Cybersecurity Accelerator Program (CSAP)

Accelerate to secure digital transformation with Inetum-Realdolmen

inetum realdolmen
Positive digital flow

Organizations are quietly reaping the benefits of the digital transformation on which they have embarked in recent years. This necessary transformation has already been a little smoother and faster in one organization than in others. But did it always proceed securely?

At least in the latest annual priorities survey by Beltug, the largest association for CIOs and IT decision-makers in Belgium, security was at the top of the agenda. **Awareness** of the importance of security and concern over its impact remain high.

Another user survey by Beltug shows that investments in **security products** have remained stable in recent years, with solutions for antivirus (81%), data backup (66%) and firewall protection (64%) emerged as the most popular purchases, unchanged from 2020. Two-thirds (64%) of the companies surveyed by Beltug expect these investments to continue in 2023. One in four respondents even see it increasing, with a majority (60%) prioritizing the purchase of additional security solutions.

However, security is about **much more than products alone**. And unfortunately, that's where the proverbial shoe can start to pinch.

> "Business leaders are setting new priorities, such as IT security strategies, data management and user awareness."
>
> Danielle Jacobs, Beltug

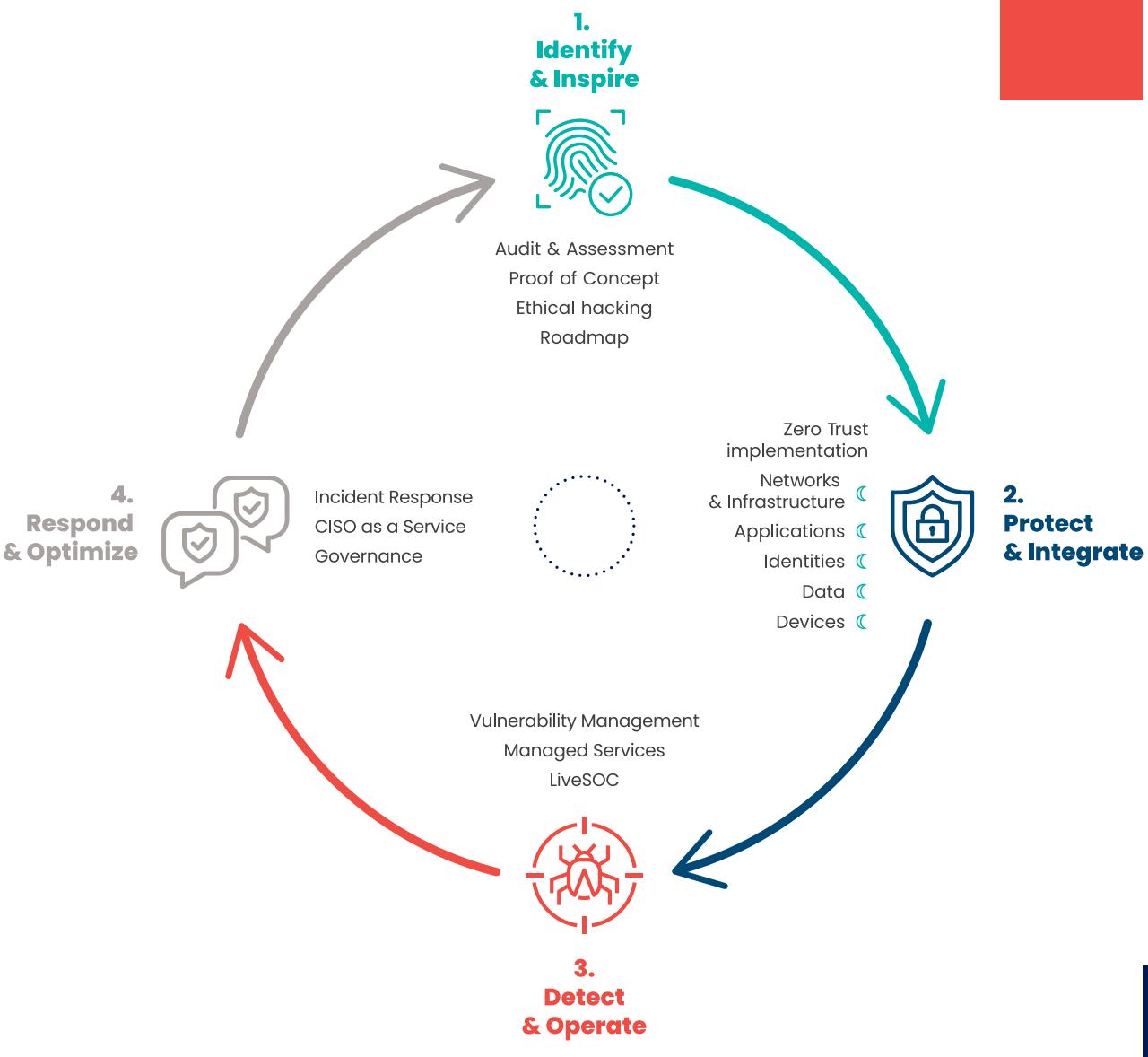
CSAP: your guarantee of secure digital acceleration

Not surprisingly, the biggest concern of Belgian CIOs, according to Beltug's annual priority survey, is defining and implementing a clear **vision** of cybersecurity in their company (46%). Challenges related to **security architecture** (39%) and increasing **involvement of people** within the organization (38%) are also high on the priority list.

All these important, unavoidable aspects of IT security, not directly related to products and sometimes not even to technology, are equally deserving of your attention. To ensure that you don't overlook any of them, we have developed our **Cybersecurity Accelerator Program (CSAP)**, a four-step umbrella program that offers you an integrated range of services and solutions from a holistic view of security. This is how Inetum-Realdolmen helps you achieve the digital transformation of your business quickly yet securely.

CURIOUS ABOUT THE FOUR STEPS OF OUR CYBERSECURITY ACCELERATOR PROGRAM?

Check it out!



1. Identify & Inspire: good preparation is half the battle

Before you can even consider a step toward better security, you obviously need to know exactly where you currently stand in your improvement journey. That's why it all starts with measuring and analyzing. And experimenting, but to inspire you!

To keep you from sailing blind and without a compass, we first carefully map your **(cyber) vulnerabilities** and determine your **cybersecurity maturity**, through a **security audit and assessment**. For this, we can use our own Cybersecurity Assessment Tool, as well as various audits especially designed for a specific technology (e.g., networks) or supplier (e.g., Microsoft).

If necessary, we also use **ethical hackers** to detect and identify your vulnerabilities, using various techniques: internal and external **penetration testing**; simulating a **ransomware attack**; **social engineering**, where we try to exploit human weaknesses such as curiosity or selfishness; and **code evaluation**.

Once the potential risks are identified, we also help you prioritize them, along with all the actions you can take to be better defended against cyberattacks. The formal outcome of this strategic analysis is a cybersecurity **roadmap** with concrete recommendations, including a list of the necessary projects and associated budgets. The roadmap can also serve as a practical guide for the coming years.

Are you unsure whether a proposed security solution is right for you? Don't worry, we'll be happy to create a **proof-of-concept** for you to explore its possibilities and added value. We also organize **workshops** on all kinds of innovations in cybersecurity to inspire you.

"Cybersecurity is not a compliance obligation, but an essential aspect of protecting your business."

Pieter Byttebier, CCB

ARE YOU READY FOR NIS2?

Not only the market itself, but also **legislators are imposing greater cybersecurity requirements on companies**. A striking example is NIS2, the **new European directive that will enter into force in 2024** and is considered the GDPR in the field of cybersecurity. Its goal is to better protect organizations and manage risk, while preventing incidents or limiting their consequences.

NIS2 covers **11 sectors** more than NIS1. According to an initial estimate by the Center for Cybersecurity Belgium (CCB), some **2400 Belgian companies** would be covered by the new directive.

If you are one of those companies, we recommend that you start working on a cybersecurity maturity analysis and roadmap now. This will give you enough time to take the necessary measures to (continue to) operate securely, in compliance with the new NIS2 directive and allow you to spread the costs.

2. Protect & Integrate: zero-trust security provides proactive protection

Once the preparatory work is done, it is important to build a solid security infrastructure tailored to your needs. The important thing is to be able to integrate this infrastructure seamlessly into your existing IT environment. More importantly, the infrastructure relies on an innovative, future-oriented security architecture known as "zero trust".

This denomination represents a **proactive approach** to security. At its heart is a process of **continuous verification** based on the most important zero-trust principle: "Never trust, always verify!"

Zero trust security allows you to respond faster and more efficiently to threats and effectively stop and even prevent attacks. To this end, the new security concept is based on a wide range of **adaptive controls and mechanisms**.

To implement zero trust, it is therefore not enough to have a single product, service, solution or technology in-house. You can't rid yourself of such attacks and threats once and for all with a single project or implementation. Zero Trust requires a sustained **long-term effort** and **constant vigilance** against new risks and hazards.

"To purchase security products, most companies prefer a local IT partner." Beltug."

Beltug. – B2B Market Survey, ICT Trends 2022: Security

ZERO TRUST ARCHITECTURE RESTS ON FIVE PILLARS:

1. **Identities:** Thoroughly verify the identity and always authenticate the user before granting them access to your work environment, via multi-factor authentication, single sign-on, identity & access management, privileged identity management and risk-based authentication.
2. **Devices:** Prevent an unsafe device from accessing your work environment through mobile device management, device compliance and endpoint protection.
3. **Networks and infrastructure:** Secure your networks and infrastructure with segmentation, threat protection and encryption.
4. **Applications and APIs:** Get your applications and APIs under control via access authorization, accessibility, monitoring and patch management.
5. **Data:** Ensure data security at all times thanks to classification, labeling, encryption, access and data loss prevention, and backup and recovery.

To secure each of these pillars, you need the right **technological solutions** and **expertise** for their proper implementation and integration. With our **end-to-end range of services and solutions**, you'll be set with all of them right away. In addition, we can guarantee you the **strongest foundation** for the pillars, with solutions for visibility and analysis, automation and orchestration, and last but not least governance.

WANT TO SEE THE CONCRETE SECURITY TECHNOLOGIES AND SOLUTIONS WE PROPOSE FOR THE IMPLEMENTATION OF ZERO-TRUST SECURITY?

Read more in our brochure: Zero Trust: the new standard in the world of cybersecurity explained.

3. Detect & Operate: alertness remains crucial

Is your security architecture and infrastructure up to date? Even if it is, stay alert!

The majority of successful cyberattacks can be traced to a known vulnerability that was not discovered and addressed in a timely manner, or worse, to a vulnerability that the organization did not know about at all and is only picked up weeks or even months after the fact. For example, six out of ten respondents (62%) to a study by the US research center Ponemon Institute claimed they were unaware of vulnerabilities in their organization prior to a cyberattack.

This also demonstrates the importance of consistent, process-based management of your vulnerabilities. The **vulnerability management** process involves defining, identifying, classifying and prioritizing vulnerabilities in your infrastructure and applications. By doing so based on thorough **risk analysis**, we help you handle a vast number of vulnerabilities, giving you exactly the focus you need to act quickly and effectively.

In a proposed resolution against Internet fraud, the Belgian House of Representatives reported a total of 37,982 incidents of cybercrime for the year 2021. That's **more than 100 cyberattacks a day** – an increase of 37% from 2019.

YOUR SAFETY, MORE THAN EVER OUR CONCERN

Implementing security infrastructure is one thing, but afterwards, you still have to **manage** and **continuously optimize** it. Even more challenging, you need to **continuously monitor** it for potential threats and vulnerabilities.

Such a **24/7 operation**, however automated, usually requires a lot of manpower and expertise. It's not a problem if you don't have that in-house: we can manage, optimize and monitor everything we implement for you, on-site and remotely.

In Belgium alone, we can rely on almost 100 security specialists for this. Together with the more than 85 nearshore experts at **LiveSOC**, our **Security Operations Center (SOC)** in Spain, they enable us to offer you a wide range of **managed security services**, from prevention to damage recovery, for your maximum unburdening.

With **SIEM & SOC as a Service**, we offer a 24/7 managed service that analyses and correlates big security data using SIEM technology (Security Information & Event Management), then putting the result under the watchful eye of the security experts in our SOC. If you want to start on a smaller scale, we also offer our MicroSOC, which ensures that the most important parts of your environment are monitored and that you are notified in case of emergencies, without the need of a fully built-out SIEM/SOC solution.

4. Respond & Optimize: the work is never done

Do you have a plan in place if things go wrong? Responding quickly and appropriately to a security incident can not only limit the damage, but helps prevent it from getting worse and speeds up the recovery time.

Just under half of companies in Belgium already have a security plan, according to the latest Beltug user survey. Although large (74%) and medium-sized companies (61%) are doing much better in this area, cybercriminals are increasingly targeting **smaller companies**. In 2020, no fewer than four out of ten SMEs (42%) in Belgium and the Netherlands suffered cyber incidents. In four out of ten companies affected (38%), the incident even led to a business shutdown.

Have you been the victim of a cyberattack? Even then, of course, we won't let you down. In addition to advice and support in drawing up a recovery plan, you can always contact us for the **actual handling of incidents**, at our Incident Response section. With our specialized **incident response teams**, we'll help you get back up and running quickly.

"48% don't know what to do or how to respond appropriately in the event of a cyberattack."

Agoria, Cybersecurity in Manufacturing – 2021

There are several reasons why a **Chief Information Security Officer (CISO)** can add value to your business – unless you are already legally required to name such a position. Is a full-time CISO still too much for you? Then we would like to introduce our **CISO as a Service**: a security expert who will take on the role of your part-time CISO.

BEFORE YOU FORGET: BE SURE NOT TO LOSE SIGHT OF GOVERNANCE

IT security is about **more than technology alone**: governance is an equally important aspect of cybersecurity. It can be translated into your **security policy**, **security procedures**, and **security culture**. For example, it is essential that you ensure that your employees be aware of the security risks and their role in protecting the organization.

It is important to realize that cybersecurity is not static, but is a dynamic, **cyclical process**. You can call it what really it is: an eternal work-in-progress. In other words, as a cybersecurity officer, your job is never really done. Therefore, effective cybersecurity governance also includes continuously improving the security attitude through regular **training**, **awareness** and incident response planning, for example.

Finally, by aligning your **cybersecurity goals** with your overall business goals and risk management strategies, cybersecurity becomes fully integrated into your organization's culture and operations. For instance, cybersecurity is no longer seen as a cost or a mandatory burden, but as a **profitable strategic investment**.

TOGETHER, WE'LL MAKE IT WORK!

How secure is your IT environment? Have you taken a "snapshot" yet? How do you ensure zero-trust architecture and keep it up-to-date? Perhaps you have already taken steps in this **Cybersecurity Accelerator Program** yourself, but you would like to farther develop certain components. In every case, you can turn to us. We have the necessary expertise for all services and technological pillars covered in this document. Together we can create a safer working environment!

CONTACT US

Powered by our Cybersecurity Partners

Microsoft · paloalto NETWORKS · FORTINET · CHECK POINT · vmware · TREND MICRO

HPE aruba networking · HOXHUNT · citrix · CROWDSTRIKE · AvePoint · CISCO

tenable · kaspersky · VEEAM · COMMVAULT · Secutec · THALES

splunk> · zscaler · netskope · MICRO FOCUS · Forcepoint

Inetum-Realdolmen
A. Vaucampslaan 42
1654 Huizingen, Belgium
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum realdolmen
Positive digital flow