## Active Response

Forced Password change

- If needed, we will force password change for users.

Disconnect active sessions and force new MFA

- We have the ability to disconnect all active sessions if the situation dictates it and force reauthentication if necessary, forcing you to log in again.

Isolate endpoint

- We can isolate endpoints if we detect suspicious activity in your systems.

Notification

- We notify in case of emergencies, notifications of what response and what the situation was.

## Service Levels

| **Managed Detection and Response from Netsecurity** | |
|---|---|
| **Service** | |
| Service time | 24/7/365 |
| Service availability (uptime during service time) | 99,5% |
| **Managed detection and response** | |
| **Guaranteed minimum time to resolution**<br>*Time from detection, through analysis/enrichment to needed response activity* | |
| • Critical detections | 30 minutes |
| • High detections | 2 hours |
| • Medium detections | 24 hours |
| • Low detections | 48 hours |
| • Informational detections | Statistics only |
| **Customer portal** | |
| Service time | 24/7/365 |
| Service availability (uptime during service time) | 99% |

## About processing of personal data (GDPR)

**The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is as follows:**
The purpose of the processing is to fulfill the agreement regarding the delivery of «managed detection and response service» on behalf of the data controller.

**Location of data processing:**
Data processing is executed in Norway

**Scope of data processing:**
Limited scope of personal data processed. The service process personal data connected to security alarms from Controllers own Microsoft 356 service.

**Data processing time:**
Data will be processed and stored for the service duration only.

**The Data Processor's processing of personal data on behalf of the Data Controller primarily involves the following (nature of the processing):**
Detection and analysis of security alarms and possible security incidents:

- Fetch security detections (alarms) from Controllers M365 enviroment
- Analyse detection/alarms
- Fetch additional information related to alarm from Controllers M365 enviroment
- Analyse alarm and set criticality
- Store data connected to alarms and analyis
- Activate technical response measures based on analysis
- The service collects data about devices (Computers, tablets etc) connected to Controllers M365 enviroment, IP adresses, names, usernames, e-mail adresses, phone numbers and activity patterns.

**The processing includes the following types of personal data about the data subjects:**
Devices (computers, phones, tablet, etc.) connected to the customer's network, IP addresses, names, usernames, e-mail adresses, phone numbers and activity patterns

**The processing includes the following categories of data subjects:**
Employees and visitors of the Controller M365 environment

**Deletion procedures regarding the processing of personal data:**
All data processed will be deleted upon service termination.