BigBear.ai

Troy (BETA)

Empowering Vulnerability Researchers and Reverse Engineering teams, Troy offers a modular and customizable solution, designed to expedite the process and provide deeper, more informed insights and guidance.

Troy is a workflow engine designed to intelligently automate and accelerate the binary reverse engineering process. Through multi-stage pipelines of input/output data and intermediate representations, Troy produces easily consumable and actionable results while enriching previous-stage data along the way. Best described as a tool to build better tools when applied to cybersecurity research and development, Troy is the result of identifying a market need and an attempt to augment the unpredictable activities associated with modern firmware and application static binary analysis. It is developed in a modular fashion allowing for multiple workflows to be pipelined following file ingest and triage. ALL consumable findings, data, metadata, and enrichments are stored for easy retrieval and analysis.

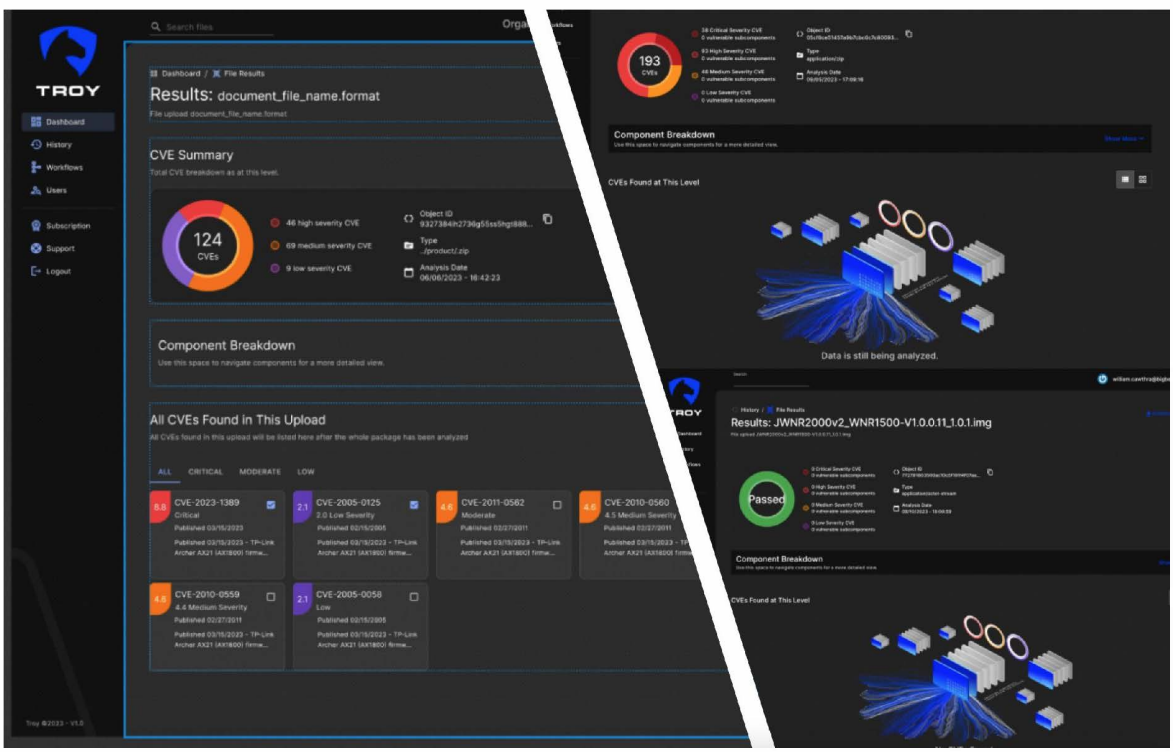
Solution Brief. ↗

Blending Cyber + AI to accelerate Binary Analysis

AI-powered, machine accelerate binary analysis platform that provides better binary visibility into the code running on your sensors and devices. Through the intelligent automation of common tools and techniques, Troy extracts all interesting data and produces unique insights and information. Core to Troy is the ability to integrate new tools, techniques, and even AI-backed analysis into ever-expanding workflows.

Reverse Software Bill of Materials (rSBOM)

Extracts and generates a reverse Software Bill of Materials (SBOM) on binaries where the original source code is not available. The product also reduces the manual labor required to conduct vulnerability assessments and increases the speed of analysis.



Email Info@BigBear.ai to request a demo of Troy. Learn more about BigBear.ai's cyber engineering capabilities at BigBear.ai.