Microsoft Defender XDR managed by Inetum

Cybersecurity insights turned into action

inetum.

In the security world, acronyms sometimes whiz around our ears. Thus, we went from AV to EPP to EDR and now XDR. These changing technologies are therefore necessary for staying a step ahead of threats. It is not always easy to keep up with them and take the appropriate actions in time to prevent an incident. With our new managed Microsoft Defender XDR, we not only provide visibility into the threats facing your IT environment, but also 24/7 incident monitoring and response.

The number of cyberattacks continues to rise. The question is not whether you will be affected, but when exactly. Fortunately, most companies are now aware of this **growing number of cyberthreats** and are trying to arm themselves as best they can against them. If they don't do this on their own initiative, there is always the growing pressure from external regulators.

NIS2 as a game changer

Governments, with the European Union leading the way, are imposing increasingly high cybersecurity requirements on companies. A striking example is the comprehensive European NIS2 directive, which will serve as a lever and accelerator for all kinds of necessary cybersecurity investments in the coming years. They should help companies reach a common minimum level or **safe lower limit** in this area as well.

NIS2 will initially apply to 180,000 companies across 18 sectors within the European Union. There is a real chance that your business will be part of it – or part of the supply chain of such organizations. If so, you too will have to take a number of measures to adequately manage your cybersecurity risks, and prevent or limit the consequences of incidents as much as possible.

Gaining insight

Specifically, there are measures applying to 10 cybersecurity domains. One such domain is **incident handling**: the **prevention, detection and response to cyber-incidents**.

The good news is that there are many solutions on the market today that can support you in this incident handling. One of the most well-known was developed by Microsoft. First and foremost, with Microsoft Defender XDR, you gain a better insight into the numerous threats to your IT environment.

However, there is also news that is not as good. Companies do not always have the necessary personnel and expertise to implement such a solution and operate it smoothly. Investing in **specialized knowledge and profiles** is not only expensive, but they are simply very hard to find in our current labor market.

Microsoft Defender XDR: a better view of danger

XDR (extended detection and response) extends the basic capabilities of EDR (endpoint detection and response) to protect **more than just endpoints**. For example, Microsoft Defender XDR also lets you secure your **hybrid identities, email, collaboration tools, apps, and cloud environment, across multiple platforms**. In other words, the solution is not limited to the Microsoft platform, and extends across your entire infrastructure.

By streamlining security data capture, analysis and workflows, Microsoft Defender XDR increases the visibility of hidden and advanced threats. The **better and additional insights** you thus gain will help you respond to those threats in a timely and appropriate manner, automatically or otherwise.

Taking action

That is where we can make the difference for you as a **trusted IT partner** with our **certified Microsoft and security experts**, especially because implementing a solution like Microsoft Defender XDR is not enough, nor is it enough to gain insights through that solution.

Reports and automatic alerts or warnings alone are insufficient: you must also be able to take **appropriate and timely actions** to prevent or successfully respond to an incident to avoid worse damage. This must be done **around the clock**, including at night and on weekends.

XDR as managed service

You may not have the people or resources for that, either. Don't worry, that's precisely why we are now offering you this indispensable and – who knows – perhaps eventually compulsory incident handling as a **managed service**.

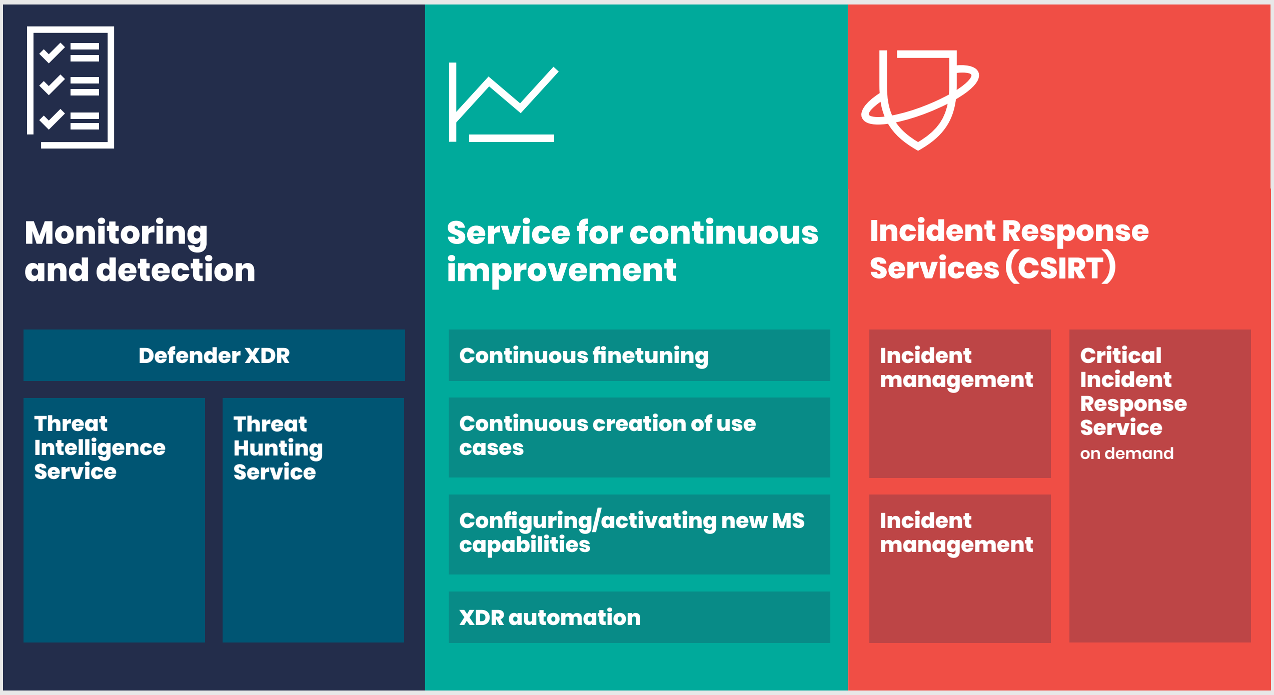
This new managed service is based on Microsoft's existing solution for extended detection and response (XDR), including the critical "Incident Response" component. Our own international **Security Operations Center (SOC)** guarantees **around-the-clock incident monitoring and response**.

At the same time, you benefit from a **local, nearby IT partner** for the actual implementation of the XDR solution – a partner who takes your broader IT environment into account. This means that you can also use this new managed service if your environment is not mainly based on Microsoft technology.

Inetum LiveSOC MDR Service

We have a **network of highly certified SOCs in three locations**. Because our SOCs operate in a coordinated manner with high availability procedures, we can guarantee the correct delivery of all our services.

Our **Managed Detection and Response (MDR)** service includes several services that complement and feed into one another.



Monitoring and detection

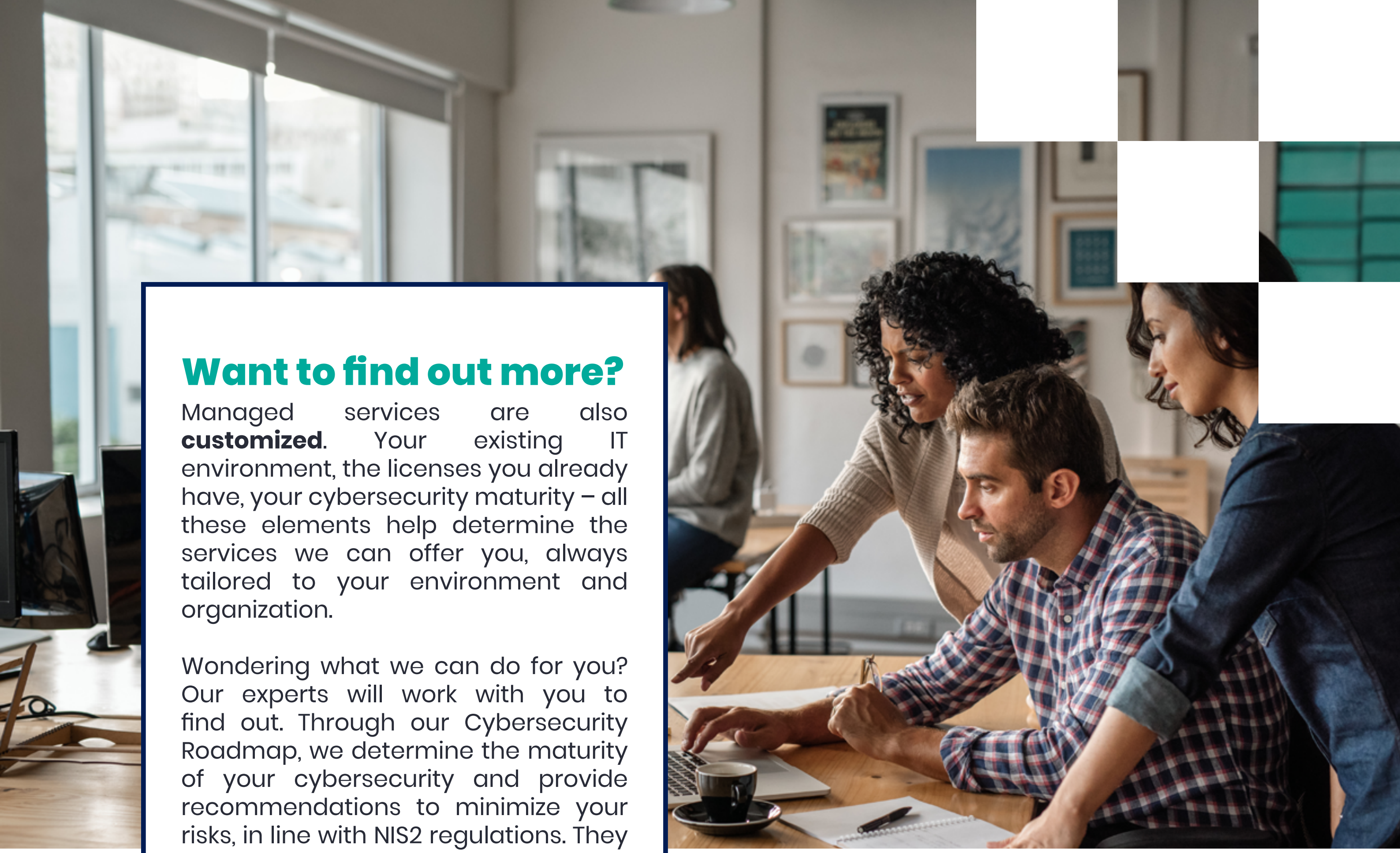
- Defender XDR
- Threat Intelligence Service
- Threat Hunting Service

Service for continuous improvement

- Continuous finetuning
- Continuous creation of use cases
- Configuring/activating new MS capabilities
- XDR automation

Incident Response Services (CSIRT)

- Incident management
- Incident management
- Critical Incident Response Service on demand



Want to find out more?

Managed services are also **customized**. Your existing IT environment, the licenses you already have, your cybersecurity maturity – all these elements help determine the services we can offer you, always tailored to your environment and organization.

Wondering what we can do for you? Our experts will work with you to find out. Through our Cybersecurity Roadmap, we determine the maturity of your cybersecurity and provide recommendations to minimize your risks, in line with NIS2 regulations. They will also be happy to inform you about other services we can offer you.

Microsoft

Inetum
Bedrijvenlaan 4
2800 Mechelen, Belgium
+32 2 801 55 55
www.inetum.com
info.belgium@inetum.com

inetum