INFN

Francesco Amori

OpenSearch

WAZUH

MISP

SURICATA

Grafana

Workshop sul Calcolo nell'INFN - Palau - 20/24 Maggio 2024

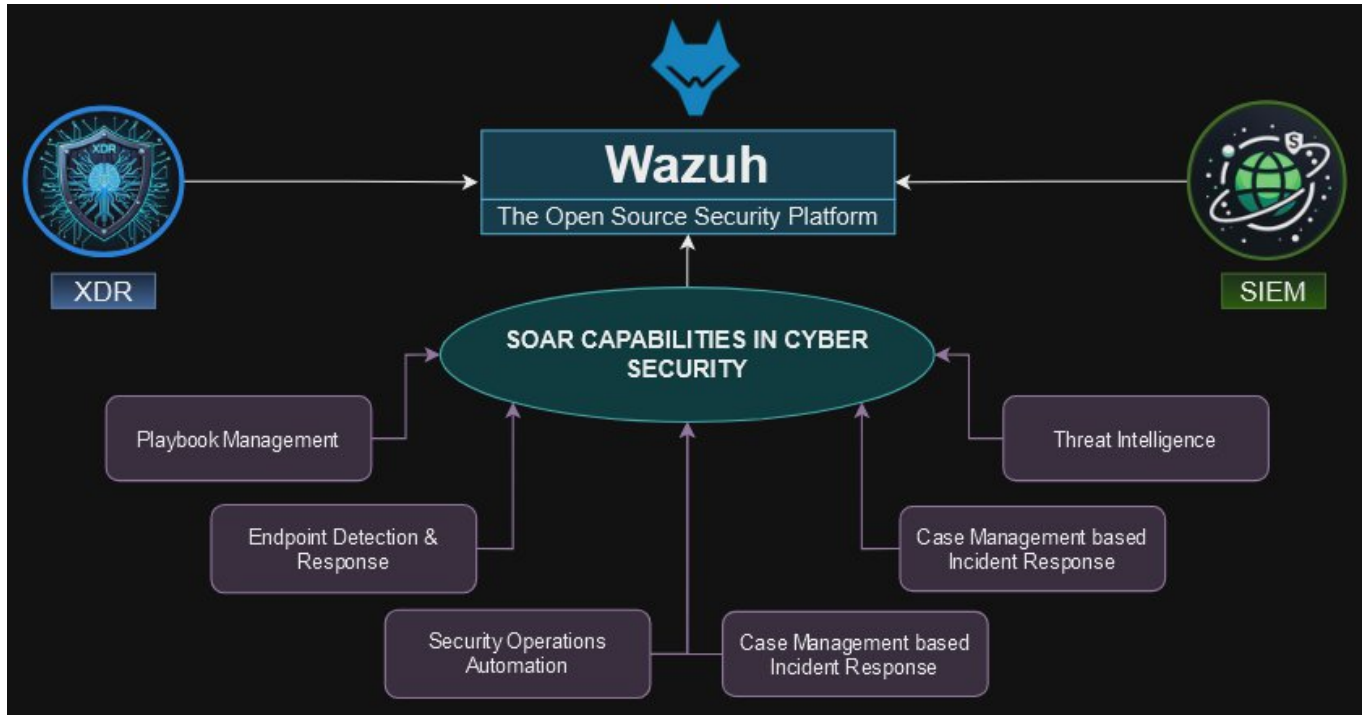
Sommario

- Cos’è WAZUH
  - SIEM-XDR-SOAR
  - Log Collectors
  - Security Response
- Integrazioni
  - Big Data Platform (BDP)
  - MISP
  - SURICATA IDS
  - Grafana

Wazuh

Piattaforma ibrida tra SIEM-XDR-SOAR

Wazuh può essere visto come strumento per il monitoraggio e gestione delle minacce nella rete pertanto si colloca nel mezzo di quelle piattaforma che si occupano delle gestione e risoluzione degli incidenti di sicurezza. Grazie alle **integrazioni** possibili può prendere aspetti specifici di ciascuno e utilizzarli al meglio. Dipende da come vogliamo sfruttare le sue potenzialità:



SIEM
- Security Events
- Management
- Logs collector

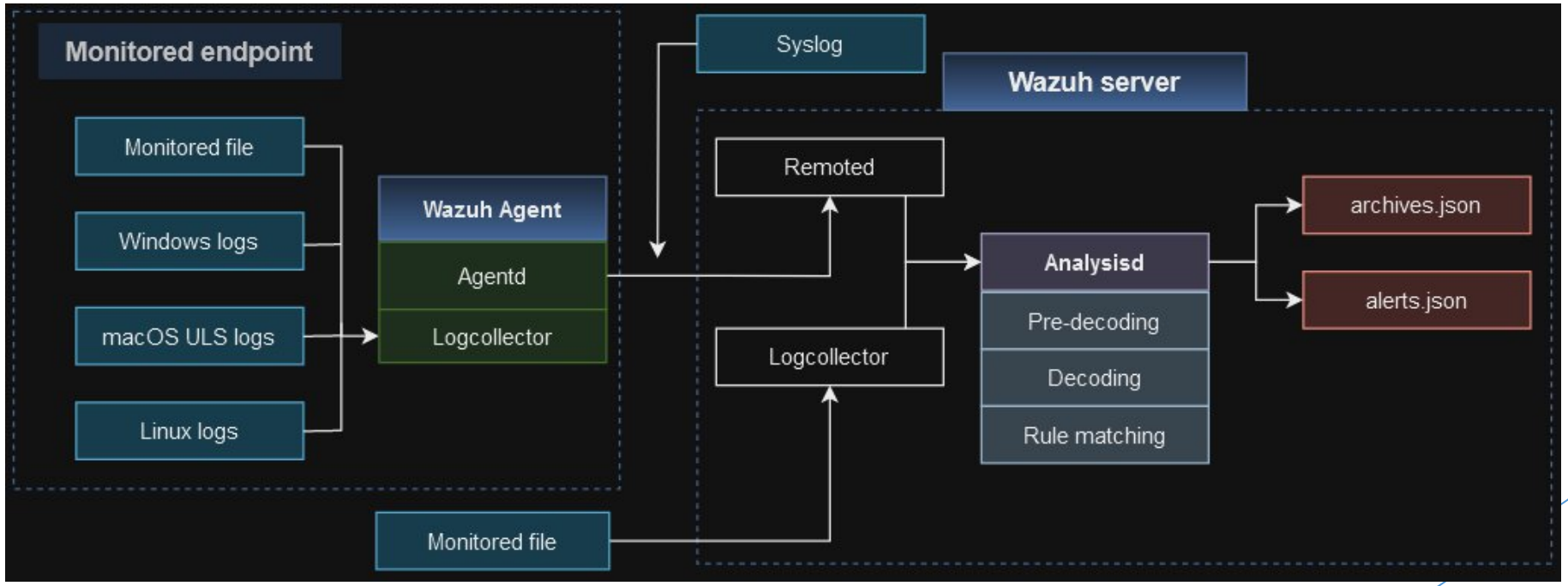
XDR
- EPS Security
- Cloud Security
- Network Security

SOAR
- CTI
- Automation Response

Logs-Collector

Custom Injection dei logs da macchine Linux

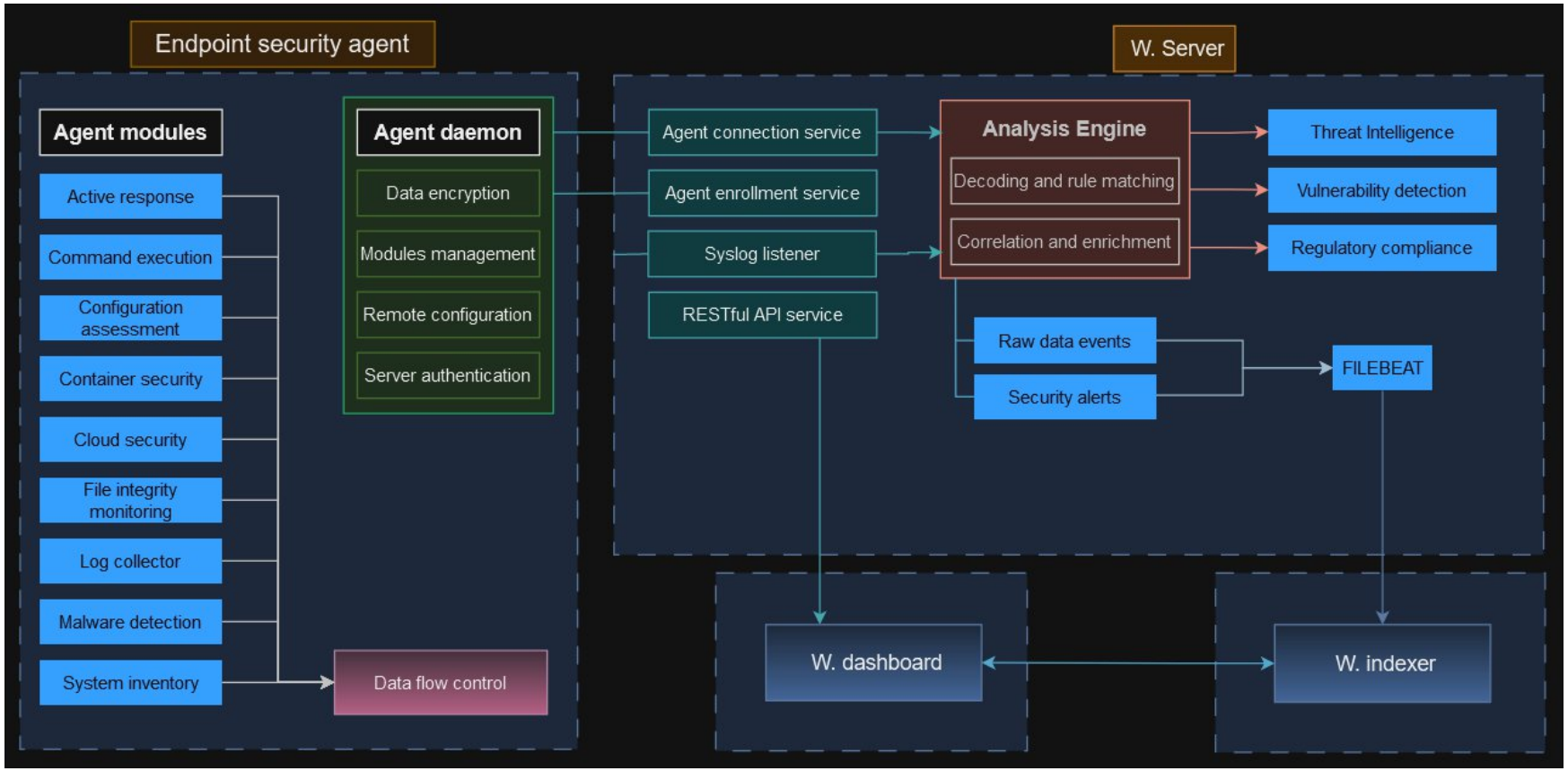
Wazuh raccoglie e analizza i logs provenienti dagli agenti installati sui sistemi monitorati, identificando comportamenti sospetti mediante regole di rilevamento delle minacce e, se necessario, genera notifiche per consentire una risposta immediata agli incidenti di sicurezza.



Alcuni Logs specifici sono stati settati all'interno di OSSEC mediante Auditd, e specifici *.json utilizzati dalle rules per verificare il matching

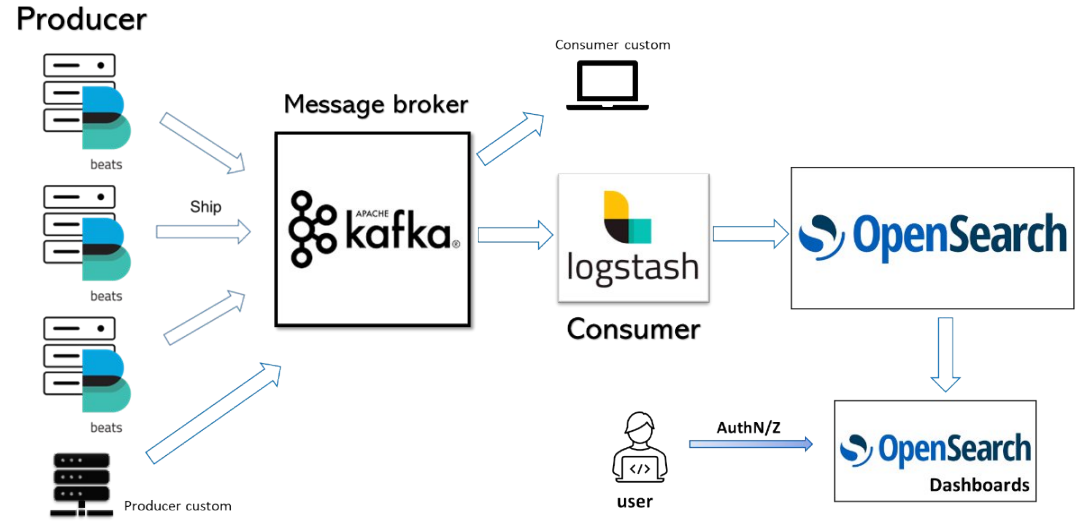
Security Response

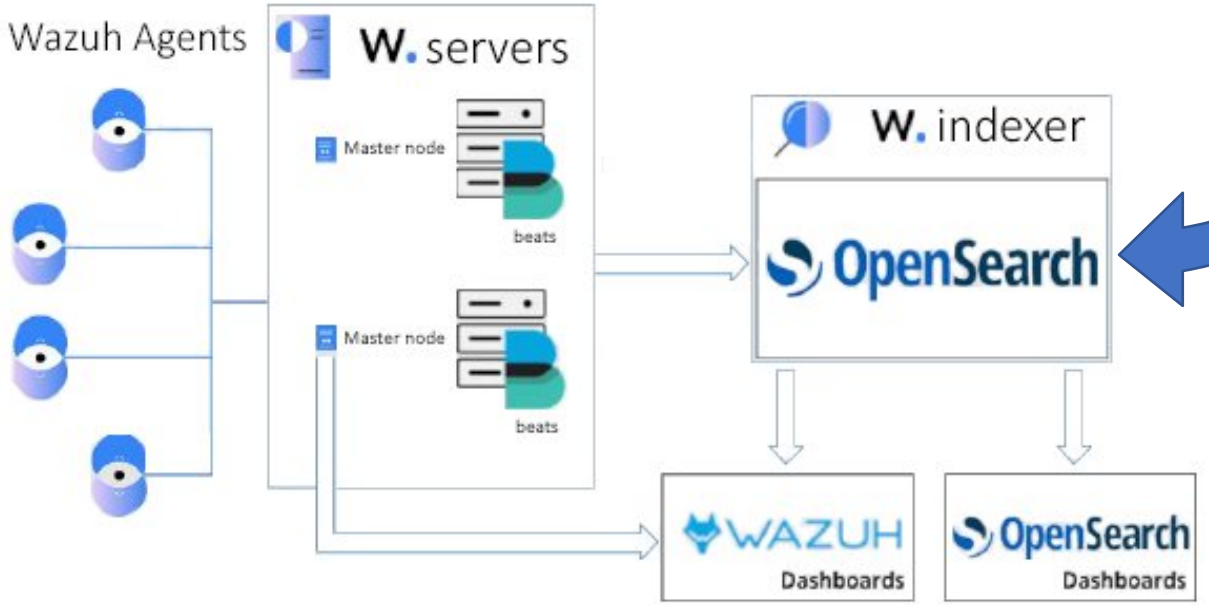
Vulenarbility Scanner and Active Response



Abilitando il Vunerabilty Scanner è possibile monitorare le vulnerabilità (CVE) presenti sulle macchine, opzione di default è disabilitata e occorre lavorare in OSSEC per renderla attiva, inoltre ogni distribuzione va customizzato secondo la propria distro

Big Data Platform Integration





Dettagli

- Dati presi dagli agents
- Compatibilità logs

Attenzione

Verifica compatibilità:

Wazuh <—> Opensearch

V.Agents ≤ V.Servers OK

V.Agents > V. Servers ??

MISP

- Integrare MISP con Wazuh NON E' un'integrazione diretta, è necessario l'utilizzo di script in Python, interrogazione delle API e (nel nostro caso custom) configurazione ad-hoc di Auditd per il settaggio delle directory specifiche da tenere sott'occhio.

VANTAGGI

- Arricchimento dei dati sulle minacce: MISP contiene informazioni dettagliate sulle minacce, compresi indicatori di compromissione (IOCs), e dettagli su campioni di malware
- Rilevamento più preciso delle minacce: Utilizzando le informazioni sulle minacce provenienti da MISP, Wazuh può migliorare la sua capacità di rilevamento, consentendo di identificare e rispondere più rapidamente alle minacce in corso.
- Automatizzazione delle risposte alle minacce: Utilizzando le informazioni sulle minacce da MISP, è possibile automatizzare le risposte in Wazuh, ad esempio bloccando gli IP sospetti, aggiornando le regole di rilevamento o avviando azioni correttive di auto-response supervisionate.

Lo script .py usato deriva da uno script gia presente su GitHub, ma riscritto per le nostre macchine Linux

Custom Setting for Specific Folders

```
DETECTION:

Sugli host:
auditctl -w /tmp -p x -k audit-wazuh-x
auditctl -w /var/tmp -p x -k audit-wazuh-x

Su manager:
/var/ossec/etc/shared/default/agent.conf

<agent_config os="Linux">
  <syscheck>
    <directories check_all="yes" realtime="yes">/tmp</directories>
    <directories check_all="yes" realtime="yes">/var/tmp</directories>
  </syscheck>
</agent_config>
```

- La configurazione mostra i settaggi che sono necessari affinché Auditd possa monitorare ciò che avviene nell'endpoint, e la configurazione specifica del manager per il controllo delle folders nelle macchine Linux secondo la nomenclatura che scegliamo

Oct 26, 2023 @ 15:39:27.097 | MISP - IoC found in Threat Intel - Category: Payload delivery, Attribute: sh.pyc | 12 | 100622

Table | JSON | Rule

@timestamp	2023-10-26T13:39:27.097Z
_id	F8M2bIsBys7TCUZTIMRt
agent.id	001
agent.ip	131.154.129.146
agent.name	elk-test-1.cr.cnaf.infn.it
data.misp.category	Payload delivery
data.misp.event_id	827
data.misp.source.description	Audit: Watch - Execute access: ./sh.pyc.: ./sh.pyc
data.misp.type	filename
data.misp.value	sh.pyc
decoder.name	json
id	1698327567.548690950
input.type	log
location	misp
manager.name	manager-wazuh-01.cnaf.infn.it
rule.description	MISP - IoC found in Threat Intel - Category: Payload delivery, Attribute: sh.pyc
rule.firedtimes	1
rule.groups	misp, misp_alert
rule.id	100622
rule.level	12
rule.mail	true
timestamp	2023-10-26T15:39:27.097+0200

Dati Endponit

ID nel Database MISP
Con questo posso vedere i dettagli direttamente nel MISP per analisi extra

AUDITD viene usato per tenere sotto osservazione specifiche direcorty
cosi facendo si pososno verificare i 3 step di rischio

- Creazione del File Malevolo
- Cambio CHMOD per tentare l'esecuzione
- Esecuzione del file

File che trova check sul MISP basandosi sul check dello SHA o del MD5

La rule.description serve per automatizzare le response

Next Steps for MISP

Mar 22, 2024 @ 19:16:43.425	008	wn-200-04-01-01-a.cr.cnaf.infn.it	MISP - IoC found in Threat Intel - Category: Payload delivery, Attribute: 0gcgs.reversed|d41d8cd98f00b204e9800998ecf8427e

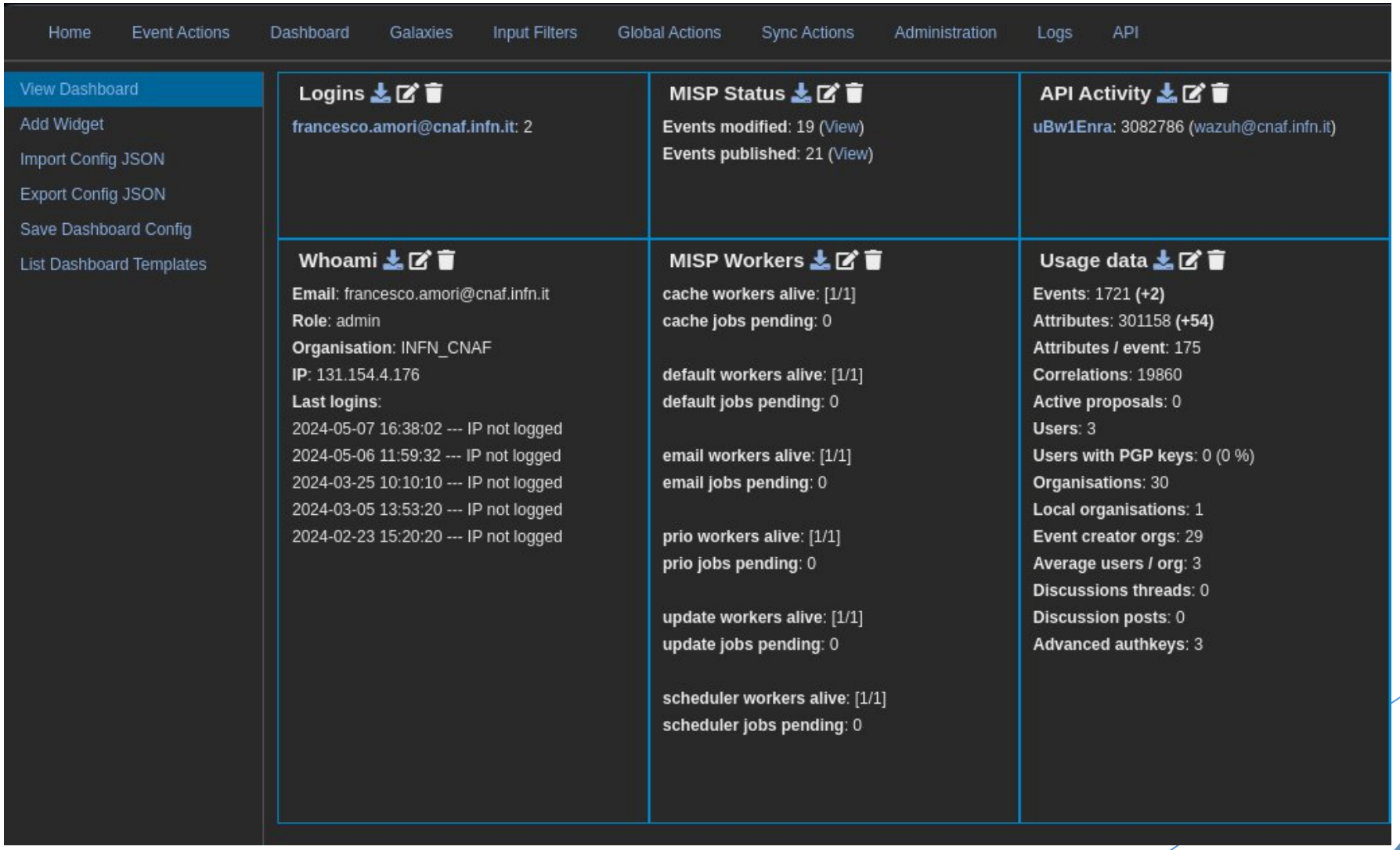
Table JSON Rule

@timestamp	2024-03-22T18:16:43.425Z
_id	UA9hZ44BpVaeJx3HKtNz
agent.id	008
agent.ip	131.154.197.114
agent.name	wn-200-04-01-01-a.cr.cnaf.infn.it
data.misp.category	Payload delivery
data.misp.event_id	127
data.misp.source.description	File added to the system.: /tmp/OUT
data.misp.type	malware-sample
data.misp.value	0gcgs.reversed|d41d8cd98f00b204e9800998ecf8427e
decoder.name	json
id	1711131403.861325967
input.type	log
location	misp
manager.name	manager-wazuh-01.cnaf.infn.it
rule.description	MISP - IoC found in Threat Intel - Category: Payload delivery, Attribute: 0gcgs.reversed|d41d8cd98f00b204e9800998ecf8427e
rule.firedtimes	2266
rule.groups	misp, misp_alert
rule.id	100622
rule.level	12
rule.mail	true
timestamp	2024-03-22T19:16:43.425+0100

Indica l'aggiunta di un file in una directory sensibile

L'attributo trova riscontro nel db del MISP e avendo un match segnala l'evento

Dashboard MISP



Suricata IDS

- L’integrazione di Suricata IDS a differenza di MISP è diretta per ciascun endpoint monitorato da Wazuh, vale a dire utilizzare l’IDS come Sniffer del traffico che avviene sulla singola macchina, cosi facendo possiamo customizzare le rules in base alla tipologia di macchina che si vuole monitorare.

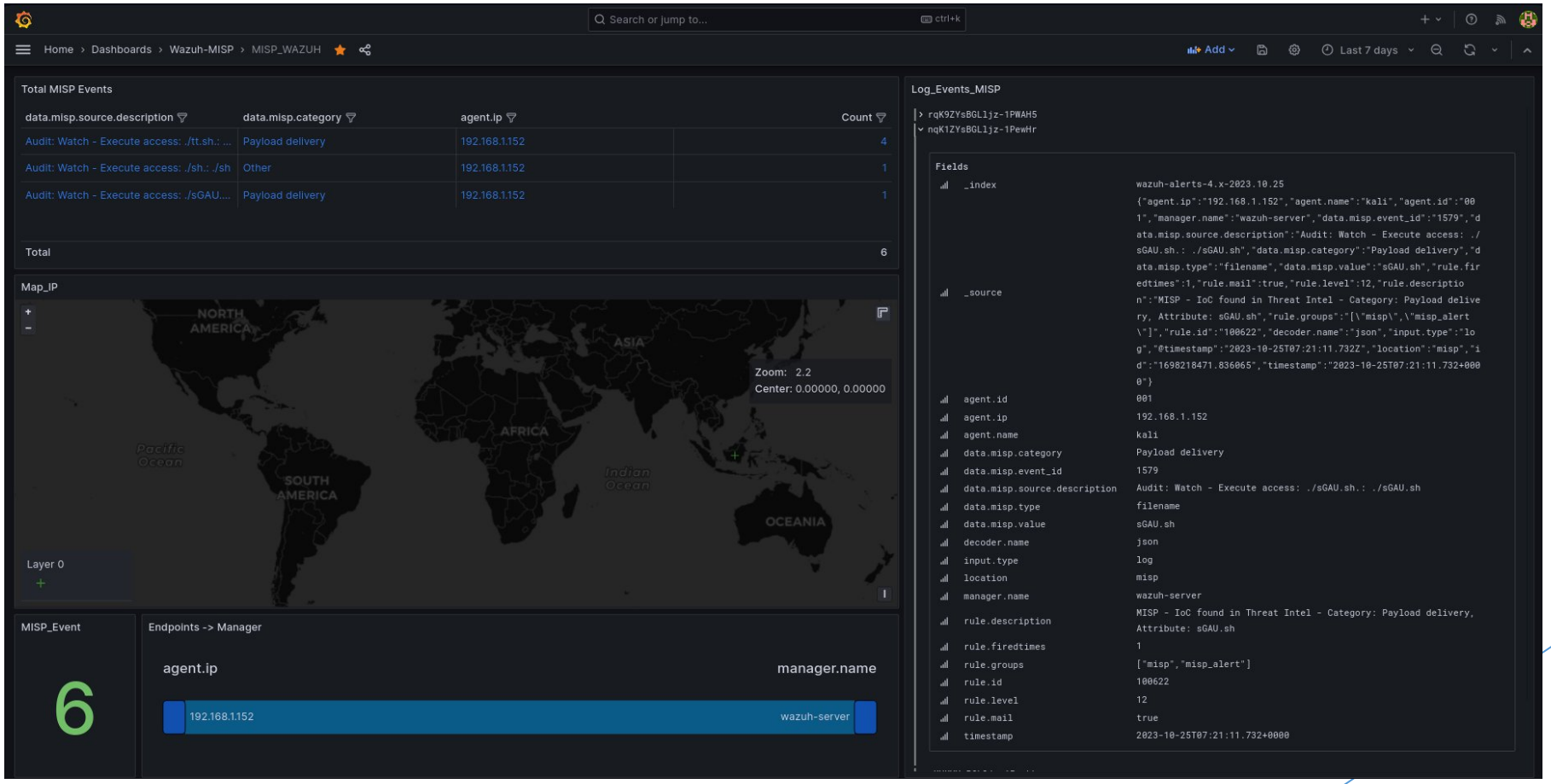
VANTAGGI

- Rilevamento delle intrusioni sulla rete con custom-rules: Integrare Suricata con Wazuh consente di sfruttare le capacità avanzate di rilevamento delle minacce di Suricata insieme alle funzionalità di gestione degli eventi e di risposta agli eventi di sicurezza di Wazuh.
- Allargamento della visibilità della rete: Suricata analizza il traffico di rete in tempo reale e rileva varie attività sospette, come tentativi di intrusioni, malware, exploit ecc... Integrare Suricata con Wazuh consente di allargare la visibilità della rete.
- Risposta rapida alle minacce: Integrando Suricata con Wazuh, è possibile automatizzare le risposte alle minacce, ad esempio bloccando gli indirizzi IP sospetti o aggiornando le regole di rilevamento delle minacce in tempo reale. Questo consente di rispondere più rapidamente alle minacce e di mitigare gli attacchi in corso.


May 7, 2024 @ 19:46:39.653
Suricata: Alert - ET EXPLOIT ownCloud Information Disclosure Attempt (CVE-2023-49103)
3
86601
data.alert.metadata.attack_target
Server
data.alert.metadata.confidence
High
data.alert.metadata.created_at
2023_12_07
data.alert.metadata.cve
CVE_2023_49103
data.alert.metadata.deployment
Internal, Perimeter
data.alert.metadata.former_category
EXPLOIT
data.alert.metadata.performance_impact
Low
data.alert.metadata.signature_severity
Major
Dati realtivi all'allert sulla base delel rules presenti in Suricata
data.alert.metadata.updated_at
2024_01_09
data.alert.rev
1
data.alert.severity
2
data.alert.signature
ET EXPLOIT ownCloud Information Disclosure Attempt (CVE-2023-49103)
Tipologia di Alert
data.alert.signature_id
2049614
data.alert.source.ip
20.27.218.246
data.alert.source.port
59168
data.alert.target.ip
131.154.48.135
Dati di rete relativi a IPs e Porte usate

Grafana

Custom Dashboard [per specifici eventi, in questo caso MISP]



Gruppo di Lavoro & Riferimenti

Security Team

- Francesco Amori
- Vincenzo Ciaschini

BDP Team

- Enrico Fattibene
- Antonio Falabella
- Diego Michelotto

Riferimenti (Slides & Immagini)

– General purpose data streaming platform for log analysis, anomaly detection and security protection
DOI 10.5281/zenodo.8285677

Grazie per l’attenzione