Group Members: Andrew Bentkowski and Ashley Dickens

Title: Project Sentinel: Confidence-Based Malware Detection for Common File Formats

Abstract:

Malicious files are an omnipresent threat to any network/system, and should they be executed by a user with administrator rights, can cripple an infrastructure and damage reputation. In an effort to assist day to day users with gauging the risk of a given file, the idea of project sentinel emerged. Sentinel offers users a way to safely check the likelihood that a file is malicious. The tool will accept PDF, EXE, .DOCX, XLSX documents and begin analysis for known threats with the given hash. Should there be a match via open-source intelligence, it will be communicated to the user. Should there be no match, it will conduct additional AI-driven analysis and assign a rating of the likelihood that a file is malicious, and a rationale for its thinking. It is always best to consult a security team if there is any doubt, but this solution offers immediate educated analysis in the event resources are unavailable or unaffordable.