For the detection component, we have done the following,

Added custom rules to /var/ossec/etc/rules/local\_rules.xml. This will make sure that only those events violating these conditions will be captured.

*<rule id="200100" level="10"> <if\_sid>554</if\_sid> <match>encrypted|\.enc|\.locky|\.cry|\.crypt|/\.encrypted\_flag|\.encrypted\_flag</match> <description>Possible ransomware encryption detected (suspicious file name)</description> <mitre><id>T1486</id></mitre> </rule>*

This above rule is to detect encryption activity. The rule has been a severity level of 10, a high-priority alert. It is linked to the existing OSSEC/Wazuh rule 554, which is triggered whenever the File Integrity Monitoring (FIM) system (known as syscheck) detects a file modification on the host. The <match> directive specifies a set of suspicious keywords and file extensions that ransomware often uses when encrypting data, such as .encrypted, .enc, .locky, .cry, and .crypt. It also includes patterns like /.encrypted\_flag to capture cases where ransomware creates hidden marker files to indicate that encryption is complete.

After this, we Create a script at /var/ossec/active-response/bin/ransomware\_logger.sh and make it an executable file. We add the rule 200100 to the ossec.conf file in the active response section. Whenever Rule 200100 triggers, Wazuh will automatically append the alert details to:

/var/ossec/logs/ransomware\_only.log.

We follow the same procedure for the other rules like:

<!-- Detect unauthorized system file modification -->

<rule id="200102" level="12">

<if\_sid>550</if\_sid>

<match>\/bin\/|\/sbin\/|\/usr\/bin\/</match>

<description>Unauthorized modification of critical system binary</description>

</rule>