Stamus Networks Announces Clear NDR Enterprise U42 with Advanced AI Integration and Enhanced Performance

Latest release delivers native AI connectivity, behavioral analytics, and high-performance architecture for modern security operations

INDIANAPOLIS and PARIS - October 23, 2025 – Stamus Networks, a global provider of high-performance network-based threat detection and response systems, today announced the general availability of Clear NDR® Enterprise U42. This major release introduces groundbreaking AI integration capabilities, advanced behavioral analytics, and significant performance enhancements that position Clear NDR as an essential foundation for AI-powered security operations.

Clear NDR Enterprise U42 addresses critical challenges facing modern security teams: integrating AI into security workflows, reducing alert fatigue in SIEM systems, and scaling detection capabilities to match growing network demands. The release introduces seven major capabilities that transform how organizations leverage network intelligence for threat detection and response.

"U42 represents a pivotal moment in network-based threat detection and response," said Eric Leblond, co-founder and CTO of Stamus Networks. "We're not just adding features – we're fundamentally changing how security teams work with AI and network intelligence. By providing native AI connectivity through Model Context Protocol and delivering high-fidelity threat context to SIEM platforms, Clear NDR becomes the intelligence layer that makes AI security investments truly effective. Combined with our performance improvements, organizations can now detect sophisticated threats faster while dramatically reducing the noise that has plagued security operations."

Key Capabilities in Clear NDR Enterprise U42

- **Model Context Protocol (MCP) Integration** - Enables native integration with AI applications (e.g., ChatGPT, Claude, Gemini, Mistral, and Copilot) via MCP endpoints for AI-powered threat hunting and investigation assistance.
- **Host Alert Outlier Detection** - Uses behavioral analytics to identify anomalous activity patterns for individual hosts, detecting needle-in-haystack threats missed by traditional volume-based detection.This feature proved extremely valuable during recent NATO live fire exercises, Crossed Swords and Locked Shields.
- **Low-noise DoC and DoPV events properly conveyed to SIEM** - Delivers Declaration of Compromise (DoC) and Declaration of Policy Violation (DoPV) incident logs to

SIEM/XDR systems with complete context, extending Clear NDR's alert fatigue reduction benefits across the entire security stack.

- **SMB Insights** - Consolidates SMB protocol metadata into composite events for accelerated session analysis and ML-based file sharing security while dramatically reducing data storage requirements and log volume.
- **Seamless IOC Ingestion** - Automatically imports threat intelligence indicators without manual rule creation, reducing deployment time from hours to minutes.
- **Multi-stage Response Workflows and Authentication** - Supports chained API calls with multiple authentication methods for complex automation workflows and response orchestration.
- **High-Performance Postprocessing** - Replaces legacy post-processing with high-performance engine for higher event throughput at lower CPU cost, enabling support for Clear NDR probes that monitor more than 200 Gbps network traffic.

Empowering AI Security Investments

As organizations invest heavily in AI-powered security operations, Clear NDR U42 ensures these systems have the comprehensive network intelligence needed to operate effectively. The Model Context Protocol integration enables security practitioners to empower generative AI and agentic AI systems directly with Clear NDR's network intelligence, creating unprecedented opportunities for automation and natural language-driven threat investigation.

Production-Ready Today

Clear NDR Enterprise U42 is available immediately to all Clear NDR Enterprise customers. Organizations interested in experiencing these capabilities can request a demonstration at www.stamus-networks.com.

About Stamus Networks

Stamus Networks is the global leader in Suricata-based network security and the creator of the innovative Clear NDR system. Providing superior network intelligence that empowers security AI platforms, Clear NDR closes visibility gaps and reduces alert fatigue, transforming raw network traffic into actionable security insights with unmatched transparency, customization, and effectiveness. Trusted by leading financial institutions, government agencies, and participants in NATO's largest cybersecurity exercises, Stamus Networks delivers proven, high-performance network detection and response solutions. For more information visit www.stamus-networks.com.

Media Contact:

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