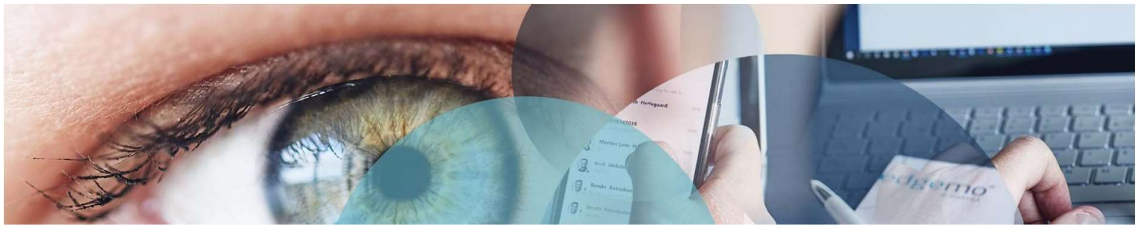
edgemo
it instinct



Get insight into all logins

Azure Sentinel gives insight into where, when and by whom your systems have been accessed and handling incidents related to possible breaches

With our Azure Sentinel workshop, in just 4 hours you will have a functional solution running – gathering telemetry from Active Directory, Azure Active Directory and Office 365.

The number of phishing attempts, brute-force attacks and similar against users and systems are rising.

Especially now when many users are working from home using Microsoft Teams, Exchange Online, VPN and a variety of filesharing services – This heightens the demands for IT-security.

Besides ensuring user identities with solutions like Conditional Access and Multifactor Authentication we should also ensure that we have **insight into all logins** on our platforms and that we **handle incidents suggesting malicious intruders**.

Azure Sentinel is built on Azure Monitor Log Analytics - an Azure service that collect and analyze telemetry from a variety of sources - both on-premise and cloud.

With Azure Sentinel you have a solution on top of Log Analytics for Detecting, Investigating and Responding to threats against your users and systems.

A good solution in just 4 hours

It does not have to be difficult – this workshop is an easy and efficient way to get started. In just 4 hours you could have a functional Azure Sentinel solution running with telemetry from Active Directory, Azure Active Directory and Office 365.

Azure Sentinel Workshop

To be able to generate incidents, Azure Sentinel needs to be connected to data sources. We start up with the most common Microsoft sources like Active Directory, Azure Active Directory and Office 365.

When these data sources have been connected to the Azure Sentinel Log Analytics workspace we can start defining the criteria for when an incident should be created – like when new Inbox Rule are created in Exchange Online – which could be a symptom of a phishing attack.

This workshop also contains a dialog of which platforms are most exposed and how can we ensure that both data and incidents reflect this.

The workshop agenda contains the following:

- Introduction to Azure Monitor Log Analytics and Azure Sentinel
- Run down of the different data sources and how to query these (using the Kusto Query Language)
- Setup of Data Connectors to Active Directory, Azure Active Directory and Office 365

- Setup of Analytics queries to generate Incidents
- Discussion on additional Data Connectors and relative Analytics to be added – like Firewall log via Syslog, Microsoft Defender ATP, Microsoft Cloud App Security or Microsoft Azure ATP.

Licensing Requirements: Office 365 Business or Enterprise. Azure subscription to Azure Sentinel can be provided by edgemo.

Technical Requirements: For on-premise (Active Directory) – the possibility of installing the Microsoft Monitoring Agent on Domain Controllers.