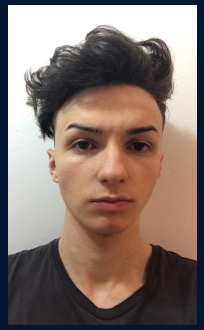
THEHIVE PROJECT

SIRP for SOC

Daniel Pérez Llurba
2ASIX-Ciber - INS Pedralbes

QUÈ DIR SOBRE NOSALTRES?



- **Daniel Pérez Llurba, 21**
  (Cybersecurity analyst)

- **Grail CyberTech**
  (Empresa Sector Ciberseguretat)

QUÈ VEUREM AVUI?

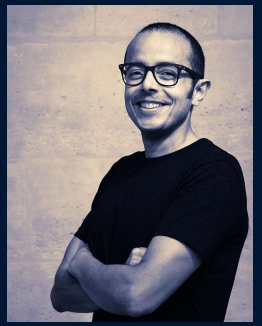
El nostre servei es basa en:

1. Què és aquest servei?
2. Qui ho ha fet possible?
3. Com ho fem?
4. Què fem utilitzar?
5. Perquè nosaltres?
6. Dubtes
7. Contacte

QUI HA DESENVOLUPAT AIXÒ?

NABIL

FRANCO



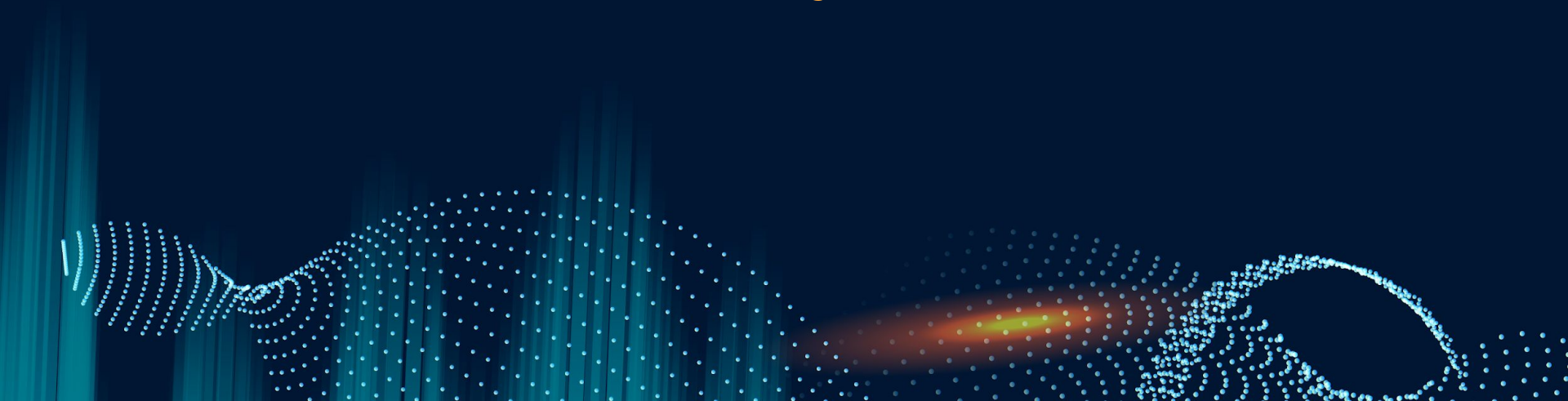
SAÂD KADHI

"cualquier producto que sale al mercado presenta vulnerabilidades y cualquier vulnerabilidad del mundo constituye una puerta de entrada a la amenaza".

— Luis Delgado Jiménez

EINES INTEGRADES

Contingut



THEHIVE

ETIQUETAR

Creem casos arràn d'alertes generades d'alimentadors, etc.

CORTEX

ACTUAR

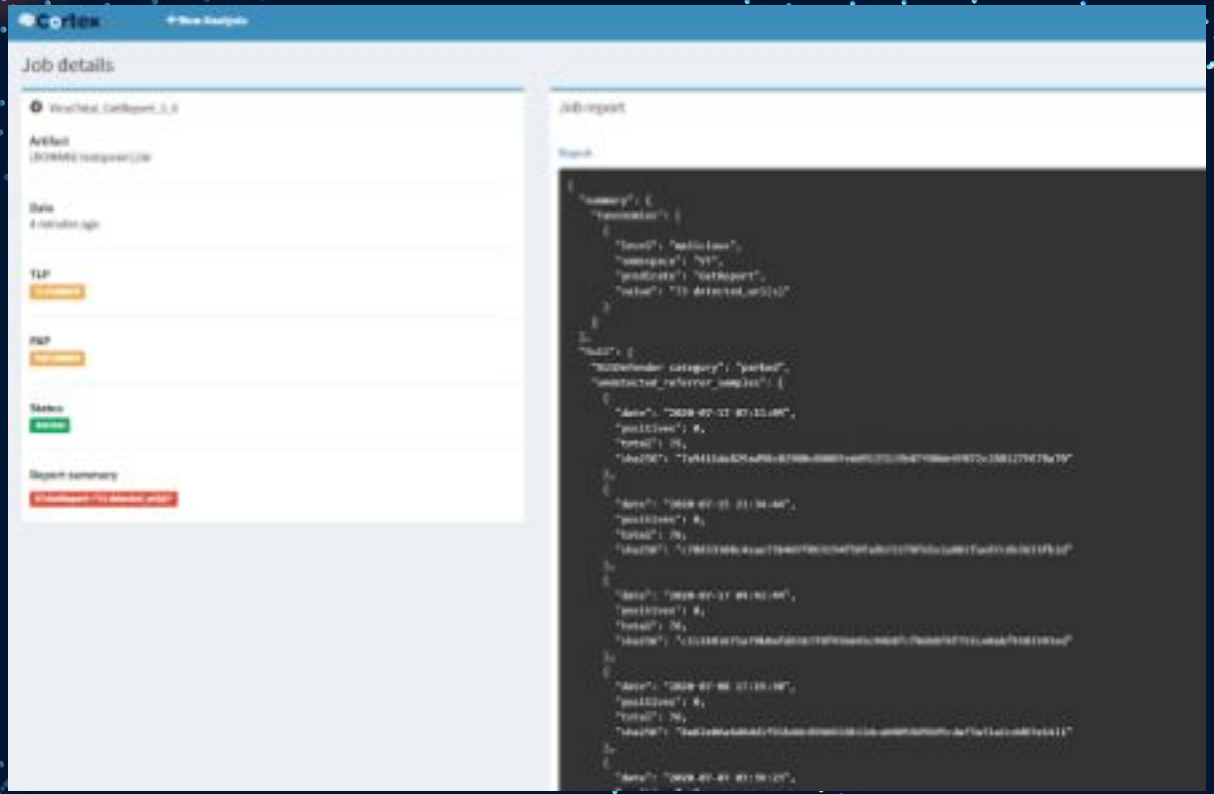
Comprovem si un IOC és maliciós

MISP

COMPARTIR

Compartim el producte de ciberintel·ligència amb tercers


TheHive
List of observables


Cortex
+ New Analysis
Job details
Artifact
TLP
PAP
Tokens
Report summary
Job report

OSINT - CVE-2015-2545: overview of current threats

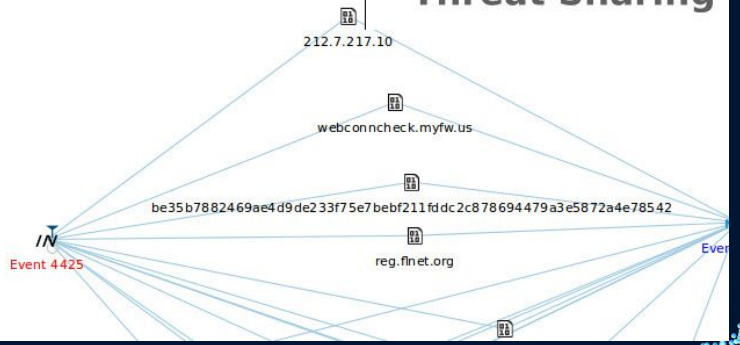
Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Related Even

2016-05-27 (3883)
2016-05-23 (3844)
2016-05-06 (3828)

Orgc: CIRCL
Date: 2016-05-23
Info: OSINT - Operation Ke3chang
Resurfaces With New TidePool Malware

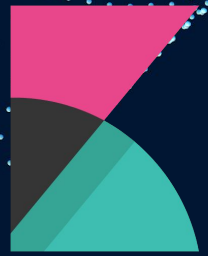
MISP Threat Sharing



Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbale - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

30%

Només comparteixen
activament dades en MISP



FILEBEAT

RECOLLIR

Amb aquest paquet recollim logs

ELASTICSEARCH

EMMAGATZE MAR

En el nostre sistema generem tickets

KIBANA

MOSTRAR

S'ha de veure en Dashboards


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Swap usage (Metricbea...
Memory usage vs total
Number of processes [...
Disk used (Metricbeat ...
Disk Usage [Metricbeat System]
Swap usage
0%
Memory usage
2.9GB
Total Memory 3.3GB
processes
28
Disk used
32.77%
46.7%
0.2%
CPU Usage [Metricbeat System]
System Load [Metricbeat System]
Memory Usage [Metricbeat System]
Disk IO (Bytes) [Metricbeat System]

Geolocalitzar en un futur

DDoS

NMAP BRUTE FORCE

ELASTALERT

ALERTAR

Generem alertes en base ES

Grafana

GRAFANA

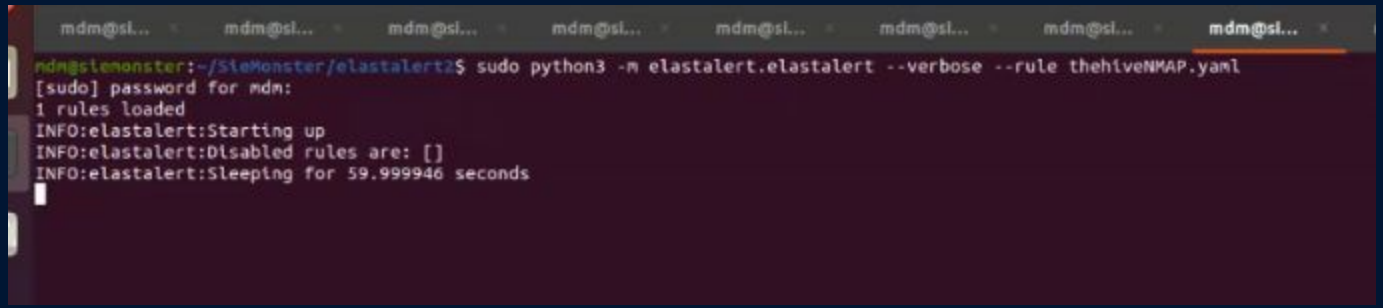
VISUALITZAR

Visualitzem en dashboards i fins i tot podem notificar al SOC, CSIRT, etc.

TELEGRAM

NOTIFICAR

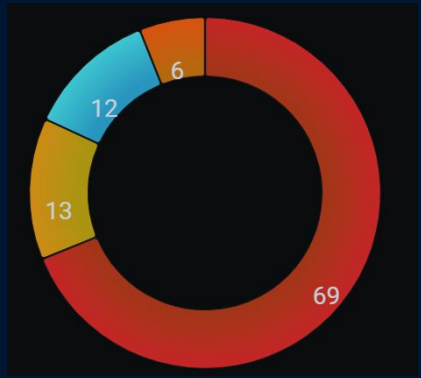
Gràcies a Grafana Alert, es pot notificar a l'equip adient


mdm@sl...
mdm@sl...
mdm@sl...
mdm@sl...
mdm@sl...
mdm@sl...
mdm@sl...
mdm@sl...
mdm@slemonster:~/SleMonster/elastalert2$ sudo python3 -m elastalert.elastalert --verbose --rule thehiveNMAP.yaml
[sudo] password for mdm:
1 rules loaded
INFO:elastalert:Starting up
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.999946 seconds

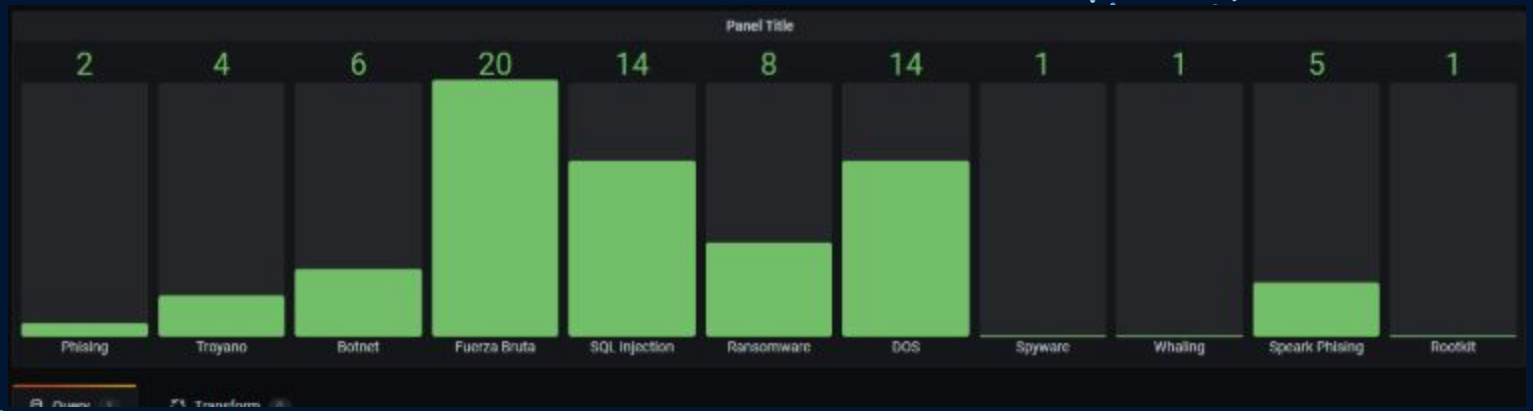
GRAFANA

Volem tenir tots els registres en dashboards que ens permetin fer observacions dels clients.

ELS ATACS I ELS CASOS ES MOSTREN



- DDoS
- NMAP
- HPING3
- SSH BRUTE FORCE


Panel Title
2
4
6
20
14
8
14
1
1
5
1
Phising
Troyano
Botnet
Fuerza Bruta
SQL Injection
Ransomware
DOS
Spyware
Whaling
Speark Phising
Rootkit

MOBILE WEB

Es vol que els nostres analistes rebin les alertes vía smartphone

dll created the group «SOC_Alertes»

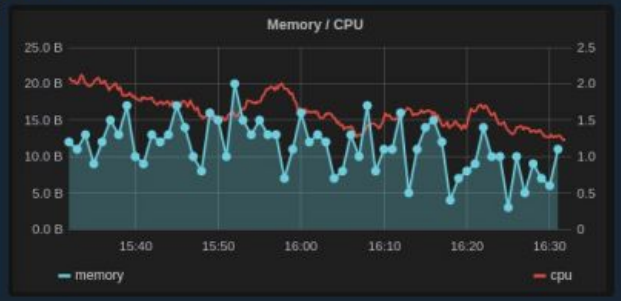
dll added DaniAlertaje

DaniAlertaje
[Alerting] Test notification
State: Test notification
Message: Someone is testing the alert notification within Grafana.
URL: https://10.200.0.35:3000/

Metrics:
High value: 100.000
Higher Value: 200.000
12:24

[Alerting] Test notification
State: Test notification
Message: Someone is testing the alert notification within Grafana.
URL: https://10.200.0.35:3000/
Image: https://grafana.com/assets/img/blog/mixed_styles.png

Metrics:
High value: 100.000
Higher Value: 200.000



D

12:26

SNORT

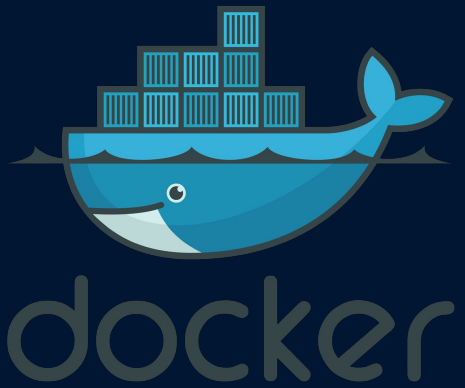
ESNIFAR

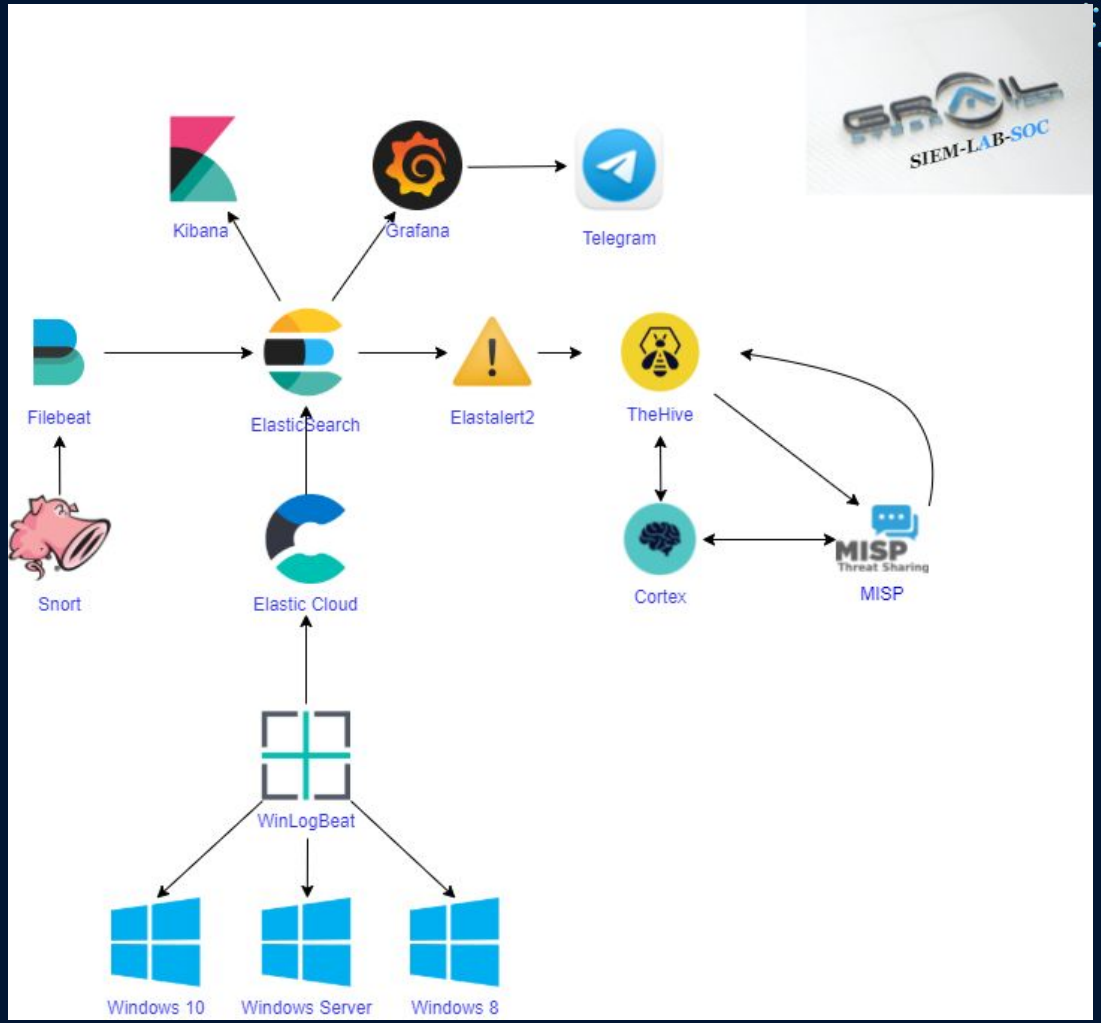
Amb aquest potent IDS veiem el trànsit de la xarxa (NIDS)


ndn@slemonster:/var/log/snort$ sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules -i ens18 -s 65535 -k none -l
/var/log/snort/

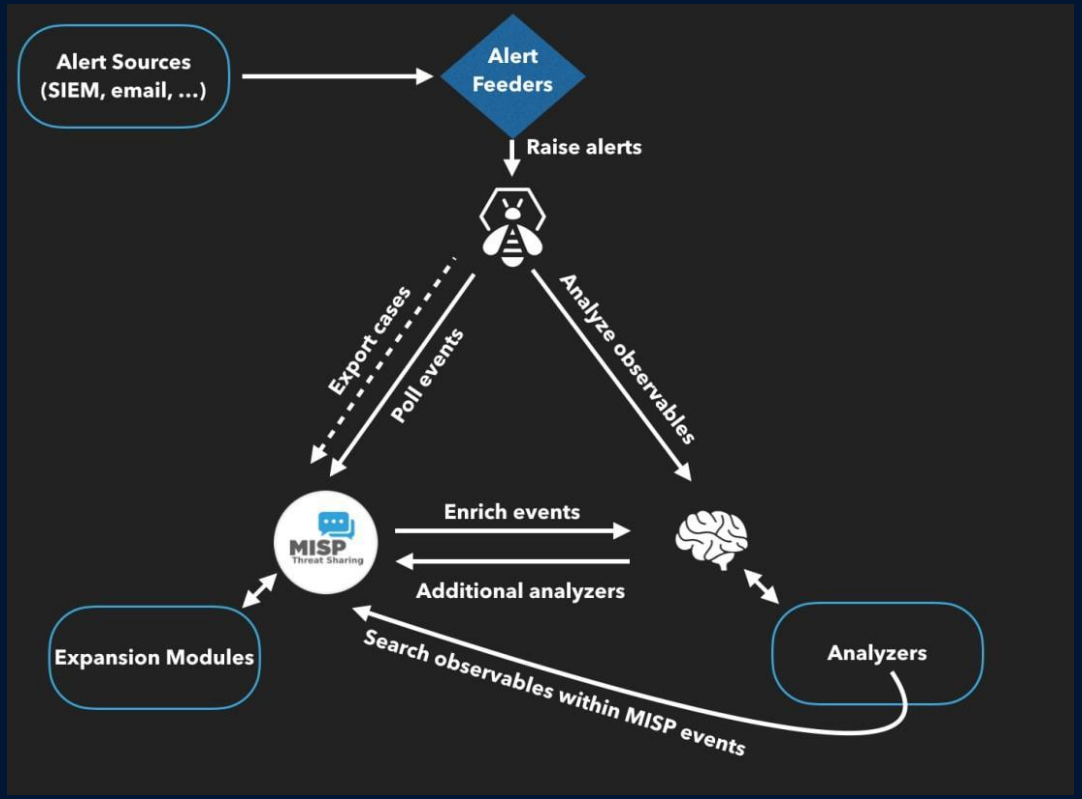
AIXECAMENT

Els serveis executats

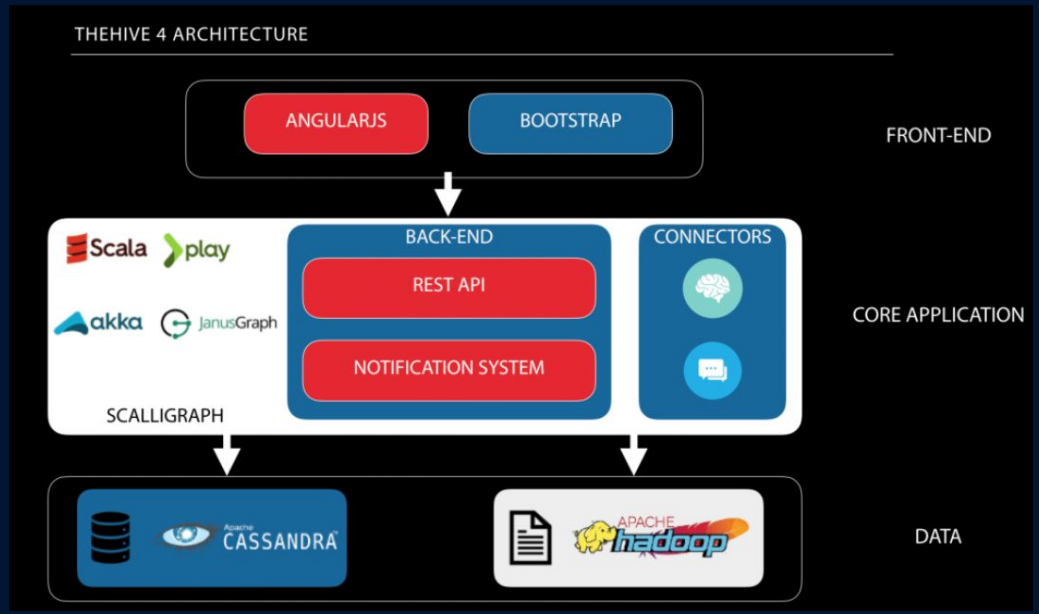



SIEM-LAB-SOC
Kibana
Grafana
Telegram
Filebeat
ElasticSearch
Elastalert2
TheHive
Snort
Elastic Cloud
Cortex
MISP
Threat Sharing
MISP
WinLogBeat
Windows 10
Windows Server
Windows 8

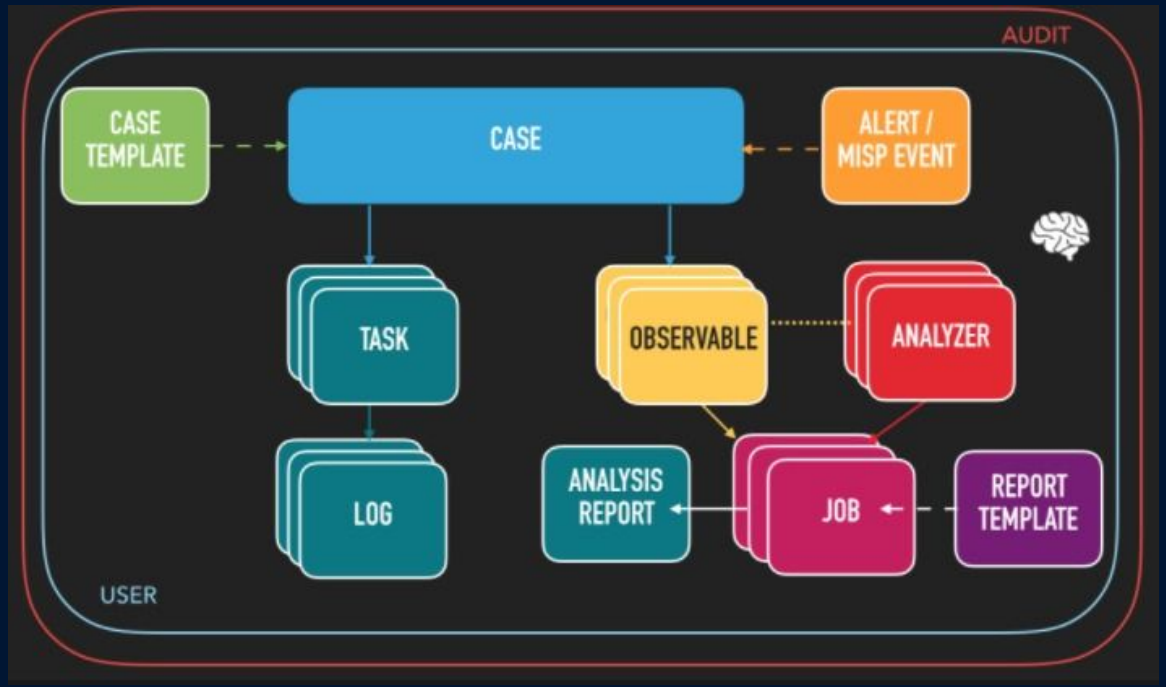
ESQUEMA



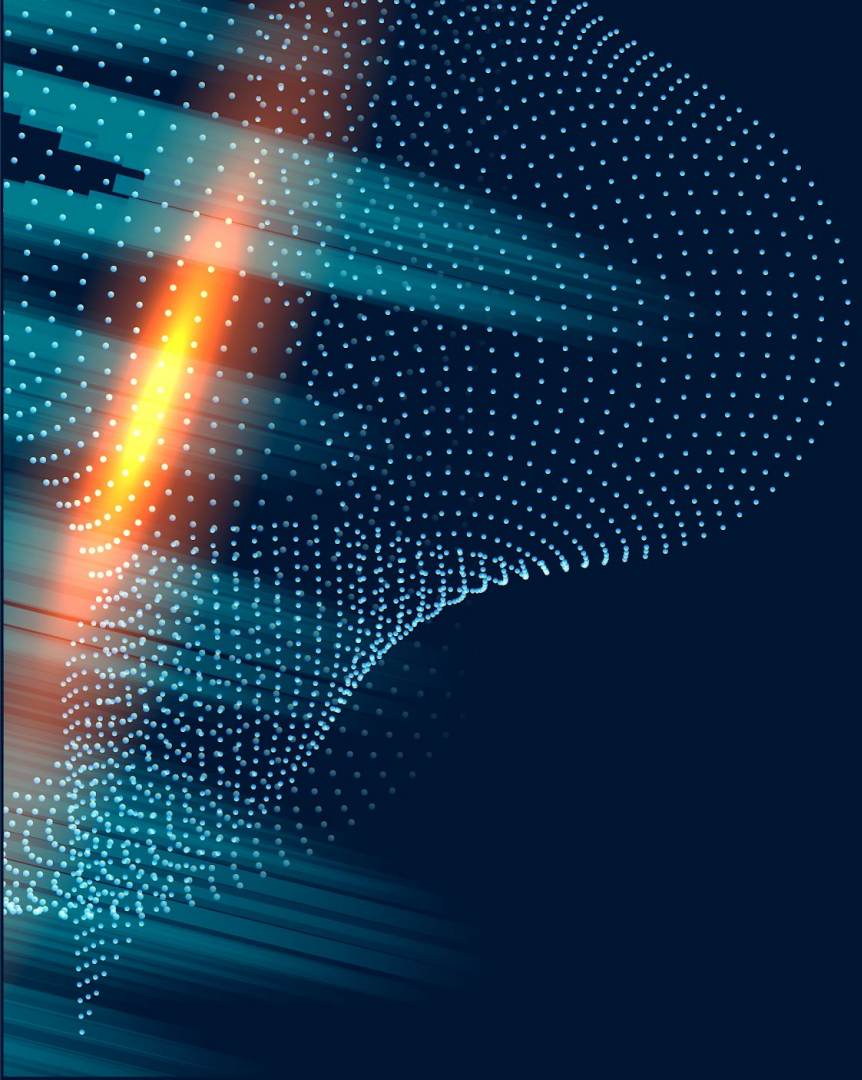
FUNCIONAMENT



FUNCIONAMENT



FUNCIONAMENT



ATAQUEN UN ENDPOINT

Què hem de fer?

01

ESNIFAR XARXA

Amb Snort esnifem els paquets .txt de Filebeat

02

RECOLLIR LOGS

Els registres són enviats a ES

03

INDEXAR

Volem indexar-los a ES

04

GRAFANA/KIBANA

Podem mostrar les dades

05

GENERAR CAS

Ens encarregariem de rebre el log, d'etiquetar-ho, crear ciberintel·ligència, etc.

06

RESPONDRE

Arràn del nostre ticket fariem una resposta adient per solventar el cas

07

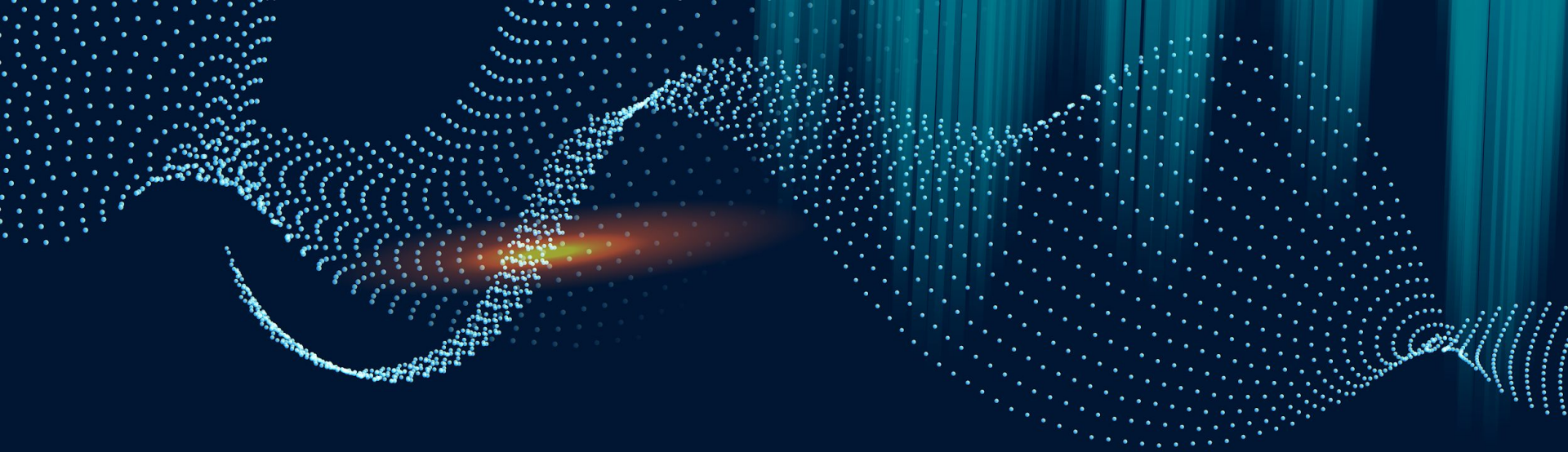
NOTIFICAR

Enviar als analistes vía Telegram dades

08

COMPARTIR

Divulgar la intel·ligència amb tercers

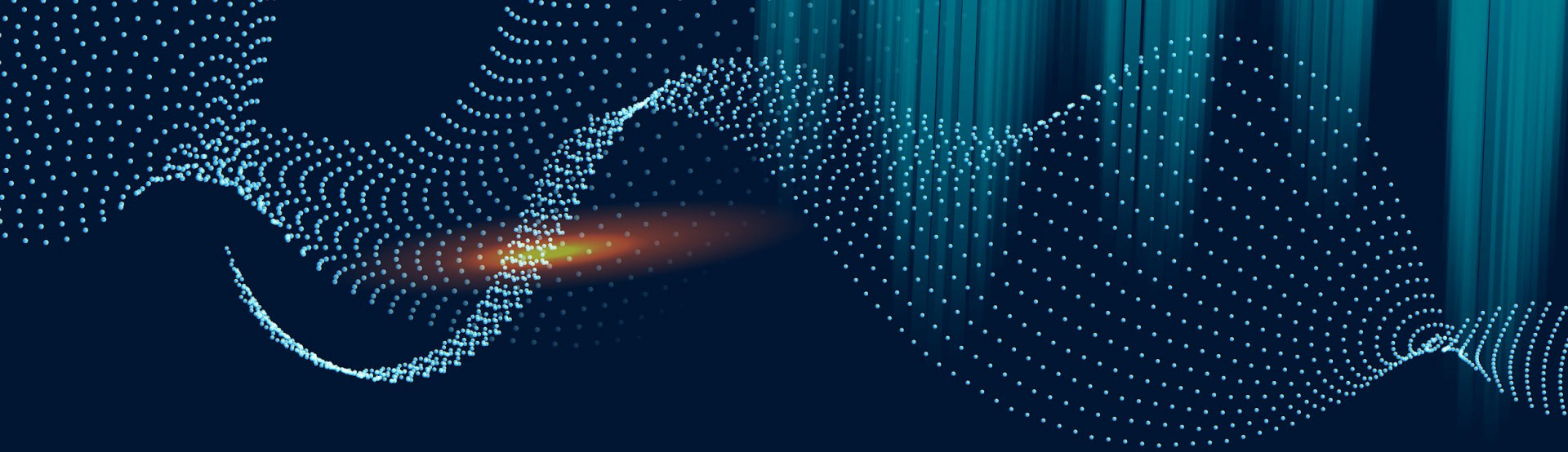


01 ESNIFAR XARXA

Com indexariem les dades del client

COM ESNIFAR?

SNORT



2+3 RECOLLIR+INDEXAR

Com indexar

COM FUNCIONA LA INDEXACIÓ?

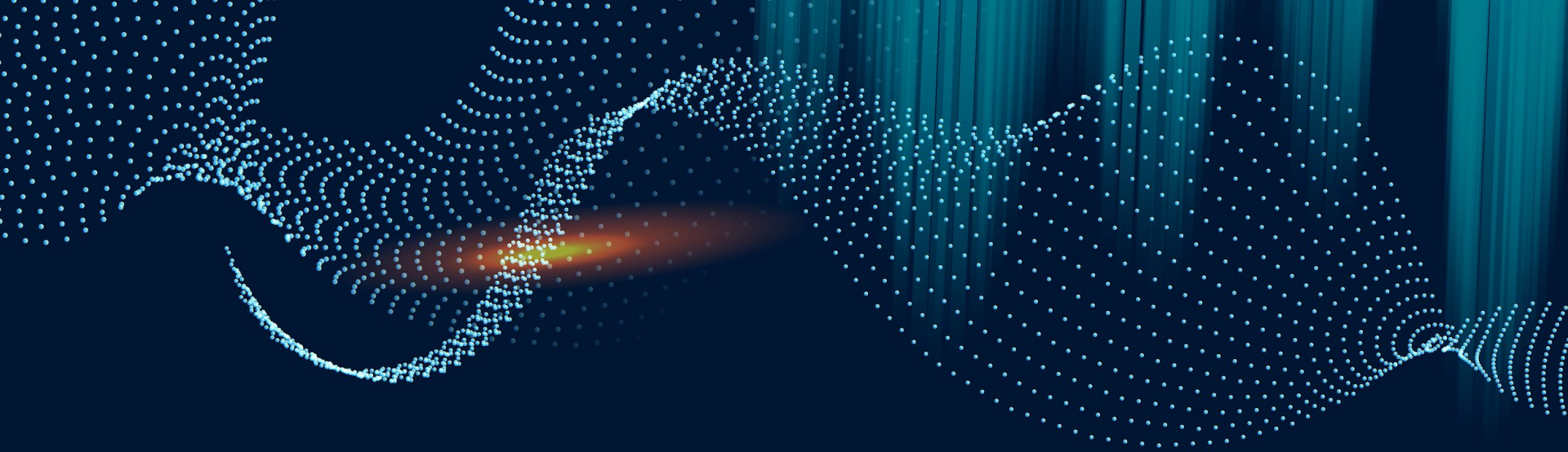
F E

AT

LOG

ELASTICSEARCH

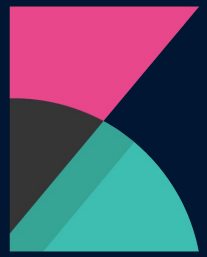
INDEX/DOC



04 VEURE

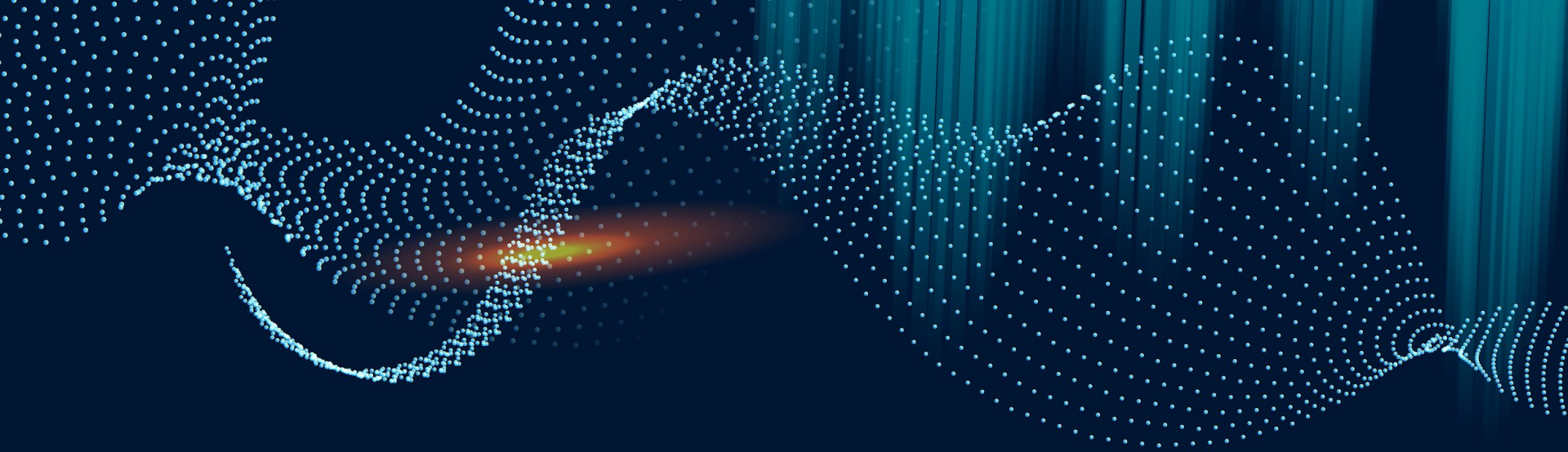
Com veure dades

COM VISUALITZAR?



GRAFANA/KIBANA

VEURE



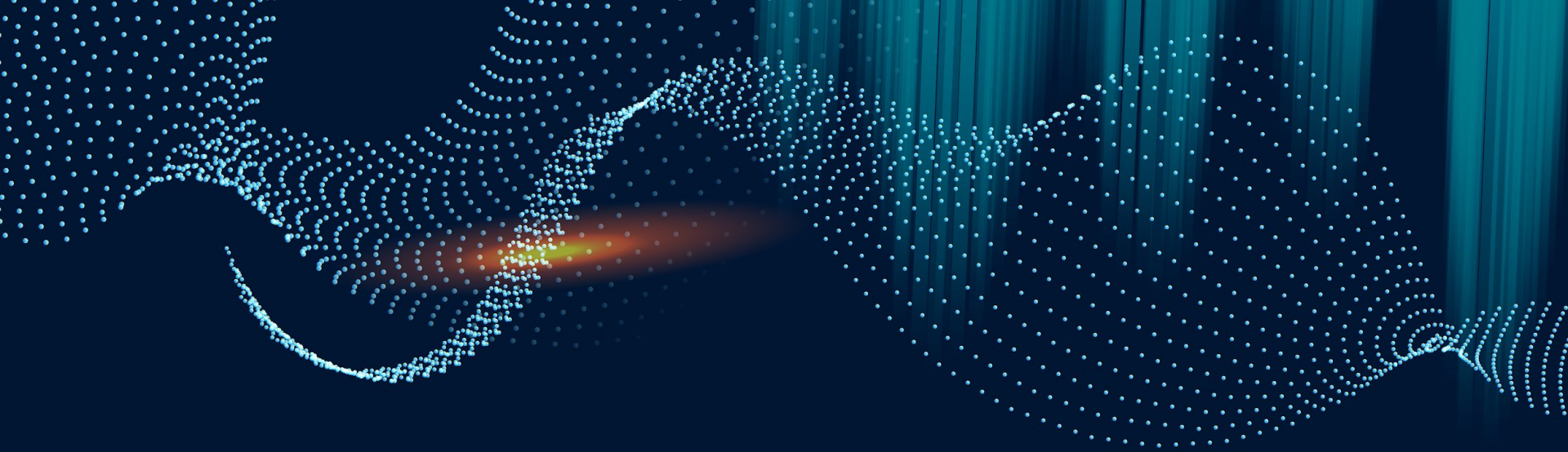
05 TICKETING

Com etiquetar els casos

COM ETIQUETAR?

THEHIVE

TICKET



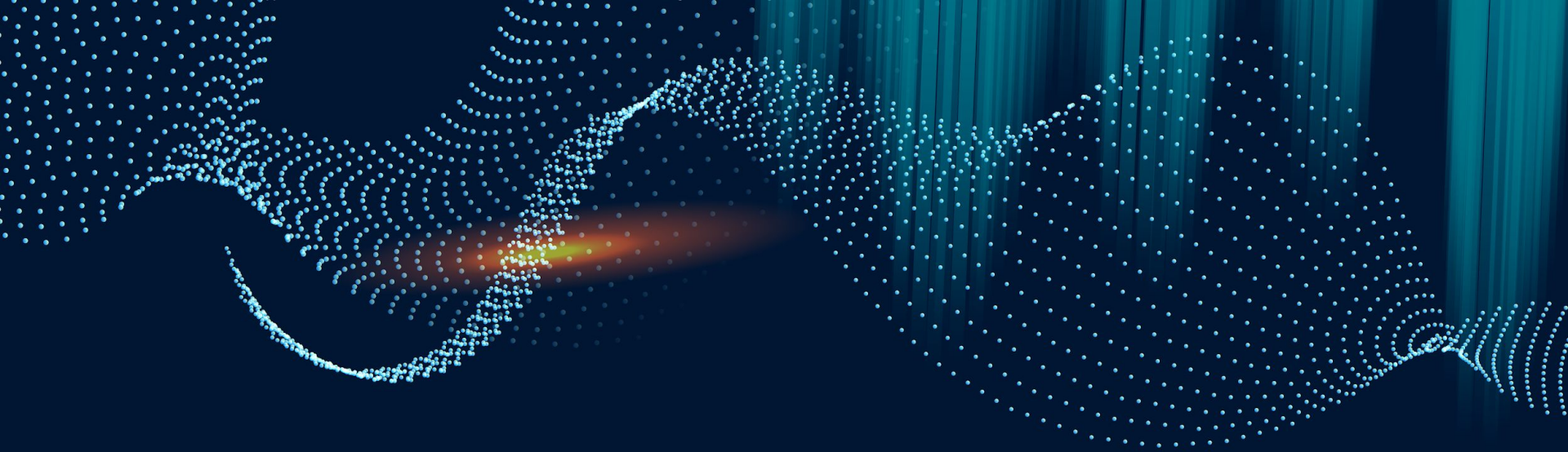
06 RESPONDRE

Com respondriem als casos

COM REACCIONAR?

CORTEX

RESPONDRE



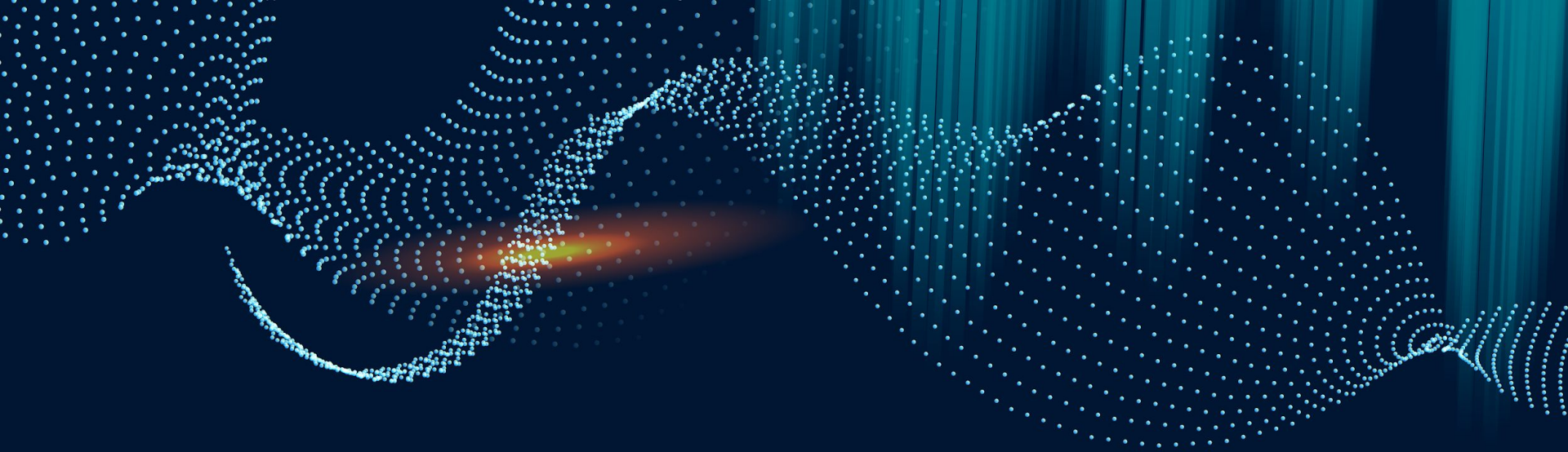
07 NOTIFICAR

Avisar als analistes

COM NOTIFICAR?

TELEGRAM

AVISAR



08 COMPARTIR

Com divulgar informació

COM COMPARTIR CIBERINTEL·LIGÈNCIA?

MISP

DIVULGAR

CRONOLOGIA FUTUR?

JUNY

TESTEJAR EN UN LAB

JULIOL

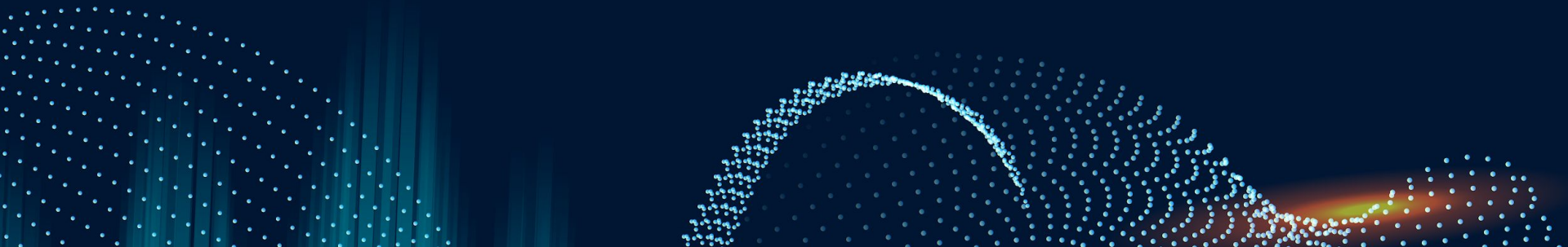
PORTAR-HO A PRODUCCIÓ

SETEMBRE

VENDRE EL SERVEI

NOVEMBRE

IMPLEMENTAR NOVES EINES

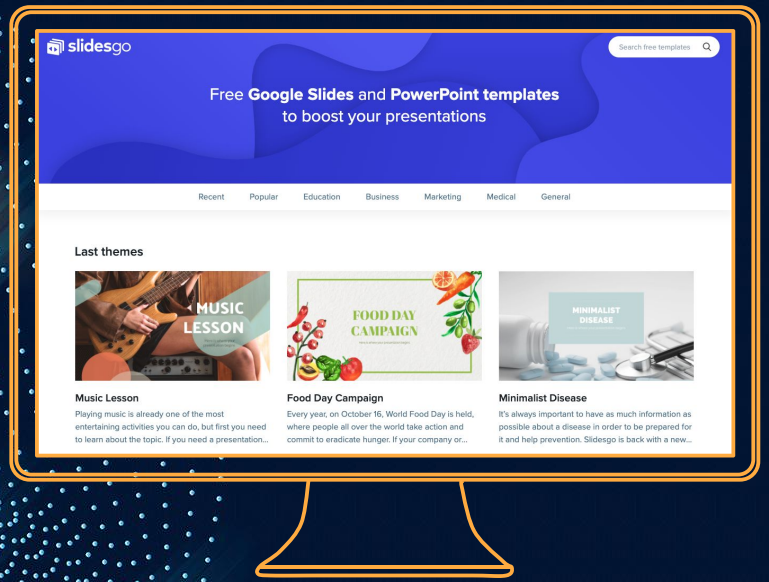


RESUM

Com funciona el nostre servei de resposta a incincidents de ciberseguretat

- Un client ens contracta
- El client rep l'atac
- Indexem els logs adients a ES
- Avisem als equips
- Responem
- Creem ciberintel·ligència

Perquè és necessari?



Qualsevol usuari pot rebre un atac en qualsevol moment, inclòs instal·lar malware per compte al·liè

PERQUÈ NOSALTRES?

Volem ser la millor competència en el mercat.

ESPERO QUE ENS CONTRACTEU

És molt important desenvolupar ciberseguretat en l'àmbit diari en qualsevol camp laboral

CONFIEU!

Teniu qualsevol dubte?

dani.perez.grail@gmail.com

+34 622926736 (B-3)

https://grailcyber.tech