SECTION: COMPUTER SCIENCE.

SEKCJA: INFORMATYKA.

How to cite: Opanovych, M. (2024). Enhancing Active Directory Security Monitoring with Sysmon. *The Science of Tomorrow: Innovative Approaches and Forecasts.* (pp. 60-64). Futurity Research Publishing. https://futurity-publishing.com/the-science-of-tomorrow-innovative-approaches-and-forecasts-archive/

Enhancing Active Directory Security Monitoring with Sysmon

Maksym Opanovych [1]

[1]*Postgraduate student of the Department of Information Security, Lviv Polytechnic National University, Lviv, Ukraine*

Accepted: March 22, 2024 | **Published**: April 19, 2024 | **Language:** English

Abstract: This study explores the integration of System Monitor (Sysmon) with Windows Event Logs to enhance security monitoring in Active Directory (AD) environments. The findings from comparative analyses show that Sysmon, when properly configured, significantly refines the detection process by reducing log noise and focusing on pertinent data, thus enhancing the effectiveness and efficiency of the monitoring system. The study confirms that combining Sysmon's targeted logging with the comprehensive logging of Windows Event Logs provides a robust security monitoring solution that is both efficient in processing and effective in threat detection, crucial for protecting against the evolving landscape of cyber threats.

Keywords: Active Directory, APT, Sysmon, Malware, Windows Event Logs, Cybersecurity.

Introduction

The majority of Windows-based IT systems rely on Active Directory (AD) as their foundation for managing users and resources. The management of policies, authorization, and authentication is made easier by this unified system. But because of its critical function, it is also a prominent target for cyberattacks. Organizations' Active Directory systems becoming increasingly complicated as they grow and change, making it more difficult to properly monitor them for security risks. The security of Active Directory is critical to the overall security posture of any organization using it. The challenges in monitoring and securing this complex system are considerable, ranging from its scale and essential nature to the

sophisticated threats targeted at it. Overcoming these challenges requires a robust strategy that includes advanced monitoring tools, rigorous compliance practices, and a proactive approach to threat detection and response. As cyber threats evolve, so must the strategies and tools used to combat them in Active Directory environments. This paper delves into the multifaceted challenges of securing Active Directory environments and the implications of these challenges on organizational security.

Research Results

Increasing the security monitoring of Active Directory (AD) is not only advantageous but also required, considering how sophisticated and important it is for overseeing network-wide rules and access controls. One powerful tool in Microsoft's Sysinternals package, System Monitor (Sysmon), offers comprehensive logging capabilities that can handle many of the inherent security issues that Active Directory environments provide. Smiliotopoulos, Barmpatsalou, and Kambourakis (2022) investigate how Sysmon can be used to improve Active Directory's security posture and successfully address a number of issues.

Sysmon extends beyond traditional logging methods by capturing detailed information about process creations, network connections, file access, and registry changes—events that can signify malicious activity. Each log entry includes comprehensive data such as timestamps, user context, and process identifiers, which are crucial for deep analysis.

Sysmon can be finely tuned to log specific types of activities, which helps in focusing on potential security breaches without getting overwhelmed by routine log data. For instance, Sysmon can be configured to track any alteration in Group Policy Objects (GPOs), which directly affect AD configurations. By monitoring these changes in real time, Sysmon helps in quickly identifying and responding to unauthorized modifications that could compromise AD integrity.

Privilege escalation is a critical threat in AD environments. Sysmon’s ability to log detailed information about process creations and network connections helps in identifying unusual activities that could indicate attempts at escalation.

Sysmon’s event logging includes the execution of scripts, remote procedure calls, and other processes that could be used by an attacker to gain elevated privileges. By creating alerts for certain high-risk events, such as the use of privileged accounts to perform unusual tasks, administrators can detect and mitigate potential breaches before they escalate.

Security teams are able to create a baseline of typical activity and then identify variations from this pattern by examining logs generated by Sysmon. Investigating whether certain behaviors are normal or indicative of insider misuse, for instance, may be prompted by Sysmon's recording of excessive file accesses or anomalous after-hours logins (Bahniuk et al., 2023).

The detailed data provided by Sysmon improves the effectiveness of incident response efforts by reducing the time needed to understand the scope of an issue and take appropriate action.

Sysmon logs include the hash values of executables and scripts run on the system, which can be vital for forensic analysis following an incident. If an unknown or unauthorized piece of software is found to be executed, Sysmon's logs can help trace its origin and determine its impact on the network.

Sysmon’s output is highly compatible with other security tools, including SIEM systems, which play a critical role in comprehensive security monitoring strategies. This compatibility allows for an integrated approach to security that enhances overall threat detection and response capabilities. By feeding Sysmon logs into the SIEM system, all security-related data can be analyzed in a centralized location, making it easier to correlate events and detect patterns that may indicate sophisticated cyber-attacks or systemic issues within Active Directory.

Sysmon assists in maintaining compliance with regulatory standards by providing detailed and tamper-proof logs that can be used to demonstrate adherence to security policies and procedures.

When it comes to modifications made to AD objects and configurations, the unchangeable logs from Sysmon provide a trustworthy audit trail. In order to demonstrate that suitable security measures are implemented and functioning, these logs are essential during audits. Significant security dangers are posed by advanced persistent threats (APTs) and zero-day exploits, especially in complex setups like Active Directory-managed environments (Xuan and Huong, 2022).

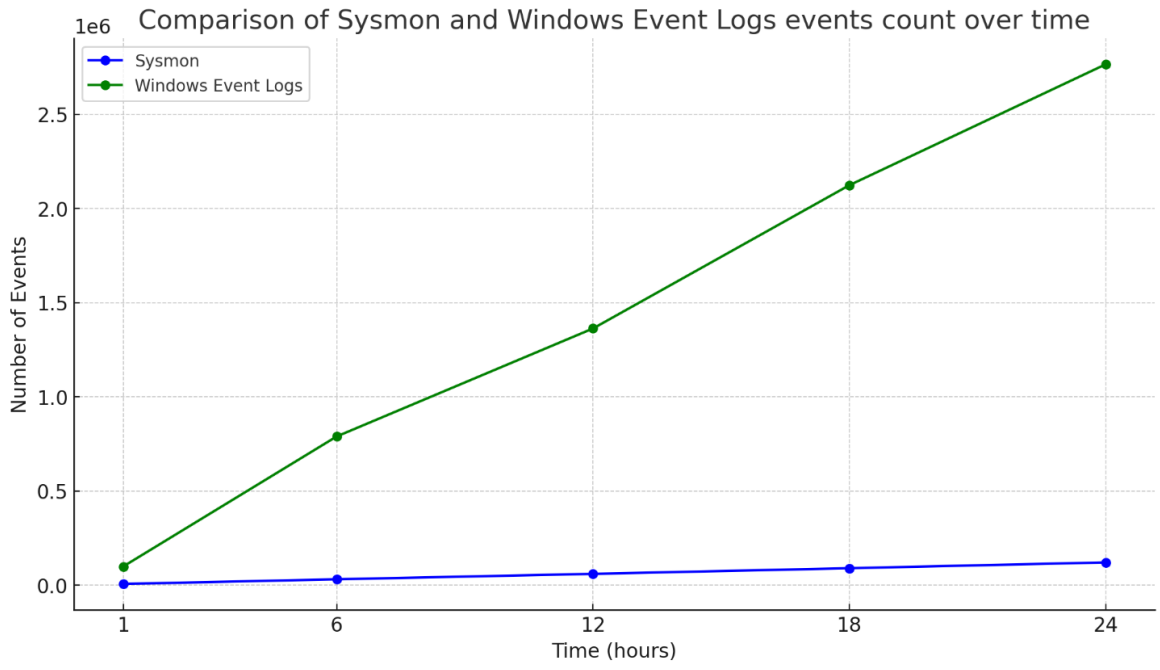
Sysmon's event filtering and logging capabilities make it an excellent tool for setting up anomaly detection rules. By flagging activities that deviate from established norms, Sysmon helps in the early detection of APTs and mitigating damages from zero-day exploits.

In our testing infrastructure, we have meticulously configured both the Windows Audit Policy and Sysmon to enhance our capabilities for detecting malicious activities effectively. The Windows Audit Policy has been set up to log a comprehensive range of system events to ensure broad coverage. Conversely, Sysmon has been configured with a focus on security-related events, such as network connections, process creations, and changes in file creation timestamps, which are critical for identifying potential security incidents early. The hash of the process image files, which might be essential for malware research and detection, is one of the many details about these occurrences that Sysmon is configured to record. As the graph (Figure 1) clearly shows, Sysmon logs fewer events than Windows Event Logs, but it collects a lot more essential information on security monitoring. Targeted logging improves the detection of security threats by concentrating on the most relevant events while reducing the amount of logged data, which makes it quicker and easier to analyze.

The efficiency of Sysmon in detecting malicious activities underscores its value as a specialized tool that, when properly configured, serves as a more effective solution for real-time security monitoring and incident response compared to the broader Windows Event Logs.

Figure 1

Comparison of Sysmon and Windows Event Logs events count over time

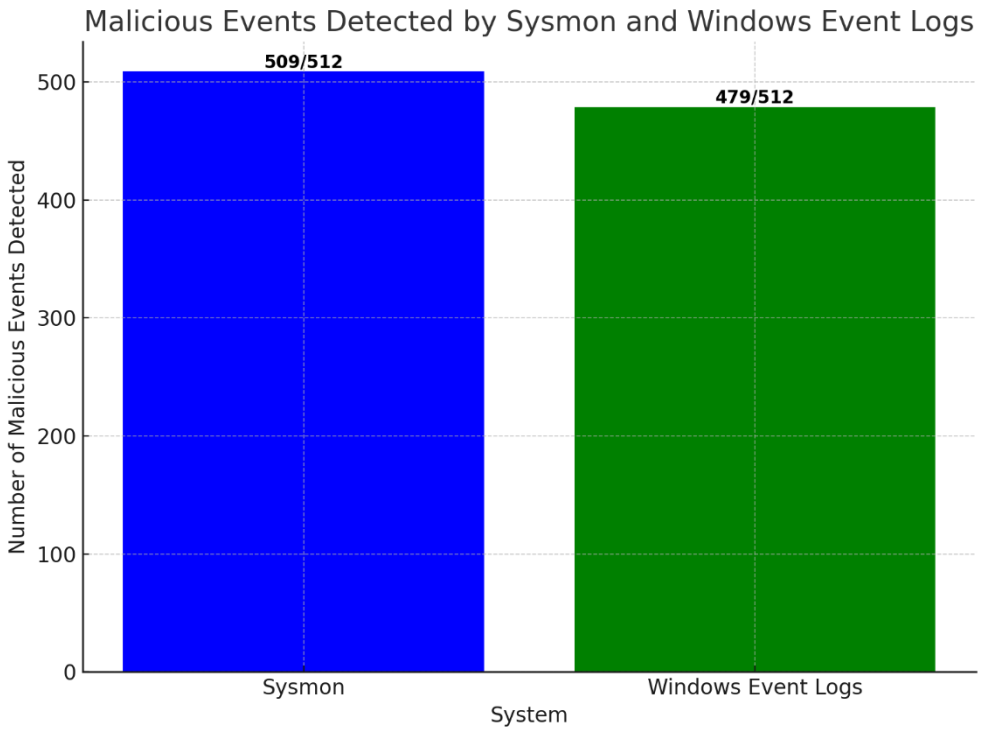


Source: author's own development

The graph (Figure 2) unequivocally shows that when it comes to identifying malicious activity, Sysmon is not only more effective but also more efficient than Windows Event Logs. With an almost flawless detection record of 99.4%, Sysmon's excellent efficacy is demonstrated by the graph, which shows that it detected 509 out of the 512 harmful events overall. However, despite being thorough, Windows Event Logs only found 479 occurrences, which translates to a 93.6% detection rate.

Figure 2

Malicious Events Detected by Sysmon and Windows Event Logs



Source: author's own development

Sysmon, when used in conjunction with Windows Event Logs, forms a comprehensive monitoring system that leverages the strengths of both tools to provide enhanced security for IT environments. While Sysmon excels at logging specific events like process creation, registry and file modifications, and network connections—which are crucial for the early detection of malware and intrusion attempts—it does not cover other critical security events such as account manipulation, login activity, and policy changes. These are robustly logged by Windows Event Logs, which track a broader range of data and provide the necessary context for understanding the scope of security breaches.

Therefore, combining Sysmon with Windows Event Logs greatly improves efficiency while also raising the monitoring system's overall efficacy. The amount of logs that must be examined and evaluated is decreased when Sysmon is trusted with the comprehensive tracking of system and network events, which expedites incident response procedures. By using focused logging, resources are concentrated on studying the most pertinent security data while noise is reduced. As a result, combining Sysmon with Windows Event Logs guarantees a whole and impartial picture of all security-related activity, enabling improved defense, quicker detections, and more calculated reactions to possible attacks. Security teams may better regulate the security posture with less overhead and more operational efficiency when they employ this dual-system approach.

Conclusions

Thus, a number of functions offered by Sysmon significantly improve the security monitoring capacities of Active Directory setups. Sysmon aids in spotting and resolving any security risks, guaranteeing prompt incident response, and upholding regulatory compliance with its comprehensive and adjustable logging and integration cutting-edge security solutions. Organizations can establish a more proactive and resilient security posture by combining Sysmon with more conventional security solutions. This is essential for defending against the constantly changing array of cyberthreats.

References

Bahniuk, N., Oleksandr, L., Kateryna, B., Inna, K., Kateryna, M., & Kondius, K. (2023). Threats detection and analysis based on SYSMON tool. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. https://doi.org/10.1109/dessert61349.2023.10416443

Smiliotopoulos, C., Barmpatsalou, K., & Kambourakis, G. (2022). Revisiting the detection of lateral movement through Sysmon. *Applied Sciences, 12*(15), 7746. https://doi.org/10.3390/app12157746

Xuan, C. D., & Huong, D. T. M. (2022). A new approach for APT malware detection based on deep graph network for endpoint systems. *Applied Intelligence, 52*(12), 14005–14024. https://doi.org/10.1007/s10489-021-03138-z