

אינטל: על יזמות, טכנולוגיה ומה שביניהם, או איד
? הגעתי לכאן בכלל

LEGAL NOTICES AND DISCLAIMERS

This presentation contains the general insights and opinions of its author, Guy Barnhart-Magen. I am speaking on behalf of myself only, and the views and opinions contained in this presentation should not be attributed to my employer.

The information in this presentation is provided for informational and educational purposes only and is not to be relied upon for any other purpose. Use at your own risk! I makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. I accept no duty to update this presentation based on more current information. I disclaim all liability for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of or reliance on the content of this presentation.

No computer system can be absolutely secure.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

*Other names and brands may be claimed as the property of others.

WHO AM I?

- Guy Barnhart-Magen
- **Security Researcher**,
Manager, Presenter
- Worked in:
 - 3 Startups, 3 Corporates
- **iSTARE** team
 - Intel Security Threat Analysis and Reverse Engineering
- “We break what we make”



a bit narcissst, isn't it?



My Journey





• https://upload.wikimedia.org/wikipedia/commons/thumb/6/69/IBM_PC_AT.jpg/1200px-IBM_PC_AT.jpg

MAIN MENU

System Commands

to Pause
(ACE) to abort
-O On-Line Help
-T Display System Time
Join Conference(if avail)
Extended Commands Menu
e -T-ransfers
On-line Programs (Doors)
defaults -G -files

Message Subs

* List Available Subs
R- remove a Message
P- post a Message
> + Advance one Sub #
< - Retreat one Sub #
N-ew Message s
Q- N-Scan Current
S- can Message Tit
Z- Continuous N-S
Goto Sub # Pres

Electronic Mail

F-eedback to Sysop
M-ailbox scan
E-Mail a U
K-ill E-mail You s

Misc Commands

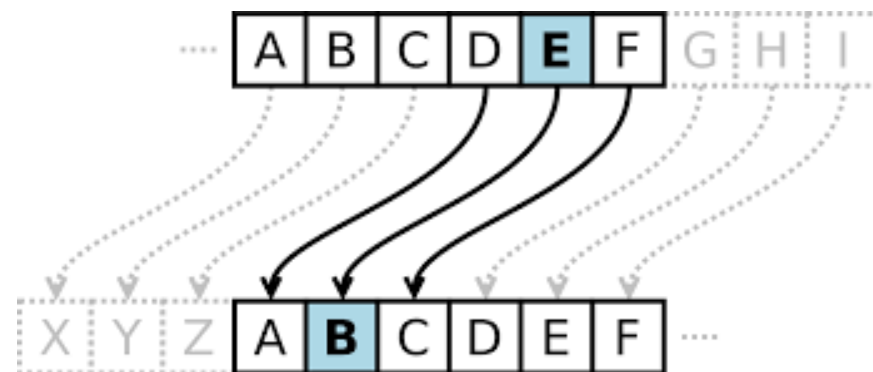
Auto-Message
O-ff
our info

U- ser List
B- BS List

C- hat with Sysop
V- oting Booth

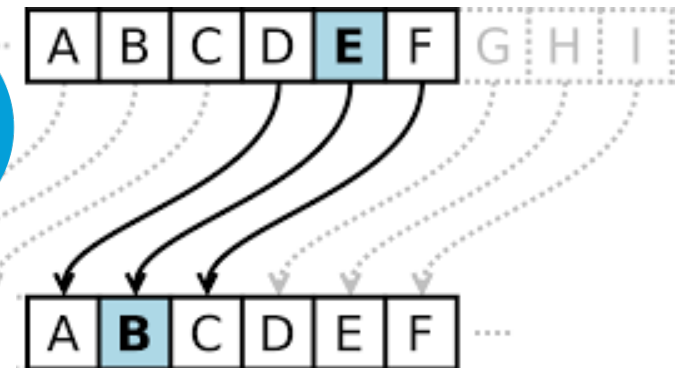
System I- nfo
L- ast Callers Today
X- Toggle Expert/Novi







CISCO

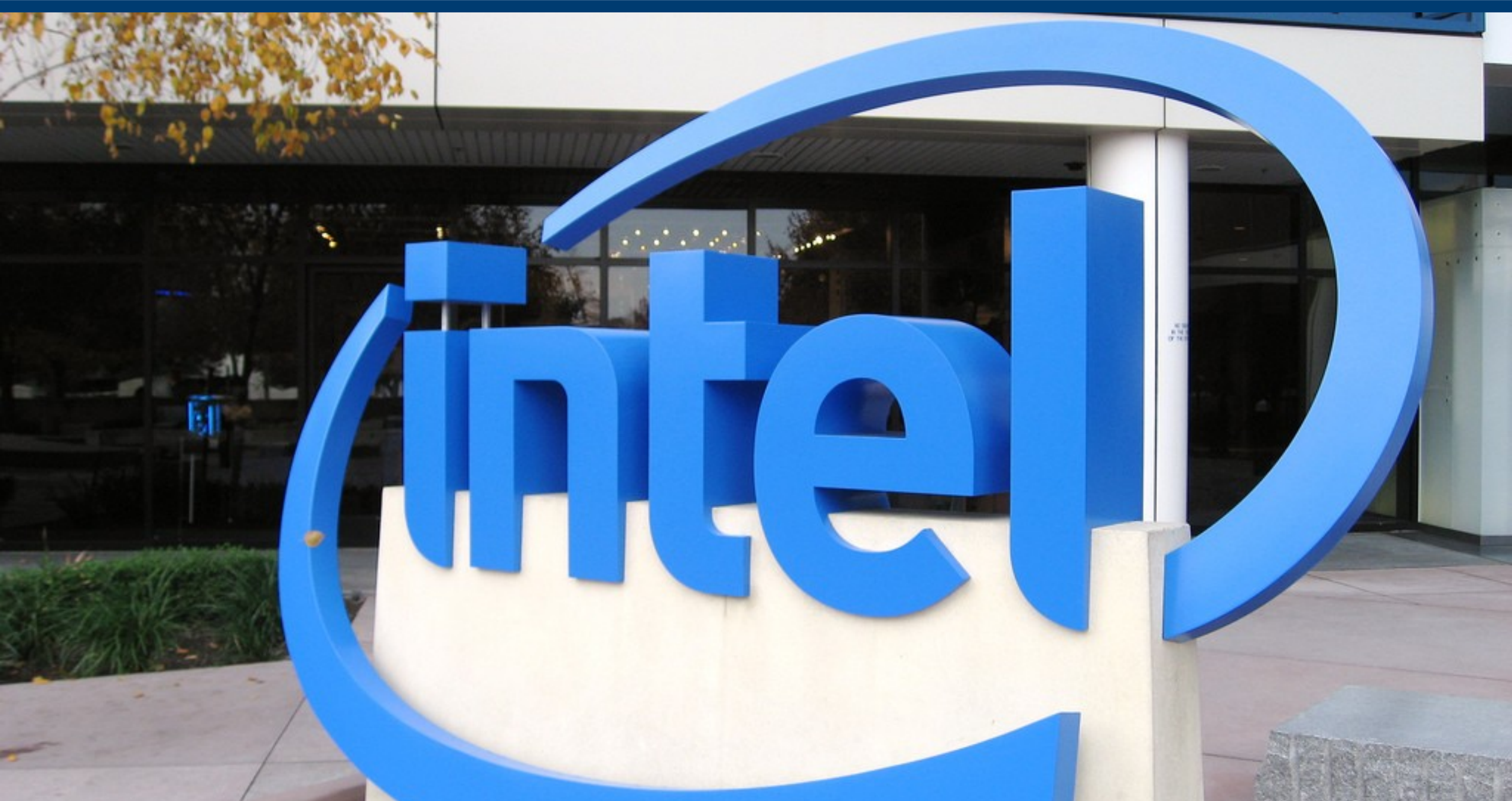


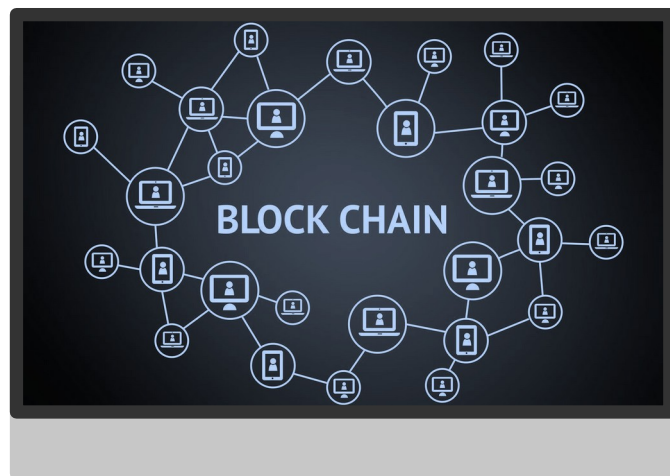
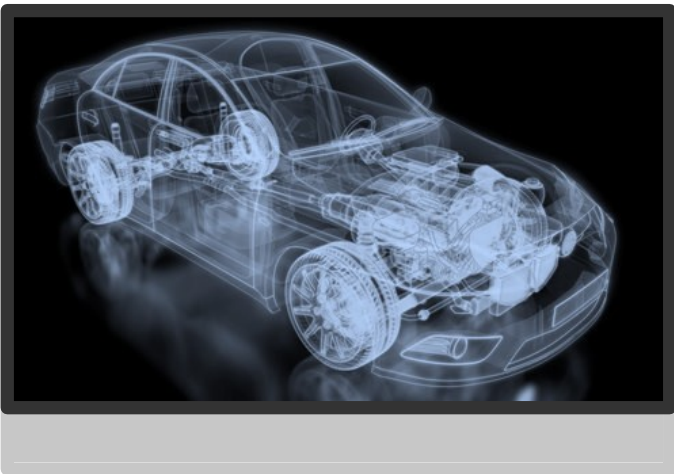


<https://i.imgur.com/XI9wDA9.png>



NATION 
where power gets smart







דברים שרואים מכאן

TRADEOFFS

- Limited resources
- Always almost out of runway
- Pressure to deliver
- Next paycheck?
- Excitement!
- Control and influence
- Lot's of resources
- Paycheck guaranteed
- Time for side projects
- More rules
- Limited control and influence

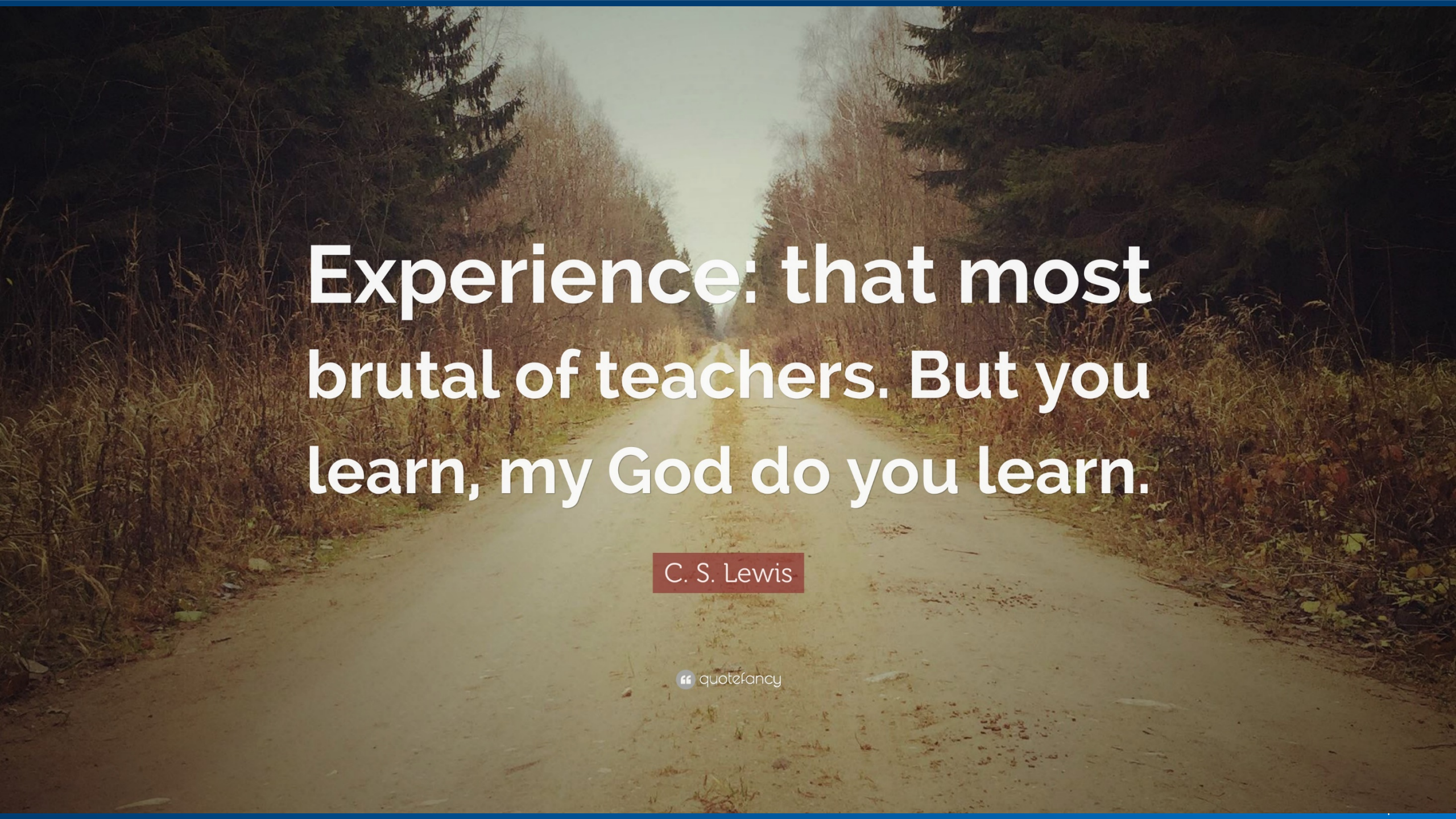
THE GOLDEN CAGE

- Payment is good
- Usually does good for your CV
- Benefits
- Less pressure
- Takes courage to leap!



WHAT SUITS YOU BETTER?

- Do you have a family to care for?
- Do you mind taking risks (don't have to like it)?
- Do you want more experience or more excitement?
- Are you OK with failing?



**Experience: that most
brutal of teachers. But you
learn, my God do you learn.**

C. S. Lewis

This is what The Imposter Syndrome sounds like

“Sometimes I find I’m beating myself up because I feel like I just can’t do enough. There’s just so much that needs to be done.”

– Sarah, CEO

“I’ve doubted myself in every career move I’ve made. In leadership, you’re expected to have all the answers, most times I’m guessing and hoping for the best.”

– Todd, VP of Customer Success

“I feel like a fraud every day. It’s a constant struggle but I have to remind myself that sometimes you have to be the best person to do something, even if you think you don’t think you’re supposed to be that person.”

– Randal, CPO

“With every new challenge, I doubt my ability to act and make the right call because I know I don't really have the information, yet I don't have time to waste getting that information before making the call.”

– Nate, CTO



2018 BSIDES TLV

19.6.18
10AM until After Party

**Bar Shira Auditorium
Tel Aviv University**

www.bsidesTLV.com

BSidesTLV takes place during Tel Aviv Cyber Week, June 17-21, 2018

• <https://pbs.twimg.com/media/DVgh2GJW0AA-IKs.jpg>

Let's get to 51%

Help Me!

Entrepreneurs Investors & Industry Leaders

Meet leading entrepreneurs top investors & industry leaders

Looking for a professional advice?

Meet top service providers & experts!



Admin

Meet Me

Boaz Katz
Co-Founder & Chief Product
Strategy at Bizzabo
Tel Aviv



Admin

Meet Me

Yonatan Zur
CEO & Co Founder
Regulus Cyber
Tel Aviv & Haifa



Meet Me

Yaniv Golan
General Partner
Iool ventures
Tel Aviv



Coming Soon

Rona Segev
Partner
TLV Partners
Tel Aviv



Meet Me

Eran Ben Shushan
CEO and Co-founder at
Bizzabo
NYC



Meet Me

Asaf Horesh
Partner at Vintage
Investment Partners
Tel Aviv & Herzlia



Coming Soon

Gigi Levy-Weiss
Founding Partner
NFX
Herzlia



Meet Me

Inbal Orpaz
High Tech Correspondent
The Marker
Tel Aviv



Email Me



Meet Me



Email Me



Email Me

GOT BALANCE?



WHAT IS A RED TEAM?

Artificial
Intelligence
Blockchain
Automotive & 5G
Trusted Execution
SW/FW Reverse
Engineering



• <https://media.giphy.com/media/9WC8WTZsFxxRi/giphy.gif>



MR. ROBOT

- <http://www.awardsdaily.com/tv/wp-content/uploads/2016/05/mr.-robot-key-art.jpg>

HACKERS?

1. Think outside the box
2. Exploit unexpected behavior
3. ...
4. Profit!
5. Greater value to our customers



- <https://2.bp.blogspot.com/-grZ1iqqZyrk/VysQmdK0aPI/AAAAAAAAAn9U/HYFNfNPcSvEbQu-7Wdt5zbzKNyFbnsBeACLcB/s1600/email-password-hack.jpg>

EXAMPLE?

WHAT IS SQL INJECTION?

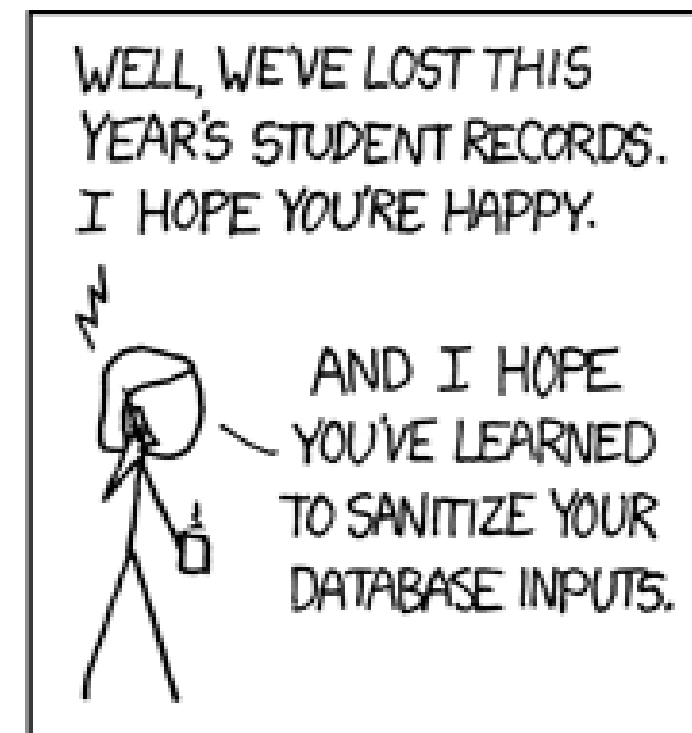
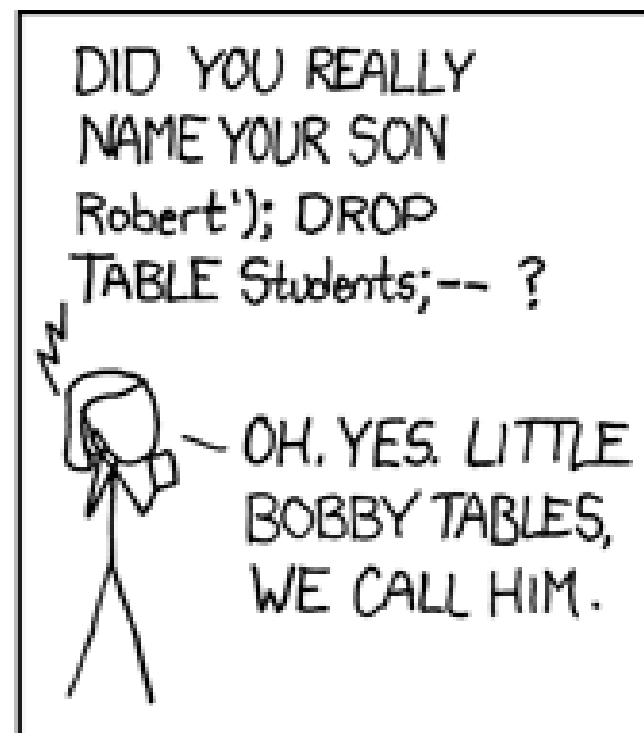
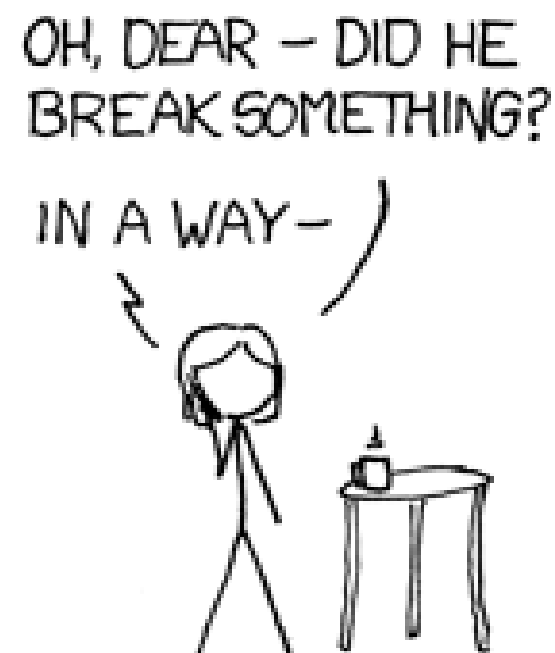
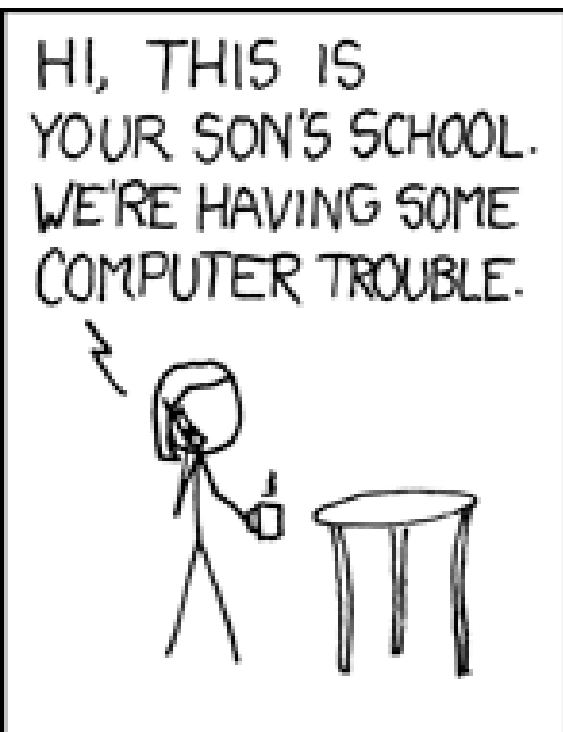
- How do I lookup a user in the database?

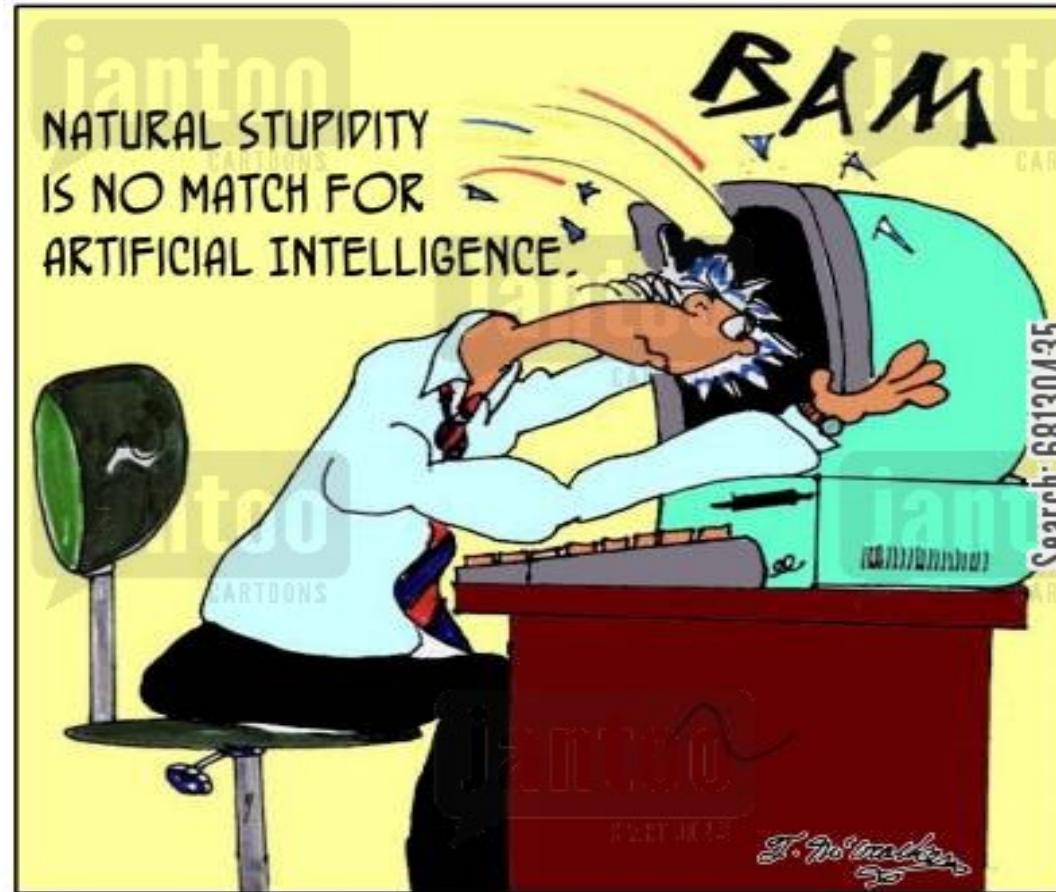
```
userQuery= "SELECT * FROM users WHERE  
name = ' " + userName + " ' ;"
```

- The user supplies the input “userName”
- What can I do with that assumption?
 - Think outside the box, don't do the expected...









- http://lowres.jantoo.com/it-computers-computer_engineer-computer_crash-software_engineer-intelligent-computer_user-68130435_low.jpg

ARTIFICIAL INTELLIGENCE



- <https://upload.wikimedia.org/wikipedia/commons/e/e3/CleverHans.jpg>

CLEVER HANS

“INTELLIGENT” SYSTEM

Building machines and algorithms which are capable of accomplishing computational tasks that would require human like cognitive abilities

Most AI were designed to solve a specific problem.



- <https://thumbs.gfycat.com/OpulentEvenBaleenwhale-max-1mb.gif>



MACHINE LEARNING TYPES

- <https://8.smash.com/u/2016/03/The-Matrix.gif>

MACHINE LEARNING TYPES

Supervised Learning

Input and Output is specified for training

Unsupervised Learning

Only input is given to recognize patterns

Reinforcement learning

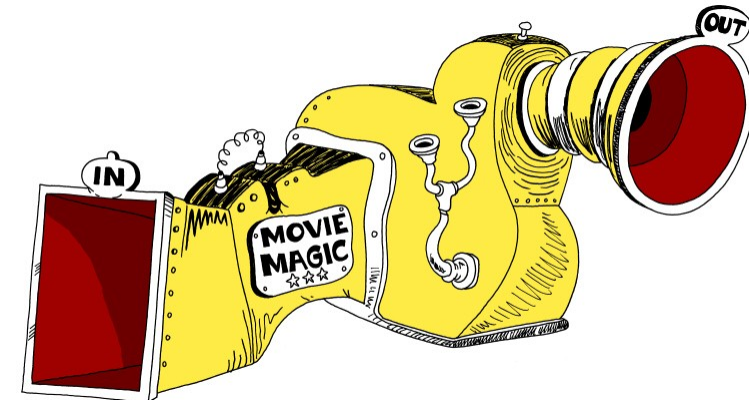
Real world feed back is provided to system on the go



CAT



DOG



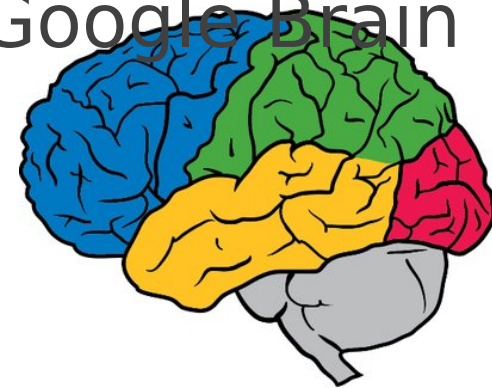
Feedback Generator

• <https://8.smash.com/u/2016/03/The-Matrix.gif>

“We have reached the point where machine learning works, but may **easily be broken**”

Nicolas Papernot, Google PhD Fellow in Security

Ian Goodfellow, Research scientist at Google Brain



<http://www.cleverhans.io/security/privacy/ml/2016/12/15/breaking-things-is-easy.html>

https://pbs.twimg.com/profile_images/799327801388077057/HcDnA1H7_400x400.jpg









Figure 5: The eyeglass frames used by S_C for dodging recognition against DNN_B .

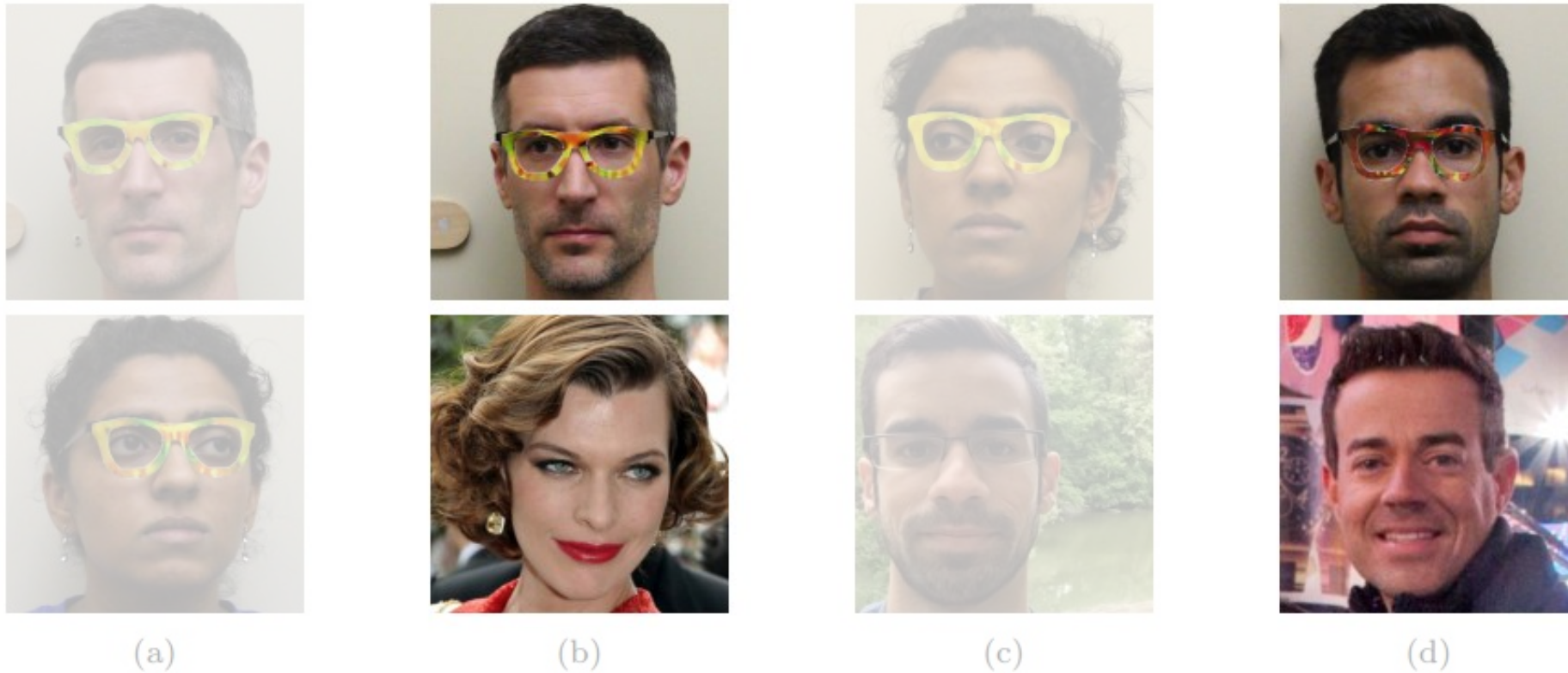


Figure 4: Examples of successful impersonation and dodging attacks. Fig. (a) shows S_A (top) and S_B (bottom) dodging against DNN_B . Fig. (b)–(d) show impersonations. Impersonators carrying out the attack are shown in the top row and corresponding impersonation targets in the bottom row. Fig. (b) shows S_A impersonating Milla Jovovich (by Georges Biard / CC BY-SA / cropped from <https://goo.gl/GlsWlC>); (c) S_B impersonating S_C ; and (d) S_C impersonating Carson Daly (by Anthony Quintano / CC BY / cropped from <https://goo.gl/VfnDct>).

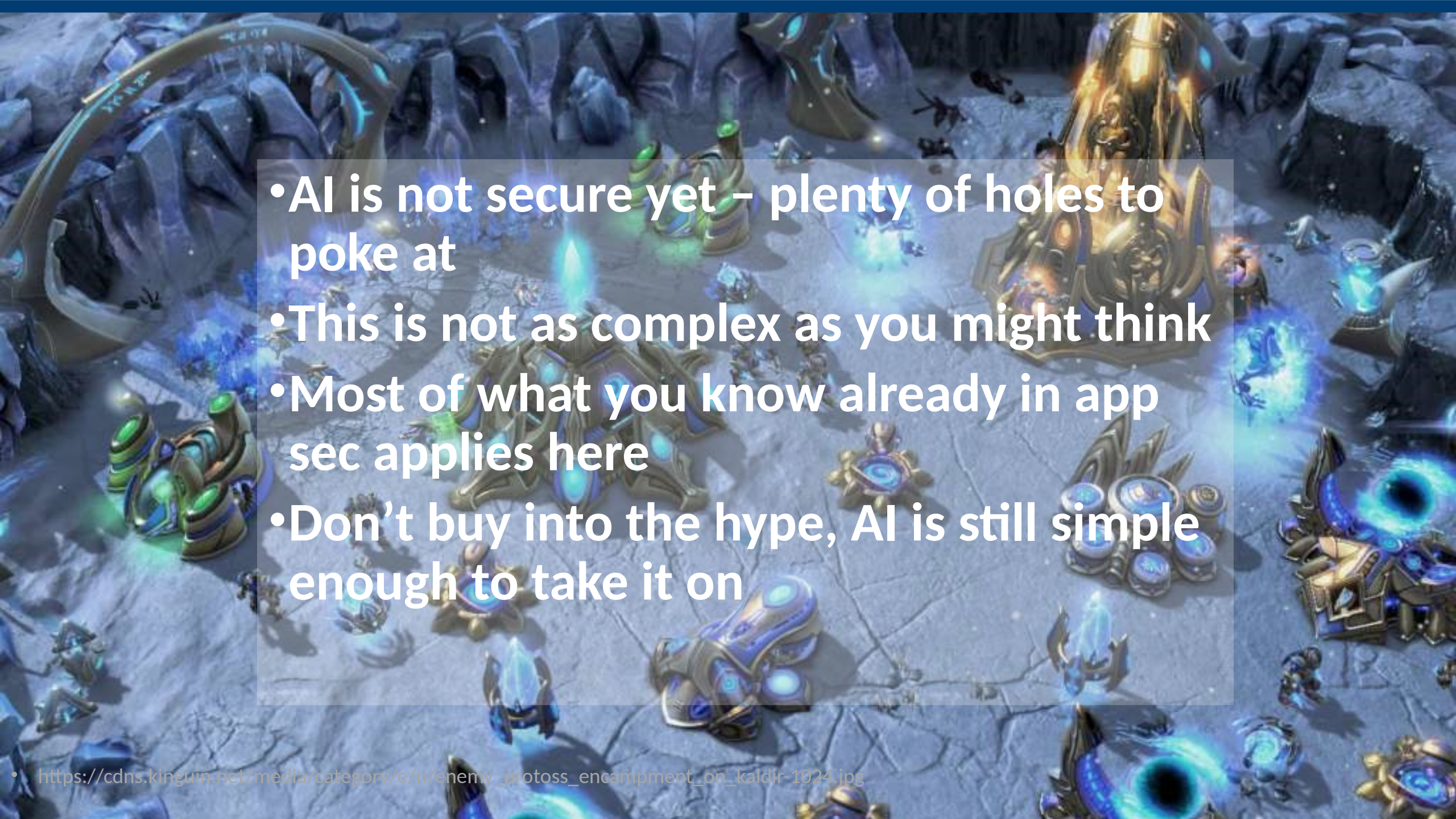


rifle

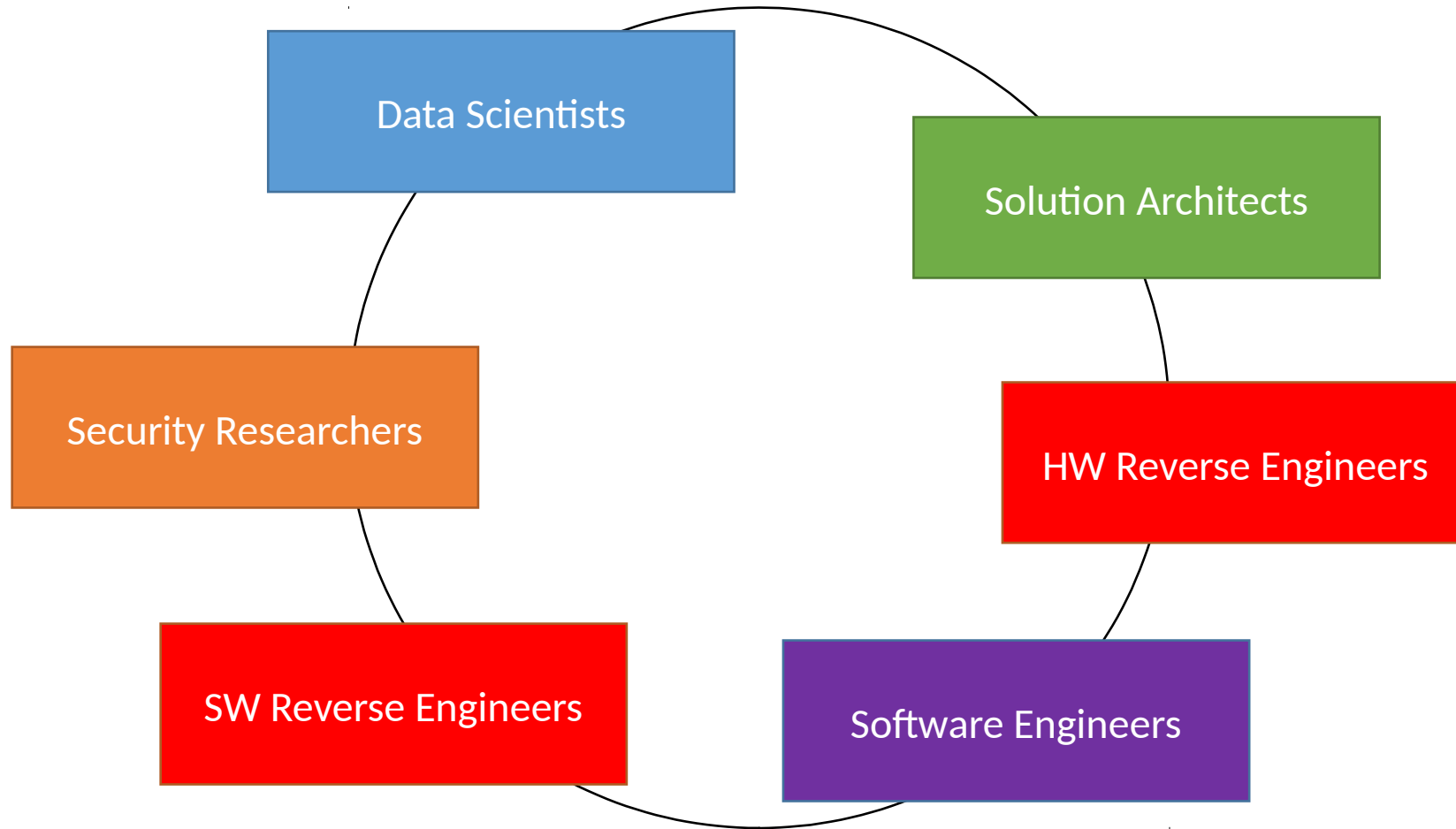
revolver, si

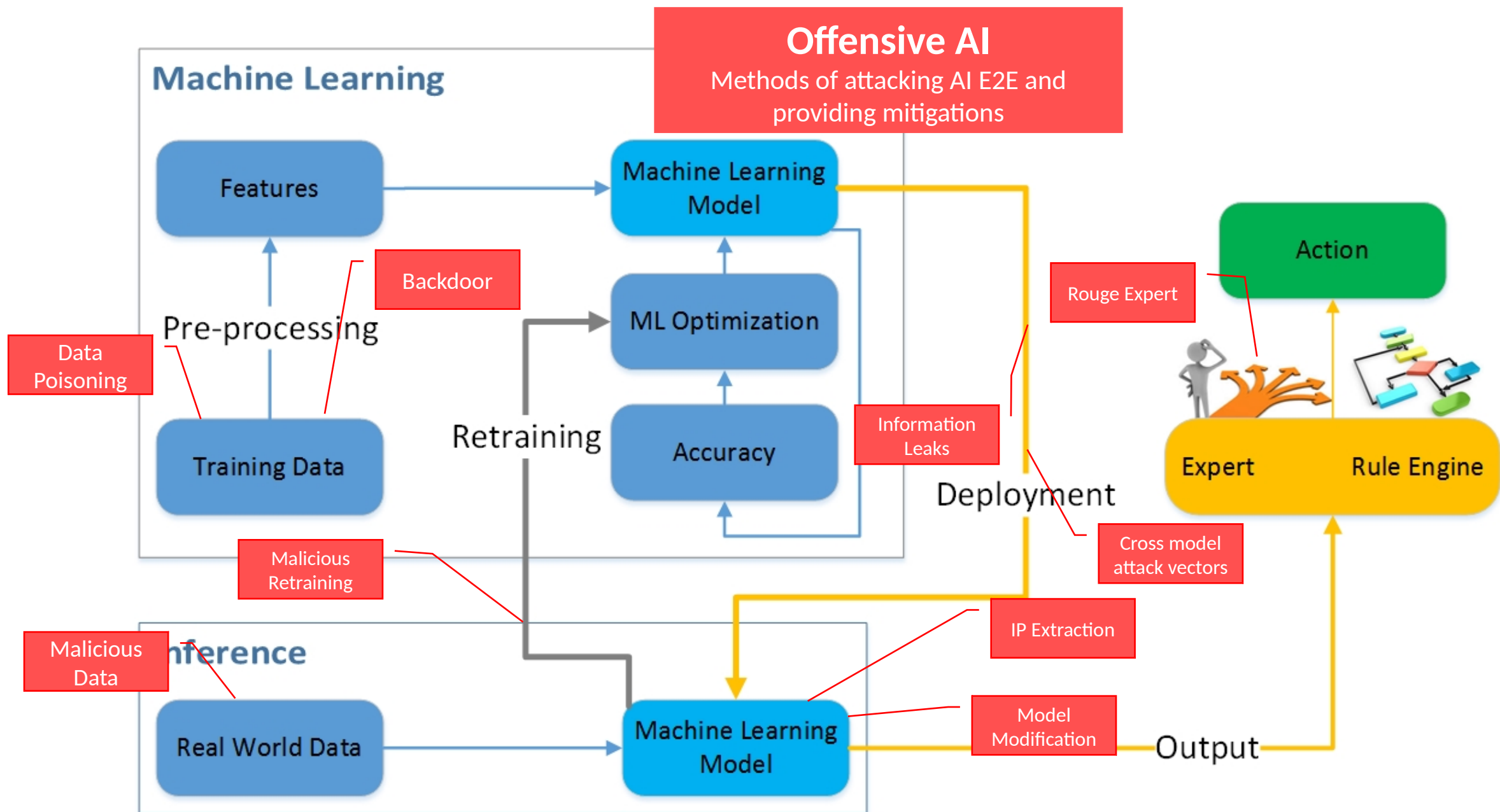
shield, buck

Classified as a **rifle** from
every angle!

- 
- AI is not secure yet – plenty of holes to poke at
 - This is not as complex as you might think
 - Most of what you know already in app sec applies here
 - Don't buy into the hype, AI is still simple enough to take it on

MULTI-DISCIPLINARY TEAM





Any Questions?



@barnhartguy

• <https://media.giphy.com/media/ejwFX1DPsfqec/giphy.gif>