

# Cognitividad: Cómo apoyará a la Ciberseguridad

---

**Juan Camilo Reyes**

Security Services Leader, SSA Region



# 191 días





# 191 días

**Demora una empresa promedio  
en detectar una brecha de seguridad**

# El día a día del analista de seguridad



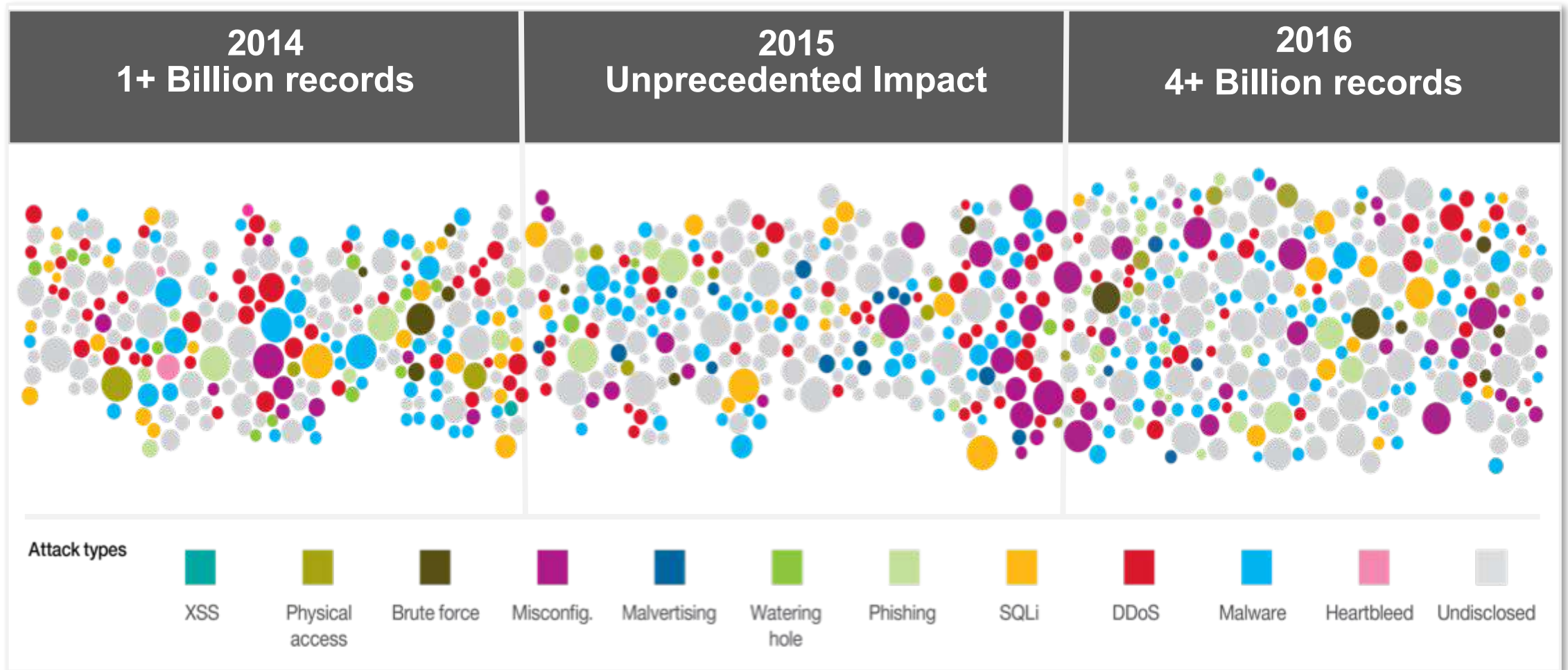


# ¿Cuál es el reto?



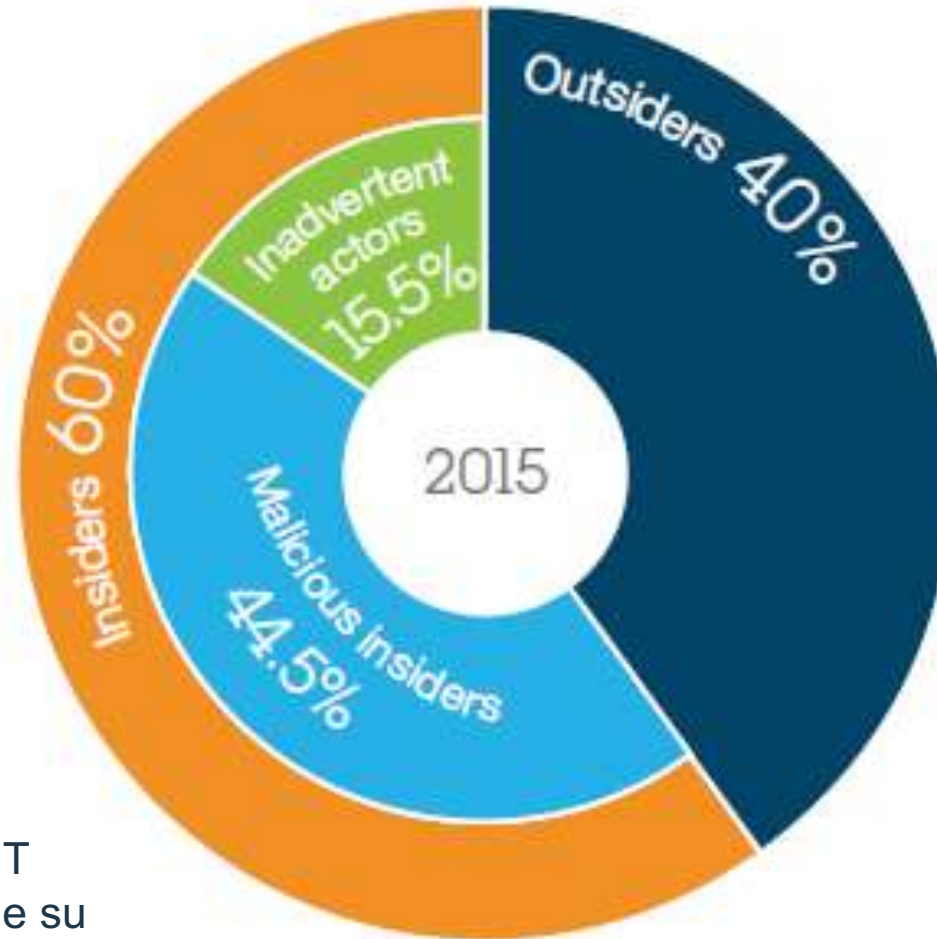
# Detectar un ataque

# 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

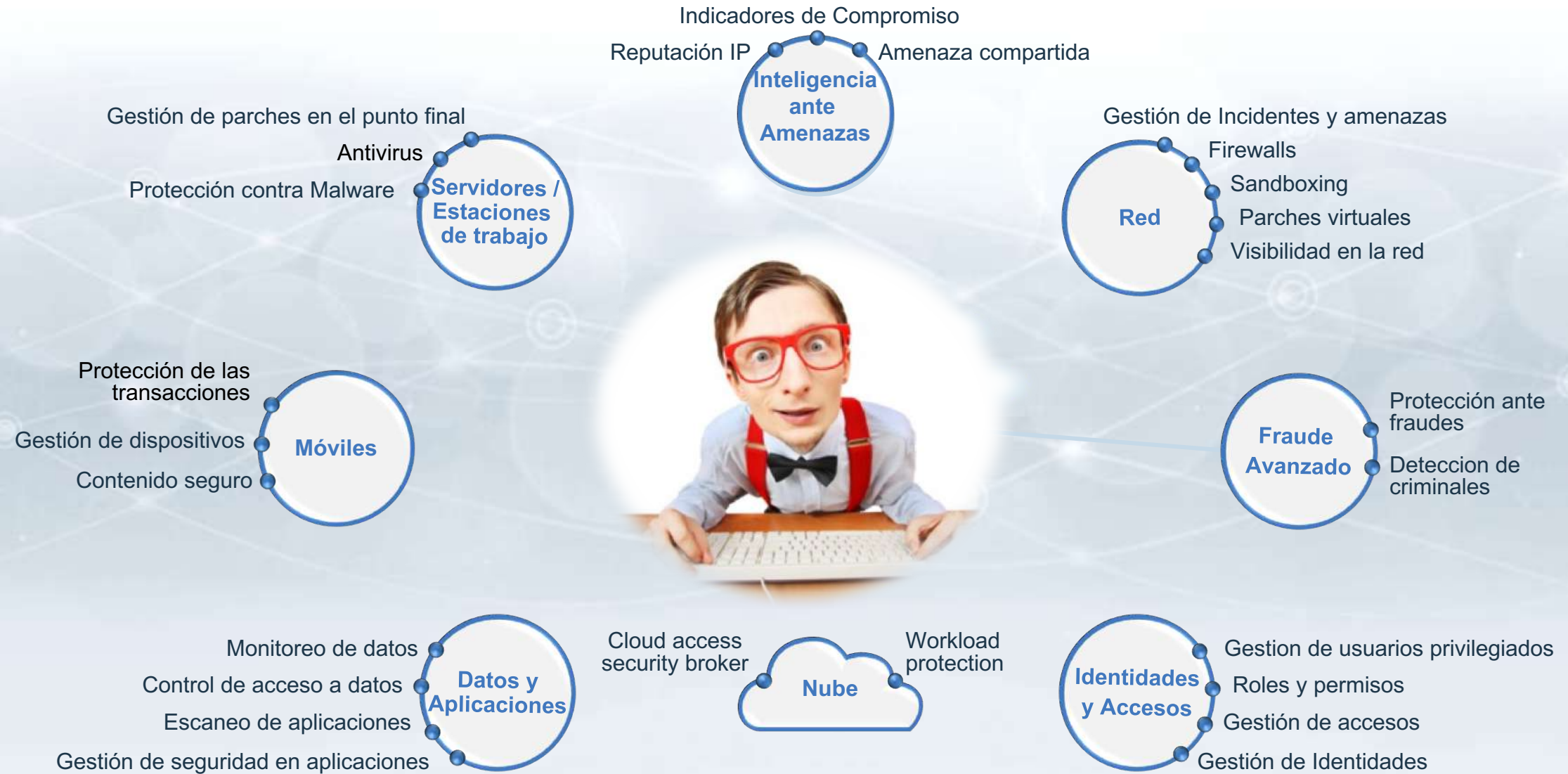
# Incrementando los costos y la complejidad



# El equipo de seguridad ve ruido



# Tiene que analizar eventos de:





**IBM Security**

**Fases de un ataque**

## Penetrar

Encontrar cómo ingresar y ganar credenciales

## Enganchar

Comprometer un servidor vulnerable

## Expandir

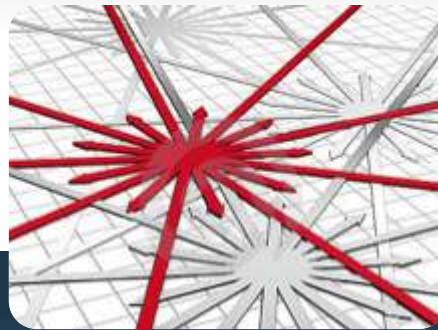
Infectar sistemas o lograr nuevos accesos

## Colectar

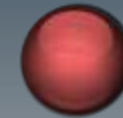
Traer la información a ser robada/expuesta

## Exfiltrar

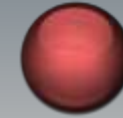
Transmitir la información fuera de la organización.



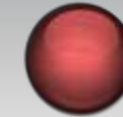
# Controles y vigilancia



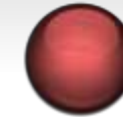
*Antispam/control de correo*



*Filtro Web / VPNs*



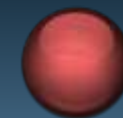
*Web Application Firewall*



*Antivirus*

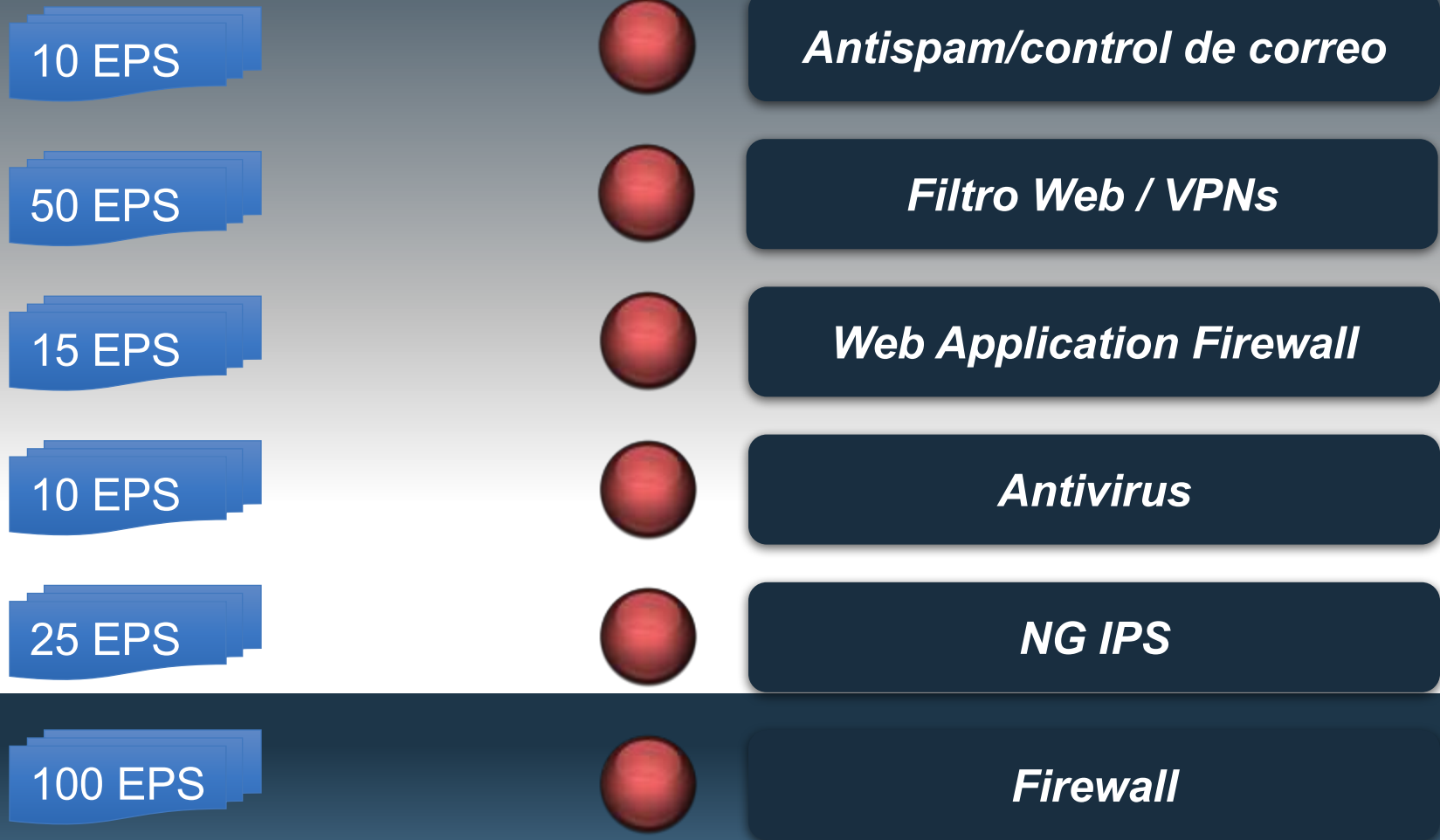


*NG IPS*

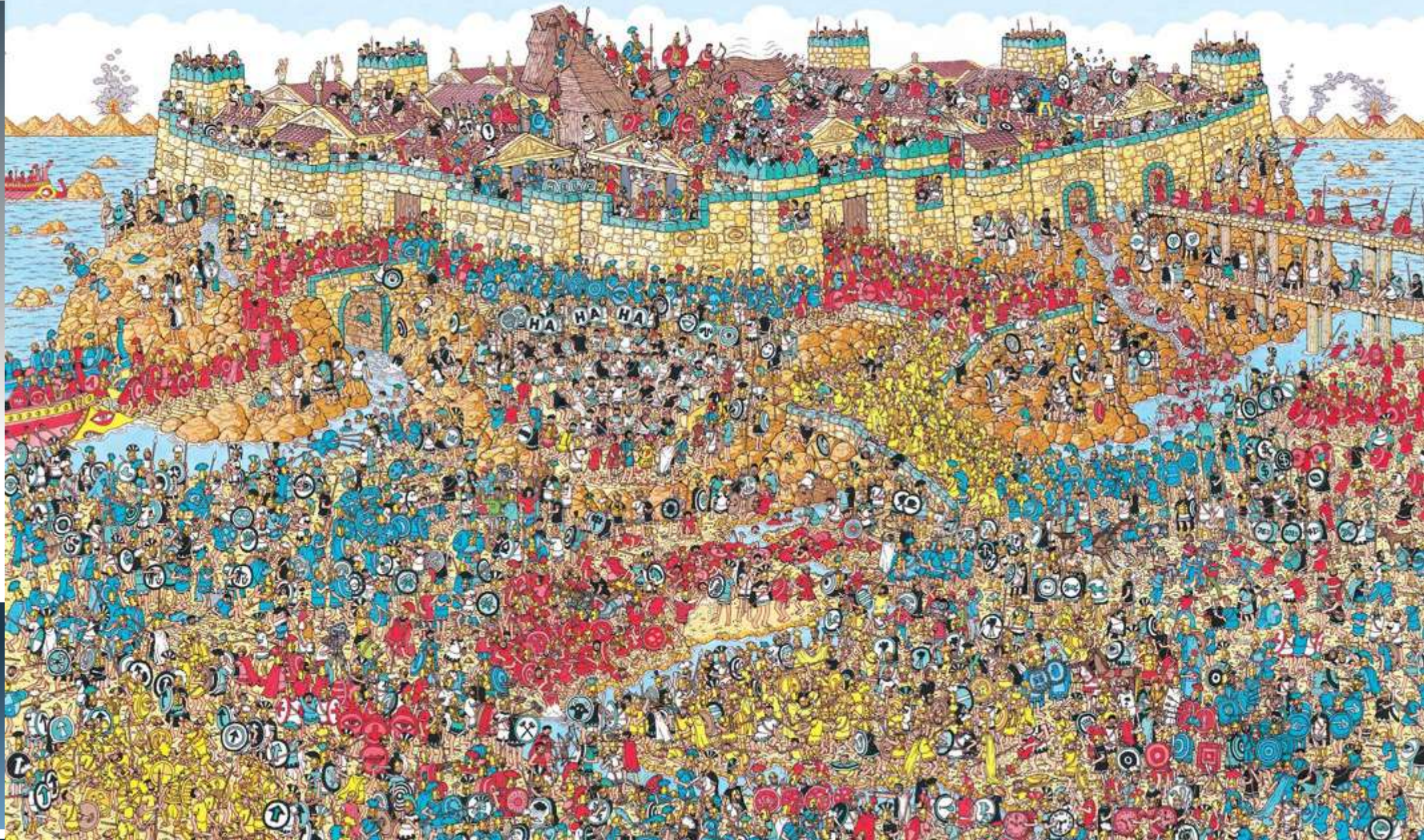


*Firewall*

# Saturación – EPS (Eventos por segundo)









# Correlación de eventos



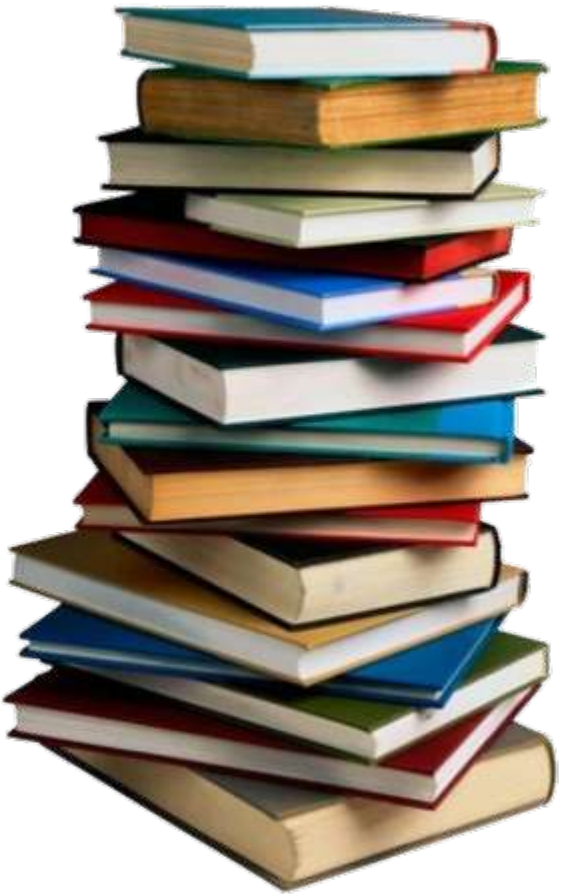
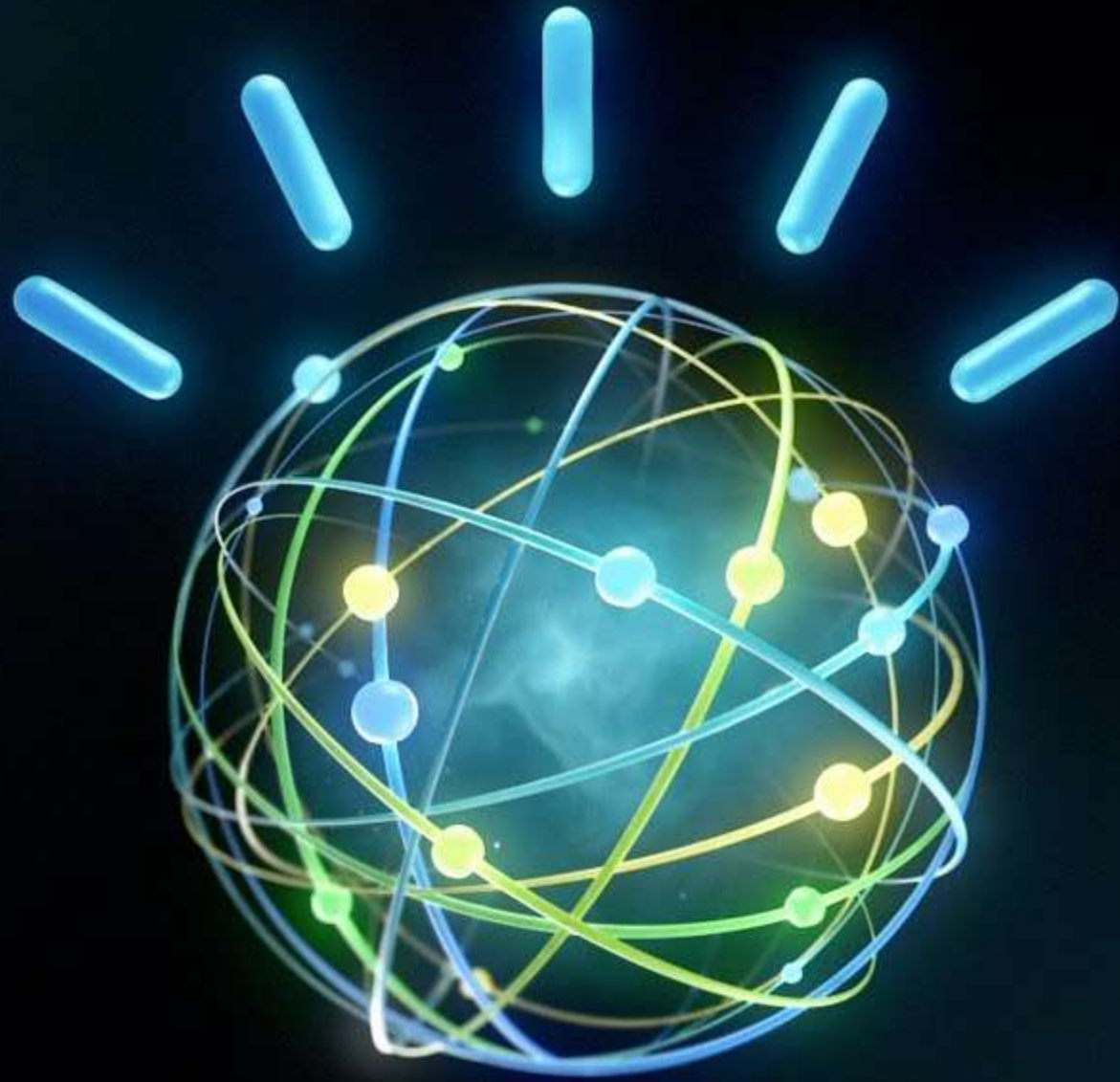


Table 1

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

ΣΜΑΧΗΙΣ

THINK

सोचिए

ΣΚΕΨΟΥ

DENKE

PENSER



**\$300,000**

Who is Stoker?  
(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

The screenshot shows a document editor interface. The main text area contains a document with several terms highlighted in different colors: 'Upatre' (red), 'Dyre' (pink), 'checkip.dyndns.org' (yellow), 'IP address' (yellow), 'IP Address' (yellow), 'malware' (red), 'STUN' (yellow), 'Session Traversal Utilities for NAT' (yellow), 'NAT' (yellow), 'Network Address Translation' (yellow), 'google.com' (yellow), 'Command & Control (C&C)' (teal), 'Upatre' (red), 'Dyre' (pink), 'metflex(.)uk(.)com' (yellow), 't\_image.jpg' (yellow), 'Dyre' (pink), and 'Upatre' (red). The right-hand sidebar displays a list of entity types with corresponding colored icons. The list includes: PLANT, PRODUCT, SECURITY\_CAMPAIGN, SECURITY\_COA, SECURITY\_EXPLOITTARGET, SECURITY\_INDICATOR, SECURITY\_MALWARE, SECURITY\_OBSERVABLE, SECURITY\_THREATACTOR, SECURITY\_TTP, SUBSTANCE, TICKER, TIME, TITLEWORK, VEHICLE, WEAPON, WEATHER, and WEB.

STEP 2: THE FIRST STAGE MALWARE IS EXECUTED - Once the **Upatre** malware is executed, its sole purpose is to download **Dyre**.

This is completed in a few stages.

It's important to note that this stage of the process is completely dynamic.

URLs and payloads are constantly shifting in order to evade detection.

The **Upatre** malware itself constantly evolves and remains obfuscated, allowing it to evade antivirus measures as well.

- 1) **Upatre** contacts **checkip.dyndns.org** in order to determine the public **IP address** of the machine it is on.

This website replies with a simple message Current **IP Address**: x.x.x.x.

The **malware** uses this information to understand who it has infected.

- 2) Next, a **STUN** (**Session Traversal Utilities for NAT**) server is contacted to determine the public **IP address** and the type of **NAT** (**Network Address Translation**) service it's sitting behind.
- 3) Internet connectivity is checked to determine if a proxy is being utilized by contacting google.com.
- 4) **Upatre** makes its initial contact with the **Command & Control (C&C)** server.
- 5) **Upatre** downloads **Dyre** from a varied list of domains as well as changing filenames.

For example, **metflex(.)uk(.)com** hosted a file named "**t\_image.jpg**", which is the **Dyre** malware.

After utilizing this domain, it is quickly changed, as is the file name for **Dyre**, including the renaming of the file extension to pdf and txt.

Regardless of the domain and URL, **Upatre** executes this file and begins the stage 2 infection.

Entity	Mention	
Type	SubType	Role
-	PLANT	
Q	PRODUCT	
-	SECURITY_CAMPAIGN	
-	SECURITY_COA	
-	SECURITY_EXPLOITTARGET	
-	SECURITY_INDICATOR	
-	SECURITY_MALWARE	
-	SECURITY_OBSERVABLE	
-	SECURITY_THREATACTOR	
-	SECURITY_TTP	
I	SUBSTANCE	
-	TICKER	
t	TIME	
y	TITLEWORK	
H	VEHICLE	
W	WEAPON	
R	WEATHER	
Z	WEB	



Video

# Ok, pero como funciona la cognitividad aplicada

## Análisis solamente usando Qradar.



EM Qradar Security Intelligence

Dashboard > Offenses > All Offenses > Offense 29383 (Summary)

Offense: **Offense 29383**

Magnitude		Status	Open	Relevance	1	Severity	7	Credibility	3
Description	Multiple Exploit/Malware Types Targeting a Single Source containing Web Exploit	Offense Type	Malicious IP	Event/Flow count	147 events and 0 flows in 6 categories				
Source IP(s)	Multiple (2)	Start	Jul 13, 2017, 3:50:41 AM						
Destination IP(s)	172.16.132.134	Duration	1 d 0h 27m 14s						
Network(s)	DMZ Internet	Assigned to	Jastilla						

IP	Location	DMZ Internet
172.16.132.134		

IP	172.16.132.134	Location	DMZ Internet
Magnitude		Vulnerabilities	0
Log Name	None	MAC Address	Unknown
Host Name	Unknown	Asset Weight	0
Asset Name	Unknown	Event/Flow	56,370
Chained	No		
Offenses	32		

Source IP(s)	Multiple (2)
Destination IP(s)	172.16.132.134

Magnitude	
Description	Multiple Exploit/Malware Types Targeting a Single Source containing Web Exploit

Event/Flow count	147 events and 0 flows in 6 categories
Start	Jul 13, 2017, 3:50:41 AM

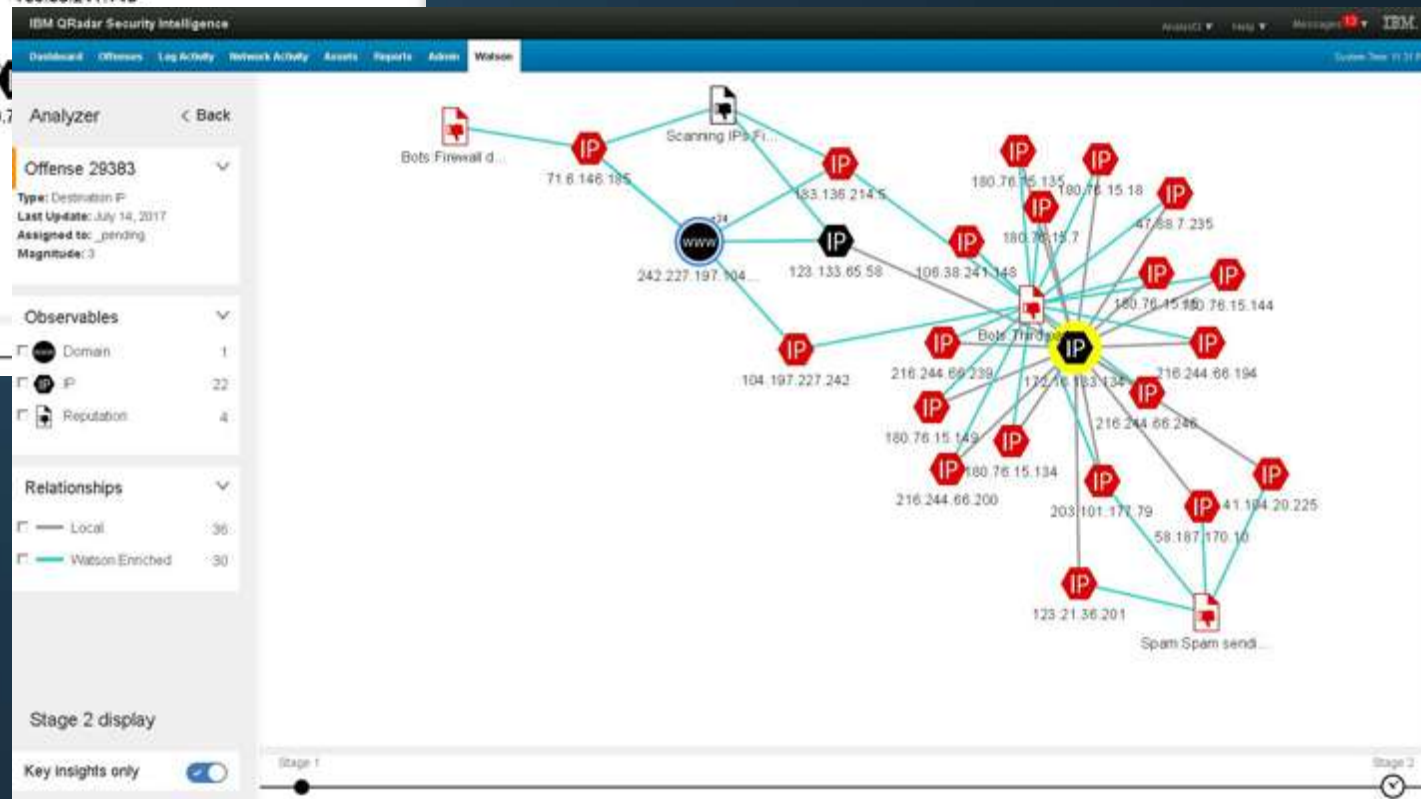
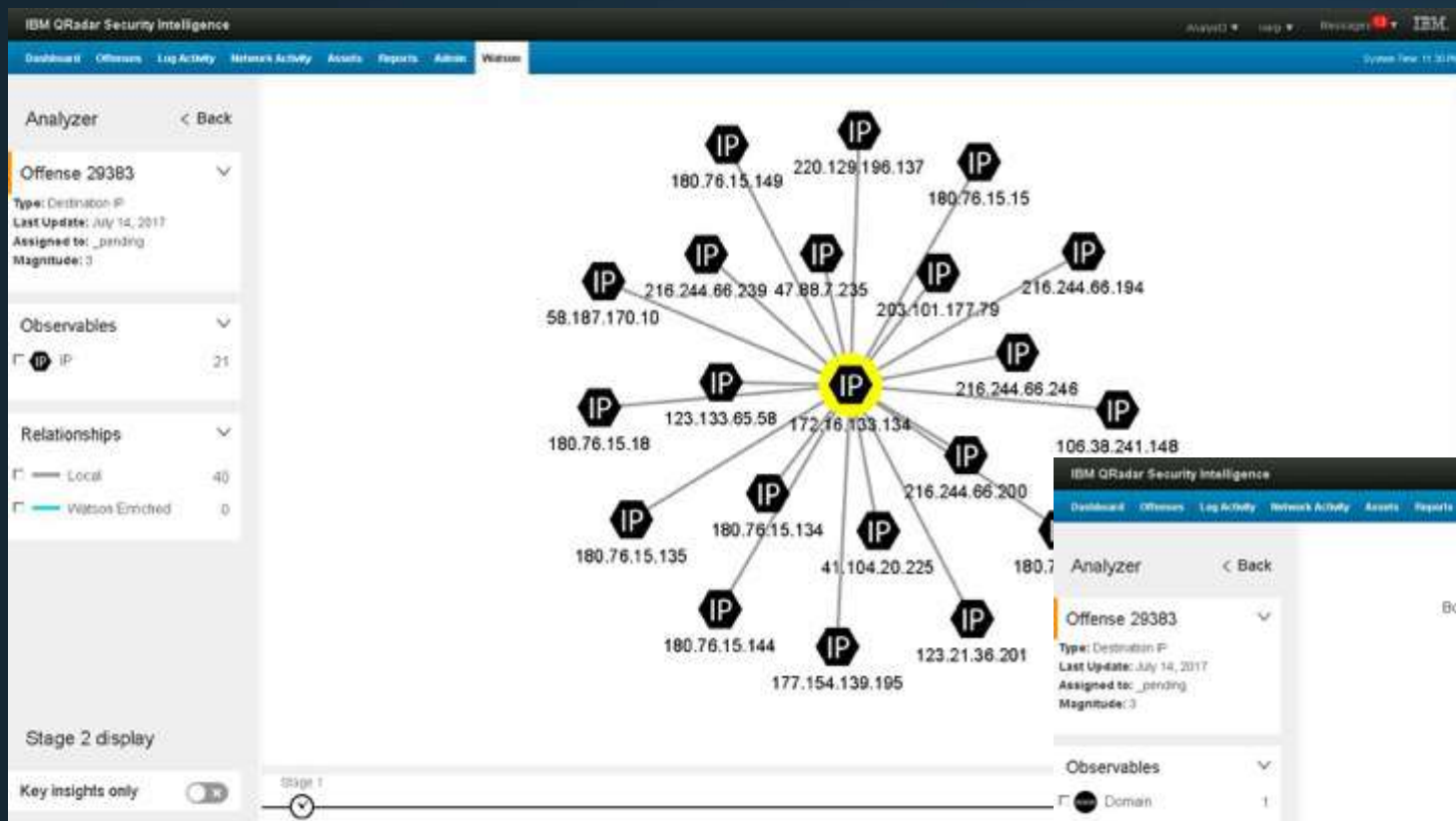


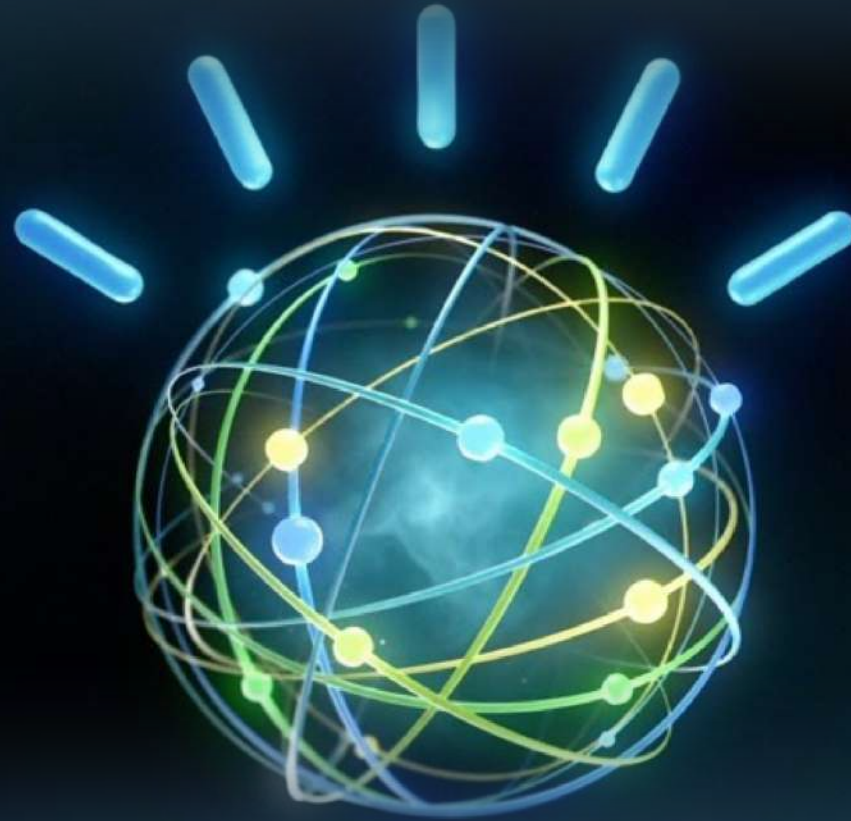
Source IP	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Overcome (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
172.16.132.134	172.16.132.134	80	Multiple (1)	Multiple (2)	Multiple (2)	TCP	None	5	75	75
172.16.132.40	172.16.132.134	80	Multiple (1)	Multiple (2)	Multiple (2)	TCP	None	5	25	25

Event Name	Log Source	Event Count	Severity	File Level Category	Source IP	Source Port	Destination IP	Relevance	Flow
HTTP_200_OK	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_204_NoContent	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_302_Redirect	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_303_Redirect	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_304_NotModified	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_400_BadRequest	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_401_Unauthorized	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_403_Forbidden	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_404_NotFound	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_405_MethodNotAllowed	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_406_NotAcceptable	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_407_ProxyAuthRequired	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_408_Timeout	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_409_Conflict	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_410_Gone	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_411_LengthRequired	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_412_PreconditionFailed	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_413_RequestEntityTooLarge	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_414_RequestURITooLong	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_415_MediaTypeNotSupported	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_416_RequestedRangeNotSatisfiable	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_417_ExpectationFailed	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_500_InternalServerError	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_501_NotImplemented	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_502_BadGateway	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_503_ServiceUnavailable	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_504_GatewayTimeout	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0
HTTP_505_HTTPVersionNotSupported	WebContentServer-g1	1	1	Web Content	172.16.132.134	80	172.16.132.40	1	0

# Cognitividad dando la real perspectiva

Análisis usando Qradar Advisor.










**Una seguridad que  
piensa e interactúa  
como los seres humanos**



# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](http://ibm.com/security)
-  [securityintelligence.com](http://securityintelligence.com)
-  [xforce.ibmcloud.com](http://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube.com/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.