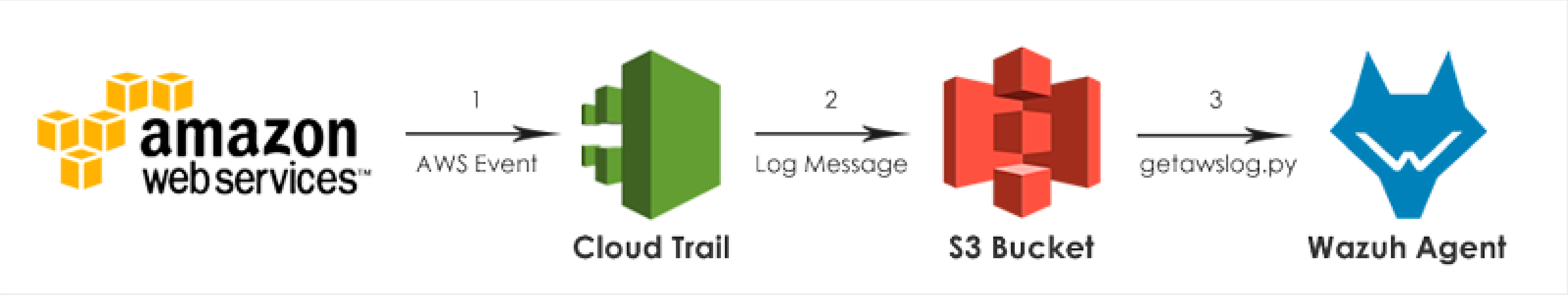
Using Wazuh for AWS

This section provides instructions to integrate Wazuh with Amazon Web Services (AWS). It also explains different use cases as examples of how the rules developed by Wazuh can be used to alert on specific events from IAM, EC2 and VPC.

The diagram below shows how a log message about an AWS event flows from AWS to a Wazuh agent. Once the agent reads the message, it sends it to the Wazuh manager which analyses it with decoders and rules. When a rule matches, an alert is triggered if the rule severity is high enough.



1. CloudTrail is a web service that records AWS API calls for your account and writes them to log files. When an AWS event occurs, CloudTrail generates the log message. Using CloudTrail we can get more visibility into AWS user activity, tracking changes made to AWS resources.
2. Once an event takes place, CloudTrail writes it to a log file on Amazon S3, where log files can be stored durably and inexpensively.
3. The script `getawslog.py` downloads CloudTrail log files from Amazon S3 to the Wazuh agent, uncompresses them and appends the new data to a local text file which is monitored by the Wazuh agent and forwarded to the Wazuh manager just like any other log file.

This diagram makes it easier to understand the integration process described in the upcoming pages.

Contents