jornadas FCCN

Quando os repositórios são alvo:

Ataques e medidas de proteção

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

CVE-2024-56525 2025-02-24 MITRE

In Public Knowledge Project (PKP) OJS, OMP, and OPS before 3.3.0.21 and 3.4.x before 3.4.0.8, an XXE attack by the Journal Editor Role can create a new role as super admin in the journal context, and insert a backdoor plugin, by uploading a crafted XML document as a User XML Plugin.

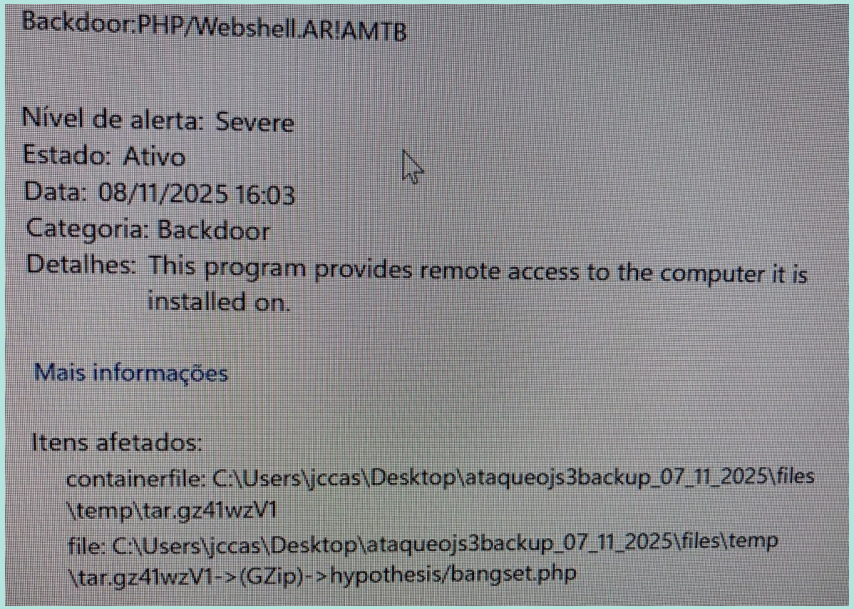
SFU.CA

SFU PKP PUBLIC KNOWLEDGE PROJECT

https://pkp.sfu.ca/software/ojs/download/

7 de Nov 2025
USI é contactada pelo administrador do serviço https://journalsojs3.fe.up.pt/ com suspeitas de intrusão. A equipa teria detetado comportamentos estranhos ao interagir com o sistema.
Ao analisar o serviço detetou-se a vulnerabilidade: https://nvd.nist.gov/vuln/detail/CVE-2024-56525

plugin malicioso : hypothesis
reverse shell php: bangset.php



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

Como medida de proteção foi movido o site journalojs3.fe.up.pt para o “umbrella” da cloudflare, enquanto se recupera serviço.

Foram identificadas referencias online para o serviço comprometido:

Foi identificado o problema no código e foi possível mitigar o risco noutro site https://ojs.up.pt, sem necessidade de upgrade direto: https://github.com/pkp/pkp-lib/commit/17b6634841c3743f656d4ea550e54545abc9eea5

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

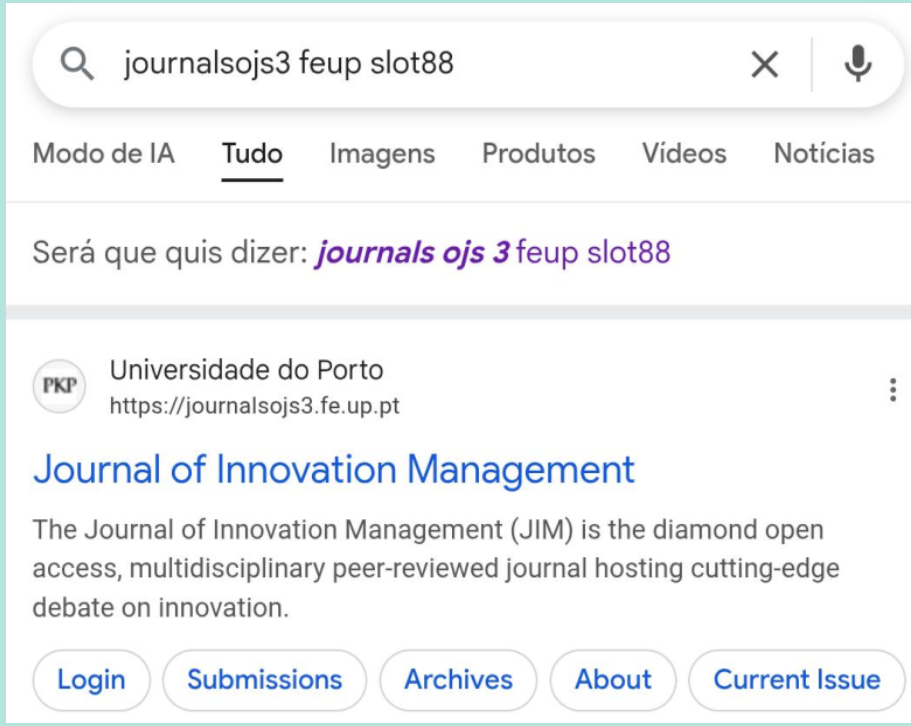
11 Nov 2025

Em conjunto com a UAS e o Administrador do OJS foi reposto o backup e configurado o serviço com reset a passwords dos utilizadores.

12 Nov 2025

Sistema reposto, atualizado e validado. Utilizadores notificados para alteração de password mandatória.

Referencias online removidas!



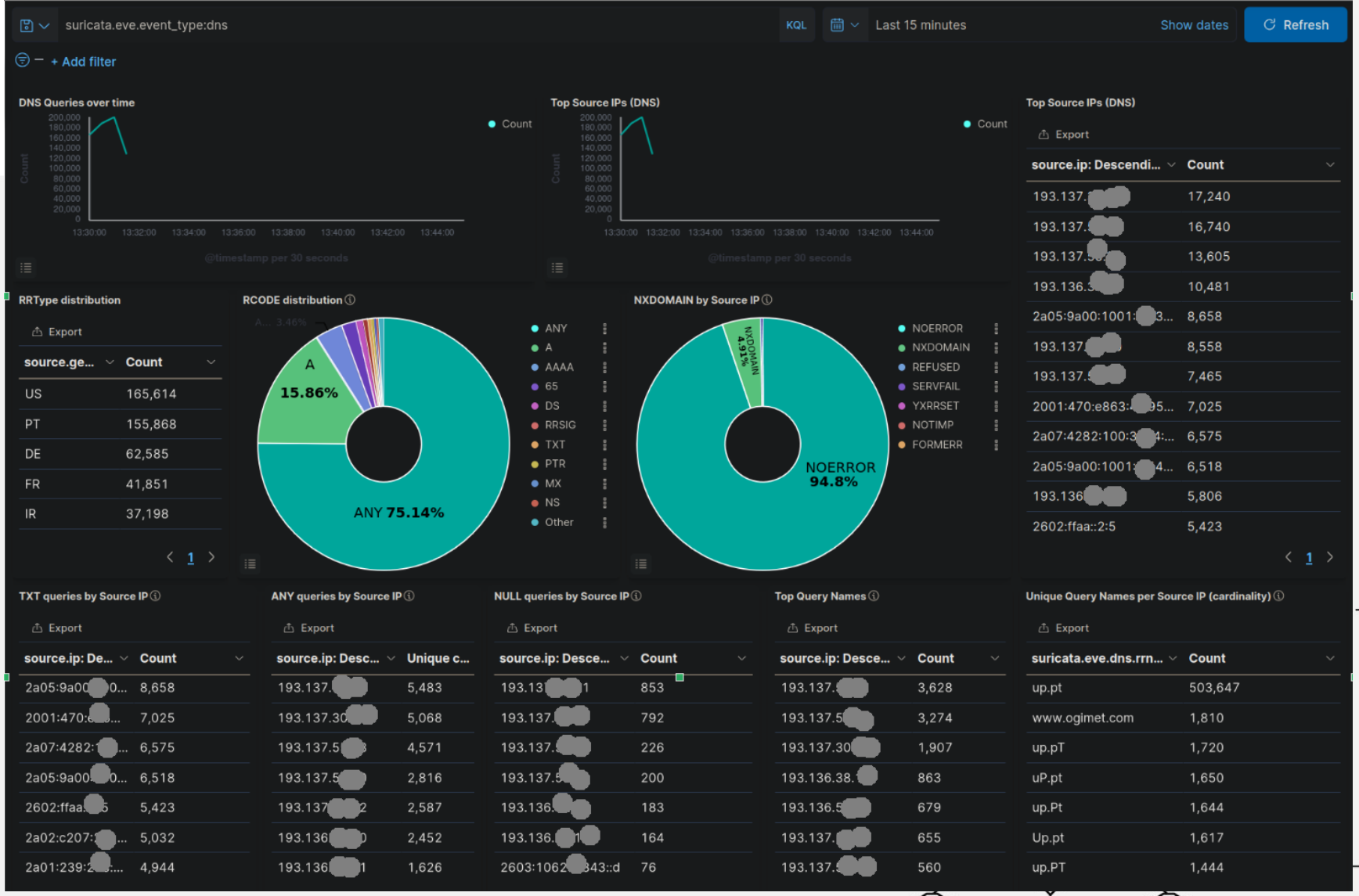
FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

SURICATA

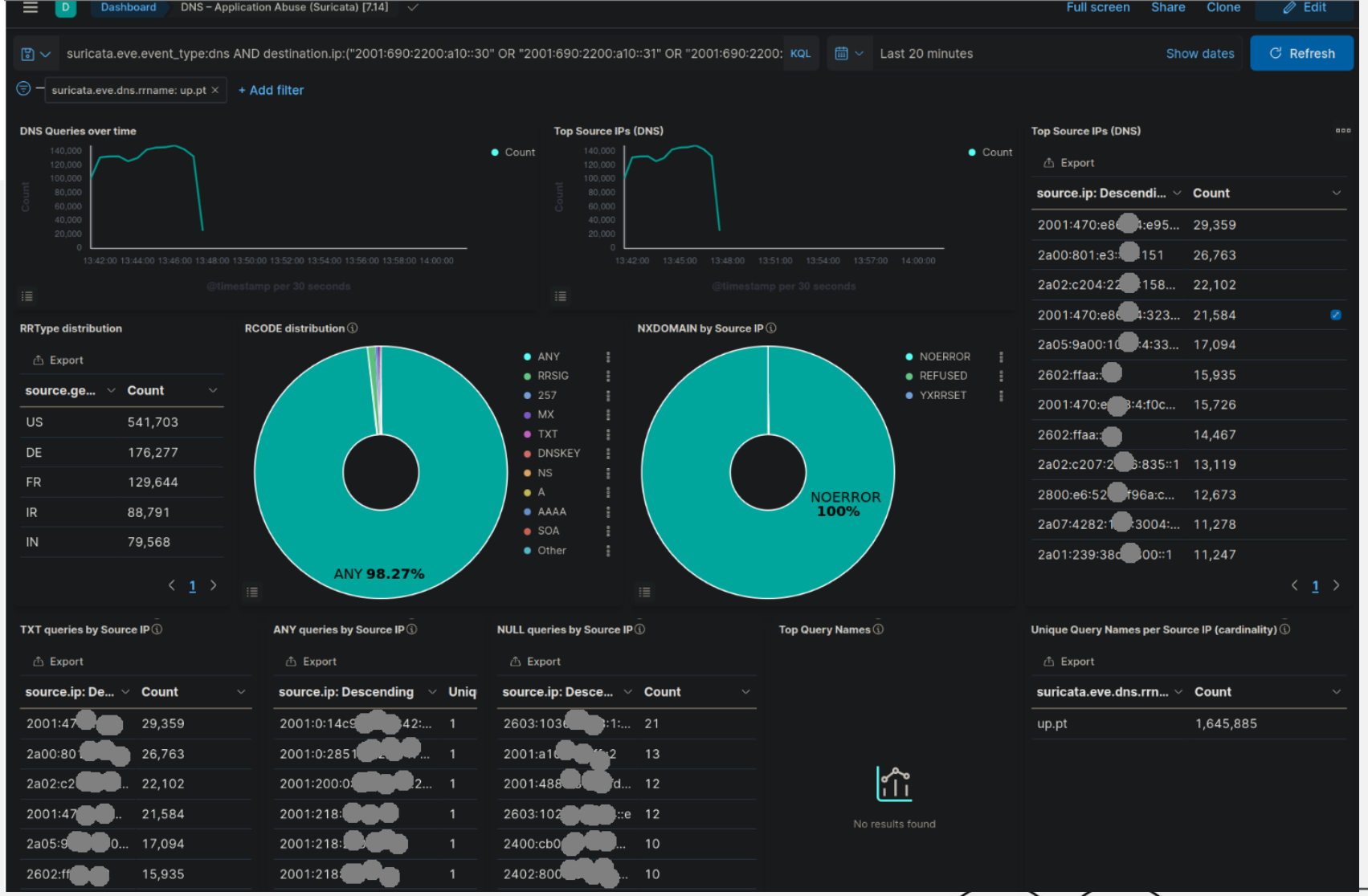
IDS – Tap Suricata

Dashboard com análise de eventos suricata.eve.dns que nos permitiu identificar os pedidos ANY em abuso e identificar falências no nosso serviço, tanto em ipv4 como em ipv6.



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

jornadas FCCN



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

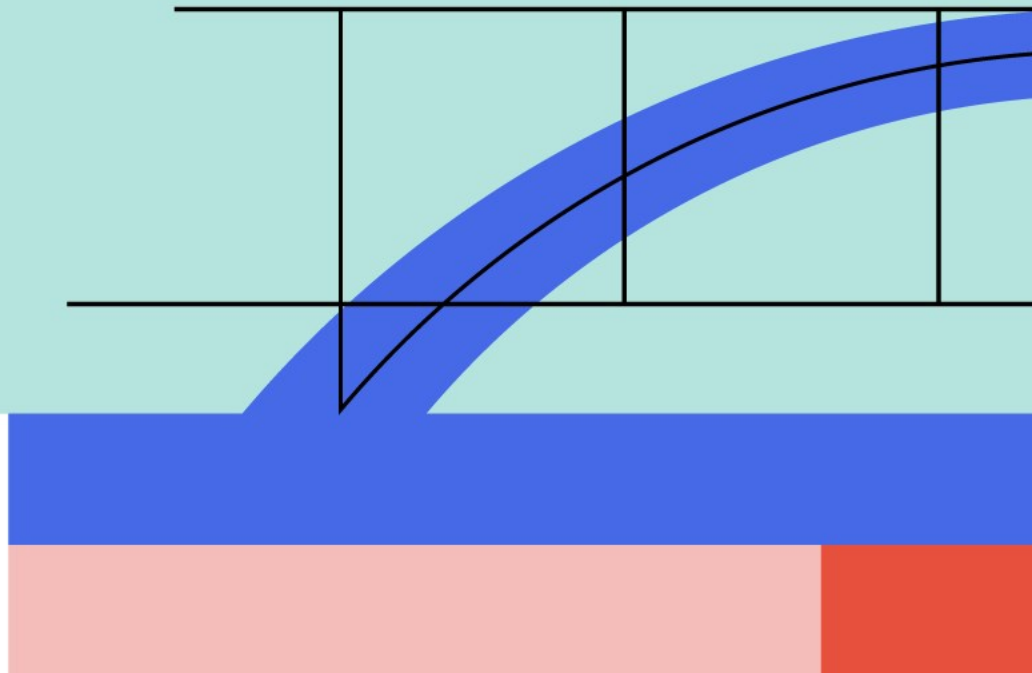
jornadas FCCN

Repositorio-aberto e outros:
https://repositorio-aberto.up.pt/
https://arquivoatom.up.pt/
https://repositorio-tematico.up.pt/

Fomos contactados por colegas da UAS onde nos indicam que a infraestrutura manifestava sintomas de ataque DOS. Não conseguia responder a todos os pedidos, demonstrando um “lag” excessivo e por vezes falha de serviço.

CrowdSec

Foi instalado o Crowdsec – com análise dos logs locais e instalação de regras e cenários inicia-se o processo de bloqueio de ip’s com ataques identificados.
Bouncer-crowdsec a bloquear LAPI (logs Locais) bem como a usufruir da lista CAPI (Global – Comunidade).



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

```
root@atom2023:~# cscli decisions list
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
53397672	crowdsec	Ip:117	crowdsecurity/http-cve-2021-42013	ban	CN	4808 China Unicom Beijing Province Network	1	46h26m25s	16237
53382670	crowdsec	Ip:45.	crowdsecurity/http-dos-swithcing-ua	ban	SE	197854 Eisenia AB	11	45h35m17s	16234
53382669	crowdsec	Ip:193	crowdsecurity/http-dos-swithcing-ua	ban	FR	39351 31173 Services AB	11	45h26m10s	16233
53382668	crowdsec	Ip:101	crowdsecurity/http-cve-2021-42013	ban	SG	150436 Byteplus Pte. Ltd.	1	44h59m24s	16232
53367666	crowdsec	Ip:66.	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	42h29m10s	16229
53352665	crowdsec	Ip:185	crowdsecurity/http-cve-2021-42013	ban	FR	51167 Contabo GmbH	1	42h1m45s	16227
53337663	crowdsec	Ip:172	crowdsecurity/http-wordpress-scan	ban	CH	8075 MICROSOFT-CORP-MSN-AS-BLOCK	4	40h1m52s	16224
53307660	crowdsec	Ip:178	crowdsecurity/http-dos-swithcing-ua	ban	IT	212238 Datacamp Limited	11	36h9m57s	16219
53307659	crowdsec	Ip:195	crowdsecurity/http-wordpress-scan	ban	BG	48090 Techoff Srv Limited	4	35h30m15s	16218
53307654	crowdsec	Ip:185	crowdsecurity/http-probing	ban	GB	201579 Hostgnome Ltd	12	34h38m18s	16213
53292653	crowdsec	Ip:146	crowdsecurity/http-dos-swithcing-ua	ban	IT	9009 M247 Europe SRL	11	33h29m5s	16211
53292652	crowdsec	Ip:158	crowdsecurity/http-probing	ban	ES	8075 MICROSOFT-CORP-MSN-AS-BLOCK	11	33h14m32s	16210
53277651	crowdsec	Ip:66.	crowdsecurity/http-bad-user-agent	ban	US		2	32h10m20s	16208
53277650	crowdsec	Ip:167	crowdsecurity/http-bad-user-agent	ban	US	398705 CENSYS-ARIN-02	2	31h46m33s	16205
53262649	crowdsec	Ip:67.	crowdsecurity/http-cve-probing	ban	US	398256 AS-ULTAHOST	1	27h24m52s	16204
53262648	crowdsec	Ip:80.	crowdsecurity/http-probing	ban	RO	47890 Unmanaged Ltd	11	27h21m1s	16202
53247647	crowdsec	Ip:144	crowdsecurity/http-probing	ban	FR	51167 Contabo GmbH	11	26h53m42s	16200
53247645	crowdsec	Ip:20.	crowdsecurity/http-cve-probing	ban	US	8075 MICROSOFT-CORP-MSN-AS-BLOCK	1	26h17m4s	16196
53202644	crowdsec	Ip:168	crowdsecurity/http-probing	ban	US		11	20h45m52s	16195
53202643	crowdsec	Ip:93.	crowdsecurity/http-open-proxy	ban	BG	48090 Techoff Srv Limited	1	20h25m8s	16192
53172642	crowdsec	Ip:66.	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	16h8m10s	16187
53112641	crowdsec	Ip:185	crowdsecurity/http-dos-swithcing-ua	ban	DE	43357 Owl Limited	11	8h22m23s	16186
53112640	crowdsec	Ip:66.	crowdsecurity/http-bad-user-agent	ban	US		2	7h5m33s	16184
53097639	crowdsec	Ip:129	crowdsecurity/http-cve-2021-42013	ban	US		1	6h26m25s	

Go to the

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

```
[root@repositorio-tematico ~]# cscli decisions list
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
54338834	crowdsec	Ip:4.	crowdsecurity/http-crawl-non_statics	ban	IT	8075 MICROSOFT-CORP-MSN-AS-BLOCK	59	42h27m30s	12470
54338830	crowdsec	Ip:47	crowdsecurity/http-cve-2021-41773	ban	US	45102 Alibaba US Technology Co., Ltd.	1	41h42m2s	12466
54338829	crowdsec	Ip:45	crowdsecurity/http-cve-2021-41773	ban	SE	215540 Global Connectivity Solutions Llp	1	41h41m42s	12465
54338828	crowdsec	Ip:4.	crowdsecurity/http-admin-interface-probing	ban	IT	8075 MICROSOFT-CORP-MSN-AS-BLOCK	3	41h29m50s	12464
54308823	crowdsec	Ip:19	crowdsecurity/http-admin-interface-probing	ban	BG	48090 Techoff Srv Limited	3	37h45m14s	12457
54248820	crowdsec	Ip:66	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	30h22m16s	12450
54233819	crowdsec	Ip:18	crowdsecurity/http-bad-user-agent	ban	US	14618 AMAZON-AES	2	29h21m23s	12448
54233818	crowdsec	Ip:67	crowdsecurity/http-cve-probing	ban	US	398256 AS-ULTAHOST	1	27h41m11s	12447
54218817	crowdsec	Ip:80	crowdsecurity/http-probing	ban	RO	47890 Unmanaged Ltd	11	27h27m11s	12445
54218816	crowdsec	Ip:20	crowdsecurity/http-cve-probing	ban	US	8075 MICROSOFT-CORP-MSN-AS-BLOCK	1	26h49m56s	12444
54218815	crowdsec	Ip:18	crowdsecurity/http-bad-user-agent	ban	US	14618 AMAZON-AES	2	26h[illegible]	12443
54188814	crowdsec	Ip:13	crowdsecurity/http-admin-interface-probing	ban	US	8075 MICROSOFT-CORP-MSN-AS-BLOCK	3	23h[illegible]	[illegible]
54188811	crowdsec	Ip:18	crowdsecurity/http-bad-user-agent	ban	US	14618 AMAZON-AES	2	23h[illegible]	[illegible]
54173810	crowdsec	Ip:18	crowdsecurity/http-bad-user-agent	ban	US	14618 AMAZON-AES	2	20h3m15s	12435
54173809	crowdsec	Ip:23	LePresidente/http-generic-403-bf	ban	US	53514 UHQ	6	20h2m0s	12434
54158808	crowdsec	Ip:11	crowdsecurity/http-cve-2021-41773	ban	CN	137718 Beijing Volcano Engine Technology Co., Ltd.	1	18h44m56s	12432
54143806	crowdsec	Ip:18	crowdsecurity/http-bad-user-agent	ban	US	14618 AMAZON-AES	2	16h57m19s	12429
54113805	crowdsec	Ip:66	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	13h9m29s	12426
54098804	crowdsec	Ip:18	crowdsecurity/http-bad-user-agent	ban	US	14618 AMAZON-AES	2	10h42m24s	12424
54053803	crowdsec	Ip:66	crowdsecurity/http-bad-user-agent	ban	US		2	5h12m30s	12420

Go to the next im

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

```
[root@repositorio-aberto ~]# cscli decisions list
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
53754034	crowdsec	Ip:185	crowdsecurity/http-dos-swithcing-ua	ban	DE	39351 31173 Services AB	11	45h53m7s	45634
53739033	crowdsec	Ip:66.	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	45h14m11s	45632
53739032	crowdsec	Ip:20.	crowdsecurity/CVE-2022-41082	ban	US	8075 MICROSOFT-CORP-MSN-AS-BLOCK	1	45h12m47s	45631
53739031	crowdsec	Ip:131	crowdsecurity/http-wordpress-scan	ban	AE	34984 Superonline Iletisim Hizmetleri A.S.	4	44h25m8s	45630
53739030	crowdsec	Ip:20.	crowdsecurity/http-crawl-non_statics	ban	CA	8075 MICROSOFT-CORP-MSN-AS-BLOCK	58	44h18m41s	45629
53739025	crowdsec	Ip:78.	crowdsecurity/http-admin-interface-probing	ban	BG	213438 ColocaTel Inc.	3	44h9m22s	45624
53739024	crowdsec	Ip:168	crowdsecurity/http-admin-interface-probing	ban	US		3	43h41m7s	45623
53739022	crowdsec	Ip:138	crowdsecurity/http-probing	ban	US	14061 DIGITALOCEAN-ASN	13	43h28m6s	45621
53724021	crowdsec	Ip:66.	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	42h14m31s	45619
53709020	crowdsec	Ip:40.	crowdsecurity/http-probing	ban	IE	8075 MICROSOFT-CORP-MSN-AS-BLOCK	13	40h48m18s	45617
53694019	crowdsec	Ip:23.	crowdsecurity/http-probing	ban	HK	8075 MICROSOFT-CORP-MSN-AS-BLOCK	11	38h37m40s	45615
53694018	crowdsec	Ip:43.	crowdsecurity/http-bad-user-agent	ban	SG	132203 Tencent Building, Kejizhongyi Avenue	2	38h37m11s	45614
53694017	crowdsec	Ip:195	crowdsecurity/http-admin-interface-probing	ban	BG	48090 Techoff Srv Limited	3	37h42m56s	45613
53679013	crowdsec	Ip:83.	crowdsecurity/http-probing	ban	NL	214967 OPTIBOUNCE	15	36h11m49s	45608
53679012	crowdsec	Ip:43.	crowdsecurity/http-bad-user-agent	ban	SG	132203 Tencent Building, Kejizhongyi Avenue	2	36h9m18s	45607
53679011	crowdsec	Ip:153	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	36h9m12s	45606
53679010	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	35h51m52s	45605
53679009	crowdsec	Ip:108	crowdsecurity/http-probing	ban	ID	16509 AMAZON-02	11	35h43m9s	45604
53679008	crowdsec	Ip:45.	crowdsecurity/http-cve-2021-41773	ban	VN	131386 Long Van System Solution JSC	1	35h36m13s	45603
53664007	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	35h25m53s	45601
53664006	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	34h38m34s	45600
53664005	crowdsec	Ip:66.	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	34h10m9s	45599
53664004	crowdsec	Ip:153	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	33h59m1s	45597
53649003	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	33h23m3s	45596
53649002	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	33h17m56s	45595
53649001	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	33h5m49s	45594
53649000	crowdsec	Ip:153	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	33h4m53s	45593
53648999	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	32h38m47s	45592
53648998	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	32h33m14s	45591
53648997	crowdsec	Ip:153	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	32h7m52s	45590
53648996	crowdsec	Ip:153	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	32h7m31s	45589
53648995	crowdsec	Ip:182	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	31h47m22s	45588
53648994	crowdsec	Ip:43.	crowdsecurity/http-bad-user-agent	ban	SG	132203 Tencent Building, Kejizhongyi Avenue	2	31h40m53s	45587
53633993	crowdsec	Ip:43.	crowdsecurity/http-bad-user-agent	ban	SG	132203 Tencent Building, Kejizhongyi Avenue	2	31h7m46s	45585
53633992	crowdsec	Ip:45.	crowdsecurity/http-bad-user-agent	ban	BR	266959 SKYINF SOLUCOES EM TECNOLOGIA DE INFORMACAO LTDA	2	29h53m59s	45584
53618991	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	28h59m59s	45582
53618990	crowdsec	Ip:67.	crowdsecurity/http-cve-probing	ban	US	398256 AS-ULTAHOST	1	27h26m39s	45581
53603989	crowdsec	Ip:149	crowdsecurity/http-probing	ban	PT	212238 Datacamp Limited	12	26h15m13s	45579
53603988	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	26h13m3s	45578
53603987	crowdsec	Ip:20.	crowdsecurity/http-cve-probing	ban	US	8075 MICROSOFT-CORP-MSN-AS-BLOCK	1	25h42m35s	45577
53588986	crowdsec	Ip:190	crowdsecurity/http-crawl-non_statics	ban	BR	272547 Servicos de Infraestrutura e Datacenter	54	25h14m56s	45575
53588985	crowdsec	Ip:112	crowdsecurity/http-bad-user-agent	ban	CN	4837 CHINA UNICOM China169 Backbone	2	24h52m1s	45574

Go to the next image

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

jornadas FCCN

SURICATA®

script IDS – Suricata

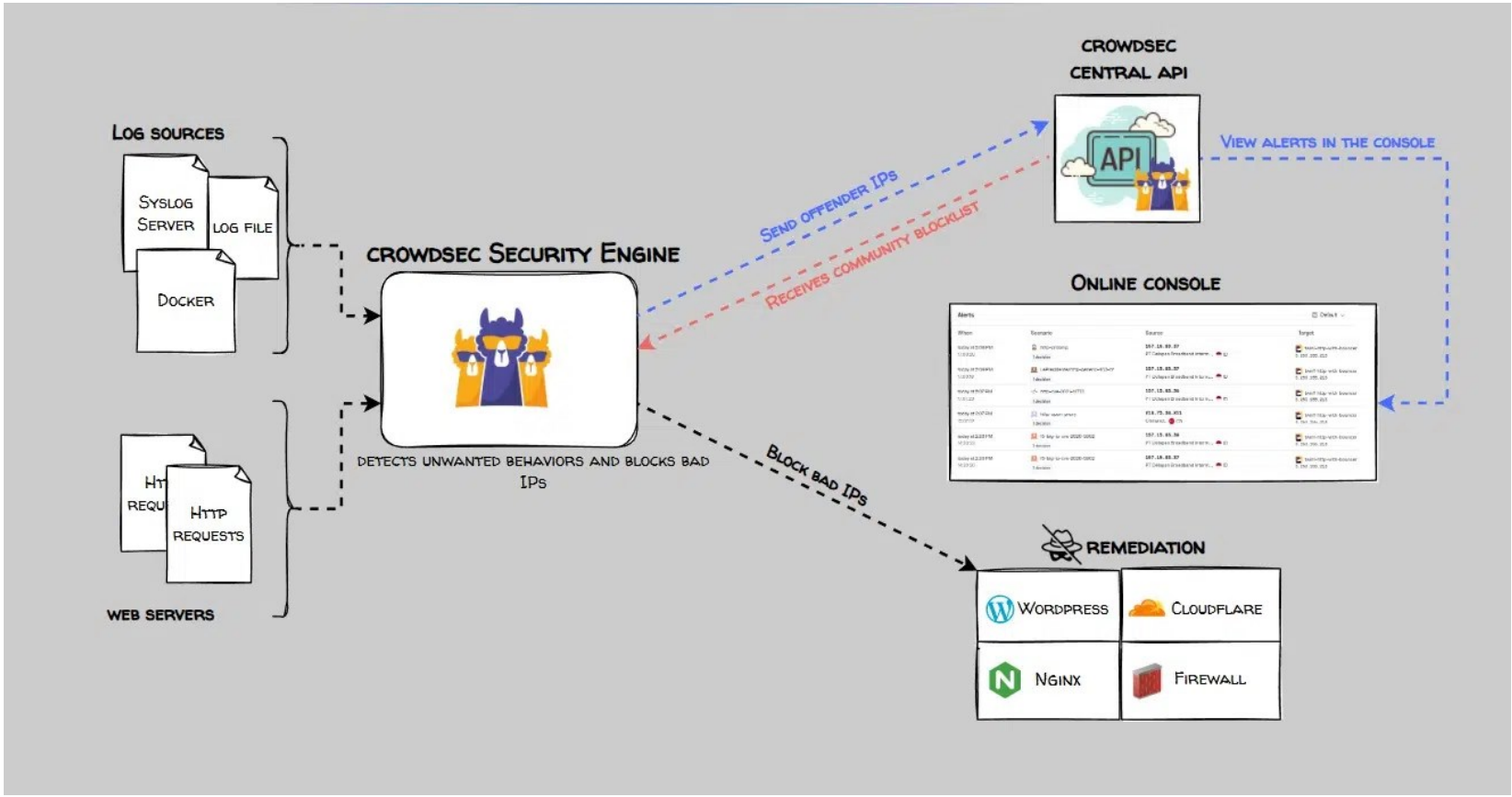
De forma a aumentarmos a nossa visibilidade foi criado um script de consulta ao IDS (elastic search em kubernetes) alimentado pela TAP central com regras Suricata da Proofpoint e outros.
Com o script conseguimos identificar vários ip's extras e manualmente foi-se adicionando os ip's aos bloqueios, conseguindo assim recuperar e manter o serviço, estando desde então a funcionar devidamente.

```
cscli decisions add -t ban --ip "172.202.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "20.65.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "135.237.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - GPL SNMP public access udp" --duration 87600h
cscli decisions add -t ban --ip "172.202.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "20.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "40.8[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN DuckDuckGo Webcrawler User-Agent (DuckDuckBot)" --duration 87600h
cscli decisions add -t ban --ip "134.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET INFO User-Agent (python-requests) Inbound to Webserver" --duration 87600h
cscli decisions add -t ban --ip "172.202.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "20.6[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "157.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - SURICATA TLS invalid record/traffic" --duration 87600h
cscli decisions add -t ban --ip "157.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - SURICATA TLS invalid record/traffic" --duration 87600h
cscli decisions add -t ban --ip "207.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - SURICATA TLS invalid record/traffic" --duration 87600h
cscli decisions add -t ban --ip "40.77.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - SURICATA TLS invalid record/traffic" --duration 87600h
cscli decisions add -t ban --ip "40.7[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - SURICATA TLS invalid record/traffic" --duration 87600h
cscli decisions add -t ban --ip "20.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET INFO Spring Boot Actuator Health Check Request;ET SCAN Zmap User-Agent (Inbound)" --duration 87600
cscli decisions add -t ban --ip "74.2[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "20.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET INFO Spring Boot Actuator Health Check Request;ET SCAN Zmap User-Agent (Inbound)" --duration 87600
cscli decisions add -t ban --ip "74.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
cscli decisions add -t ban --ip "20.[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET INFO Spring Boot Actuator Health Check Request;ET SCAN Zmap User-Agent (Inbound)" --duration 87600
cscli decisions add -t ban --ip "74.2[redacted]" --reason "Suricata alert - US - AS8075 Microsoft Corporation - ET SCAN Zmap User-Agent (Inbound)" --duration 87600h
```

https://www.crowdsec.net/

No Projeto DC4EU criámos um “mix” das 2 soluções, IDS e Crowdsec.

- Crowdsec
- logs locais
- CAPI (Lista Global de ip’s)
- script IDS – Suricata
- Crontab de 3 em 3 minutos com Query a elastic Search pelo ip. Ban por 4 horas dos ip’s detetados.



```
root@lspup:/home/ubuntu# cscli parsers list
```

PARSERS

Name	📦 Status	Version	Local Path
crowdsecurity/dateparse-enrich	✔️ enabled	0.2	/etc/crowdsec/parsers/s02-enrich/dateparse-enrich.yaml
crowdsecurity/endlessh-logs	✔️ enabled	0.5	/etc/crowdsec/parsers/s01-parse/endlessh-logs.yaml
crowdsecurity/geoip-enrich	✔️ enabled	0.5	/etc/crowdsec/parsers/s02-enrich/geoip-enrich.yaml
crowdsecurity/http-logs	✔️ enabled	1.3	/etc/crowdsec/parsers/s02-enrich/http-logs.yaml
crowdsecurity/nginx-logs	✔️ enabled	1.7	/etc/crowdsec/parsers/s01-parse/nginx-logs.yaml
crowdsecurity/nginx-proxy-manager-logs	✔️ enabled	0.3	/etc/crowdsec/parsers/s01-parse/nginx-proxy-manager-logs.yaml
crowdsecurity/pkexec-logs	✔️ enabled	0.1	/etc/crowdsec/parsers/s01-parse/pkexec-logs.yaml
crowdsecurity/public-dns-allowlist	✔️ enabled	0.1	/etc/crowdsec/parsers/s02-enrich/public-dns-allowlist.yaml
crowdsecurity/segfault-logs	✔️ enabled	0.4	/etc/crowdsec/parsers/s01-parse/segfault-logs.yaml
crowdsecurity/sshd-logs	✔️ enabled	3.0	/etc/crowdsec/parsers/s01-parse/sshd-logs.yaml
crowdsecurity/sshd-success-logs	✔️ enabled	0.1	/etc/crowdsec/parsers/s01-parse/sshd-success-logs.yaml
crowdsecurity/syslog-logs	✔️ enabled	0.8	/etc/crowdsec/parsers/s00-raw/syslog-logs.yaml
crowdsecurity/whitelist-my-ip	🏠 enabled,local		/etc/crowdsec/parsers/s02-whitelists/whitelist-my-ip.yaml
crowdsecurity/whitelists	⚠️ enabled,tainted	?	/etc/crowdsec/parsers/s02-enrich/whitelists.yaml
thespad/sshesame-logs	✔️ enabled	0.2	/etc/crowdsec/parsers/s01-parse/sshesame-logs.yaml

```
root@lspup:/home/ubuntu# cscli collections list
```

COLLECTIONS

Name	📦 Status	Version	Local Path
crowdsecurity/base-http-scenarios	✔️ enabled	1.2	/etc/crowdsec/collections/base-http-scenarios.yaml
crowdsecurity/endlessh	✔️ enabled	0.1	/etc/crowdsec/collections/endlessh.yaml
crowdsecurity/http-cve	✔️ enabled	2.9	/etc/crowdsec/collections/http-cve.yaml
crowdsecurity/http-dos	✔️ enabled	0.2	/etc/crowdsec/collections/http-dos.yaml
crowdsecurity/linux	✔️ enabled	0.3	/etc/crowdsec/collections/linux.yaml
crowdsecurity/linux-lpe	✔️ enabled	0.2	/etc/crowdsec/collections/linux-lpe.yaml
crowdsecurity/nginx	✔️ enabled	0.2	/etc/crowdsec/collections/nginx.yaml
crowdsecurity/sshd	✔️ enabled	0.7	/etc/crowdsec/collections/sshd.yaml
crowdsecurity/sshd-impossible-travel	✔️ enabled	0.1	/etc/crowdsec/collections/sshd-impossible-travel.yaml
crowdsecurity/whitelist-good-actors	✔️ enabled	0.2	/etc/crowdsec/collections/whitelist-good-actors.yaml
thespad/sshesame	✔️ enabled	0.1	/etc/crowdsec/collections/sshesame.yaml

```
root@lspup:/home/ubuntu# cscli scenarios list
```

SCENARIOS

Name	Status	Version	Local Path
crowdsecurity/apache_log4j2_cve-2021-44228	✔ enabled	0.6	/etc/crowdsec/scenarios/apache_log4j2_cve-2021-44228.yaml
crowdsecurity/CVE-2017-9841	✔ enabled	0.2	/etc/crowdsec/scenarios/CVE-2017-9841.yaml
crowdsecurity/CVE-2019-18935	✔ enabled	0.2	/etc/crowdsec/scenarios/CVE-2019-18935.yaml
crowdsecurity/CVE-2021-4034	✔ enabled	0.2	/etc/crowdsec/scenarios/CVE-2021-4034.yaml
crowdsecurity/CVE-2022-26134	✔ enabled	0.4	/etc/crowdsec/scenarios/CVE-2022-26134.yaml
crowdsecurity/CVE-2022-35914	✔ enabled	0.2	/etc/crowdsec/scenarios/CVE-2022-35914.yaml
crowdsecurity/CVE-2022-37042	✔ enabled	0.2	/etc/crowdsec/scenarios/CVE-2022-37042.yaml
crowdsecurity/CVE-2022-40684	✔ enabled	0.3	/etc/crowdsec/scenarios/CVE-2022-40684.yaml
crowdsecurity/CVE-2022-41082	✔ enabled	0.4	/etc/crowdsec/scenarios/CVE-2022-41082.yaml
crowdsecurity/CVE-2022-41697	✔ enabled	0.2	/etc/crowdsec/scenarios/CVE-2022-41697.yaml
crowdsecurity/CVE-2022-42889	✔ enabled	0.3	/etc/crowdsec/scenarios/CVE-2022-42889.yaml
crowdsecurity/CVE-2022-44877	✔ enabled	0.3	/etc/crowdsec/scenarios/CVE-2022-44877.yaml
crowdsecurity/CVE-2022-46169	✔ enabled	0.2	/etc/crowdsec/scenarios/CVE-2022-46169.yaml
crowdsecurity/CVE-2023-22515	✔ enabled	0.1	/etc/crowdsec/scenarios/CVE-2023-22515.yaml
crowdsecurity/CVE-2023-22518	✔ enabled	0.3	/etc/crowdsec/scenarios/CVE-2023-22518.yaml
crowdsecurity/CVE-2023-49103	✔ enabled	0.3	/etc/crowdsec/scenarios/CVE-2023-49103.yaml
crowdsecurity/CVE-2023-4911	✔ enabled	0.5	/etc/crowdsec/scenarios/CVE-2023-4911.yaml
crowdsecurity/CVE-2024-0012	✔ enabled	0.1	/etc/crowdsec/scenarios/CVE-2024-0012.yaml
crowdsecurity/CVE-2024-38475	✔ enabled	0.1	/etc/crowdsec/scenarios/CVE-2024-38475.yaml
crowdsecurity/CVE-2024-9474	✔ enabled	0.1	/etc/crowdsec/scenarios/CVE-2024-9474.yaml
crowdsecurity/endlessh-bf	✔ enabled	0.3	/etc/crowdsec/scenarios/endlessh-bf.yaml
crowdsecurity/f5-big-ip-cve-2020-5902	✔ enabled	0.3	/etc/crowdsec/scenarios/f5-big-ip-cve-2020-5902.yaml
crowdsecurity/fortinet-cve-2018-13379	✔ enabled	0.3	/etc/crowdsec/scenarios/fortinet-cve-2018-13379.yaml
crowdsecurity/grafana-cve-2021-43798	✔ enabled	0.3	/etc/crowdsec/scenarios/grafana-cve-2021-43798.yaml
crowdsecurity/http-admin-interface-probing	✔ enabled	0.4	/etc/crowdsec/scenarios/http-admin-interface-probing.yaml
crowdsecurity/http-backdoors-attempts	✔ enabled	0.6	/etc/crowdsec/scenarios/http-backdoors-attempts.yaml
crowdsecurity/http-bad-user-agent	✔ enabled	1.2	/etc/crowdsec/scenarios/http-bad-user-agent.yaml
crowdsecurity/http-crawl-non_statics	✔ enabled	0.7	/etc/crowdsec/scenarios/http-crawl-non_statics.yaml
crowdsecurity/http-cve-2021-41773	✔ enabled	0.3	/etc/crowdsec/scenarios/http-cve-2021-41773.yaml
crowdsecurity/http-cve-2021-42013	✔ enabled	0.3	/etc/crowdsec/scenarios/http-cve-2021-42013.yaml
crowdsecurity/http-cve-probing	✔ enabled	0.6	/etc/crowdsec/scenarios/http-cve-probing.yaml
crowdsecurity/http-dos-bypass-cache	✔ enabled	0.5	/etc/crowdsec/scenarios/http-dos-bypass-cache.yaml
crowdsecurity/http-dos-invalid-http-versions	✔ enabled	0.7	/etc/crowdsec/scenarios/http-dos-invalid-http-versions.yaml
crowdsecurity/http-dos-random-uri	✔ enabled	0.4	/etc/crowdsec/scenarios/http-dos-random-uri.yaml
crowdsecurity/http-dos-switching-ua	✔ enabled	0.5	/etc/crowdsec/scenarios/http-dos-switching-ua.yaml
crowdsecurity/http-generic-bf	✔ enabled	0.9	/etc/crowdsec/scenarios/http-generic-bf.yaml
crowdsecurity/http-generic-test	✔ enabled	0.2	/etc/crowdsec/scenarios/http-generic-test.yaml
crowdsecurity/http-open-proxy	✔ enabled	0.5	/etc/crowdsec/scenarios/http-open-proxy.yaml
crowdsecurity/http-path-traversal-probing	✔ enabled	0.4	/etc/crowdsec/scenarios/http-path-traversal-probing.yaml
crowdsecurity/http-probing	✔ enabled	0.4	/etc/crowdsec/scenarios/http-probing.yaml
crowdsecurity/http-sap-interface-probing	✔ enabled	0.1	/etc/crowdsec/scenarios/http-sap-interface-probing.yaml
crowdsecurity/http-sensitive-files	✔ enabled	0.4	/etc/crowdsec/scenarios/http-sensitive-files.yaml
crowdsecurity/http-sqli-probing	✔ enabled	0.4	/etc/crowdsec/scenarios/http-sqli-probing.yaml
crowdsecurity/http-wordpress-scan	✔ enabled	0.3	/etc/crowdsec/scenarios/http-wordpress-scan.yaml
crowdsecurity/http-xss-probing	✔ enabled	0.4	/etc/crowdsec/scenarios/http-xss-probing.yaml
crowdsecurity/impossible-travel	✔ enabled	0.2	/etc/crowdsec/scenarios/impossible-travel.yaml
crowdsecurity/impossible-travel-user	✔ enabled	0.1	/etc/crowdsec/scenarios/impossible-travel-user.yaml
crowdsecurity/jira_cve-2021-26086	✔ enabled	0.3	/etc/crowdsec/scenarios/jira_cve-2021-26086.yaml
crowdsecurity/netgear_rce	✔ enabled	0.4	/etc/crowdsec/scenarios/netgear_rce.yaml
crowdsecurity/nginx-req-limit-exceeded	✔ enabled	0.3	/etc/crowdsec/scenarios/nginx-req-limit-exceeded.yaml
crowdsecurity/pulse-secure-sslvpn-cve-2019-11510	✔ enabled	0.3	/etc/crowdsec/scenarios/pulse-secure-sslvpn-cve-2019-11510.yaml

No active decisions
root@lspup:/home/ubuntu# cscli alerts list

ID	value	reason	country	as	decisions	created_at
308783	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:54:17 +0000 UTC
308782	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:51:17 +0000 UTC
308781	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:48:17 +0000 UTC
308780	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:48:17 +0000 UTC
308779	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:45:18 +0000 UTC
308778	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:45:17 +0000 UTC
308777	Ip:35.233.103.83	Suricata alert - N/A - N/A - ET SCAN Potential VNC Scan 5800-5820			ban:1	2026-05-01 13:42:17 +0000 UTC
308776	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:42:17 +0000 UTC
308775	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:42:17 +0000 UTC
308774	Ip:35.233.103.83	Suricata alert - N/A - N/A - ET SCAN Potential VNC Scan 5800-5820			ban:1	2026-05-01 13:39:18 +0000 UTC
308773	Ip:201.132.11.46	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:39:18 +0000 UTC
308772	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:39:17 +0000 UTC
308771	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:39:17 +0000 UTC
308770	Ip:45.61.129.23	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:36:19 +0000 UTC
308769	Ip:35.233.103.83	Suricata alert - N/A - N/A - ET SCAN Potential VNC Scan 5800-5820			ban:1	2026-05-01 13:36:19 +0000 UTC
308768	Ip:201.132.11.46	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:36:18 +0000 UTC
308767	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:36:18 +0000 UTC

No active decisions
root@lspup:/home/ubuntu# cscli alerts list

ID	value	reason	country	as	decisions	created_at
308783	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:54:17 +0000 UTC
308782	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:51:17 +0000 UTC
308781	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:48:17 +0000 UTC
308780	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:48:17 +0000 UTC
308779	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:45:18 +0000 UTC
308778	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:45:17 +0000 UTC
308777	Ip:35.233.103.83	Suricata alert - N/A - N/A - ET SCAN Potential VNC Scan 5800-5820			ban:1	2026-05-01 13:42:17 +0000 UTC
308776	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:42:17 +0000 UTC
308775	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:42:17 +0000 UTC
308774	Ip:35.233.103.83	Suricata alert - N/A - N/A - ET SCAN Potential VNC Scan 5800-5820			ban:1	2026-05-01 13:39:18 +0000 UTC
308773	Ip:201.132.11.46	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:39:18 +0000 UTC
308772	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:39:17 +0000 UTC
308771	Ip:125.179.39.89	Suricata alert - N/A - N/A - ET CINS Active Threat Intelligence Poor Reputation IP group 173			ban:1	2026-05-01 13:39:17 +0000 UTC
308770	Ip:45.61.129.23	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:36:19 +0000 UTC
308769	Ip:35.233.103.83	Suricata alert - N/A - N/A - ET SCAN Potential VNC Scan 5800-5820			ban:1	2026-05-01 13:36:19 +0000 UTC
308768	Ip:201.132.11.46	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:36:18 +0000 UTC
308767	Ip:187.226.36.78	Suricata alert - N/A - N/A - ET SCAN Suspicious inbound to MSSQL port 1433			ban:1	2026-05-01 13:36:18 +0000 UTC

jornadas FCCN

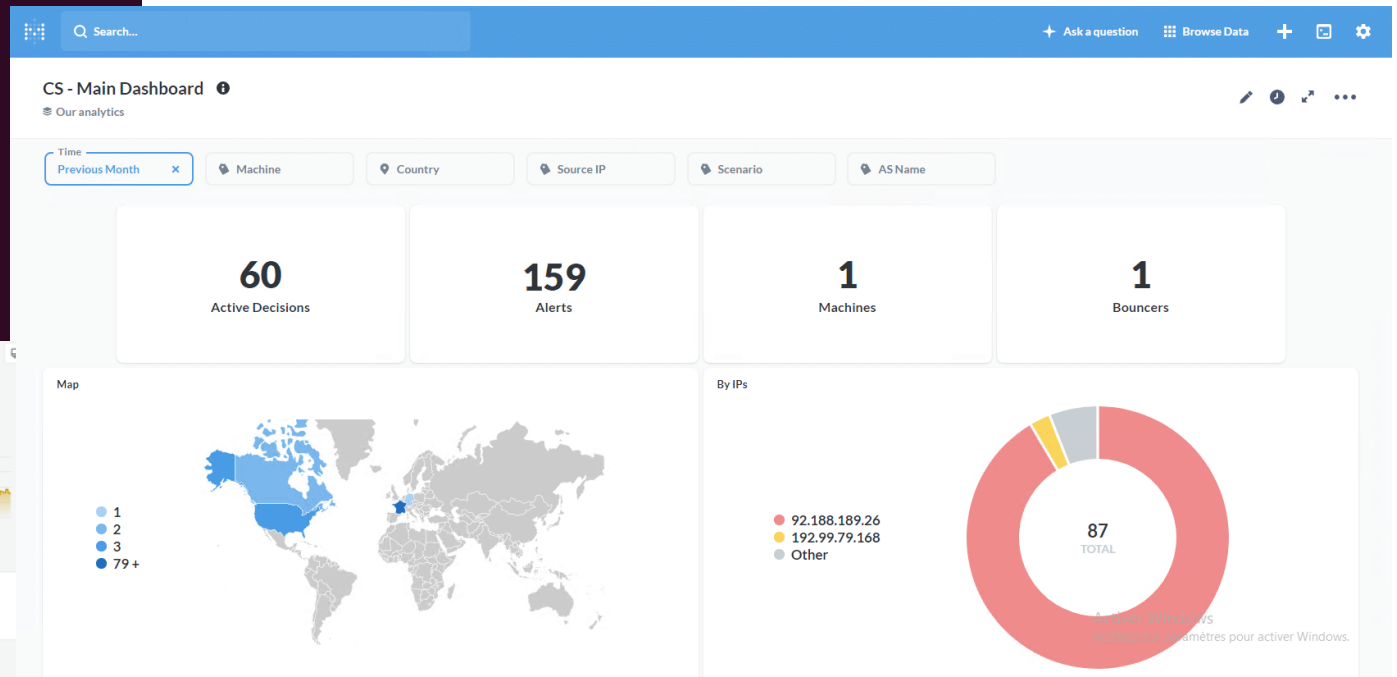
Bouncer Metrics (crowdsec-firewall-bouncer) since 2026-04-24 20:32:59 +0000 UTC

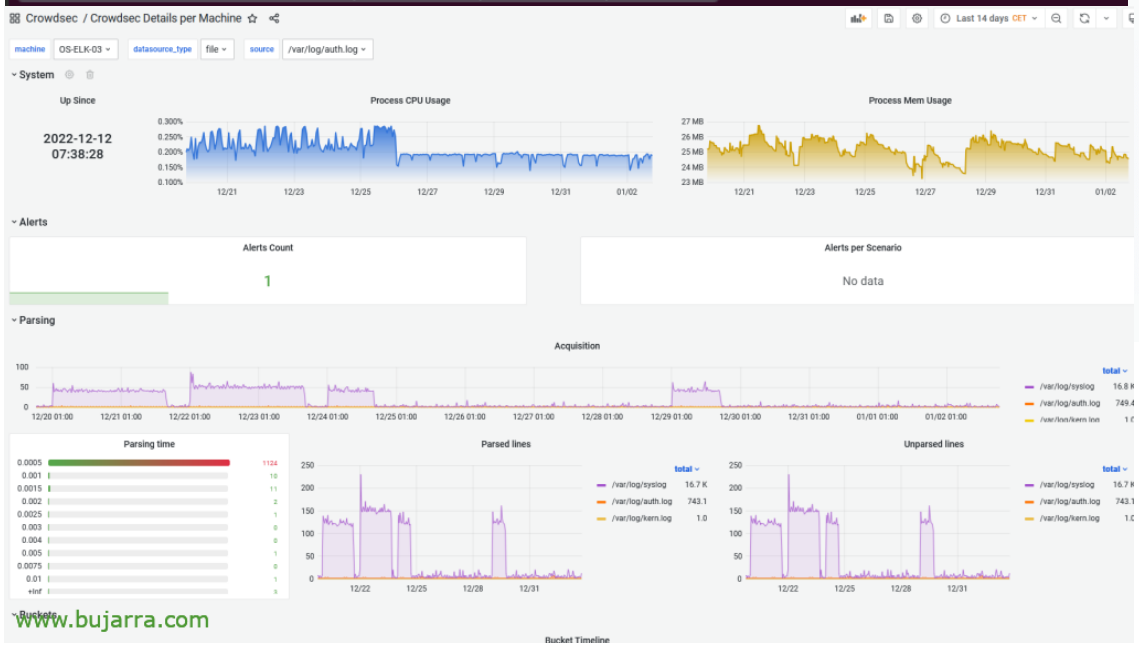
Origin	active_decisions IPs	dropped bytes	dropped packets	processed bytes	processed packets
CAPI (community blocklist)	9.90k	14.38k	310	-	-
cscli (manual decisions)	0	0	0	-	-
Total	9.90k	14.38k	310	398.47M	1.25M

Local API Decisions

Reason	Origin	Action	Count
generic:exploit	CAPI	ban	372
generic:scan	CAPI	ban	435
http:bruteforce	CAPI	ban	2050
http:dos	CAPI	ban	1220
http:exploit	CAPI	ban	1225
http:scan	CAPI	ban	3279
ssh:bruteforce	CAPI	ban	1144
http:crawl	CAPI	ban	144
ssh:exploit	CAPI	ban	27
vm-management:exploit	CAPI	ban	1

Dashboard (é possível ativar Web-Dashboard local ou na Cloud)





2C:
- Hub Crowdsec
– Quando um dos elementos despoleta uma regra para um ip, esse ip é partilhado e bloqueado por todas as maquinas que pertencem ao HUB
- HoneyPots Crowdsec
- Quando alertas despoletados redirecionar comunicações para HoneyPots

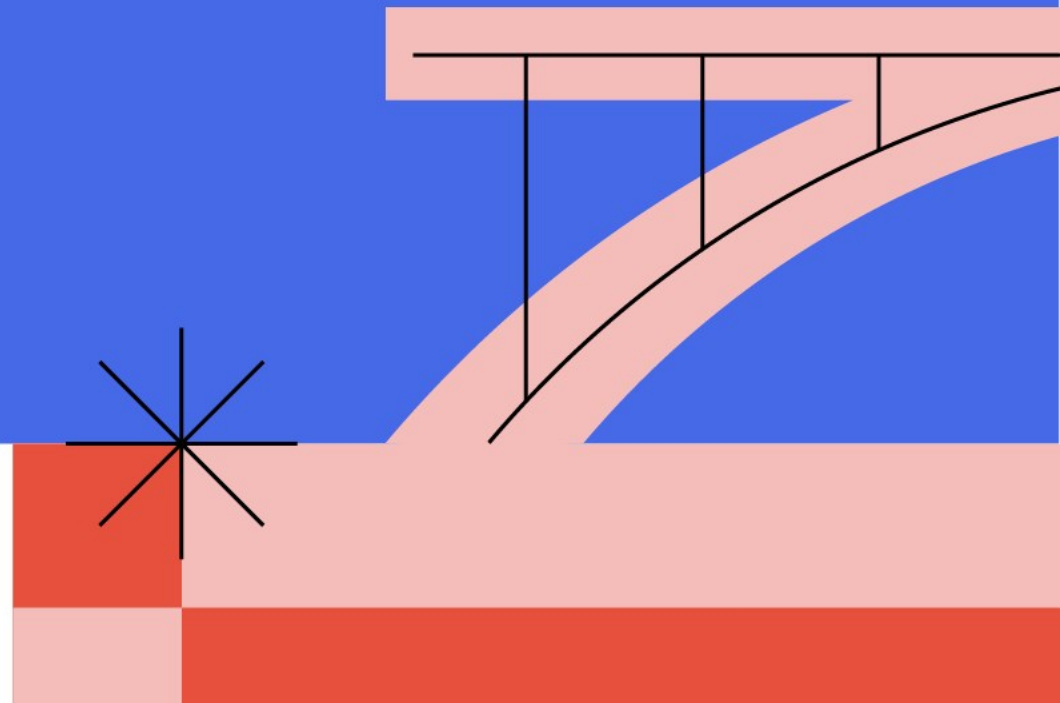
Mais Projectos OpenSource em curso:
- SOC – Security Onion

- Log centralizados de PaloAlto, office365, cloudflare, AD, etc
- Suricata para Sensores espalhados em pontos estratégicos na rede
- Agentes com alarmística e regras sigma, entre outras, no SOC
- etc

jornadas FCCN

Obrigado!

jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO