



# **MEDUSA** **LAB**

FIAP CHALLENGE 2023 - SBT

Murillo Fiorin Gimenez – RM 93600  
Carlos Henrique Pereira Santos – RM 95495  
Gabriel Flauzino dos Santos – RM 96050  
Matheus Santos Carvalho – RM 94551

# O QUE VIMOS ATÉ AGORA:

SPLUNK REALIZANDO DETECÇÃO DE ATAQUES VIA CALDERA



INTRODUÇÃO AO MISP E O QUE ELE PODE OFERECER



INTELIGÊNCIA PARA DETECTAR AMEAÇAS



# FERRAMENTAS UTILIZADAS NO FINAL DO PROJETO

splunk>




Google Cloud

**COMO FOI O PROJETO DE  
IMPLEMENTAÇÃO E  
SUAS DIFICULDADES?**



# THE HIVE



[+ New Case](#)

[My tasks 1](#)

[Waiting tasks 2](#)

[Alerts 22](#)

[Dashboards](#)

[Search](#)

[Organisation](#)

GF

MedusaLab/Gabriel Flauzin

List of cases (3 of 3)

[+ Show live stream](#)

No case selected

Quick Filters

Sort by

Custom Fields

Stats

Filters

15 per page

Filters

[+ Add a filter](#)

<input type="checkbox"/>	Status	# Number	Title	Severity	Details	Assignee	Dates	S.	C.	U.
<input type="checkbox"/>	<div>Open</div> <div>5 hours</div>	#8	SSH Brute force	M	<div>Tasks1</div> <div>Observables13</div> <div>TTPs0</div>	GF	S. 09/26/23 18:41 C. 09/26/23 18:41			
<input type="checkbox"/>	<div>Open</div> <div>12 hours</div>	#7	SSH Brute force	M	<div>Tasks1</div> <div>Observables6</div> <div>TTPs0</div>	GF	S. 09/26/23 11:47 C. 09/26/23 11:47			
<input type="checkbox"/>	<div>Open</div> <div>a day</div>	#3	Malicious Domain Communication	H	<div>Tasks2</div> <div>Observables3</div> <div>TTPs0</div>	GF	S. 09/25/23 14:59 C. 09/25/23 15:00 U. 09/26/23 11:09			



# Cortex

Cortex

+ New Analysis

Jobs History

Analyzers

Responders

Organization

ML Medusa/Medusa Lab

Jobs History (21)

Data Types (14)

Job Type (2)

Analyzers (7)

Observable

Select

Select

Select

Search for observable data

Search

Clear

Pagination

50 / page

Status	Job details	TLP	PAP
Success	<div>[ip] 58[.]8[.]178[.]26</div> <div>Analyzer: VirusTotal_GetReport_3_1</div> <div>Date: 5 hours ago</div> <div>User: Medusa/api</div>	TLP:AMBER	PAP:AMBER
Success	<div>[ip] 58[.]8[.]178[.]26</div> <div>Analyzer: AbuseIPDB_1_0</div> <div>Date: 5 hours ago</div> <div>User: Medusa/api</div>	TLP:AMBER	PAP:AMBER

## ANALYSERS





# STEP BY STEP DE UM ALERTA (EDR, WAF, FIREWALL)

ACTION NO SPLUNK PARA ABRIR ALERTA NO THEHIVE VIA API



APOS GERAR O ALERTA, HÁ OS CAMPOS DE OBSERVAÇÃO (STATS FEITO NO SPLUNK)



RODAR ANALYZERS PARA AUTOMATIZAR O PROCESSO DE INGESTÃO DE DADOS



# EXECUÇÃO DO ANALYZER

ip

34[.]176[.]111[.]233

field:src

VT:GetReport="0 resolution(s)"

VT:GetReport="0/88"

AbuseIPDB:Records="0"

MISP:Search="0 events"

S. 09/26/23 11:47

C. 09/26/23 11:47

U. 09/26/23 11:47





# O QUE ESSE PROCESSO PODE GERAR DE PROTEÇÃO?

AGILIDADE NA RESPOSTA A INCIDENTES



IDENTIFICAÇÃO DE BEACONS DE COBALTSTRIKE VIA REQUISIÇÕES NO PROXY/THREAT INTELLIGENCE



COM OS LOGS DE ANTIVÍRUS/PROXY/FIREWALL, É POSSÍVEL INGERIR COMUNICAÇÕES TANTO DE FORA PRA DENTRO, QUANTO DE DENTRO PRA FORA, GERANDO VISIBILIDADE NAS IOCS.



# AUTOMATIZAÇÃO DE RESPOSTAS COM O RESPONDER

SCRIPTS EM PYTHON QUE RODAM VIA CORTEX PARA REALIZAR ACTIONS



UTILIZADO PARA BLOQUEAR USUÁRIO, ESTAÇÃO E ATÉ IP UTILIZANDO API



# PONTOS IMPORTANTES

TODAS AS FERRAMENTAS PODEM SER SUBSTITUÍDAS POR OPÇÕES LICENCIADAS OU OPEN SOURCE



PRINCIPAIS APIS UTILIZADAS PARA O INTELL SÃO AS DO ABUSEIPDB, VIRUS TOTAL, MISP (SERVIDOR PRÓPRIO)



# DADOS PÓS APRESENTAÇÃO



# DASHBOARD ENVIO DE LOGS

## Index Monitoring

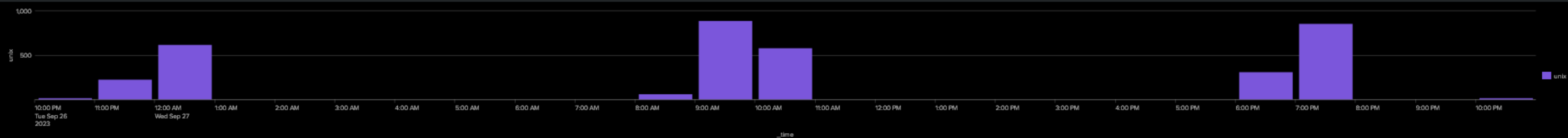
Monitoramento de eventos no ambiente

Edit

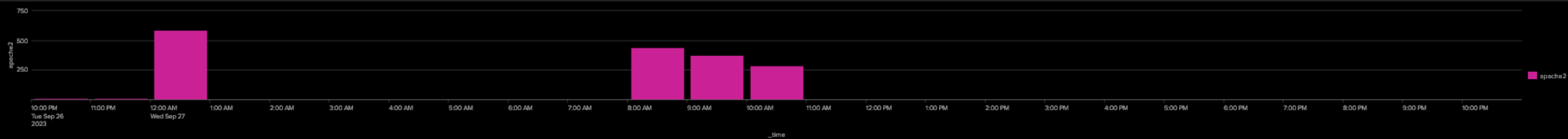
Export

...

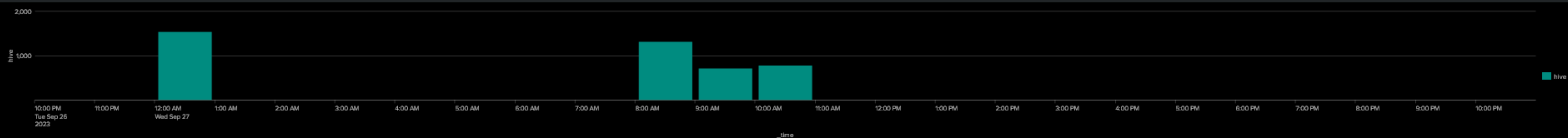
### UNIX



### WEB SERVER



### HIVE



# MISP

My Events

Org Events

Enter value to search

Event info

Filter

	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
			2689			143002	21	admin@admin.test	2023-09-23	List of malicious domains in Poland feed	Organisation	
			2688		osint:source-type="block-or-filter-list"	24315	88	admin@admin.test	2023-09-23	James Brine Bruteforce IPs feed	Organisation	
			2687		osint:source-type="block-or-filter-list"	1884	507	admin@admin.test	2023-09-23	threatfox indicators of compromise feed	Organisation	
			2686		osint:source-type="block-or-filter-list"	284	6	admin@admin.test	2023-09-23	URL Seen in honeypots feed	Organisation	
			2118		osint:source-type="block-or-filter-list"	1861	173	admin@admin.test	2023-09-20	Malware Bazaar feed	Organisation	
			1688		osint:source-type="block-or-filter-list"	39	24	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 8 - no false positives feed	Organisation	
			1686		osint:source-type="block-or-filter-list"	1351	36	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 6 - no false positives feed	Organisation	
			1687		osint:source-type="block-or-filter-list"	211	28	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 7 - no false positives feed	Organisation	
			1685		osint:source-type="block-or-filter-list"	4136	44	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 5 - ultra false positives feed	Organisation	
			1684		osint:source-type="block-or-filter-list"	8952	62	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 4 - very low false positives feed	Organisation	
			1683		osint:source-type="block-or-filter-list"	19745	140	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 3 - low false positives feed	Organisation	
			1682		osint:source-type="block-or-filter-list"	46676	251	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 2 - medium false positives feed	Organisation	
			1681		osint:source-type="automatic-collection"	325706	907	admin@admin.test	2023-09-20	IPsum (aggregation of all feeds) - level 1 - lot of false positives feed	Organisation	
			1680			20272	468	admin@admin.test	2023-09-20	Panels Tracker feed	Organisation	
			1679			7913	183	admin@admin.test	2023-09-20	malshare.com - current all feed	Organisation	
			1675			2564	39	admin@admin.test	2023-09-20	mirai.security.gives feed	Organisation	
			1671			299	18	admin@admin.test	2023-09-20	CyberCure - IP Feed feed	Organisation	

# REQUESTS NO WEBSERVER





# REPORT ANALYZER THEHIVE/CORTEX

## Report of VirusTotal\_GetReport\_3\_1 analysis

### Summary

Malicious 5/89

Suspicious 1/89

Undefined 21/89

Last analysis date 2023-09-26 21:16:56

SHA-256 45.88.90.116

VirusTotal Report <https://www.virustotal.com/gui/search/45.88.90.116>

### Scans

Scanner	Detected	Method	Update	Version
Bkav	?	blacklist	//	
CMC Threat Intelligence	✓	blacklist	//	
Snort IP sample list	✓	blacklist	//	
0xSI_f33d	?	blacklist	//	
ViriBack	✓	blacklist	//	
PhishLabs	?	blacklist	//	
K7AntiVirus	✓	blacklist	//	
CINS Army	✓	blacklist	//	

# ALERTAS SPLUNK / THEHIVE

<input type="checkbox"/>	Time ▾	Fired Alerts ▴	App ▴	Type ▴	Severity ▴	Mode ▴	Actions
<input type="checkbox"/>	2023-09-27 22:30:01 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 19:45:02 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 19:30:02 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 19:15:01 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 18:45:01 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 10:45:01 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 10:30:02 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 10:15:13 -03	BadIP make many requests	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 10:15:02 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 10:00:02 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 09:50:18 -03	BadIP make many requests	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 09:45:01 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 09:35:15 -03	BadIP make many requests	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 09:30:15 -03	BadIP make many requests	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>
<input type="checkbox"/>	2023-09-27 09:30:02 -03	SSH Brute force	search	Scheduled	<div></div> Low	Per Result	<a href="#">View Results</a> <a href="#">Edit Search</a> <a href="#">Delete</a>

<input type="checkbox"/>	Severity ▴▾	Read ▴▾	Title	# Case	Type ▴▾	Source ▴▾	Reference ▴▾	Observables
<input type="checkbox"/>	<div>M</div>	<div>Unread</div>	SSH Brute force	<div>None</div>	alert	splunk	SPK1695821403	19
	<div> None</div>							
	<div>&lt;/&gt; None</div>							
<input type="checkbox"/>	<div>M</div>	<div>Unread</div>	SSH Brute force	<div>None</div>	alert	splunk	SPK1695820503	19
	<div> None</div>							
	<div>&lt;/&gt; None</div>							
<input type="checkbox"/>	<div>M</div>	<div>Unread</div>	SSH Brute force	<div>None</div>	alert	splunk	SPK1695819605	19
	<div> None</div>							
	<div>&lt;/&gt; None</div>							
<input type="checkbox"/>	<div>M</div>	<div>Unread</div>	SSH Brute force	<div>None</div>	alert	splunk	SPK1695819604	21
	<div> None</div>							
	<div>&lt;/&gt; None</div>							
<input type="checkbox"/>	<div>M</div>	<div>Unread</div>	SSH Brute force	<div>None</div>	alert	splunk	SPK1695819603	18
	<div> None</div>							
	<div>&lt;/&gt; None</div>							
<input type="checkbox"/>	<div>L</div>	<div>Unread</div>	BadIP make many requests	<div>None</div>	alert	splunk	SPK1695819020	9
	<div> None</div>							
	<div>&lt;/&gt; None</div>							

# GERAR UM RESPONDER EM CIMA DE UMA IOC

Case # 13 - BadIP make many requests

---

Gabriel Flauzino 
 09/27/23 10:33 
 12 hours 
 1 alert

Sharing (0) | 
 Close | 
 Flag | 
 Merge | 
 Remove | 
 Responders

---

Details

Tasks 0

Observables 9

TTPs

45[.]88[.]90[.]116
✕

[IP]: 45[.]88[.]90[.]116

---

⚙ Shodan:ASN="AS138687"

Shodan:Org="Des Capital B.V."

Shodan:VULNS="126"

Shodan:Location="Netherlands"

Shodan:Location="Netherlands"

Shodan:ASN="AS49581"

Shodan:Org="Inverse Hosting Ltd"

MISP:Search="3 event(s)"

VT:GetReport="6/89"

VT:GetReport="2 resolution(s)"

Basic Information

Sharing 
 Responders 
 Links

# ALGUNS RESPONDERS DISPONÍVEIS

MSDefender-IsolateMachine\_1\_0

Version: 1.0

Author: Keijo Korte

License: AGPL-V3

Type: Docker

Isolate machine with Microsoft Defender for Endpoints

+ Enable

PaloAltoCortexXDR\_isolate\_1\_0

Version: 1.0

Author: Joe Lazaro

License: AGPL-V3

Type: Docker

Isolate endpoints identified by hostname or IP list

PaloAltoNGFW\_block\_external\_IP\_address\_2\_0\_0

Version: 2.0.0

Author: Maxim Konakin, OSCD Initiative

License: AGPL-V3

Type: Docker

Block external IP address

PaloAltoNGFW\_block\_external\_domain\_2\_0\_0

Version: 2.0.0

Author: Maxim Konakin, OSCD Initiative

License: AGPL-V3

Type: Docker

Block external domain

CheckPoint\_Lock\_1\_0

Version: 1.0

Author: @dadokkio LDO-CERT

License: AGPL-V3

Type: Docker

Lock ip on CheckPoint Gaia

CheckPoint\_Unlock\_1\_0

Version: 1.0

Author: @dadokkio LDO-CERT

License: AGPL-V3

Type: Docker

Unlock ip on CheckPoint Gaia



# OBRIGADO!!

FIAP CHALLENGE 2023 - SBT