CYBERSECURITY 101 · eBuilder Security

MDR

Managed detection and response is how organisations get round-the-clock threat detection without building their own security team. Here is what MDR is, why it matters and how to choose it.

WHAT IT IS

MDR, or managed detection and response, is a service where an outside team watches your systems around the clock, detects attacks and responds to them for you. It delivers the work of a security operations centre without you having to build and staff one. For most organisations, running that kind of 24-hour cover in-house is out of reach, which is why the service exists.

WHY IT MATTERS

241 days

The average time to identify and contain a breach in 2025, roughly eight months.

IBM and Ponemon, 2025

44%

Share of breaches that involved ransomware in 2025, up from 32% a year earlier.

Verizon DBIR, 2025

88%

Of organisations suffered a security problem tied to a skills gap in the past year.

ISC2, 2025

WHAT HAPPENED

In January 2024 the Akira ransomware group breached a Tietoevry data centre in Sweden and encrypted its hosting servers. Payroll and HR systems went down across most Swedish universities and more than 30 government authorities, and recovery ran into weeks. The attackers got in through an unpatched remote-access system, the kind of intrusion continuous monitoring is built to catch early. (Bloomberg, 2024)

RED FLAGS TO WATCH FOR

You have a detection gap if any of these is true, and attackers look for exactly these gaps.

- No one is watching your security alerts at night or over weekends.
- You own EDR or antivirus but no one reviews what it flags.
- You could not say how quickly a breach would be spotted and contained.
- You do not know which suppliers hold your data or how you would report a breach in time.

THE ONE RULE THAT STOPS IT

Make sure detection and response covers every hour, with a human able to act, because attacks do not wait for office hours.

THEN BUILD THE HABIT AROUND IT

- Ensure EDR or equivalent telemetry covers all laptops and servers.

- Enforce multi-factor authentication on every remote-access route.
- Patch internet-facing systems quickly, as these are common entry points.
- Agree in advance who can contain a threat, and rehearse your reporting steps.

MYTHS AND FACTS

MYTH

MDR is just antivirus with a new name.

FACT

MDR is a service, not a product. It puts human analysts on your data around the clock to investigate and respond, which tools cannot do alone.

MYTH

If we have EDR, we do not need MDR.

FACT

EDR produces the signals. MDR is the team that watches them full time and acts, and most breaches happen when no one is looking.

MYTH

MDR stops every attack.

FACT

MDR limits damage and shortens an attacker's time inside, but it is not prevention. It works alongside patching, backups and training.

THE LEGAL DUTY

Continuous monitoring and incident reporting are now legal duties under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs managed detection and response as a service for Swedish organisations. Read the full guide at the link below.

Read the Full Article →