Stamus Networks – the global leader in enterprise class Suricata-based network security

Stamus Networks helps enterprise security teams accelerate their response to threats with solutions that uncover serious and imminent risk from cloud and on-premise network activity. Our advanced network detection and response (NDR) systems expose threats to critical assets and empower your rapid response.

Trusted by the most-targeted organisations in the world

Government CERTs

Global Central Banks

Insurance Providers

Managed Service Providers

Multinational Gov't Institutions

Financial Institutions

SaaS and DevOps Software

Cybersecurity Vendors

Proven in NATO Cybersecurity Exercises

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

For the past five years, Stamus Networks and SSP have been invited by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) to join their annual Locked Shields and Crossed Swords exercises where we refine and validate our latest threat detection capabilities.

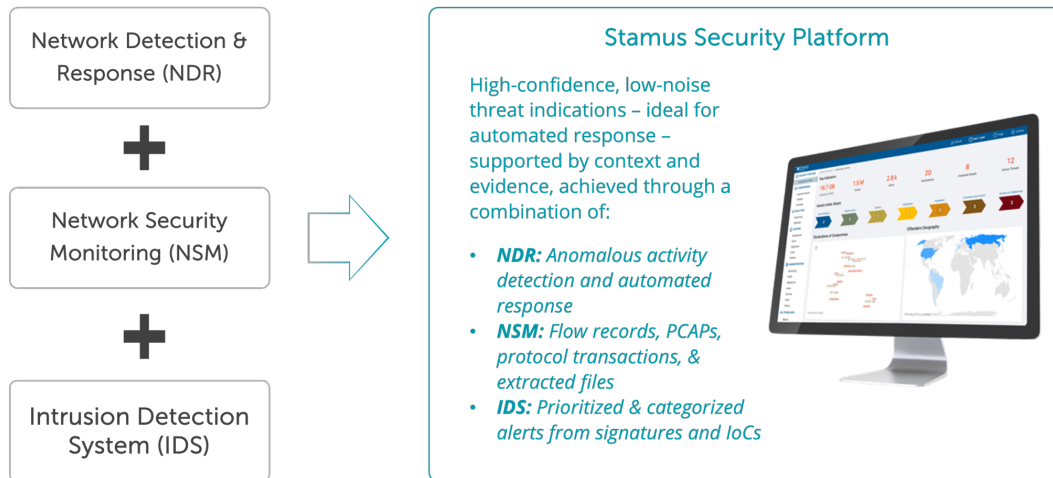# Expose serious threats and unauthorised activity lurking in your network.

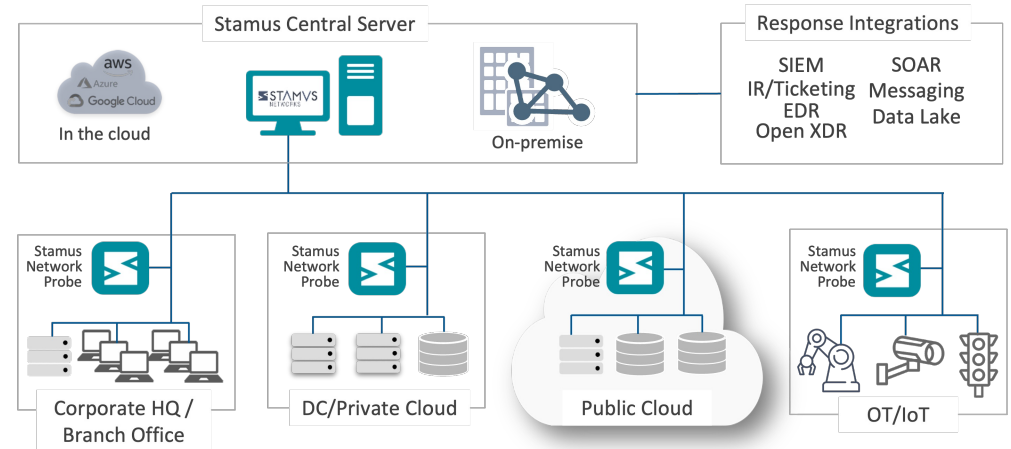With network-based threat detection & response solutions from Stamus Networks

STAMVS
NETWORKS

www.Stamus-Networks.com

Stamus Security Platform™ (SSP) is an open network detection and response solution (NDR) built on a Suricata foundation that delivers actionable network visibility and powerful threat detection.

Network Detection & Response (NDR)

+

Network Security Monitoring (NSM)

+

Intrusion Detection System (IDS)

Stamus Security Platform

High-confidence, low-noise threat indications – ideal for automated response – supported by context and evidence, achieved through a combination of:

- **NDR:** *Anomalous activity detection and automated response*
- **NSM:** *Flow records, PCAPs, protocol transactions, & extracted files*
- **IDS:** *Prioritized & categorized alerts from signatures and IoCs*

By combining the best capabilities of intrusion detection systems (IDS), network security monitoring (NSM), and network detection and response (NDR), the Stamus Security Platform is a new generation of NDR that helps organizations know more, respond sooner, and mitigate risk.

Stamus Central Server

In the cloud — On-premise

Response Integrations
SIEM   SOAR
IR/Ticketing   Messaging
EDR
Open XDR   Data Lake

Stamus Network Probe — Corporate HQ / Branch Office

Stamus Network Probe — DC/Private Cloud

Stamus Network Probe — Public Cloud

Stamus Network Probe — OT/IoT

Why Stamus Security Platform

Stamus Security Platform consists of two components: Stamus Network Probe(s) and Stamus Central Server, which may be deployed in private cloud, public cloud, on-premise, or hybrid environments.

Greater visibility into threat & network activity - Uncover even the weakest attack signals and unauthorised activity

Transparent detections with evidence - Know exactly what triggered an event with a detailed attack timeline & evidence

Open and extensible for your environment - Incorporate third-party threat intel. Easily integrate into your tech stack

Built for enterprise-scale operations - Scale to multi-site, multi-100Gbps deployments while tracking millions of hosts

Optional air-gapped deployment - Deploy analytics in the cloud or on premise – even in an air-gapped environment

Our probes or your Suricata sensors - Start with your Suricata sensors, transition to more advanced Stamus probes