Configuration

Basic usage

Active response is configured in ossec.conf, within the Active Response and Command sections.

In this example, a command with the name *"restart-ossec"* is configured to use the *"restart-ossec.sh"* script with no data element. The **Active response** is configured to initiate the *"restart-ossec"* command on the local host when the rule with ID 10005 fires. This is a *Stateless* response as no timeout parameter is defined.

Command:

```
<command>
  <name>restart-ossec</name>
  <executable>restart-ossec.sh</executable>
  <expect></expect>
</command>
```

Active response:

```
<active-response>
  <command>restart-ossec</command>
  <location>local</location>
  <rules_id>10005</rules_id>
</active-response>
```

Windows automatic remediation

In this example, a command with the name *"win_rout-null"* is configured to use the *"route-null.cmd"* script using the data element *"srcip"*. The **Active response** is configured to initiate the *"win_rout-null"* command on the local host when the rule has a higher alert level than 7. This is a *Stateful* response with a timeout set at 900 seconds.

Command:

```
<command>
  <name>win_route-null</name>
  <executable>route-null.cmd</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

Active response:

```
<active-response>
  <command>win_route-null</command>
  <location>local</location>
  <level>8</level>
  <timeout>900</timeout>
</active-response>
```

Block an IP with PF

In this example, a command with the name *"pf-block"* is configured to use the *"pf.sh"* script using the data element *"scrip"*. The **Active response** is configured to initiate the *"pf-block"* command on agent *"001"* when a rule in either the *"authentificaiton_failed"* or *"authentication_failures"* rule group fires. This is a *Stateless* response as no timeout parameter is defined.

Command:

```
<command>
  <name>pf-block</name>
  <executable>pf.sh</executable>
  <expect>srcip</expect>
</command>
```

Active response:

```
<active-response>
  <command>pf-block</command>
  <location>defined-agent</location>
  <agent_id>001</agent_id>
  <rules_group>authentication_failed,authentication_failures</rules_group>
</active-response>
```

Add an IP to the iptables deny list

In this example, a command with the name *"firewall-drop"* is configured to use the *"firewall-drop.sh"* script using the data element *"scrip"*. The **Active response** is configured to initiate the *"firewall-block"* command on all systems when a rule in either the *"authentificaiton_failed"* or *"authentication_failures"* rule group fires. This is a *Stateful* response with a timeout of 700 seconds. The repeated offenders parameter increases the timeout period for each subsequent offence by a specific IP address.

Note: This parameter is specified in minutes rather than seconds.

Command:

```
<command>
  <name>firewall-drop</command>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
</command>
```

Active response:

```
<active-response>
  <command>firewall-block</command>
  <location>all</location>
  <rules_group>authentication_failed,authentication_failures</rules_group>
  <timeout>700</timeout>
  <repeated_offenders>30,60,120</repeated_offenders>
</active-response>
```

Active response for a specified period of time

The action of a stateful response continues for a specified period of time.

In this example, a command with the name *"host-deny"* is configured to use the *"host-deny.sh"* script using the data element *"scrip"*. The **Active response** is configured to initiate the *"host-deny"* command on the local host when a rule with a higher alert level than 6 is fired.

Command:

```
<command>
  <name>host-deny</name>
  <executable>host-deny.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

Active response:

```
<active-response>
  <command>host-deny</command>
  <location>local</location>
  <level>7</level>
  <timeout>600</timeout>
</active-response>
```

More info: command

Active response that will not be undone

The action of a stateless command is a one-time action that will not be undone.

In this example, a command with the name *"mail-test"* is configured to use the *"mail-test.sh"* script with no data element. The **Active response** is configured to initiate the *"mail-test"* command on the server when the rule with ID 1002 fires.

Command:

```
<command>
  <name>mail-test</name>
  <executable>mail-test.sh</executable>
  <timeout_allowed>no</timeout_allowed>
  <expect />
</command>
```

Active response:

```
<active-response>
    <command>mail-test</command>
    <location>server</location>
    <rules_id>1002</rules_id>
 </active-response>
```