ZABBIX '25

CONFERENCE

LATIN AMERICA

ZABBIX '25
CONFERENCE
LATIN AMERICA

Monitoramento, detecção e resposta a eventos de segurança cibernética com Zabbix e suricata

Paulo Deolindo

Zabbix Trainer

Monitorar
Detectar
Responder

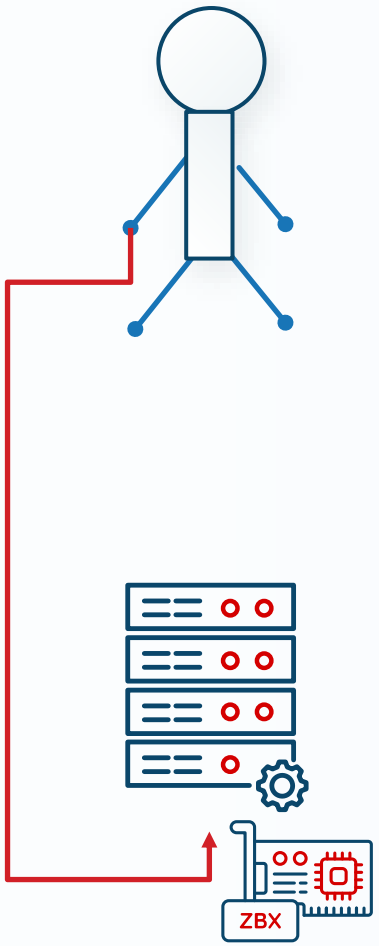
Lidando com eventos de segurança cibernética!

Monitorar

Sobre o Suricata

O Suricata é um software de análise de rede e detecção de ameaças de alto desempenho e de código aberto usado pela maioria das organizações públicas e privadas e incorporado por grandes fornecedores para proteger seus ativos.

Eventos com Suricata



- ANOMALY
- HTTP
- DNS
- FTP
- TLS
- TFTP
- SMB
- TORRENT
- SSH
- FLOW
- RDP
- RFB
- MQTT
- HTTP2
- PGSQL
- IKE
- MODBUS
- QUIC
- DHCP
- ARP
- POP

Eventos no Suricata

Extensible Event Format

(EVE)

Extensible Event Format

ZABBIX '25 CONFERENCE LATIN AMERICA


```
{
  "timestamp": "2025-05-23T18:03:21.692447-0300",
  "flow_id": 1611972622053204,
  "in_iface": "eth0",
  "event_type": "http",
  "src_ip": "80.82.77.202",
  "src_port": 60000,
  "dest_ip": "165.227.65.66",
  "dest_port": 80,
  "proto": "TCP",
  "pkt_src": "stream (flow timeout)",
  "tx_id": 0,
  "http": {
    "url": "/",
    "http_user_agent": "Mozilla/5.0 (Linux; U; Android 2.1; en-us; HTC Legend Build/cupcake) AppleWebKit/530.17
(KHTML, like Gecko) Version/4.0 Mobile Safari/530.17",
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.0",
    "status": 200,
    "length": 7742
  }
}
```


```
grep 'event_type\":\"http\"' /var/log/suricata/eve.json | tail -1 | jq
```

Gerando Eventos

/var/log/suricata/eve.json

root@some-server: ~

```
root@some-server:~# tail -1f /var/log/suricata/eve.json | grep 64.225.60.171
```

Gerando eventos diversos

Arquivo Editar Exibir

```
Gerando eventos diversos

1- ICMP ATTACK
ping -c1 165.227.65.66

2- SCAN
nmap 165.227.65.66

3- SSH ATTEMPT
ssh 165.227.65.66

4- FTP ATTEMPT
```

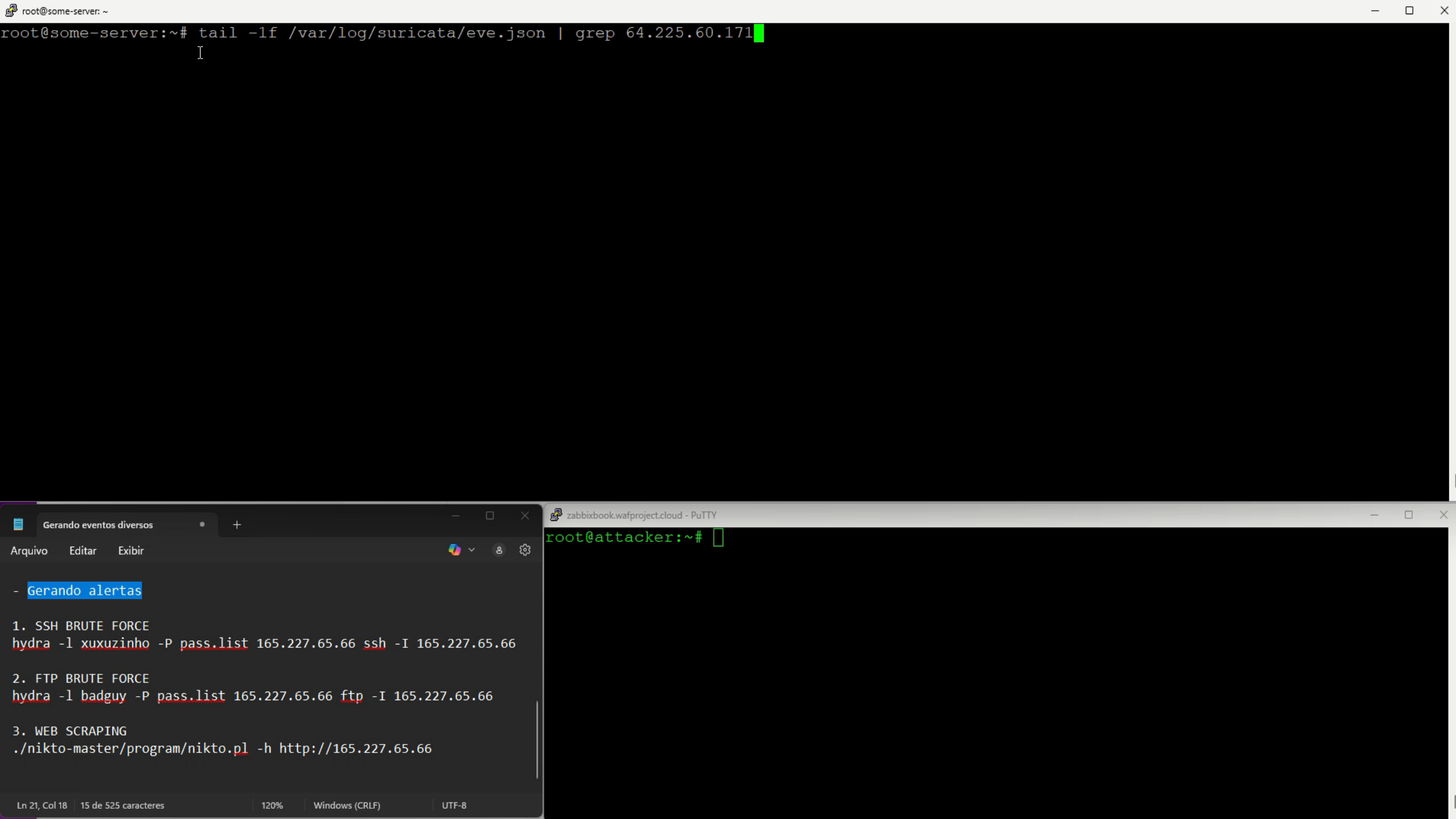
Ln 32, Col 1 | 526 caracteres | 120% | Windows (CRLF) | UTF-8

zabbixbook.wafproject.cloud - PuTTY

```
root@attacker:~#
```

Gerando Alertas

/var/log/suricata/eve.json


root@some-server: ~
root@some-server:~# tail -1f /var/log/suricata/eve.json | grep 64.225.60.171
Gerando eventos diversos
Arquivo
Editar
Exibir
- Gerando alertas
1. SSH BRUTE FORCE
hydra -l xuxuzinho -P pass.list 165.227.65.66 ssh -I 165.227.65.66
2. FTP BRUTE FORCE
hydra -l badguy -P pass.list 165.227.65.66 ftp -I 165.227.65.66
3. WEB SCRAPING
./nikto-master/program/nikto.pl -h http://165.227.65.66
Ln 21, Col 18
15 de 525 caracteres
120%
Windows (CRLF)
UTF-8
zabbixbook.wafproject.cloud - PuTTY
root@attacker:~#

Detectar

Logs no Suricata

/var/log/suricata/fast.log

O registro em fast.log

ZABBIX '25 CONFERENCE LATIN AMERICA

1. **Timestamp**: 05/26/2025-12:27:40
2. **Rule info**: [1:2038967:1]
3. **Message**: ET INFO SSH-2.0-Go version string Observed in Network Traffic
4. **[Classification**: Misc activity]
5. **[Priority**: 3]
6. **Protocol**: {TCP}
7. **SRC_IP**: 154.48.239.11
8. **SRC_PORT**: 47796
9. **DST_IP**: 165.227.65.66
10. **DST_PORT**: 22

Detecção objetiva de alertas

ZABBIX '25 CONFERENCE LATIN AMERICA

REGULAR EXPRESSION

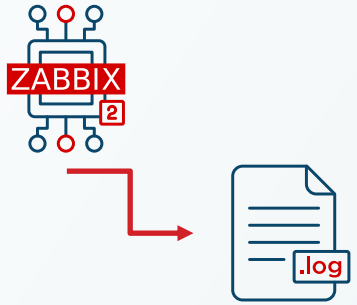
12 matches (68.507 steps, 8.16ms)

```
/ (\d+\/\d+\/\d+-\d+:\d+:\d+)\..*?\[\*\*\]\s\[(\S+)\]\s+(.*).*?\s\[\*\*\]\s\[Classification:\s(.*?)\]\s+\[Priority:\s(\d)\]\s+\{(.*)\}\s+(\d+.\d+.\d+.\d+):(\d+)\s->\s(\d+.\d+.\d+.\d+):(\d+)
/ gm
```

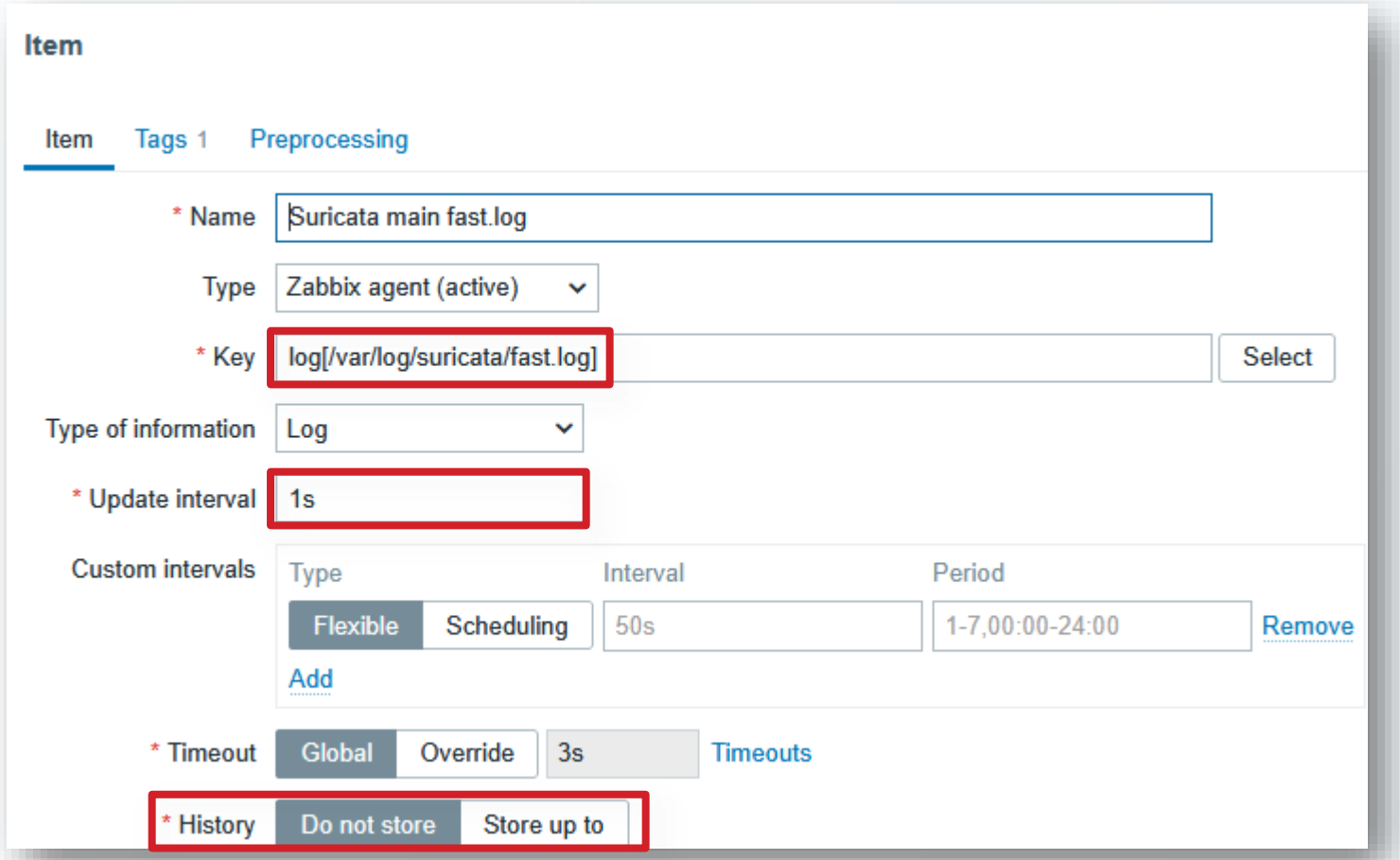
TEST STRING

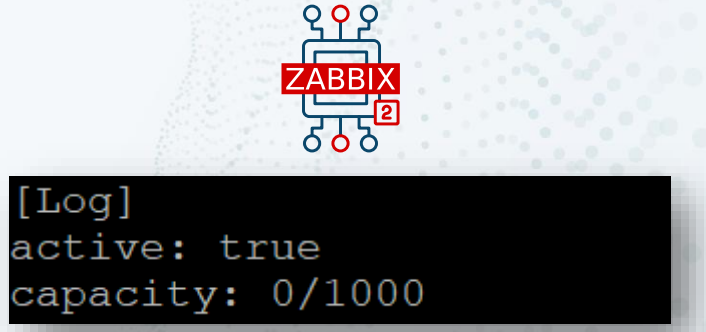
```
05/25/2025-10:40:35.587178  [**] [1:2402000:7274] ET DROP Dshield Block Listed Source group 1 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 64.62.197.125:50683 -> 165.227.65.66:8123
05/25/2025-10:40:35.587178  [**] [1:2402000:7274] ET DROP Dshield Block Listed Source group 1 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 64.62.197.125:50683 -> 165.227.65.66:8123
05/25/2025-10:48:10.616973  [**] [1:2402000:7274] ET DROP Dshield Block Listed Source group 1 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 64.62.197.200:48028 -> 165.227.65.66:9000
05/25/2025-10:48:42.312038  [**] [1:2402000:7274] ET DROP Dshield Block Listed Source group 1 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 35.203.210.89:51000 -> 165.227.65.66:45450
05/25/2025-10:48:42.312038  [**] [1:2403329:98189] ET CINS Active Threat Intelligence Poor Reputation IP group 30 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 35.203.210.89:51000 -> 165.227.65.66:45450
05/25/2025-10:48:52.087605  [**] [1:2403365:98189] ET CINS Active Threat Intelligence Poor Reputation IP group 66 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 47.236.42.190:39239 -> 165.227.65.66:12233
05/25/2025-10:50:02.496161  [**] [1:2402000:7274] ET DROP Dshield Block Listed Source group 1 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 35.203.210.152:56318 -> 165.227.65.66:54445
05/25/2025-10:50:02.496161  [**] [1:2403326:98189] ET CINS Active Threat Intelligence Poor Reputation IP group 27 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 35.203.210.152:56318 -> 165.227.65.66:54445
05/25/2025-10:50:14.048670  [**] [1:2403370:98189] ET CINS Active Threat Intelligence Poor Reputation IP group 71 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 47.251.91.34:53103 -> 165.227.65.66:8237
```

Uma integração Light



Monitorando o fast.log



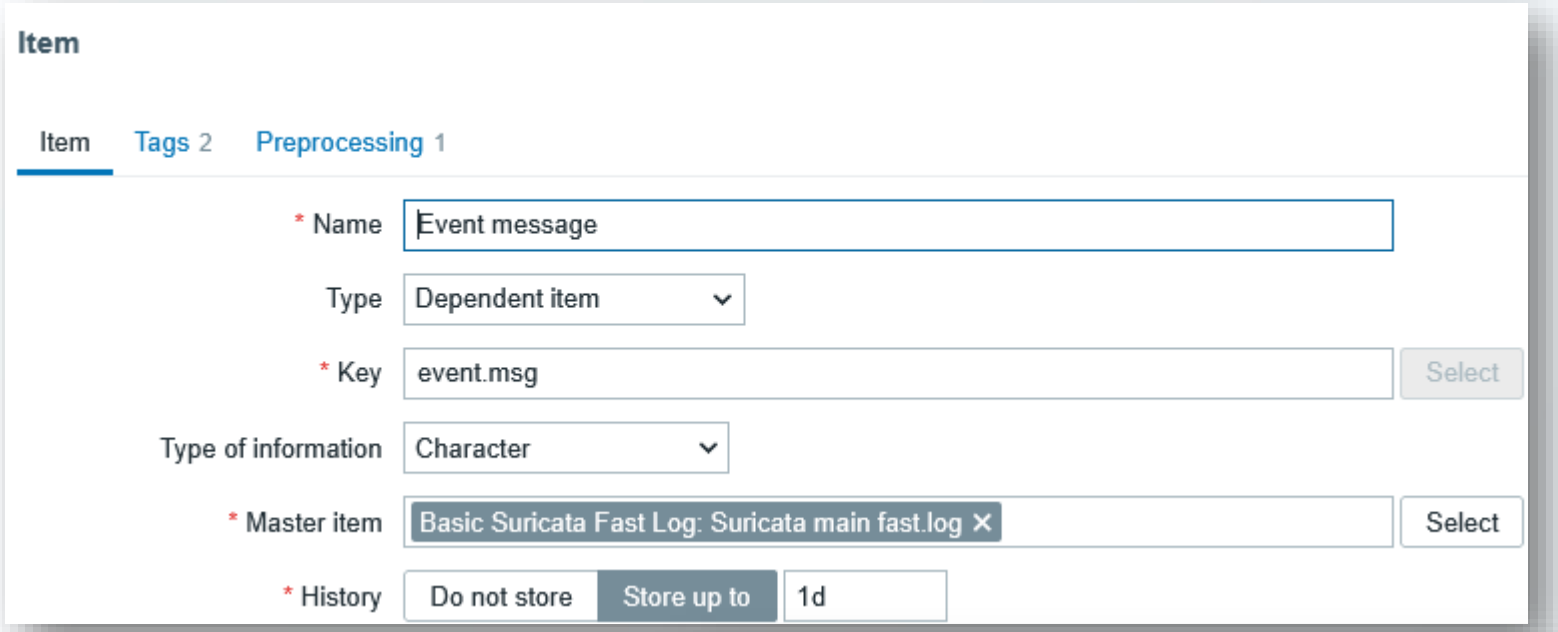


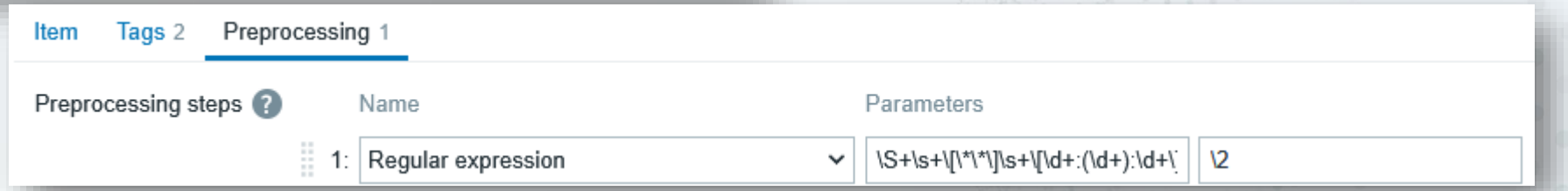
Dependent Items + Preprocessing

ZABBIX '25 CONFERENCE LATIN AMERICA

Name	Triggers	Key	Interval	History
Basic Suricata Fast Log: Suricata main fast.log: Event classification		event.classification		1d
Basic Suricata Fast Log: Suricata main fast.log: Event date		event.date		1d
Basic Suricata Fast Log: Suricata main fast.log: Event destination IP		event.dstip		1d
Basic Suricata Fast Log: Suricata main fast.log: Event dst port		event.dstport		1d
Basic Suricata Fast Log: Suricata main fast.log: Event message		event.msg		1d
Basic Suricata Fast Log: Suricata main fast.log: Event priority		event.priority		1d
Basic Suricata Fast Log: Suricata main fast.log: Event protocol		event.protocol		1d
Basic Suricata Fast Log: Suricata main fast.log: Event rule id		event.rule.id		1d
Basic Suricata Fast Log: Suricata main fast.log: Event source port		event.sourceport		1d
Basic Suricata Fast Log: Suricata main fast.log: Event source IP	Triggers 1	event.srcip		1d
Basic Suricata Fast Log: Suricata main fast.log: Event time		event.time		1d

Extraindo o alerta (exemplo)





05/27/2025-07:18:03.517591 [**] [1:2402000:7274] **ET DROP Dshield Block Listed Source group 1** [**] [Classification: Misc Attack] [Priority: 2] {UDP} 193.163.125.175:23240 -> 165.227.65.66:5060

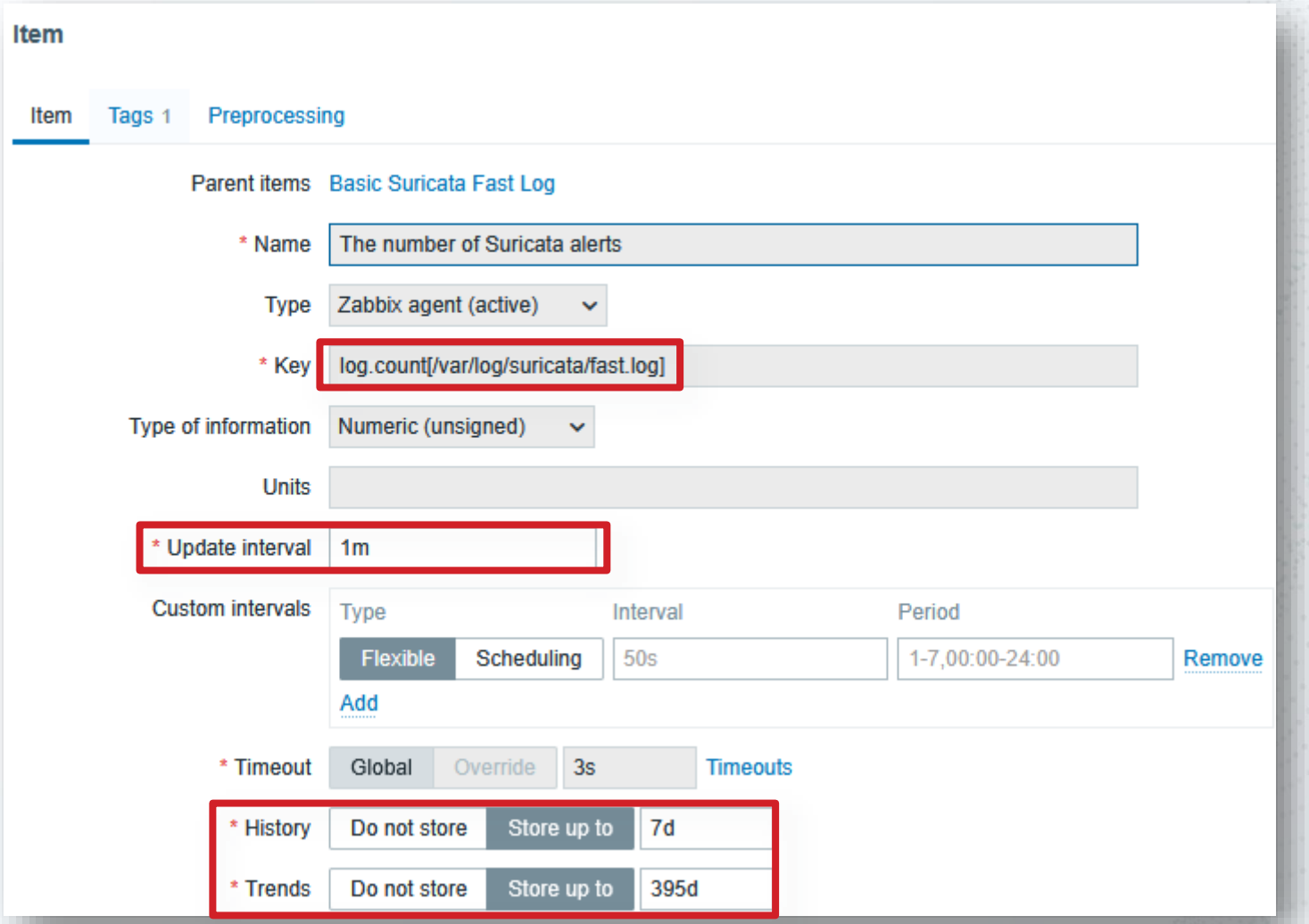
O fast.log e o widget “Item history”

ZABBIX '25 CONFERENCE LATIN AMERICA

Last events

Event date	Event time	Event message	Classification	Priority	SRC IP	SRC port	DST IP	DST port	Protocol
05/25/2025	16:57:40	ET EXPLOIT Fortinet FortiOS/FortiProxy SSL VPN Web Portal Path Traversal (CVE-2018-13379)	Attempted Administrator Privilege Gain	1	64.225.60.171	59832	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET EXPLOIT FortiOS SSL VPN - Information Disclosure (CVE-2018-13379)	Attempted Administrator Privilege Gain	1	64.225.60.171	59832	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET WEB_SERVER Tilde in URI - potential .php~ source disclosure vulnerability	Web Application Attack	1	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET WEB_SERVER Tilde in URI - potential .php~ source disclosure vulnerability	Web Application Attack	1	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET EXPLOIT Cisco RV320/RV325 Config Disclosure Attempt Inbound (CVE-2019-1653)	Attempted Administrator Privilege Gain	1	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET WEB_SERVER /etc/hosts Detected in URI	Attempted Information Leak	2	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET EXPLOIT MVPower DVR Shell UCE	Attempted Administrator Privilege Gain	1	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET WEB_SERVER /etc/hosts Detected in URI	Attempted Information Leak	2	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET EXPLOIT D-Link DSL-2750B Command Injection Attempt (CVE-2016-20017)	Attempted Administrator Privilege Gain	1	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET EXPLOIT D-Link DSL-2750B - OS Command Injection	Attempted User Privilege Gain	1	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET WEB_SERVER /etc/hosts Detected in URI	Attempted Information Leak	2	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET WEB_SERVER /etc/hosts Detected in URI	Attempted Information Leak	2	64.225.60.171	59814	165.227.65.66	80	TCP
05/25/2025	16:57:40	ET WEB_SERVER /etc/hosts Detected in URI	Attempted Information Leak	2	64.225.60.171	59814	165.227.65.66	80	TCP

Contagem dos alertas



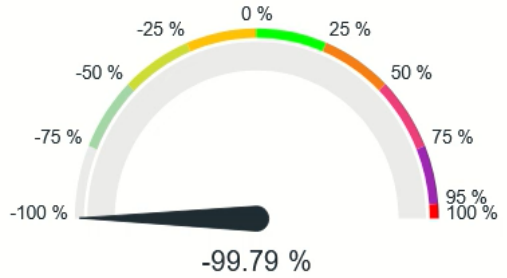
Analisar

17:05:25

ENDPOINT SECURITY MONITORING BY USING SURICATA

THE NUMBER OF ALERTS IN THE LAST HOUR

HOURLY EVENTS % CHANGE



THIS YEAR

256356

THIS MONTH

79257

THIS WEEK

29750 ↑

TODAY SO FAR

9569 ↑

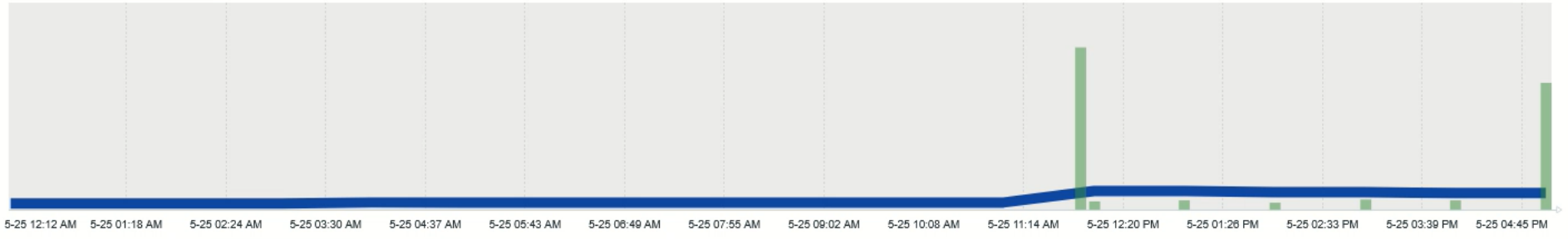
THIS HOUR

0 ↓

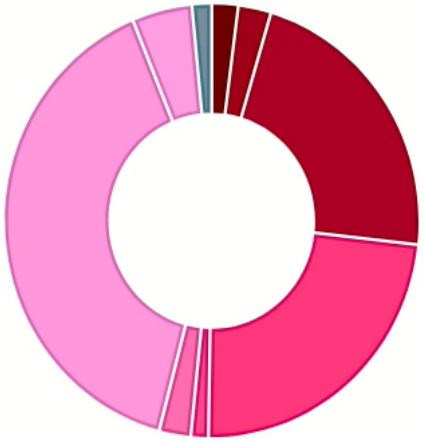
MACHINE LEARNING ANALYSIS

PRIORITY & CATEGORY

EVENTS BASELINE OVER TIME



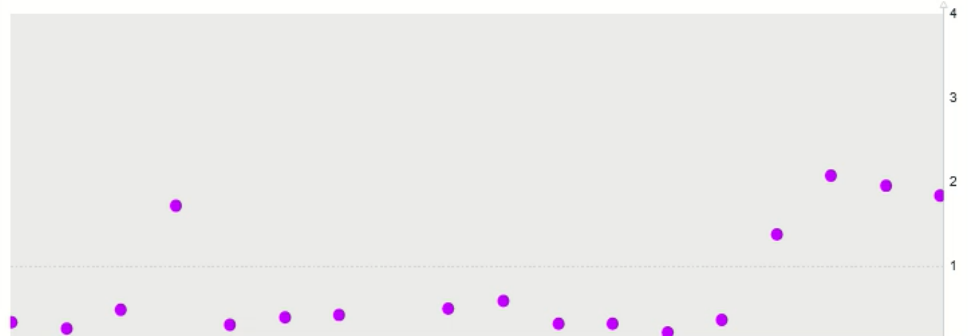
CLASSIFICATION



Value

- ubuntu-client: Counting classification: A Network Trojan was detected 24
- ubuntu-client: Counting classification: Attempted Administrator Privilege Gain 30
- ubuntu-client: Counting classification: Attempted Information Leak 260
- ubuntu-client: Counting classification: Information Leak 276
- ubuntu-client: Counting classification: Misc Attack 16
- ubuntu-client: Counting classification: Potentially Bad Traffic 29
- ubuntu-client: Counting classification: Web Application Attack 466

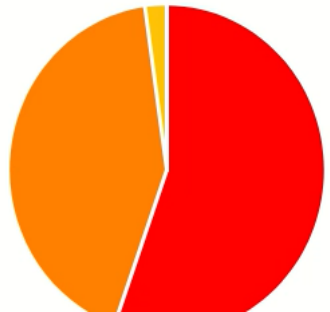
BASELINE DEVIATION MONITORING OVER TIME



ANOMALY RATE

0.79 ↑

EVENTS PRIORITIES

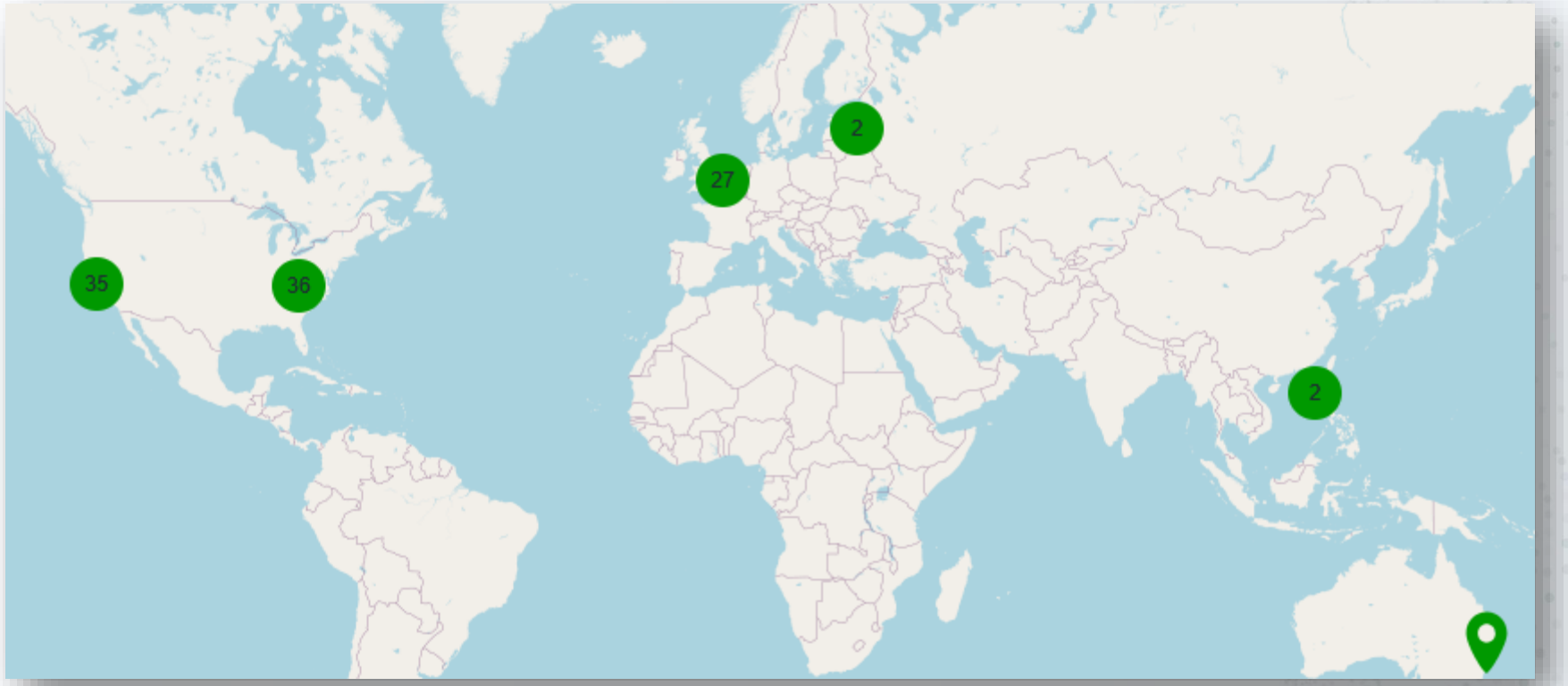


Localizando IPs

De {ITEM.VALUE} para “HOST PROTOTYPE”

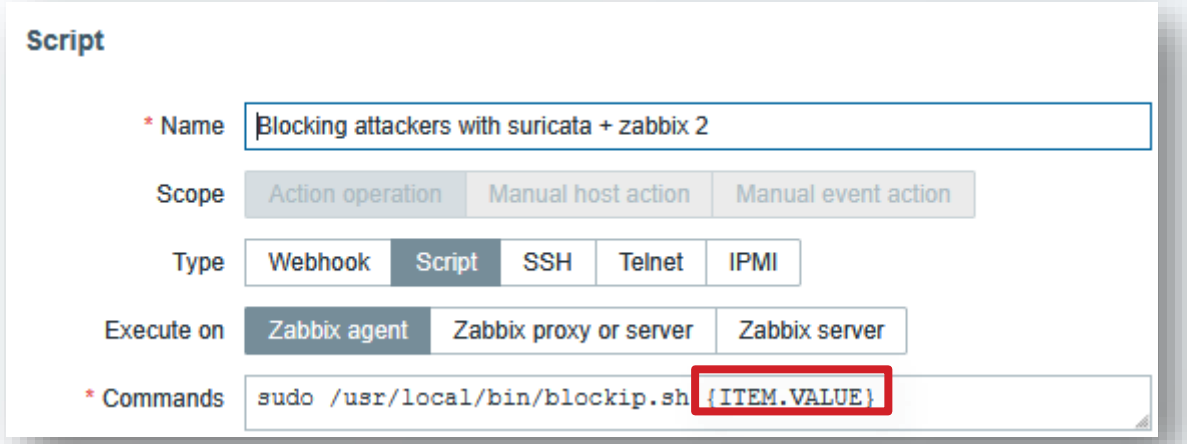
ZABBIX '25 CONFERENCE LATIN AMERICA

Name ▲	Hosts	Info
Hosts from Suricata	121	23.239.4.211, 35.203.210.180, 35.203.211.51, 35.203.211.173, 35.203.211.232, 45.33.94.76, 45.33.105.182, 45.56.83.247, 45.56.111.60, 45.79.82.114, 45.79.104.47, 45.79.109.130, 45.79.153.72, 45.79.186.176, 45.91.171.220, 45.142.193.91, 45.156.129.86, 45.156.129.93, 64.225.60.171, 64.225.62.179, 139.19.117.131, 147.185.132.153, 147.185.132.211, 147.185.132.238, 147.185.133.81, 147.185.133.88, 162.216.149.78, 162.216.149.176, 162.216.150.117, 162.216.150.234, 162.216.150.247, 163.181.49.195, 165.227.65.66, 167.94.138.104, 167.94.138.131, 167.94.138.147, 185.242.226.26, 185.242.226.154, 193.163.125.80, 193.163.125.84, 193.163.125.99, 193.163.125.254, 196.251.114.98, 198.235.24.90, 198.235.24.232, 198.235.24.240, 198.235.24.253, 204.76.203.219, 205.210.31.103, 206.168.34.152 ...



Responder

active-response com Zabbix



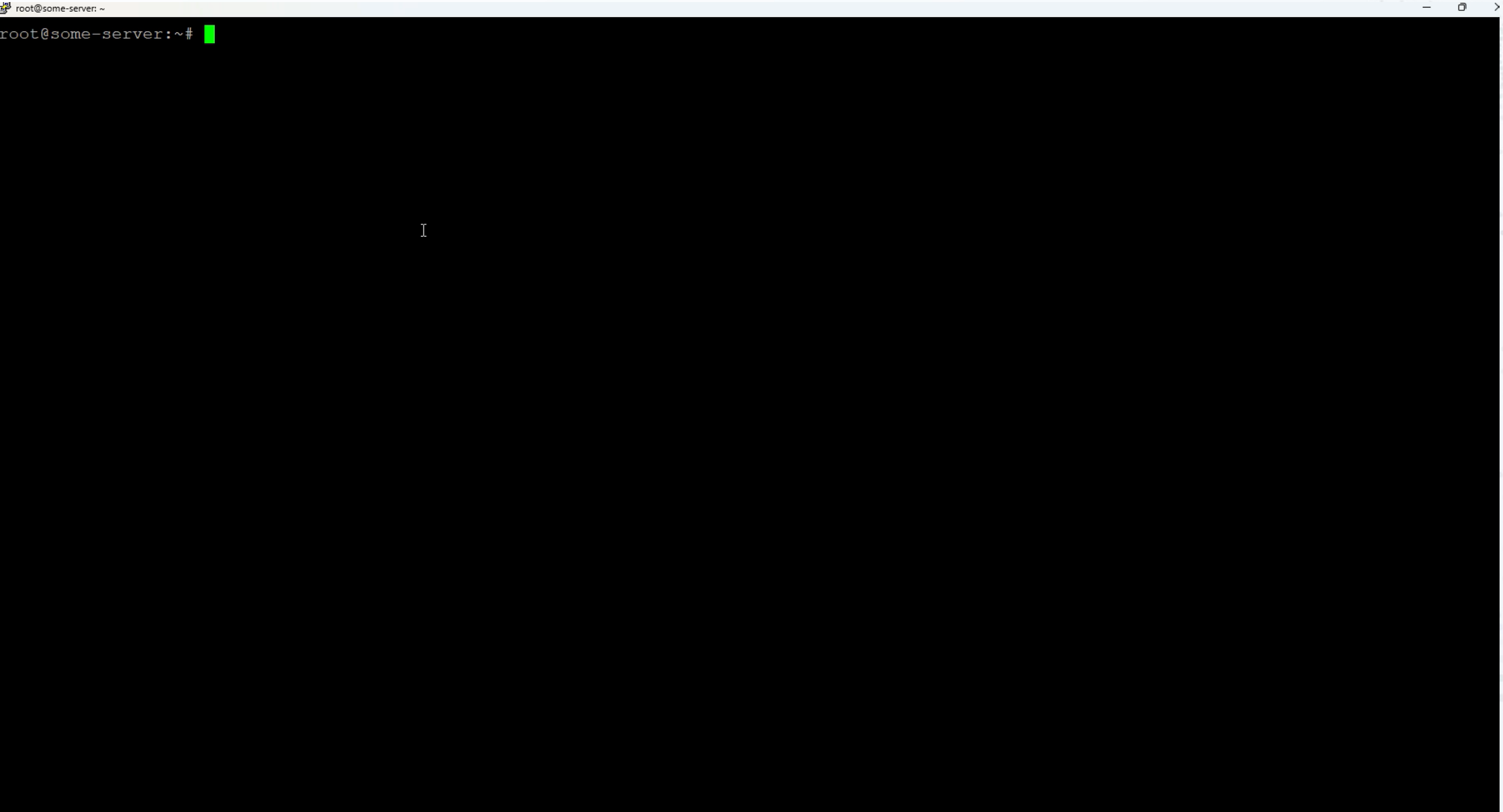

```
#!/bin/bash

IP="$1"

# Verifica se o IP já está na regra
iptables -C INPUT -s "$IP" -m recent --name BLOQUEADOS --rcheck -j DROP 2>/dev/null

# Se não estiver, adiciona
if [ $? -ne 0 ]; then
    iptables -A INPUT -s "$IP" -m recent --name BLOQUEADOS --set -j DROP
fi
```

Report / Action logs

ZABBIX '25 CONFERENCE LATIN AMERICA

Time	Action	Media type	Recipient	Message	Status	Info
2025-05-27 07:27:25 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 47.74.46.203	Executed	
2025-05-27 07:27:15 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 193.163.125.131	Executed	
2025-05-27 07:25:40 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 167.94.138.134	Executed	
2025-05-27 07:24:45 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 196.221.164.156	Executed	
2025-05-27 07:23:40 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 206.168.34.166	Executed	
2025-05-27 07:23:15 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 148.113.214.204	Executed	
2025-05-27 07:23:05 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 185.100.87.136	Executed	
2025-05-27 07:23:05 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 185.100.87.136	Executed	
2025-05-27 07:20:00 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 193.163.125.175	Executed	
2025-05-27 07:18:40 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 147.185.133.149	Executed	
2025-05-27 07:18:20 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 167.94.138.111	Executed	
2025-05-27 07:16:50 AM	Blocking attackers with zabbix and suricata			**Command:** ubuntu-client:sudo /usr/local/bin/blockip.sh 193.163.125.142	Executed	

Conferindo os bloqueios

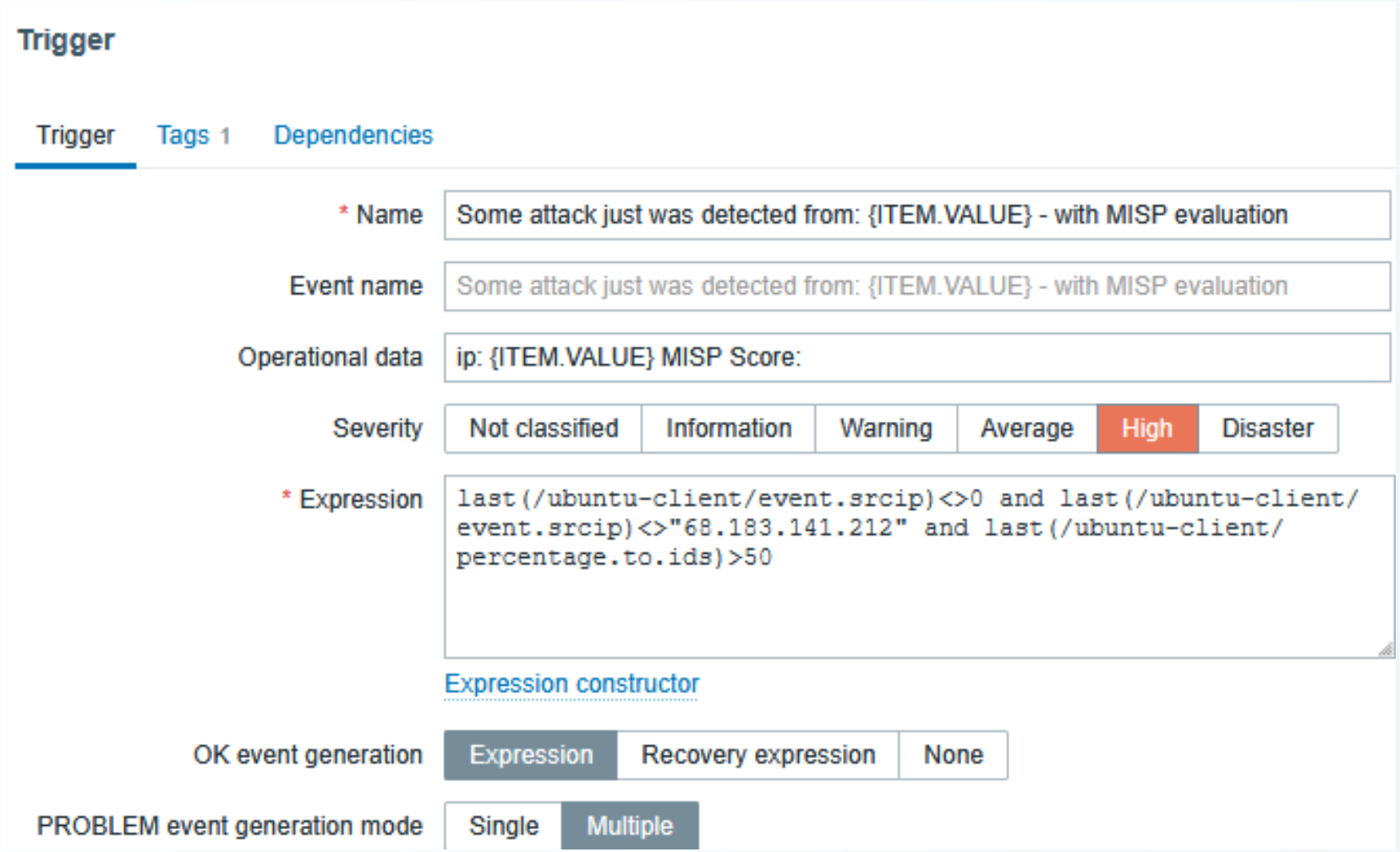


Threat Intelligence MISP

O que é o MISP?

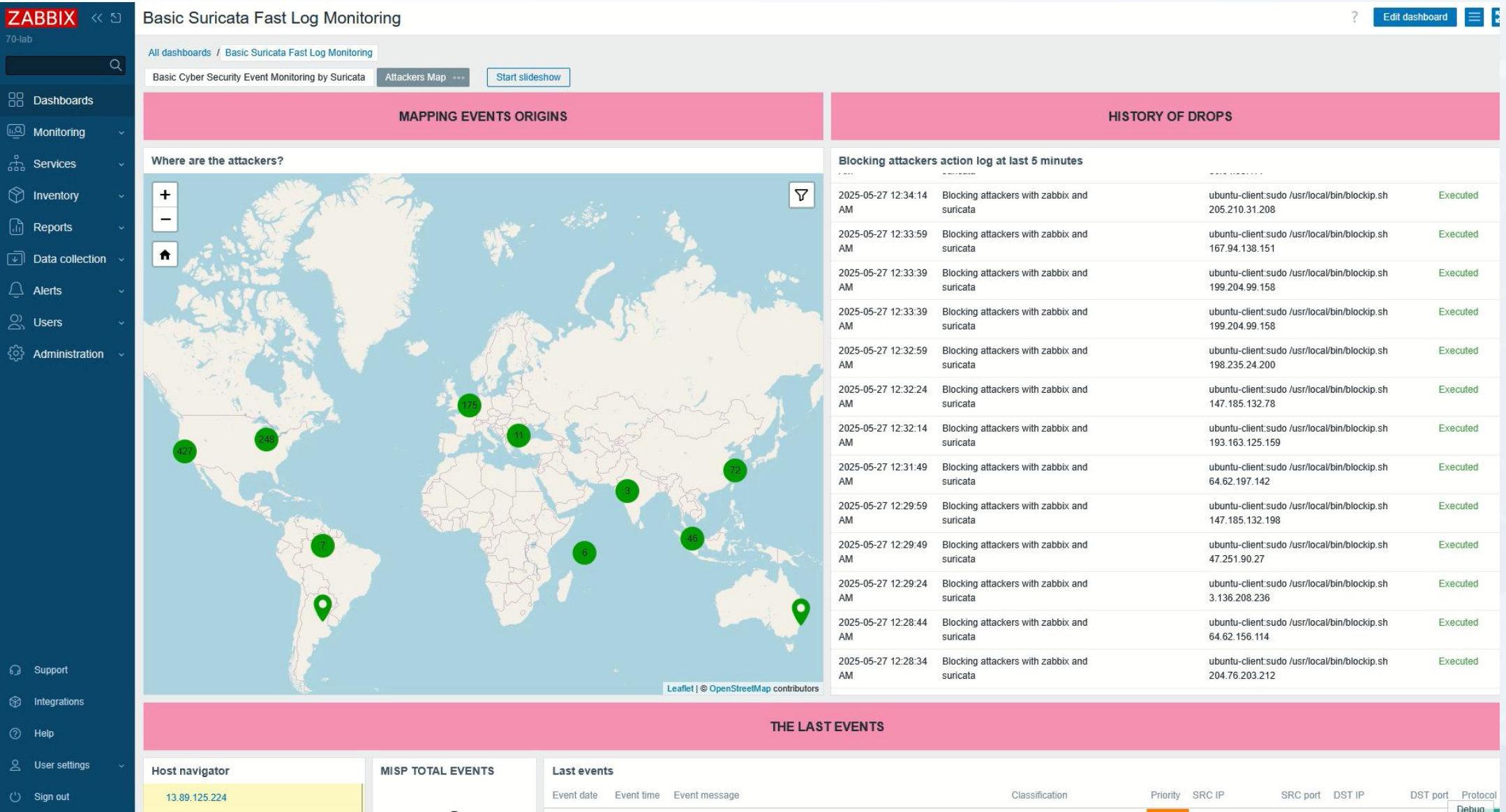
O MISP (Malware Information Sharing Platform & Threat Sharing) é uma plataforma open-source de Threat Intelligence projetada para facilitar a coleta, compartilhamento, armazenamento e correlação de indicadores de comprometimento (IOCs) e outros dados relacionados a ameaças cibernéticas.

Bloqueio considerando o MISP Score



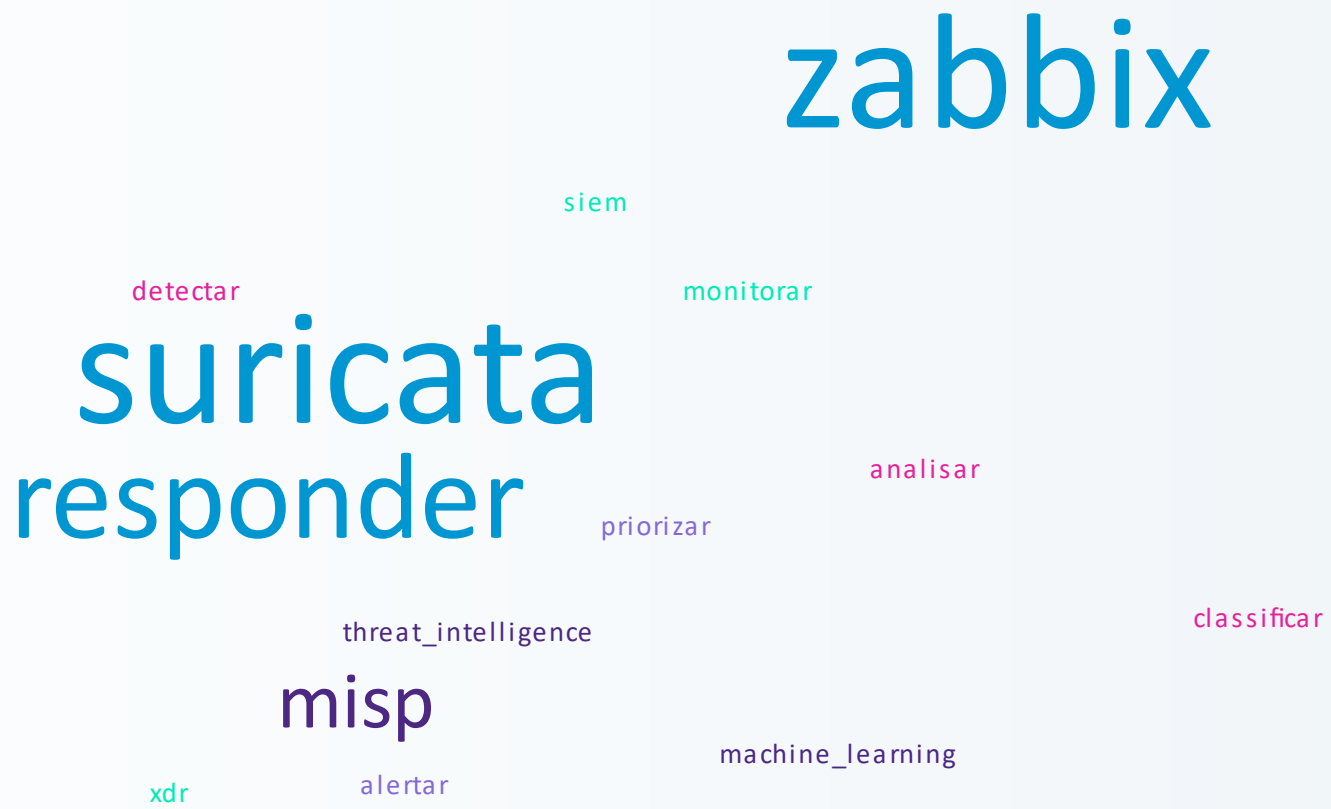
Zabbix + Threat Intelligence

ZABBIX '25 CONFERENCE LATIN AMERICA



Conclusão

A Stack open source utilizada



Benefícios da integração

ZABBIX '25 CONFERENCE LATIN AMERICA

1. Centralização e Visibilidade Unificada: O Zabbix atua como camada de gestão e interface única para dados de IDS (Suricata), inteligência de ameaças (MISP) e decisões automatizadas.

2. Automação de Respostas a Incidentes: Ação proativa com bloqueio de IPs maliciosos diretamente via triggers baseadas em análise de confiabilidade e score de ameaça.

3. Adoção de Machine Learning no Zabbix: Aplicação de padrões comportamentais e aprendizado contínuo a partir de eventos de segurança, tornando o sistema adaptável e dinâmico.

Benefícios da integração

ZABBIX '25 CONFERENCE LATIN AMERICA

4. Enriquecimento de Dados com Threat Intelligence: Cruzamento em tempo real dos IPs detectados com reputações no MISP aumenta a assertividade na tomada de decisão.

5. Medição de Confiabilidade com Cálculo Personalizado: A criação de itens calculados com base em eventos e indicadores fornece uma métrica objetiva de ação (ex: score ≥ 80%).

6. Aderência a Políticas de Zero Trust: A arquitetura favorece ações baseadas em evidência e confiança derivada, o que é fundamental para ambientes de segurança moderna.
7. Infraestrutura Open Source e Modular: Solução escalável, livre de custos de licenciamento e com possibilidade de adoção gradual em ambientes existentes.

Desafios da integração

ZABBIX '25 CONFERENCE LATIN AMERICA

1. Zabbix não é uma plataforma SIEM: A leitura dos logs requer expertise em Zabbix e a construção das triggers, noções coerentes de segurança cibernética.

2. Implementação da Resposta Automatizada (XDR-like): O uso do Zabbix como plataforma de resposta requer cuidado para evitar ações precipitadas ou indevidas.

3. Atualização contínua da plataforma de Threat Intelligence (MISP): Os feeds devem ser confiáveis, bem mantidos e atualizados para garantir decisões baseadas em dados atuais.

Desafios da integração

ZABBIX '25 CONFERENCE LATIN AMERICA

4. Qualidade das Regras do Suricata: O Suricata é a base de detecção, e sua eficiência depende diretamente da qualidade, cobertura e manutenção das regras.

5. Confiança no score de confiabilidade gerado pelo MISP: O modelo de score precisa ser validado e monitorado constantemente para garantir decisões seguras. Falhas no modelo ou dependência excessiva de poucos indicadores podem comprometer a efetividade da resposta.

6. ML no Zabbix não reflete os acontecimentos em tempo real: O modelo de aprendizado é baseado em trends e reflete no máximo a hora anterior. A baseline e a Taxa de Anomalia podem ser mal interpretados pelo analista de segurança.

Convite

ZABBIX '25
CONFERENCE
LATIN AMERICA

ZABBIX '25
CONFERENCE
LATIN AMERICA

Obrigado!

Paulo Deolindo

Zabbix Trainer