Cyrius

Human Detection and Response and its impact in 2023

How this technology will help security teams adapt to the evolving cyber threat landscape

Table of contents

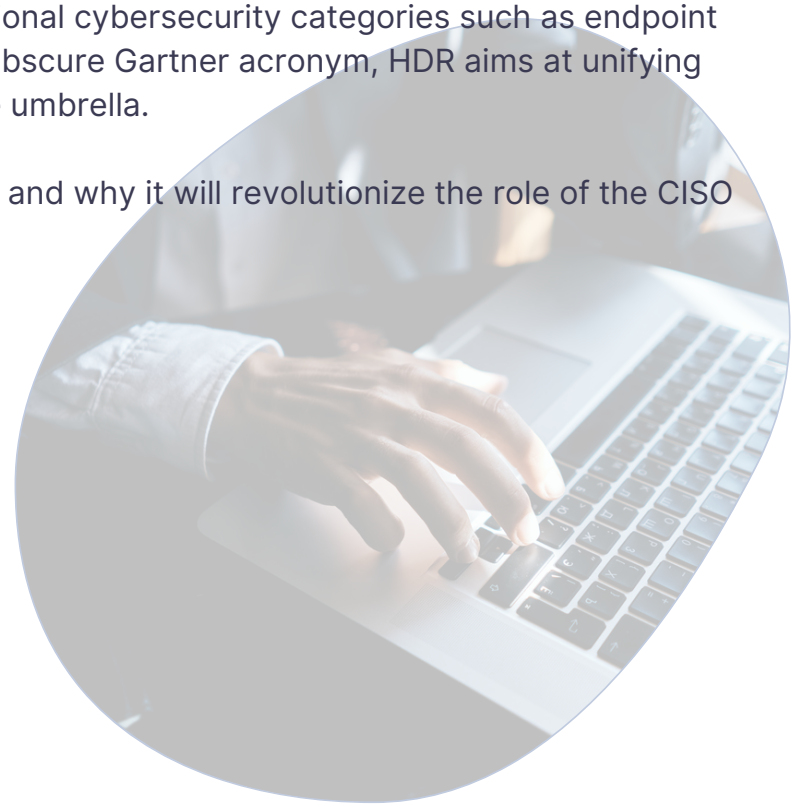
Introduction

Security awareness training is broken

In today's business landscape, the threat of cyber attacks is more prevalent than ever before. The field of cybersecurity is distinct from others in that it spans across all industries and is interwoven into the core of each industry's operations. It's not a standalone function like other specialized fields such as food delivery or human resources technology. Instead, it is a fundamental aspect that everything relies on and cannot be separated from its application. And as the volume of attacks keeps growing every year, all organizations must consider cybersecurity as a major concern. Hence, the role of CISOs is becoming increasingly important.

Let’s say it straight, security awareness training is broken. It fails to efficiently prevent mistake to be made, and thus companies to be really protected.
In that tensed context, Human Detection and Response (HDR) is an emerging technology that aims to address the vulnerability of human factor in cybersecurity. It closely monitors user activity for any unusual patterns and promptly responds to mitigate potential data breaches. HDR also provides employees with cybersecurity training to raise their awareness and ability to identify and avoid threats. It is a complementary technology to traditional cybersecurity categories such as endpoint protection. Far from being another obscure Gartner acronym, HDR aims at unifying all user-related mitigation under one umbrella.

This report will explore what is HDR, and why it will revolutionize the role of the CISO in 2023.



01

Addressing the human factor

Addressing the human factor

1.1 You already know what's the weakest point in your security posture

The human factor is the #1 weakness in cybersecurity. As the 2022 Verizon Data Breach Investigations Report highlights, the human factor is involved in 82% of data breaches. Employees often fall for phishing scams, use weak passwords, or mishandle sensitive information. Human error, lack of awareness and poor security habits can easily be exploited by cybercriminals to gain access to an organization's sensitive information. Taken from the latest report from SoSafe, every third user clicks on harmful content in phishing emails.

BREACHES

82%

of data breaches are due to a human error

Additionally, the potential for malicious intent from employees such as data breaches caused by insiders can also be considered as part of the human factor. These breaches can be particularly damaging as they are often carried out by people who have legitimate access to sensitive information and systems, making them difficult to detect. The number of insider-caused cyber security incidents has increased 47% in just two years from 2018 and 2020, according to Ponemon Institute.

5

reasons to develop a strong defense layer

1. Minimize risks
2. Stay compliant
3. Protect your reputation
4. Ensure business continuity
5. Promote employee engagement

Addressing the human factor

1.2 HDR creates a human firewall and reduces potential for human error and malicious intent

Creating a "human firewall" refers to the ability to use the human element as a means of protection rather than just a weakness to be overcome. Security awareness training stays a critical first step of a strong human firewall, as it plays a significant role in helping employees to recognize and avoid potential threats, and to develop good security habits. When employees are trained on how to recognize and respond to potential security threats, they become better equipped to identify and avoid phishing scams, detect and report suspicious activity, and protect sensitive information. You want employees to stay aware and updated on the latest threat patterns and trends.

PHISHING

58%

of employees are more vigilant against phishing attacks after a dedicated training

CybSafe's 2022 report notes that a third of employees who received training declared a change of behavior regarding passord hygiene, updates, data back-ups, and MFA. This proves that awareness training does have some kind of positive effect.
But it can't be enough.

HDR combines security awareness and technology: it can detect, analyze and respond to security threats in real-time and then, with a security awareness platform, it can provide immediate training and education to the employees - who triggered the alert.
This means that not only the incident is resolved, but also the employee who caused the incident is trained and will hopefully not repeat the same mistake in the future.

> **Teams are empowered with the explanation of WHY their behavior is dangerous, unlike traditional security software that merely prevent it.**

HDR helps to create a shared understanding of the importance of security within an organization. This includes promoting a culture of security and encouraging employees to understand and adopt good security practices, and to understand the role that they play in protecting the organization. The security culture is established by continuously promoting security awareness and providing the means to measure and improve the organization's overall security posture.

Addressing the human factor

1.3 HDR analyses, identifies, and responds to user-related security behavior

What can CISOs do against human mistakes or bad intents? Security awareness training has been the answer for long. Although it can help to spread the building blocs of a cyber culture, it is hard to get a clear ROI from these actions.

HDR addresses the issue of the human factor in cybersecurity by analyzing and detecting any abnormal behavior in user activity. Then it sends real-time notifications to your user in a timely manner, empowering them with the ability to mitigate the risks.

What are the use cases of HDR?

Risky behavior monitoring and detection

HDR technology continuously monitors user behavior through integrations with your tools. It gives the organisation much more visibility to what users are doing.

Real-time alerting

Once a risky behavior is detected, such as visiting malicious websites, clicking on suspicious links, or sharing sensitive data, the user is notified via a real-time notification (email, Teams, Slack). This allows the organization to quickly take action to prevent the attack from happening, and to provide additional training to the employees involved in the risky behavior.

Phishing simulation and Training

HDR technology can also simulate phishing attacks to educate employees on how to identify and respond to phishing attempts. This will help employees to develop the ability to identify suspicious emails and to report them to the appropriate team. Employees will also receive regular training on identifying phishing attempts and understanding how to avoid them.

Security awareness

HDR technology provide employees with regular cybersecurity training and education, which will help them to understand the importance of security within the organization, and to develop good security habits. This will help employees to stay aware of the latest threat patterns and trends and they will be better equipped to identify and avoid potential security threats.

Demonstrate a clear ROI

By combining all of the above, HDR can finally provide the ROI traditional awareness campaigns lack. CISOs can get a tangible amount of bad behaviors detected at any given moment, and compare it to the following months. Say goodbye to random money throwing, and hello to profitable investments.

1.4 Use-case: How HDR reduces human risk on DLP

HDR is fully integrated to your business and security tools. You can install it via API or directly from the marketplaces of the tools.

Integration API-first to SaaSs tools

Selection and definition of trigger rules

WHEN a user shares a Google Doc publicly
AND this user is from marketing department
THEN send him/her a direct message on Slack

Detection of a suspicious behavior caused by an employee

13/01/2023 12:03:11 - "Sales roadmap 23Q1"
Google Doc shared **publicly** by John Smith
from **marketing department**

Instant notification for risk remediation

Cyrius 12:04
Hello John!
You've just shared the **Google Doc** "Sales roadmap 23Q1" **publicly**. Please change the access rules :)

Change rules | Contact support

Dedicated awareness training sent

Cyrius 12:06
Good job John!
Now that your security issue has been **fixed**, it's the **perfect time** for me to explain you WHY this type of behavior is **dangerous**.

Let's start

Data updated in admin dashboard

Nb of issues this month

59 (81% fixed)
+1 fixed issue today

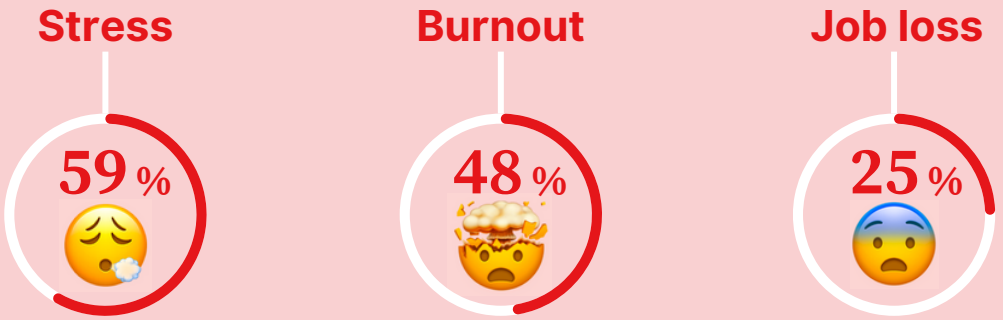
02

Reducing the workload of the CISO and security team

2.1 Security teams are burned out

A recent survey from executive search firm Heidrick & Struggles points out on of the main struggles of CISOs: stress and burnout. And indeed, the workload of CISOs and security teams can be quite demanding and challenging. They are responsible for protecting an organization's assets and information against cyber threats, and ensuring that the organization is in compliance with legal and regulatory requirements. Managing security incidents and responding to security breaches often require them to work under high pressure and tight deadlines. They also need to keep abreast of the latest threats and vulnerabilities, as well as new security technologies, in order to continuously improve the organization's security posture.

What are the most significant personal risks relating to your role of CISO?



Additionally, they also need to be able to communicate effectively with different teams, from the board of directors to the IT team, to ensure that security concerns are understood and addressed effectively. Fostering a security culture among employees is also part of their requirements, but these are time consuming.

Reducing the workload of the CISO and security team

2.2 HDR can help to reduce CISOs' workload

HDR is designed to lighten CISOs' burden with automations and integrations. The goal is simple: save CISOs from the need to spend time manually monitoring and responding to potential security incidents, allowing them to focus on more strategic tasks such as identifying and addressing new and emerging threats, and developing and implementing security policies and procedures.

Top 5 benefits when integrating HDR

1 Streamlined incident response

HDR automates tasks such as collecting data, identifying threats, and notifying the appropriate stakeholders, which would otherwise need to be performed manually. This can help to reduce the workload for a CISO by reducing the need for manual monitoring and incident response.

2 Customizable policies

HDR technology can be customized with organization-specific policies and procedures, which allows it to adapt to the unique needs and requirements of the organization.

3 Security awareness

As mentioned earlier, distributing security knowledge among teams can help to reduce the risk of security incidents caused by human error - thereby reducing the workload of the CISO.

4 Reporting and visibility

HDR provides a centralized view of the organization's security posture, granting CISOs with real-time visibility of security-related activities across the organization. This can help CISOs to quickly identify potential threats and respond to them quickly, reducing the need for a security team to manually monitor these activities.

5 Integration with other systems

HDR technology can integrate with other tools. From one side, it connects with productivity tools such as Microsoft 365 or Google Workspace. It can also connect with security systems such as intrusion detection systems, firewalls, and security information and event management (SIEM) systems, this way it can get the latest threat intelligence and feeds from those systems to better identify and respond to threats.

2.3 HDR allows security teams to focus on the highest priority threats

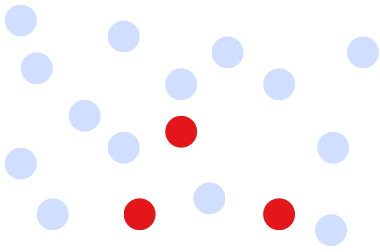
Helping the CISO is great, but what makes HDR special is that it can be also he used by a larger security team. So whether you have a SOC already, or you are a team of three security professionals, HDR has something for you.

First, HDR is extremely useful in reducing alert noise. With thousands of events and alerts generated daily, it can be hard for security teams to separate the meaningful alerts from the noise. HDR technology can help to reduce the volume of alert noise by identifying and responding to the most critical events, allowing security teams to focus on the high-priority threats.

HDR technology can also correlate security events across multiple systems and sources, reducing the number of alerts and providing more context to investigate more efficiently. This allows the security teams to focus on the most critical incidents, rather than wasting time on low-priority alerts.

Finally, your root cause analysis can easily be improved. HDR technology can provide detailed information about the root cause of security incidents, enabling security teams to quickly identify and remediate the underlying problems. This can help to reduce the time and effort required to investigate and resolve security incidents.

Step 1: Reception of all logs



Step 2: Detection of suspicious behaviors

Step 3: Automated remediation by employees

Step 4: Investigation on the relevant issue by sec team

03

Adapting to the changing threat landscape

3.1 Cyber threats are becoming more frequent and sophisticated

According to the latest Global Threat Report from Crowdstrike, 1 organization out of 3 experienced a cyberattack in 2022. And this will most likely keep increasing in 2023. Cyber threats are becoming more sophisticated as criminals are using advanced techniques such as artificial intelligence, machine learning and automation to carry out their attacks. Deepfakes, voice cloning, and automated, large-scale spear phishing will soon become the new norm.
The increase in connectivity and the number of devices, systems and networks connected to the internet create more opportunities for attackers to gain access to sensitive information and disrupt operations.

Cybercrime has become a highly profitable business, criminals are well-organized and well-funded, and willing to invest in developing new techniques. Social engineering techniques such as phishing, pretexting, and baiting are becoming more personalised, making it harder to detect and prevent.

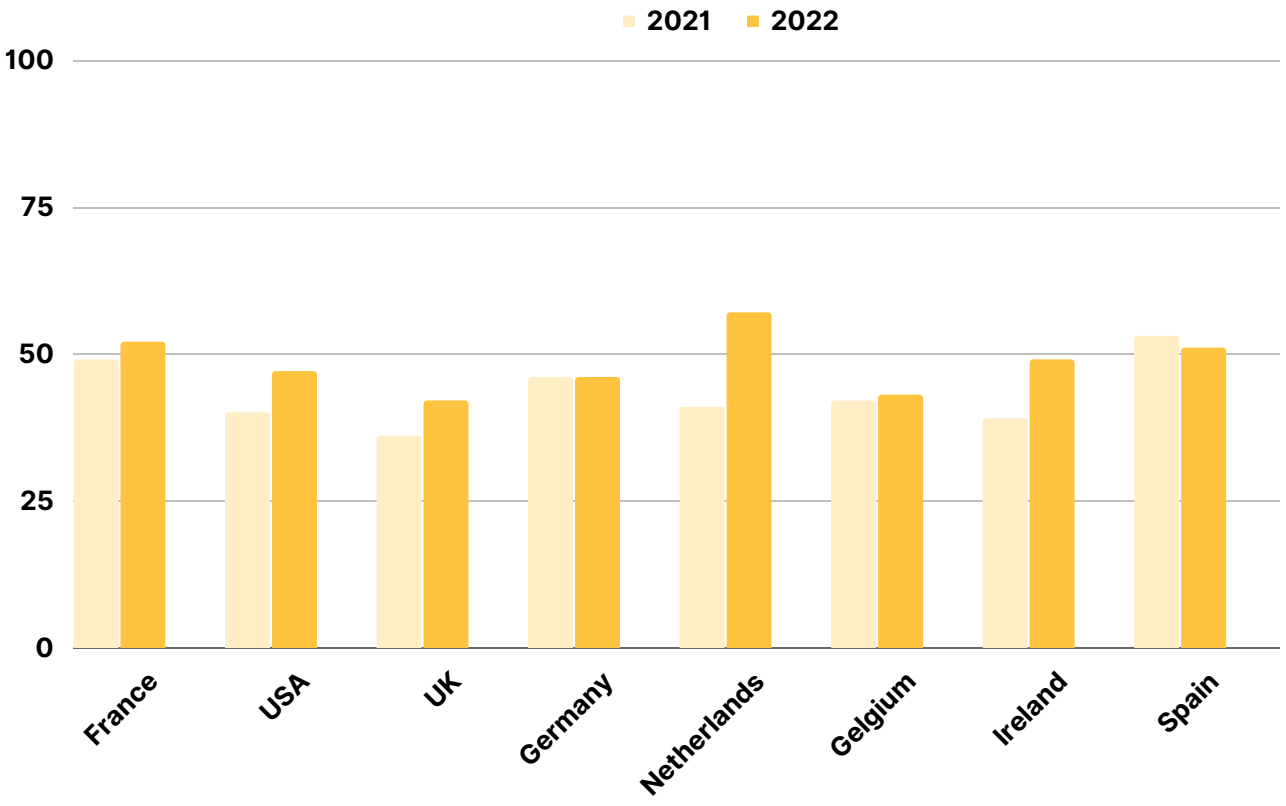
All of this means that 2023 will be a tough year in security.

CYBERATTACKS

150%

increase of cyberattacks year-to-year since 2020

Percentage of companies that have experienced at least one cyberattack



3.2 Traditional security measures will no longer be enough of a protection

As cyber threats become more advanced and sophisticated, hackers can evade traditional security defenses. Traditional cybersecurity measures, such as firewalls, antivirus software, and intrusion detection systems, are designed to protect against known threats. Since traditional cybersecurity measures are based on predetermined rules or models, they can be bypassed by attackers. Because attackers are continually developing new techniques, traditional measures may no longer be able to detect or prevent unknown threats.

> **According to the European Union Agency for Cybersecurity (ENISA), we are living in a "golden era" for cyber criminals.**

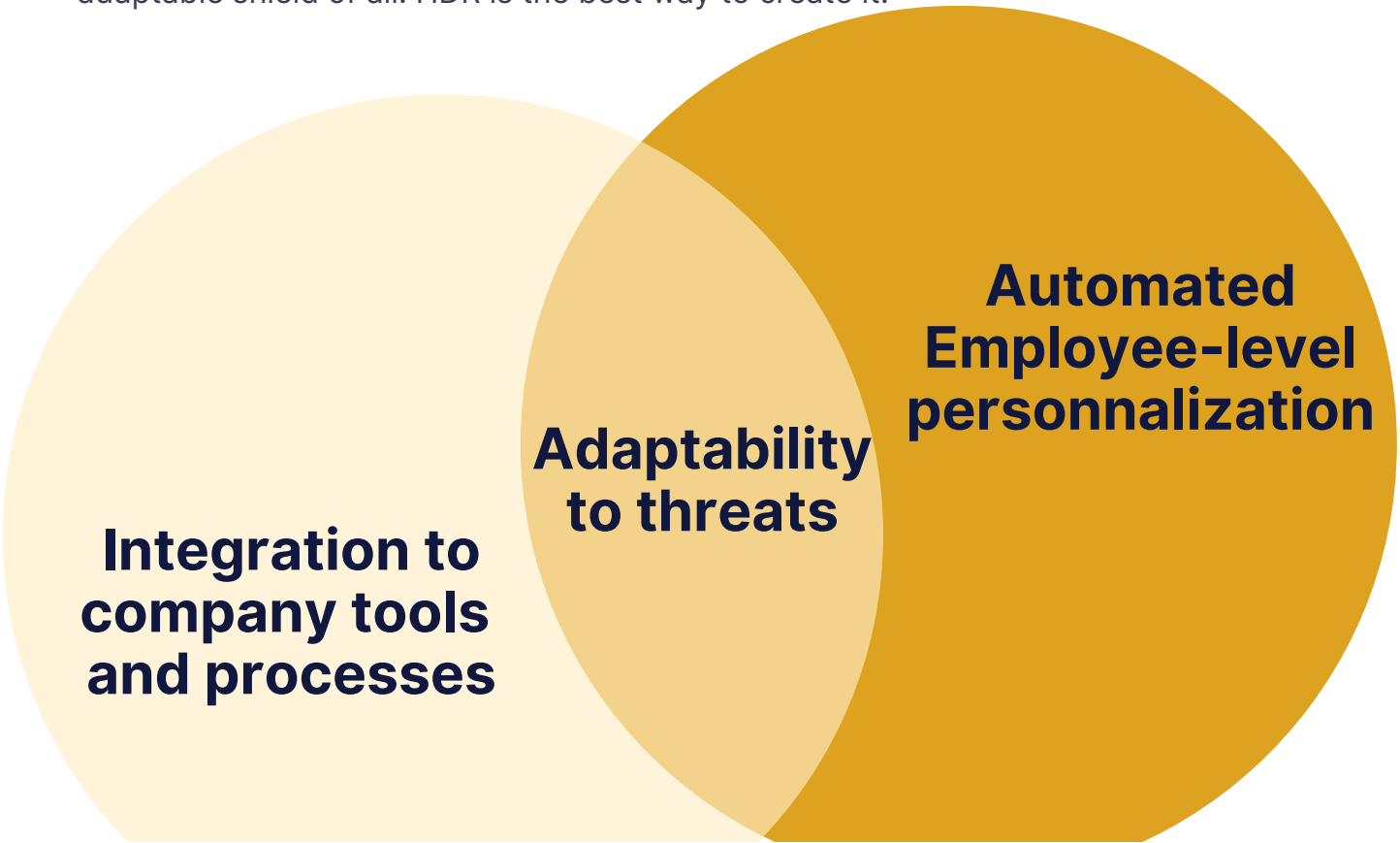
On the other hand, well-prepared employees can act as a first line of defense against unknown threats by being able to recognize and respond to potential security risks and incidents in a timely and effective manner. They can identify and report suspicious activity, follow security best practices, continuously monitor and assess security of the devices and systems, think critically and process the context, and adapt to new security risks and threat patterns as they emerge. Through their role as a human firewall, well-prepared employees can help to protect the organization from security breaches caused by unknown threats.

3.3 HDR is a flexible technology that can adapt to the changing threat landscape

Human Detection and Response is an adaptive technology by nature. This means that it is designed to be flexible and responsive to the changing needs of the organization and to the constantly evolving threat landscape. One of the ways it achieves this is by connecting to business or security tools, which provides a granularity of events that makes it possible for each company, department, or employee to have different, specific, and relevant content. This is very different from the generic modules of an awareness program or the strict rules of a pre-configured tool, which may not be tailored to the specific needs of the organization.

From another perspective, establishing a human firewall is the only actual way to counter emerging threats, as humans can instinctively detect fraud when their are properly trained. HDR helps you adapting to the changing threat landscape by empowering you users with the right knowledge at the right moment. Additionally, regular training and educational programs are also part of the benefits of HDR in that context. They can be tailored to the evolving threat landscape and updated on best practices and policies. This helps users to stay informed about the latest threat patterns and trends, and to develop the ability to identify and avoid potential security threats.

Combining extreme personnalisation and contextual learning is key against the next generation of cyberattacks. Only a strong cybersecurity culture within the organisation will be efficient in front of unknown threats, as your teams are the most adaptable shield of all. HDR is the best way to create it.



Conclusion

Finally taking the human risk seriously

Human Detection and Response (HDR) can finally put an end to unproductive security awareness training. It addresses the human factor by empowering users with real-time security alerts and notifications, which allows them to make better choices while facing potential or new security risks.

It reduces the workload of IT and security teams by automatically identifying and responding to potential security threats in real-time, which frees up resources to focus on other tasks. By technology and human expertise, it creates a strong defense layer that can adapt to the constantly changing threat landscape.
HDR builds a security culture by providing regular education and training to employees on security best practices and policies, which helps to raise awareness on potential security risks and incidents.

HDR will revolutionize the role of the CISO in 2023 by providing them with a more comprehensive and proactive approach to cybersecurity.
Detecting real-time risky behavior, customizing policies and procedures, and integrating with other security systems will enable the CISO to get a more complete view of the organization's security posture. That will allow them to take action faster and better, which will in turn help to minimize the impact of security breaches.

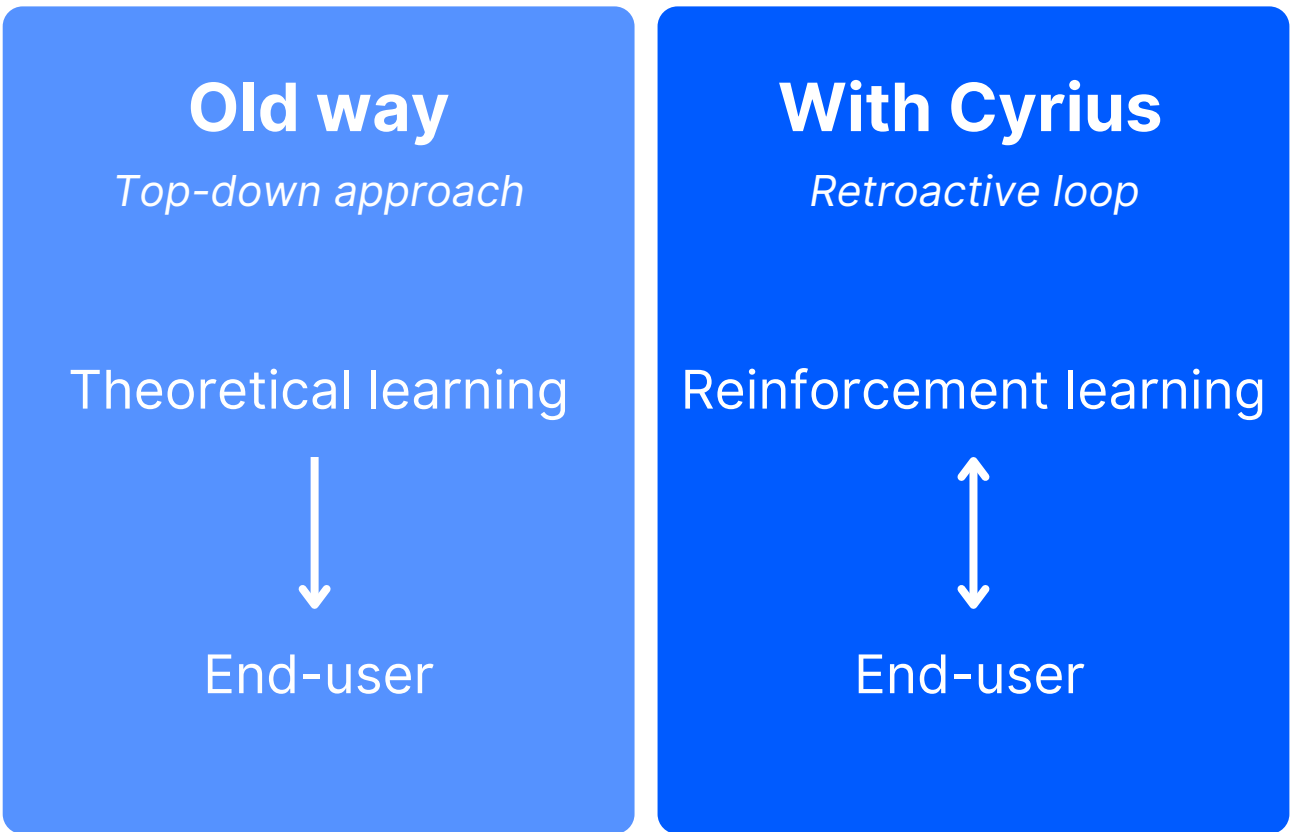
The consequence? HDR will enable the CISO to create a more proactive, efficient and adaptable security strategy. All in all, HDR will allow the CISO to focus on more strategic initiatives, such as developing and implementing security policies and procedures, and building a security culture within the organization.

About us

At Cyrius, we think security awareness training is outdated and inefficient, and want to change that. Organizations and their employees deserve the best protection. That is why we are building the world's first HDR.

Cyrius allows you to manage the cyber risk related to employees, from their first day in the organization to their departure. With our first product, we already cover +20,000 employees, across dozens of customers (4.5/5 satisfaction rate).
Thanks to 5 complementary pillars, the platform allows security managers to visualize the risk behaviors of their users, to notify them in case of a potential breach, and to train them efficiently. With API-first integrations, you can connect it in one click to all everyday tools, whether they are business or security tools.
We are confident that, very soon, HDR will be the next standard in the most advanced security organizations.

We are still in beta mode, and actively looking for testers who passionately share our vision. We need you to make it a reality! So if you think you are a fit, feel free to contact us at achille@cyrius.co



Sources

- Ross Haleliuk - Venture in Security
  https://ventureinsecurity.net/p/game-of-thrones-in-cybersecurity
- 2022 Verizon Data Breach Investigations Report
  https://www.verizon.com/business/resources/reports/dbir/
- Human Risk Review 2022:
  https://sosafe-awareness.com/resources/reports/human-risk-review/
- Proofpoint 2022 Cost of Insider Threats Report
  https://go.crowdstrike.com/global-threat-report-2022.html
- 2022 Global Chief Information Security Officer (CISO) Survey:
  https://www.heidrick.com/en/insights/compensation-trends/2022-global-chief-information-security-officer-ciso-survey
- The Annual Cybersecurity Attitudes and Behaviors Report 2022:
  https://www.cybsafe.com/whitepapers/cybersecurity-attitudes-and-behaviors-report/
- Hackers-for-Hire drive the Evolution of the New ENISA Threat Landscape:
  https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape