Stamus Networks Expands AI-Driven Investigation and Threat Hunting Capabilities with Clear NDR Update

New release U42.2 expands MCP toolset to 14 AI-ready capabilities, introduces a redesigned Analyst Operations Console, and adds 55 new hunting and analytics assets to accelerate modern security operations

PARIS & INDIANAPOLIS – May 19, 2026 – Stamus Networks, the creator of Clear NDR® - the network intelligence foundation for AI-powered security operations - today announced the general availability of Clear NDR U42.2, a major platform release that significantly advances the company's AI-driven security operations capabilities. The release introduces four new Model Context Protocol (MCP) tools, bringing the total to 14, alongside a redesigned Analyst Operations Console, 23 new advanced protocol analytics dashboards, 32 new threat hunting filter sets, and significant performance and scalability improvements supporting deployments with more than 500 probes and 500 million simultaneously tracked hosts.

Security teams are under increasing pressure to investigate and respond to threats faster while reducing operational complexity. Clear NDR U42.2 addresses those challenges by extending AI-assisted investigation workflows, improving analyst efficiency, and expanding access to network telemetry and detection insights.

AI-Powered Investigation: From Network Signal to Confirmed Threat

A major enhancement in U42.2 is the expansion of Clear NDR's MCP toolset, which enables AI agents and automation workflows to interact directly with the platform's network investigation capabilities. With four new tools and enhanced threat verdict reporting, the expanded toolset now supports direct access to raw network telemetry, behavioral frequency analysis, detection coverage validation, and Clear NDR's highest-confidence threat verdicts. Declarations of Compromise® and Declarations of Policy Violations® now include direct hyperlinks into the Analyst Operations Console, enabling analysts to move from AI-generated findings to full investigation workflows with a single click. The result is a faster investigation workflow that connects detection, validation, and evidence within a single operational environment.

"We introduced the MCP integration in Clear NDR to extend investigative capabilities into the AI workflow," said Éric Leblond, co-founder and CTO of Stamus Networks. "With U42.2, AI agents can query raw network events, validate detection coverage, analyze behavioral patterns across metadata, and guide analysts directly to the underlying evidence without disrupting the

investigation process. That is the type of architecture modern SOC teams require as AI becomes more deeply integrated into security operations."

A Faster, More Modern Analyst Experience

U42.2 also introduces a major redesign of the Clear NDR Analyst Operations Console, delivering a faster and more responsive analyst experience with improved navigation, enhanced visualizations, richer contextual tooltips, and customizable interface options. The redesign focuses on reducing operational friction so analysts can investigate threats more efficiently. Every second an analyst spends navigating their tools is a second not spent on threats.

"Effective threat hunting and incident investigation depend on analysts having fast access to the right data and workflows," said Peter Manev, co-founder of Stamus Networks. "The new hunting filter sets in U42.2 reflect years of field experience with what analysts actually need in OT and IoT environments, where diverse protocols and device behaviors can make investigation slow and difficult. Combined with the new analytics dashboards and redesigned Analyst Operations Console, the release gives security teams stronger visibility and a more efficient foundation for uncovering threats that traditional detection workflows often miss."

Expanded Integrations and Enterprise-Scale Security Operations

U42.2 also adds new REST API endpoints that extend Analyst Operations Console capabilities to third-party integrations, SOAR platforms, and custom automation workflows, making Clear NDR network intelligence more accessible across the broader security operations ecosystem.

Additional performance and scalability improvements deliver faster configuration and threat detection updates while supporting deployments of 500 or more probes. When combined with the proven Host Insights™ tracking of 60+ security parameters simultaneously across 500 million hosts, Clear NDR is well-positioned for very large enterprise and MSSP environments.

Availability

Clear NDR U42.2 is available now for Clear NDR Enterprise deployments. Existing customers should contact their Stamus Networks customer success representative for upgrade information. For more details, visit www.stamus-networks.com.

For a deeper technical look at the enhancements included in U42.2 and how they improve network threat investigation and visibility, read the accompanying blog post: https://www.stamus-networks.com/blog/clear-ndr-enterprise-u42.2-is-now-available

About Stamus Networks

Stamus Networks is the network intelligence foundation for AI-powered security operations and the creator of the Clear NDR® system. Built on Suricata, the world's leading open-source network security engine, Clear NDR transforms raw network traffic into actionable security insights with unmatched transparency, customization, and effectiveness. Designed to close visibility gaps and reduce alert fatigue, Clear NDR is trusted by leading financial institutions, government agencies, and critical infrastructure – and has been battle-tested over ten years in NATO's largest cybersecurity exercises. Stamus Networks empowers security teams with greater control, fewer false positives, faster response times, and a more responsive, open approach than legacy vendors. For more information visit www.stamus-networks.com.

# # #

Media Contact:
Kim Schofield
kim@stamus-networks.com
+1 (603) 234-4000