ossec-logtest

The ossec-logtest program is a useful tool when working with Wazuh rules. This tool allows the testing and verification of rules against provided log examples in a way that simulates the action of ossec-analysisd. This can also assist with writing and debugging custom rules and troubleshooting false positives and negatives.

-a	Analysis of input lines as though they are live events.	
-c <config>	Run using `config` as the configuration file.	
	Default Value	/var/ossec/etc/ossec.conf
-D <dir>	Specifies the chroot before it completes loading all rules,decoders, and lists and processing standard input.	
-d	Run as a Print debug output to the terminal. This option may be repeated to increase the verbosity of the debug messages.group.	
-h	Display the help message.	
-t	Test configuration. This will display file details on the rules to be loaded by ossec-analysisd, decoders, and lists as they are loaded and the order they were processed.	
-U <rule-id:alert-level:decoder-name>	This option will cause ossec-logtest to return a zero exit status if the test results for the provided log line match the criteria in the arguments. Only one log line should be supplied for this to be useful.	
-V	Display the version and license information for Wazuh and ossec-logtest.	
-v	Display the verbose results.	

Note

- U ossec-logtest code requires access to all ossec configuration files.

Note

-v is the key option to troubleshoot a rule or decoder problem.