



**XIV
JORNADAS
STIC
CCN-CERT**

**NUEVOS RETOS,
MISMO COMPROMISO.**

#XIVJORNADASCNCERT

**Del control del dato hasta la
generación de inteligencia**



All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

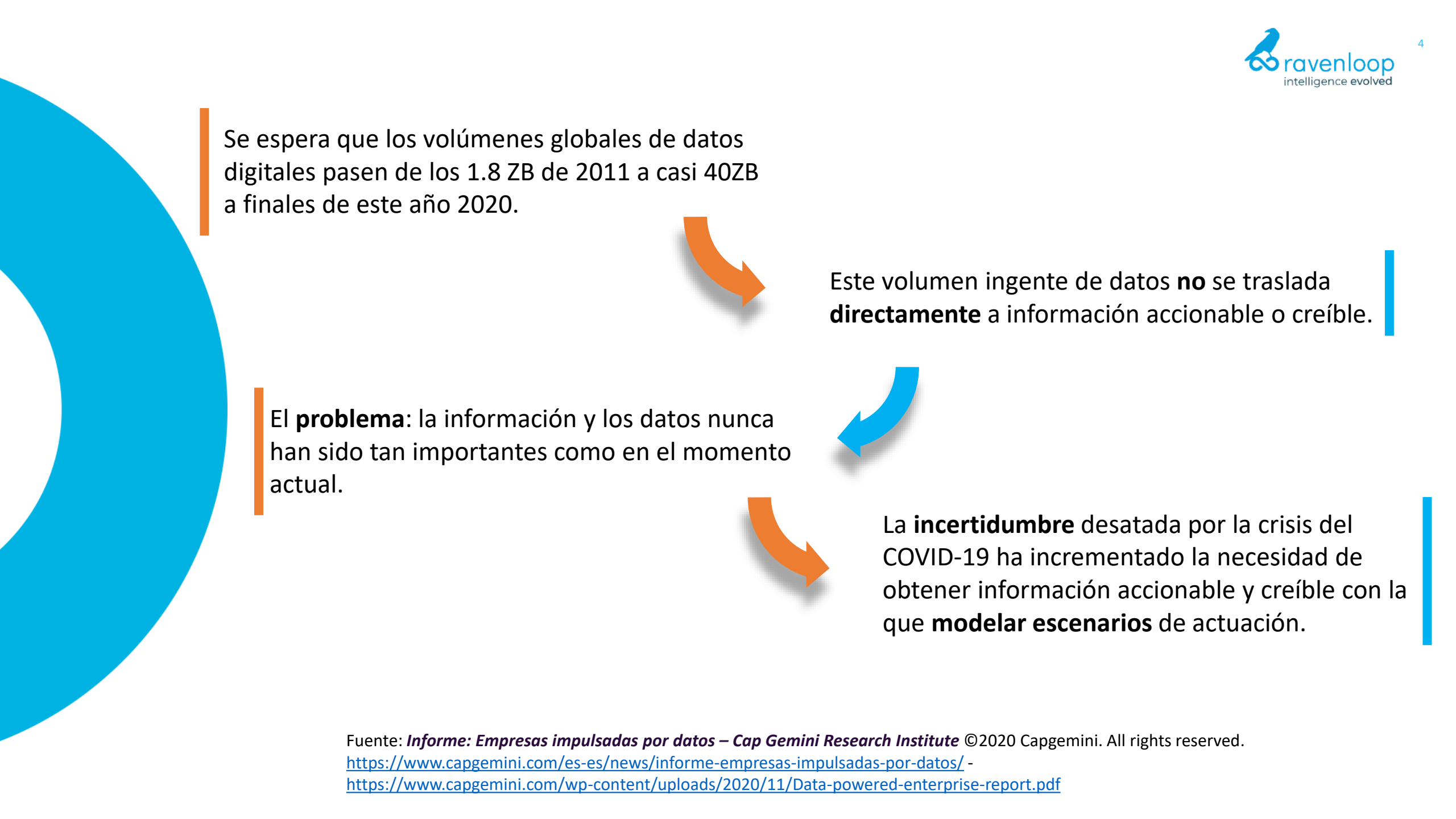
Third party logos are provided for information purposes only, and are property of their respective owners.

For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address contacto@seccion7.com

¿Están sus **datos** generando
valor?



¿Está su **información**
generando **inteligencia**?



Se espera que los volúmenes globales de datos digitales pasen de los 1.8 ZB de 2011 a casi 40ZB a finales de este año 2020.

Este volumen ingente de datos **no** se traslada **directamente** a información accionable o creíble.

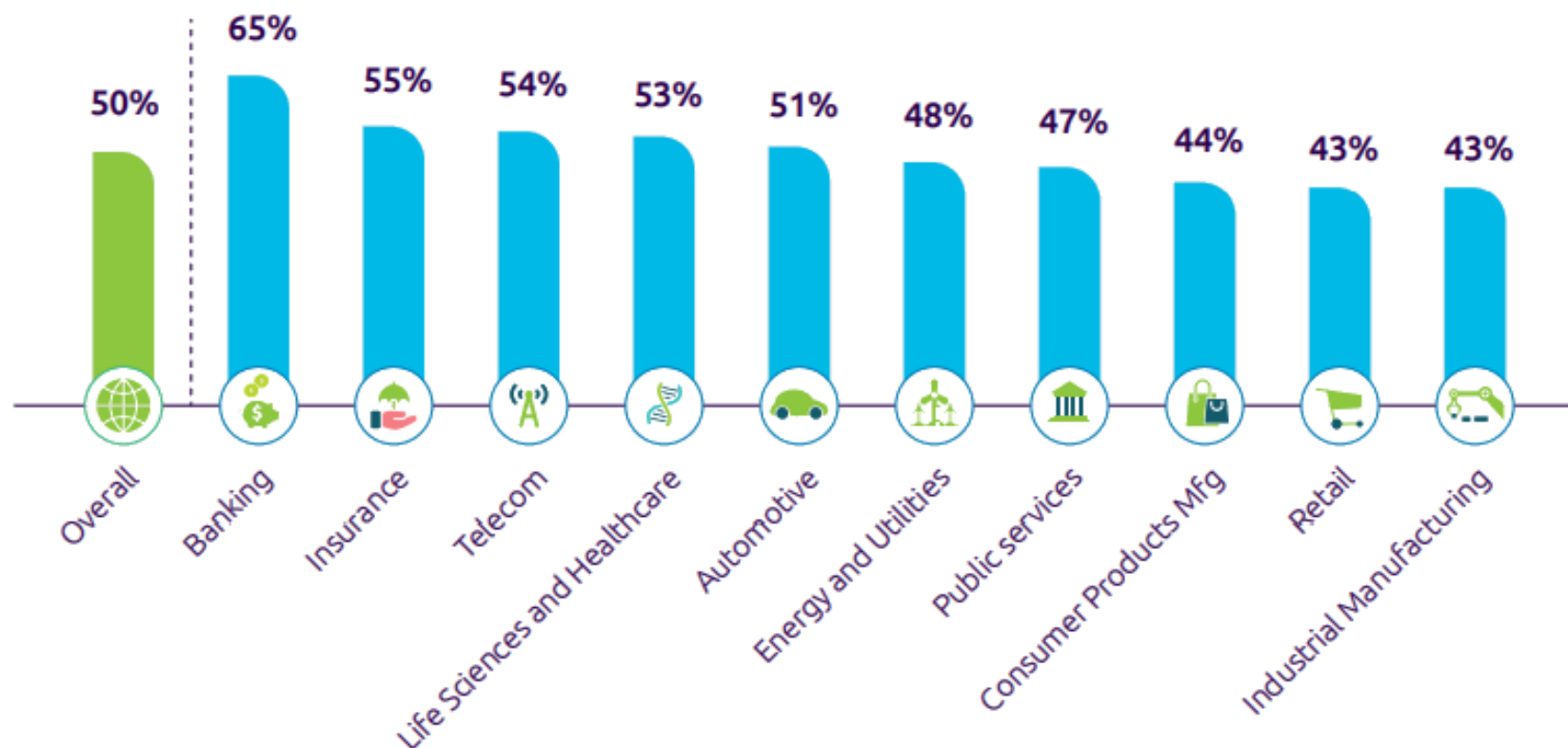
El **problema**: la información y los datos nunca han sido tan importantes como en el momento actual.

La **incertidumbre** desatada por la crisis del COVID-19 ha incrementado la necesidad de obtener información accionable y creíble con la que **modelar escenarios** de actuación.

Figure 4

Banking, insurance, and telecom sectors lead in data-driven decision making

Decision making in our organization is completely data-driven



Fuente: **Informe: Empresas impulsadas por datos – Cap Gemini Research Institute** ©2020 Capgemini. All rights reserved.

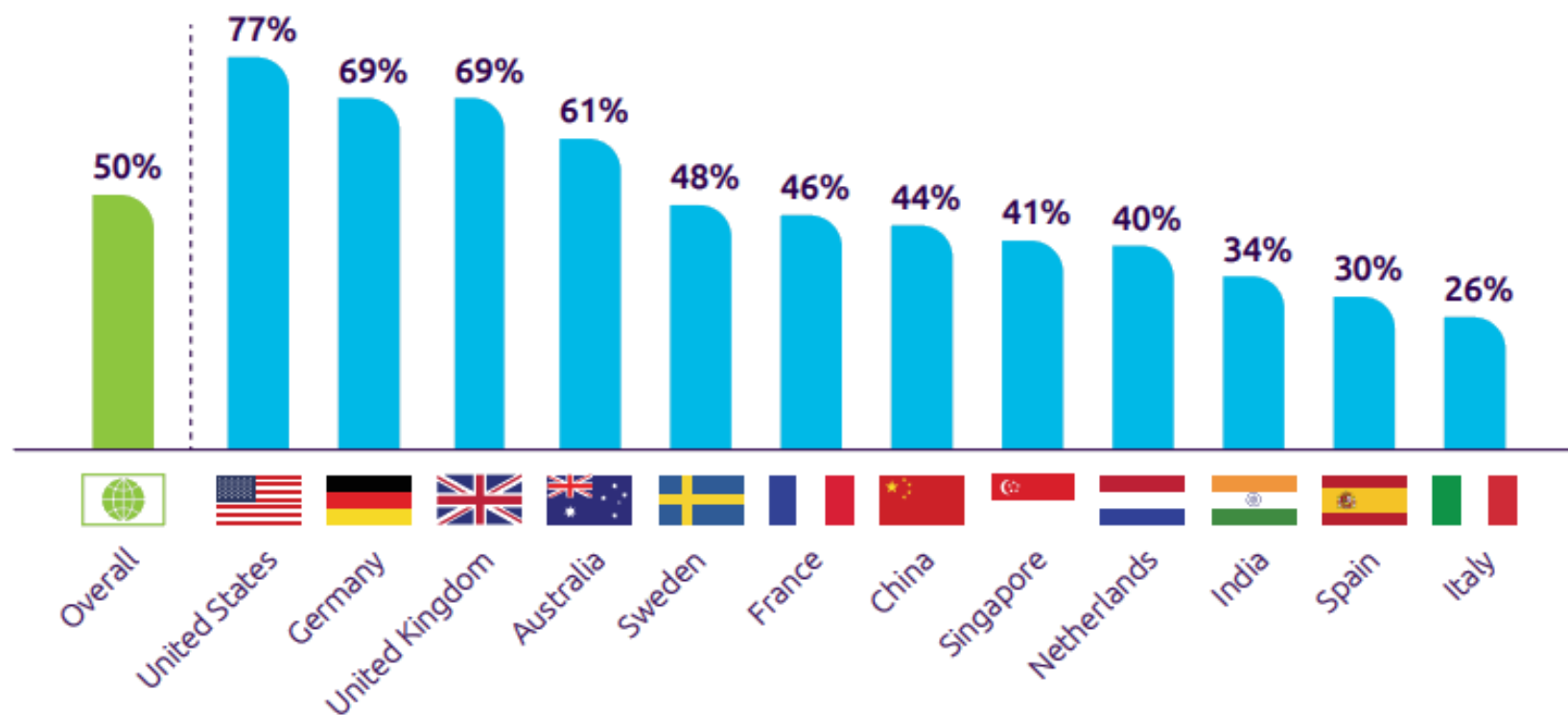
<https://www.capgemini.com/es-es/news/informe-empresas-impulsadas-por-datos/> -

<https://www.capgemini.com/wp-content/uploads/2020/11/Data-powered-enterprise-report.pdf>

Figure 5

US, Germany and UK top the charts in data-driven decision making

Decision making in our organization is completely data-driven

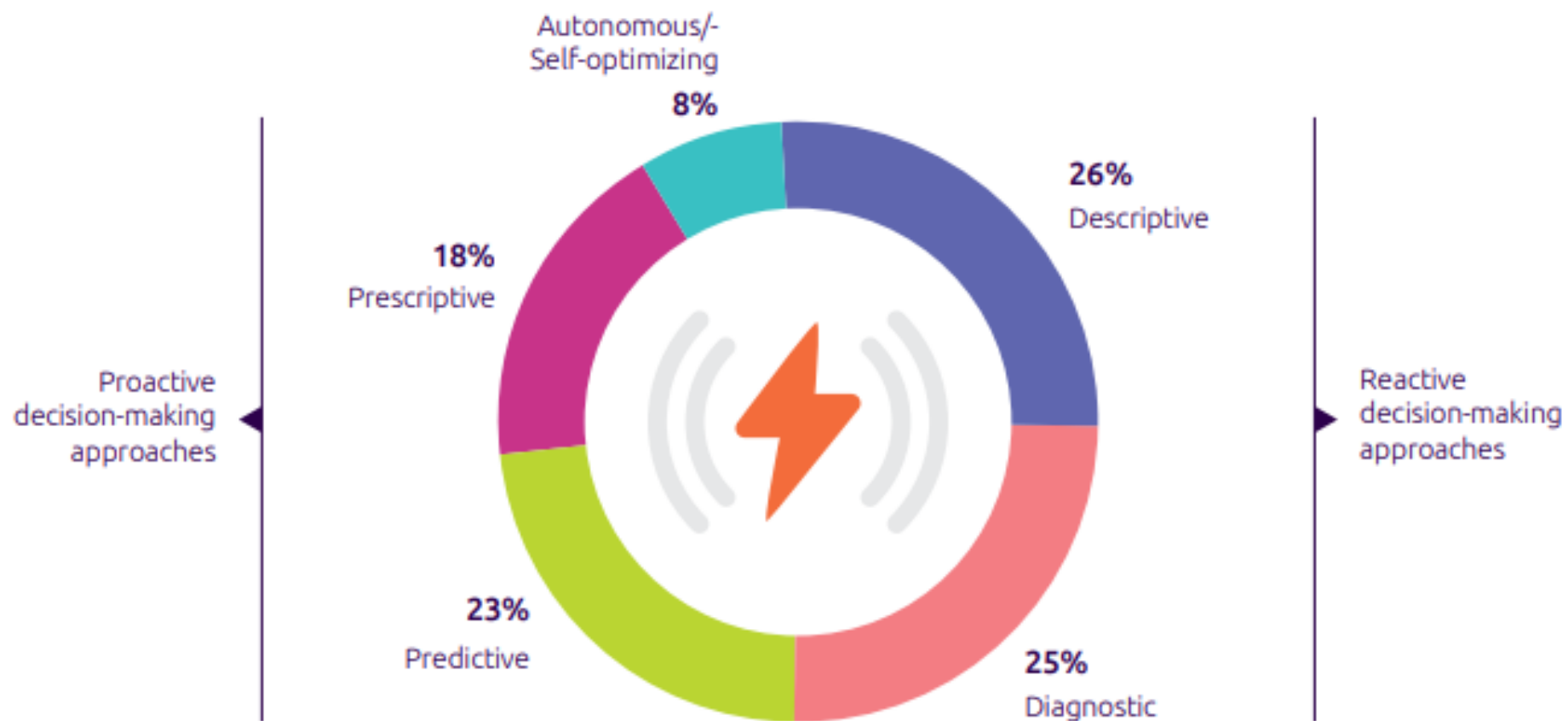


Fuente: **Informe: Empresas impulsadas por datos – Cap Gemini Research Institute** ©2020 Capgemini. All rights reserved.

<https://www.capgemini.com/es-es/news/informe-empresas-impulsadas-por-datos/> -

<https://www.capgemini.com/wp-content/uploads/2020/11/Data-powered-enterprise-report.pdf>

Figure 3 Majority of the decision-making in an organization remains reactive



Fuente: *Informe: Empresas impulsadas por datos – Cap Gemini Research Institute* ©2020 Capgemini. All rights reserved.

<https://www.capgemini.com/es-es/news/informe-empresas-impulsadas-por-datos/> -

<https://www.capgemini.com/wp-content/uploads/2020/11/Data-powered-enterprise-report.pdf>

Conclusiones

“[...] la proliferación de datos **no se traduce de forma directa en un incremento de la inteligencia organizacional generada.**

Cada vez más empresas dicen que están siendo impulsadas por datos, pero hemos descubierto que un número significativo de estas **no son capaces de crear planes o previsiones de futuro, monetizar estos datos o generar algún tipo de ventaja competitiva** avalada por esos crecientes volúmenes de información.”

Fuente: **Informe: Empresas impulsadas por datos – Cap Gemini Research Institute** ©2020 Capgemini. All rights reserved.

<https://www.capgemini.com/es-es/news/informe-empresas-impulsadas-por-datos/> -

<https://www.capgemini.com/wp-content/uploads/2020/11/Data-powered-enterprise-report.pdf>

Ciberinteligencia es no tener que decir **nunca**:

“Si lo hubiera sabido antes...”



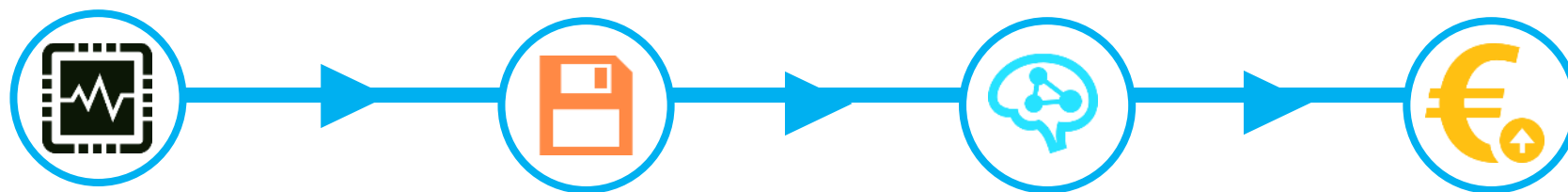


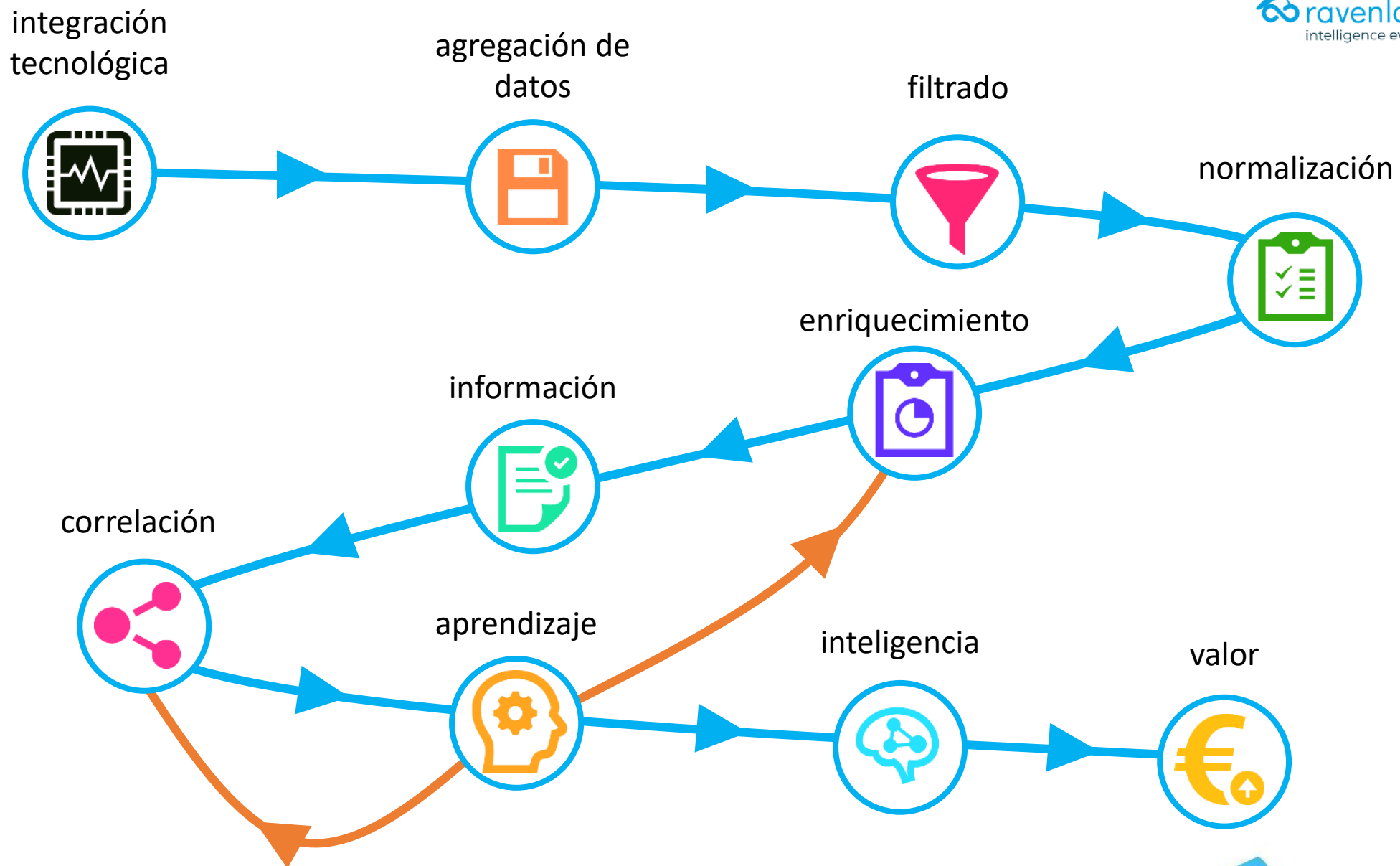
¿Cómo generamos
inteligencia organizacional
a partir de una
variedad heterogénea
de tecnologías de
análisis de malware y
eventos de seguridad?



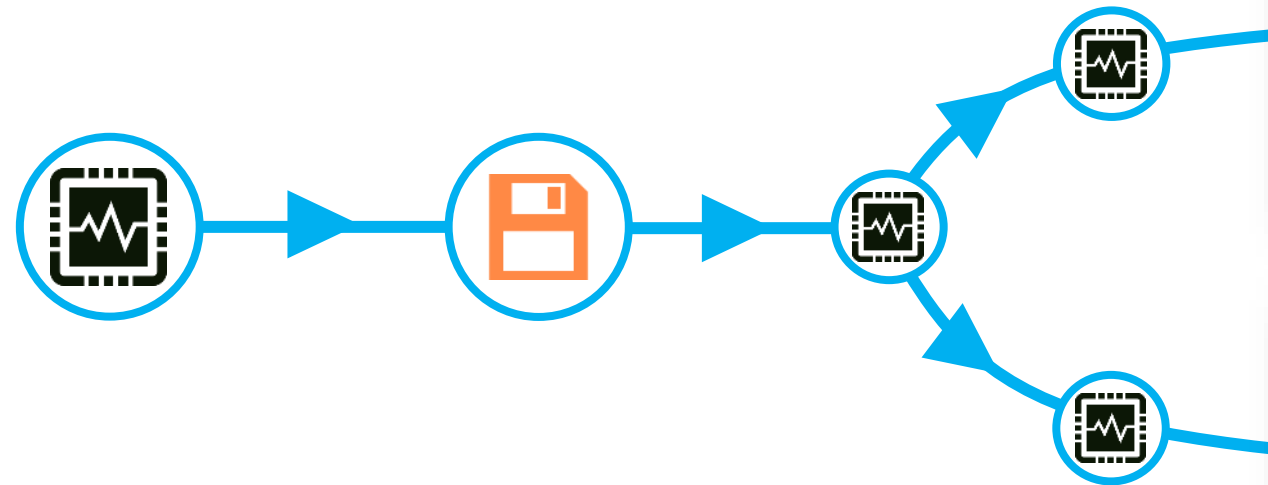
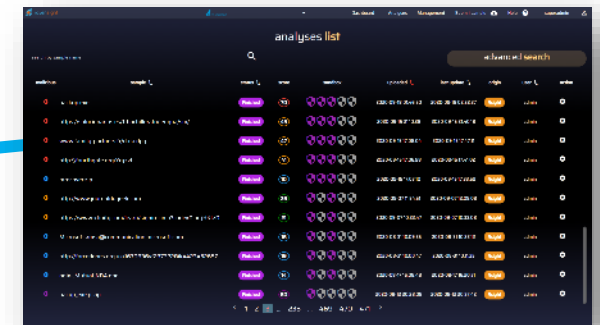
Del control del dato hasta la generación de inteligencia

Ravensight es una plataforma de **ciberinteligencia** diseñada desde cero para ayudarle a expresar y **obtener valor** de los datos generados por su **infraestructura de ciberseguridad**.





Los **datos** agregados de las diferentes **tecnologías** son enviados a los diferentes componentes de **Ravensight** para su procesamiento y análisis, donde muestras de malware son sometidas a un proceso de análisis **estático** y **dinámico** que utiliza el **100%** de su infraestructura.

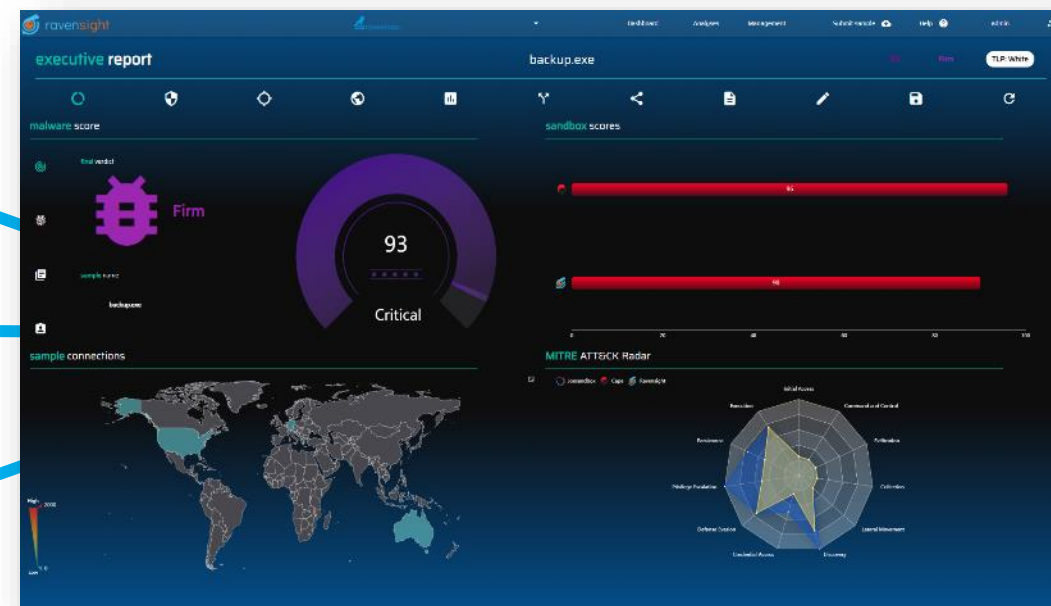
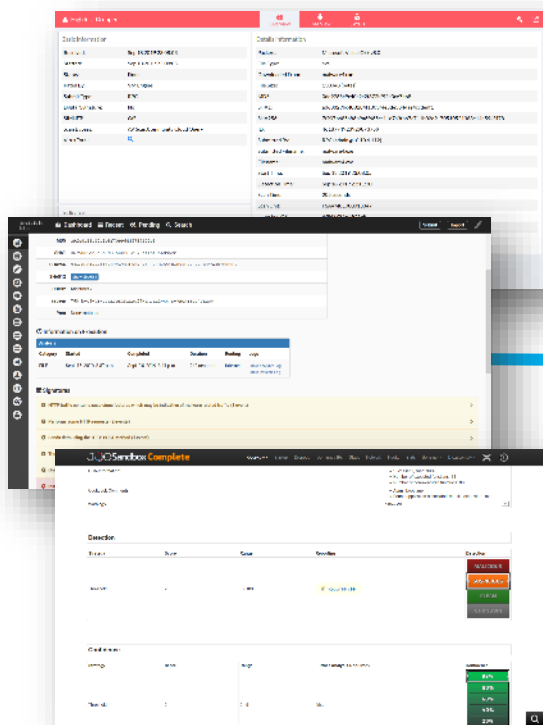



name	status	priority	progress	created	updated	owner	actions
Analysis 1	Running	High	100%	2023-10-10 10:00	2023-10-10 10:00	John Doe	Stop
Analysis 2	Completed	Medium	100%	2023-10-09 15:30	2023-10-09 15:30	Jane Smith	View
Analysis 3	Pending	Low	0%	2023-10-11 08:00	2023-10-11 08:00	John Doe	Start



name	status	priority	progress	created	updated	owner	actions
MultiAnalysis 1	Running	High	100%	2023-10-10 10:00	2023-10-10 10:00	John Doe	Stop
MultiAnalysis 2	Completed	Medium	100%	2023-10-09 15:30	2023-10-09 15:30	Jane Smith	View
MultiAnalysis 3	Pending	Low	0%	2023-10-11 08:00	2023-10-11 08:00	John Doe	Start

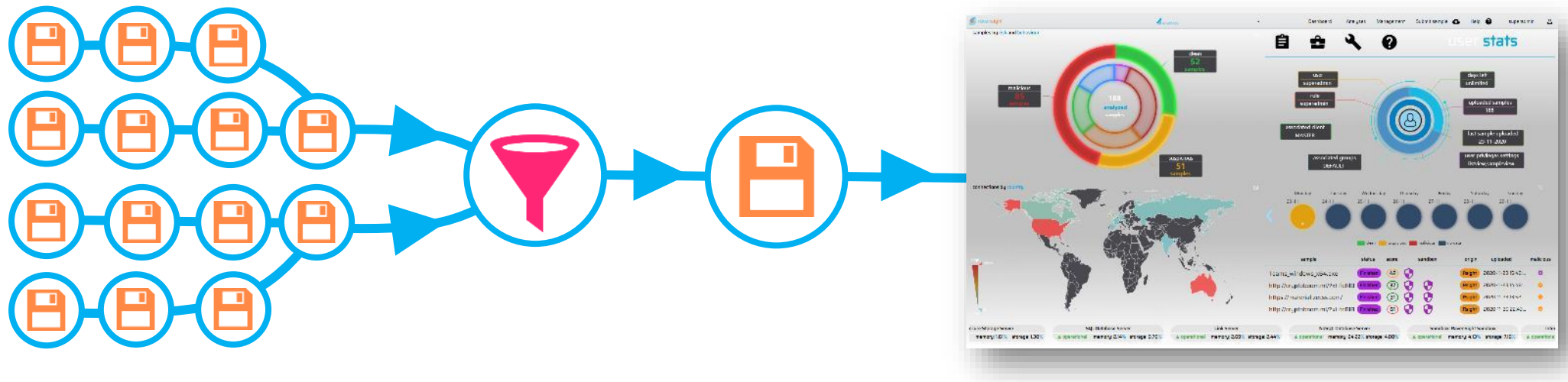
Ravensight simplifica el proceso de integración tecnológica y **agregación de datos** mediante el uso de una **única** interfaz **all-in-one** fácil de dominar.





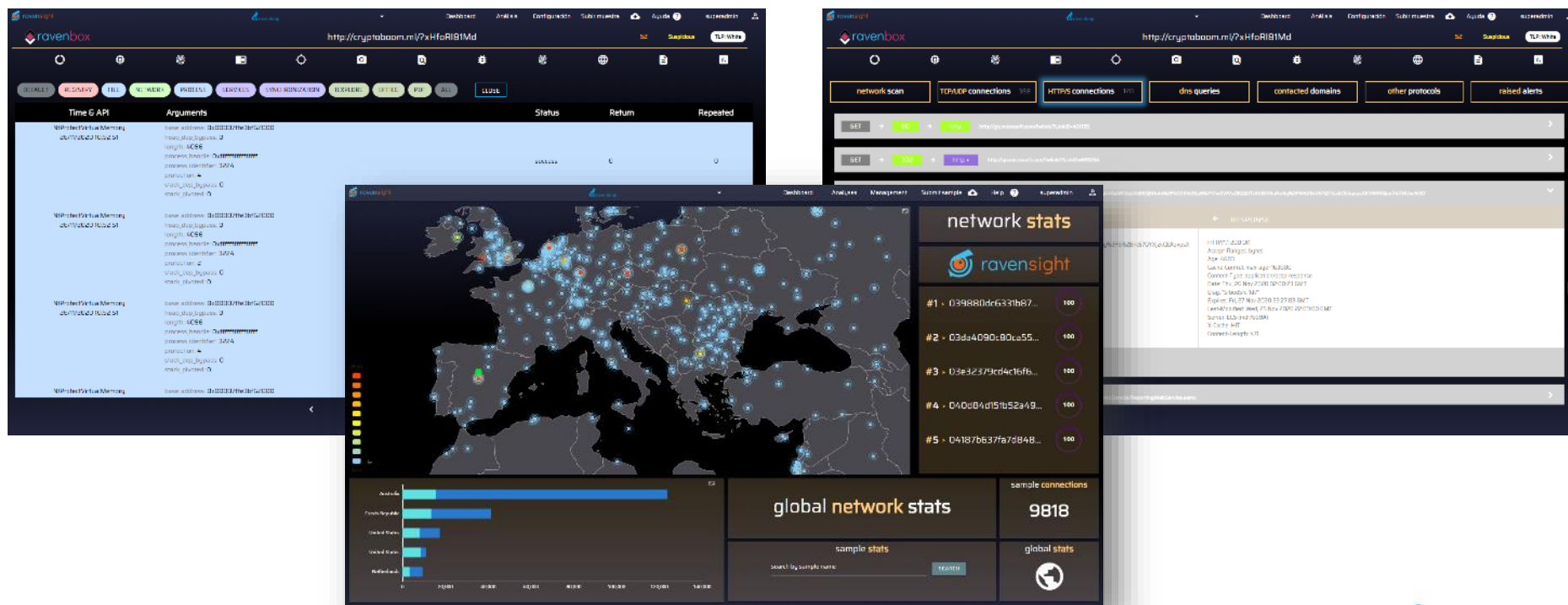
Esta **interfaz** ha sido **diseñada** desde **cero** para mejorar la **experiencia del usuario** y es completamente **independiente** de la **plataforma**: aprenda una vez, **acceda a todo**.

El volumen de **ingesta de datos** requiere encontrar un **compromiso** cuidadosamente medido entre **cantidad** y **calidad**.

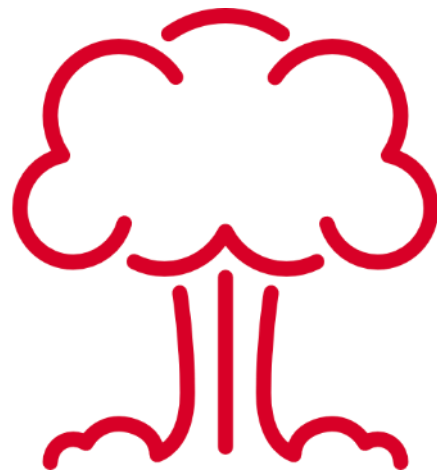


Ravensight automatiza y simplifica el filtrado, recopilando solo aquellos datos significativos que producen información de calidad.

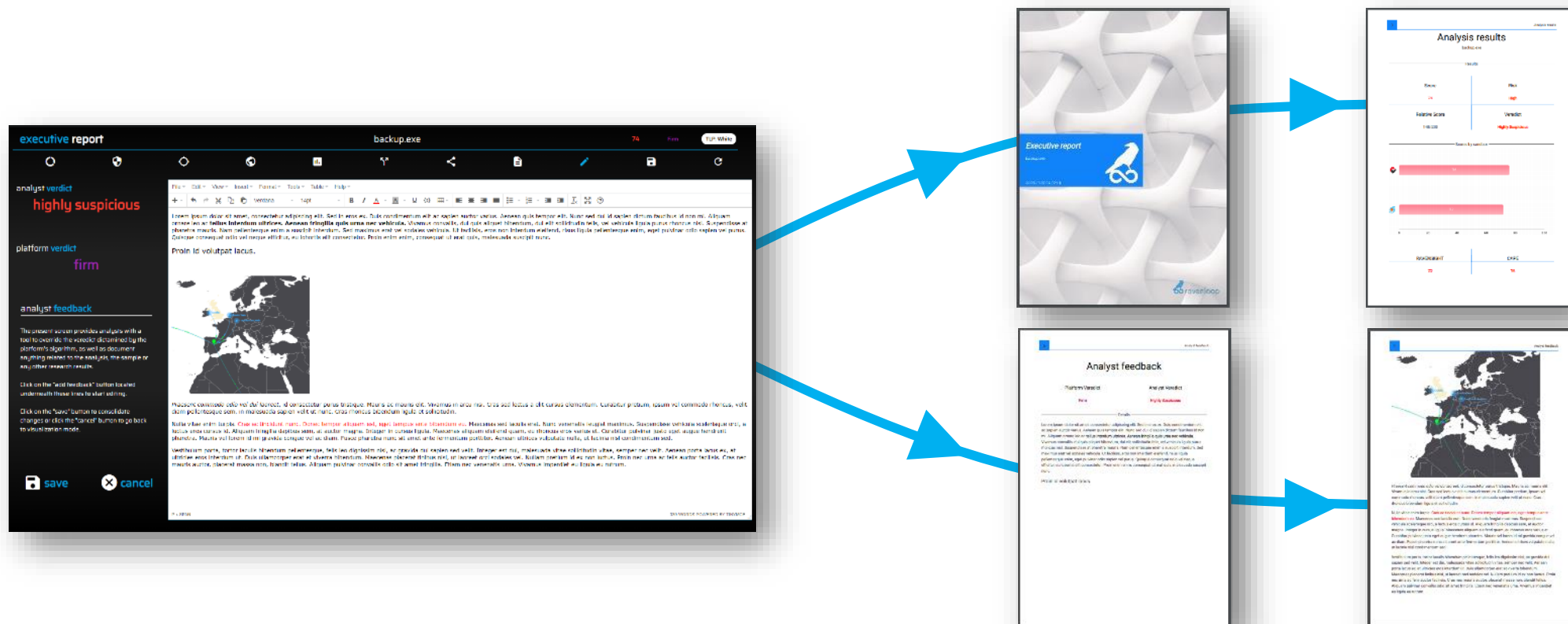
Los **datos** de todas las soluciones integradas se **normalizan**, agregan y representan de la manera **más útil** para que **los analistas, los equipos SOC y el personal no técnico** pueda consumirla.

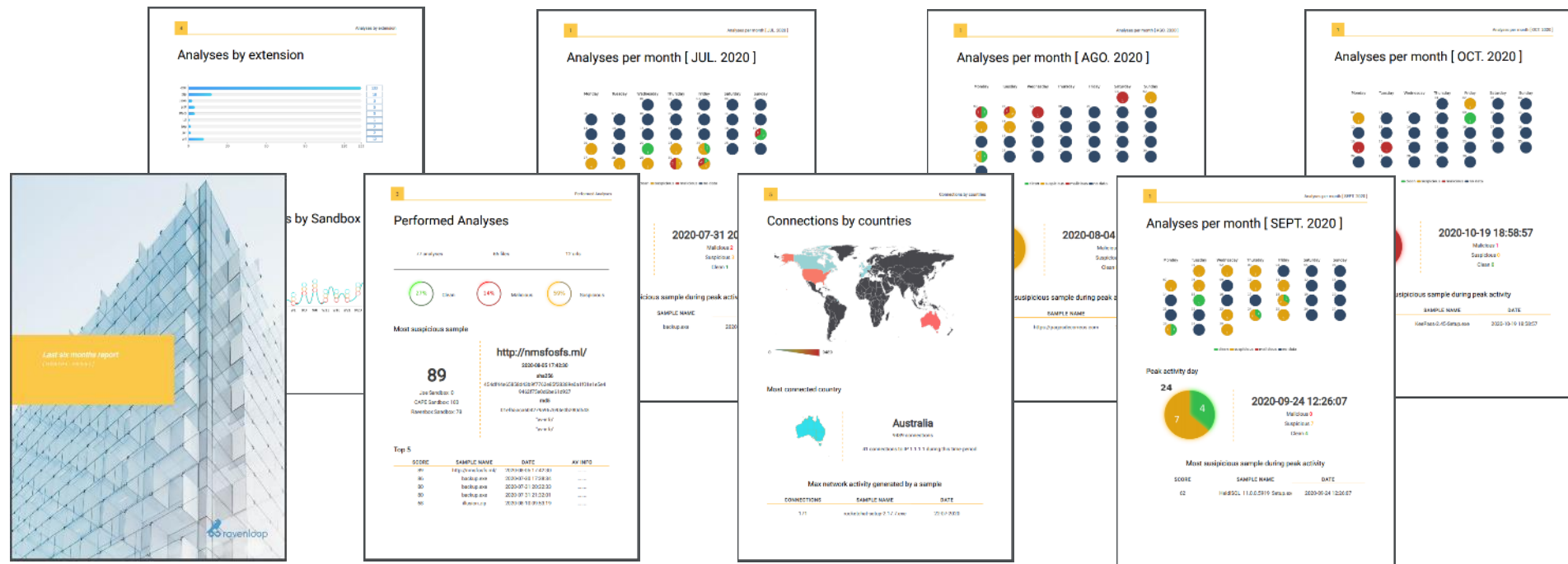


Sus datos permanecerán **disponibles**
en **Ravensight** incluso si los
proveedores de tecnología
integrados **desaparecen.**



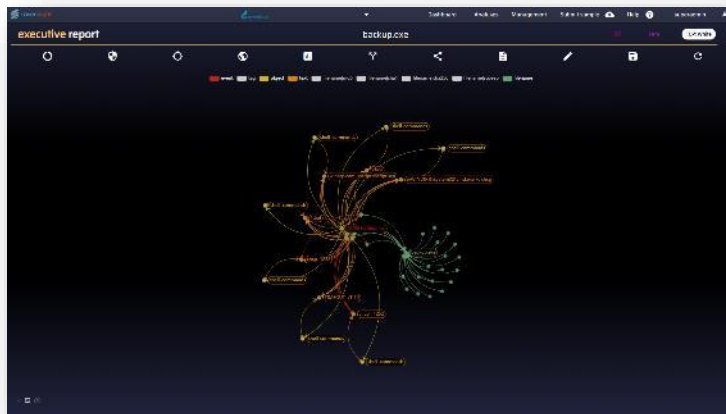
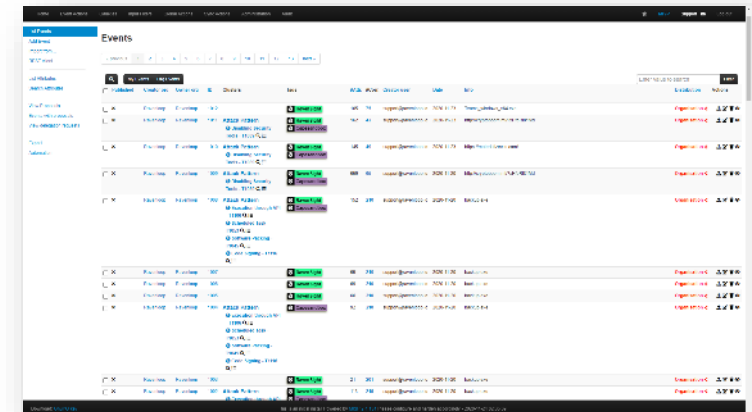
La **información** generada no solo se **enriquece** mediante algoritmos de búsqueda y **agregación**: los propios usuarios pueden añadir **feedback** e incluso generar **informes** completos.





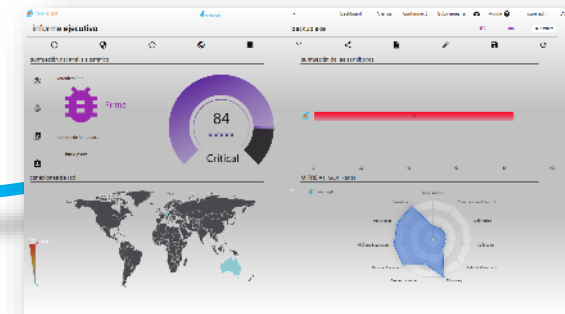
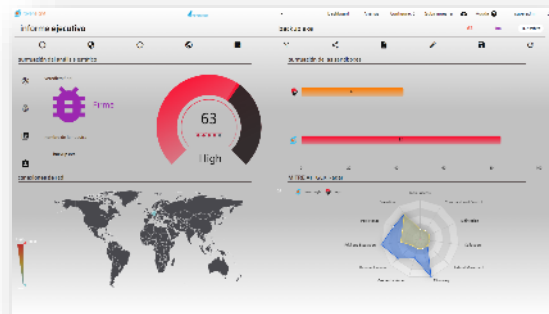
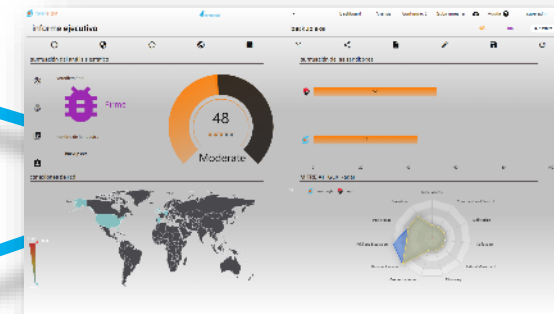
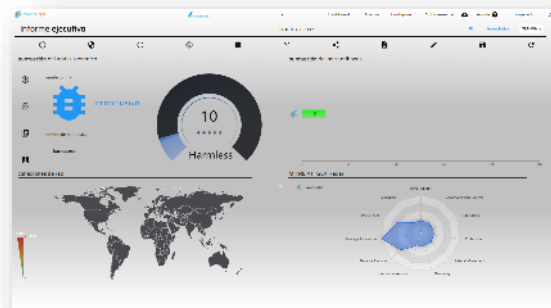
Una vez enriquecidos, los datos normalizados se convierten en información para el **personal de seguridad**, que consigue que su trabajo sea **reconocido** y sea **útil desde el primer minuto**.

Además del motor de **correlación interno**, **Ravensight** permite exportar la inteligencia **generada** a plataformas de correlación de inteligencia como **MISP**.

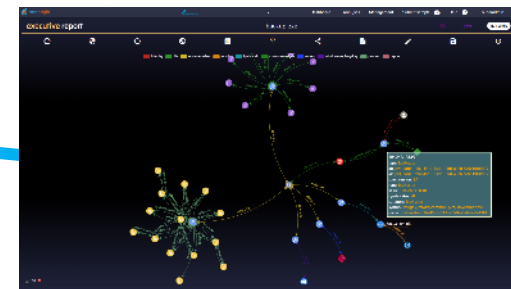
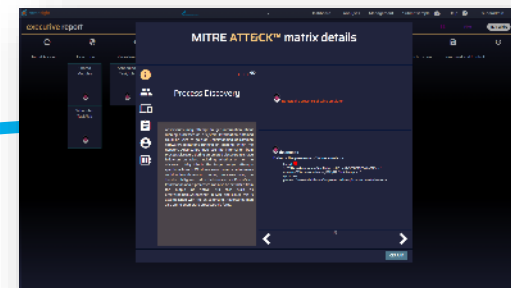
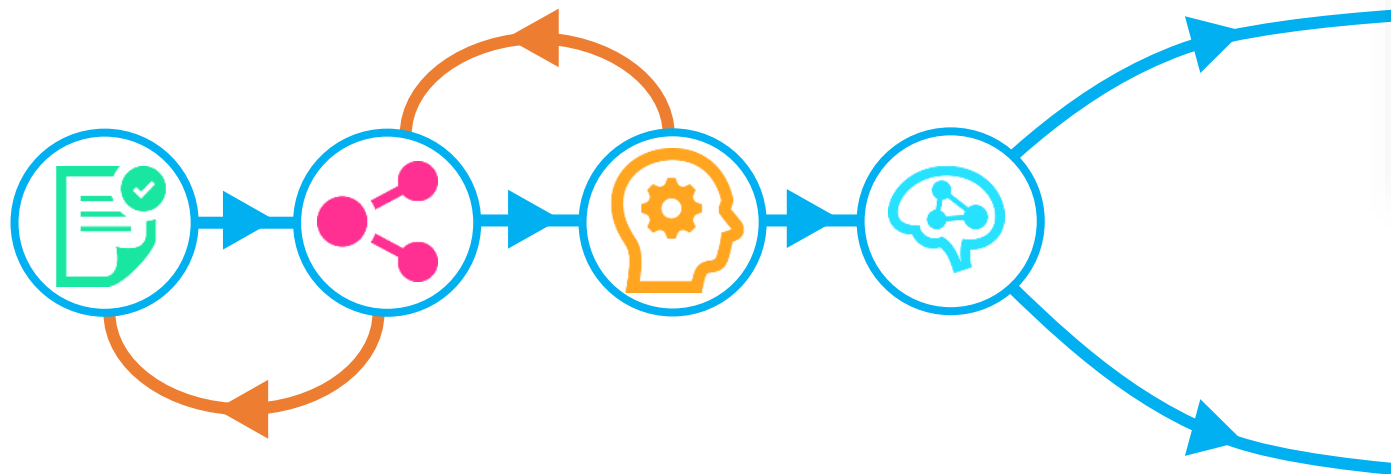

MISP
Threat Sharing

Event ID	Name	Type	Severity	Source	Destination	Tags	Score
1	Example event 1	Malware	High	Example source	Example destination	Example tags	2.5
2	Example event 2	Malware	High	Example source	Example destination	Example tags	2.5
3	Example event 3	Malware	High	Example source	Example destination	Example tags	2.5
4	Example event 4	Malware	High	Example source	Example destination	Example tags	2.5
5	Example event 5	Malware	High	Example source	Example destination	Example tags	2.5
6	Example event 6	Malware	High	Example source	Example destination	Example tags	2.5
7	Example event 7	Malware	High	Example source	Example destination	Example tags	2.5
8	Example event 8	Malware	High	Example source	Example destination	Example tags	2.5
9	Example event 9	Malware	High	Example source	Example destination	Example tags	2.5
10	Example event 10	Malware	High	Example source	Example destination	Example tags	2.5

Los algoritmos de **aprendizaje** detectan patrones **heurísticos** y enriquecen el proceso de **correlación**, aumentando su **precisión** de forma evolutiva.

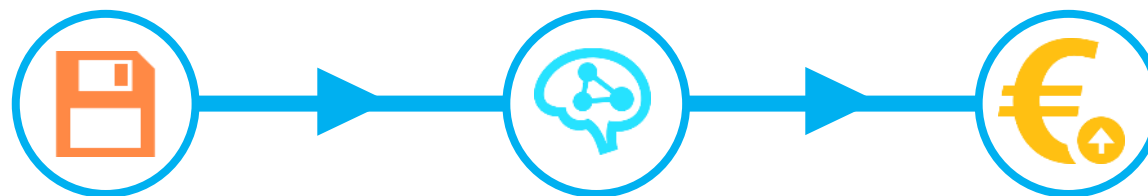


Una vez convertida la **información** en **inteligencia**, esta es **validada** mediante la generación de diversos exportables a todos los **estándares** del mercado.



Los **datos** se han convertido en **inteligencia** y esa a su vez
en **información accionable**:

Ahora puede tomar **decisiones** fundamentadas en
información **creíble** y **contrastada**.



Ahora puede **convertirse** en una
empresa **impulsada por datos**.



Comience a generar **valor** a
través de sus propios **datos**
hoy.



ravensight

**Consulte nuestras opciones de
licenciamiento y despliegue.**



contacto@ravenloop.io



ravenloop.io

Gracias

contacto@ravenloop.io

Telf: 912 532 315

C/ Hermanos Bècquer 7

Madrid-Spain

Avd/ Fuente Nueva 12A

SS.RR.-Spain