

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

- [How it works](#)
 - [When is an active response triggered?](#)
 - [Where are active response actions executed?](#)
 - [Active response configuration](#)
 - [Default Active response scripts](#)
- [Configuration](#)
 - [Basic usage](#)
 - [Windows automatic remediation](#)
 - [Block an IP with PF](#)
 - [Add an IP to the iptables deny list](#)
 - [Active response for a specified period of time](#)
 - [Active response that will not be undone](#)
- [FAQ](#)
 - [Can I use a custom script for active response?](#)
 - [Can I configure active response for only one host?](#)
 - [Can active response remove the action after a time?](#)

