MDR SOC Onboarding Prerequisites

Steps required for onboarding

# About

This document details all requirements before Degea can assist with SOC onboarding.

# Licensing

For full XDR onboarding the following licenses are required:  
*All licenses are included in Microsoft 365 E5 Security addon*

Services:

* Defender for Endpoint
  + Defender for Endpoint P2
* Defender for Office
  + Defender for Office P2
* Defender for Identity
  + Defender for Identity
* Defender for Cloud Apps
  + Defender for Cloud Apps
* Entra ID Protection
  + Entra ID P2

Functionality:

* User isolation
  + Entra ID P2
  + Defender for Cloud Apps

## Services

* A dedicated pay-as-you-go Azure Subscription for Microsoft Sentinel (if Microsoft Sentinel is already in use you can use the existing setup).

# Settings

## Change subscription state to Defender for Endpoint Plan 2

Requires enough Defender for Endpoint P2 licenses to cover all endpoints. Minimum licenses are 1 license per 5 endpoints to change the licensing model. To be compliant with Microsoft’s requirements you need to have one license per workstation user.

This setting will take up to 24 hours to take effect.

<https://security.microsoft.com> 🡺Settings 🡺 Endpoints 🡺 [General] Licenses

A screenshot of a computer

AI-generated content may be incorrect.

# SOP Setup

Degea can assist with setting up according to the SOP. If all requirements above are met, we can do the entire setup for you. For a fully hands-off onboarding we will require the following:

* Global Administrator account. This is required to consent to all applications and to set up Sentinel delegation to all subscriptions.
* A contact person at the company to create a test alert. The final step before onboarding requires generating a test alert on the user’s endpoint.  
    
  One of the fall-back methods to generate an alert requires local administrator privileges, so having a way for the user to elevate to administrator is required.   
    
  E.g. LAPS password is stored in Intune, or user has a self-service way to elevate to administrator