Stamus Networks Announces Production-Ready Clear NDR Community 1.0

The open-source edition of the company's network detection and response (NDR) solution incorporates Suricata 8 and empowers AI security operations with integrated model context protocol (MCP)

INDIANAPOLIS and PARIS - September 9, 2025 - Stamus Networks, a global provider of high-performance network-based threat detection and response systems, today announced the general availability of Clear NDR® Community 1.0, marking the open-source solution's official production-ready status. This release transforms the popular Suricata-based open-source security monitoring platform with significant enhancements in deployment flexibility, threat intelligence integration, AI integration, and incident investigation capabilities.

Clear NDR Community 1.0 builds upon [last year's initial beta release](#) with a more robust architecture, expanded deployment options, and workflow improvements that make it suitable for production environments in small-to-medium sized organizations as well as researchers, educators, students, and hobbyists who wish to explore what is possible with Suricata and the network protocol monitoring logs and alerts it produces.

"With Clear NDR Community 1.0, we're delivering on our promise to provide the most complete open and transparent network security solution that organizations can trust for many smaller environments," said Peter Manev, co-founder and chief strategy officer at Stamus Networks. "As the only open source NDR on the market, and the only one with Suricata 8 and AI-native interfaces, it is uniquely positioned to help security teams experience the power of deep network visibility before considering an upgrade to our Enterprise edition."

Expanded Deployment Options

Clear NDR Community 1.0 introduces multiple deployment options to accommodate diverse infrastructure requirements:

- Debian ISO with Desktop environment - for those who prefer a graphical interface
- Debian ISO without Desktop environment - for headless server deployments
- Containerized version for any Linux environment - continuing support for Docker containerized deployments

These options enable deployment on bare metal hardware or virtual machines, providing greater flexibility than the Docker-only format available in the previous beta release.

Key Enhancements in Version 1.0

Clear NDR Community 1.0 includes several significant improvements:

- **Production-Grade Foundation**: Upgraded to OpenSearch 2.0 data lake for enhanced performance and reliability
- **Built on Suricata 8.0**: The latest version of Suricata delivers better threat detection accuracy, improved performance at scale, and expanded protocol coverage
- **Model Context Protocol (MCP)**: Standardized interfaces to enable integration of third-party generative and agentic AI
- **New Dashboards and Visualizations**: Over 400 visualizations and 58 new dashboards for enhanced Suricata 8 network data
- **Streamlined Threat Intelligence**: Native ability to ingest threat intelligence feeds without writing custom Suricata rules
- **Advanced Data Management**: New facilities to help users control data retention
- **Accelerated Investigation**: "Two-Click to Evidence" workflow that speeds incident response
- **External Integration**: UI integration with other systems via configurable Deep Linking
- **Notification System**: Keeps users informed of new releases and best practices

Supporting the Security Community

Clear NDR Community is widely used by network security practitioners, researchers, educators, students, and hobbyists to explore what's possible with Suricata IDS/IPS/NSM and the network protocol monitoring logs and alerts it produces. Version 1.0 continues this tradition while offering even more capabilities for experimentation and learning.

"We believe in the power of open security tools to advance the industry's collective defense capabilities," added Peter Manev. "Clear NDR Community 1.0 represents our commitment to supporting both professional security teams in smaller organizations and the broader community of security enthusiasts."

Enterprise Capabilities Available

For organizations requiring enterprise-scale deployments, Stamus Networks offers Clear NDR Enterprise, which builds upon the Community edition with additional capabilities for large-scale environments with high-fidelity security and compliance incident detection, machine learning and additional AI capabilities, advanced threat hunting, and automated response workflows.

Availability

Clear NDR Community 1.0 is available for download beginning immediately, from the Stamus Networks website. For more information, visit www.stamus-networks.com/clear-ndr-community.

Join one of the following webinars to learn more:

- "Open Source Network Detection and Response (NDR) for Real-World Security," (in English) on September 10, 2025 at 11:00 am ET. To register for this webinar, visit **https://us02web.zoom.us/webinar/register/WN_KvD422zGRvquvLkiG0t-IQ#/registration**
- "Détection et Réponse Réseau (NDR) Open-Source Pour une Cybersécurité Pragmatique," (in French) on September 10, 2025 at 13h00 CET. To register for this webinar, visit **https://us02web.zoom.us/webinar/register/WN_QrovkmlASZmPCQ1PrP9ttw#/registration**

About Stamus Networks

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR® – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain. For more information visit www.stamus-networks.com.

Media Contact:

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