SOC and MDR: would anyone stop an attack at 3 a.m.?

This quarter, make sure someone can contain a high-severity alert within an hour, day or night, usually by buying managed detection and response (MDR) with written authority to isolate devices and disable accounts. Judge any provider by planted tests and the alerts it closed, not by its monthly report.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.0**

Written for

IT and security leads in small and mid-size organizations, many in Germany and the EU, deciding whether to build a SOC, buy managed detection and response or combine both, and larger organizations reviewing a provider

Latest version

sheets.einblick.dev/soc-mdr/

If you only do five things

1. **Get someone on alerts around the clock.**
   In case data from MDR vendor Sophos, 88% of ransomware was deployed outside weekday business hours[1]. If nobody on your team is on call at night, buy 24/7 coverage before another tool.
2. **Authorize containment in writing.**
   Mandiant advises remediating at initial access, before hands-on attackers arrive[2]. Pre-authorize isolating devices, disabling accounts and revoking sessions, and list what needs a call.
3. **Find out what it can't see.**
   Get covered sources and severities in writing. Microsoft advises watching firewalls, VPNs, identity systems, RMM tools, email gateways and file transfer services[3]; its own MDR takes only High and Medium incidents, and none from iOS, Android, IoT, DLP or custom detections[8].
4. **Line up incident response separately.**
   Check where the service stops: Microsoft's MDR doesn't provide incident response for an active compromise[7]. Agree who takes over, and how fast, through the retainer in the incident response sheet.
5. **Test it yourself, out of hours.**
   Each quarter, plant a harmless attack on a weekend night and time it until someone calls you. Each month, read a sample of the alerts it closed as benign and check the evidence.

Build, buy or combine

1. **Who answers a high-severity alert at 3 a.m. on a Sunday?**
   If nobody does, buy 24/7 MDR. One seat staffed around the clock is 8,760 hours a year, at least five full-time people. A 24/7 SOC also loses much of its value if the IT teams it needs work 9 to 5 with no on-call, the NCSC notes[4].
2. **Do you have staff who know your systems?**
   Then combine. Let the provider take nights, weekends and first triage, and keep tuning, context and business decisions in-house. In-house teams have better business context, and most SOCs outsource some functions[4].
3. **Which detection tools do you already run?**
   Buy MDR for the EDR or XDR you have, so the provider can act inside it, rather than adding a second agent.
4. **Does anything force you to build?**
   Build only for what no provider covers well, such as OT or in-house applications. Even KRITIS detection doesn't need your own staff: the BSI accepts named staff of a service provider[13].
5. **Can the provider show its own security?**
   Ask for its ISO 27001 scope and latest audit report. A managed security services provider based in Germany with 50 or more staff, or turnover and balance sheet above €10 million each, is itself at least an important entity under the BSIG[14].

Contract terms that matter

Add these to the five clauses in the supplier risk sheet.

- **Times from alert to containment.** In the NCSC's guide to choosing an IT provider, response time ends when work starts, and under an hour is standard for urgent issues[6]. For High severity, ask for work within 15 minutes and containment or a call within 60, from alert creation.
- **A fallback when nobody answers.** Sophos, for one, offers to act on its own once it has phoned all your contacts without reply[11]. Agree the actions, exclusions and wait.
- **Data location.** Defender Experts keeps case notes in the EU only for tenants in the EU Data Boundary[9]. Require notice before locations change.
- **Your own logs.** Keep 12 months yourself, as in the logging sheet. Firewall log defaults of 7 days left gaps in Sophos's cases[1].
- **Exit.** Export case history and rules written for you first: Defender Experts deletes its data within 30 days of termination[9].
- **Its access to your tenant.** Require time-limited roles, used from managed devices with MFA and logged in your sign-in logs, as Microsoft sets up for its experts[10].

Onboard and tune

1. **Hunt before you baseline.**
   Ask for a compromise check first: a baseline taken on a compromised system includes the attacker, the NCSC warns[5].
2. **Hand over your context.**
   List critical systems, VPN ranges, service accounts and scheduled admin jobs: Microsoft says baselines like these let detections suppress noise[3]. In Germany, agree the scope with the works council, which co-determines tools able to monitor staff[15,16].
3. **Turn on what lets it act.**
   Run your EDR in active mode: with Defender in passive mode, Microsoft's experts may only be able to advise[9].
4. **Tune with end dates, and hunt.**
   Give each suppression an expiry date[5] and an owner, and report new systems so the provider recalibrates[13]. Mandiant advises routine hunting beyond alerts[2]: ask each quarter what was hunted and found.

How to tell whether it works

- **Plant a test each quarter.** Out of hours, on a test machine or mailbox, add a local admin, install an unapproved remote tool or forward mail outside. Agree the window with one contact at the provider, not its analysts. Microsoft counts an unsanctioned RMM agent among the most reliable signs of a hands-on attacker[3].
- **Purple team once a year.** Testers and the provider replay techniques and fix gaps as they go[5]; see the penetration testing sheet.
- **Sample what it closed.** Each month, read 10 incidents closed as false positives and check the evidence. Microsoft's MDR triages with AI that analysts validate[8].
- **Ask for outcomes, not alert counts.** Time to triage, time to containment and how long incidents waited for you. Microsoft says alert counts no longer measure a SOC's maturity[3].

What you can skip

- **A SIEM before MDR.** An MDR can work in the XDR you run; Microsoft's Defender Experts Plan 1 needs no Sentinel[8]. Not for KRITIS: the BSI expects all logs correlated centrally[13].
- **Long RFP questionnaires.** A planted test in the trial tells you more than 300 answers.
- **Analyst rankings and feature counts.** They describe other networks; a timed test in yours decides.
- **Your own 24/7 shift below enterprise size.** Five people per seat buy one pair of eyes. Use them for context and response.

What changed in 2026

- **Hand-offs take seconds.** Mandiant's median from initial access to a second group fell to 22 seconds, from over 8 hours in 2022. It advises treating routine malware alerts as high priority[2].
- **AI agents now investigate incidents.** Microsoft says its own security team has custom AI agents autonomously investigate 75% of incoming incidents[3]. Ask your provider which closures no analyst saw.
- **An EU certificate is in draft.** ENISA's July 2026 draft scheme for managed security services covers only incident response so far[17]. Don't wait for it to choose an MDR provider.
- **Microsoft's MDR dropped third-party network enrichment from Plan 1.** It was deprecated on 1 September 2026 and ends at your renewal; Plan 2, from 1,500 seats, covers some non-Microsoft sources through Sentinel[7].

Mistakes that cost the most

- **Leaving the provider on notify-only.** It can then only watch. Sophos advises against its notify-only mode for long[11].
- **Contacts who sleep through the call.** Test the phone chain with every planted test, and name a deputy.
- **Coverage nobody checks.** Compare the provider's device count with your inventory monthly. A laptop without EDR is invisible to it.
- **Standing admin rights for the provider.** Use time-limited roles[10] and remove partner roles you don't need, as in the supplier risk sheet.

What this looks like at your size

Small team, no security staff

- Buy MDR for the EDR you already run, with authority to isolate devices and disable accounts.
- Check the license first: Microsoft's MDR covers Defender for Endpoint Plan 2 but doesn't list Defender for Business, and works only in English[9].
- Give the provider two night contacts and your IT firm's emergency number.
- Time a planted test on a spare laptop.

Growing, with IT or security staff

- Co-manage: the provider takes nights, weekends and first triage; your team keeps tuning and daytime response.
- Add identity, email and firewall or VPN sources, and review 10 closed incidents a month.
- Pick a retainer firm that knows your MDR provider. In Germany, the BSI's list for KRITIS operators names 64 qualified APT response firms[12].

Enterprise or regulated

- Run a yearly purple team with the provider and track each missed technique to closure.
- KRITIS operators must run attack detection (BSIG § 31(2))[14]; the BSI expects automatic response where it can't endanger the critical service[13].
- Under NIS2 or DORA, require notice fast enough for the EU security laws sheet's clocks, and use the supplier risk sheet's clauses.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which tied coverage and licensing claims to Microsoft's and Sophos's own documentation, added the Federal Labour Court ruling on monitoring tools and limited KRITIS points to KRITIS operators.

Sources

1. Active Adversary Report 2026 (vendor case data). Sophos, 24 Feb 2026. sophos.com
2. M-Trends 2026 Executive Edition. Google Cloud (Mandiant), Mar 2026. services.google.com
3. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
4. Building a SOC: Designing an operating model. NCSC (UK), 23 May 2022. ncsc.gov.uk
5. Building a SOC: Detection practices. NCSC (UK), 23 May 2022. ncsc.gov.uk
6. Choosing a managed service provider (MSP). NCSC (UK), 24 Nov 2025. ncsc.gov.uk
7. What is Microsoft Defender Experts MDR. Microsoft Learn, 7 Aug 2026. learn.microsoft.com
8. General information on Defender Experts MDR service. Microsoft Learn, 7 Aug 2026. learn.microsoft.com
9. Before you begin using Defender Experts MDR. Microsoft Learn, 1 Sep 2026. learn.microsoft.com
10. How Microsoft Defender Experts permissions work. Microsoft Learn, 1 Jul 2026. learn.microsoft.com
11. MDR threat response. Sophos Docs, 14 Sep 2026. docs.sophos.com
12. Qualifizierte APT-Response-Dienstleister. BSI, 1 Jun 2026. bsi.bund.de
13. Orientierungshilfe Angriffserkennung, version 1.1. BSI, 18 Nov 2024. bsi.bund.de
14. BSIG, §§ 2, 28 and 31 and Annex 1. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de
15. BetrVG, § 87. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de
16. Decision 1 ABR 7/15 (co-determination over monitoring devices). Federal Labour Court (Germany), 13 Dec 2016. bundesarbeitsgericht.de
17. Have your say on the certification of EU Managed Security Services. ENISA, 24 Jul 2026. certification.enisa.europa.eu