Register Microsoft Custom Detections API access application

1. Prerequisites

- Representative with Global Administrator role access.

2. Background

Truesec SOC utilizes a multi-tenant application to manage custom detection rules in Defender XDR in our customers tenants. A consent must be made to allow the application to perform its tasks.

3. Tasks

- Visit the link and log in with an administrator account to the organization that shall consent to the application.

https://login.microsoftonline.com/common/adminconsent?client_id=5d051ad5-01ff-41de-8336-6962ea18a341

Author: Emil Norman   Date: 2024-05-15   Classification: TS Public   Version: 1.0

Truesec Detect AB

Corp ID: 559121-7046

www.truesec.com

Sweden

US

+46 810 00 10
info@truesec.se

+1 (425) 818-8044
info@truesec.com

1

- A consent dialogue like the one below (Figure 1) will appear. Click "Accept" to consent to the application.
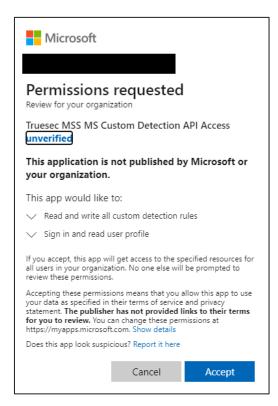

Figure 1 Consent dialogue – the logged on user's email will be shown instead of the black box.

- Visit https://portal.azure.com
- Navigate to "Enterprise applications"
- Under Overview, search for "Truesec MSS"
- Click "Truesec MSS MS Custom Detection API Access"
- Click "Properties"
- Verify that "Application ID" is "5d051ad5-01ff-41de-8336-6962ea18a341".
- Switch "Visible to users?" to "No"
- Add the following text under Notes:

  `"This application is used by Truesec SOC to manage custom detection rules in Defender XDR".`

- Click "Save"