Wazuh: Rules and decoders

Rinor Gimolli - 221241836

Introduction to Wazuh

Wazuh is a powerful SIEM (Security Information and Event Management) platform/tool that monitors, analyses and responds to security threats in a variety of different environments. It collects and analyses data from multiple sources to provide a comprehensive threat detection incident response.

Overview of rules and decoders

Wazuh uses rules and decoders to enable high quality success. Rules are predefined or custom configurations that detect specific patterns or behaviors in logs and initiate alerts or actions when they are detected. Decoders, on the other hand, parse, and structure raw log data so that Wazuh's rules engine can read and analyse it.

Rules and decoders: In relation to Redback Operations' projects

Project 1: VR SunCycle and SmartBike

Custom solutions would be required for VR game data integration. Wazuh mainly deals with security-related logs, so handling VR game data would require the development of custom loggers within the game or the use of APIs that display game events as loggable data. Custom decoding mechanisms and rules for game-related security flaws may also be required. The process of integrating exercise bike metrics into Wazuh is similar. As Wazuh does not interact with exercise bike data by default, a middleware or interface layer would be required for converting bike metrics into loggable events. The data would then be analysed for anomalies or security-related insights using custom decoding configurations and rules – similarly as mentioned above.

Project 2: Wearable Tech sensor

Wazuh is not designed to interact directly with GPS tracking data by default. Integrating GPS tracking data requires the development of custom decoders to parse the GPS device's unique data format, as well as middleware to bridge the communication gap between the device and Wazuh. This entails interpreting GPS data, converting it to a loggable format, and configuring rules to analyse relevant data.

Project 3 and 4: (Sport Performance Analysis and Data Warehousing)

As these two projects work with data and logs, the same implementations can be used of creating custom decoders to read the data. Custom rules can be integrated to monitor access patterns, suspicious activity and data integrity as a whole.

Alternatives and other Solutions

Development of Middleware: Create middleware or API (Application Programming Interface) to translate the device's data into readable logs for Wazuh

Custom Integration: Creating custom solutions to connect devices and Wazuh, allowing data transformation for security analysis.

External monitoring: By applying specialised monitoring solutions, or platforms designed specifically for the respective devices - we can integrate them with Wazuh to match data for overall security insights.

References

Wazuh, *Home Page*, Wazuh Inc 2023 (accessed 11/24/2023) - https://wazuh.com/platform/overview/

GeeksforGeeks, *Introduction to Wazuh*, GeeksforGeeks Pty Ltd (accessed 11/25/2023) - https://www.geeksforgeeks.org/introduction-to-wazuh/

Wazuh, *How it works,* Wazuh Inc 2023 (accessed 11/25/2023) - https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/how-it-works.html