Today. Tomorrow. Together.

MANAGED DETECTION AND RESPONSE (MDR)

Protect your business from cyber threats

Imagine if a cyberattack could shut down your business for an entire day – what effect would that have on your business? With MDR, we make sure to minimize the risks of something happening. Our team of experts monitors around the clock and responds directly to threats, so your business keeps running no matter what security challenges you face.

itm8®

+46 40 59 24 00
information@itm8.com
itm8.se

Managed Detection and Response (MDR)

Having your own security team can be expensive and complicated, but with MDR, you get the same protection as an advanced security team – at a fraction of the cost. We monitor and respond to serious security threats, and you only pay for the peace of mind you actually need. This is a smart solution for companies that want to increase security without expensive investments.

Simple and smooth proactive response

You don't need any technical expertise – we'll take care of everything for you and give you the insights you need to keep your business safe. Automated actions to quickly respond to threats, such as isolating devices, remotely wiping data, and blocking network access.

Expert team 24/7

We monitor security events in Microsoft 365 24/7, detecting and responding quickly to threats such as ransomware, phishing, data breaches, and compromised user accounts or devices

– all in real time!

Rapid response to serious threats

We act immediately in the event of serious threats to minimize damage and stop intrusions before they escalate. With fast, automated response and effective measures, we ensure that your business continues uninterrupted, even in the event of security incidents.

Today. Tomorrow. Together.

MANAGED DETECTION AND RESPONSE (MDR)

How does Managed Detection and Response work?

With continuous monitoring and management of security alerts from Microsoft Business Premium, we ensure that potential threats are identified and remediated in real time. We respond quickly to alerts, isolate threats and protect your business around the clock, giving you peace of mind and security

itm8®

+46 40 59 24 00
information@itm8.com
itm8.se

Alert types that are handled

Devices

Malware detected on devices:
If Microsoft Defender or another security solution detects malware on a user's device, this is classified as a "high" alert, especially if it is advanced malware such as ransomware or Trojans. itm8's action: Automatic isolation if the incident is rated as "High". The client and the end user are notified that isolation has taken place.

Identities

High Risk Users:
If an account has been or is suspected to be compromised, such as if it has been used in suspicious logins or for unauthorized actions, this is classified as a serious incident. Itm8’s action: Manual assessment on the alerts that are classified as "High". If the situation requires it, itm8 locks the user's account and notifies the user and the requester.

Office 365

Suspicious bulk emails from compromised accounts:
If a user's account is used to send out large amounts of malicious email (e.g., phishing or spam), this is considered a critical alert. This indicates that the account is likely compromised and is being used to spread threats internally or externally. itm8's action: Password reset on affected account and allow the user to send emails after the incident. The end user is notified.

Users restricted from sending emails:
A user may be blocked in order to prevent them from sending emails to prevent phishing or malicious messages. itm8's action: Password reset on affected account and allow the user to send emails after the incident. The end user is notified.

Users restricted from sharing forms and collecting responses / The form itself gets blocked by suspected phishing attempt:
A user has been prevented from sharing forms, often due to suspicious phishing attempts. itm8's action: Password reset on affected account and allow the user to share forms again after the incident. The end user is notified.

A user clicked on a potentially malicious link:
This type of alert is handled automatically according to the regulations that are set up during the implementation.

Suspicious forwarding of email activity:
Emails are forwarded without the user's knowledge, often a sign of a hijacked account. itm8 action: Disable forwarding, audit the account, and reset the password if the account is compromised. Notify the end user via SMS.