Prevent further cyber threats with Sweepatic's automated attack surface management platform

Our reliance on technology is increasing every day, and the need to secure our data and online information has also become inevitable. The internet growth has led to an increase in computer networks, so organizations must consider the principles of confidentiality, integrity and availability as their number one priority. When working on the internet, network security is one of the crucial aspects to pay attention to. Every network connected to the internet is prone to attacks regardless of its size or its organization. An efficient network security system will protect the clients' data and prevent businesses from becoming victims of cyberattacks.

The automated Sweepatic Platform discovers and analyzes the attack surface of companies to determine their exposure to attacks. It is using advanced reconnaissance techniques to automatically *"sweep"* for internet-facing assets such as domains, subdomains, web applications, published files, third party frameworks, and much more in a continuous, non-intrusive mode. By means of its Artificial Intelligence layer, the Sweepatic Platform is transforming enriched data in actionable findings that are accessible through a clear and easy-to-use portal. Sweepatic was founded late 2016, operates on a global scale and has its HQ in Leuven, Belgium. Sweepatic's customers stay ahead of threat actors by continuously monitoring their internet-facing assets and seeing how they evolve over time. Many large enterprises — especially those who have grown through acquisition — lack this outside-in visibility. Their attack surface is very large, and they usually rely on complicated and slow processes to keep track of their assets. Sweepatic solves this problem with automatic asset discovery, monitoring and testing, saving these organizations time and money while giving them peace of mind.

In conversation with Stijn Vande Casteele, Co-founder and CEO of Sweepatic

What motivated you to reinvent enterprise network security services?

I met my technical co-founder Martin at a cyber-security workshop in Tallinn, Estonia. I quickly realized that we had the same experience after years of working for all types of different organizations. We found that in many, if not all cases, organizations have no idea of how exposed they really are in cyberspace. To fill this gap, I founded Sweepatic along with Martin and built an attack surface management platform. Enterprises still rely heavily on traditional and reactive cybersecurity programs and solutions, like one-off penetration tests and vulnerability scans. With Sweepatic, we want to create awareness about proactive cybersecurity: attack surface hygiene. If your attack surface is lean and clean, it will be harder to break into or breach. After all, what is not there cannot be hacked.

Where do you think the modern enterprise security system is lacking behind, and how is your company filling the void?

The main issues of enterprises are understanding and keeping track of the organization's online attack surface and how that is perceived and can be misused by others. Understanding attack surfaces and being aware of how they evolve is critical in proactively organizing the right defenses around an organization. With increased teleworking and the boost of online services as a result of the COVID-19 pandemic, digitization has become an even bigger priority for organizations. It makes it even harder to keep track, and it increases cyber exposure significantly. Additionally, the modern enterprise security system is too often reactive in its approach: if or when a security incident occurs, the enterprise reacts when the damage is already done. Sweepatic is proactive: prevent a security incident from happening by cleaning up your attack surface. It's about making organizations cyber resilient in the first place. Sweepatic fills the void in two ways: attack surface visibility and proactive attack surface reduction to stay a step ahead of the threat actors.

Modern cyber-attacks are equally automated. How do you help organizations to fight fire with fire?

The first step in the cyber kill chain is the reconnaissance phase. Cybercriminals try to find as much

information as they can about the victim organization before they execute an attack. They search the internet for weaknesses and entry points. Our automated Sweepatic Platform mimics these reconnaissance techniques so that the organization knows about these weak points before others do and can fix them before they are taken advantage of. This allows organizations staying a step ahead of threat actors and modern automated cyberattacks to become cyber resilient. Internal inefficiencies in an organization undermine security analytics and operations.

Do you help your clients patch their internal operations?

The Sweepatic Platform is designed to provide a clear and simple dashboard, an intuitive user experience, actionable insights, and quick fixes. This unburdens the internal security team since there is an easy onboarding, a globally accessible portal, and no learning curve. The Sweepatic Platform automatically discovers all internet-facing assets, so the security operations don't have to this manually by combining many tools and excel files. Using the Sweepatic Platform, security analytics and operations can work together and streamline their patching process. Thanks to our notifications, the security teams will receive alerts about changes in their attack surface that need evaluating or fixing. Issues can then easily be tracked and assigned to the right person. We are currently also working on our API and with a technical partner to facilitate technical integrations towards organizational processes and existing capabilities (e.g., Jira, SIEM, VM, etc.) for our customers.

Do you have any new services ready to be launched?

The Sweepatic Platform takes a continuous improvement approach, launching new features in bi-weekly sprints. On our short-term roadmap are the extension of CVE detection, auto-tagging & annotation feature and security testing of cloud resources. We have big plans for the coming months, so make sure you keep an eye on our website! Sweepatic already set up successful partnerships with MSSPs and resellers, and we aim to scale this to the US. Apart from establishing partnerships in the US, we are looking to grow our base of US *"champion"* customers as well. Since the Attack Surface Management market is even bigger over there, we are sure we can be of service on the American continent. Interested? Please request a free trial, a demo, or a call with us!

> ***"Organizations can track their (new) internet-facing assets continuously, get actionable insights and quick fixes and make the attack surface as lean and agile as possible to demotivate threat actors."***

Stijn Vande Casteele, Co-founder & CEO

Meet the leader behind the success of Sweepatic

Stijn Vande Casteele, an MSc in Information Security, is an entrepreneur and seasoned cyber security professional with 19 years of experience. He is the Co-Founder and CEO of Sweepatic. Stijn gained industry recognition based on his business insights and by coaching and steering several teams in successfully creating, delivering and operating enterprise enabled cyber security solutions for large organizations like NATO, BNP Paribas, Proximus and Deloitte. He is now fully focused on successfully scaling Sweepatic into a renowned cyber security business.