Documentation › User manual › Ruleset › Dynamic fields

Dynamic fields

Traditional decoders

An important step for the detection and processing of threats is the extraction of information from each event received. Wazuh uses decoders to identify event types and then extract the most relevant fields, thus enriching events and allowing them to be more deeply analyzed and indexed.

Traditionally, OSSEC has provided thirteen predefined fields for storing extracted information (*user, srcip, dstip, srcport, dstport, protocol, action, id, url, data, extra_data, status, system_name*), of which only eight can be extracted simultaneously.

Static fields:

```
<decoder name="web-accesslog">
  <type>web-log</type>
  <prematch>^\d+.\d+.\d+.\d+ - </prematch>
  <regex>^(\d+.\d+.\d+.\d+) - \S+ [\S+ -\d+] </regex>
  <regex>"\w+ (\S+) HTTP\S+ (\d+) </regex>
  <order>srcip,url,id</order>
</decoder>
```

Dynamic decoders

It is often necessary to extract more than eight relevant fields from an event, and often the actual data items extracted have no relationship to the limited list of predefined field names. Knowing that we cannot afford to operate within these constraints, Wazuh has extended OSSEC to allow the decoding of an unlimited number of fields with field names that clearly relate to what is being extracted. Even nested field names are supported.

Dynamic fields:

```
<decoder name="auditd-config_change">
  <parent>auditd</parent>
  <regex offset="after_regex">^auid=(\S+) ses=(\S+) op="(\.+)"</regex>
  <order>audit.auid,audit.session,audit.op</order>
</decoder>
```

Wazuh transforms any field name included in the `<order>` tag into a JSON field.

The next example shows how the auditd decoder extracts the information from an alert:

```
** Alert 1486483073.60589: - audit,audit_configuration,
2017 Feb 07 15:57:53 wazuh-example->/var/log/audit/audit.log
Rule: 80705 (level 3) -> 'Auditd: Configuration changed'
type=CONFIG_CHANGE msg=audit(1486483072.194:20): auid=0 ses=6 op="add rule" key="audit-wazuh-a" list=4 res=1
audit.type: CONFIG_CHANGE
audit.id: 20
audit.auid: 0
audit.session: 6
audit.op: add rule
audit.key: audit
audit.list: 4
audit.res: 1
```

JSON Output:

```
{
  "rule": {
    "level": 3,
    "description": "Auditd: Configuration changed",
    "id": 80705,
    "firedtimes": 2,
    "groups": [
      "audit",
      "audit_configuration"
    ]
  },
  "agent": {
    "id": "000",
    "name": "wazuh-example"
  },
  "manager": {
    "name": "wazuh-example"
  },
  "full_log": "type=CONFIG_CHANGE msg=audit(1486483072.194:20): auid=0 ses=6 op=\"add rule\" key=\"audit-wazuh-a\" list=4 res=1",
  "audit": {
    "type": "CONFIG_CHANGE",
    "id": "20",
    "auid": "0",
    "session": "6",
    "op": "add rule",
    "key": "audit",
    "list": "4",
    "res": "1"
  },
  "decoder": {
    "parent": "auditd",
    "name": "auditd"
  },
  "timestamp": "2017 Feb 07 15:57:53",
  "location": "/var/log/audit/audit.log"
}
```

Note

By default, the number of fields that can be extracted simultaneously from an `<order>` tag is **64**. This value can be modified by changing the variable `analysisd.decoder_order_size` seen in `/var/ossec/etc/internal_options.conf`. If you need to change this value, copy the `analysisd.decoder_order_size` section from `/var/ossec/etc/internal_options.conf` to `/var/ossec/etc/local_internal_options.conf` and change it there, since Wazuh software updates can replace `/var/ossec/etc/internal_options.conf`