STAMVS NETWORKS

SANS | Research Program

Product Briefing

RSA Conference Takeaways with Stamus Networks:

Insights from the SANS 2024 Top Attacks and Threats Report

July 2024

Security professionals have a lot on their plates. A deluge of alerts, coupled with the pressure to detect and respond to increasingly sophisticated threats, is pushing teams to their limits. IDS and NSM tools, advanced antivirus software, and modern firewalls provide greater detection and response abilities than their predecessors, but face their own challenges.

Simply put, these systems are not advanced enough to serve as effective means of threat detection in an enterprise environment.

Stamus Networks

Legacy intrusion detection and prevention systems (IDS/IPS) are struggling to keep pace with the rapidly evolving threat landscape, but many organizations are hesitant to update their aging systems, leaving them vulnerable to attack. The reasons are many, but usually come down to budget, operational challenges, resource constraints, and, once again, budget.

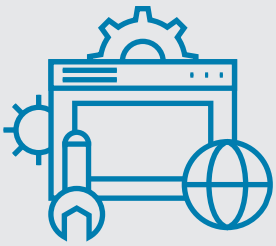
These legacy tools pose some common problems. Among them:

- Too many alerts and false positives, which overwhelm security teams trying to ascertain their validity, or they are suppressed or ignored.
- Alerts are missing contextual information needed to understand an event
- Lack of hybrid network deployment flexibility and east-west monitoring leaves users with numerous blind spots

Key Findings

Security operations center (SOC) teams are inundated with false and often irrelevant alerts, hindering their ability to focus on imminent threats.

Blind spots in network visibility prevent timely threat detection and allow bad actors to avoid detection and do more damage.



Understaffed SOC teams working with traditional intrusion detection systems (IDS) and network security monitoring (NSM) tools struggle to keep pace with a rapidly evolving threat landscape.

Stamus Security Platform (SSP) combines the functionality you have come to rely on from legacy IDS and NSM systems and incorporates AI and traditional detection mechanisms, host insights, guided threat hunting, and automated alert triage. The platform empowers organizations to detect threats faster, with greater confidence and with a low rate of noise. With this level of confidence—secure enough to be a part of NATO's live-fire cyber exercises—your organization can automate responses and jump-start investigations with the extra context and evidence that Stamus provides.

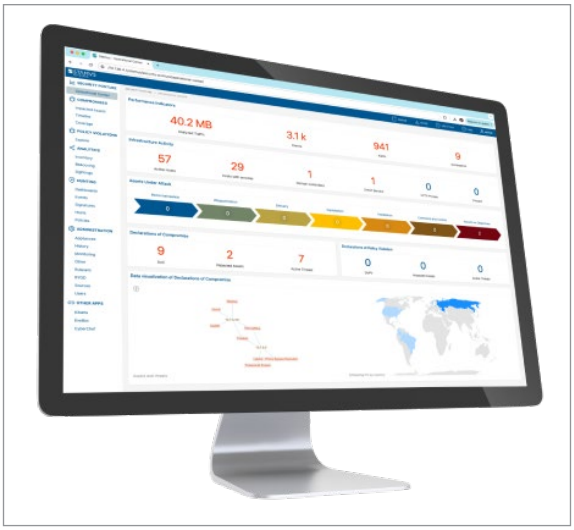


Figure 1. Network-Based Threat Detection and Response Solutions from Stamus Networks

As cyberattacks become more sophisticated, analysts need software that empowers their investigations with significant details and logic behind detection algorithms. With Stamus, your team can write your own detection algorithms or tune preinstalled ones for maximum control and visibility into why a specific alert was triggered.

SSP is built on the open source Suricata system. Stamus's experts are major contributors to Suricata, the co-founders are on the OISF board and executive teams, and the company is invested in ongoing development and support for the Suricata community. Additionally, Stamus adds proprietary incident response, machine learning, and third-party integrations to provide an upgrade path that has proven popular with large organizations and managed security service providers (MSSPs).

Unlike many security solutions currently on the market, SSP is not strictly cloud-based. It consists of two components: Stamus Network Probe™ and Stamus Central Server™, which can be deployed in private cloud, public cloud, on-premise, or hybrid environments. This level of control is especially important for organizations that have a strong need for data sovereignty.

Many organizations choose to put Stamus Network Probes close to the most vulnerable or attractive workflows, but they can go anywhere, including branch offices, in the cloud, and on industrial machinery. SSP starts gathering information immediately, so there's no long deployment delay. Once in place, it performs deep packet inspection to identify threats and unauthorized activity, and funnels probe findings into the central server for additional threat detection, event triage, and further communication with APIs and response automation. It also sends consolidated telemetry to a SIEM or combined data link.

Unlike the generic alerts produced by legacy systems and false-positive prone anomaly events produced by other NDR systems, SSP delivers high-fidelity Declarations of Compromise™ (DoC), which can be used to trigger an automated response. Although weak attack signals are often undetected by other systems or trigger false positives, DoCs are high-priority alerts that signal an imminent threat and are enriched with detailed metadata and evidence to expedite investigations and bolster response efforts.

DoCs can be custom-programmed and used for training in your environment to help sharpen analysts' skills. Your team also can fine-tune them and can even enable Declarations of Policy Violations (DoPV) to help with your audit documentation. That leads to a sustainable response—one that dramatically improves SOC efficiency and effectiveness, reduces operational costs, and mitigates the risk of data breaches.

If you're ready to step up to more powerful network threat detection and response, visit **www.stamus-networks.com**