Thank you, Thomas, for the valuable information, regarding the Endpoint Detection Response software (EDR), Cybersecurity and Infrastructure Security Agency (CISA) designated endpoint detection response software as a critical component for cybersecurity (CISA, 2021).

According to (Infocyte, 2021) EDR software is designed to protect endpoints from malware and malicious activities, in addition, it collects and monitors any data related to the potential security threats, which could be analyzed to discover the main and root cause of the cybersecurity issues.

(Karantzas & Patsakis, 2021) through their empirical assessment for EDR systems show that no EDR software can efficiently detect or prevent the Four attacks under test, the DLL attack sideloading was the most successful attack which all of EDR systems failed to detect, moreover, EDR software could be blinded by attacking their core.

In summary, no one EDR software or solution can provide full protection for an organization, otherwise, depending on a wide range of security tools, procedures, policies, and regulations may help increase the security of an organization.

References

CISA (2021) Executive Order on Improving the Nation’s Cybersecurity. Available from: https://www.cisa.gov/executive-order-improving-nations-cybersecurity [Accessed 1 October 2021]

Infocyte (2021) 10 Considerations Before Buying an Endpoint Detection and Response (EDR) Security Solution - Part 1. Available from: https://www.infocyte.com/blog/2020/01/09/10-considerations-before-buying-an-endpoint-detection-and-response-edr-security-solution/ [Accessed 1 October 2021]

Karantzas, G. & Patsakis, C. (2021) An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. Journal of Cybersecurity and Privacy. *Journal of Cybersecurity and Privacy* 1 (3): 387-421. Available from: https://www.mdpi.com/2624-800X/1/3/21/htm [Accessed 1 October 2021]