

Kymatio® is the leader in human risk management, with a comprehensive approach, our platform identifies and analyzes risks, trains and raises awareness, transforming the organization to be prepared for cyber-attacks and regulatory requirements.

**“Our clients report
up to 80% reduction
in human errors”**

+80%

Why does my organization needs Kymatio®?

The information security attacks that organizations are suffering are increasingly focused on their employees, reaching 90%* of security breaches in 2024. Fortunately, we are witnessing a consensus between those responsible for security, the management of organizations and the regulations in force in the main sectors, in which It is essential to address and manage human cyber risk.

Kymatio® provides agile but profound management of the risk associated with people, obtaining metrics, visualizing their evolution over time and providing recommendations for mitigation plans.

360° human cyber risk management aims to enable understanding of the level of cyber risk faced by the organization, facilitate new generation awareness, increase and maintain the alertness of the workforce through training.

This approach to strengthening the workforce (user hardening) results in multiple benefits, from generating intelligence related to human cyber risk, mitigating the main weaknesses and vulnerabilities of employees, to facilitating regulatory compliance and its demands regarding awareness and training of people.

* Forrester Report: The Human Risk Management Solutions Landscape

People at the center of security

Kymatio® incorporates everything necessary to manage employee cyber risk and is made up of the following services:

1.A new approach to awareness program (A&A - Assessment & Awareness)

It automates employee awareness and the evaluation of their alertness in an unattended and personalized way according to the needs of each one.

The new methodology, based on the best practices of cybersecurity and neuroscience, It allows the time that employees invest in the awareness program to be as little as possible for each case. Adjusting each session to the level of situation resolution and alertness of each employee. Studies tell us that content retention increases by 60% by personalizing awareness for each user.

UP TO
60%

**Increases retention of
contents by customizing the
awareness for each user**

Kymatio® Assessment

It has interactive features that allow users to perform exercises, through chatbot-guided interviews and decision sessions in real situations, to evaluate user behavior in the face of social engineering, malware, communications, password management, workplace, data protection or compliance.

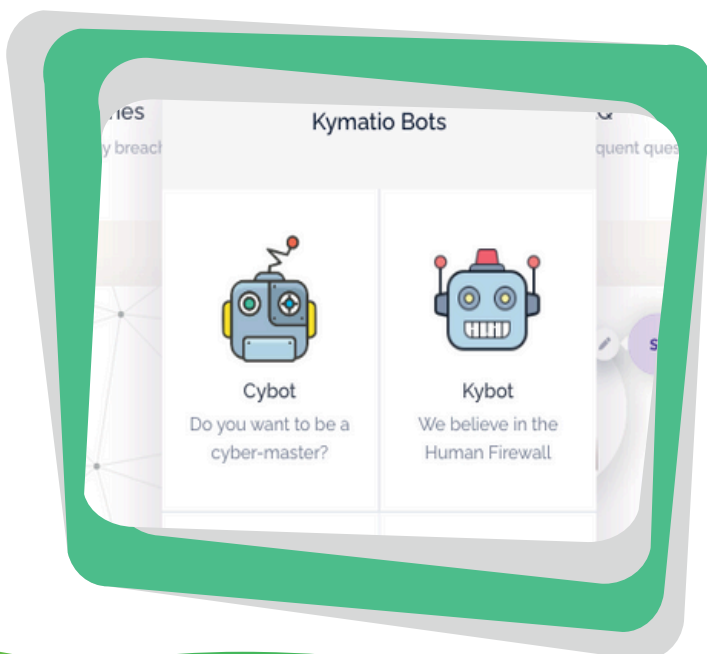
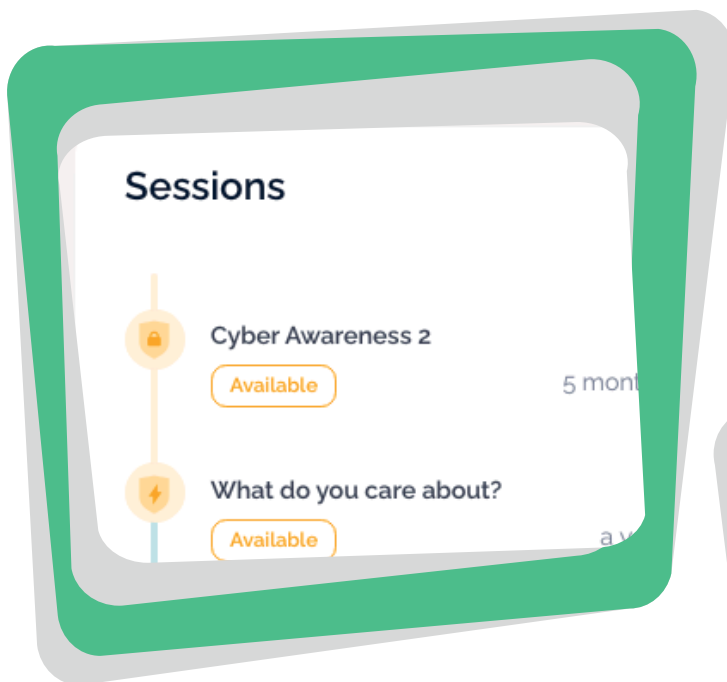
Automatically manages the periodic evaluation of risks, impact, awareness, monitoring and recommendations.

Kymatio® Awareness

Personalized and fully automated cybersecurity awareness.

It includes everything necessary in a portal created for the employee themselves, providing thousands of micro and nano learning cybersecurity content selected to create a personalized itinerary for each user, always based on the results of the evaluation sessions.

- ✓ Training in real situations, guided by chatbot, both in the work and personal spheres.
- ✓ Continuous and personalized awareness for each employee, with short and enjoyable sessions.
- ✓ More than 4 years of original multimedia content, with different sessions and documentation for each month..

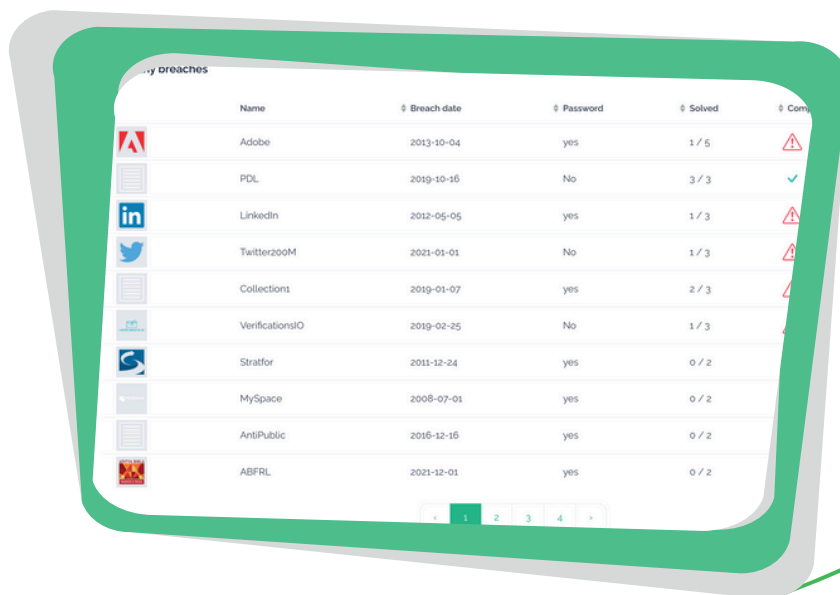






















2. Account Breach Scanner (ABS)

Connecting credential exposure risk surveillance and mitigation and awareness program.

Analysis of exposed credentials with ABS

- Periodically scan online repositories and detect organizational credentials exposed in security breaches. Surveillance is essential to protect the organization's assets and improve its security.
 - It allows teams to take preventive measures before an attacker can exploit these vulnerabilities. A multitude of laws and regulations require organizations to adequately protect their sensitive information, including access credentials. Organizations can thus comply with these regulatory requirements.
 - If credential information is found online, notify both the organization and the employee of the detection of exposures. Raises employee awareness about the importance of mitigating the risk of kidnapping and impersonation and provides a tool that enhances risk mitigation collaboratively.
- ✓ With Kymatio® ABS you obtain updated information about your organization's accounts involved in security breaches. It also provides aggregate metrics for your organization and by departments.
- ✓ Periodic monitoring of exposed credentials (emails, passwords, hints)
- ✓ It offers each affected employee the type of information compromised in the breaches and indicates the actions to take to reduce the risk, thus raising awareness about the use and criticality of credentials with real data.



Name	Breach date	Password	Solved	Com
 Adobe	2013-10-04	yes	1 / 5	
 PDL	2019-10-16	No	3 / 3	
 LinkedIn	2012-05-05	yes	1 / 3	
 Twitter200M	2021-01-01	No	1 / 3	
 Collection1	2019-01-07	yes	2 / 3	
 VerificationsIO	2019-02-25	No	1 / 3	
 Stratfor	2011-12-24	yes	0 / 2	
 MySpace	2008-07-01	yes	0 / 2	
 AntiPublic	2016-12-16	yes	0 / 2	
 ABFRL	2021-12-01	yes	0 / 2	

3. Social Engineering Simulations (Trickster)

It allows achieving the necessary visibility on the exposure of the workforce to potential information security incidents, allowing measurement and training with social engineering attack simulations.

- Launching campaigns to simulate automatable social engineering attacks such as phishing, spear phishing, malware download simulation, malicious QR codes, smishing, with a wide variety of templates. Perform simulations allowing you to evaluate the preparation of employees to detect and respond to attack attempts.
- This allows organizations to establish a baseline of their employees' behavior in these situations, as well as identify areas for improvement and provide additional training where necessary. In this way, the effectiveness of the awareness program and risk reduction can also be observed.

- ✓ With Kymatio® Trickster the analysis of employee behavior in the face of phishing, spear phishing, ransomware, malicious QR and smishing attacks.
- ✓ Training users in social engineering attacks and increasing the global alert level, with the option of using our exclusive neurophishing system.
- ✓ Identification of vulnerable areas of the organization to define action plans based on real data, reducing human risk.



4. Kymatio® Human Risk Management (HRM)

Kymatio® HRM integrates everything needed for advanced human risk management based on the intelligence gained by the other individual services A&A, ABS and Trickster.

- Provides organizations with a complete and detailed view of their risk levels, facilitating strategic decision making to strengthen cybersecurity and secure employee habits.
- It allows organizations to know and manage risk, tracking key metrics in real time, with a focus on critical areas such as impact analysis, where we evaluate the potential impact of incidents or breaches in each position, considering the pillars of confidentiality, integrity and availability of information handled by each employee. This information is combined with the alert status of each employee, social engineering simulations, exposed credentials or special modules such as Wellness and Burnout.

With all this information, Kymatio® HRM provides a detailed and accurate view of human risk, allowing the implementation of effective strategies to manage and mitigate risks, thus enhancing the security of the organization and the empowerment of its employees.









- ✓ Significantly improves employee cybersecurity awareness and content retention.
- ✓ Regulatory compliance requirement (DORA, ENS, GDPR, ISO/IEC, NIS2, NIST, PCI DSS, ...).
- ✓ Mitigation of possible sanctions in the event of a breach.

With Kymatio HRM, your organization not only identifies risks, but also has the necessary tools to manage them proactively and efficiently.





Features	Kymatio	Others
Chatbot Enjoyable and dynamic sessions	✓	✗
Time saving Optimizes the time the employee invests in the training program awareness and automates organizational awareness	✓	✗
High participation Improve employee engagement in awareness	✓	✗
Personalized Content adapted to the needs of each user	✓	✗
Simulation of Social Engineering attacks Multi-vector attacks (phishing / smishing) with training advanced (spear phishing, neurophishing based on archetypes, customization)	✓	✓
Metrics Results of the different actions and simulations (user/department/organization)	✓	✓
Own content library Continuous delivery of unique content in format micro/nano learning	✓	✗
Social engineering Personalized recommendations based on particular vulnerabilities	✓	✗
Immediate Deployment SaaS technology allows you to start working without the need of integrations	✓	✗
Advanced modules Archetype: Identification of social engineering vulnerabilities Wellbeing: Measurement of the work environment in its relationship with safety Burnout: Helps avoid problems derived from this syndrome	✓	✗

Features	Kymatio	Others
<p>SAML Federation Authentication with SSO: goodbye to passwords</p>		
<p>SCIM automatic provisioning Automatic synchronization with SCIM systems such as Azure AD</p>		
<p>Branding Logo and custom subdomain</p>		
<p>Human Risk Dashboard Risk metrics associated with each active service, evaluated based on the impact and probability of a possible incident at each workstation, taking into account the confidentiality, integrity and availability of information.</p>		



WANNA A DEMO!

