Student Name: Nathan Mack

Research Topic: "Quantifying the Effectiveness of Microsoft Defender for Endpoint Against Zero-Day Exploits."

Research Objectives:

1. Assessing detection rates
2. Analyzing response times
3. Evaluating false positive/negative rates
4. Assessing adaptive capabilities

Research Description:

The study's goal is to objectively evaluate the efficiency of Microsoft Defender for Endpoint (formerly Windows Defender Advanced Threat Protection (ATP)) against zero-day exploits, which are particularly complex cybersecurity threats due to their unknown nature. My research will have four main objectives. First, it aims to assess MDE detection rates by evaluating historical data on known zero-day vulnerabilities. The percentage of successful detections and false positives is calculated to measure the detection mechanism's accuracy and reliability. Second, the study examines response times in order to determine how well MDE responds to identified zero-day exploits. The third purpose is to evaluate false positive and false negative rates, with the goal of quantifying the occurrences of both types of errors and assessing their impact on the tool's overall performance. Finally, the research evaluates MDE's adaptive capabilities, namely its capacity to evolve and combat emerging zero-day exploit techniques over time. Through these objectives, my study will seek to give a comprehensive and data-driven knowledge of the tool's performance in mitigating one of the most powerful cybersecurity threats.

Deliverables: Detailed charts and graphs presenting detection rates, response times, and false negative/positive rates to illustrate Microsoft Defender for Endpoint's performance in various simulated attack scenarios.

Rough Research Timeline:

February – Digging into historical evidence on the efficacy of MDE and reading into professionally measured detection rates and response times.

March – Performing my own tests in a virtual Windows environment with simulated attack scenarios and measuring and collecting data.

March/April – Compiling results of research and testing into a well-documented paper.

References:

https://www.optiv.com/sites/default/files/2020-07/ThoughtLeadership_R%26D_Microsoft%20Defender%20ATP_White%20Paper_Whitepaper.pdf

https://www.jstor.org/stable/j.ctv2k88t3d

https://www.techtarget.com/searchsecurity/definition/Windows-Defender-Advanced-Threat-Protection-ATP#:~:text=Microsoft%20Defender%20for%20Endpoint%20%2D%2D,and%20respond%20to%20security%20threats.

https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/?view=o365-worldwide

https://www.bluevoyant.com/knowledge-center/microsoft-defender-for-endpoint-architecture-features-and-plans

https://jeffreyappel.nl/microsoft-defender-for-endpoint-series-what-is-defender-for-endpoint-part1/