proximus enterprise

Consulting services: Security

Microsoft Sentinel Workshop

On the way to a secure digital ecosystem

An increasing number of companies adopt a cloud-centric strategy. Security transformation is an important and often underestimated element of this shift to the cloud. As your assets are scattered across multiple environments it is important to keep a single overview of your digital estate to be able to quickly respond to the ever-growing threat landscape. Microsoft Sentinel provides this single pane of glass across your digital estate to monitor both cloud and on-premise resources. It helps to automate responses to security alerts generated by your IT landscape as it allows your security analysts to focus on what is most important.

The security challenges of your digital workplace

In the digital workplace, a growing number of cloud applications are accessible from everywhere in the world and from any device. And many times your employees use unsecured devices and networks. This is a sure way to expose your organization to new cyber threats, which traditional security methods cannot adequately protect against.

You run the risk of:

- Losing control over your security posture as resources become scattered
- Leaking sensitive company and client data by means of malware, phishing, hacking, credential theft, or human errors
- Breaching GDPR legislation
- Alert fatigue of your security analysts

Microsoft offers an ecosystem of solutions that will protect your employees, assets, and information wherever they are. However, in this fast-changing world there will always be threats that will be able to evade your protection layers. To keep pace with the threat actors, it is highly recommended to monitor all your resources and automate responses to incidents so that your security analysts can focus on what matters most.

Kickstart the security monitoring of your digital workplace

The Microsoft Sentinel Workshop gives you a **realistic and extensive overview** of:

- The **cybersecurity risks** that you are faced with **right now**
- The security **infrastructure** of your IT landscape

Microsoft Sentinel Workshop

Your Microsoft Sentinel Workshop in 5 steps

A **standard Microsoft Sentinel workshop** takes about **1 month to collect information**. During a few workshops we will work with your security team to show the capabilities and automation of Sentinel. You can supplement the assessment with extra **workshops or managed services that we tailor to your company's needs.**

THE ASSESSMENT CONSISTS OF

1. **A pre-engagement meeting**
2. **Kick-off workshop to define desired log sources and technical set-up**
3. **Collection of all data (4 weeks)**
4. **Workshop on Microsoft Sentinel – collection of findings and explanation of the capabilities to the security team**
5. **Presentation of the report and roadmap to management**

During the entire evaluation we **minimize the workload** on your security teams as much as possible, and the evaluation has absolutely no impact on your end users.

In your own Microsoft Azure environment
We only use Microsoft Sentinel to analyze your security logs and warnings. Moreover, **we process all information in your own Microsoft tenant**. This means that your data remain secure in your own environment.

Including evaluation of real security breaches
In your evaluation report, we not only evaluate your as-is cybersecurity capabilities and measures, but we also include a number of security issues that occurred at your company during the period of data collection.

After the assessment
We are also there to help after the assessment, if required, for the configuration and management of your cybersecurity roadmap.

Why Proximus?

- More than **15 years of experience in cyber security and running a security operations center**
- Experience **in all sectors**: services, industry, finance, government, ...
- A **Microsoft Gold Partner for Security**, which means that you are always guaranteed the best service and the best advice
- Advanced specialization in **Threat Protection** and **Identity and Access Management**
- Unburdening support in everything from **assessment**, **architecture**, and **implementation** up to **managed services**

Find out more?

Contact your Proximus contact person or talk to an expert:
proximus.be/securitycontact