BI GUARDIAN. Sistema de detección proactiva de amenazas de Ciberseguridad

Machine Learning Workshop Galicia 2016

Fecha

Centro para el Desarrollo Tecnológico Industrial

FEDER INNTERCONECTA Una manera de hacer Europa

Wellness Telecom

CITIC

INTRODUCCIÓN

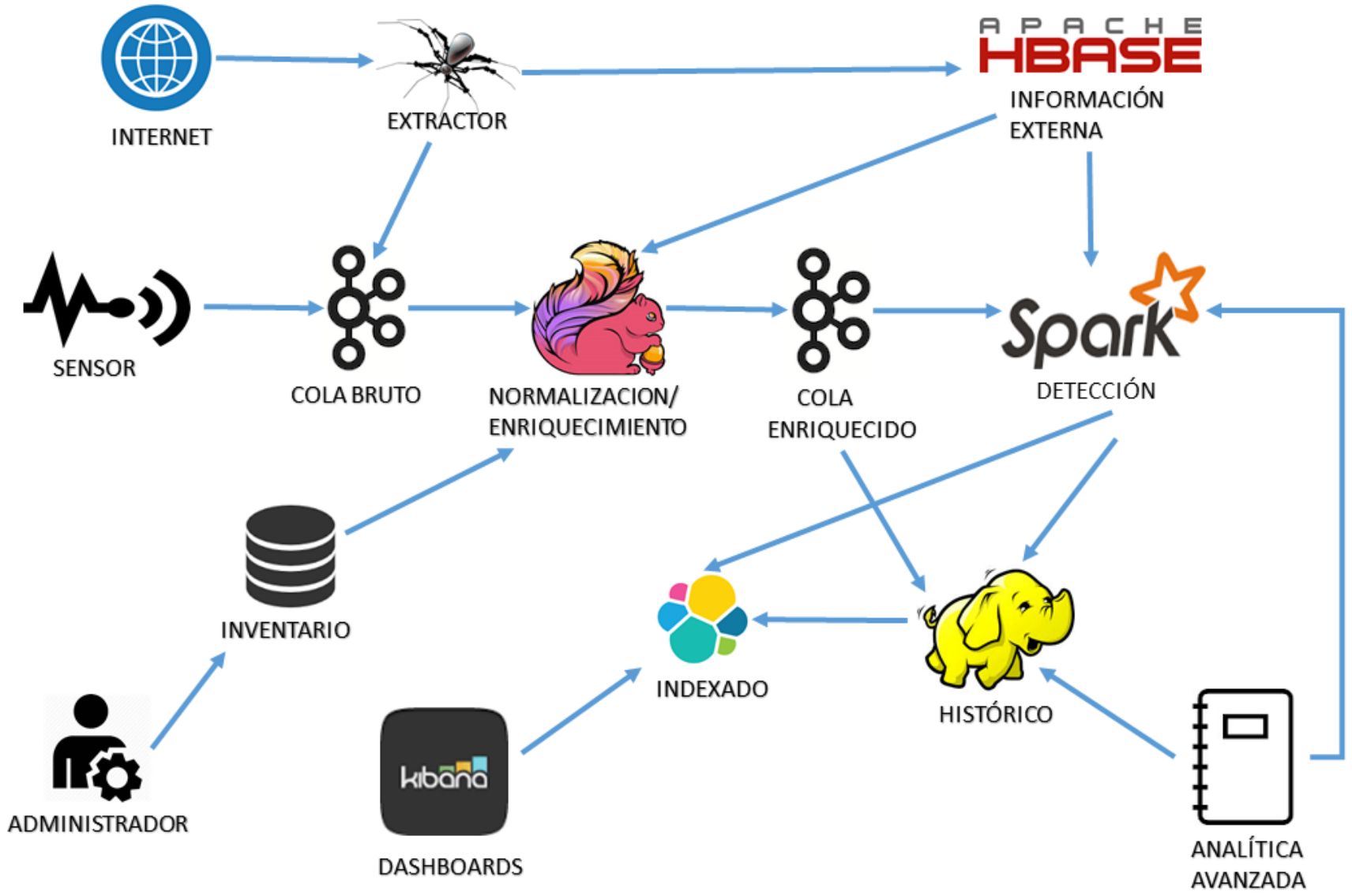
- **El cibercrimen es una amenaza creciente:**
  - Interior informa de un aumento de un 106% de ataques a infraestructuras críticos
  - Fugas de datos: Linkedin
  - Organizaciones criminales vs hackers aislados
  - Nuevos tipos de ataque: Ransomware, DDoS
- **Las herramientas de seguridad actuales no funcionan:**
  - Seguridad perimetral
  - Sistemas basados en firmas
- **BI-Guardian es una nueva aproximación a este problema:**
  - Detección de anomalías vs seguridad perimetral
  - Visión 360º de lo que ocurre en la organización y el exterior
  - Big Data, Fast Data. Histórico infinito. Detección en tiempo real
  - Data Science: Últimos avances en Machine Learning: Deep Learning, Graph Analytics

SENSORES

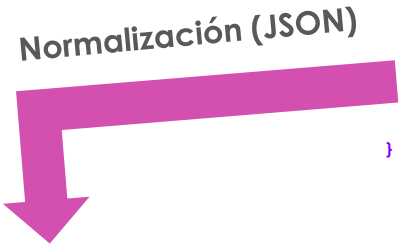
- **REDES INTERNAS:**
  - Tcpdump
  - Netflow
  - Firewall
  - IDS
  - Antivirus
  - Syslog

- **REDES EXTERNAS:**
  - Listas negras
  - Exploits
  - Dorks
  - Redes sociales
  - Deep Web

PLATAFORMA BIG DATA



PROCESADO EN TIEMPO REAL



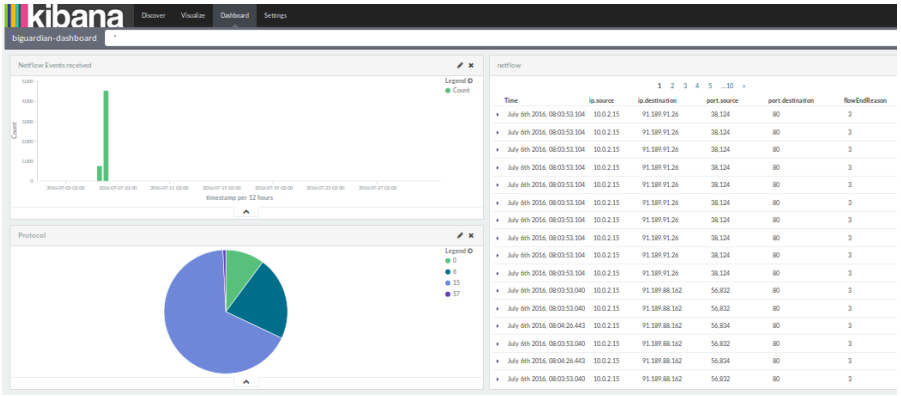

```
{
  "flowStartMilliseconds": 1467785027357,
  "reversePacketTotalCount": 238,
  "packetTotalCount": 183,
  "octetTotalCount": 9829,
  "sourceTransportPort": 38124,
  "flowEndMilliseconds": 1467785033104,
  "destinationIPv4Address": "91.189.91.26",
  "flowEndReason": 3,
  "sourceIPv4Address": "10.0.2.15",
  "reverseFlowAttributes": 0,
  "port.destination": 80,
  "protocolIdentifier": 6,
  "flowAttributes": 0,
  "destinationTransportPort": 80,
  "reverseOctetTotalCount": 562074,
  "silkAppLabel": 0
}
```

```
{
  "startTime": "2016-07-06T06:03:47.357Z",
  "timestamp": "2016-07-06T06:03:53.104Z",
  "flowStartMilliseconds": 1467785027357,
  "reversePacketTotalCount": 238,
  "packetTotalCount": 183,
  "octetTotalCount": 9829,
  "sourceTransportPort": 38124,
  "ip.destination": "91.189.91.26",
  "flowEndMilliseconds": 1467785033104,
  "destinationIPv4Address": "91.189.91.26",
  "flowEndReason": 3,
  "port.source": 38124,
  "sourceIPv4Address": "10.0.2.15",
  "endTime": "2016-07-06T06:03:53.104Z",
  "sensor": "netflow",
  "reverseFlowAttributes": 0,
  "port.destination": 80,
  "protocolIdentifier": 6,
  "flowAttributes": 0,
  "destinationTransportPort": 80,
  "reverseOctetTotalCount": 562074,
  "silkAppLabel": 0,
  "protocol": 6,
  "ip.source": "10.0.2.15"
}
```

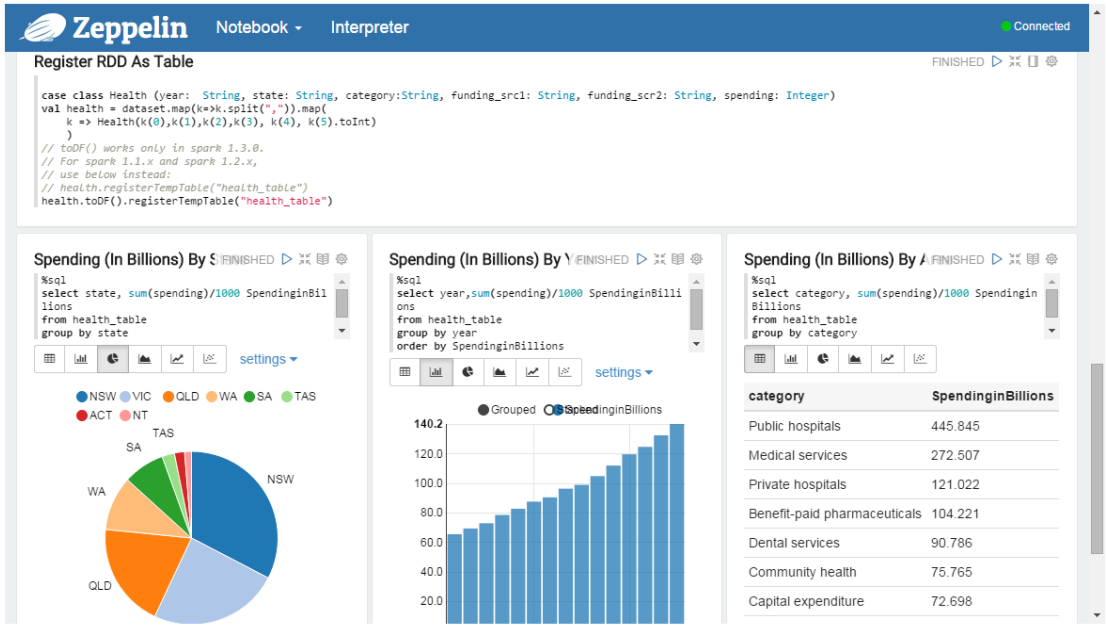
```
{
  "startTime": "2016-07-06T06:03:47.357Z",
  "timestamp": "2016-07-06T06:03:53.104Z",
  "flowStartMilliseconds": 1467785027357,
  "reversePacketTotalCount": 238,
  "packetTotalCount": 183,
  "octetTotalCount": 9829,
  "sourceTransportPort": 38124,
  "ip.destination": "91.189.91.26",
  "destination.location": {
    "lat": 42.3583984375,
    "lon": -71.05979919433594
  },
  "flowEndMilliseconds": 1467785033104,
  "destinationIPv4Address": "91.189.91.26",
  "flowEndReason": 3,
  "port.source": 38124,
  "sourceIPv4Address": "10.0.2.15",
  "endTime": "2016-07-06T06:03:53.104Z",
  "sensor": "netflow",
  "reverseFlowAttributes": 0,
  "port.destination": 80,
  "protocolIdentifier": 6,
  "destination.country": "United States",
  "flowAttributes": 0,
  "destination.city": "Boston",
  "destinationTransportPort": 80,
  "reverseOctetTotalCount": 562074,
  "silkAppLabel": 0,
  "protocol": 6,
  "ip.source": "10.0.2.15" }
```

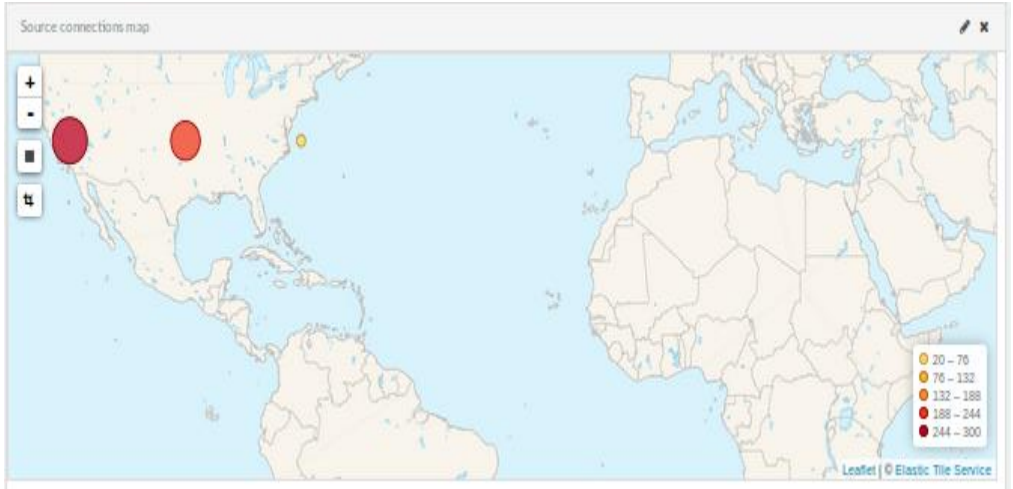
EXPLOTACIÓN DE DATOS

- **DASHBOARDS**
  - Análisis rápido y sencillo de datos indexados
  - Actualizado en tiempo real



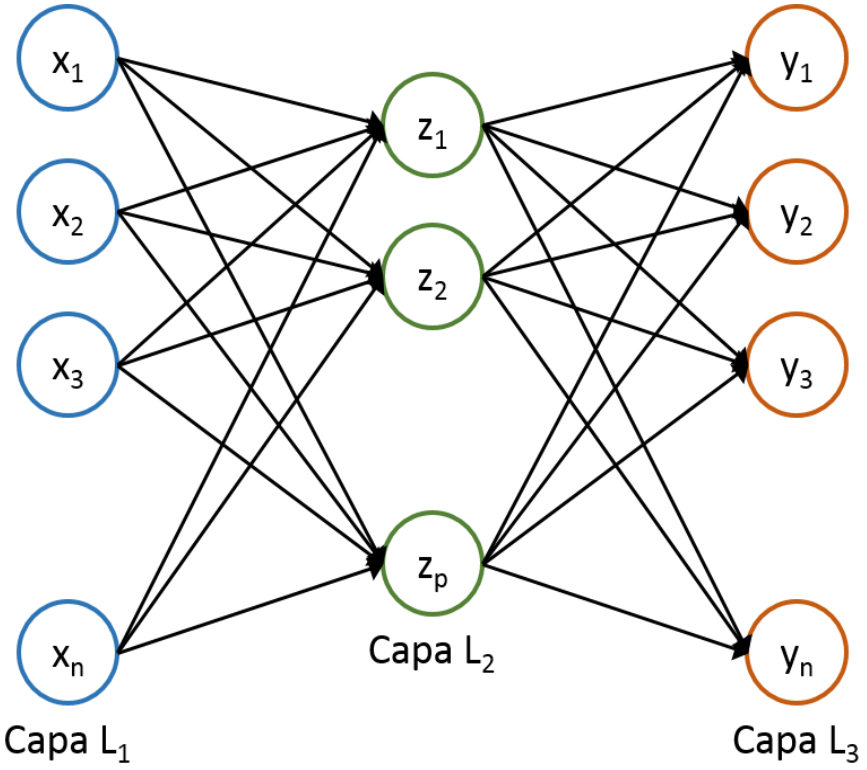
- **NOTEBOOKS**
  - Análisis avanzado del histórico de datos
  - Creación de modelos estadísticos
  - Análisis forense





DETECCIÓN DE ANOMALÍAS

- **Modelos estadísticos**
  - GMM
  - LDA
- **Deep Learning**
  - Autocodificadores Apilados
- **Análisis de Grafos**:
  - Centralidad
- **Modelo semisupervisado**:
  - Random Forests
  - Feedback Analista Seguridad



PRÓXIMOS PASOS

- **INSTALAR SENSORES EN OESÍA y HCS**
- **INVENTARIO DE RED**
- **TESTEO DE ALGORITMOS**
- **VULNERABILIDADES**
- **ETC.**