STAMUS NETWORKS

Customer Story

When EDR Can't Get the Job Done, NDR Will

Situation:

A hosting services business with encrypted traffic passing among multiple public sector and commercial organizations does not have control over the endpoints, server installations, or hosting setups. They sought a network-based threat detection solution that provided visibility into a tricky network with a lot of moving parts, something EDR was not capable of doing in this scenario.

Discovery:

During an initial week-long trial on the organization's network, a single NDR network sensor monitoring a 10G connection generated 16 billion raw detections, collected activity data on over 37 million endpoints, and was able to uncover and isolate 28 high-priority, actionable alerts on 95 different impacted assets — all with completely passive, non-intrusive network monitoring.

Outcome:

Not only were the analysts able to quickly uncover several serious and imminent threats during their trial run, but the NDR also identified several new nefarious threat actors associated with an APT group and supported it all with detailed timeline of events and associated evidence.

Read the complete story »

A single NDR network sensor monitoring a 10G connection generated 16 billion raw detections, collected activity data on over 37 million endpoints, and was able to uncover and isolate 28 high-priority, actionable alerts on 95 different impacted assets

Network Detection and Response

Network detection and response (NDR) is a critical component of a comprehensive cyber defense strategy, monitoring and analyzing network traffic to identify and thwart malicious activities that traditional security measures may miss.

Using a combination of automated detection algorithms, incident investigation, and threat hunting tools, NDR enables organizations to proactively detect, investigate, and respond to threats that pose a risk to network infrastructure.

At Stamus Networks, we have enjoyed the privilege of working closely with a diverse range of organizations around the world.

During our deployments, we have witnessed remarkable success stories. In each example, NDR has played a pivotal role in safeguarding networks, mitigating attacks, and minimizing the impact of security incidents.

Each story provides a quick example of how NDR achieves one or more of the following three use-cases:

Threat Detection and Response [TD]

NDR empowers users to automatically detect threats and respond quickly, filling gaps left by traditional security measures and ultimately strengthening organizations overall security posture.

Network Visibility and Incident Response [NV]

NDR enhances network visibility by capturing and analyzing network traffic, enabling organizations to gain comprehensive insights into their network activities and identify potential threats in a timely manner.

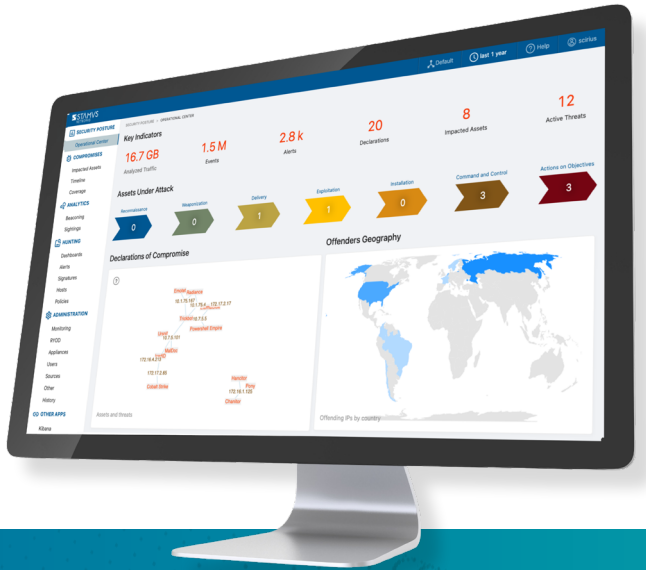
Threat Hunting [TH]

NDR enables security teams to proactively explore network data, detect potential threats that may have evaded traditional security measures, and investigate suspicious activities, shadow IT, and policy violations.

The Stamus Security Platform

The Stamus Security Platform is an open network-based threat detection and response (NDR) solution built on a Suricata foundation that delivers actionable network visibilityand powerful threat detection with:

- **Greater visibility into threats & activity**
- **Optional air-gapped deployment**
- **Our advanced probes or your Suricata sensors**
- **Transparent detections with detailed evidence**
- **Open and extensible for your environment**
- **Built for enterprise-scale operations**



Stamus Security Platform is trusted by some of the world's most targeted organizations, including government CERTs, central banks, insurance providers, managed security service providers, multinational government institutions, broadcasters, travel and hospitality companies, and even a market-leading cybersecurity SaaS vendor.

Like these organizations, your organization could likely benefit from including Stamus Security Platform in your cybersecurity strategy.

To learn more about SSP, visit us at www.stamus-networks.com