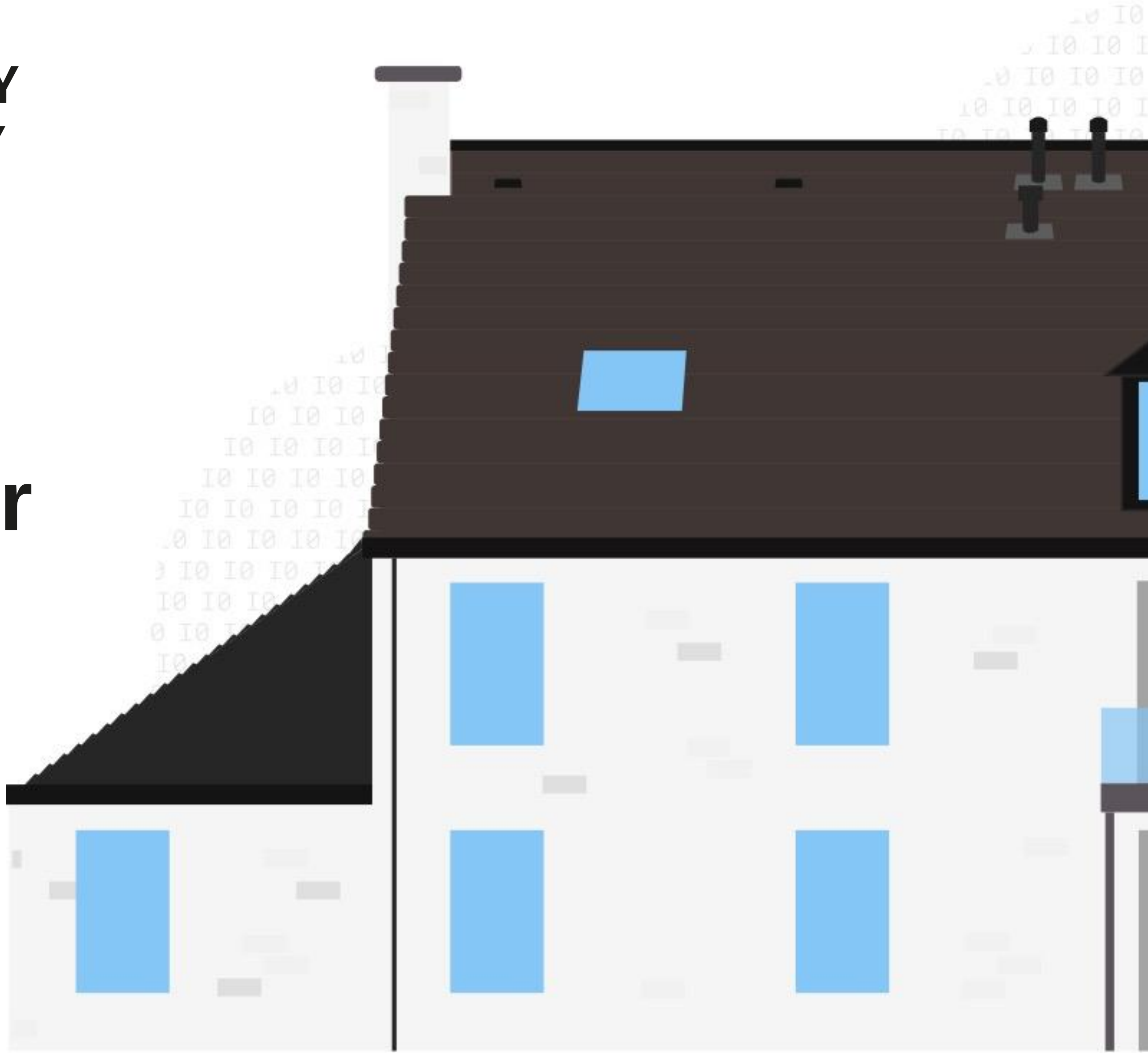
TSF

THE SECURITY FACTORY

Certified pentest partner

Let our ethical hackers test your environment, before someone else does.



Who are we

- Founded in 2013 in the believe that there is a need for a dedicated security testing company
  - Create a home for security enthusiasts who want a career in ethical hacking
  - Provide a focused and specialized service towards the market

- 15 **dedicated and certified pentesters**
  - Full focus on testing, both **technical** and **human/awareness**
  - Experience in a wide variety of sectors and company sizes
  - **Yearly more than 400 pentests** performed by our consultants

Ethical hacking is our DNA

TSF | THE SECURITY FACTORY

Why is security testing important?

Why is security testing important?

- 60 – 70% of companies will deal with a cyberattack of any size this year (source: Axa)

- Average cost (direct and indirect) of a cyberattack: 441 000 € (source: Proximus)

- More and more consumers take reputational security into account before ordering or working together with a company (souce FOD Economie)

Why is security testing important?

- Picanol (damage: >1 000 000€)
- Belnet (attacked from 29 countries)
- ASCO (damage: milions, were back to working with pen and paper)
- AML Labs (hit in crucial timeframe –> COVID: analyzing results)

Why is security testing important?

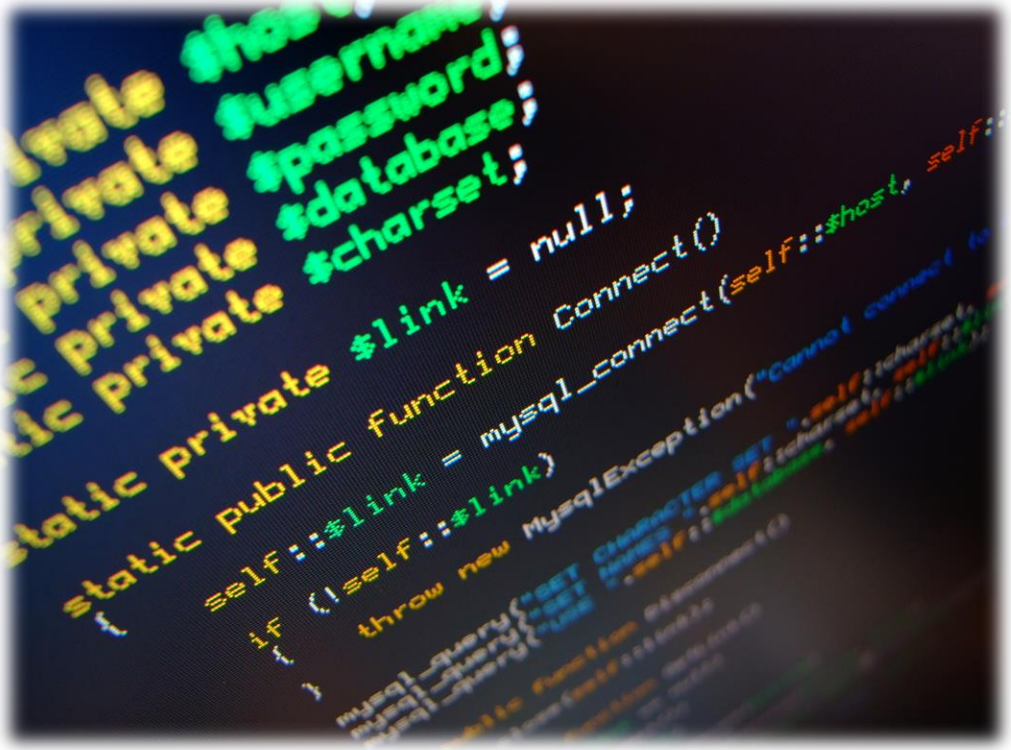
- Validate and improve the security posture
- Roadmap of concrete actions
- ***Let us test it before someone else does***
  - Avoid financial losses
  - Avoid reputational damage

Our focus

Testing Security

Our Focus

Technical testing



```
ivate $host;
rivate $username;
private $password;
 private $database;
c private $charset;
ic private $link = null;
static public function Connect()
{
    self::$link = mysql_connect(self::$host, self::
    if (!self::$link)
    {
        throw new MysqlException("Cannot connect
    }
```

Human testing

Technical Testing

Manual focus

- Automated tools lack the hacking mindset e.g. authorization issues are hard to detect for tools
- More qualitative results
- Demonstrating the impact

Infrastructure testing

- External
  - Public IP range: most realistic scenario
- Internal
  - Scenario of external breach, malware through phishing, malicious employee, …
- Wifi
  - Validate the strength of the Wifi setup and segmentation towards the entire network
- Industrial
  - Testing the (reachability of the) industrial setup/components: e.g. PLC, automated factory

Software testing

- Testing for development flaws e.g. database compromise through the application, account takeover, scripting attacks, …
- Possibilities:
  - Web application
  - Web service
  - Mobile

Testing people

Testing people

Focus on testing and improving security awareness

- Physical social engineering
- Phishing simulations
- Vishing simulations
- Live hacking demo
- USB drops
- Awareness as a service

Red team – the ultimate exercise

Red Team

- Large, more creative scope
- Little to no internal information
- Detection avoidance focus
- Search for the path of least resistance

Pentesting

- Smaller scope
- Tested from an internal position
- No detection avoidance
- Will try to cover as many vulnerabilities as possible

Advantages of red teaming

- Perfect for companies who are already used to penetration testing
- Due to the large scope combined with the creativity of our testers we find new issues
    - Out of the box issues
    - Vulnerability chains
    - Etc.

References

DKV

AG
INSURANCE

GROUPE P&V

UNILIN

GlobalSign®

COLRUYT
GROUP

brussels
airlines

Car-Pass

H.ESSERS

TSF | THE SECURITY FACTORY

Contact us

+32 3 369 33 99

www.thesecurityfactory.be

info@thesecurityfactory.be

Samenwerkingsstraat 50, Niel 2845