A PRIMER ON ENDPOINT DETECTION & RESPONSE (EDR)

Although computer system security has been around for decades, endpoint detection and response (EDR) is still a relatively new term. It also goes by the name endpoint threat detection and response (ETDR), but both expressions indicate the same goal: to identify and counter threats that occur at endpoints of a network.

EDR provides continuous monitoring and response capabilities that can detect, respond to, and prevent advanced threats to system security. But what makes EDR different from other standard threat solutions like antivirus or firewalls? The answer lies in visibility and advanced capabilities that succeed in identifying and addressing threats where other standard security measures frequently fail.

How Other Security Solutions Fail

Modern threats are becoming more advanced by the day, practically guaranteeing that even the most robust systems will experience a breach at some point or another. Meanwhile, standard security measures like antivirus software are fairly easy for skilled adversaries to sidle past, and more importantly, they allow silent breaches. Attackers can gain access to the networks while silently evading such defenses, causing no security alerts that signal a breach.

This silence allows the adversaries to not only get through defenses, but also stay inside. They can even gain opportunities to create backdoors that allow them to return at will, making them essentially invisible. EDR removes this invisibility cloak to reveal malicious or suspicious incidents

that would otherwise remain unseen.

Primary Capabilities of EDR

Detection Through Endpoint Visibility

The primary security capability that EDR provides is visibility, specifically at endpoints such as desktops, laptops, tablets, servers, and even smaller personal devices like smartphones, smartwatches, and digital assistants. These endpoints communicate back and forth with the network while connected, but they are also weak points that cyber attackers tend to target.

The typical IT department usually manages thousands of endpoints, making it crucial to maintain visibility of the associated changes and events they go through. Without visibility, the organization can't see what's happening at the most vulnerable points in their network. Being able to see these parts of the system means being able to know what exactly occurred during a breach, how to fix it, and how to prevent it in the future.

EDR achieves the necessary visibility by recording activities at the network endpoints in real-time. It monitors information such as connections, activity volume, processes, and data transfers for signs of irregular activity. If a threat slips past an endpoint prevention component such as antivirus software, then EDR still detects the activity and alerts the security team. The team can then work to contain and shut down the attack.

Response Through Vigilance and Alerts

An EDR solution comes with pre-configured rules to help identify security breaches and attacks via monitored data. When it detects a problem, the rules trigger one or more of several possible automatic responses, such as logging off the user or sending alerts to the security team. Ultimately, the goal is to detect a threat or an attack before it becomes a full breach, responding to it rapidly to prevent it from developing any further.

Some response methods include incident response plans and threat hunting. The former is a plan put in place to help an organization define what exactly constitutes a threatening incident. Then, it provides a clear process that the team should follow. The main parts of an incident response plan include preparation, identification, containment, eradication, recovery, and result evaluation. An EDR can form an integral part of planning and executing such plans.

Threat hunting is a more proactive approach involving seeking out threats before the successful execution of an attack. It forms part of general threat detection, but it is specifically an early stage of the process that focuses on identifying threats as early as possible before they even create a breach.

The methodology starts with an assumption that adversaries already gained access to the system and may try to spread laterally if given the opportunity. The security team typically forms a hypothesis about the type of threat based on various data and testing from EDR. To test the hypothesis, an investigation starts based on indicators of attack (IOAs) and indicators of compromise (IOCs). These indicators, particularly IOAs, come from behavioral protection approaches of EDR that use baseline data to detect suspicious activity before any adversaries have the chance to complete an attack.

Prevention Through Data Analysis

As EDR tools gather massive amounts of data, they use advanced analytics and sometimes machine learning and artificial intelligence (AI) to sort through it and detect irregularities that need to be addressed. Even if there is no immediate threat, EDR stores the data gathered from endpoints for further analysis and investigation. It can use this information to create a baseline against which it can compare new data, working to create the optimal response plan.

The combination of real-time analytics and investigation of data from previous threats and breaches allows security teams to better understand both their system and those trying to infiltrate it. The methods that attackers use frequently act as a sort of signature that EDR can recognize. Even if factors such as IP addresses, domain numbers, and registry keys change, the methods that adversaries use often remain constant over time. Learning to recognize those behaviors can prove key to detecting otherwise variable threats.

Key Features to Look for in EDR

Not all EDR tools are the same, so you should keep an eye out for specific features that interest your organization. For example, you may desire **strong capabilities for incident response** and **threat hunting** as discussed above.

Other characteristics of an ideal EDR solution are a **high level of protection** but a **low level of investment and effort**. There is always a delicate balance between these two sides of the coin for any service, but in the case of EDR **machine learning and AI** can help considerably. Such integrated intelligence improves speed and thoroughness, allowing security teams to detect and remediate even the most sophisticated threats.

Through the use of intelligent tools, EDR should compile a **threat database**. The data collected from endpoints should be evaluated with a variety of analytic techniques that include behavioral approaches focusing on IOAs rather than IOCs. After all, the goal is to avoid compromise in the first place by detecting the attack before it becomes a breach. The analysis should use context to determine a baseline for comparing new data and searching for abnormalities.

The EDR should also employ **intelligence and insight** to provide context on the adversary. Determining who the attacker is, motives for the strike, methods of infiltration, and other information about the attack can aid all steps of the process.

With regards to speed, **real-time visibility** of all network endpoints is crucial for effective EDR. One good option is to look for a cloud-based solution. By using the cloud, you can ensure zero impact on the endpoint while still making sure that other capabilities such as searching, analysis, and investigation of data remain accurate in real-time.

If the day comes where an adversary gets through network defenses, EDR with the above features will promptly address the problem. It will ensure that the breach won't be silent and will provide immediate options for a strong response, allowing your organization to quickly return to business.