



Collaborative Detection Engineering with Rulezet

Building a Trusted Community for Detection Rules (NGSOTI project)

GEFFE Théo 22 october 2025







Summary

- Introduction of Rulezet's project
- How to contribute
- Roadmap
- Tool's demonstration







Introduction

- RULEZET: An Open Collaborative and Open-Source Cybersecurity Detection Rules Repository
 - Online instance: https://rulezet.org
 - GitHub project : https://github.com/ngsoti/rulezet-core.git





Origin of rulezet

- SOC analysts and security engineers face the challenge of **developing effective detection rules**.
 - There are **countless security rules scattered across the internet** (GitHub, blogs, repositories), making it difficult to filter the reliable and actionable ones.
 - Detection rules come in many formats, YARA, Sigma, Suricata, and many others, making unification and reuse more difficult.
 - Rules may contain syntax errors, and even valid ones offer no guarantee of real effectiveness.



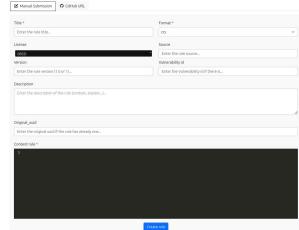




What can you do with Rulezet

- Create, manage, and import rules.
- Comment, vote, and propose changes to rules.
- Bundle (create, manage) rules together.
- User management.
- API.

Create a Rule









Goal of the platform

- Simplify rule management and the collaborative evaluation of rules.
- Collaborative management and contribution of different detection rules.
- Reduce the chaos of open-source detection rules and make them easier to use effectively.
- Validating the syntax and effectiveness of every detection rule.







How to contribute

- Start by registering on rulezet.org,
- Vote on rules, leave comments, and propose improvements.
- Integrate new sources of open-source detection rules to expand coverage.
- Claim ownership of the detection rules.
- Help improve Rulezet by proposing new formats and suggesting enhancements.







Roadmap

- Ability to import and export rules/bundles from/to MISP.
- Integrate vulnerability references (such as CVE identifier) to map detection rules in Vulnerability Lookup and improve traceability (https://vulnerability.circl.lu)
- ...



Tool Demonstration

Time to start...







