EDR, NDR, and XDR: Exploring Three Approaches to Threat Detection and Response

STAMUS NETWORKS

INTRODUCTION AND OVERVIEW

To better uncover and address increasingly sophisticated cyber threats, organizations should consider a threat detection and response system as a critical component of their defensive strategy. With a threat detection and response (TDR) program, organizations can be better prepared to swiftly identify and mitigate potential threats, safeguard sensitive data, protect assets, demonstrate compliance with regulatory frameworks, and maintain the trust of their customers. However, it can be a challenge to identify which type of threat detection and response system – or systems – is the best choice for your situation.

In this white paper, we review three modern approaches to threat detection and response — Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Extended Detection and Response (XDR) — and discuss the benefits and challenges of each.

We discuss the importance of a proactive and comprehensive approach to cyber defense that we hope will help readers make more informed decisions about the most effective way to protect their organizations against evolving threats.

UNDERSTANDING THREAT DETECTION AND RESPONSE

Threat detection and response is a proactive approach to cybersecurity that involves continuously monitoring networks, systems, and digital assets to rapidly identify and respond to potential security breaches and cyber-attacks. It can encompass a range of tools, technologies, and processes designed to detect, analyze, and mitigate threats in real time.

By deploying advanced threat intelligence, along with signature, IoC dataset, anomaly, and machine learning detection algorithms, organizations can detect both known and unknown threats such as malware, ransomware, phishing attempts, unauthorized user behaviors, and more.

Modern threat detection and response systems are designed address the shortcomings of existing systems, such as antivirus, host and network intrusion detection systems, primitive network security monitoring, and log management systems.

The significance of threat detection and response in a modern cybersecurity program

Threat detection and response is a crucial component of a modern cybersecurity program. It enables early identification of potential security incidents, helping organizations minimize the impact of cyber-attacks and prevent financial losses, data breaches, and reputation damage. Swift incident response allows organizations to mitigate risks, neutralize attacks, and restore normal operations promptly, minimizing data exfiltration and containing breaches.

Additionally, by proactively assessing their cybersecurity posture, organizations can identify vulnerabilities and implement countermeasures, staying ahead of cybercriminals and reducing potential risks. Robust threat detection and response measures also help organizations demonstrate compliance with regulatory frameworks, avoiding legal penalties related to data protection and privacy.

Beyond Prevention: Moving past traditional approaches

While prevention measures such as network and web application firewalls and zero trust architectures play a crucial role in fortifying an organization's cybersecurity defenses, threat detection and response offers complementary and essential capabilities.

Prevention measures focus on blocking known threats and unauthorized access, but they cannot provide foolproof protection against constantly evolving and sophisticated attacks.

Threat detection and response, alternatively, takes a proactive stance by actively monitoring networks, systems, and digital assets to identify potential security incidents in near-real time. This proactive approach enables organizations to detect both known and unknown threats which may bypass traditional prevention measures.

When an attack does manage to bypass traditional measures, timely detection becomes crucial to minimize the impact and mitigate the consequences.

Upon threat detection, the security team initiates incident response (IR) which includes steps to contain and eradicate the threat and then recover back to normal operations. Using a proactive threat detection and response system, organizations can identify and respond to threats sooner, containing breaches as quickly and effectively as possible.

While traditional prevention measures provide a strong and necessary foundation, threat detection and response systems enhance the overall security posture of an organization. So, combining both prevention and detection/response measures can create a comprehensive and robust defense strategy.

From false alarms to missed threats: Solving the challenges of legacy detection systems

Due to a need for more proactive security measures, cybersecurity professionals have developed numerous threat detection systems that solve some of the challenges of prevention-focused approaches.

Intrusion Detection (IDS) and Network Security Monitoring (NSM) systems, advanced anti-virus software, and modern firewalls all provide greater detection abilities and response tools than their predecessors, but these systems still routinely face challenges of their own.

Simply put, these systems are not advanced enough to serve as effective means of threat detection in an enterprise.

Some of the challenges of legacy threat detection and response systems are:

- **Limited Visibility and Context:** Legacy systems often provide limited visibility into advanced threats and lack context for effective analysis. They rely on predefined signatures and patterns, making them less effective against sophisticated, zero-day attacks and targeted threats that exhibit novel techniques.

- **High False Positives and Negatives:** Traditional systems can generate a high number of false positives and false negatives. False positives occur when benign activities are incorrectly flagged as threats, leading to unnecessary alerts and wasted resources. False negatives, on the other hand, occur when actual threats go undetected, exposing organizations to potential risks.

- **Inability to Detect Insider Threats:** Traditional systems are primarily focused on external threats, often overlooking internal risks posed by insider attacks. Detecting unauthorized access or malicious activities originating from within the organization requires more advanced monitoring and behavioral analysis capabilities.

- **Reactive Rather than Proactive:** Many traditional systems rely on known signatures and patterns, making them more reactive rather than proactive. They can only detect threats that are already identified and have corresponding signatures. As a result, emerging threats and zero-day attacks can easily bypass these systems, leaving organizations vulnerable.

To address these challenges, organizations are increasingly turning towards more advanced and intelligent threat detection and response solutions that leverage machine learning, artificial intelligence, and behavioral analytics to enhance detection accuracy, reduce false positives, and provide comprehensive visibility into both external and internal threats.

THE EVOLUTION OF DETECTION AND RESPONSE

Threat detection and response systems have undergone significant evolutions to keep pace with the growing complexity and sophistication of cyber threats. This evolution has led to the emergence of advanced solutions such as Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Extended Detection and Response (XDR). It is important to note that these modern systems often include the capabilities of traditional approaches (IDS, NSM, firewalls, anti-virus, etc) and expand on them with advanced features.

Understanding Endpoint Detection and Response (EDR)

An endpoint is any device that connects to and communicates with the network. These include laptops, desktops, servers, and tablets. And they may also include video surveillance cameras, industrial control systems, printer, gasoline pumps, automated teller machines, sensors, medical devices, industrial robots, and numerous other devices.

Endpoint Detection and Response (EDR) is a cybersecurity solution designed to protect and secure individual endpoints against advanced threats. A modern EDR records and stores endpoint-system-level behaviors, uses various data analytics techniques to detect suspicious system behavior, provides contextual information, and is able to block malicious activity and provide remediation suggestions to restore affected systems.

EDR solutions offer an improvement over legacy antivirus software by leveraging advanced techniques like behavioral analysis, machine learning, and anomaly detection to detect and respond to threats. These solutions monitor various endpoint activities – like file executions, registry modifications, network connections, and user behaviors – to identify signs of malicious behavior or suspicious activities.

The best EDR solutions can detect both known and unknown threats, including malware infections, advanced persistent threats (APTs), and insider threats.

Endpoint Detection and Response (EDR) use cases

DR systems offer a range of use-cases which enable organizations to effectively detect, respond to, and mitigate threats that can be managed at the endpoint. There are four key applications of EDR:

- **Automated Threat Detection:** EDR agents are installed on individual devices to identify potential threats from an endpoint level. This allows them to detect malware infections, APTs, insider threats, and more.

- **Incident Investigation and Forensics:** By providing visibility into endpoint events, processes, and network connections, EDR allows security teams to reconstruct the timeline of an endpoint-related incident, identify the root cause, and understand the attack methodology. EDR logs and data can be used as evidence during forensic investigations and can aid in determining the extent of a security breach.

- **Mitigation:** By monitoring endpoint processes, file modifications, network connections, and user behavior, EDR tools can identify suspicious or abnormal activities indicative of potential threats. Behavioral analysis capabilities help detect anomalies and deviations from normal patterns, enabling proactive threat detection and reducing false positives.

- **Remediation:** EDR systems can help organizations take immediate remedial action to prevent further damage or attacks. Once a threat is identified, whether by EDR or another integrated system, EDR can automatically trigger a response action to block suspicious IP addresses, isolate compromised end-user devices, or implement access control policies. These actions can help contain the threat, prevent lateral movement, and minimize the impact of a security incident.

The Challenges of Endpoint Detection and Response (EDR)

EDR is a highly capable system, but it does come with some limitations. This is why most experts recommend that organizations develop a comprehensive cybersecurity strategy that includes the other systems described in this paper.

Some of the challenges of EDR include:

- **Endpoint Coverage and Scalability:** Most EDR solutions require agents to be installed on individual endpoints to collect and analyze data. Managing and scaling these agents across 1000s of endpoints can be challenging, especially in dynamic and diverse environments. Ensuring comprehensive coverage and scalability while minimizing performance impact and resource consumption is a key challenge for EDR implementations.

- **Endpoint Agent Compatibility:** In some situations – such as an organization that supports a bring-your-own-device (BYOD) model, an Internet of Things (IoT) environment, military, medical, automotive, or industrial control systems. – it is impossible to install endpoint agents. Many of these environments do not have typical endpoints that are even capable of installing agents. In these situations, the organization must look towards other threat detection and response systems, such as NDR, to provide coverage

- **False Positives and Alert Fatigue:** EDR systems generate alerts based on suspicious or anomalous activities detected on endpoints. However, these alerts may sometimes result in false positives, indicating threats that turn out to be benign. Dealing with a high volume of false positives can lead to alert fatigue, where security teams may become overwhelmed and potentially miss genuine threats amidst the noise.

- **Endpoint Performance and User Impact:** EDR solutions continuously monitor and analyze endpoint activities, which can impact system performance, especially on resource-constrained devices. Heavy resource usage by EDR agents may lead to latency or compatibility issues. Finding a balance between security monitoring and minimizing disruption to end-user experience is a challenge for effective EDR deployment.

- **Privacy and Data Protection:** EDR systems collect and analyze data from endpoints, which can raise concerns related to privacy and data protection. Organizations need to ensure that proper data governance and privacy policies are in place to handle sensitive information. Balancing the need for visibility and security with privacy requirements and regulatory compliance is a challenge that organizations must address when implementing EDR.

- **Skill and Resource Requirements:** EDR systems generate vast amounts of endpoint data that require skilled security personnel to analyze and respond effectively. Organizations need trained professionals with the expertise to interpret EDR alerts, investigate incidents, and perform forensic analysis. The shortage of skilled cybersecurity professionals and the cost associated with building and maintaining a capable security team can pose challenges to maximizing the value of EDR systems.

Addressing these challenges requires careful planning, adequate resource allocation, and ongoing optimization of EDR deployments. Organizations should consider these limitations while implementing EDR solutions and develop strategies to overcome them for successful threat detection and response capabilities. The most proactive organizations seek to fill the gaps in EDR visibility and coverage by using additional threat detection and response systems, creating a more comprehensive and effective cyber defense strategy.

The Power of Network Detection and Response (NDR)

Network Detection and Response (NDR) is an advanced cybersecurity approach that focuses on monitoring and analyzing network traffic to identify and respond to potential threats. NDR solutions are designed to detect malicious activities, anomalies, and indicators of compromise (IOCs) within network traffic in real time.

By leveraging machine learning, behavioral analytics, and signature-based detection techniques, NDR systems can identify and mitigate a wide range of network-based threats, including malware infections, unauthorized access attempts, data exfiltration, lateral movement, policy violations, anomalies, and other suspicious network behaviors.

What sets NDR apart from other threat detection and response systems is its specific focus on network traffic analysis. While Endpoint Detection and Response (EDR) systems primarily monitor and analyze activities on and inside individual devices, NDR solutions use network traffic to gain a more comprehensive view of the organization's entire digital infrastructure. NDR systems extract and analyze network packets, flow data, and metadata to identify potential threats and anomalies, providing valuable insights into network-based attacks.

Additionally, NDR differs from legacy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) by adopting a more proactive and intelligent approach. NDR solutions go beyond simple rule-based detection and signature matching by leveraging advanced analytics and machine learning algorithms to detect sophisticated and evasive threats that may bypass traditional security measures.

NDR systems can provide deep visibility into network traffic, discover unknown threats through anomaly detection, and perform behavioral analysis to identify malicious patterns.

Ultimately, by leveraging the network, NDR systems provide a comprehensive view of network infrastructure to identify attacks, which is vital for effective threat detection and response.

There are two distinct approaches to NDR:

DPI Approach: In this approach, network probes use deep packet inspection (DPI) on live network traffic to feed various detection engines and extract files, flows, packets, and metadata.

Flow Approach: In this approach, a central analytics engine extracts network flow logs from various network devices and applies various algorithms to detect threats and suspicious activity.

The Unique Capabilities of Network Detection and Response

Like EDR, NDR can provide advanced threat detection, and anomaly detection. NDR has the following advantages over EDR:

- **Passive Monitoring:** NDR systems are non-intrusive, inspecting a copy of the network traffic from a packet broker or mirror port. This allows organizations to gain real-time insights and detect potential threats without impacting network performance or disrupting operations.

- **Anomaly Detection:** NDR systems analyze network traffic patterns and behaviors to detect anomalies, helping organizations identify potential security breaches, unauthorized activity, and insider threats.

- **Lateral Movement Detection:** NDR solutions can identify lateral movement within the network, helping organizations detect and prevent the spread of threats from one system or user to another, enhancing overall network security.

- **Agentless Deployment:** Unlike Endpoint Detection and Response (EDR) systems, NDR systems are agentless. This eliminates the need to install software on individual endpoints, simplifying deployment and reducing maintenance and support overhead. This is especially beneficial in environments where there are not typical endpoints, such as an organization that supports a bring-your-own-device (BYOD) model, an Internet of Things (IoT) environment, military, medical or industrial control systems.

- **Forensic Analysis:** NDR systems provide detailed network logs, file extraction, packet capture, and other critical event metadata, aiding in incident investigation and forensic analysis. This helps users understand the attack methodology, support legal proceedings, and prevent future incidents.

- **Threat Hunting:** NDR systems facilitate proactive threat hunting activities by allowing security teams to search for potential threats, identify novel or unknown malware, and uncover malicious or unauthorized activities that may have evaded other security measures.

- **Compliance and Regulatory Requirements:** NDR solutions provide the necessary visibility, logging, and reporting capabilities to meet compliance obligations, ensuring organizations adhere to industry regulations and data protection standards.

- **Network Performance Optimization:** NDR solutions can offer insights into network performance, including traffic patterns, bandwidth utilization, and application performance, helping organizations optimize their network infrastructure and enhance overall efficiency.

- **Network Hygiene Audit:** NDR systems can provide insights into the health of an organization's network systems. By continuously monitoring traffic, organizations can better identify and address potential security risks, misconfigurations, and vulnerabilities.

Challenges of Network Detection and Response (NDR)

Unfortunately, no tool is perfect for every situation. NDR does have its limitations, which is why mature security teams pursue a comprehensive threat detection and response strategy which mitigates the challenges presented by individual systems. It is important to note that while NDR systems do have limitations, the value they provide outweighs the potential impact of those challenges. Some challenges that you might face when deploying an NDR are:

- **DPI Approach:** Those NDRs that require DPI require changes to network infrastructure to monitor network traffic, detect threats, and extract its insights. This may require additional investment in network taps or packet brokers.

- **Flow-based Approach:** When the NDR uses network flow records as the primary method of data ingestion, they are working with severely limited data and therefore are be blind to critical network payloads and metadata, even in unencrypted traffic.

- **Encryption:** NDR systems face challenges in detecting threats within encrypted network traffic. As encryption becomes more prevalent, particularly with the widespread adoption of Transport Layer Security (TLS), it becomes more difficult for NDR solutions to analyze the contents of encrypted communication. In the face of encrypted traffic, many NDRs use advanced algorithmic detection techniques to detect attacks. If payload analysis is critical, organizations can deploy additional measures like SSL/TLS decryption proxies or specialized decryption software that would allow their security teams to inspect encrypted traffic.

- **False Positives and Negatives:** Like any threat detection system, NDR solutions may generate false positives and false negatives. False positives occur when benign activities are mistakenly flagged as threats, leading to unnecessary alerts and potentially diverting valuable resources. False negatives, on the other hand, occur when actual threats go undetected, posing a risk to the organization. Fine-tuning NDR systems to minimize false positives while maintaining high detection accuracy can be challenging, though some modern systems, like the Clear NDR™, provide solutions to this problem.

- **Scalability and Performance:** NDR systems can experience scalability and performance challenges, particularly in large and complex network environments. Processing and analyzing vast amounts of network data in real-time can require significant computational resources. There are NDR systems capable of handling high network traffic volumes, so it is imperative that organizations seek a solution that can handle their specific performance requirements.

- **Limited Endpoint Visibility:** NDR primarily focuses on monitoring and analyzing network traffic. While it provides insights into network-based threats and behaviors, it offers limited visibility into endpoints, such as individual devices and user activities on those devices. This limitation can hinder the ability to detect threats originating from endpoints and may require integration with Endpoint Detection and Response (EDR) solutions for more comprehensive coverage.

- **False Sense of Security:** When choosing to implement any threat detection and response system, it is important to not rely solely on a single system. Whether the organization chooses to primarily use NDR, EDR, or XDR, they should not neglect other crucial security measures and instead seek to integrate multiple systems to maximize coverage

Introducing Extended Detection and Response (XDR)

Extended detection and response, or XDR, has generated substantial interest in recent years - and rightfully so. According to research from Enterprise Strategy Group (ESG), 58% of security professionals said 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.

The purpose of XDR is to provide more comprehensive detection coverage and visibility, consolidate security telemetry/logs, and coordinate auto-response from a single system.

As with many new technology categories, the hope for and hype surrounding XDR has become overblown. As is often the case, each vendor is staking claim to their own 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).

Three Approaches: Open XDR, TDR Extended, and Single Vendor XDR

Three distinct approaches to extended detection and response (XDR) have emerged, each with its own characteristics and implications:

The first approach is known as **Open XDR**, where vendors seek to develop a versatile system that is accepting of various sources of telemetry and seamlessly integrates with different components like EDR, NDR, server logs, etc. Open XDR evolved from the community of SOAR and SIEM vendors, aiming to create an improved version of the traditional SIEM and SOAR combo by providing greater flexibility, interoperability, and functionality.

The second approach, which could be considered "**TDR Extended**", involves vendors extending their existing threat detection and response (TDR) technology, such as EDR or NDR, to incorporate additional capabilities. This extension typically involves integrating diverse telemetry sources into a broader analytics, hunting, and response system.

The goal with this approach is to leverage the foundation of the vendor's established TDR solution and enhance it with additional visibility and more advanced features. This approach allows organizations to build upon their existing investments and expand their threat detection and response capabilities.

The third approach is **Single Vendor XDR**, where a vendor with an extensive portfolio of security solutions repackages their individual point solutions into a comprehensive XDR system. This integrated system is positioned as seamlessly interconnected and capable of delivering exceptional collaboration among its components.

While Single Vendor XDR promises benefits of integration and unified management, it also presents potential drawbacks such as vendor lock-in and the "weakest link" syndrome, where the effectiveness of the entire system relies heavily on the performance of its weakest component.

By understanding these different approaches to XDR, organizations can assess which approach aligns best with their needs, infrastructure, and security objectives, as each approach comes with its own benefits and limitations.

Unique Benefits of Extended Detection and Response (XDR)

Regardless of the approach, XDR seeks to provide a more holistic solution to detect and respond to threats. Aside from general threat detection, XDR has several unique benefits:

- **Correlated Enterprise Visibility:** identify and correlate threat indicators across different platforms, enabling the detection of sophisticated attacks that may use multiple entry points.

- **Centralized Event Triage:** Because XDR integrates the functionality of SIEM and SOAR platforms, it inherently enables its users to prioritize or triage alerts and quickly respond to the most crucial ones. Most XDR vendors assert that their platform helps security teams reduce the noise of alerts by correlating and prioritizing a high volume of alert events into a smaller number of more actionable ones.

- **Centralized incident Response and Investigation:** XDR promotes greater visibility into different types of environments including the network, endpoints, and the cloud. This visibility, paired with telemetry from different sources and features for automated analysis, allow security teams to quickly and easily establish where a threat originated, how it spread, and what other users or devices might be affected. This is important not only for removing threats, but also for identifying vulnerabilities within the organization that need to be patched.

- **Threat Hunting:** With XDR's advanced analytics and machine learning capabilities, security teams can spot patterns, anomalies, and indicators of compromise across endpoints, networks, and cloud services. By identifying threats at their early stages, organizations can respond swiftly, contain the attack, and minimize potential damage.

Limitations of Extended Detection and Response (XDR)

While XDR promises a single system that provides more comprehensive detection coverage and visibility, consolidates security telemetry/logs, and coordinates auto-response, it too comes with limitations. Most of the challenges associated with XDR depend upon the approach taken:

- **The open approach** requires extensive integration with various sources of telemetry, including EDR, NDR, and server logs.

- **The "TDR extended" approach** nearly always provides incomplete coverage, and its coverage tends to favor the original threat detection and response approach which was 'extended' to create the XDR.

- While **Single Vendor XDR** promises the benefits of built-in integration and unified management, it also presents potential drawbacks such as vendor lock-in and the "weakest link" syndrome, where the effectiveness of the entire system relies heavily on the performance of its weakest component.

- Because XDR aims to incorporate functionality currently delivered by multiple systems, all approaches can require the organization to perform a **wholesale rip-and-replace** of the entrenched system and a retraining of SOC personnel.

SUMMARIZING ALL THREE APPROACHES

Each of these systems can bring a security team substantial benefit. And each bring challenges of their own. The table below summarizes these:

	Good	Limitations
EDR	Endpoint visibility & detection Rapid threat remediation Behavioral analytics Endpoint-level forensic analysis Rollback	Requires agent False positives and alert fatigue Performance impact Privacy and data protection Skill and resource requirements
NDR	Visibility into single source of truth Passive monitoring Lateral movement detection No agents required Complete view of the 'crime scene'	DPI approach requires installation Flow approach extremely limited data Encrypted traffic Scalability and performance Limited endpoint visibility
XDR	Correlated enterprise visibility Cross environment threat detection Centralized event triage Centralized response and investigation	Open approach requires integration TDR extended approach is incomplete Single vendor approach - lock-in Requires rip-and-replace and retraining Still requires SIEM

EDR: Endpoint Detection and Response focuses on individual devices within the network, such as computers or servers, providing deep visibility into endpoint activities and detecting potential threats at the device level. EDR offers benefits such as detailed forensic analysis, threat hunting capabilities, and rapid incident response. However, it also suffers from limitations including its requiring agents to be installed on every endpoint, its susceptibility to bypass, and its limited scope to detect threats that traverse across multiple endpoints or network boundaries.

NDR: Network Detection and Response excels in providing visibility into network traffic, detecting suspicious activities, and identifying potential threats in real time. Its benefits lie in its being non-intrusive and relatively easy to deploy and its ability to monitor network traffic across the entire infrastructure, enabling the identification of network-based threats and facilitating rapid response. However, NDR can have limitations in terms of its focus solely on network data, which may not capture threats at the endpoint level.

XDR: Extended Detection and Response, the newest of these TDR systems, seeks to take a more holistic approach by incorporating several sources of telemetry to achieve cross-environment visibility. XDR can enable organizations to identify and correlate threat indicators across different platforms, enabling the detection of sophisticated attacks that may use multiple entry points. It is important to note that while XDR often relies on NDR and EDR systems to perform optimally, and as a result it is not yet able to completely replace those systems.

When these three systems work together, organizations can achieve a comprehensive approach to threat detection and response. NDR provides network visibility, EDR focuses on endpoint protection, and XDR integrates the insights from both domains while incorporating additional telemetry sources. This collaboration allows for enhanced threat detection, rapid incident response, and a more proactive defense posture, ultimately leading to a more robust and comprehensive cybersecurity strategy.

KEY CONSIDERATIONS

In summary, to enhance threat detection and response capabilities, organizations should consider the following:

1. Organizations can strengthen their overall cybersecurity posture and effectively protect against a wide range of threats by incorporating one or more of these technologies.

2. Adopt a comprehensive and integrated approach to cybersecurity, leveraging multiple layers of defense and integrating various threat detection and response systems to achieve maximum coverage and visibility.

3. While incorporating all three is ideal, organizations can achieve nearly complete coverage with just EDR and NDR.

4. XDR can extend visibility and simplify response by consolidating the orchestration of available telemetry and remediation mechanisms.

5. Prioritize ongoing evaluation of security systems to ensure they remain effective against evolving threats. Regularly assess system performance, conduct security assessments, and stay informed about emerging threats and technologies.

6. Recognize the importance of people and processes alongside technology. Invest in skilled security professionals, establish clear policies and procedures, and provide continuous training and awareness programs to empower your team and enhance incident response capabilities.

By considering these measures, organizations can strengthen their overall cybersecurity posture and effectively protect against a wide range of threats.

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

