



Collaborative Detection Engineering with Rulezet

Building a Trusted Community for Detection Rules (NGSOTI project)

GEFFE Théo

22 october 2025

TLP:CLEAR



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>

TLP:CLEAR



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**.

TLP:CLEAR



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.

TLP:CLEAR

Create a Rule

☐ Manual Submission ☐ GitHub URL

Title *	Format *
<input type="text" value="Enter the rule title..."/>	<input type="text" value="crl"/>
License	Source
<input type="text" value="CC0"/>	<input type="text" value="Enter the rule source..."/>
Version	Vulnerability id
<input type="text" value="Enter the rule version (1.0 or 1)..."/>	<input type="text" value="Enter the Vulnerability id if there is..."/>
Description	
<input type="text" value="Enter the description of the rule (context, explain...)/"/>	
Original_uid	
<input type="text" value="Enter the original uid if the rule has already one..."/>	
Content rule *	
<div>1</div> <div></div>	

Create 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.

TLP:CLEAR



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.

TLP:CLEAR



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>)
- ...


TLP:CLEAR



Tool Demonstration

Time to start..

TLP:CLEAR

RULEZET

[Home](#) [Bundle](#) [Security Rules](#) [Ownership Requests](#) [Control Access](#) [admin](#)

Recent Rules

[Add Rule](#)

Potential F5 Config or Backup File Downl...

Description: Detects large HTTP responses containing F5 config, backup, or UCS file names.

Author: Alexandre

Created: 2025-10-16 09:49

Modified: 2025-10-16 10:03

[View more](#) [👍 0](#) [👎 0](#)

Suspicious TMSH or CLI Activity Outside A...

Description: Detects tmsh or tnm process executions outside scheduled admin periods. (adapted with a time range with your business hours)

Author: Alexandre

Created: 2025-10-16 09:58

Modified: 2025-10-16 09:58

[View more](#) [👍 0](#) [👎 0](#)

Encoded or Base64 Payload in HTTP POST

Description: Detects long base64 strings in HTTP POST body to management or shared endpoints.

Author: Alexandre

Created: 2025-10-16 09:50

Modified: 2025-10-16 09:50

[View more](#) [👍 0](#) [👎 0](#)

Suspicious F5 iControl REST Access from

Description: Detects HTTP access to /mgmt or /mgmt/tm endpoints from unauthorized IPs.

Author: Alexandre

Created: 2025-10-16 09:47

Modified: 2025-10-16 09:47

[View more](#) [👍 0](#) [👎 0](#)