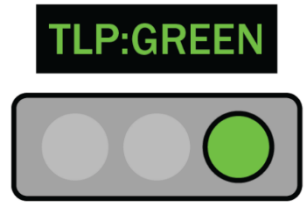


RNEP-GW

MÓDULO HONEYPOTS

fct csirt

RNEP-GW

O QUE SÃO HONEYPOTS?

Sistemas de segurança projetados para atrair, monitorar e analisar atividades maliciosas

“Iscas digitais”

O QUE SÃO HONEYPOTS?

Casa falsa = honeypot

Casa verdadeira = sistemas reais e críticos

Ladrão = o invasor

Subsolo = rede isolada, backup seguro ou segmentação

HISTÓRIA DO USO DE HONEYPOTS

1980-90: Primeiras armadilhas

1989: The Cuckoo's Egg

2000: Honeynet Project

Hoje: Parte de estratégias de defesa e pesquisa de ameaças

TIPOS DE HONEYPOTS

Por nível de interação

Baixa Interação: simulam apenas partes de um sistema ou serviços básicos. Ex.: Honeyd

Alta interação: Sistemas reais (ou quase) com vulnerabilidades propositais. Ex: Cowrie

Interação média: Simulam mais do que um serviço básico, mas não são máquinas completas. Ex.: Dionaea

TIPOS DE HONEYPOTS

Por objetivo

Pesquisa (Research Honeypots)

- Para entender novas ameaças e comportamentos de invasores
- Usadas por universidades, equipas de segurança e grandes empresas

Produção (Production Honeypots)

- Implantadas em redes reais como parte da defesa
- Servem para distrair invasores ou detetar movimentos suspeitos

Client Honeypots

- São proativas: não esperam ser atacadas, buscam servidores maliciosos

EXEMPLOS PRÁTICOS

Honeynet Project (rede global)

Equipas de segurança especializadas e ISPs

Equipas de resposta a incidentes

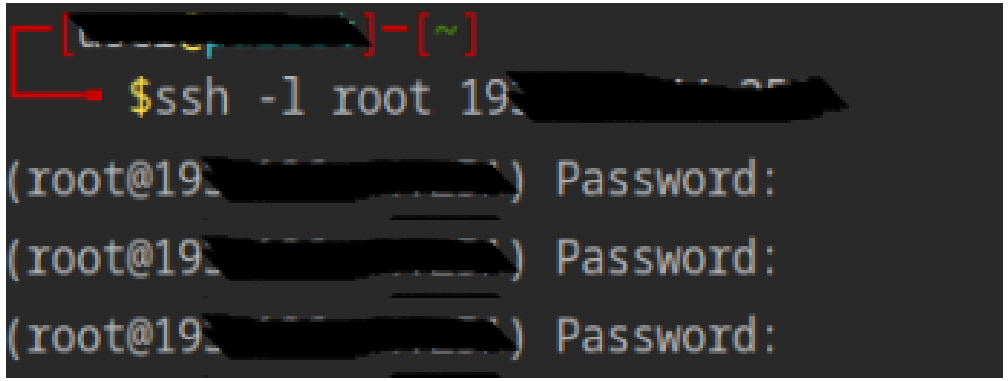
T-POT

Sistema de honeypots com 20+ tipos de honeypots

Open source

Elastic Stack

T-POT – SIMULAÇÃO DE ATAQUE



123456

root

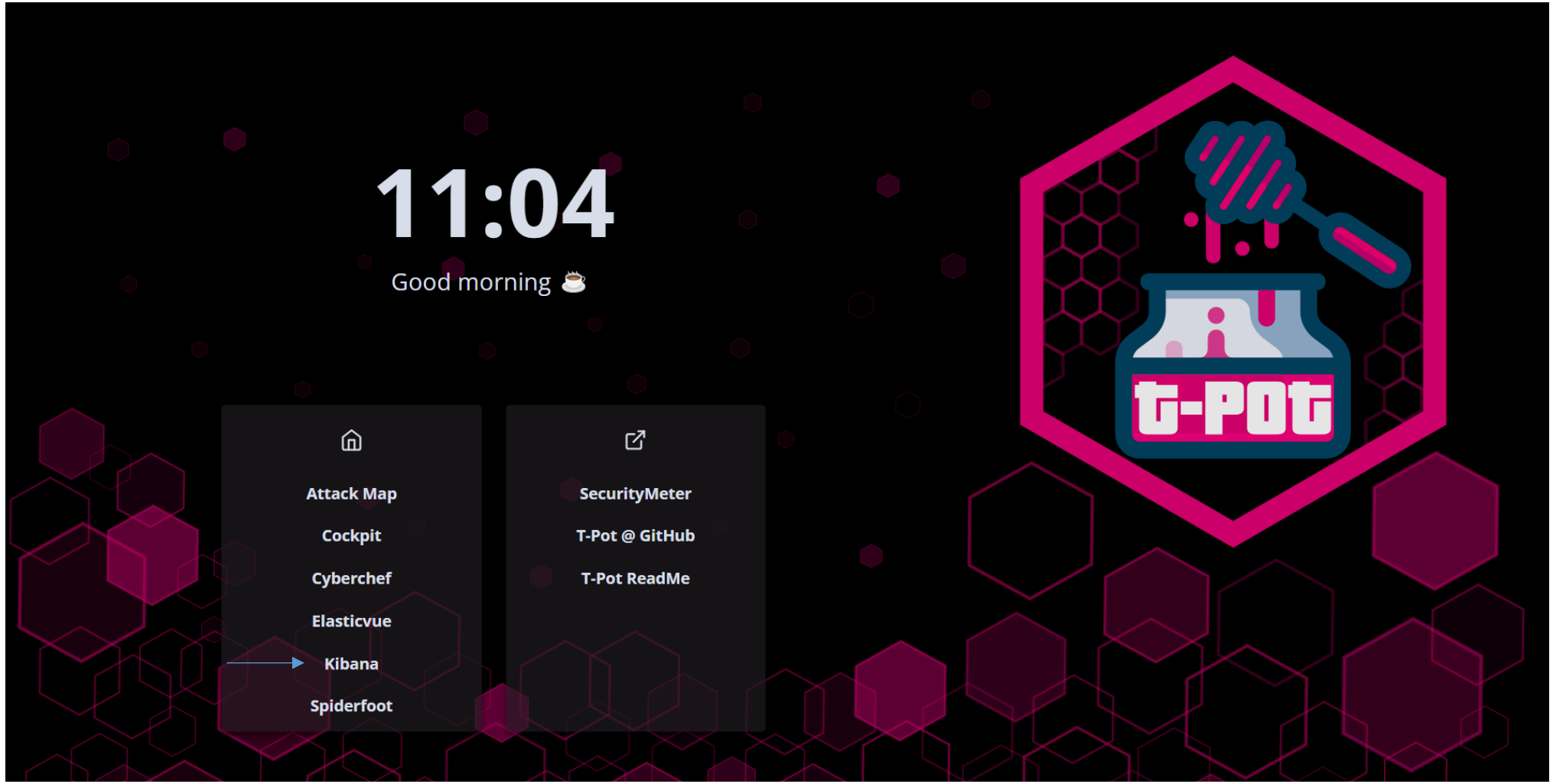
(empty)

T-POT – SIMULAÇÃO DE ATAQUE

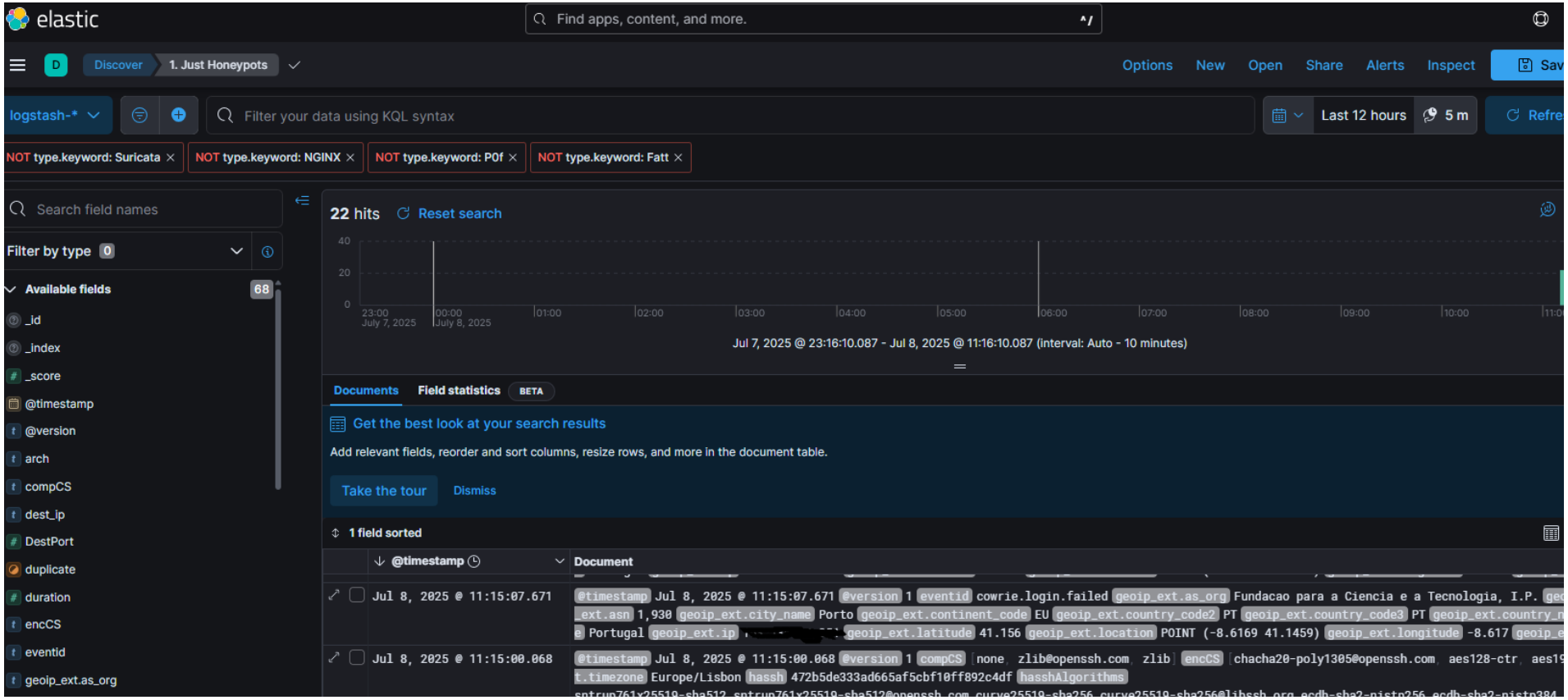
```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@ubuntu:~# pwd
/root
root@ubuntu:~# ls -la
drwx------ 1 root root 4096 2013-04-05 12:25 .
drwxr-xr-x 1 root root 4096 2013-04-05 12:03 ..
drwx------ 1 root root 4096 2013-04-05 11:58 .aptitude
-rw-r--r-- 1 root root  570 2013-04-05 11:52 .bashrc
-rw-r--r-- 1 root root  140 2013-04-05 11:52 .profile
drwx------ 1 root root 4096 2013-04-05 12:05 .ssh
root@ubuntu:~# Connection to [redacted] closed.
```

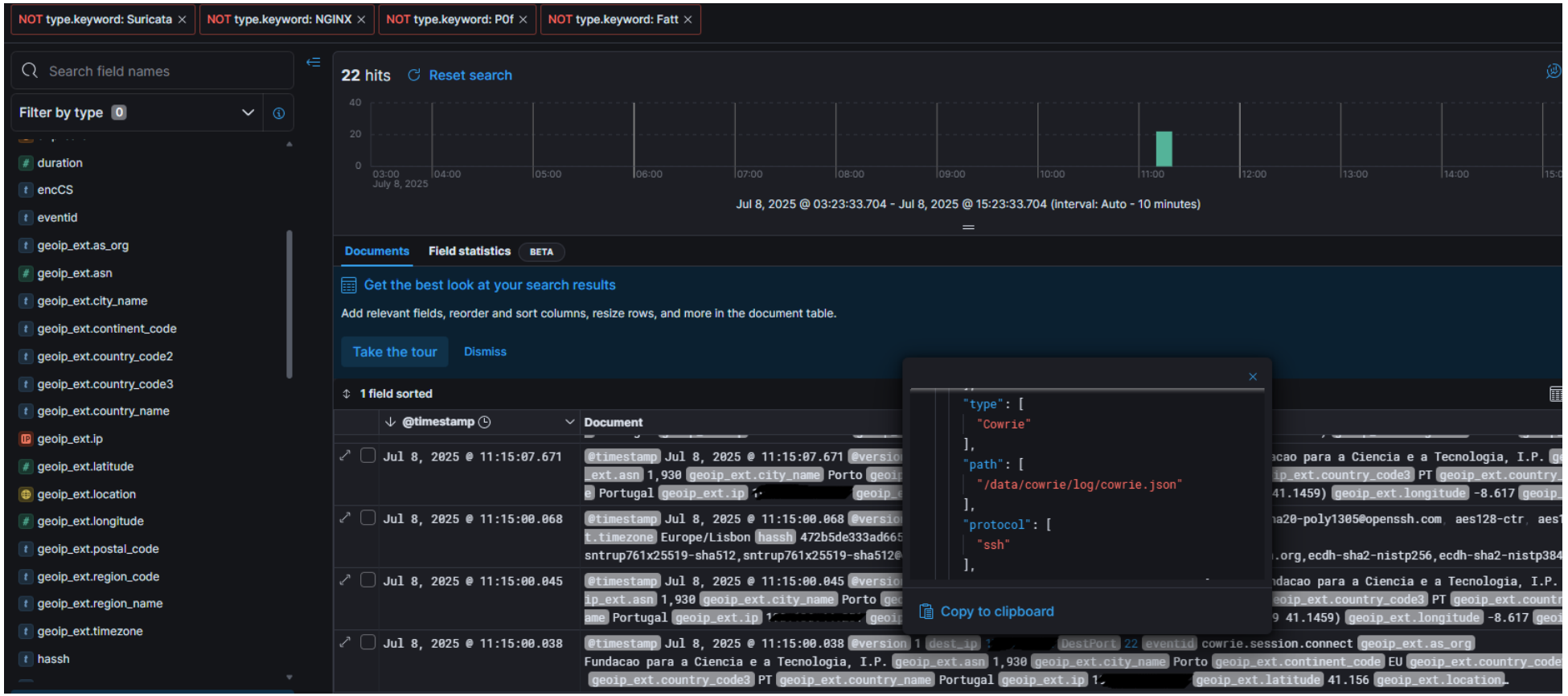
T-POT - LOGS


11:04
Good morning
Attack Map
Cockpit
Cyberchef
Elasticvue
Kibana
Spiderfoot
SecurityMeter
T-Pot @ GitHub
T-Pot ReadMe
t-POT

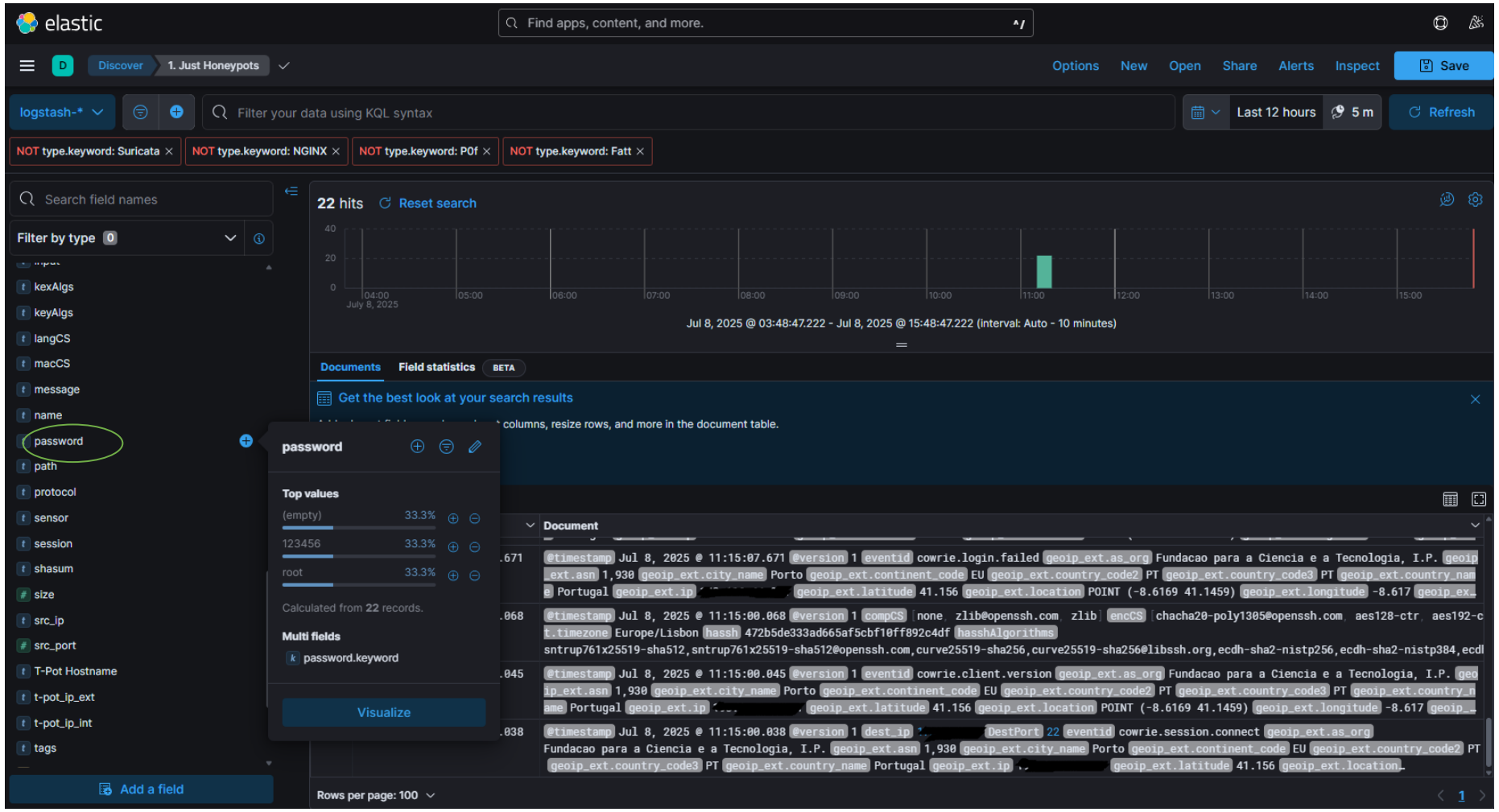
T-POT - LOGS


elastic
Find apps, content, and more.
Discover
1. Just Honeypots
Options
New
Open
Share
Alerts
Inspect
logstash-*
Filter your data using KQL syntax
Last 12 hours
5 m
NOT type.keyword: Suricata
NOT type.keyword: NGINX
NOT type.keyword: P0f
NOT type.keyword: Fatt
Search field names
Filter by type 0
Available fields 68
_id
_index
_score
@timestamp
@version
arch
compCS
dest_ip
DestPort
duplicate
duration
encCS
eventid
geoip_ext.as_org
22 hits
Reset search
Jul 7, 2025 @ 23:16:10.087 - Jul 8, 2025 @ 11:16:10.087 (interval: Auto - 10 minutes)
Documents
Field statistics
BETA
Get the best look at your search results
Add relevant fields, reorder and sort columns, resize rows, and more in the document table.
Take the tour
Dismiss
1 field sorted
@timestamp
Document
Jul 8, 2025 @ 11:15:07.671
Jul 8, 2025 @ 11:15:00.068

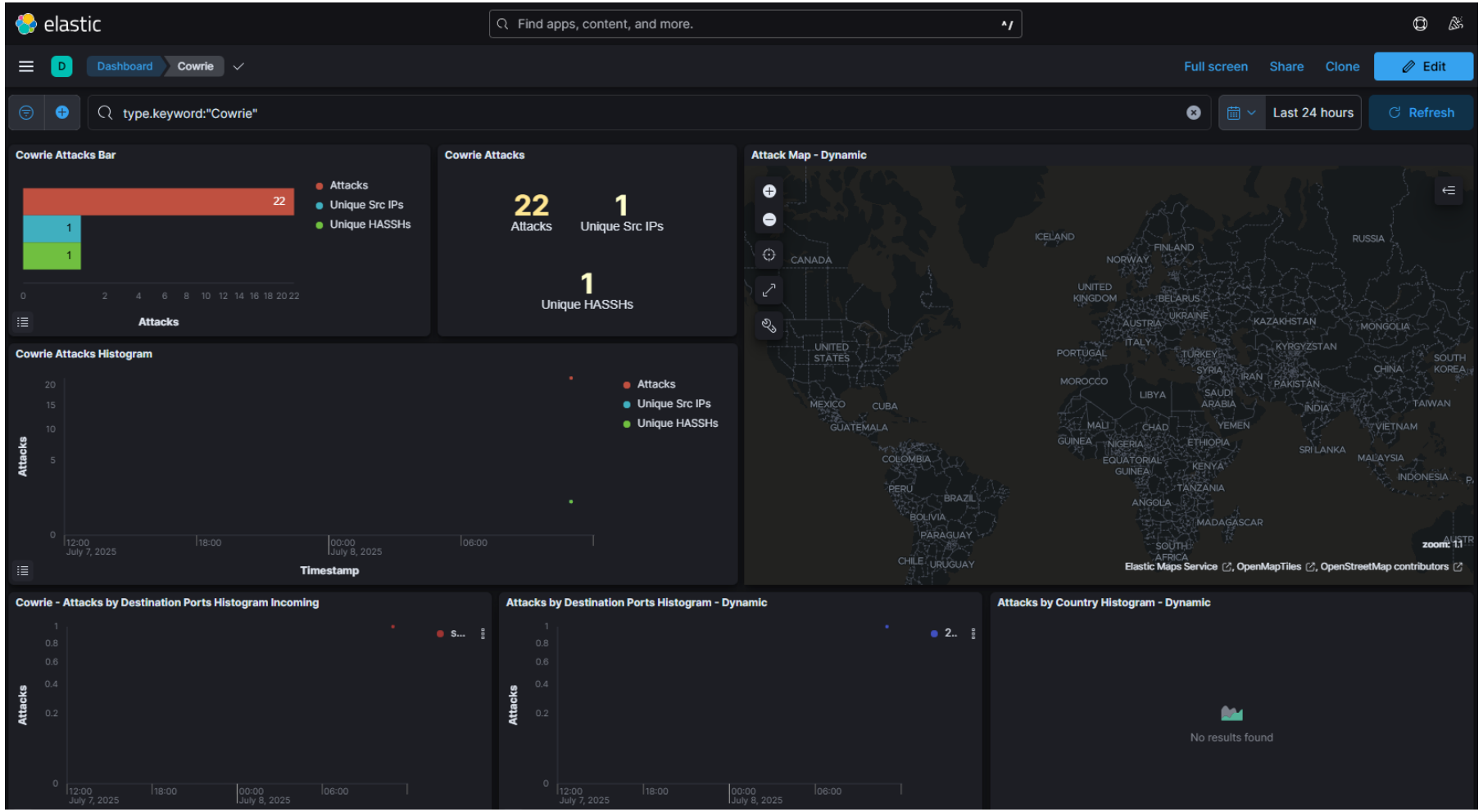
T-POT - LOGS


NOT type.keyword: Suricata
NOT type.keyword: NGINX
NOT type.keyword: P0f
NOT type.keyword: Fatt
Search field names
Filter by type 0
duration
encCS
eventid
geoip_ext.as_org
geoip_ext.asn
geoip_ext.city_name
geoip_ext.continent_code
geoip_ext.country_code2
geoip_ext.country_code3
geoip_ext.country_name
geoip_ext.ip
geoip_ext.latitude
geoip_ext.location
geoip_ext.longitude
geoip_ext.postal_code
geoip_ext.region_code
geoip_ext.region_name
geoip_ext.timezone
hassh
22 hits
Reset search
Jul 8, 2025 @ 03:23:33.704 - Jul 8, 2025 @ 15:23:33.704 (interval: Auto - 10 minutes)
Documents
Field statistics
BETA
Get the best look at your search results
Add relevant fields, reorder and sort columns, resize rows, and more in the document table.
Take the tour
Dismiss
1 field sorted
@timestamp
Document
"type": [
"Cowrie"
],
"path": [
"/data/cowrie/log/cowrie.json"
],
"protocol": [
"ssh"
],
Copy to clipboard

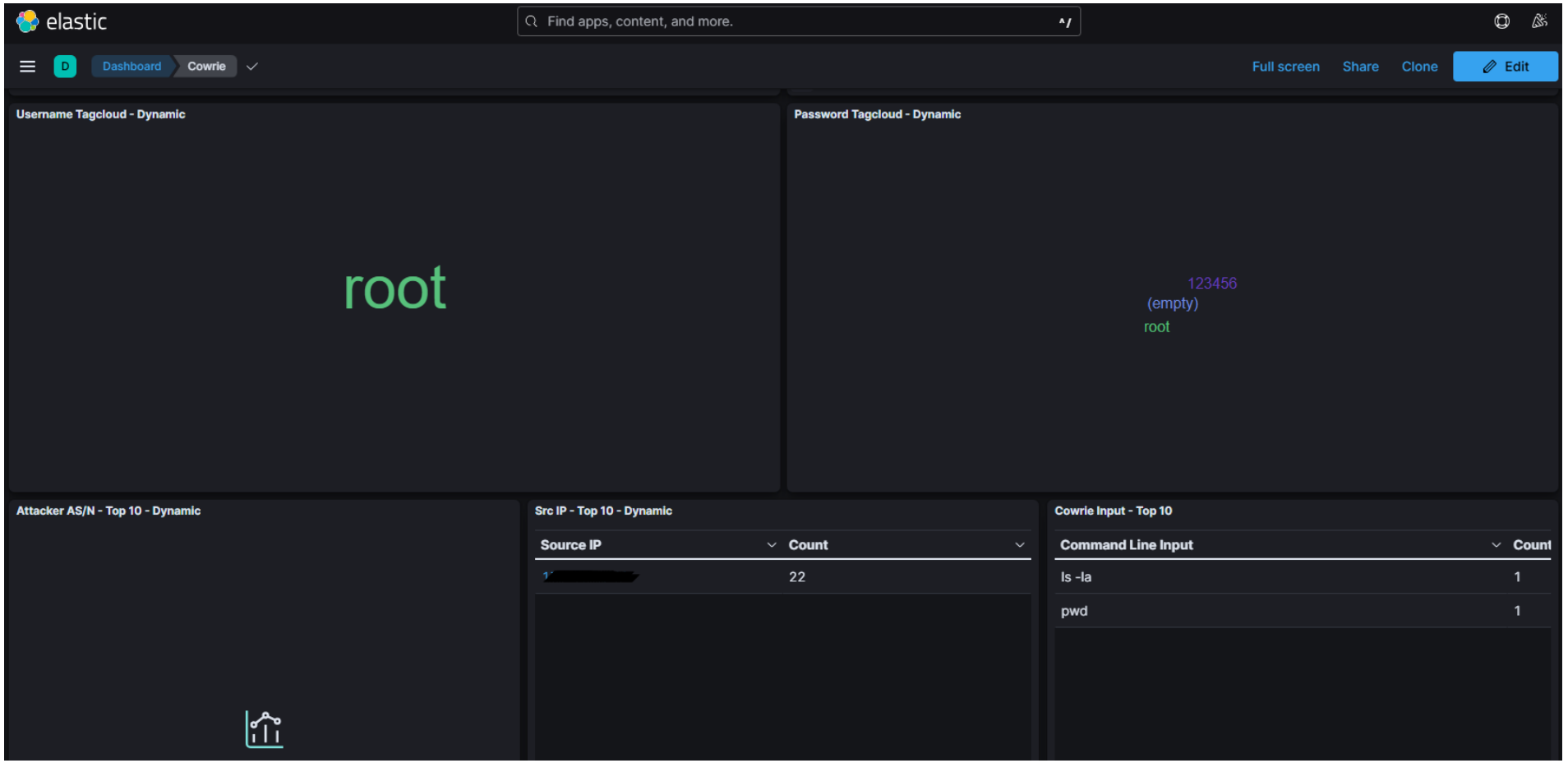
T-POT - LOGS


elastic
Find apps, content, and more.
Discover
1. Just Honeypots
Options
New
Open
Share
Alerts
Inspect
Save
logstash-*
Filter your data using KQL syntax
Last 12 hours
5 m
Refresh
NOT type.keyword: Suricata
NOT type.keyword: NGINX
NOT type.keyword: P0f
NOT type.keyword: Fatt
Search field names
Filter by type 0
22 hits
Reset search
Jul 8, 2025 @ 03:48:47.222 - Jul 8, 2025 @ 15:48:47.222 (interval: Auto - 10 minutes)
Documents
Field statistics
BETA
Get the best look at your search results
columns, resize rows, and more in the document table.
kexAlgs
keyAlgs
langCS
macCS
message
name
password
path
protocol
sensor
session
shasum
size
src_ip
src_port
T-Pot Hostname
t-pot_ip_ext
t-pot_ip_int
tags
Add a field
password
Top values
(empty) 33.3%
123456 33.3%
root 33.3%
Calculated from 22 records.
Multi fields
password.keyword
Visualize
Document
Rows per page: 100

T-POT - DASHBOARD



T-POT - DASHBOARD



T-POT - ALERTA

Event from Cowrie occurred on sensor vlan-[redacted]

timestamp: 2025-07-08T10:15:00.068850Z
type: Cowrie

Detected connection by vlan-[redacted] 1[redacted]
*** Details if available:
- Honeypot: Cowrie
- Source IP: 1[redacted]
- Destination Port: <MISSING VALUE>
- Related Message: login attempt [root/123456] failed
- Username: root
- Password: 123456
- Method: <MISSING VALUE>
* FULL LOG BELLOW *

VANTAGENS E DESVANTAGENS

VANTAGENS ✓	DESVANTAGENS ⚠
Coleta de inteligência real	Risco de comprometimento
Baixo volume de falsos positivos	Manutenção e monitoramento constante
Funciona como distração	Deteção por atacantes experientes
Custo relativamente baixo	Não substituem defesas tradicionais

QUESTÕES ÉTICAS E LEGAIS

ÉTICA	LEGALIDADE
Consentimento do invasor	Leis de privacidade e monitoramento
Risco de coletar dados de terceiros	Responsabilidade civil
Isolamento para não causar danos indesejados	Uso de logs como evidência

IDEIAS CHAVE

- Honeypots são armadilhas digitais que ajudam a entender, detetar e responder a ataques
- Possuem riscos e exigem responsabilidade
- Complementam, mas não substituem, outros tipos de defesa

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc