Analisis Perbandingan Cakupan Deteksi Wazuh Pada Sistem Operasi Windows 10 Yang Dilengkapi Sysmon Dan Powershell Script Block Logging Yang Divalidasi Menggunakan Framework Atomic Red Team = Comparative Analysis Of Wazuh Detection Coverage On Windows 10 Operating System Equipped With Sysmon And Powershell Script Block Logging Validated Using The Atomic Red Team Framework

Muhammad Haekal Al Ghifary, author

Abstrak

Sistem Informasi dan Manajemen Keamanan (Security Information and Event Management) telah menjadi elemen kunci dalam mengelola keamanan informasi di berbagai organisasi. Wazuh sebagai Host Intrusion Detection System (HIDS) memberikan solusi untuk mendeteksi ancaman keamanan melalui analisis log dan event. Penelitian ini bertujuan untuk menganalisis deteksi serangan berbasis host melalui implementasi Wazuh sebagai SIEM dan HIDS pada sistem operasi Windows 10 yang dikustomisasi dengan kapabilitas logging tambahan menggunakan Sysmon dan PowerShell script block logging. Penggabungan keduanya dievaluasi melalui simulasi serangan menggunakan framework Atomic Red Team. Atomic Red Team adalah kerangka kerja yang digunakan untuk melakukan uji coba dan validasi terhadap kemampuan deteksi dan respons pada sistem keamanan jaringan. Atomic Red Team menyediakan serangkaian skenario atau teknik serangan yang direplikasi secara terkontrol berdasarkan taktik dan teknik MITRE untuk menguji seberapa efektif sistem keamanan dalam mendeteksi dan merespons ancaman. Skenario serangan terdiri dari 10 teknik paling berdampak berdasarkan laporan Red Canary tahun 2023. Hasil pengujian menunjukkan bahwa konfigurasi endpoint menggunakan Sysmon berhasil mendeteksi 60,89% serangan, menggunakan PowerShell logging berhasil mendeteksi 39,11% serangan, dan konfigurasi tanpa keduanya tidak dapat mendeteksi serangan sama sekali (0%). Selain itu, Sysmon dapat mendeteksi seluruh teknik emulasi serangan, sedangkan PowerShell hanya dapat mendeteksi 50% dari total teknik.
.....Security Information and Event Management (SIEM) has become a key element in managing information security in various organizations. Wazuh, as a Host Intrusion Detection System (HIDS), provides a solution for detecting security threats through log and event analysis. This study aims to analyze host-based attack detection through the implementation of Wazuh as SIEM and HIDS on a Windows 10 operating system customized with additional logging capabilities using Sysmon and PowerShell script block logging. The combination of these tools is evaluated through attack simulations using the Atomic Red Team framework. Atomic Red Team is a framework used to test and validate the detection and response capabilities of network security systems. Atomic Red Team provides a series of controlled replicated attack scenarios or techniques based on MITRE tactics and techniques to test the effectiveness of security systems in detecting and responding to threats. The attack scenarios consist of the 10 most impactful techniques based on the Red Canary report of 2023. The test results show that endpoint configuration using Sysmon successfully detected 60.89% of attacks, using PowerShell logging successfully detected 39.11% of attacks, and configurations without either did not detect any attacks at all (0%). Furthermore, Sysmon was able to detect all emulated attack techniques, while PowerShell was only able to detect 50% of the total techniques.