ANTIVIRUS SOLUTIONS AND THEIR VARIATIONS: EDR, MDM, SIEM

Yevheniev A.M., Shulika K.M.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Antivirus solutions have long become an integral part of the modern cyber world. They help protect computers and networks from malicious software and other threats. However, with the development of technologies, many variations of antivirus protection have emerged, including EDR, MDM, and SIEM [1, 2].

The purpose of the report is to analyze each of these options, their features, and benefits.

EDR is an endpoint protection technology that includes monitoring, detection, response to threats, and recovery after incidents. It extends the capabilities of traditional antivirus products by adding advanced analysis and tracking of anomalous behavior on user devices. EDR provides companies with the ability to detect new attacks that have bypassed traditional antivirus products and quickly respond to security incidents [1].

MDM is a mobile device management system that allows organizations to control access to corporate resources, security settings, installation of antivirus programs, and updates on employees' mobile devices. Using MDM helps to increase the level of protection for mobile devices and reduce the risk of data loss or theft.

SIEM is a comprehensive solution for monitoring, analyzing, and managing IT infrastructure security. It collects and analyzes data from various sources, such as antivirus programs, firewalls, intrusion detection systems, and other security tools. SIEM is used to detect anomalies, track changes in the network, and correlate events for early detection and response to cyberattacks.

Modern antivirus solutions and their variations, such as EDR, MDM, and SIEM, provide different levels of protection against cyber threats. Using these technologies helps organizations protect their infrastructure, data, and users from malicious software and other malicious actions. However, it is important to understand that there is no universal solution that would provide complete protection against all types of threats [3, 4]. Therefore, it is essential to use a comprehensive approach to security, which includes various technologies, products, and practices to adequately respond to constantly changing threats in cyberspace.

References

1. Antonishchev, V. V., & Kravchenko, A. V. (2020). Analysis of antivirus technologies for corporate networks. Bulletin of V. N. Karazin Kharkiv National University. Series "Radiophysics and Computer Systems", (22), 101-106.

2. Gerasimov, V. O. (2019). Methods and technologies for protection against malicious software. Cybersecurity: education, science, technology, 2(6), 36-46.

3. Rostyslav G., Martovytskyi V., Sievierinov O., Sukhoteplyj V., Soloviova O., Kortyak Y. (2020). A Method for Identifying and Countering HID Attacks-Virus Detection in BMP Images. International Journal of Emerging Trends in Engineering Research, Volume 8, (7).

4. Sievierinov O., Ovcharenko M., Vlasov A. (2021). Enterprise Security Operations Center. COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES.