

External Attack Surface Management

Stijn Vande Castele

Agenda

1. Problem
2. Solution
3. Live demo

Why are you an attractive target?

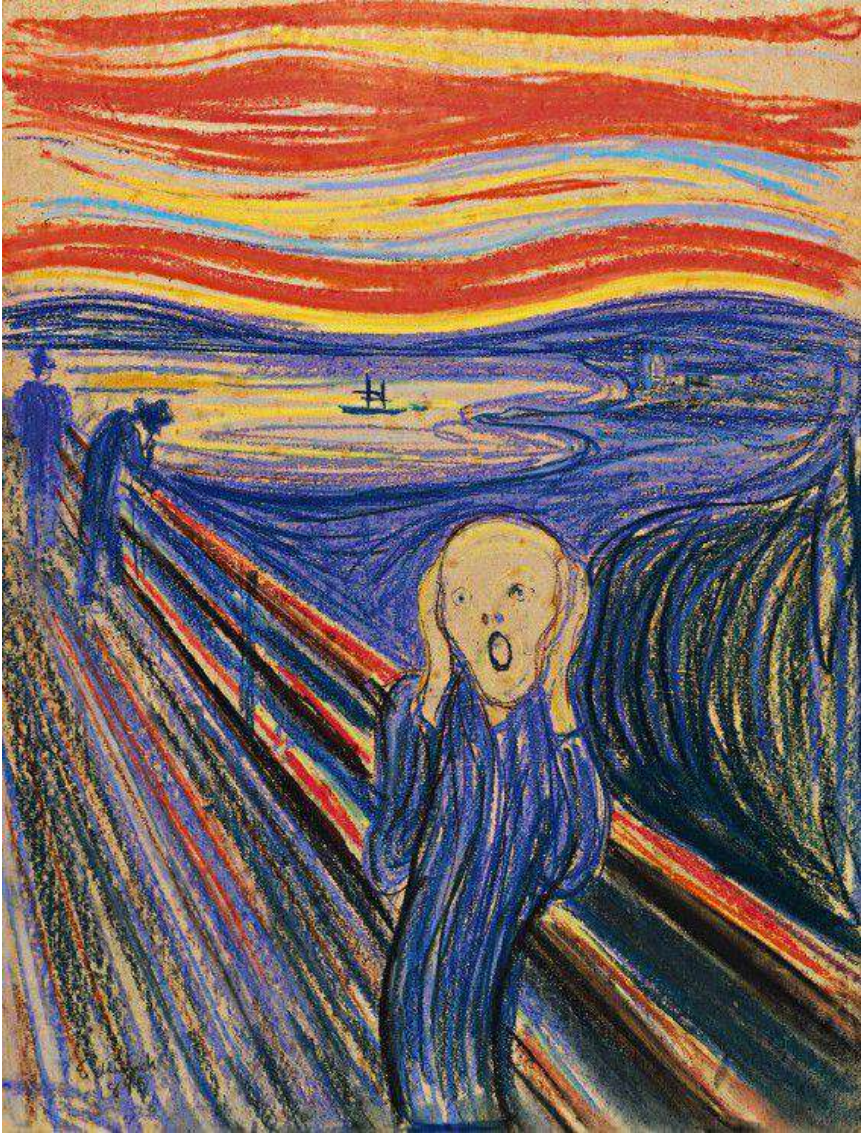
The growing attack surface

Digitalization is evolving fast & continuous



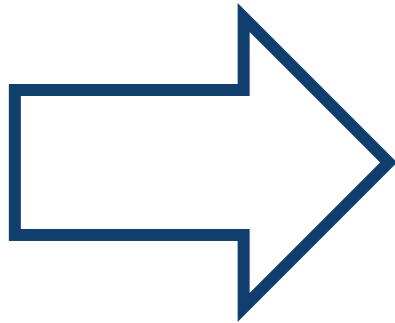
- Digitalization is key for organizations to survive.
- IT is increasingly easier & faster deployed: Fuelled by cloud service, SAAS offerings,
- Decentralized more and more via different IT & business departments, expert organizations, third parties, hosting providers,
- Cybersecurity has become a top-management concern, but is complex.
- Security Tools: Many specialized internet-facing scanners, free scripts, open source, ... But do they provide the full coverage, the needed insights and speed?
- Speed has the upper hand, but security is considered equally important.

Security Challenges Companies Face



- **Business risk mgt:** Business Managers struggle to understand and manage security risks without understanding the technical details.
- **Extended IT ecosystem risks:** CISOs and security staff find it hard to understand and follow up the extended IT ecosystem that is managed by different IT teams or external providers.
- **Remote workforce risks:** Employees, admins and specialized vendors are remote, and given remote access to key infra via insecure/unapproved applications (like RDP, Telnet, VNC, etc...)
- **Old IT assets** are forgotten but still online, and are increasingly more insecure backdoors.
- **Fake business websites:** Lure customers for fraud.
- **One-time security:** Security settings and audits are done once, but not improved when needed or re-assessed.
- **Weak encryption:** Allowing man-in-the-middle attacks.
- **Limited Resources:** Cybersecurity staff and one-time audits are expensive and limited.

The burglars of cyberspace



How to become more cyber resilient with Attack surface management

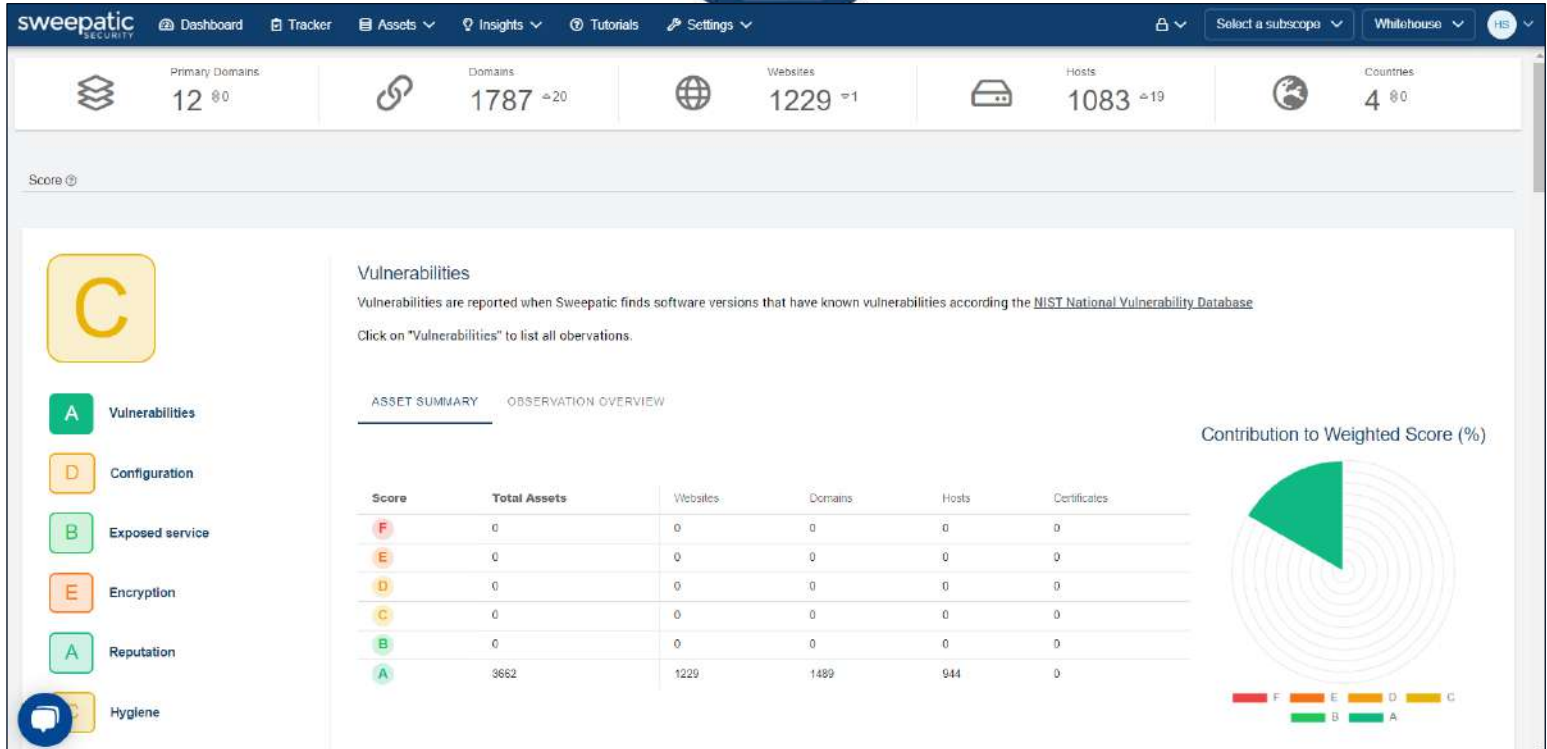
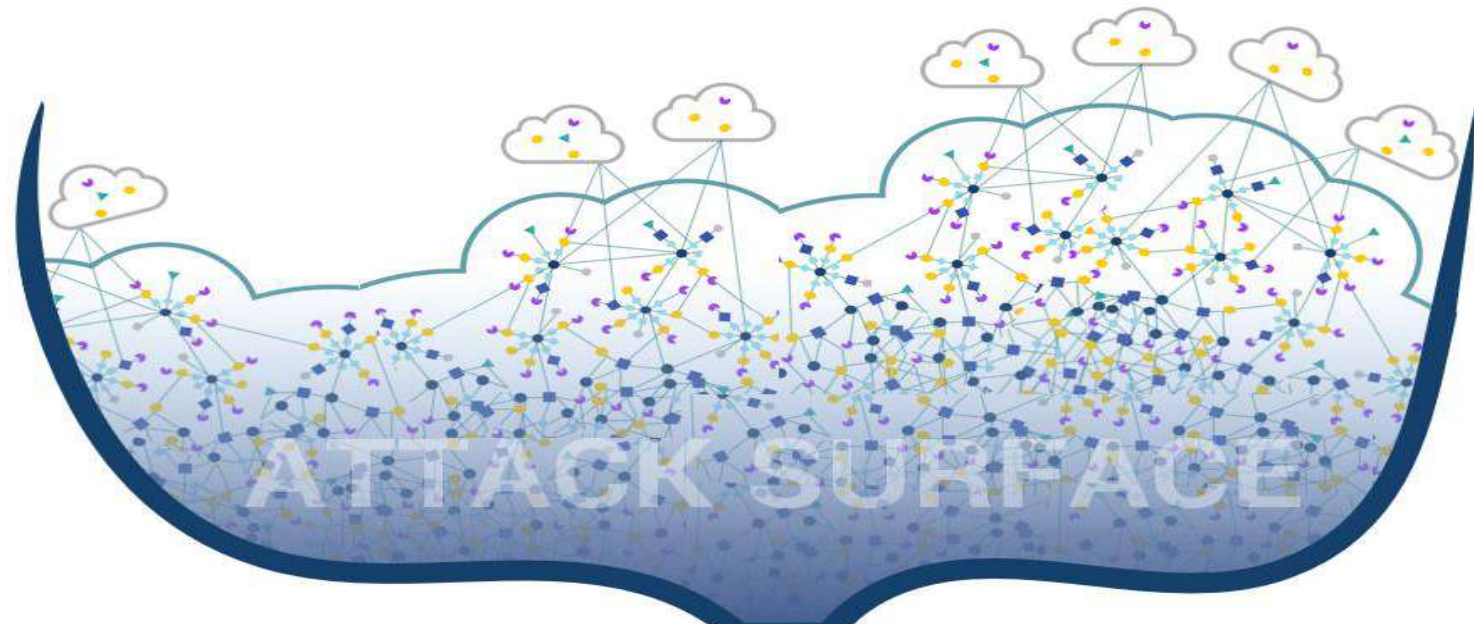
Discover, assess, prioritize, and remediate

Do you know your attack surface?

1. Do you run penetration tests? Vulnerability scans?
2. Do you know all your (sub)domains, websites, IP hosts? Do you have a central, up-to-date inventory?
3. Which technologies are used in your online infrastructure and are they up to date?

The Sweepatic Platform

We automate the continuous discovery, security analysis & follow-up of your internet-facing IT assets



The solution: mapping, monitoring and managing the attack surface

REPRESENTATION

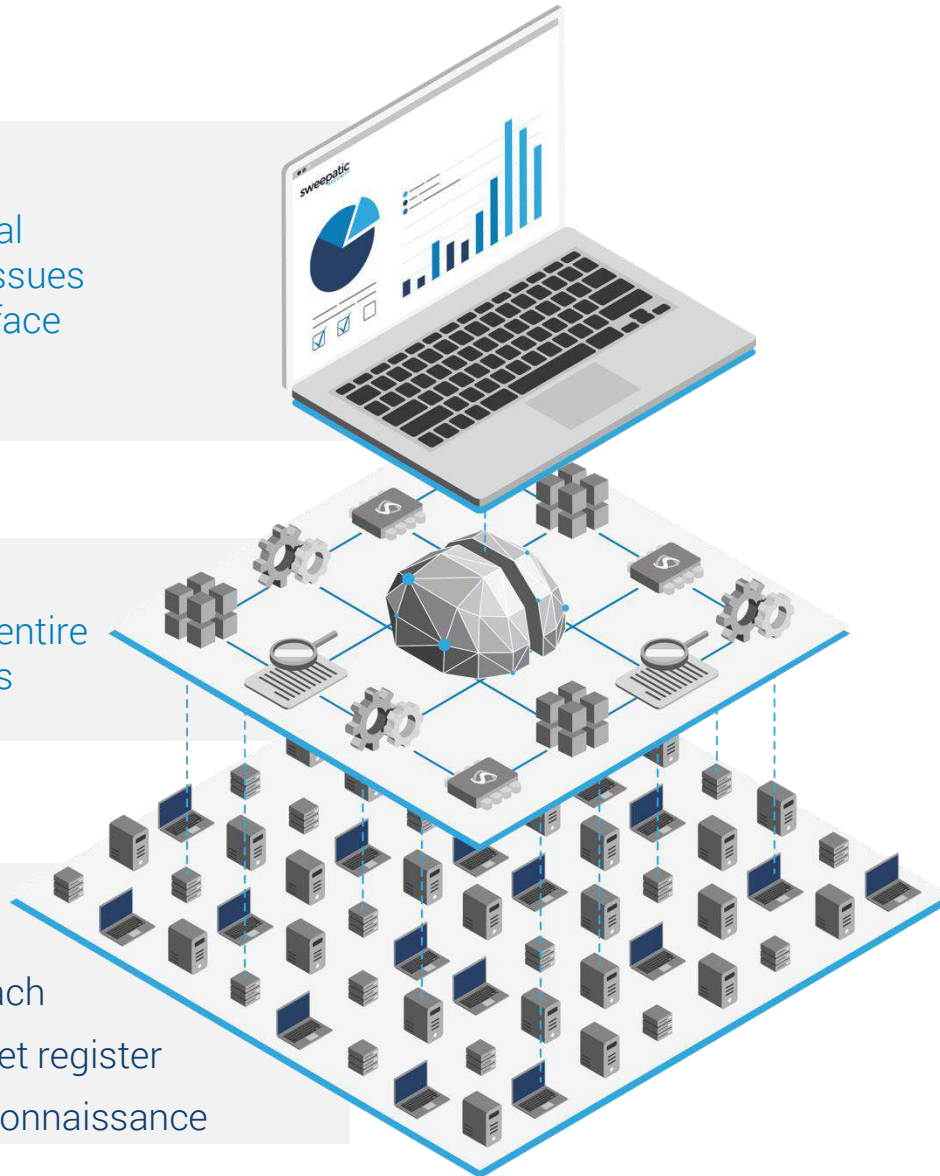
A clear and simple portal allowing to remediate issues in the global attack surface

INTELLIGENCE

Automated analysis of entire attack surfaces in hours

DISCOVERY

Zero-knowledge approach
Automated, central asset register
Based on advanced reconnaissance



Business use cases

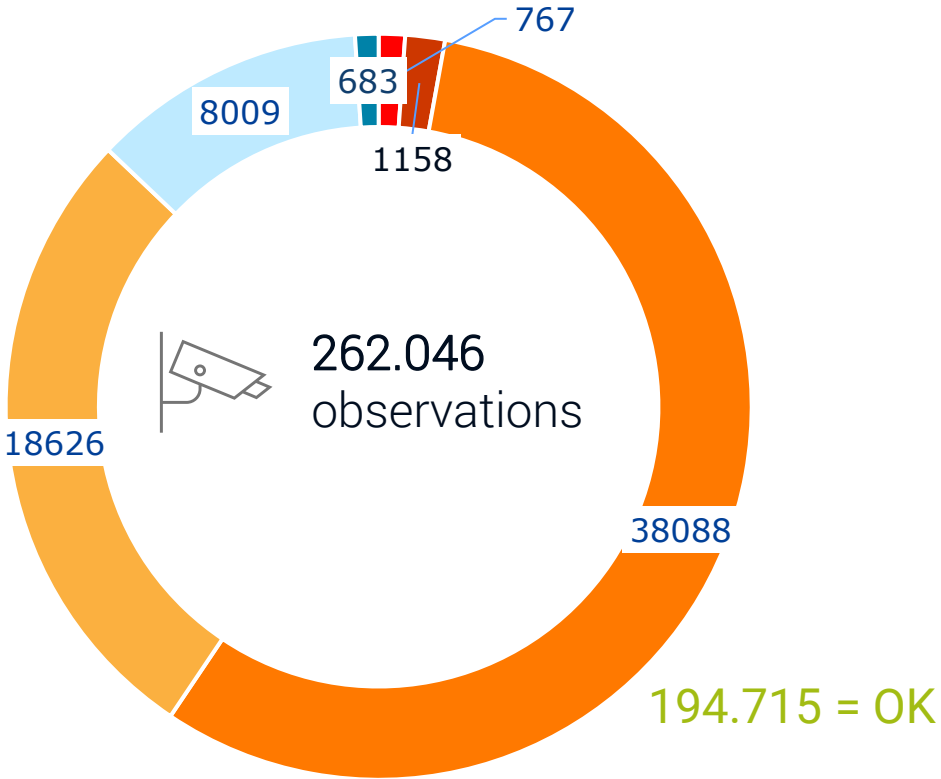
- **Detecting known and unknown assets**, Shadow IT and rogue projects
- **Finding weak spots and risks** that are not discovered by traditional vulnerability scanners
- **Assessing risks** from suppliers and IT vendors
- **Assessing M&A targets** and subsidiary risks
- **Saving time** and expensive cybersecurity resources by **automating the manual work** that needs to be done

Platform statistics

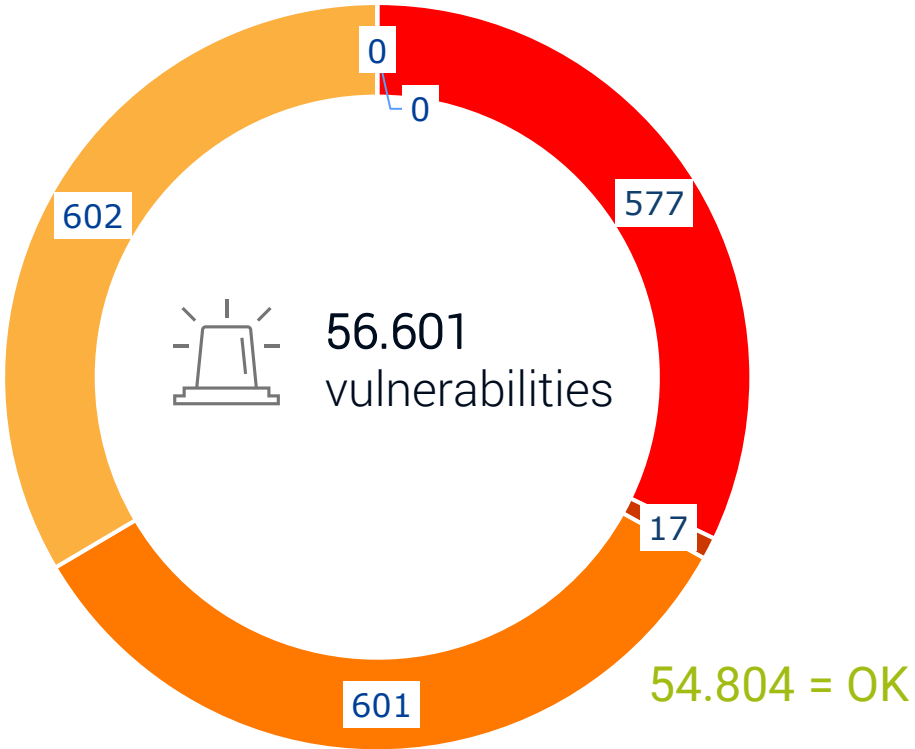
Snapshot 08/06/22

59.031	38.432	20.944	3.506
domains	websites	hosts	certificates

67 Critical-High Observations
per 100 assets

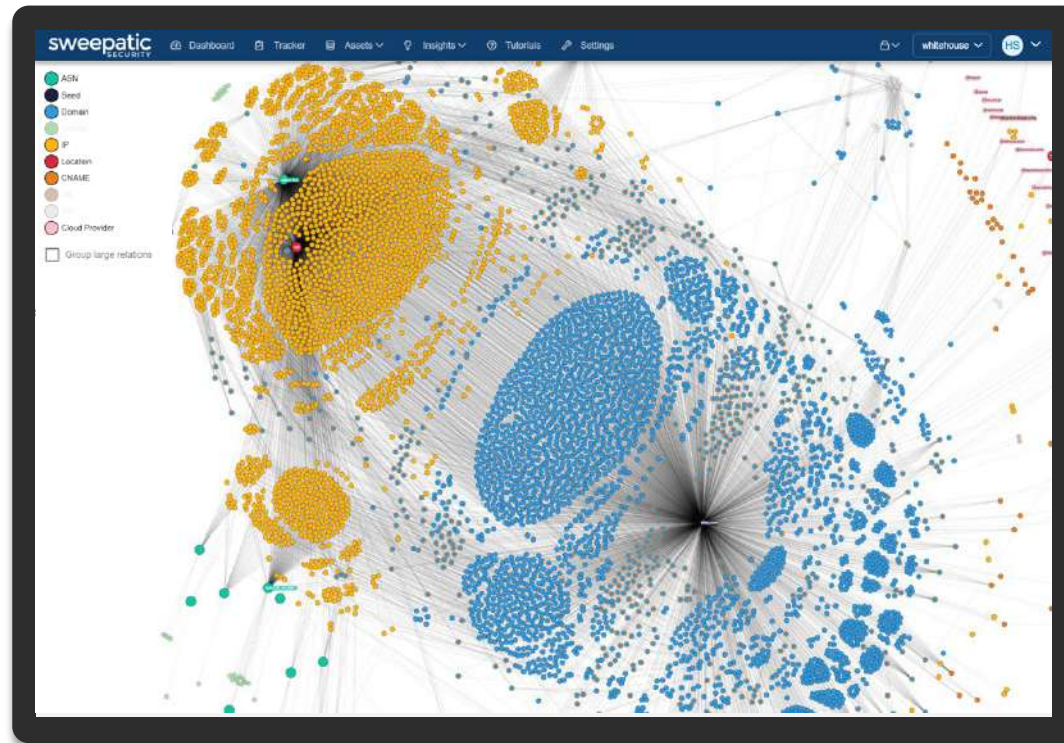


1 Critical Vulnerability
per 100 assets

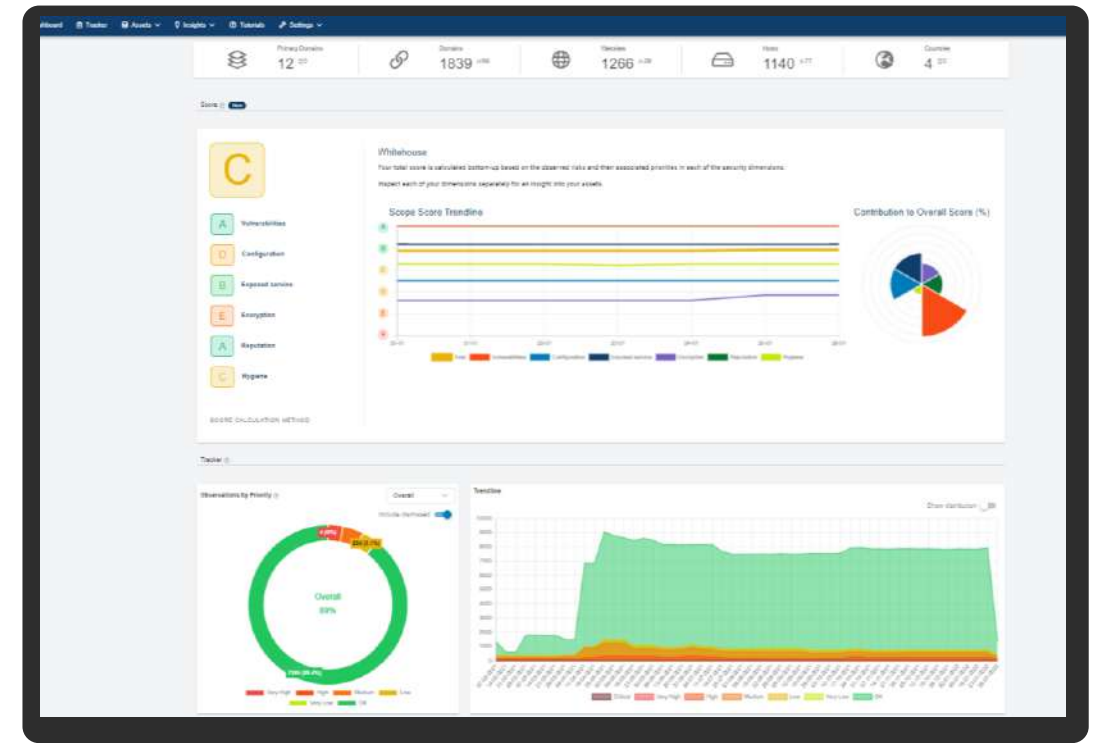


The Sweepatic Platform

Automatically generating **high-impact insights**
and **easy-to-remediate findings**



Network graph: A topological, bird's eye view of your global attack surface with all assets and their interrelation.



Dashboard: Overview of key information elements about your attack surface evolution allowing to drill down to all details.

Final thoughts

- All companies across all sectors lack visibility on the security state of their known and unknown internet-facing assets
- Possible attack paths are detectable by bad actors without using disruptive scanning tools

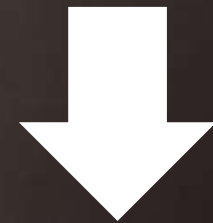
3 step approach

- Continuously track all your internet-facing assets and check them regularly
- Take an “IT-Hygiene first” strategy
- Remove what no longer has a business justification



- How can my organization **become a less attractive target** for cyber attacks?
- Which assets are **exposed** in my attack surface?
- What are **priority actions** to take?
- What **remediations** are required to get my attack surface in order?

Request your demo



Hannah Smeyers
Marketing & Sales Assistant
h.smeyers@sweepatic.com