Solution Brief

XDR - eXtending Detection and Response to the Network

Extended detection and response, or XDR, has generated substantial interest in recent years - and rightfully so. According to new research from Enterprise Strategy Group (ESG), 58% of security professionals say XDR could modernize the SOC by enhancing, improving, or aggregating current security analytics capabilities. It makes sense to evolve (or extend) a concept that is working well.

Unfortunately, industry analysts and vendors have done a disservice to the market by delivering multiple interpretations of the term.

In this solution brief, we share the Stamus Networks perspective on XDR and make the case for why it is crucial that any credible definition of XDR must include a network component.

THE POWER OF THE NETWORK

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. And in many environments – for example, those with extensive bring your own devices (BYOD) or Internet of things (IoT) usage – you simply can't rely on endpoint detection to uncover threats.

At Stamus Networks, we tap into the inherent power of network traffic to uncover critical threats and facilitate a rapid response. We deliver the best possible automated detection and asset-oriented insights to help organizations cut through the clutter and focus on only serious and imminent threats.

SO, WHAT ABOUT XDR?

Well, as much as we believe in our network-based solutions, we recognize that many organizations wish to take a defense-in-depth approach and therefore also need visibility and coverage in other areas such as endpoint and email security. And because security operations center (SOC) teams want more centralized control over the incident response and remediation, the industry has responded with a new product category - extended detection and response, or XDR.

As with many new technology categories, the hope for and hype surrounding XDR is a little crazy. As is often the case, each vendor is staking claim to their own particular definition of XDR. Some see it merely as an extension to their endpoint detection and response (EDR), while others see it as a natural extension of their security information and event management system (SIEM) or their security orchestration, automation, and response system (SOAR).

At Stamus Networks, our view of XDR is closely aligned with that of Gartner's: "... a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components."

XDR MUST INCLUDE NDR

These “multiple proprietary security components” from this definition include sources of telemetry and detection from endpoints, networks, email and other systems. So yes, a complete XDR solution does include a network detection and response (NDR) component.

This is the new ‘holy grail’ for those organizations looking for a single pane of glass and a single platform on which to automate a response from all its sources of security telemetry data.

Today XDR is a relatively new concept, and it involves many different technology disciplines and specialties, which really makes this vision too broad for any single company to tackle.

That’s why we at Stamus Networks are proponents of Open XDR.

With Open XDR, typically one solution provider is focused on back-end analytics and a workflow engine to deliver a single orchestration plane across multiple telemetry and detection sources from complementary solution providers.

This way, the security operations center (SOC) team benefits from best of breed components at the network, endpoint, email and other sources of security telemetry and detection while primarily working with a single pane of glass for their every-day operations.

In this model, the Open XDR tech stack is really an ecosystem of like-minded solution providers who strive to work together using open interfaces and a collaborative approach, as illustrated in **Figure 1**, below.

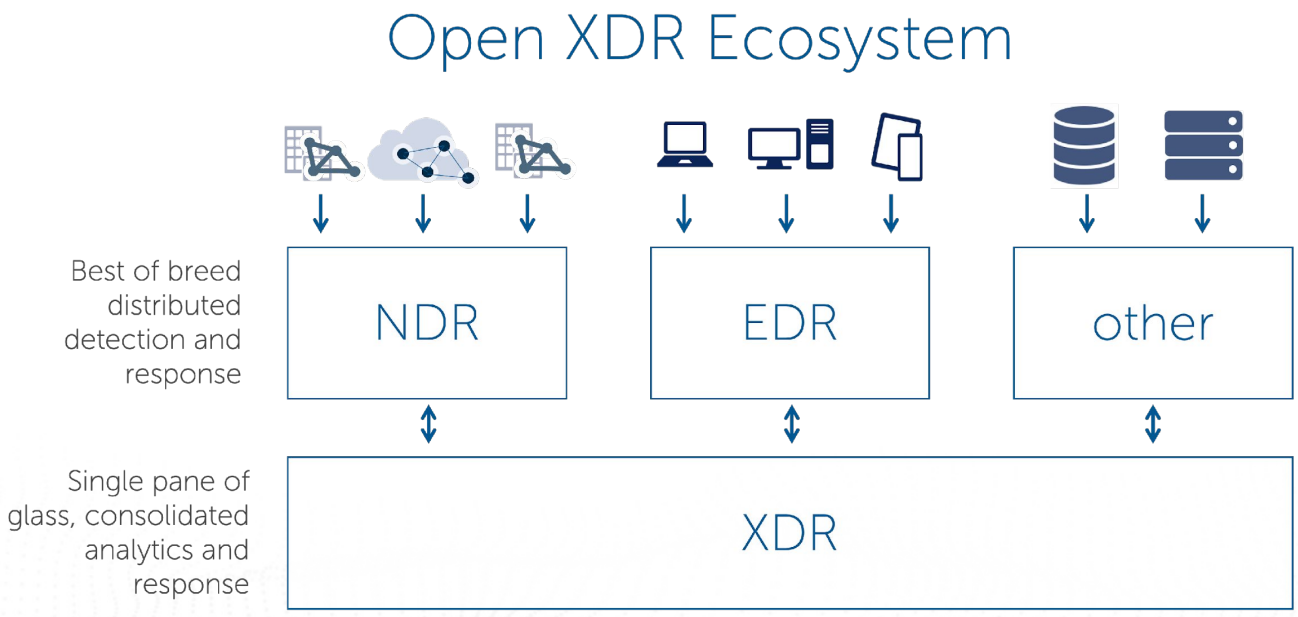

Figure 1. Open XDR ecosystem includes NDR

Stamus Networks and Open XDR

As discussed above, Stamus Networks is a network security solution provider. The Stamus Network Detection and Response (Clear NDR) is ideally suited for integration into the Open XDR architecture.

Customers of Stamus Networks have shared five things they want from their NDR solutions:

- **Advanced detection** - broad-based threat detection to uncover both known and unknown threats
- **Transparent, explainable results with evidence** - detailed insights into what is happening on the network and when, helping explain the results of detections and facilitate incident investigation
- **Automated response** - high-fidelity notifications that can be used to trigger a response from an XDR, SOAR or incident response system (IR)
- **Guided threat hunting** - the tools and guidance to facilitate proactive security, based on network data
- **Openness and extensibility** - the ability to integrate into their tech stack and customize detection to suit their specific requirements

Stamus Networks has embraced these ideas in its solution, Clear NDR.

Figure 2 below illustrates where Clear NDR fits in the Open XDR ecosystem.

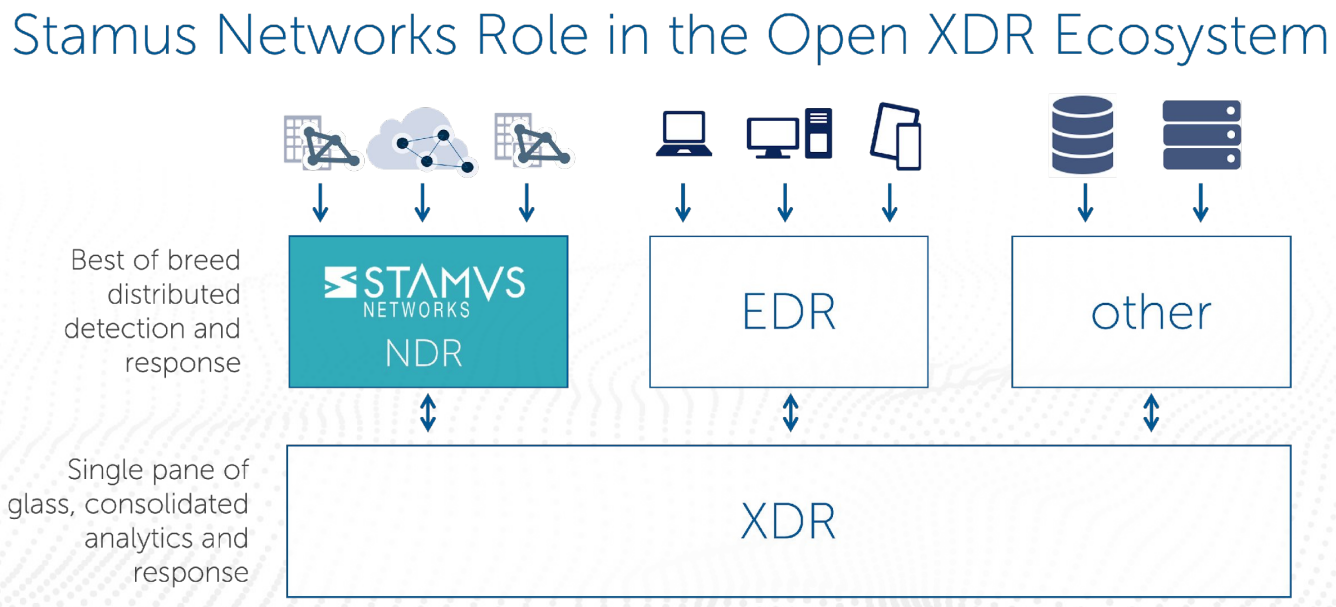

Figure 2. Stamus Network's role in the Open XDR ecosystem

ABOUT Clear NDR

Clear 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
- Simple integration with XDR, SOAR, SIEM, XDR, IR
- Access to third-party and custom threat intelligence
- Explainable and transparent results with evidence
- Integrated guided threat hunting

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

LEARN MORE

To learn more about Clear NDR, please visit the Clear NDR section of the Stamus Networks website here: https://www.stamus-networks.com/clear-ndr.

If you'd like to get a live demonstration of Clear NDR or discuss how it might fit into your Open XDR environment to help you detect and respond to threats in your network, please visit the Stamus Networks website to request a demo.

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

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

