Feeding MISP with OSSEC

Pass-The-Salt 2024 | TLP:Clear

Xavier Mertens | July 2024

OSSEC

"Open Source Security Event Correlator"

- OSSEC is a comprehensive, open-source host-based intrusion detection system (HIDS).
- It is designed to monitor and analyze system logs, detect suspicious activities, and provide real-time alerts for security incidents.
- OSSEC can perform log analysis, file integrity monitoring, rootkit detection, and **active response** to mitigate threats.
- It supports various platforms including Linux, Windows, and macOS, and can be integrated with various security tools and SIEM solutions.

Active-Response

- Active-Response allows to automatically take predefined actions in response to detected security events or threats.
- When a specific rule is triggered, OSSEC can execute scripts or commands to mitigate the threat, such as blocking an IP address, disabling a user account, or restarting a service.
- This feature enhances the system's security by providing real-time, automated reactions to potential intrusions or malicious activities, reducing the window of opportunity for attackers to exploit vulnerabilities.

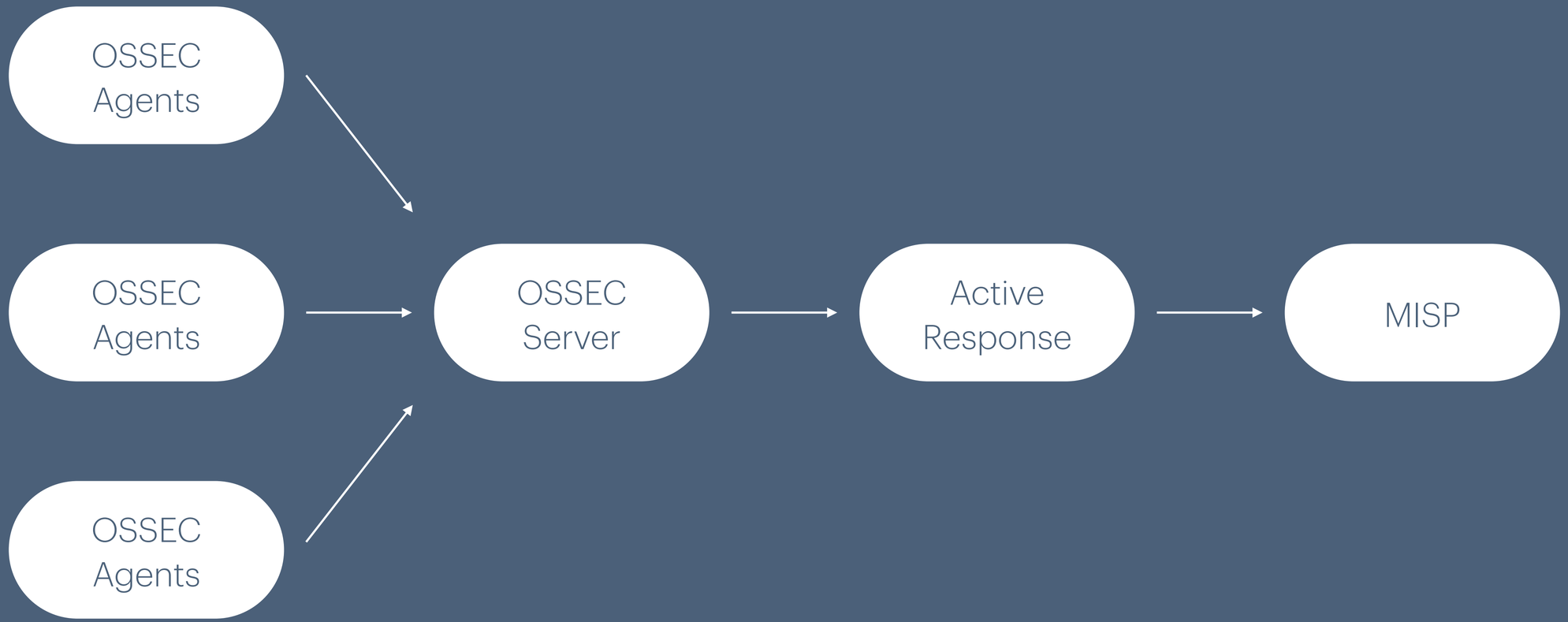
MISP

(No need to introduce the projet 😝)

- Collect IOC’s and store them
- Classify them
- Share them
- Improve hunting by correlating with many 3rd party tools

Automation

Because we are (again) lazy!


OSSEC
Agents
OSSEC
Agents
OSSEC
Agents
OSSEC
Server
Active
Response
MISP

- Step 1 - Define the Active-Response rule

```
<active-response>
  <disabled>no</disabled>
  <command>ossec2misp</command>
  <location>server</location>
  <rules_id>100213,100201,31509</rules_id>
</active-response>
```

- Step 2 - Define hunting rules

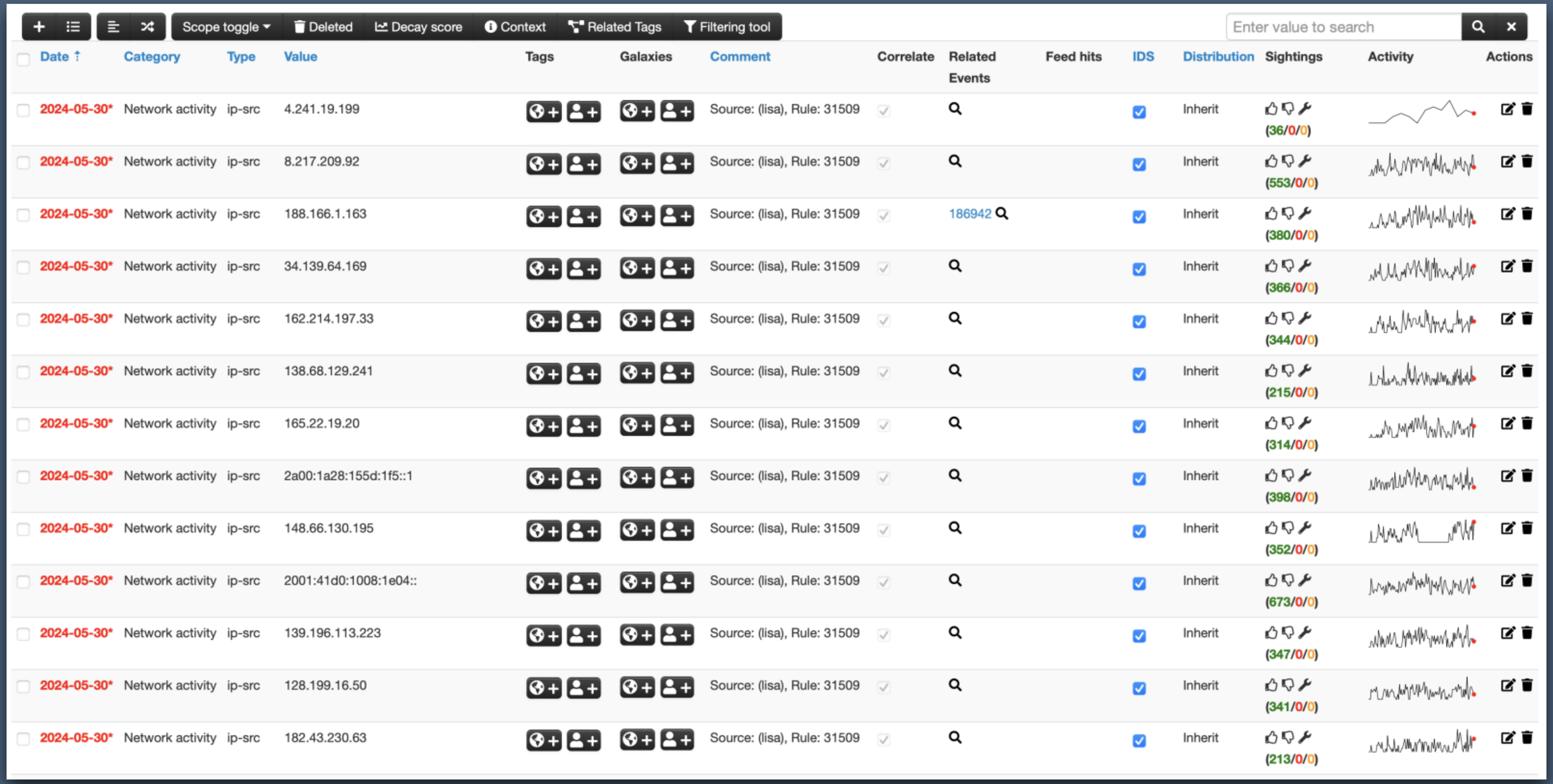
```
<!-- WordPress wp-login.php brute force -->
  <rule id="31509" level="3">
    <if_sid>31108</if_sid>
    <url>wp-login.php|/administrator</url>
    <regex>] "POST \S+wp-login.php| "POST /administrator</regex>
    <description>CMS (WordPress or Joomla) login attempt.</description>
</rule>
```

- Step 3 - Define the script to trigger

```
<command>
  <name>ossec2misp</name>
  <executable>ossec2misp.py</executable>
  <expect>srcip</expect>
  <timeout_allowed>no</timeout_allowed>
</command>
```

- Step 4 - Configure the script

```
misp_url            = "https://misp.domain.tld"
misp_key            = "<redacted>"
misp_verifycert     = True
misp_info           = "OSSEC ActiveResponse"  # Event title
misp_last           = "30d"                   # Max period to search for IP
address
misp_new_event      = False                   # Force the creation of a new event for every report
misp_distribution = 0                         # The distribution setting used for the newly created
                                              # event, if relevant. [0-3]
misp_analysis       = 1                       # The analysis level of the newly created event, if
applicable. [0-2]
misp_threat         = 3                       # The threat level ID of the newly created event, if
applicable. [1-4]
misp_tags           = [ "source:OSSEC" ]      # Tags for the newly created event, if applicable
misp_publish        = True                    # Automatically puslish the event
syslog_server       = "192.168.1.1"           # If defined, enable syslog logging
redis_server        = "redis"                 # Redis server hostname/ip
redis_port          = 6379                    # Redis server port
redis_db            = 0                       # Redis server db
```



Date	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2024-05-30*	Network activity	ip-src	4.241.19.199			Source: (lisa), Rule: 31509					Inherit	(36/0/0)		
2024-05-30*	Network activity	ip-src	8.217.209.92			Source: (lisa), Rule: 31509					Inherit	(553/0/0)		
2024-05-30*	Network activity	ip-src	188.166.1.163			Source: (lisa), Rule: 31509		186942			Inherit	(380/0/0)		
2024-05-30*	Network activity	ip-src	34.139.64.169			Source: (lisa), Rule: 31509					Inherit	(366/0/0)		
2024-05-30*	Network activity	ip-src	162.214.197.33			Source: (lisa), Rule: 31509					Inherit	(344/0/0)		
2024-05-30*	Network activity	ip-src	138.68.129.241			Source: (lisa), Rule: 31509					Inherit	(215/0/0)		
2024-05-30*	Network activity	ip-src	165.22.19.20			Source: (lisa), Rule: 31509					Inherit	(314/0/0)		
2024-05-30*	Network activity	ip-src	2a00:1a28:155d:1f5::1			Source: (lisa), Rule: 31509					Inherit	(398/0/0)		
2024-05-30*	Network activity	ip-src	148.66.130.195			Source: (lisa), Rule: 31509					Inherit	(352/0/0)		
2024-05-30*	Network activity	ip-src	2001:41d0:1008:1e04::			Source: (lisa), Rule: 31509					Inherit	(673/0/0)		
2024-05-30*	Network activity	ip-src	139.196.113.223			Source: (lisa), Rule: 31509					Inherit	(347/0/0)		
2024-05-30*	Network activity	ip-src	128.199.16.50			Source: (lisa), Rule: 31509					Inherit	(341/0/0)		
2024-05-30*	Network activity	ip-src	182.43.230.63			Source: (lisa), Rule: 31509					Inherit	(213/0/0)		

Thank You

https://github.com/xme/ossec/blob/main/ossec2misp.py

Need more info? Catch me!