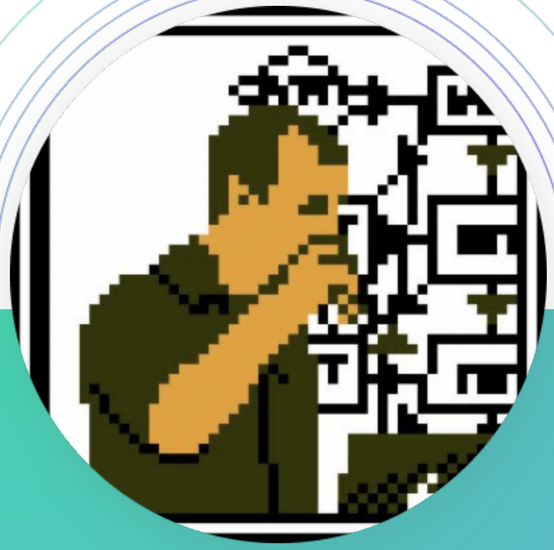
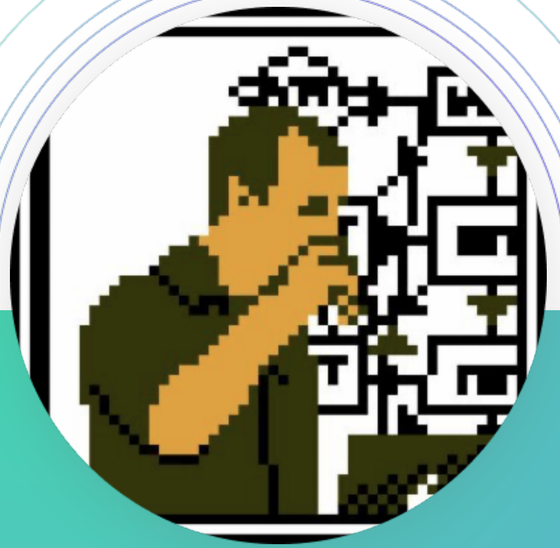
The Journey to **Mastery**

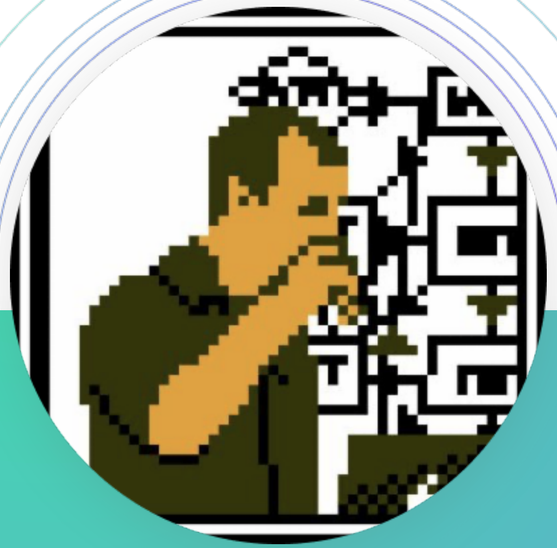
Louis Nyffenegger - BSides Canberra

30/09/2023





ABOUT ME:



ABOUT ME:

- Founder and CEO of PentesterLab

ABOUT ME:

- Founder and CEO of PentesterLab
- I run customer support 🛠️

ABOUT ME:

- Founder and CEO of PentesterLab
- I run customer support 🛠️
- Office Hours 🗓️


F.R.I.E.N.D.S

Customer Support

Customer Support

- Same issue… again & again & again

Customer Support

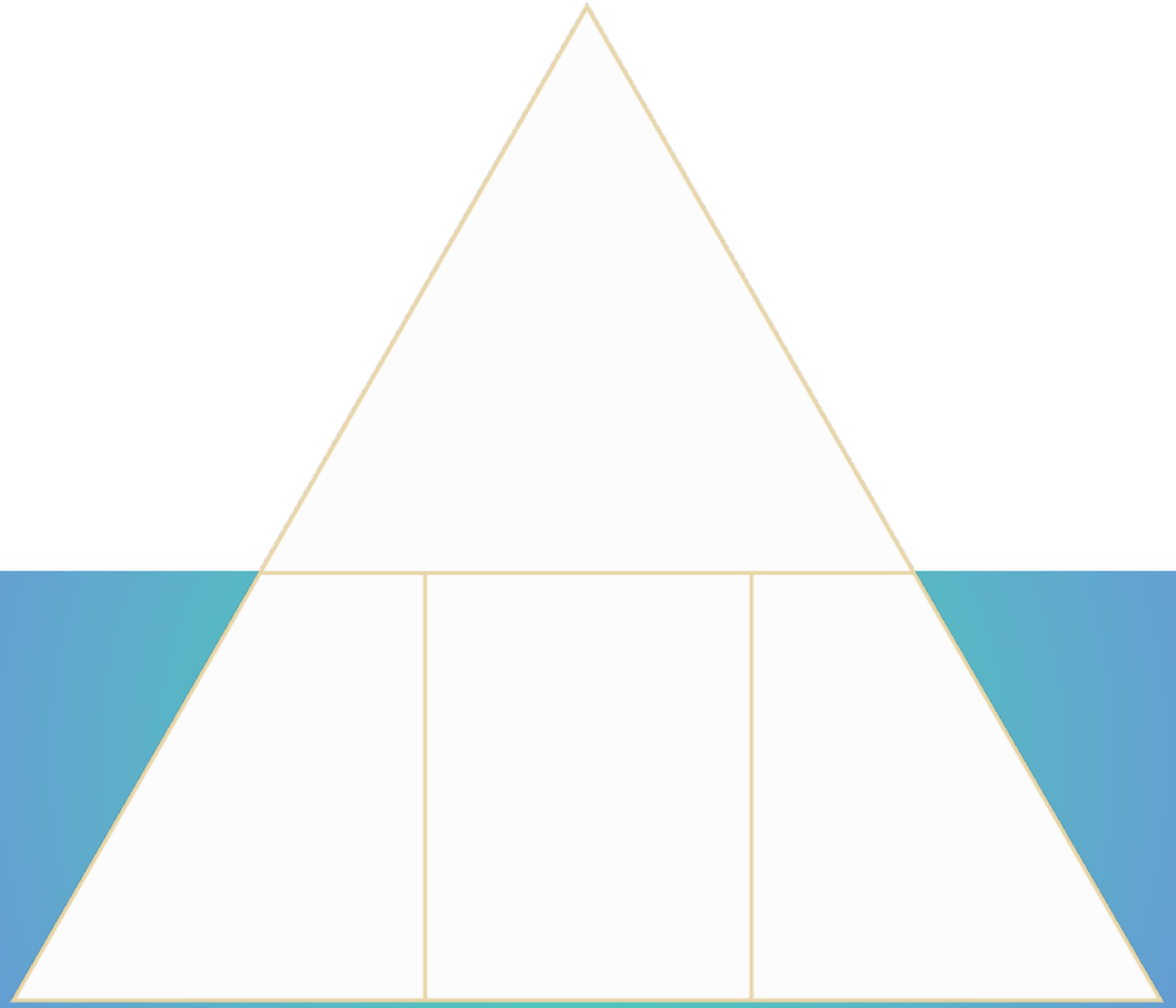
- Same issue… again & again & again
- Can you guess what the issue is?

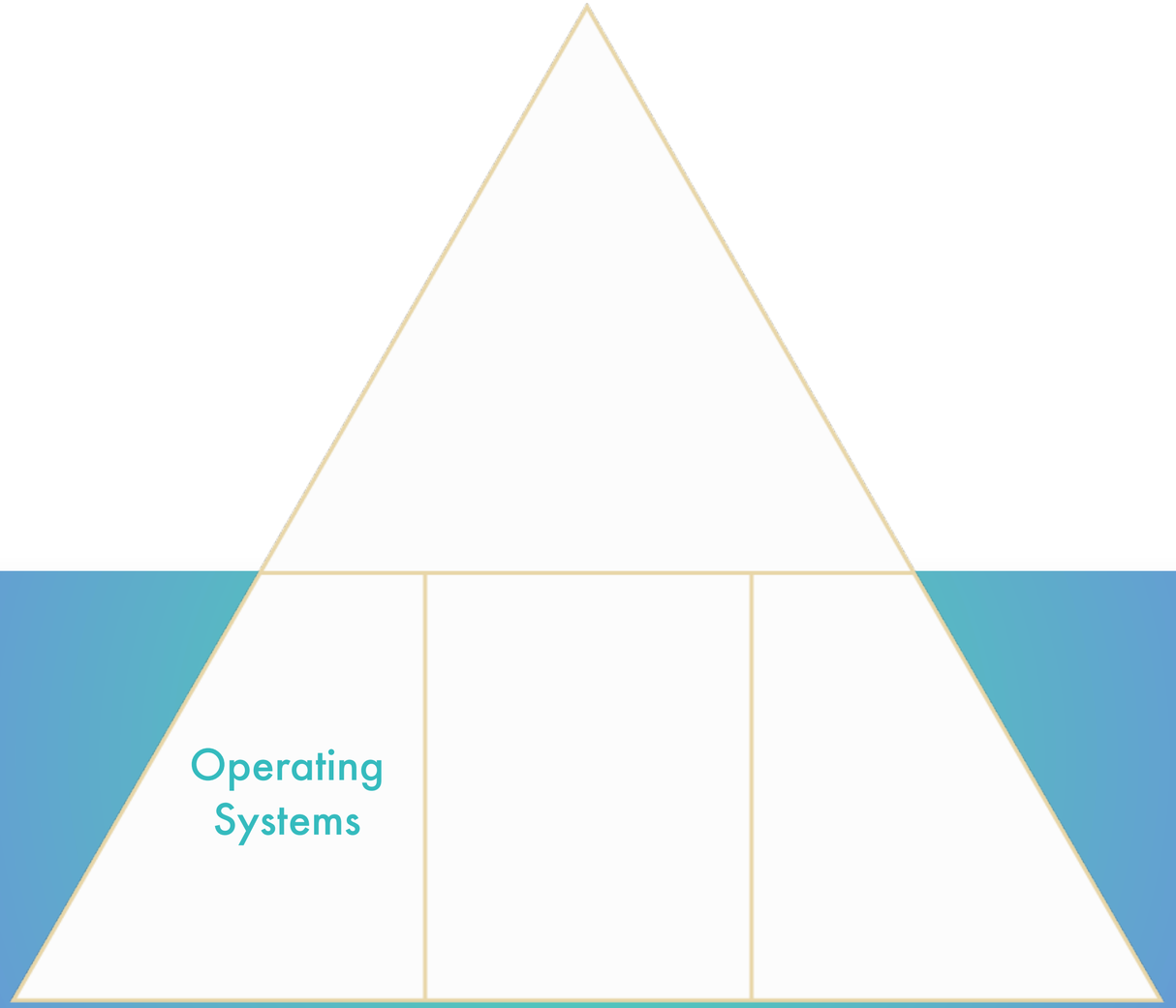
Customer Support

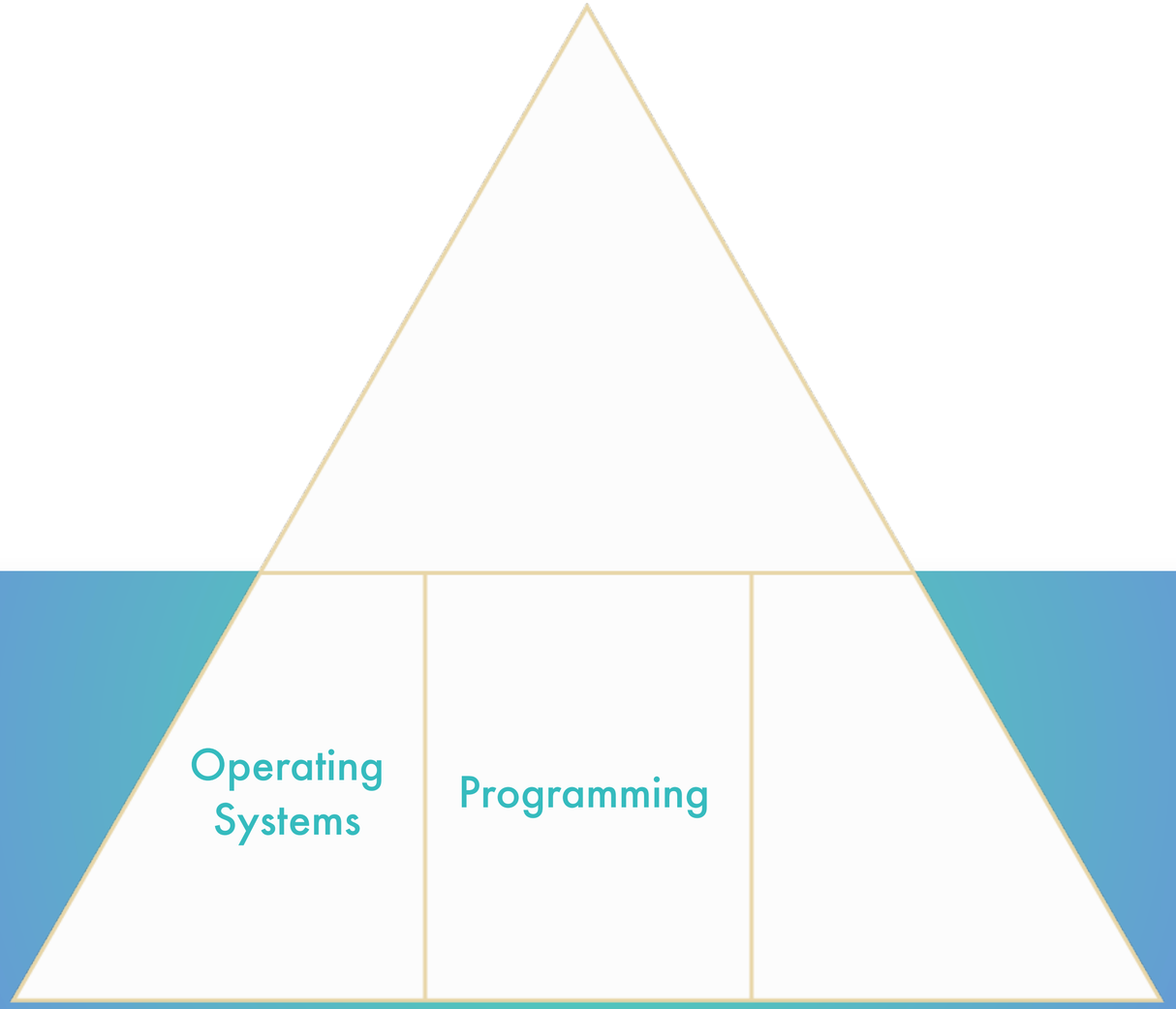
- Same issue… again & again & again
- Can you guess what the issue is?
- I'll give you a hint

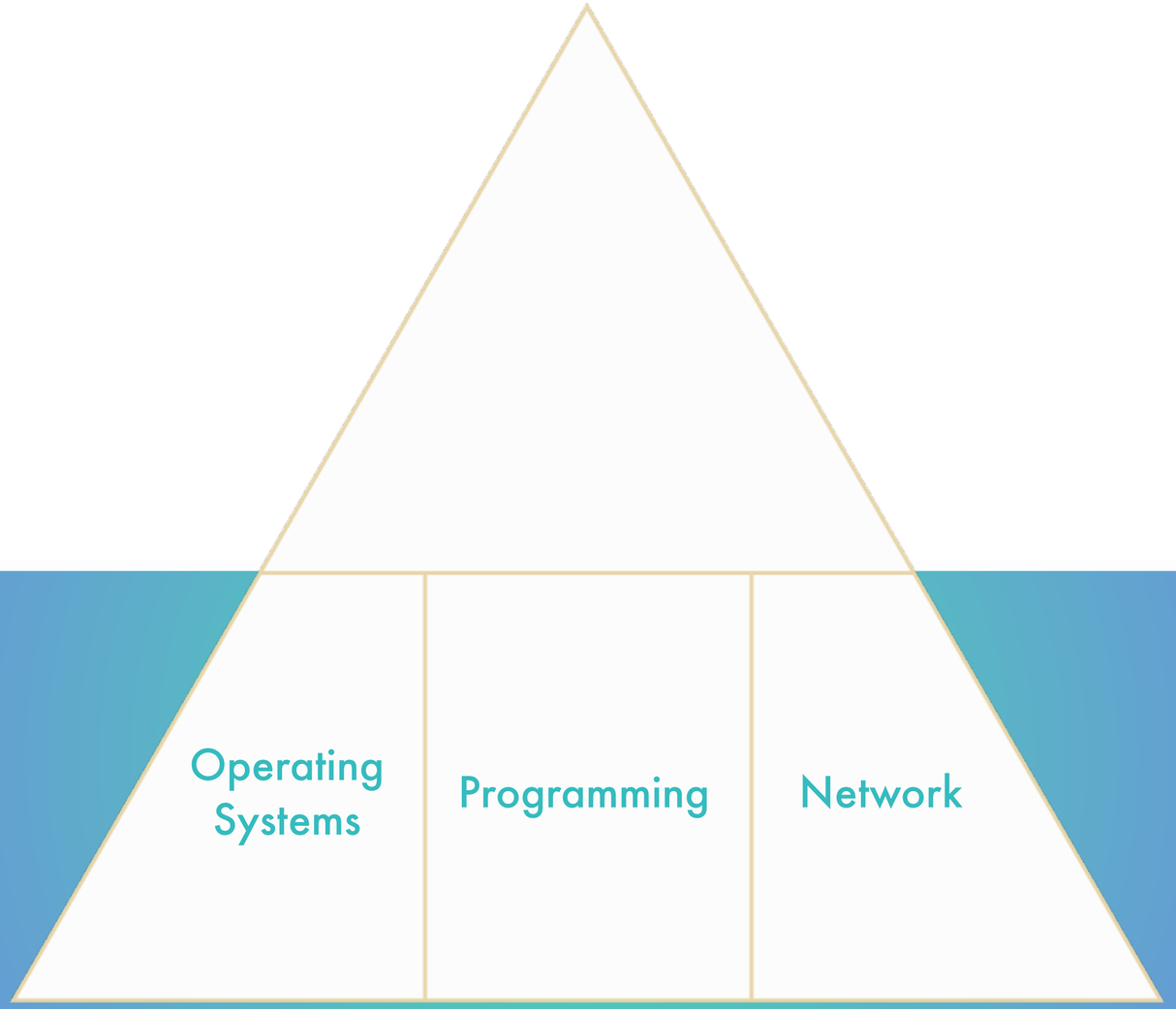
RFC 1918

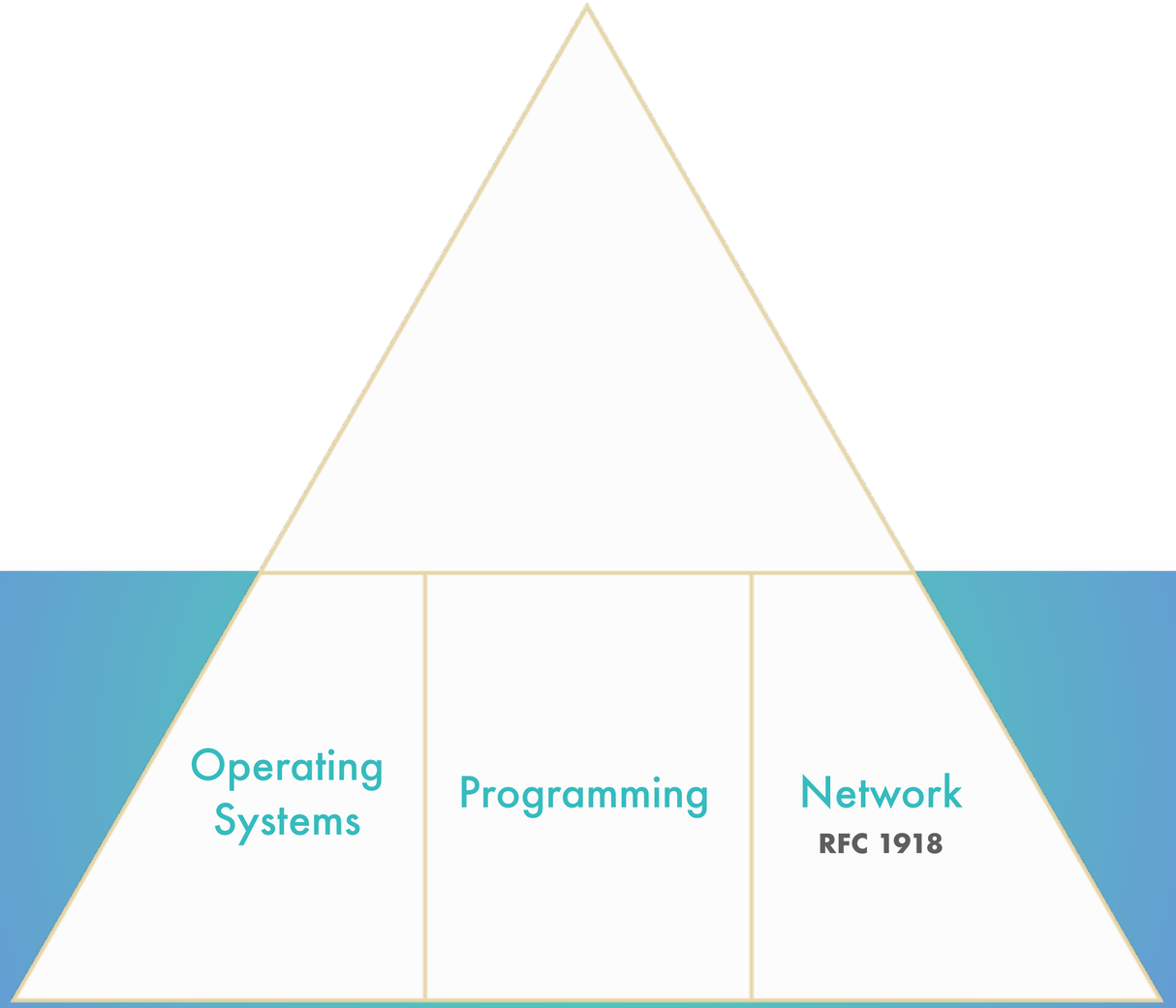

Speed Touch USB

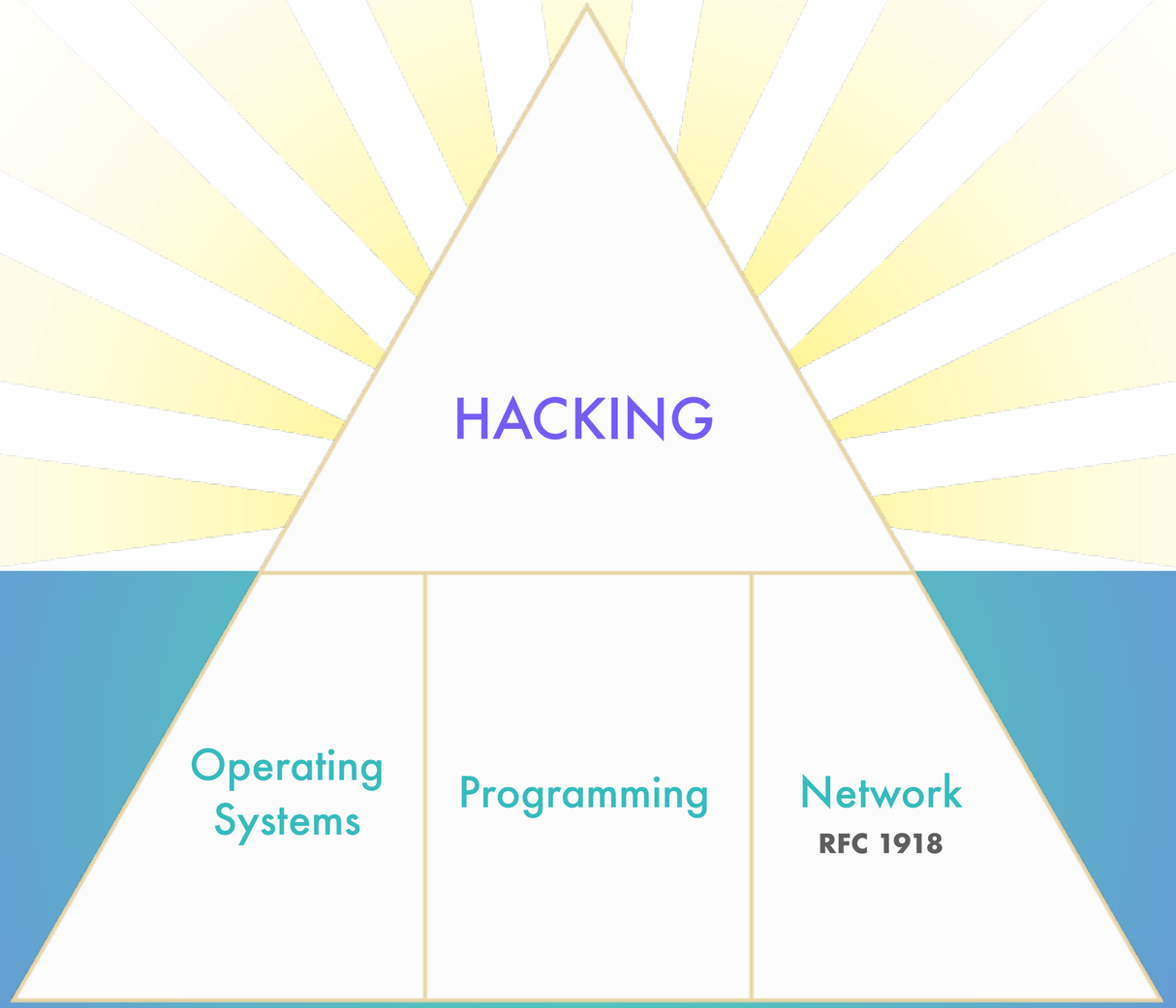



Operating
Systems


Operating Systems
Programming


Operating Systems
Programming
Network


Operating Systems
Programming
Network
RFC 1918


HACKING
Operating Systems
Programming
Network
RFC 1918

HACKING

HACKING

Network

HACKING

Network

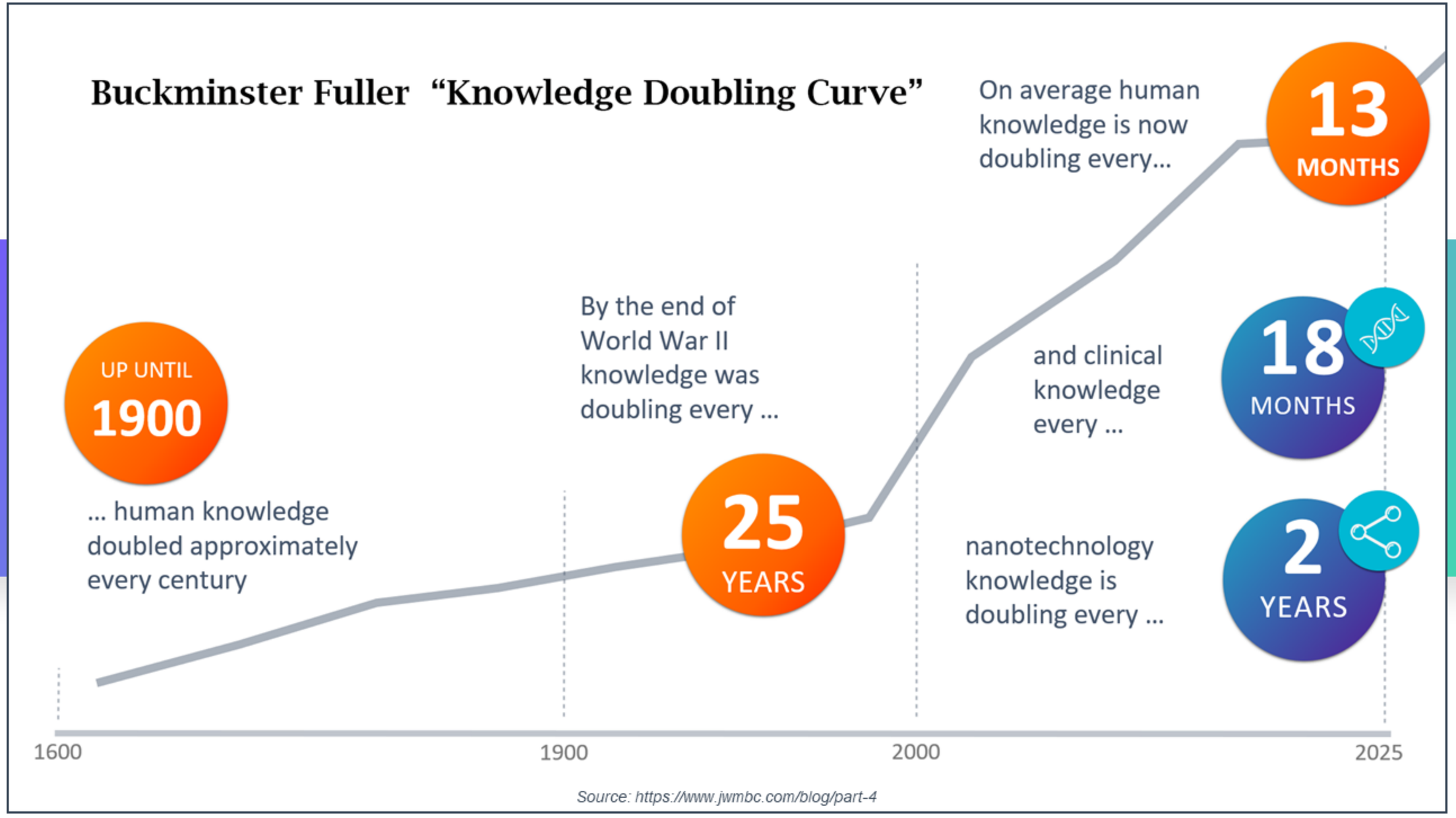
RFC 1918

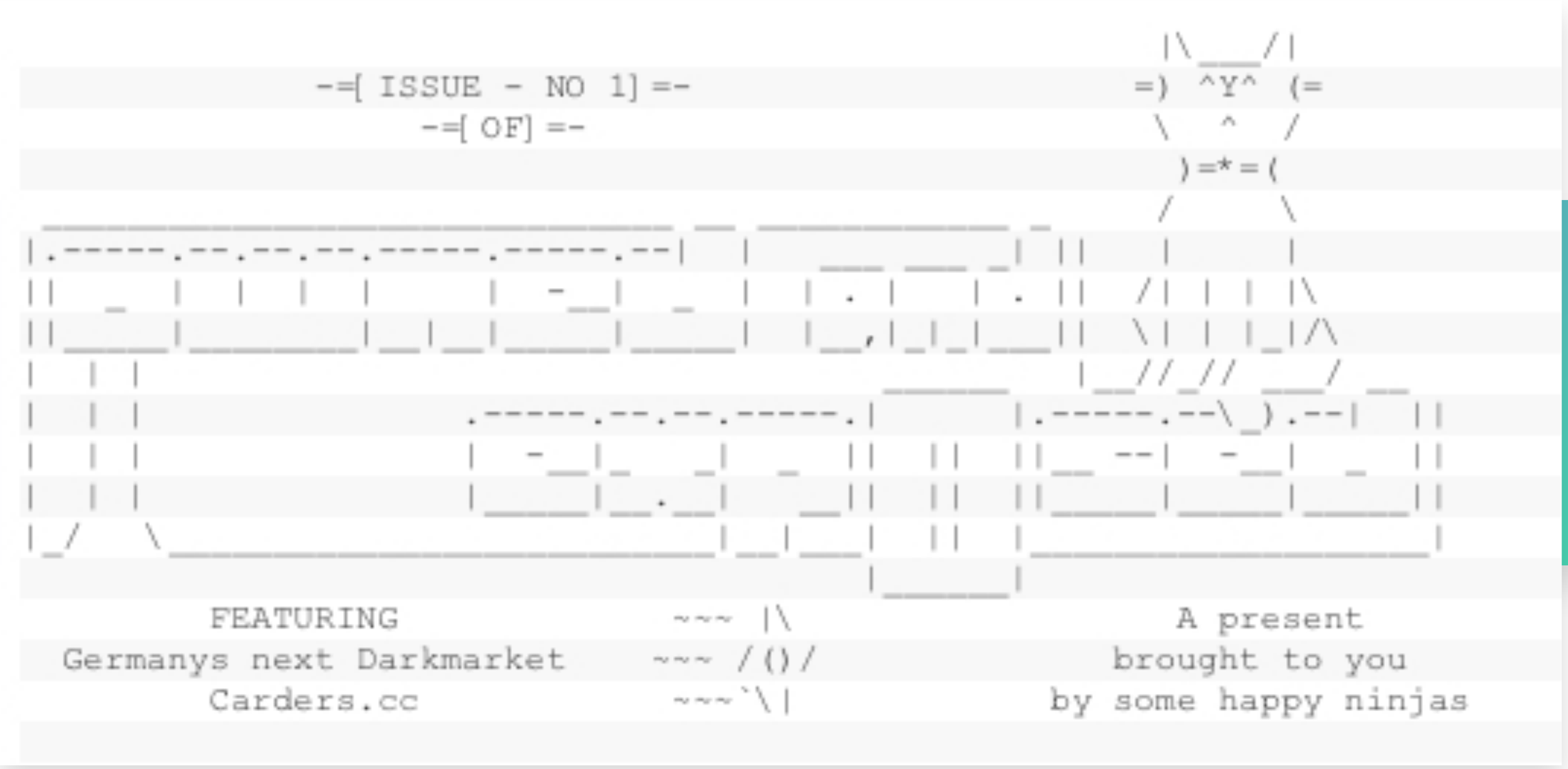
HACKING

JIT Learning…

Network

RFC 1918


Buckminster Fuller "Knowledge Doubling Curve"
UP UNTIL
1900
… human knowledge doubled approximately every century
By the end of World War II knowledge was doubling every …
25
YEARS
On average human knowledge is now doubling every…
13
MONTHS
and clinical knowledge every …
18
MONTHS
nanotechnology knowledge is doubling every …
2
YEARS
1600
1900
2000
2025
Source: https://www.jwmbc.com/blog/part-4


-=[ISSUE - NO 1] =-
-=[OF] =-
FEATURING
Germanys next Darkmarket
Carders.cc
A present
brought to you
by some happy ninjas

SOME KNOWLEDGE IS **NOW DISAPPEARING...**

SOME KNOWLEDGE IS **NOW DISAPPEARING…**

- Private research

SOME KNOWLEDGE IS **NOW DISAPPEARING…**

- Private research
- We forget

SOME KNOWLEDGE IS **NOW DISAPPEARING…**

- Private research
- We forget
- Artificial Intelligence

守　破　離

守　破　離

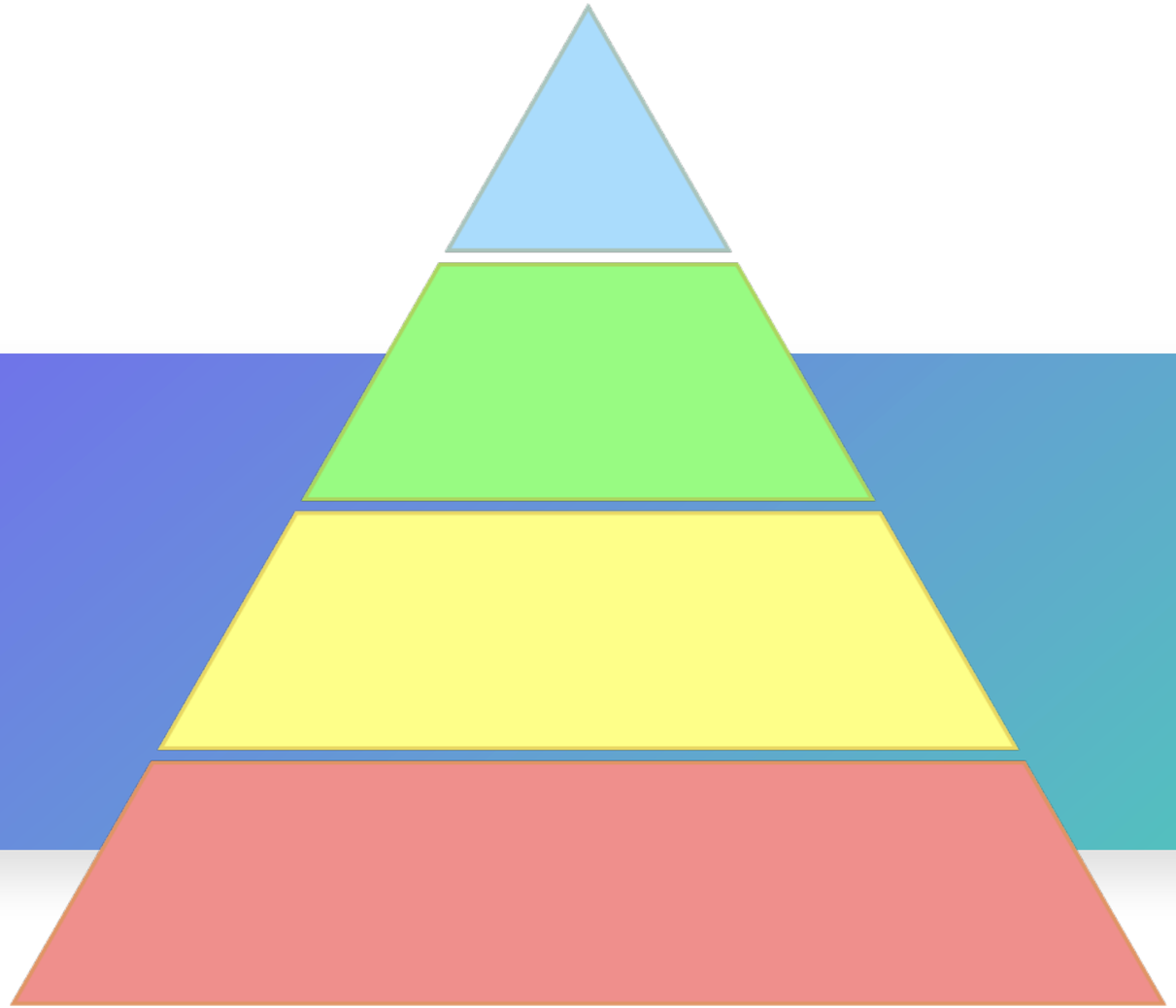
SHU

守　破　離

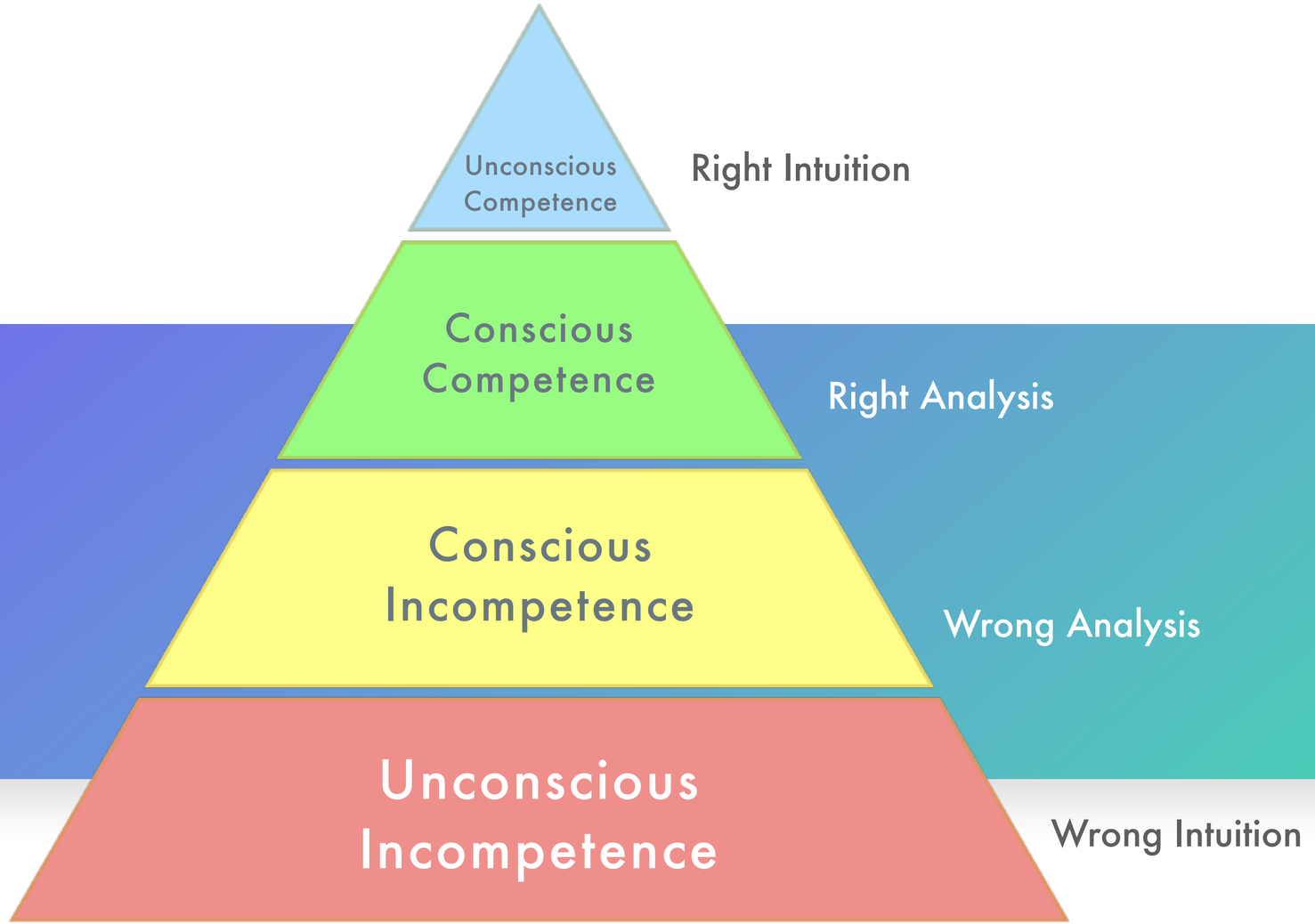
SHU　　HA

守　破　離

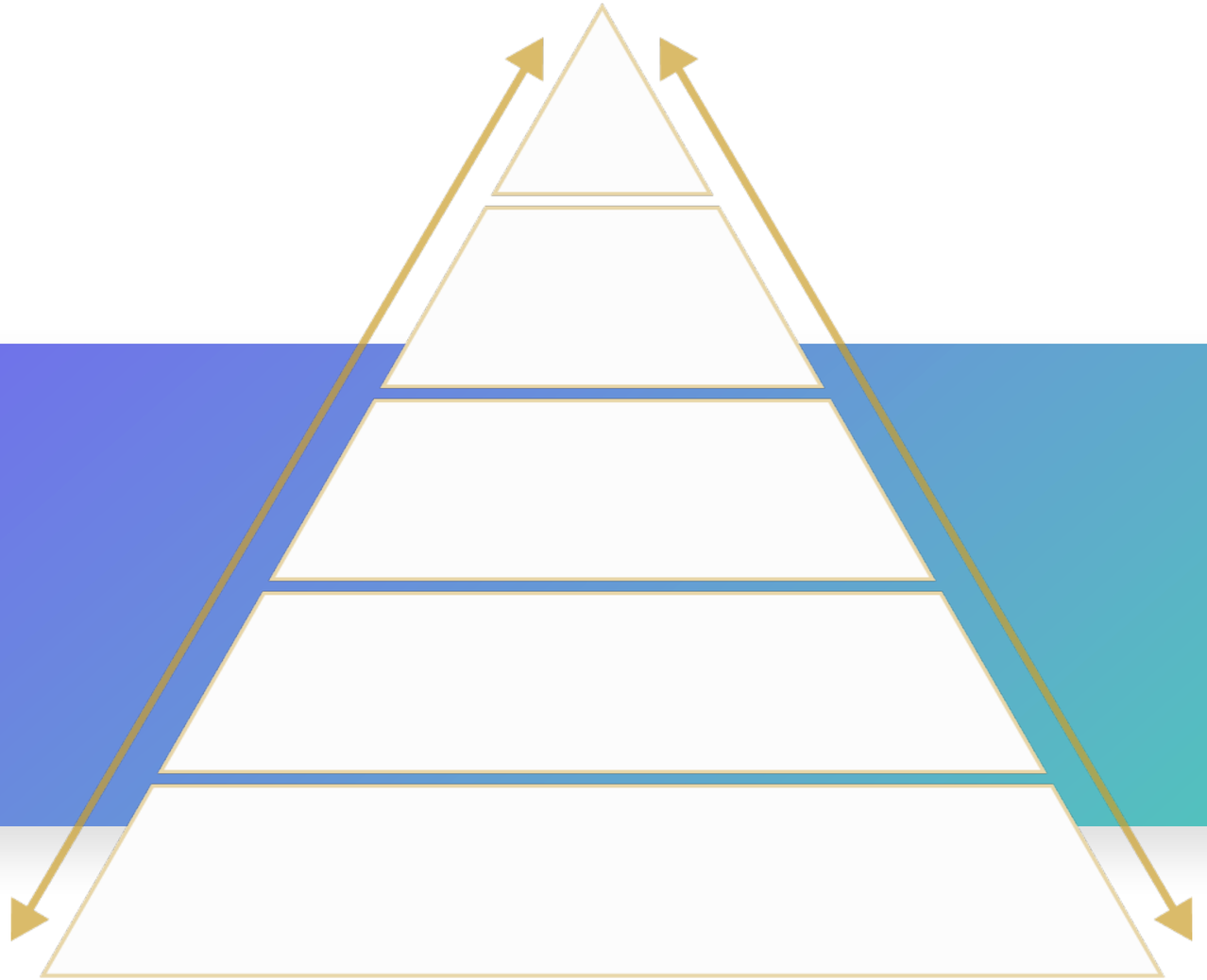
SHU　　HA　　RI



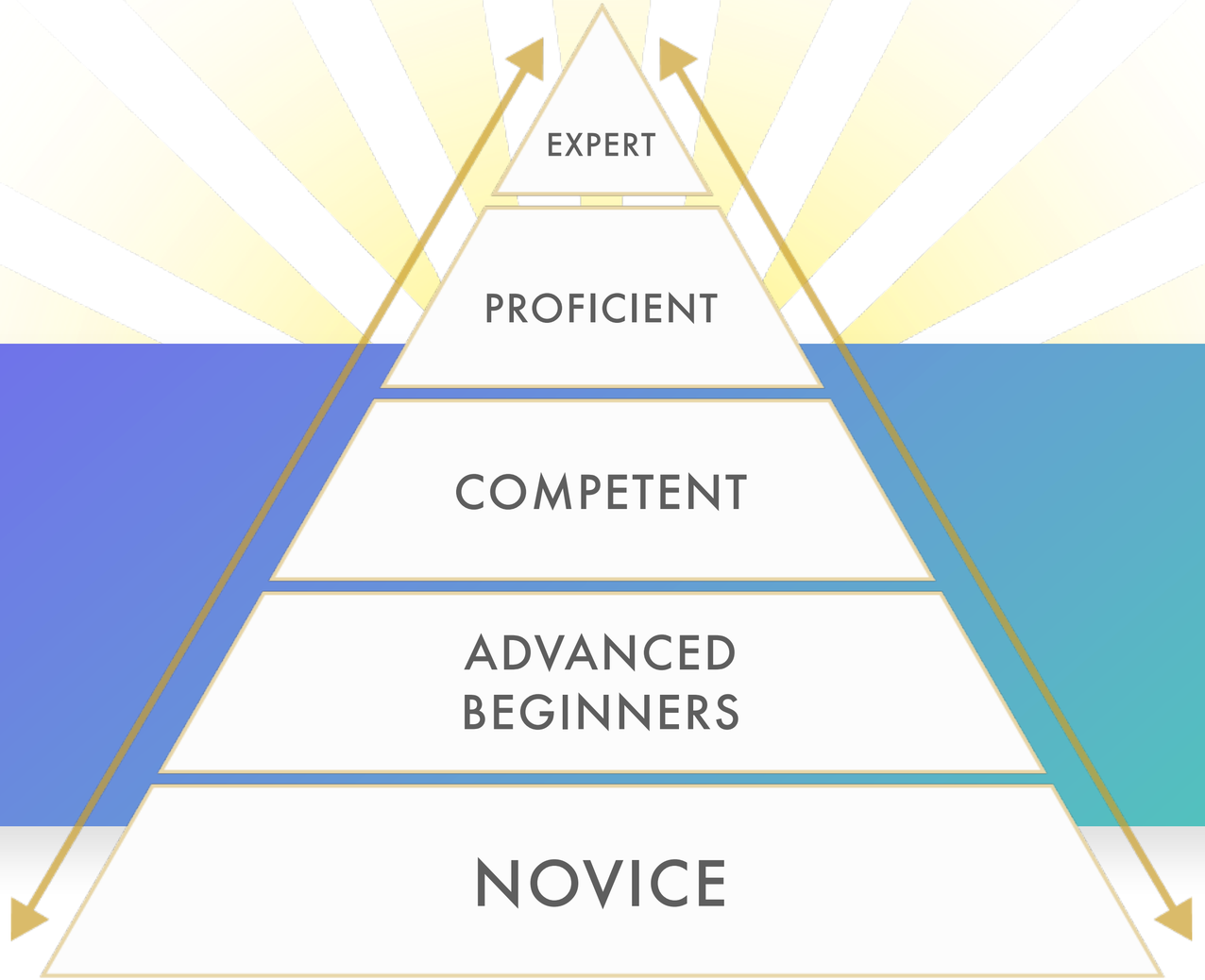
Unconscious Incompetence



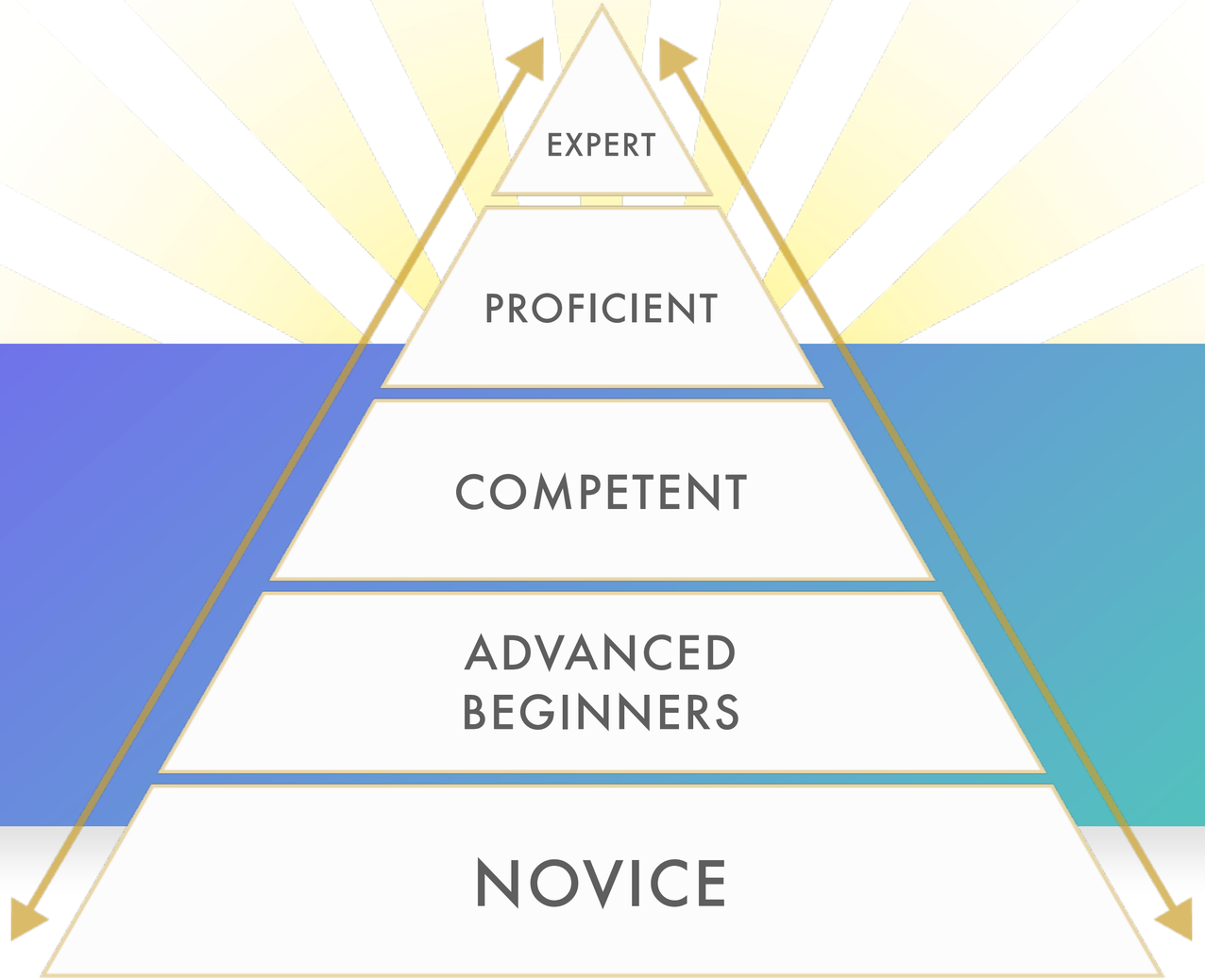
Unconscious Incompetence

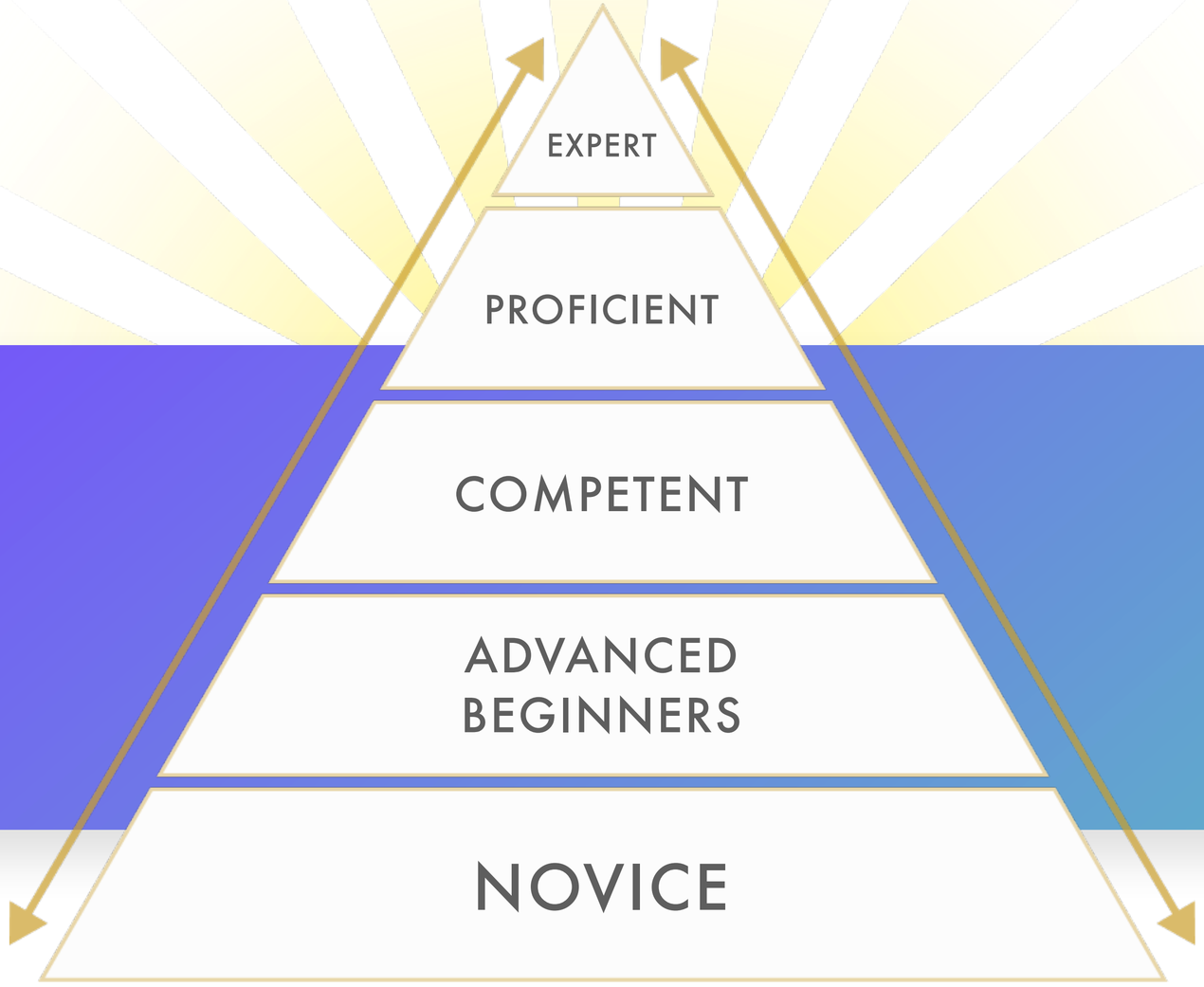


DREYFUS Model of Skill Acquisition - 1980

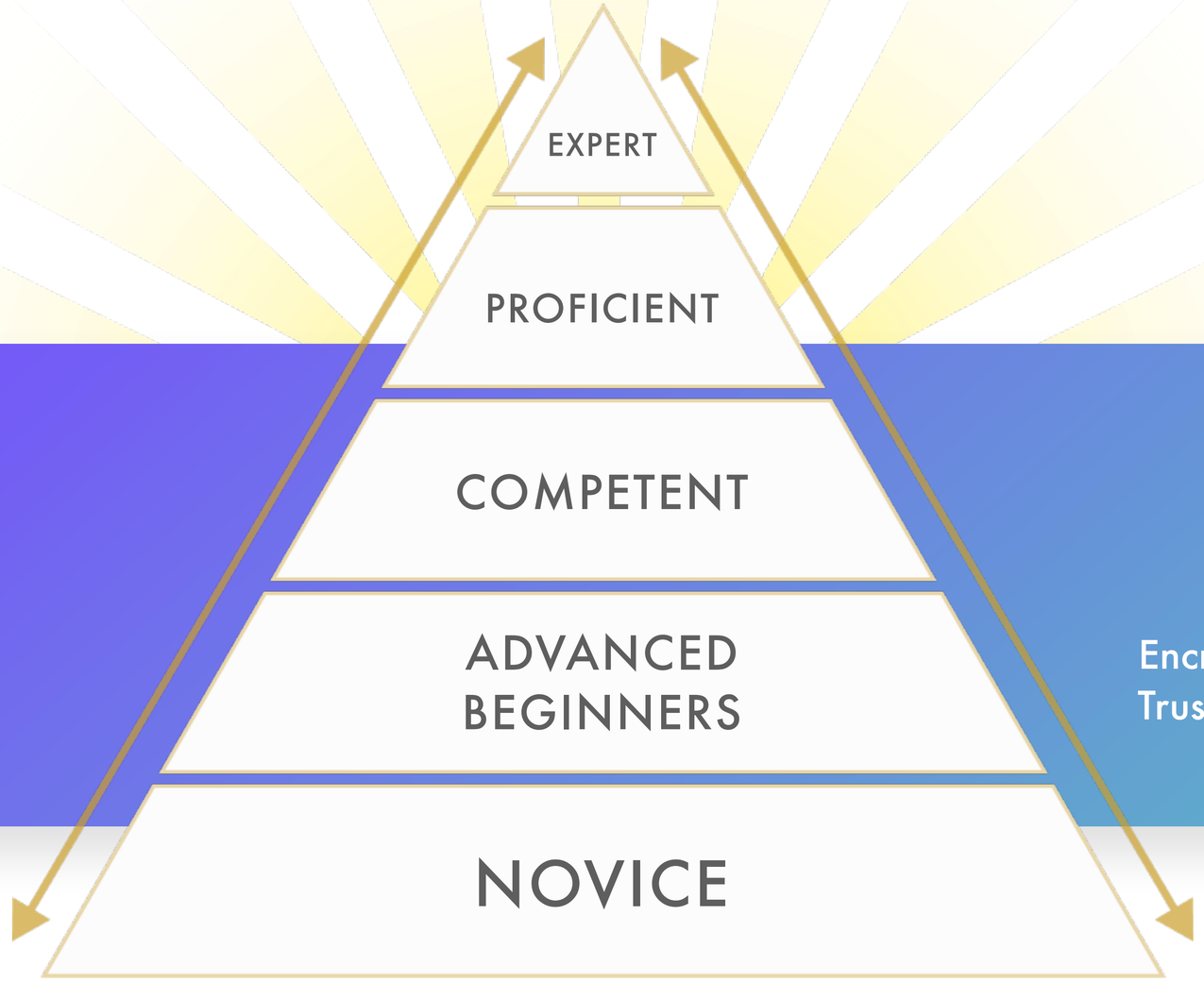


DREYFUS Model of Skill Acquisition - 1980

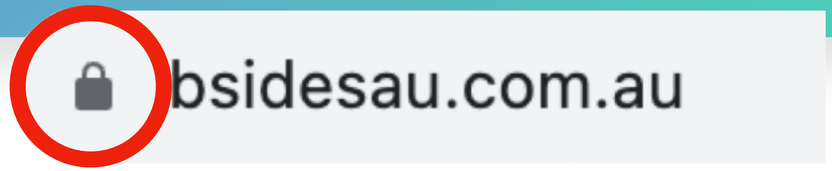

EXPERT
PROFICIENT
COMPETENT
ADVANCED
BEGINNERS
NOVICE

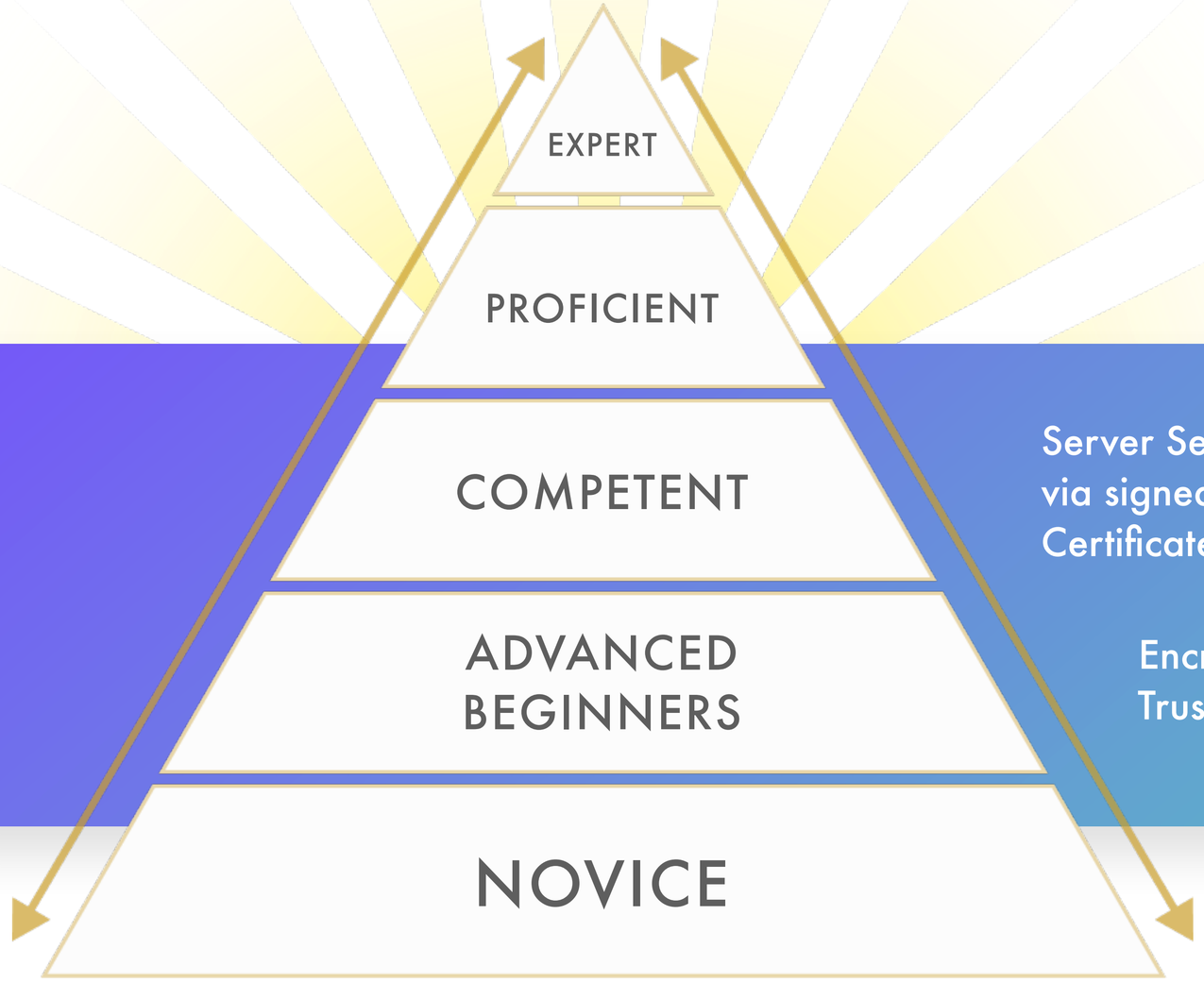


bsidesau.com.au



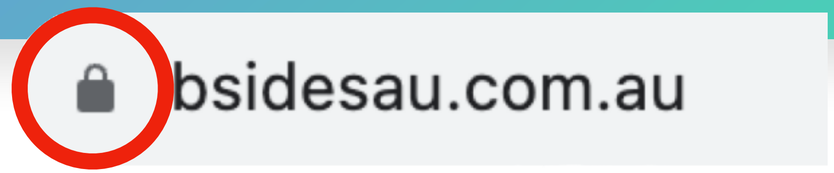
Encrypted tunnel +
Trust relationship

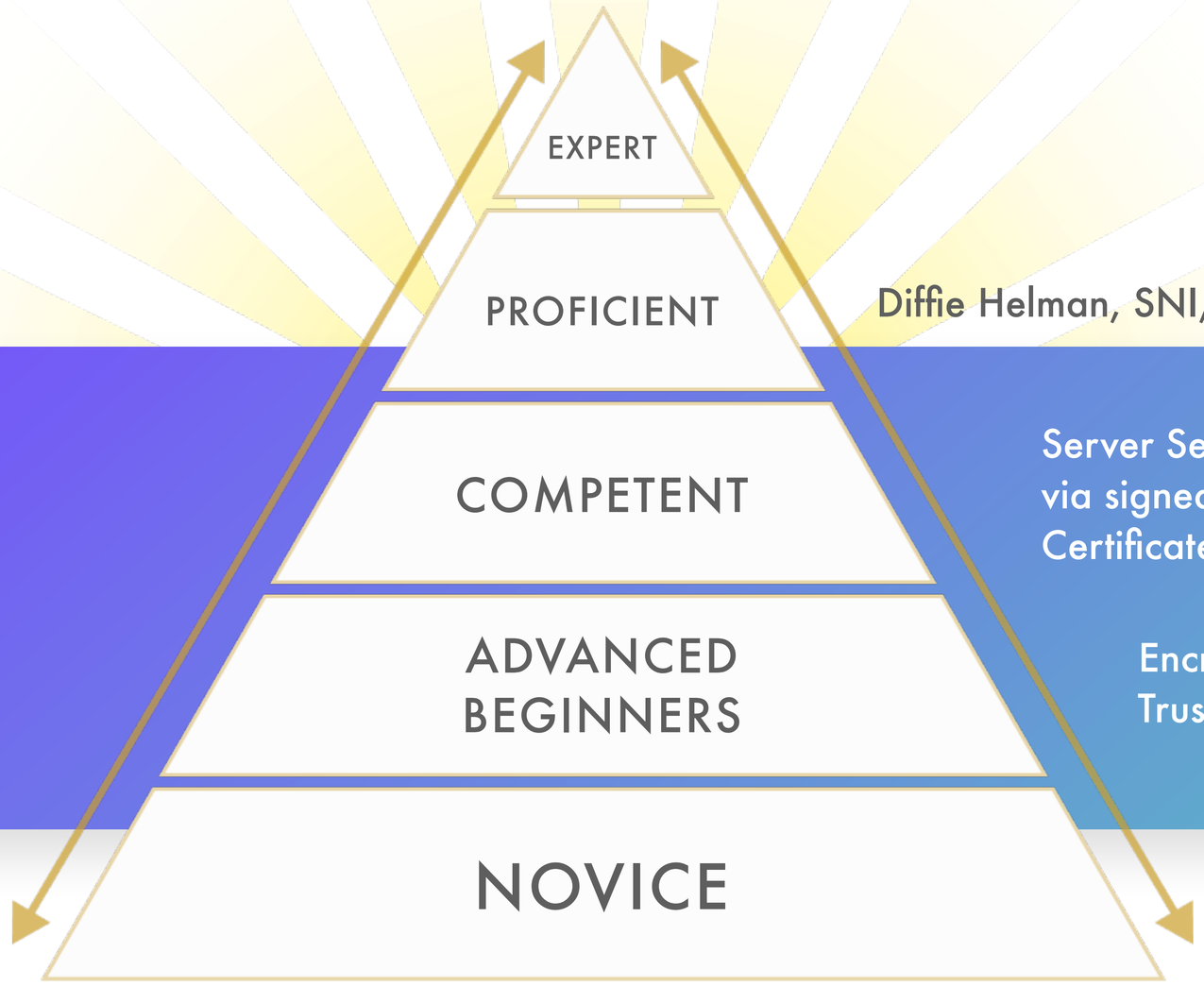




Server Secret key verified
via signed data +
Certificate authorities

Encrypted tunnel +
Trust relationship

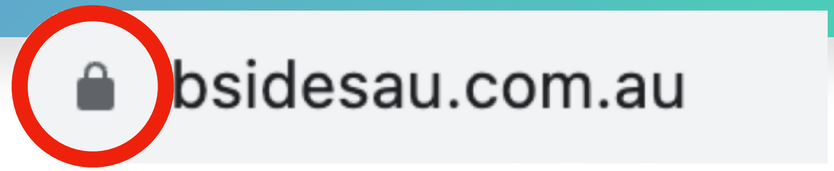


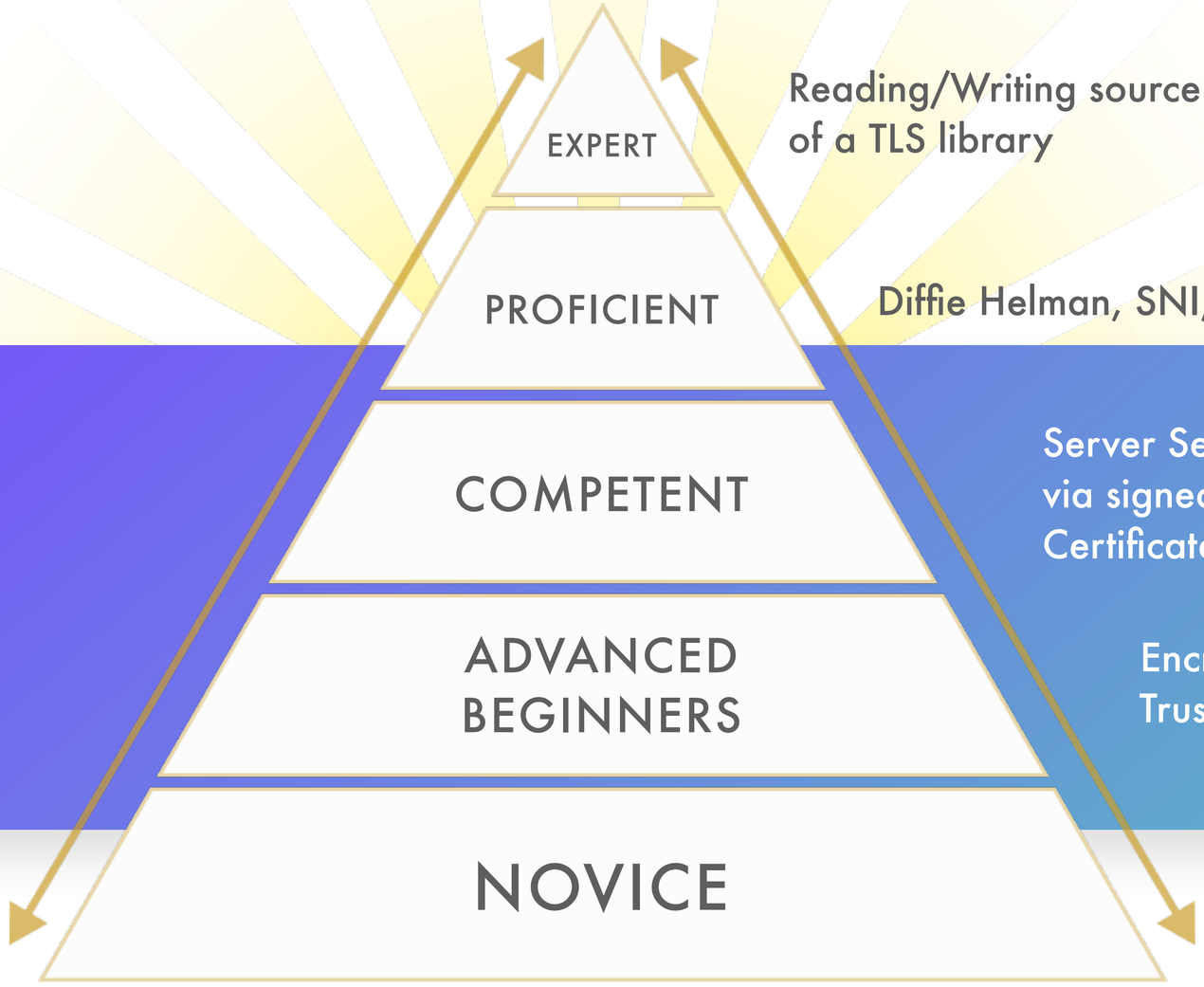


Diffie Helman, SNI,...

Server Secret key verified
via signed data +
Certificate authorities

Encrypted tunnel +
Trust relationship



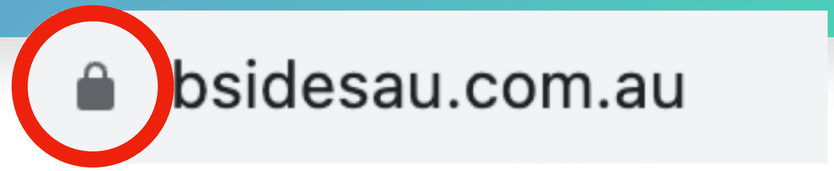


Reading/Writing source code
of a TLS library

Diffie Helman, SNI,...

Server Secret key verified
via signed data +
Certificate authorities

Encrypted tunnel +
Trust relationship



Advanced

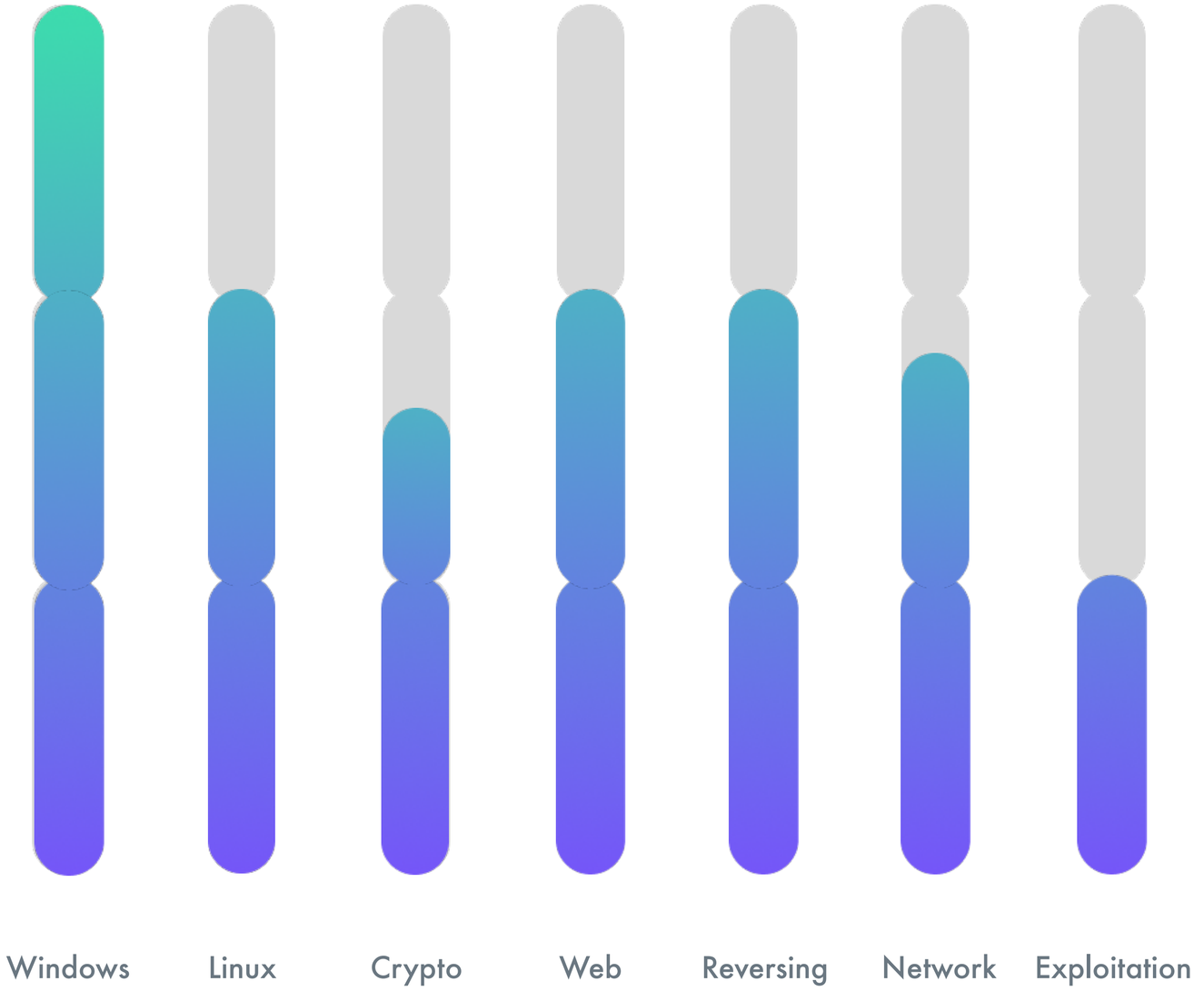
- Own research
- Discover new vulnerabilities and patterns
- Complex Tool development

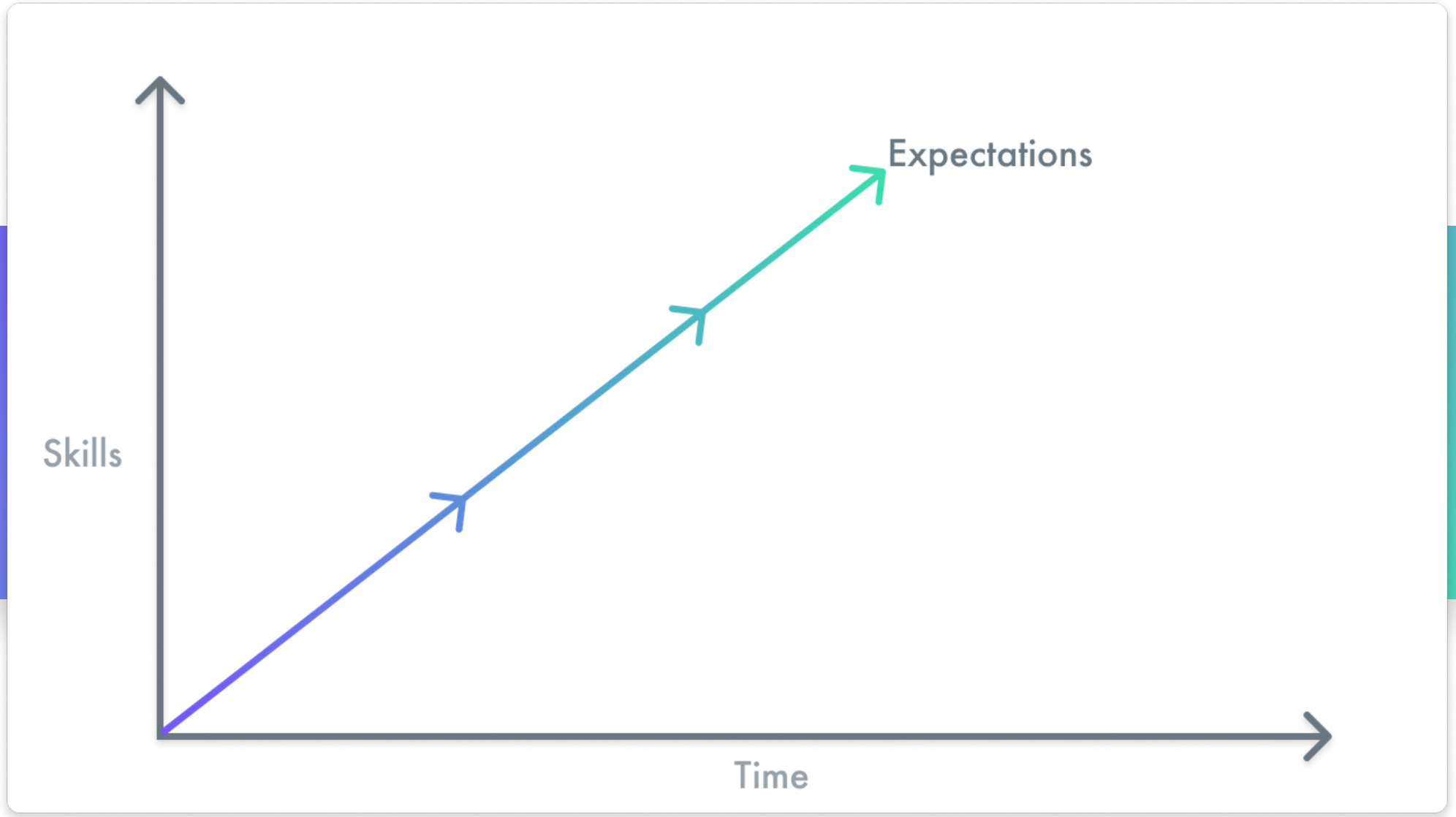
Intermediate

- Deepened understanding of systems, networks, and application security.
- Recognition of Patterns
- Proficiency with various tools

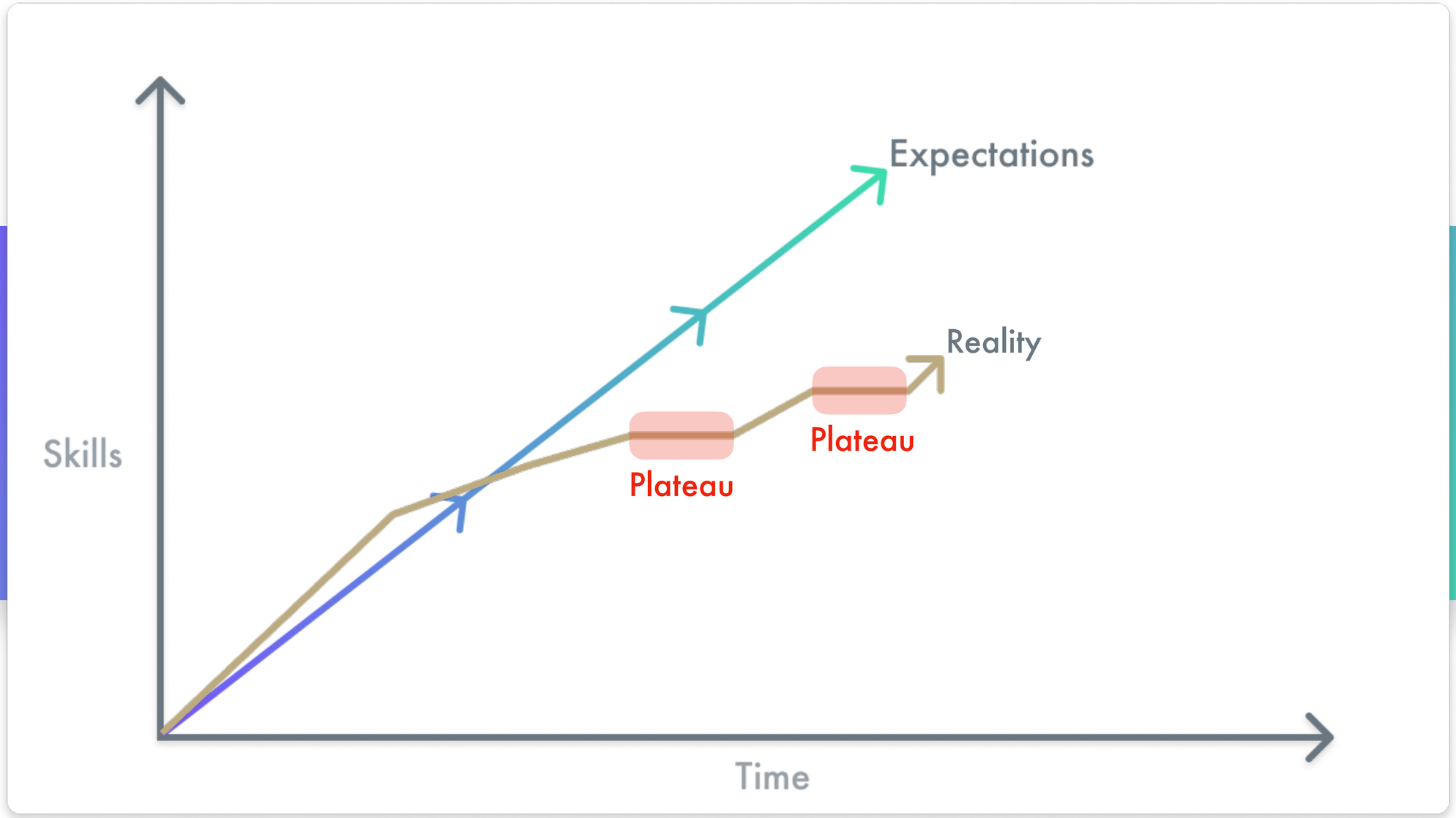
Beginner

- Understanding of common vulnerabilities and exploits
- Understanding the fundamentals of computer science and networking.
- Familiarity with different operating systems


Windows
Linux
Crypto
Web
Reversing
Network
Exploitation


Expectations
Skills
Time


Expectations
Reality
Skills
Time


Expectations
Reality
Plateau
Plateau
Skills
Time

Mistakes you can make...
Not judging, I have made these mistakes.
Some of these **multiple** times...

Early on…

No direction!
You need
to have goals

$$$ or job title
over
learning
(TEAM + TYPE OF WORK)

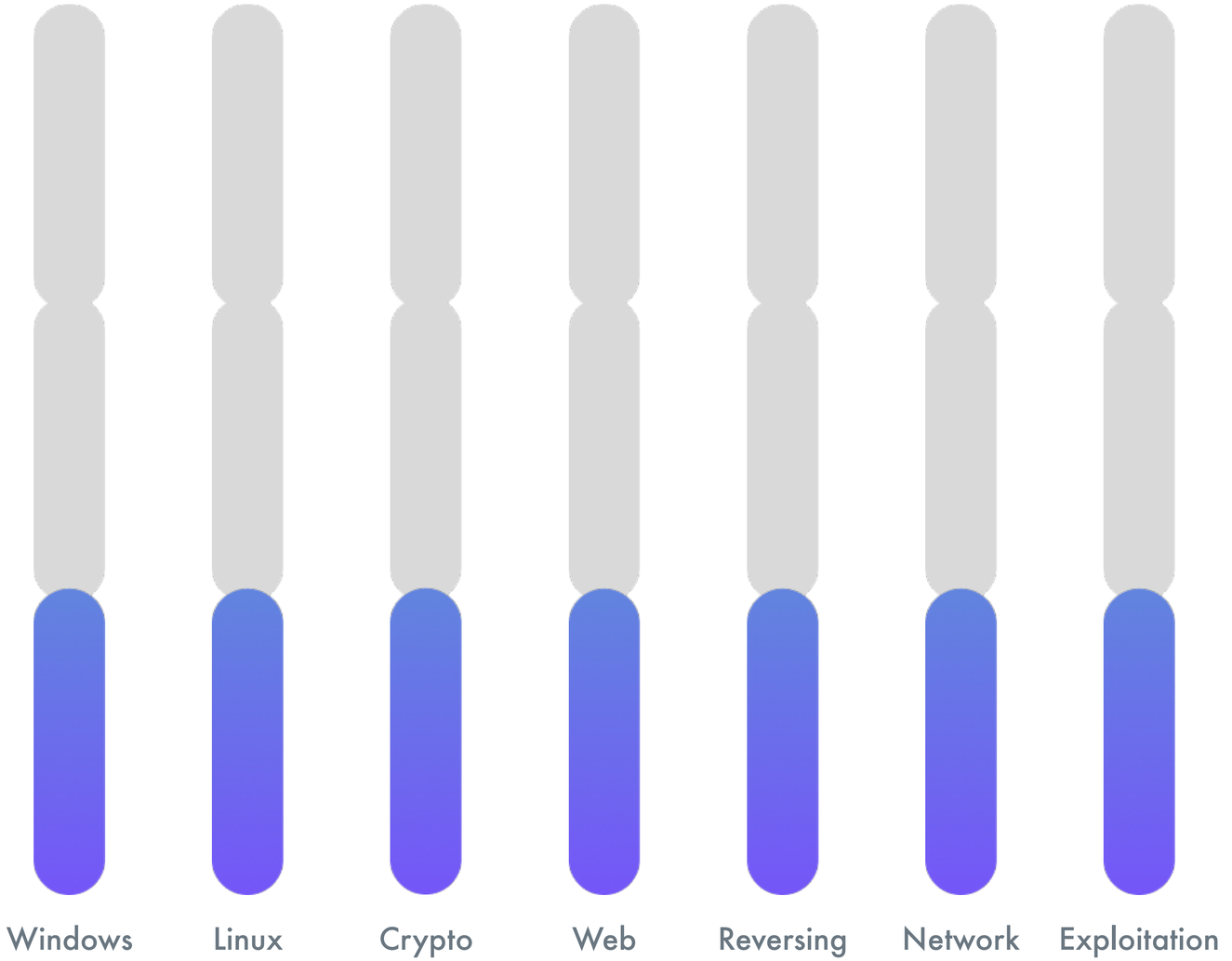
TRAINING

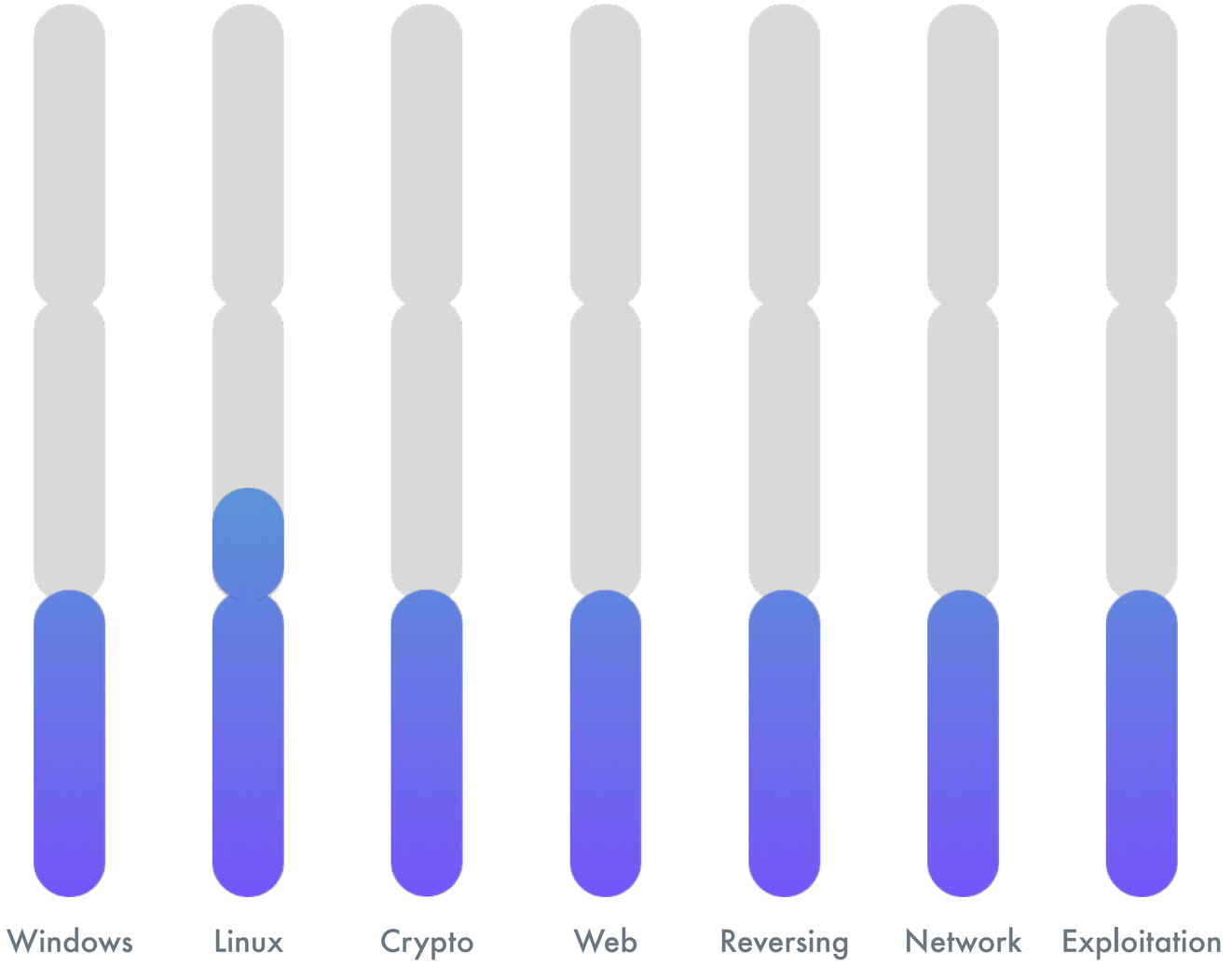
Catalyst

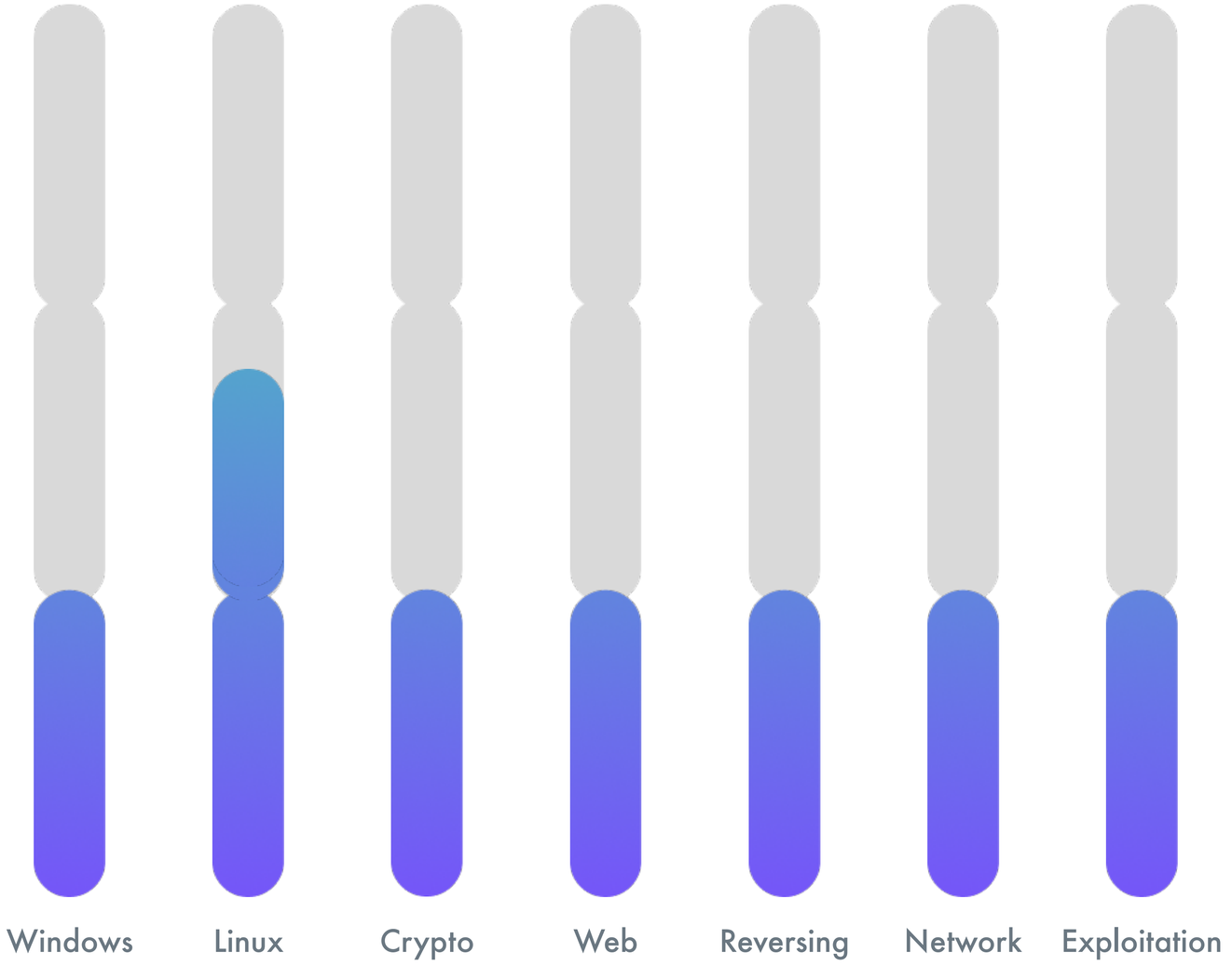
a substance that speeds up a chemical reaction, or lowers the temperature or pressure needed to start one, without itself being consumed during the reaction

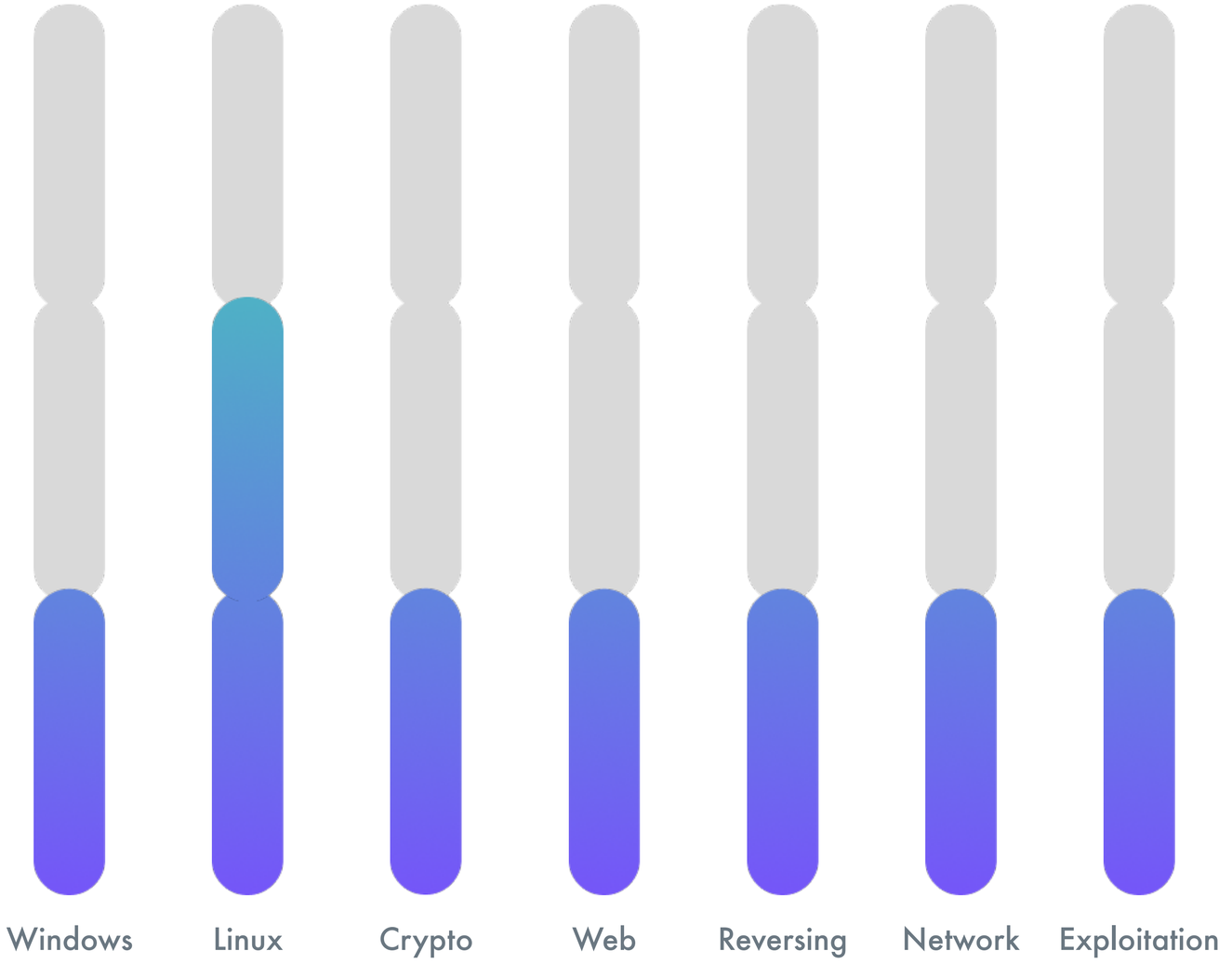
The Impact of AI

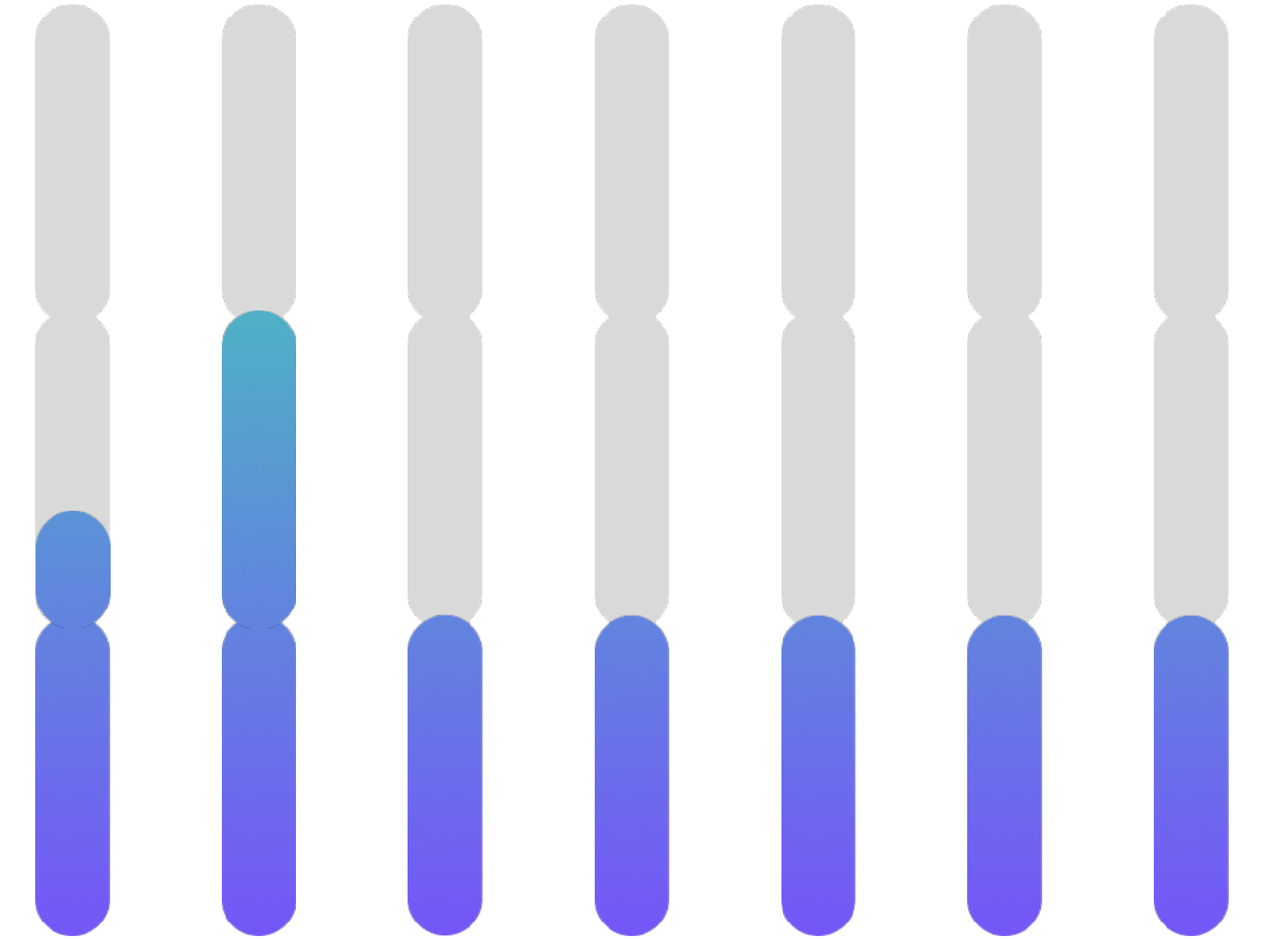
Intermediate ...

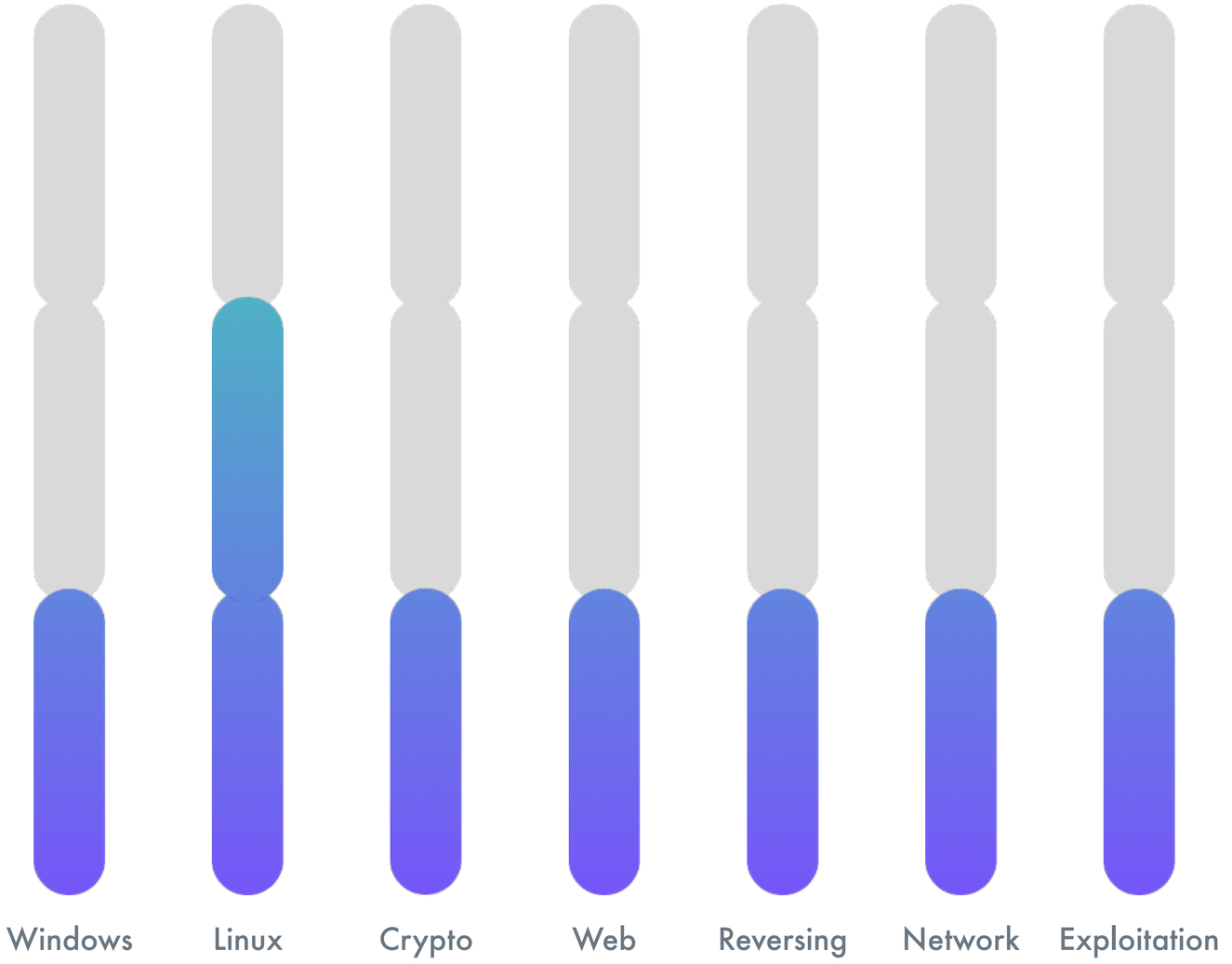

Windows
Linux
Crypto
Web
Reversing
Network
Exploitation

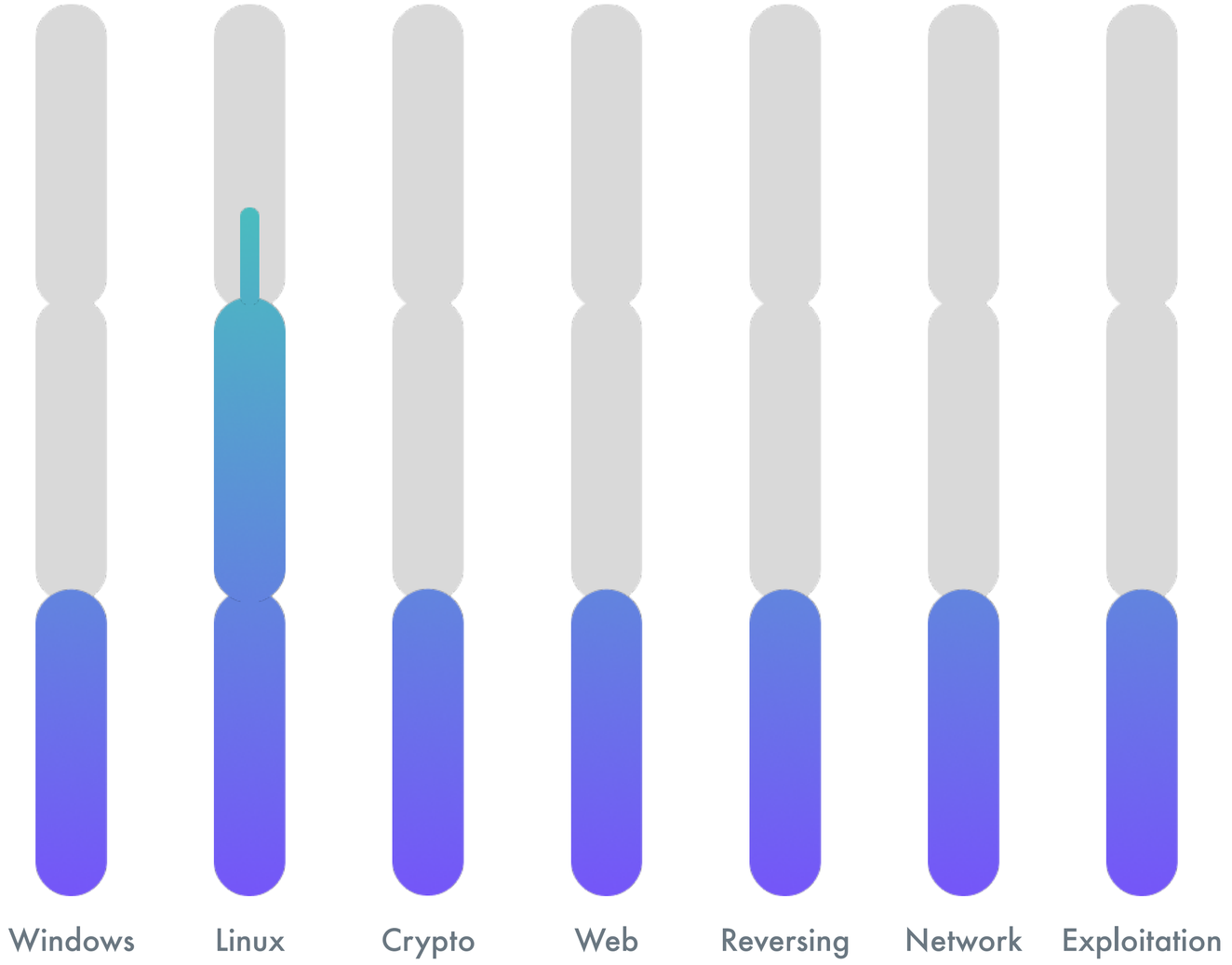

Windows
Linux
Crypto
Web
Reversing
Network
Exploitation

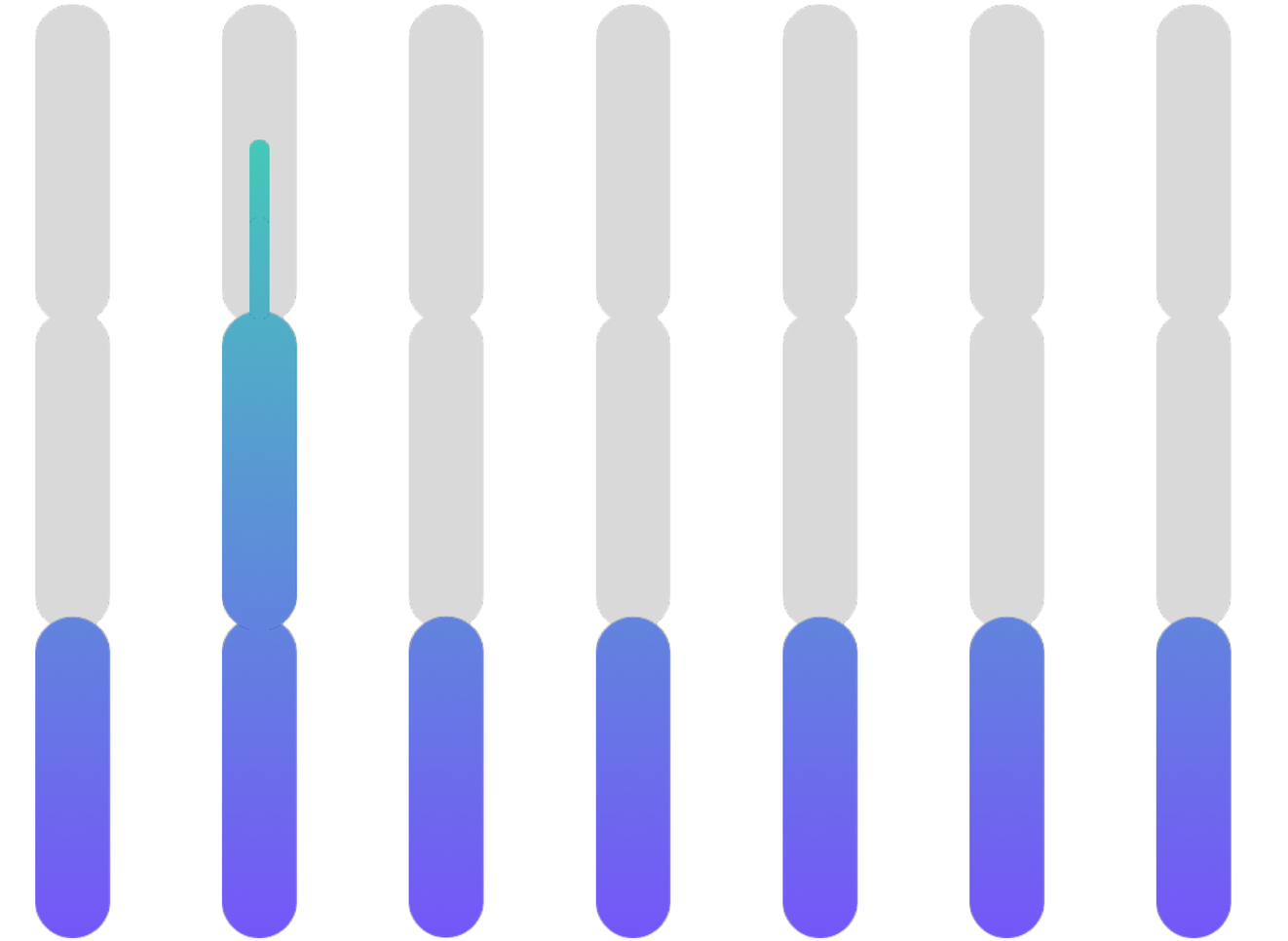

Windows
Linux
Crypto
Web
Reversing
Network
Exploitation


Windows
Linux
Crypto
Web
Reversing
Network
Exploitation

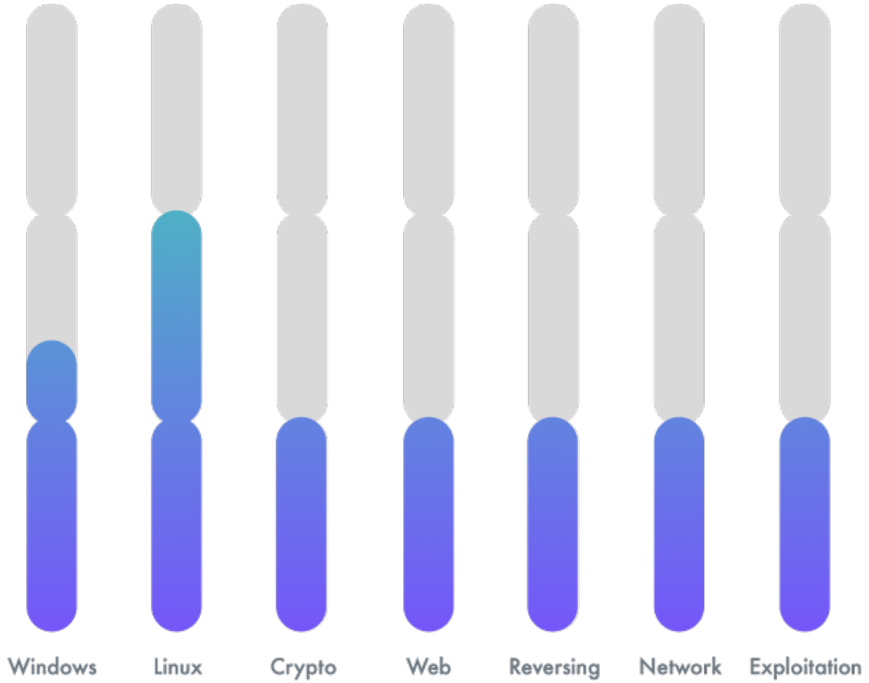

Windows
Linux
Crypto
Web
Reversing
Network
Exploitation


Windows
Linux
Crypto
Web
Reversing
Network
Exploitation

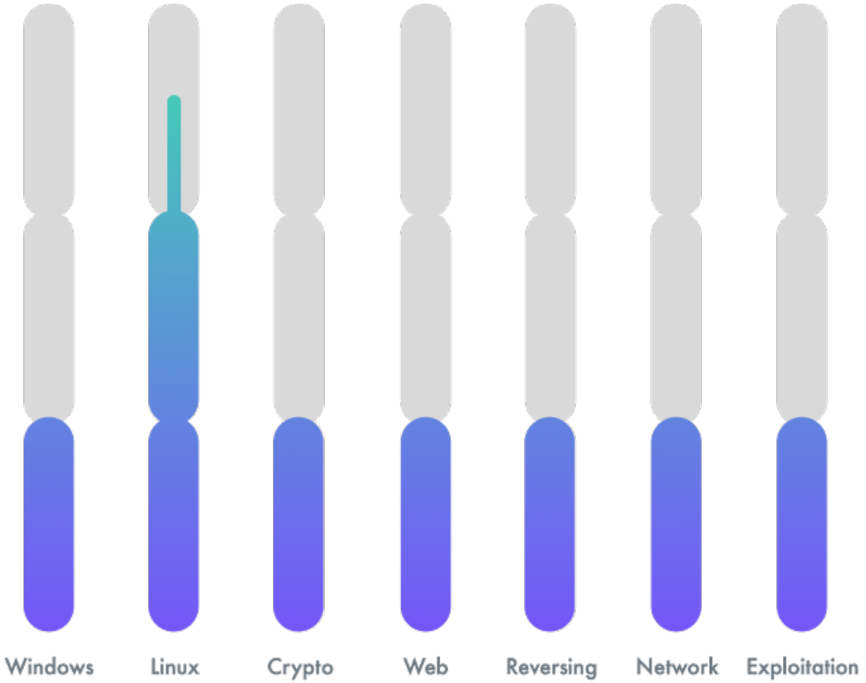

Windows
Linux
Crypto
Web
Reversing
Network
Exploitation


Windows
Linux
Crypto
Web
Reversing
Network
Exploitation

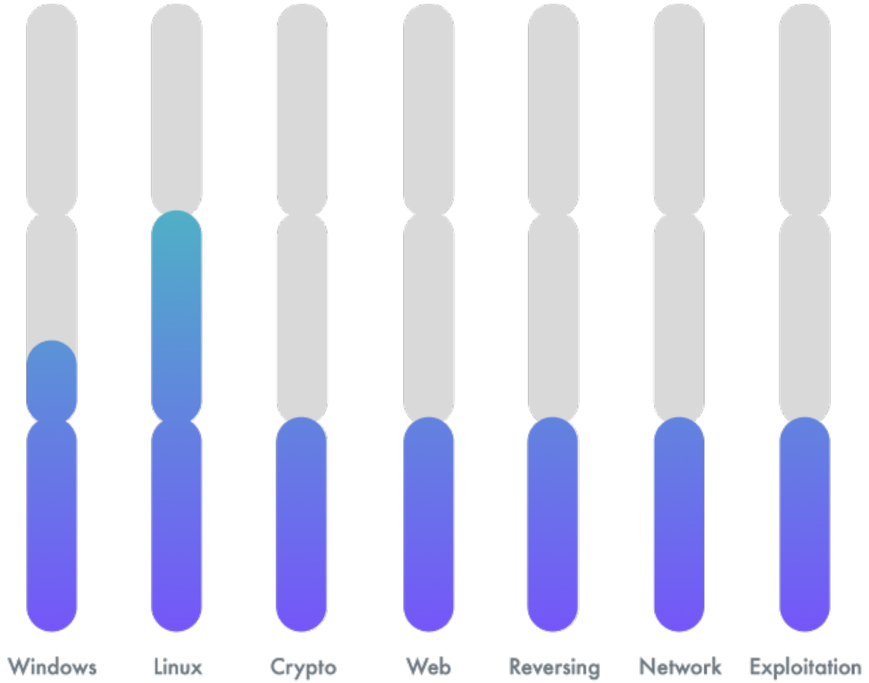
Comfortable



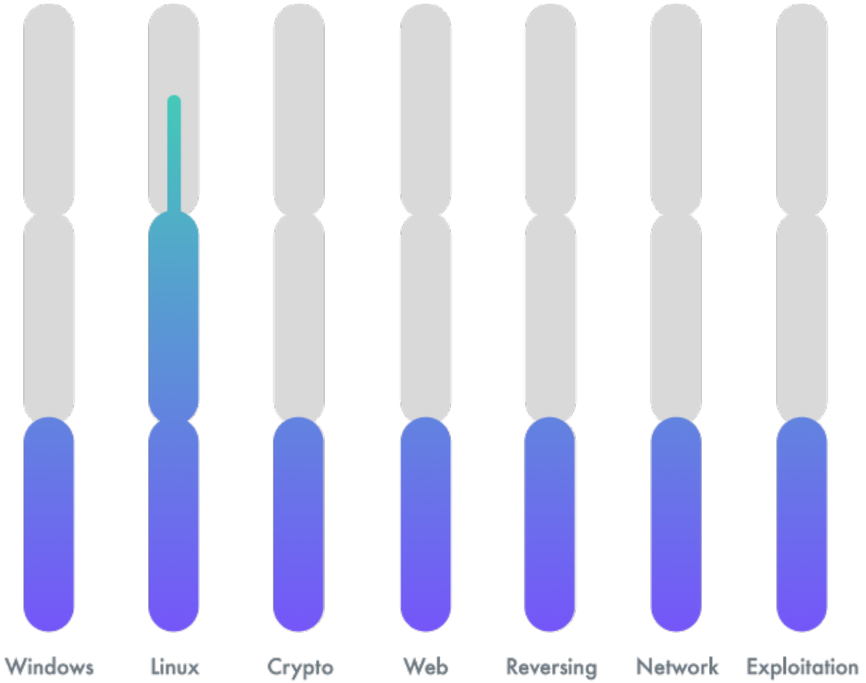
Uncomfortable



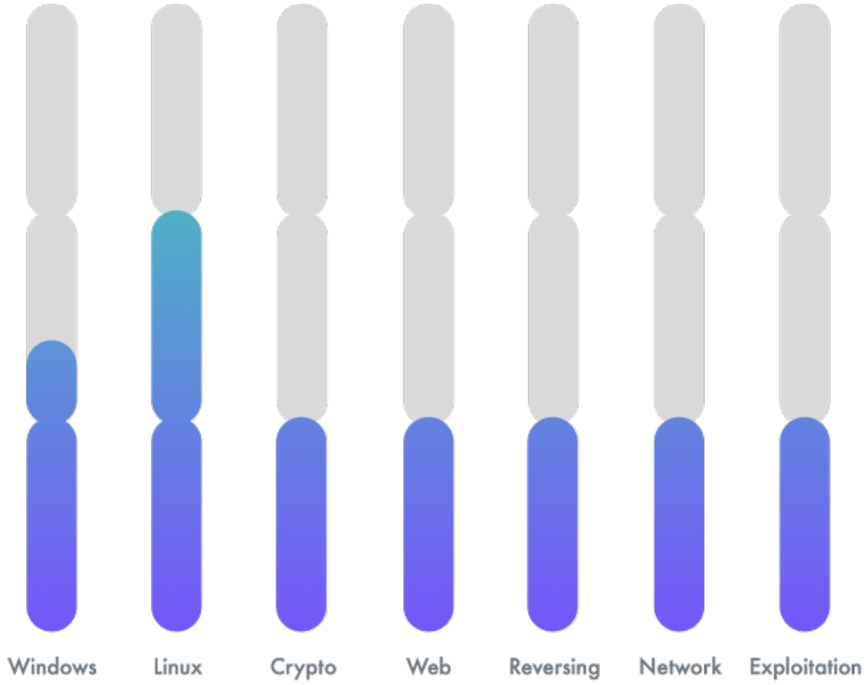
"Manager"

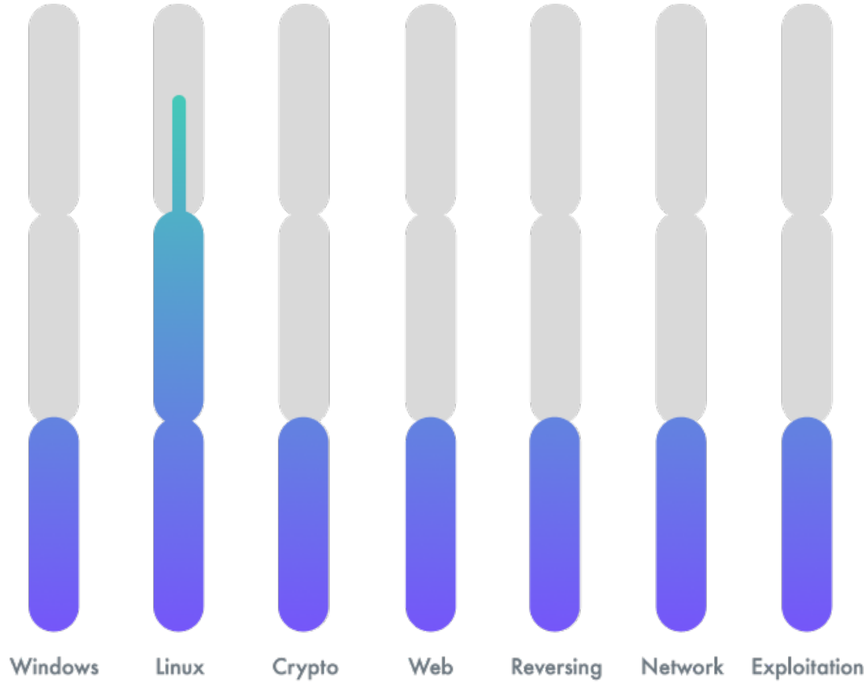


Practitioner



Team dynamics





Moving to a manager role

It's not a bad thing, but it will definitely impact your progression

Not keeping Notes

Resilience Exploratory work


Dum

People at advanced level do good talks and you may think they do the research for the talks

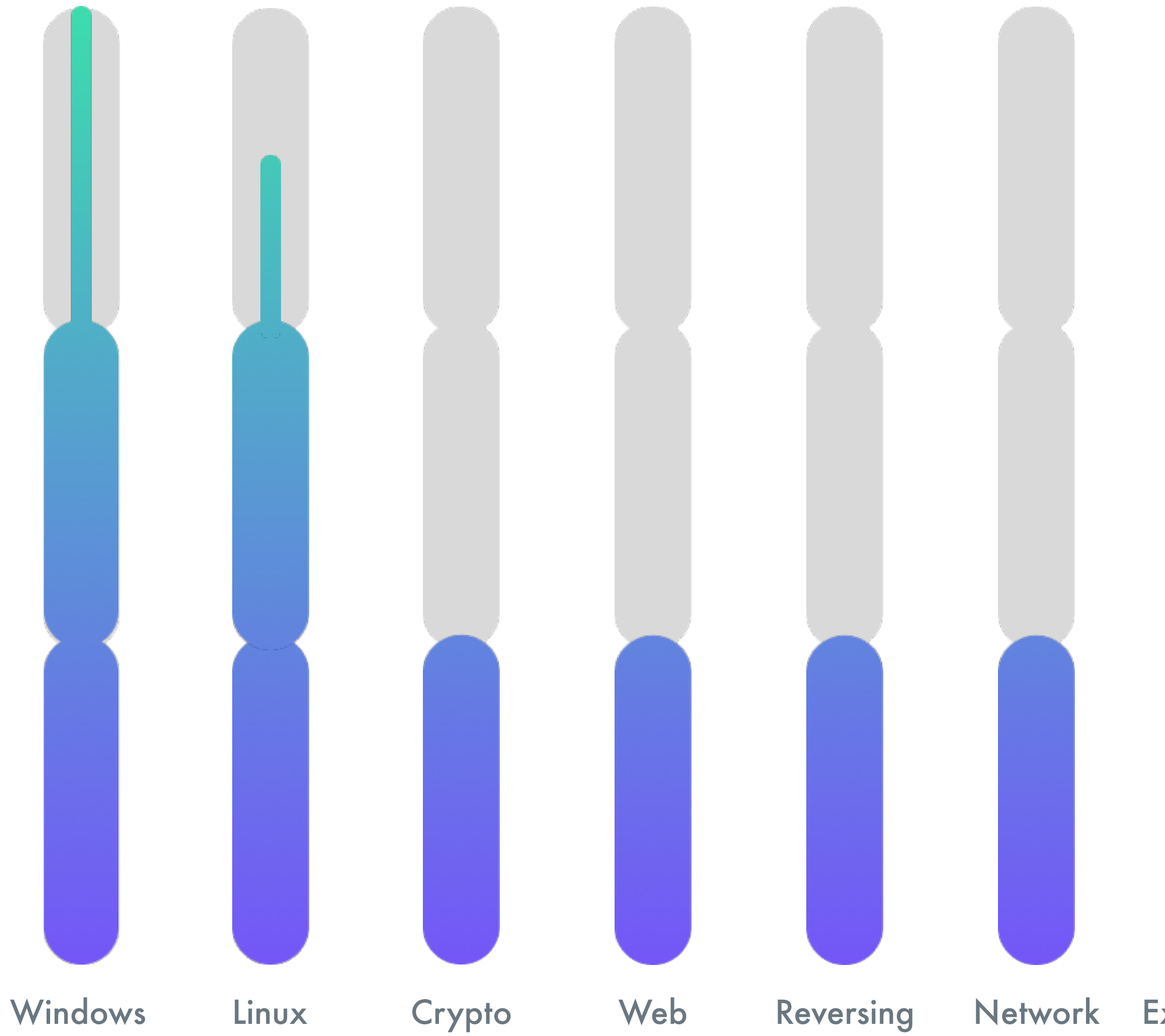
But what actually happens is these people do talks because they *do* the research

They don't necessarily enjoy doing talks, they *enjoy* doing the research

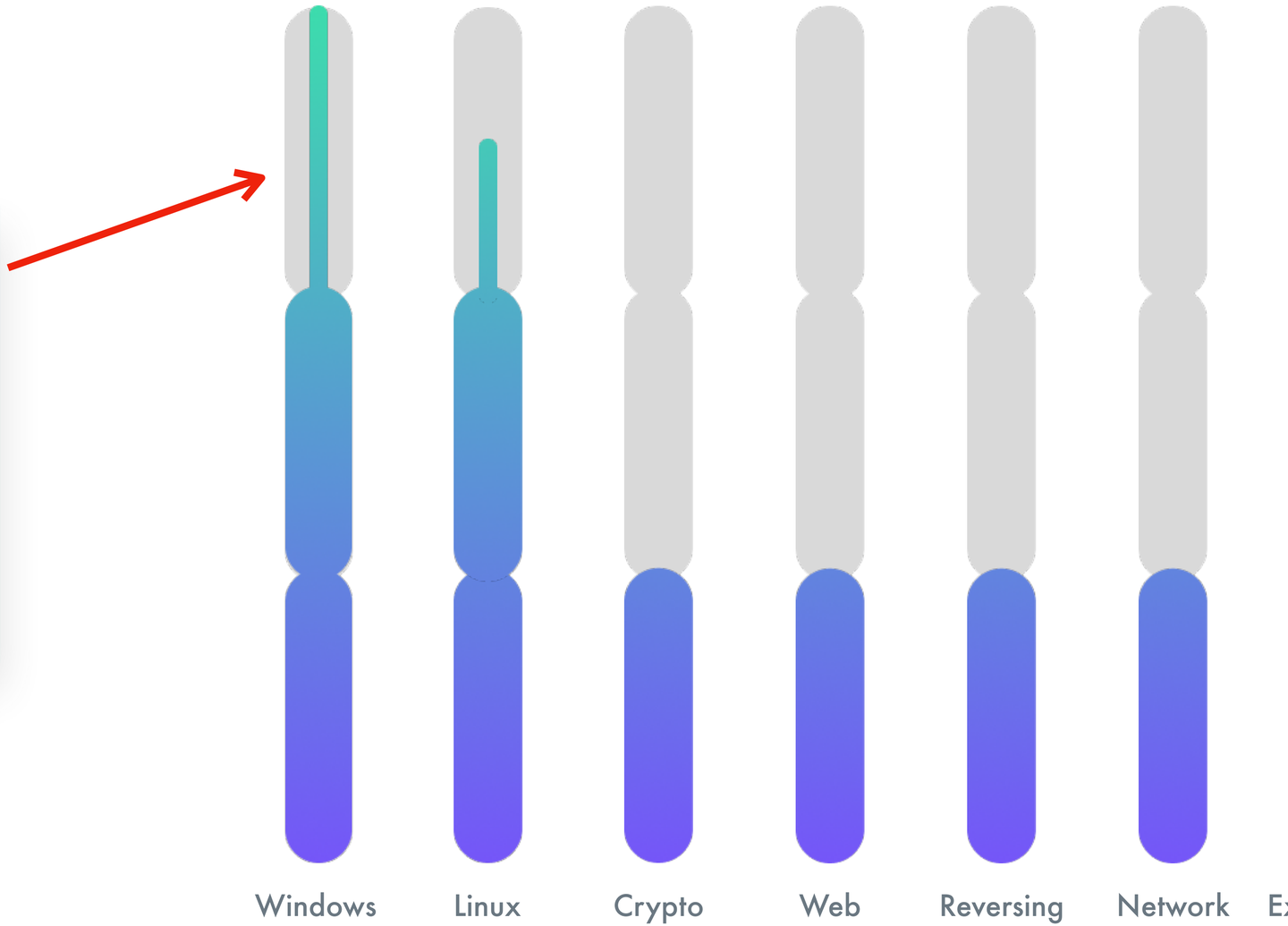
What got you here…

Won’t get you here…

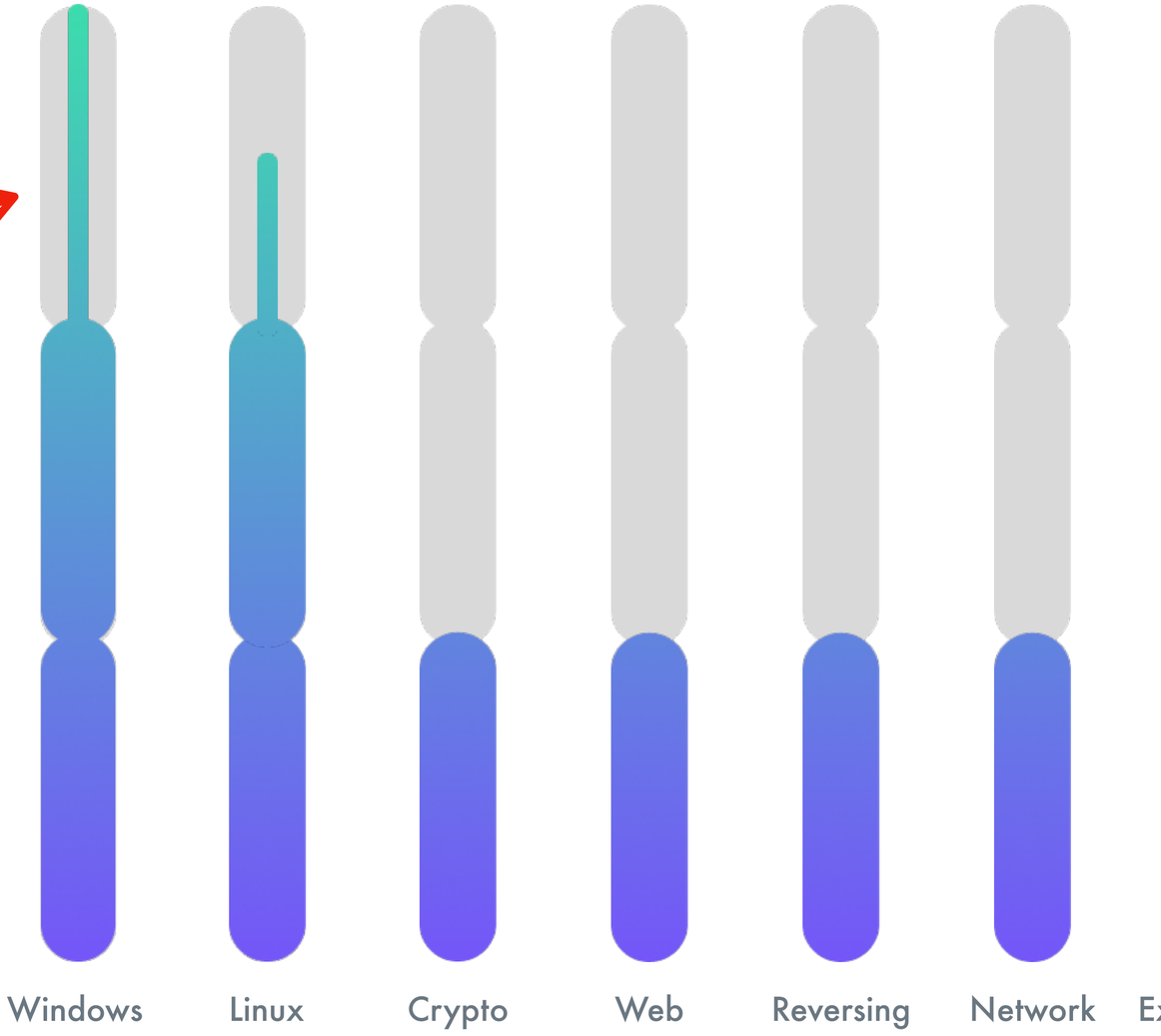
Lessons learnt here are the hardest



Lessons learnt here are the hardest



Lessons learnt here
are the hardest
But also the most valuable

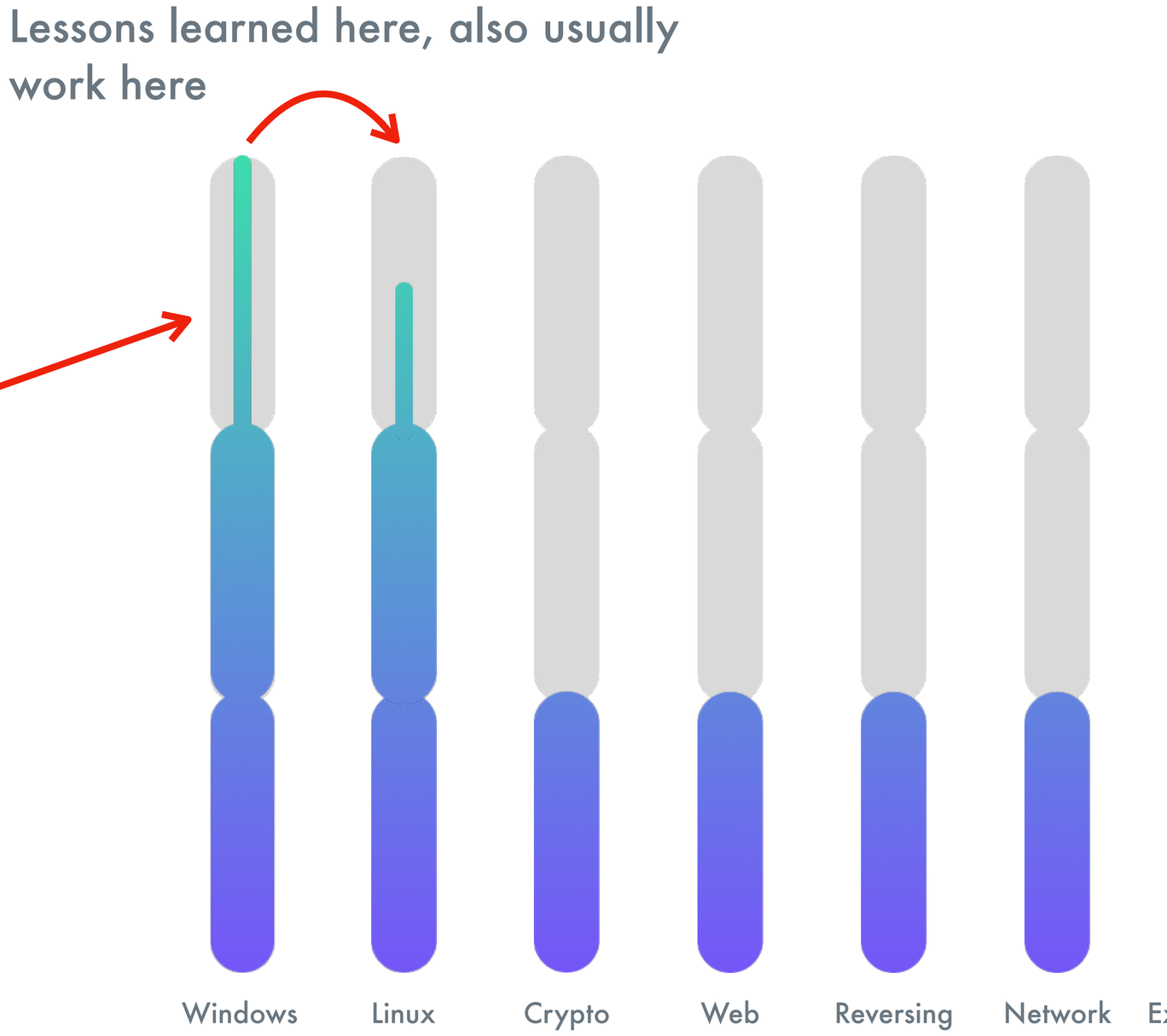


Lessons learnt here
are the hardest

But also the most valuable

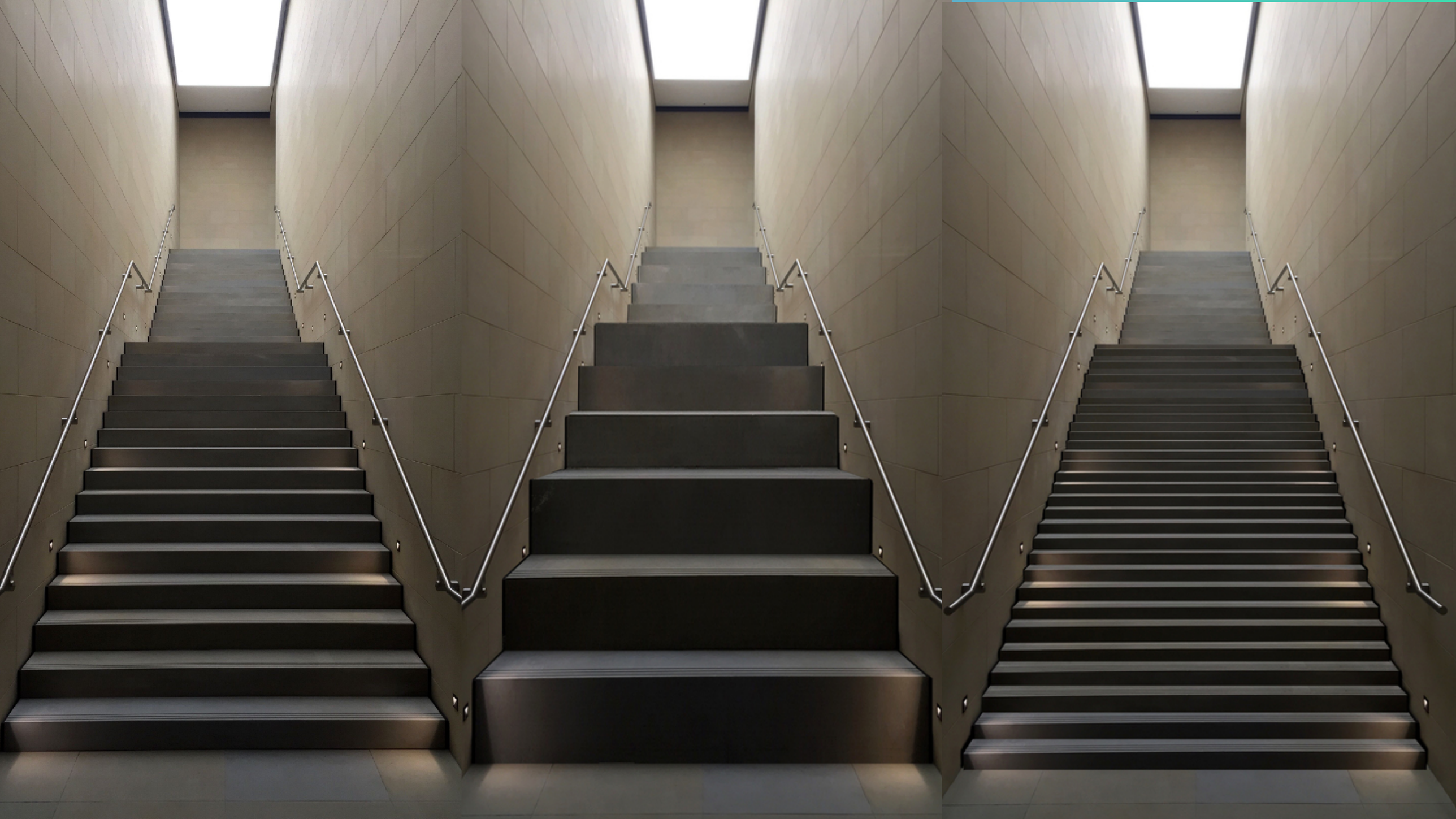
Lessons learnt here
are the hardest
But also the most valuable

Code Review
Advanced Debugging
Methodologies
Autonomy
Complex patterns



Not staying up to date.

Finding the right difficulty to work on…



Be Lucky

Challenge your **Assumptions**

Challenge your **Assumptions**

CVE-2022-39299

Challenge your **Assumptions**

CVE-2022-39299

<xml></xml>
<xml></xml>

FAILURE

FAILURE

CVE-2021-40525

FAILURE

CVE-2021-40525

/var/spool/mail/../../../../etc/passwd

FAILURE

CVE-2021-40525

/var/spool/mail/../../../../etc/passwd

CVE-2022-22931

FAILURE

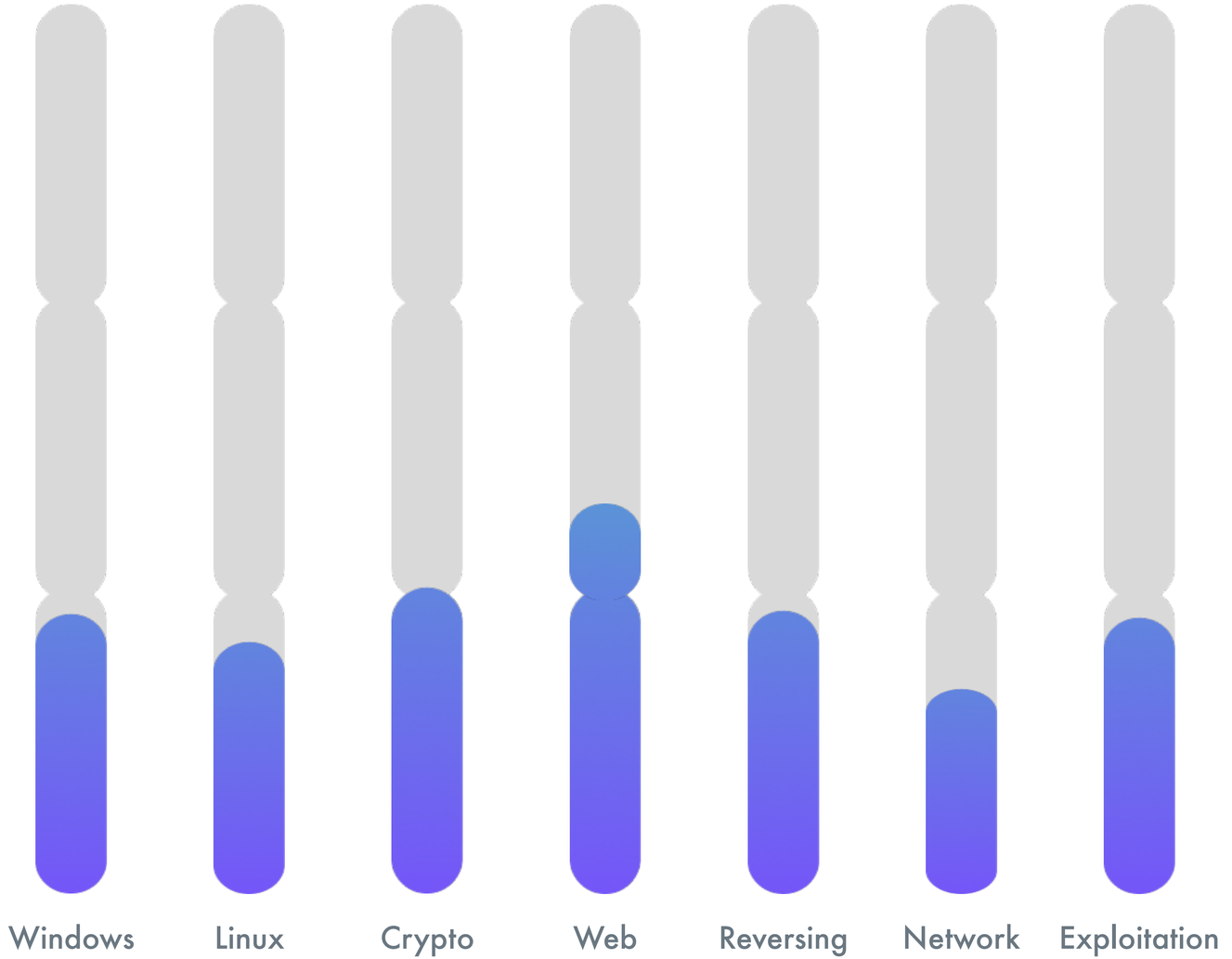
CVE-2021-40525

/var/spool/mail/../../../../etc/passwd

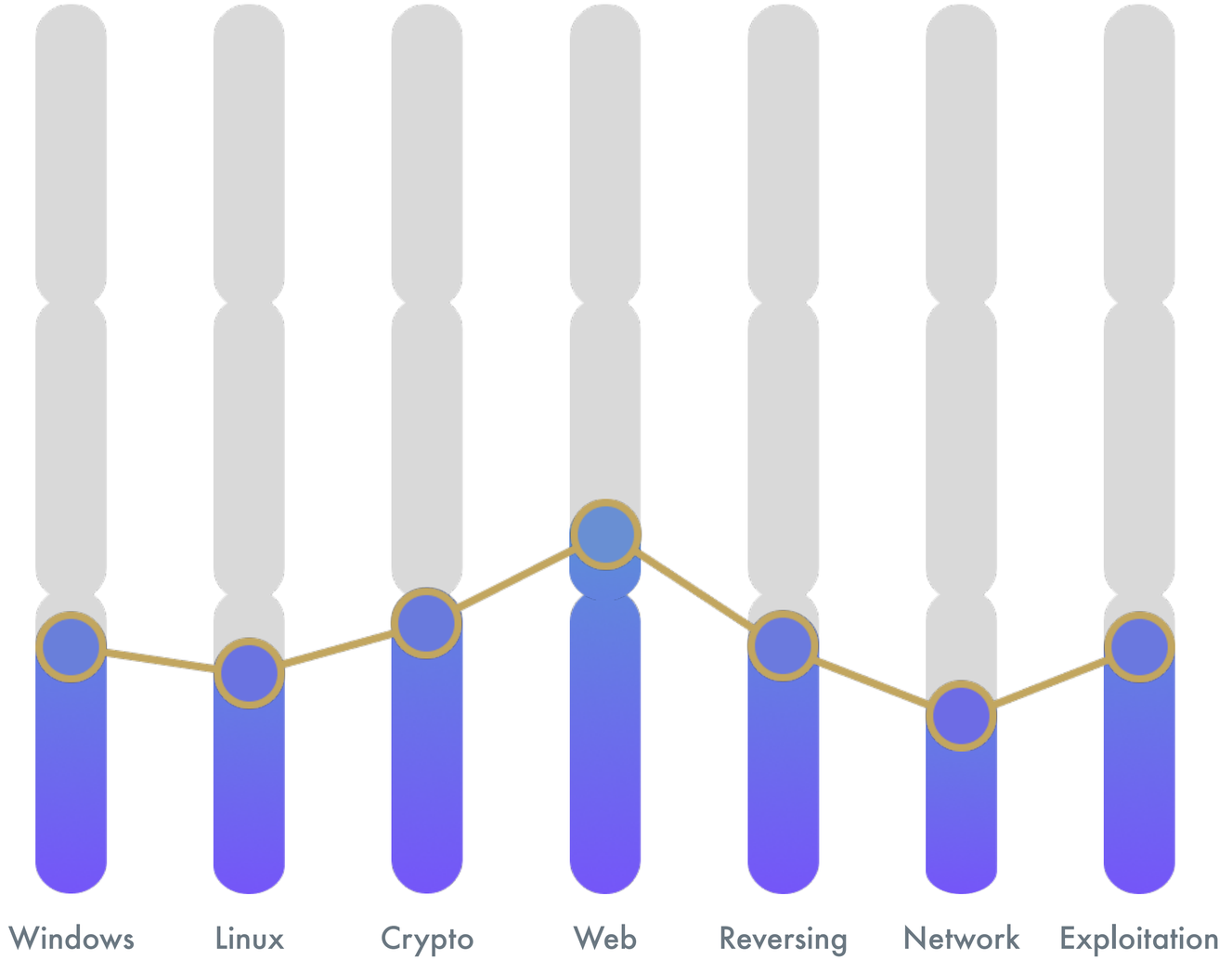
CVE-2022-22931

/var/spool/mail/root as user root123

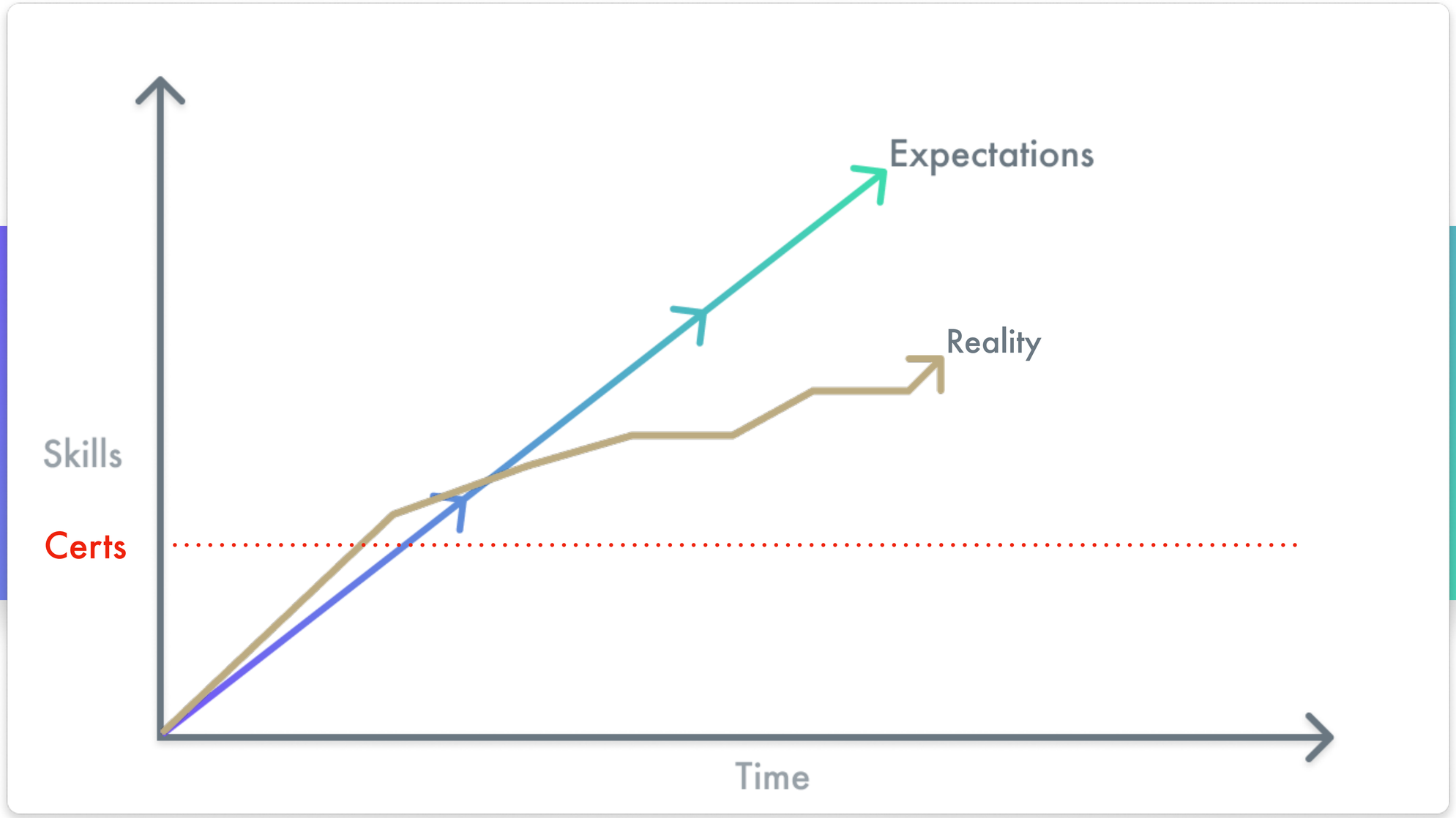
Certifications

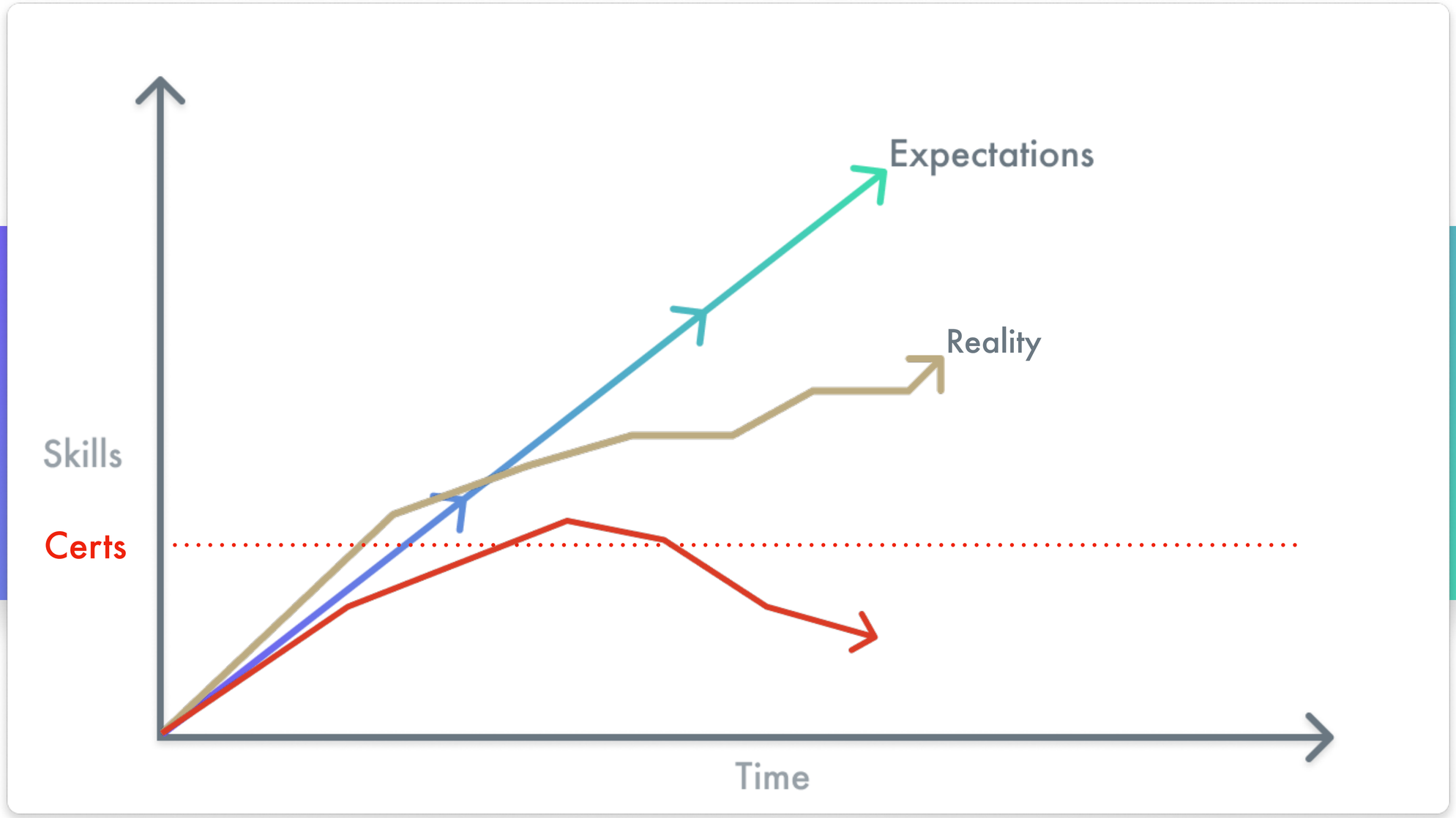


Certifications




Expectations
Reality
Skills
Time


Expectations
Reality
Skills
Certs
Time


Expectations
Reality
Skills
Certs
Time

But how do I get **better** at learning?

HACK THE WAY YOU **LEARN**

Joshua Waitzkin

Joshua Waitzkin

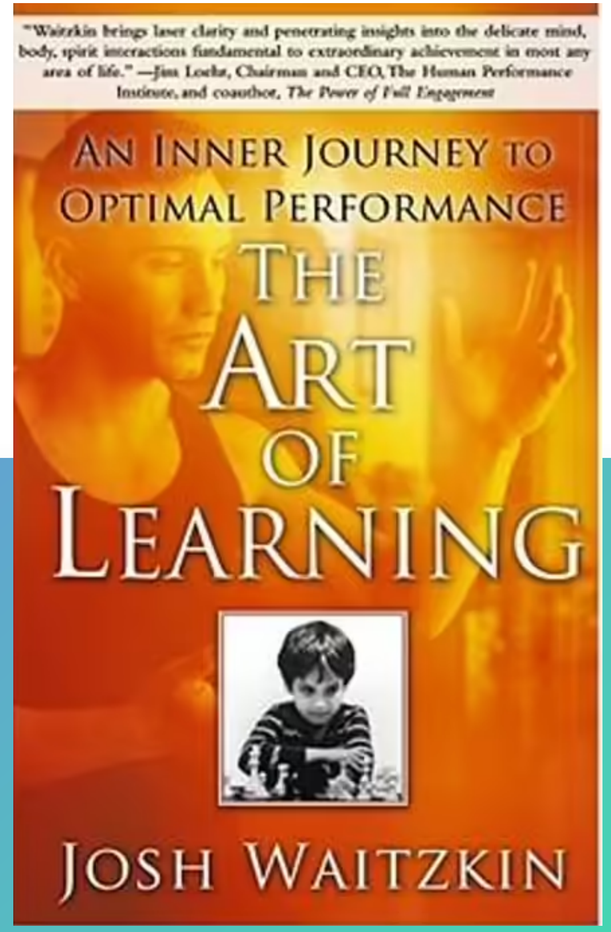
Won U.S. Junior Chess championship

Joshua Waitzkin

Won U.S. Junior Chess championship

World Champion in Taiji Push Hands

HACK THE WAY YOU **LEARN**



Spaced Repetition

Active Recall

Mind Mapping

Pomodoro

Interleaved Learning

Chunking

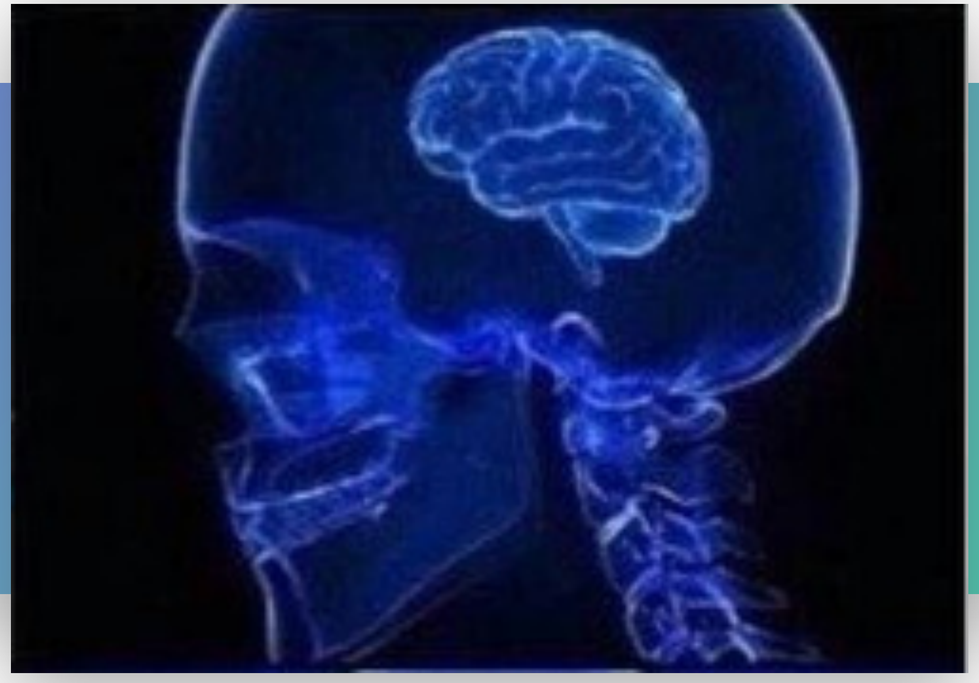
Deep Work

...

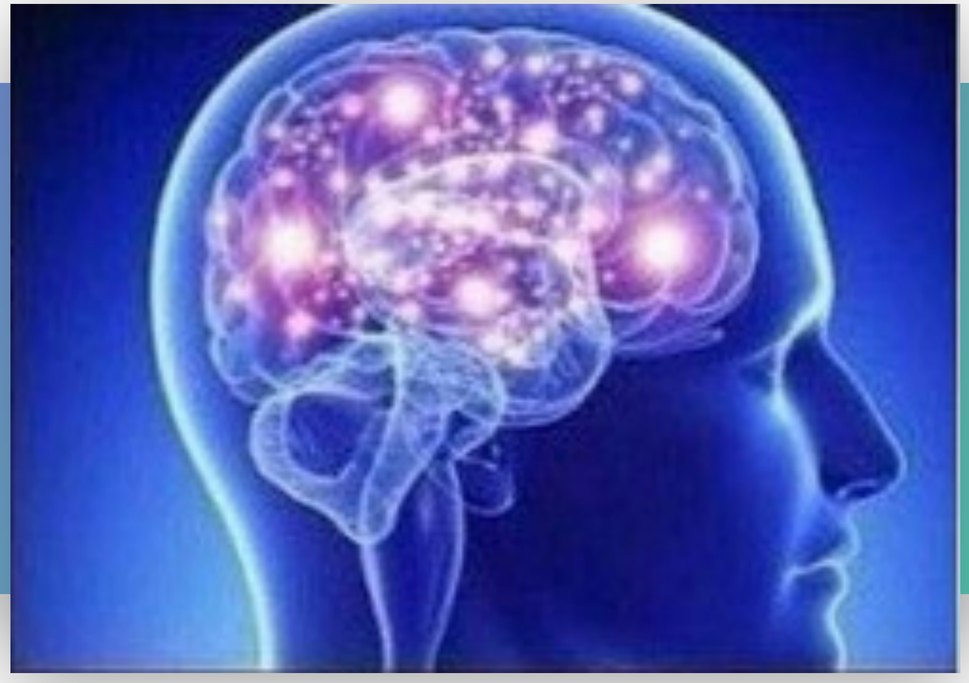
LEARNING FROM **CHESS**

LEARNING FROM **CONTENT**

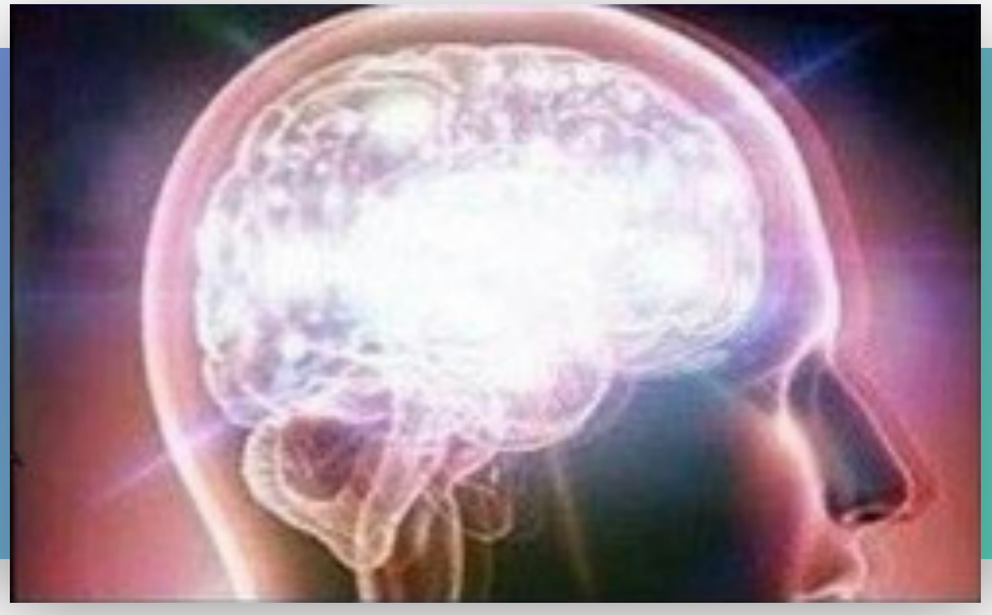
What is the **Impact** of this?



What can I **learn** from of this?



What **patterns** can I apply to something else?



Why didn’t I find it?

CVE-2022-21449

1. Check that Q_A is not equal to the identity element O, and its coordinates are otherwise valid.
2. Check that Q_A lies on the curve.
3. Check that $n \times Q_A = O$.

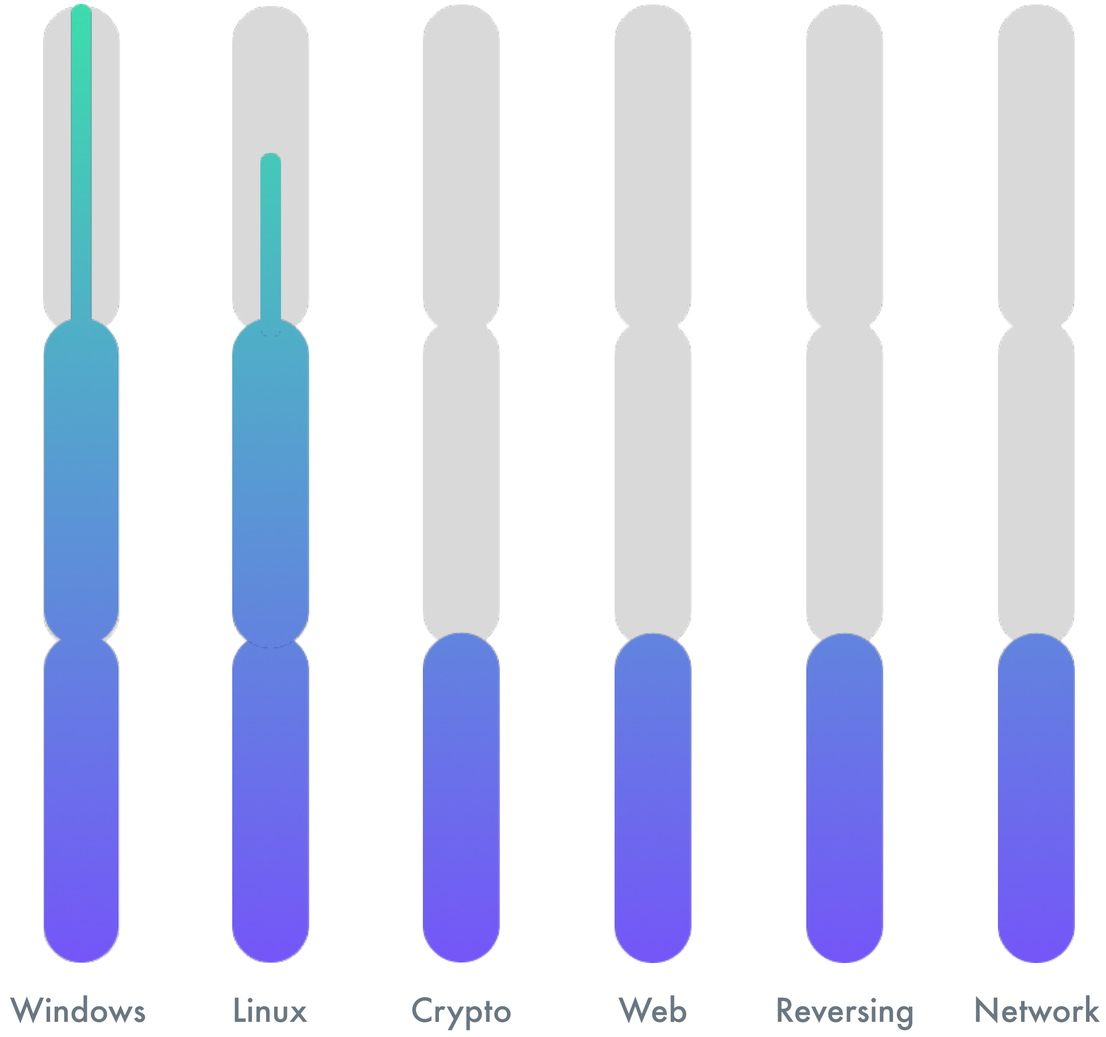
After that, Bob follows these steps:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \mathrm{HASH}(m)$, where HASH is the same function used in the signature generation.

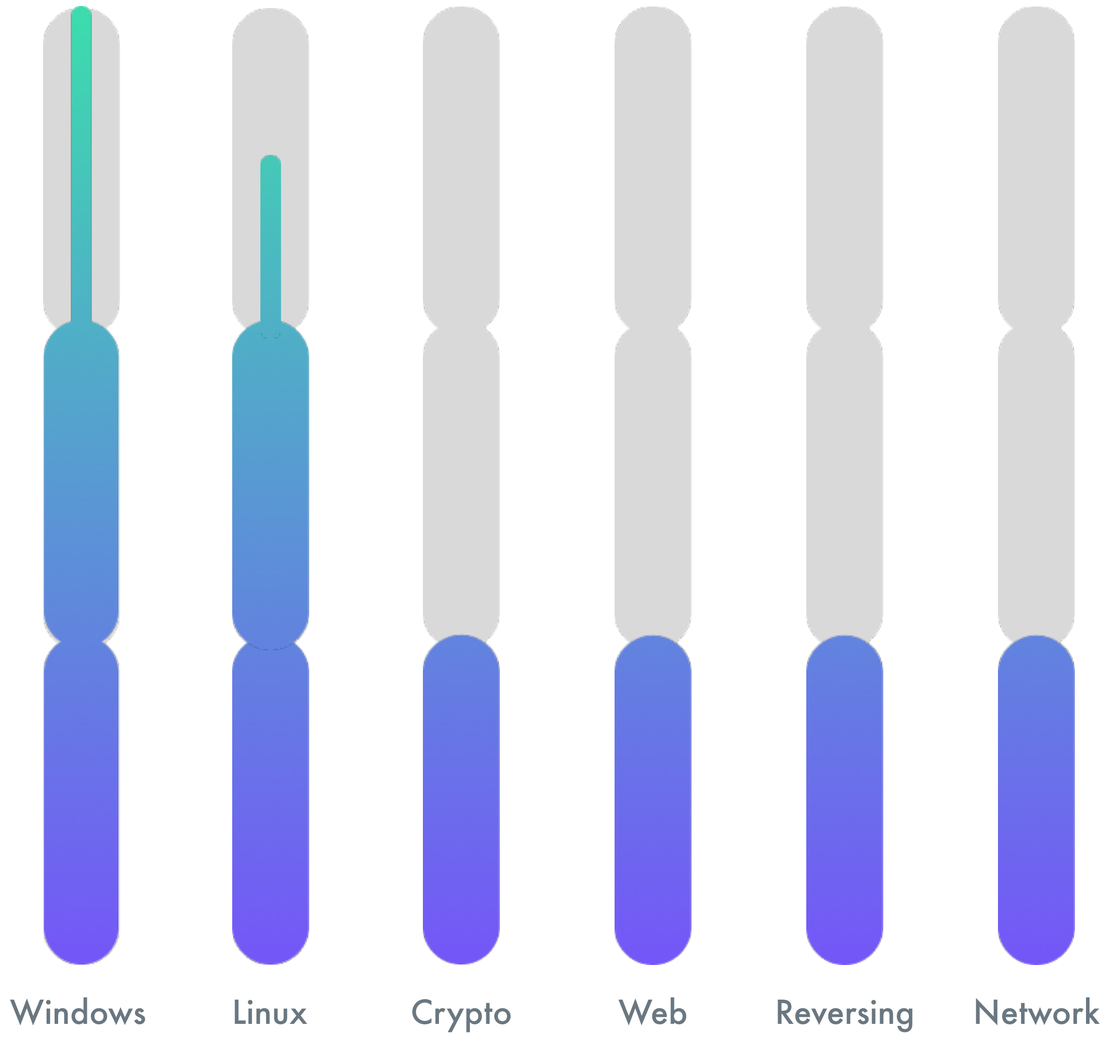
Look at or ask people you look up to how they learn and try emulating this.

ADDICTIONS

Wrapping it up!

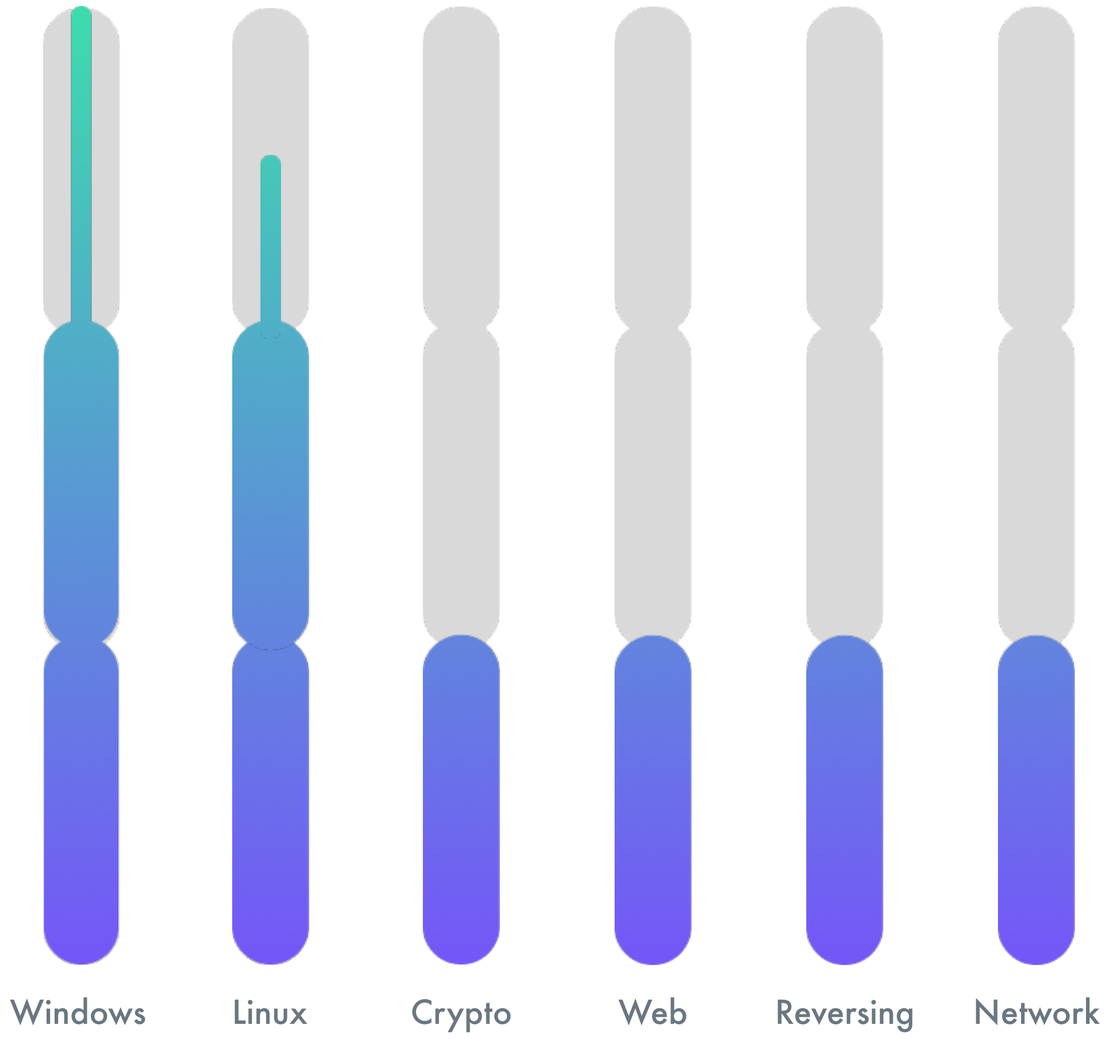


Wrapping it up!



Wrapping it up!

HACK THE WAY YOU LEARN
ENJOY FAILING
DO HARD THINGS
GET UNCOMFORTABLE
HAPPY HACKING



Nothing in the world is worth having or worth doing unless it means effort, pain, difficulty…

-Theodore Roosevelt


THANKS FOR
YOUR TIME...