DESPLEGAR L'EINA "ZEEK IDS" I LA SEVA POSTERIOR EXPLOTACIÓ PER A L'ANÀLISI D'ACTIVITATS SOSPITOSES A LA XARXA

Autor del TFM:

Adrià Adell Barbarà

Titulació:

Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions

Àrea:

Anàlisi de dades

Consultor:

Borja Guaita Perez

PRA:

Victor Garcia Font

Data:

06/2020

ÍNDEX


1. Introducció
Context i justificació
Objectius
Enfocament i mètode seguit
Planificació
2. Investigació i disseny
Escenari i Components HW/SW
Desenvolupament
Arquitectura final
3. Implantació i funcionament
Entorn de treball
Instal·lació i configuració de la solució
Detecció d'activitats sospitoses
Dashboards
Demostració del funcionament
4. Conclusions
Objectius plantejats
Seguiment de la planificació
Treball futur

ÍNDEX

INTRODUCCIÓ

CONTEXT I JUSTIFICACIÓ

- Necessitats
  - Protegir els pilars de la seguretat de la informació
  - Minimitzar els riscos de seguretat
- Que podem fer?
  - Monitoritzar el tràfic de la xarxa amb un IDS
  - Actuar ràpidament en cas d'observar activitats o incidents de seguretat

INTRODUCCIÓ

OBJECTIUS

Desplegar Zeek IDS, per a la detecció d'activitats sospitoses a la xarxa i representació en Dashboards mitjançant ELK Stack

- Anàlisi dels requeriments hardware/software: Switch, Raspberry Pi, Oracle VirtualBox...
- Estudi sobre les eines a utilitzar i la seva integració: Zeek, Beats, Elasticsearch, Logstash, Kibana...
- Pla de proves
- Memòria del treball

INTRODUCCIÓ

ENFOCAMENT I MÈTODE SEGUIT

- Etapa 1: Pla de treball
- Etapa 2: Investigació i estudi
- Etapa 3: Implantació de la solució
- Etapa 4: Presentació

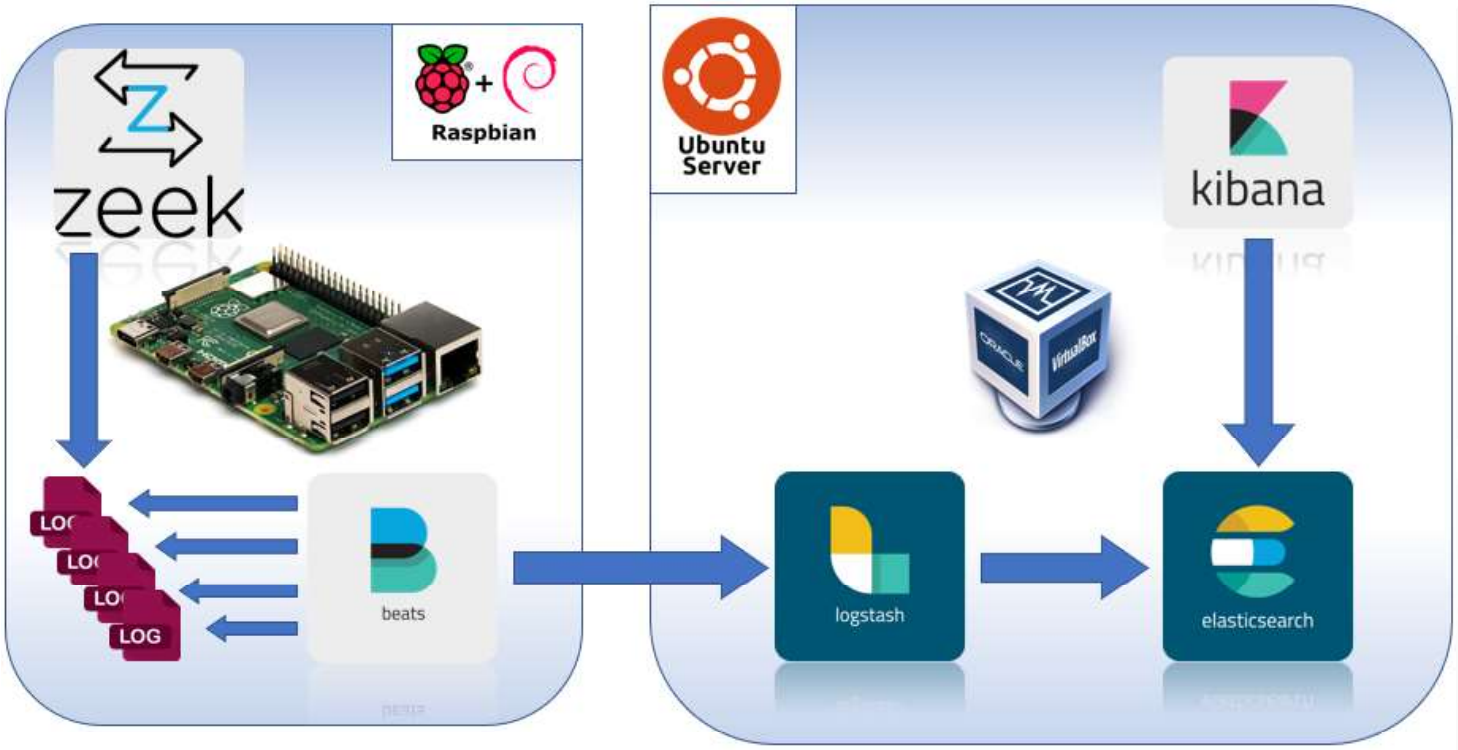
INTRODUCCIÓ

PLANIFICACIÓ

ÍNDEX

INVESTIGACIÓ I DISSENY

ESCENARI I COMPONENTS



INVESTIGACIÓ I DISSENY

DESENVOLUPAMENT

Infraestructura de xarxa: Router, switch i Raspberry Pi

Capturar el tràfic de la xarxa: Zeek IDS

Recol·lectar fitxers de registre: Beats (Filebeat)

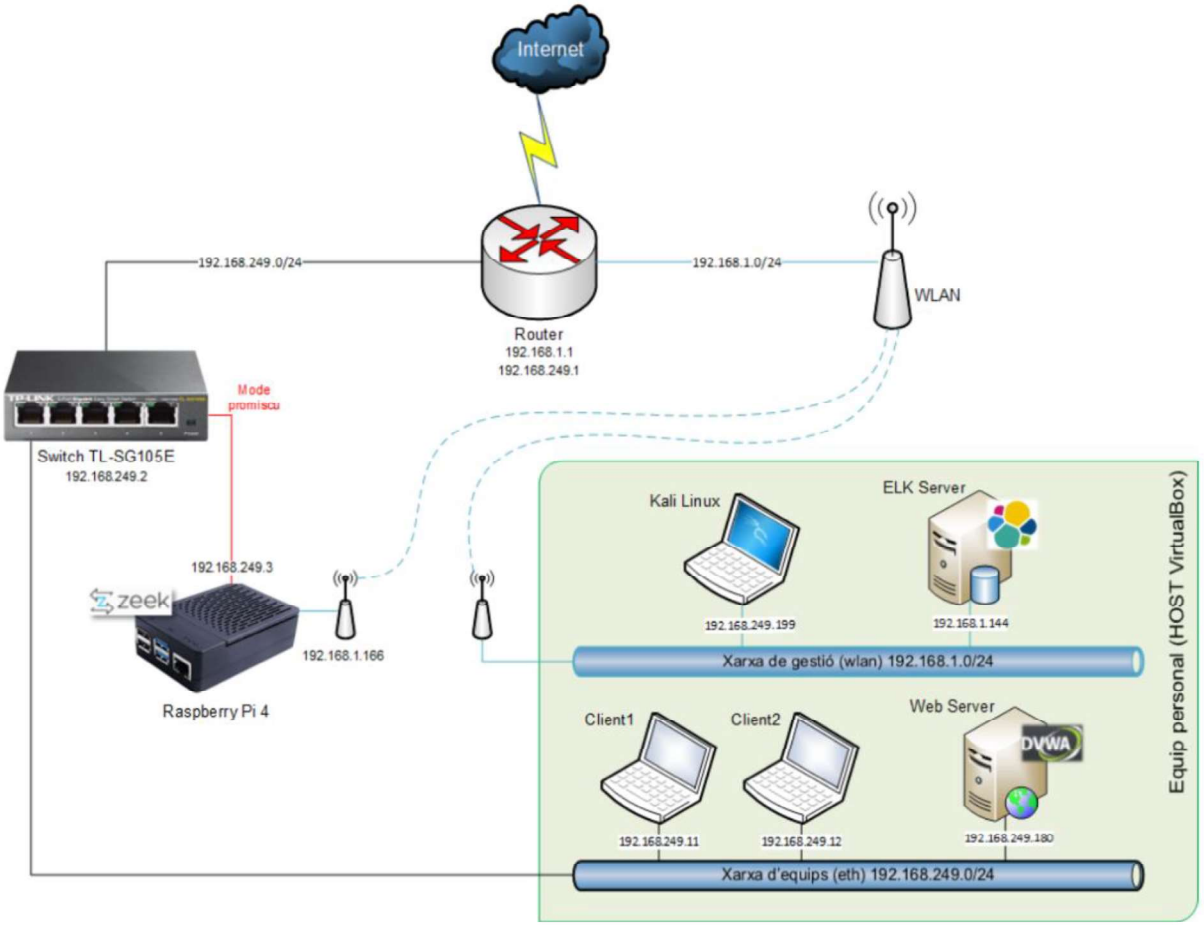
Processar i enriquir informació: Logstash

Emmagatzemar la informació: Elasticsearch

Visualitzar les dades: Kibana

INVESTIGACIÓ I DISSENY

ARQUITECTURA FINAL

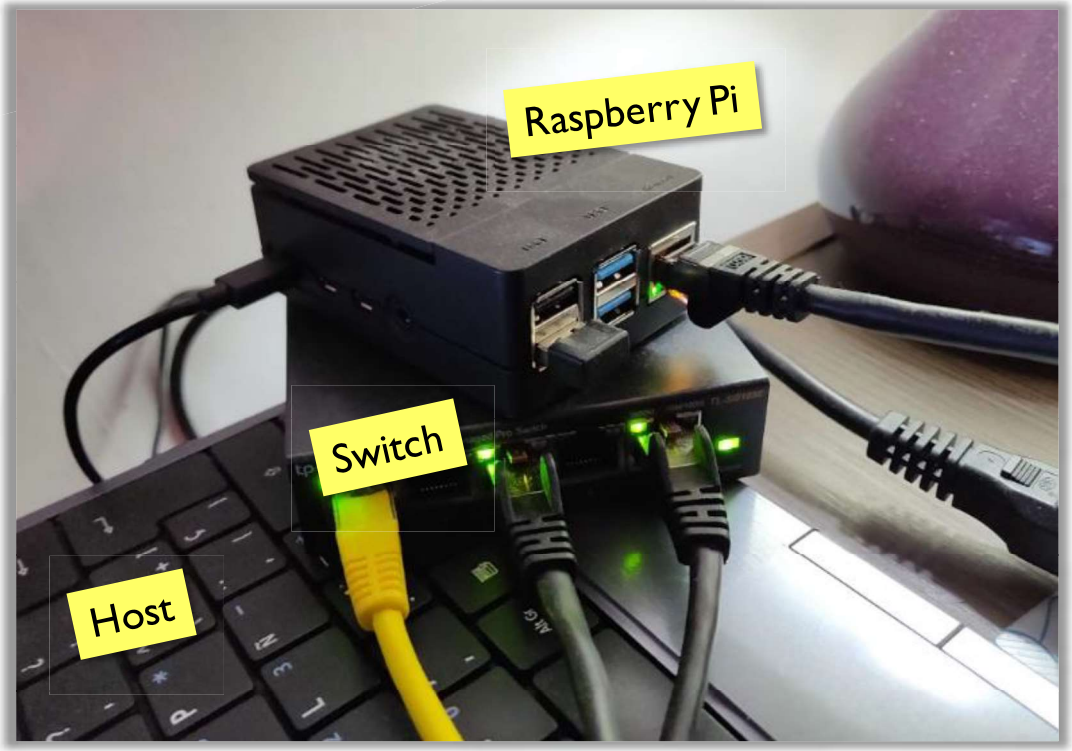


ÍNDEX

IMPLANTACIÓ I FUNCIONAMENT

ENTORN DE TREBALL

- Dispositius de xarxa
  - Router
  - Switch: Port mirroring
- Raspberry Pi
  - Raspbian 10
- Servidor virtual per ELK
  - Ubuntu Server



IMPLANTACIÓ I FUNCIONAMENT

INSTAL·LACIÓ I CONFIGURACIÓ DE LA SOLUCIÓ

- Zeek
- Filebeat (Beats)

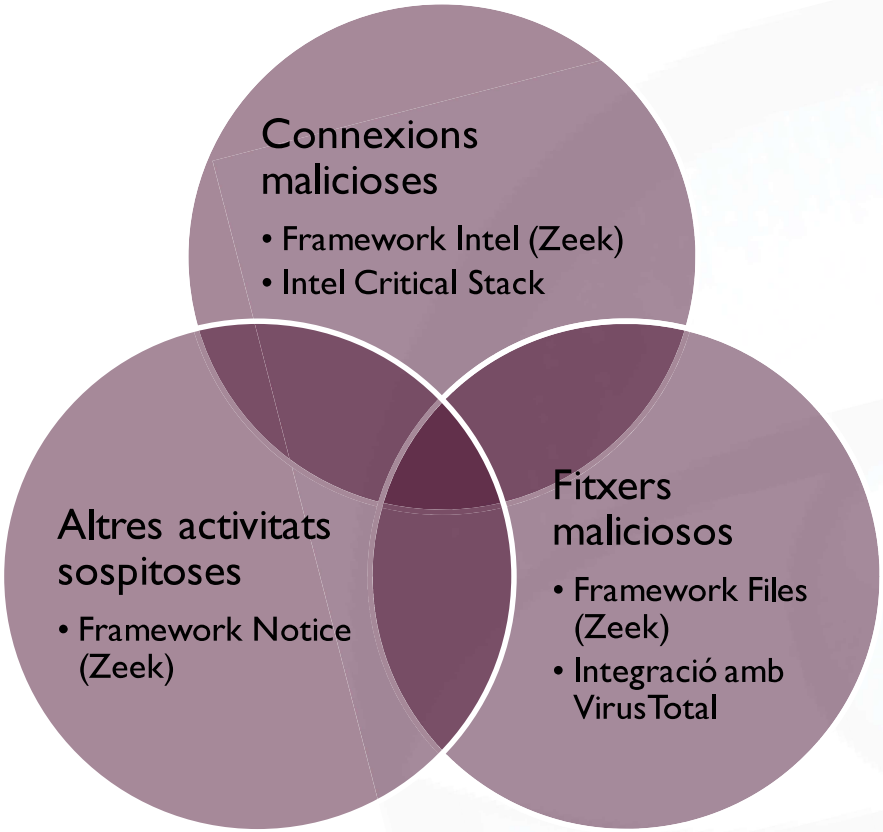
Raspberry Pi

- Logstash
- Elasticsearch
- Kibana
  - Nginx

Servidor ELK

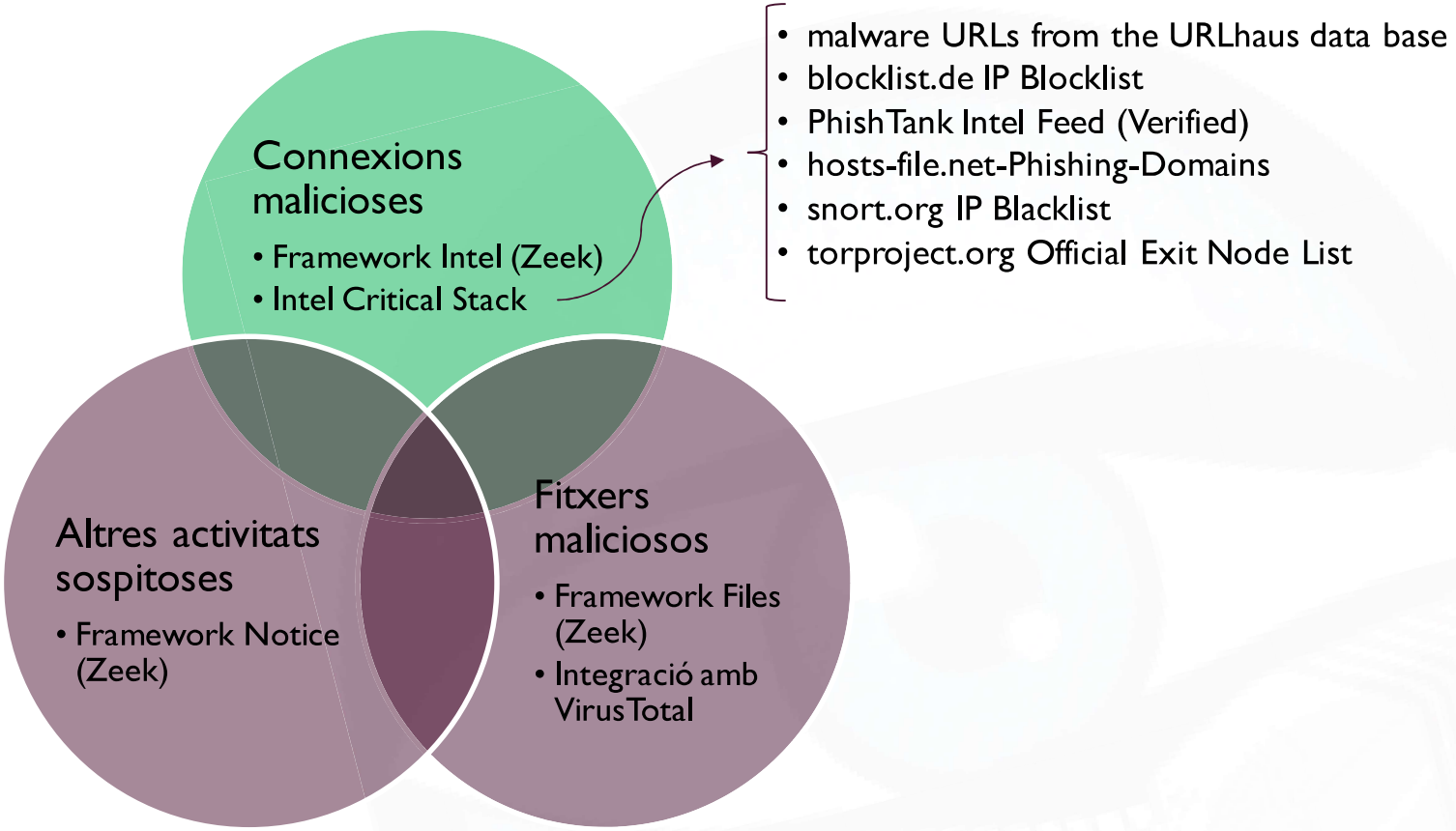
IMPLANTACIÓ I FUNCIONAMENT

DETECCIÓ D'ACTIVITATS SOSPITOSES



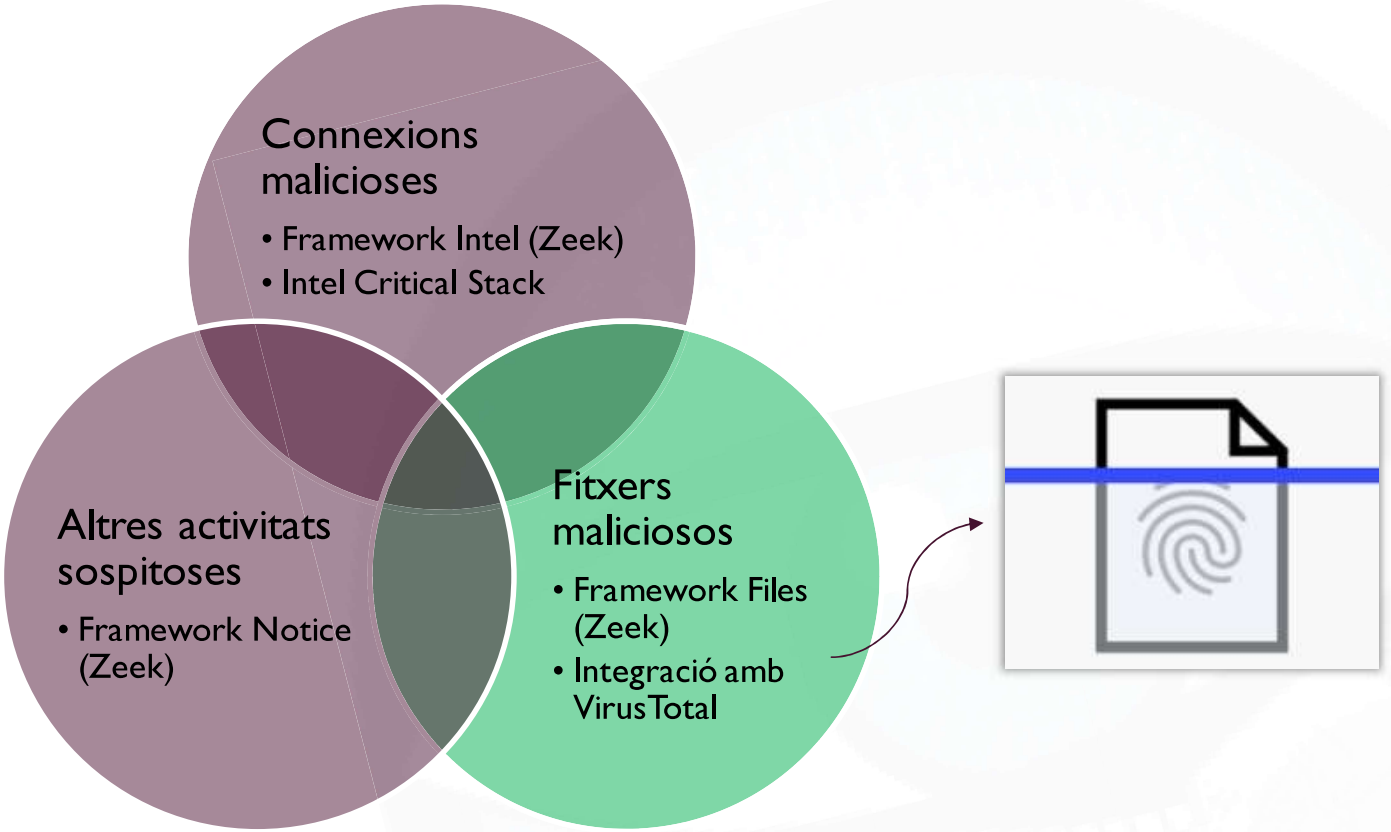
IMPLANTACIÓ I FUNCIONAMENT

DETECCIÓ D'ACTIVITATS SOSPITOSES



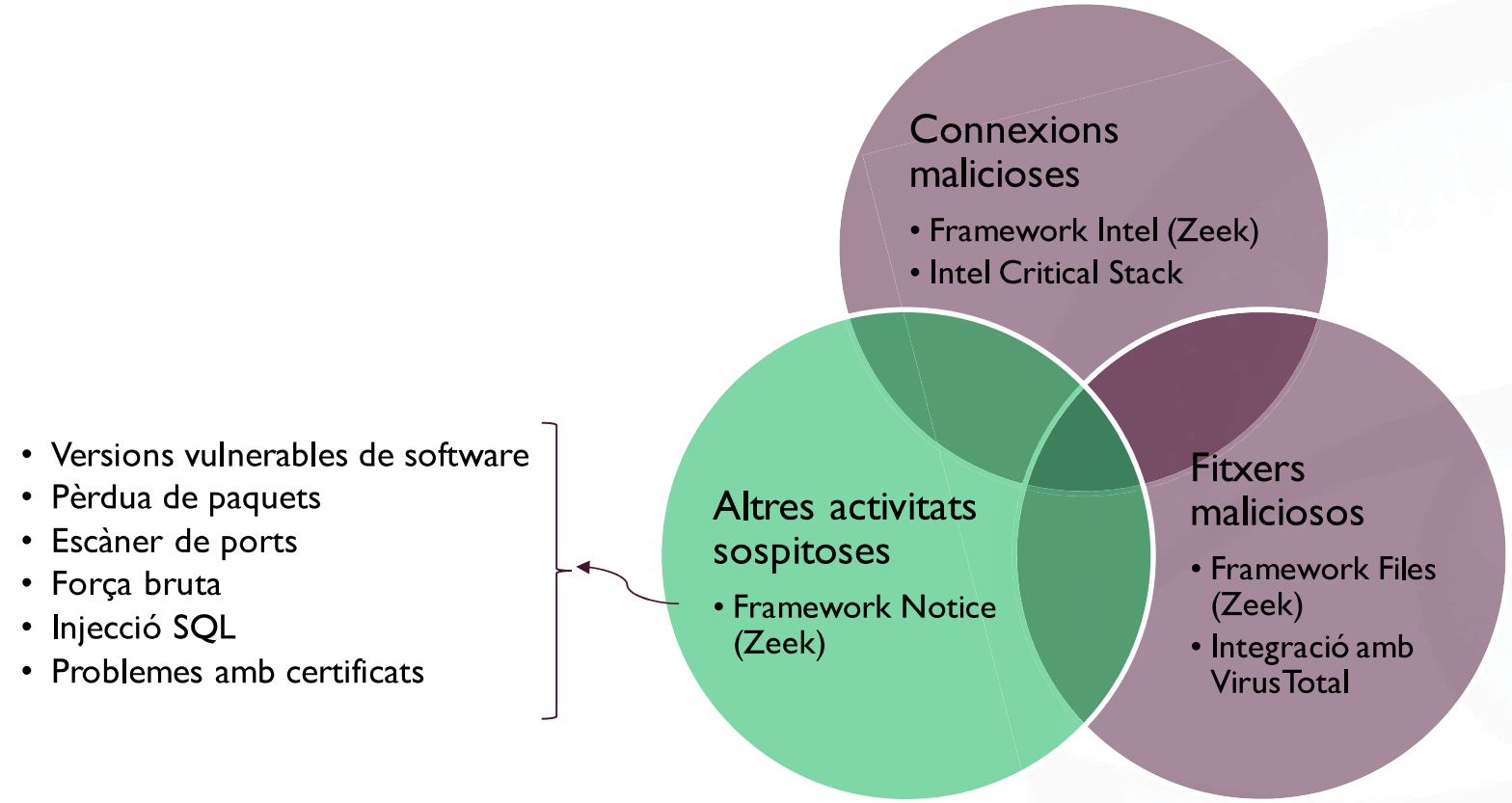
IMPLANTACIÓ I FUNCIONAMENT

DETECCIÓ D'ACTIVITATS SOSPITOSES



IMPLANTACIÓ I FUNCIONAMENT

DETECCIÓ D'ACTIVITATS SOSPITOSES



IMPLANTACIÓ I FUNCIONAMENT

DASHBOARDS

- Dashboard general de seguretat
- Dashboard de fitxers i deteccions de virus
- Dashboard de connexions malicioses
- Dashboard d'altres activitats sospitoses

IMPLANTACIÓ I FUNCIONAMENT

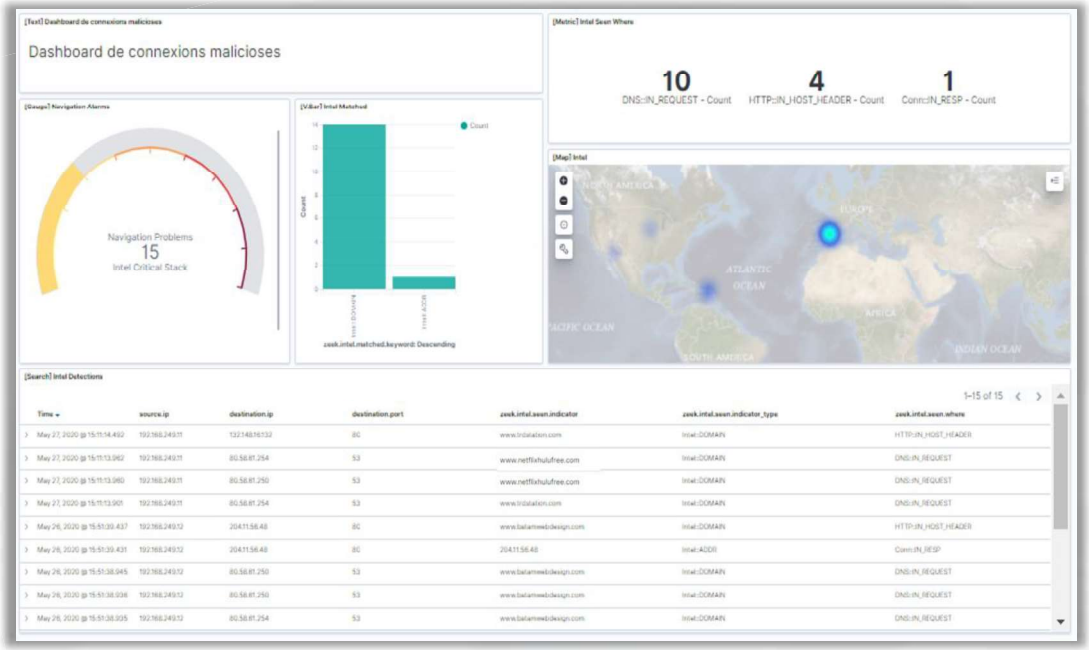
DASHBOARDS

- **Dashboard general de seguretat**
- Dashboard de fitxers i deteccions de virus
- Dashboard de connexions malicioses
- Dashboard d'altres activitats sospitoses

IMPLANTACIÓ I FUNCIONAMENT

DASHBOARDS

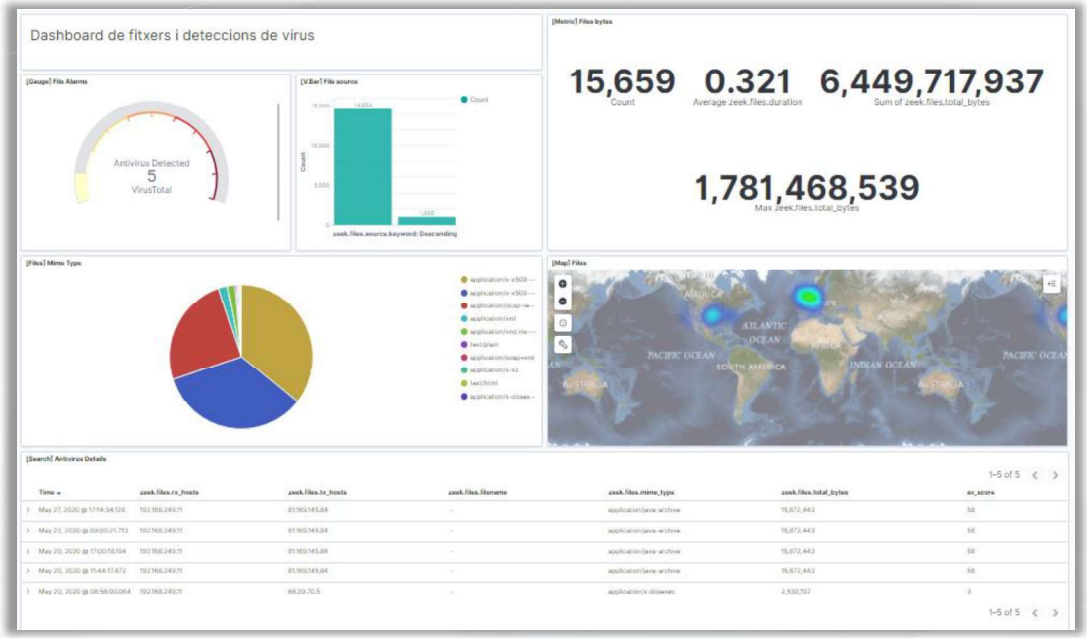
- Dashboard general de seguretat
- **Dashboard de fitxers i deteccions de virus**
- Dashboard de connexions malicioses
- Dashboard d'altres activitats sospitoses



IMPLANTACIÓ I FUNCIONAMENT

DASHBOARDS

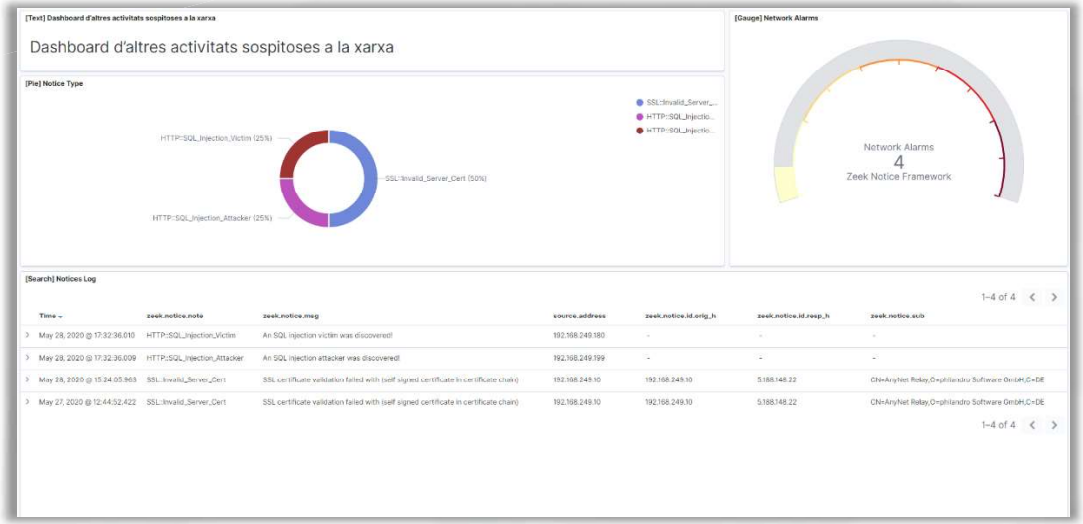
- Dashboard general de seguretat
- Dashboard de fitxers i deteccions de virus
- **Dashboard de connexions malicioses**
- Dashboard d'altres activitats sospitoses



IMPLANTACIÓ I FUNCIONAMENT

DASHBOARDS

- Dashboard general de seguretat
- Dashboard de fitxers i deteccions de virus
- Dashboard de connexions malicioses
- **Dashboard d'altres activitats sospitoses**



IMPLANTACIÓ I FUNCIONAMENT

DEMOSTRACIÓ DEL FUNCIONAMENT

- Zeek detecta tràfic i guarda els logs
- Integració de Zeek amb ELK Stack (extracció de logs)
- Detectar connexions a URLs
- Detectar fitxers maliciosos
- Detectar altres activitats sospitoses
- Mostrar les alertes als Dashboards

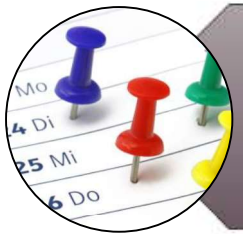
ÍNDEX

CONCLUSIONS

OBJECTIUS PLANTEJATS, SEGUIMENT DE LA PLANIFICACIÓ I TREBALL FUTUR

Objectius plantejats

- Estudi i implantació de les eines Zeek i ELK Stack
- Detecció de les activitats sospitoses
- Creació de dashboards de seguretat



Seguiment de la planificació

- Metodologia
- Imprevistos

Treball futur

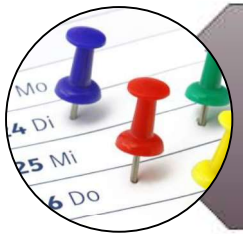
- Inspecció de connexions SSL
- Clúster Zeek, no standalone
- Configuració SSL accés a Kibana
- Potenciar Raspberry Pi
- Beats en altres ubicacions
- Alternatives a la instal·lació d'ELK Stack

CONCLUSIONS

OBJECTIUS PLANTEJATS, SEGUIMENT DE LA PLANIFICACIÓ I TREBALL FUTUR

Objectius plantejats

- Estudi i implantació de les eines Zeek i ELK Stack
- Detecció de les activitats sospitoses
- Creació de dashboards de seguretat



Seguiment de la planificació

- Metodologia
- Imprevistos

Treball futur

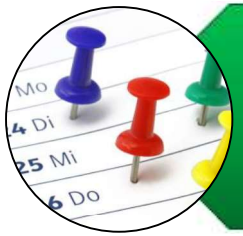
- Inspecció de connexions SSL
- Clúster Zeek, no standalone
- Configuració SSL accés a Kibana
- Potenciar Raspberry Pi
- Beats en altres ubicacions
- Alternatives a la instal·lació d'ELK Stack

CONCLUSIONS

OBJECTIUS PLANTEJATS, SEGUIMENT DE LA PLANIFICACIÓ I TREBALL FUTUR

Objectius plantejats

- Estudi i implantació de les eines Zeek i ELK Stack
- Detecció de les activitats sospitoses
- Creació de dashboards de seguretat



Seguiment de la planificació

- Metodologia
- Imprevistos

Treball futur

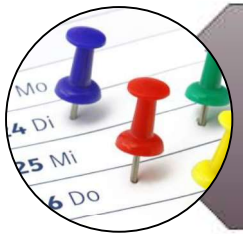
- Inspecció de connexions SSL
- Clúster Zeek, no standalone
- Configuració SSL accés a Kibana
- Potenciar Raspberry Pi
- Beats en altres ubicacions
- Alternatives a la instal·lació d'ELK Stack

CONCLUSIONS

OBJECTIUS PLANTEJATS, SEGUIMENT DE LA PLANIFICACIÓ I TREBALL FUTUR

Objectius plantejats

- Estudi i implantació de les eines Zeek i ELK Stack
- Detecció de les activitats sospitoses
- Creació de dashboards de seguretat



Seguiment de la planificació

- Metodologia
- Imprevistos

Treball futur

- Inspecció de connexions SSL
- Clúster Zeek, no standalone
- Configuració SSL accés a Kibana
- Potenciar Raspberry Pi
- Beats en altres ubicacions
- Alternatives a la instal·lació d'ELK Stack

MOLTES GRÀCIES.