Onboard Microsoft Sentinel

1. Prerequisites

- Representative with Global Administrator role access
- Representative with permissions required to create a sentinel workspace and connect required data sources (Owner of the relevant subscriptions)
- Correct licenses in place, also for Defender for Identity to have the separate sensor installed on all of your Domain Controllers and if applicable also on your ADFS machines.

2. General information

The subscription should reside within the tenant where the Azure services to be monitored are placed. In the special cases where no Azure services are to be connected the location is more flexible.

3. Basic flow

1. Create Sentinel Workspace
2. Set data retention period
3. Connect data sources
4. Set retention period

4. Tasks

4.1. Create Sentinel workspace

- Browse to https://portal.azure.com
- Use the search function to find “Microsoft Sentinel”
- Go to the Microsoft Sentinel pane and click “+ Create”
- Click “+ Create a new workspace”
    - This will create a new Log Analytics workspace
- Select subscription
- Create a new resource group
    - Select a name that follow the organizations naming convention. Truesec recommend that the name contain at least one of the following words: sentinel, soc or siem.
- Select a name for the instance
    - Truesec recommend putting a company name in the beginning of the name (e.g. “companyname-sentinel”)
- Select region
    - Truesec recommend “West Europe”.
- Click “Review + Create” and then “Create”
    - Use “Refresh” if the newly created workspace does not show.
- Select the workspace and click “Add”

Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

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

4.2. Set data retention period

- Go to the Microsoft Sentinel pane and click on the Sentinel workspace.
- Click “Settings” → “Workspace settings >”
- Click “Usage and estimated costs” under “General” in the menu to the left
- Click “Data retention”
- Set the data retention period to 90 days and click OK

4.3. Connect data sources

The data sources will bring in alert information and sometimes log from other services.
Note that it sometimes takes a while before the status is reported as connected after activating a data connector.

- Go to the Microsoft Sentinel pane and click on the Sentinel workspace.
- Click “Content Hub”
- This is a common baseline of services to connect. The connectors to activate can be longer or shorter depending on the set of services that the SOC shall monitor.
- Search for each connector and click “Install”. When installed, select the connector and click manage.

    - Azure Activity. Recommended but Optional Connector
        - To enable this connector, Subscription Owner is required for all relevant Subscriptions
            - Click “Launch Azure Policy Assignment wizard”
            - Select the subscription under “Scope”
            - On the “Parameters” tab, select the Log Analytics workspace to use.
            - On the “Remediation” tab, change region of the “System assigned identity location” to “West Europe”.
            - Click “Review + Create” and “Create”

    - Microsoft Entra ID
            - Sign in and Audit logs (free with E5)

    - Microsoft Defender XDR
            - Click “Connect incidents & alerts”
            - Enable “DeviceInfo” and all “Microsoft Defender for Office 365” events.
            - Click “Apply Changes”
            - This will activate several different 365 Defender suite connectors:
                - Entra Identity Protection
                - Microsoft Defender for Cloud Apps
                - Microsoft Defender for Endpoint
                - Microsoft Defender for Identity
                - Microsoft Defender for Office 365

Truesec Detect AB
Corp ID: 559121-7046
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

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