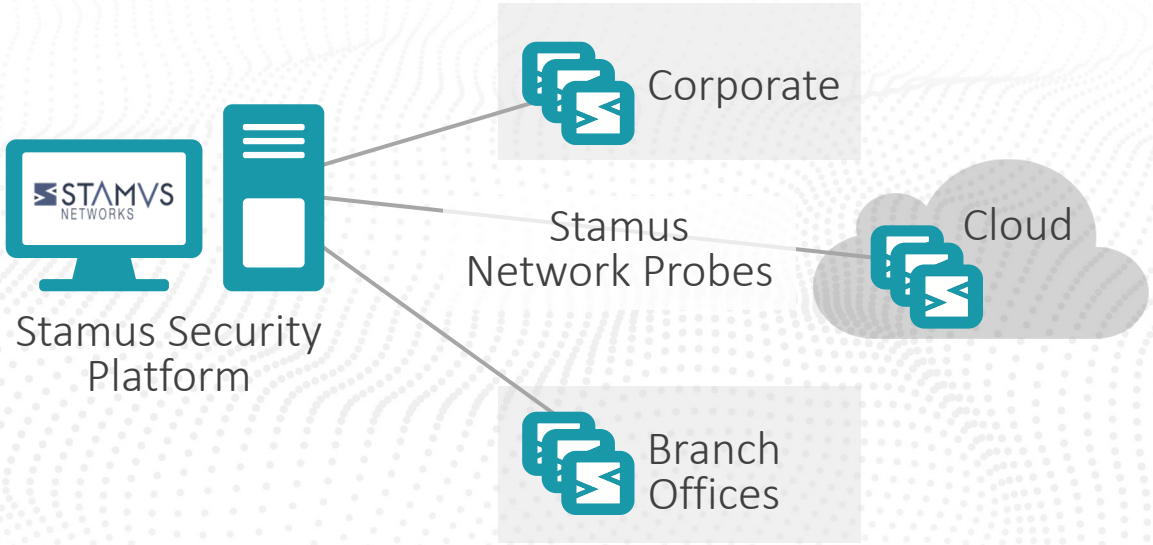
Datasheet

Stamus Network Detection and Response (NDR)

Stamus NDR is a broad-spectrum and open network detection and response (NDR) system that delivers:

- Declarations of Compromise™ - response-ready high fidelity threat detection events derived from advance threat intelligence, machine learning, stateful logic, and signatures
- Suspicious Sightings™ - machine learning insights into unusual behavior determined to be suspicious
- Open interfaces for SOAR, SIEM, XDR, IR
- Access to third-party and custom threat intelligence
- Explainable and transparent results with evidence
- Integrated guided threat hunting

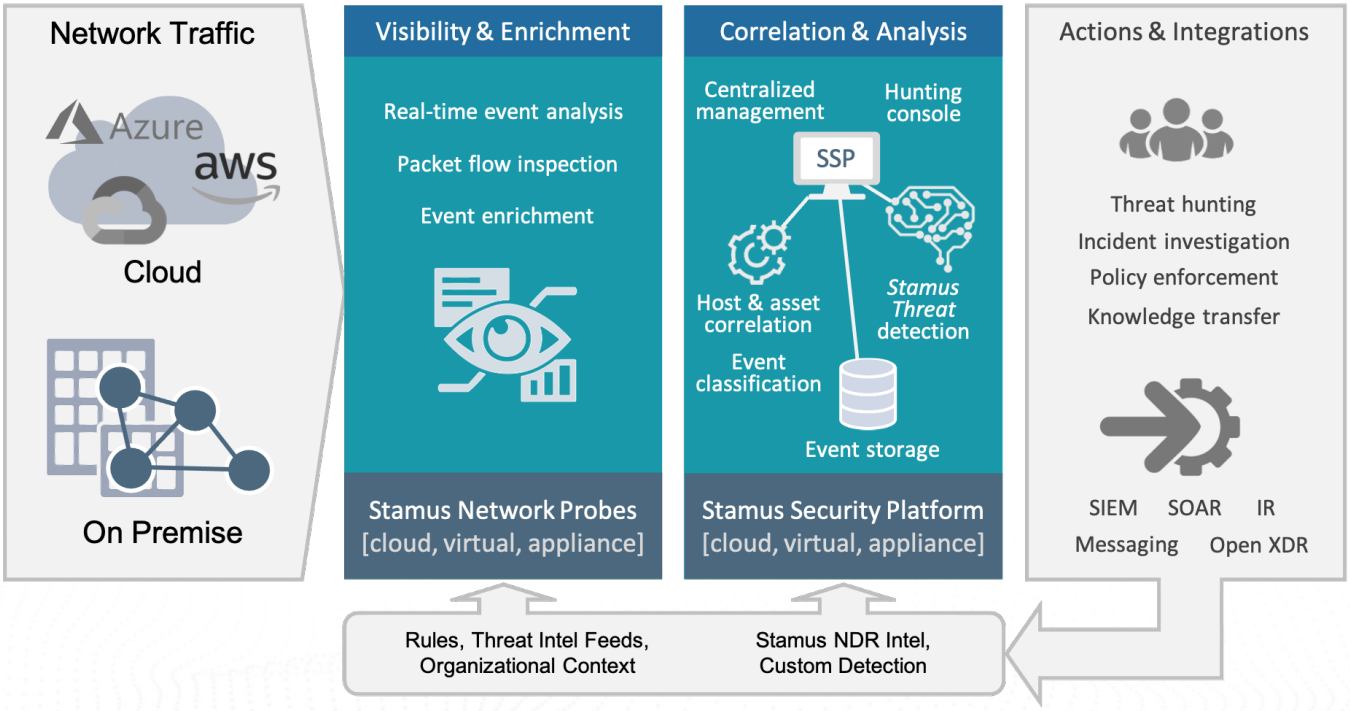
Stamus NDR consists of two components: Stamus Network Probe(s) and Stamus Security Platform. Each play a critical role in scaling the system. Stamus Security Platform and Stamus Network Probes can be deployed in private cloud, public cloud, on-premise, or hybrid environments.



STAMUS NETWORK PROBES

The probes may be deployed in the cloud, on premise or a combination of the two. Typically, multiple probes are connected to a network tap, packet broker, or span/mirror port in locations giving the system visibility into both north-south and east-west network traffic.

The function of the Stamus Network Probe is to inspect and analyze all traffic flows to perform real-time threat detection, enrich the resulting events with extensive metadata, and capture network protocol transactions. The probe delivers all this data to the Stamus Security Platform for additional analytics, processing and another layer of threat detection.



The probe is based on the Suricata engine which provides both network security monitoring (NSM) protocol transaction logs and intrusion detection (IDS) alerts.

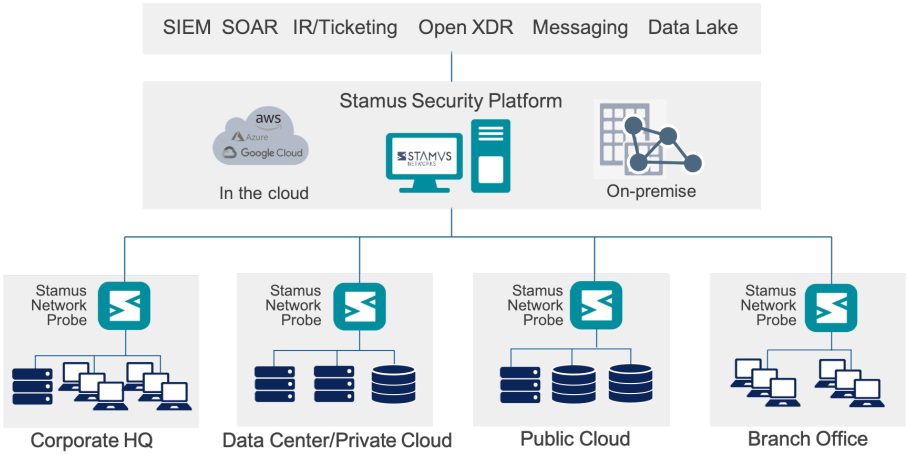
The probes are available as turnkey physical appliances (from Stamus Networks) or may be installed as a software image* on bare metal hardware, virtual machines, public or private cloud

* Stamus Networks appliances are required to monitor data rates above 10 Gbps

STAMUS SECURITY PLATFORM

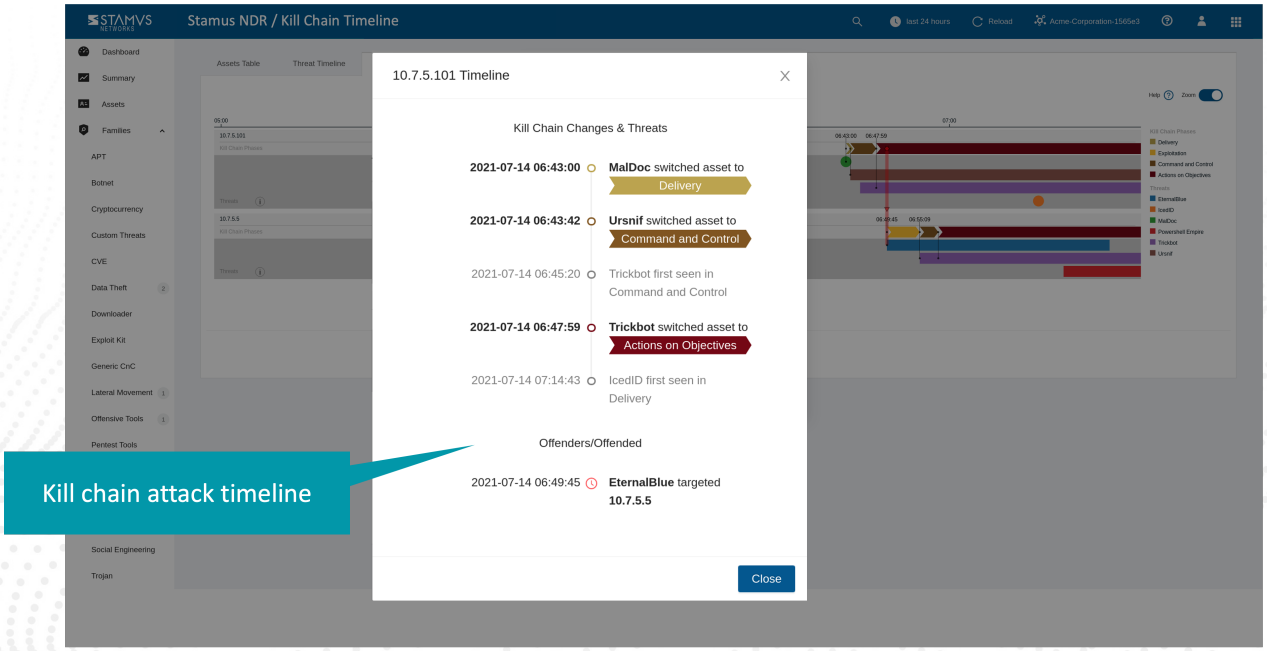
Stamus Security Platform (SSP) provides the centralized management of the probes along with several other critical functions, including:

SSP consolidates event storage and provides the central integration point for the rest of your security tech stack, such as SIEM, SOAR, Open XDR, IR or messaging systems

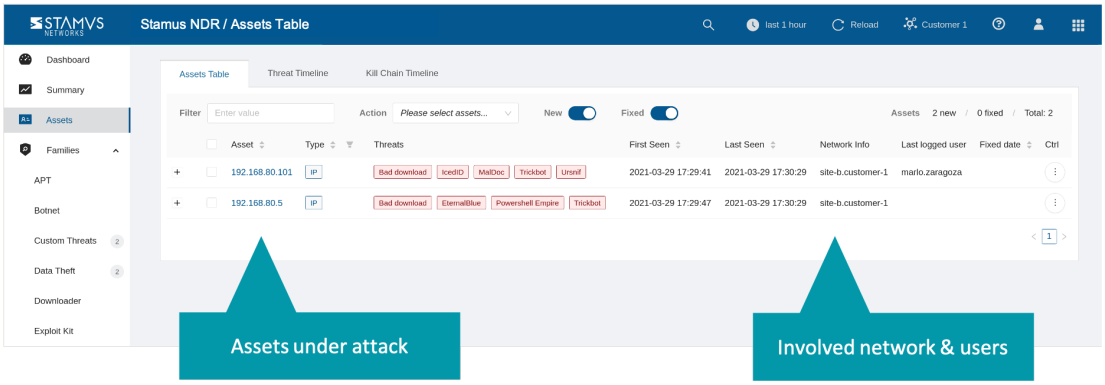


With Stamus NDR, SSP brings an additional layer of machine learning and algorithmic threat detection that identifies high-confidence threats (Declarations of Compromise™) to your critical assets, maps the advancement of those threats along the stages of the cyber kill chain, and serves as a "smoke alarm" to alert your personnel or systems when a serious and imminent threat is discovered.

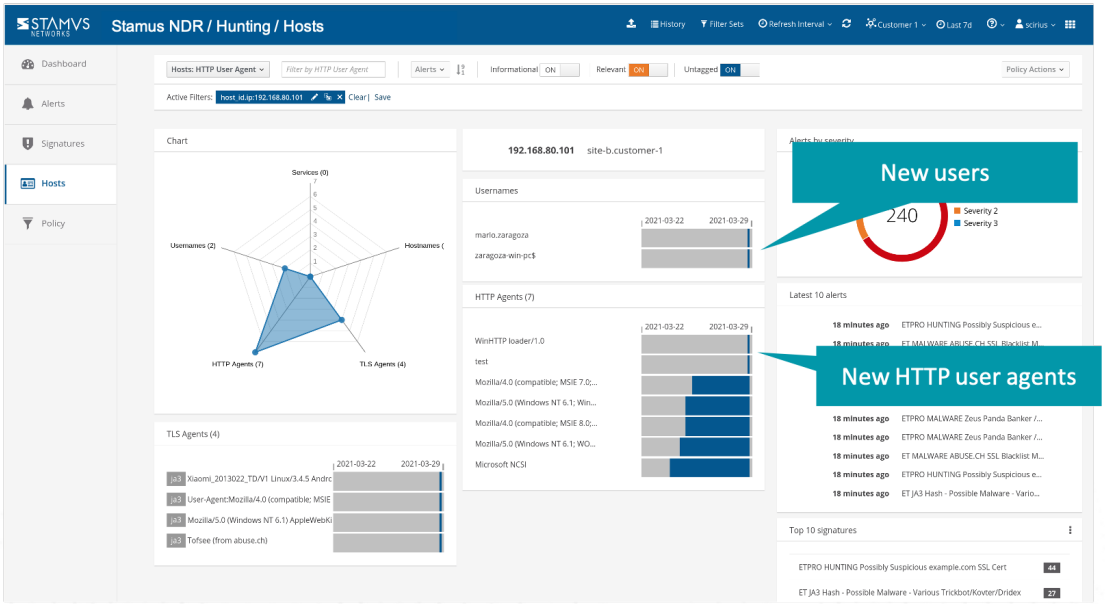
The entire event is reconstructed into an attack timeline for rapid assessment and response.



SSP includes a guided threat hunting console for proactive threat hunting and incident investigation



SSP extracts and organizes the data for hosts, assets and users to bring the security event data to life, making sense out of it in the context of your organization



Additional SSP capabilities include:

- Automated event triage - enabled by a tagging and classification workflow - to dramatically reduce the time spent by analysts reviewing security events
- Management of third-party threat intelligence and rulesets as well as support for custom threat detection that leverages the experience and organization-specific knowledge of your team

Like the probe software, SSP may be installed on turnkey physical appliances (available from Stamus Networks) or as a software image that you deploy either on bare metal hardware, a virtual machine, or a virtual machine in the cloud.

HOW STAMUS NDR IMPROVES YOUR SECURITY

Security teams use Stamus NDR for automated detection, proactive threat hunting, incident investigation and IT policy enforcement. Ultimately, the system helps security (SecOps) and network (NetOps) operations teams:

Reduce your organization's risk – uncover known and unknown threats to critical assets from your cloud and on-premise networks.

Eliminate network blind spots – monitor north-south as well as east-west traffic with Stamus Network Probes at all critical points in your cloud and on-premise networks.

Eradicate alert fatigue – the system notifies incident response systems and personnel only when urgent and imminent threats are identified.

Reduce the workload of your SOC analysts – free your valuable staff, allowing them to focus on proactive security measures, rather than pouring through 1000s of alerts.

THE NETWORK DOES NOT LIE

In fact, the network holds the ground truth for an enterprise's security posture. Even as more organizations shift to cloud-based resources, encrypted transmission, and remote workforces, nearly all cyber threats generate communications that can be observed on the network.

At Stamus Networks, we tap into the inherent power of network traffic to uncover every possible threat to your organization. We offer the best possible asset-oriented visibility and automated detection to help practitioners cut through the clutter and focus on only those serious and imminent threats.

Dramatically accelerate incident response - quickly investigate potential issues with transparent, explainable results, backed up with extensive evidence.

See results immediately – Stamus NDR is easy to install, configure and integrate with other elements of your security tech stack.

Extend your capabilities – leverage third-party threat intelligence and rulesets; and easily transform a threat hunt into custom detection logic.

Uncover hidden threats – because even the most advanced system cannot automatically detect everything, Stamus NDR comes with an integrated guided threat hunting console that make the hunt both effective and efficient.

Broad-Spectrum Detection		Multiple detection engines (machine learning, rules, threat intelligence, stateful logic). Alerts only on serious and imminent threats (DoCs).
Open Interfaces & Explainable Results		Open interfaces for SOAR, SIEM, XDR & third-party threat intel. Transparent and explainable results backed by extensive evidence.
Asset-Oriented Attack Insights		High-fidelity insights into attacks on your hosts and user accounts mapped to stages on the kill chain
Built-in Guided Threat Hunting		Guided threat hunting interface with advanced pivoting on enriched data, event tagging and knowledge transfer workflow
It Just Works		Easy to install, integrate, configure, and operate. It just works - all the time.

BUILT BY OPEN-SOURCE SECURITY TECHNOLOGY EXPERTS

Stamus Networks' product development is led by Éric Leblond and Peter Manev. Éric and Peter are members of the Open Information Security Foundation leadership team and developers on the Suricata project, the widely-deployed open-source intrusion detection and network security monitoring engine. The OISF is a non-profit organization created to build community and to support open-source security technologies like Suricata. Under the leadership of Éric and Peter, Stamus Networks applies its extensive Suricata and network expertise to develop our advanced network security solutions.

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

