STAMUS NETWORKS

In The Trenches With Network Detection and Response

Real World Success Stories

Introduction

Cyber threats are becoming increasingly sophisticated and pervasive, so protecting your organization's network from malicious actors has never been more critical. This e-book showcases real-world success stories of organizations that have harnessed the power of Network Detection and Response (NDR) to safeguard their assets and expose serious and imminent threats and unauthorized activity lurking in their network.

What exactly is Network Detection and Response?

In a world where cybercriminals and rogue nation states are constantly evolving their tactics, NDR serves as a critical component of a comprehensive defense strategy. It monitors and analyzes network traffic to identify and thwart malicious activities that traditional security measures may miss. By 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 their network infrastructure.

We have had the privilege of working closely with a diverse range of organizations around the world, and during those deployments have witnessed remarkable successes. In each of these stories, NDR played a pivotal role in safeguarding networks, mitigating attacks, and minimizing the impact of security incidents.

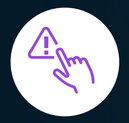
By sharing these success stories we hope to inspire, inform, and showcase the tangible results achieved by these organizations and demonstrate the effectiveness of NDR in real-world scenarios. Each story serves as a testament to the power of NDR and the positive impact it can have on businesses of all sizes.

Whether you're a security professional seeking validation for your cybersecurity strategy or an executive looking for ways to enhance your organization's security posture, these stories will offer valuable lessons and practical guidance.

> "In a world where cybercriminals and rogue nation states are constantly evolving their tactics, NDR serves as a critical component of a comprehensive defense strategy.

Network Detection and Response Use Cases

For the purposes of this e-book, we have divided the success stories into categories based on three primary NDR use cases. Each of these use cases highlights a different capability of NDR to showcase its various benefits and applications. As you are reading, look for the icon next to each story to identify which category each story falls under.



Threat Detection and Response
In this group of stories, we highlight success stories where NDR has proven to be highly effective in detecting and responding to various cyber threats. These use cases demonstrate situations where traditional security measures fall short and NDR fills the gap by identifying malicious activities that may have been missed. These organizations' stories showcase how NDR empowers users to automatically detect threats and respond quickly, ultimately strengthening their overall security posture.

Network Visibility and Incident Response
This group emphasizes the importance of network visibility. These use cases demonstrate how NDR enhances network visibility by capturing and analyzing network traffic, enabling organizations to gain comprehensive insights into their network activities and identify potential threats. By improving network visibility, NDR can help organizations effectively safeguard their networks and respond to threats in a timely manner.

Threat Hunting
NDR systems empower organizations to conduct effective threat hunting. By providing advanced network visibility and powerful analytics, NDR can enable 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. These success stories highlight how NDR has enabled organizations to proactively uncover hidden risks, identify emerging threats, and take proactive measures to mitigate them, bolstering their overall security defenses.

Identification of Unexpected Proxy Network Service Leads to Discovery of Shadow IT

Situation

A Financial Services organization has a mix of physical and virtual network sensors, but found it nearly impossible to rely on IP addresses for threat detection as most devices changed their IP every 30 minutes.

Discovery

Using the NDR's guided threat hunting interface, the customer was able to discover that a group of engineers had installed a temporary encrypted proxy service, which allowed them to bypass organizational infrastructure and install any software they wished, leaving the organization open to possible exploitation by malware actors.

Outcome

The increased visibility provided by the NDR enabled the customer to identify a stealthy policy violation that their other systems had missed. They were able to quickly resolve the problem, and easily set up automations to detect the similar proxy service use in the future.

Read More

> The increased visibility provided by the NDR enabled the customer to identify a stealthy policy violation that their other systems missed.

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 More

A single NDR network sensor monitoring a 10G connection:

- Generated **16 BILLION** raw detections
- Collected activity data on over **37 MILLION** endpoints
- Uncovered and isolated **28** high-priority, actionable alerts

Proactive Threat Hunting Detects MoDI Rat Malware Before Damage Can Be Done

Situation

A financial services organization had the NDR configured to automatically classify certain types of events as “relevant” to the security posture of the organization. During a regular check-in with the NDR vendor’s support team, the organization reviewed a set of these relevant events — just 20 of the 500 million total events gathered in the previous 24 hours.

Discovery

One particular event — triggered by an ETPro malware IDS rule — stood out. Upon further investigation, the team discovered that a user had visited a Wordpress blog that was infected with MoDi RAT malware.

Outcome

The customer was able to escalate the event, quarantine the device, and even notify the owner of the blog, catching the malware on the network before it caused any impact to the organization.

Read More

Threat Hunting Locates Raiz0WorM Instance on Large Research University Network

Situation

This organization is a university-based supercomputing center in Europe, which is frequently targeted by threat actors. They have deployed the NDR system with a single network sensor monitoring 40Gbps of traffic.

Discovery

Using the NDR's guided hunting filters, the customer was able to filter through 12.5 million alerts and over 1 billion network events — collected over a 24 hour period — to search for specific threats. By filtering their alerts for http requests/responses that both used base64 functions and returned HTTP status code 200, the customer uncovered Raiz0WorM activity.

Outcome

The security team was easily able to escalate the alert to incident response and create an automation to identify any future or past occurrences of similar activity — all in the matter of a few minutes.

Read More

Using the NDR's hunting filters, the customer was able to:

Filter through **12.5** Million alerts

Filter through over **1 BILLION** network events

Financial Services Customer's EDR Misses Clever Spyware Attempt

Situation

A customer manages a vast datacenter and remote workforce with a mix of physical and virtual network sensors for their large financial institution. Due to the nature of their industry, their devices change IP addresses an average of every 30 minutes, making it nearly impossible to rely on IP addresses for threat detection.

Discovery

While testing a new feature in their NDR — "Sightings" which identifies never-seen-before network communications — the customer discovered that a laptop belonging to a trusted member of the infrastructure team had unintentionally installed an adware program. The agent appeared to change its objectives, and was now attempting spyware-like exfiltration.

Outcome

This spyware had managed to evade the endpoint defenses (EDR) and the company-wide browser restrictions and posed a growing risk to the organization. Detecting this from the network allowed the customer to open an incident and engage their EDR/SoC teams to evaluate further impact and other potential points of quarantine that may be needed.

Read More

Multiple Security Vendors Miss Suspicious HTTP User Agent Activity

Situation

A subsidiary of a large European banking and insurance conglomerate has a mix of on-premise, branch office, public and private cloud assets. In addition to NDR, their substantial security infrastructure includes endpoint detection (EDR), VPN, firewall, and multi-factor authentication from many of the industry's top security vendors.

Discovery

By reviewing the host insights data available in the NDR's integrated threat hunting interface, the customer discovered a series of transactions involving very unusual HTTP user agents. They identified what appeared to be Chinese and Korean alphabet characters in the HTTP user agent fields within protocol transactions on the accounting department's network. This was suspicious because the bank does not do business in China or Korea, and would not expect to see these characters from any of its systems.

Outcome

The customer isolated the internal sources of this unusual communication to a specific department (accounting) and group of staffers from within that department. The security team determined that the staffers were accessing an unapproved legacy software system that was generating the communications, leading the customer to escalate the activity and launch a formal investigation.

Read More

By reviewing the host insights data available in the NDR's integrated threat hunting interface, the customer discovered a series of transactions involving very unusual HTTP user agents.

NDR Dominates Detections at NATO Crossed Swords 2022

Situation

Every year, NATO CCDCOE hosts an annual technical red teaming cyber exercise — called Crossed Swords — to train penetration testers, digital forensics experts, and situational awareness experts with teams from more than 20 countries. In 2022, Stamus Networks once again participated on the yellow team, monitoring the red team exercises using NDR (Stamus Security Platform).

Discovery

The 9 members of the yellow team identified a total of 113 threats during the course of the exercise. Notably, the 2 yellow teamers from Stamus Networks using NDR identified 67 (or 60%) of the findings.

Outcome

NDR was the standout threat detection system on the yellow team, enabling two analysts to exceed the output of dozens of other NATO participants combined.

Nine members of the yellow team identified **12.5 MILLION** threats

Two yellow teamers from Stamus Networks using NDR identified **67 (60%)** of the findings

NDR enabled two analysts to exceed the output of **DOZENS** of NATO participants

Central Bank: European Institution Achieves Greater Network Visibility With NDR

Challenge

A Large Central Bank customer in Europe was using a legacy IDS that limited their ability to rapidly identify and respond to imminent threats and lacked full network visibility. After an extensive evaluation, they replaced this aging system with a modern NDR to solve their challenges.

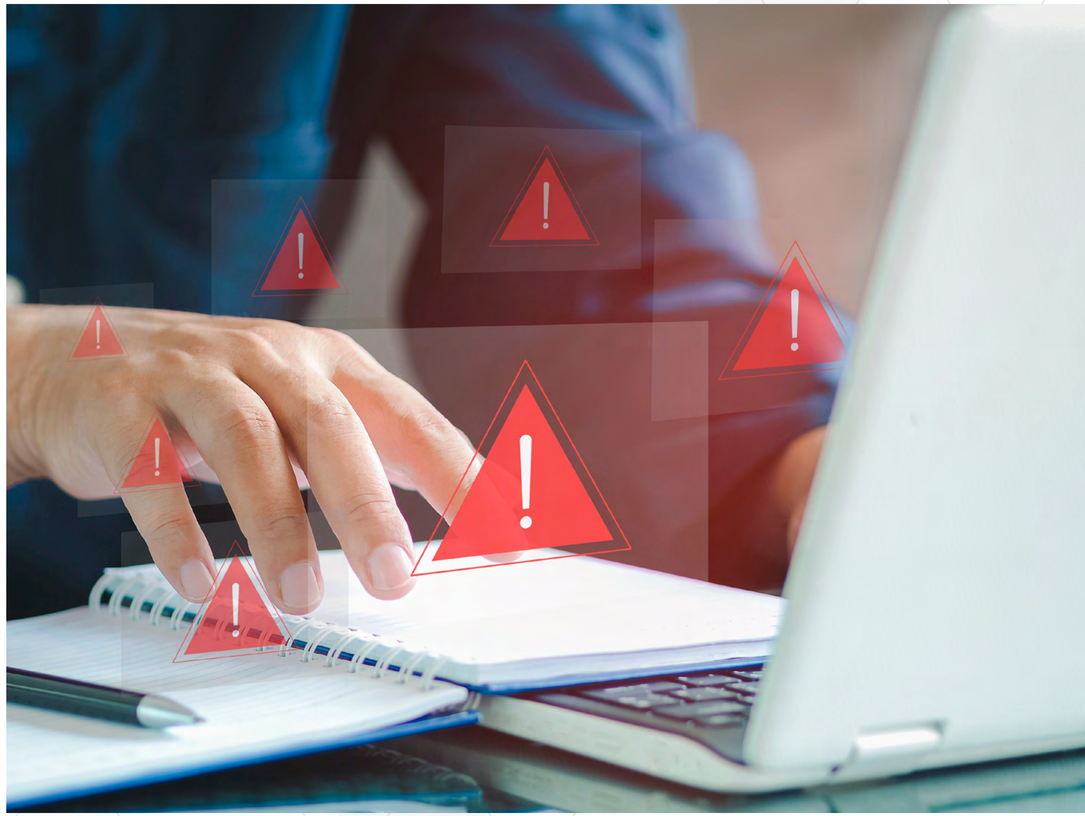
Solution

Using the NDR, the bank has eliminated numerous blind spots on the network, automatically prioritized their security events, and seamlessly integrated network telemetry into their existing tech stack.

Outcome

As a result of implementing the NDR, the bank improved their threat detection, decreased their incident response time, and increased their confidence in the security of their organization.

Read More



Center Grove: Indiana Public School District Ditches MSSP and Replaces With SSP

Challenge

An Indiana public school district with a small IT team managed a variety of technology assets for 8,500 students. This included a one-to-one device program for students who access educational programs through a mix of self-hosted and cloud-based resources. They outsourced their security services to a MSSP provider that lacked sufficient visibility into their unusual network of connected devices and routinely missed serious and imminent threats.

Solution

They selected an NDR system that would provide them with greater levels of visibility while meeting compliance objectives in an environment that is not conducive to deploying an endpoint-based system.

Outcome

They used the NDR to make their security strategy more efficient by relying on the system's high-confidence prioritized alert events that cut through the noise and notify personnel on only the most serious and imminent threats. They were also able to eliminate their outsourced managed security service provider.

Read More

European MDR Designs Advanced NDR into Their Product Offering

Challenge

A European managed security provider wanted to include an advanced Suricata-based network detection and response (NDR) into their nascent managed detection and response (MDR) service offering. They needed an NDR that was flexible enough for their unique needs and also integrated seamlessly into their technical stack which included cloud-based SIEM and SOAR systems.

Solution

They selected the leading Suricata-based NDR that delivers an open interface, flexible deployment options, and is backed by strong commitment to ongoing support and partnership.

Outcome

The service provider now includes an NDR option for their customers, something they previously could not do. They now enjoy the benefits of advanced network monitoring, providing them greater visibility into their customers' networks, improved detection, lower time to respond, and less risk.

Read More

14

Penfield: NDR Provides Peace of Mind for Small US School District

Challenge

A small US school district servicing 6000 students on a one-to-one device program felt like they were lacking visibility and availability of network traffic data. This is because their only means of threat detection was a SIEM, an app blocker, and an antivirus. They sought a more advanced solution that didn't require any endpoint installations.

Solution

They chose an NDR, opting to monitor the network rather than each individual device. They deployed two sensor appliances into cloud environments and began using the NDR to perform proactive threat hunting, troubleshooting, and incident investigation.

Outcome

The NDR gave the school district maximum visibility into network traffic across 5000 endpoints, enabled thorough investigation into policy violations and user behaviors, and minimized false positives and alert fatigue — all while functioning in the customers preferred environment without regular maintenance or support. The inclusion of the NDR provided additional comfort and confidence in the school district's ability to protect their students and teachers from cyberthreats.

Read More

The NDR gave the school district maximum visibility into:
Network traffic across **5000** endpoints

The Stamus Security Platform

In each of these NDR success stories, the organizations used the Stamus Security Platform (SSP).

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

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

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