



Automated Threat Intelligence Pipeline: Wazuh + MISP + IRIS

Overview

I designed and implemented a real-time **Network Detection and Response (NDR)** workflow. This project automates the cross-referencing of endpoint file activity against global threat intelligence feeds to significantly reduce the "Mean Time to Detect" (MTTD).

The Technology Stack

- **Wazuh (XDR/SIEM):** Monitored endpoints via File Integrity Monitoring (FIM).
- **MISP (Threat Intel):** Served as the source of truth for malicious MD5/SHA256 hashes.
- **Python 3:** A custom bridge script connecting Wazuh alerts to the MISP REST API.
- **IRIS (Incident Response):** Automated ticket generation for high-severity matches.

Technical Implementation

1. Real-Time Detection (FIM)

Configured Wazuh to monitor specific directories. As seen in my logs, Rule **554** ("File added to the system") triggers immediately upon file creation.

Document Details		View surrounding documents	View single document	X
Table	JSON			
t _index	wazuh-alerts-4.x-2026.02.01			
t agent.id	004			
t agent.ip	192.168.110.158			
t agent.name	MISP			
t data.integration	misp_file_hashes			
o data.misp.event_id	130			
o data.misp.found	1			
o data.misp.info	44d88612fea8a8f36de82e1278abb62f			
o data.misp.permalink	https://192.168.110.158/events/view/130			
t decoder.name	json			
t full_log	{"misp": {"found": 1, "event_id": "130", "info": "44d88612fea8a8f36de82e1278abb62f", "permalink": "https://192.168.110.158/events/view/130"}, "integration": "misp_file_hashes"}			
t id	1769928223.87408			
t input.type	log			
t location	misp			
t manager.name	wazuh			
t rule.description	MISP: file hash matched			
x rule.firetimes	1			
t rule.groups	misp, malware			
t rule.id	100002			
x rule.level	12			
o rule.mail	true			
o timestamp	Feb 1, 2026 @ 12:43:43.193			

2. Automated Intelligence Querying

I developed a Python integration script that intercepts the FIM alert, extracts the MD5 hash, and queries MISP.

- **Challenge:** Standard integrations often fail due to SSL certificate verification in lab environments.
- **Solution:** Optimized the script to handle self-signed certificates and implemented a fallback logic to prevent "NoneType" crashes.

```
root@wazuh:~# grep "MISP" /var/ossec/logs/integrations.log
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
MISP_DEBUG: Querying MISP for hash: 44d88612fea8a8f36de82e1278abb02f
MISP_DEBUG: Match found and sent to Wazuh!
root@wazuh:~#
```

3. Custom Alert Engineering

I authored a custom ruleset ([Rule 100802](#)) that elevates any hash match to a **Level 12 (High Severity)** alert.

- **Rule Logic:** If `misp.found == 1`, generate a critical alert including the MISP Permalink and Event ID.

4. Automated Incident Response (IRIS Integration)

The final stage of the pipeline automatically pushes critical alerts to the **IRIS dashboard**. This allows security analysts to see the full "Forensic Story" (MD5, file path, and threat category) in one place.

The screenshot shows the IRIS interface with a central alert card. The card title is "MISP: FILE HASH MATCHED #1225-2A844949-BB7d-4DBF-9C6B-BBEA56AA1BD". Below the title, it lists alert details: Rule ID: 100802, Rule Level: 12, Rule Description: MISP: file hash matched, Agent ID: 004, Agent Name: MISP, MITRE ID: N/A, MITRE Tactics: N/A, MITRE Techniques: N/A, Location: misc_file_hashes. It includes a "Full Log" snippet and a "General info" section with fields like Source: Wazuh, Source Link: <https://192.168.110.120/api/wz-home>, Source Reference: 1769924324.70811, Source Event Time: 01/02/2026, 05:38:44 UTC, IRIS Creation Time: 01/02/2026, 05:38:46 UTC, and Alert note. At the top right, there are buttons for Merge, Assign, Set status, Close with note, and Close.

Key Achievements

- **Automated Intelligence:** Successfully integrated feeds from **MalwareBazaar** and **CIRCL OSINT**.
- **SOC Optimization:** Level 0 "noise" is filtered out, ensuring analysts only see Level 10+ alerts in IRIS.
- **MITRE Mapping:** Mapped file execution alerts to **MITRE ATT&CK T1204.002** (Malicious File).