ATROPOS

Beyond the endpoint:

My Adventures in API Security Research

Bsides Sofia 2024

VANGELIS STYKAS

CTO at Atropos and
independent security researcher

Research interests are mainly API for IoT devices and web application security

@evstykas

www.stykas.com

ATROPOS

HOW IT STARTED

- I could see 12 million locations
- Started pwning stuff for fun

Security Research

- Find vulnerabilities in anything
- Some of them pay bounties
- Get some internet fame

ATROPOS

RESEARCH TYPES

API / WEB	Low hanging fruits, http knowledge , cutting corners
SOFTWARE	Understanding of software, cutting corners and possibly reversing
HARDWARE	Reversing, assembly, understanding of hardware

ATROPOS

ATROPOS

ATROPOS

ATROPOS

THANK YOU

Getting Started

ATROPOS

GETTING STARTED

Jumped from a **CTO** position

Took a **PAY CUT**

NEVER **LOOKED BACK**.

ATROPOS

Gain a solid understanding of CS

Look at O/S

Databases & Networks

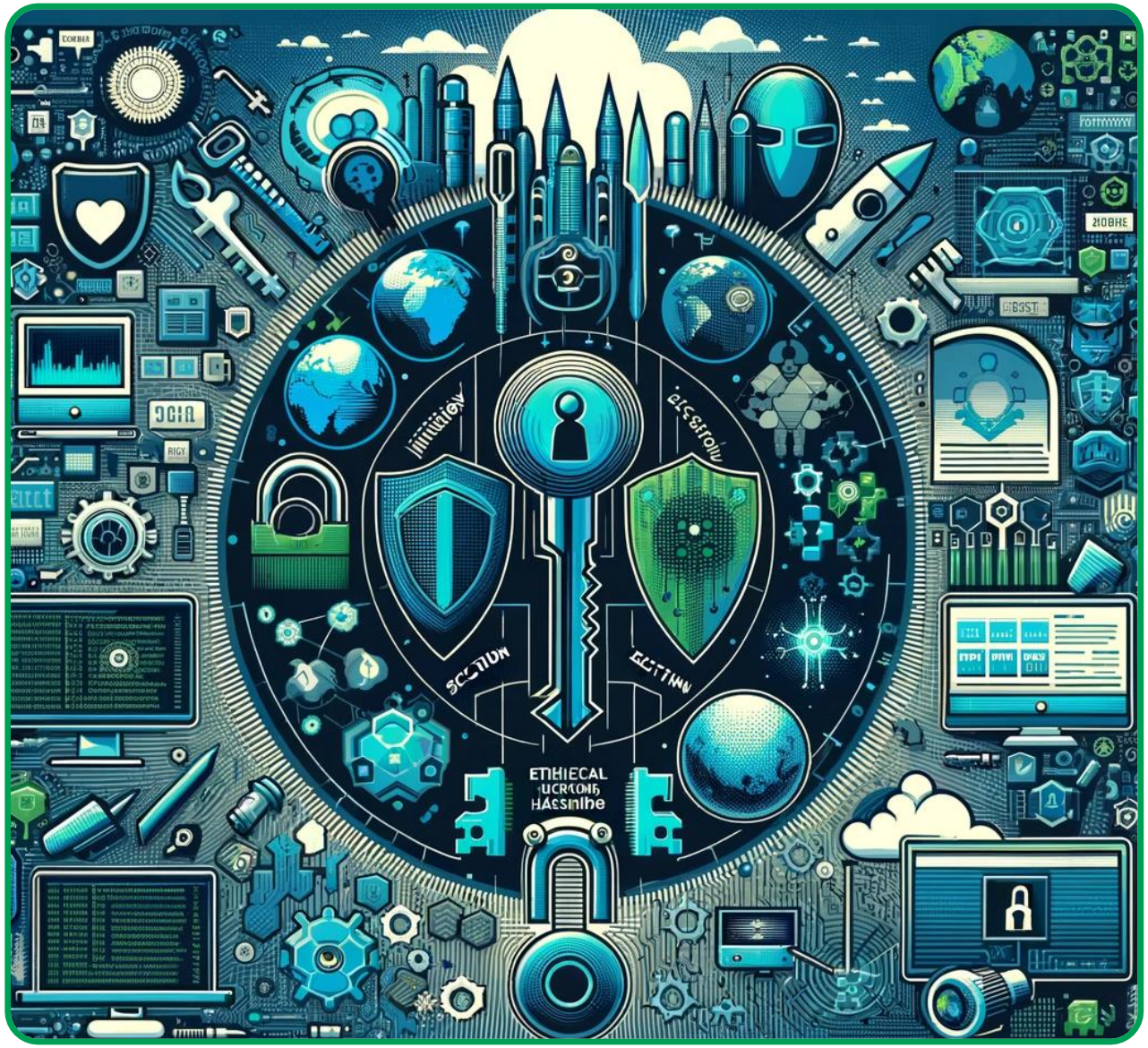
Web application fundamentals

ATROPOS

Familiarize with your tools

What got you here might not get you there

Don’t ALWAYS follow the wave



ATROPOS

Conferences (BSIDES FTW!)

Twitter / Mastodon / Bluesky

Follow & interact

ATROPOS

Security is ever evolving

Stay updated

Follow all the trends and vulnerabilities

Keep moving is the key to success

ATROPOS

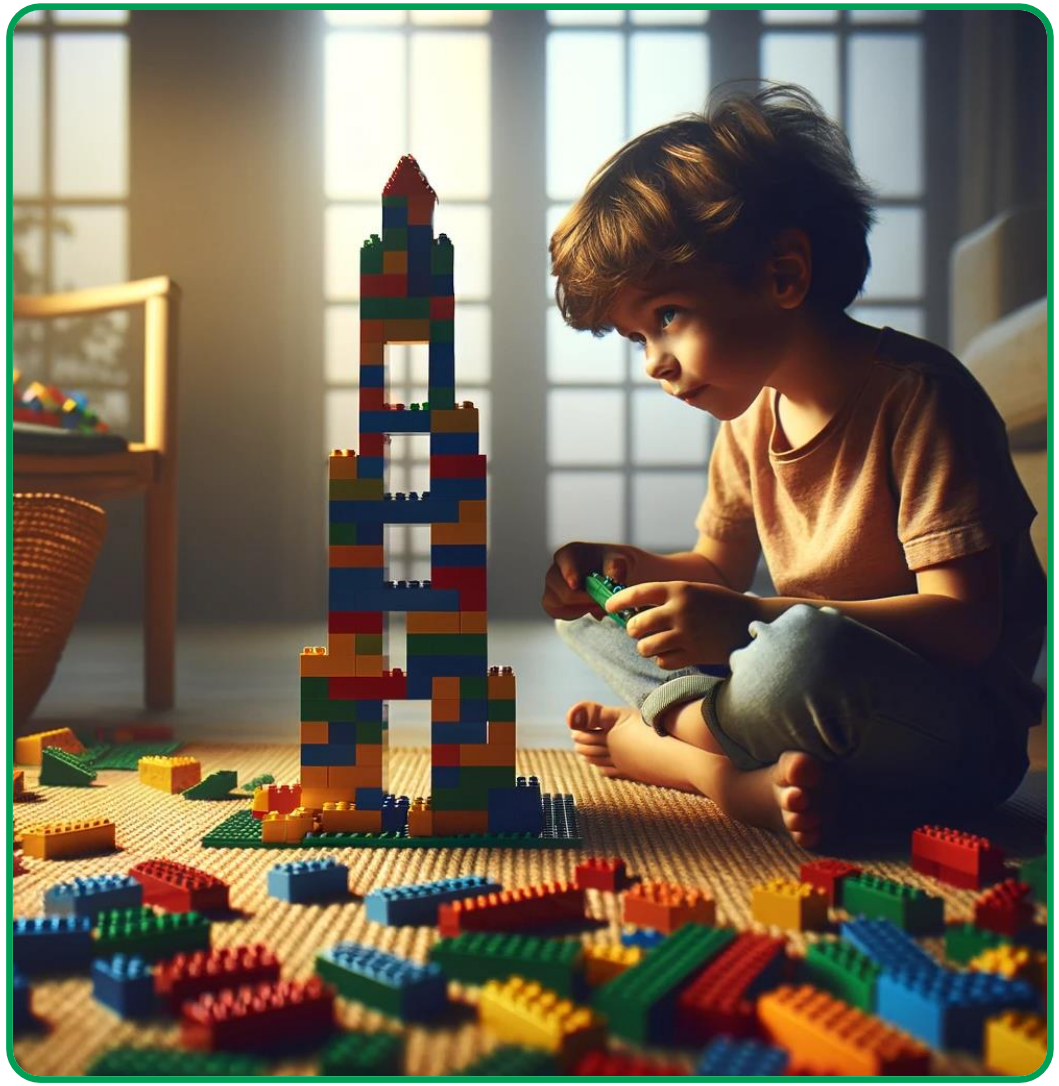
GETTING STARTED

BASICS	Gain a solid understanding of computer science fundamentals, including networks, operating systems, and databases
TOOLS	Familiarize yourself with security tools and software
COMMUNITY	Join cybersecurity forums, attend conferences, and follow security researchers on social media
KEEP LEARNING	Cybersecurity is a rapidly evolving field. Stay updated with the latest security news, vulnerabilities, and research findings. Continuous learning is key to success.

ATROPOS

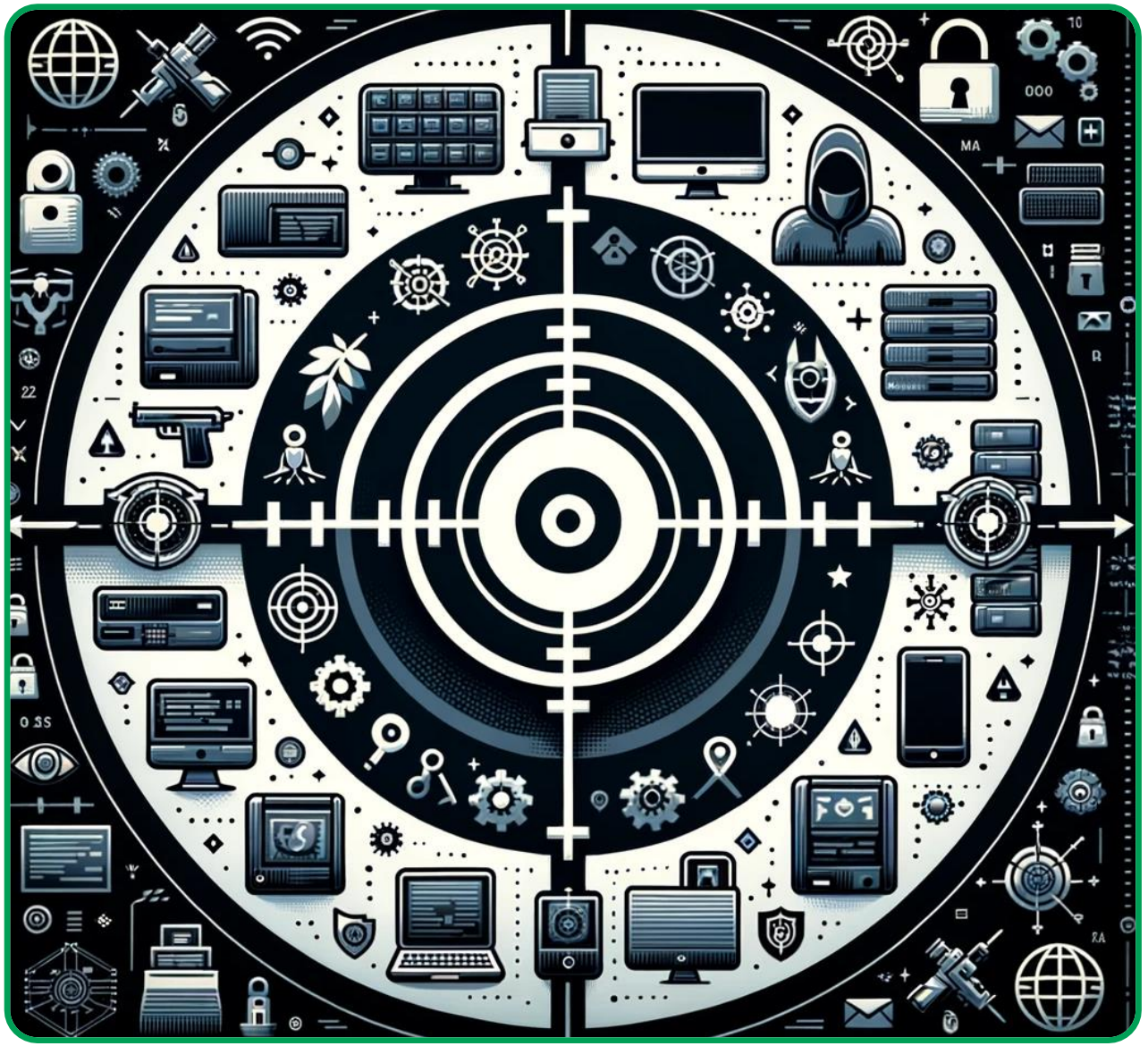
Getting Started

ATROPOS



ATROPOS

Targets



ATROPOS

TARGETS

DON'T go around hacking random stuff

DON'T break the law!

You are going to need a **lawyer**.

ATROPOS

TARGETS

Bug bounties!

$$$

Most of it is **automated**.

You will probably be **disappointed**.

ATROPOS

TARGETS

Regular research

Buy equipment and licenses

Rarely **paid**.

Could drive **traffic** to your company

ATROPOS

TARGETS

Common penetration testing

Paid

You might find a 0-day and not be able to publish it

Furious!

ATROPOS

Personal Brand

ATROPOS

PERSONAL BRAND

Create a **Blog**

Speak at conferences

Videos!

Social media is the way to go

ATROPOS

PERSONAL BRAND

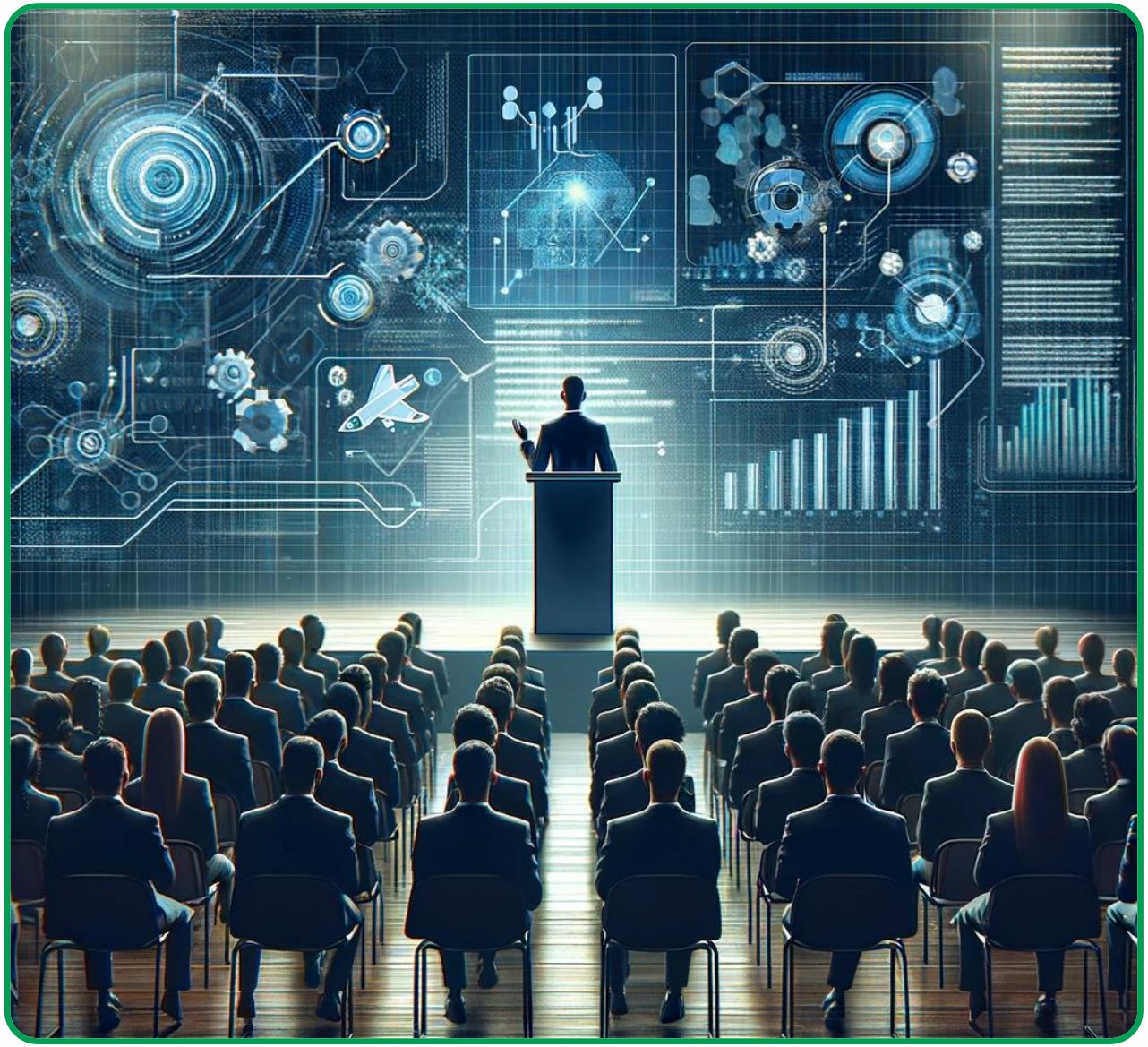
Increased **Visibility**

Opportunities

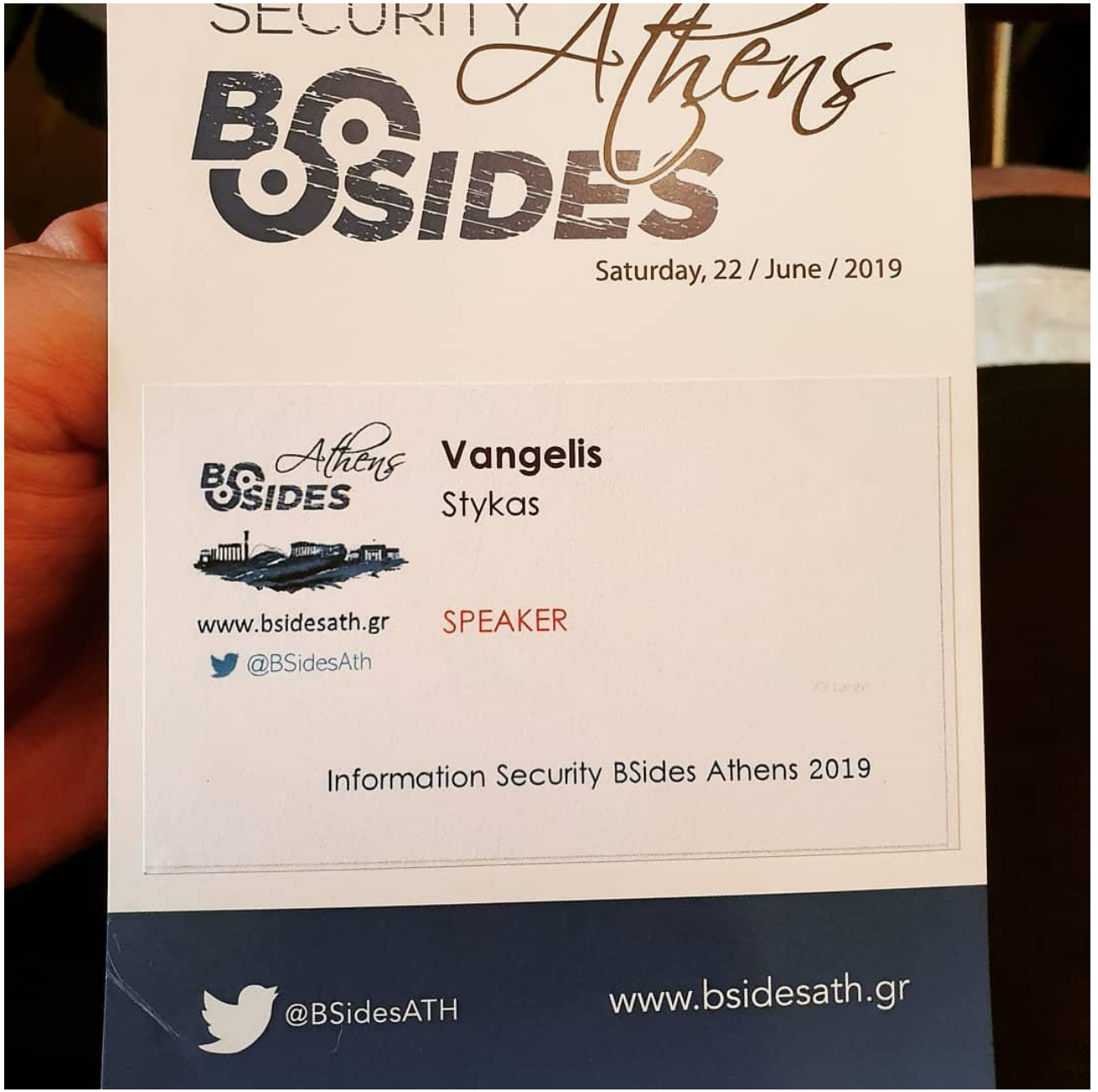
Trust and credibility

ATROPOS

Speaking



ATROPOS


SECURITY
BSIDES Athens
Saturday, 22 / June / 2019
BSIDES Athens
www.bsidesath.gr
@BSidesAth
Vangelis
Stykas
SPEAKER
Information Security BSides Athens 2019
@BSidesATH
www.bsidesath.gr

ATROPOS

Speaking

Introverts accepted

Outside comfort zone

You will **have to learn** to tell **stories**

ATROPOS

Speaking

Personal brand

Enhanced reputation

Increased visibility

ATROPOS

Disclosure

ATROPOS

Don’t be a malakas

Disclosure

- Report should be able to **replicate** the issue
- Should be **detailed**
- **Enough** time
- Prepare for a **fight**
- **Don’t be a beg bounty!**
- Be prepared **not** to disclose too

ATROPOS

Disclosure

Vulnerabilities **will** happen

Someone just **helped** you

Be **kind**

Be **thankful**

Give some **$**

Don’t press charges or force them to do illegal stuff

ATROPOS

I.P.

ATROPOS

Intellectual Property

Much like academia

Trust but verify

Mixed bunch

ALWAYS use your name!

ATROPOS

Intellectual Property

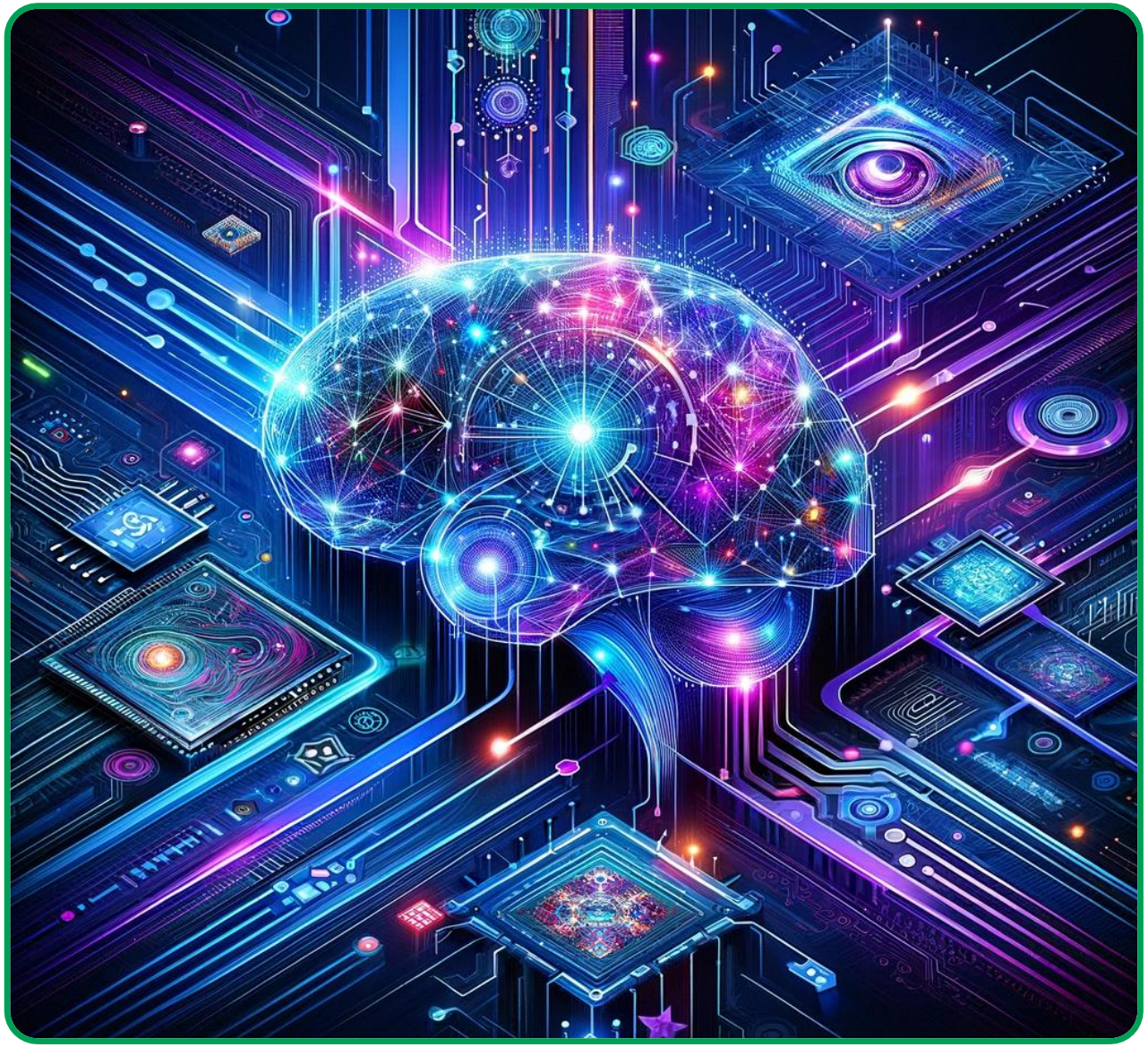
PAY!

DON'T remove employee's name!

If you make money **PAY!**

ATROPOS

A.I.



ATROPOS

ATROPOS

A.I.

Adapt

Use it in your advantage.

Have it **do** the legwork

Look at **low hanging fruits** in there!

ATROPOS

ETHICS

ATROPOS

ETHICS

POTENTIAL ISSUES

- Accessing other people data/devices
- Conflict of interest
- Overstepping legal boundaries
- Government and Corporate Pressure
- Responsible Reporting
- Decline Disclosure

ATROPOS

Don’t be a malakas

ETHICS

Proper approach

- **Don’t** break the law
- **Calculated** risk
- **Co-operate** with agencies
- **Listen** to the agencies

ATROPOS

MENTAL HEALTH

ATROPOS

MENTAL HEALTH

Elephant in the room

Be there for everyone

Don’t depend only on the company

We are all that we have!

ATROPOS

MENTAL HEALTH

Ethical dilemmas

High stakes

Imposter syndrome

Constant vigilance

ATROPOS

IMPOSTER SYNDROME

ATROPOS

IMPOSTER SYNDROME

All been there

New roles

Perfectionists

Expectations

ATROPOS

IMPOSTER SYNDROME

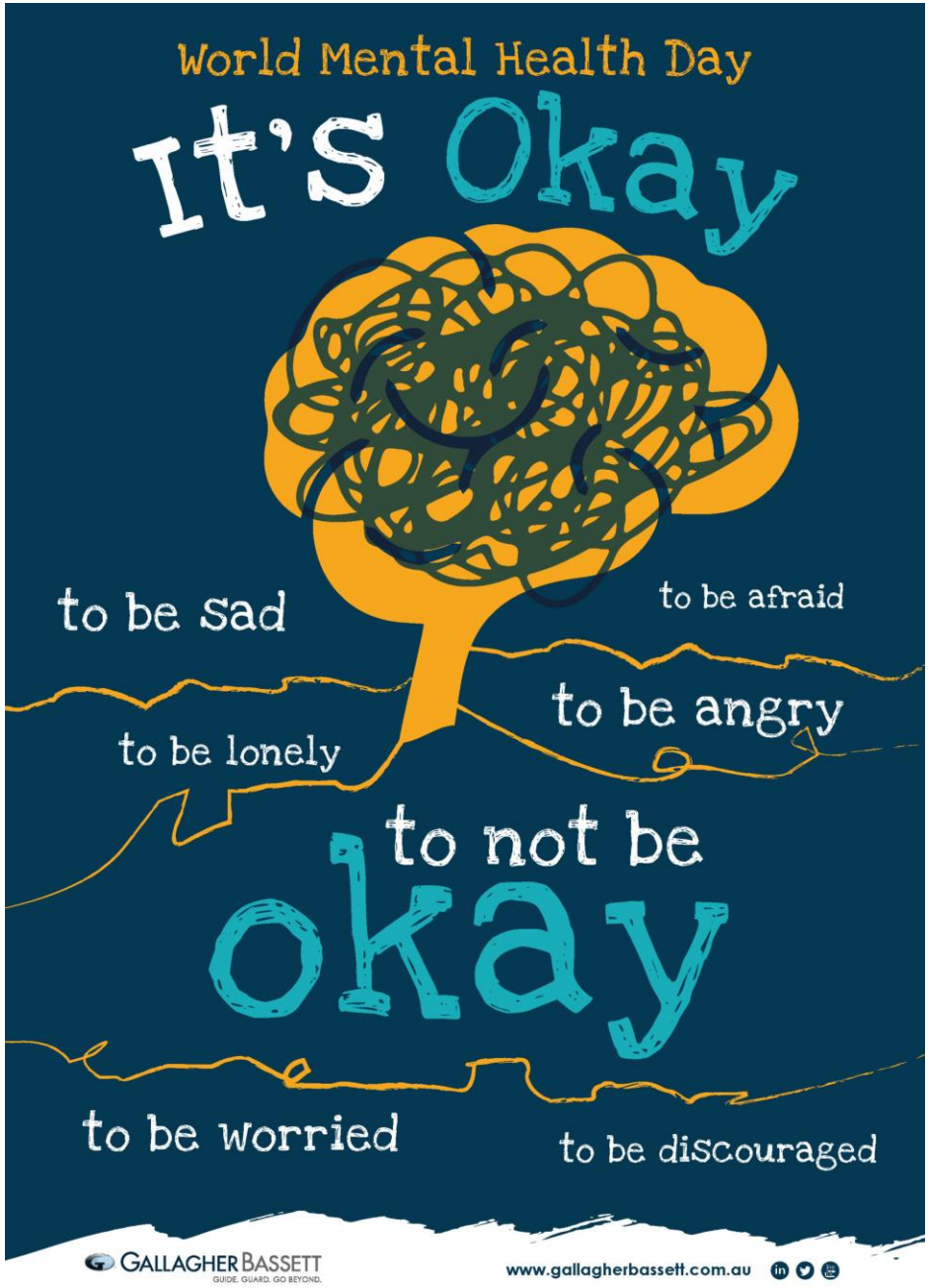
Acknowledge your feelings

Assess your abilities **realistically**

Set **realistic** goals – **Adjust** for time

STOP COMPARING YOURSELF TO OTHERS

ATROPOS


World Mental Health Day
It's Okay
to be sad
to be afraid
to be angry
to be lonely
to not be
okay
to be worried
to be discouraged
GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.
www.gallagherbassett.com.au

ATROPOS

FINAL THOUGHTS

ATROPOS

FINAL THOUGHTS

Be consistent

Participate

Never stop learning

Learn by doing

Prepare for challenges

ATROPOS

FIND YOUR NICHE

Consider market demand

Identify your strenghts

Assess your interests

Do what you love

Love what you do

ATROPOS

ATROPOS

THANK YOU