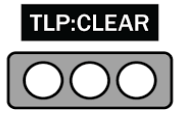
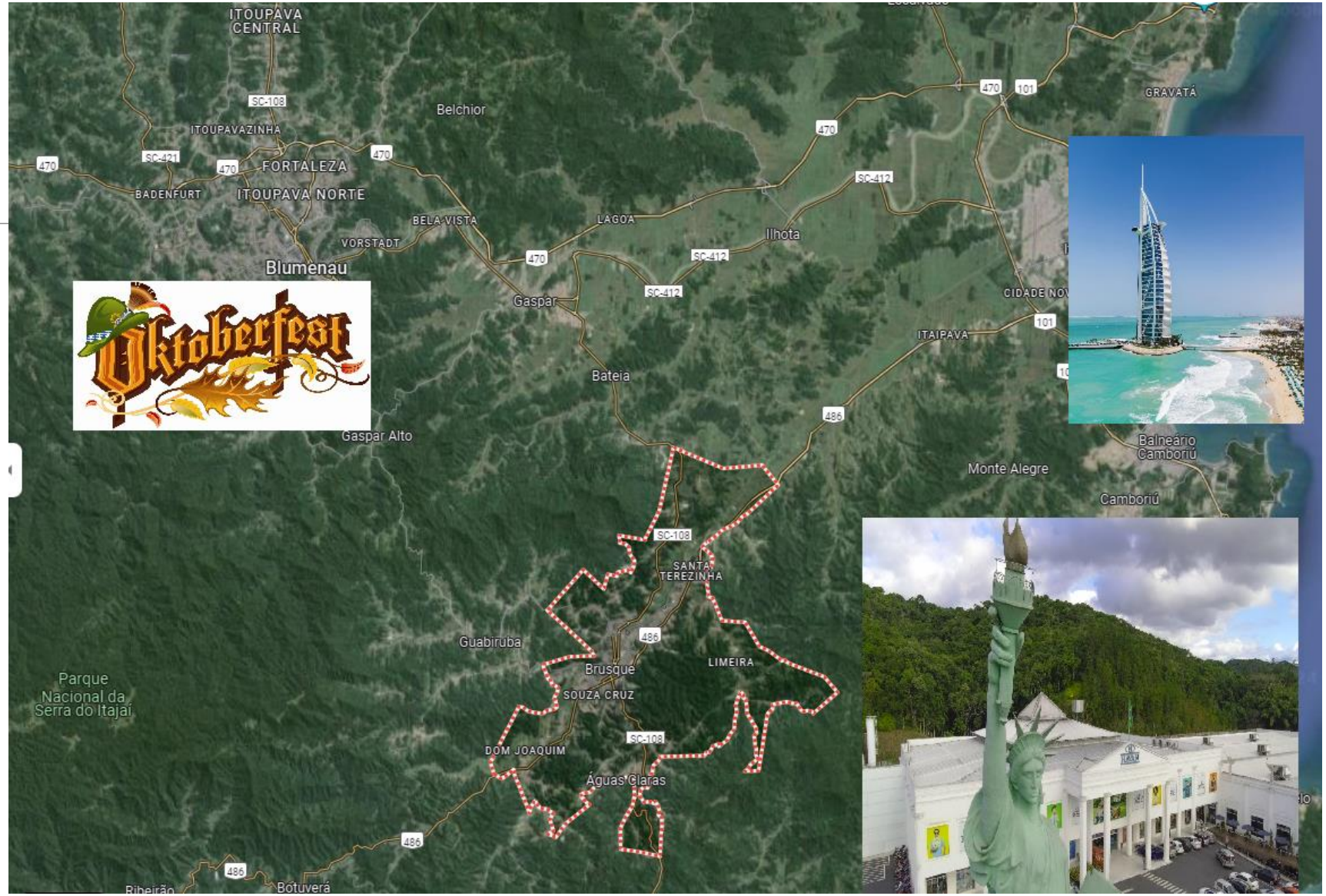
# AUTOMATIZAÇÃO DE PROCESSOS DE SOC COM FERRAMENTAS OPEN-SOURCE

**ALEXANDRE KRIEGER**, AK CONSULTORIA E GESTÃO EM TECNOLOGIAS

ESTA APRESENTAÇÃO ABORDARÁ COMO AS FERRAMENTAS AUTOMATIZADAS PODEM OTIMIZAR A EFICIÊNCIA NO TRATAMENTO DE INCIDENTES DE SEGURANÇA. DISCUTIREI UM ESTUDO DE CASO SOBRE  A IMPLEMENTAÇÃO EM UM AMBIENTE DE SEGURANÇA OPERACIONAL, DESTACANDO AS SEGUINTES FERRAMENTAS: **WAZUH, GRAYLOG, CORTEX, MISP E GRAFANA.** TAMBÉM SERÁ MOSTRADO UM ESTUDO DE CASO COM OBJETIVO DE EXPANDIRAS POSSIBILIDADES E APRESENTAR O DESENVOLVIMENTO DE MELHORIAS DURANTE O PROCESSO.



# Brusque




TLP:CLEAR

# Quem é o Alexandre

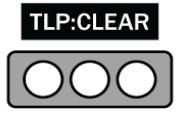
CURSOU:

- ENGENHARIA ELÉTRICA - 6/10
- SISTEMAS DE INFORMAÇÃO
- PÓS CYBER SEGURANÇA OFENSIVA ACADI-TI 04
- PÓS COMPUTAÇÃO FORENSE E SEGURANÇA DA INFORMAÇÃO IPOG RECFSBRA023

CERTIFICADOS:

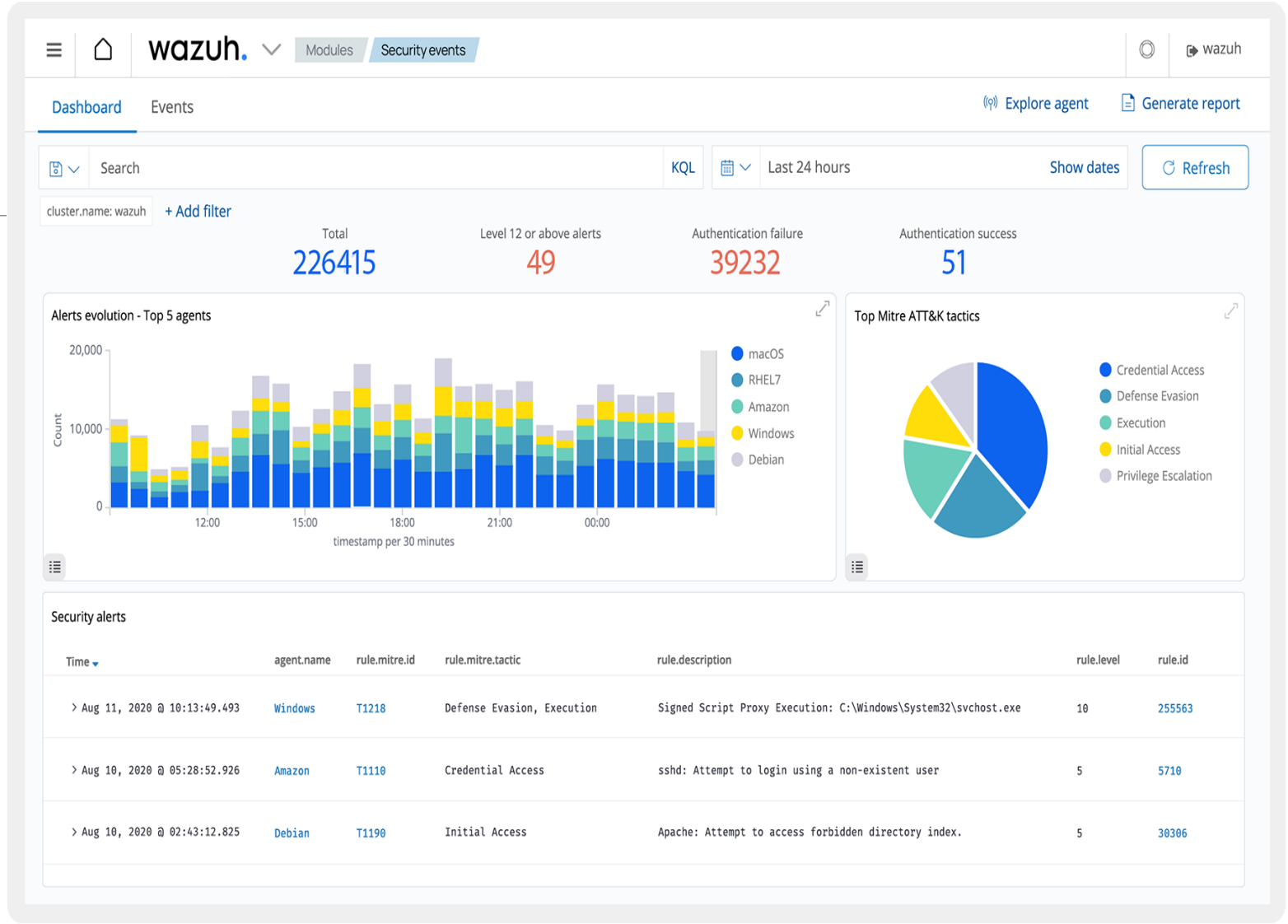
- FURUKAWA DATA CABLING SYSTEM E MCT FLUKE NETWORKS
- WINDOS SERVER 2012 ADMINISTRATION ORACLE DATABASE 10G OCA
- MIKROTIK: MTCNA-MTCRE-MTCTCE-MTCSE
- EC-COUNCIL- CEH – CHFI
- FIM - CERT

LINKEDIN: ALEXANDRE-KRIEGER



# O que é o Wazuh

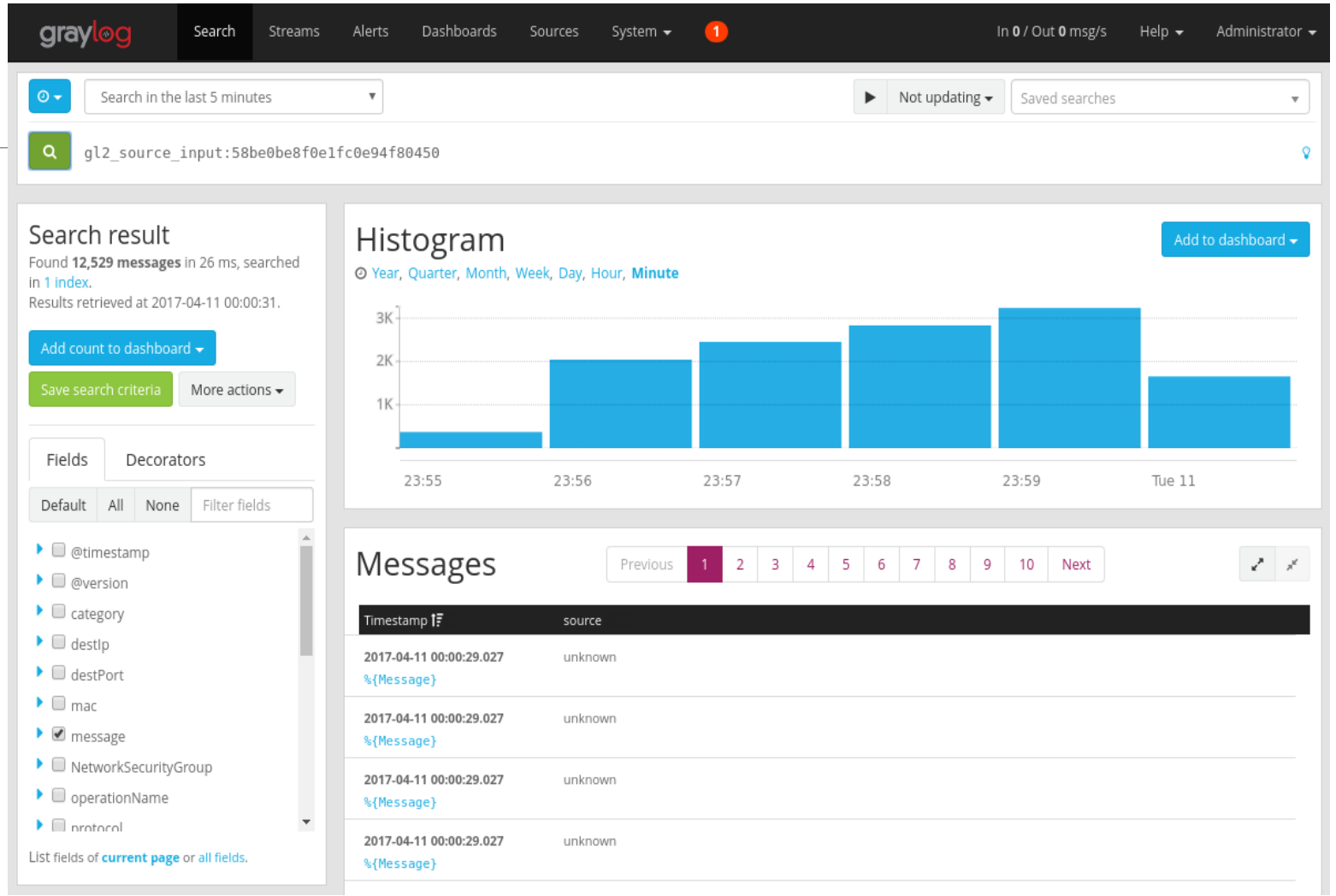
Wazuh é uma plataforma SIEM (Security Information and Event Management), que integra várias funções de segurança em uma solução unificada.




TLP:CLEAR

# O que é o Graylog

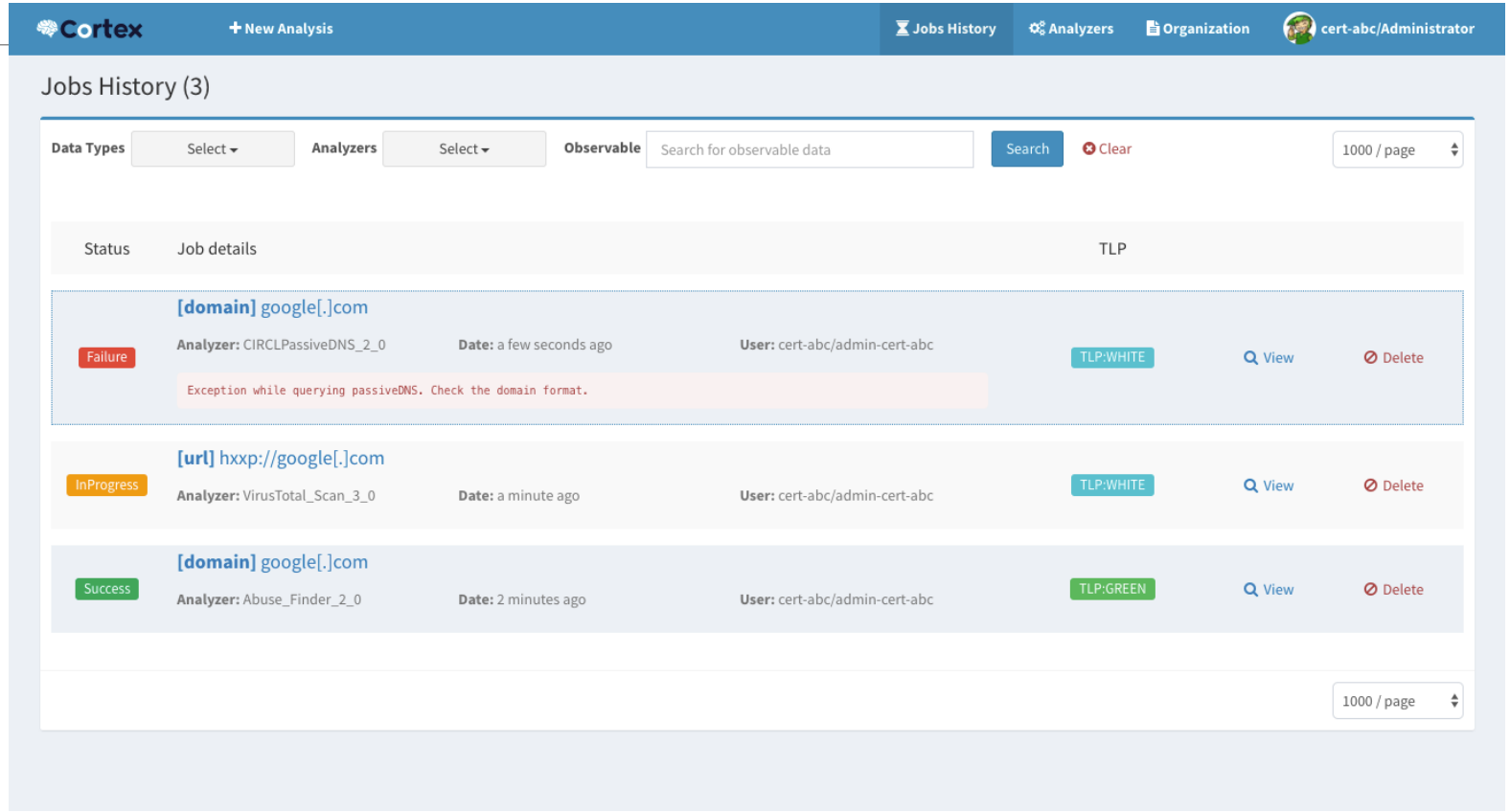
Graylog é uma plataforma de código aberto para gerenciamento de logs, projetada para coletar, indexar e analisar grandes volumes de dados de log em tempo real.




TLP:CLEAR

# O que é o Cortex

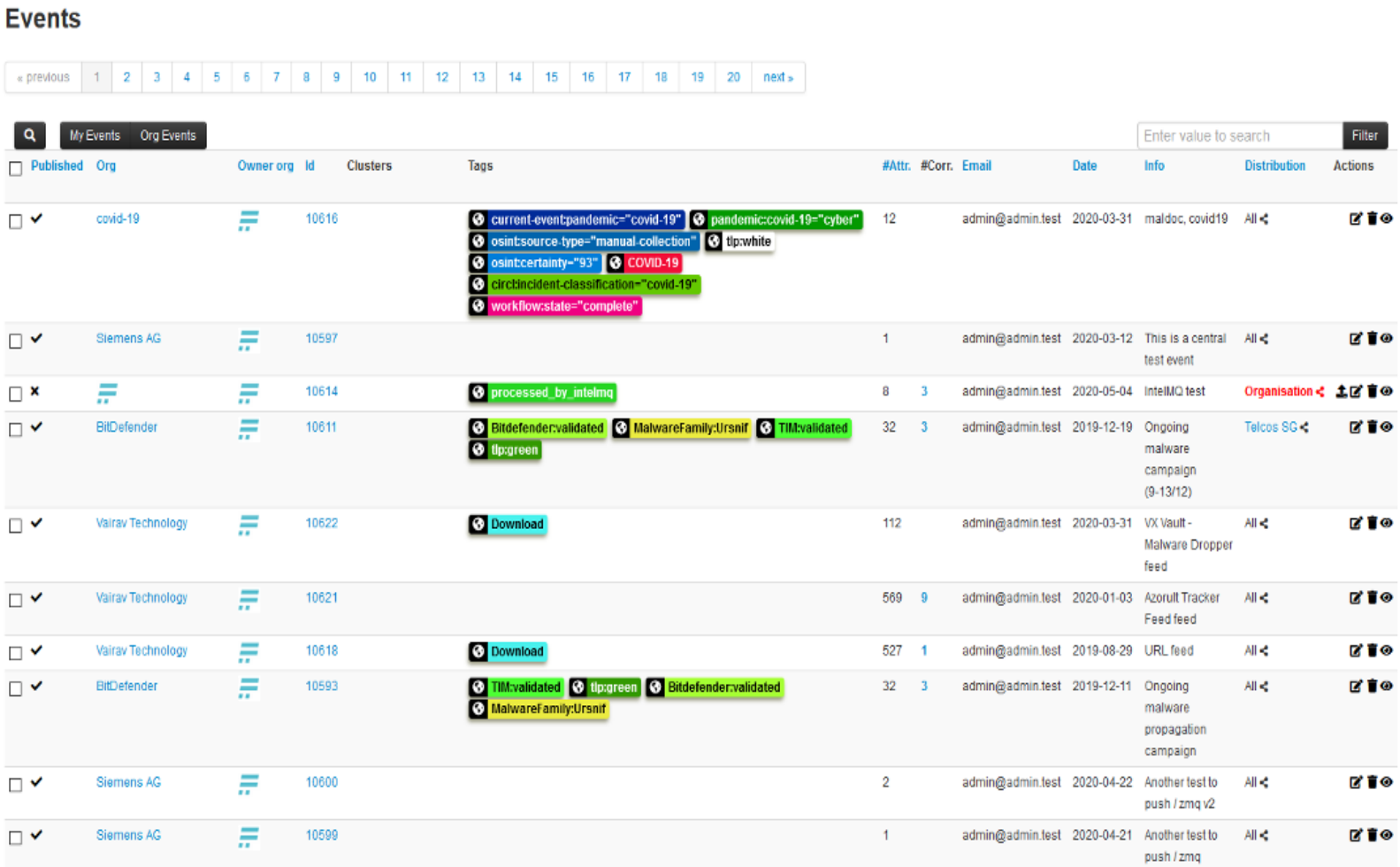
Cortex tenta resolver um problema comum frequentemente encontrado por SOCs, CSIRTs e pesquisadores de segurança, analisar observáveis que eles coletaram, em grande escala, consultando uma única ferramenta em vez de várias.




TLP:CLEAR

# O que é o Misp

MISP (Malware Information Sharing Platform & Threat Sharing) é uma plataforma de código aberto para compartilhamento de informações sobre ameaças cibernéticas, projetada para ajudar as organizações a coletar, armazenar, compartilhar e correlacionar dados sobre ameaças.



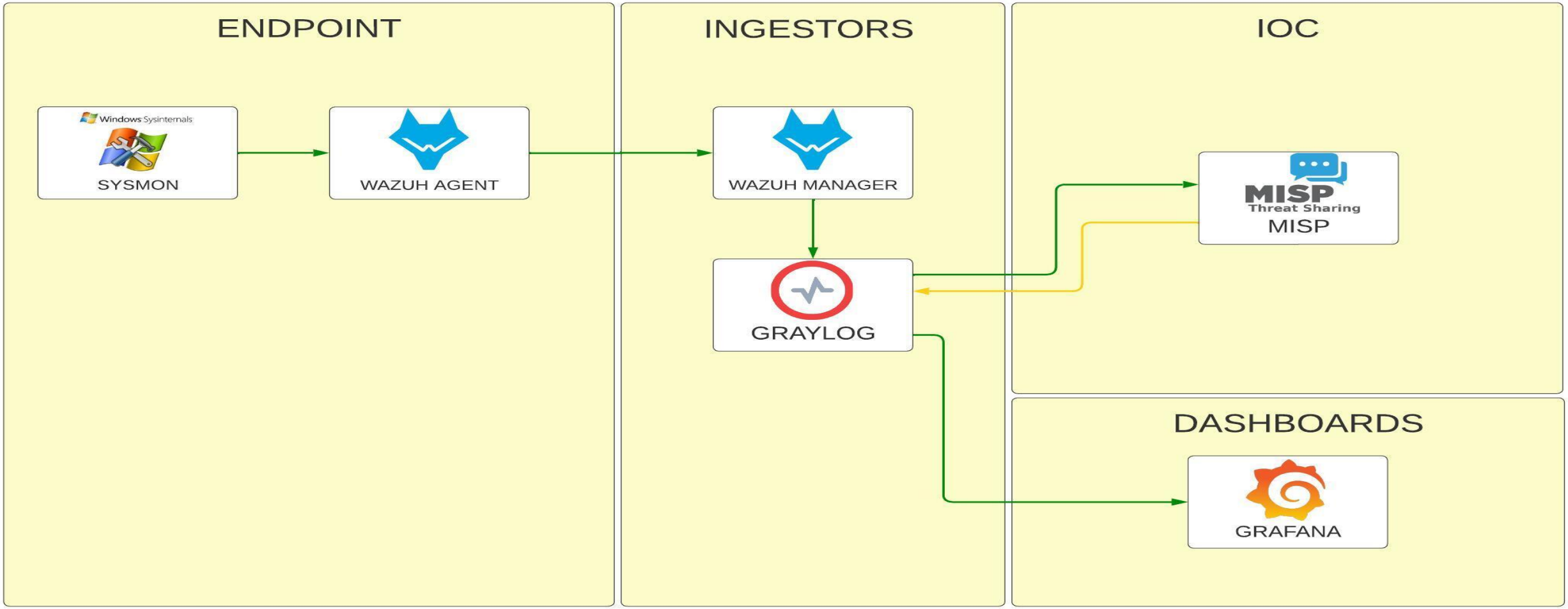

TLP:CLEAR

# O que é o Grafana

Grafana é uma plataforma de código aberto para visualização e monitoramento de dados, projetada para criar dashboards interativos e intuitivos que exibem métricas e logs em tempo real.


TLP:CLEAR

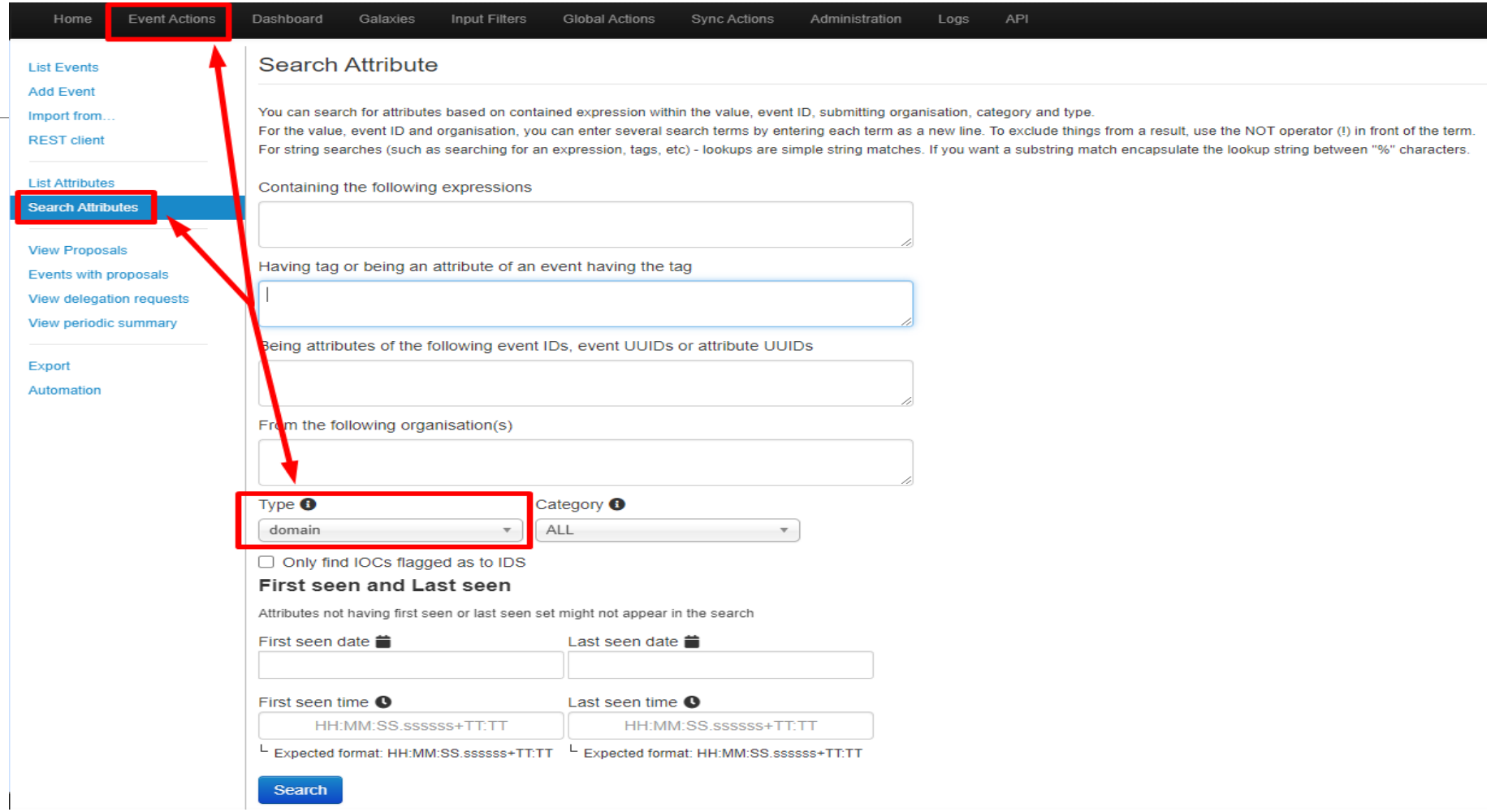
# Fluxo Simples




TLP:CLEAR

# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

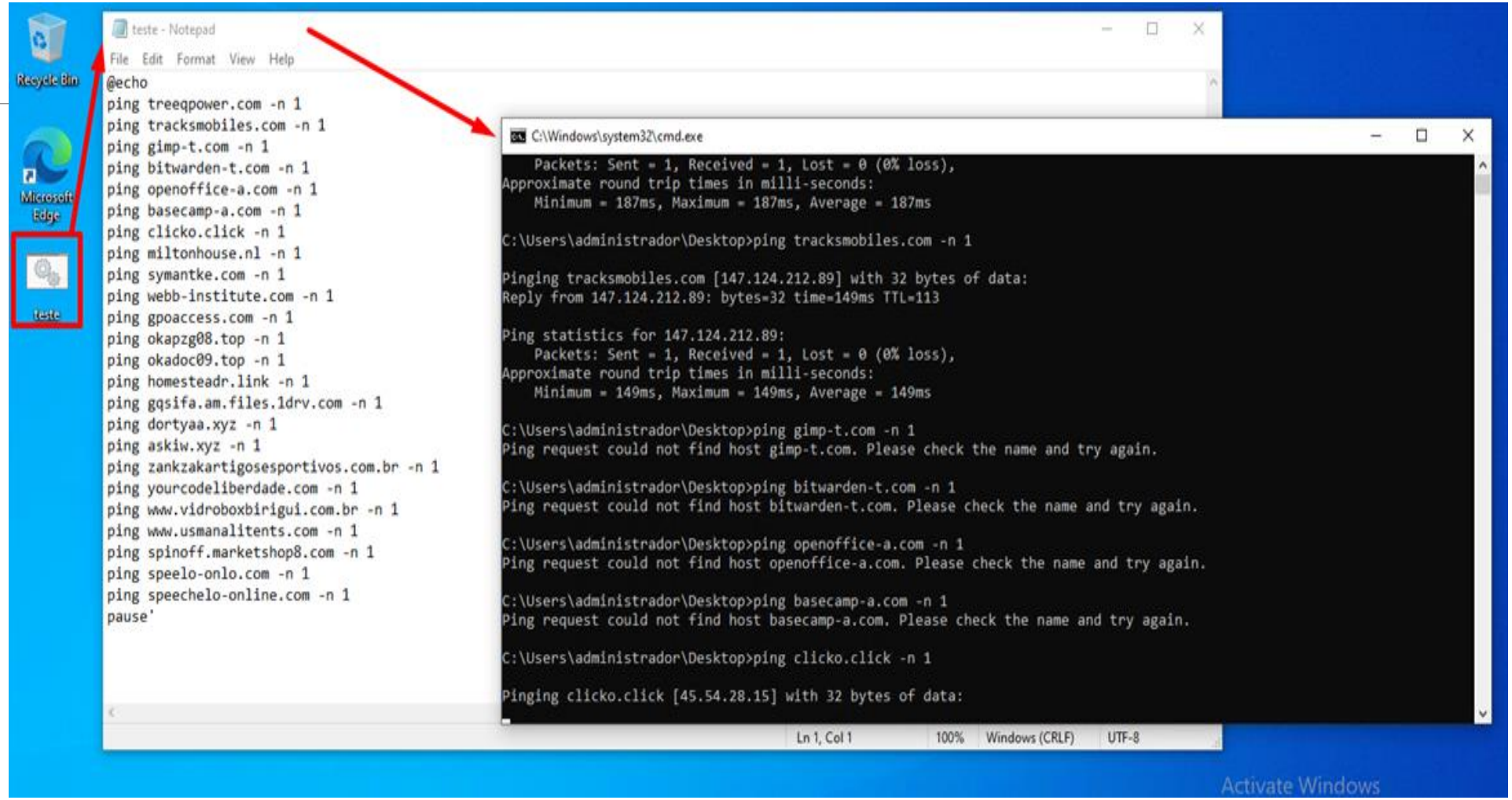
Coletar Domains dentro do MISP




TLP:CLEAR

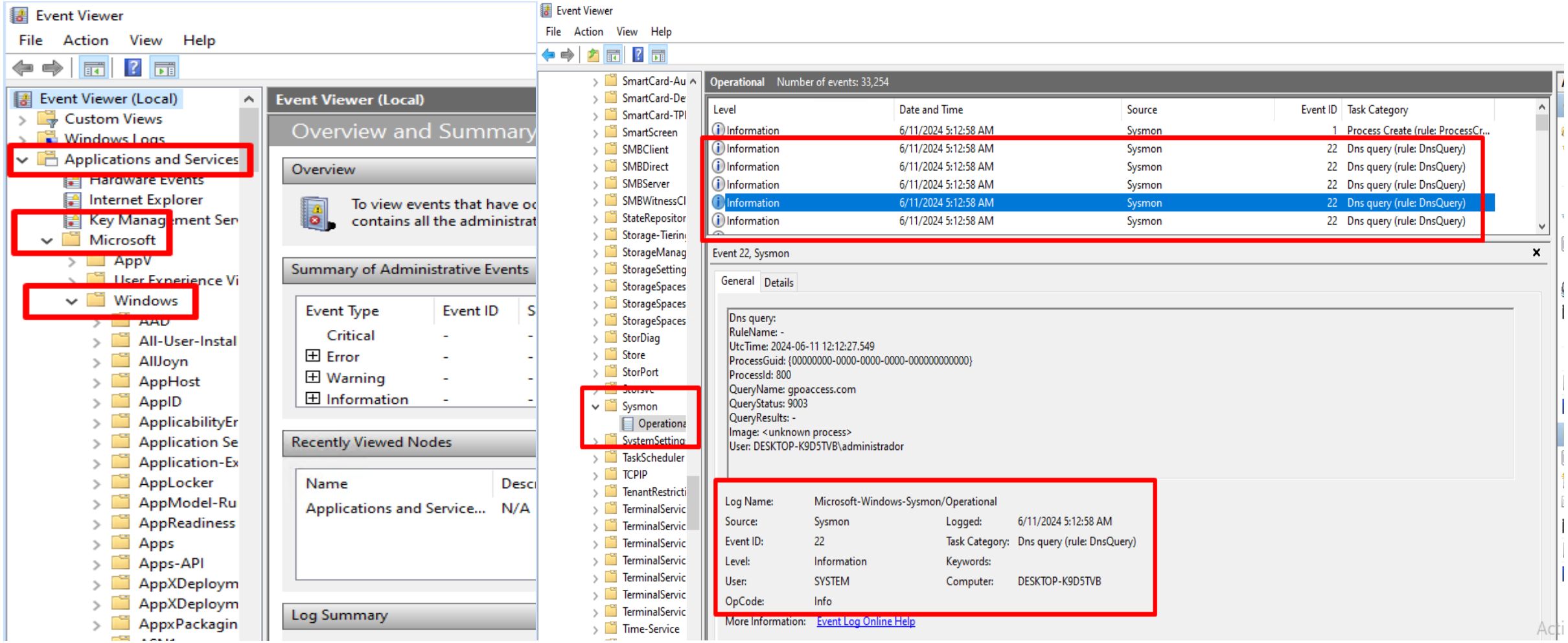
# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

Teste com .BAT




TLP:CLEAR

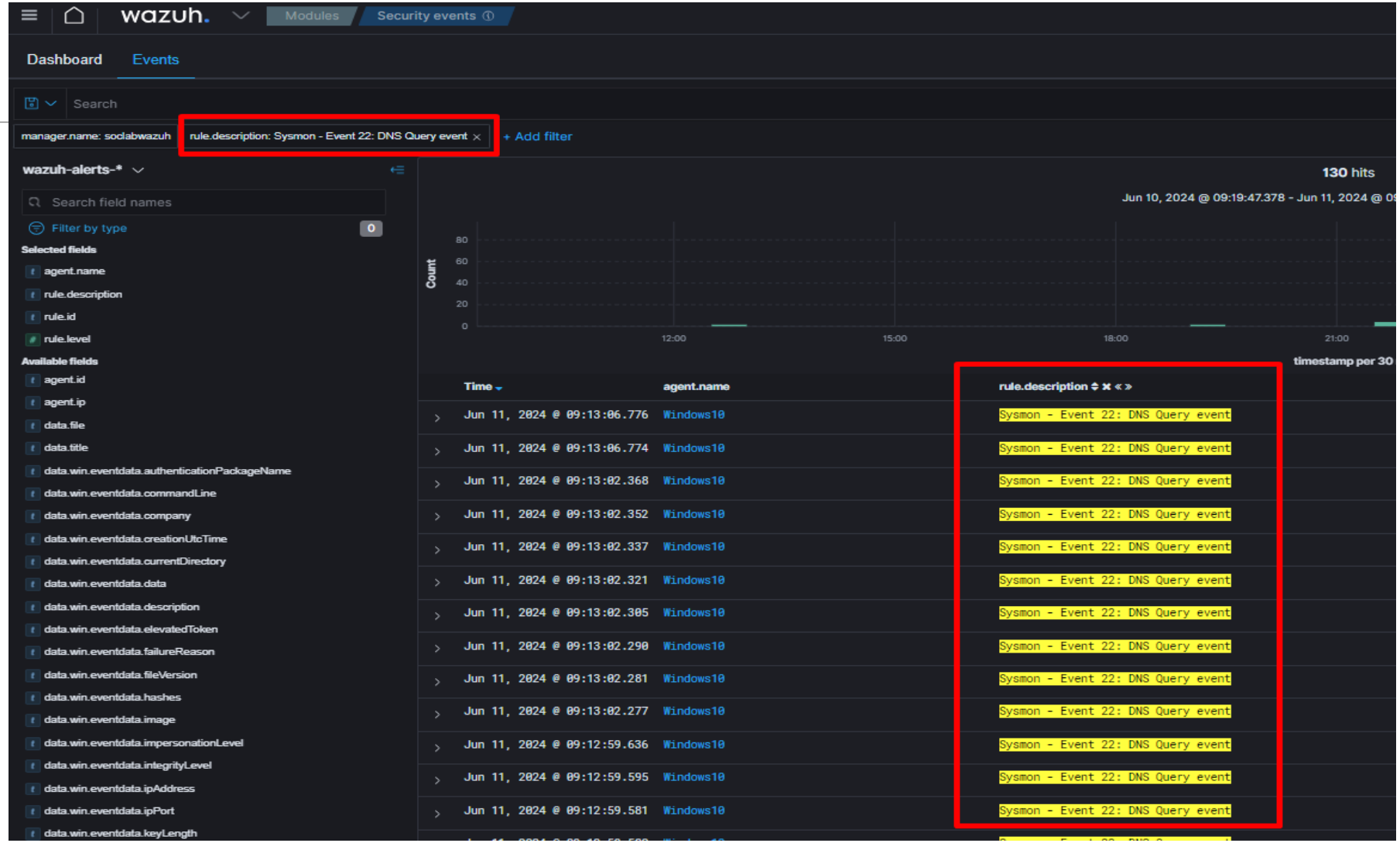
# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana




TLP:CLEAR

# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

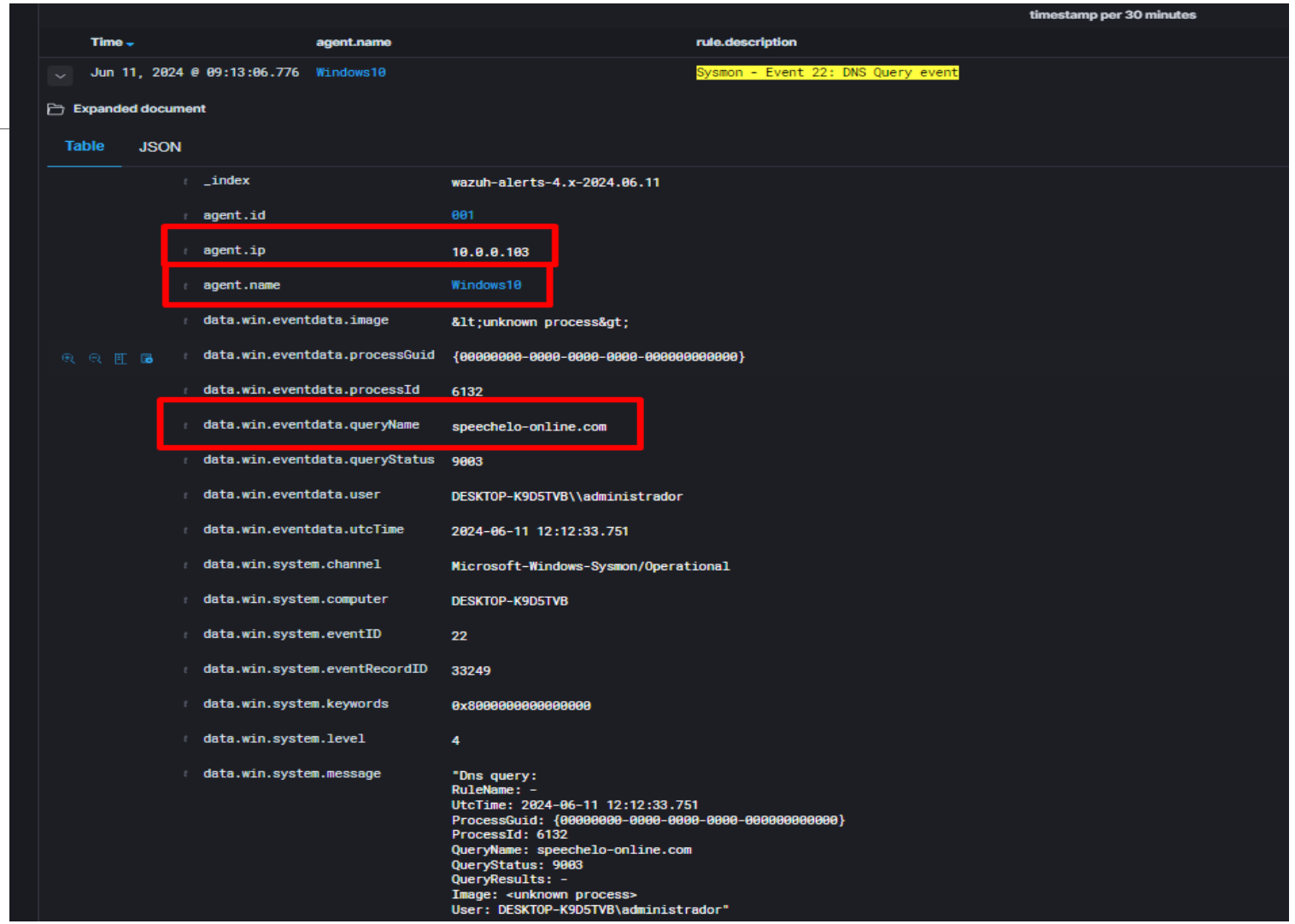
Alerta gerado no wazuh. Sysmon – Event 22 – DNS Query.




TLP:CLEAR

# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

Alerta gerado no wazuh.
Atenção as variaveis:
Agent.ip
Agent.name
QueryName



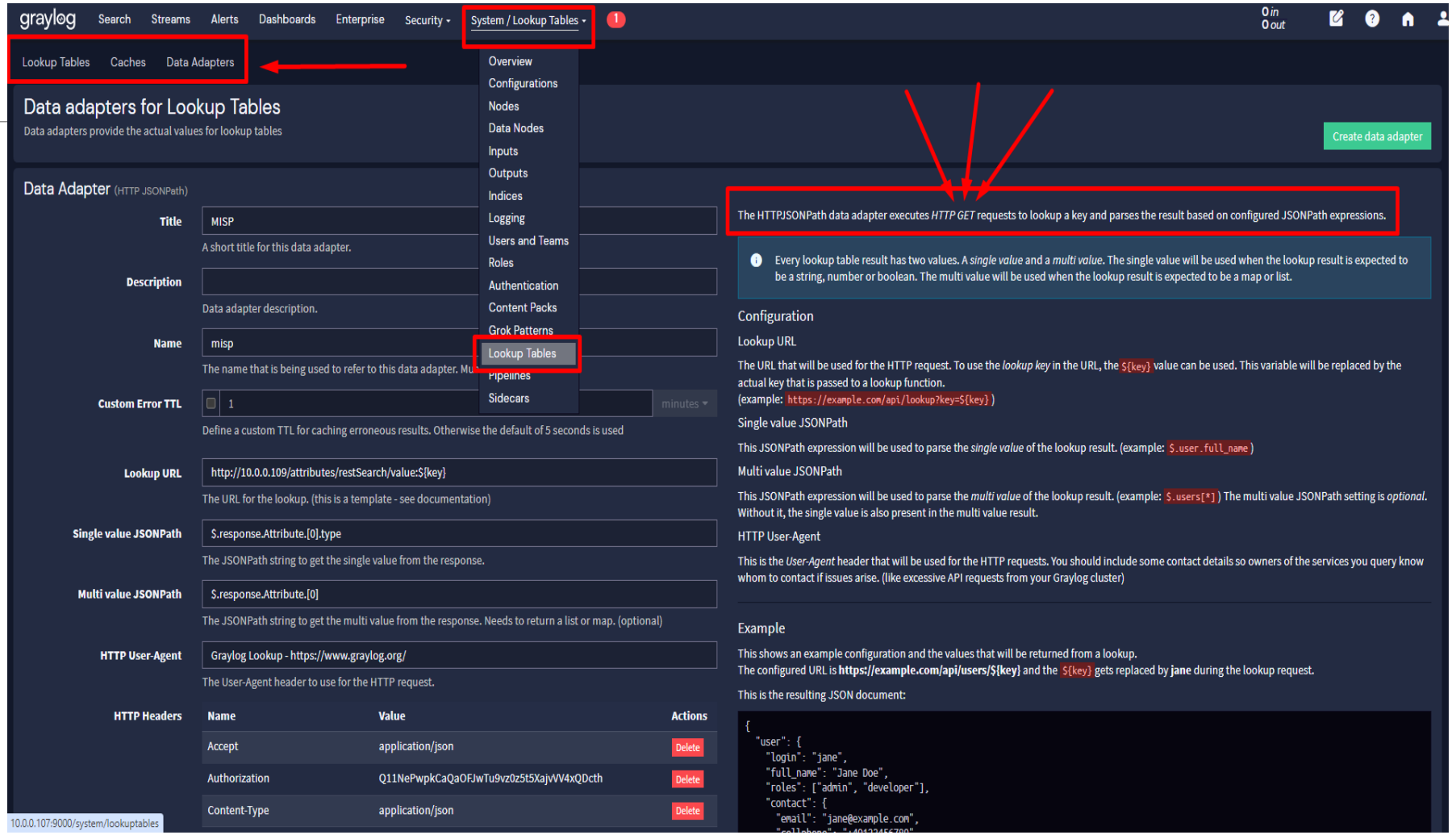

TLP:CLEAR

# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

Dentro do Graylog

Configurando a saida

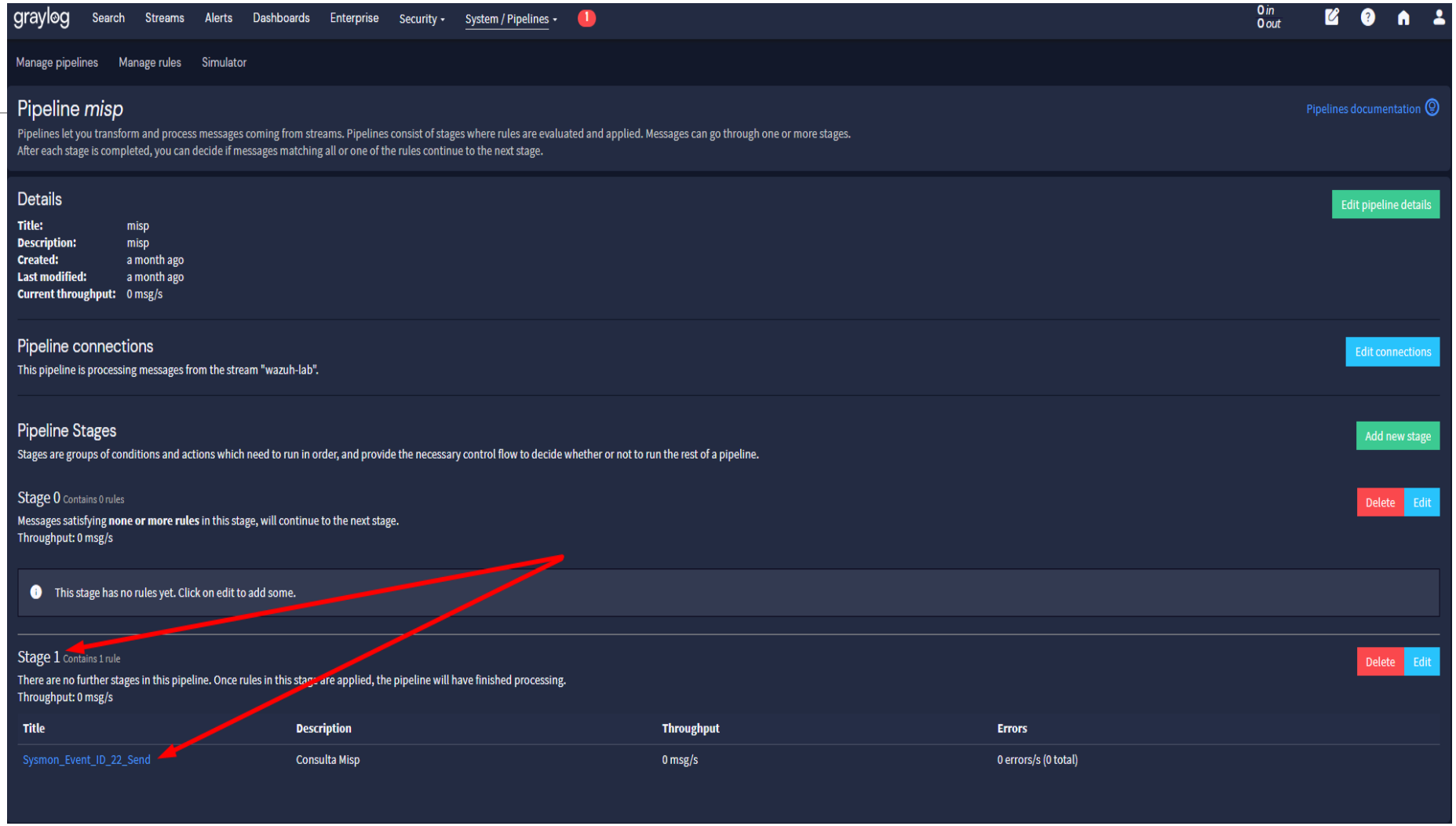
Lookup Tables:
Data Adapters + Caches + Lookup Tables



# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

Pipeline

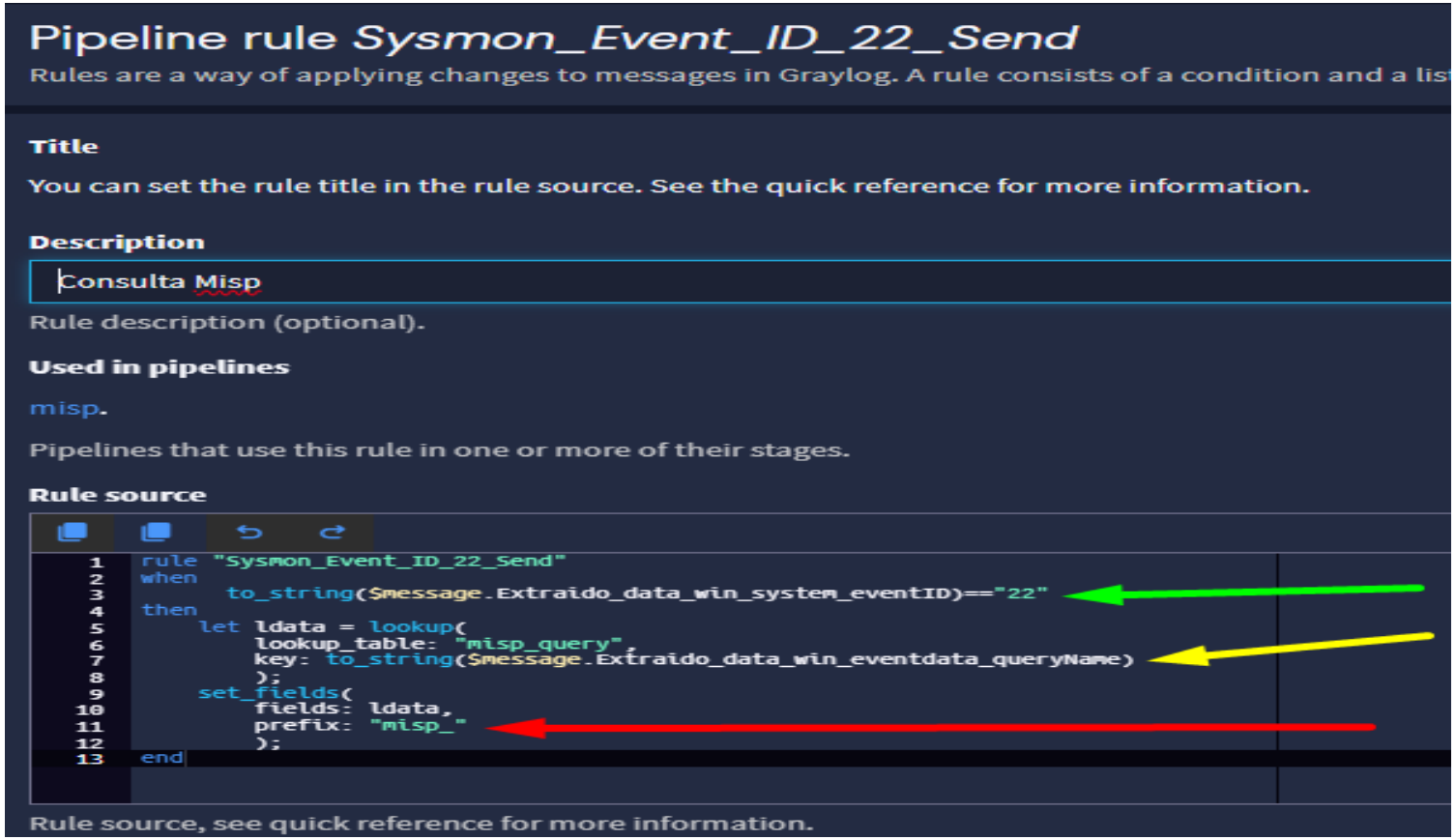
Stages + Rules




TLP:CLEAR

# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

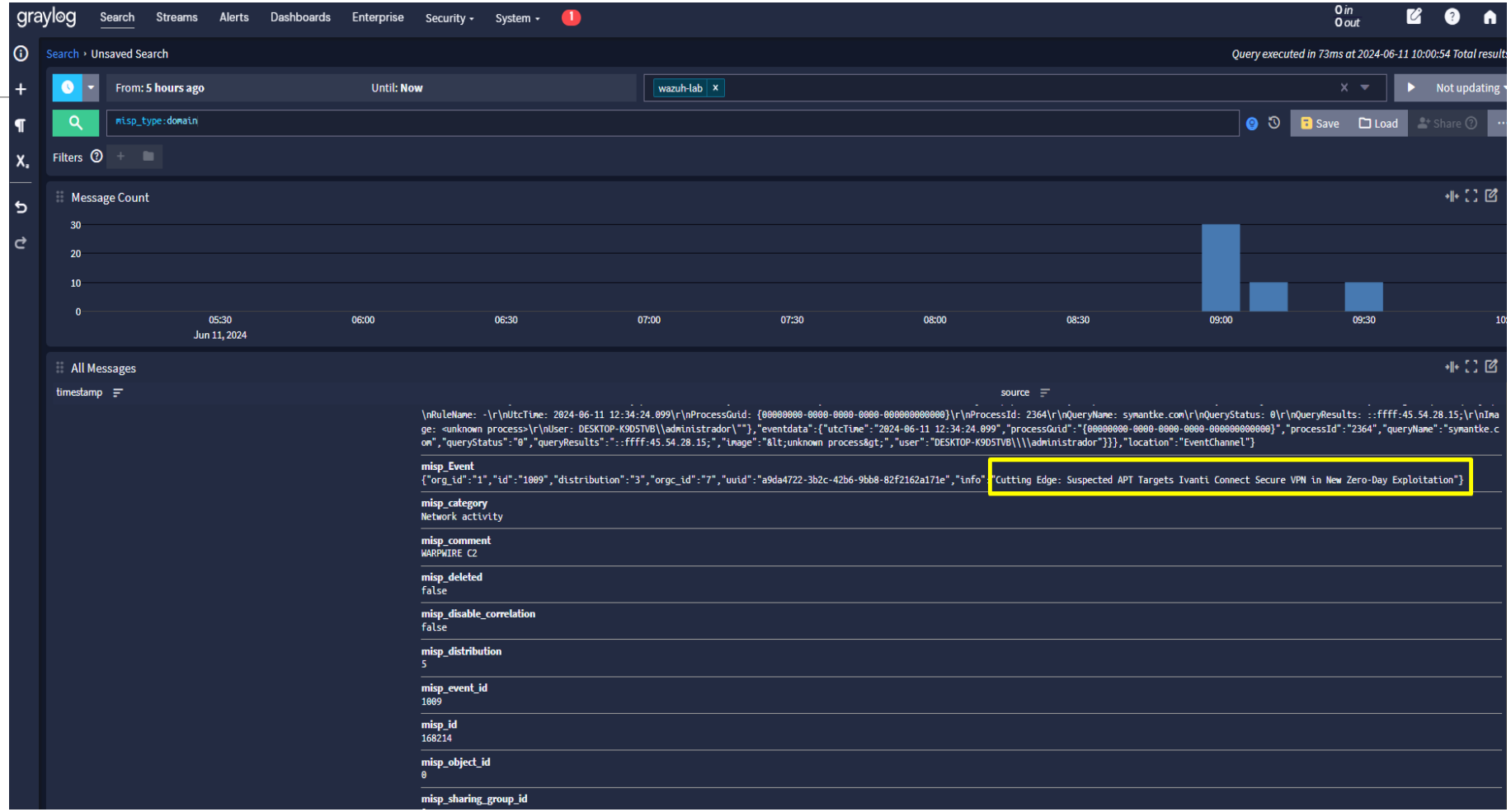
Rules




TLP:CLEAR

# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

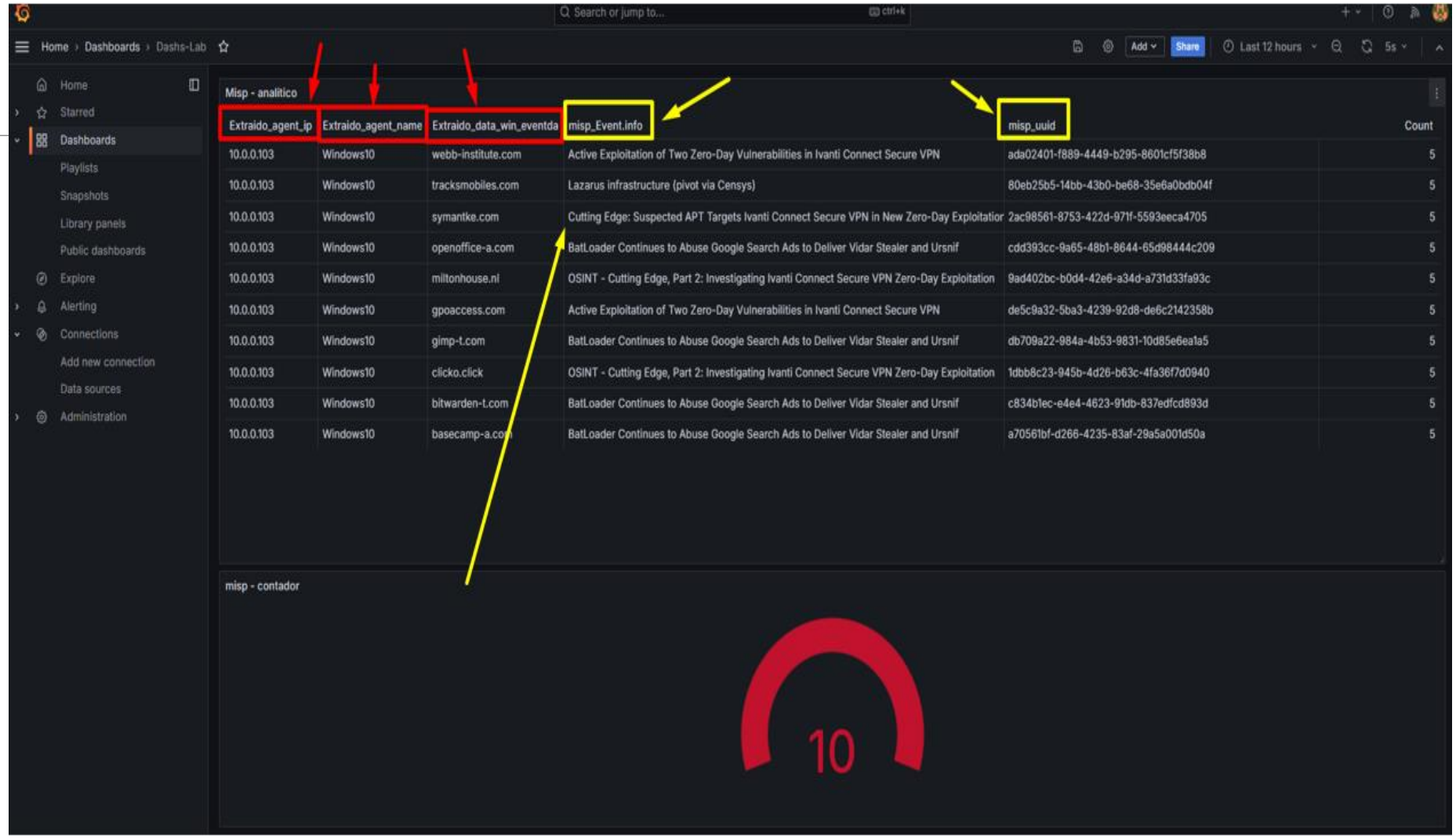
Retorno no Graylog




TLP:CLEAR

# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

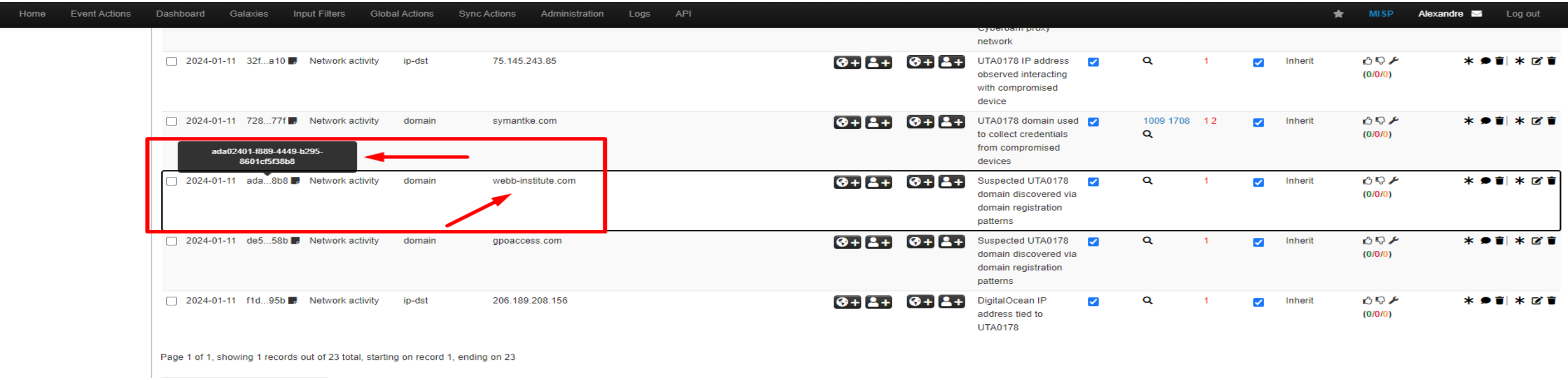
Dashboard Grafana




TLP:CLEAR

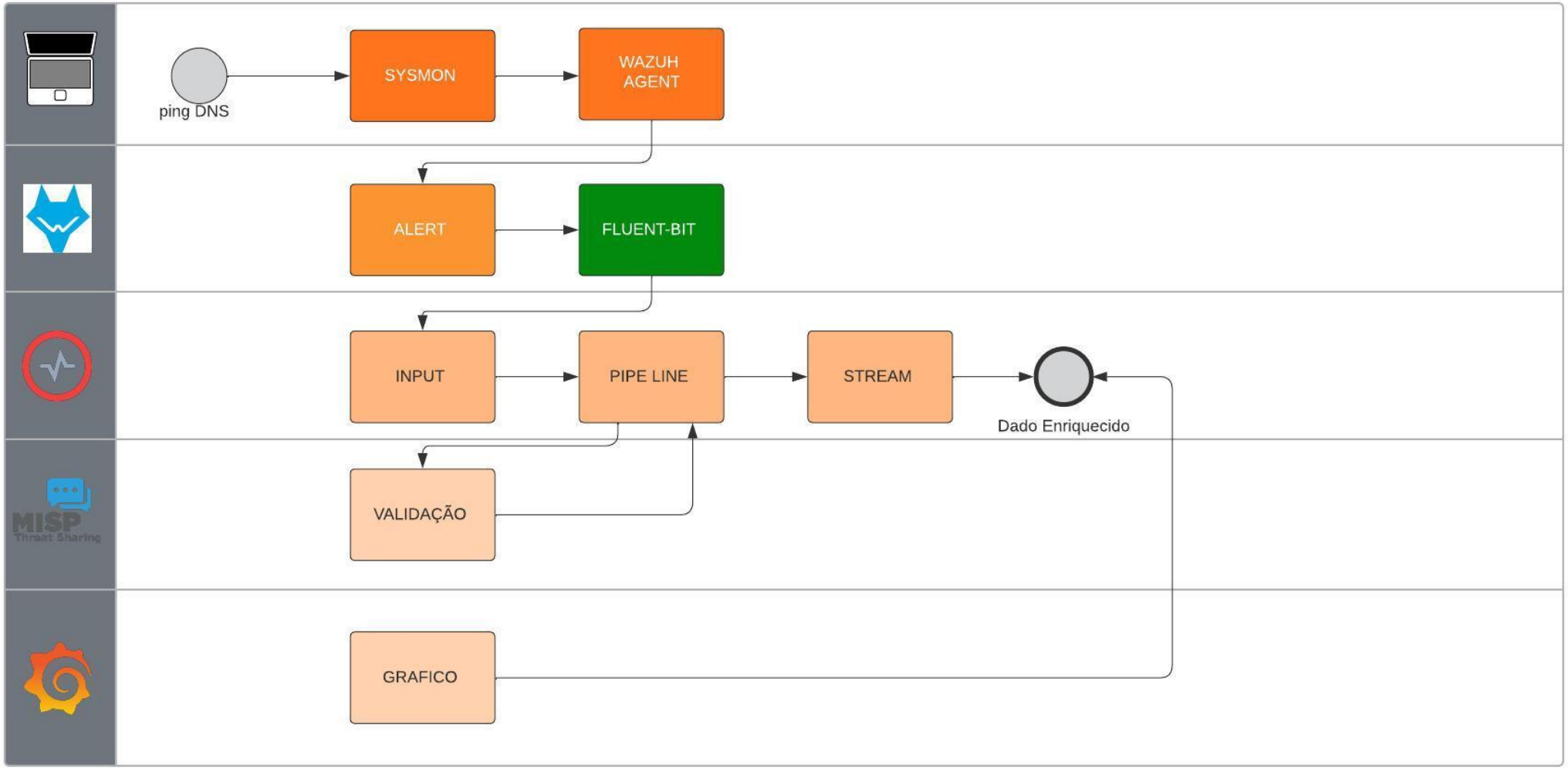
# Fluxo Simples Wazuh<>Graylog<>Misp<>Grafana

Verificando no Misp

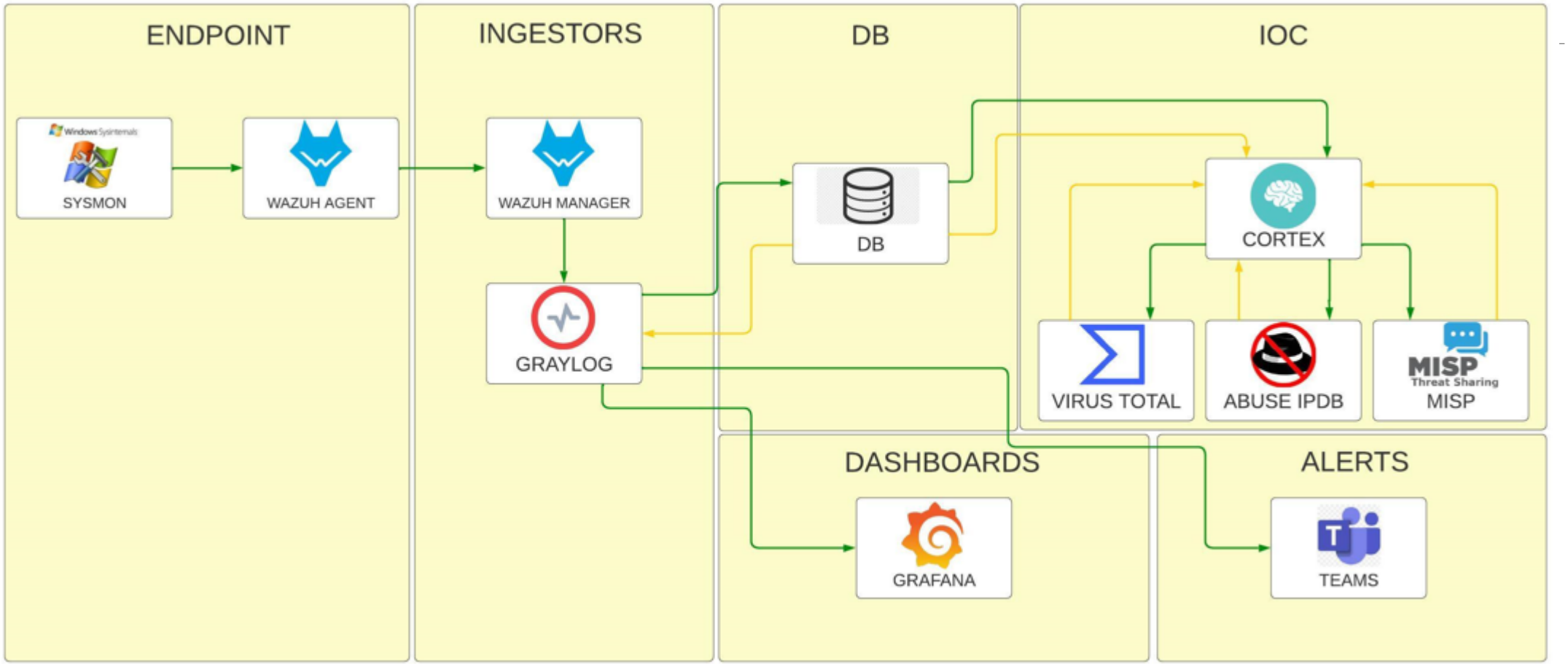

TLP:CLEAR

# O que foi feito




TLP:CLEAR

# Wazuh<>Graylog<>DB<>Cortex(VirusTotal, Abuse IP, Misp)

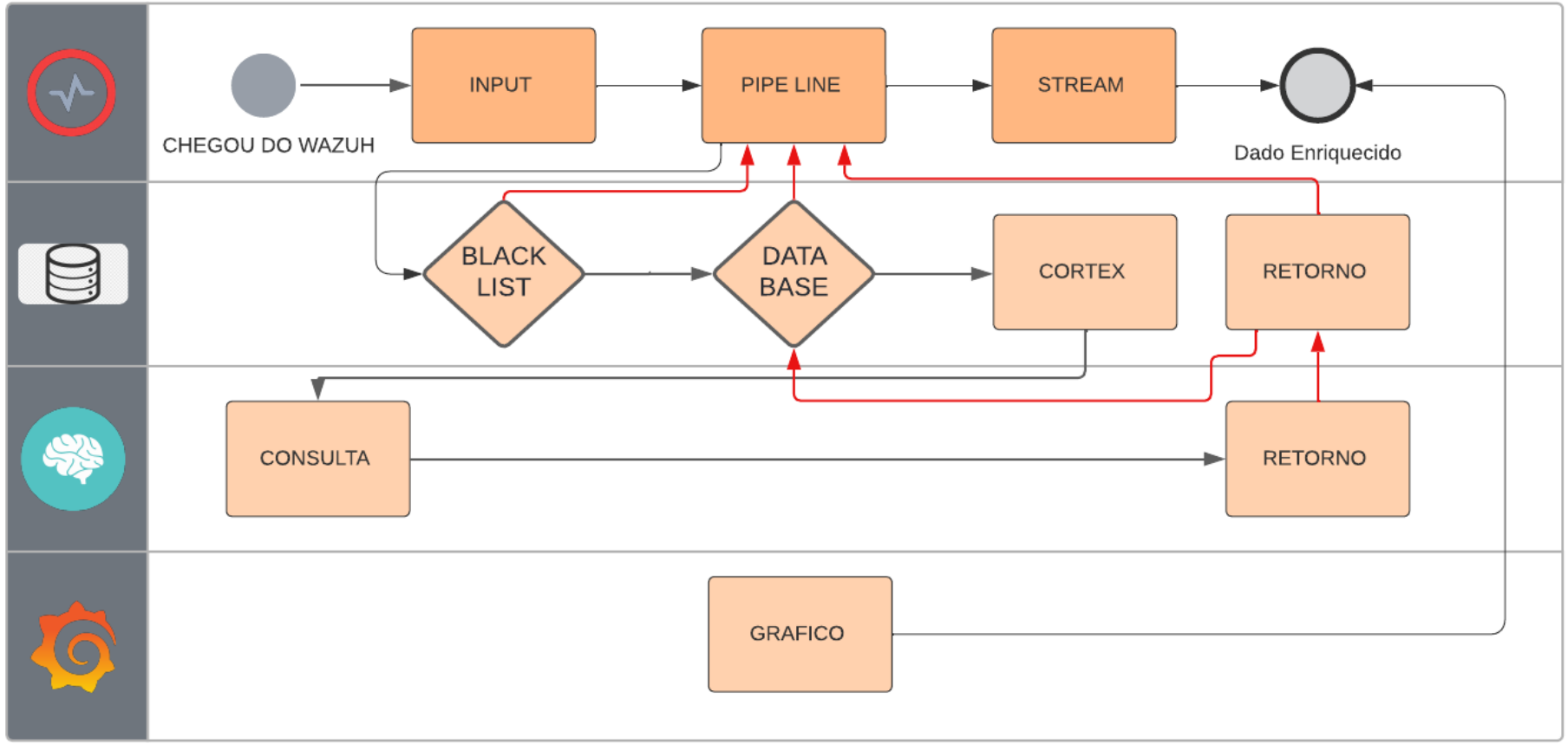



TLP:CLEAR

# Wazuh<>Graylog<>DB<>Cortex(VirusTotal, Abuse IP, Misp)

DB

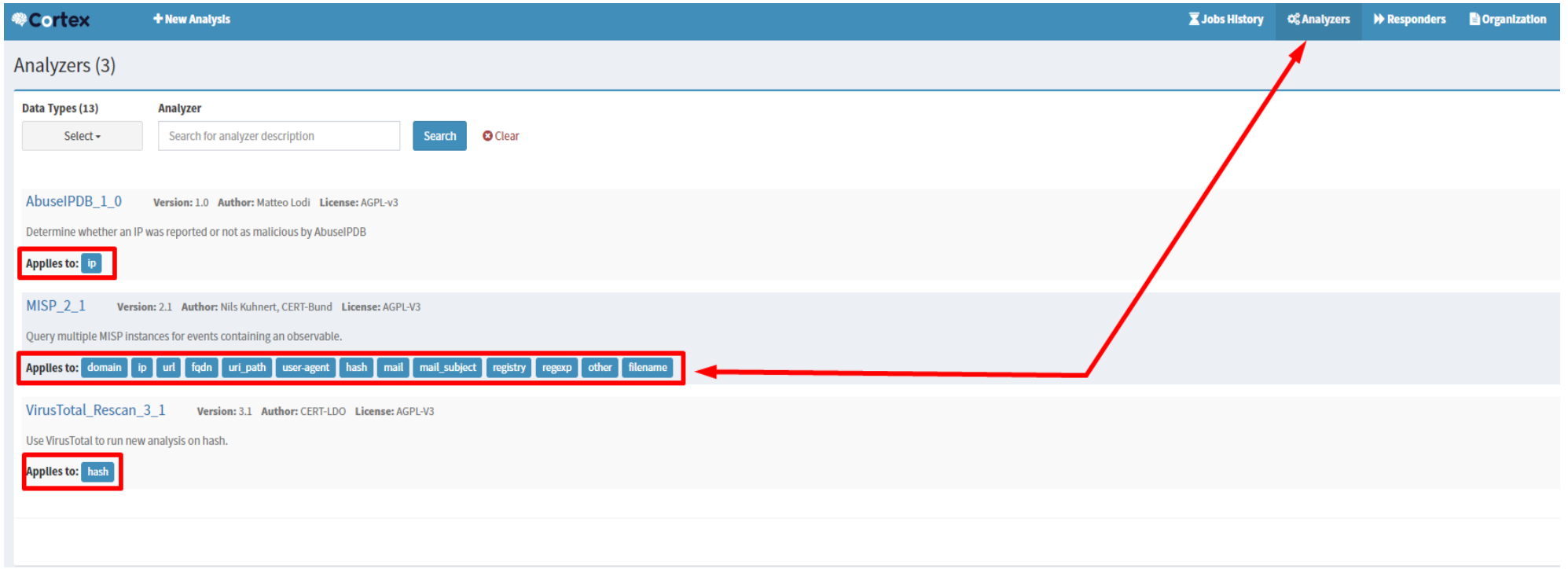
Cortex




TLP:CLEAR

# Wazuh<>Graylog<>DB<>Cortex(VirusTotal, Abuse IP, Misp)

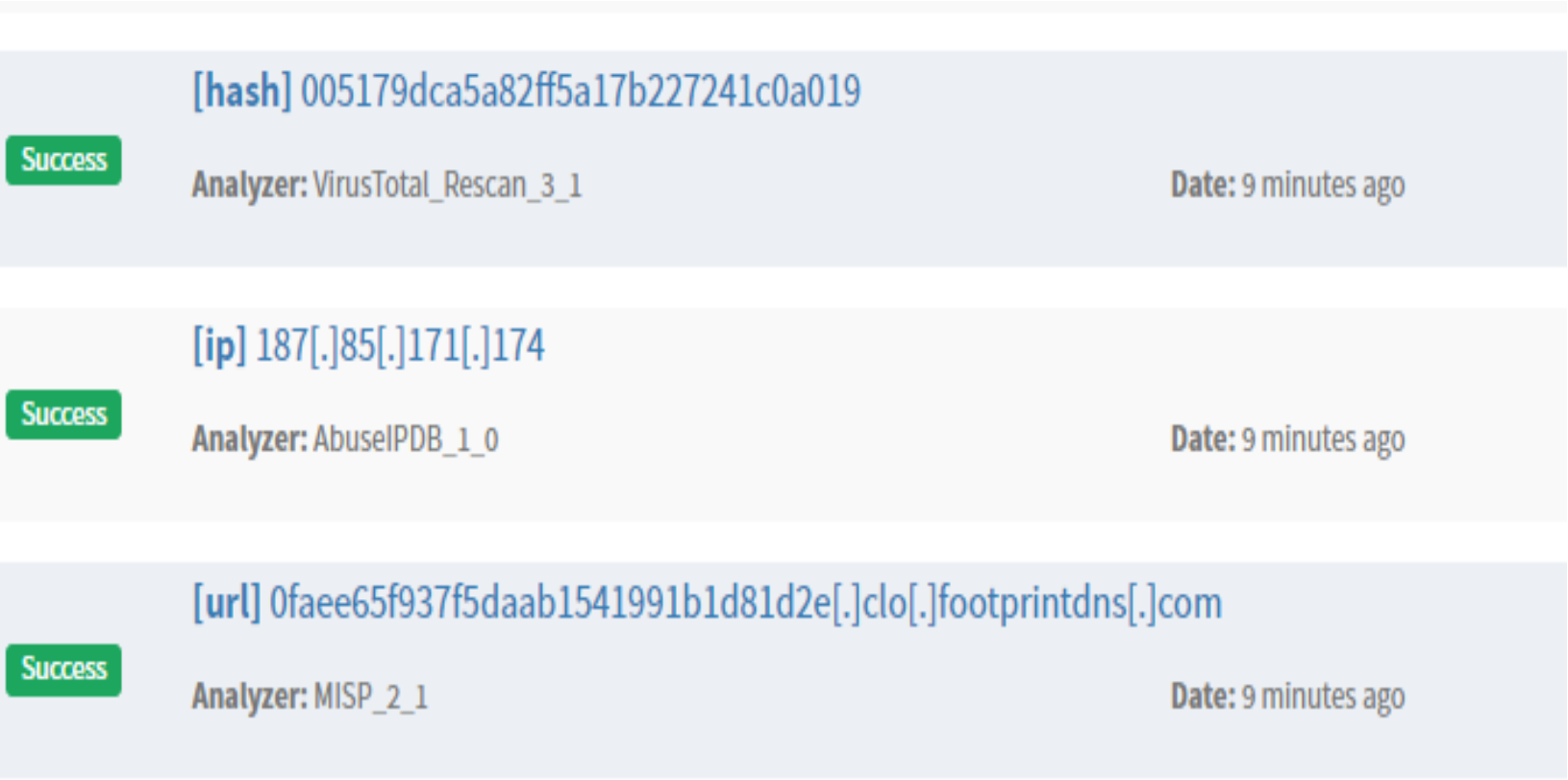
Cortex APIs




TLP:CLEAR

# Wazuh<>Graylog<>DB<>Cortex(VirusTotal, Abuse IP, Misp)

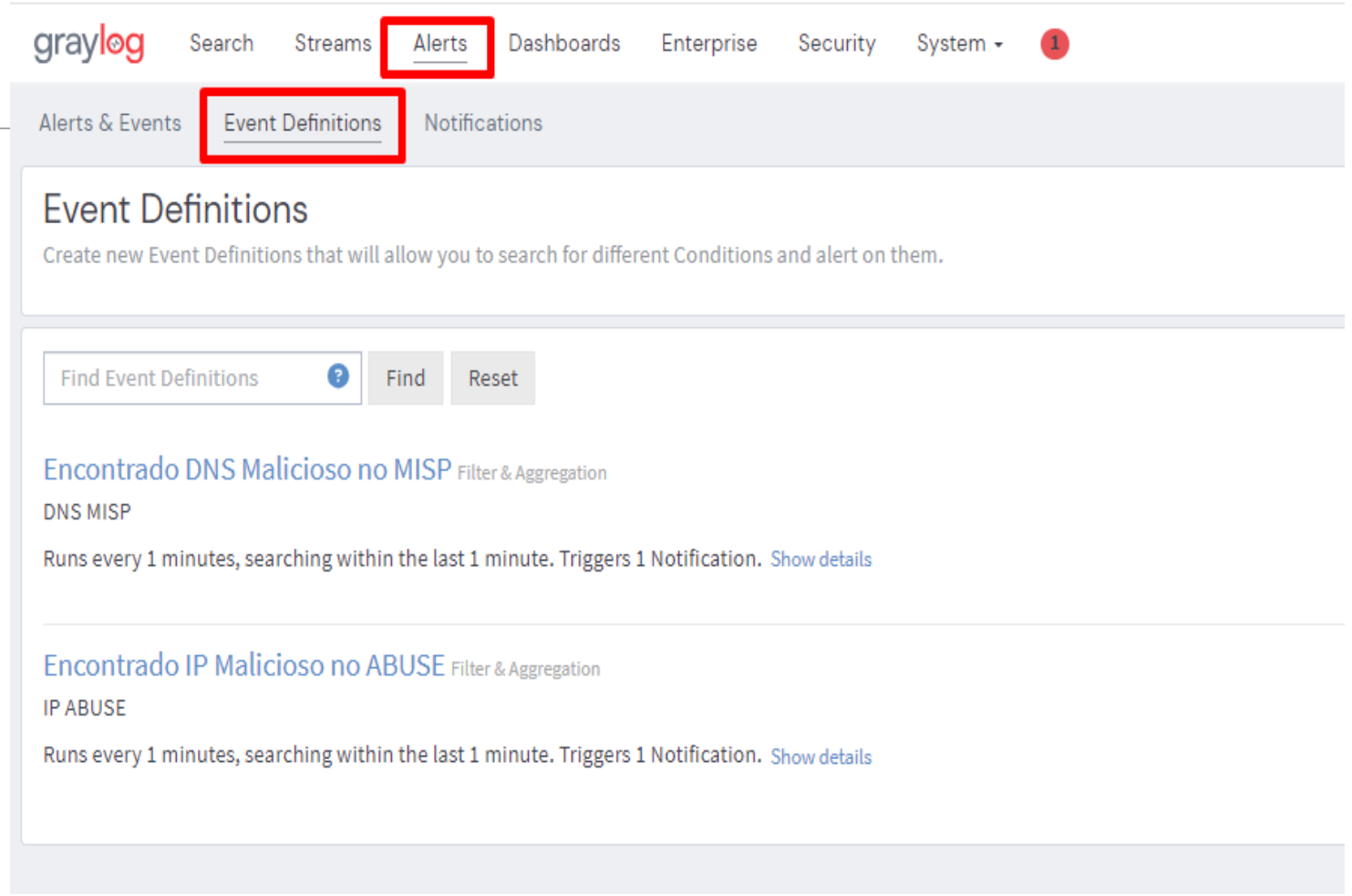
Cortex
Hash
IP
Domain




TLP:CLEAR

# Graylog>Teams

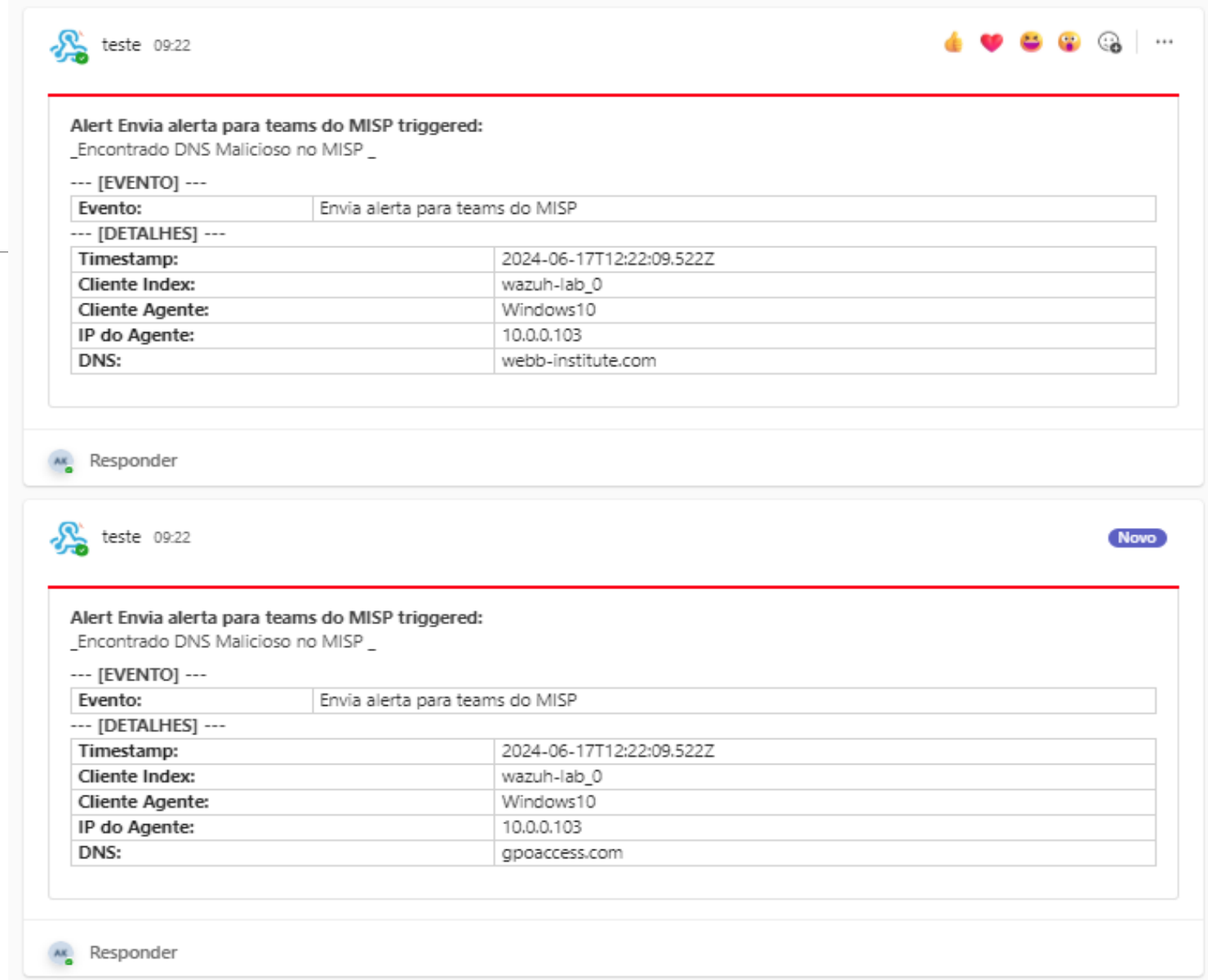
https://github.com/hidapple/graylog-plugin-teams




TLP:CLEAR

# Graylog>Teams

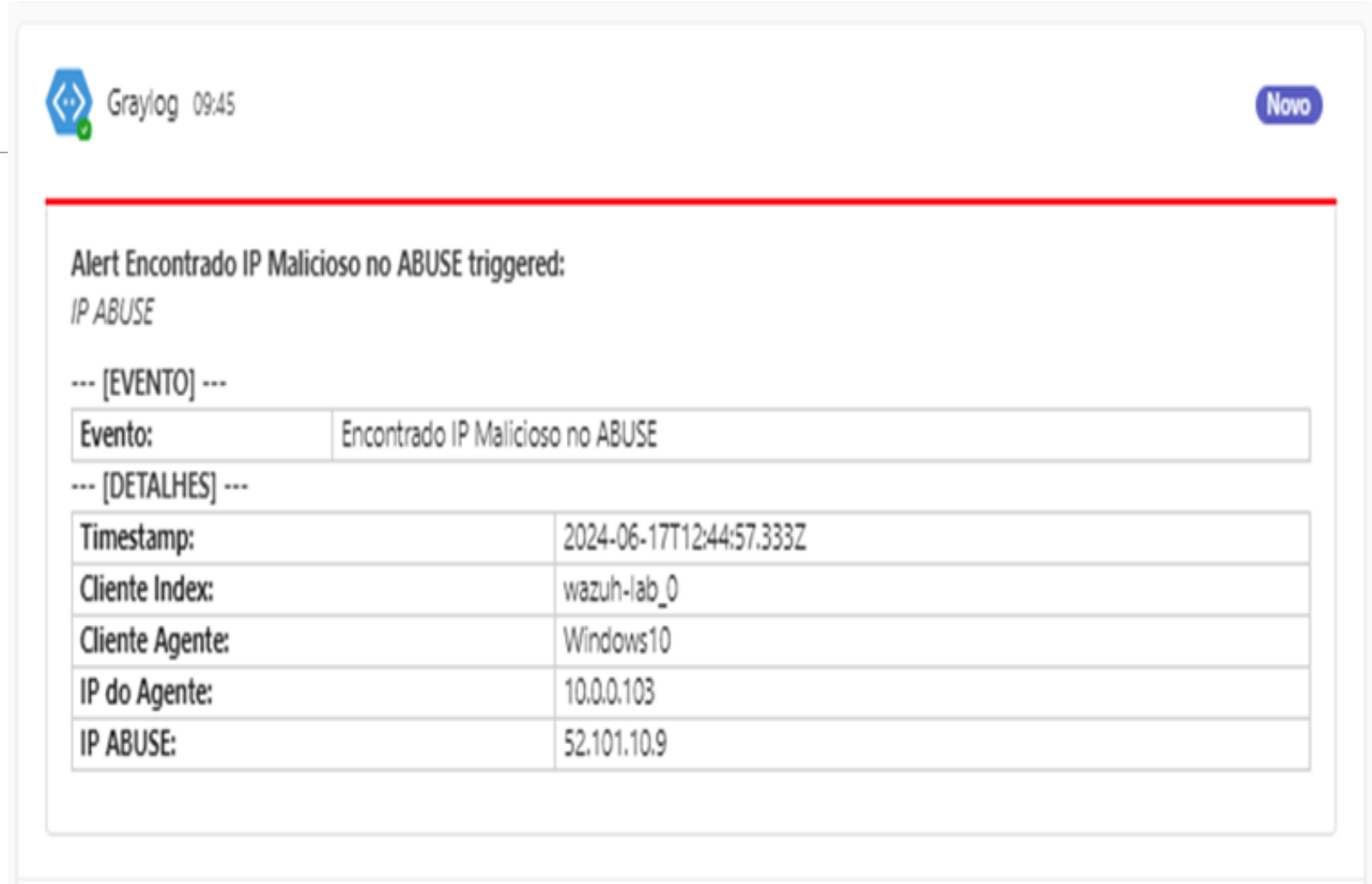
Recebendo no Teams




TLP:CLEAR

# Graylog>Teams

Cuidar com uma fonte só.
Falso Positivo




TLP:CLEAR

# Falso Positivo

Abuse apontou que era malicioso.

**52.101.10.9** was found in our database!

This IP was reported **1** times. Confidence of Abuse is **2%**: ?

2%

| | |
|---|---|
| **ISP** | Microsoft Corporation |
| **Usage Type** | Data Center/Web Hosting/Transit |
| **Domain Name** | microsoft.com |
| **Country** | United States of America |
| **City** | Boydton, Virginia |

*IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.*

REPORT 52.101.10.9 WHOIS 52.101.10.9

IP Abuse Reports for **52.101.10.9**:

This IP address has been reported a total of **1** time from 1 distinct source. It was most recently reported **2 weeks ago**.

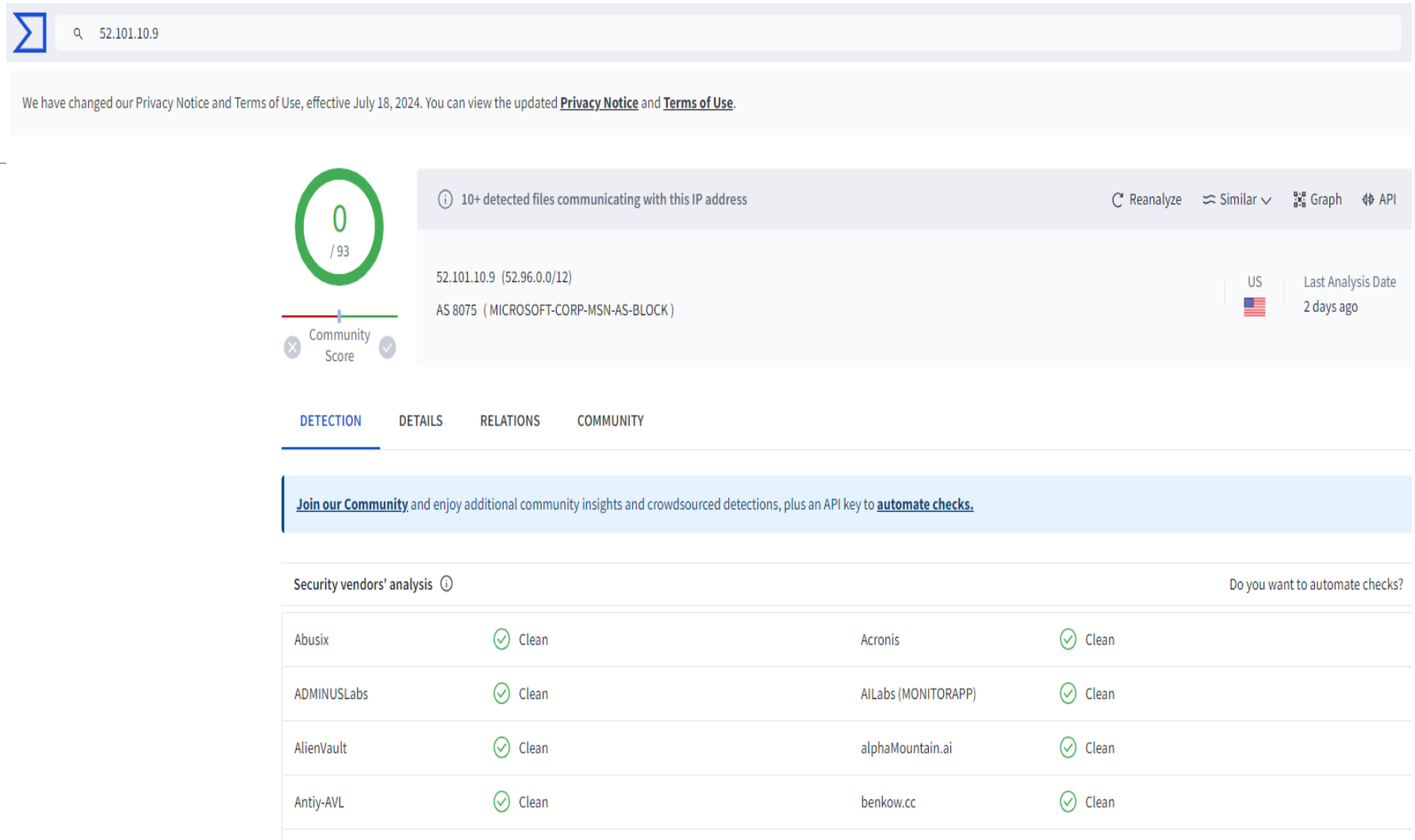
**Old Reports:** The most recent abuse report for this IP address is from **2 weeks ago**. It is possible that this IP is no longer involved in abusive activities.

| Reporter | IoA Timestamp in UTC | Comment | Categories |
|---|---|---|---|
| ✔ Anonymous | 2024-05-30 22:05:42 (2 weeks ago) | 2024-05-31T00:05:21.819931+02:00 zelda postfix/smtp [1315965]: DE16488C33A: lost connection with hotm ... show more | Brute-Force |

TLP:CLEAR

# Falso Positivo

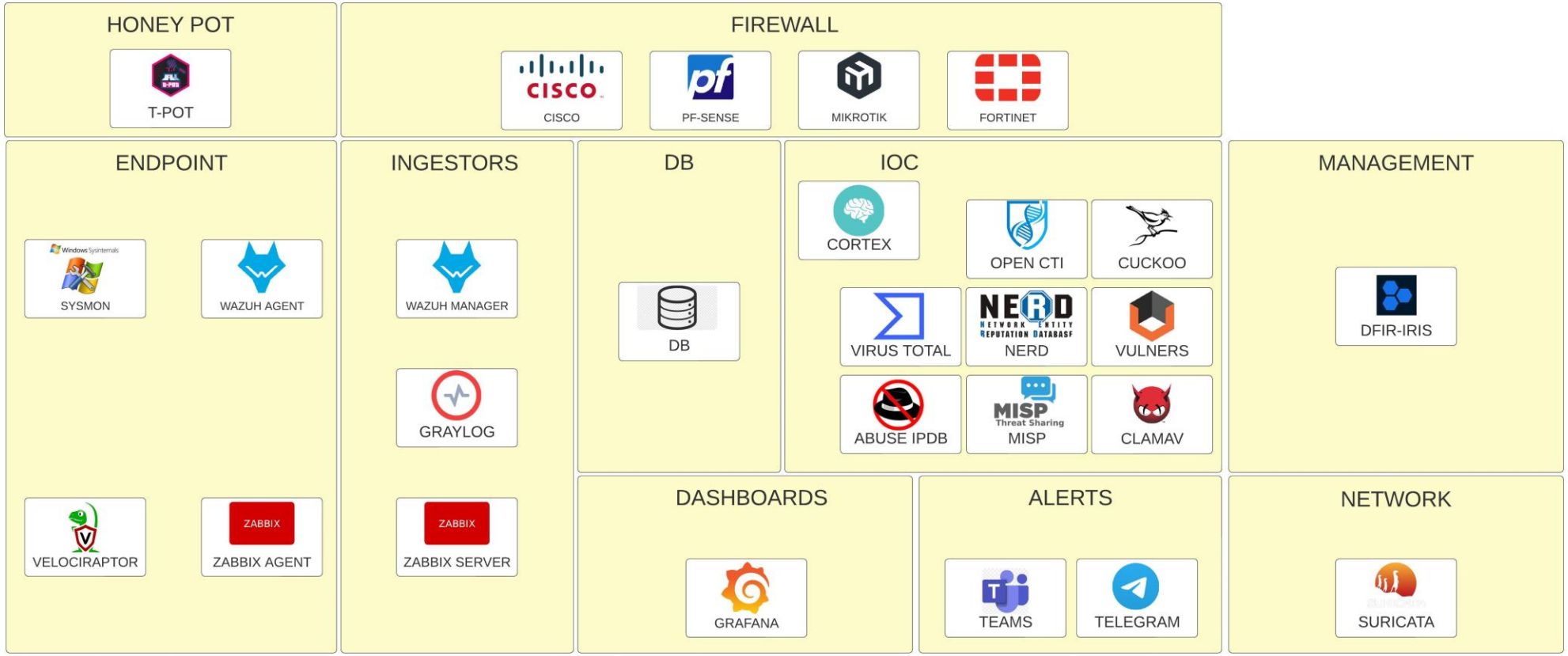
Não encontrado nada
no Virus Total.




TLP:CLEAR

# Desenvolvimento do Fluxo

Podemos melhorar?




TLP:CLEAR

# Referências


- https://wazuh.com/
- https://graylog.org/
- https://docs.thehive-project.org/cortex/
- https://www.misp-project.org/
- https://grafana.com/
- https://blog.reconinfosec.com/detecting-threats-with-graylog-pipelines-part-3
- https://socfortress.medium.com/build-your-own-siem-stack-with-open-source-tools-series-39da0f2d412a
- https://socfortress.medium.com/maximizing-threat-detection-and-response-with-cortex-63e7b653c2cb
- https://socfortress.medium.com/part-6-best-open-source-siem-dashboards-5dad09fa4d0e
- https://socfortress.medium.com/part-3-wazuh-manager-install-log-analysis-e819f28b0f9e
- https://socfortress.medium.com/part-11-wazuh-events-and-misp-automation-68109a887736

# Agradeço a atenção!