Vajra - Threat Detection and Response in Linux End Points

Problem Statement: Malware attacks can put IT infrastructure at risk. Many malware attacks are difficult to detect using standard methods. For example, fileless malware, a recent development, operates in the computer's memory, thus avoiding signature scanners like antiviruses. To bolster security, an IT department may implement various endpoint security solutions over time. However, multiple standalone security tools can complicate the threat detection and prevention process, especially if they overlap and produce similar security alerts. A better approach is an integrated Endpoint Security solution. The current need of the hour is to design a system to quickly detect, analyse, block, and contain attacks in progress. It needs to collaborate with other security technologies to give administrators visibility into advanced threats to speed detection and remediation response times.

Uniqueness of the Solution: Existing endpoint detection and response (EDR) solutions mostly focus on Windows systems, and no comprehensive solution is available for Linux systems. The tool developed by the team focuses explicitly on Linux systems with support for container security. Currently, no indigenous tools on EDR solutions exist, and this tool fills this void. The tool allows system administrators to detect lateral movements and privilege escalation and quickly control the damage. Also, the researchers will be providing continuous R&D support and constantly updating the rule engines to detect and provide protection against new malware.

Current Status of Technology: The system prototype is ready and tested in a lab environment. The product will be tested under various operational environments (TRL-6).

Societal Impact: Privacy and security are essential aspects that need to be guaranteed to all the users of digital services. This tool helps keep users' information safe and thus helps build a safer digital society.

Patent(s): Nil

Relevant Industries: Cybersecurity, Information and Communication Technology.

Faculty: Prof. Manjesh K. Hanawal, Industrial Engineering and Operations Research.