LOGICALIS

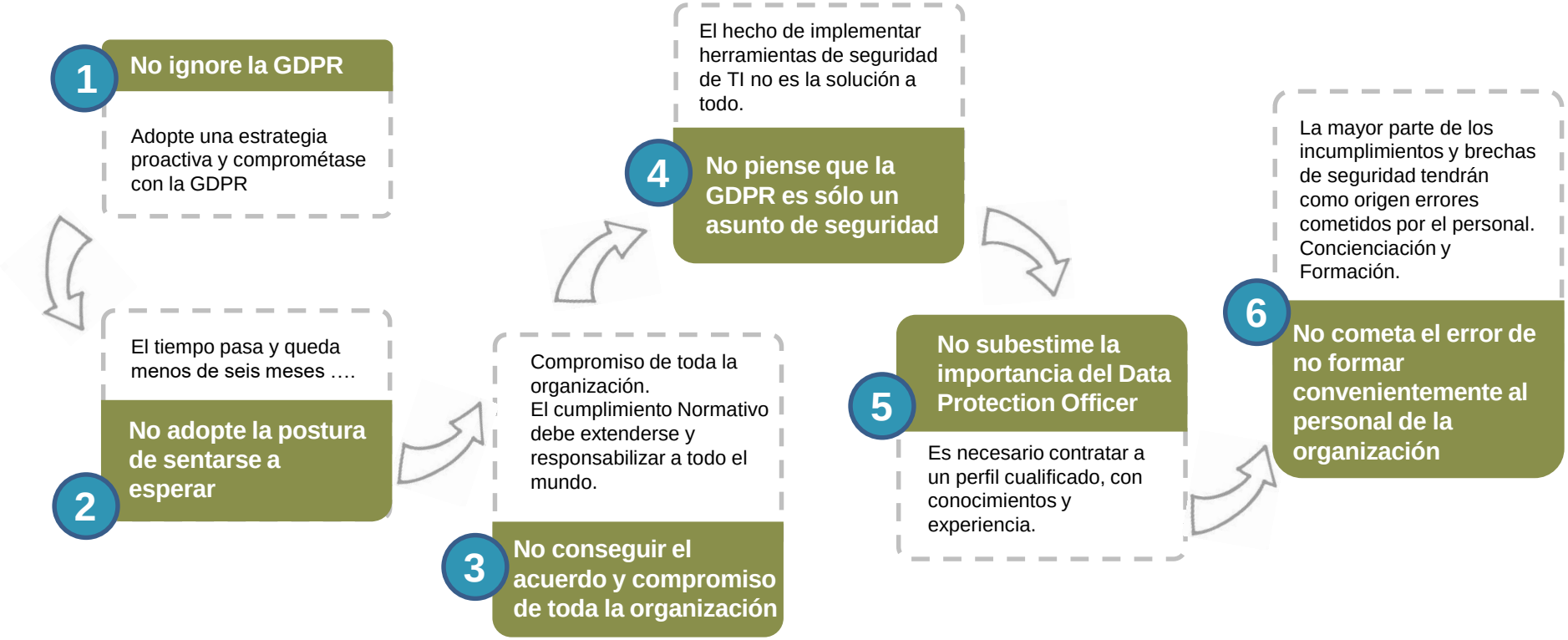
Business and technology working as one

BU Seguridad

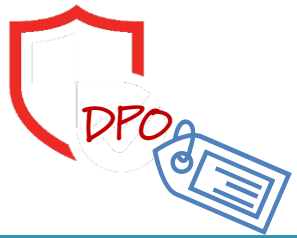
Retos GDPR

LOGICALIS Security

GDPR: Qué no debemos hacer



Aproximación Logicalis



Servicio de Adecuación a la GDPR

Análisis GAP

- Assessment Tecnológico

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

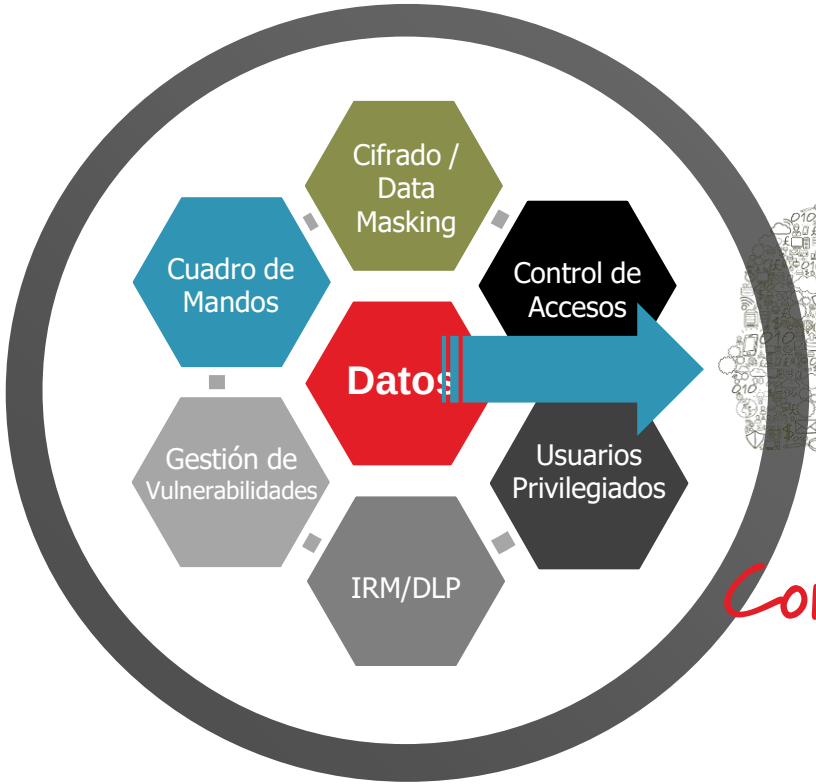
Medidas Tecnológicas

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

Servicios Gestionados

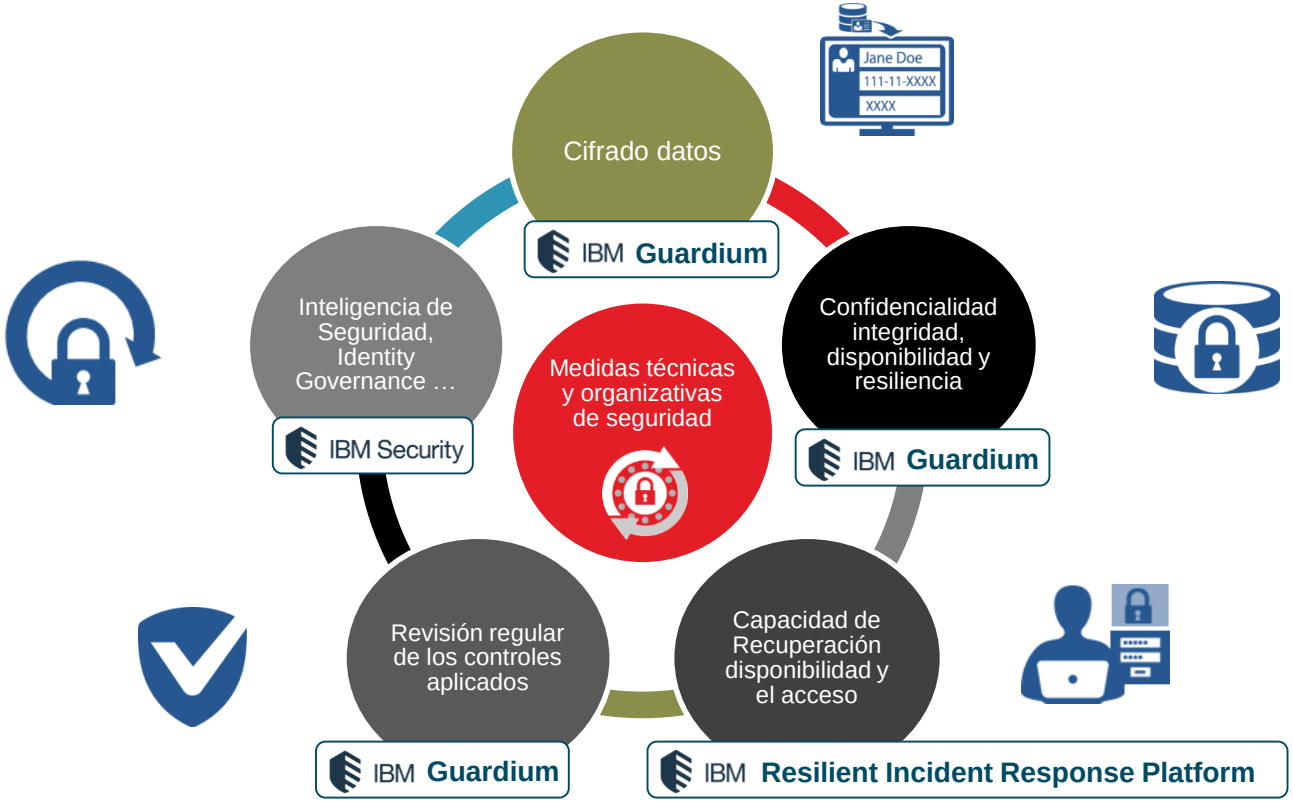
- Soporte correctivo, preventivo y evolutivo
- Servicios Avanzados de Seguridad
- SOC

Medidas Tecnológicas



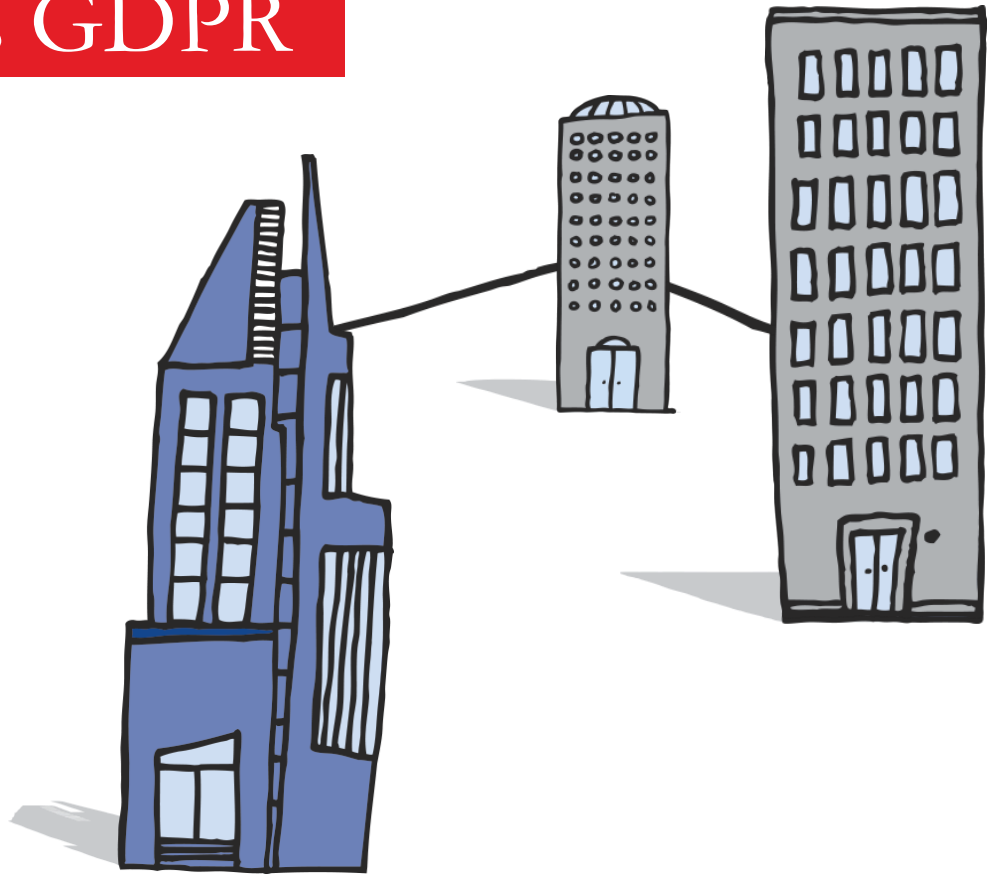
Concienciación

IBM Security GDPR Privacy

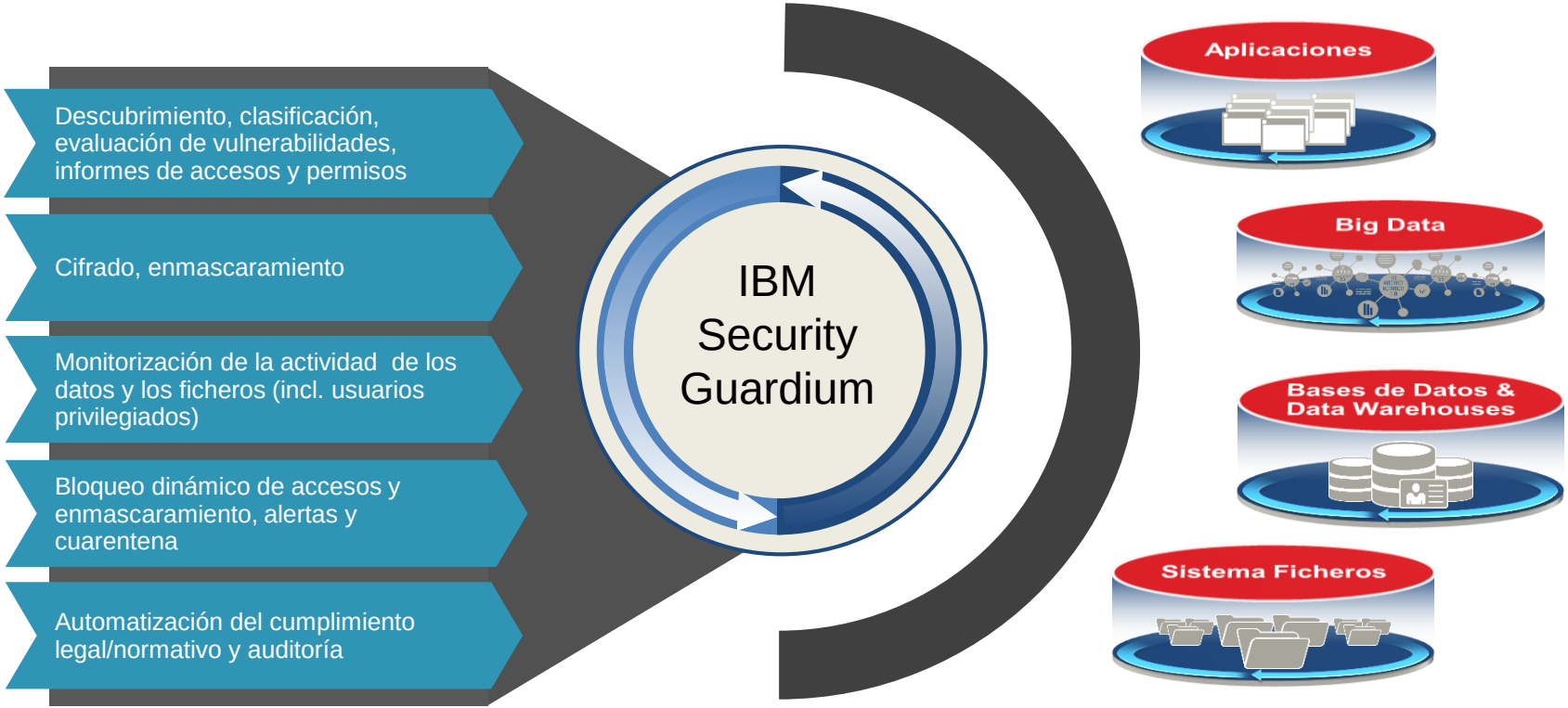


Soluciones GDPR

IBM



Data Protection



Data Protection. Ejemplos

Dónde están mis datos

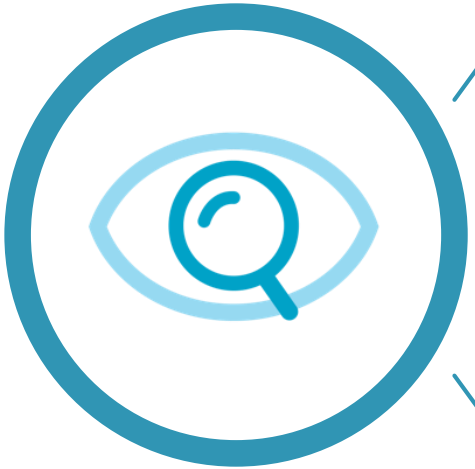
Escaneo de vulnerabilidades

Monitorización y Auditoría

Guardium GDPR Accelerator

Data Protection. Ejemplos (I)

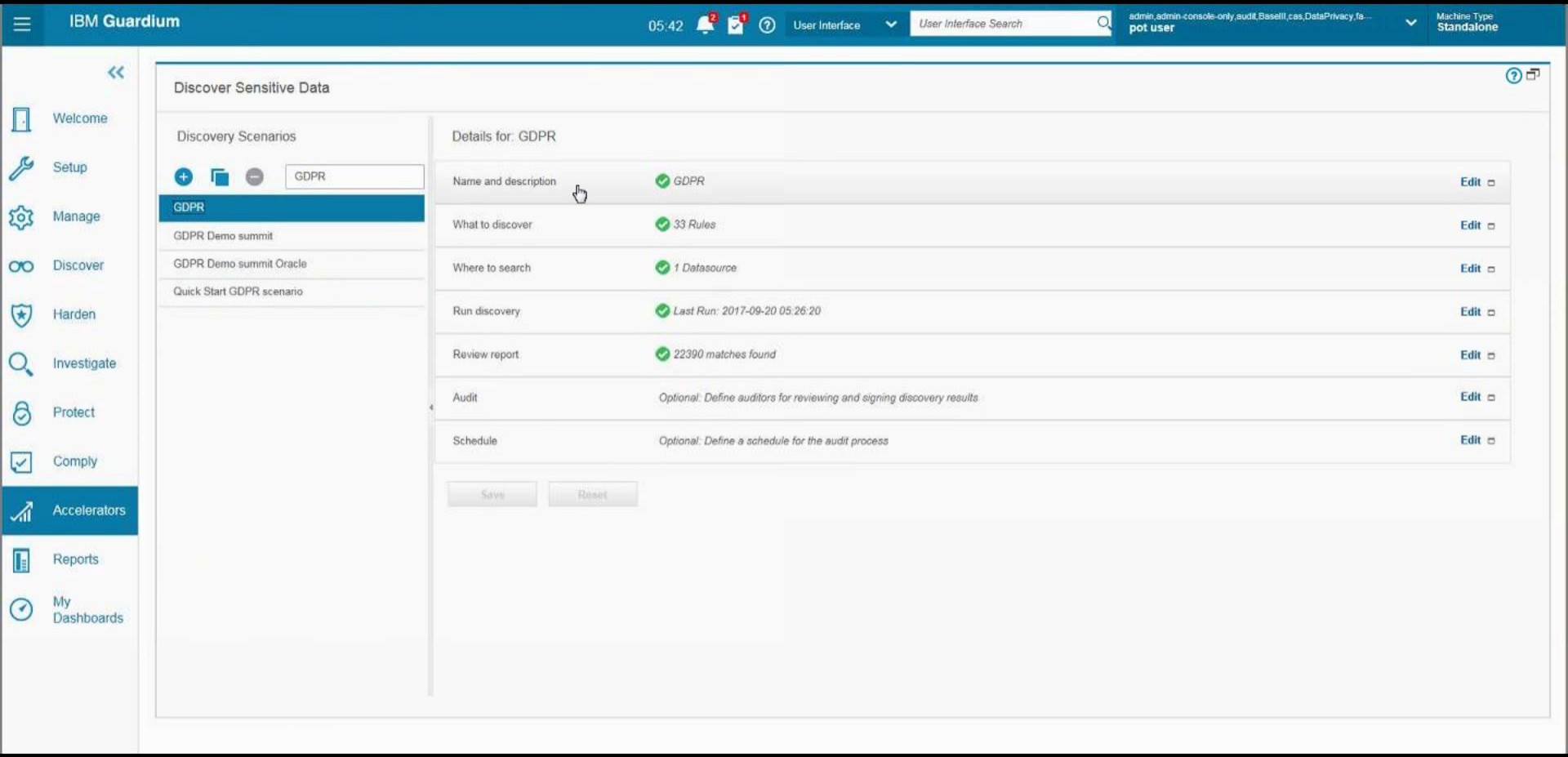
Dónde están mis datos



Soluciones al Desafío de Inventario

Descubrimiento de Activos de Base de Datos

Descubrimiento de Datos Sensibles


IBM Guardium
05:42
User Interface
User Interface Search
admin,admin-console-only,audit,BaseIII,cas,DataPrivacy,fa...
pot user
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Discover Sensitive Data
Discovery Scenarios
GDPR
GDPR
GDPR Demo summit
GDPR Demo summit Oracle
Quick Start GDPR scenario
Details for: GDPR
Name and description
GDPR
Edit
What to discover
33 Rules
Edit
Where to search
1 Datasource
Edit
Run discovery
Last Run: 2017-09-20 05:26:20
Edit
Review report
22390 matches found
Edit
Audit
Optional: Define auditors for reviewing and signing discovery results
Edit
Schedule
Optional: Define a schedule for the audit process
Edit
Save
Reset

Data Protection. Ejemplo (II)

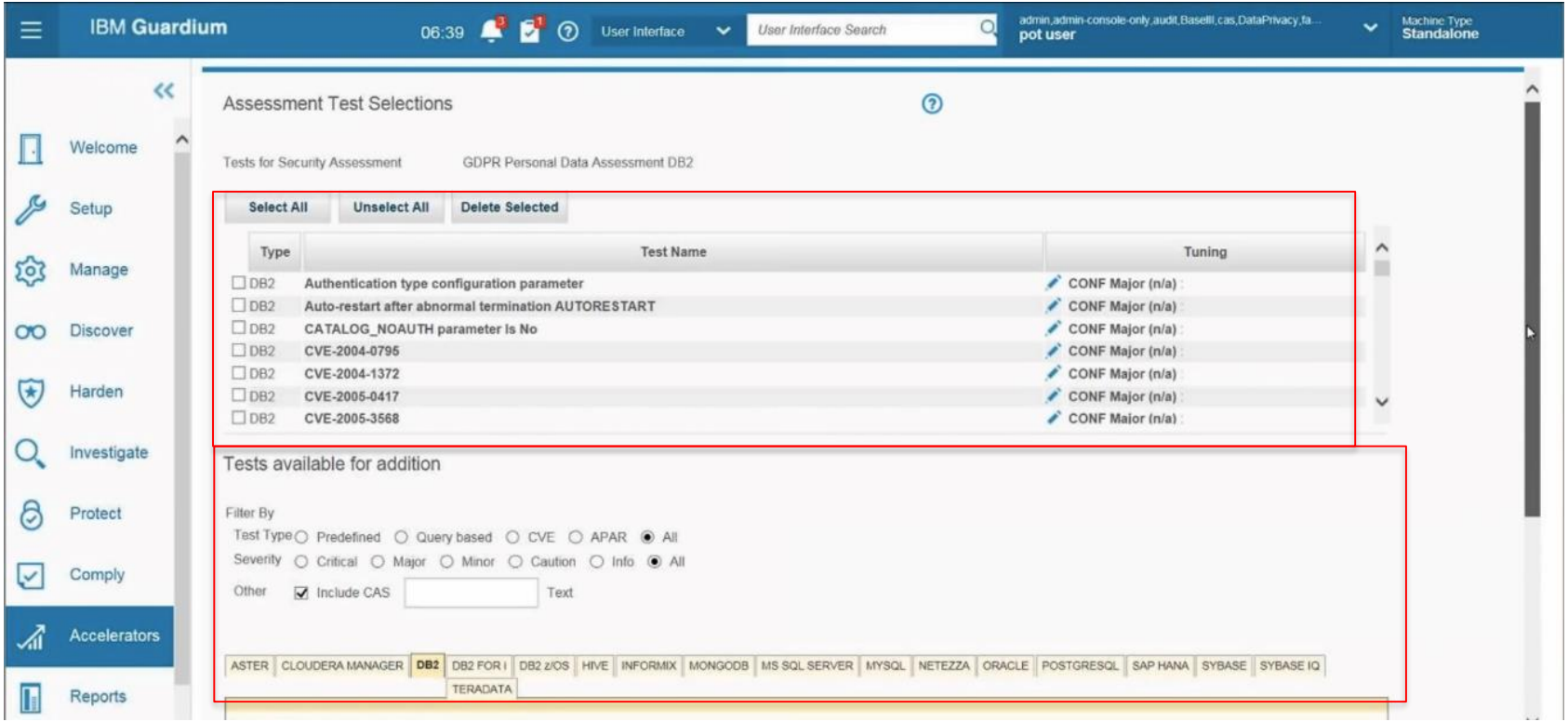
Escaneo de Vulnerabilidades

Plantillas de Escaneo por defecto

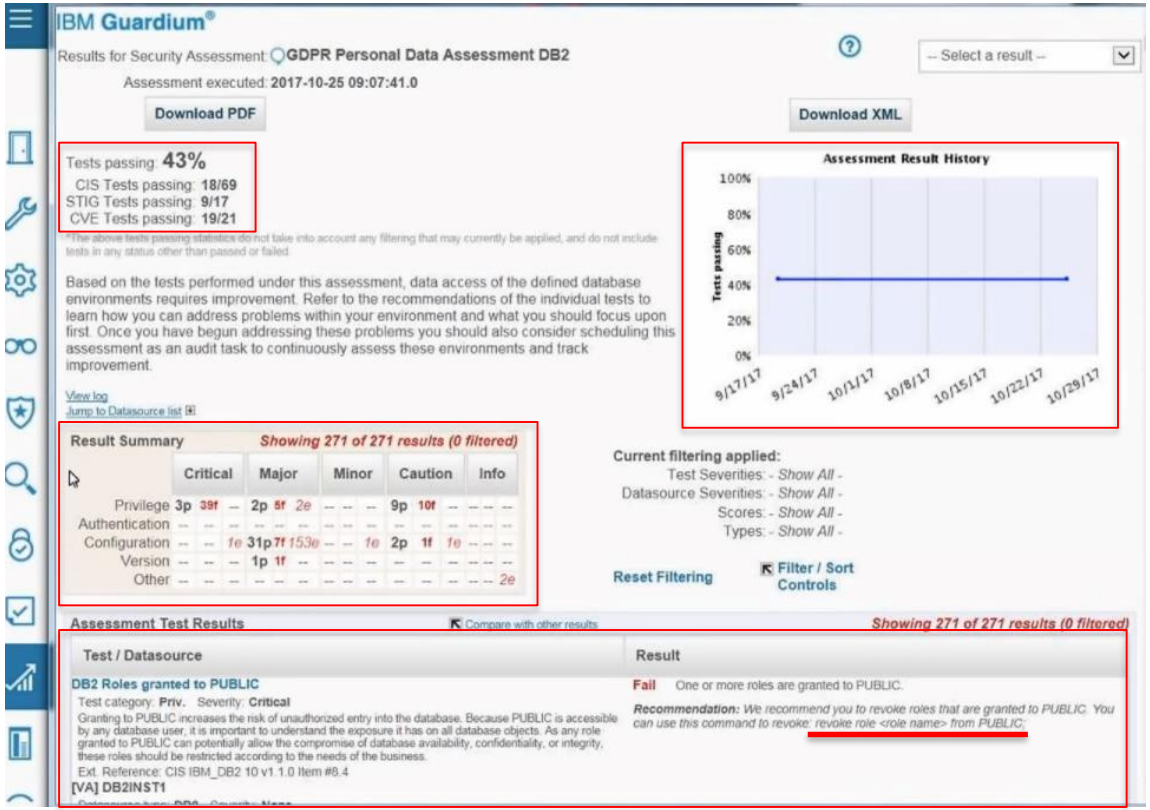
Múltiples tecnologías: DB2, AS400, Oracle, SQL, SAP HANA, Cloudera

Reporting y seguimiento para cumplimiento normativo

Data Protection. Ejemplo (II)



Data Protection. Ejemplo (II)



Data Protection. Ejemplos (III)

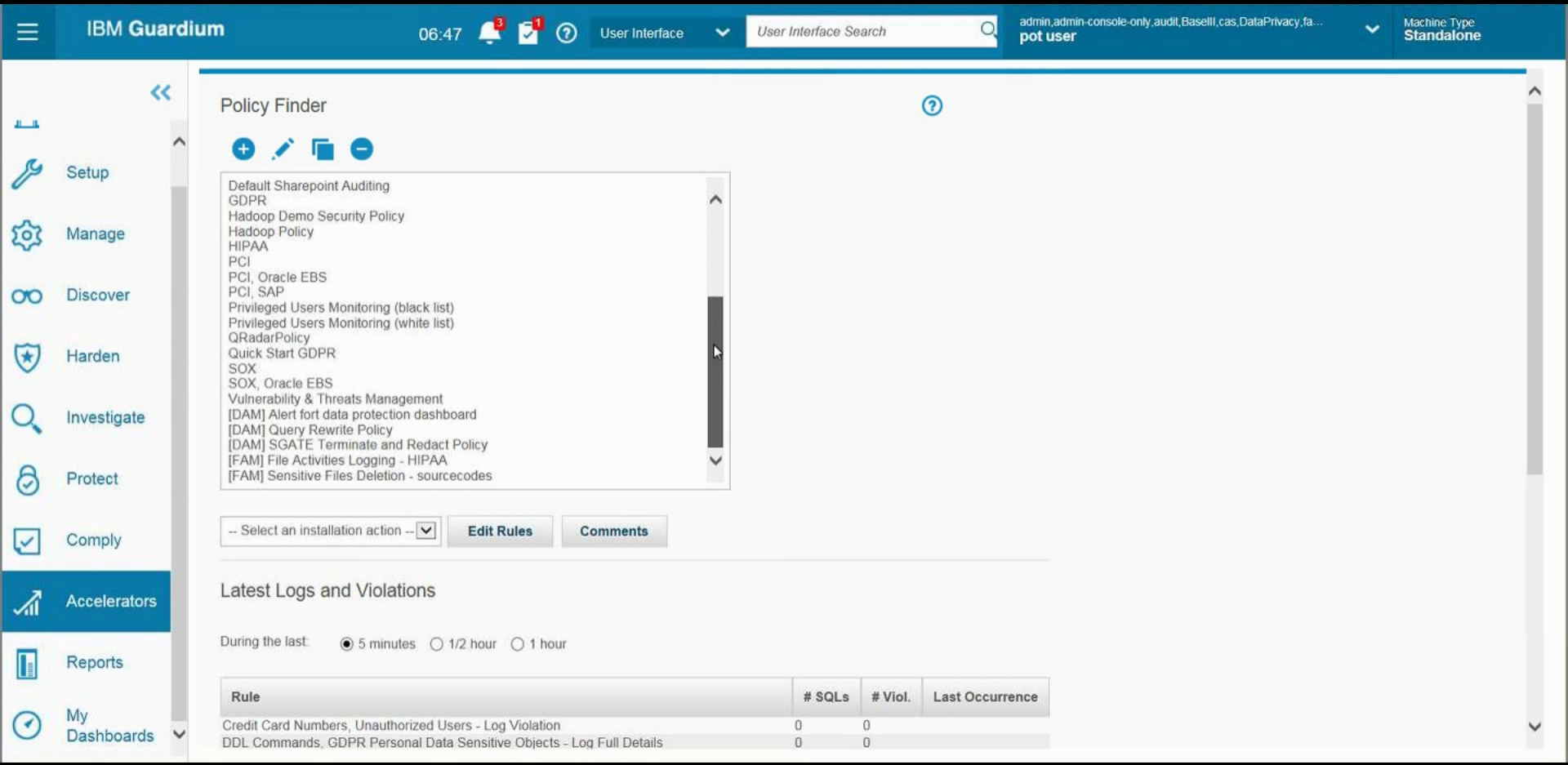
Monitorización y Auditoría

Caso de Uso: Data Breach

Políticas de Auditoría

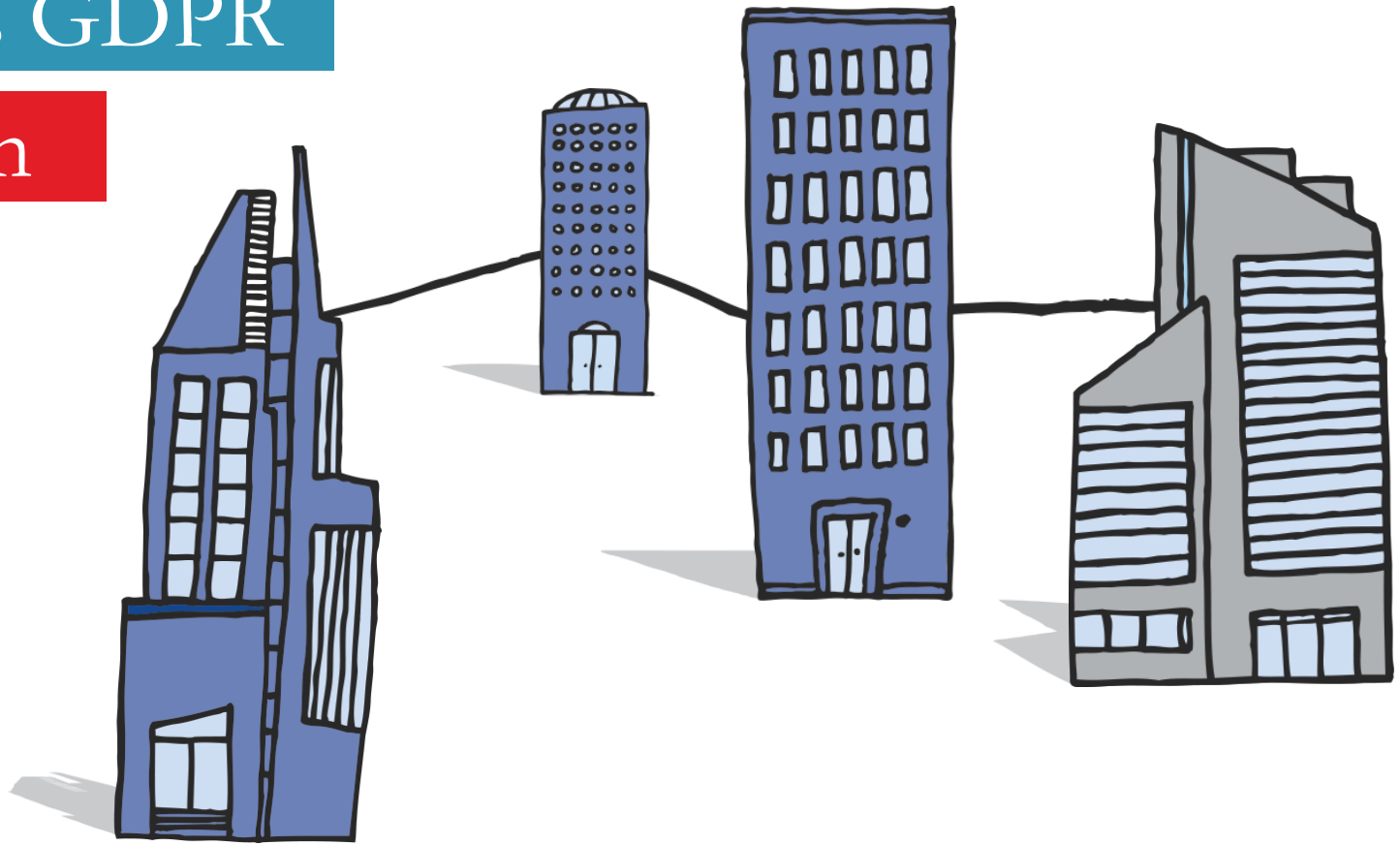
Análisis de actividad de usuarios en tiempo real

Violación de políticas. Enmascaramiento


IBM Guardium
06:47
User Interface
User Interface Search
admin,admin-console-only,audit,BaseIII,cas,DataPrivacy,fa...
pot user
Machine Type
Standalone
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Policy Finder
Default Sharepoint Auditing
GDPR
Hadoop Demo Security Policy
Hadoop Policy
HIPAA
PCI
PCI, Oracle EBS
PCI, SAP
Privileged Users Monitoring (black list)
Privileged Users Monitoring (white list)
QRadarPolicy
Quick Start GDPR
SOX
SOX, Oracle EBS
Vulnerability & Threats Management
[DAM] Alert fort data protection dashboard
[DAM] Query Rewrite Policy
[DAM] SGATE Terminate and Redact Policy
[FAM] File Activities Logging - HIPAA
[FAM] Sensitive Files Deletion - sourcecodes
-- Select an installation action --
Edit Rules
Comments
Latest Logs and Violations
During the last:
5 minutes
1/2 hour
1 hour
Rule
SQLs
Viol.
Last Occurrence
Credit Card Numbers, Unauthorized Users - Log Violation
0
0
DDL Commands, GDPR Personal Data Sensitive Objects - Log Full Details
0
0

Soluciones GDPR

Integración



Data Protection & SIEM (I)

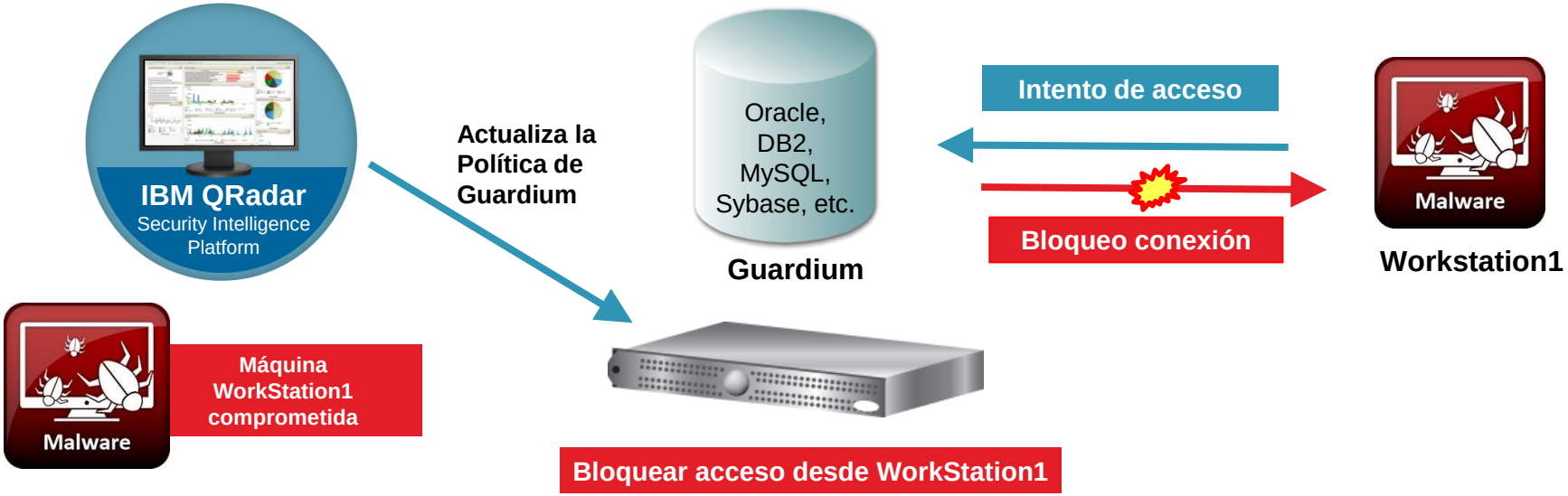
Es posible mantener las políticas de Guardium actualizadas en tiempo real y de forma automática en respuesta a eventos de seguridad de QRadar

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.*

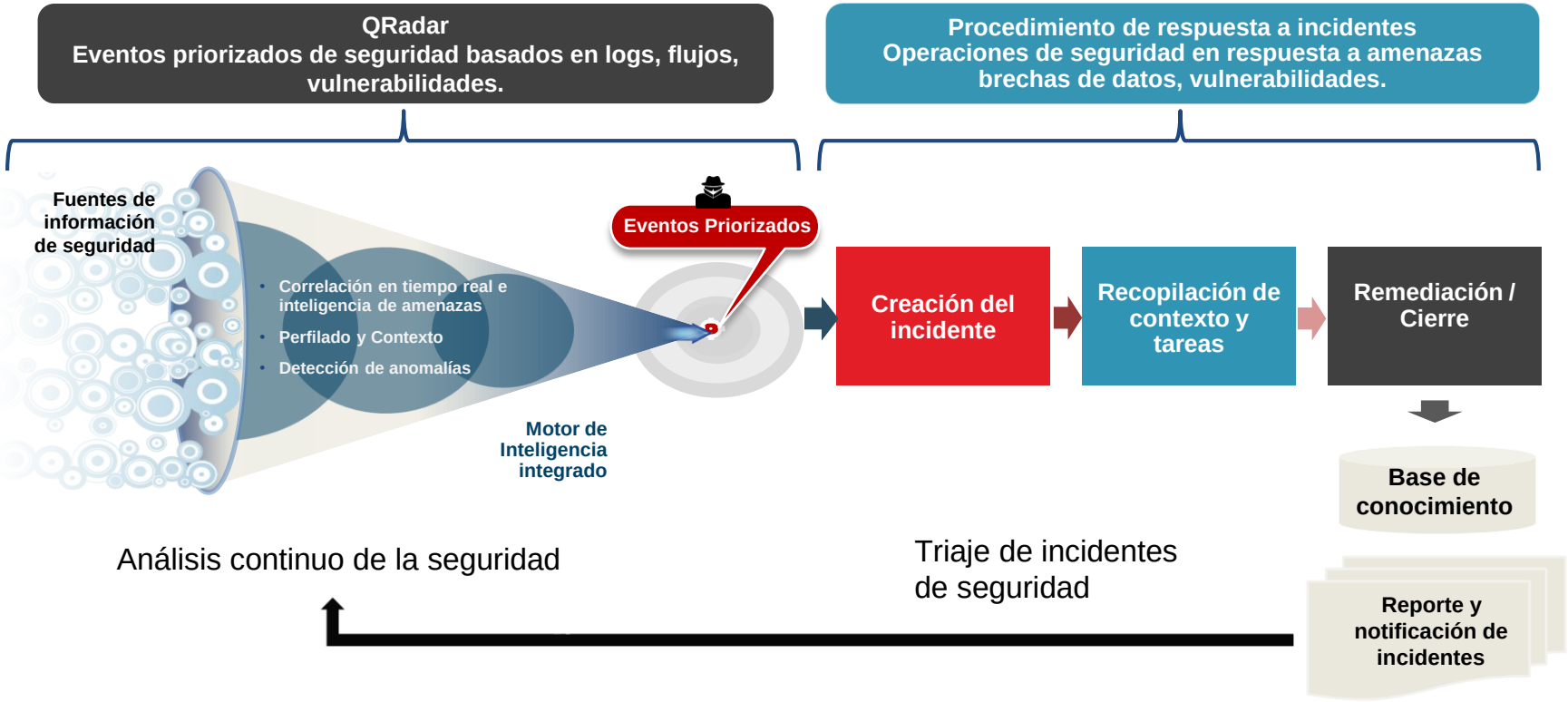
Reduce tiempos, mejora la orquestación, facilita la recolección de evidencias

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 hacia 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).

SIEM & Resilient



LOGICALIS
Business and technology working as one

Próximos pasos …

Gracias !!!

LOGICALIS Security