CERIAS

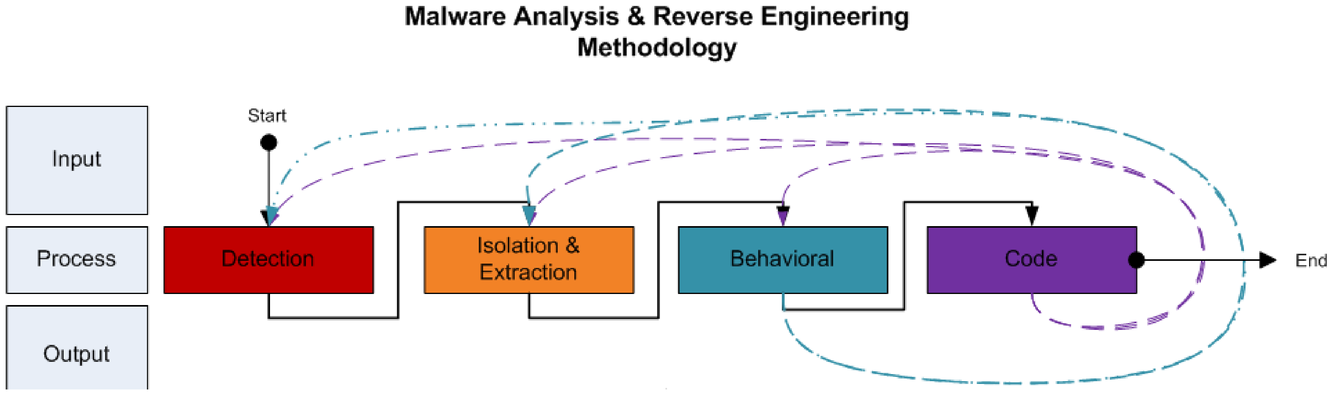
the center for education and research in information assurance and security

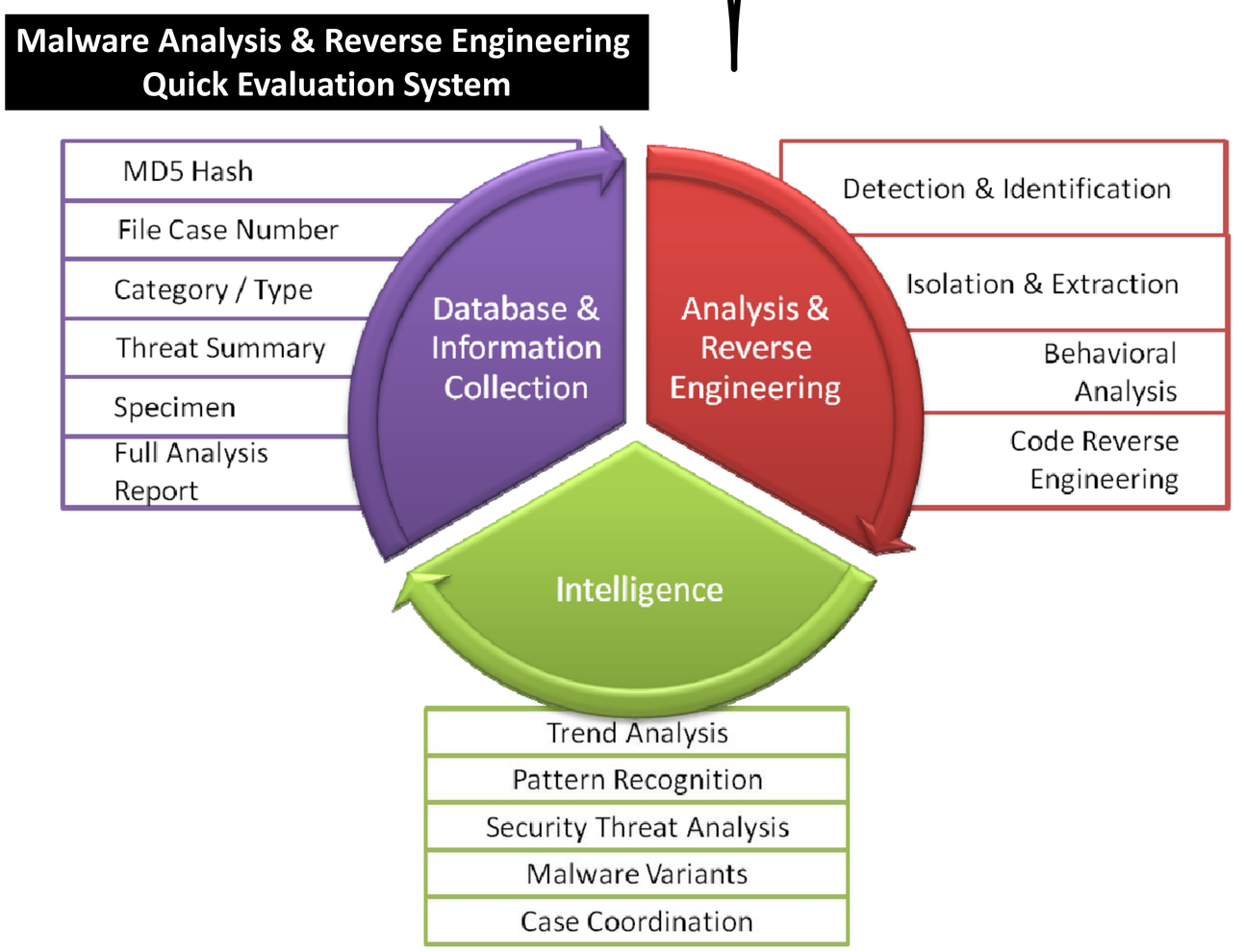
Malware Analysis & Reverse Engineering Quick Evaluation System

James E. Goldman, Cory Q. Nguyen, Anthony E. Smith
Purdue Malware Lab

The Malware Analysis & Reverse Engineering Quick Evaluation System (MARQUES) is a system designed to create a preliminary analysis report that would give security administrators and investigators immediate information and insight into a suspected malware's capabilities, functions, and purpose. MARQUES has the ability to automate analysis of malware not only on a behavioral level but also on a code level. The ability to automate analysis of malware on a code level separates it from the conventional existing malware services. This information is vital in responding and combating malware attacks and infection on network systems. The MARQUES system aims at increasing the response time to malware incidents and aims at providing valuable insight into pattern recognitions and trend analysis of existing and zero-day malware specimens.

The MARQUES system incorporates the established Malware Analysis & Reverse Engineering (MARE) methodology developed by the Purdue Malware Lab research team. The MARE methodology is the engine of the MARQUES system that automates the behavioral and code analysis of suspected malware.





PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center