Monitoring, Detecting, and Responding to Security Incidents with Zabbix, Suricata, and MISP

A Practical Integration

ZABBIX SUMMIT

OCTOBER 8 · 10, 2025
RIGA · LATVIA

Who am I?

Paulo Deolindo – Unirede by Selbetti - Brazil

Talking about...

The problem

Infra-centric monitoring

Proposed solution

Specialized integrations

Expected outcome

Zabbix as part of the SOC & cyberdefense

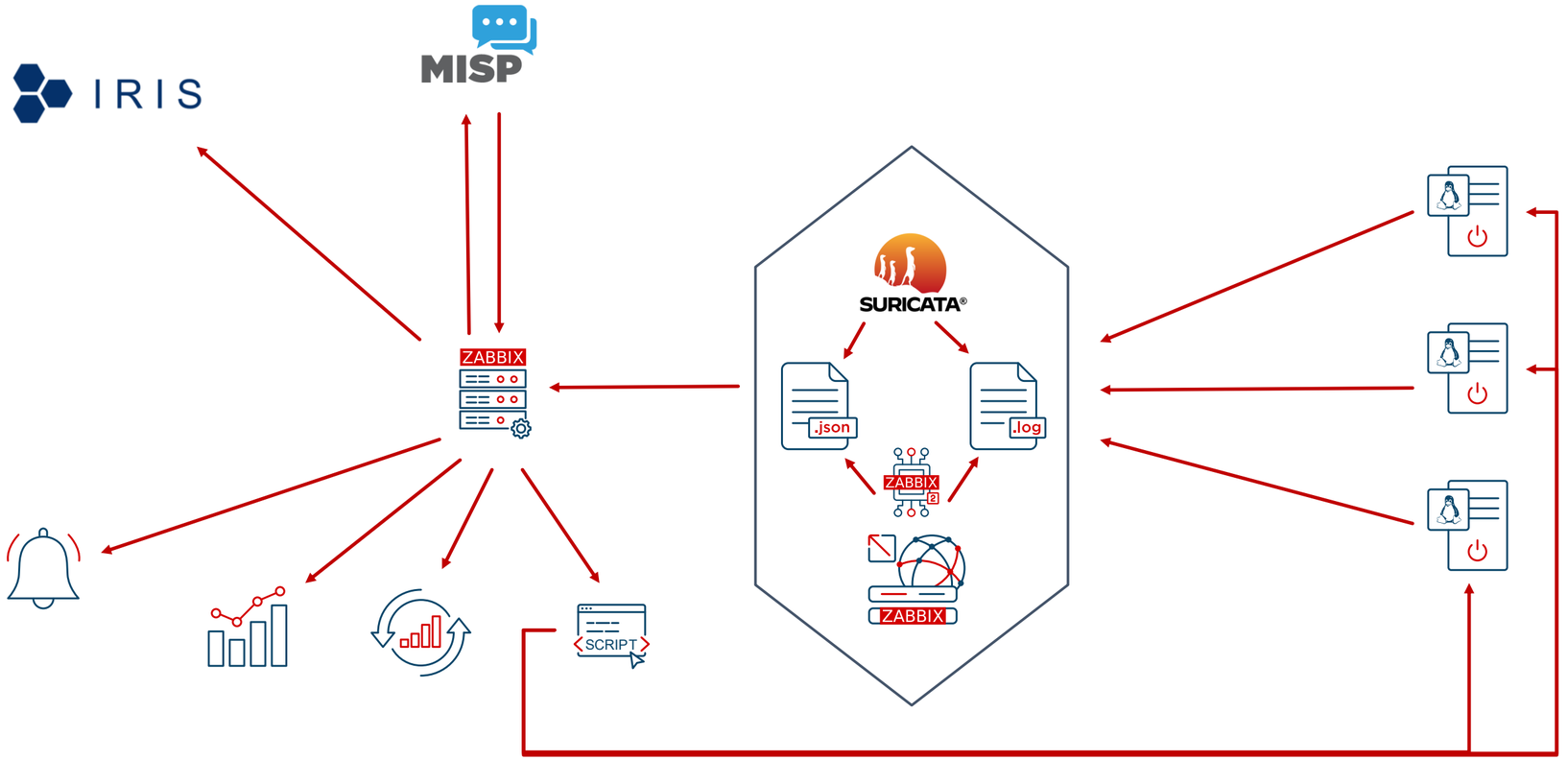
ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

A simple ask...

Do you have any thoughts on network scans?

ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

A basic design


IRIS
MISP
ZABBIX
SURICATA
.json
.log
ZABBIX
ZABBIX
SCRIPT

ZABBIX SUMMIT
OCTOBER 8 · 10, 2025
RIGA · LATVIA

What’s Suricata?

Suricata Event types

SSH

HTTP

FTP

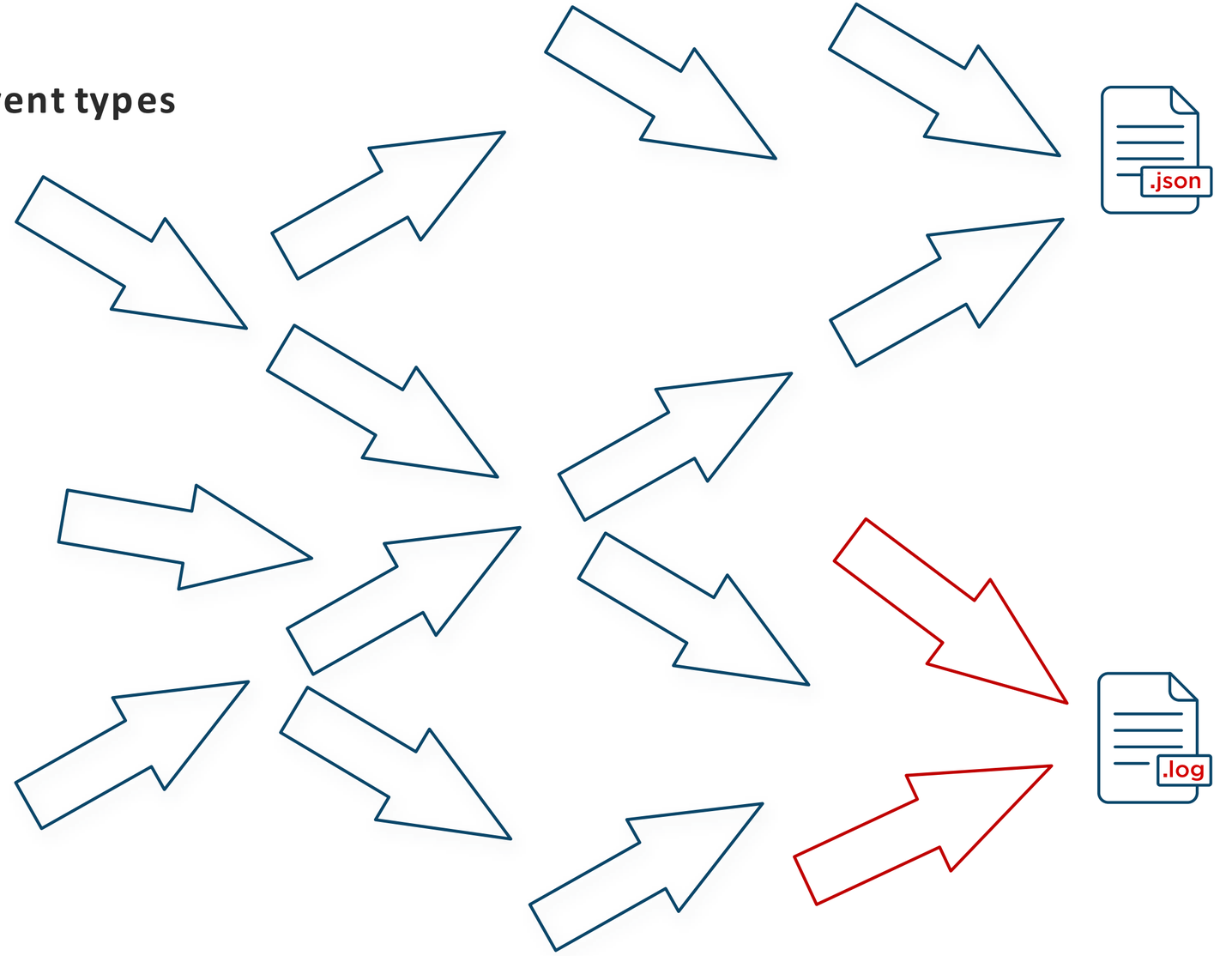
SMB

DNS

TLS

RDP

...



eve.json

all type of events

only alerts

fast.log

Reading Suricata Logs

Reading Suricata Logs

eve.log – Extensible Event Format

A DNS event type

{"timestamp":"2025-08-06T07:01:36.018133…","flow_id":77551404024423,"in_iface":"gre2",
"event_type":"dns","src_ip":"127.0.0.1","src_port":32854,"dest_ip":"127.0.0.53","dest_port":53,"proto":"UDP","ip_v":4,"pkt_src":"
wire/pcap","dns … "rrtype":"AAAA"}]}}

An alert event type

{"timestamp":"2025-09-04T23:24:40.880063-0300","flow_id":120669195496490,"in_iface":"gre3",
"event_type":"alert","src_ip":"78.153.140.176","src_port":48007,"dest_ip":"167.71.246.150","dest_port":443,"proto":"TCP","ip_v":4,"pkt_src":"
wire/pcap", … "dest_ip":"167.71.246.150","src_port":48007,"dest_port":443}}

Reading Suricata Logs

fast.log – standardized line-based

A DNS alert log

09/04/2025-15:05:51.181848 [**] [1:2101616:9] **GPL DNS named version attempt** [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 118.194.250.2:34647 -> 167.71.246.150:**53**

An exploit alert log

09/02/2025-12:05:53.783763 [**] [1:2063094:1**] ET EXPLOIT Zyxel ZyWALL/USG OS Command Injection (CVE-2023-28771)** [**] [Classification: Web Application Attack] [Priority: 1] {UDP} 74.113.97.40:53926 -> 104.236.206.185:**500**

Extracting data from Suricata

Relevant data from fast.log

Timestamp

(\d\d\/\d\d\/\d\d\d\d)-(\d\d:\d\d:\d\d)

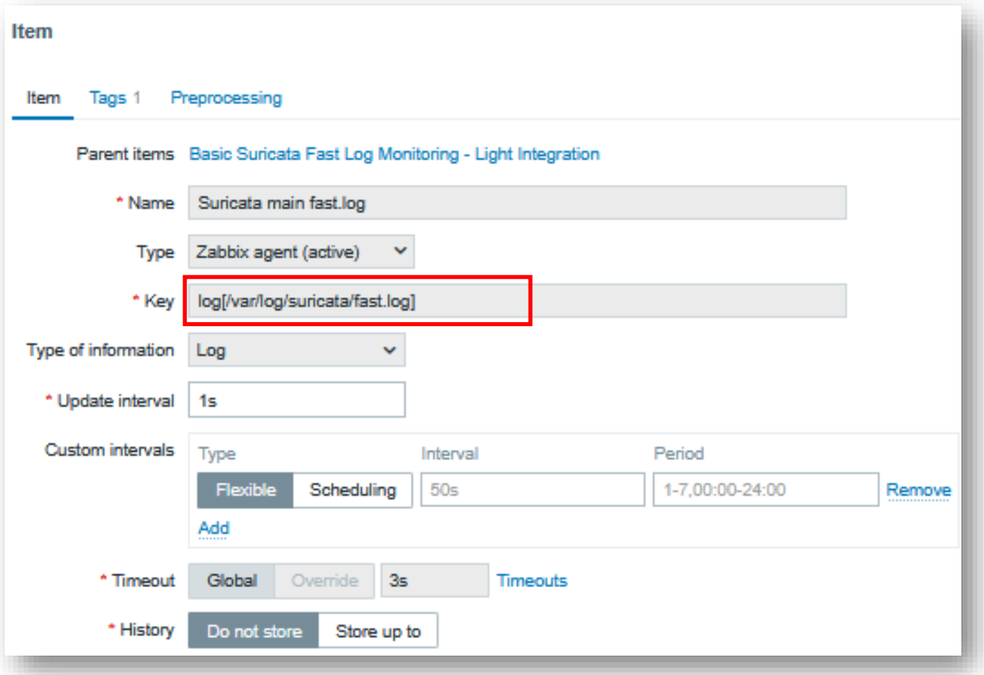
\1 \2

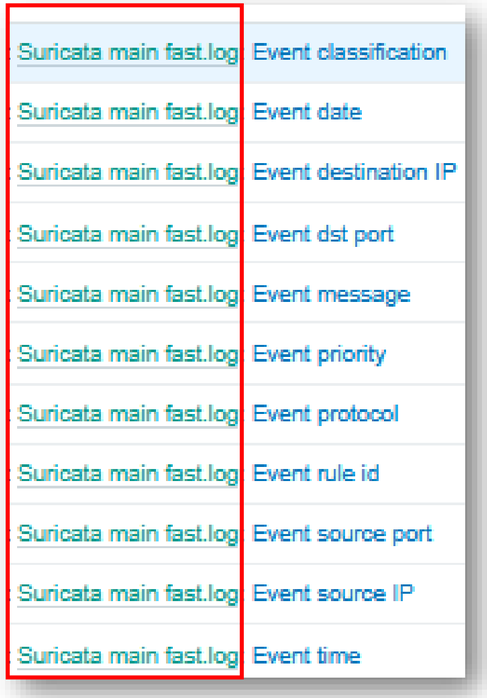
To other pieces of information

\[\d+:(\d+):\d+\]\s+(.*)\s+\[**\]\s+\[Classification:\s+(.*)\]\s+\[Priority:\s+(\d+)\]\s+\{(.*)\}\s+(\d+.\d+.\d+.\d+):(\d+).*?(\d+.\d+.\d+.\d+):(\d+)

\1 \2 \3 \4 \5 \6 \7 \8 \9

First configuration and results

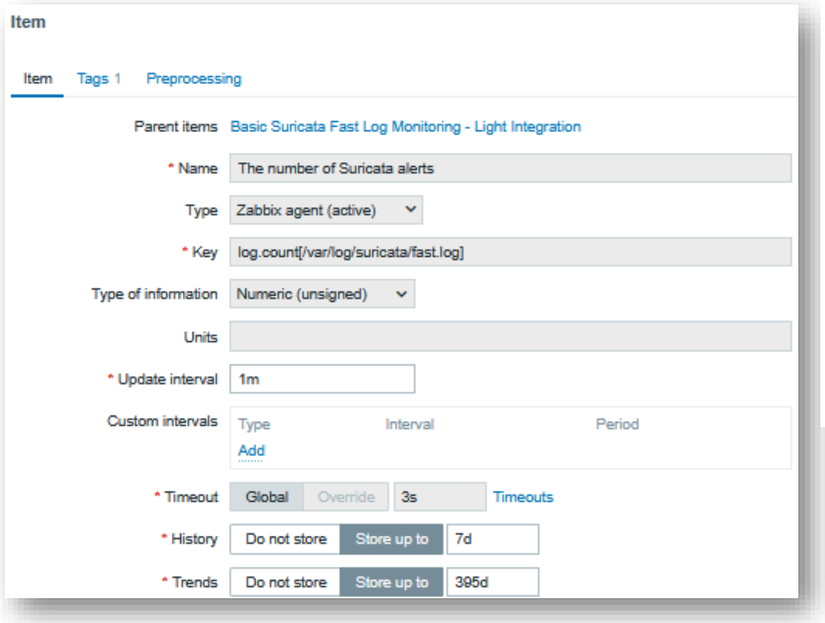


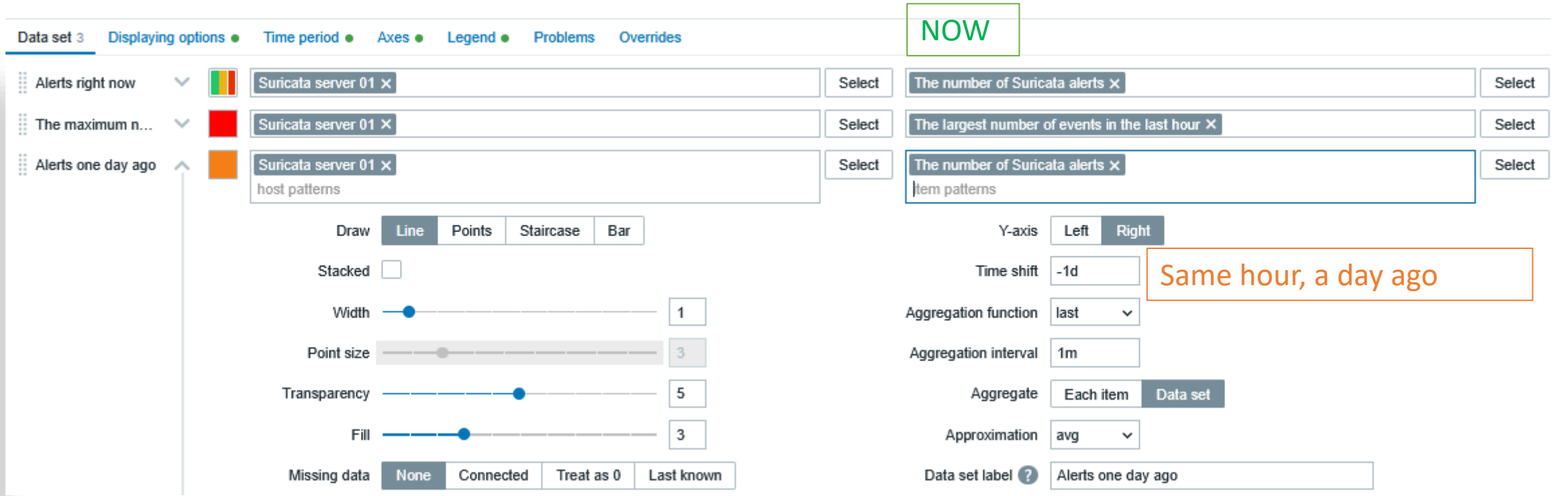


LATEST ALERTS

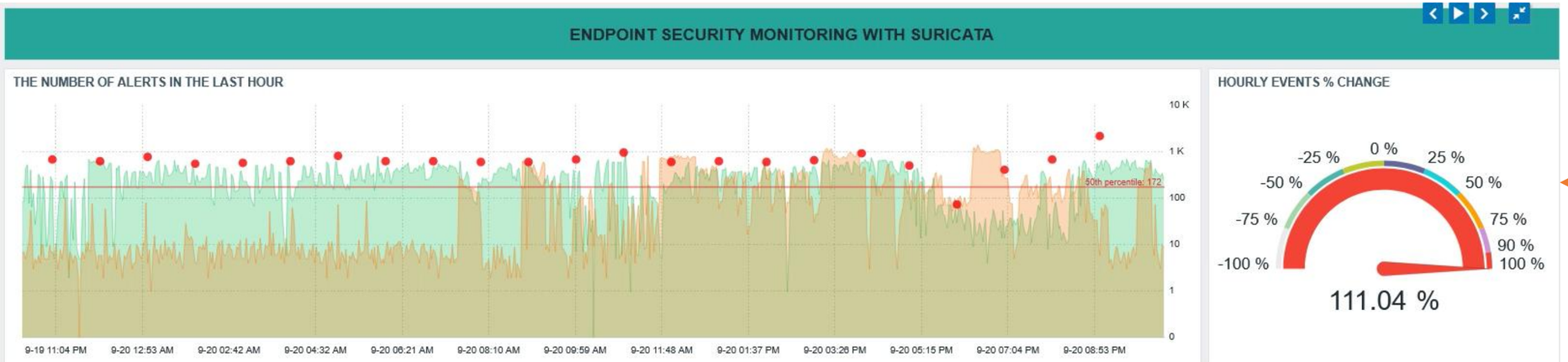
Event date	Event time	Message	Classification	Priority	Source port	Source	Destination IP	Destination port	Protocol
09/05/2025	00:01:20	ET DROP Spamhaus DROP Listed Traffic Inbound group 46	Misc Attack	2	51824	196.251.114.29	174.138.69.162	22	TCP
09/05/2025	00:00:39	ET DROP Dshield Block Listed Source group 1	Misc Attack	2	50824	206.168.34.138	167.71.246.150	52317	TCP
09/05/2025	00:00:20	ET CINS Active Threat Intelligence Poor Reputation IP group 47	Misc Attack	2	57108	35.203.211.219	174.138.69.162	911	TCP
09/05/2025	00:00:13	ET CINS Active Threat Intelligence Poor Reputation IP group 69	Misc Attack	2	33990	45.79.132.41	104.236.206.185	6697	TCP
09/05/2025	00:00:08	ET DROP Dshield Block Listed Source group 1	Misc Attack	2	35240	64.62.197.132	167.71.246.150	8070	TCP

Abnormal events (alerts)

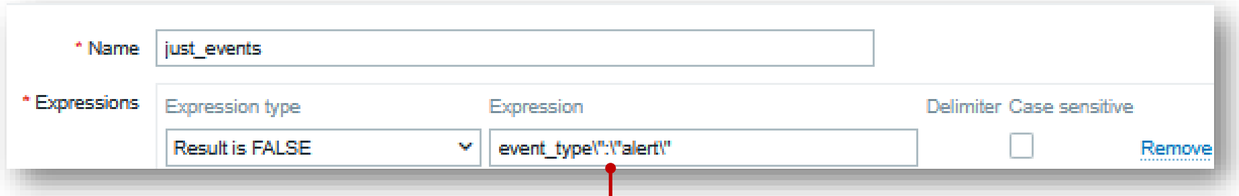





```
((sum(//log.count[/var/log/suricata/fast.log],1h:now/h+1h) -
sum(//log.count[/var/log/suricata/fast.log],1h:now/h)) /
sum(//log.count[/var/log/suricata/fast.log],1h:now/h)) * 100
```



Counting only normal events



Excluding “alerts” from eve.json

– log.count[/var/log/suricata/eve.json,"@just_events",,,skip]

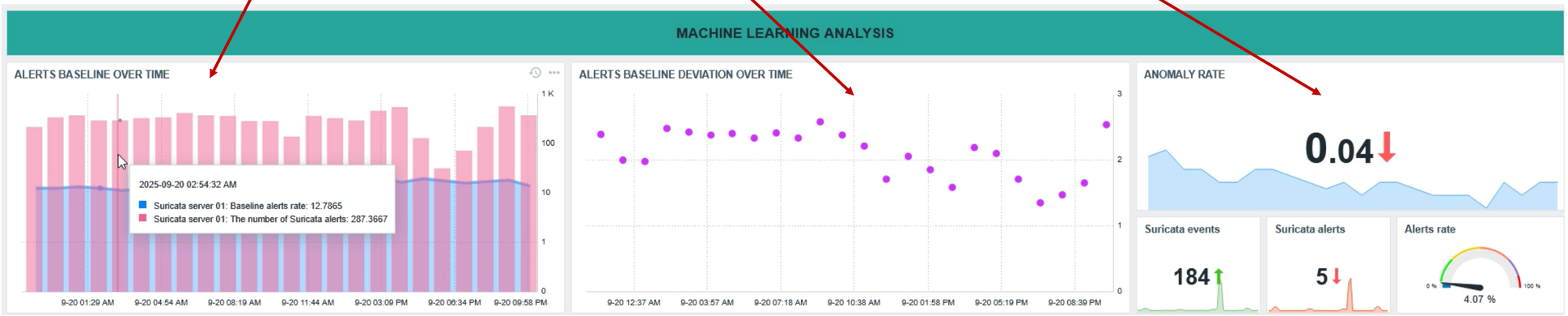
  - Where "@just_events“ is a global regular expression

```
(
   last(//log.count[/var/log/suricata/fast.log]) /
   (last(//log.count[/var/log/suricata/fast.log]) +
   last(//log.count[/var/log/suricata/eve.json,”@just_events”,,,skip]))
)
 * 100
```

Including AI/ML

Out-of-the-box Zabbix machine learning features

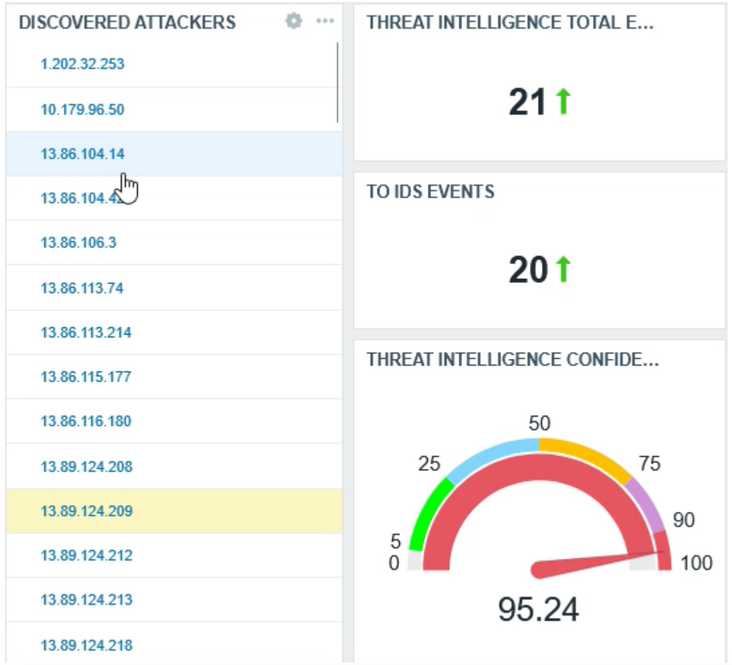
- To calculate events baseline, deviations, and anomaly rate

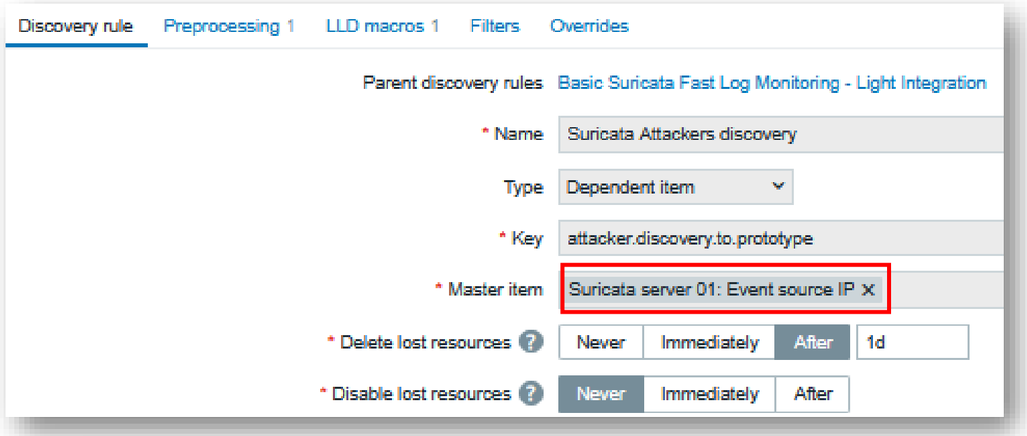


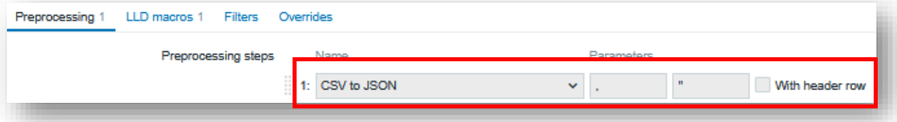
Discovering attackers

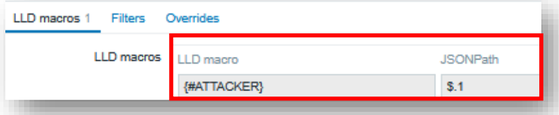
Based on the attacker source IP

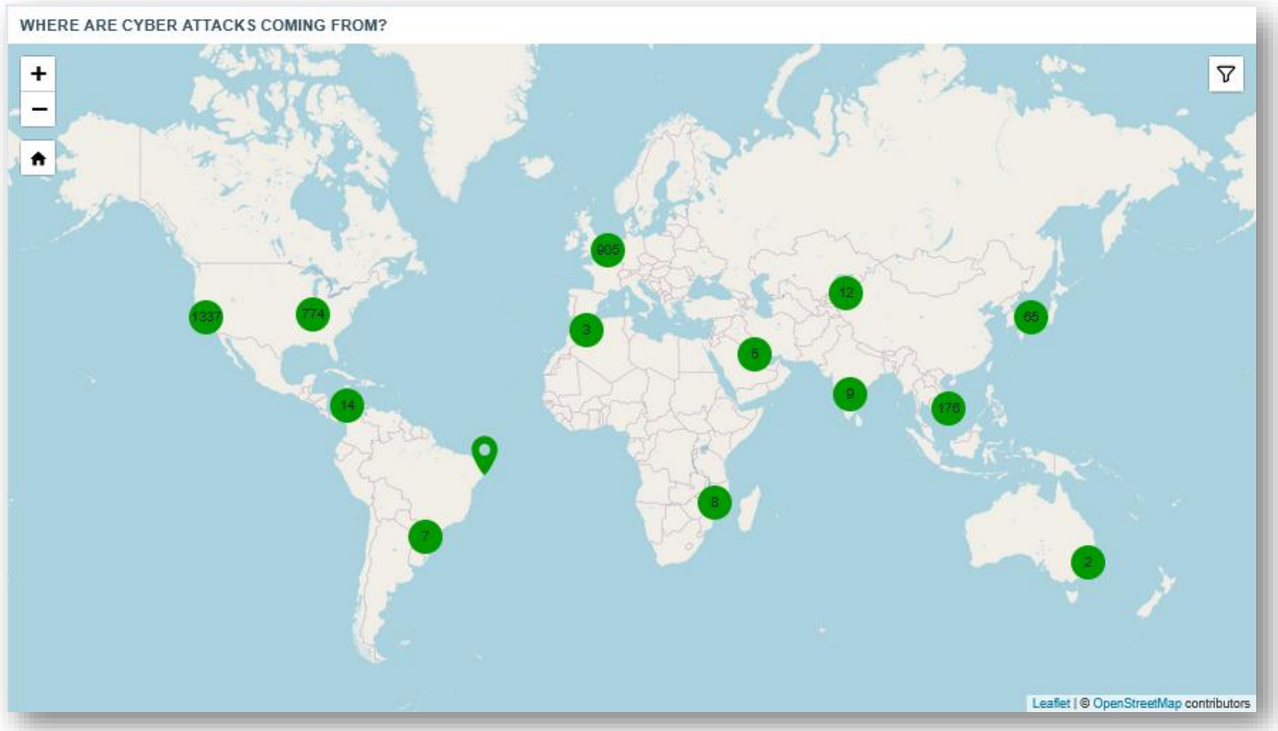
- Appling "geolocation" and "Basic MISP" templates









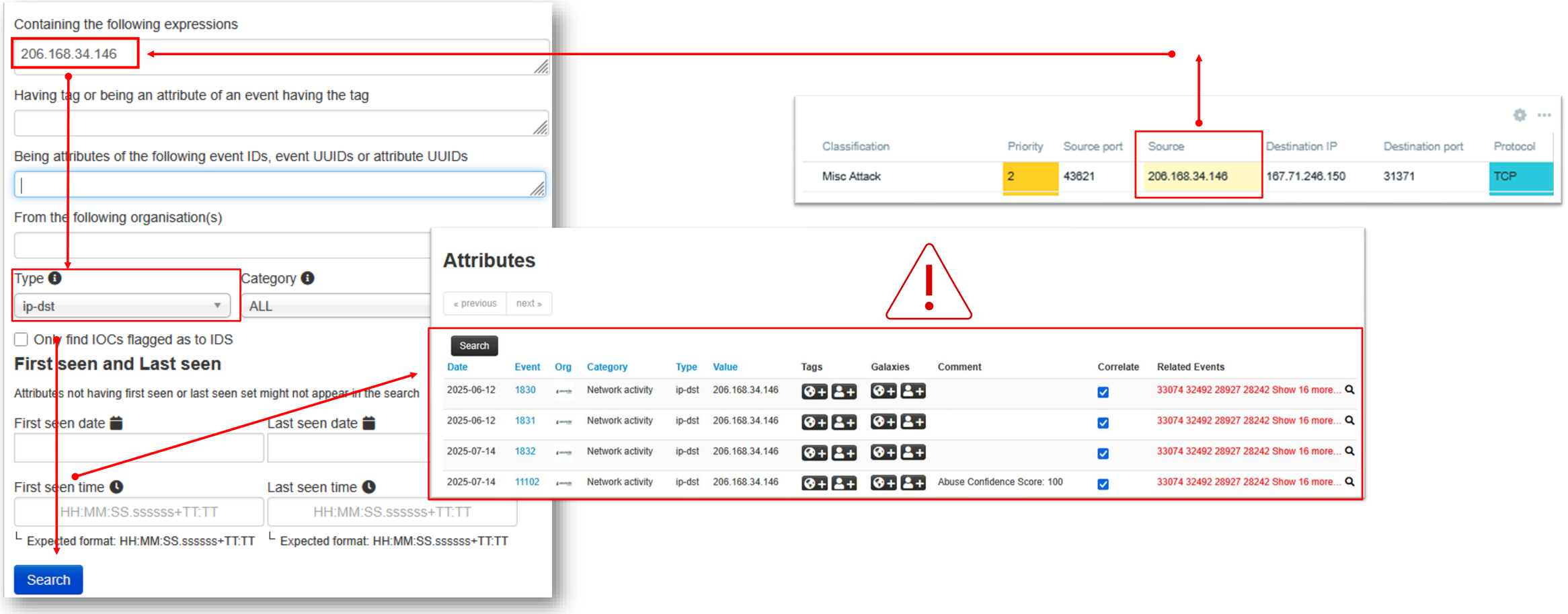


What’ s MISP?

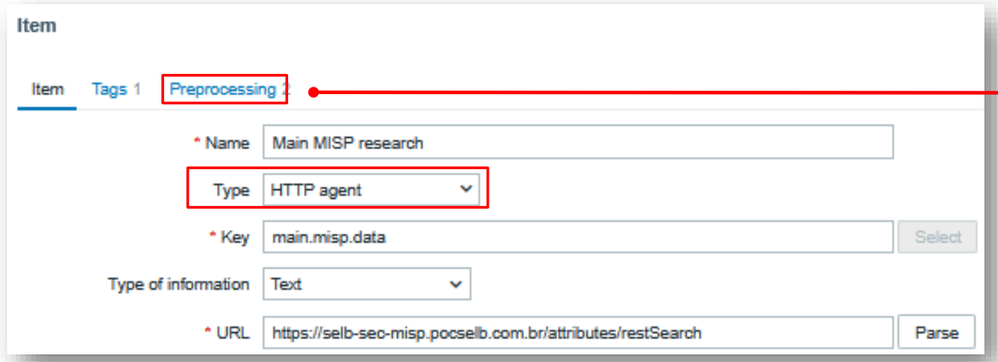
Malware Information Sharing Platform

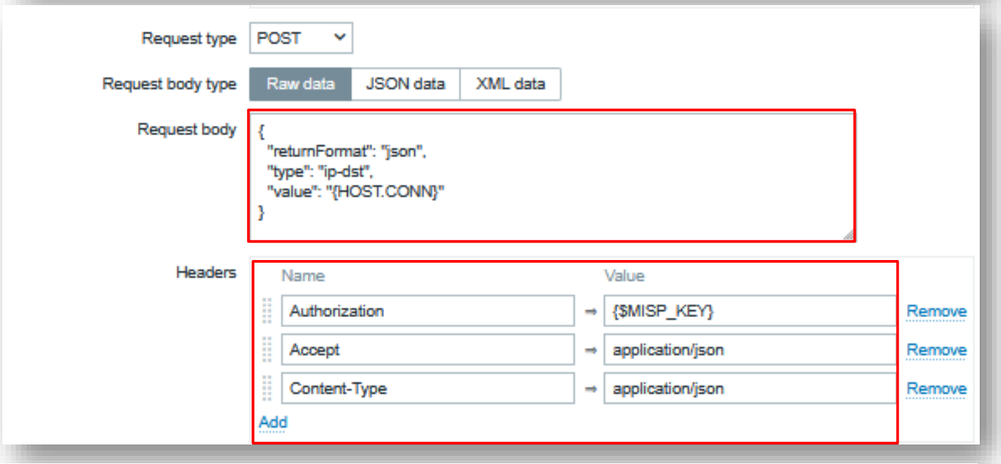
Searching for IoCs in MISP

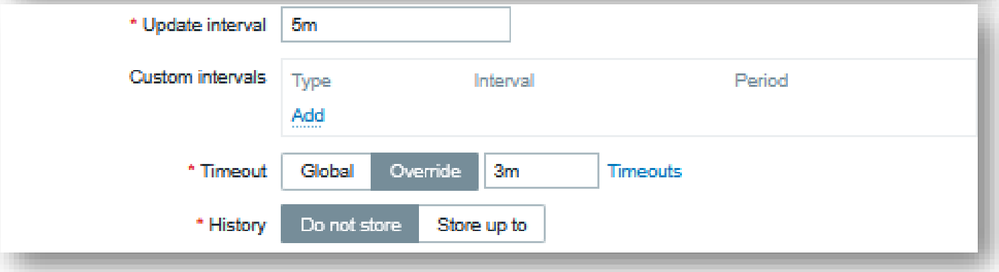
Based on the attacker source IP



The Zabbix way





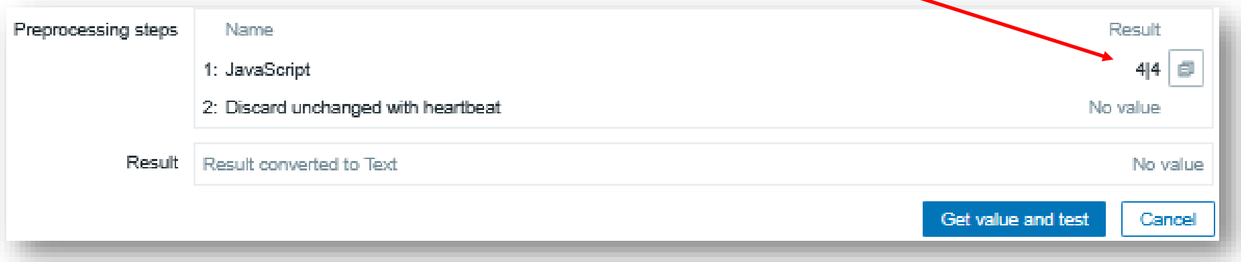



```
var data = JSON.parse(value);

var total = 0;
var to_ids_true = 0;

for (var i = 0; i < data.response.Attribute.length; i++) {
   var attr = data.response.Attribute[i];
   total = total + 1;
   if (attr.to_ids) {
      to_ids_true = to_ids_true + 1;
   }
}

// Retorna no formato total|to_ids_true
return total + "|" + to_ids_true;
```



Basic Results and Reliability Score

MISP total events

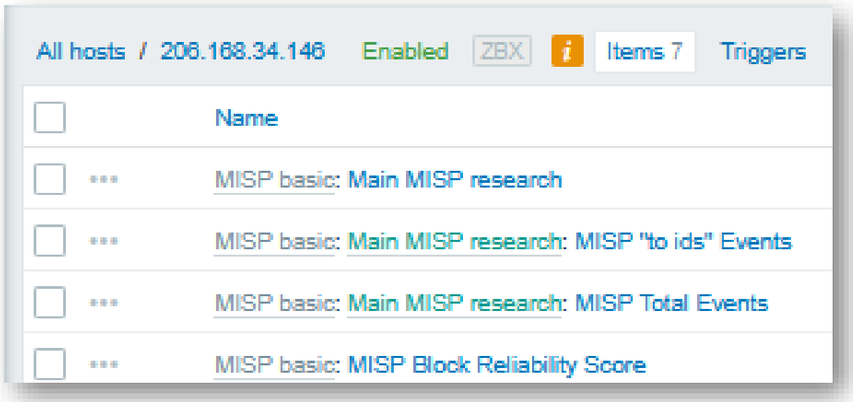
The number of total events in MISP for an attacker

MISP “to ids” events

The number of total events in MISP indicating a drop for the attacker

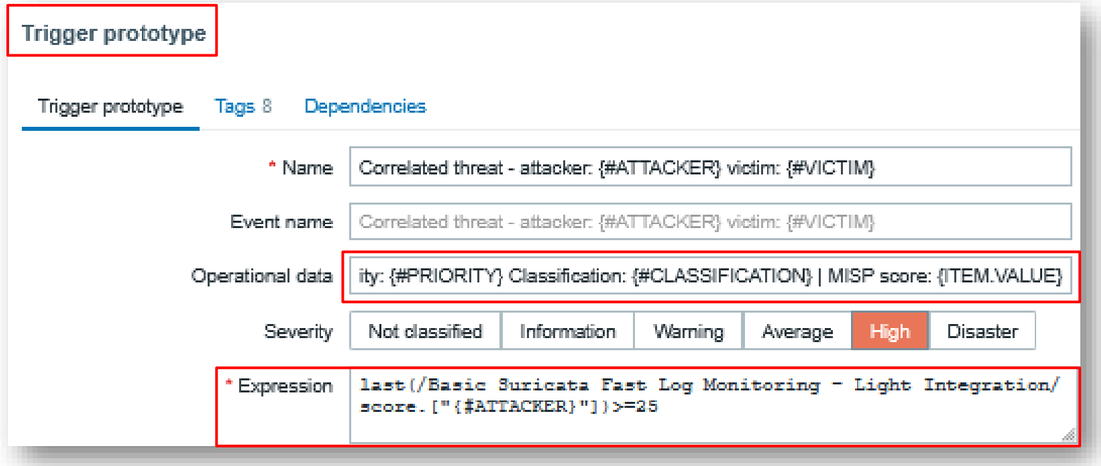
MISP Reliability Score

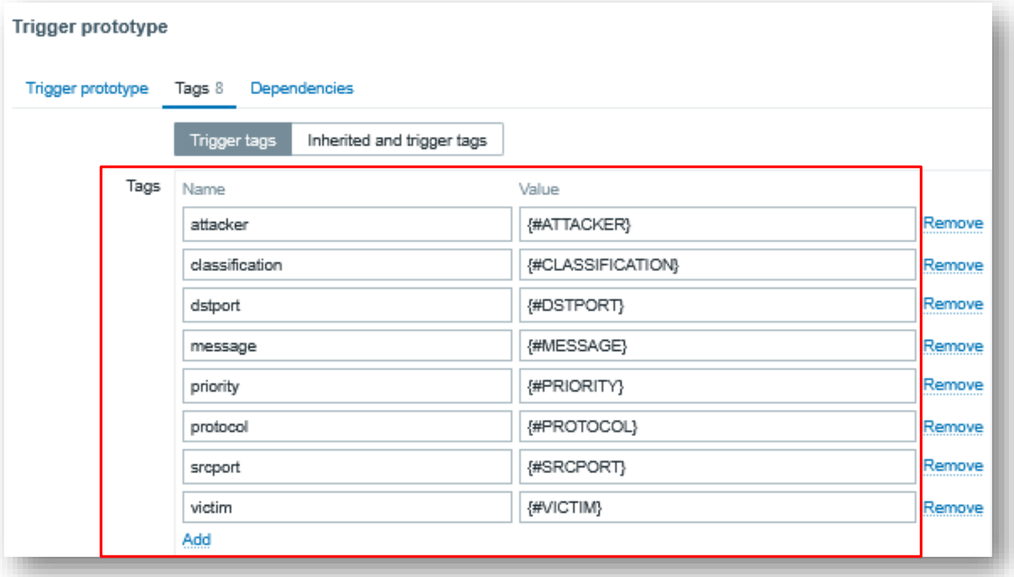
This is a customized “Confidence Score”

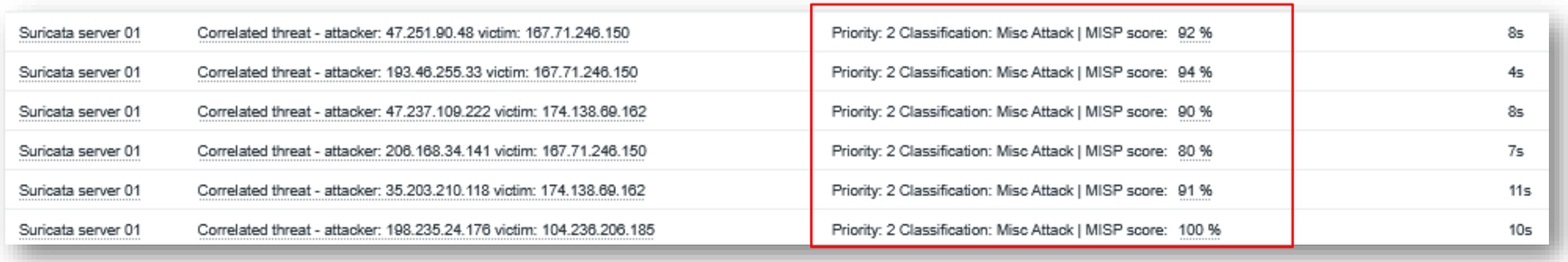



```
last(//misp.toids.events) / last(//misp.total.events) * 100
```

Threat intelligence-based trigger







IR and Zabbix Actions

Zabbix Scripts to IR (XDR feature)

To block the IP

Blocking the attacker IP at the source endpoint

To feed MISP

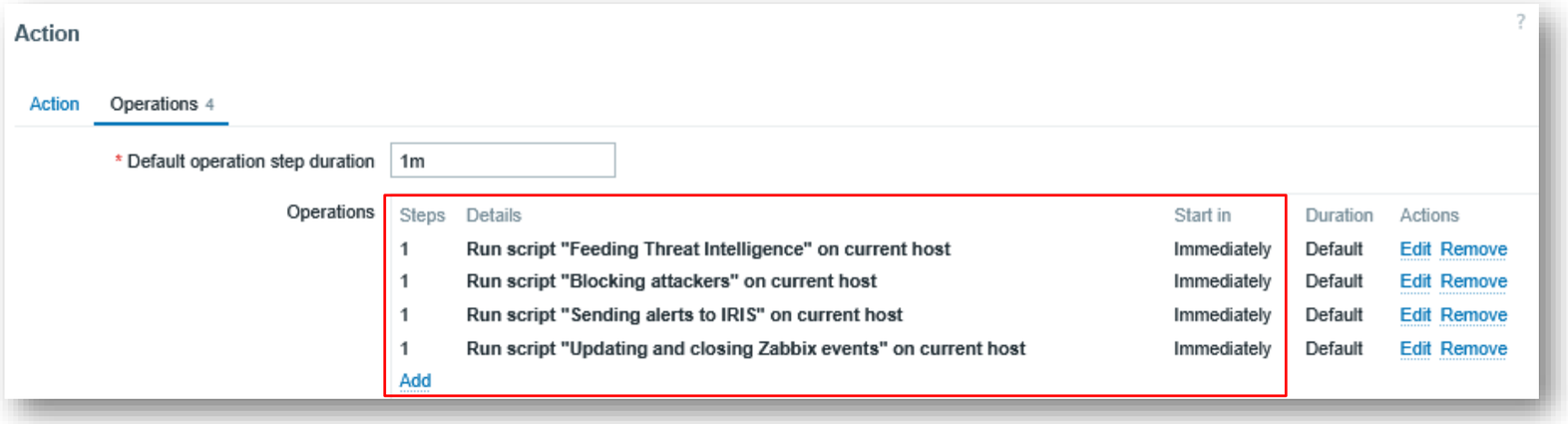
Feeding MISP to contribute with the others

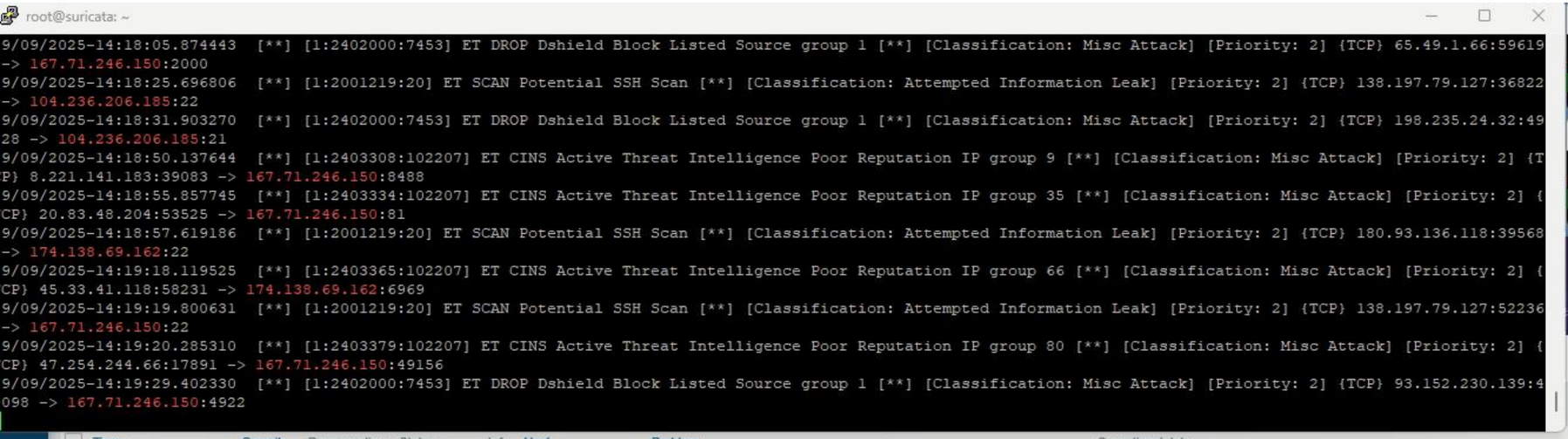
To send a DFIR alert

Opening a Forensic Case to investigate

To close the problem

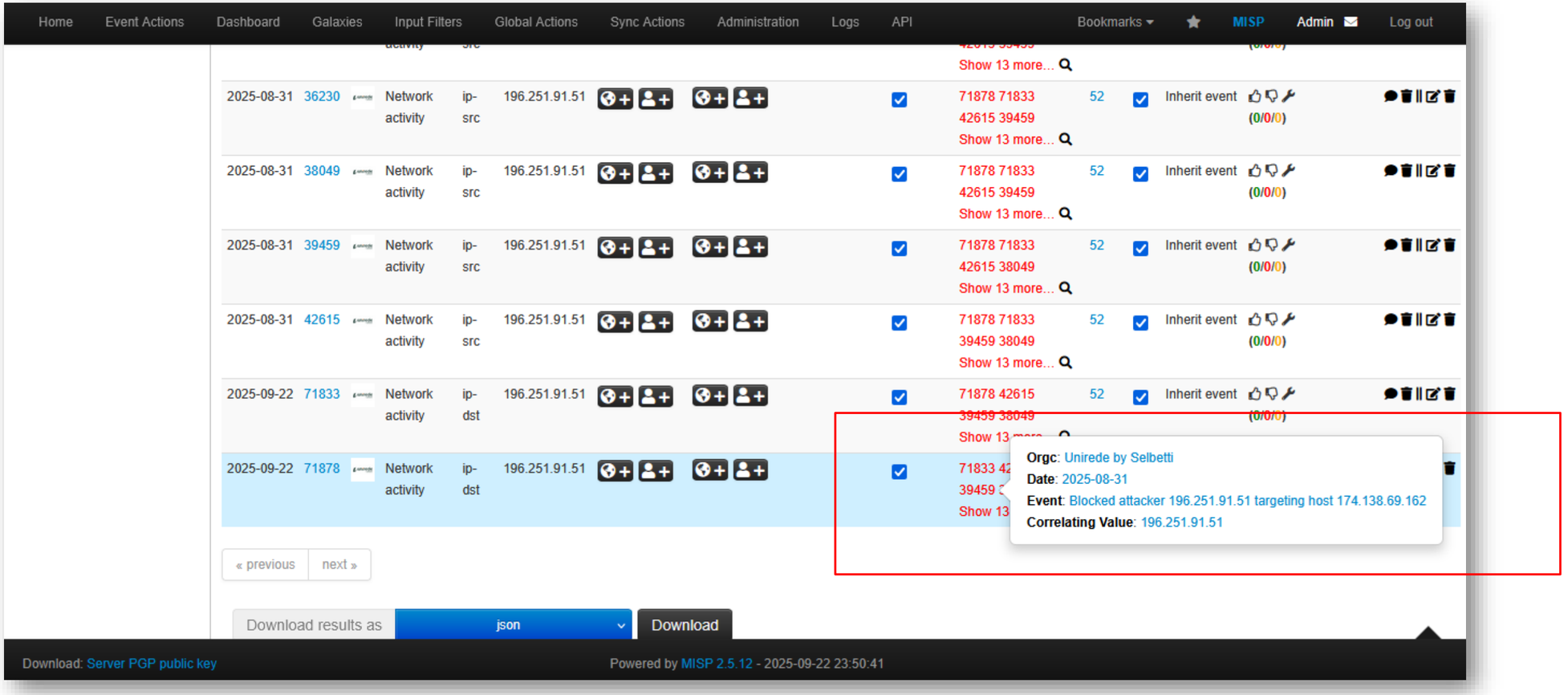
Closing the original Zabbix event





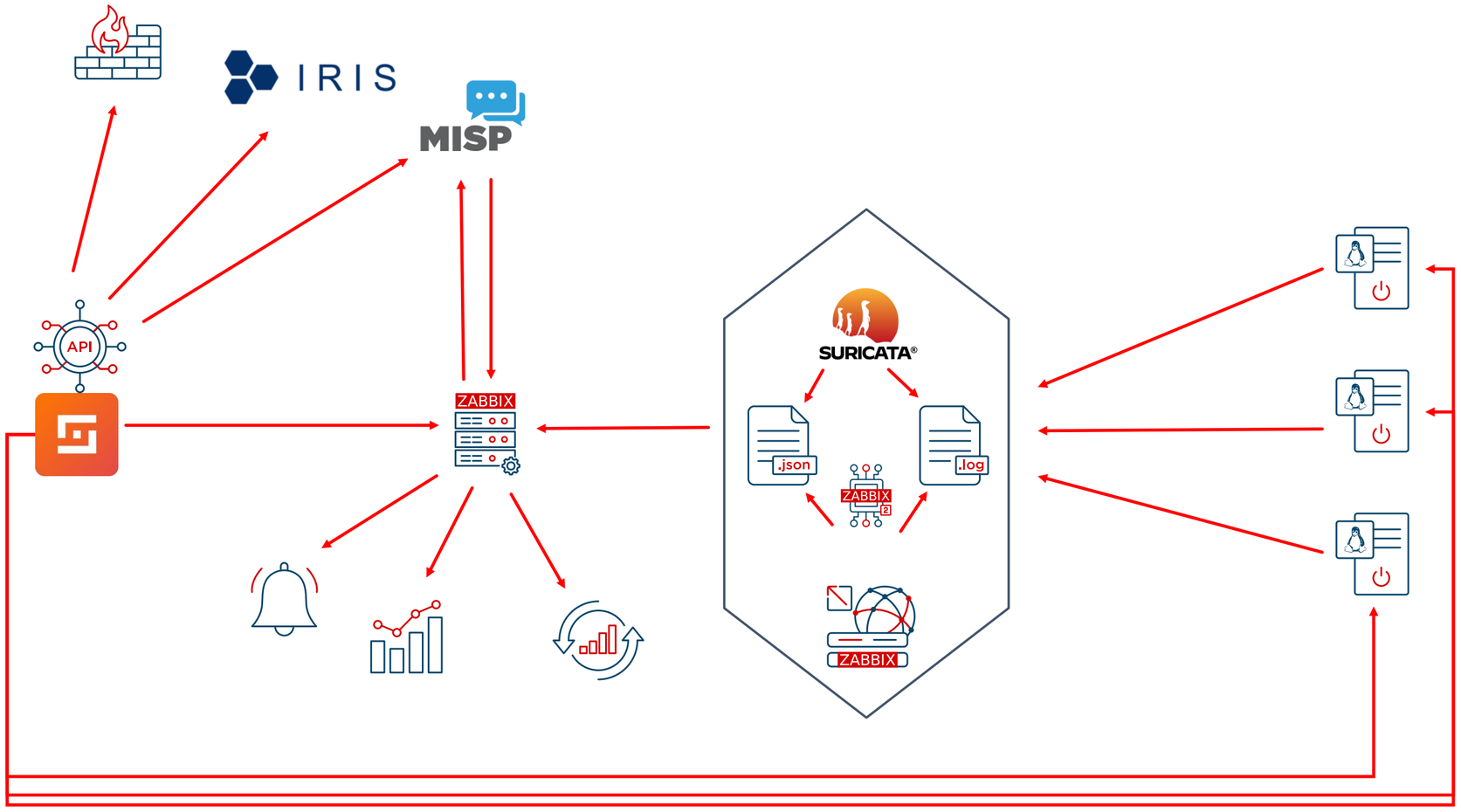
Time	Severity	Recovery time	Status	Info	Host	Problem	Operational data	Duration	Update	Actions	Tags
02:19:36 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 35.203.210.73 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 94 %	2s	Update		attacker: 35.203.210.73 classification: Misc Att...
02:19:35 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 65.49.1.66 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 94 %	3s	Update		attacker: 65.49.1.66 classification: Misc Att...
02:19:23 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 65.49.1.59 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 100 %	15s	Update		attacker: 65.49.1.59 classification: Misc Att...
02:19:21 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 5.63.107.38 victim: 104.236.206.185	Priority: 2 Classification: Potentially Bad Traffic | MISP score: 89 %	17s	Update		attacker: 5.63.107.38 classification: Potentia...
02:19:19 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 45.142.193.27 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 100 %	19s	Update		attacker: 45.142.193.27 classification: Misc Att...
02:19:17 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 35.203.211.17 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 89 %	21s	Update		attacker: 35.203.211.17 classification: Misc Att...
02:19:07 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 45.142.193.176 victim: 104.236.206.185	Priority: 2 Classification: Misc Attack | MISP score: 100 %	31s	Update		attacker: 45.142.193.176 classification: Misc Att...
02:19:05 PM	High		PROBLEM		Suricata server 01	Correlated threat - attacker: 45.91.171.169 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 93 %	33s	Update		attacker: 45.91.171.169 classification: Misc Att...
02:18:40 PM	High		CLOSING		Suricata server 01	Correlated threat - attacker: 147.185.132.94 victim: 104.236.206.185	Priority: 2 Classification: Misc Attack | MISP score: 94 %	58s	Update		attacker: 147.185.132.94 classification: Misc Att...
02:18:27 PM	High	02:19:35 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 176.65.148.189 victim: 104.236.206.185	Priority: 2 Classification: Misc Attack | MISP score: 100 %	1m 8s	Update		attacker: 176.65.148.189 classification: Misc Att...
02:18:11 PM	High	02:19:25 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 45.79.177.245 victim: 104.236.206.185	Priority: 2 Classification: Misc Attack | MISP score: 93 %	1m 14s	Update		attacker: 45.79.177.245 classification: Misc Att...
02:18:06 PM	High	02:19:25 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 45.82.76.97 victim: 104.236.206.185	Priority: 2 Classification: Misc Attack | MISP score: 92 %	1m 19s	Update		attacker: 45.82.76.97 classification: Misc Att...
02:18:03 PM	High	02:19:25 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 65.49.1.199 victim: 104.236.206.185	Priority: 2 Classification: Misc Attack | MISP score: 93 %	1m 22s	Update		attacker: 65.49.1.199 classification: Misc Att...
02:17:57 PM	High	02:19:25 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 20.55.88.100 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 90 %	1m 28s	Update		attacker: 20.55.88.100 classification: Misc Att...
02:17:55 PM	High	02:19:20 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 205.210.31.141 victim: 104.236.206.185	Priority: 2 Classification: Misc Attack | MISP score: 100 %	1m 25s	Update		attacker: 205.210.31.141 classification: Misc Att...
02:17:53 PM	High	02:19:20 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 47.254.255.250 victim: 174.138.69.162	Priority: 2 Classification: Misc Attack | MISP score: 93 %	1m 27s	Update		attacker: 47.254.255.250 classification: Misc Att...
02:17:52 PM	High	02:19:20 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 185.93.89.222 victim: 174.138.69.162	Priority: 2 Classification: Misc Attack | MISP score: 100 %	1m 28s	Update		attacker: 185.93.89.222 classification: Misc Att...
02:17:44 PM	High	02:19:10 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 23.239.4.211 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 94 %	1m 26s	Update		attacker: 23.239.4.211 classification: Misc Att...
02:17:36 PM	High	02:19:10 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 35.203.210.73 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 93 %	1m 34s	Update		attacker: 35.203.210.73 classification: Misc Att...
02:17:28 PM	High	02:18:35 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 45.79.73.216 victim: 174.138.69.162	Priority: 2 Classification: Misc Attack | MISP score: 89 %	1m 7s	Update		attacker: 45.79.73.216 classification: Misc Att...
02:17:25 PM	High	02:18:30 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 45.82.76.86 victim: 174.138.69.162	Priority: 2 Classification: Misc Attack | MISP score: 88 %	1m 5s	Update		attacker: 45.82.76.86 classification: Misc Att...
02:17:21 PM	High	02:18:30 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 5.63.107.38 victim: 104.236.206.185	Priority: 2 Classification: Potentially Bad Traffic | MISP score: 88 %	1m 9s	Update		attacker: 5.63.107.38 classification: Potentia...
02:17:17 PM	High	02:18:20 PM	RESOLVED		Suricata server 01	Correlated threat - attacker: 35.203.211.17 victim: 167.71.246.150	Priority: 2 Classification: Misc Attack | MISP score: 88 %	1m 3s	Update		attacker: 35.203.211.17 classification: Misc Att...

Feeding MISP with the current attack data

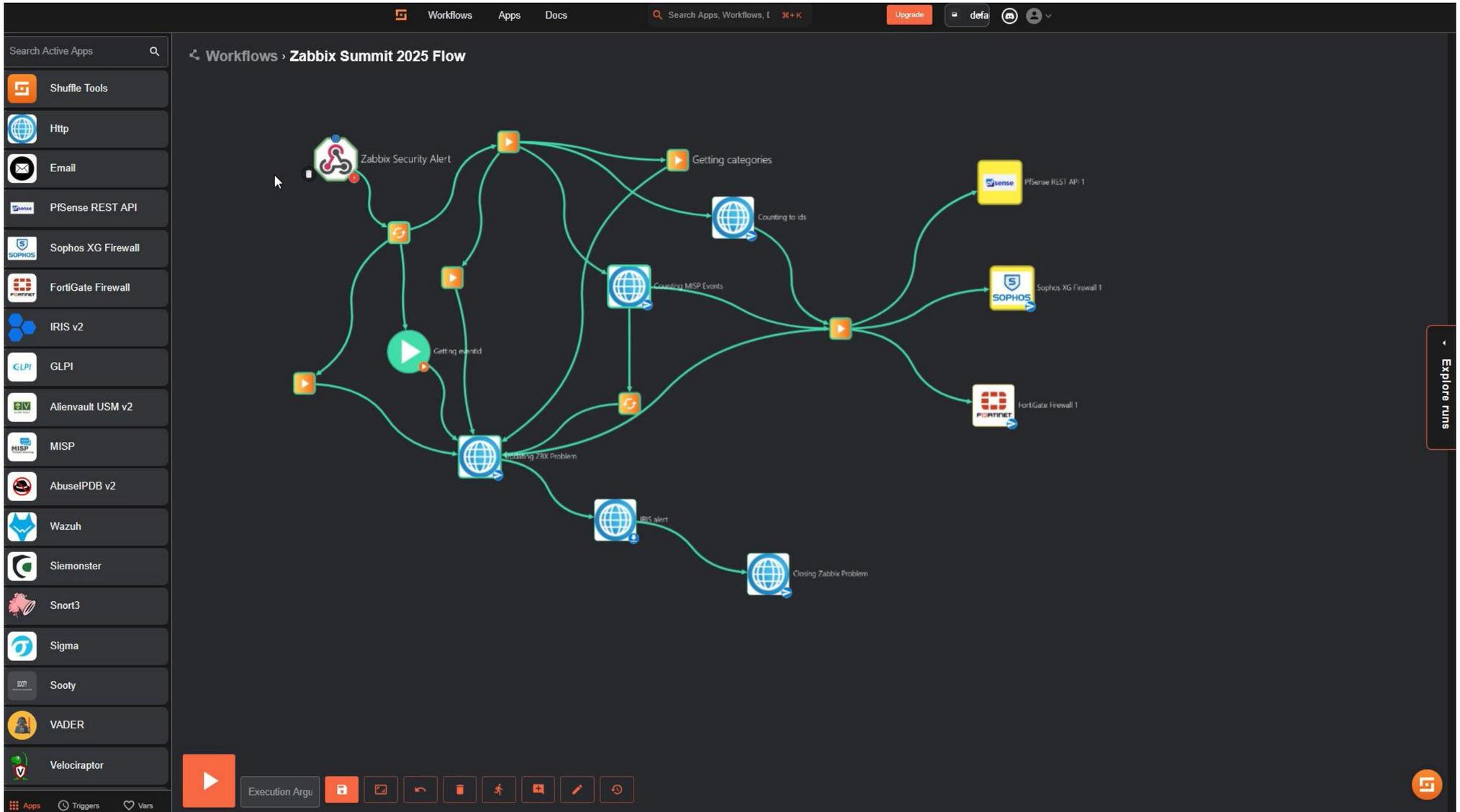


Shuffle

To offload Zabbix Server


IRIS
MISP
API
ZABBIX
SURICATA®
.json
.log
ZABBIX
ZABBIX

How it works?


Workflows
Apps
Docs
Search Apps, Workflows, ⌘+K
Upgrade
Search Active Apps
Workflows › Zabbix Summit 2025 Flow
Shuffle Tools
Http
Email
PfSense REST API
Sophos XG Firewall
FortiGate Firewall
IRIS v2
GLPI
Alienvault USM v2
MISP
AbuseIPDB v2
Wazuh
Siemonster
Snort3
Sigma
Sooty
VADER
Velociraptor
Zabbix Security Alert
Getting categories
Counting to ids
Counting MISP Events
Getting eventid
Updating ZBX Problem
IRIS alert
Closing Zabbix Problem
PfSense REST API 1
Sophos XG Firewall 1
FortiGate Firewall 1
Explore runs
Execution Argu
Apps
Triggers
Vars

In conclusion

Zabbix can...

Perform Incident Response

Be careful with Zabbix resources

Get extra intelligence

From Suricata and MISP

Be part of a SOC

Not as a central component, but in collaboration with other tools

Offload Zabbix is important because it can...

Focus on AI/ML

Learn the behavior of the environment

Focus on Threat Intelligence

Generate visibility to attackers and its confidence scores

Focus on analysis

Powerful functions to analyze Suricata data and generate valuable insights

Thank you!

Paulo Deolindo – Zabbix Trainer

Unirede by Selbetti - Brazil