IBM Security

Cognitividad:
Cómo apoyará a la Ciberseguridad

Juan Camilo Reyes
Security Services Leader, SSA Region

CISSP® Certified Information Systems Security Professional

IBM

IBM Security

191 días

191 días

Demora una empresa promedio en detectar una brecha de seguridad

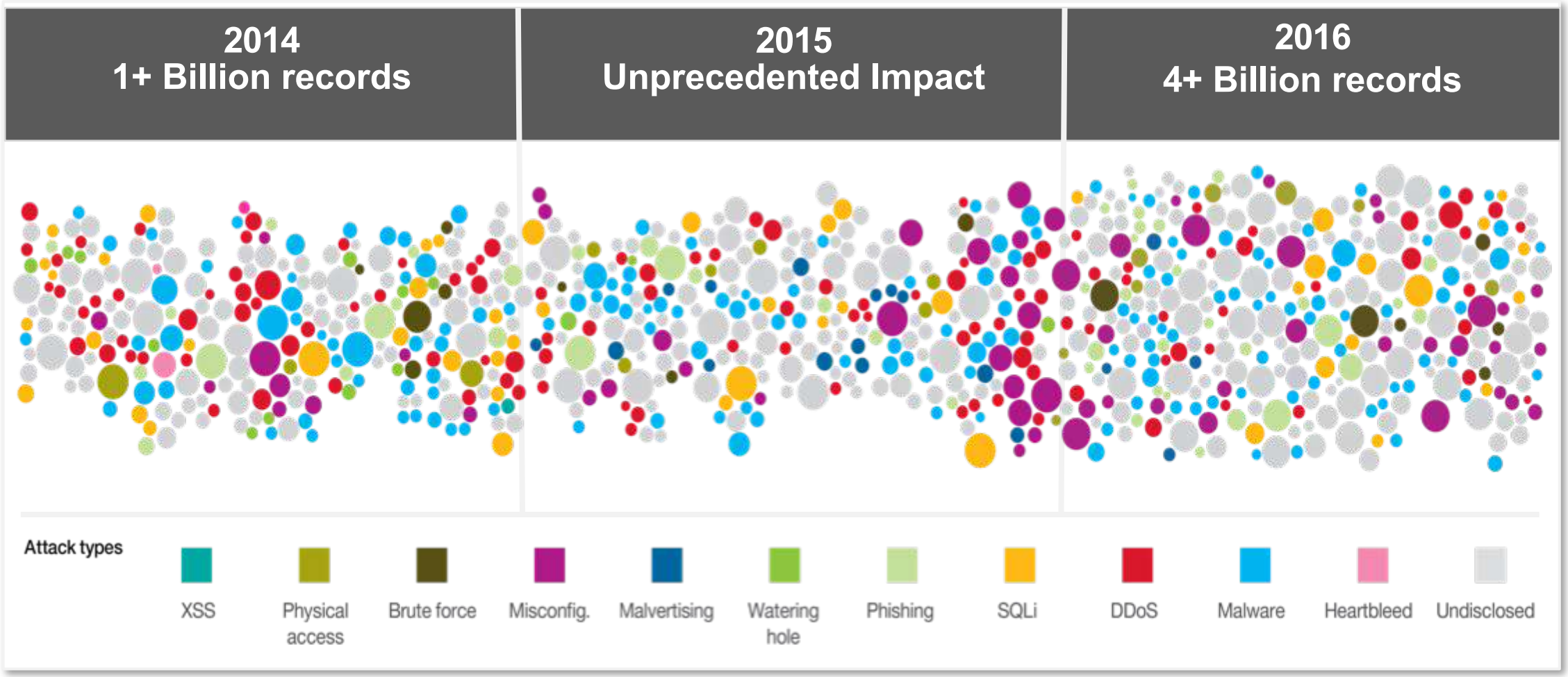
Ponemon Institute: 2017 Cost of Data Breach

El día a día del analista de seguridad

¿Cuál es el reto?

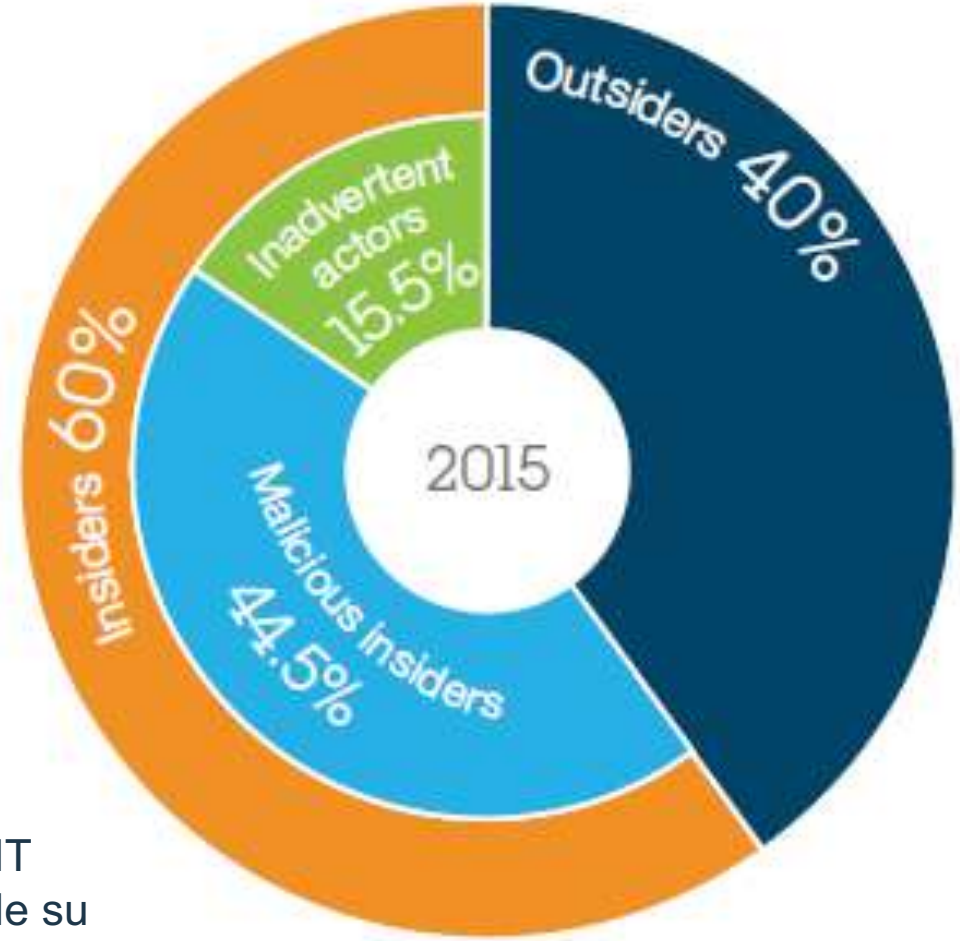
Detectar un ataque

Los atacantes rompen las defensas tradicionales todos los días



Source: *IBM X-Force Threat Intelligence Index - 2017*

¿De dónde vienen los ataques?



$445 BILLONES
Pérdidas estimadas para la economía global

49%
De los profesionales de IT mantienen los accesos de su anterior empleo

Las organizaciones continúan invirtiendo en productos puntuales

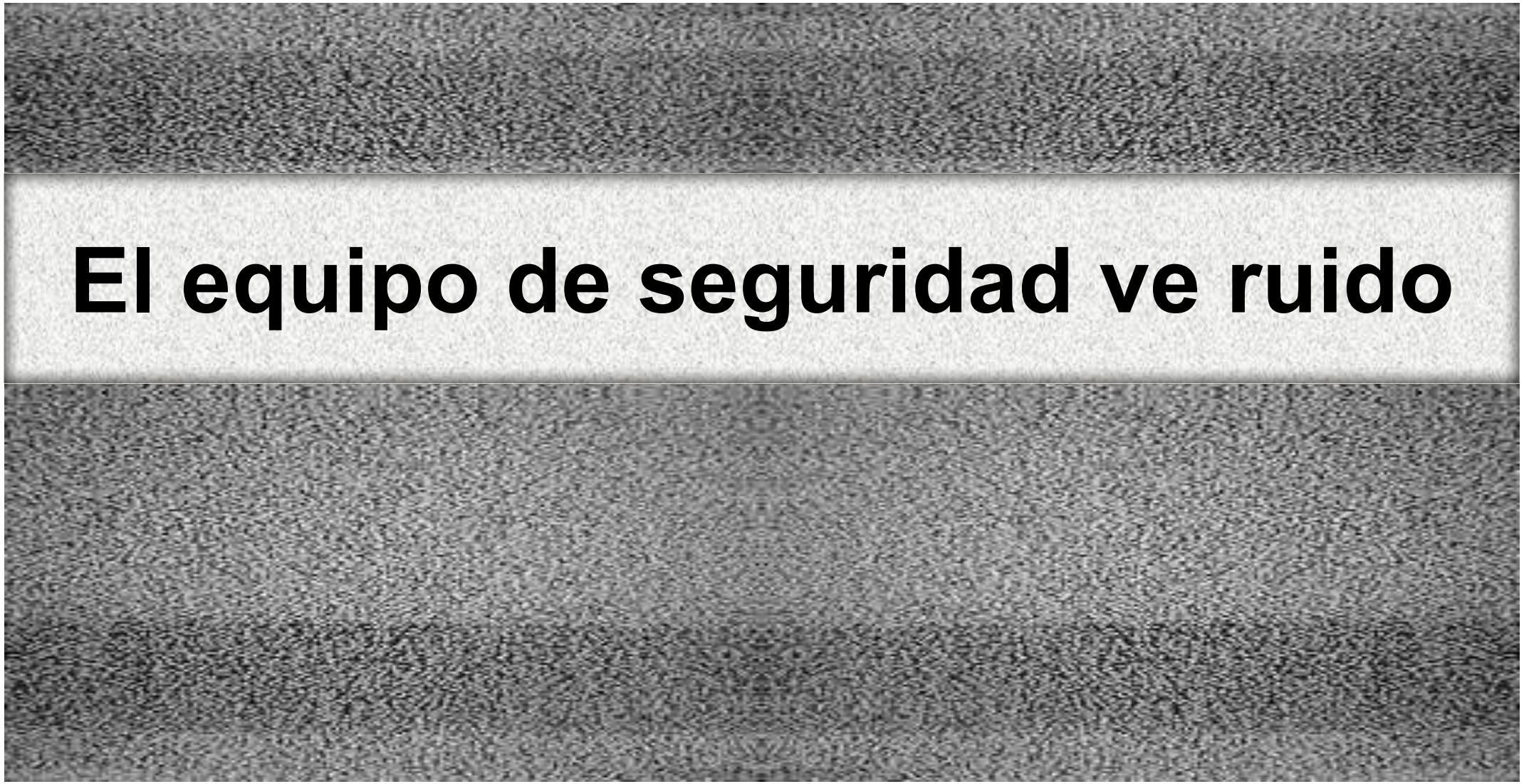
85 Herramientas de seguridad de

45 Fabricantes

Source: IBM Client Example

Número de productos a través del tiempo

Incrementando los costos y la complejidad


El equipo de seguridad ve ruido

Tiene que analizar eventos de:

- **Inteligencia ante Amenazas**
  - Indicadores de Compromiso
  - Reputación IP
  - Amenaza compartida
- **Servidores / Estaciones de trabajo**
  - Gestión de parches en el punto final
  - Antivirus
  - Protección contra Malware
- **Red**
  - Gestión de Incidentes y amenazas
  - Firewalls
  - Sandboxing
  - Parches virtuales
  - Visibilidad en la red
- **Móviles**
  - Protección de las transacciones
  - Gestión de dispositivos
  - Contenido seguro
- **Fraude Avanzado**
  - Protección ante fraudes
  - Deteccion de criminales
- **Datos y Aplicaciones**
  - Monitoreo de datos
  - Control de acceso a datos
  - Escaneo de aplicaciones
  - Gestión de seguridad en aplicaciones
- **Nube**
  - Cloud access security broker
  - Workload protection
- **Identidades y Accesos**
  - Gestion de usuarios privilegiados
  - Roles y permisos
  - Gestión de accesos
  - Gestión de Identidades

IBM Security

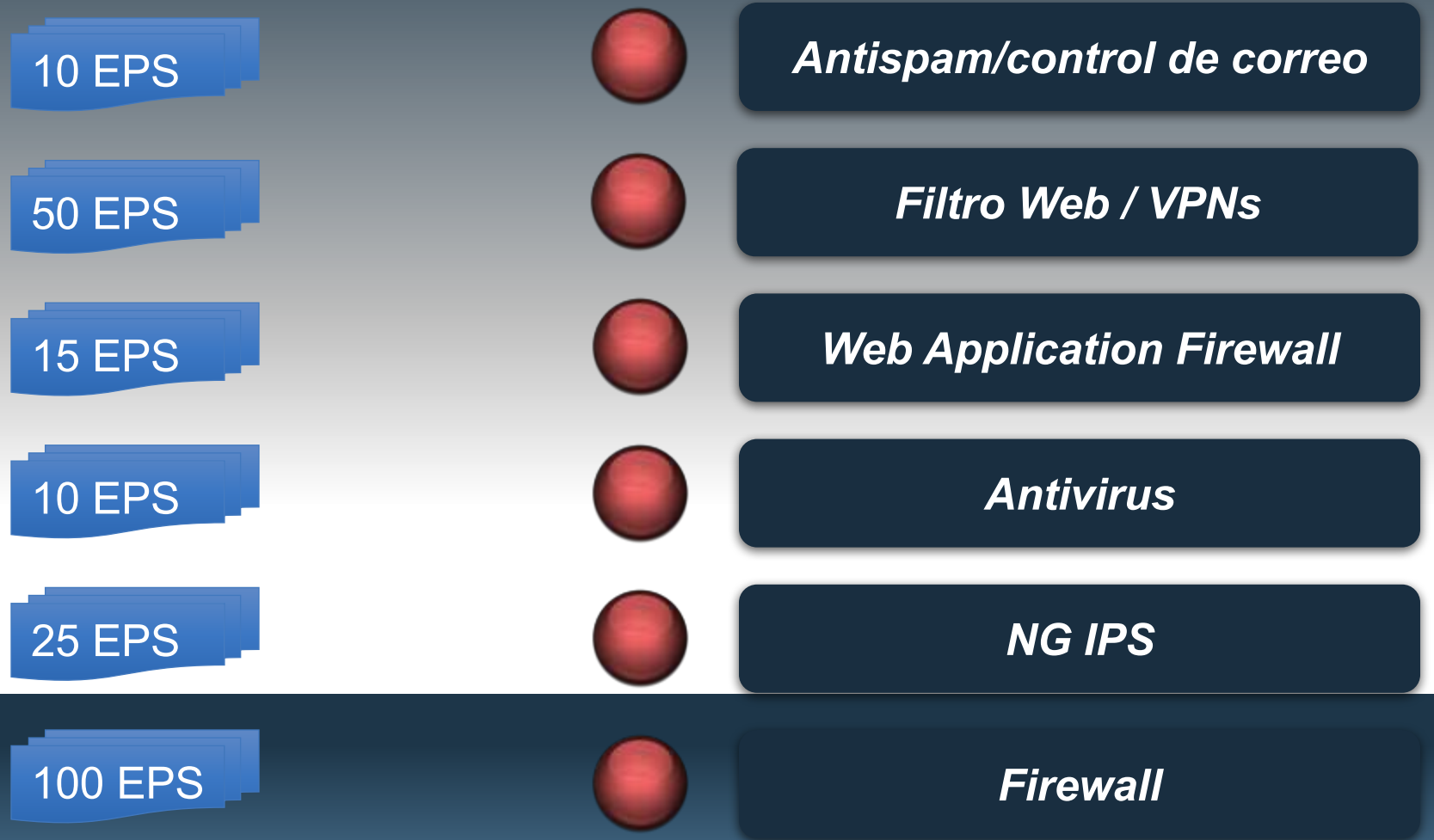
Fases de un ataque

Penetrar	Enganchar	Expandir	Colectar	Exfiltrar
Encontrar cómo ingresar y ganar credenciales	Comprometer un servidor vulnerable	Infectar sistemas o lograr nuevos accesos	Traer la información a ser robada/expuesta	Transmitir la información fuera de la organización.

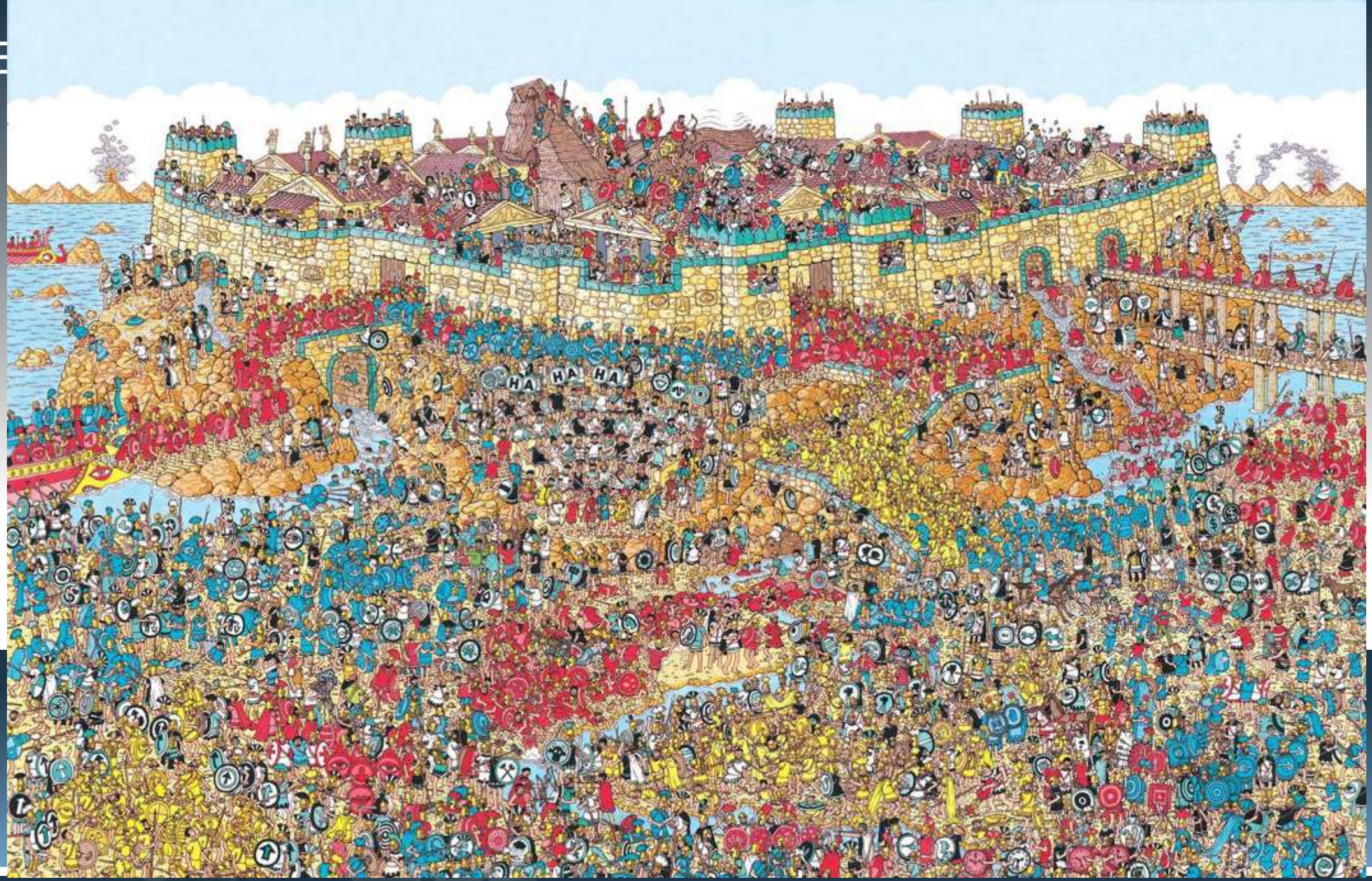
Controles y vigilancia

- *Antispam/control de correo*
- *Filtro Web / VPNs*
- *Web Application Firewall*
- *Antivirus*
- *NG IPS*
- *Firewall*

Saturación – EPS (Eventos por segundo)



E



Correlación de eventos

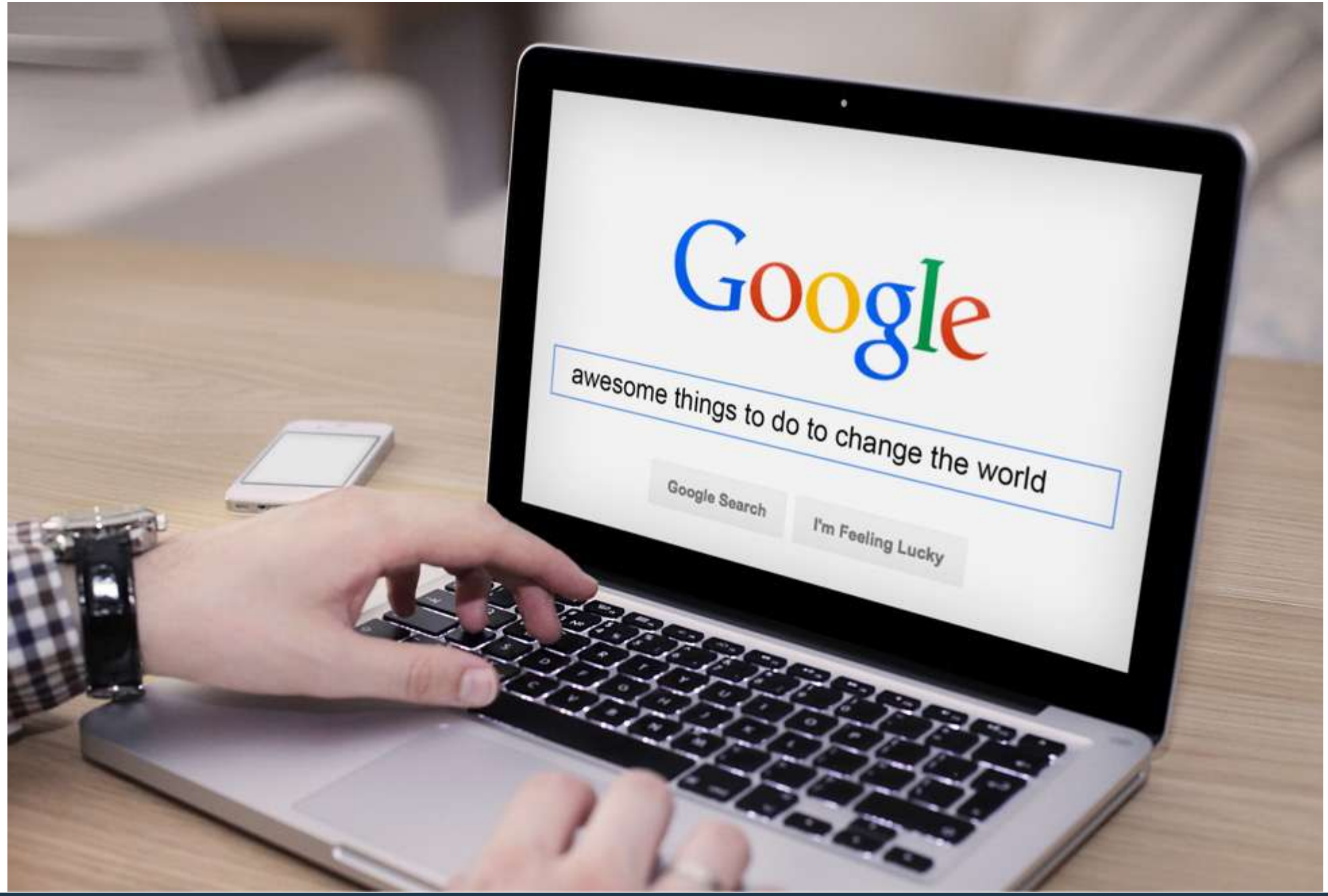
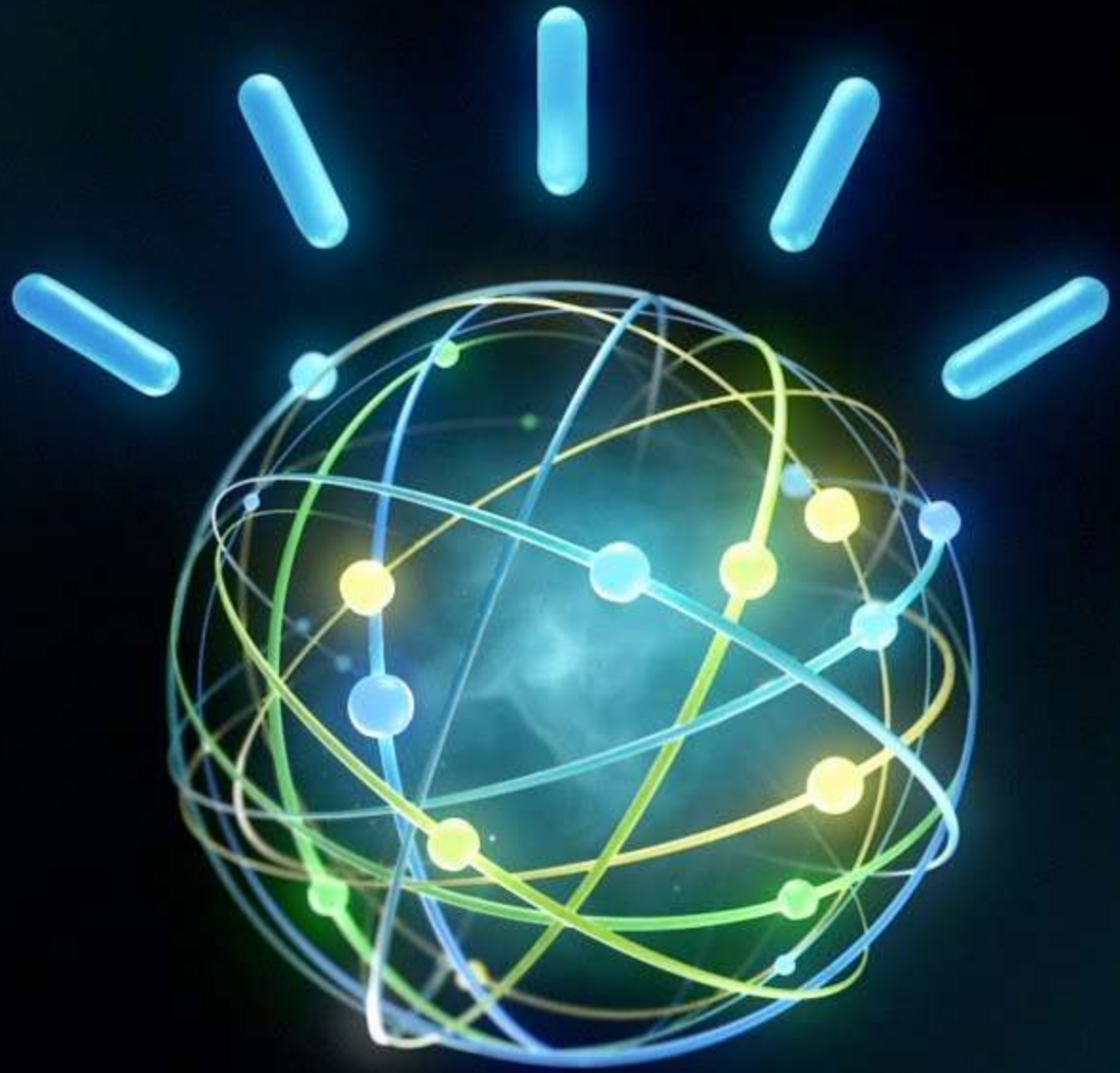

Google
awesome things to do to change the world
Google Search
I'm Feeling Lucky

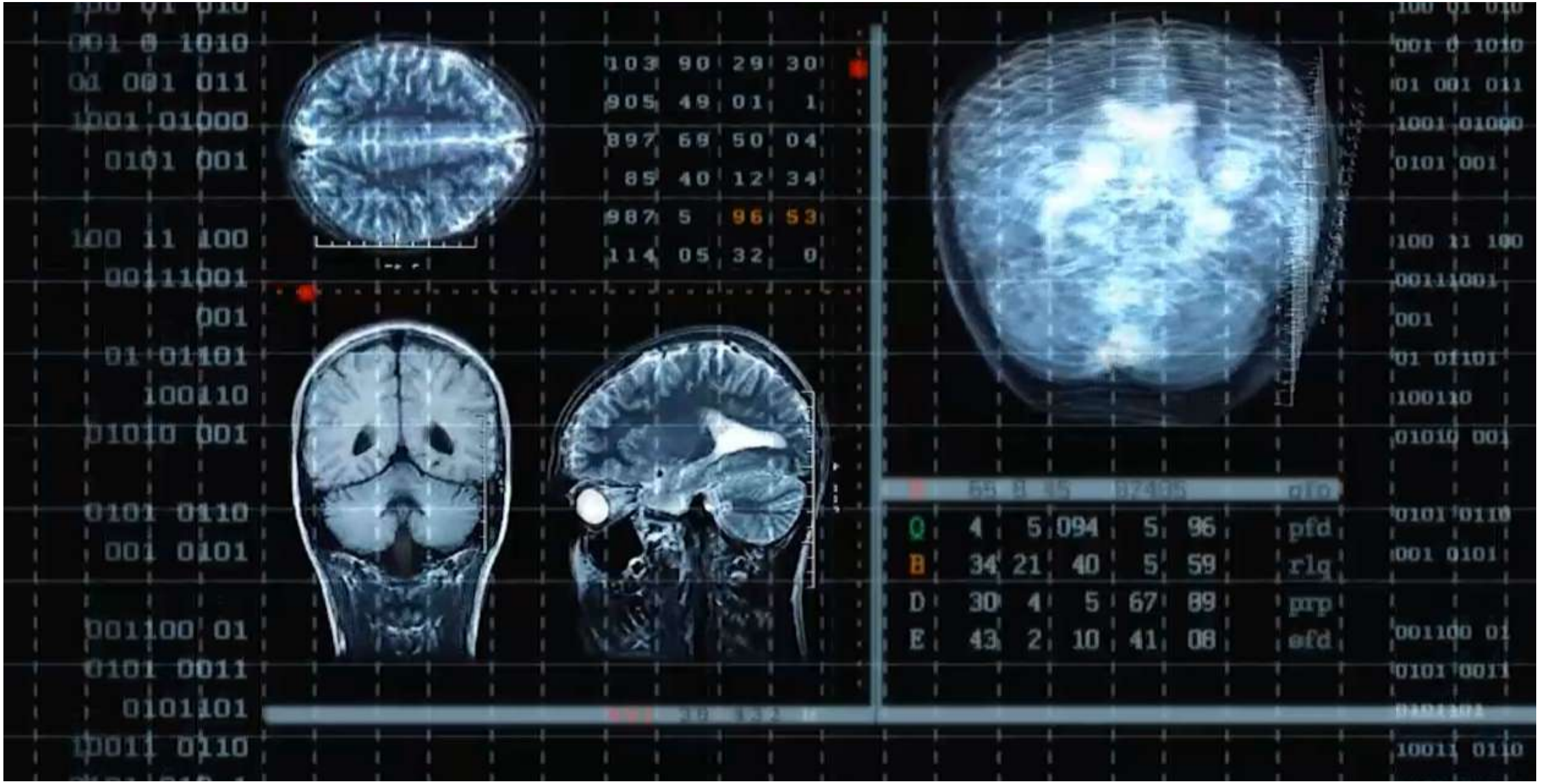
Table 1

Information Number	4-bit binary information	6-bit binary information			3-bit ternary information
1	0000	01	00	00	100
2	0001	01	00	01	101
3	0010	01	00	10	102
4	0011	01	01	00	110
5	0100	01	01	01	111
6	0101	01	01	10	112
7	0110	01	10	00	120
8	0111	01	10	01	121
9	1000	01	10	10	122
10	1001	10	00	00	200
11	1010	10	00	01	201
12	1011	10	00	10	202
13	1100	10	01	00	210
14	1101	10	01	01	211
15	1110	10	01	10	212
16	1111	10	10	00	220

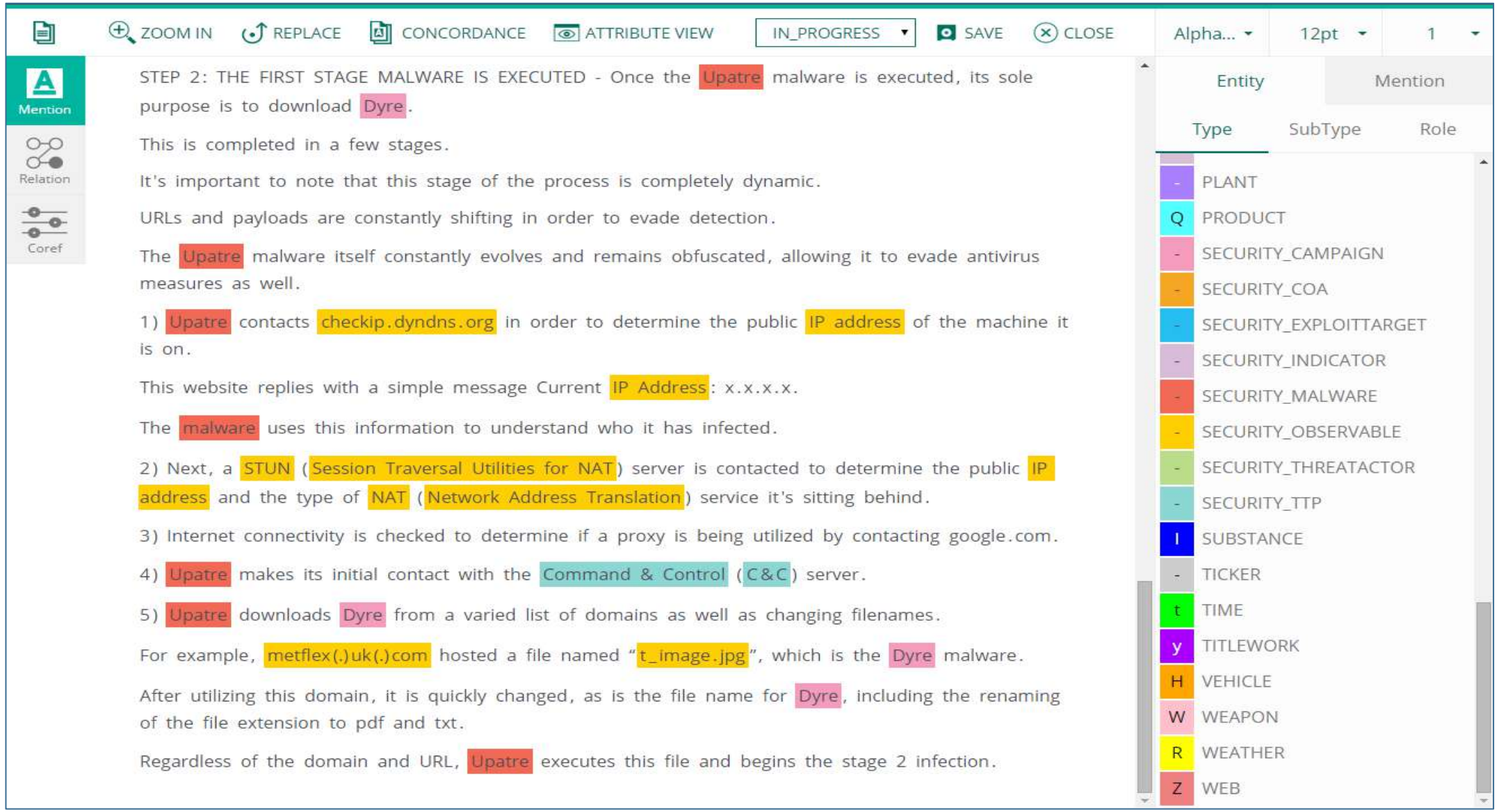



PIENSE
THINK
ΣΚΕΨΟΥ
DENKE
PENSER
सोचिए
$300,000
Who is Stoker?
(I FOR ONE WELCOME OUR NEW COMPUTER OVERLORDS)
$1,000
$1,000,000
Who is Bram Stoker?
$ 17,973
$200,000
WHO IS BRAM STOKER?
$5600

Watson luchando contra enfermedades



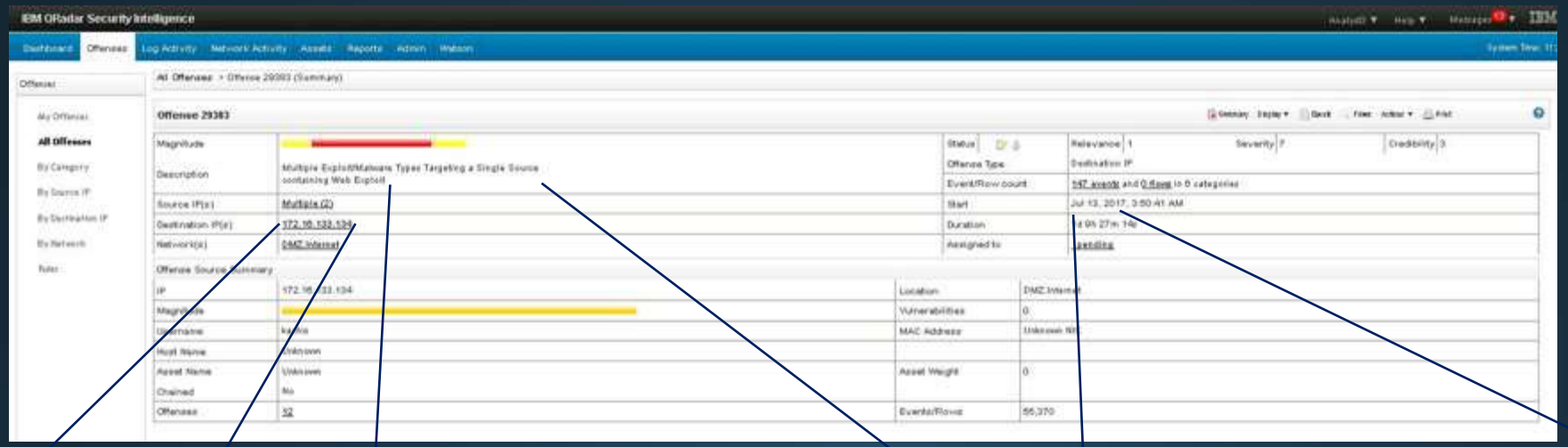
Entrenando a Watson en el lenguaje de ciberseguridad

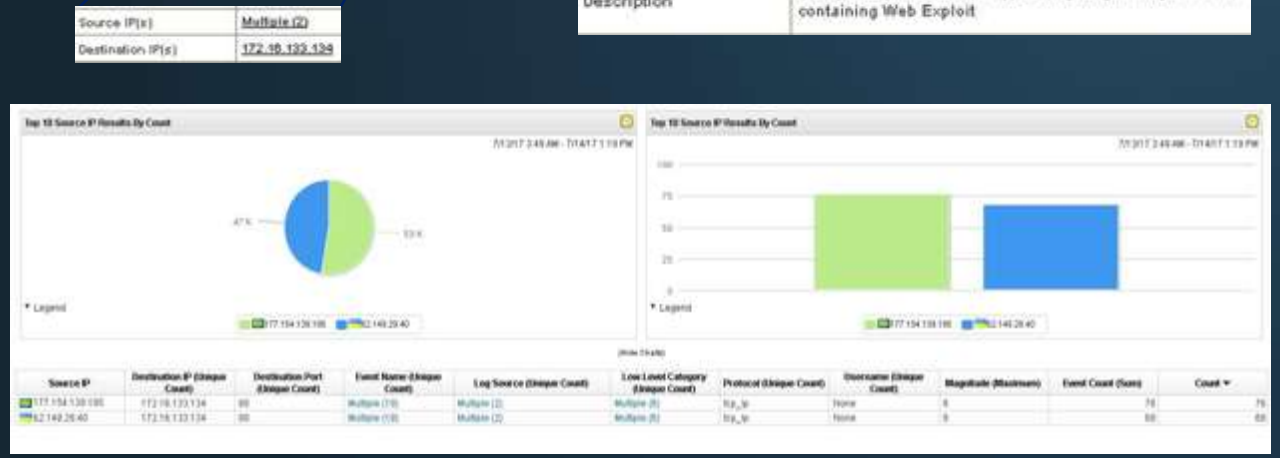


Video

Ok, pero como funciona la cognitividad aplicada

Análisis solamente usando Qradar.

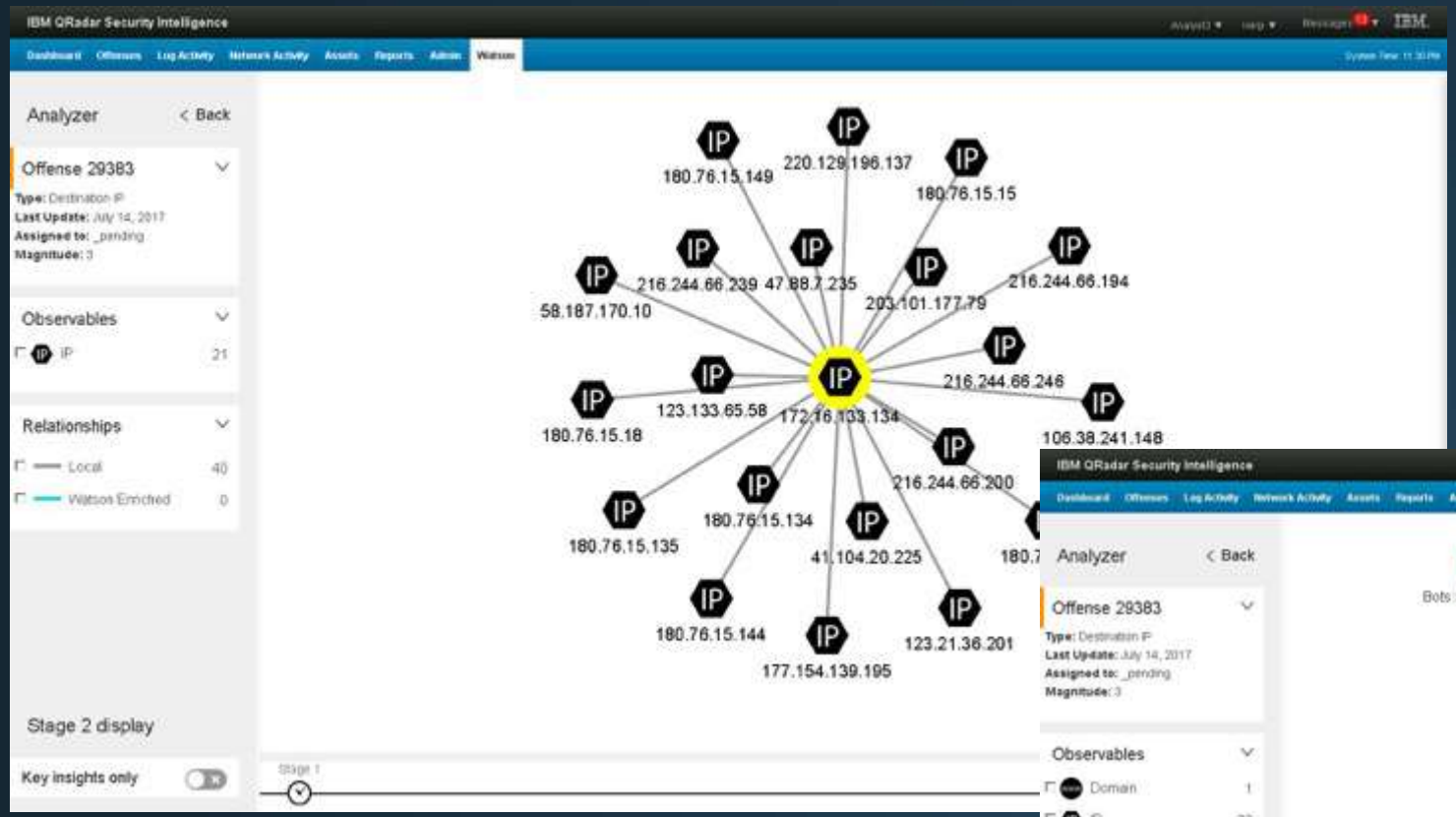


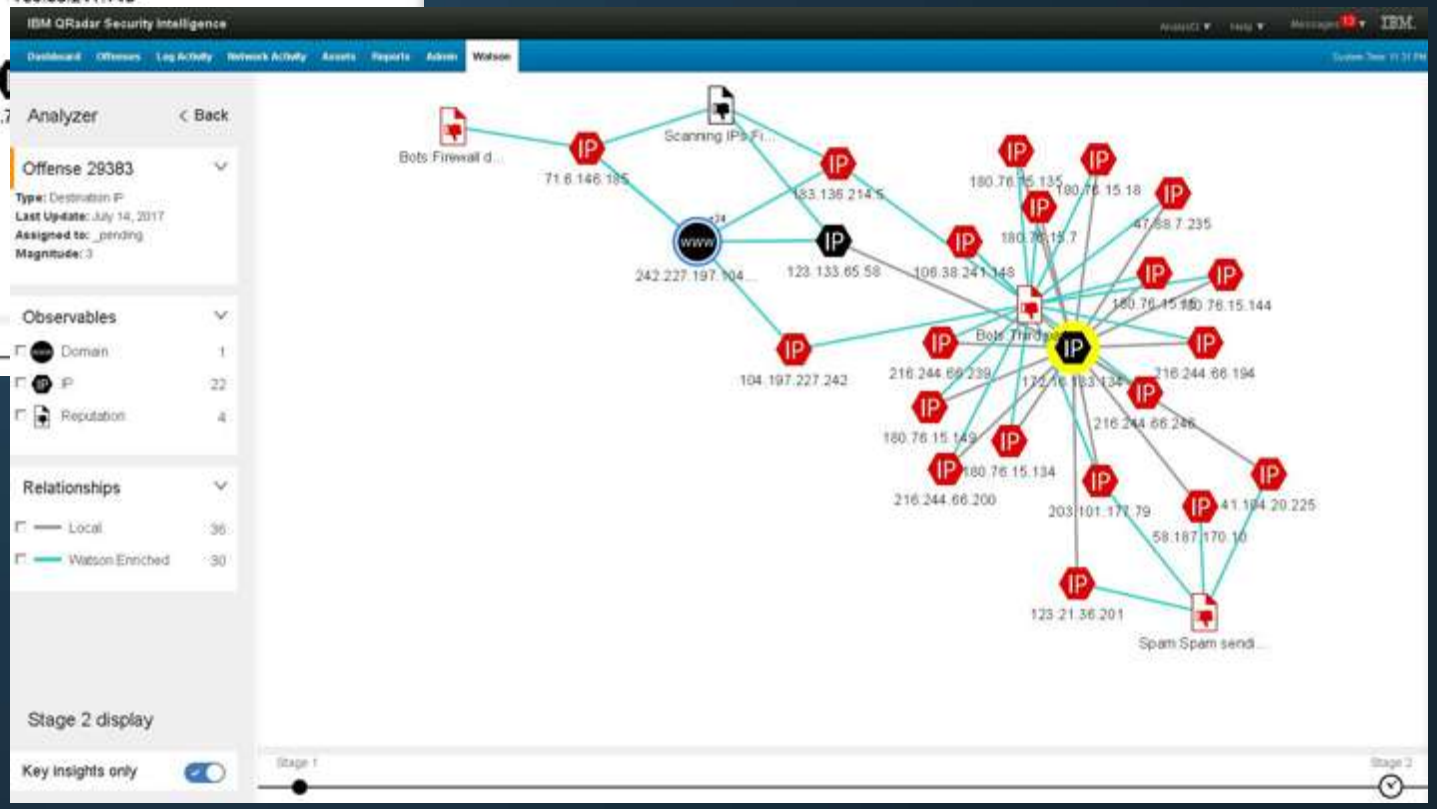


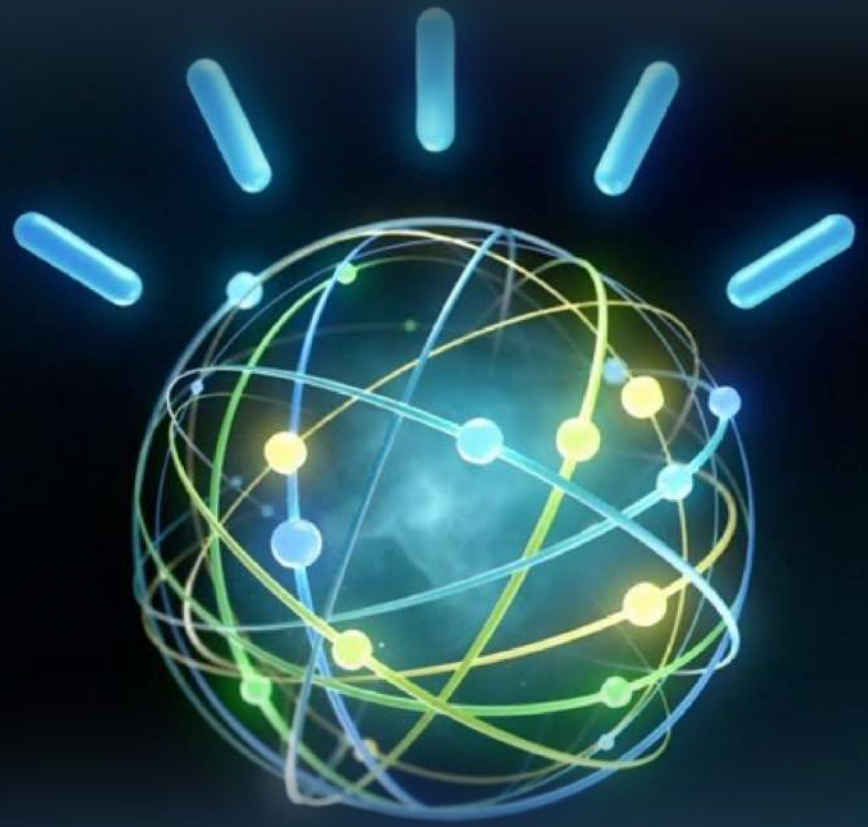
IBM Security

Cognitividad dando la real perspectiva

Análisis usando Qradar Advisor.







Una seguridad que piensa e interactúa como los seres humanos

IBM Security

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM