The Latest Trend in Network Cybersecurity: NDR

Contents

Network Detection and Response is the latest trend in network-based cybersecurity. NDR follows years of product categories and three-letter algorithms to help define how an enterprise should consider defending itself from cybersecurity. Over the years security has been defined by IPS, IDS, DLP, ATD, ADR, NAV, NTA, and more.

Fidelis has participated in magic quadrants, waves, market studies, and terminology changes since our first network cybersecurity solutions in the mid-2000's. NDR culminates years of research and software advances to bring together the basic elements of security requirements: Detection and Response.

What is NDR?

Network Detection and Response is similar to more recent trends in network cybersecurity, including Network Traffic Analysis (NTA) and Network Analysis and Visibility (NAV). While all three terms emphasize detection, NDR elevates the role of response on the network. This is an extremely different message and cybersecurity professionals need to understand the difference.

Detection uses network data to provide visibility into network data. Based on visibility a variety of techniques can be applied to detect cyber threats and risks. These techniques include signature analysis, malware detection, sandboxing, indicators analysis, email security, web security, machine learning and AI, deception, and asset risk analysis. Detection via traffic analysis or visibility remains the keystone of NDR.

NDR proposes that *Response* is equally important to the role of security. Detection can be judged in a sliding scale between false positive and false negative results. Too many detections can inundate the security team with too many alerts, too much information, and a feeling of too many false positive detections. Too few detections lead to a false sense of security where no-news is good-news, masking vital information required to truly secure the enterprise.

Response is an automated method to analyze detections to determine – what happens next? Providing the answer of "what next" with reports and automated analysis based on network visibility, is the key to NDR.

Response within Network Traffic

NDR begins with detections. Network traffic needs to analyze traffic, provide visibility, and detect security problems in the form of an alert or an anomaly. Once a detection is determined, the security team can spend hours reviewing every detection or it can use automated response to determine the highest priority actions as opposed to a triage of thousands of alerts.

Response requires several forms:

- **PREVENTION**
  Let's begin with the most basic form of network response — prevention. In the network, prevention includes packet or session dropping, TCP resets, email quarantine, and web blocking or redirection. In the simplest form, prevention is based on URL filters, email gateways, firewalls, and Intrusion Prevention. However, modern threats can evade these simple solutions so a more granular approach is required.

  Detection must be based on inbound-outbound (north-south) and internal (east-west) network traffic. Furthermore, analysis must be based on the files, scripts, users, and protocols that comprise the traffic – no matter how embedded, encapsulated, and encrypted. Prevention must be based on the same granular approach that allows prevention of detected data without compromising the business objects of the enterprise.

  Email and Web solutions are also important for network response. Email can quarantine data for analysis and web data can be redirected to secure locations. However, attackers live in the network stack beyond email and web, so a solution based on email and web will not adequately detect and respond to cyber-attacks – an all-ports; all-protocols approach is required to support NDR.

- **AUTOMATED INVESTIGATION**
  What happens when a detection is found? Studies have shown that an advanced attack requires approximately 18 minutes from the time of the initial detection to an undistinguishable event.

  As the attacker begins to hide in plain daylight, they can mask their objectives and behave within the normal user patterns within your enterprise. The lost opportunity to react can lead to months of undetected dwell time.

  Sometimes, prevention can alleviate the problem, however prevention measures are not always available due the risk of blocking business operations. In order to react quickly and effectively, automation is required.

  The role of the playbook is a key concept because it allows for automation of investigation. Detection of anomalies, machine learning and artificial intelligence, encrypted traffic analysis, and DNS detection all lead to several possibilities. Is the anomaly the result of nefarious operations or justified within some change in user behavior? Is traffic analysis the result of a change in a web site or normal operations of a behavior that needs to be investigated? In the detection of deception, is the cause an insider threat or a misconfigured system? These questions can consume hours of analyst time, and repeated infractions leads the security team to ignore the signals because analyst time is a precious resource.

  The use of playbooks provides the required automation to investigate the signals over all possible domains in the environment – multiple network segments can be queried, and user behaviors can be investigated. The analyst is presented with automated analysis, including remediation techniques that lead to file deletion, system rollback, endpoint isolation, firewall and IPS modifications, and DNS blacklisting and decoy investigation.

- **INCIDENT ANALYSIS**

  Detections are often granular events within the network. Such events can generate many thousands of detections which create an unending list of investigations.

  An incident is a higher-level analysis of the detections where many detections can be correlated to reduce the analysis on the response team. Examples include incidents on an asset or a user; analysis to global scope of similar detections; and anomalies connected to other detections across the enterprise

  When response is rooted in detection analysis, the response team is often inundated with information. Incident analysis can eliminate the noise that allows the security team to focus on the most important incidents.

- **EFFICIENT ANALYST TOOLS**

  The terms NTA and NAV emphasize the ability to detect threats within network traffic. Detection combines many methods including the latest trend to apply data science to comprehend the data created by advances in network visibility. Detection of anomalous activity, probability of compromise, and the analysis of known and unknown data can produce high confidence and actionable alerts.

  However, many of these detections are just noise signals. Anomalies, probabilities, and unknown data can lead to malicious outcomes, but can also detect justified user behavior. The ability to distinguish malicious outcomes requires aggressive response behaviors.

  The distinction between noise and efficiency is the ability of the visibility provided in response to a detection. The analyst must quickly answer the relevant questions – who, what, where, when, and how. The answers lead to investigations as well as tuning to correct and adjust data models within the enterprise.

  If your response to a detection is to peruse log files and to correlate data over multiple tools, then you are suffering without efficient response. Rather, NDR must emphasize the response equally to the detection side.

- **RETROSPECTIVE ANALYSIS**

  Within the Detection part of NDR, visibility is an essential component of NDR. In this context, visibility includes the ability to see and to extract metadata of all network activity. The response aspect requires solutions that can hunt and automate information that occurred in the past.

  New information becomes available constantly through new detections – not only in your enterprise, but also by data available from industry and internal experts that may pertain to your vertical industry, your geography, and to your enterprise. The ability to connect the dots between current events a past behavior is an important aspect of NDR.

  Past behavior is based on time. If your solution collects historical data, you are ahead of the curve. However, is your data sufficient? Are you struggling to store 7-days of information when 60 - 90 days or more is required? Are you saddled with net flow data and not able to reconstruct the full network data including file names, file attributes, embedded files, protocol attributes, user attributes, machine and asset data, encrypted data attributes, and more? The requirement is to ascertain all relevant information to understand root cause of current events to take the appropriate actions.

  Automation is a key element of retrospective capabilities. When new information is available, automation can detect past occurrences without requiring manual intervention. New IOCs can be easily digested into automated response, which provides valuable information within your response capabilities.

- **PROACTIVE CAPABILITIES**

  Perhaps the most important aspect of NDR is to determine security gaps in your environment and to correct your posture before an attack occurs. Proactive capabilities include several aspects to both ascertain your risk profile and to improve. These capabilities include:

  - **Decryption:**

    More than 80% of typical network traffic is encrypted. Attackers use decryption to hide in plain sight, evading nearly all the detection capabilities of an NDR solution.

    Some NDR solutions offer encrypted analysis capability to detect some aspect of malicious behavior on the network. These detections can be valuable, but the lack of visibility and response leads to minimal effectiveness of NDR. The analyst is left to peruse log files to attempt to understand how the attack started, the scope of the compromise, and what data was stolen.

    Decryption of TLS is an essential tool in NDR. It allows visibility to all network traffic, while allowing configuration to secure data for privacy concerns. Use of decryption can be applied by the analysts – when detections warrant further investigation decryption can be an important tool in your response arsenal.

  - **Cyber Terrain:**

    The discussion about network visibility includes the ability to detect and identify assets on the network. The collection of all computer systems within the enterprise constitutes the cyber terrain.

    Terrain is the collective environment of all assets. It includes the identification of assets, the communication paths and protocols within the environment, analysis of new assets that appear on the network, and the analysis of the environment, including incidents and risks.

    Network analysis is the sole source of data in the environment. It can include identification of assets with and without endpoint capability as well as any other security coverage – including email gateways, web gateways, email, firewalls, and more.

    In order to create a proactive security environment, you need to begin with an inventory of all assets. In other words, the cyber terrain.

  - **Risk:**

    The analysis of risk follows the cyber terrain. If you can detect assets and users, you can now assess risk to the organization. A risk assessment begins the understanding of security gap analysis and corrective actions.

    Asset risk includes:

    - Vulnerability analysis: Frequent analysis of all known vulnerabilities.
    - Alert data or threat detections: Current events that include network and endpoint detections and how they related to the severity and priority.
    - Coverage: Understand where assets are protected by endpoints, firewalls, email gateways, decoys, and all other security tools that estimate the risk in terms of security awareness.
    - Attack frameworks: The ability to relate all detections toward an attack framework, such as MITRE ATT&CK helps to align risk toward current events. Relying on frameworks can help to estimate the highest priority of risk.

  - **Risk simulation:**

    Building on asset risk, simulation can be applied. Risk simulation can be covered by red-team or blue-team analysis. The red team is performed to estimate an attack, beginning from a compromised host to evaluate network communication that can expand the attack laterally within the enterprise.
    The blue-team simulation begins from analysis of important or high value assets to estimate how an attack may comprise these assets.

    Based on a simulation, the enterprise can determine security gaps that need to be addressed to improve the environment. In this analysis, the response component of NDR is geared toward improvement, not necessarily working from detections.

Summary

Network Detection and Response provides cybersecurity professionals with a hope to combat threats. The first step is to detect cyberattacks – without a detection, criminals can attack your environment, steal information, and cause financial and political harm.

However, robust response is equally important. The role of response provides efficiency to cyber operations. To analyze current practices and to remedy security gaps prior to an attack; to view data as incidents rather than individual alerts; to automate actions as a result of incident awareness; to witness all network activity by relying on efficient tools; to automate retrospective analysis; and by providing holistic visibility into your cyber terrain.

Detection solutions without the ability to respond, just add noise. Operational efficiency is gained by NDR.

Contact Us Today to Learn More

Fidelis Security | 800.652.4020 | info@fidelissecurity.com

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure.

Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.