Active response

Active response performs various countermeasures to address active threats such as blocking access to an agent from the threat source. This automated remediation is called active response in Wazuh.

Active response executes a script in response to being triggered by a specific alert based on alert level or rule group. Any number of scripts can be initiated in response to a trigger, however these responses should be carefully considered as poor implementation of rules and responses could increase the vulnerability of the system.

Contents