Hi Beatrice,

Thank you for the post, it was wonderful to view your thoughts on how Endpoint Protection Software protect critical endpoints and servers from known threats. To build on endpoint protection, endpoint detection and response (EDR) takes a step further.

Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is a comprehensive solution that is built on the principles of continuous real-time monitoring and collecting of endpoint data in coherence with automated response and analysis based on rules.

The primary functions of an EDR security system are to monitor and collect activity data from the device which detected a threat, analyse this data and identify threat patterns, automatically respond to such identified actors in order to eliminate or contain them, and lastly, notify security personnel, in order to research potential identified threats and search for suspicious activity.

Even though, modern antivirus systems are capable of identifying and blocking a large number of new form malwares, threat actors are continually developing them to be a step further. For instance, fileless malware—a relatively new concept— functions by operating entirely inside the memory of the machine, thus evading malware signature scanners.

To aide in the efficiency of an EDR, threat intelligence services provide an organisation with access to a worldwide database of current threats and their indicators. This collective intelligence enables an EDR to detect more exploits, particularly multi-layered and zero-day assaults.

Moving into the mindset of a threat actor, MITRE’s ATT&CK framework identifies cyberthreats according to a variety of variables, including the strategies employed to compromise an IT system, the sort of system vulnerabilities exploited, the malware tools utilised, and the cyber groups involved in the assault. The approach focuses on discovering patterns and traits that persist despite modest modifications to an attack.

**References**

* FireEye. (n.d.). Endpoint Detection and Response (EDR). Available from: https://www.fireeye.com/products/endpoint-security/endpoint-detection-response.html [Accessed 22 Apr. 2022].
* Palo Alto Networks. (n.d.). What is endpoint detection and response (EDR)? Available from: https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr [Accessed 22 Apr. 2022].
* www.mcafee.com. (n.d.). What Is Endpoint Detection and Response? | EDR Security | McAfee. Available from: https://www.mcafee.com/enterprise/en-in/security-awareness/endpoint/what-is-endpoint-detection-and-response.html [Accessed 22 Apr. 2022].