Softwares para Monitoramento da Segurança

Centro de TI – RP - USP
MSc. Eng. Ali Faiez Taha
aftaha@usp.br

São Paulo, 25 de Abril de 2017

USP SUPERINTENDÊNCIA
Tecnologia da Informação

Softwares para monitoramento da Segurança

Objetivos:

- Monitorar Serviços de Rede, Servidores, Vulnerabilidades, Vírus, Malwares, **Scan na Rede, Intrusão, Ameaças**, etc.
- Detectar e identificar padrões encontrados nos **Incidentes de Segurança**.
- Análise de tráfego anômalo.
- Detecção do ponto de falha e correção.
- Alertas e recomendações.
- Aprimorar a Segurança na USPnet.

Armazenamento de Logs

Objetivos:

- Coletar logs de autenticação de usuários Wireless USPnet
- Gateways da Wireless USPnet enviam Logs para Gateways Pfsenses.
- Armazena logs em banco de dados
- Relaciona diferentes níveis de logs, usuários conectados na Wireless, datas e horários, Endereços IP, Logins, Mac Address, etc.

**** Não possui logs da EDUROAM.***

Recomendações para os Logs

- **NBR ISO/IEC 17799** recomenda fortemente o armazenamento de Logs.
- **ISO/IEC 27002** estabelece a **proteção das informações dos registros dos sistemas operacionais e de informação**.

Deve-se armazenar:

- **datas e horários** de entrada e saída no sistema;
- Identidades e **localização**;
- Registro das **tentativas de acesso ao sistema;**
- Registro das **tentativas de acesso a outros recursos e dados;**
- Registros de auditoria e **coleta de evidências**.
- Registros para a **geração de evidências e técnicas de fraude computacionais e na informática forense**.

PHP Syslog-NG

- **Syslog-ng** possui muitas vantagens sobre o **syslog** tradicional.
- Formato das mensagens usando Unix shell-like
- Múltiplos destinos de mensagens.
- Envia mensagens para aplicações locais.
- Suporte ao controle de fluxo das mensagens.
- Registra logs diretamente em banco de dados.
- Classifica as mensagens de logs ao mesmo tempo que extrai informações estruturadas de mensagens syslogs desestruturadas.
- Processa mensagens estruturadas. Exemplo: extrair colunas de arquivos CSV.

(Dados de Rede dos Gateways) (Relação de Gateways)

USING TABLE: logs

USING CACHE TO POPULATE HOST, FACILITY, AND PROGRAM FIELDS.
Cache last updated on 2017-04-04 09:10:42.

HOSTS: 19

Include ○
Exclude ●
RegExp Matching? ☐
Hostname match
=====AND=====

- gwcem
- gwcreu
- gwfdrp
- gwrp01
- gwrp02
- gwrp03

PROGRAMS: 21

Include ○
Exclude ●
RegExp Matching? ☐
Program match
=====AND=====

- NONE
- check_reload_st
- cron
- dnsmasq
- filterdns
- kernel

SYSLOG FACILITY:

Include ○
Exclude ●

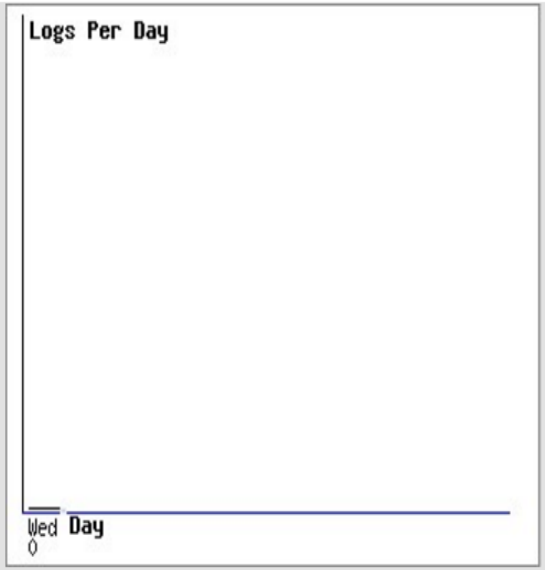
- auth
- console
- cron
- daemon
- kern
- local4
- local5
- ntp

SYSLOG PRIORITY:

Include ○
Exclude ●

- debug
- info
- notice
- warning
- err
- crit
- alert
- emerg

DATE TIME
From:
To:



RECORDS PER PAGE 1000
TopX 10
ORDER BY datetime
SEARCH ORDER DESC

SEARCH MESSAGE:

Exclude ☐ RegExp ☐ **AND**
Exclude ☐ RegExp ☐ **AND**
Exclude ☐ RegExp ☐

Search Tail Graph Reset

(Dados de Rede dos Gateways) (Relação de Gateways)

BACK TO SEARCH

Number of Entries Found: **433**

SEVERITY LEGEND

DEBUG | INFO | NOTICE | WARNING | ERROR | CRIT | ALERT | EMERG

SEQ	HOST	FACILITY	DATE TIME	PROGRAM	MESSAGE
N/A	gwcreu	local4	11:30:21	logportalauth	Zone: uspnet - FAILURE: aloliveira @cirp.usp.br, , 172.16.75.57
N/A	gwcreu	local4	11:27:24	logportalauth	Zone: uspnet - TIMEOUT: fabrileo@rp.usp.br, , 172.16.73.215
N/A	gwcreu	local4	11:27:22	logportalauth	Zone: uspnet - TIMEOUT: Leonara@rp.usp.br, , 172.16.74.113
N/A	gwcreu	local4	11:27:19	logportalauth	Zone: uspnet - TIMEOUT: guilherme0016@rp.usp.br, , 172.16.77.204
N/A	gwcreu	local4	11:25:29	logportalauth	Zone: uspnet - USER LOGIN: seninha@rp.usp.br, , 172.16.79.116
N/A	gwcreu	local4	11:24:15	logportalauth	Zone: uspnet - TIMEOUT: bauducone@cirp.usp.br, , 172.16.76.7
N/A	gwcreu	local4	11:23:12	logportalauth	Zone: uspnet - TIMEOUT: eheld@rp.usp.br, , 172.16.74.160
N/A	gwcreu	local4	11:21:08	logportalauth	Zone: uspnet - TIMEOUT: luishpeixoto@rp.usp.br, , 172.16.73.6
N/A	gwcreu	local4	11:17:04	logportalauth	Zone: uspnet - TIMEOUT: dadalt@rp.usp.br, , 172.16.79.154
N/A	gwcreu	local4	11:15:01	logportalauth	Zone: uspnet - TIMEOUT: Willy@rp.usp.br, , 172.16.76.165
N/A	gwcreu	local4	11:10:57	logportalauth	Zone: uspnet - TIMEOUT: juliamendez@rp.usp.br, , 172.16.74.231
N/A	gwcreu	local4	11:08:05	logportalauth	Zone: uspnet - USER LOGIN: kamilloe10@rp.usp.br, , 172.16.75.168
N/A	gwcreu	local4	11:07:51	logportalauth	Zone: uspnet - FAILURE: kamilloe10@rp.usp.br, , 172.16.75.168
N/A	gwcreu	local4	11:03:54	logportalauth	Zone: uspnet - USER LOGIN: caroljanucci@rp.usp.br, , 172.16.75.13
N/A	gwcreu	local4	11:03:51	logportalauth	Zone: uspnet - TIMEOUT: stedruzian@rp.usp.br, , 172.16.78.135
N/A	gwcreu	local4	11:03:48	logportalauth	Zone: uspnet - TIMEOUT: Murilofaleiro@rp.usp.br, , 172.16.77.73
N/A	gwcreu	local4	10:59:22	logportalauth	Zone: uspnet - USER LOGIN: jerodrigues@rp.usp.br, , 172.16.75.113
N/A	gwcreu	local4	10:56:42	logportalauth	Zone: uspnet - TIMEOUT: janielfidelis@rp.usp.br, , 172.16.79.94
N/A	gwcreu	local4	10:55:37	logportalauth	Zone: uspnet - USER LOGIN: libras@rp.usp.br, , 172.16.75.6
N/A	gwcreu	local4	10:54:38	logportalauth	Zone: uspnet - TIMEOUT: assaoka@cirp.usp.br, , 172.16.78.104
N/A	gwcreu	local4	10:52:58	logportalauth	Zone: uspnet - CONCURRENT LOGIN - TERMINATING OLD SESSION: bfreitas63@rp.usp.br, , 172.16.75.167
N/A	gwcreu	local4	10:52:55	logportalauth	Zone: uspnet - USER LOGIN: bfreitas63@rp.usp.br, , 172.16.78.99
N/A	gwcreu	local4	10:50:19	logportalauth	Zone: uspnet - USER LOGIN: lucianorosa, , 172.16.78.148
N/A	gwcreu	local4	10:48:01	logportalauth	Zone: uspnet - USER LOGIN: 240830@rp.usp.br, , 172.16.73.26
N/A	gwcreu	local4	10:44:33	logportalauth	Zone: uspnet - TIMEOUT: ninopirani@usp.br, , 172.16.73.18
N/A	gwcreu	local4	10:41:58	logportalauth	Zone: uspnet - USER LOGIN: lauans@rp.usp.br, , 172.16.79.229

Possível ataque DNS-rebind

Logout Search Config Help About

(Dados de Rede dos Gateways) (Relação de Gateways)

BACK TO SEARCH

Number of Entries Found: **26**

SEVERITY LEGEND

DEBUG INFO NOTICE WARNING ERROR CRIT ALERT EMERG

SEQ	HOST	FACILITY	DATE TIME	PROGRAM	MESSAGE
N/A	gw[redacted]	daemon	11:32:23	dnsmasq	possible DNS-rebind attack detected: www.seriesfree.co.cc
N/A	gw[redacted]	daemon	11:25:11	dnsmasq	possible DNS-rebind attack detected: ccs-pr-iaa.cloudapp.net
N/A	gw[redacted]	daemon	11:09:00	dnsmasq	possible DNS-rebind attack detected: ccs-pr-iaa.cloudapp.net
N/A	gw[redacted]	daemon	10:52:20	dnsmasq	possible DNS-rebind attack detected: ccs-pr-iaa.cloudapp.net
N/A	gw[redacted]	daemon	10:47:21	dnsmasq	possible DNS-rebind attack detected: smartsourcestaging.dell.com
N/A	gw[redacted]	daemon	10:41:59	dnsmasq	possible DNS-rebind attack detected: fbwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:41:59	dnsmasq	possible DNS-rebind attack detected: gwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: gwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: fbwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: gwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: fbwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: fbwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: gwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: fbwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	10:18:48	dnsmasq	possible DNS-rebind attack detected: gwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	09:53:54	dnsmasq	possible DNS-rebind attack detected: ccs-pr-iaa.cloudapp.net
N/A	gw[redacted]	daemon	09:44:25	dnsmasq	possible DNS-rebind attack detected: smartsourcestaging.dell.com
N/A	gw[redacted]	daemon	09:40:57	dnsmasq	possible DNS-rebind attack detected: smartsourcestaging.dell.com
N/A	gw[redacted]	daemon	09:37:30	dnsmasq	possible DNS-rebind attack detected: ccs-pr-iaa.cloudapp.net
N/A	gw[redacted]	daemon	09:31:14	dnsmasq	possible DNS-rebind attack detected: smartsourcestaging.dell.com
N/A	gw[redacted]	daemon	09:30:16	dnsmasq	possible DNS-rebind attack detected: dc-poisk.no-ip.org
N/A	gw[redacted]	daemon	09:22:58	dnsmasq	possible DNS-rebind attack detected: ccs-pr-iaa.cloudapp.net
N/A	gw[redacted]	daemon	09:17:11	dnsmasq	possible DNS-rebind attack detected: ccs-pr-iaa.cloudapp.net
N/A	gw[redacted]	daemon	09:00:13	dnsmasq	possible DNS-rebind attack detected: smartsourcestaging.dell.com
N/A	gw[redacted]	daemon	07:57:21	dnsmasq	possible DNS-rebind attack detected: fbwallcheck.api-alliance.com
N/A	gw[redacted]	daemon	07:57:21	dnsmasq	possible DNS-rebind attack detected: gwallcheck.api-alliance.com

Result Page: [1]

Executed in **0.61590313911438 seconds**

Servidores DNS com monitoramento DSC

Baseado em **Coletores e Apresentadores**

- Instalado em servidor DNS ou em servidor separado.
- **Coletores usam a biblioteca pcap como sniffer do tráfego de rede. Captura o tráfego bidirecional de servidores DNS.**
- **Captura estatísticas:**

Tipos de Queries, códigos de respostas,TLDs mais solicitadas, nomes populares de domínios, abusos de root IPv6, comprimento dos nomes das queries, tamanhos das respostas, etc.

- **Permite identificar:**

Queries excessivas, configurações, bugs em Softwares DNS, medida de tráfego (pacotes/bytes), e possivelmente problemas de roteamento.

Projeto : https://www.dns-oarc.net/oarc/data/dsc

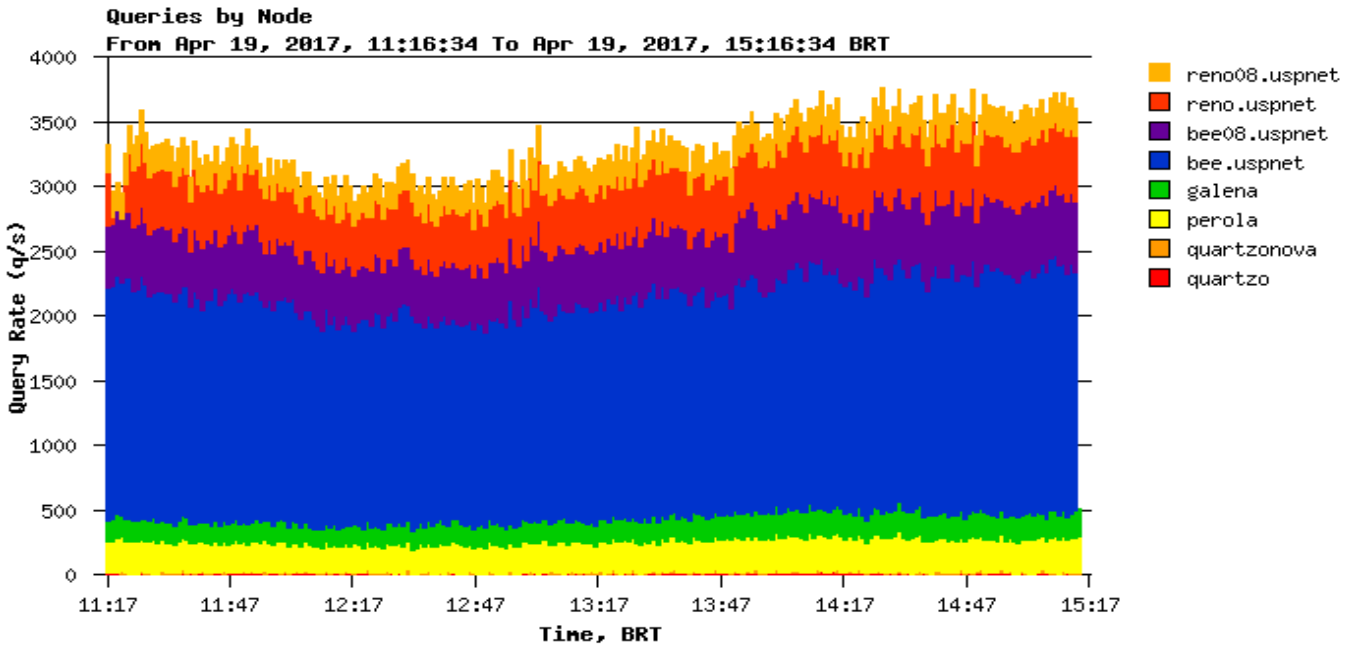
Servidores DNS com monitoramento DSC

Servers/Nodes

Server
› quartzo
› quartzonova
› perola
› galena
› bee.uspnet
› bee08.uspnet
› reno.uspnet
› reno08.uspnet

Plots

By Node
Qtypes
Rcodes
Classification
Client Geography
TLDs
2nd Level Domains
3rd Level Domains
Rcodes by Client Address
Popular Names
IPv6 root abusers
Opcodes
Query Attributes
Reply Attributes
CHAOS
IP Version
DNS Transport
IP Protocols
Qname Length
Reply Lengths
Source Ports
Priming Queries
Priming Responses



The **Queries by Node** plot shows the amount of queries coming from each node in the server cluster. If you would like to see the traffic for a single node, select the node name in the Servers/Nodes menu on the left.

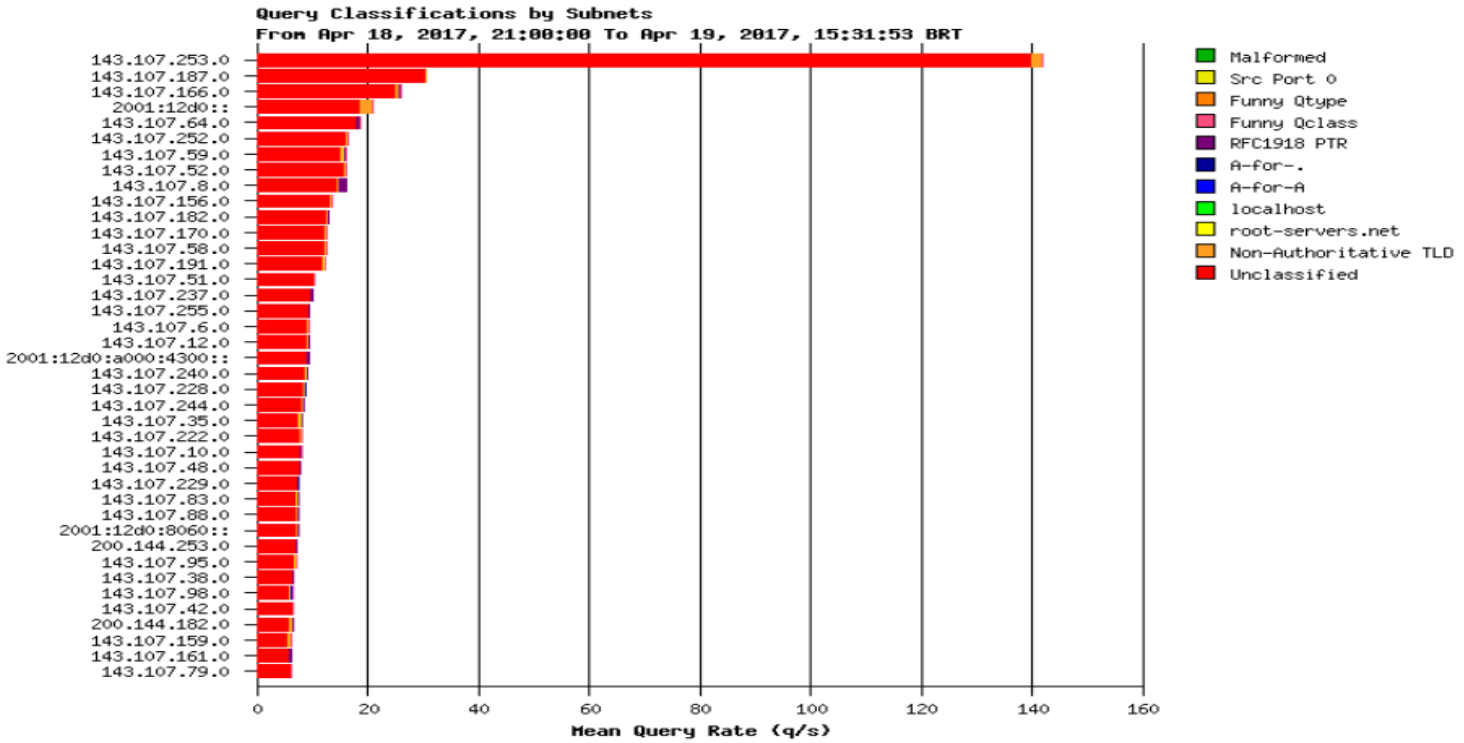
Note that the *By Node* option disappears from the Plots list when you are viewing the data for a single node. It reappears if you click on the Server name in the Servers/Nodes menu.

Servidores DNS com monitoramento DSC

Servers/Nodes
Server
› quartzo
› quartzonova
› perola
› galena
› bee.uspnet
› bee08.uspnet
› reno.uspnet
› reno08.uspnet

Plots
Qtypes
Rcodes
Classification
› trace
› count
Client Geography
TLDs
2nd Level Domains
3rd Level Domains
Rcodes by Client Address
Popular Names
IPv6 root abusers
Opcodes
Query Attributes
Reply Attributes
CHAOS
IP Version
DNS Transport
IP Protocols
Qname Length
Reply Lengths
Source Ports
Priming Queries
Priming Responses

Time Scale
1hour
2hour
4hour
6hour
8hour
10hour
12hour
1day
2days
3days
1week
2week
3week
4week



The **Query Classifications by Subnets** plot shows a kind of "quality report" for each /24 subnet. Queries are classified according to a number of known misbehaviors, shown in the legend:

- Malformed - The DNS message was malformed and could not be entirely parsed
- Src port 0 - The UDP query came from source port 0
- Funny Qtype - Query type was not one of the documented types
- Funny Qclass - Query class was not IN
- RFC1918PTR - The query type was PTR and the name was in an in-addr.arpa zone covered by RFC1918 private address space
- A-for-. - The query name was empty (equal to the root zone)
- A-for-A - The query name was already an IPv4 address
- localhost - The query was for localhost
- root-servers.net - The query was for a root-servers.net name
- Non-Authoritative TLD - The query was for a known-invalid TLD
- Unclassified - the query did not fall into one of the other categories.

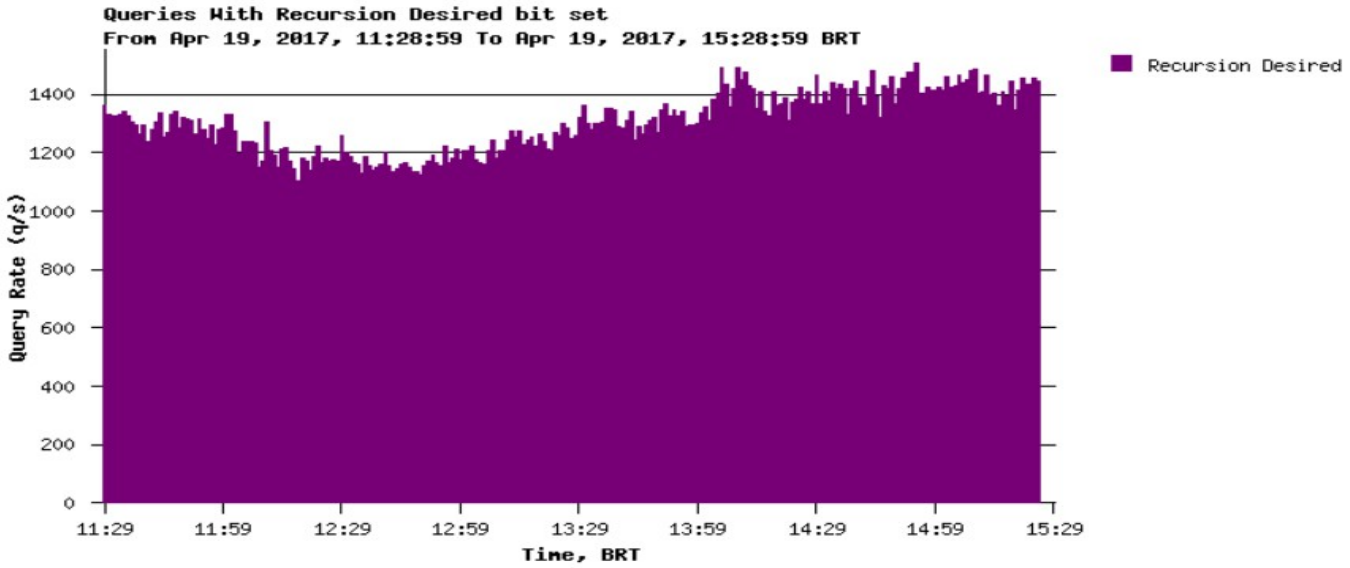
Servidores DNS com monitoramento DSC

Servers/Nodes

Server
› quartzo
› quartzonova
› perola
› galena
› bee.uspnet
› bee08.uspnet
› reno.uspnet
› reno08.uspnet

Plots

Qtypes
Rcodes
Classification
Client Geography
TLDs
2nd Level Domains
3rd Level Domains
Rcodes by Client Address
Popular Names
IPv6 root abusers
Opcodes
Query Attributes
› IDN Qnames
› RD bit
› DO bit
› QR and AA bits
› EDNS version
› EDNS buffer size
Reply Attributes
CHAOS
IP Version
DNS Transport
IP Protocols
Qname Length
Reply Lengths
Source Ports
Priming Queries
Priming Responses



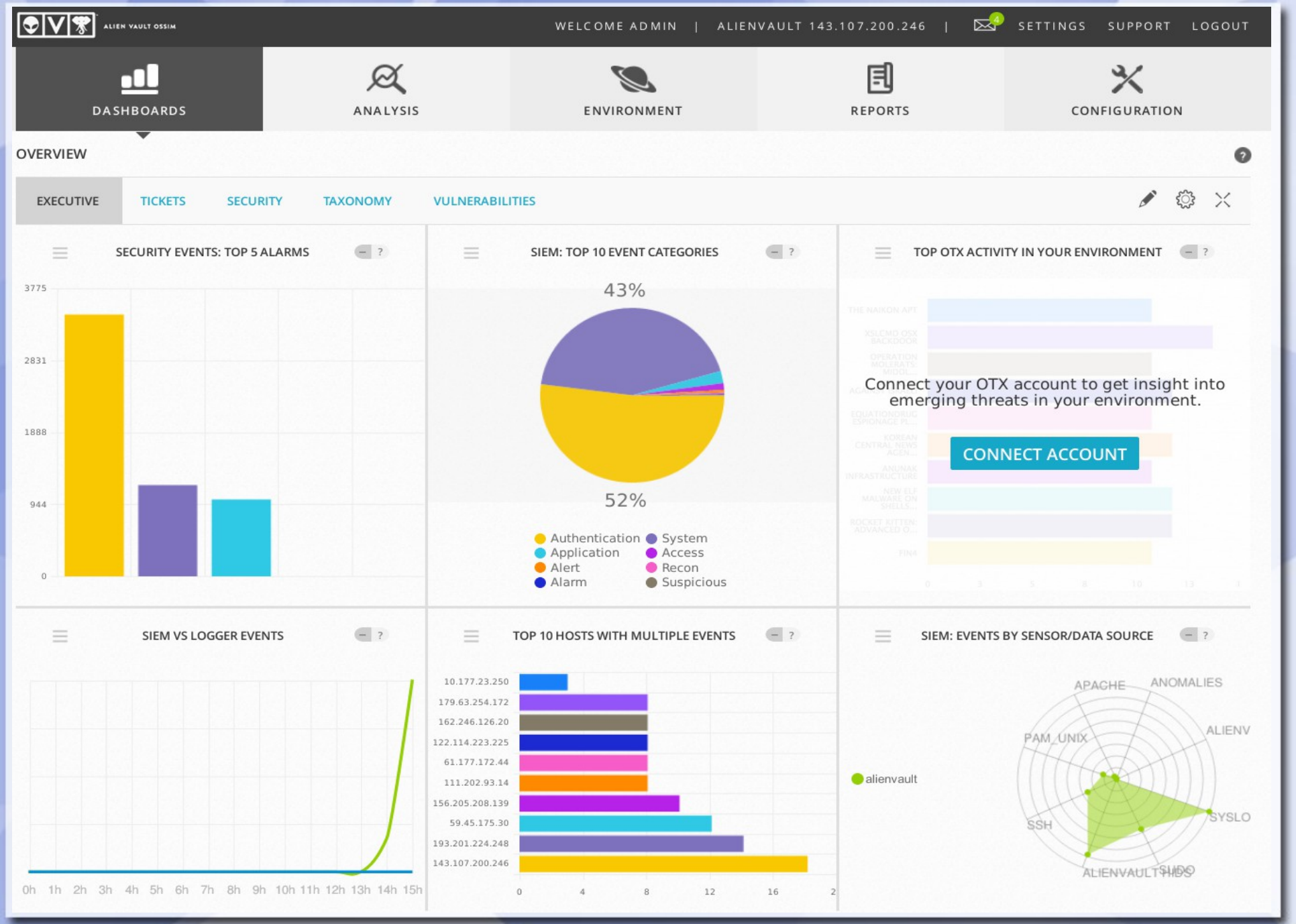
AlienVault OSSIM

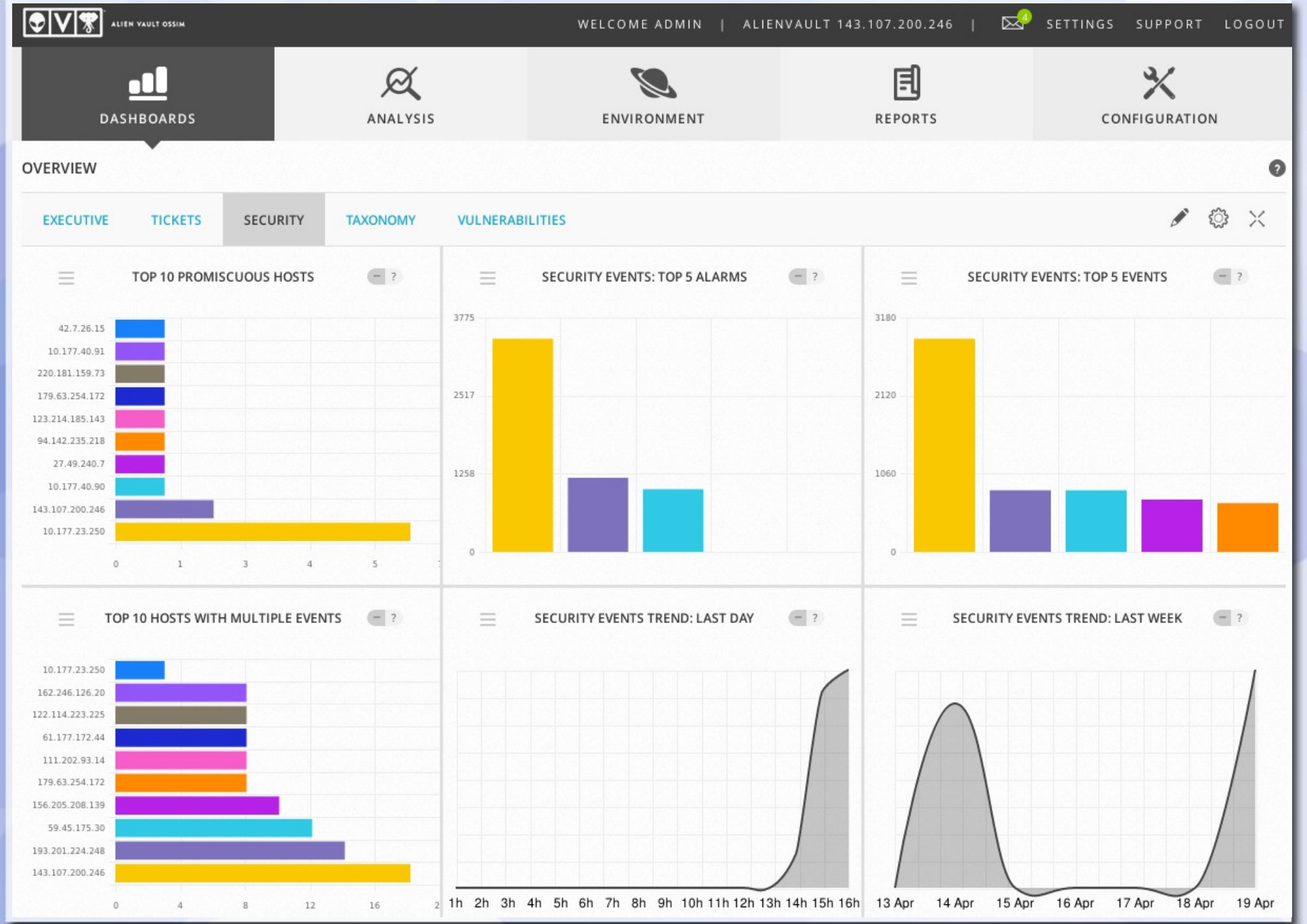
OSSIM (AlienVault's Open Source Security Information) e Event Management (SIEM)

- Coleta de eventos, normalização e correlação.

Funcionalidades mais avançadas: **AlienVault Unified Security Management (USM)** , com OSSIM:

- Gerenciamento de Logs.
- Tarefas de detecção e constante atualização de bibliotecas de correlações pré fabricadas,
- Atualização inteligente a partir de AlienVault Labs Security Research Team.
- Painéis de análise e visualização de dados.
- **Detecção de intrusão com IDS e HIDS.**
- Live demo: www.alienvault.com/live-demo-site


ALIEN VAULT OSSIM
WELCOME ADMIN | ALIENVAULT 143.107.200.246 |
SETTINGS SUPPORT LOGOUT
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
OVERVIEW
EXECUTIVE
TICKETS
SECURITY
TAXONOMY
VULNERABILITIES
SECURITY EVENTS: TOP 5 ALARMS
3775
2831
1888
944
0
SIEM: TOP 10 EVENT CATEGORIES
43%
52%
Authentication
System
Application
Access
Alert
Recon
Alarm
Suspicious
TOP OTX ACTIVITY IN YOUR ENVIRONMENT
Connect your OTX account to get insight into emerging threats in your environment.
CONNECT ACCOUNT
SIEM VS LOGGER EVENTS
0h 1h 2h 3h 4h 5h 6h 7h 8h 9h 10h 11h 12h 13h 14h 15h
TOP 10 HOSTS WITH MULTIPLE EVENTS
10.177.23.250
179.63.254.172
162.246.126.20
122.114.223.225
61.177.172.44
111.202.93.14
156.205.208.139
59.45.175.30
193.201.224.248
143.107.200.246
0
4
8
12
16
SIEM: EVENTS BY SENSOR/DATA SOURCE
alienvault
APACHE
ANOMALIES
ALIENV
PAM_UNIX
SYSLO
SSH
ALIENVAULTHIDS


ALIEN VAULT OSSIM
WELCOME ADMIN | ALIENVAULT 143.107.200.246 | SETTINGS SUPPORT LOGOUT
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
OVERVIEW
EXECUTIVE
TICKETS
SECURITY
TAXONOMY
VULNERABILITIES
TOP 10 PROMISCUOUS HOSTS
42.7.26.15
10.177.40.91
220.181.159.73
179.63.254.172
123.214.185.143
94.142.235.218
27.49.240.7
10.177.40.90
143.107.200.246
10.177.23.250
0 1 3 4 5
SECURITY EVENTS: TOP 5 ALARMS
3775
2517
1258
0
SECURITY EVENTS: TOP 5 EVENTS
3180
2120
1060
0
TOP 10 HOSTS WITH MULTIPLE EVENTS
10.177.23.250
162.246.126.20
122.114.223.225
61.177.172.44
111.202.93.14
179.63.254.172
156.205.208.139
59.45.175.30
193.201.224.248
143.107.200.246
0 4 8 12 16
SECURITY EVENTS TREND: LAST DAY
1h 2h 3h 4h 5h 6h 7h 8h 9h 10h 11h 12h 13h 14h 15h 16h
SECURITY EVENTS TREND: LAST WEEK
13 Apr 14 Apr 15 Apr 16 Apr 17 Apr 18 Apr 19 Apr

ALIEN VAULT OSSIM

WELCOME ADMIN | ALIENVAULT 143.107.200.246 | 4 SETTINGS SUPPORT LOGOUT

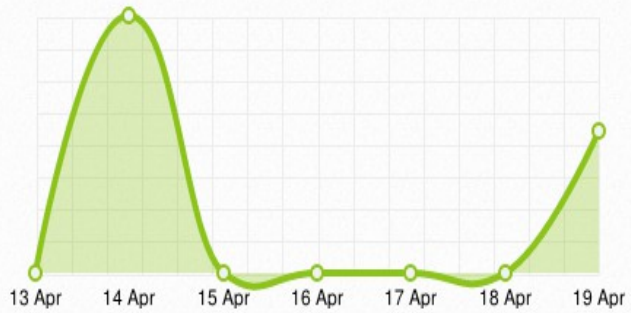
DASHBOARDS | ANALYSIS | ENVIRONMENT | REPORTS | CONFIGURATION

DETECTION

HIDS | WIRELESS IDS

OVERVIEW | AGENTS | AGENTLESS | EDIT RULES | CONFIG | HIDS CONTROL

HIDS EVENTS TREND



HIDS DATA SOURCES

Search

AGENT INFORMATION

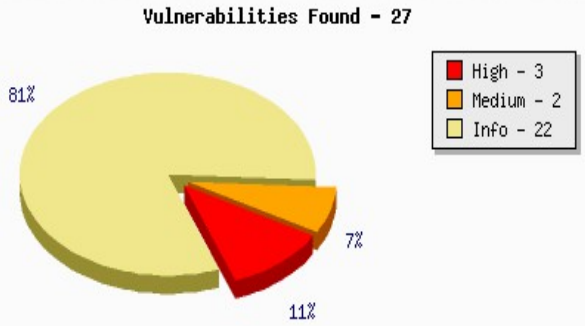
ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	TREND [TIME UTC]
000	alienvault (server)	iolita	127.0.0.1	127.0.0.1	-	Active/local	13 Apr 14 Apr 15 Apr 16 Apr 17 Apr 18 Apr 19 Apr

SHOWING 1 TO 1 OF 1 AGENTS

FIRST PREVIOUS 1 NEXT LAST

VULNERABILITIES

OVERVIEW | SCAN JOBS | THREAT DATABASE



SUMMARY OF SCANNED HOSTS

HOST	HOSTNAME	Serious	High	Medium	Low	Info
10.177.40.84	Host-10-177-40-84	-	3	2	-	22

☐ View false positives

✓ - True result ✗ - False positive result ⓘ - Additional information is available

10.177.40.84 - Host-10-177-40-84

REPORTED PORTS	
80/tcp	135/tcp
139/tcp	445/tcp
1801/tcp	3389/tcp

Scans via Shadow Server

Objetivos:

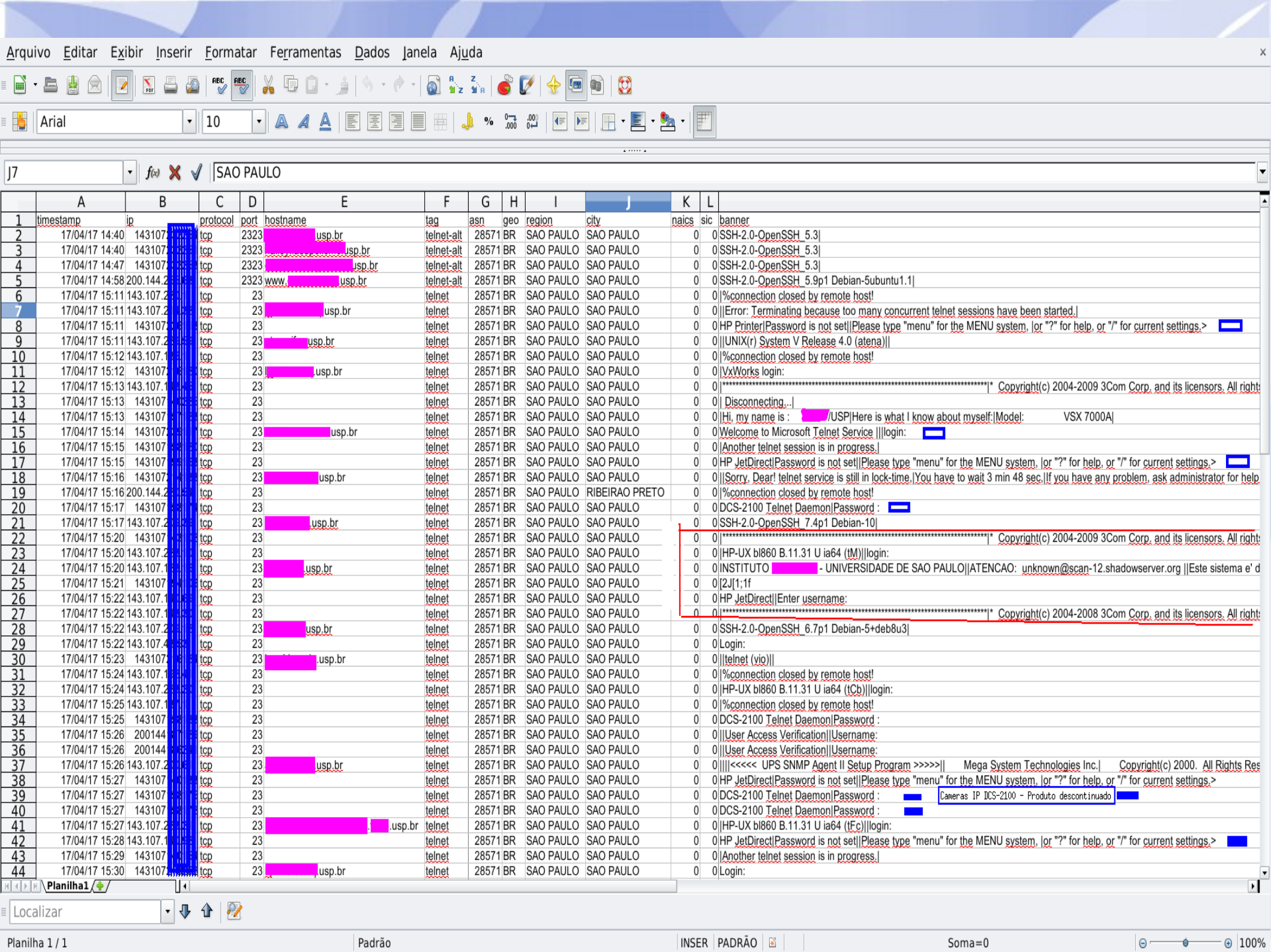
Relatórios de varredura autorizada na rede USPnet

Serviços scaneados:

blacklist, compromised_website, dns_openresolver, chargen, cwmp, elasticsearch, ipmi, ldap, mdns, memcached, mongodb, mssql, nat_pmp, netbios, ntp, portmapper, scan_qotd, scan_rdp, ssdp, ssl_poodle, telnet, tftp, vnc, xdmcp, sinkhole_http_drone, botnet_drone

Dados obtidos:

Timestamp, ip, protocol, port, hostname, asn, geo, region, city,...,..., product, banner,...,...



Arquivo Editar Exibir Inserir Formatar Ferramentas Dados Janela Ajuda

Arial 10

J7 SAO PAULO

	A	B	C	D	E	F	G	H	I	J	K	L
1	timestamp	ip	protocol	port	hostname	tag	asn	geo	region	city	naics	sic
2	17/04/17 14:40	143107	tcp	2323	usp.br	telnet-alt	28571	BR	SAO PAULO	SAO PAULO	0	0
3	17/04/17 14:40	143107	tcp	2323	usp.br	telnet-alt	28571	BR	SAO PAULO	SAO PAULO	0	0
4	17/04/17 14:47	143107	tcp	2323	usp.br	telnet-alt	28571	BR	SAO PAULO	SAO PAULO	0	0
5	17/04/17 14:58	200.144.2	tcp	2323	www. usp.br	telnet-alt	28571	BR	SAO PAULO	SAO PAULO	0	0
6	17/04/17 15:11	143.107.2	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
7	17/04/17 15:11	143.107.2	tcp	23	usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
8	17/04/17 15:11	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
9	17/04/17 15:11	143.107.2	tcp	23	usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
10	17/04/17 15:12	143.107.1	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
11	17/04/17 15:12	143107	tcp	23	.usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
12	17/04/17 15:13	143.107.1	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
13	17/04/17 15:13	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
14	17/04/17 15:13	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
15	17/04/17 15:14	143107	tcp	23	usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
16	17/04/17 15:15	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
17	17/04/17 15:15	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
18	17/04/17 15:16	143107	tcp	23	usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
19	17/04/17 15:16	200.144.2	tcp	23		telnet	28571	BR	SAO PAULO	RIBEIRAO PRETO	0	0
20	17/04/17 15:17	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
21	17/04/17 15:17	143.107.2	tcp	23	.usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
22	17/04/17 15:20	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
23	17/04/17 15:20	143.107.2	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
24	17/04/17 15:20	143.107.1	tcp	23	.usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
25	17/04/17 15:21	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
26	17/04/17 15:22	143.107.1	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
27	17/04/17 15:22	143.107.1	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
28	17/04/17 15:22	143.107.2	tcp	23	usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
29	17/04/17 15:22	143.107.4	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
30	17/04/17 15:23	143107	tcp	23	.usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
31	17/04/17 15:24	143.107.1	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
32	17/04/17 15:24	143.107.2	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
33	17/04/17 15:25	143.107.1	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
34	17/04/17 15:25	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
35	17/04/17 15:26	200144	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
36	17/04/17 15:26	200144	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
37	17/04/17 15:26	143.107.2	tcp	23	.usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
38	17/04/17 15:27	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
39	17/04/17 15:27	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
40	17/04/17 15:27	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
41	17/04/17 15:27	143.107.2	tcp	23	.usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
42	17/04/17 15:28	143.107.1	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
43	17/04/17 15:29	143107	tcp	23		telnet	28571	BR	SAO PAULO	SAO PAULO	0	0
44	17/04/17 15:30	143107	tcp	23	usp.br	telnet	28571	BR	SAO PAULO	SAO PAULO	0	0

	banner
2	SSH-2.0-OpenSSH_5.3|
3	SSH-2.0-OpenSSH_5.3|
4	SSH-2.0-OpenSSH_5.3|
5	SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1|
6	|%connection closed by remote host!
7	||Error: Terminating because too many concurrent telnet sessions have been started.|
8	HP Printer|Password is not set||Please type "menu" for the MENU system, |or "?" for help, or "/" for current settings.>
9	||UNIX(r) System V Release 4.0 (atena)||
10	|%connection closed by remote host!
11	|VxWorks login:
12	|**********|* Copyright(c) 2004-2009 3Com Corp. and its licensors. All right
13	| Disconnecting...|
14	Hi, my name is : /USP|Here is what I know about myself:|Model: VSX 7000A|
15	Welcome to Microsoft Telnet Service |||login:
16	|Another telnet session is in progress.|
17	HP JetDirect|Password is not set||Please type "menu" for the MENU system, |or "?" for help, or "/" for current settings.>
18	||Sorry, Dear! telnet service is still in lock-time.|You have to wait 3 min 48 sec.|If you have any problem, ask administrator for help
19	|%connection closed by remote host!
20	DCS-2100 Telnet Daemon|Password :
21	SSH-2.0-OpenSSH_7.4p1 Debian-10|
22	|**********|* Copyright(c) 2004-2009 3Com Corp. and its licensors. All right
23	|HP-UX bl860 B.11.31 U ia64 (tM)||login:
24	INSTITUTO - UNIVERSIDADE DE SAO PAULO||ATENCAO: unknown@scan-12.shadowserver.org ||Este sistema e' d
25	|2J[1;1f
26	HP JetDirect||Enter username:
27	|**********|* Copyright(c) 2004-2008 3Com Corp. and its licensors. All right
28	SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3|
29	Login:
30	||telnet (vio)||
31	|%connection closed by remote host!
32	|HP-UX bl860 B.11.31 U ia64 (tCb)||login:
33	|%connection closed by remote host!
34	DCS-2100 Telnet Daemon|Password :
35	||User Access Verification||Username:
36	||User Access Verification||Username:
37	||||<<<<< UPS SNMP Agent II Setup Program >>>>>|| Mega System Technologies Inc.| Copyright(c) 2000. All Rights Res
38	HP JetDirect|Password is not set||Please type "menu" for the MENU system, |or "?" for help, or "/" for current settings.>
39	DCS-2100 Telnet Daemon|Password : Cameras IP DCS-2100 - Produto descontinuado
40	DCS-2100 Telnet Daemon|Password :
41	|HP-UX bl860 B.11.31 U ia64 (tFc)||login:
42	HP JetDirect|Password is not set||Please type "menu" for the MENU system, |or "?" for help, or "/" for current settings.>
43	|Another telnet session is in progress.|
44	Login:

Planilha1

Localizar

Planilha 1 / 1 Padrão INSER PADRÃO Soma=0 100%

Scans via Shadow Server

Protocolos de amplificação: (Fator de amplificação de banda)

- BitTorrent (any) **3.8**, CharGEN (UDP/19) **358.8**
- DNS (UDP/53) (Open Resolver Project) **28~54**
- Kad (UDP/6429) **16.3**, MS-SQL (UDP/1434)
- NetBIOS (UDP 137 to 139) **3.8**
- NTP Mode 6 (UDP/123) (Open NTP Project) **556.9**
- NTP Mode 7 (UDP/123)
- QOTD (UDP/17) **140.3**
- Quake Network Protocol (UDP/26000 and UDP/27960) **63.9**
- SNMPv2 (UDP/161) (Open SNMP Project) **6.3**
- SDP (UDP/1900) (Open SSDP Project) **30.8**
- Steam Protocol (Many – UDP/27015) **5.5**

Scans via Shadow Server

Protocolos que não deveriam estar expostos:

- CWMP (TCP/7547), DB2 (UDP/523), Elastic Search (TCP/9200)
- HDFS (TCP/50070, TCP/50075, TCP/50090, TCP/50105, TCP/50030, TCP/50060)
- **IPMI (UDP/623), LDAP (UDP/389), mDNS (UDP/5353)**
- MemCached (TCP/11211)
- **MongoDB (TCP/27017, TCP/27018, TCP/27019, TCP/28017)**
- NAT-PMP (UDP/5351), **NetBIOS (TCP/137 to 139)**
- **Portmapper (UDP/111), REDIS (TCP/6379)**
- **RDP (TCP/3389 and UDP/3389), VNC (TCP/5900), XDMCP (UDP/177)**
- **rlogin (TCP/513), SSDP (TCP/1900)**
- **TFTP (UDP/69), Telnet (TCP/23), Telnet, Alternative (TCP/2323)**

Scans via Shadow Server

Protocolos vulneráveis:

- ISAKMP (UDP/500)
- Netcore/Netis Router (UDP/53413)
- SSL/FREAK (TCP/443)
- SSLv3 (TCP/443)
- Synful Knock (TCP/80)

Protocolos Botnet:

- Conficker (TCP/445)
- Gameover Zeus (Takedown by the FBI on 2014-05-30)
- Sality
- Zeroaccess

Projeto Honeypots – CERT.BR

Objetivos:

Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro.

Atividades:

Rede distribuída de **honeypots** de baixa interatividade (utilizando **Honeyd**), cobrindo uma quantidade razoável do espaço de endereços IPv4 da Internet no Brasil.

Notificação diária aos grupos de tratamento de incidentes (**CSIRTs**) das redes responsáveis por originar ataques aos **honeypots.**

Estatísticas:

- Gráficos diários dos fluxos de rede do tráfego direcionado a todos os **honeypots.**
- Sumário do tráfego TCP e UDP direcionado aos **honeypots** e tendências.

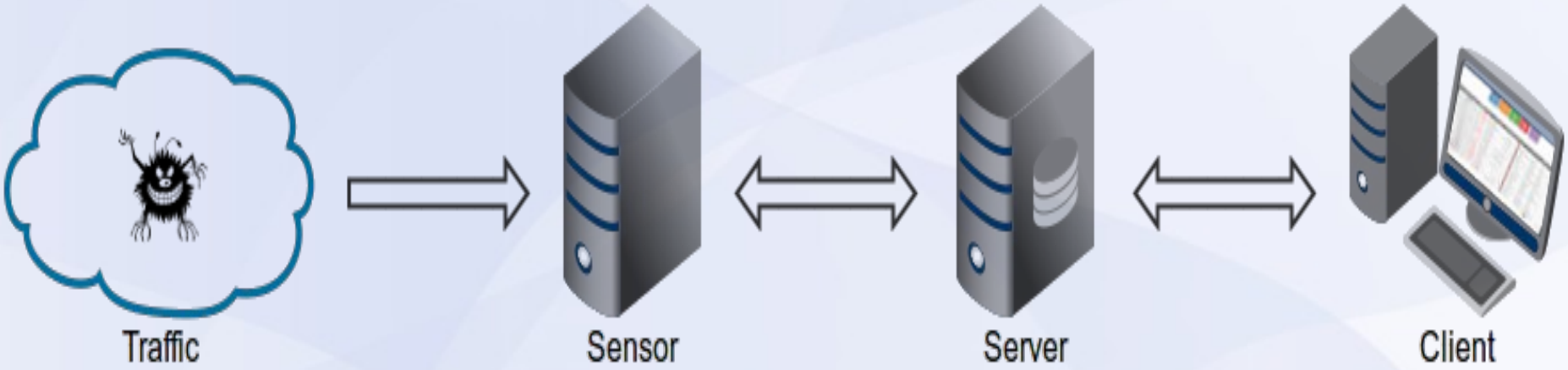
Maltrail

- Software para detectar tráfego de atividades maliciosas. Feito em linguagem Python.
- Utiliza registros de fontes suspeitas presentes em listas negras.
- Estatísticas de várias fontes de Anti Vírus e listas customizadas.
- Busca por Malwares conhecidos, programas maliciosos, padrões de ataques a servidores HTTP, SQL injections, etc.
- Mecanismo de busca heurística para ameaças desconhecidas, novos Malwares, etc.

Maltrail

- Arquitetura

  Traffic -> Sensor <-> Server <-> Client



Arquitetura do Maltrail

- Um equipamento com Linux conectado passivamente a uma porta SPAN ou porta espelhada, ou bridge transparente.
- Ou um equipamento Honeypot que vai monitorar o tráfego em busca de items presentes nas listas negras.
- Logs podem ser armazenados no Servidor ou no Sensor.
- Opção de armazena Logs no servidor de Logs via UDP.
- Dados são armazenados diariamente e apresentados ao cliente via interface WEB.
- Logs também podem ser armazenados em formato CSV.
- Utiliza linguagem **Python** e biblioteca **python-pcapy**
- Arquivo de configuração bastante simplificado.

25 threats per page

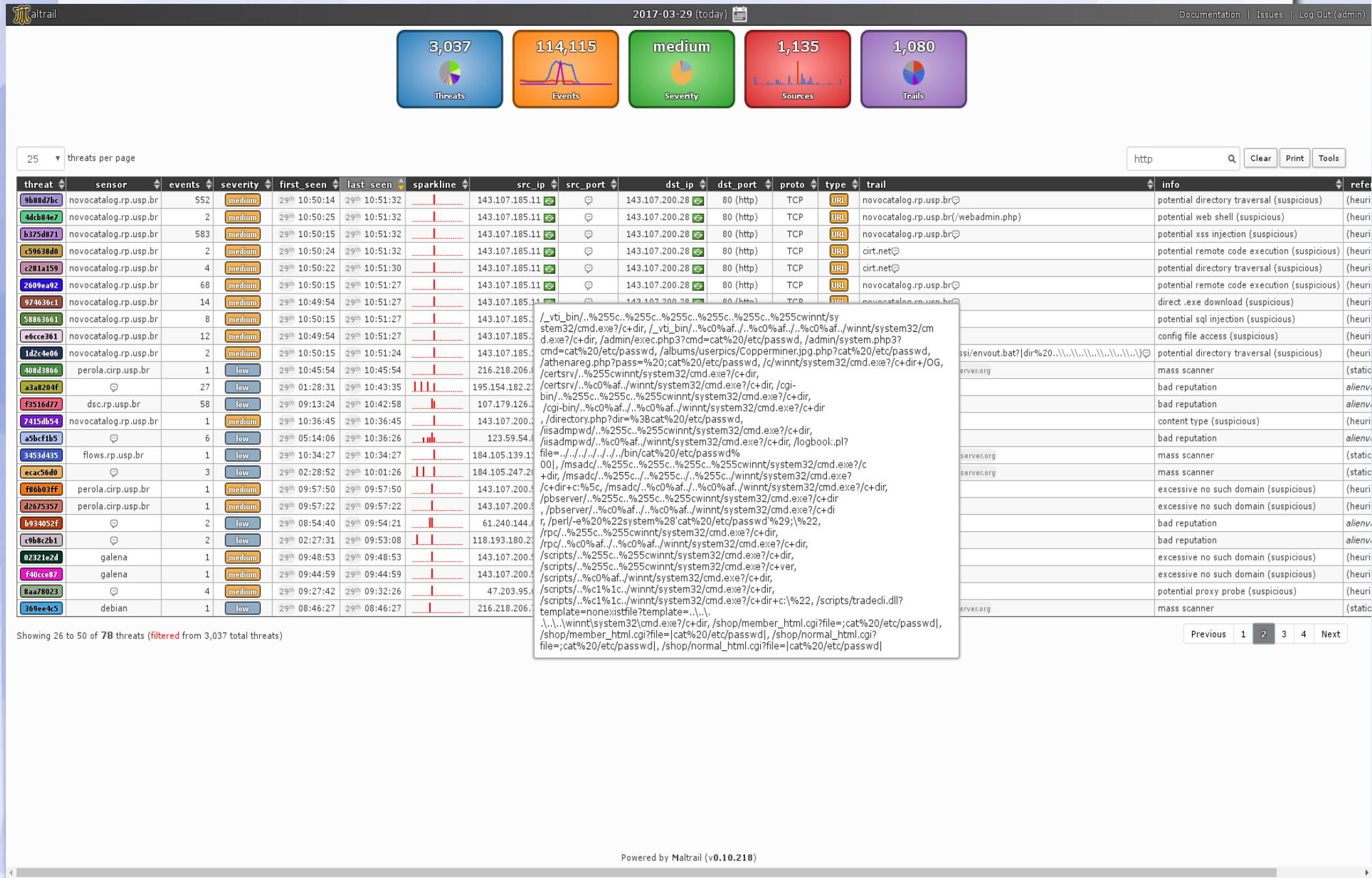
Filter Clear Print Tools

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
5d56b050	debian	390	low	29th 06:44:17	29th 11:12:09		61.177.172.46		143.107.185.13	22 (ssh)	TCP	IP	61.177.172.46	known attacker	*blocklist.de* +2	
47049a2f	debian	116	low	29th 10:32:29	29th 11:12:08		61.177.172.28		143.107.185.13	22 (ssh)	TCP	IP	61.177.172.28	known attacker	*blocklist.de* +3	
3c16e90a	debian	11	low	29th 00:18:02	29th 11:11:40		91.223.133.13				TCP	IP	91.223.133.13	bad reputation	*alienvault.com*	
6be378be	debian	1	low	29th 11:08:26	29th 11:08:26		93.103.179.52		143.107.185.13	22 (ssh)	TCP	IP	93.103.179.52	known attacker	*badips.com* +4	
fd10c3df	debian	1	low	29th 11:05:32	29th 11:05:32		104.243.44.187	59962	143.107.185.13	1900 (upnp)	UDP	IP	104.243.44.187 choopa	bad reputation	*alienvault.com*	
09b13495	debian	1	low	29th 11:01:16	29th 11:01:16		195.154.181.172	19784	143.107.185.13	88 (kerberos)	TCP	IP	195.154.181.172	known attacker	*voipbl.org*	
43a32656	debian	2	low	29th 09:31:39	29th 10:57:03		139.162.86.84			8001	TCP	IP	139.162.86.84	bad reputation	*alienvault.com* +1	
fa931f20	debian	1	low	29th 10:56:32	29th 10:56:32		137.226.113.7	42143	143.107.185.13	80 (http)	TCP	IP	137.226.113.7 comsys.rwth-aachen.de	mass scanner	(static) +1	
faa569ca	debian	1	low	29th 10:50:20	29th 10:50:20		71.6.158.166	58022	143.107.185.13	5555 (rplay)	TCP	IP	71.6.158.166 cari.net	mass scanner	(static) +4	
ae767ee3	debian	1	low	29th 10:44:48	29th 10:44:48		139.162.122.110		143.107.185.13	22 (ssh)	TCP	IP	139.162.122.110	known attacker	*blocklist.de* +2	
9fe57240	debian	1	low	29th 10:44:47	29th 10:44:47		139.162.120.98	60700	143.107.185.13	22 (ssh)	TCP	IP	139.162.120.98	known attacker	*packetmail.net*	
f22da551	debian	11	low	29th 01:00:43	29th 10:38:59		163.172.91.161			5060 (sip)	UDP	IP	163.172.91.161	bad reputation	*alienvault.com* +1	
024c789e	debian	5	low	29th 00:14:23	29th 10:34:54		80.82.77.139					IP	80.82.77.139	bad reputation	*alienvault.com* +3	
81ede6fe	debian	1	low	29th 10:32:41	29th 10:32:41		114.241.51.51		143.107.185.13	22 (ssh)	TCP	IP	114.241.51.51	known attacker	*blocklist.de* +1	
11db2c0f	debian	1	low	29th 10:24:20	29th 10:24:20		183.214.141.100	54065	143.107.185.13	22 (ssh)	TCP	IP	183.214.141.100	known attacker	*openbl.org*	
2fc4ad82	debian	3	low	29th 01:35:45	29th 10:20:45		185.94.111.1		143.107.185.13		UDP	IP	185.94.111.1	known attacker	*blocklist.de*	
edbaf3d6	debian	1	low	29th 10:20:45	29th 10:20:45		143.107.185.13	111 (sunrpc)	185.94.111.1	46352	UDP	IP	185.94.111.1	known attacker	*blocklist.de*	
238faa5d	debian	1	low	29th 10:17:43	29th 10:17:43		74.82.47.52	37943	143.107.185.13	5900 (vnc)	TCP	IP	74.82.47.52 shadowserver.org	mass scanner	(static) +1	
71f1a6e8	debian	1	low	29th 10:13:07	29th 10:13:07		176.58.124.35	53294	143.107.185.13	21 (ftp)	TCP	IP	176.58.124.35 linode	known attacker	*packetmail.net*	
79fca742	debian	1	low	29th 10:11:12	29th 10:11:12		84.54.160.160	2913	143.107.185.13	2323	TCP	IP	84.54.160.160	bad reputation	*alienvault.com*	
db8cff8c	debian	30	low	29th 10:00:43	29th 10:05:37		193.201.224.248		143.107.185.13	22 (ssh)	TCP	IP	193.201.224.248 prohoster.info	known attacker	*blocklist.de* +5	
a5368320	debian	1	low	29th 09:55:23	29th 09:55:23		115.209.63.224		143.107.185.13	22 (ssh)	TCP	IP	115.209.63.224	known attacker	*blocklist.de* +1	
08f63339	debian	1	low	29th 09:51:25	29th 09:51:25		47.222.158.25		143.107.185.13	22 (ssh)	TCP	IP	47.222.158.25	known attacker	*blocklist.de*	
2b6714d9	debian	1	low	29th 09:49:57	29th 09:49:57		121.55.89.115	28683	143.107.185.13	1900 (upnp)	UDP	IP	121.55.89.115	bad reputation	*alienvault.com*	
f9ac1f1e	debian	1	low	29th 09:33:19	29th 09:33:19		123.115.51.110	56800	143.107.185.13	22 (ssh)	TCP	IP	123.115.51.110	known attacker	*blocklist.de* +3	

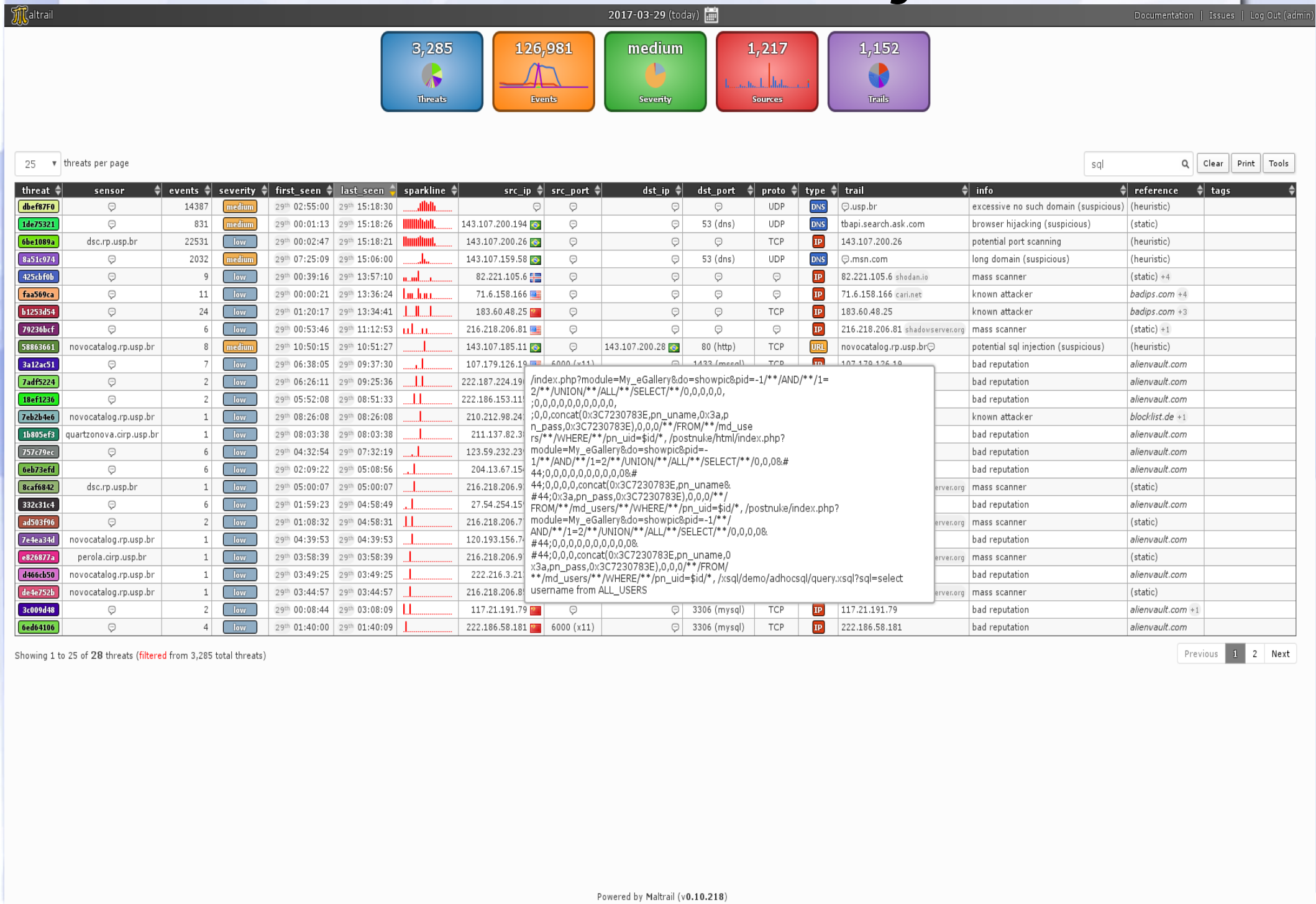
Showing 1 to 25 of 142 threats

Previous 1 2 3 4 5 6 Next

Identificando HTTP suspeito



Identificando SQL Injection



FIM

- Perguntas
- Sugestões
- Dúvidas

?

USP SUPERINTENDÊNCIA Tecnologia da Informação

Flows e Nfsen

Iniciativa Unicamp/Cert.BR

Também adotado na USP: CeTI-SP e CeTI-RP

Objetivos:

Uso de flows no tratamento de Incidentes de Segurança.

Recurso disponível nos roteadores

Amostra de fluxo de dados (1/512)

Coletar o tráfego nos roteadores

Protocolo utilizado: SFLOW (coleta por amostragem)

Baixo impacto na performance dos roteadores e do cliente

Relatórios Flows

Relatórios por E-Mail:

Scripts que relacionam os dados coletados e produzem os seguintes relatórios:

- R**eport-DNS -** Dados relacionados a amplificação de DNS
- **Report-top-rdp-talkers -** Dados relacionados a uso de porta RDP - Remote Desktop
- **Report-top-submission -** Dados relacionados ao tráfego de SMTP
- **Report-amp** - Amplificadores (DNS, SSDP, NTP, SNMP, Chargen)
- **Report-drop -** IPs vistos na lista DROP (eDROP) da Spamhaus (Projetos Drop e eDrop - Spamhaus)

Relatórios Flows

Report-top-SMTP-talkers - Dados relacionados ao uso de SMTP

Report-top-talkers - Os que mais consomem banda

Report-botcc - Dados de IPs encontrados em Botnets.

Projeto botnet-cc - The World's Worst Botnet Countries - Spamhaus

top-seen.honeypot - Dados de IPs encontrados no projeto Honeypot (não apresenta dados atualmente)

Habilitado em Roteadores do CeTI-SP, do CeTI-RP e em Gateways PFSense da Wireless USPnet - RP. **Software Softflow**

Instalação de Flows e SNMP em servidores e Desktops.

Monitoramento de servidores via SNMP

Objetivos:

Monitorar recursos de Servidores, Desktops, No-breaks, Impressoras, etc, via SNMP.

Elementos e serviços de Rede, CPU, Memórias, utilização dos recursos, gráficos estatísticos.

Softwares Observium e LibreNMS

Material didático

- Entendendo a ISO 17799

granito2.rp.usp.br/NBR17799/

- Ferramentas de Segurança

granito2.cirp.usp.br/Ferramentas.de.Seguranca/geral.html

- Site Security Handbook

penta.ufrgs.br/gereseg/rfc2196/