DO YOU MASTER YOUR **ATTACK SURFACE ON INTERNET?**

Everything starts with a

weakspot

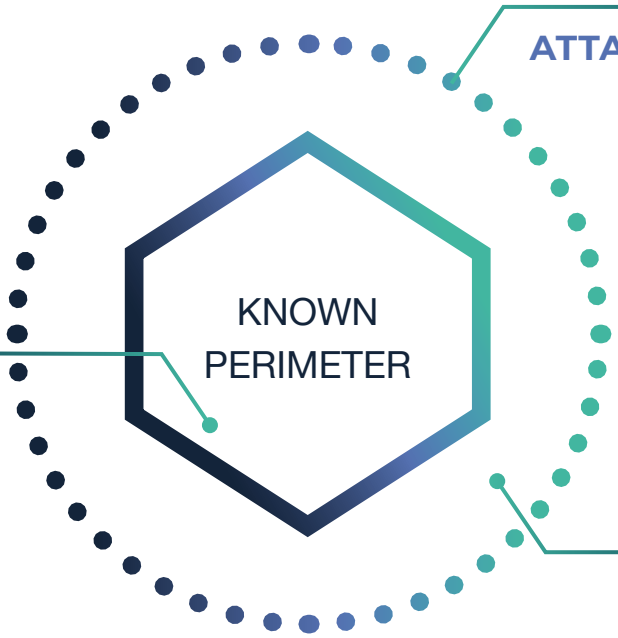
CONTEXT

THE RISE OF THE DIGITALIZATION OF COMPANIES

- **Ressources outsourced in the Cloud**
- **Deployment of SaaS solutions**
- **Employees, BUs or subsidiaries working autonomously**
- **Integration of IT Systems from Mergers & Acquisitions**

DIFFICULT CONTROL OF THE INTERNET ATTACK SURFACE

CISO TOOLBOX



ATTACKER POINT OF VIEW
Larger scope & weakposts first

weakspot
Complementarity with the CISO's toolbox

TOOLBOX
Pentests
Bug bounties
Vulnerabilities scans
Rating solutions
Expertise on specific issue

SHADOW IT

WHO ARE WE?

Weakspot is a French cybersecurity startup specialized in the identification of risks related to Internet exposure.

WHAT'S OUR SOLUTION?

Weakspot is a non-intrusive, automated SaaS solution that monitors a company's Internet attack surface. The aim is to complement the external view of the IS from an attacker's point of view.

FOR WHO?

For any company with a confirmed cyber exposure.

HOW DOES IT WORK?

FULLY AUTOMATED AND NON-INTRUSIVE SAAS SOLUTION

1

MAPPING

Hybrid approach
OSINT
Technical scans
Public databases
Configuration scans

ENTER YOUR DOMAINS AND LAUNCH THE ANALYSIS IN ONE-CLICK

WEAKSPOT maps the technical elements exposed on Internet from an attacker's point of view for an enhanced scope.

2

ANALYSIS

Controls
Compliance
Vulnerabilities
Supply Chain
Custom

The technical elements discovered are analyzed according to the controls defined by the user's issue.

3

DASHBOARD

Double purpose
Managers
Operational team

FIND YOUR EVOLUTION AND PERFORMANCE INDICATORS ON YOUR DASHBOARD

KPI's view: check your evolution since the previous launch, your exposed elements and your severity score.

CONSIDER YOUR EVOLUTION AND YOUR CRITICS AREA FOR IMPROVEMENT

Forensic view: access your data to follow the controls implemented and consider the areas to be corrected

DEFINE A RECURRENT BASE

Set-up a recurrence according to your needs and work on your risk level continuously

CUSTOMER USE CASES

1.COMPLIANCE

Company: **Big account in Industrial Sector**

Contact: **CISO**

Issue: The CISO has just been appointed CISO Group. He wants to check compliance with international standards (ANSSI IT hygiene Guide, NIST, ISSP's client, etc.) of the company and its subsidiaries in order to know where his team must focus their efforts but also monitor the evolution.

2.NEW THREAT

Company: **Big account in Defense sector**

Contact: **Information System Director**

Issue: The ISD has just been informed of a new threat and he would like to know if its company is concerned by this new vulnerability and where.

3.SUPPLIER RISK

Company: **Banking sector**

Contact: **Information System Director**

Issue: The Information System Director wants to have an idea of its suppliers' maturity. It's not in an evolution way but more an support one, that allows him to continue working with these supplier and help them to meet the Group's requirements.

4.SHADOW IT

Company: **Mass-Market retailing sector**

Contact: **CISO**

Issue: The CISO is tired of the Shadow IT and looking for a way to identify it. **100% of our clients discover things that they didn't know.**

Everything starts with a

weakspot

www.weakspot.io

contact@weakspot.io - Follow us on Linkedin and Twitter