# Defendable
## MDR service

Cyber defense starts by knowing how attackers can strike by forming an understanding of the threat landscape and by knowing your own vulnerabilities.

This understanding forms the foundation for robust cyber defence.

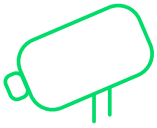
Defendable's MDR service combines cyber intelligence and vulnerability assessment to utilize as a basis for detection and response.

**The tuning and assessments made by Defendable's experienced cybersecurity team, combined with automated processes provide an optimal mix for early detection, and fast response.**

Defendable's MDR Microsoft service is a 24/7 service optimized for organizations using Microsoft products, including Sentinel.

# How it works

The MDR Microsoft 365 service is designed to be a complete cyber defense solution for organizations that primarily use Microsoft 365 and Azure to access, manage and develop their IT services.



## Defendable SOC

The heart of Defendable's MDR service is the Security Operations Centre (SOC), where security analysts are actively monitoring and responding to threats 24/7, 365 days a year.

Depending on the severity of an incident, a dedicated Incident Response analyst or an entire Incident Response Team may be mobilized to assist customers in the investigation, containment, eradication and recovery from a serious incident.

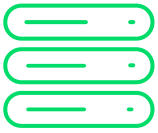
Defendable has SOCs in Oslo and Gjøvik for geo-redundancy.

## CTI

Together with vulnerability assessment, CTI is the key to achieving effective cyber defence.

Defendable monitors various open and proprietary threat intelligence feeds and utilizes these to find suspicious events and incidents on customer networks.

Defendable also extracts CTI from the dark web where leaked or stolen information is shared and traded. Dark web surveillance can give early warning of planning of attacks on a particular organisation or supply chains.



## SIEM & SOAR

Defendable converts threat intelligence and vulnerability analysis into collections of Microsoft Sentinel Security Information and Event Management (SIEM) workbooks and Security Orchestration and Automated Response (SOAR) playbooks.

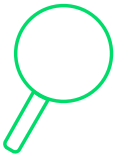
Workbooks provide our customers a high-level overview of security events and trends in the organisation, whilst playbooks trigger automated response or enrichment processes when alerts or incidents are detected.

## Vulnerability analysis

Defendable combines the functionality in Microsoft Defender and conducts regular vulnerability scanning to discover vulnerabilities in exposed services for our customers.

This activity is important to identify and close security holes before they can be exploited by threat actors.

Scanning is performed with market leading tools which are continuously updated with the latest vulnerability signatures.



## Threath hunting

In parallel with SIEM and SOAR operations, Defendable performs proactive threat hunting in customer environments.

Defendable analysts will actively look for signs of malicious activity where static detection mechanisms have not yet been developed, and have been missed by tools such as Microsoft Defender.

# Onboarding and operations

Defendable has a well-defined process for onboarding new organizations to the MDR Microsoft 365 service.

## 1. IDENTIFY

Type and number of endpoints and users that shall be monitored.

## 2. PLAN

How to monitor and perform response to incidents for the various types of endpoints and users.

## 3. ESTABLISH

Ensuring the right data is available in Defendable's MDR platform. This could for example, involve connecting your instance of Microsoft Sentinel to Defendable's MSSP tenant via Microsoft Lighthouse.

## 4. EXECUTE

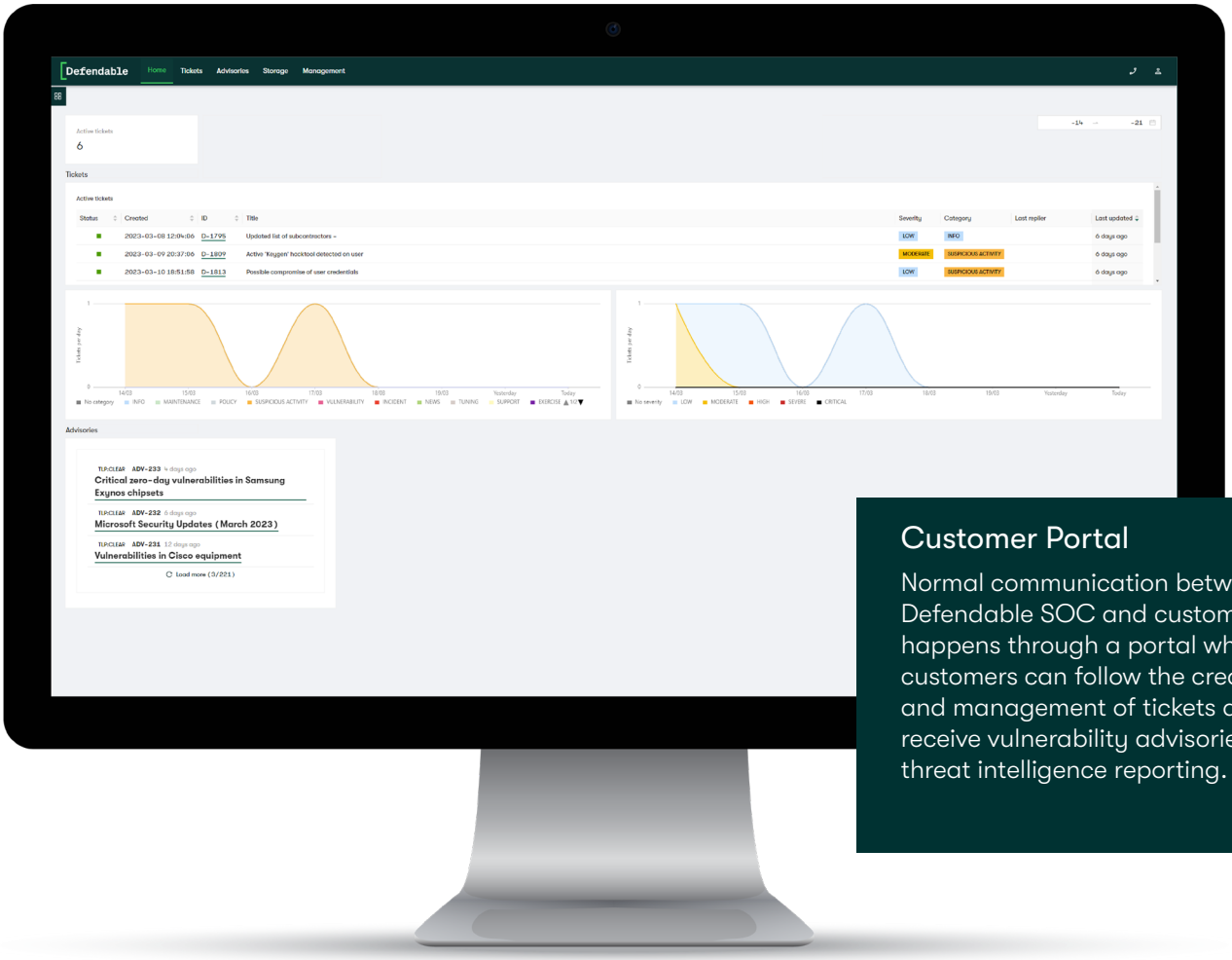
**Calibrate** the detection mechanisms for an optimal true-false positive ratio.


**Monitor 24/7** and **Threat hunt** from the SOCs in Oslo and Gjøvik.

**Analyse**, **Contain**, **Eradicate**, **Recover** and **Report** any incidents.

**Improve** detection and response mechanisms based on new threat research, intelligence and vulnerability analysis.

MDR connections can be to any device containing a compatible security agent including laptops, on-premises servers, cloud VMs, network equipment, OT and IoT devices.




## Customer Portal

Normal communication between Defendable SOC and customers happens through a portal where customers can follow the creation and management of tickets and receive vulnerability advisories and threat intelligence reporting.

# Flexible configurations and multiple options

Defendable actively encourages customers to collect and retain as much relevant security log data as possible, as more data allows us to better detect and investigate incidents. However we recognize that the collection and storage of more log data comes with an increased cost.

Customers can choose to store additional log data in their own tenant using Microsoft Log Analytics or for a more cost-efficient solution, customers can also store log data in Defendable's own log management platform.

Defendable's MDR service comprises an up to date collection of detection and response methods, which can be supplemented by working with customers on developing specific detection and response actions for particular assets, users or security scenarios.

Defendable