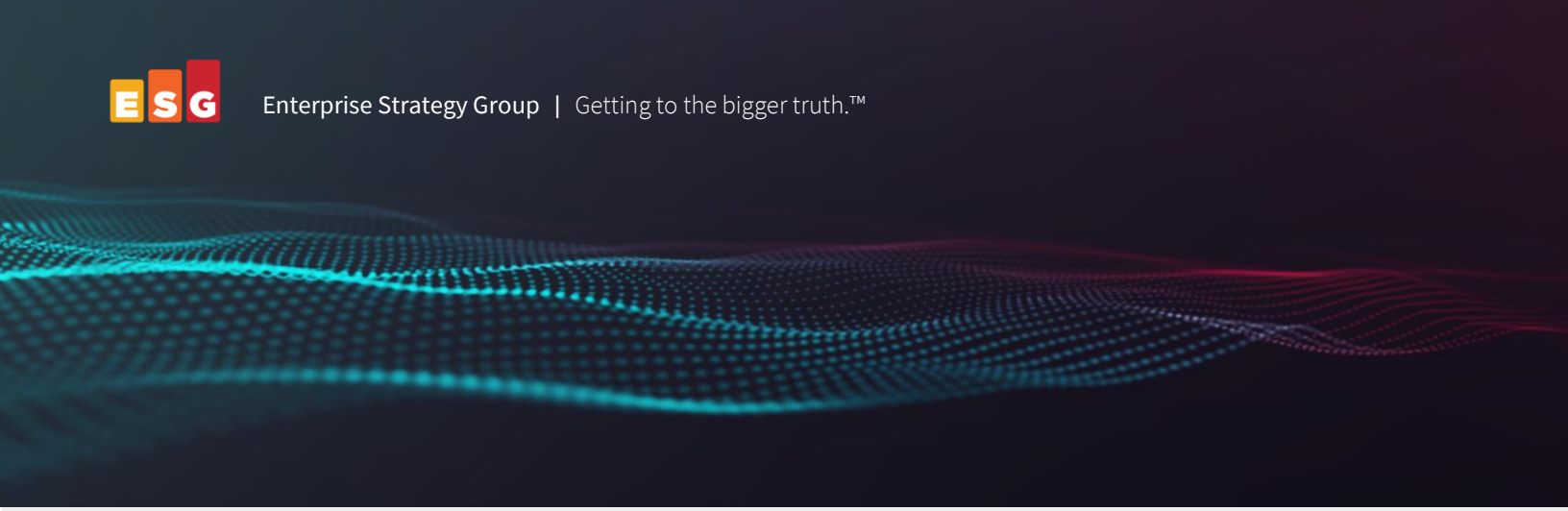


ESG WHITE PAPER

Open Network Detection and Response (Open NDR): What It Is and Why It's Needed

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

March 2021

This ESG White Paper was commissioned by Corelight and is distributed under license from ESG.

Contents

Executive Summary

According to ESG research, 43% of organizations use network detection and response (NDR) tools as a first line of defense for threat detection and response.[1] Why? As the old security saying goes, "the network doesn't lie." Cyber-attacks always move laterally across networks as they connect to external command-and-control (C2) servers, harvest credentials, discover valuable assets, and exfiltrate sensitive data. Therefore, recognizing suspicious/malicious network traffic patterns in a timely manner and then combining network telemetry with endpoint detection and response (EDR) and threat intelligence sources is a key to effective threat detection and response.

While the link between NDR and threat detection/response may be common knowledge, many organizations continue to struggle with network security operations, extending timeframes for mean time to detect (MTTD) and mean time to respond (MTR) to dangerous cyber-threats. Most organizations also admit that network security continues to grow more difficult, opening them up to damaging cyber-attacks.

Why is network security so difficult and what can be done to address this unacceptable situation? This white paper concludes:

- Network security difficulties are driven by internal and external factors. Security teams are forced to deal with increasing threats and a growing attack surface of more devices, cloud-based assets, and remote users. As if this wasn't hard enough, organizations monitor and protect their networks using armies of disconnected point tools. It has become nearly impossible for security operations teams to deploy, configure, manage, and operate their network security technologies with any degree of efficiency. Meanwhile, security efficacy (i.e., the ability to prevent, detect, and respond to threats) suffers.This is especially true in light of advanced persistent threates (APTs) like those used in the SolarWinds hack. Patient attackers can dwell on networks and then operate stealthily for months longer before being detected. Lacking a clear picture of network activity going back months or years can handicap security investigations of breaches like these.
- Organizations are consolidating vendors and integrating tools. Recognizing the perils of their current approach, security teams are on an active path to reduce complexity. To do so, most organizations are winnowing down vendors and tools while building a more tightly integrated security operations and analytics platform architecture (SOAPA). The goal here is to create a shared data repository so that all network security analytics tools have real-time access to a single source of truth.
- Open NDR provides an alternative path. Security technology consolidation and integration can reduce tools sprawl, but organizations remain dependent upon numerous vendors, each with their own product designs, release schedule, security engineering teams, maintenance, and support. So, while technical integration may improve interoperability, SOC teams are still left with multiple data repositories and vendor interpretations of what is and isn't needed for network security. ESG believes there is a viable and increasingly attractive alternative, however: Open NDR, built upon widely distributed and battle-tested open source software. Many security professionals don't realize that open source network security tools like Zeek (an industry standard for cybersecurity-focused network metadata), Suricata, and PCAP capabilities already enjoy tight integration, driven by the open source community, while providing open access to the underlying data (i.e., Zeek logs or Suricata alerts). Open NDR can also be extended, modified, or customized using packages and other contributions from the open source communities involved, while establishing a single network security data lake, and then collecting, processing, and analyzing this data in concert with other data sources (like endpoint data) and existing security operations tools to improve use cases like threat detection/hunting and incident response.

[1] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

The State of Cybersecurity Operations

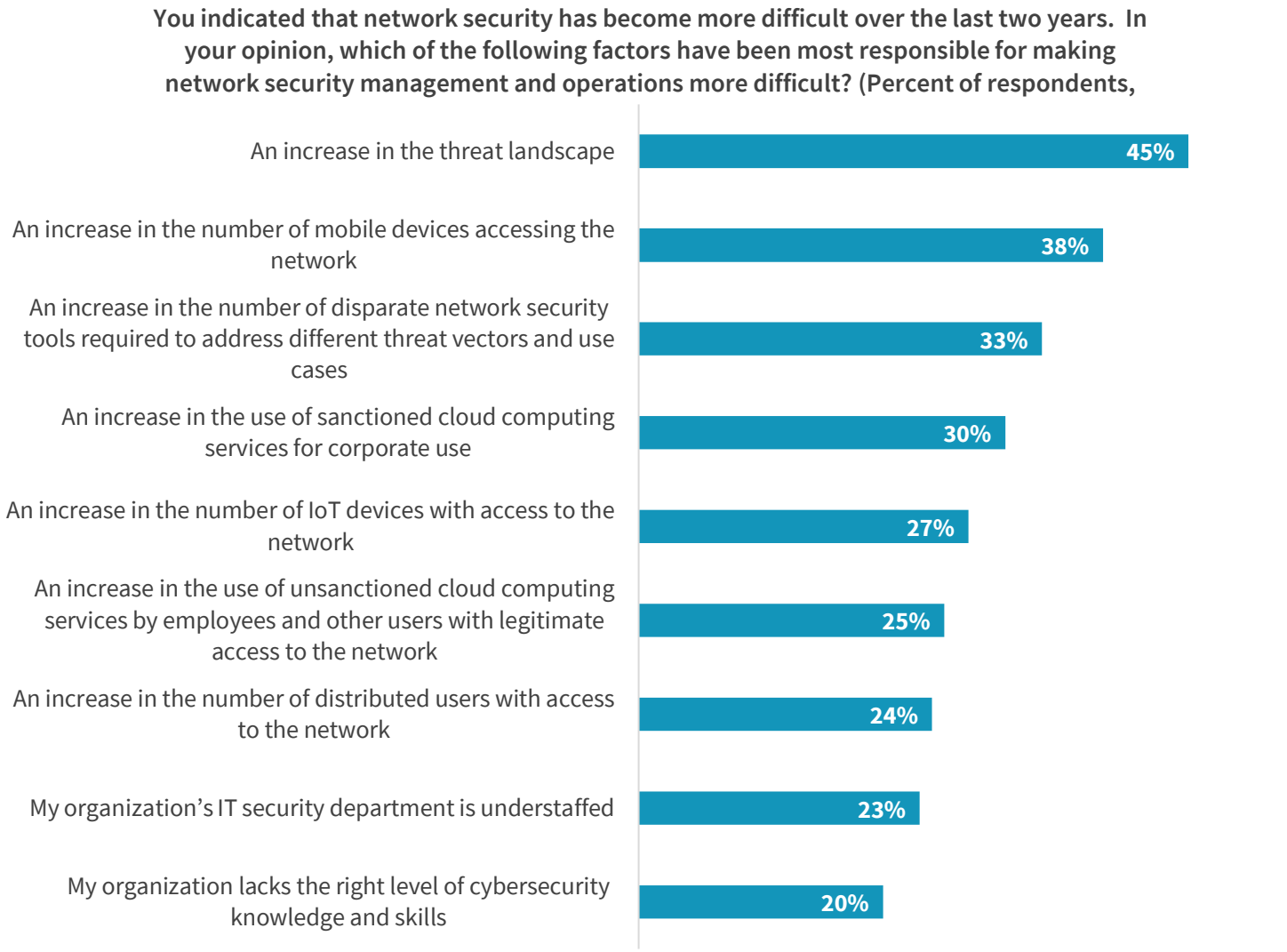
According to recent ESG research, 85% of organizations believe that network security is more difficult today than it was 2 short years ago. This belief is based on several factors including (see Figure 1):[2]

- An increase in cyber threats. As in years past, security difficulties are a function of increasing and dangerous cyber threats that move laterally across networks. Security teams are tasked with understanding cyber-adversaries, their campaigns, and how these things impact internal networks, a daunting set of responsibilities requiring time, knowledge, and threat intelligence experience. With the late 2020 exposure of the SolarWinds Sunburst hack, this difficulty will only continue in 2021.
- A growing attack surface. The ESG research points to network security difficulties associated with a growing attack surface in areas like an increase in mobile device use, growing use of sanctioned and unsanctioned public cloud infrastructure, and the proliferation of IoT/OT devices on the network. Attack surface growth means more connections, protocol types, and traffic patterns that must be monitored and secured. Security operations teams need to be able to scale network monitoring to keep up.
- The proliferation of network security tools. With the growing attack surface comes more network security technologies for areas like microsegmentation, packet filtering, and threat detection. Already overwhelmed cybersecurity staff must figure out how to deploy, configure, and operate these tools, making network security more difficult.

Additionally, more network traffic is encrypted by default. Encrypted traffic creates a growing blindspot, minimizing the effectiveness of signature-based detection tools like IDS/IPS and sandboxes.

[2] Source: ESG Research Report, *The State of Network Security: A Market Poised for Transition*, March 2020.

Figure 1. Reasons Why Network Security Has Become More Difficult



Source: Enterprise Strategy Group

As the attack surface and network threats surge, enterprise organizations must monitor all traffic at key points on the network (i.e., ingress/egress points, data centers, within public clouds, etc.). To do so, CISOs typically rely on all sorts of network and security monitoring tools like network detection/response (NDR) systems, network traffic analysis (NTA), full packet capture (PCAP), IDS/IPS, device health logs (e.g., firewalls), NetFlow data, and even some for network operations like network performance management (NPM). Some large enterprises use a combination of commercial and some open source or even different "flavors" of various tools, used by different groups.

Unfortunately, network security tools sprawl like this inevitably leads to a host of issues like:

- Operations overhead. When the security operations team wants to observe network behavior or dig into specific data for threat detection, they are forced to gather disparate data elements from a variety of tools and then manually piece things together. Since there is no single source of network security truth, this process requires knowledge of where the data is, how to get it, and then how to use it within investigations. This leads to time-consuming security operations complexity, limiting the efficacy and efficiency of security operations.

- Data sprawl. ESG research indicates that 76% of organizations collect, process, and analyze more data today than they did 2 years ago to support security operations[3] and network security is no exception. Regrettably, network security data is not synchronized, uses different formats, and is collected from different and often incompatible sources at many organizations. This creates huge volumes of data but much of it of little real value.

- Visibility gaps. Despite all of the data, visibility gaps remain due to data source limitations. NetFlow data provides basic connectivity data but not much information about payloads, and it isn't too valuable in security investigations. PCAP data is normally only retained for short timeframes and when it is available, it is dominated by large volumes of irrelevant data, making searches difficult and time-consuming. With attacks like SUNBURST, two or three weeks of PCAP would be utterly useless in an investigations into network access nine months in the past. Network performance management (NPM) tools may contain a few nuggets relevant to security, but they aren't really designed for security use cases. Once again, this forces analysts to spend too much time finding whatever data elements are available when they should be focused on analyzing and acting upon the data.

The data issues described above can really hold back strong security and operations best practices. Rather than base security operations processes on the data that's needed, the SOC team settles on the data that's available from network security vendors and tools. This is far from an ideal situation.

Toward Open NDR

Recognizing how broken this model is, many organizations are actively consolidating tools and integrating security operations technologies to drive greater security operations efficiency. In fact, ESG research indicates that 84% of organizations are actively integrating disparate security operations tools to build a more cohesive security operations technology architecture.[4] Network security tools integration is part of this type of initiative.

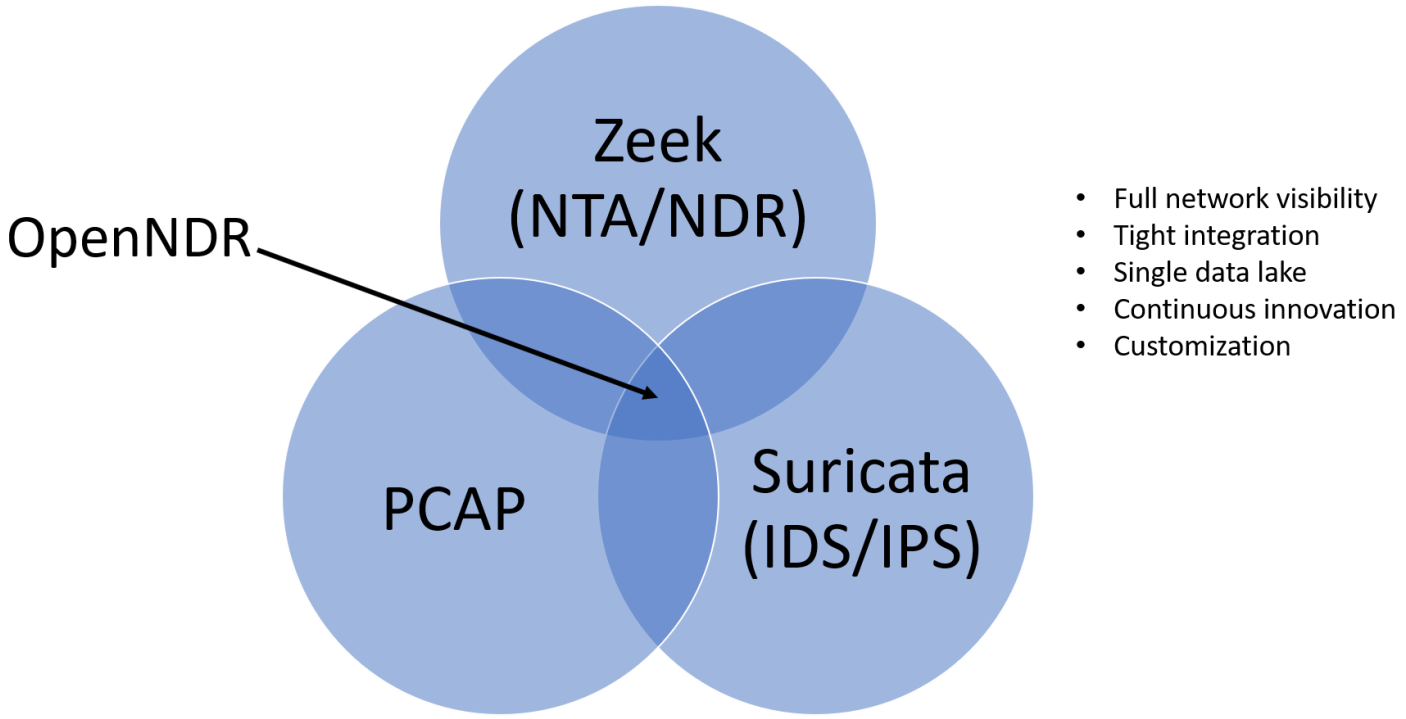
When building a security operations technology architecture, many organizations consolidate their existing tools, settle on a few vendors, and then integrate heterogeneous tools through software APIs or some type of messaging bus. This type of custom integration project can be a cumbersome engineering undertaking since integration will need to be guided by what each vendor makes available in its software.

Rather than betting on vendors and proprietary tools, ESG has noticed a burgeoning trend toward Open NDR solutions based upon 3 open source projects (see Figure 2):

1. Zeek: For network traffic analysis, incident response (IR), and threat hunting with community support.
2. Suricata: For threat detection based upon community rule sets.
3. Full packet capture (PCAP) based on triggers.

[3] Source: ESG Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019.
[4] Ibid.

Figure 2. Open NDR



Source: Enterprise Strategy Group

Just what is Open NDR? It is a comprehensive flexible approach to network security that takes advantage of the power of open source software development and an open design. Integrated Open NDR architectures offer a number of advantages over proprietary alternatives, such as:

- The open source community. Unlike proprietary products that keep customers dependent upon vendor innovation, Open NDR is anchored by the global reach and continuous innovation driven by the open source community. For example, open source Zeek has over 10k deployments worldwide, over 2900 GitHub stars, and over 20 years of community development. The "network effect" is especially useful in areas like the proliferation of IoT and OT devices. Zeek supporters continually develop and share homegrown parsers and scripts used for monitoring specific IT/IoT protocols. Additionally, the open source community is already hard at work on software integration. For example, Zeek, Suricata, and PCAP now share common data field known as "CommunityID" (a hash of the five-tuple), making it easier to pivot back and forth when investigating suspicious traffic. This integration alone can help organizations streamline incident response processes.
- A data-first model. With open source Zeek, Suricata, and PCAP, SOC teams can collect and process large volumes of network data in an open format, creating a data lake that acts as a single source of truth. Security professionals can then take advantage of the comprehensiveness of open data formats. For example, Zeek can parse network metadata across 35 different network protocols, providing rich logs of what's happening on the network. Open data has the additional advantage of better extensibility, portability, and filterability than proprietary alternatives, making it easier to integrate with SIEM platforms and analytics stacks so it can be contextualized against other data from endpoints, system logs, or threat intelligence telemetry. Because everything starts with the data, SOC teams aren't hamstrung by the limitations of proprietary technologies. Rather, they can be more proactive, independent, and comprehensive about hunting for threats, digging into logs and alerts themselves to understand context. And, because the underlying network metadata isn't tied to any particular SIEM or analytic stack, SOC teams can change that part of their infrastructure without fear of losing the data.

- Customized detections. With proprietary solutions, detection rules are provided by individual vendors. These rule sets tend to be generic, for use by the vendor's installed base of customers across industries and geographies. And with proprietary solutions, network security professionals are placing single bets on their vendors' ability to retain engineering staff; keep up with cyber-adversary tactics, techniques, and procedures (TTPs); and continually advance and innovate their products. With Open NDR, security teams can take advantage of community detection innovation while developing their own custom detection rules that align with their specific applications, infrastructure, geographic location, and any attributes specific to threat actors or attack campaigns targeting their organization. Once detections are established, security teams can also test and tune them regularly rather than waiting for vendor updates. Yes, this involves more work, but Open NDR can help SOC teams increase detection coverage, increase alert fidelity, and reduce false positives.

Open NDR can provide a one-stop shop for an entire network security stack that includes IDS/IPS, network traffic analysis (NTA), network detection/response (NDR), full packet capture (PCAP), and even functionality for network performance management (NPM). With the right data, customization, and the support of the open source community, Open NDR offers cost, functionality, and operational benefits over traditional proprietary options (see Table 1). And while open source carries the stigma of complexity, most enterprise SOCs have the engineering talent to create a useful Open NDR architecture. Further help is always available from the open source community or from commercial specialists like Corelight.

Table 1. Open NDR versus Proprietary Options

	Open NDR	Proprietary Option
Cost	Software is free but support may require a third-party service provider or open source specialist like Corelight	Expensive software and support
Data	Single data lake, strong data portability, filtering, and extensibility	Multiple data repositories, limited data portability, filtering, and extensibility
Detections	Driven by global community and highly customizable, file extraction and scripting language built in	Reliance on individual vendors, limited customization; file extraction and scripting may or may not be part of software functionality
Community	Global, tens of thousands of organizations; some government funding for development	Based on reach and installed base of vendor(s); may be a user community but development tends to rely on vendor engineering
Operational benefits	Software integration can streamline IR processes, typically integrated into SIEM/SOC analytics tools to provide a common UI	Integration dependent upon third-party software such as SIEM and SOAR, each tool typically provides its own UI, making security operations complex

Source: Enterprise Strategy Group

Corelight for Open NDR

Open NDR may be especially attractive for budget conscious organizations since it is based upon free open source security software. This may be a bit deceptive, however, as it can take advanced skills and several months to customize an Open NDR stack for a production environment. Furthermore, maintaining Open NDR means dealing with OS upgrades; NIC integration; open source project releases; incompatibility issues among OS, software, and hardware; and integration issues among adjacent systems, APIs, and data management tools. Finally, even organizations with ample resources may have reservations here, as many of the same people doing threat detection, response, and hunting would be needed to build and customize an Open NDR technology stack.

Rather than undertake this type of do-it-youself project, organizations can gain the benefits of Open NDR by working with Corelight, a network security vendor based out of San Francisco, California. Corelight was founded in 2013 by Vern Paxson, the creator of open source BRO (now called Zeek), with a vision of commercializing open source network security software. Today, Corelight provides a fully integrated Open NDR offering, featuring:

- Full Open NDR capabilities. Corelight integrates Zeek and Suricata, providing metadata for network security analysis, detection rules, file extraction, and packet capture for forensics and investigations.
- Rapid deployment. While a customized Open NDR stack can take weeks or months before it is production-ready, Corelight Open NDR can be deployed quickly, usually within a few hours.
- High Performance. Corelight offerings can scale to 26 gbps of throughput, making it a good fit for global enterprise-class networks. This performance is especially useful for tasks like optimizing file extraction.
- Out-of-box integration. Corelight delivers Zeek data and Suricata alerts to the customer's data analytics stack/SIEM, which means they don't have to trust our judgement; they can dig into the logs and alerts themselves to understand context. Remediation actions can be taken through SOAR integration, while SOC analysts can use SIEM or analytics tools as a UI for threat hunting across network data.

Through integration, packaging, and continuous innovation, Corelight can help organizations achieve the benefits of Open NDR without the overhead necessary with open source software alone. Additionally, Corelight offers support and maintenance, which will be welcome by organizations without open source software expertise. Finally, Corelight's engineering team remains active in open software project support and development. In this way, Corelight is a safe bet to keep its customers current with advances within the open source software community.

Organizations looking for integrated and open solutions for network security should contact Corelight to see how its Open NDR aligns with their requirements and network security strategies.

The Bigger Truth

The current state of network security monitoring has become untenable, as there are too many tools, data repositories, manual processes, etc., a mismatch for today's hybrid networks and sophisticated threats. This situation leads to lengthy and complex security operations processes, resulting in longer adversary "dwell time" to move laterally across the network, disrupt operations, or steal valuable data.

Organizations are addressing these challenges by consolidating vendors and integrating tools. This is a good start, but integrating proprietary tools leaves organizations dependent upon individual vendors and their product designs, roadmaps, the quality of their code and support/maintenance, and so on.

This paper presents an alternative to cobbling together proprietary tools based upon broadly distributed and time-tested open source tools (Zeek, Suricata, and PCAP), a powerful model that has proven successful in other sectors. Clearly, there is a cost advantage to open source, but as described previously, Open NDR also offers some functional and operational advantages over proprietary alternatives. Rather than rely on a limited vendor engineering team, Open NDR enjoys constant innovation and improvement from a global community. Open NDR is built on a data-first foundation, allowing organizations to collect the right data to support SOC operations like threat detection, forensic investigations, incident response, threat hunting, etc. Detection rules are provided by the community and can be customized for individual organizations' usage.

Open NDR is built by security professionals for security professionals without any associated profit motivation. Based upon this alone, SOC teams should consider whether Open NDR could be a superior option for network security at their organizations.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188