

BU Seguridad

Retos GDPR



Resumen del Reglamento

Estrategia de seguridad tecnológica centralizada en prevenir brechas de seguridad basadas en "State of Art".

1 Protección de los datos

- Perímetro del tratamiento
- Período del tiempo de retención
- Limitar acceso y datos recogidos

2 Seguridad del tratamiento

- Trazabilidad de los datos
- Prevención de fugas
- Proteger la identidad de los usuarios y tratamiento de datos
- Protección de las aplicaciones

3 Notificación en 72h

- Descripción de la violación de los datos
- Consecuencias y medidas adoptadas
- Plan definido de respuesta ante incidentes

GDPR

4 Evaluación continua

- Gestión de riesgo de información e impacto
- Security by design
- Reforzar detección continua amenazas

5 Concienciación

- Cultura de seguridad
- Concienciación ciberseguridad

Aproximación Seguridad Logicalis



Servicio de Adecuación a la GDPR

Análisis GAP

- Assessment Tecnológico

Diagnóstico de la situación actual frente a marcos normativos en materia de seguridad



Medidas Tecnológicas

- Plan de Acción Tecnológico
- Análisis y definición de soluciones
- Implantación y adecuación tecnológica

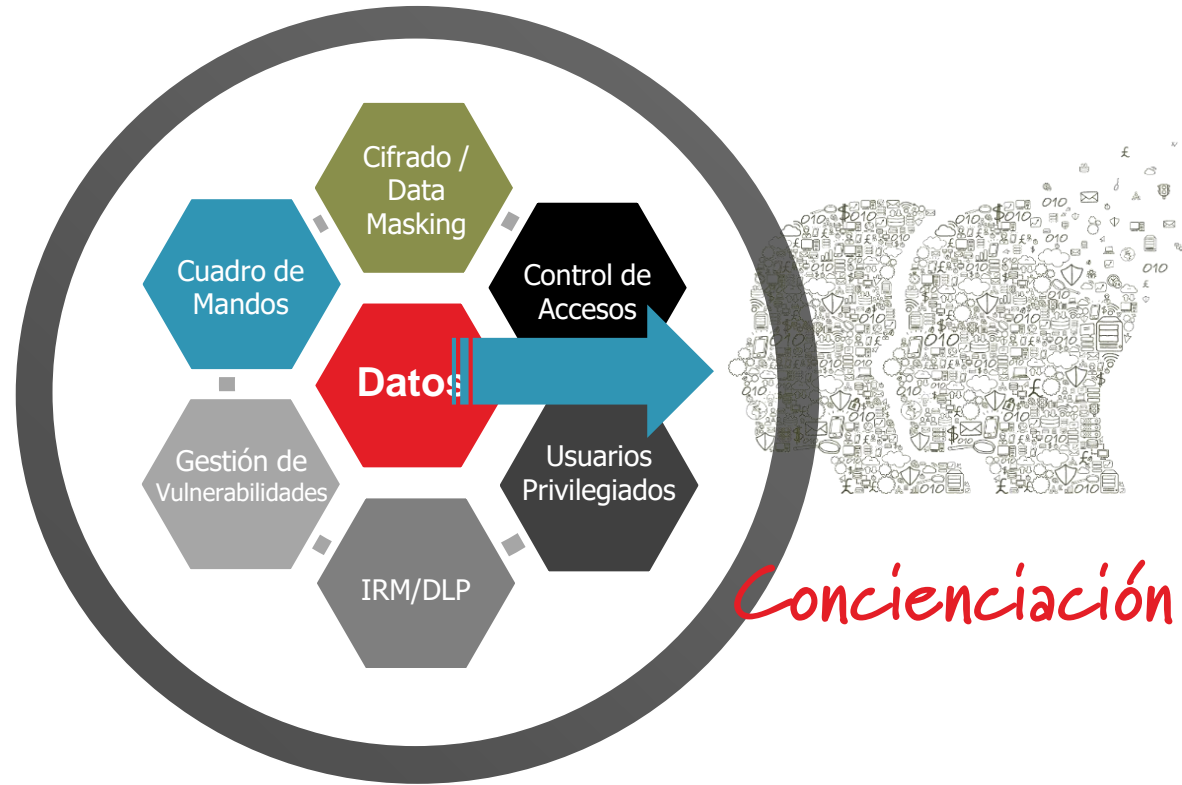


Servicios Gestionados

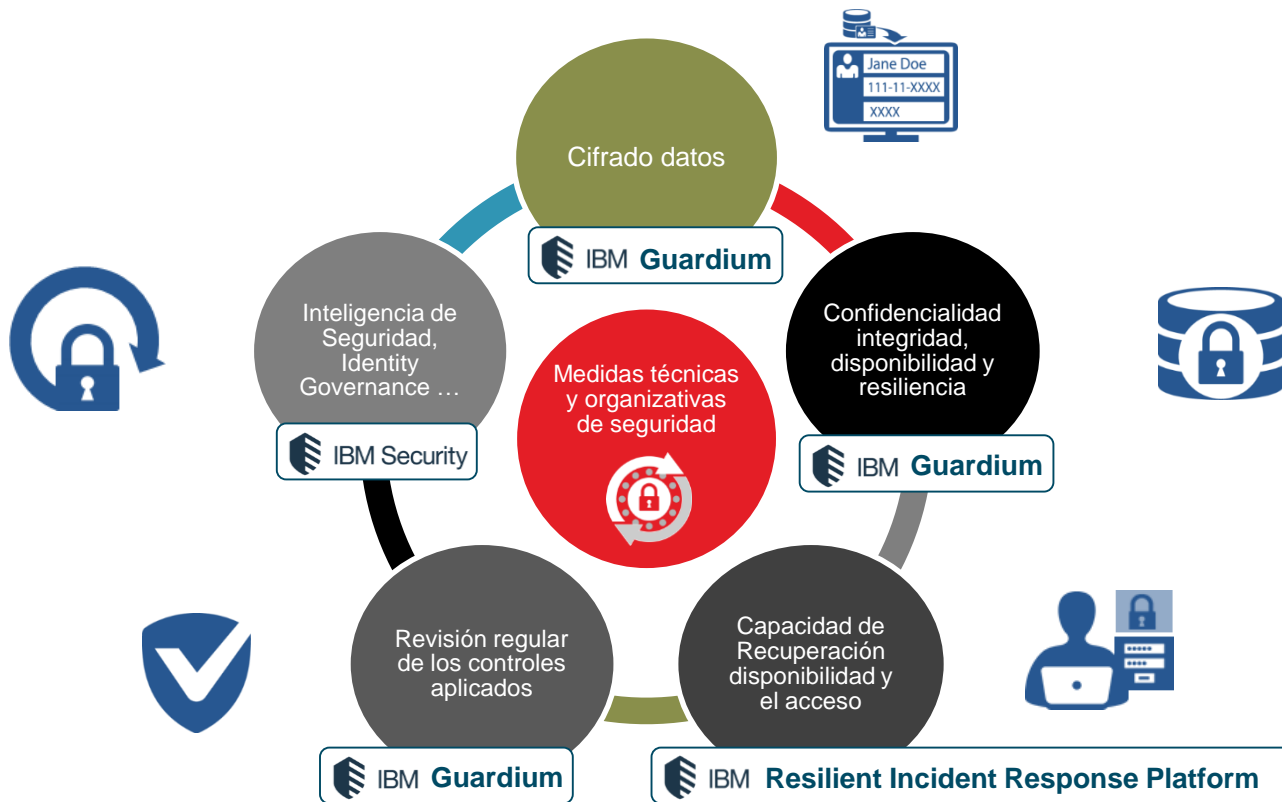
- Soporte correctivo, preventivo y evolutivo
- Servicios Avanzados de Seguridad
- SOC



Medidas Tecnológicas

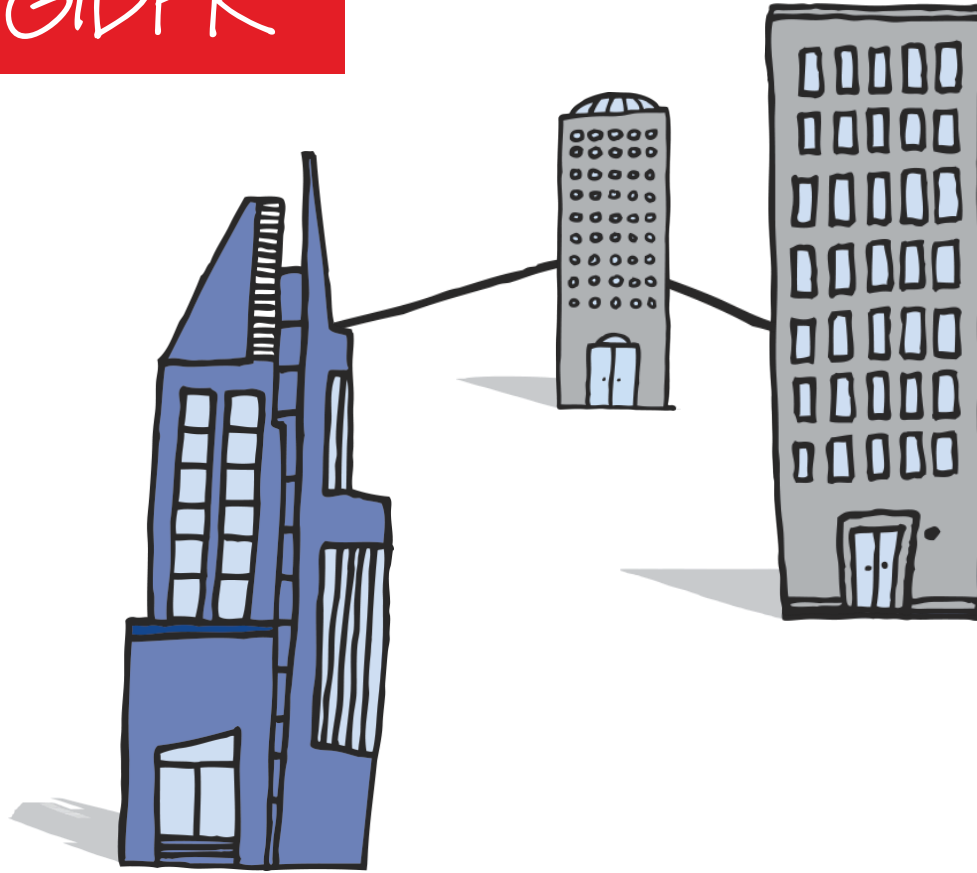


IBM Security GDPR Privacy

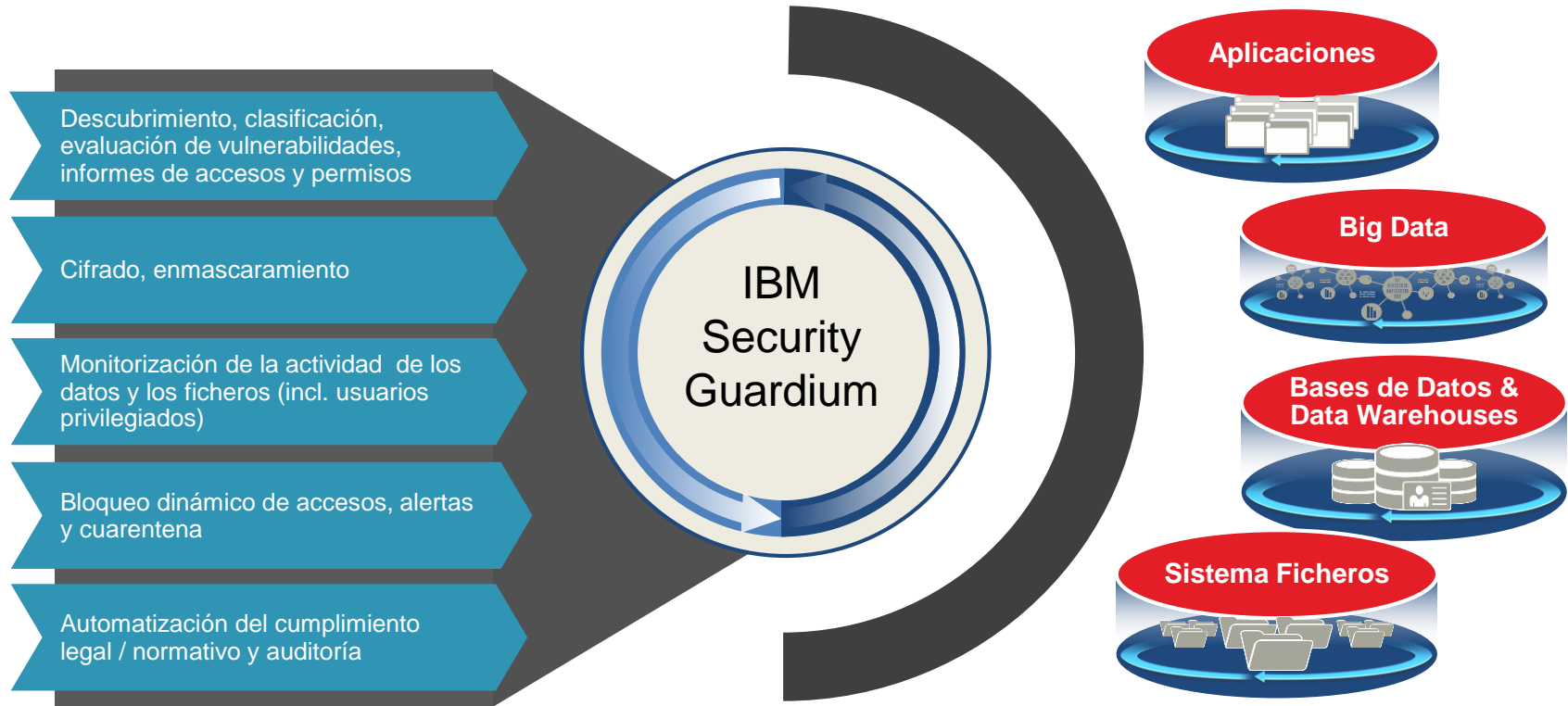


Soluciones GDPR

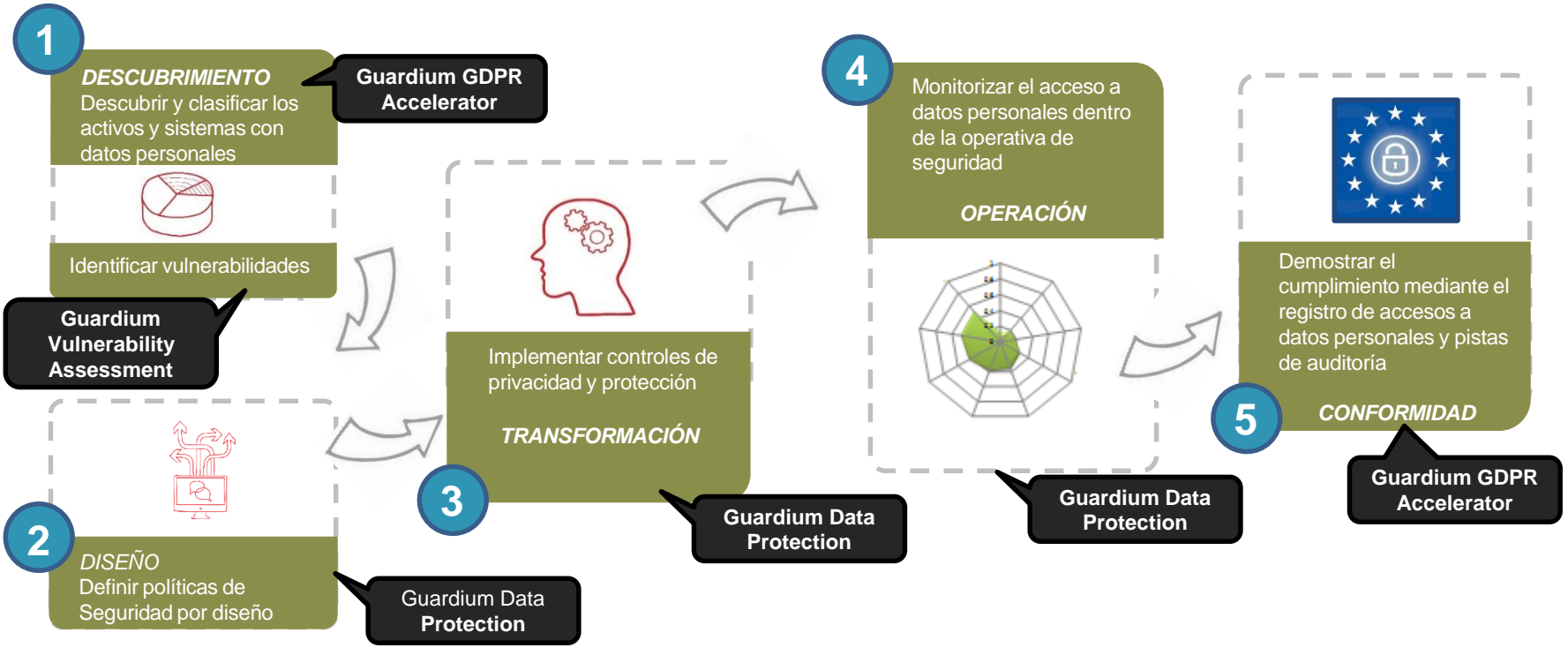
IBM



Data Protection



Aproximación por fases





**Dónde están
mis datos**



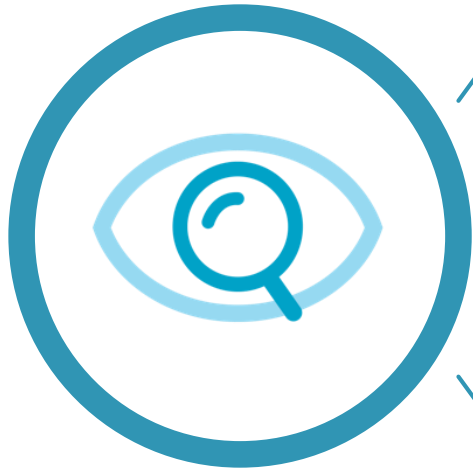
**Escaneo de
vulnerabilidades**



**Monitorización y
Auditoría**

Guardium GDPR Accelerator

Dónde están mis datos



Soluciones al Desafío de Inventario

Descubrimiento de Activos de Base de Datos

Descubrimiento de Datos Sensibles

¿Dónde están mis datos? (1)

The screenshot shows the IBM Guardium console interface for configuring a GDPR discovery scenario. The main area is titled 'Discover Sensitive Data' and 'Details for: GDPR'. A red box highlights the 'What to discover' section, which contains a 'Define classification rules for discovery' link and a 'Classification Rule Templates' table. A callout bubble points to this section with the text '¿Sobre qué parámetros?'. Another red box highlights the 'Selected Classification Rules' table, with a callout bubble pointing to it with the text '¿Qué datos quiero descubrir?'. The interface includes a left sidebar with navigation options like 'Welcome', 'Setup', 'Manage', 'Discover', 'Harden', 'Investigate', 'Protect', 'Comply', 'Accelerators', and 'Reports'. The top navigation bar shows the time as 05:42 and the user as 'User Interface'.

¿Sobre qué parámetros?

¿Qué datos quiero descubrir?

Predefined	Filter
<input type="checkbox"/>	Template Category
<input type="checkbox"/>	Template Pattern
<input type="checkbox"/>	Bank Card
<input type="checkbox"/>	Credit Card Number
<input type="checkbox"/>	Bank Card
<input type="checkbox"/>	American Express
<input type="checkbox"/>	Bank Card
<input type="checkbox"/>	MasterCard
<input type="checkbox"/>	Bank Card
<input type="checkbox"/>	Visa
<input type="checkbox"/>	Bank Card
<input type="checkbox"/>	Union Pay
<input type="checkbox"/>	Personal Identifier
<input type="checkbox"/>	Brazil: Cadastro Nacional de Pessoas Jurídicas (CNPJ)
<input type="checkbox"/>	Personal Identifier
<input type="checkbox"/>	Brazil: Cadastro de Pessoas Físicas (CPF)
<input type="checkbox"/>	Personal Identifier
<input type="checkbox"/>	Brazil: Registro Geral (RG)

Search Type	Name	Continue On Match
<input type="checkbox"/>	Catalog	affiliation
<input type="checkbox"/>	Catalog	age
<input type="checkbox"/>	Catalog	criminal
<input type="checkbox"/>	Catalog	conviction
<input type="checkbox"/>	Catalog	arrest
<input type="checkbox"/>	Catalog	dob
<input type="checkbox"/>	Catalog	date

¿Dónde están mis datos? (2)

IBM Guardium

05:43 User Interface User Interface Search admin, admin - console-only, audit, Baseline, cas, DataPrivacy, fa... pot user Machine Type Standalone

Discover Sensitive Data

Discovery Scenarios

GDPR

GDPR Demo summit

GDPR Demo summit Oracle

Quick Start GDPR scenario

Where to search *Add datasources to search during the classification process*

Available Datasources

¿En qué BBDD?

Name	Type	Host	User Name
<input type="checkbox"/> [VA] ORACLEXE	Oracle(SID)	10.10.9.56	system
<input type="checkbox"/> login failed [Policy Violation] osprey_informix	Informix	10.10.9.56	informix
<input type="checkbox"/> login failed [policy Violation] ORACLEXE	Oracle(SID)	10.10.9.56	system
<input checked="" type="checkbox"/> osprey_db2inst1	DB2	10.10.9.56	db2inst1
<input type="checkbox"/> osprey_informix	Informix	10.10.9.56	informix

Next

Selected Datasources

Name	Type	Host	User Name
<input type="checkbox"/> osprey_system	Oracle(SID)	10.10.9.56	system

Run discovery ✔ Last Run: 2017-09-20 05:26:20 [Edit](#)

Review report ✔ 22390 matches found [Edit](#)

¿Dónde están mis datos? (3)

The screenshot shows the IBM Guardium Discover Sensitive Data interface. The main area displays a table of sensitive data findings. A red box highlights the table content, and several callouts point to specific parts of the interface.

Callouts:

- ¿Qué evidencias? (Points to the table)
- ¿En qué tabla? (Points to the Table Name column)
- ¿Qué regla? (Points to the Rule Description column)
- ¿En qué esquema? (Points to the Schema column)
- ¿En qué columna? (Points to the Column Name column)
- ¿En qué fuente de datos? (Points to the Datasour column)

Generation Time	Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Datasour
2017-09-20 05:26:20	<input type="checkbox"/>	BENJI	CHANGEREQUEST	REQDATE	date		osprey_sys
	<input type="checkbox"/>	FLows_FILES	WWV_FLOW_FILE_OBJECTS\$	LANGUAGE	age		osprey_sys
	<input type="checkbox"/>	FLows_FILES	WWV_FLOW_FILE_OBJECTS\$	UPDATED_BY	date		osprey_sys
	<input type="checkbox"/>	FLows_FILES	WWV_FLOW_FILE_OBJECTS\$	UPDATED_ON	date		osprey_sys

Escaneo de Vulnerabilidades



Fallos de configuraciones

Exceso de privilegios

CVEs

Escaneo de Vulnerabilidades (1)

IBM Guardium 06:39 User Interface User Interface Search admin, admin-console-only, audit, Baselli, cas, DataPrivacy, fa... Machine Type Standalone

Assessment Test Selections

Tests for Security Assessment GDPR Personal Data Assessment DB2

Select All Unselect All Delete Selected

Type	Test Name	Tuning
<input type="checkbox"/>	DB2 Authentication type configuration parameter	CONF Major (n/a)
<input type="checkbox"/>	DB2 Auto-restart after abnormal termination AUTORESTART	CONF Major (n/a)
<input type="checkbox"/>	DB2 CATALOG_NOAUTH parameter is No	CONF Major (n/a)
<input type="checkbox"/>	DB2 CVE-2004-0795	CONF Major (n/a)
<input type="checkbox"/>	DB2 CVE-2004-1372	CONF Major (n/a)
<input type="checkbox"/>	DB2 CVE-2005-0417	CONF Major (n/a)
<input type="checkbox"/>	DB2 CVE-2005-3568	CONF Major (n/a)

Tests available for addition

Filter By

Test Type Predefined Query based CVE APAR All

Severity Critical Major Minor Caution Info All

Other Include CAS Text

ASTER CLOUDERA MANAGER **DB2** DB2 FOR I DB2 z/OS HIVE INFORMIX MONGODB MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SAP HANA SYBASE SYBASE IQ TERADATA

¿Qué tipo de prueba?

¿Sobre qué BBDD?

Escaneo de Vulnerabilidades (2)

Estado actual

Results for Security Assessment: **GDPR Personal Data Assessment DB2**
Assessment executed: 2017-10-25 09:07:41.0

Download PDF Download XML

Tests passing **43%**
CIS Tests passing: 18/69
STIG Tests passing: 9/17
CVE Tests passing: 19/21

Assessment Result History

Date	Tests passing
9/17/17	43%
9/24/17	43%
10/1/17	43%
10/8/17	43%
10/15/17	43%
10/22/17	43%
10/29/17	43%

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

Detalle de severidad

Result Summary *Showing 271 of 271 results (0 filtered)*

	Critical	Major	Minor	Caution	Info
Privilege	3p 39f	2p 8f 2e	-- --	9p 10f	-- --
Authentication	-- --	-- --	-- --	-- --	-- --
Configuration	-- --	1e 31p 7f 153e	-- --	1e 2p 1f 1e	-- --
Version	-- --	1p 1f	-- --	-- --	-- --
Other	-- --	-- --	-- --	-- --	2e

Current filtering applied:
Test Severities: - Show All -
Datasource Severities: - Show All -
Scores: - Show All -
Types: - Show All -

Detalle de la Vulnerabilidad

Assessment Test Results *Showing 271 of 271 results (0 filtered)*

Test / Datasource	Result
DB2 Roles granted to PUBLIC Test category: Priv. Severity: Critical Granting to PUBLIC increases the risk of unauthorized entry into the database. Because PUBLIC is accessible by any database user, it is important to understand the exposure it has on all database objects. As any role granted to PUBLIC can potentially allow the compromise of database availability, confidentiality, or integrity, these roles should be restricted according to the needs of the business. Ext. Reference: CIS IBM_DB2 10 v1 1.0 Item #6.4 [VA] DB2INST1	Fail One or more roles are granted to PUBLIC. Recommendation: We recommend you to revoke roles that are granted to PUBLIC. You can use this command to revoke: <code>revoke role <role name> from PUBLIC;</code>

Recomendaciones

Monitorización y Auditoría



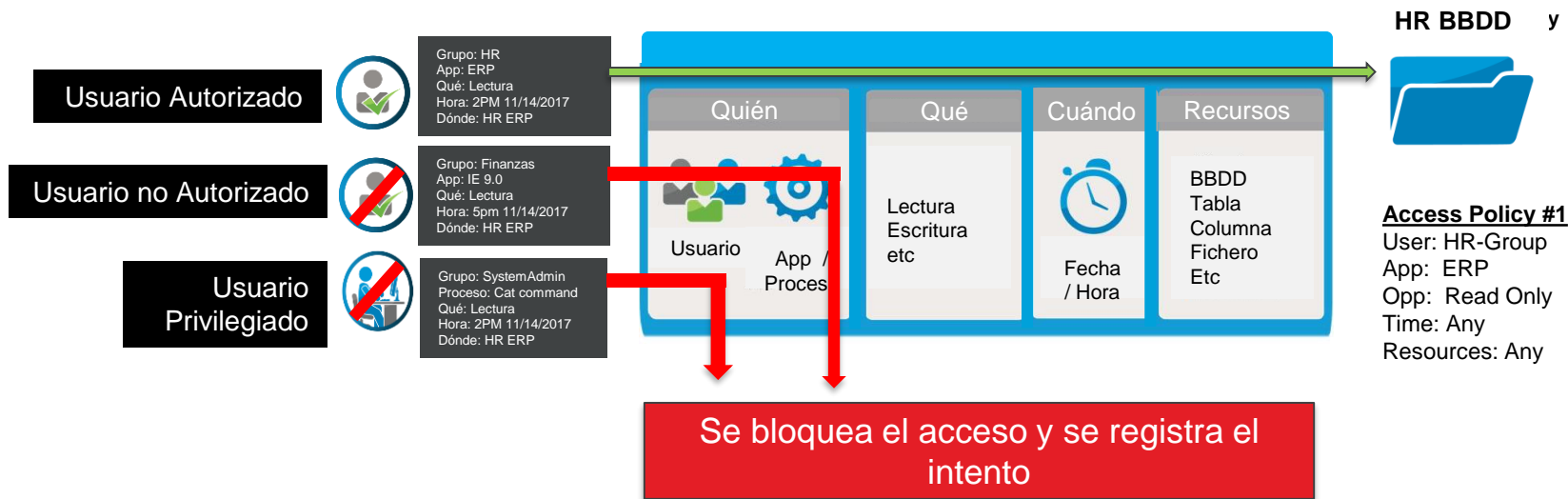
Caso de Uso: Data Breach

Políticas de Auditoría

Análisis de actividad de usuarios en tiempo real

Violación de políticas. Enmascaramiento

Monitorización y Auditoría (1)



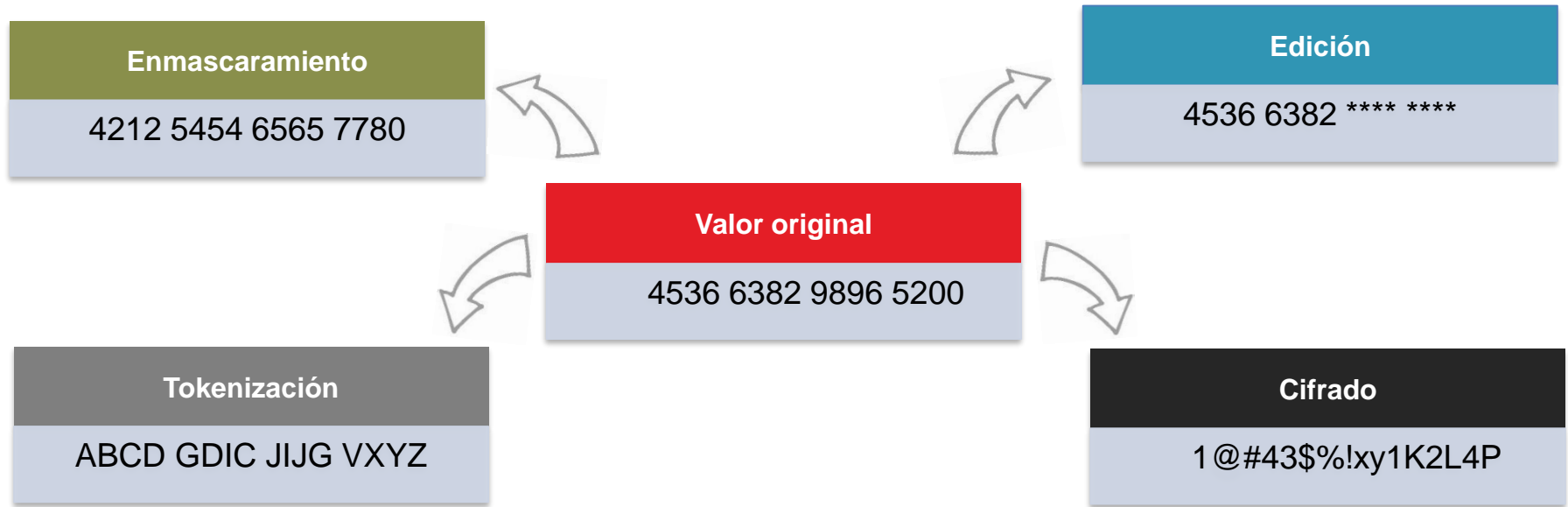
Toma de decisiones dinámica en base al comportamiento del usuario

Monitorización y Auditoría (2)

The screenshot displays the IBM Guardium interface for monitoring database activity. The main content area shows a table titled "GDPR - Personal Data Admin Activity" with a sub-header "GDPR - After Hours Access to Personal Data". The table lists various database users and their activities. One row, corresponding to user JOE performing a SELECT query, is highlighted with a red border and labeled "Posible Violación".

DB User Name	Client IP	Server IP	Database Name	Server Type	SQL Verb	Count of Object Name	Total access
JOE	10.10.9.56	10.10.9.56	XE@XE	ORACLE	BEGIN	2	9
JOE	10.10.9.56	10.10.9.56	XE@XE	ORACLE	CREATE TABLE	1	1
JOE	10.10.9.56	10.10.9.56	XE@XE	ORACLE	DELETE	1	1
JOE	10.10.9.56	10.10.9.56	XE@XE	ORACLE	DROP TABLE	1	1
JOE	10.10.9.56	10.10.9.56	XE@XE	ORACLE	INSERT	1	2
JOE	10.10.9.56	10.10.9.56	XE@XE	ORACLE	QUERY HINT	1	1
JOE	10.10.9.56	10.10.9.56	XE@XE	ORACLE	SELECT	9	68
LARRY	10.10.9.56	10.10.9.56	XE@XE	ORACLE	BEGIN	1	2
LARRY	10.10.9.56	10.10.9.56	XE@XE	ORACLE	SELECT	5	8
POLLY	10.10.9.56	10.10.9.56	XE@XE	ORACLE	BEGIN	1	2
POLLY	10.10.9.56	10.10.9.56	XE@XE	ORACLE	SELECT	5	8
RODRIGO	10.10.9.56	10.10.9.56	XE@XE	ORACLE	BEGIN	2	3
RODRIGO	10.10.9.56	10.10.9.56	XE@XE	ORACLE	select	7	10
SYSTEM	10.10.9.56	10.10.9.56	XE@XE	ORACLE	BEGIN	2	3
SYSTEM	10.10.9.56	10.10.9.56	XE@XE	ORACLE	select	1	1
Total: 16							

Monitorización y Auditoría (3)



Toma de decisiones dinámica en base al comportamiento del usuario

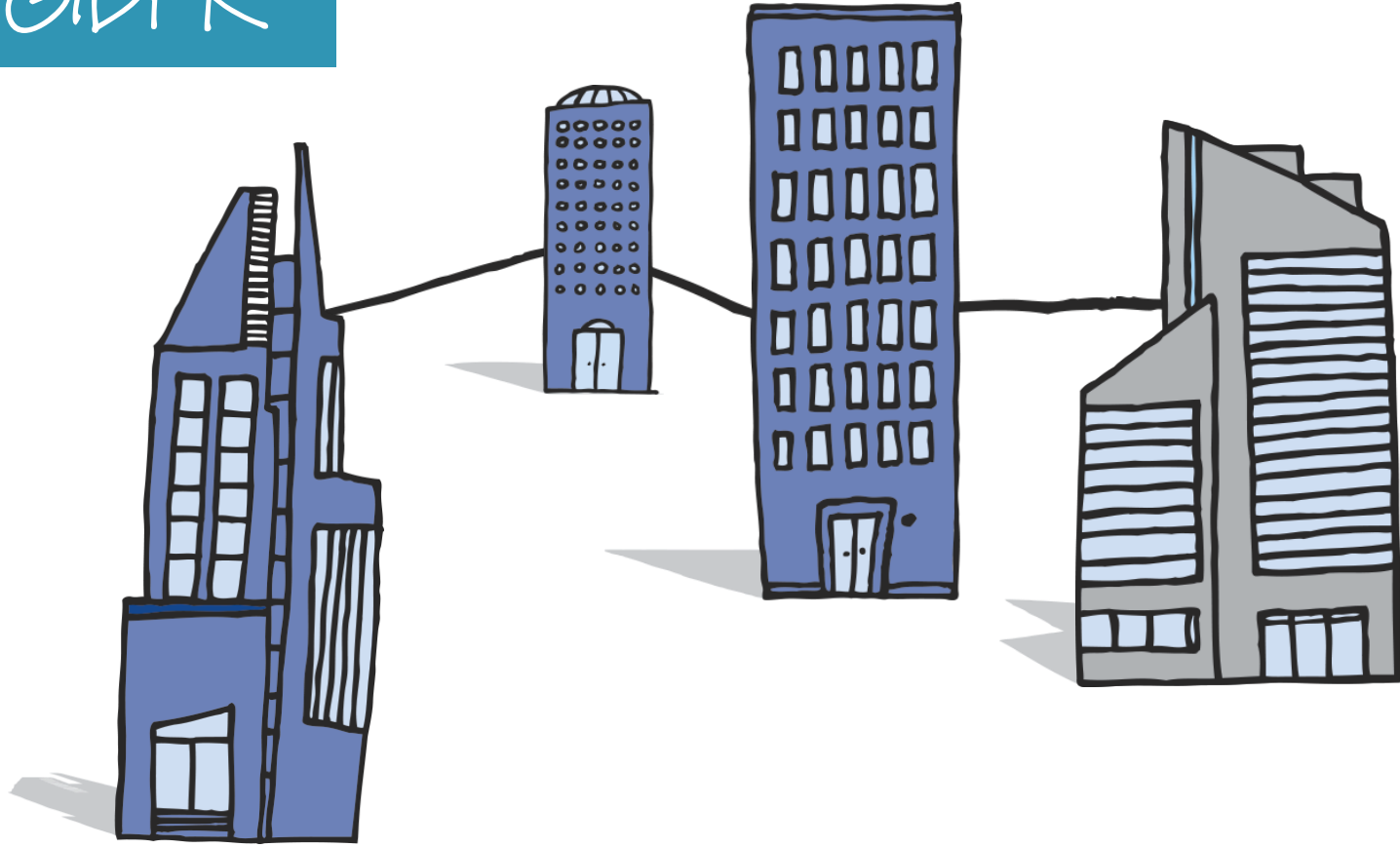
Monitorización y Auditoría (4)

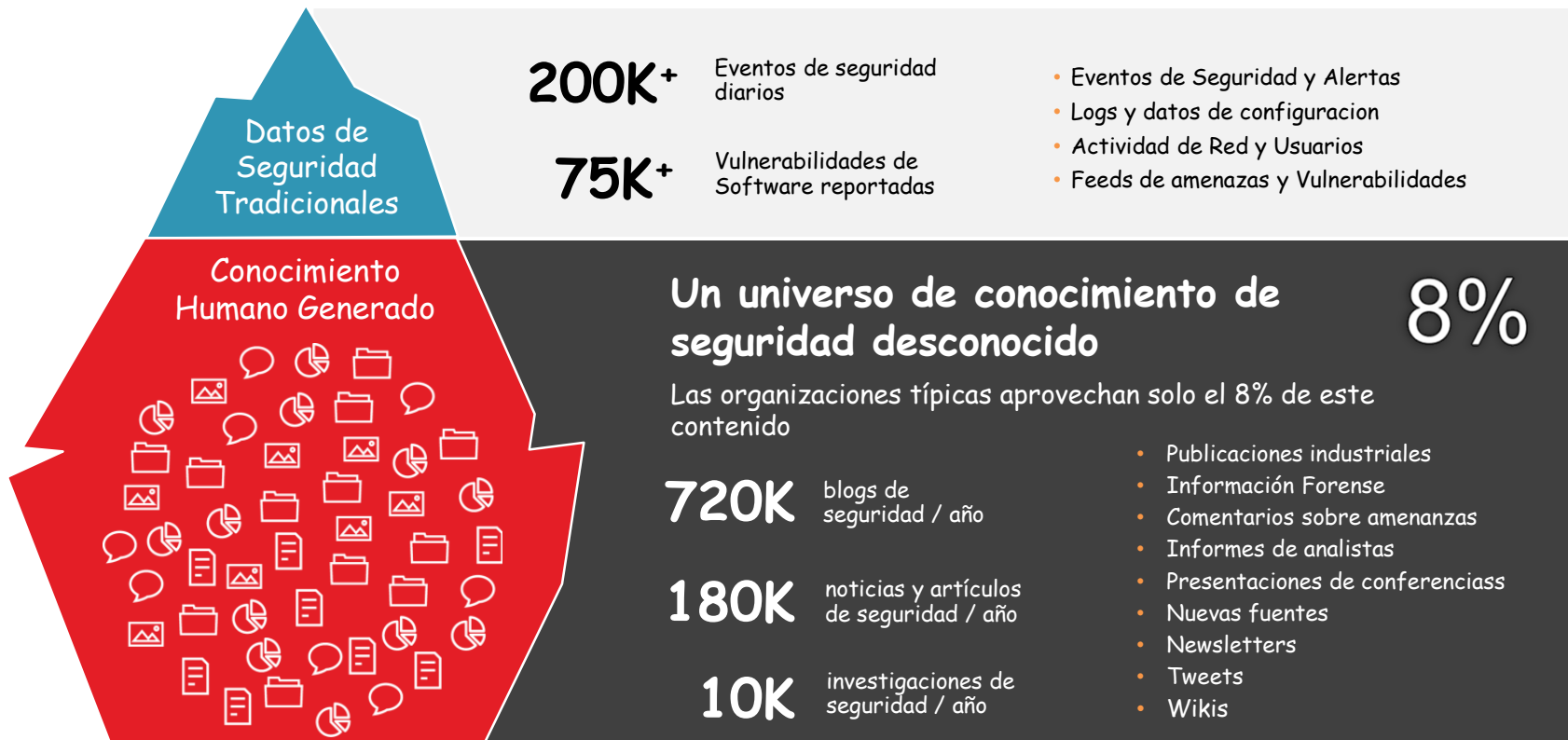
The screenshot displays the IBM Guardium interface for monitoring policy violations. The main content area is titled "Policy Violations" and shows a table of violations. The table has the following columns: Timestamp, Category Name, Access Rule Description, Client IP, Server IP, DB User Name, Full SQL String, Severity Description, and Count of Policy Rule Violations. Two violations are listed, both with a timestamp of 2017-11-02 07:20:28 and a category of GDPR. The first violation's "Access Rule Description" is "Credit Card Numbers, Unauthorized Users - Log Violation" and its "Full SQL String" is a complex query. A callout box labeled "Acceso no autorizado" points to the "Access Rule Description" column. Another callout box labeled "Enmascaramiento" points to the "Full SQL String" column, which contains a list of credit card numbers. The interface also shows a navigation menu on the left with options like Setup, Manage, Discover, Harden, Investigate, Protect, Comply, Accelerators, Reports, and My Dashboards. The top bar includes the IBM Guardium logo, time (07:22), user interface settings, and search functionality.

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Count of Policy Rule Violations
2017-11-02 07:20:28	GDPR	Credit Card Numbers, Unauthorized Users - Log Violation	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.creditcard Extrusion Values. 123456789012345 0,12345678901234 51,1234567890123 452,123456789012 3453,12345678901 23454,1234567890 123455,123456789 0123456,12345678 90123457,1234567 890123458,123456 7890123459,12345 67890123510,1234 567890123511,123 4567890123512,12 34567890123513,1 234567890123514	LOW	1
2017-11-02 07:20:28	GDPR	Credit Card Numbers, Unauthorized Users - Log Violation	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.creditcard Extrusion Values. 123456789012351 5,12345678901235 16,1234567890123 517,123456789012 3518,12345678901	LOW	1

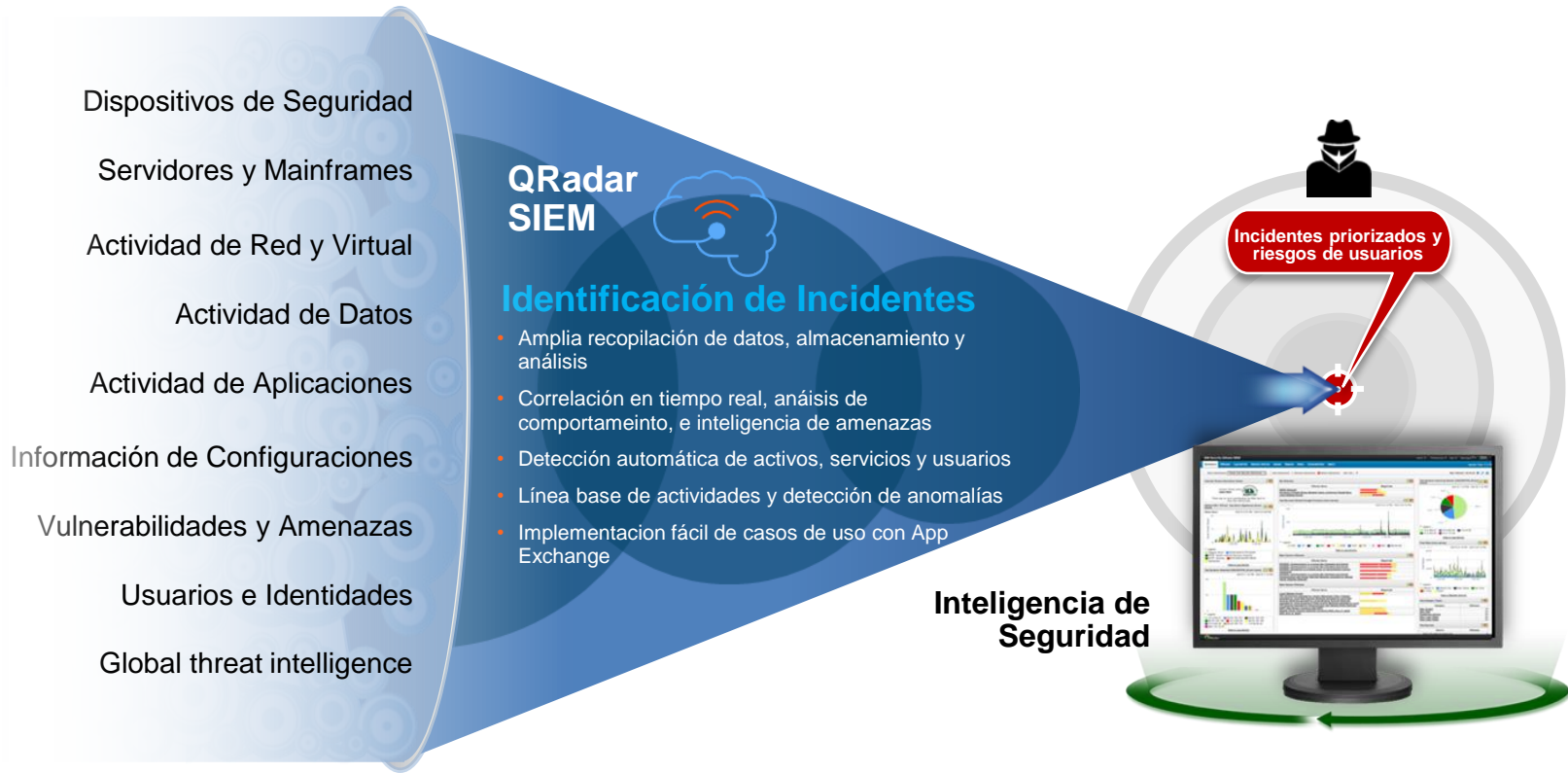
Soluciones GDPR

Integración

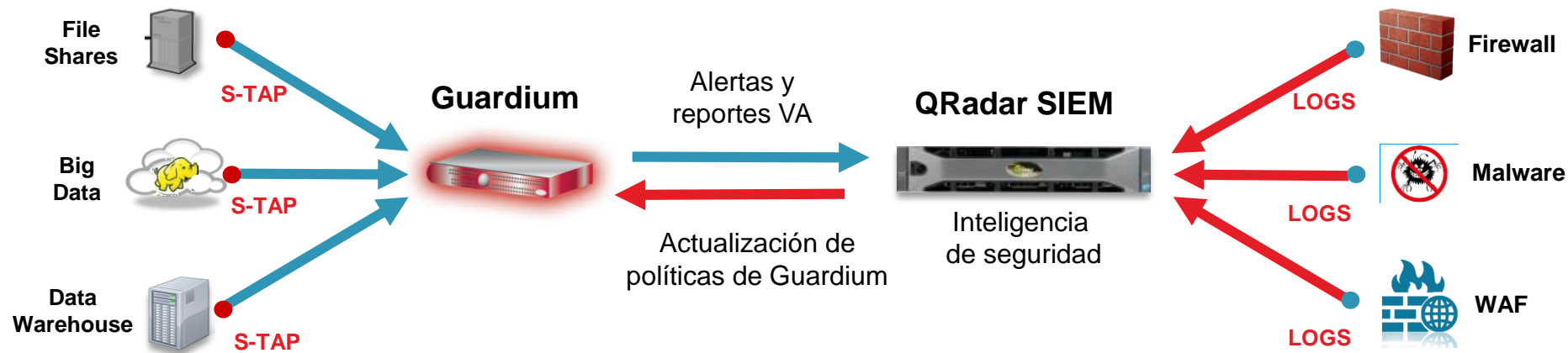




Plataformas SIEM QRadar



Data Protection & SIEM (I)



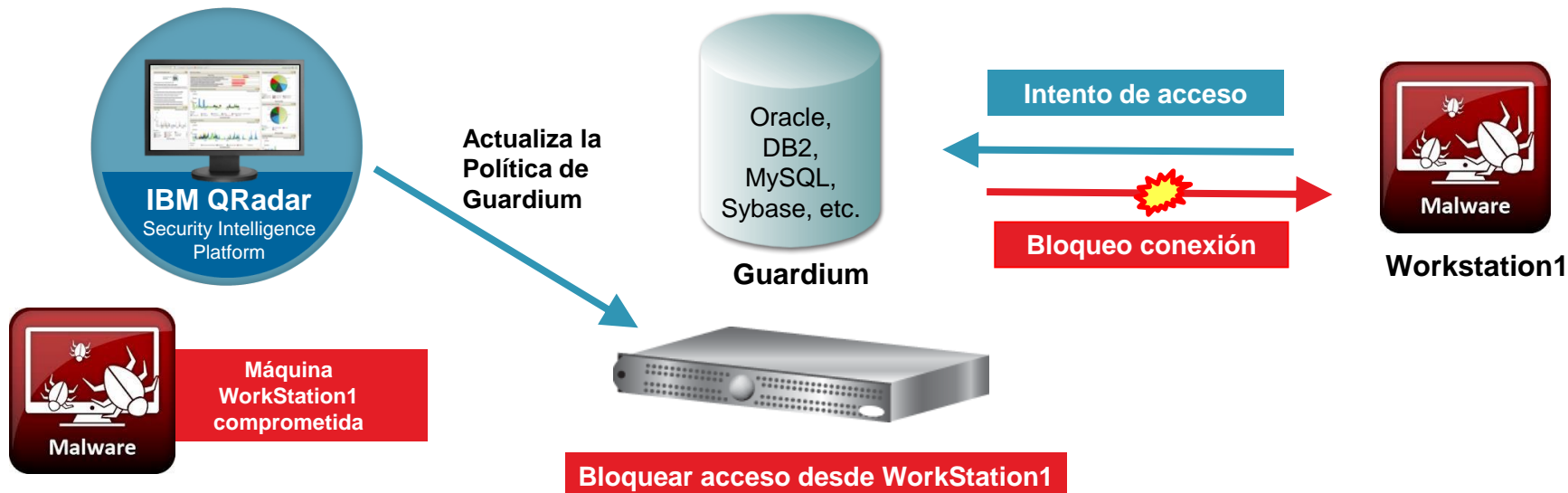
Es posible mantener las políticas de Guardium actualizadas en tiempo real y de forma automática en respuesta a eventos de seguridad de QRadar

Flujo de información bidireccional

Data Protection & SIEM (II)

Caso de Uso

- Detección de una máquina infectada con Malware y bloqueo automático del acceso



Respuesta Incidentes de Seguridad

Los desafíos en la comunicación de brechas de seguridad

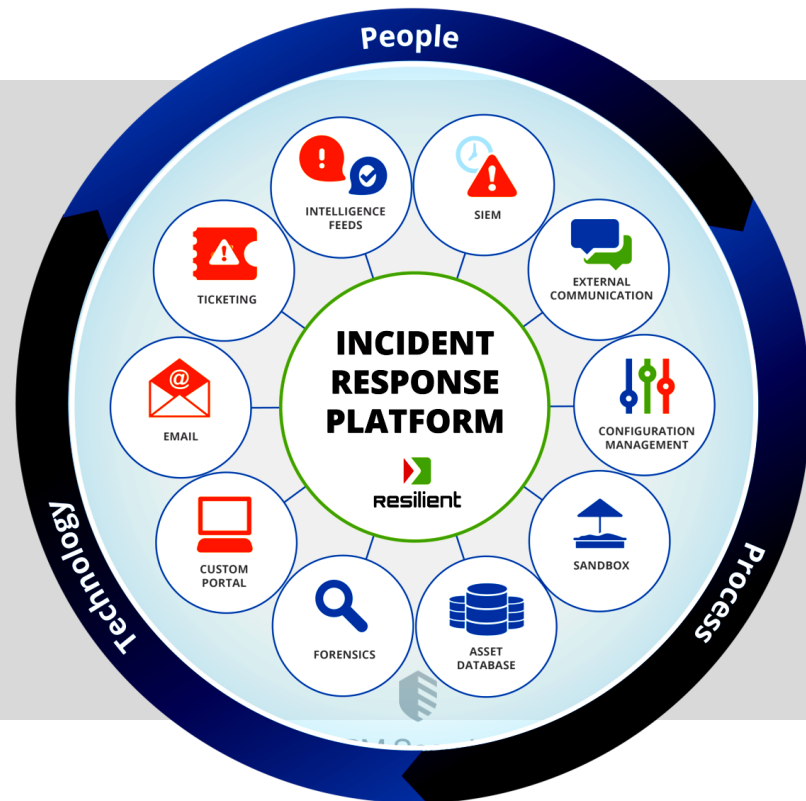
GDPR Obligará a reportar a las autoridades una brecha de seguridad en menos de **72 horas** y a notificar a los clientes afectados por las mismas. Lo que plantea un gran reto en los equipos de seguridad.

Reduce tiempos, mejora la orquestación, facilita la recolección de evidencias

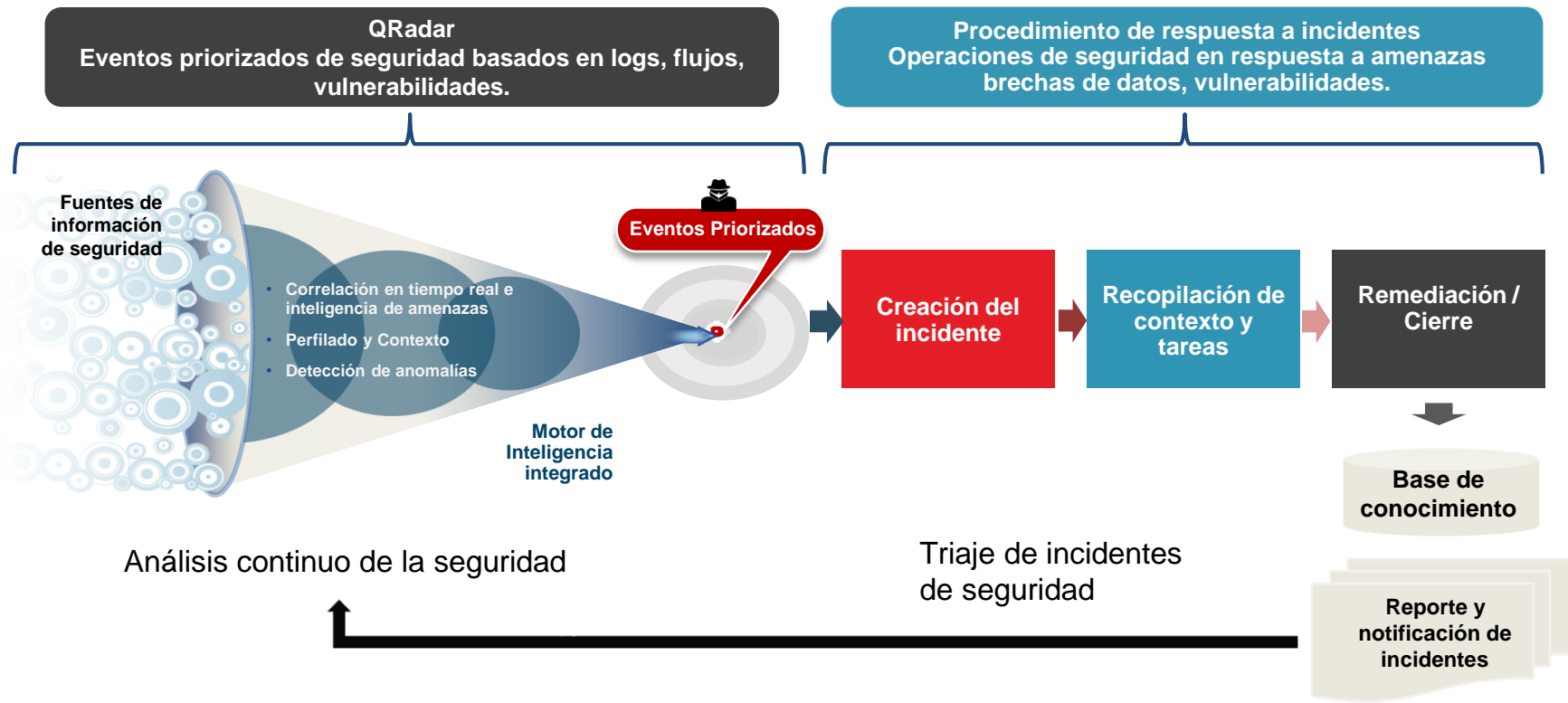
Permitirá a los equipos de seguridad orquestar los procesos de respuesta, y resolver incidentes más rápido y de forma más inteligente. Lo que antes se hacía en días/semanas ahora puede hacerse en horas/días.

Se integra a la perfección con productos de IBM y de terceros

Además posee funcionalidades específicas para cumplimiento y seguimiento GDPR (GDPR Enhanced Privacy Module).



Respuesta Incidentes & SIEM



QRadar Watson. Tiempo de Respuesta

Análisis Manual de Amenazas



QRadar Advisor con Asistencia de Watson



Análisis rápido y preciso de las amenazas de seguridad, ahorrando tiempo y recursos valiosos

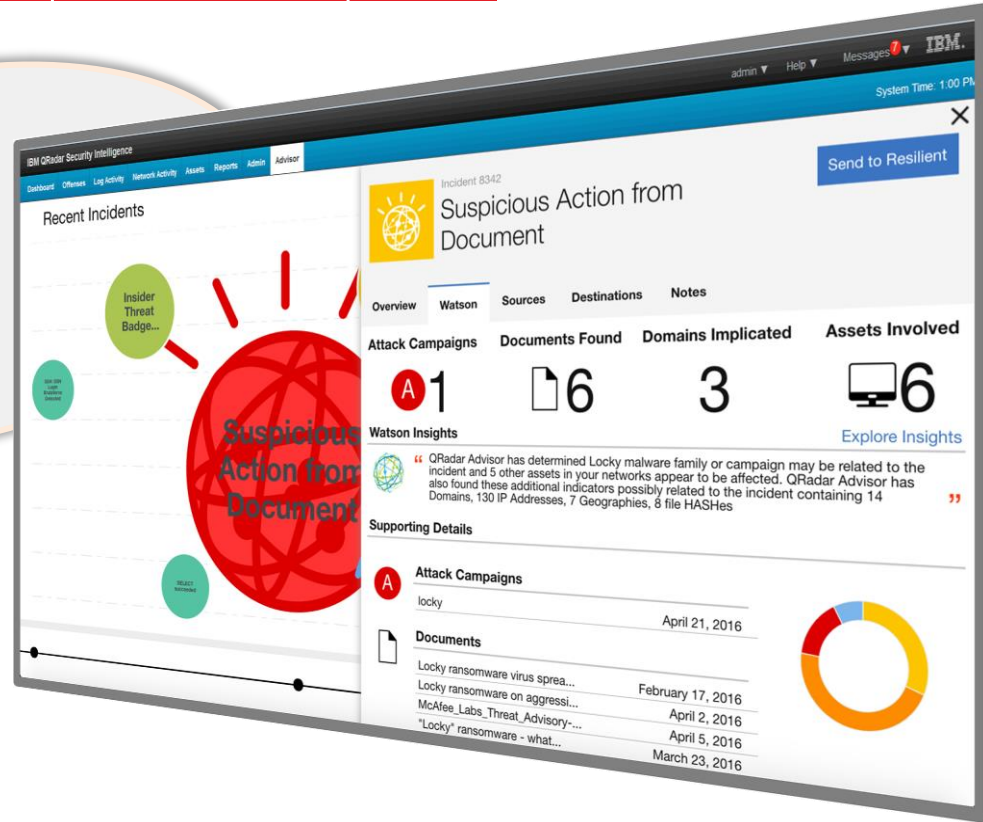
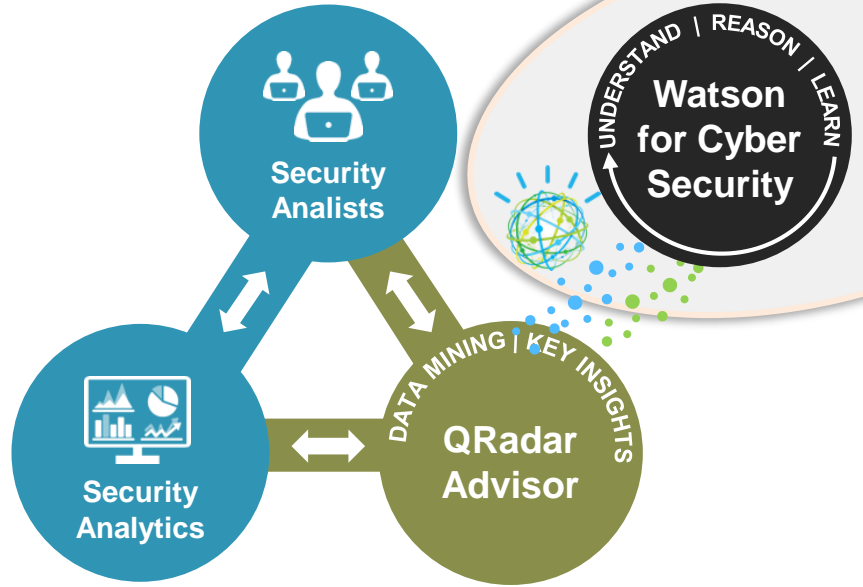
Enterprise Security Analytics



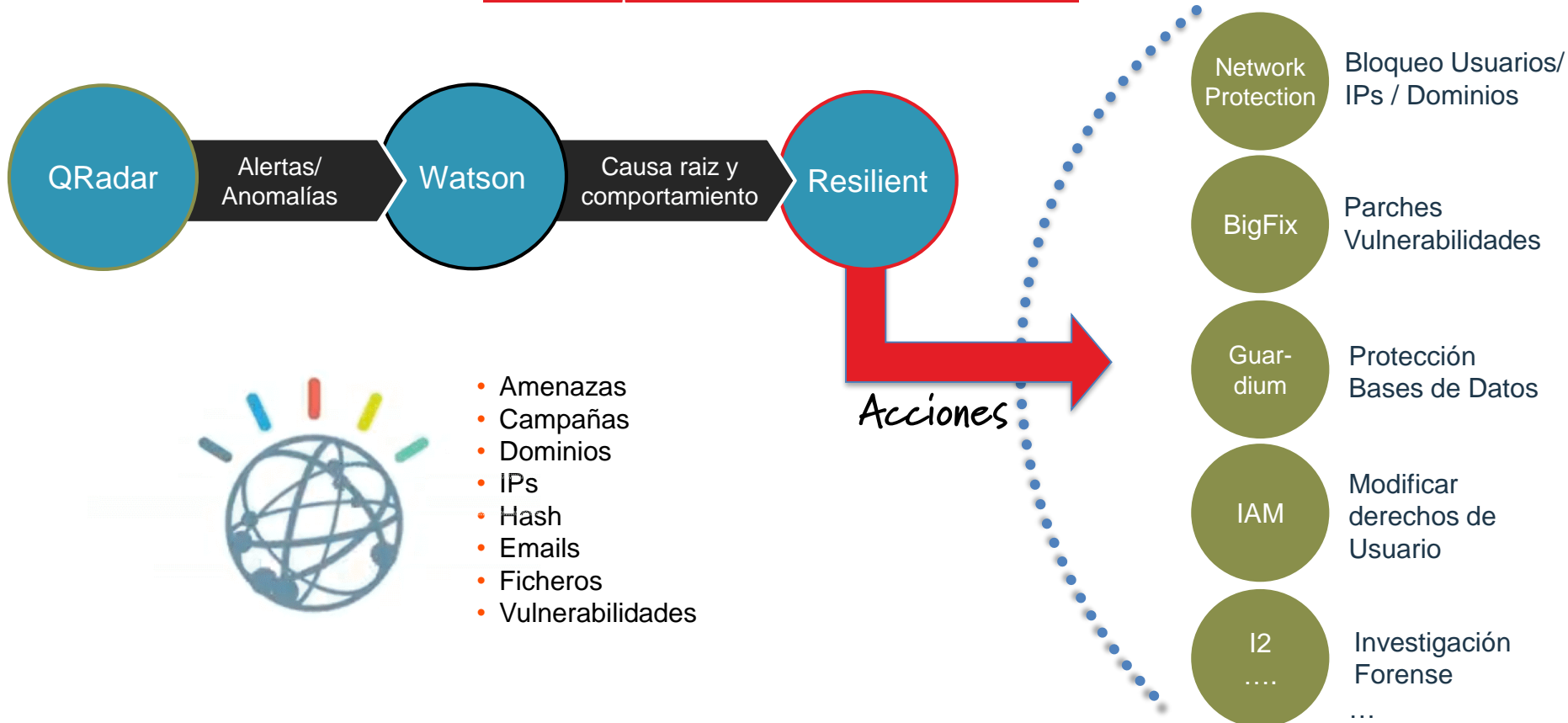
Human Generated Security Knowledge

- **Acelera** el triaje de incidentes con más automatización y profundidad en el análisis
- **Alivia** presión en el gap de habilidades de Seguridad
- **Reduce** el riesgo de perder el análisis de enlaces ya descubiertos previamente
- **Aumenta** la contribución de los equipos de seguridad

Watson for CyberSecurity



Respuesta End-to-End



Aproximación Seguridad Logicalis



Servicio de Adecuación a la GDPR

Análisis GAP

- Assessment Tecnológico
- Diagnóstico de la situación actual frente a marcos normativos en materia de seguridad

Medidas Tecnológicas

- Plan de Acción Tecnológico
- Análisis y definición de soluciones
- Implantación y adecuación tecnológica

Servicios Gestionados

- Soporte correctivo, preventivo y evolutivo
- Servicios Avanzados de Seguridad
- SOC

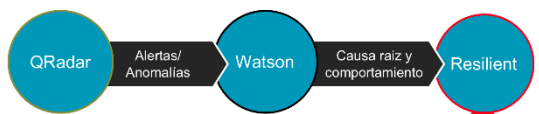
Data Protection

- Descubrimiento, clasificación, evaluación de vulnerabilidades, informes de accesos y permisos
- Cifrado, enmascaramiento
- Monitorización de la actividad de los datos y los ficheros (incl. usuarios privilegiados)
- Bloqueo dinámico de accesos, alertas y cuarentena
- Automatización del cumplimiento legal / normativo y auditoría



Retos GDPR

Respuesta End-to-End



- Amenazas
- Campañas
- Dominios
- IPs
- Hash
- Emails
- Ficheros
- Vulnerabilidades

Acciones

- Network Protection: Bloqueo Usuarios/ IPs / Dominios
- BigFix: Parches Vulnerabilidades
- Guardium: Protección Bases de Datos
- IAM: Modificar derechos de Usuario
- I2: Investigación Forense
- ...



Business and technology working as one

Próximos pasos ...

Gracias !!!

