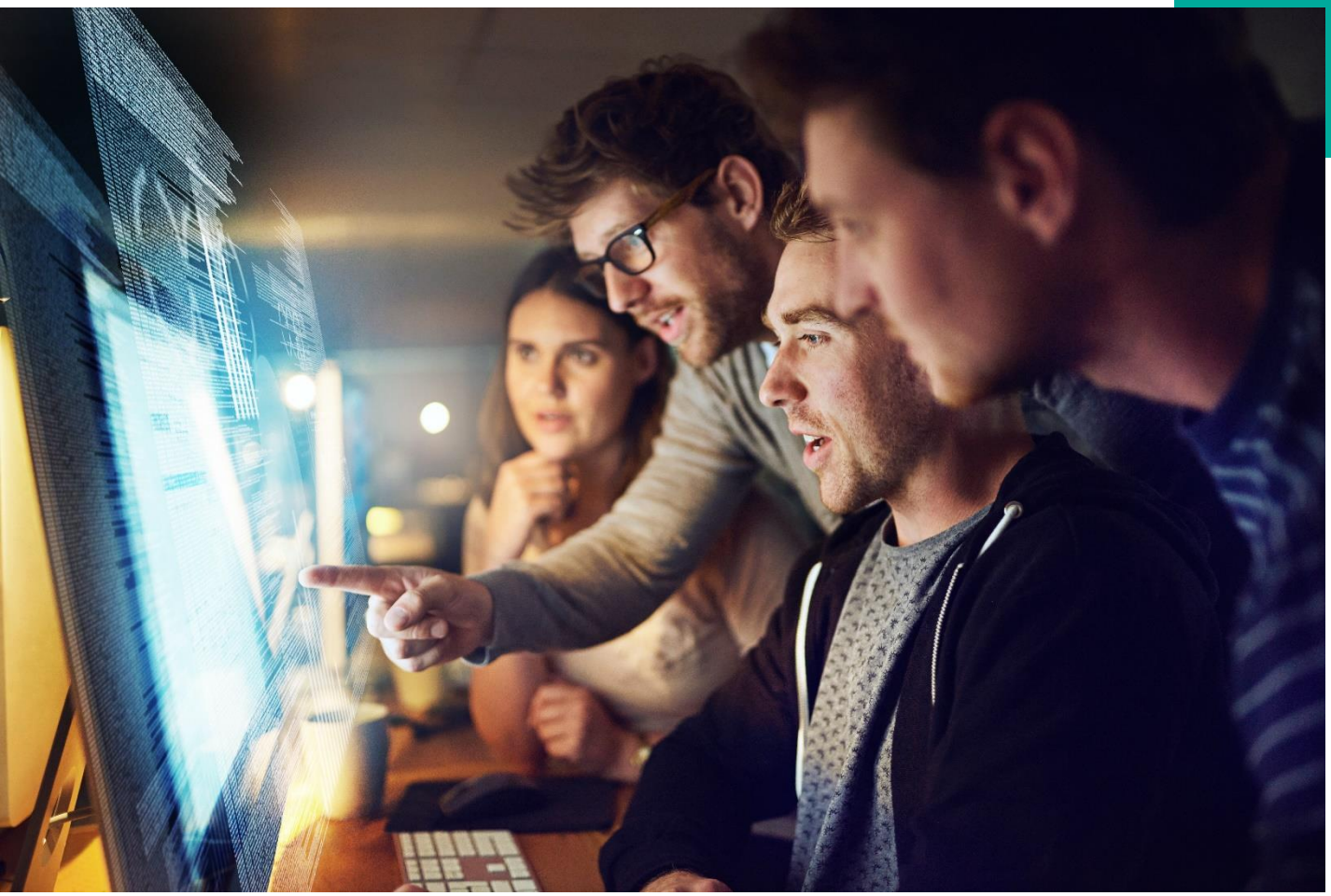


Azure Sentinel Discovery Workshop

Discover the value of Azure Sentinel

As more and more corporate data and assets are accessed from locations outside the traditional corporate network, security has become a major concern. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further. Organizations must protect themselves from these security risks through an **in-depth security strategy**.
In addition to taking those proactive measures, it is important to **constantly monitor your environment for potential security threats** and have a clear view on both what is going on in the environment and has happened in the past, thanks to a reliable audit trail.

That's where Azure Sentinel comes in.

Microsoft Azure Sentinel is a scalable, cloud-native, **Security Information Event Management (SIEM)** and **Security Orchestration, Automation and Response (SOAR)** solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.
Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

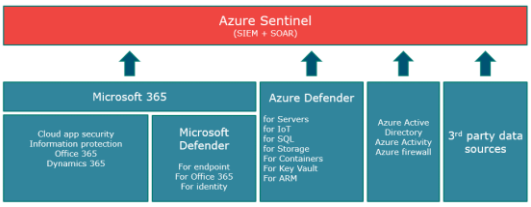
During our 5-days Azure Sentinel Discovery Workshop, our experienced consultants will inform and inspire you about the Azure Sentinel capabilities, zoom in on those features that bring value for your environment and proof the value through a Proof-of-Concept.

inetum realdolmen
Positive digital flow

Azure Sentinel Discovery Workshop
What will we cover?

Amongst others, we will cover following topics:

- Positioning of Sentinel in the Microsoft Security eco-system
- Architecture of Sentinel and overview of the Sentinel components
- How to collect data across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds?
- How to use queries and do threat hunting?
- How to make use of artificial intelligence and hunt for suspicious activities at scale?
- How to respond to incidents with built-in orchestration and automation of common tasks?
- How to get insights using standard and custom dashboards?
- How to estimate the Azure cost of a Sentinel implementation?



The Discovery Workshop consists of following steps:

Kick-off workshop
During the first day, we will position Azure Sentinel in relation to the other Security offerings like Azure Security Center.
What are their value propositions? What can you expect from Sentinel? How does it work & what is required to get started? We also discuss the current security maturity level and desired outcomes of Azure Sentinel.

Onboarding workshop
During the 2nd day of the engagement, we will onboard the relevant data sources and activate the rules that are most relevant for the environment, in line with the scope defined during the Kick-off workshop.
After the initial setup we need to let Azure Sentinel gather some data.

Analysis & finetuning
After a couple of days, we do an initial assessment to make sure data ingestion is successful for all data sources. We define an approach to avoid false positives, we discuss together on the investigation workflow and investigate what the real events uncover.

Closing workshop
We reserve the last day of the engagement to report and present the conclusions, to follow up the open questions and to present an estimation of the Azure Sentinel consumption cost. Realdolmen maps the findings to the requirements and security maturity level and makes a recommendation on how to proceed.

And afterwards?
Now that you understand the potential of Azure Sentinel, we can prepare for setting up Sentinel in production, or decide first to extend the Proof-of-Concept for other data sources.

WANT MORE INFORMATION?

Contact our experts with any questions, suggestions, or challenges.
We are looking forward to informing you about other Azure services Inetum-Realdolmen can offer.

INFO@INETUM-REALDOLMEN.WORLD

Inetum-Realdolmen HQ – A. Vaucampslaan 42, 1654 Huizingen, Belgium | +32 2 801 55 55 | info@realdolmen.com