dracmaservice

software house and web solutions

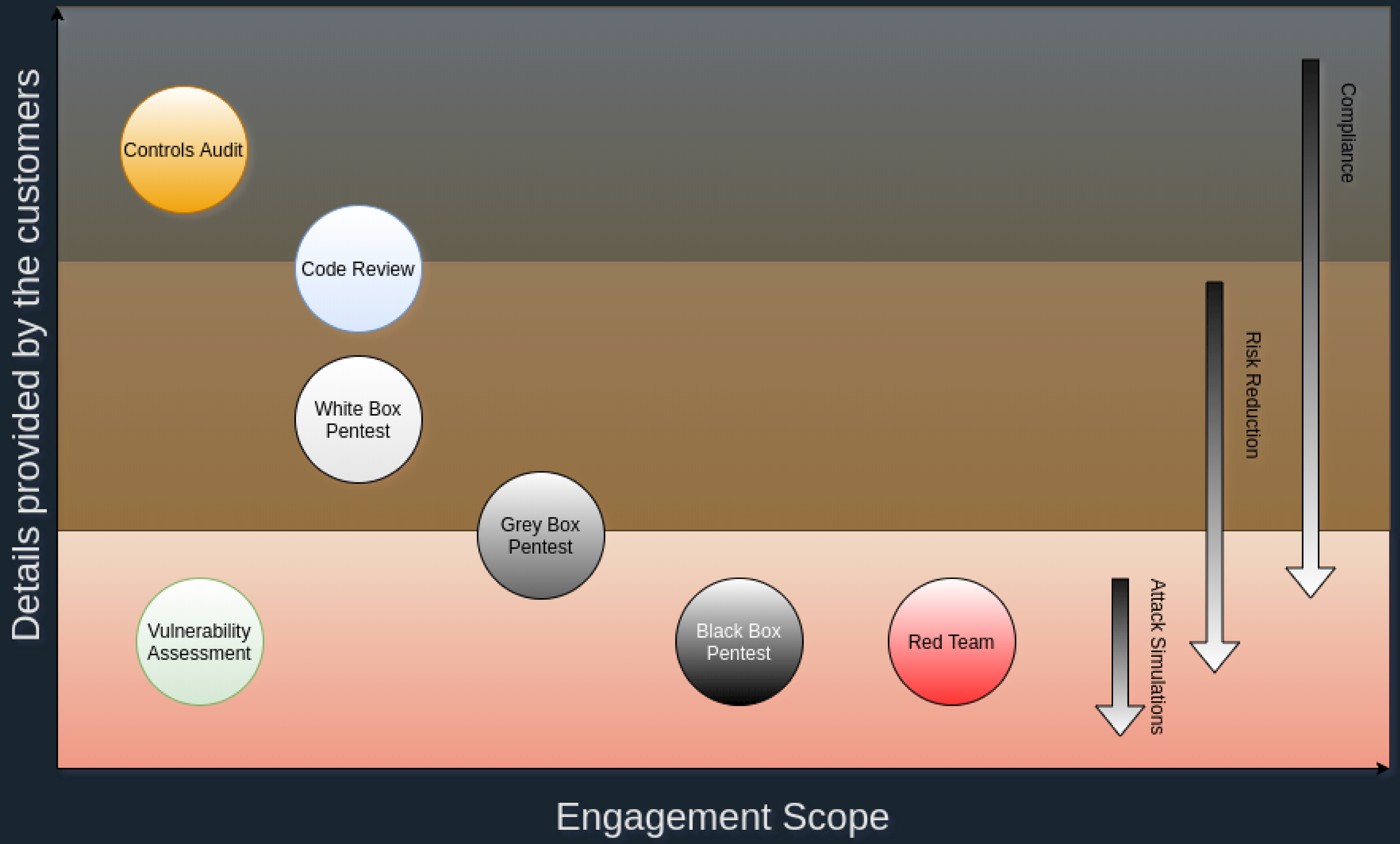
# CYBER SEC SOLUTIONS

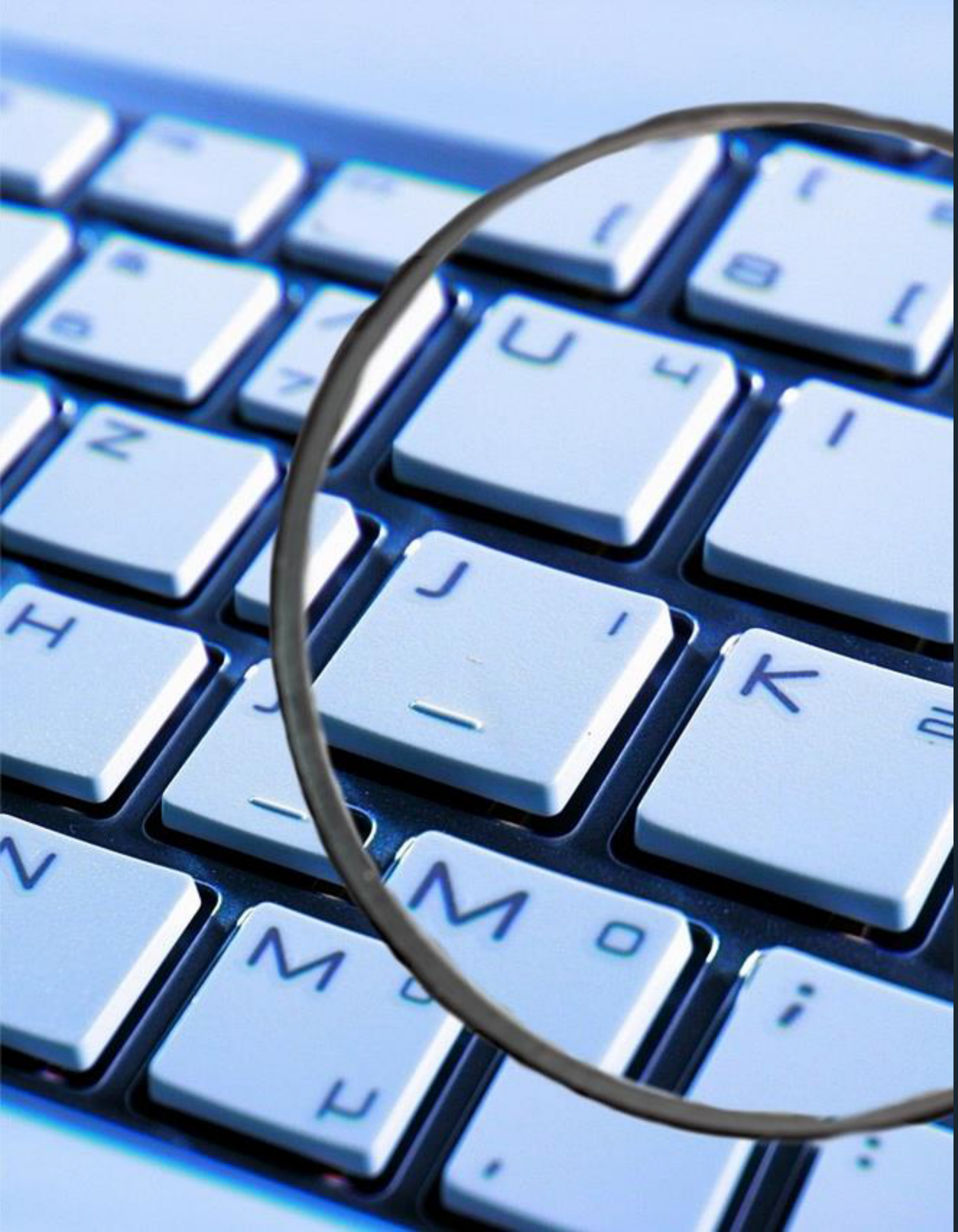
There are no secrets to success. It is the result of preparation, hard work, and learning from failure.

Conrad Hilton

# ETHICAL HACKING SERVICES

# Security Assessments





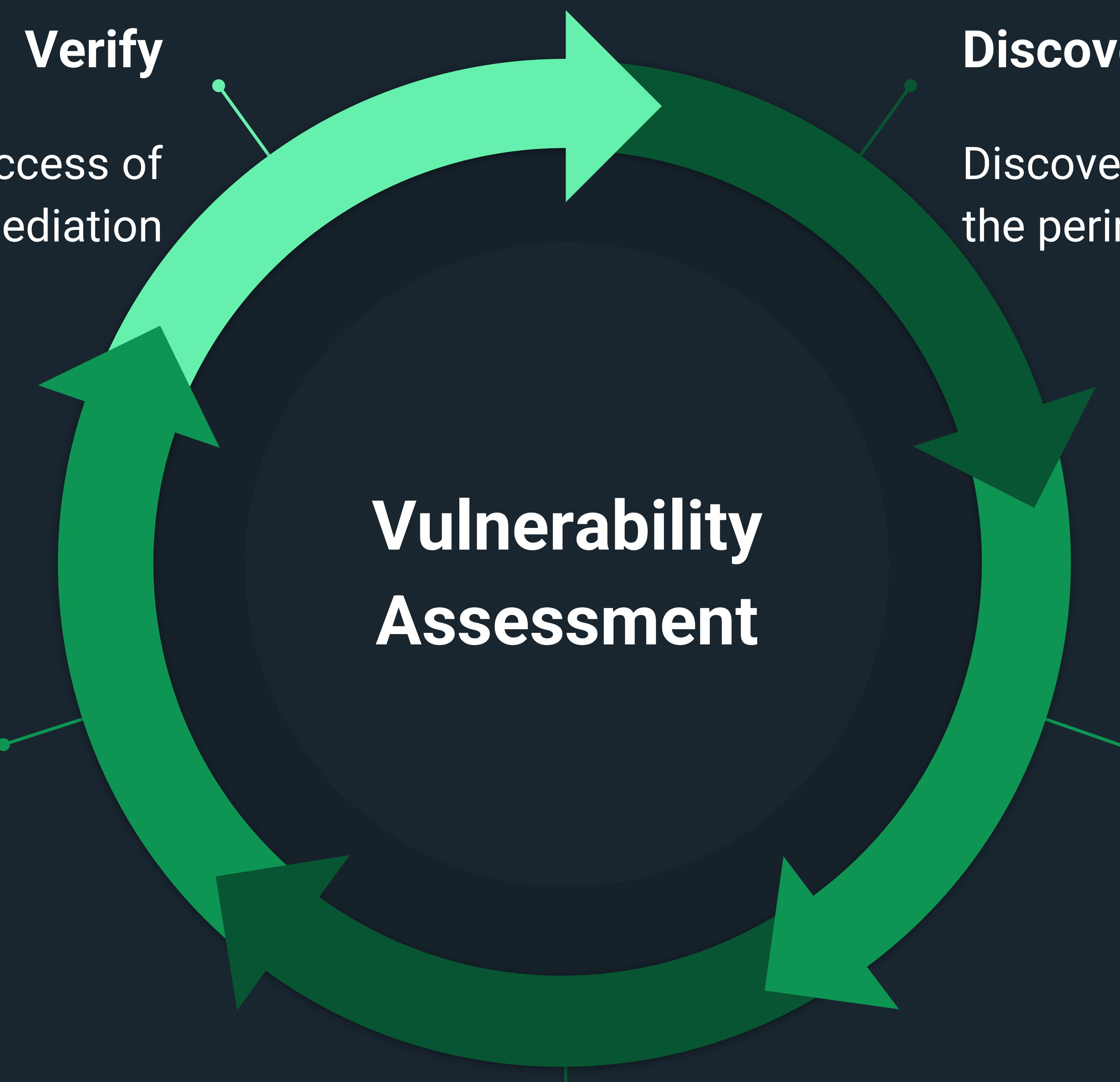
# Vulnerability Assessment

Vulnerability Assessment is the process of identifying, quantifying and prioritizing vulnerabilities that are present on systems or networks.

Vulnerabilities can be found on network devices, systems, applications from third-party vendors or internally made software.

Vulnerability Assessment discovers which vulnerabilities are present, but do not differentiate between flaws that can be exploited to cause damage and those who can not. VA alerts companies to the existing flaws and where they are located.

# Phases of Vulnerability Assessment



**Discover**

Discovering host and the perimeter

**Assess**

Scan and find vulnerabilities

**Report**

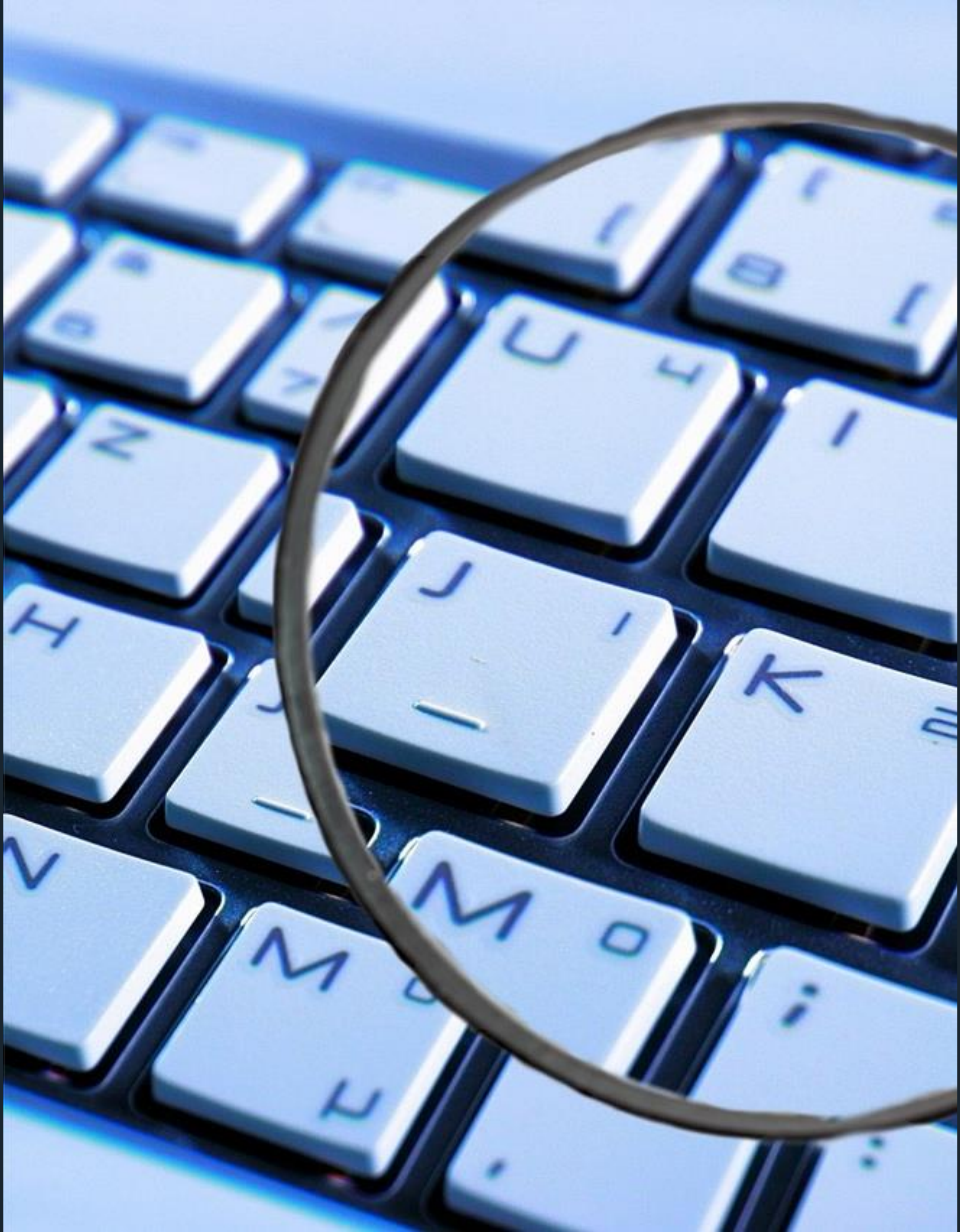
Report and prioritize the remediation of the findings

**Remediate**

Assign tickets for remediation and monitor vulnerabilities

**Verify**

Confirm the success of remediation



# Penetration Test

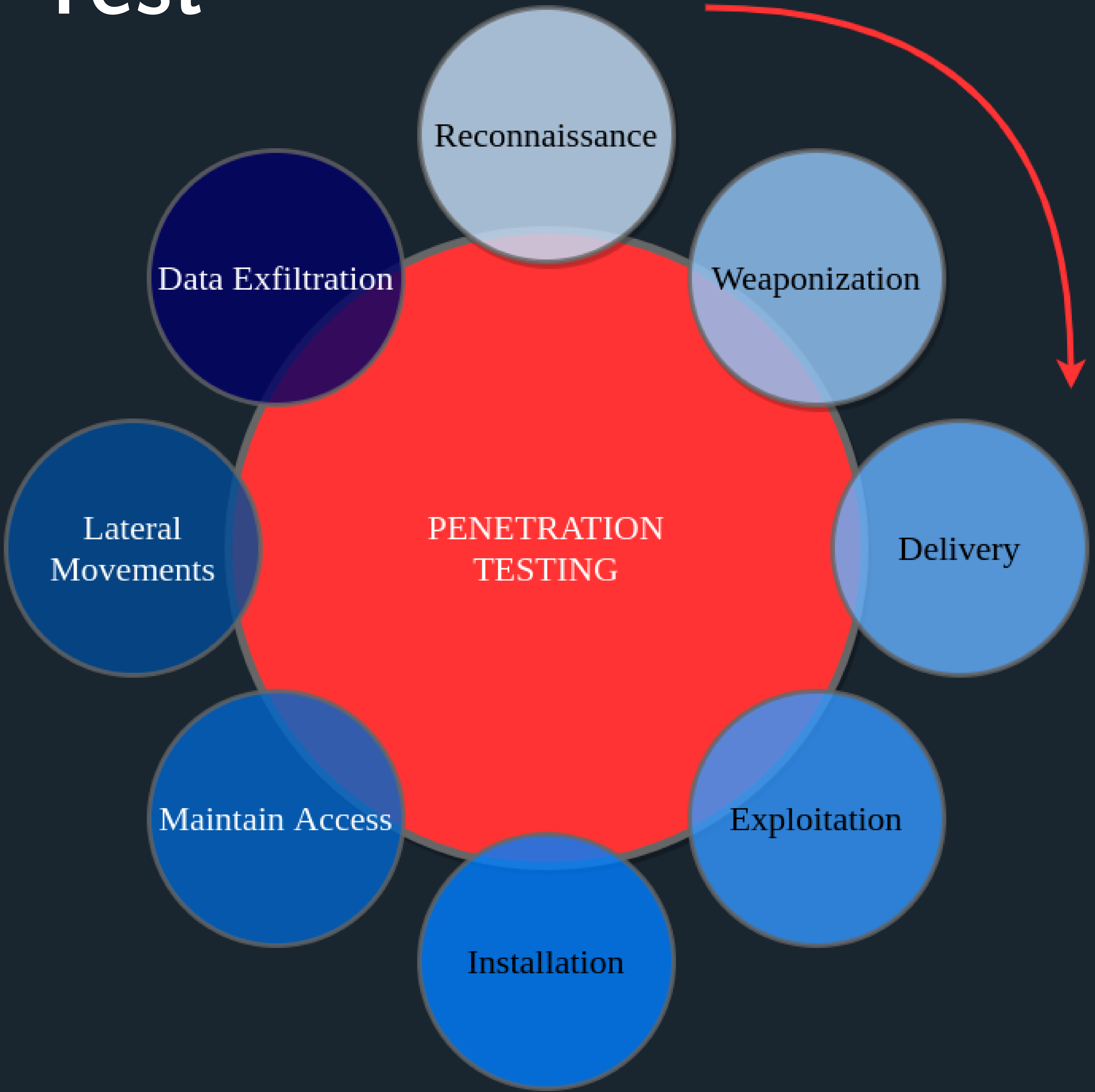
Penetration test is an authorized simulated attack on a network or computer system performed to evaluate the security of the system .

The process typically identifies the target systems and a particular goal.

A penetration test can be:

- White box: pentesters are provided information about the systems
- Grey box: pentesters are provided some information about the systems
- Black box: pentesters know only the company name
- Pentest is a more in-depth test than vulnerability assessment, because vulnerabilities are exploited and it’s possible to verify the consequences .

# Phases of Penetration Test



# Red Team Assessment

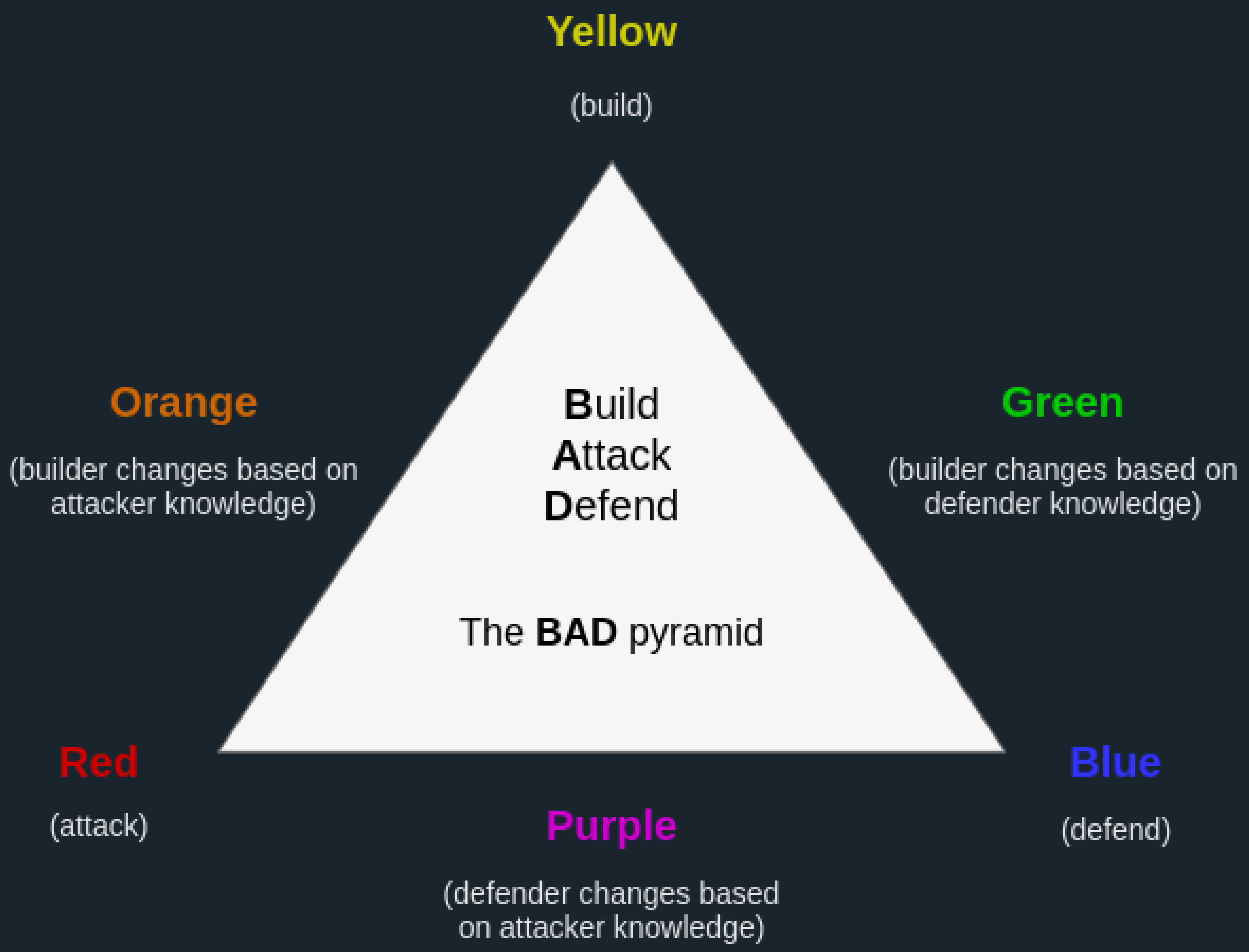
Red Team Assessment is similar to a Penetration Test but is more targeted.

The goal of the Red Team is not to conduct a full assessment of the network, but to test the organization's response capabilities.

The Red Team will try to get in using all the possible techniques and access sensitive information without getting caught.

This kind of test has a longer duration than other security tests, up to 1-2 months and it's suggested for companies with a strong security dedication.

# Security Teams



Yellow

(build)

Orange

(builder changes based on attacker knowledge)

Build
Attack
Defend

The **BAD** pyramid

Green

(builder changes based on defender knowledge)

Red

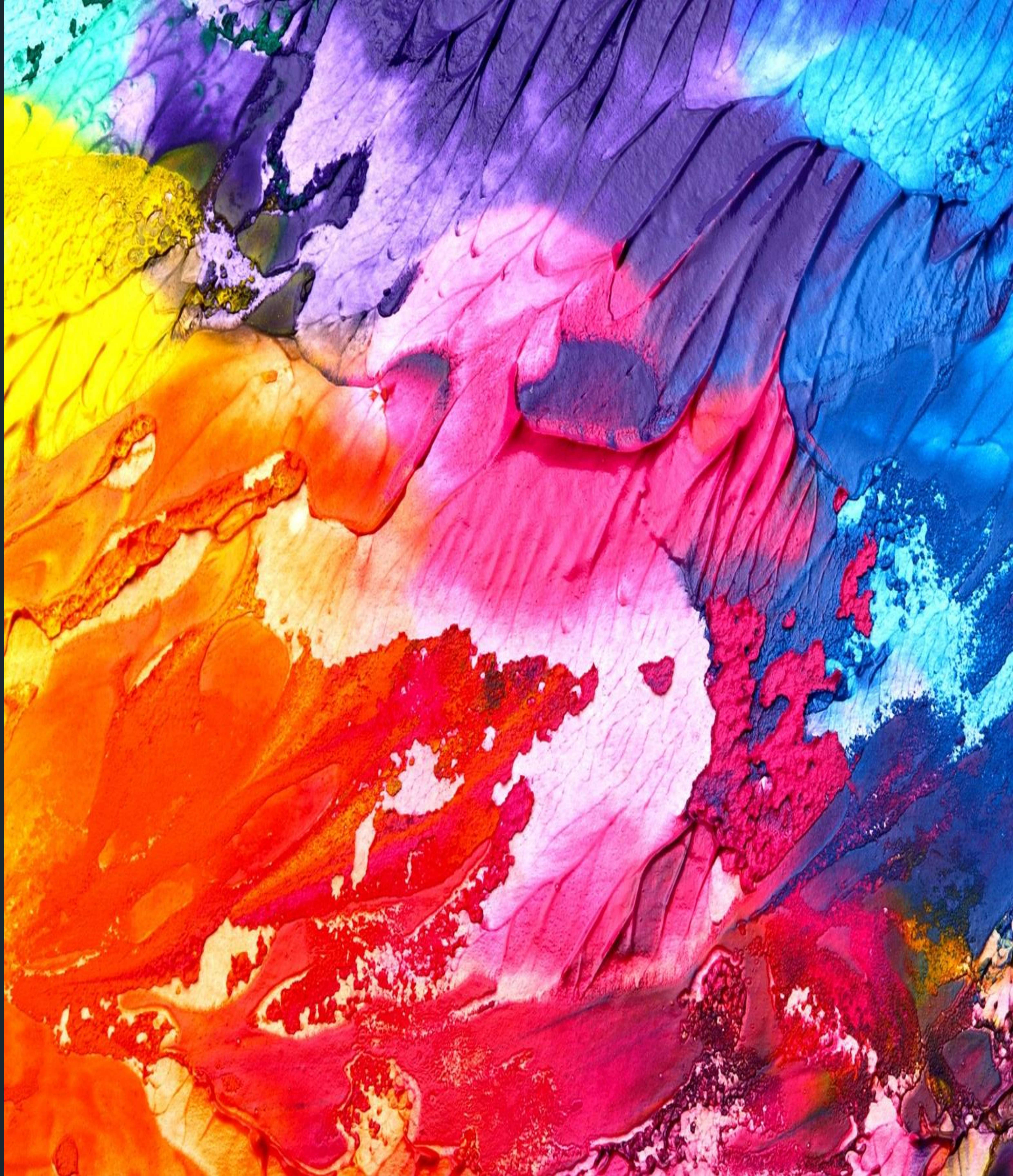
(attack)

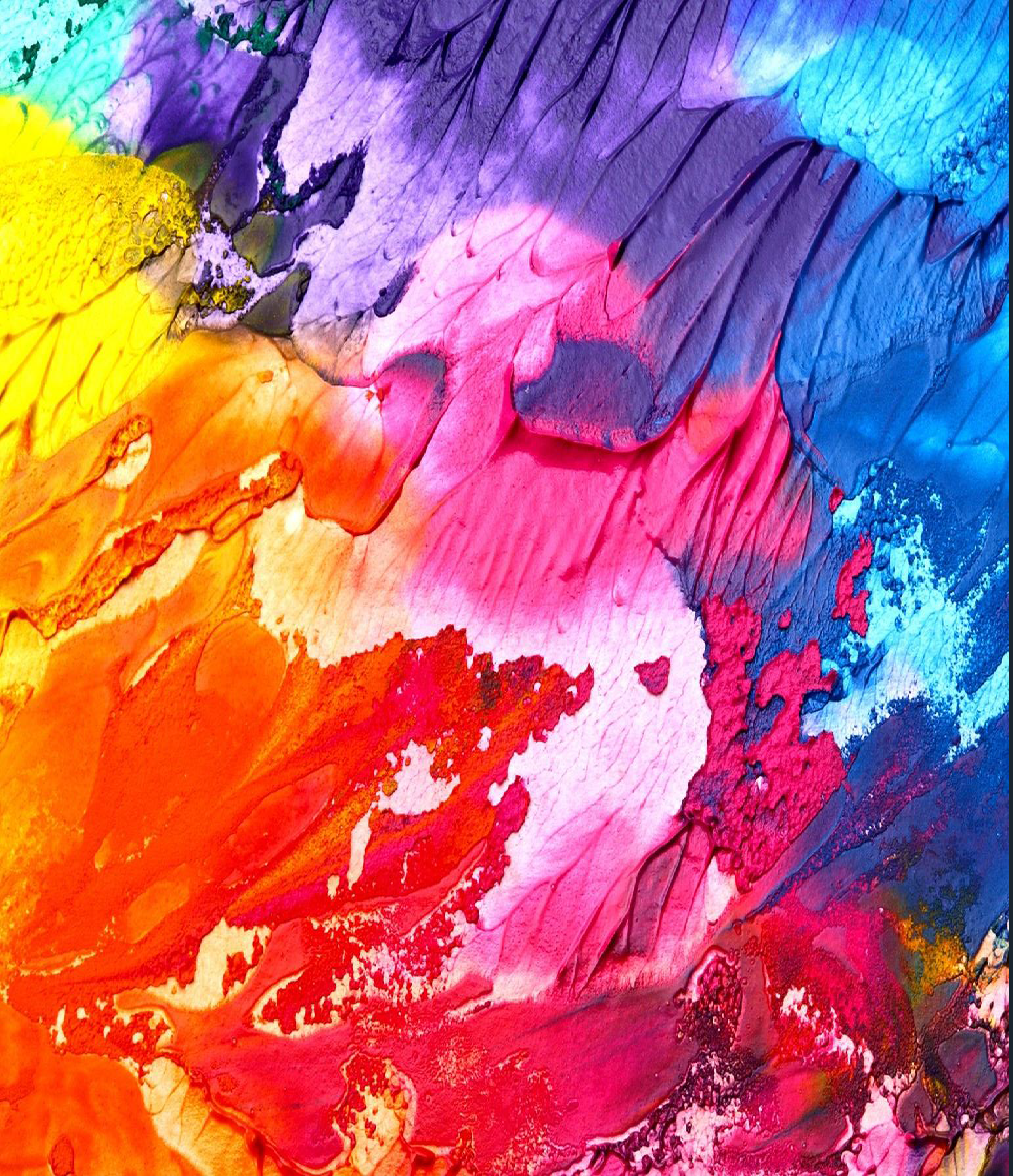
Purple

(defender changes based on attacker knowledge)

Blue

(defend)





# Purple Team

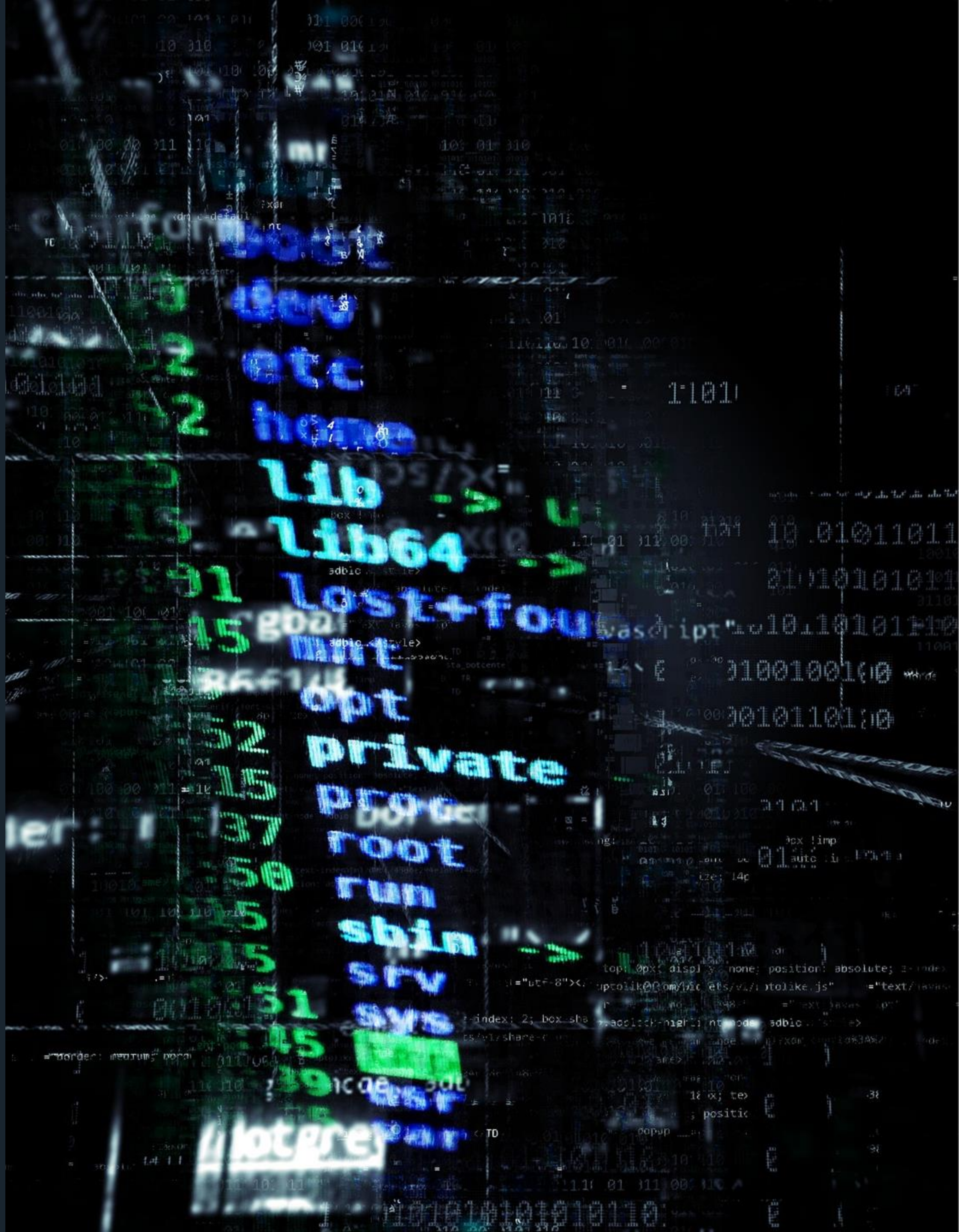
- Yin and Yang
- It's a cooperative mindset between attackers and defenders working on the same side
- Ensure and maximize effectiveness of the red and blue team
- Integration of defensive tactics and controls from the Blue Team with the threats and vulnerabilities found by the Red Team into a single narrative
- It's permanent and dynamic between red and blue team

# Web Application Assessment

For many companies, web applications are a crucial part of their operations.

They allow customers to access sensitive information, they process credit card orders, they allow the company to conduct business and they are a presentation of it for the external world.

Web Application Assessment identify, categorize and verify the impact of vulnerabilities on the company assets, to protect your data, your customers and your reputation.



# Simulated Phishing Campaign

Simulated Phishing Campaign is part of the security awareness program for the company staff.

Most of the attacks take advantage of the weak link in the organizations, people.

A Phishing campaign involves the delivery of fake emails containing links or attachments. Almost 30 % of the global users open phishing emails every year.

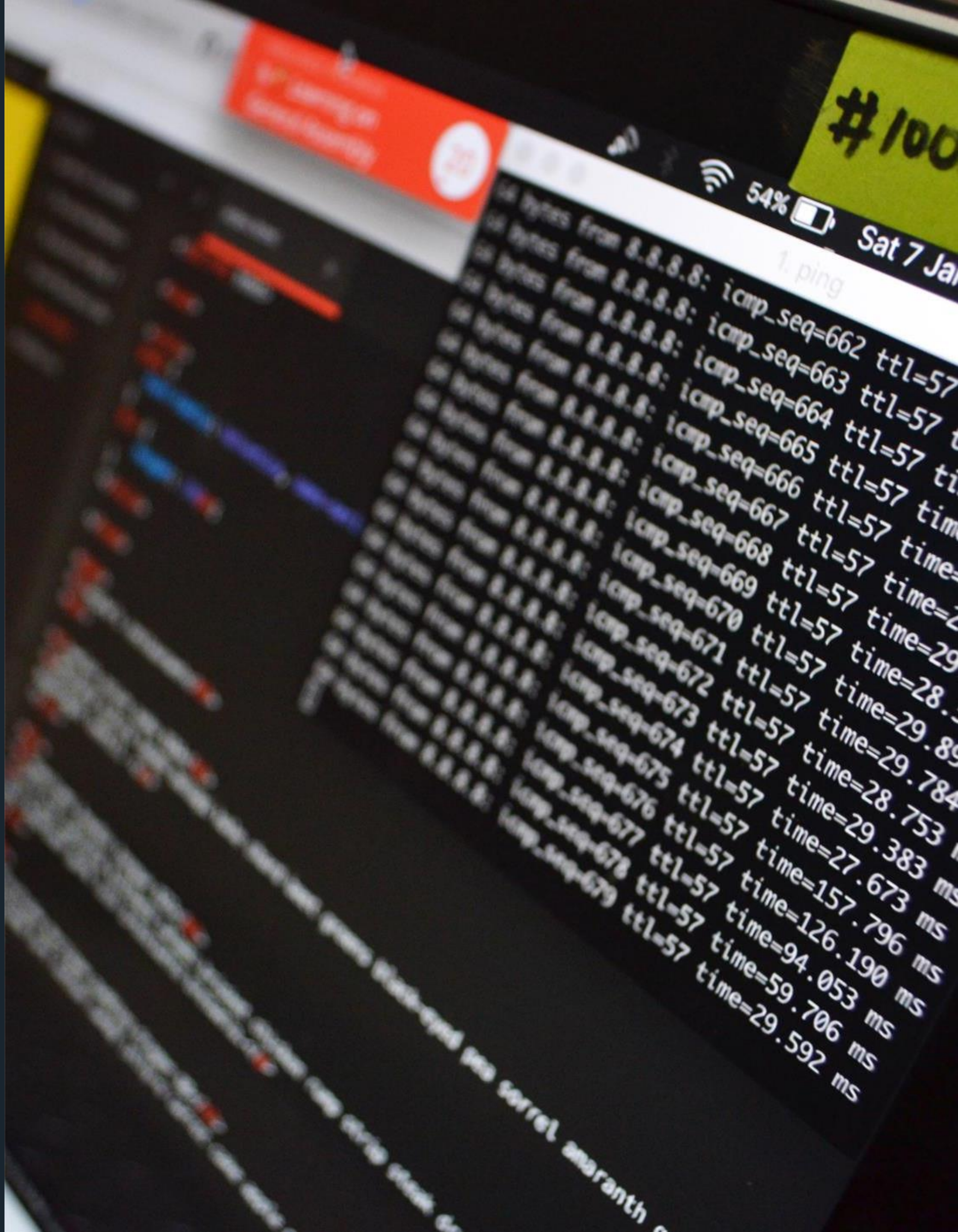
At the end of the test, for people who consistently fell for spoofed emails, there will be a course follow up to avoid this kind of behavior.

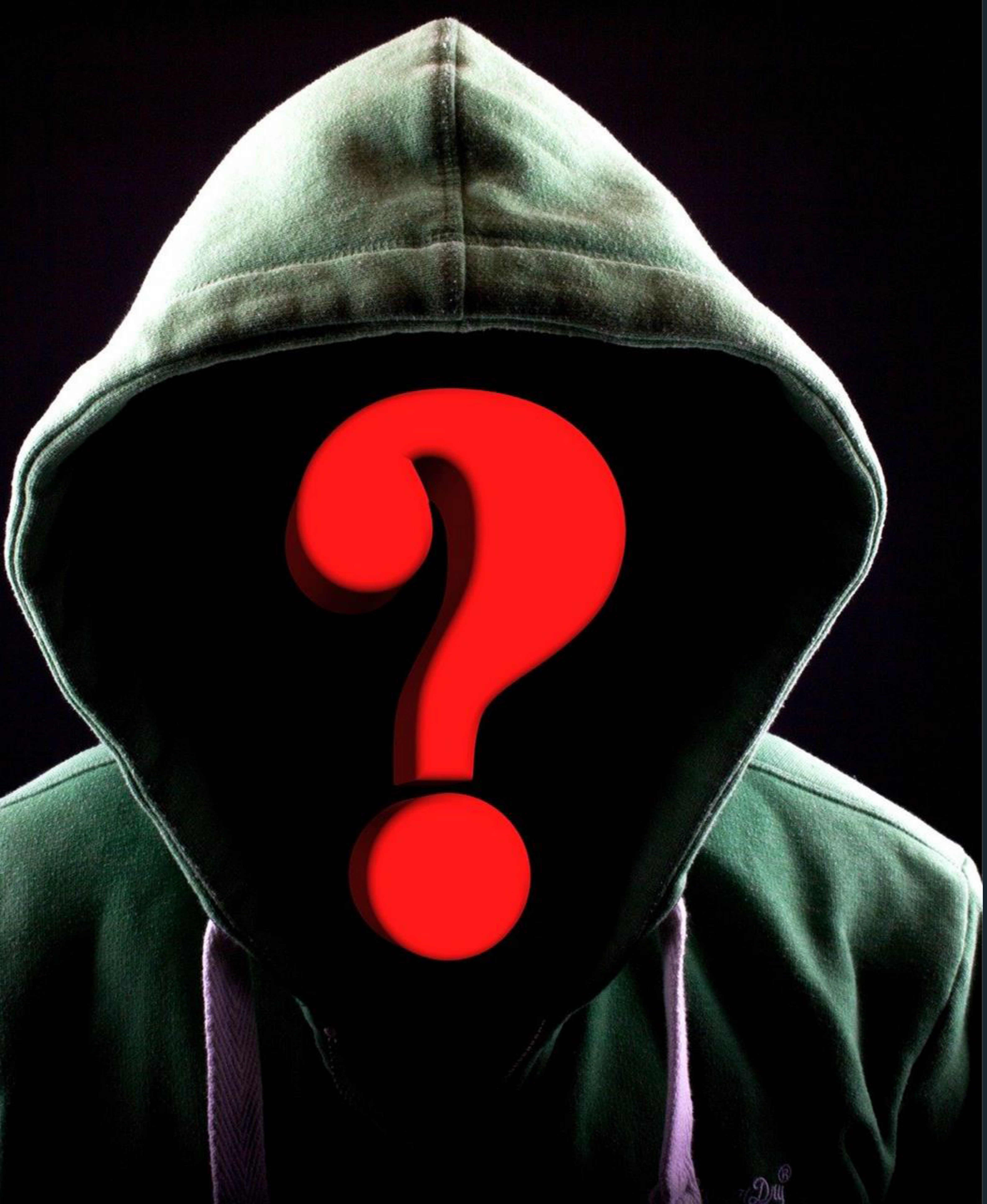
# CIS Controls

CIS controls are developed by a community of IT experts who apply their expertise to create globally recognized security best practices.

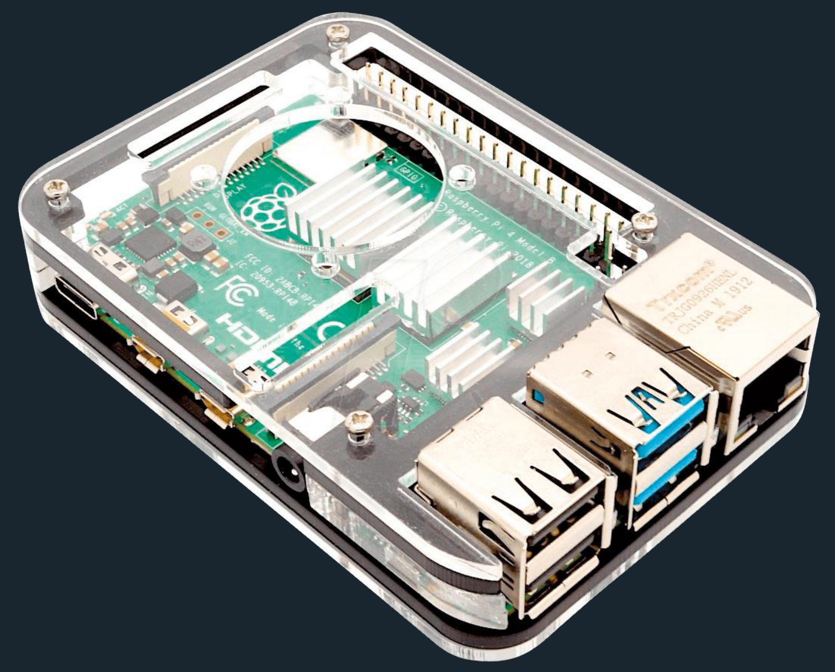
The framework consists of 18 essential controls, capable of defining an effective defense path that every company should undertake to assess, monitor and manage cyber risk. The security controls derive from the main attack patterns highlighted by the threat reports and therefore represent direct countermeasures to reduce the risk.

The main advantage of CIS Security Controls is to be found in the fact that they represent and prioritize a minimum number of extremely effective actions, both in terms of benefits and costs.





# Code name: IAS



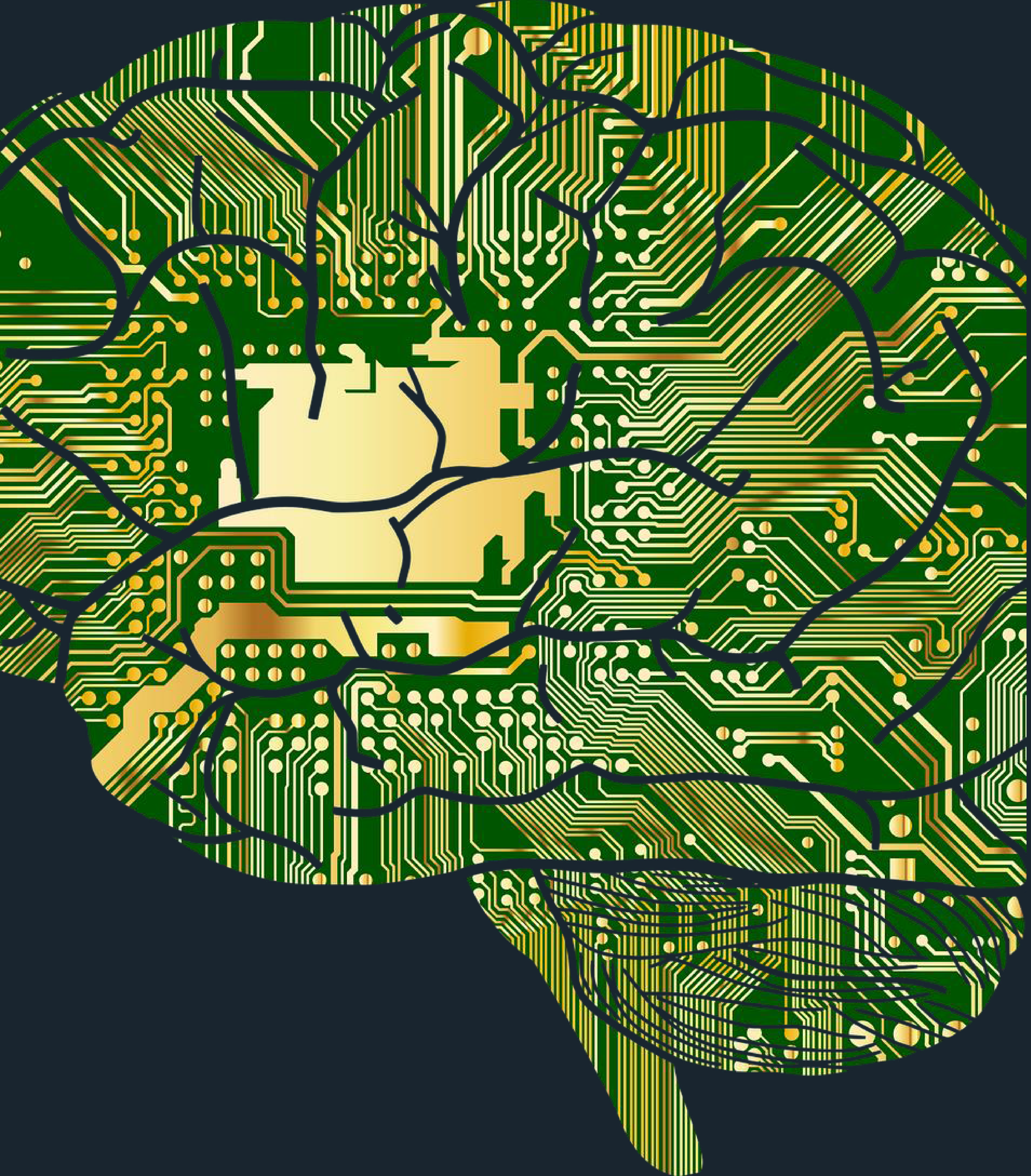
IAS is the new proactive cyber security service that allows you to have an objective feedback on the security posture of your network infrastructure.

- Developed and engineered in house by the EH team
- Advanced Adversary Simulation
- C&C Server Simulation
- Scanning and analysis of internal devices
- Scan for internal device vulnerabilities
- Subject to authorization, possibility of exploit execution

# OSINT

OSINT is an intelligence discipline that deals with the research, collection, analysis and correlation of data obtained from public and open sources.

OSINT activities can provide an idea of corporate exposure and what information is publicly available. They allow to identify and identify the security posture with respect to which data cybercriminals could exploit to carry out direct or social engineering attacks.



# THANK YOU

dracmaservice

software house and web solutions