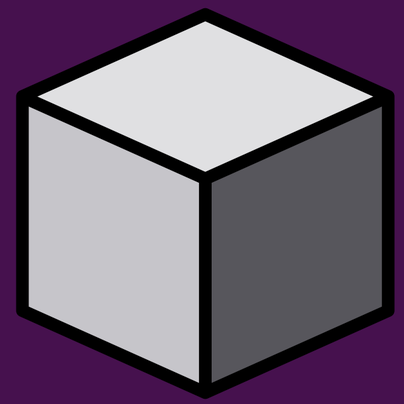
MOEDA--

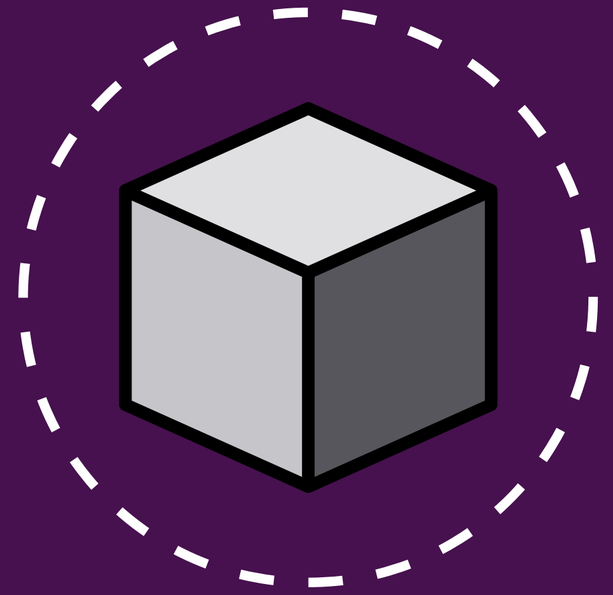
TRÍADE CIA

CONFIDENCIALIDADE
INTEGRIDADE
DISPONIBILIDADE

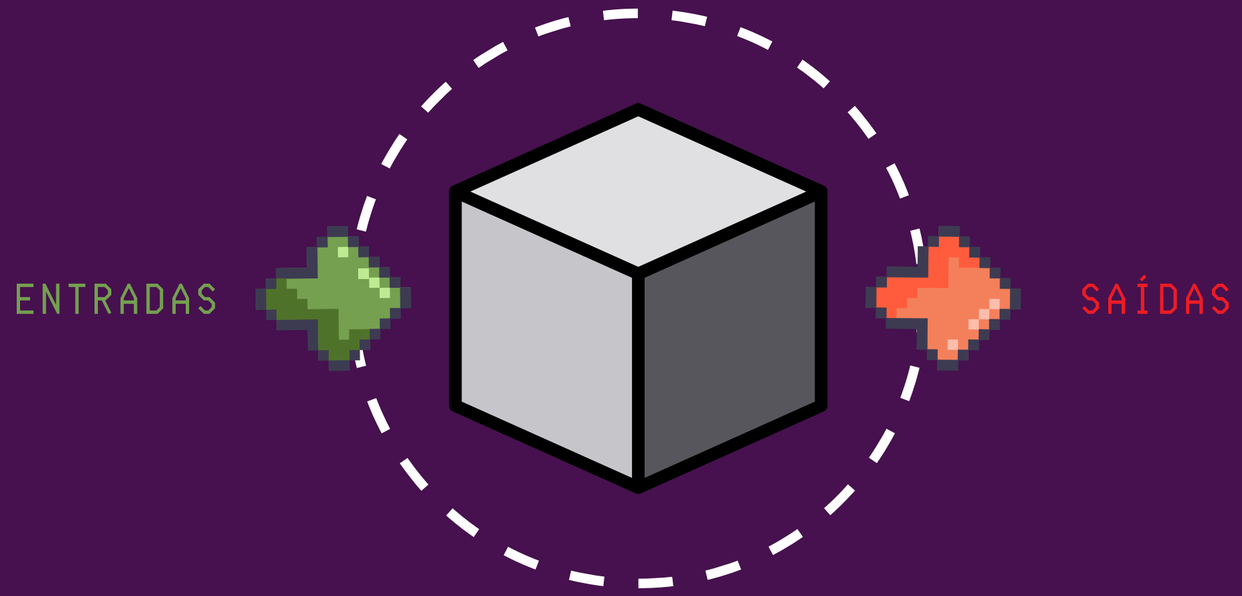
TESTE

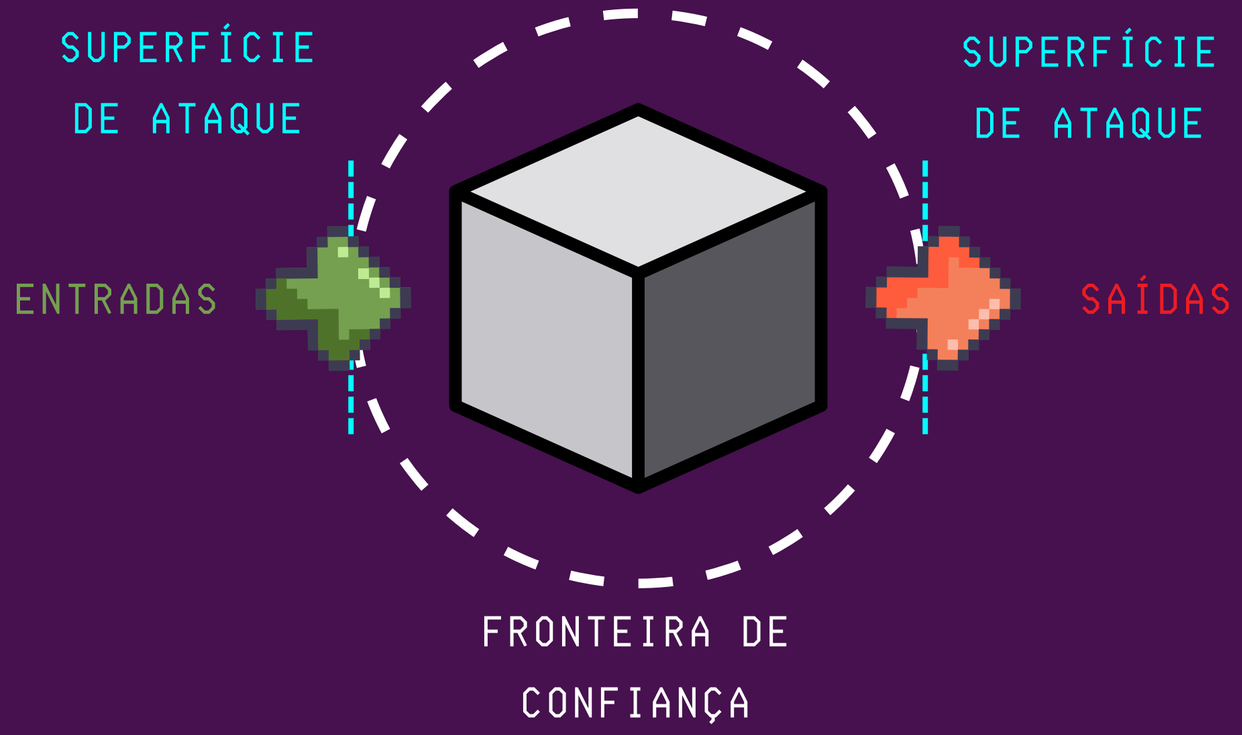
Atividade de executar um programa e verificar se o comportamento dele é o esperado, com o objetivo de revelar defeitos.



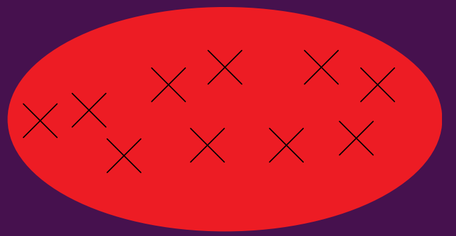


FRONTEIRA DE
CONFIANÇA

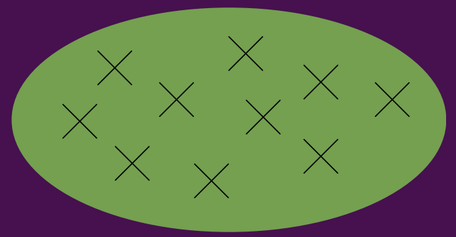

ENTRADAS
SAÍDAS
FRONTEIRA DE
CONFIANÇA


SUPERFÍCIE
DE ATAQUE
SUPERFÍCIE
DE ATAQUE
ENTRADAS
SAÍDAS
FRONTEIRA DE
CONFIANÇA

UNIVERSO DE SAÍDAS

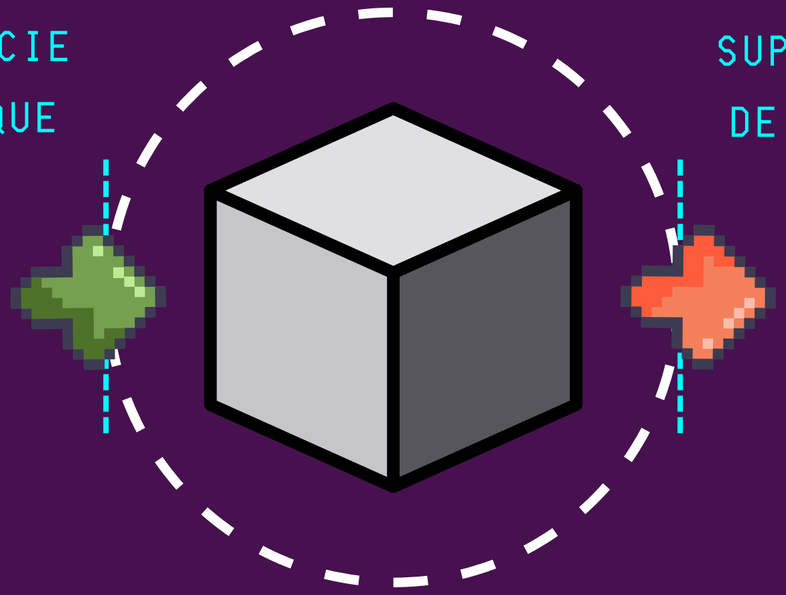


UNIVERSO DE ENTRADAS



SUPERFÍCIE DE ATAQUE

SUPERFÍCIE DE ATAQUE

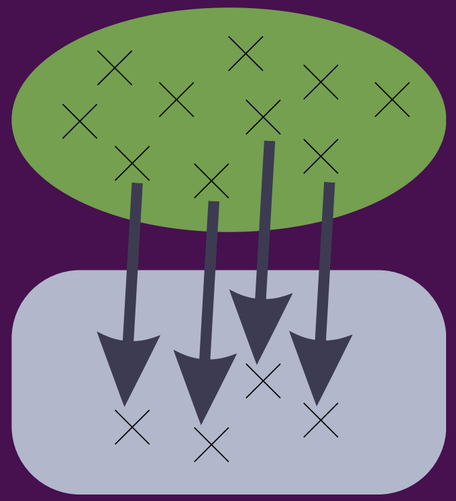


ENTRADAS

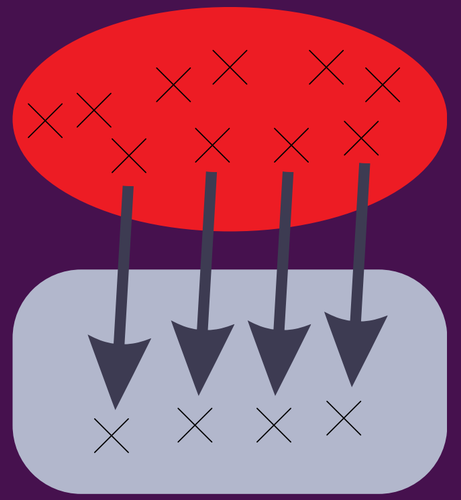
SAÍDAS

FRONTEIRA DE CONFIANÇA

UNIVERSO DE
ENTRADAS



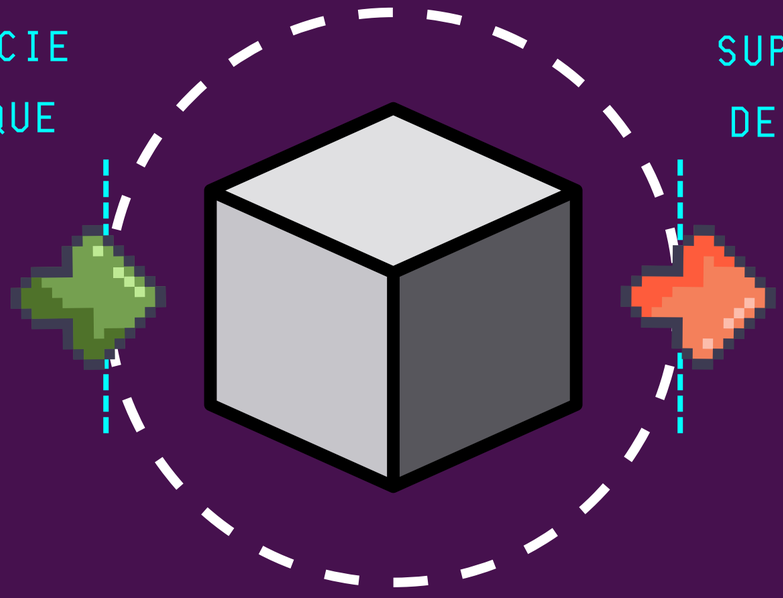
UNIVERSO DE
SAÍDAS



SUPERFÍCIE
DE ATAQUE

SUPERFÍCIE
DE ATAQUE

ENTRADAS

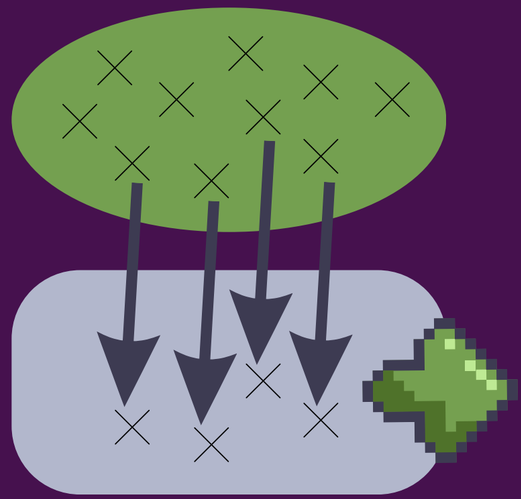


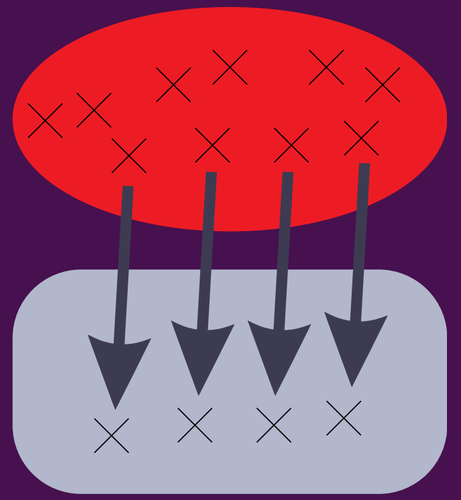
SAÍDAS

FRONTEIRA DE
CONFIANÇA

UNIVERSO DE SAÍDAS

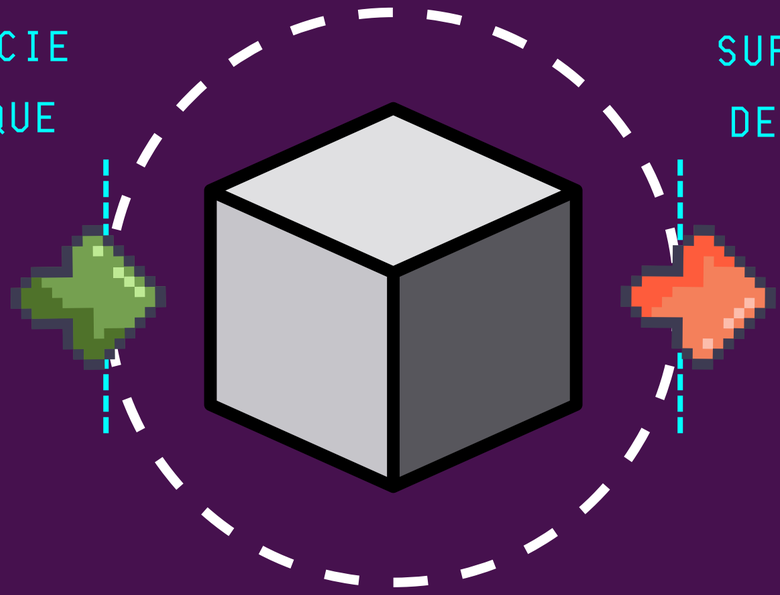
UNIVERSO DE ENTRADAS





SUPERFÍCIE DE ATAQUE

SUPERFÍCIE DE ATAQUE



ENTRADAS

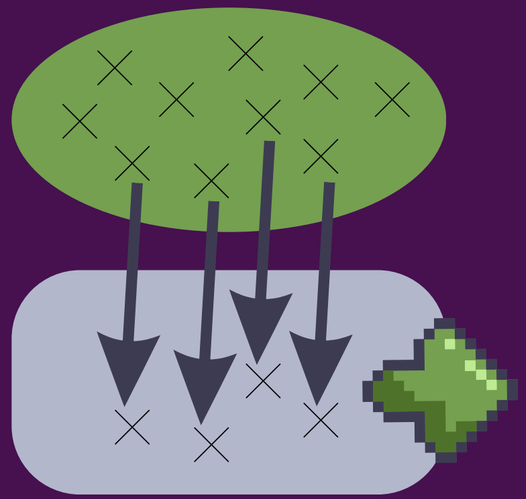
SAÍDAS

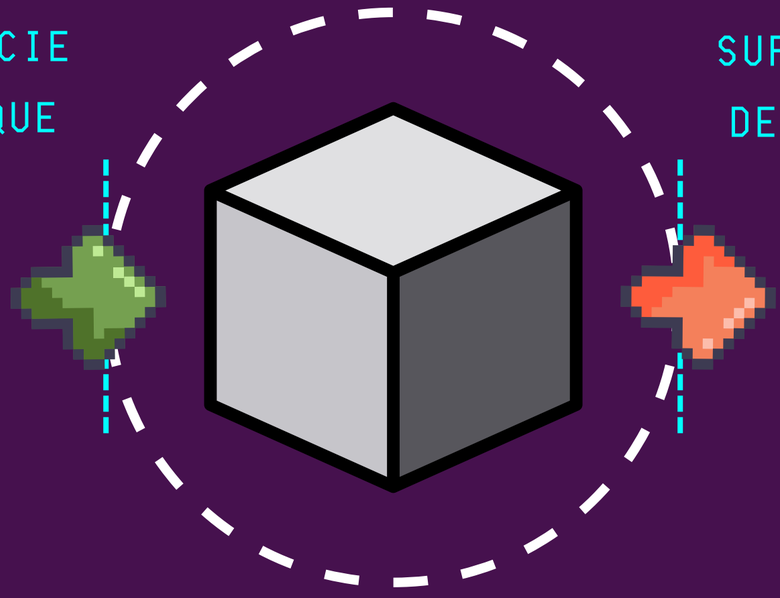
FRONTEIRA DE CONFIANÇA

UNIVERSO DE
ENTRADAS

SUPERFÍCIE
DE ATAQUE

ENTRADAS



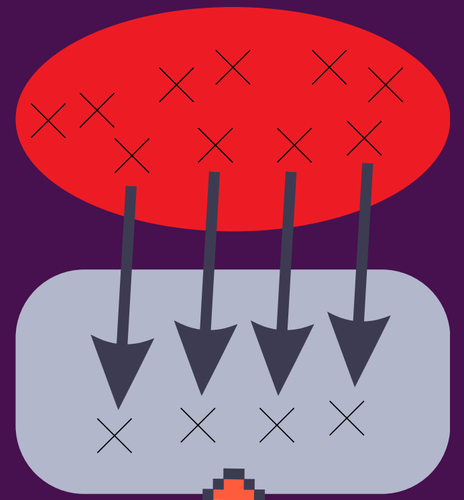


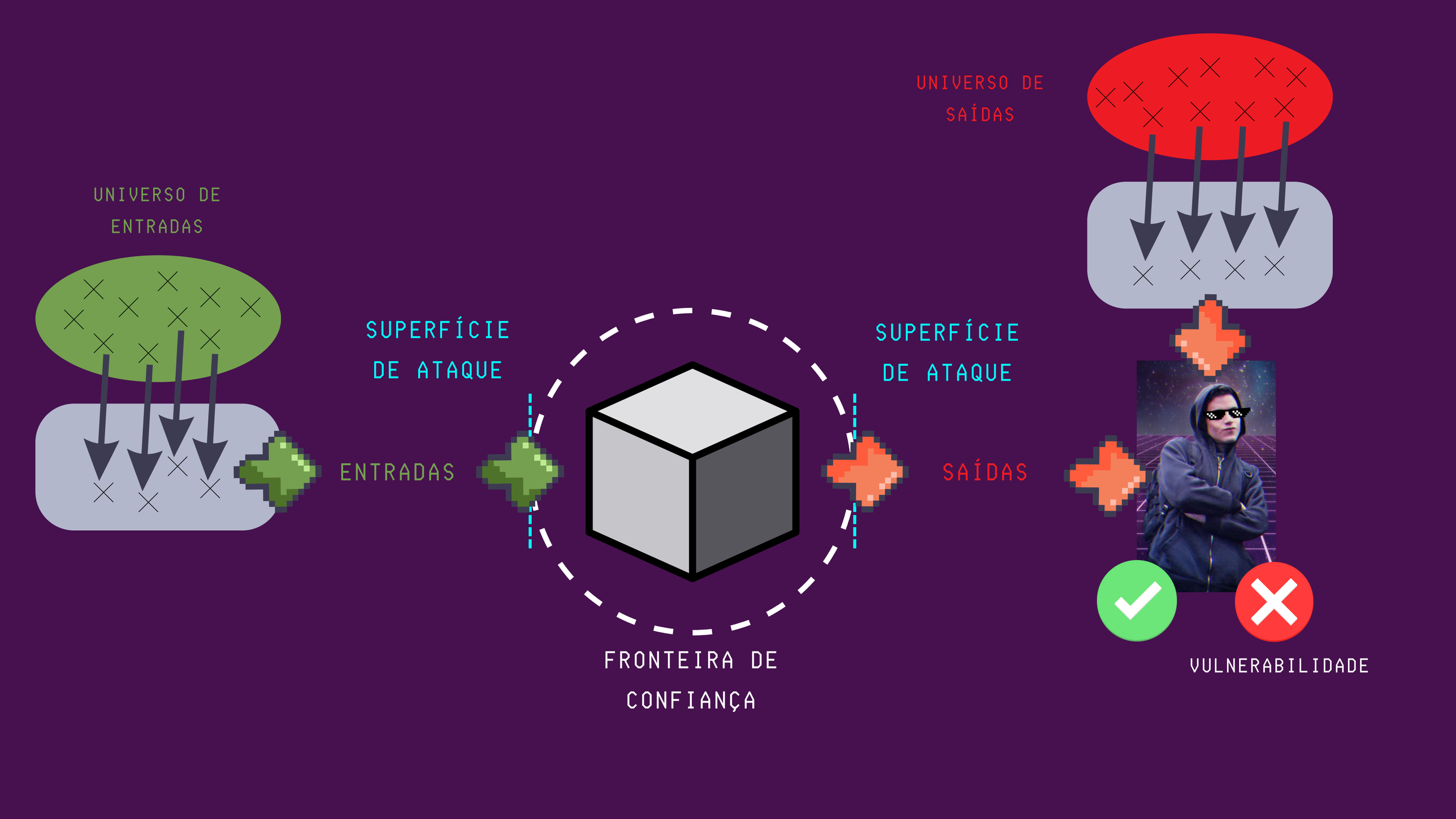
FRONTEIRA DE
CONFIANÇA

SUPERFÍCIE
DE ATAQUE

SAÍDAS

UNIVERSO DE
SAÍDAS




UNIVERSO DE
ENTRADAS
SUPERFÍCIE
DE ATAQUE
ENTRADAS
FRONTEIRA DE
CONFIANÇA
SUPERFÍCIE
DE ATAQUE
SAÍDAS
UNIVERSO DE
SAÍDAS
VULNERABILIDADE

MENU

Básico de Sec em “5” minutos a.k.a. Missão: Impossível

A TODO list perdida de um analista de segurança

A TODO list perdida de um engenheiro de segurança

Gostei! Por onde eu começo?

Dois dedos de juízo: não seja a vergonha da profission!

Não paramos por aqui

Q&A

A TODO LIST PERDIDA DE UM ANALISTA DE SEGURANÇA

```
~$ cat todo.txt
Revisar código do app X
Esclarecer vulnerabilidade X para a engenharia
Escrever PoC para explorar vulnerabilidade X
Escrever relatório de teste do app X
Reunião com Fulano do(a) marketing/comercial/engenharia/etc.
Kickoff de teste com cliente X
Resolver crackme/VM novo(a) # TODO detail
Estudar para certificação X # TODO detail
```

MENU

Básico de Sec em “5” minutos a.k.a. Missão: Impossível

A TODO list perdida de um analista de segurança

A TODO list perdida de um engenheiro de segurança

Gostei! Por onde eu começo?

Dois dedos de juízo: não seja a vergonha da profission!

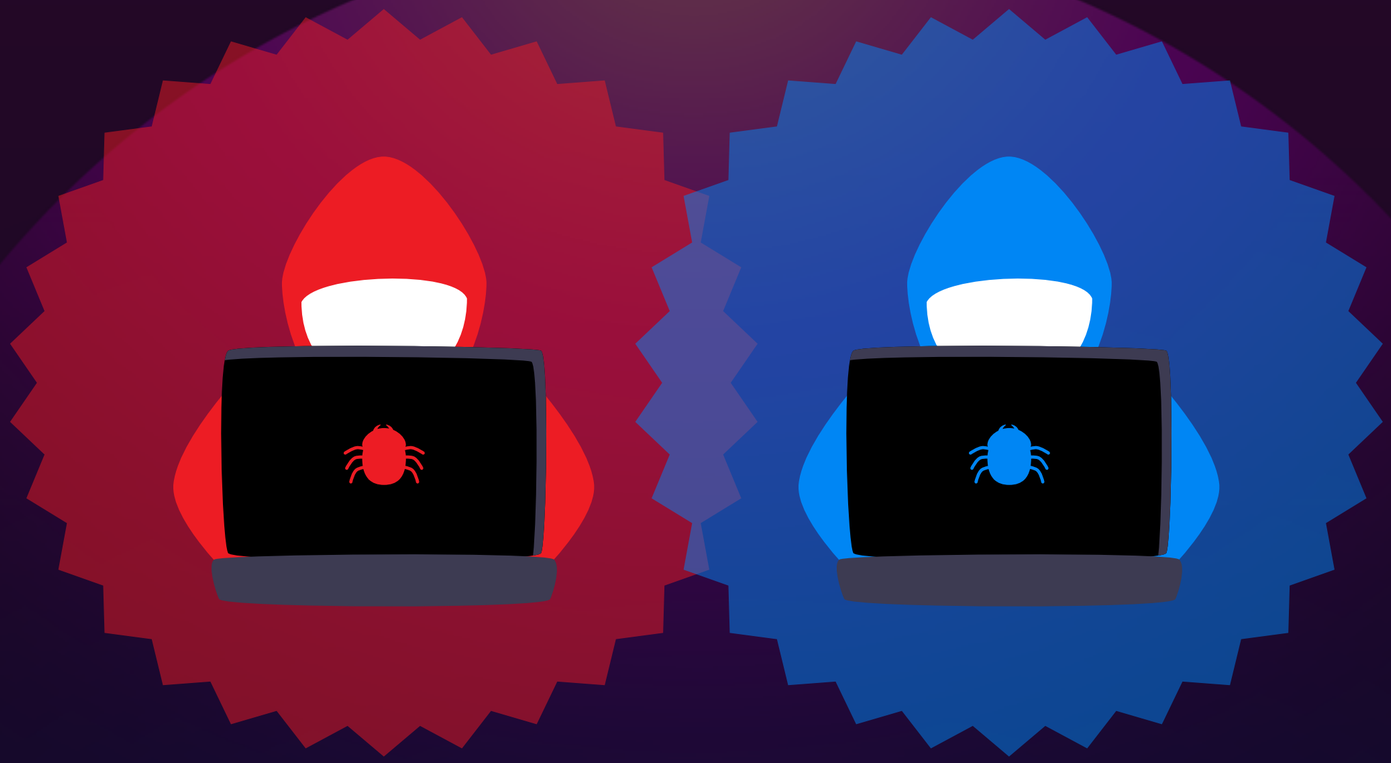
Não paramos por aqui

Q&A

A TODO LIST PERDIDA DE UM ENGENHEIRO DE SEGURANÇA

```
~$ cat todo.txt
Entender como estão fraudando o fluxo X do app X
Integrar lib de segurança X no app X e abrir MR/PR
Consertar job de segurança X da pipeline do app X e abrir MR/PR
Reunião com Fulano do(a) marketing/comercial/engenharia/etc.
Kickoff de projeto X com a engenharia
Desenhar fluxo sensível X do app X
Resolver crackme/VM novo(a) # TODO detail
Estudar para certificação X # TODO detail
```

RED TEAM BLUE TEAM



MENU

Básico de Sec em “5” minutos a.k.a. Missão: Impossível

A TODO list perdida de um analista de segurança

A TODO list perdida de um engenheiro de segurança

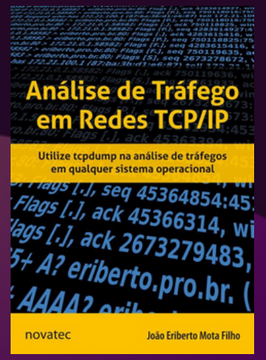
Gostei! Por onde eu começo?

Dois dedos de juízo: não seja a vergonha da profission!

Não paramos por aqui

Q&A

Aproveite a universidade. Preocupe-se com aprender, leve a sério, envolva-se.



Aprenda redes. A prática é tão importante quanto a teoria.

Aprenda a escrever software. Você não precisa ser um engenheiro de software excepcional, mas muito ajuda.

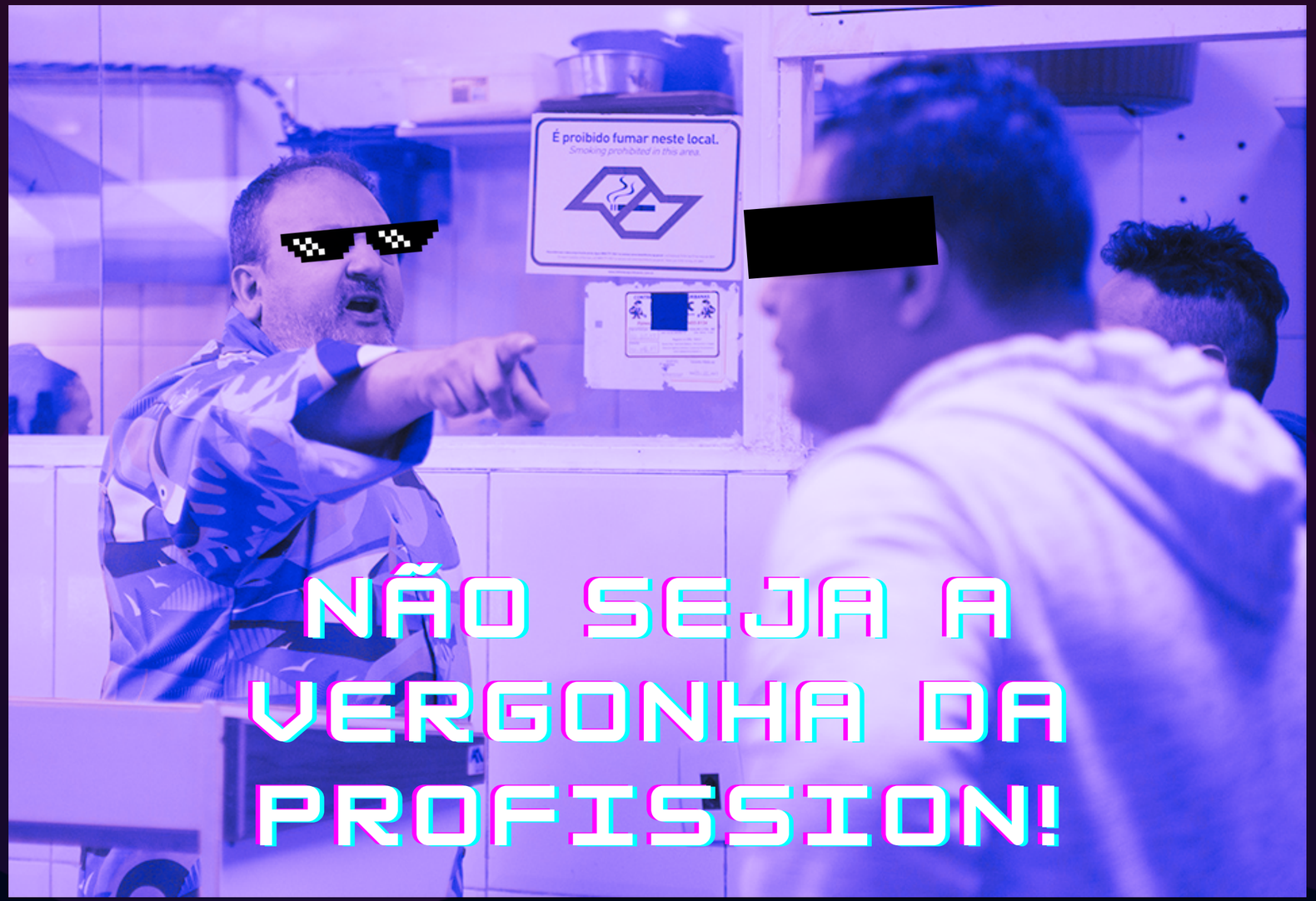
Vários links no final dessa apresentação!

Comece a aprender sobre segurança. Existem diversos recursos gratuitos e/ou baratos. Preocupe-se com aprender direito, não com volume.

Aprenda Linux.

Encontre um nicho de segurança que você goste e procure aprender mais sobre ele. Existem vários.

DOIS DEDOS DE JUÍZO



Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Vigência

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

MENU

Básico de Sec em “5” minutos a.k.a. Missão: Impossível

A TODO list perdida de um analista de segurança

A TODO list perdida de um engenheiro de segurança

Gostei! Por onde eu começo?

Dois dedos de juízo: não seja a vergonha da profission!

Não paramos por aqui

Q&A

ALGUNS RECURSOS DE APRENDIZAGEM

https://tryhackme.com/
https://www.hackthebox.com/
https://portswigger.net/web-security
https://blueteamlabs.online/
https://mas.owasp.org/crackmes/
https://owasp.org/www-project-vulnerable-web-applications-directory/
https://www.youtube.com/@_JohnHammond
https://www.youtube.com/@TCMSecurityAcademy

CONTINUAR EM CONTATO/SLIDES

https://vasconcedu.github.io/