SECURITY ANALYST / THREAT HUNTER

Full time employee.
Place: Leuven, Belgium

Your day-to-day responsibilities

You will be a key member within the Sweepatic technical team that will be tasked with the service delivery around our Sweepatic reconnaissance and counterintelligence platforms for our growing customer base.

Main focus is the triage, assigning trust levels and writing event annotations on the results produced by the Sweepatic capability.

Quick, ad-hoc development of Proof of Concepts (leveraging existing tools, scripts, 3rd party datasets) as necessary to aid/streamline your hunting activities.

Based on your daily hunting activities further improve and fine tune our pre-processing engines in the solution to further automate the hunting.

Manage the different outputs / deliverables for our customers: producing fact-based reports detailing the observations in a clear, professional way.

On board and training other platform users how to leverage the full Sweepatic capability.

Provide basic technical support on the Sweepatic reconnaissance and counterintelligence solutions.

Help us define the landscape, prevalence, and evolution of our reconnaissance and counterintelligence solutions by participating in future requirements definition discussions with the Sweepatic product owner.

Conduct research on current ongoing reconnaissance and/or OSINT trends as needed with a goal of reporting noticed threats applicable to our customers and developing feature requests on how to address them from a technical roadmap perspective.

What you bring to the team

Experience in organizing, conducting and improving security analysis, threat hunting related work.

Strong written and verbal communication skills (in English), including the ability to convey highly technical information in an accessible manner.

Familiarity/experience with Linux, Python, RegEX, Bash scripting.

Good understanding and a passion for both cyber security and intelligence analysis.

Interest in Cyber security research, Open Source Intelligence gathering, reconnaissance and counterintelligence techniques.

Willingness to interact with customers (web, phone-based support and occasionally physical meetings) to explain observations, risks and recommendations.

Ability to work independently.

Can-do attitude with a focus on problem solving, quality, and a strong desire to get the job done.

Requirements/Education

A university degree (i.e. Computer Science, Cyber Security, Political Science, International relations) or equivalent through experience.

Cyber security certifications such as CEH are an advantage.

Apply

E-mail your CV and motivation to Stijn Vande Casteele at stijn@sweepatic.com

About us

Sweepatic, based in Leuven, is an innovative data driven cybersecurity venture and operates on a global scale. Sweepatic's unique reconnaissance platform discovers, monitors and analyses companies' attack surfaces 24/7 across the world.

Founded in 2016, Sweepatic is a venture incubated in the Start it @KBC and CyLon programs. We secured funding from eCAPITAL, a German venture capital firm.