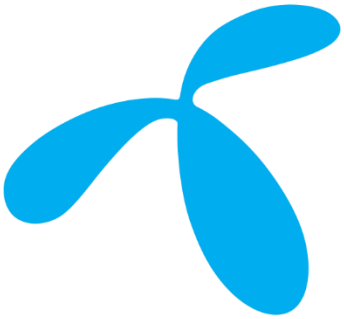
MDR for Microsoft 365

Service Description



telenor | cyberdefence

October 2024
Telenor Cyberdefence

Sensitivity: Open

Table of contents

Sensitivity: Open

1. MDR FOR MICROSOFT 365

MDR for Microsoft 365 is a 24/7-365 SOC service delivered by the providers Security Operation Centers (SOC), located in Grimstad and Oslo. We integrate with the Customer's Microsoft Defender XDR solution via Microsoft Sentinel and actively monitor and respond to security incidents.

MDR for Microsoft 365 supports the following products:

- Microsoft Defender for Endpoint Plan 2
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Entra ID Protection

The Service is continuously being developed by a team of dedicated Microsoft Security specialists in our SOC, including Security Architects and Security Analysts, with domain expertise related to the Microsoft 365 Security portfolio.

The following features are included in the service:

Feature	**Included**	**Description**
24/7-365 Monitoring	X	24/7-365 Eyes-On-Screen Monitoring by Telenor Cyberdefence SOC
24/7-365 Notification	X	Notifications regarding Security Incidents through Email, SMS, Phone and/or Security Portal. The notifications include recommended actions.
Active Response: Isolating Endpoint(s)	X	Isolating Endpoint(s) according to agreed routines
Active Response: Blocking User Account(s)	*X*	Blocking User Account(s) according to agreed routines
Bi-Directional Sync of Incidents	X	Through use of XDR Connector in Microsoft Sentinel
Customer Portal	X	Contains Case History, Escalation Paths, Contact and Notification Details, and Reports
Monthly Report	X	Contains a summary of analyzed security incidents.
Service Management	X	Dedicated Service Manager Regular status meetings where we discuss relevant incidents and potential improvements related to the service.
SLA	X	SLA is based on Incident Severity

Table 1 – Included Features

2. SYNCHRONIZATION OF SECURITY INCIDENTS

Security Events are ingested to the provider's Sentinel solution using Azure Lighthouse. We use the Defender XDR Connector to ensure that the status of all Security Events is synchronized between the Customer's environment and our own.

A dynamic ruleset developed and operated by Telenor is then applied to all Security Events that are ingested. This means that all the Security Events we receive are enriched with additional context and information which makes it easier for our Security Analysts to make an informed decision in terms of what action to take in based on the information we have available.

3. MONITORING AND RESPONSE

The provider monitors and respond to any identified Security Incidents in the customers environment 24/7/365. Microsoft 365 Security Environment 24/7/365. If the Security Event requires follow-up or is of interest for the Customer, we will always contact the Customer with information about 1) What we have found and 2) Recommended action(s)/next step(s).

We also aim to *actively respond to* cyber security threats by performing mitigating actions, namely disabling User Accounts and/or isolating Endpoints on behalf of the Customer.

In addition, we provide automated, immediate response to specific Security Incidents before manually performing in-depth analysis.

4. COMPETENCE

All the Security Analysts responsible for delivering this service are required to pass a list of requirements, including a MS SC-200 Cyber Security Operations Analyst course, before handling live customer data.

5. SERVICE MANAGEMENT

All customers have a dedicated Service Manager.

The Service Manager:

- Is the Customer's escalation point related to the service delivery
- Coordinates activities and resources in TSOC to answer questions related to the service
- Organises recurring status meeting with the Customer
- Gives risk-reducing advice to Customers to avoid that reported cyber security incidents occur again
- Makes sure the Customer handles any reported Security Events

Sensitivity: Open

6. ONBOARDING

After the contract is signed, our Onboarding team contacts the Customer and book dates for General and Technical Onboarding Meetings. After the contract is signed, our Onboarding team contacts the Customer and book dates for General and Technical Onboarding Meetings.

General Onboarding Meeting (1-1,5 hours)
A questionnaire is sent to the Customer before the meeting.

During this meeting, we will take the Customer through the onboarding process and discuss escalation routines – who to contact, when, and what kind of response are we allowed to do on the Customer's behalf.

Technical Onboarding Meeting (1-2 hours):
A technical onboarding-guide is sent to the Customer before the meeting.

In the meeting, we discuss the technical onboarding process and answer any questions the Customer might have regarding this.

If required by the Customer, Telenor Cyberdefence will remotely guide the Customer through the implementation and configuration process for an additional cost.

Service Activation Process
Once our onboarding team can see that the integration is complete, Telenor Cyberdefence starts the process with implementing you as a customer to a set of internal tools that are necessary to enable 24/7 monitoring and response.

Once this is set up, the Customer is invited to a Go-Live meeting where the Customer and Telenor Cyberdefence collectively verify that the technical setup is complete and works as intended, and to answer any questions from the Customer.

The service is now live.

The onboarding process usually takes 1-2 weeks, depending on available resources.

7. MICROSOFT LICENSING AND PRODUCT REQUIREMENTS

7.1. Microsoft 365 Licensing Requirements

The Customer must have one of the following licensing agreements from Microsoft:

- Microsoft Frontline F5 Security
- Microsoft Frontline F5 Sec + Comp
- Microsoft 365 Enterprise E3 + E5 Security
- Microsoft 365 Enterprise E5
- Microsoft 365 Education A5
- Microsoft 365 Education A5 Security
- Microsoft Defender for Endpoint Plan 2 Stand-Alone

Sensitivity: Open

7.2. Microsoft Sentinel Requirements

1. The Customer needs to set-up Microsoft Sentinel through their Azure Portal.
2. XDR Connector needs to be set-up – Only Alert/Incident Log Data is required.
3. Entra (Azure AD) Connector needs to be set-up – Sign-In Logs are required.

8. ALARM LEVELS AND NOTIFICATION METHODS

The following is an overview of alarm levels and their definition and notification method:

Alarm Level	Definition	Notification
Yellow	Endpoint(s) and/or User Account(s) may be compromised if no action is taken	According to agreed routines
Orange	Indication of an endpoint and/or a User Account is compromised	According to agreed routines
Red	Endpoint and/or User Account compromised	According to agreed routines

Tabel 1: Alarm levels, definitions, and notification methods

Alarm Level Yellow corresponds to Microsoft Alert Severity Low (Yellow)

Alarm Level Orange corresponds to Microsoft Alert Severity Medium (Orange)

Alarm Level Red corresponds to Microsoft Alert Severity High (Red)

9. SERVICE LEVEL

Severity	**Service**	**Maximum time from classification until notification and/or mitigating action has been initiated**
Red event (High)	MDR for Microsoft 365	30 minutes
Orange event (Medium)	MDR for Microsoft 365	60 minutes
Yellow event (Low)	MDR for Microsoft 365	Best effort, but no longer than 12 hours

Sensitivity: Open

10. CUSTOMER PORTAL

The Customer has access to Telenor's web-based Security Portal, which contains the following functionality:

- Security incidents
- Tickets
- Statistics
- Reports
- Contact and Notification matrix

The Customer Portal is protected by MFA.

11. CONTACT INFORMATION – SOC

Telenor Cyberdefence SOC is the Customer's contact point and is responsible for all technical and operations-related questions regarding the MDR for Microsoft 365 Service. Questions can be routed to the SOC 24x7x365.

Please mention that your question is related to the MDR for Microsoft 365 Service.

Telenor Cyberdefence SOC		

Table 3: Telenor Cyberdefence SOC – Contact Details

12. PRICING

The service has two pricing components:

- Base price per month: Fixed Monthly Price
- User price per month: Fixed Price per User per Month

Definitions:
User: The same total number of user licenses the Customer has for:

- Microsoft Frontline F5 Security
- Microsoft Frontline F5 Sec + Comp
- Microsoft 365 Enterprise E3 + E5 Security
- Microsoft 365 Enterprise E5
- Microsoft 365 Education A5
- Microsoft 365 Education A5 Security
- Microsoft Defender for Endpoint Plan 2 Stand-Alone
- Microsoft Defender for Servers P1/P2

The Customer is billed monthly according to the prices specified in the contract.

The Service Provider assumes no liability for any errors. The Service Provider reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.