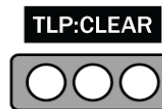


AUTOMATIZAÇÃO DE PROCESSOS DE SOC COM FERRAMENTAS OPEN-SOURCE

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 SEGUINTE 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

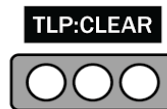
CURSOS:

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

CERTIFICADOS:

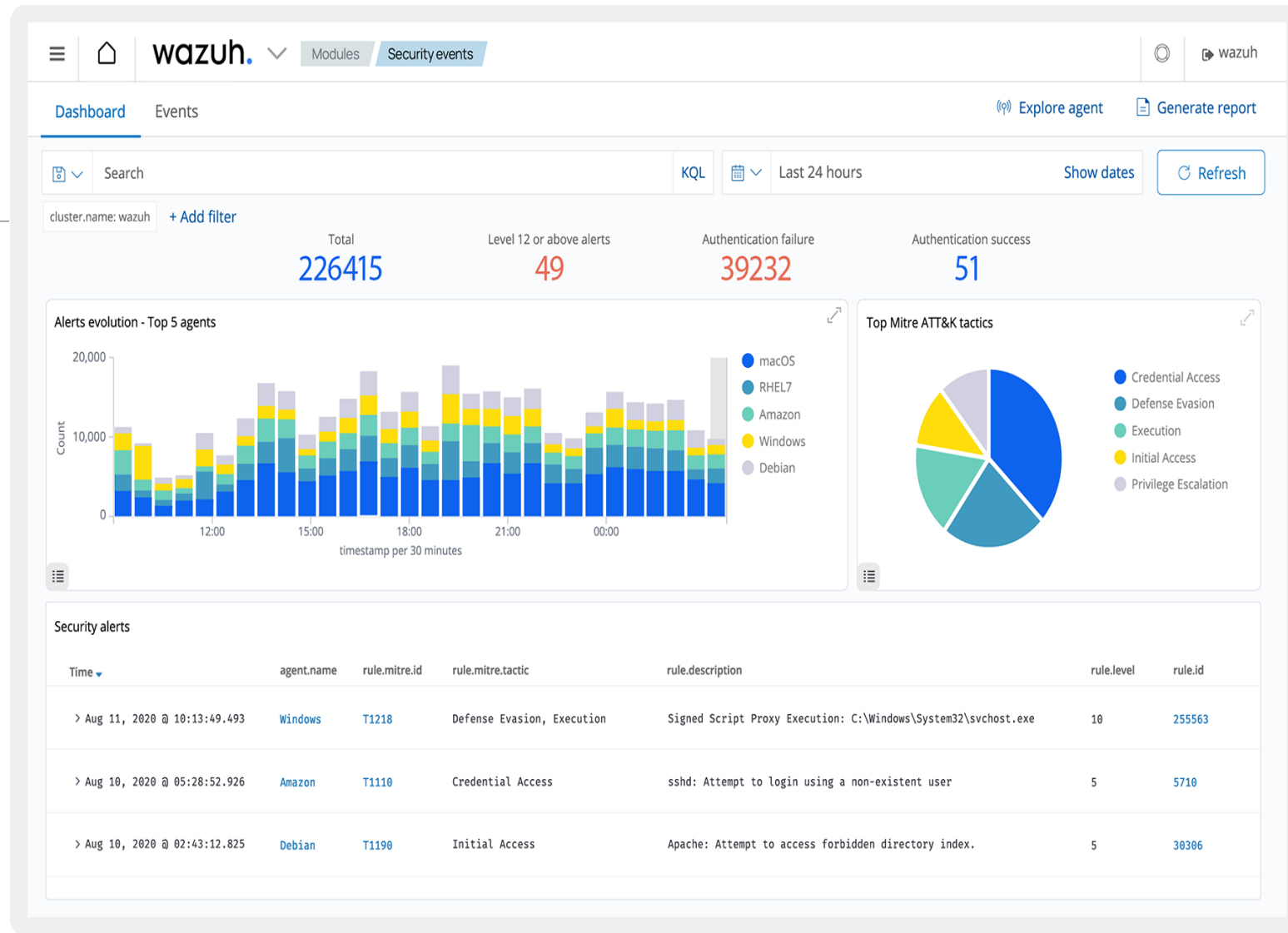
- FURUKAWA DATA CABLING SYSTEM E MCT
FLUKE NETWORKS
- WINDOS SERVER 2012 ADMINISTRATION
ORACLE DATABASE 10G OCA
- MIKROTIK: MTCNA-MTCRE-MTCTCE-MTCSE
- EC-COUNCIL- CEH – CHFI
- FIM - CERT

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.

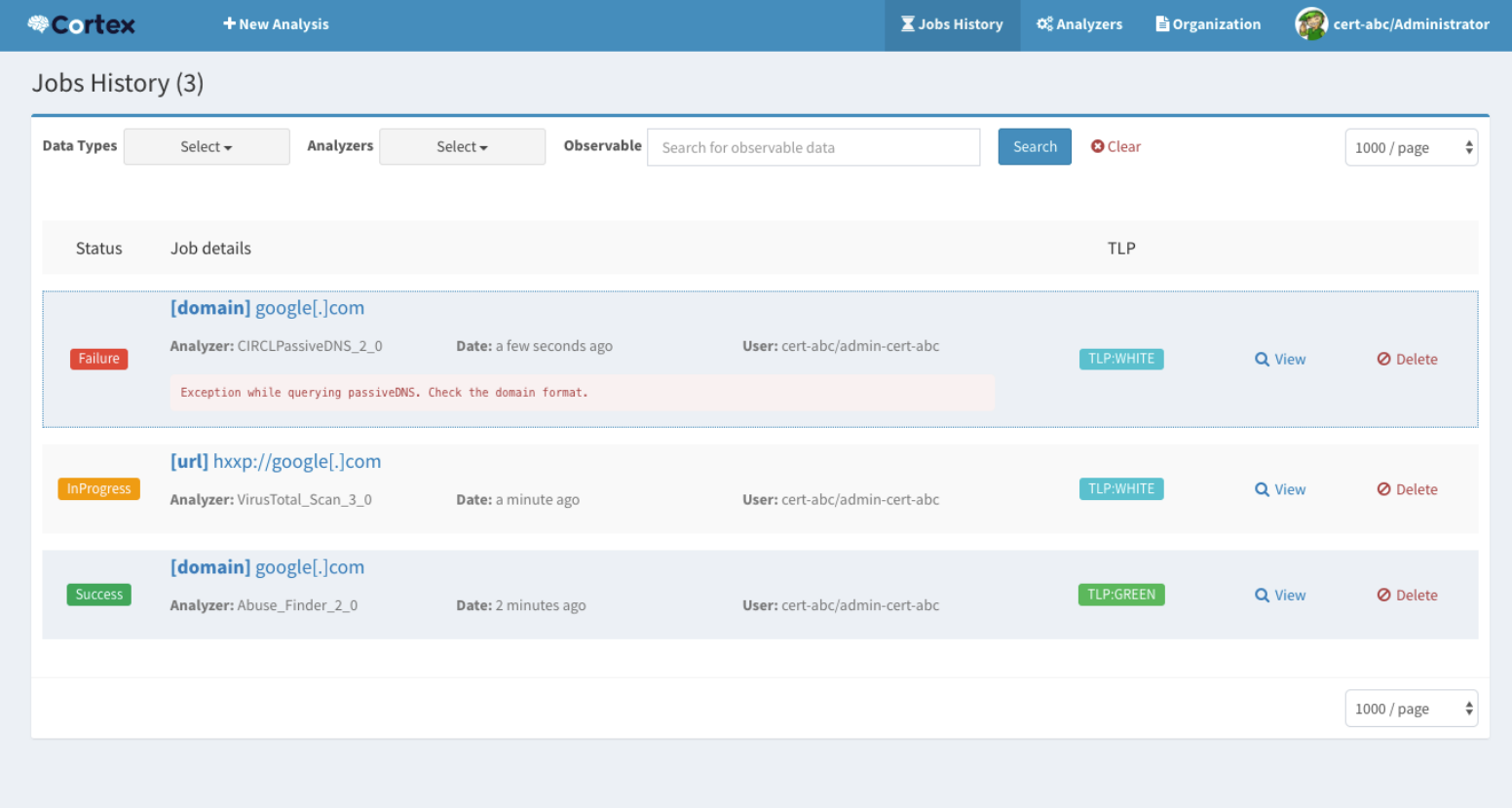
The screenshot displays the Graylog web interface. At the top, there is a navigation bar with the Graylog logo and menu items: Search, Streams, Alerts, Dashboards, Sources, System, and a notification icon. The user is logged in as 'Administrator'. Below the navigation bar, there is a search input field with the query 'g12_source_input:58be0be8f0e1fc0e94f80450'. The search results section shows 'Found 12,529 messages in 26 ms, searched in 1 index.' and 'Results retrieved at 2017-04-11 00:00:31.' There are buttons for 'Add count to dashboard', 'Save search criteria', and 'More actions'. A 'Fields' and 'Decorators' section is visible, with a list of fields including @timestamp, @version, category, destIp, destPort, mac, message (checked), NetworkSecurityGroup, operationName, and nrotoal. To the right, a 'Histogram' chart shows the distribution of messages over time, with bars for 23:55, 23:56, 23:57, 23:58, 23:59, and Tue 11. Below the histogram is a 'Messages' table with columns for 'Timestamp' and 'source'. The table contains four rows of messages, all with the same timestamp '2017-04-11 00:00:29.027' and source 'unknown'. The messages are displayed as '%{Message}'.

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.



The screenshot displays the Cortex web interface. At the top, there is a navigation bar with the Cortex logo, a '+ New Analysis' button, and links for 'Jobs History', 'Analyzers', and 'Organization'. The user is logged in as 'cert-abc/Administrator'. The main content area is titled 'Jobs History (3)' and features a search bar for 'Observable' data. Below the search bar, there are filters for 'Data Types' and 'Analyzers'. The job history is presented as a table with columns for 'Status', 'Job details', and 'TLP'. Three jobs are listed:

Status	Job details	TLP
Failure	<p>[domain] google[.]com</p> <p>Analyzer: CIRCLPassiveDNS_2_0 Date: a few seconds ago User: cert-abc/admin-cert-abc</p> <p>Exception while querying passiveDNS. Check the domain format.</p>	TLP:WHITE
InProgress	<p>[url] hxxp://google[.]com</p> <p>Analyzer: VirusTotal_Scan_3_0 Date: a minute ago User: cert-abc/admin-cert-abc</p>	TLP:WHITE
Success	<p>[domain] google[.]com</p> <p>Analyzer: Abuse_Finder_2_0 Date: 2 minutes ago User: cert-abc/admin-cert-abc</p>	TLP:GREEN

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.

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 next »

Q My Events Org Events Filter

<input type="checkbox"/>	Published	Org	Owner org	Id	Clusters	Tags	#Attr.	#Corr.	Email	Date	Info	Distribution	Actions
<input type="checkbox"/>	✓	covid-19		10616		current-event:pandemic="covid-19" pandemic:covid-19="cyber" osint:source-type="manual-collection" tip:white osint:certainty="93" COVID-19 circ:incident-classification="covid-19" workflow:state="complete"	12		admin@admin.test	2020-03-31	maldoc, covid19	All	
<input type="checkbox"/>	✓	Siemens AG		10597			1		admin@admin.test	2020-03-12	This is a central test event	All	
<input type="checkbox"/>	✗			10614		processed_by_intelmq	8	3	admin@admin.test	2020-05-04	IntelMQ test	Organisation	
<input type="checkbox"/>	✓	BitDefender		10611		Bitdefender:validated MalwareFamily:Ursnif TIM:validated tip:green	32	3	admin@admin.test	2019-12-19	Ongoing malware campaign (9-13/12)	Telcos SG	
<input type="checkbox"/>	✓	Vairav Technology		10622		Download	112		admin@admin.test	2020-03-31	VX Vault - Malware Dropper feed	All	
<input type="checkbox"/>	✓	Vairav Technology		10621			569	9	admin@admin.test	2020-01-03	Azorult Tracker Feed feed	All	
<input type="checkbox"/>	✓	Vairav Technology		10618		Download	527	1	admin@admin.test	2019-08-29	URL feed	All	
<input type="checkbox"/>	✓	BitDefender		10593		TIM:validated tip:green Bitdefender:validated MalwareFamily:Ursnif	32	3	admin@admin.test	2019-12-11	Ongoing malware propagation campaign	All	
<input type="checkbox"/>	✓	Siemens AG		10600			2		admin@admin.test	2020-04-22	Another test to push / zmq v2	All	
<input type="checkbox"/>	✓	Siemens AG		10599			1		admin@admin.test	2020-04-21	Another test to push / zmq	All	

TLP:CLEAR



O que é o Grafana

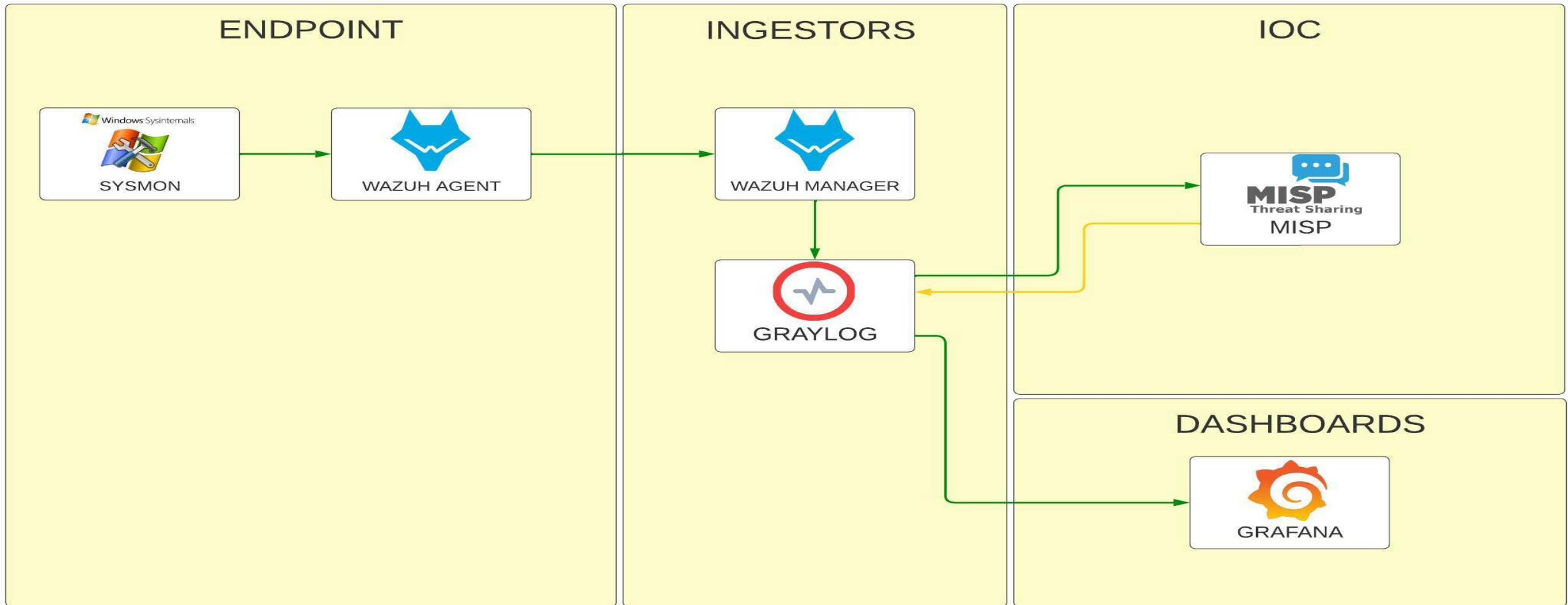
Grafana é uma plataforma de código aberto para visualização e monitoramento de dados, projetada para criar dashboards interativos e intuitivos que exibem métricas e logs em tempo real.



TLP: CLEAR



Fluxo Simples



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

The screenshot shows the MISP 'Search Attribute' page. The 'Event Actions' menu item in the top navigation bar is highlighted with a red box. A red arrow points from this menu item to the 'Search Attributes' option in the left sidebar, which is also highlighted with a red box. Another red arrow points from the 'Search Attributes' option to the 'Type' dropdown menu, which is currently set to 'domain' and is also highlighted with a red box. The 'Category' dropdown menu is set to 'ALL'. Below the dropdowns, there is a checkbox for 'Only find IOCs flagged as to IDS' and a section for 'First seen and Last seen' with date and time input fields. A 'Search' button is located at the bottom of the form.

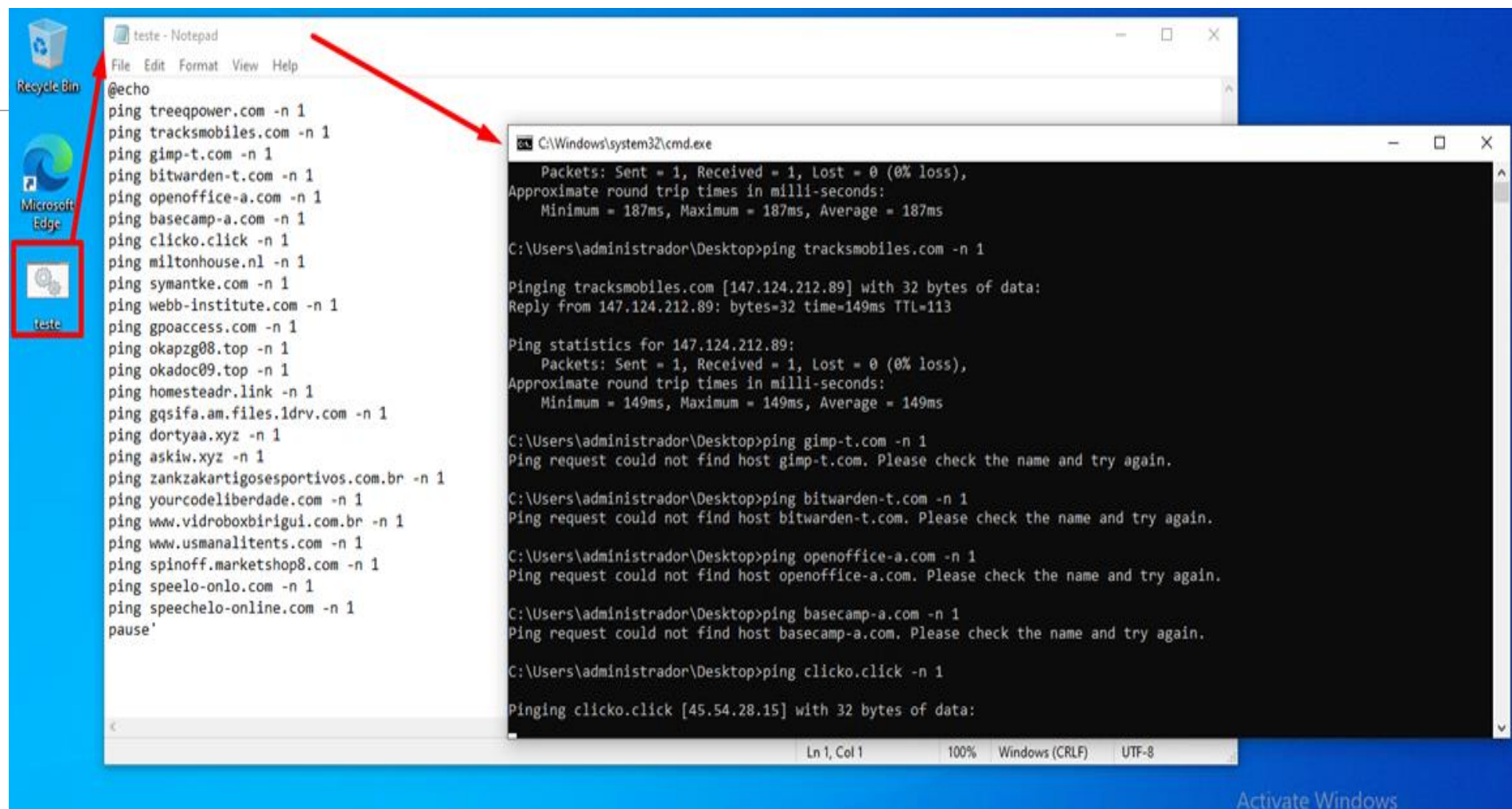
Coletar Domains dentro do MISP

TLP:CLEAR



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

Teste com .BAT



TLP: CLEAR



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

The image displays two screenshots of the Windows Event Viewer application. The left screenshot shows the navigation pane on the left side, with the following folders highlighted in red: 'Applications and Services', 'Microsoft', and 'Windows'. The right screenshot shows a list of events in the 'Operational' category. A red box highlights a specific event with the following details:

Level	Date and Time	Source	Event ID	Task Category
Information	6/11/2024 5:12:58 AM	Sysmon	1	Process Create (rule: ProcessCr...
Information	6/11/2024 5:12:58 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/11/2024 5:12:58 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/11/2024 5:12:58 AM	Sysmon	22	Dns query (rule: DnsQuery)
Information	6/11/2024 5:12:58 AM	Sysmon	22	Dns query (rule: DnsQuery)

The detailed view of the selected event (Event 22, Sysmon) shows the following information:

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 22
Level: Information
User: SYSTEM
OpCode: Info

Additional details from the event view:

- Logged: 6/11/2024 5:12:58 AM
- Task Category: Dns query (rule: DnsQuery)
- Keywords: Dns query (rule: DnsQuery)
- Computer: DESKTOP-K9D5TVB

TLP: CLEAR



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

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

The screenshot shows the Wazuh Security Events dashboard. At the top, there is a search bar and a filter bar. The filter bar contains the text "rule.description: Sysmon - Event 22: DNS Query event" which is highlighted with a red box. Below the filter bar, there is a section for "wazuh-alerts-*" with a search field and a "Filter by type" button. The "Selected fields" section lists "agent.name", "rule.description", "rule.id", and "rule.level". The "Available fields" section lists various fields including "agent.id", "agent.ip", "data.file", "data.title", "data.win.eventdata.authenticationPackageName", "data.win.eventdata.commandLine", "data.win.eventdata.company", "data.win.eventdata.creationUtcTime", "data.win.eventdata.currentDirectory", "data.win.eventdata.data", "data.win.eventdata.description", "data.win.eventdata.elevatedToken", "data.win.eventdata.failureReason", "data.win.eventdata.fileVersion", "data.win.eventdata.hashes", "data.win.eventdata.image", "data.win.eventdata.impersonationLevel", "data.win.eventdata.integrityLevel", "data.win.eventdata.ipAddress", "data.win.eventdata.ipPort", and "data.win.eventdata.keyLength".

Below the filter bar, there is a graph showing the count of events over time. The graph has a y-axis labeled "Count" ranging from 0 to 80 and an x-axis showing time from 12:00 to 21:00. The graph shows several small bars indicating event counts at specific times.

Below the graph, there is a table of events. The table has columns for "Time", "agent.name", and "rule.description". The "rule.description" column is highlighted with a red box. The table contains 130 hits, all of which are "Sysmon - Event 22: DNS Query event".

Time	agent.name	rule.description
Jun 11, 2024 @ 09:13:06.776	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:06.774	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.368	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.352	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.337	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.321	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.305	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.290	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.281	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:13:02.277	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:12:59.636	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:12:59.595	Windows10	Sysmon - Event 22: DNS Query event
Jun 11, 2024 @ 09:12:59.581	Windows10	Sysmon - Event 22: DNS Query event

TLP: CLEAR



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

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

The screenshot displays a Wazuh alert in Graylog. The alert is titled "Sysmon - Event 22: DNS Query event" and is associated with the agent "Windows10". The alert details are shown in a table format, with the following fields highlighted in red:

Field	Value
agent.ip	10.0.0.103
agent.name	Windows10
data.win.eventdata.queryName	speache1o-online.com

The full alert details are as follows:

```
{
  "_index": "wazuh-alerts-4.x-2024.06.11",
  "agent.id": "001",
  "agent.ip": "10.0.0.103",
  "agent.name": "Windows10",
  "data.win.eventdata.image": "&lt;unknown process&gt;",
  "data.win.eventdata.processGuid": "{00000000-0000-0000-0000-000000000000}",
  "data.win.eventdata.processId": "6132",
  "data.win.eventdata.queryName": "speache1o-online.com",
  "data.win.eventdata.queryStatus": "9003",
  "data.win.eventdata.user": "DESKTOP-K9D5TVB\\administrador",
  "data.win.eventdata.utcTime": "2024-06-11 12:12:33.751",
  "data.win.system.channel": "Microsoft-Windows-Sysmon/Operational",
  "data.win.system.computer": "DESKTOP-K9D5TVB",
  "data.win.system.eventID": "22",
  "data.win.system.eventRecordID": "33249",
  "data.win.system.keywords": "0x8000000000000000",
  "data.win.system.level": "4",
  "data.win.system.message": "\"Dns query:
  RuleName: -
  UtcTime: 2024-06-11 12:12:33.751
  ProcessGuid: {00000000-0000-0000-0000-000000000000}
  ProcessId: 6132
  QueryName: speache1o-online.com
  QueryStatus: 9003
  QueryResults: -
  Image: <unknown process>
  User: DESKTOP-K9D5TVB\\administrador\""}"
```

TLP:CLEAR



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

Dentro do Graylog

Configurando a saida

Lookup Tables:
Data Adapters + Caches +
Lookup Tables

The screenshot shows the Graylog web interface for configuring a data adapter. The navigation menu at the top includes 'System / Lookup Tables', 'Lookup Tables', 'Caches', and 'Data Adapters'. The main configuration form is titled 'Data Adapter (HTTP JSONPath)' and includes the following fields:

- Title:** MISP
- Description:** A short title for this data adapter.
- Name:** misp
- Custom Error TTL:** 1 minutes
- Lookup URL:** http://10.0.0.109/attributes/restSearch/value:\${key}
- Single value JSONPath:** \$.response.Attribute.[0].type
- Multi value JSONPath:** \$.response.Attribute.[0]
- HTTP User-Agent:** Graylog Lookup - https://www.graylog.org/
- HTTP Headers:** A table with columns Name, Value, and Actions.

Name	Value	Actions
Accept	application/json	Delete
Authorization	Q11NePwpkCaQaOFJwTu9vz0z5t5XajVV4xQDctH	Delete
Content-Type	application/json	Delete

The configuration summary section includes the following information:

- Configuration:** The HTTPJSONPath data adapter executes HTTP GET requests to lookup a key and parses the result based on configured JSONPath expressions.
- Lookup URL:** The URL that will be used for the HTTP request. To use the lookup key in the URL, the `${key}` value can be used. This variable will be replaced by the actual key that is passed to a lookup function. (example: `https://example.com/api/lookup?key=${key}`)
- Single value JSONPath:** This JSONPath expression will be used to parse the single value of the lookup result. (example: `$.user.full_name`)
- Multi value JSONPath:** This JSONPath expression will be used to parse the multi value of the lookup result. (example: `$.users[*]`) The multi value JSONPath setting is optional. Without it, the single value is also present in the multi value result.
- HTTP User-Agent:** This is the User-Agent header that will be used for the HTTP requests. You should include some contact details so owners of the services you query know whom to contact if issues arise. (like excessive API requests from your Graylog cluster)
- Example:** This shows an example configuration and the values that will be returned from a lookup. The configured URL is `https://example.com/api/users/${key}` and the `${key}` gets replaced by `jane` during the lookup request. This is the resulting JSON document:

```
{
  "user": {
    "login": "jane",
    "full_name": "Jane Doe",
    "roles": ["admin", "developer"],
    "contact": {
      "email": "jane@example.com",
      "cellphone": "40123456789"
    }
  }
}
```

TLP: CLEAR



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

The screenshot shows the Graylog web interface for a pipeline named 'misp'. The interface includes a navigation bar with 'graylog' and various menu items like 'Search', 'Streams', 'Alerts', 'Dashboards', 'Enterprise', 'Security', and 'System / Pipelines'. Below the navigation bar, there are tabs for 'Manage pipelines', 'Manage rules', and 'Simulator'. The main content area is titled 'Pipeline misp' and includes a description: 'Pipelines let you transform and process messages coming from streams. Pipelines consist of stages where rules are evaluated and applied. Messages can go through one or more stages. After each stage is completed, you can decide if messages matching all or one of the rules continue to the next stage.' There are several sections: 'Details' with fields for Title, Description, Created, Last modified, and Current throughput; 'Pipeline connections' showing the pipeline is processing messages from the stream 'wazuh-lab'; 'Pipeline Stages' with a description and an 'Add new stage' button; 'Stage 0' which contains 0 rules and has 'Delete' and 'Edit' buttons; and 'Stage 1' which contains 1 rule. A table at the bottom lists the rules for Stage 1:

Title	Description	Throughput	Errors
Sysmon_Event_ID_22_Send	Consulta Misp	0 msg/s	0 errors/s (0 total)

Two red arrows point from the 'Sysmon_Event_ID_22_Send' rule in the table to the 'Add new stage' button and the 'Delete' button of Stage 0.

Pipeline

Stages + Rules

TLP: CLEAR



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

Rules

Pipeline rule *Sysmon_Event_ID_22_Send*
Rules are a way of applying changes to messages in Graylog. A rule consists of a condition and a list of actions.

Title
You can set the rule title in the rule source. See the quick reference for more information.

Description
`Consulta Misp`
Rule description (optional).

Used in pipelines
`misp.`
Pipelines that use this rule in one or more of their stages.

Rule source

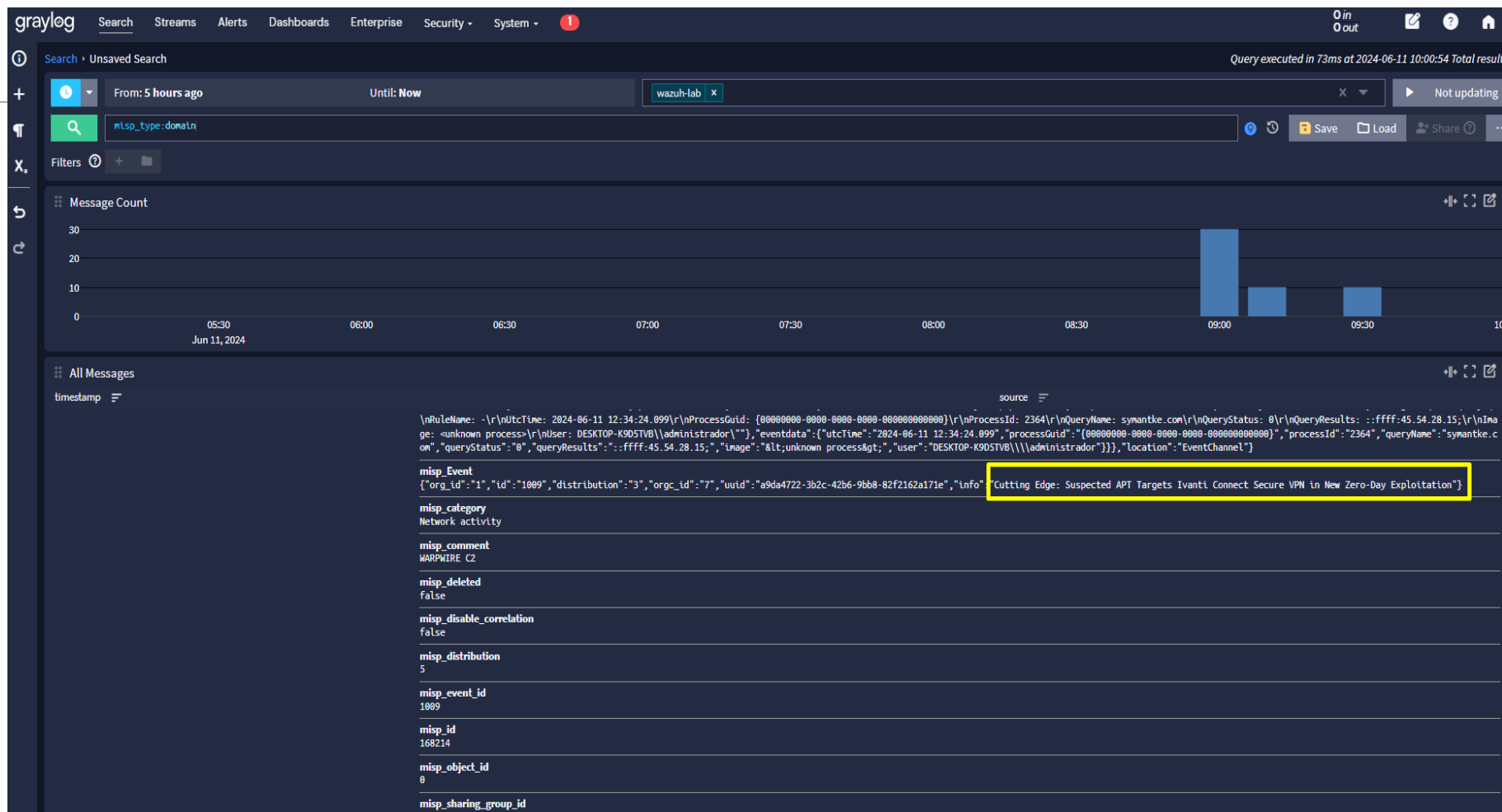
```
1 rule "Sysmon_Event_ID_22_Send"
2 when
3     to_string($message.Extraido_data_win_system_eventID)=="22"
4 then
5     let ldata = lookup(
6         lookup_table: "misp_query",
7         key: to_string($message.Extraido_data_win_eventdata_queryName)
8     );
9     set_fields(
10        fields: ldata,
11        prefix: "misp_"
12    );
13 end
```

Rule source, see quick reference for more information.

TLP:CLEAR



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



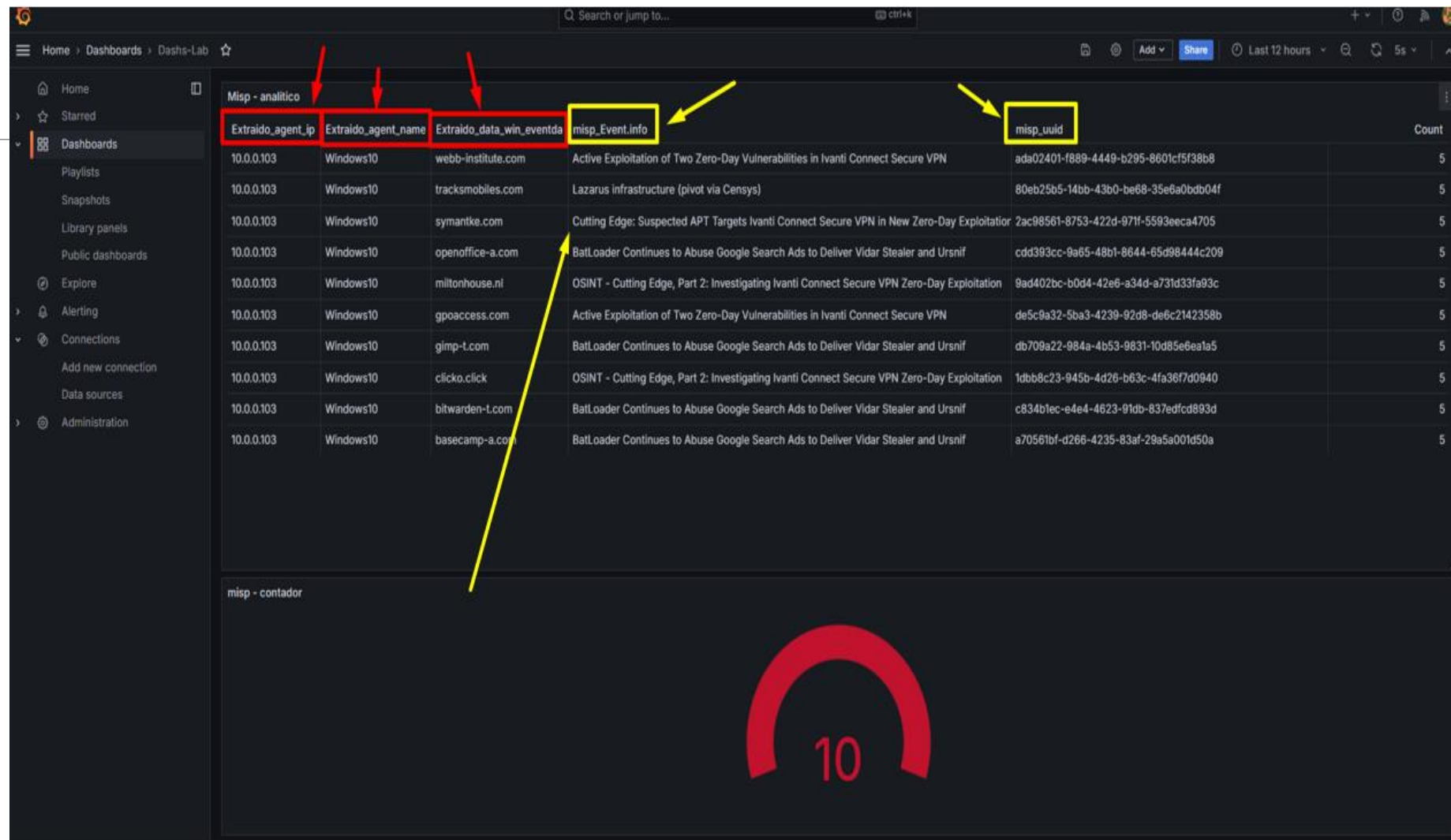
Retorno no Graylog

TLP: CLEAR



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

Dashboard Grafana



TLP: CLEAR



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

Verificando no Misp

The screenshot shows the MISP interface with a table of attributes. The 'Event' column contains the value '1705' and the 'Value' column contains 'webb-institute.com', both highlighted with red boxes. The table has columns for Date, Event, Org, Category, Type, Value, Tags, Galaxies, and Comment. The event is categorized as 'Network activity' and 'domain'.

Date	Event	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2024-01-11	1705		Network activity	domain	webb-institute.com			Suspected UTA0178 domain discovered via domain registration patterns	<input checked="" type="checkbox"/>	Q	1	<input checked="" type="checkbox"/>	Inherit event	0/0/0		

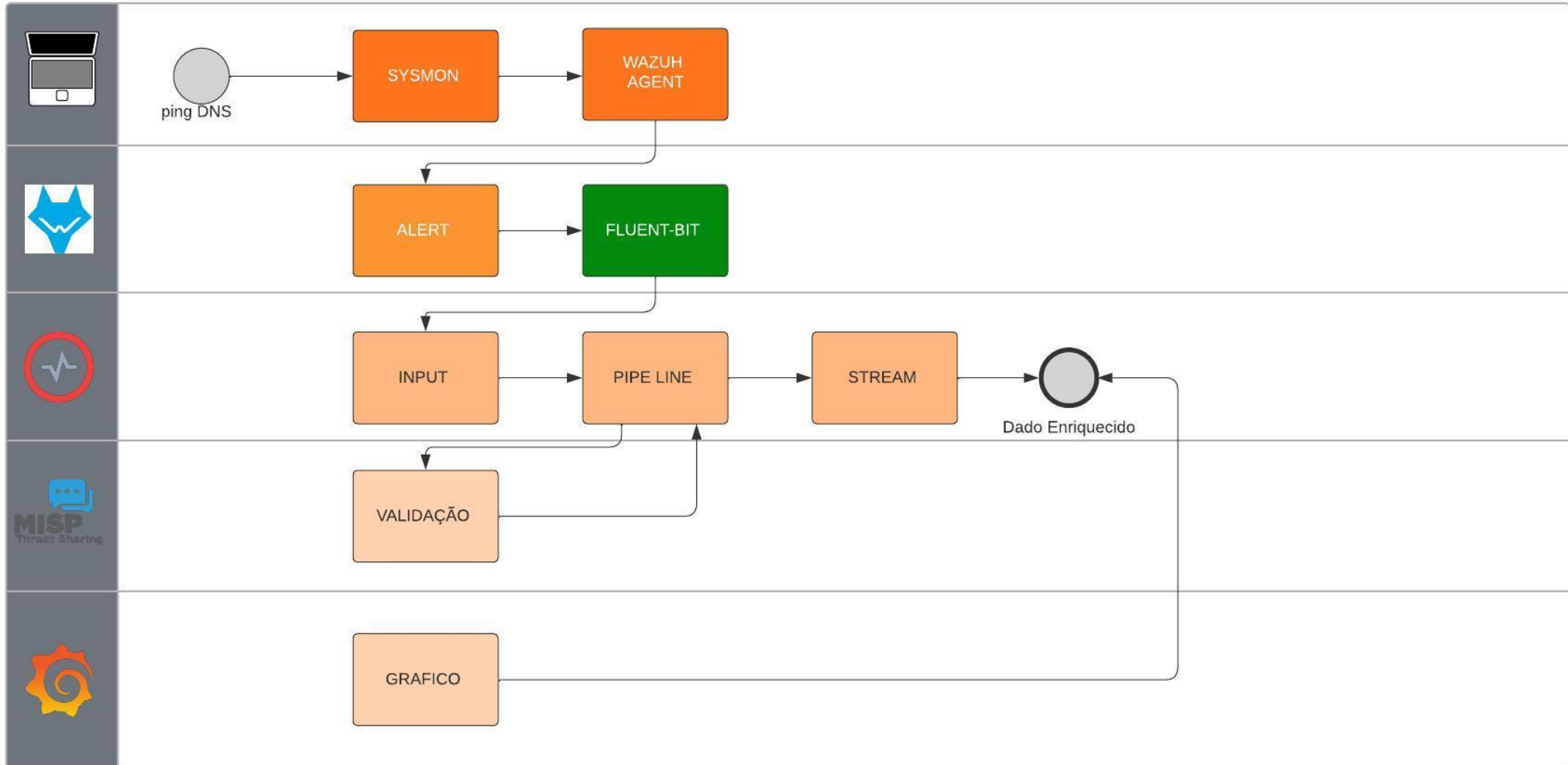
The screenshot shows a list of events in the MISP interface. The event with ID 'ada02401-f889-4449-b295-8601cf5f38b8' is highlighted with a red box. A red arrow points from this event to the 'webb-institute.com' attribute shown in the previous screenshot. The table has columns for Date, ID, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, Distribution, Sightings, Activity, and Actions.

Date	ID	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2024-01-11	32f...a10		Network activity	ip-dst	75.145.243.85			UTA0178 IP address observed interacting with compromised device	<input checked="" type="checkbox"/>	Q	1	<input checked="" type="checkbox"/>	Inherit	0/0/0		
2024-01-11	728...77f		Network activity	domain	symantke.com			UTA0178 domain used to collect credentials from compromised devices	<input checked="" type="checkbox"/>	Q	1009 1708 1 2	<input checked="" type="checkbox"/>	Inherit	0/0/0		
2024-01-11	ada02401-f889-4449-b295-8601cf5f38b8		Network activity	domain	webb-institute.com			Suspected UTA0178 domain discovered via domain registration patterns	<input checked="" type="checkbox"/>	Q	1	<input checked="" type="checkbox"/>	Inherit	0/0/0		
2024-01-11	de5...58b		Network activity	domain	gpoaccess.com			Suspected UTA0178 domain discovered via domain registration patterns	<input checked="" type="checkbox"/>	Q	1	<input checked="" type="checkbox"/>	Inherit	0/0/0		
2024-01-11	f1d...95b		Network activity	ip-dst	206.189.208.156			DigitalOcean IP address tied to UTA0178	<input checked="" type="checkbox"/>	Q	1	<input checked="" type="checkbox"/>	Inherit	0/0/0		

TLP: CLEAR



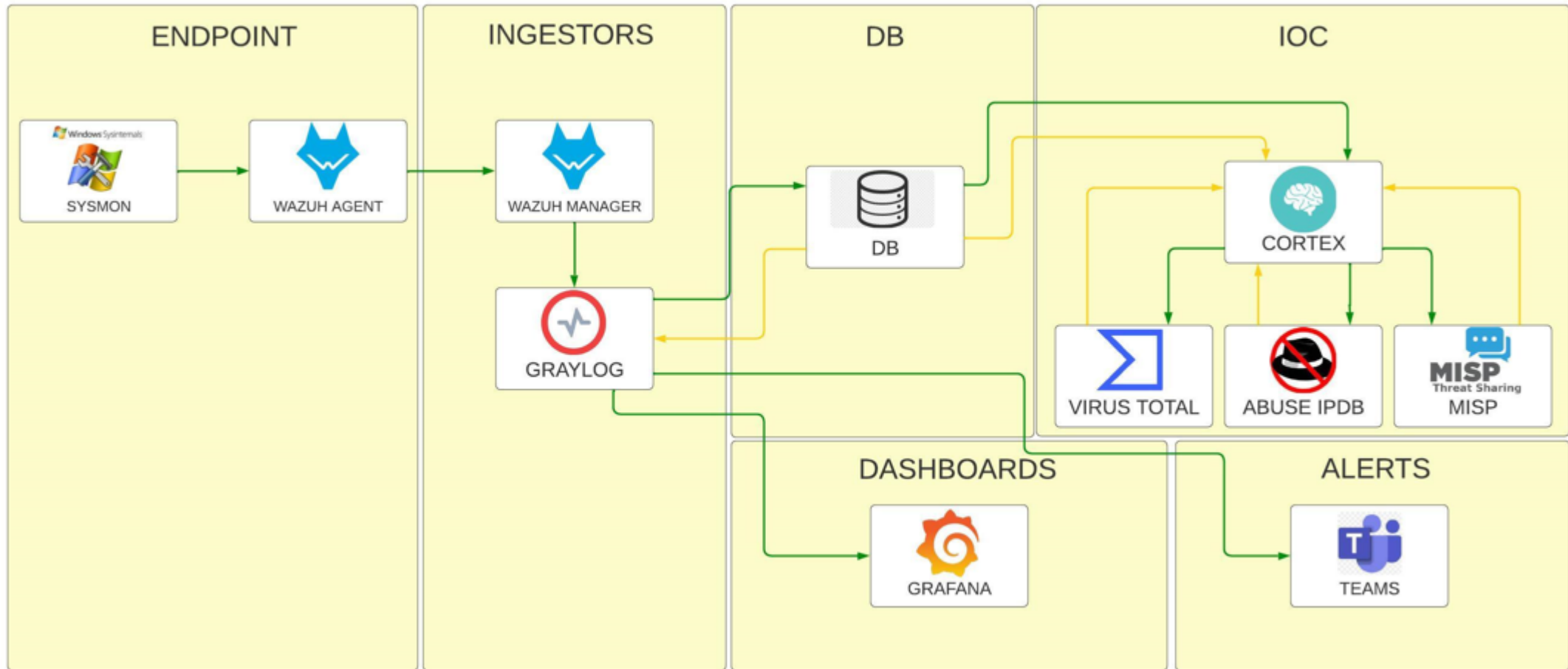
O que foi feito



TLP:CLEAR



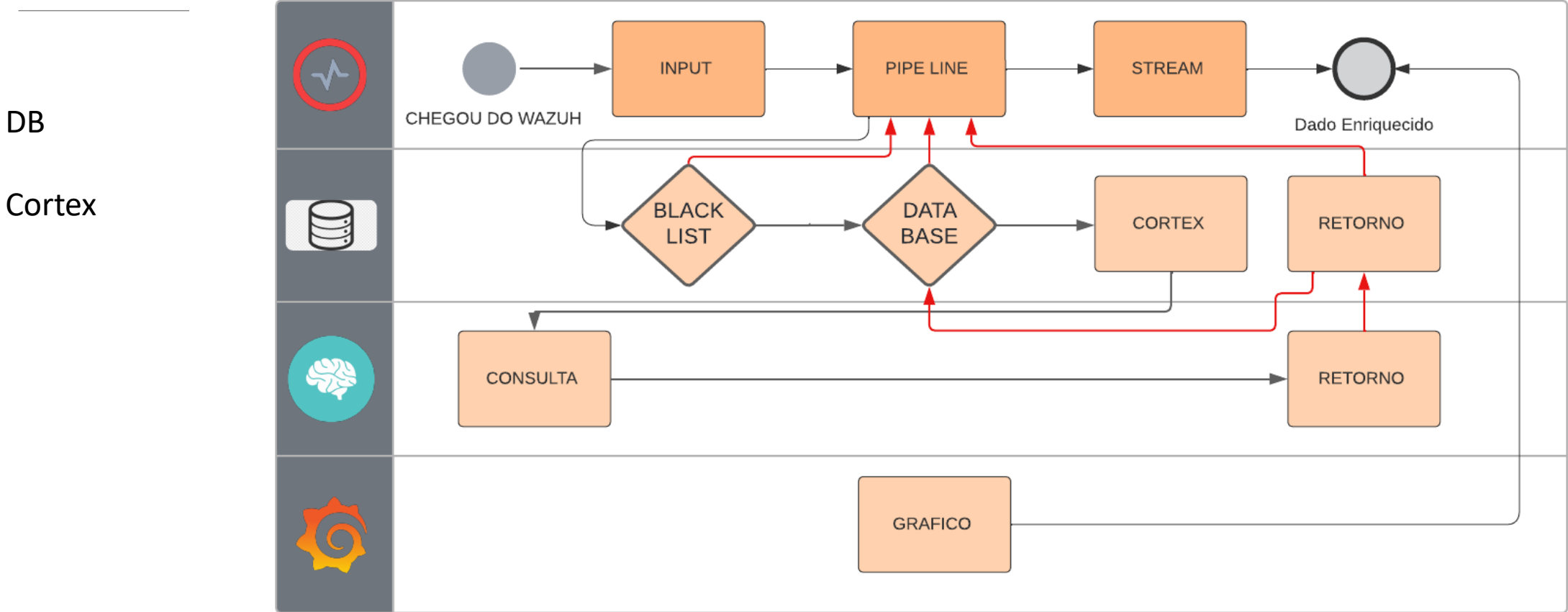
Wazuh<>Graylog<>DB<>Cortex(VirusTotal, Abuse IP, Misp)



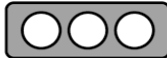
TLP:CLEAR



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



TLP: CLEAR



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

Cortex APIs

The screenshot shows the Cortex web interface with the following details:

- Header:** Cortex logo, + New Analysis, Jobs History, Analyzers (selected), Responders, Organization.
- Section:** Analyzers (3)
- Data Types (13):** Select -
- Analyzer Search:** Search for analyzer description, Search, Clear.
- AbuseIPDB_1_0:** Version: 1.0, Author: Matteo Lodi, License: AGPL-v3. Description: Determine whether an IP was reported or not as malicious by AbuseIPDB. **Applies to:** ip.
- MISP_2_1:** Version: 2.1, Author: Nils Kuhnert, CERT-Bund, License: AGPL-V3. Description: Query multiple MISP instances for events containing an observable. **Applies to:** domain, ip, uri, fqdn, uri_path, user-agent, hash, mail, mail_subject, registry, regexp, other, filename.
- VirusTotal_Rescan_3_1:** Version: 3.1, Author: CERT-LDO, License: AGPL-V3. Description: Use VirusTotal to run new analysis on hash. **Applies to:** hash.

TLP: CLEAR



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

Cortex
Hash
IP
Domain

Success	[hash] 005179dca5a82ff5a17b227241c0a019	Analyzer: VirusTotal_Rescan_3_1	Date: 9 minutes ago
Success	[ip] 187[.]85[.]171[.]174	Analyzer: AbuseIPDB_1_0	Date: 9 minutes ago
Success	[url] 0faee65f937f5daab1541991b1d81d2e[.]clo[.]footprintdns[.]com	Analyzer: MISP_2_1	Date: 9 minutes ago

TLP:CLEAR



Graylog>Teams

<https://github.com/hidappliance/graylog-plugin-teams>

The screenshot shows the Graylog web interface. At the top, the navigation bar includes 'graylog', 'Search', 'Streams', 'Alerts', 'Dashboards', 'Enterprise', 'Security', and 'System'. The 'Alerts' menu item is highlighted with a red box. Below the navigation bar, a secondary menu shows 'Alerts & Events', 'Event Definitions', and 'Notifications'. The 'Event Definitions' menu item is also highlighted with a red box. The main content area is titled 'Event Definitions' and contains a search bar with the text 'Find Event Definitions', a 'Find' button, and a 'Reset' button. Below the search bar, there are two event definitions listed:

- Encontrado DNS Malicioso no MISP** (Filter & Aggregation)
DNS MISP
Runs every 1 minutes, searching within the last 1 minute. Triggers 1 Notification. [Show details](#)
- Encontrado IP Malicioso no ABUSE** (Filter & Aggregation)
IP ABUSE
Runs every 1 minutes, searching within the last 1 minute. Triggers 1 Notification. [Show details](#)

TLP:CLEAR



Graylog>Teams

Recebendo no Teams

teste 09:22

Alert Envia alerta para teams do MISP triggered:
_Encontrado DNS Malicioso no MISP _

--- [EVENTO] ---

Evento:	Envia alerta para teams do MISP
---------	---------------------------------

--- [DETALHES] ---

Timestamp:	2024-06-17T12:22:09.522Z
Cliente Index:	wazuh-lab_0
Cliente Agente:	Windows10
IP do Agente:	10.0.0.103
DNS:	webb-institute.com

Responder

teste 09:22 Novo

Alert Envia alerta para teams do MISP triggered:
_Encontrado DNS Malicioso no MISP _

--- [EVENTO] ---

Evento:	Envia alerta para teams do MISP
---------	---------------------------------

--- [DETALHES] ---

Timestamp:	2024-06-17T12:22:09.522Z
Cliente Index:	wazuh-lab_0
Cliente Agente:	Windows10
IP do Agente:	10.0.0.103
DNS:	gpoaccess.com


Responder

TLP:CLEAR



Graylog>Teams

Cuidar com uma fonte só.
Falso Positivo

 Graylog 09:45 Novo

Alert Encontrado IP Malicioso no ABUSE triggered:
IP ABUSE

--- [EVENTO] ---

Evento:	Encontrado IP Malicioso no ABUSE
---------	----------------------------------

--- [DETALHES] ---

Timestamp:	2024-06-17T12:44:57.333Z
Cliente Index:	wazuh-lab_0
Cliente Agente:	Windows10
IP do Agente:	10.0.0.103
IP ABUSE:	52.101.10.9


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.

52.101.10.9

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

0 / 93
Community Score

10+ detected files communicating with this IP address

52.101.10.9 (52.96.0.0/12)
AS 8075 (MICROSOFT-CORP-MSN-AS-BLOCK)

US Last Analysis Date
2 days ago

Reanalyze Similar Graph API

DETECTION DETAILS RELATIONS COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ Do you want to automate checks?

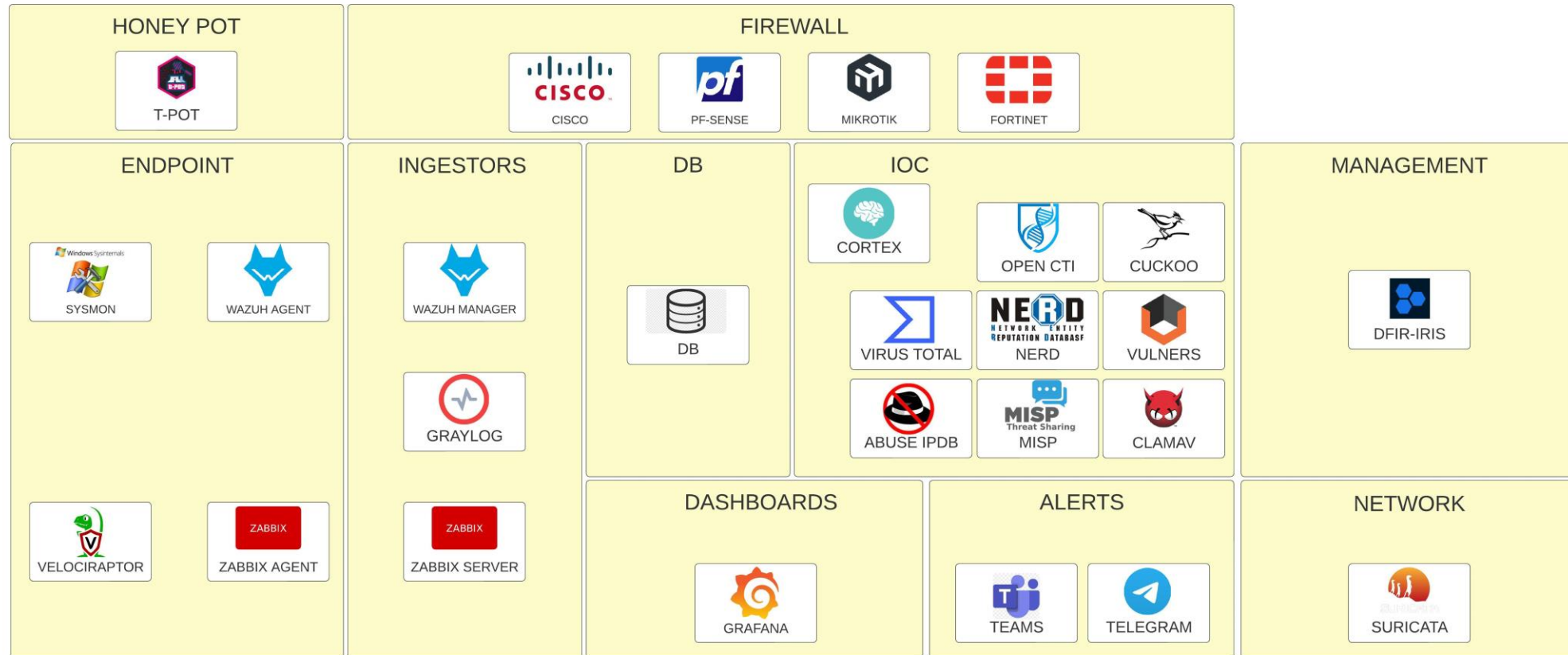
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean

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>

TLP:CLEAR



Agradeço a atenção!

