WHYSECURITY
CYBER SECURITY

Zabbix for CyberSecurity

Different approaches to manage Cyber challenges

https://www.whysecurity.it

Who’s speaking?

Gabriele Minniti

CyberSecurity Expert

WhySecurity CEO

Vincenzo Morrone

Software Engineer

Penetration Tester

Introduction

Zabbix is one of the crucial systems we use to deliver our **SOC** and **SNOC** services
In recent years, it has been necessary to developer integrations with third parties cybersecurity software
in order to have single pane of glass about “What’s going on”

We have worked on different methods in order to achieve our integration requirements.

Who are we?

We specialize in cybersecurity and much more; we develop applications and integrations.
Since 10 years already.

Different approach for different challanges

- Broker approach:
  - Use external application to manage the orchestration of operations

- Serverless approach:
  - No external application required

We'll talk about:

SHODAN

Veeam

Sophos

Nozomi

vtiger

Objectives

1) Global visibility — View **everything in one place**

2) Realtime monitoring — **Accurate data** and no time waste

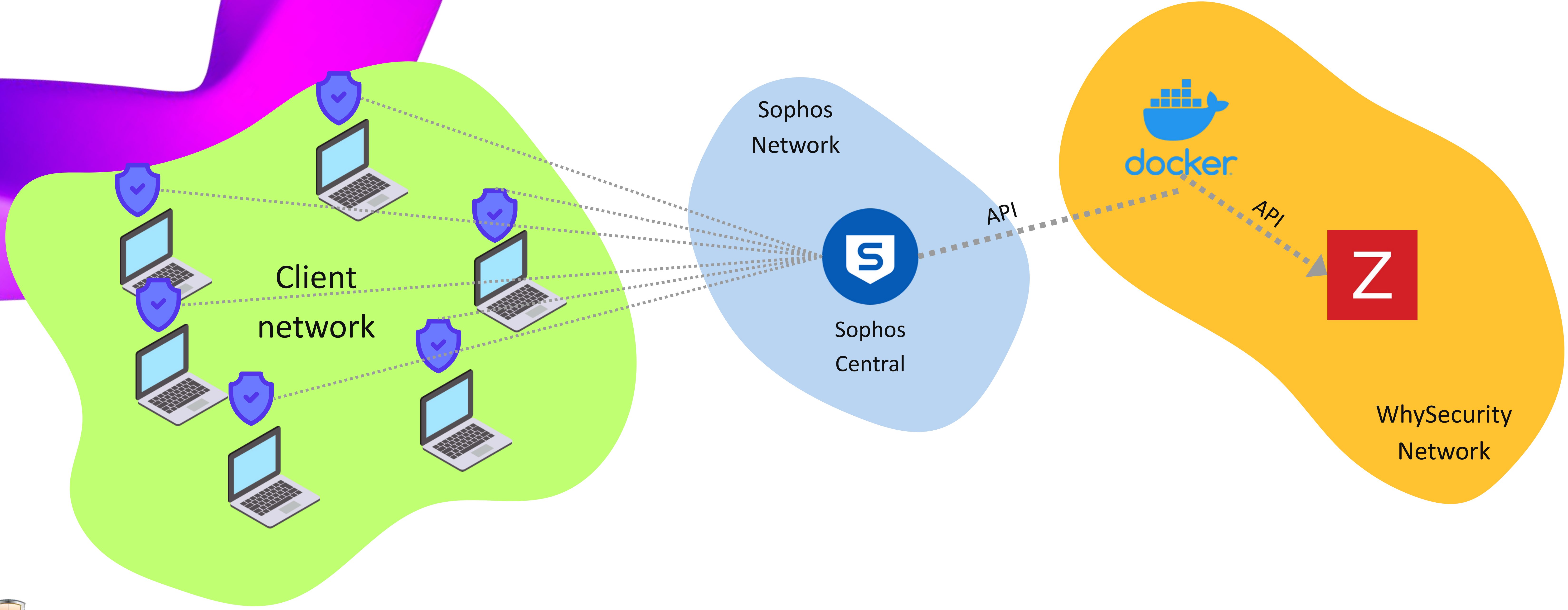
3) Instant notification — **Alert the team** quickly in any way possible

4) Rapid response — **No long process**

Event Detection by the Sophos Endpoints Security Agents

Using Sophos **APIs & Zabbix API.**

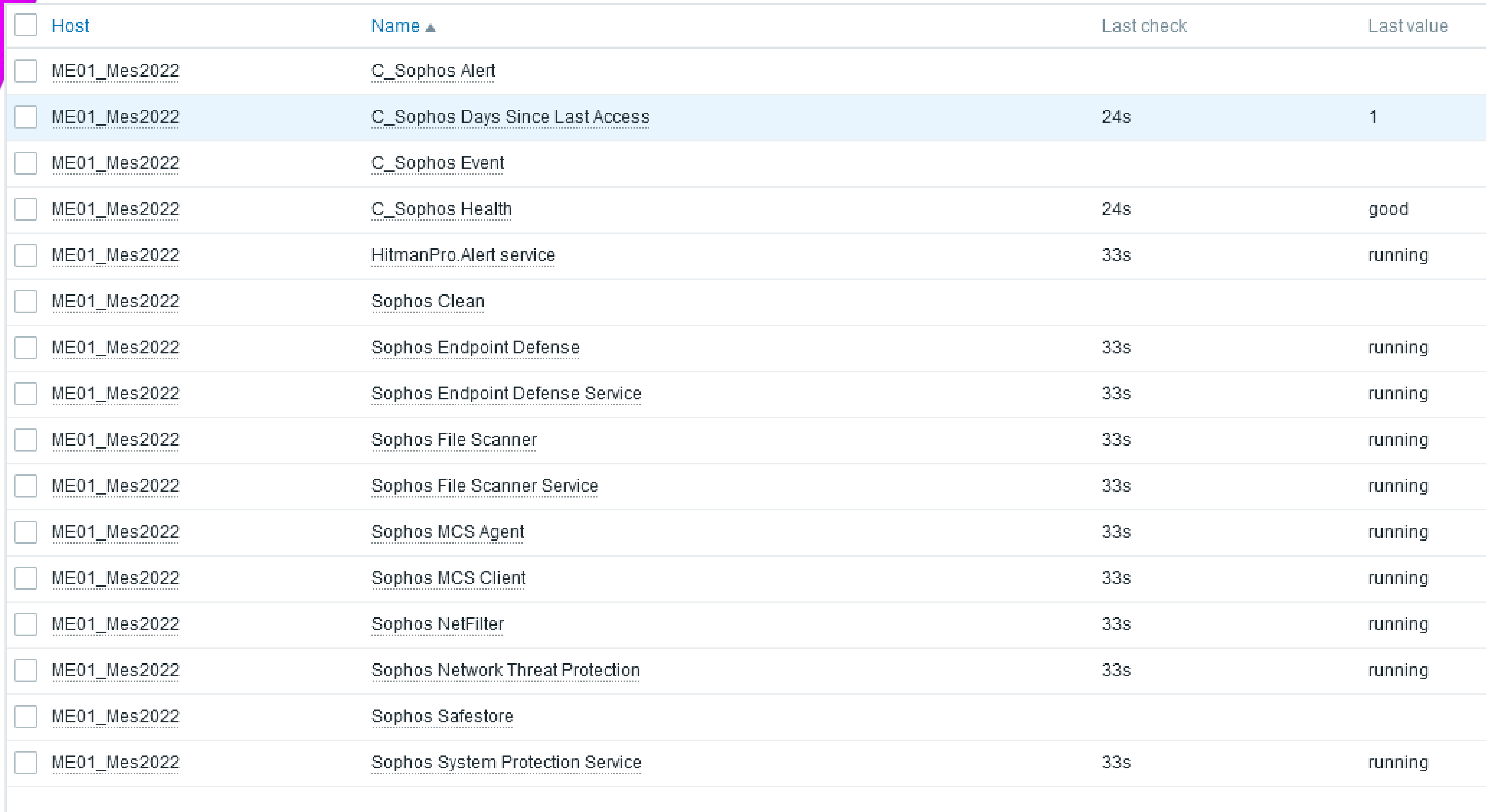
Application Flow



Event Detection by the Sophos Endpoints Security Agents

Using Sophos **APIs & Zabbix API.**

What we see on Zabbix



□	Host	Name ▲	Last check	Last value
□	ME01_Mes2022	C_Sophos Alert		
□	ME01_Mes2022	C_Sophos Days Since Last Access	24s	1
□	ME01_Mes2022	C_Sophos Event		
□	ME01_Mes2022	C_Sophos Health	24s	good
□	ME01_Mes2022	HitmanPro.Alert service	33s	running
□	ME01_Mes2022	Sophos Clean		
□	ME01_Mes2022	Sophos Endpoint Defense	33s	running
□	ME01_Mes2022	Sophos Endpoint Defense Service	33s	running
□	ME01_Mes2022	Sophos File Scanner	33s	running
□	ME01_Mes2022	Sophos File Scanner Service	33s	running
□	ME01_Mes2022	Sophos MCS Agent	33s	running
□	ME01_Mes2022	Sophos MCS Client	33s	running
□	ME01_Mes2022	Sophos NetFilter	33s	running
□	ME01_Mes2022	Sophos Network Threat Protection	33s	running
□	ME01_Mes2022	Sophos Safestore		
□	ME01_Mes2022	Sophos System Protection Service	33s	running

Event Detection by the Sophos Endpoints Security Agents

Using Sophos **APIs & Zabbix API.**

Thanks to the use of Zabbix APIs, we have automated the creation of:

- Hosts
- Items
- Triggers

We created a fully automatic and autonomous process for registering hosts from Sophos to Zabbix.

- **4000+** Hosts created using API.
- **0h** Time wasted by Humans.

Pros:

- Numerous methods provided by the Zabbix APIs.

Cons:

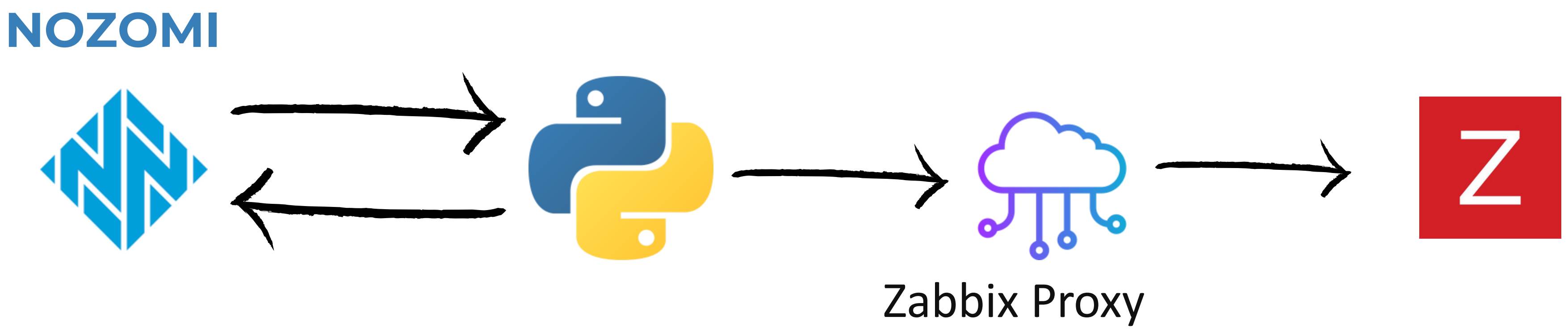
- It is necessary to create an external application for orchestrating the HTTP Calls.

SOC OT Vulnerabilities Detection

Using **Zabbix Trapper** and NOZOMI

Nozomi is a cybersecurity platform that provides solutions for monitoring and securing industrial control systems (ICS) and operational technology (OT) environments

Nozomi's technology uses network monitoring and artificial intelligence to gain visibility into complex industrial networks, identify vulnerabilities, and offer actionable insights to prevent potential security incidents.

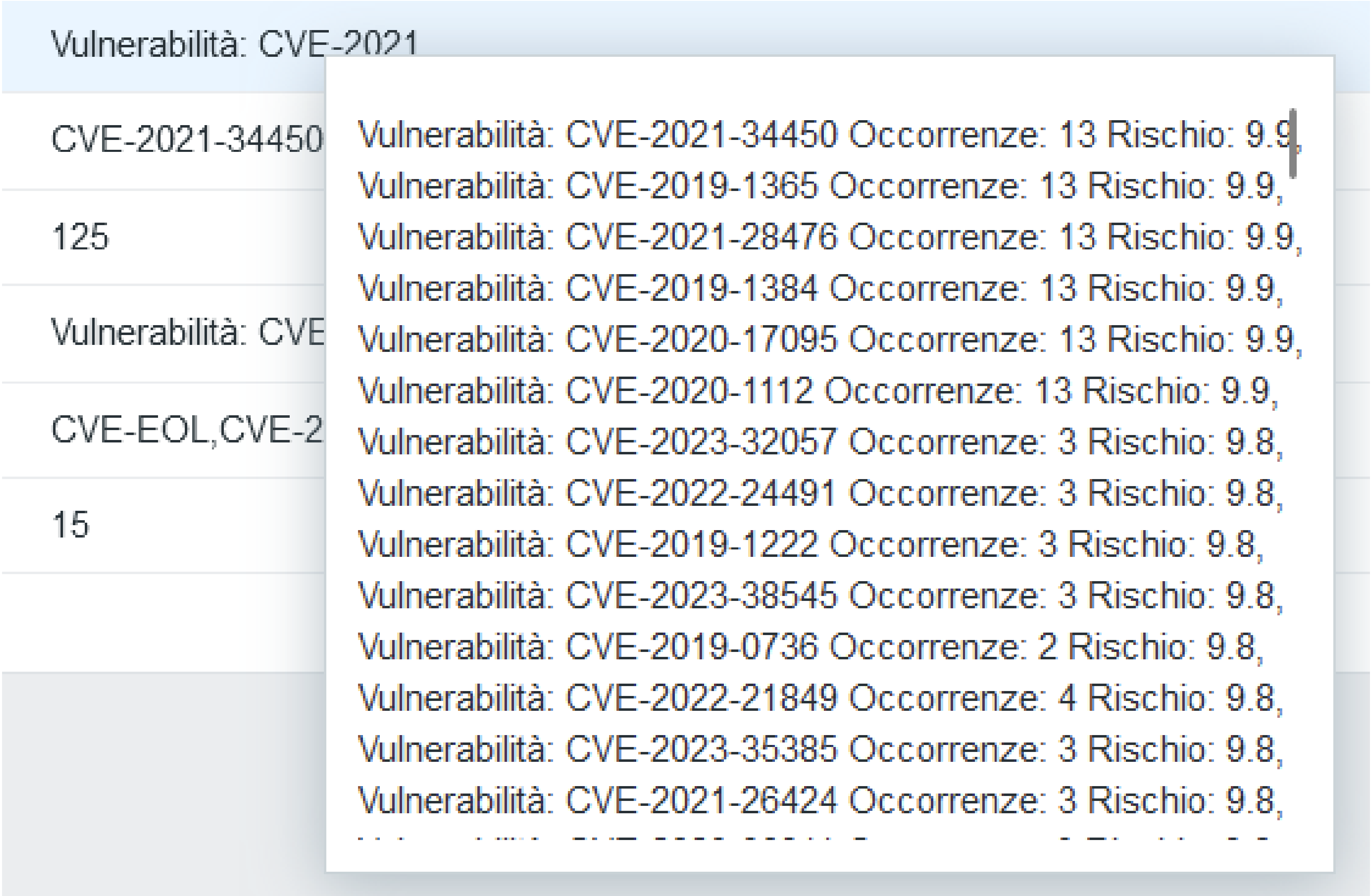


WHYSECURITY
CYBER SECURITY

SOC OT Vulnerabilities Detection

Using **Zabbix Trapper** and NOZOMI

We used a Master item to collect the raw data and dependent item with **Javascript preprocessing.**



```
Vulnerabilità: CVE-2021
CVE-2021-34450
125
Vulnerabilità: CVE
CVE-EOL,CVE-2
15
```

```
Vulnerabilità: CVE-2021-34450 Occorrenze: 13 Rischio: 9.9,
Vulnerabilità: CVE-2019-1365 Occorrenze: 13 Rischio: 9.9,
Vulnerabilità: CVE-2021-28476 Occorrenze: 13 Rischio: 9.9,
Vulnerabilità: CVE-2019-1384 Occorrenze: 13 Rischio: 9.9,
Vulnerabilità: CVE-2020-17095 Occorrenze: 13 Rischio: 9.9,
Vulnerabilità: CVE-2020-1112 Occorrenze: 13 Rischio: 9.9,
Vulnerabilità: CVE-2023-32057 Occorrenze: 3 Rischio: 9.8,
Vulnerabilità: CVE-2022-24491 Occorrenze: 3 Rischio: 9.8,
Vulnerabilità: CVE-2019-1222 Occorrenze: 3 Rischio: 9.8,
Vulnerabilità: CVE-2023-38545 Occorrenze: 3 Rischio: 9.8,
Vulnerabilità: CVE-2019-0736 Occorrenze: 2 Rischio: 9.8,
Vulnerabilità: CVE-2022-21849 Occorrenze: 4 Rischio: 9.8,
Vulnerabilità: CVE-2023-35385 Occorrenze: 3 Rischio: 9.8,
Vulnerabilità: CVE-2021-26424 Occorrenze: 3 Rischio: 9.8,
```

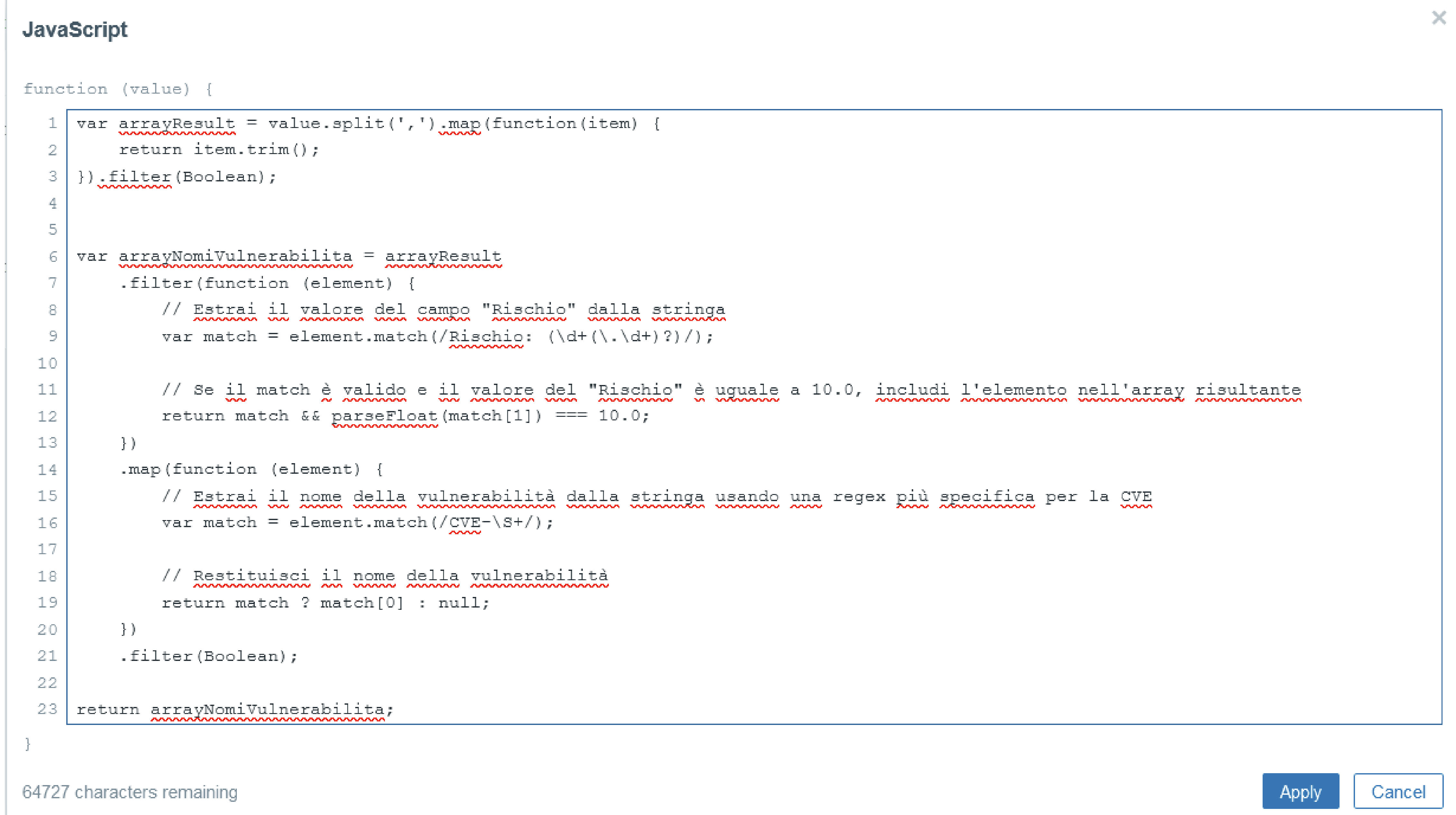
Master Item - Trapper

WHYSECURITY
CYBER SECURITY

SOC OT Vulnerabilities Detection

Using **Zabbix Trapper** and NOZOMI

Using Javascript we filter the vulnerabilities based on the score.



JavaScript

```
function (value) {
var arrayResult = value.split(',').map(function(item) {
    return item.trim();
}).filter(Boolean);


var arrayNomiVulnerabilita = arrayResult
    .filter(function (element) {
        // Estrai il valore del campo "Rischio" dalla stringa
        var match = element.match(/Rischio: (\d+(\.\d+)?)/);

        // Se il match è valido e il valore del "Rischio" è uguale a 10.0, includi l'elemento nell'array risultante
        return match && parseFloat(match[1]) === 10.0;
    })
    .map(function (element) {
        // Estrai il nome della vulnerabilità dalla stringa usando una regex più specifica per la CVE
        var match = element.match(/CVE-\S+/);

        // Restituisci il nome della vulnerabilità
        return match ? match[0] : null;
    })
    .filter(Boolean);

return arrayNomiVulnerabilita;
}
```

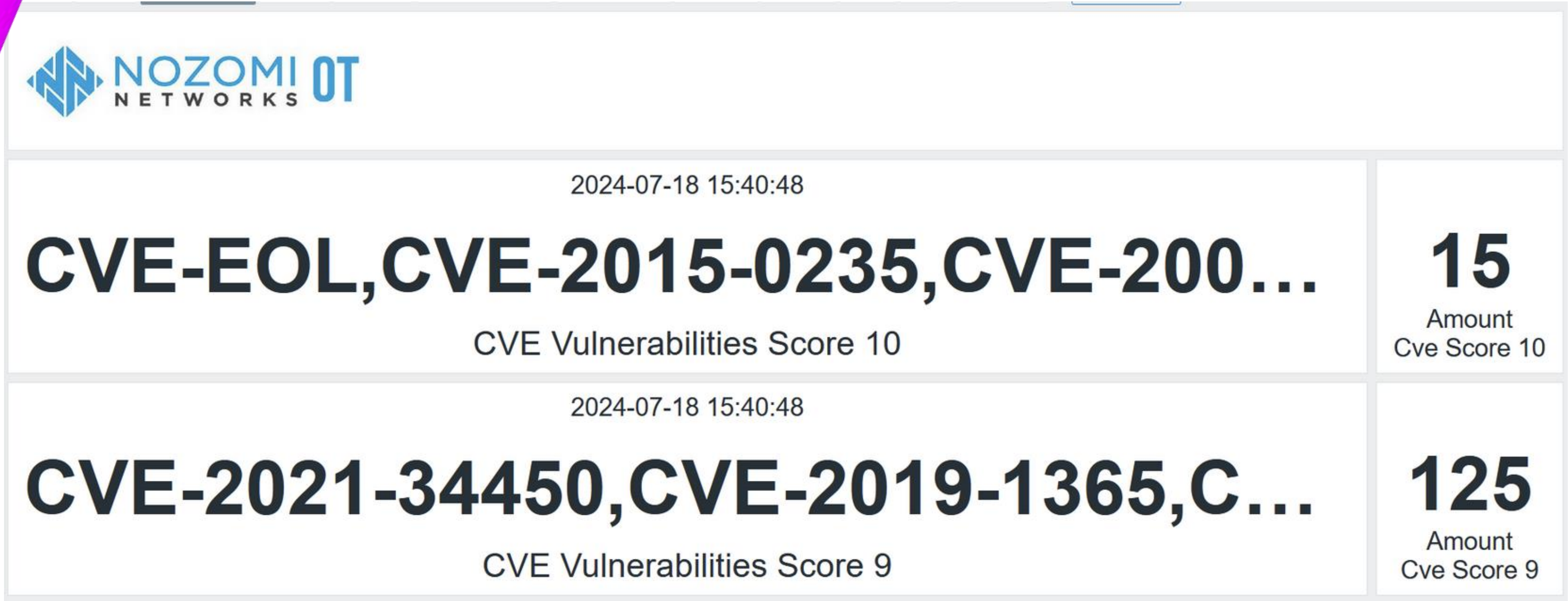
64727 characters remaining

Dependent Item - Trapper

SOC OT Vulnerabilities Detection

Using **Zabbix Trapper** and NOZOMI

The final result is this.



2024-07-18 15:40:48

CVE-EOL,CVE-2015-0235,CVE-200...

CVE Vulnerabilities Score 10

15

Amount Cve Score 10

2024-07-18 15:40:48

CVE-2021-34450,CVE-2019-1365,C...

CVE Vulnerabilities Score 9

125

Amount Cve Score 9

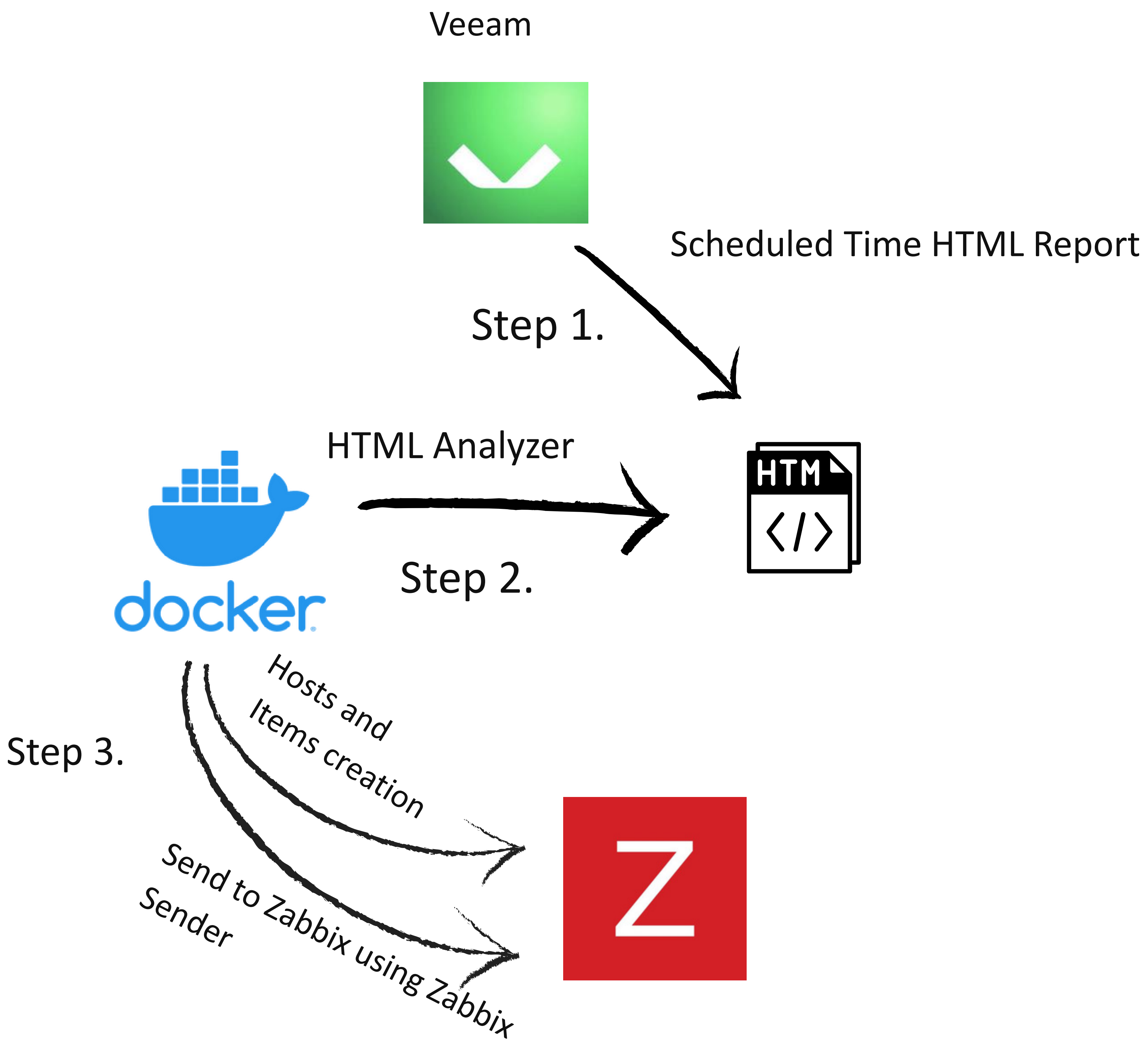
Cyber Resilience: Backup with Veeam

Using **HTML Report** and **Zabbix Trapper**.

We needed to integrate **Veeam Backup** statistics in **Zabbix** using Powershell, Zabbix API and Python.

Cyber Resilience: Backup with Veeam

Using **HTML Report** and **Zabbix Trapper**.



Veeam

Scheduled Time HTML Report

Step 1.

HTML Analyzer

Step 2.

Step 3.

Hosts and Items creation

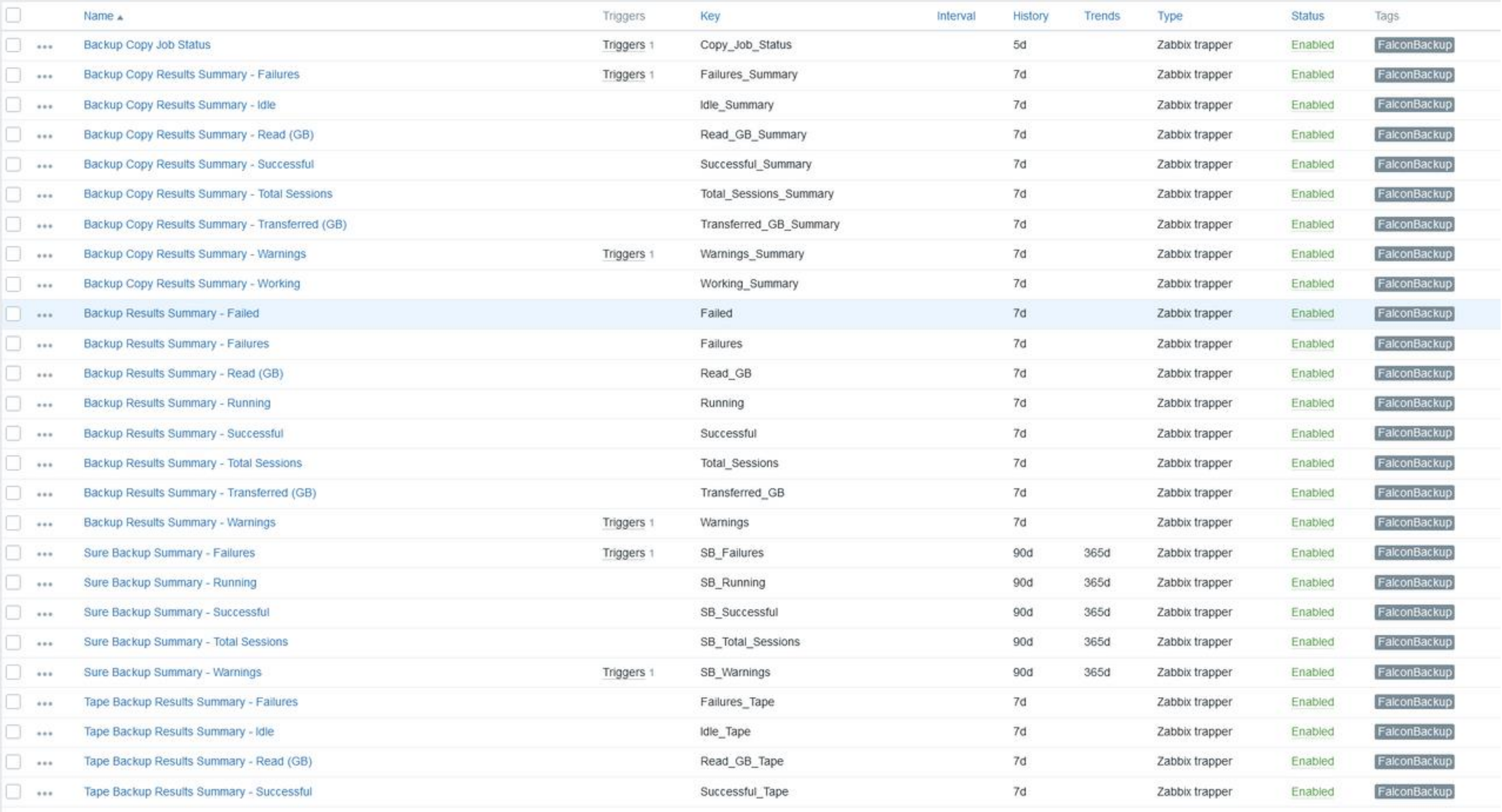
Send to Zabbix using Zabbix Sender

WHYSECURITY
CYBER SECURITY

Cyber Resilience: Backup with Veeam

Using **HTML Report** and **Zabbix Trapper**.

We extract 35 properties with relevant VM information from each HTML report.



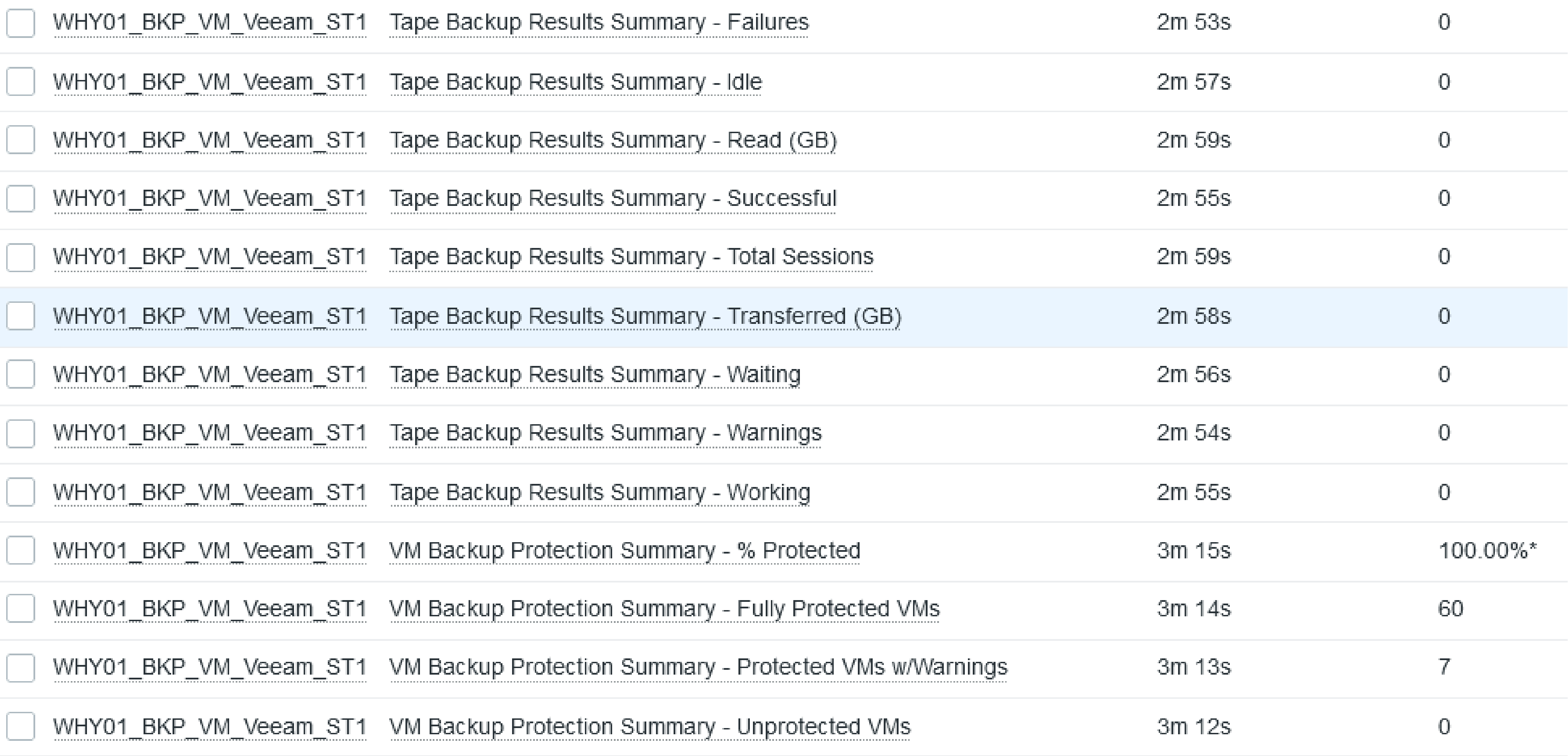
□		Name ▲	Triggers	Key	Interval	History	Trends	Type	Status	Tags
□	•••	Backup Copy Job Status	Triggers 1	Copy_Job_Status		5d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Failures	Triggers 1	Failures_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Idle		Idle_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Read (GB)		Read_GB_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Successful		Successful_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Total Sessions		Total_Sessions_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Transferred (GB)		Transferred_GB_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Warnings	Triggers 1	Warnings_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Copy Results Summary - Working		Working_Summary		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Failed		Failed		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Failures		Failures		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Read (GB)		Read_GB		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Running		Running		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Successful		Successful		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Total Sessions		Total_Sessions		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Transferred (GB)		Transferred_GB		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Backup Results Summary - Warnings	Triggers 1	Warnings		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Sure Backup Summary - Failures	Triggers 1	SB_Failures		90d	365d	Zabbix trapper	Enabled	FalconBackup
□	•••	Sure Backup Summary - Running		SB_Running		90d	365d	Zabbix trapper	Enabled	FalconBackup
□	•••	Sure Backup Summary - Successful		SB_Successful		90d	365d	Zabbix trapper	Enabled	FalconBackup
□	•••	Sure Backup Summary - Total Sessions		SB_Total_Sessions		90d	365d	Zabbix trapper	Enabled	FalconBackup
□	•••	Sure Backup Summary - Warnings	Triggers 1	SB_Warnings		90d	365d	Zabbix trapper	Enabled	FalconBackup
□	•••	Tape Backup Results Summary - Failures		Failures_Tape		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Tape Backup Results Summary - Idle		Idle_Tape		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Tape Backup Results Summary - Read (GB)		Read_GB_Tape		7d		Zabbix trapper	Enabled	FalconBackup
□	•••	Tape Backup Results Summary - Successful		Successful_Tape		7d		Zabbix trapper	Enabled	FalconBackup

Template items

Cyber Resilience: Backup with Veeam

Using **HTML Report** and **Zabbix Trapper**.

We extract 35 properties with relevant VM information from each HTML report.



☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Failures	2m 53s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Idle	2m 57s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Read (GB)	2m 59s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Successful	2m 55s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Total Sessions	2m 59s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Transferred (GB)	2m 58s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Waiting	2m 56s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Warnings	2m 54s	0
☐	WHY01_BKP_VM_Veeam_ST1	Tape Backup Results Summary - Working	2m 55s	0
☐	WHY01_BKP_VM_Veeam_ST1	VM Backup Protection Summary - % Protected	3m 15s	100.00%*
☐	WHY01_BKP_VM_Veeam_ST1	VM Backup Protection Summary - Fully Protected VMs	3m 14s	60
☐	WHY01_BKP_VM_Veeam_ST1	VM Backup Protection Summary - Protected VMs w/Warnings	3m 13s	7
☐	WHY01_BKP_VM_Veeam_ST1	VM Backup Protection Summary - Unprotected VMs	3m 12s	0

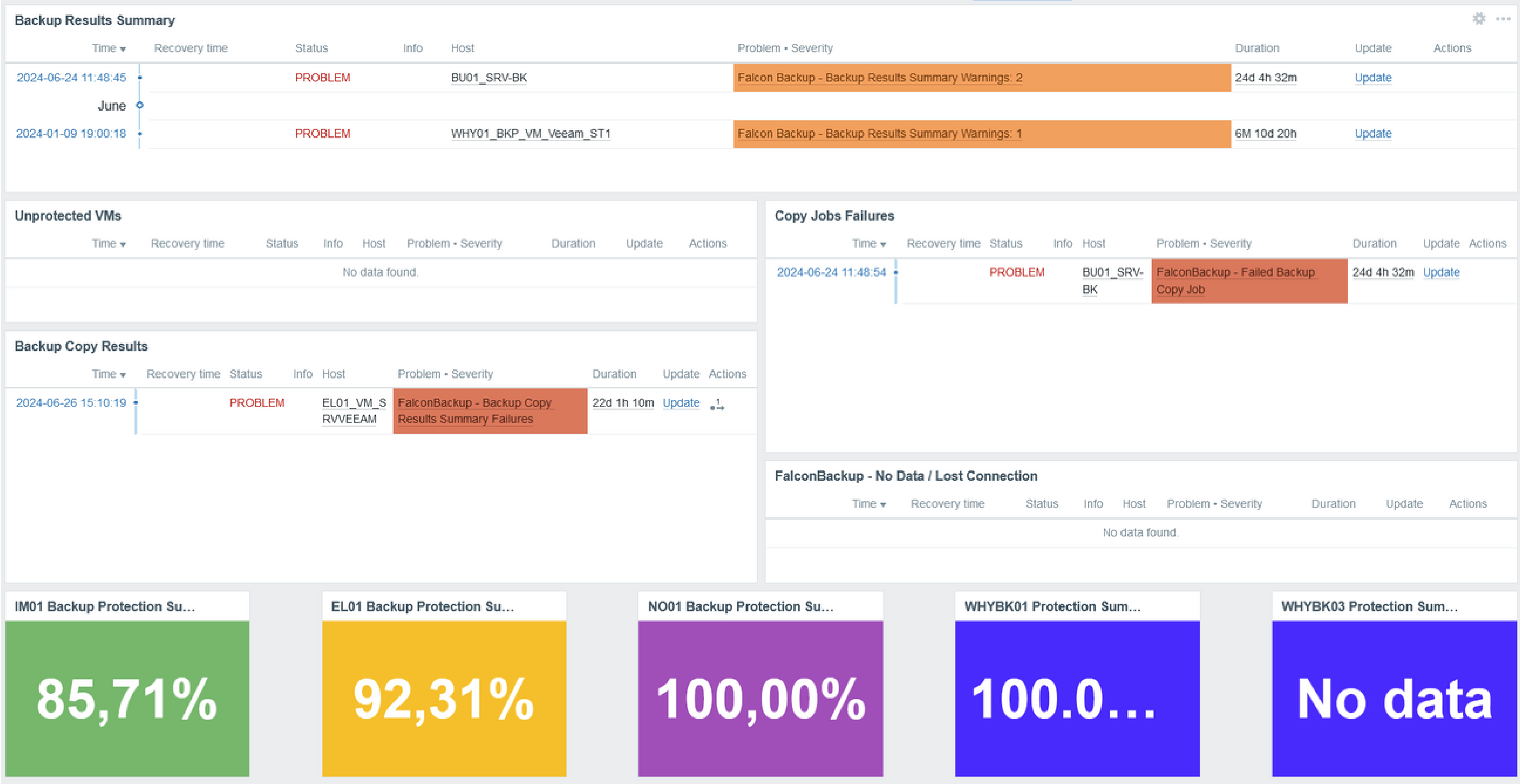
Raw data example

WHYSECURITY
CYBER SECURITY

Cyber Resilience: Backup with Veeam

Using **HTML Report** and **Zabbix Trapper**.

With the Zabbix APIs, we create the hosts representing VM's and populate the trappers with information obtained from the HTML Veeam Report.



Backup Results Summary

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Actions
2024-06-24 11:48:45		PROBLEM		BU01_SRV-BK	Falcon Backup - Backup Results Summary Warnings: 2	24d 4h 32m	Update	
June								
2024-01-09 19:00:18		PROBLEM		WHY01_BKP_VM_Veeam_ST1	Falcon Backup - Backup Results Summary Warnings: 1	6M 10d 20h	Update	

Unprotected VMs

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Actions
No data found.								

Copy Jobs Failures

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Actions
2024-06-24 11:48:54		PROBLEM		BU01_SRV-BK	FalconBackup - Failed Backup Copy Job	24d 4h 32m	Update	

Backup Copy Results

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Actions
2024-06-26 15:10:19		PROBLEM		EL01_VM_SRVVEEAM	FalconBackup - Backup Copy Results Summary Failures	22d 1h 10m	Update	1

FalconBackup - No Data / Lost Connection

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Actions
No data found.								

IM01 Backup Protection Su...	EL01 Backup Protection Su...	NO01 Backup Protection Su...	WHYBK01 Protection Sum...	WHYBK03 Protection Sum...
85,71%	92,31%	100,00%	100.0...	No data

WHYSECURITY
CYBER SECURITY

Serverless Approach

Using Zabbix only, *no external app required*.

Directly using HTTP Items we can make HTTP Calls to our technologies.

Pros:

- Easy to write
- Easy to debug
- Easy to change

Cons:

- No automatic host creation
- Manual application of the template/items to the hosts.

Shodan Vulnerabilities and network exposure

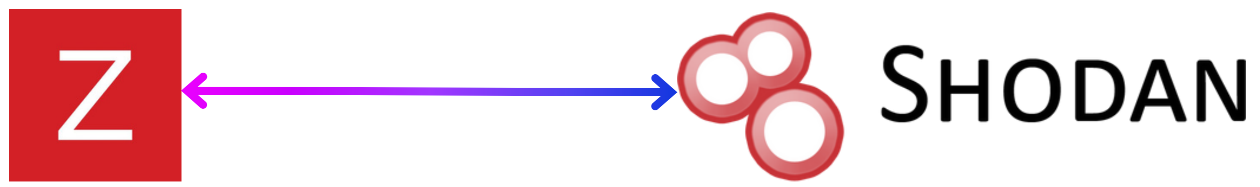
Using Zabbix only, *no external app required*.

Let’s start with Shodan!

Shodan is a **internet search engine for** Internet-connected devices. It allows users to discover **security vulnerabilities**, monitor network exposure, and assess potential risks by providing detailed information about each device's open ports, services, and software versions.

We do cybersecurity, so it's obvious that we need it.

But how to integrate it into Zabbix?

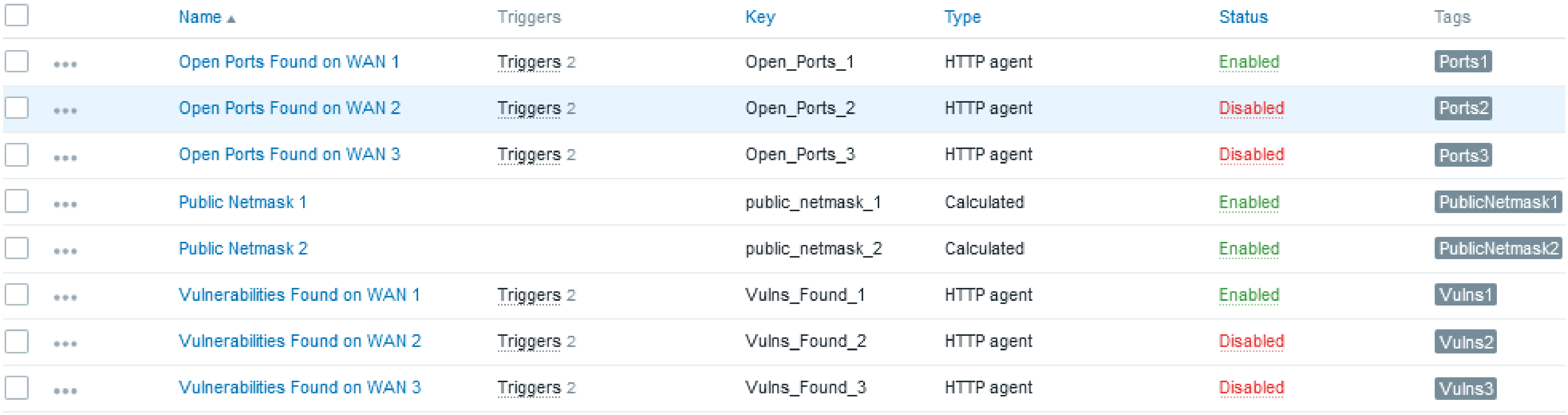


Shodan Vulnerabilities and network exposure

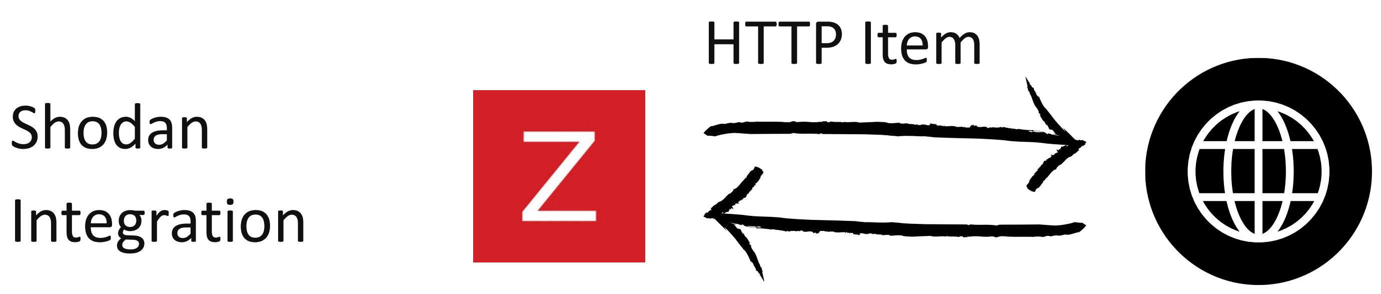
Using Zabbix only, *no external app required*.

By combining the power of HTTP items and JavaScript, we can achieve a good results!

First, we created a template: **Shodan_Template** then we created some HTTP Items like this:



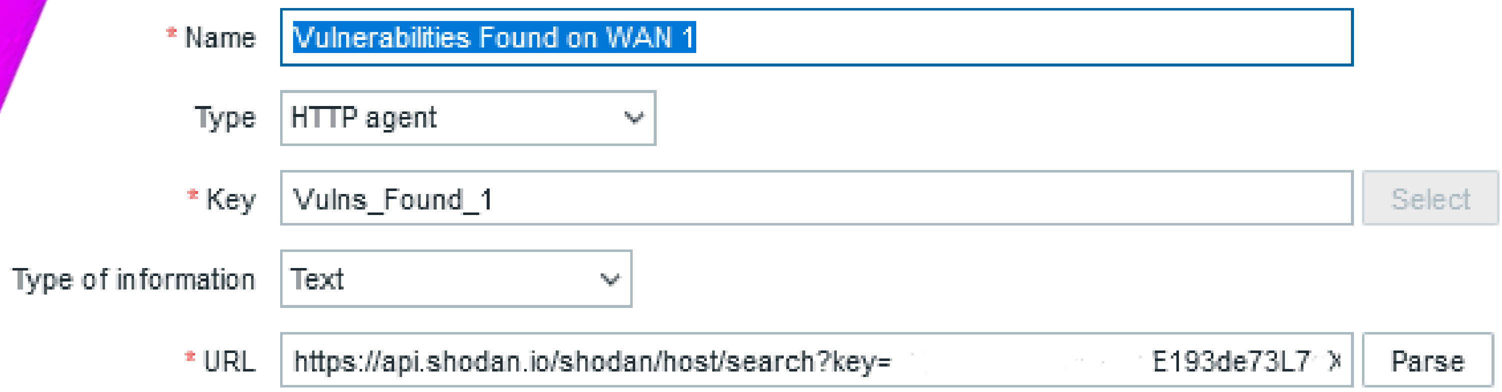
□		Name ▴	Triggers	Key	Type	Status	Tags
□	•••	Open Ports Found on WAN 1	Triggers 2	Open_Ports_1	HTTP agent	Enabled	Ports1
□	•••	Open Ports Found on WAN 2	Triggers 2	Open_Ports_2	HTTP agent	Disabled	Ports2
□	•••	Open Ports Found on WAN 3	Triggers 2	Open_Ports_3	HTTP agent	Disabled	Ports3
□	•••	Public Netmask 1		public_netmask_1	Calculated	Enabled	PublicNetmask1
□	•••	Public Netmask 2		public_netmask_2	Calculated	Enabled	PublicNetmask2
□	•••	Vulnerabilities Found on WAN 1	Triggers 2	Vulns_Found_1	HTTP agent	Enabled	Vulns1
□	•••	Vulnerabilities Found on WAN 2	Triggers 2	Vulns_Found_2	HTTP agent	Disabled	Vulns2
□	•••	Vulnerabilities Found on WAN 3	Triggers 2	Vulns_Found_3	HTTP agent	Disabled	Vulns3



Shodan Vulnerabilities and network exposure

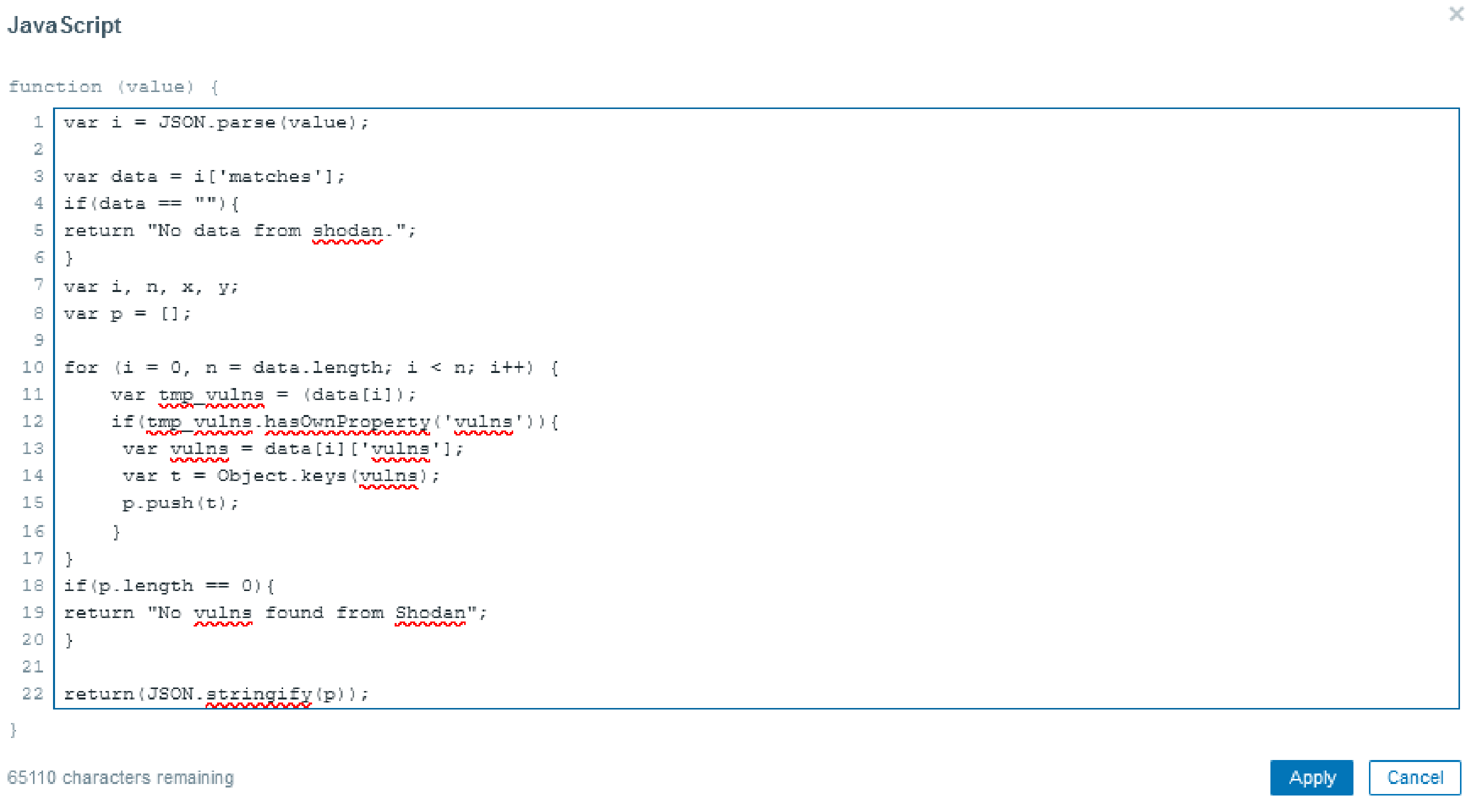
Using Zabbix only, *no external app required*.

Then we used Shodan API to get the informations.



* Name	Vulnerabilities Found on WAN 1
Type	HTTP agent
* Key	Vulns_Found_1
Type of information	Text
* URL	https://api.shodan.io/shodan/host/search?key=[redacted]E193de73L7

And a bit of Macros and Javascript preprocessing.



JavaScript

```
function (value) {
var i = JSON.parse(value);

var data = i['matches'];
if(data == ""){
return "No data from shodan.";
}
var i, n, x, y;
var p = [];

for (i = 0, n = data.length; i < n; i++) {
    var tmp_vulns = (data[i]);
    if(tmp_vulns.hasOwnProperty('vulns')){
     var vulns = data[i]['vulns'];
     var t = Object.keys(vulns);
     p.push(t);
    }
}
if(p.length == 0){
return "No vulns found from Shodan";
}

return(JSON.stringify(p));
}
```

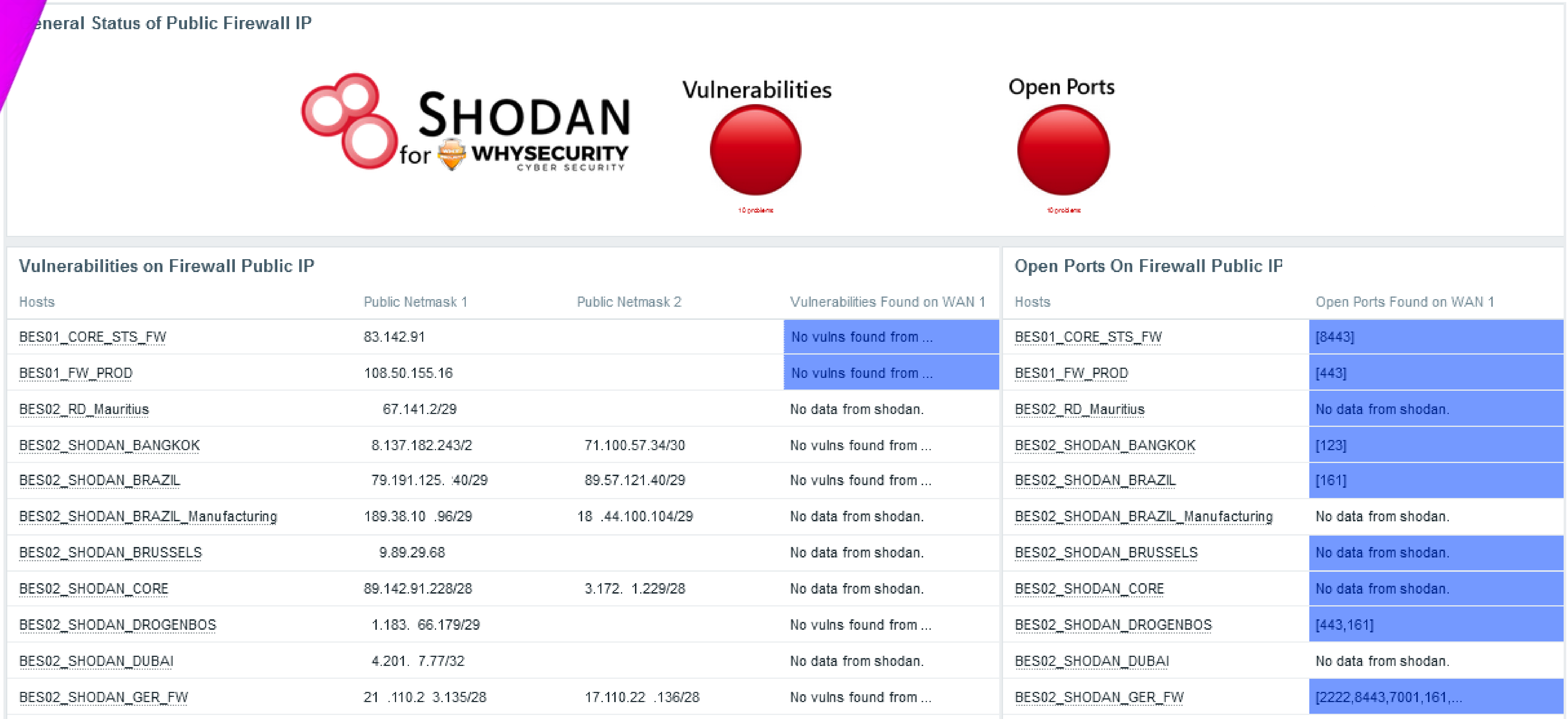
65110 characters remaining

WHYSECURITY
CYBER SECURITY

Shodan Vulnerabilities and network exposure

Using Zabbix only, *no external app required*.

Combined with the addition of a few triggers, this is the result



eneral Status of Public Firewall IP

Vulnerabilities on Firewall Public IP

Hosts	Public Netmask 1	Public Netmask 2	Vulnerabilities Found on WAN 1
BES01_CORE_STS_FW	83.142.91		No vulns found from ...
BES01_FW_PROD	108.50.155.16		No vulns found from ...
BES02_RD_Mauritius	67.141.2/29		No data from shodan.
BES02_SHODAN_BANGKOK	8.137.182.243/2	71.100.57.34/30	No vulns found from ...
BES02_SHODAN_BRAZIL	79.191.125. :40/29	89.57.121.40/29	No vulns found from ...
BES02_SHODAN_BRAZIL_Manufacturing	189.38.10 .96/29	18 .44.100.104/29	No data from shodan.
BES02_SHODAN_BRUSSELS	9.89.29.68		No data from shodan.
BES02_SHODAN_CORE	89.142.91.228/28	3.172. 1.229/28	No data from shodan.
BES02_SHODAN_DROGENBOS	1.183. 66.179/29		No vulns found from ...
BES02_SHODAN_DUBAI	4.201. 7.77/32		No data from shodan.
BES02_SHODAN_GER_FW	21 .110.2 3.135/28	17.110.22 .136/28	No vulns found from ...

Open Ports On Firewall Public IP

Hosts	Open Ports Found on WAN 1
BES01_CORE_STS_FW	[8443]
BES01_FW_PROD	[443]
BES02_RD_Mauritius	No data from shodan.
BES02_SHODAN_BANGKOK	[123]
BES02_SHODAN_BRAZIL	[161]
BES02_SHODAN_BRAZIL_Manufacturing	No data from shodan.
BES02_SHODAN_BRUSSELS	No data from shodan.
BES02_SHODAN_CORE	No data from shodan.
BES02_SHODAN_DROGENBOS	[443,161]
BES02_SHODAN_DUBAI	No data from shodan.
BES02_SHODAN_GER_FW	[2222,8443,7001,161,...

WHYSECURITY
CYBER SECURITY

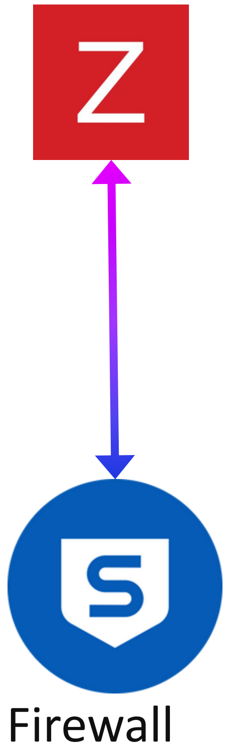
Sophos Firewall Surveillance

Using Zabbix only, *no external app required.*

We monitor **over 60 propertie**s using Zabbix HTTP items, without using external software.

What we used:

- **HTTP Items**
- Master & dependent item
- Javascript Preprocessing

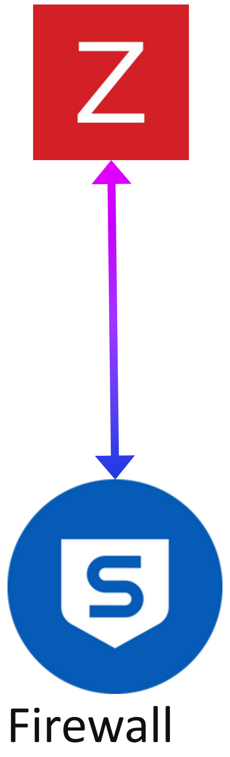


Sophos Firewall Surveillance

Using Zabbix only, *no external app required.*

These are some of the properties that we monitor:

- VPN Status
- HA Status
- SNMP Status
- SSH Port
- License Expiration

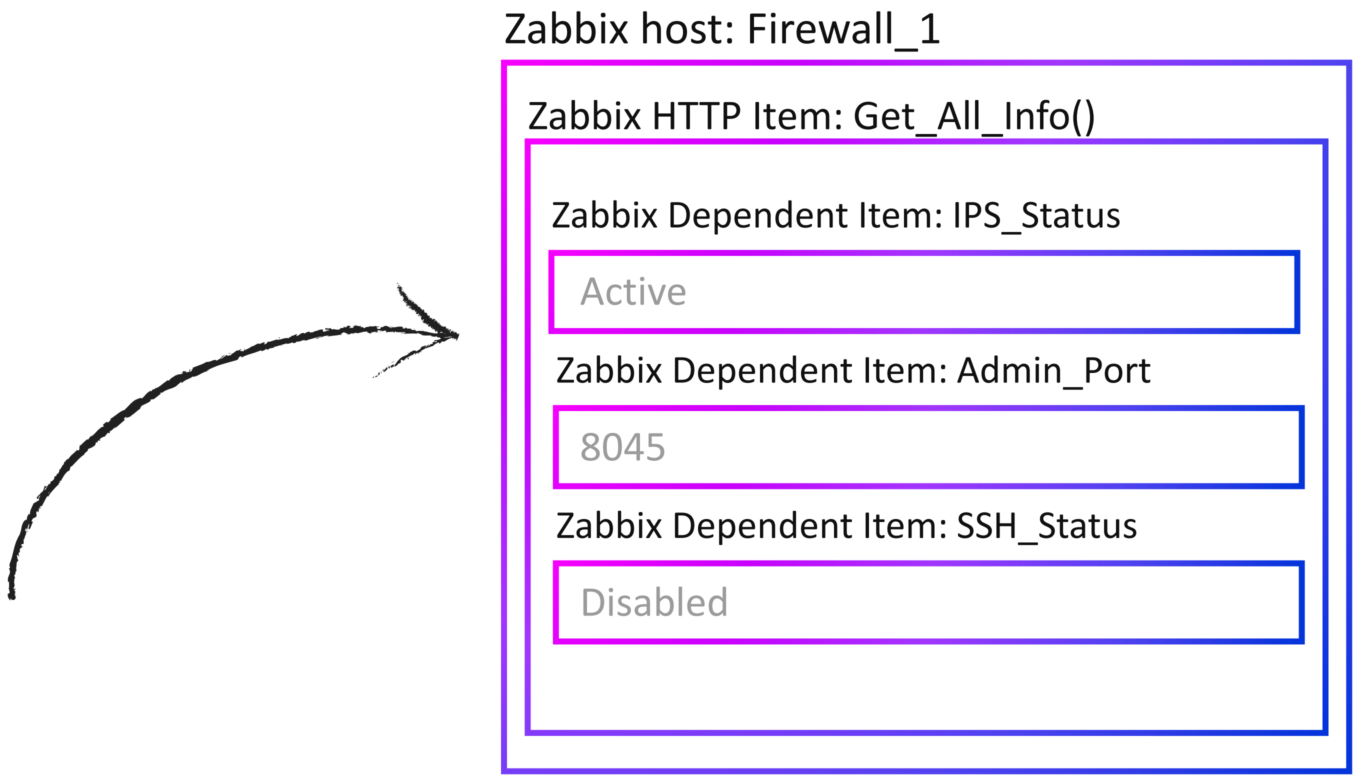


With Zabbix, we can monitor if some of these properties change over time and take action.

Sophos Firewall Surveillance

Using Zabbix only, *no external app required.*

We used an HTTP Item to get all infos from Sophos Firewall



Zabbix host: Firewall_1

Zabbix HTTP Item: Get_All_Info()

Zabbix Dependent Item: IPS_Status

Active

Zabbix Dependent Item: Admin_Port

8045

Zabbix Dependent Item: SSH_Status

Disabled

- Each **host is autonomous in identifying its own changes**.
- No new container deployment is necessary in case of code changes.
- **Instant visualization of the HTTP call** result.

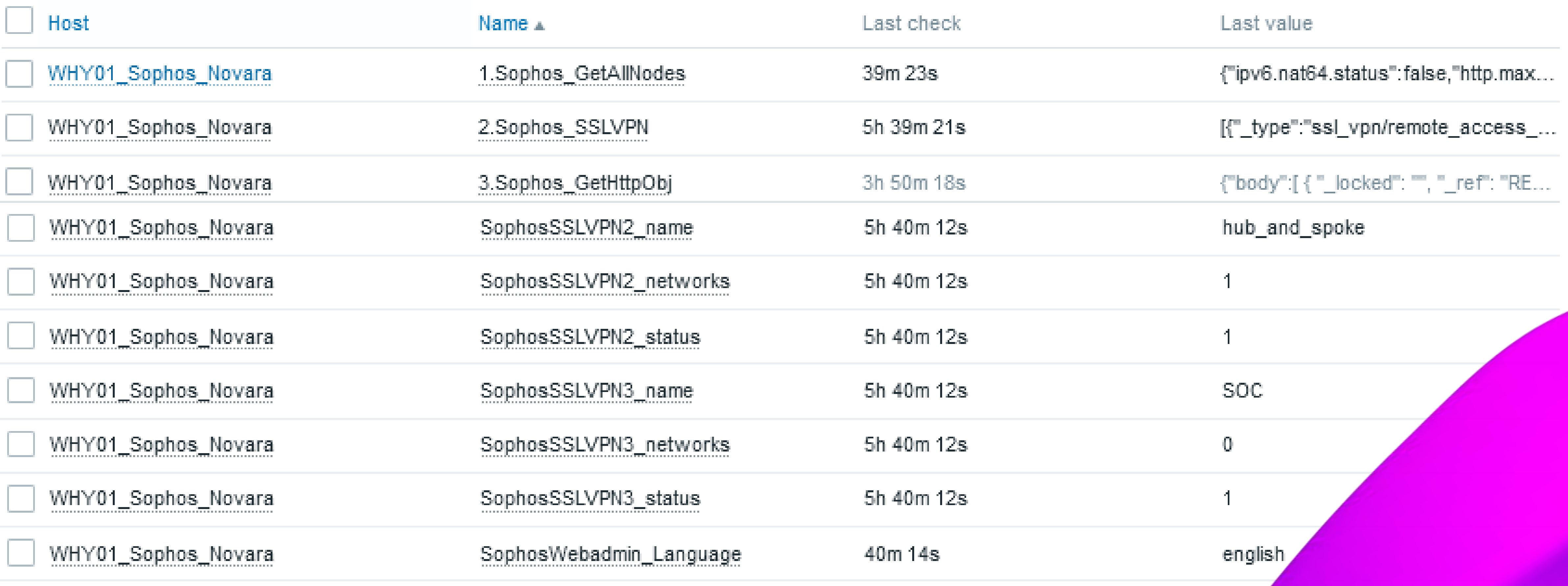
WHYSECURITY
CYBER SECURITY

Sophos Firewall Surveillance

Using Zabbix only, *no external app required.*

HTTP Items

Depend items



□	Host	Name ▲	Last check	Last value
□	WHY01_Sophos_Novara	1.Sophos_GetAllNodes	39m 23s	{"ipv6.nat64.status":false,"http.max...
□	WHY01_Sophos_Novara	2.Sophos_SSLVPN	5h 39m 21s	[{"_type":"ssl_vpn/remote_access_...
□	WHY01_Sophos_Novara	3.Sophos_GetHttpObj	3h 50m 18s	{"body":[{ "_locked": "", "_ref": "RE...
□	WHY01_Sophos_Novara	SophosSSLVPN2_name	5h 40m 12s	hub_and_spoke
□	WHY01_Sophos_Novara	SophosSSLVPN2_networks	5h 40m 12s	1
□	WHY01_Sophos_Novara	SophosSSLVPN2_status	5h 40m 12s	1
□	WHY01_Sophos_Novara	SophosSSLVPN3_name	5h 40m 12s	SOC
□	WHY01_Sophos_Novara	SophosSSLVPN3_networks	5h 40m 12s	0
□	WHY01_Sophos_Novara	SophosSSLVPN3_status	5h 40m 12s	1
□	WHY01_Sophos_Novara	SophosWebadmin_Language	40m 14s	english

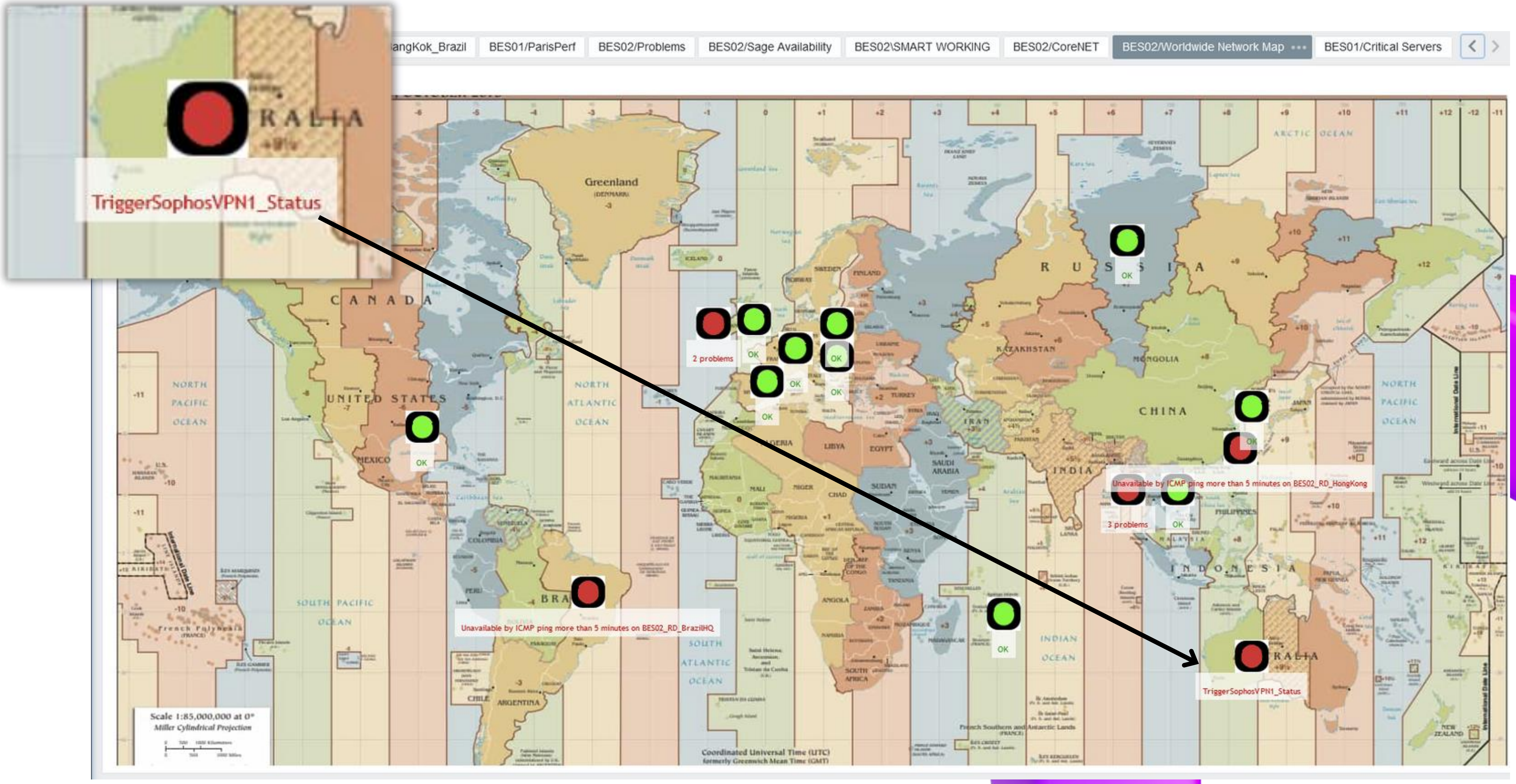
Preprocessing is the key!

We used Javascript and JSON Path preprocessing.

Sophos Firewall Surveillance

Using Zabbix only, *no external app required.*

We show all the information on a map.



TriggerSophosVPN1_Status

Unavailable by ICMP ping more than 5 minutes on BES02_RD_BrazilHQ

Unavailable by ICMP ping more than 5 minutes on BES02_RD_HongKong

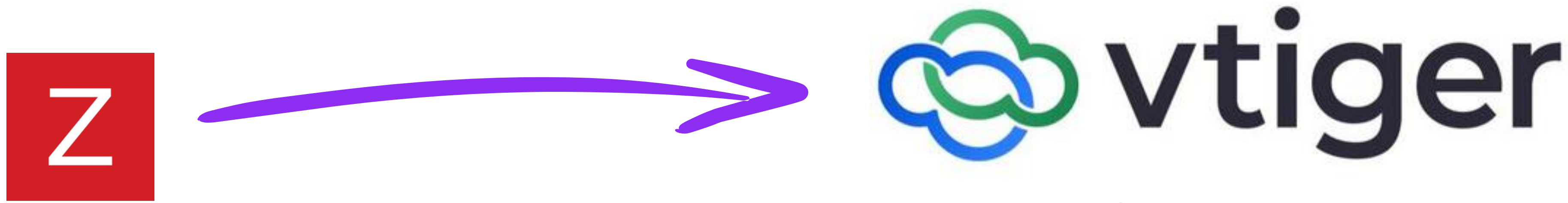
From Zabbix to Ticketing System

Open Ticket on CRM directly from Zabbix

Monitoring is crucial for identifying issues,

and once identified, they need to be handled by our team.

We have also integrated Zabbix with our CRM.



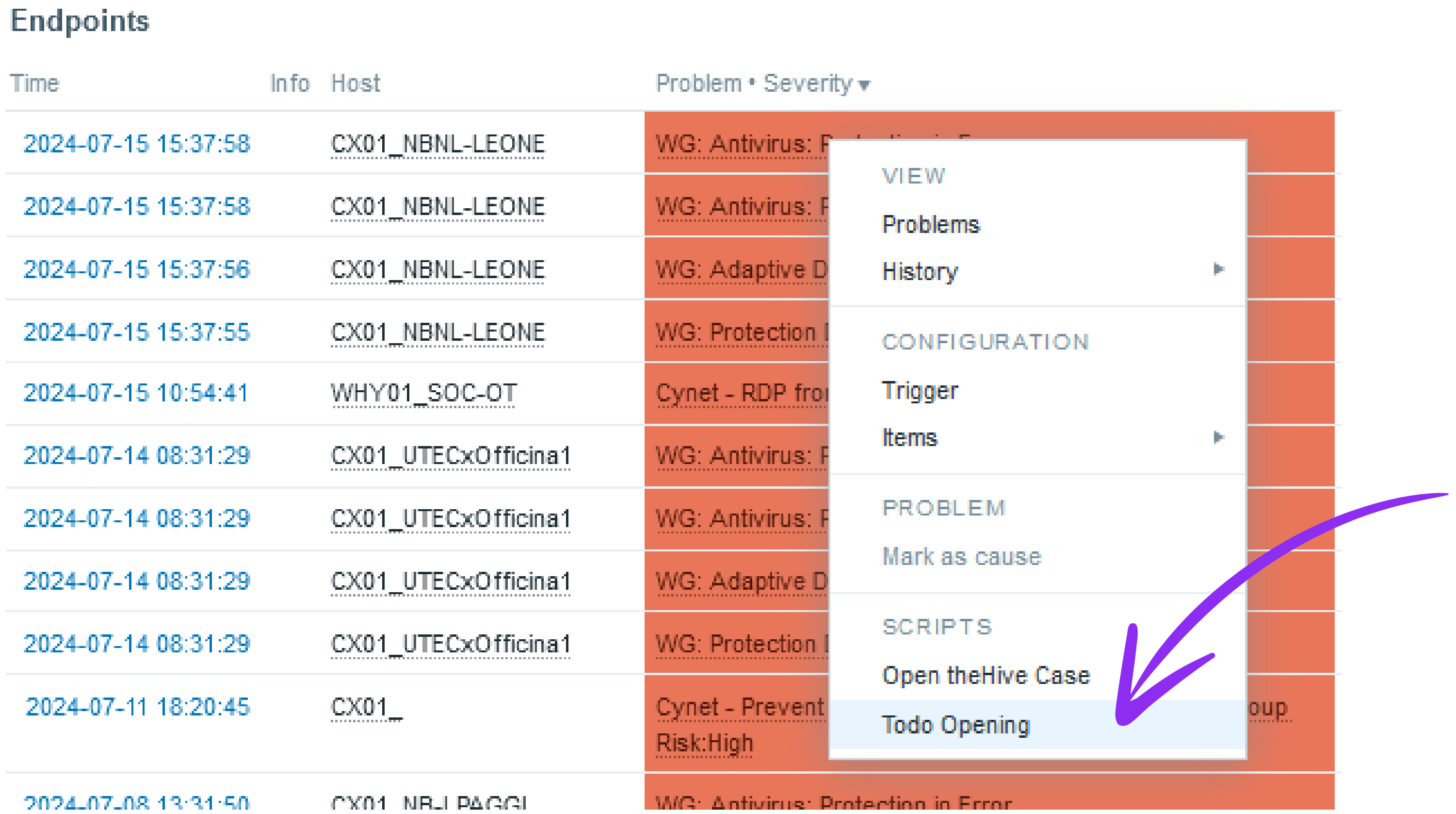
Zabbix

Our CRM

From Zabbix to Ticketing System

Open Ticket on CRM directly from Zabbix

By clicking on the problem, a manual action can be performed that results in the creation of a To-Do in our CRM.



Endpoints

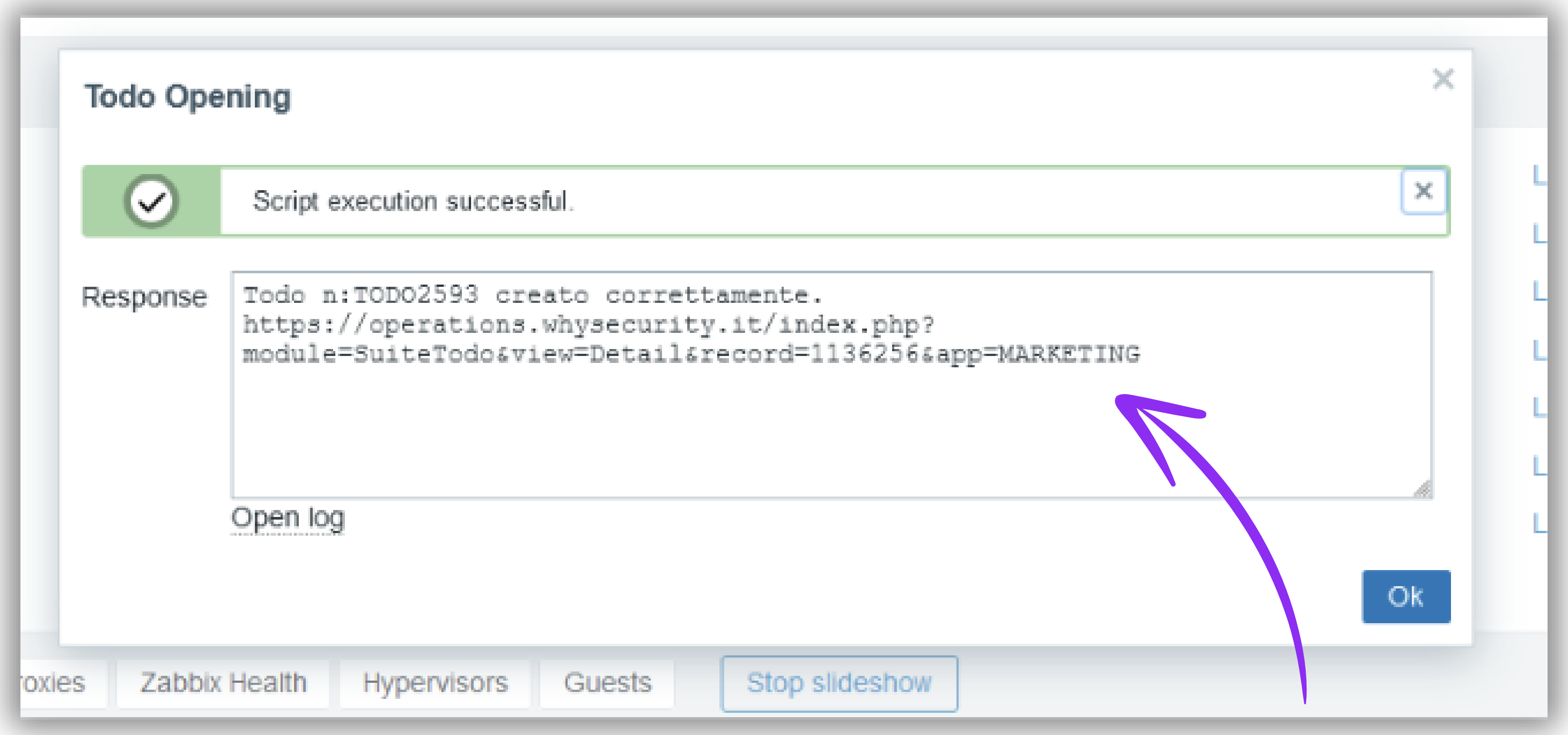
Time	Info	Host	Problem • Severity ▾
2024-07-15 15:37:58		CX01_NBNL-LEONE	WG: Antivirus: P
2024-07-15 15:37:58		CX01_NBNL-LEONE	WG: Antivirus: P
2024-07-15 15:37:56		CX01_NBNL-LEONE	WG: Adaptive D
2024-07-15 15:37:55		CX01_NBNL-LEONE	WG: Protection I
2024-07-15 10:54:41		WHY01_SOC-OT	Cynet - RDP fro
2024-07-14 08:31:29		CX01_UTECxOfficina1	WG: Antivirus: P
2024-07-14 08:31:29		CX01_UTECxOfficina1	WG: Antivirus: P
2024-07-14 08:31:29		CX01_UTECxOfficina1	WG: Adaptive D
2024-07-14 08:31:29		CX01_UTECxOfficina1	WG: Protection I
2024-07-11 18:20:45		CX01_	Cynet - Prevent … oup Risk:High
2024-07-08 13:31:50		CX01_NB-LPAGGI	WG: Antivirus: Protection in Error

Step 1

From Zabbix to Ticketing System

Open Ticket on CRM directly from Zabbix

By clicking on the problem, a manual action can be performed that results in the creation of a To-Do in our CRM.



Todo Opening

Script execution successful.

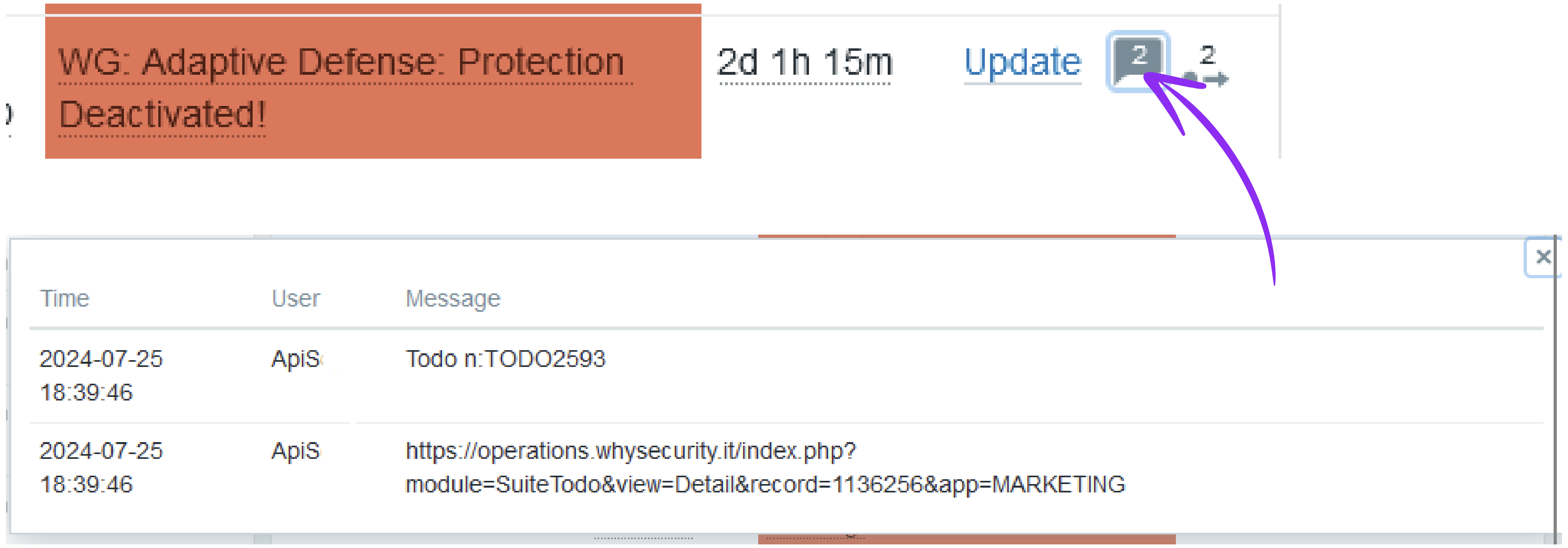
Response

```
Todo n:TODO2593 creato correttamente.
https://operations.whysecurity.it/index.php?
module=SuiteTodo&view=Detail&record=1136256&app=MARKETING
```

From Zabbix to Ticketing System

Open Ticket on CRM directly from Zabbix

By clicking on the problem, a manual action can be performed that results in the creation of a To-Do in our CRM.

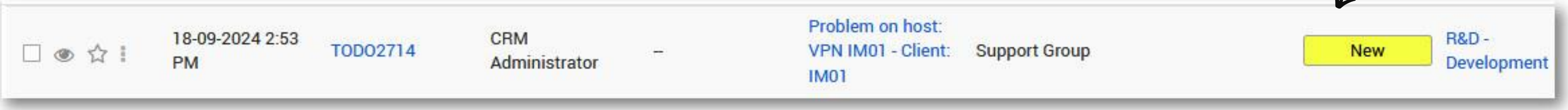


Time	User	Message
2024-07-25 18:39:46	ApiS	Todo n:TODO2593
2024-07-25 18:39:46	ApiS	https://operations.whysecurity.it/index.php?module=SuiteTodo&view=Detail&record=1136256&app=MARKETING

From Zabbix to Ticketing System

Open Ticket on CRM directly from Zabbix

By clicking on the problem, a manual action can be performed that results in the creation of a To-Do in our CRM.



CRM

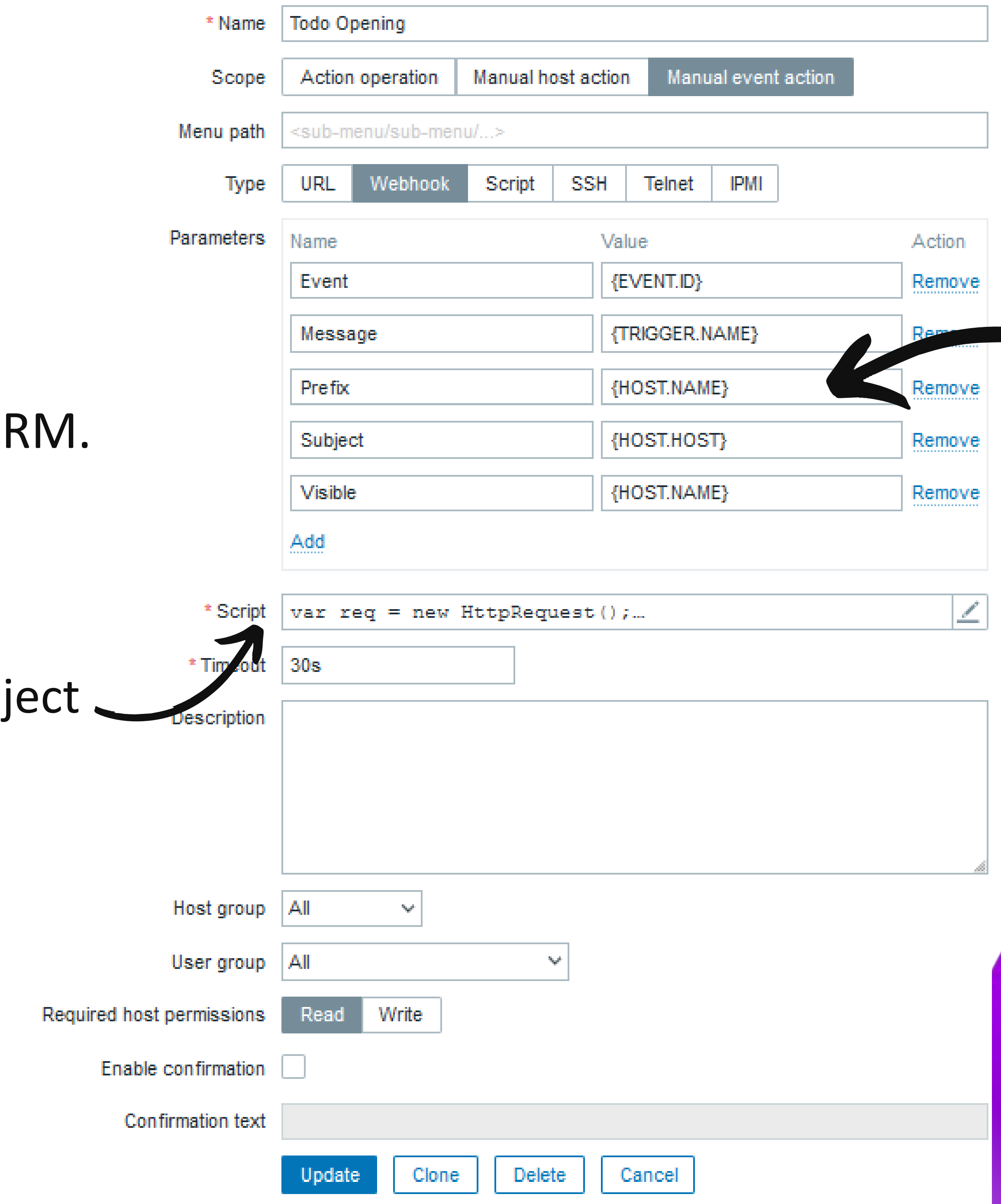
☐	18-09-2024 2:53 PM	TODO2714	CRM Administrator	–	Problem on host: VPN IM01 - Client: IM01	Support Group	New	R&D - Development

WHYSECURITY
CYBER SECURITY

From Zabbix to Ticketing System

Open Ticket on CRM directly from Zabbix

We used a **manual script** and **some macros.** Subsequently, an HTTP call handles contacting the CRM.



* Name: Todo Opening

Scope: Action operation | Manual host action | **Manual event action**

Menu path: <sub-menu/sub-menu/...>

Type: URL | **Webhook** | Script | SSH | Telnet | IPMI

Parameters

Name	Value	Action
Event	{EVENT.ID}	Remove
Message	{TRIGGER.NAME}	Remove
Prefix	{HOST.NAME}	Remove
Subject	{HOST.HOST}	Remove
Visible	{HOST.NAME}	Remove

Add

* Script: `var req = new HttpRequest();…`

* Timeout: 30s

Description:

Host group: All

User group: All

Required host permissions: **Read** | Write

Enable confirmation: □

Confirmation text:

Update | Clone | Delete | Cancel

Macros

Script with HttpRequest() object to make HTTP Call.

Vincenzo

WHYSECURITY
CYBER SECURITY

Much more is coming.

Thanks for your attention

Let’s keep in touch.

For any questions: info@whysecurity.it

https://www.whysecurity.it

Gabriele