Stamus Networks Announces Suricata Language Server 2.0 with AI Agent Skills and Continuous Integration Support

A major architectural upgrade introduces workspace-wide intelligence, AI-assisted signature development, and automated validation for large-scale Suricata deployments.

PARIS and INDIANAPOLIS – March 19, 2026 – Stamus Networks, the global leader in Suricata-based network security and the creator of the innovative Clear NDR® system, today announced the release of Suricata Language Server (SLS) 2.0. This new release of the **no-cost open source** tool delivers a substantial update that introduces workspace-wide intelligence, automated SID conflict detection, AI-assisted signature development, and architectural modernization.

Built to support modern detection engineering workflows, SLS 2.0 introduces powerful new capabilities designed to streamline rule development, reduce errors, and accelerate validation across complex rule deployments.

AI-Assisted Rules Writing

While many mainstream LLMs are capable of generating Suricata signatures, the results are often approximate, frequently relying on deprecated features and lacking reliable validation.

Stamus Networks has introduced AI agent skills that integrate with Suricata Language Server to assist engineers in writing and explaining Suricata signatures. Generated signatures are automatically validated using SLS, helping ensure syntax accuracy, performance considerations, and adherence to best practices.

GitHub Action

Modern engineering workflows require robust validation pipelines, yet until now, no comprehensive solution existed for Suricata rules production.

SLS 2.0 addresses this gap with a GitHub Action that verifies signatures within repositories, enabling automated quality checks in CI/CD pipelines and allowing builds to fail on syntax errors or warnings.

Workspace-Wide SID Awareness

SLS 2.0 now tracks Signature IDs (SIDs) across the full workspace and automatically detects conflicts between rule files. Engineers receive immediate warnings when duplicate SIDs are introduced, reducing deployment errors and improving ruleset integrity.

The update also delivers multi-threaded workspace analysis, significantly accelerating validation for large rule collections.

Real-Time Diagnostics and Deprecation Handling

With on-the-fly validation, SLS 2.0 analyzes rules directly from the editor buffer, providing instant feedback without requiring file saves.

SLS 2.0 also highlights deprecated Suricata keywords directly within the editor, helping teams modernize rule syntax and migrate away from outdated constructs.

Architectural Modernization

SLS 2.0 includes a complete migration to pygls 2.0+, removing custom Language Server Protocol handling and simplifying the codebase. The refactored architecture improves reliability, performance, and maintainability while positioning the project for future enhancements.

“Detection engineering has become more complex as rule environments grow in scale and collaboration increases,” said Eric Leblond, co-founder and CTO of Stamus Networks. “With SLS 2.0, we focused on bringing CI workflows and AI-assisted capabilities to Suricata rule development, helping detection engineers validate signatures before production and leverage AI assistance when writing rules as Suricata syntax continues to evolve.”

This 2.0 release reflects both technical advancement and a commitment to supporting the evolving needs of detection engineers managing increasingly complex Suricata deployments.

Installation

Suricata Language Server 2.0 is available now. Find full documentation, release details, and installation instructions on the Stamus Networks website:
https://www.stamus-networks.com/suricata-language-server

Read more about SLS 2.0 here:
https://www.stamus-networks.com/blog/suricata-language-server-2.0

About Stamus Networks

Stamus Networks is the global leader in Suricata-based network security and the creator of the innovative Clear NDR® system. Designed to close visibility gaps and reduce alert fatigue, Clear NDR transforms raw network traffic into actionable security insights with unmatched transparency, customization, and effectiveness. Trusted by leading financial institutions, government agencies, and battle-tested over 9 years in NATO's largest cybersecurity exercises, Stamus Networks delivers proven, high-performance network detection and response solutions. Stamus empowers security teams – delivering clarity amidst complexity – with greater control, fewer false positives, faster response times, and a more responsive, open approach than legacy vendors.

# # #

Media Contact

Kim Schofield
Stamus Networks
kschofield@stamus-networks.com
+1 (603) 234-4000