

We keep watch while you run the business

24/7 monitoring. We spot suspicious activity early, validate what matters, and escalate with clear next steps.

Most monitoring services sell alerts, not answers

A service that forwards everything it sees is not monitoring. It is a second inbox. Your team still has to work out what is real, what matters, and what to do about it, usually at the least convenient hour.

We investigate before we escalate. What reaches you has already been validated, given context, and paired with a recommendation. Detections are tuned to your environment and keep improving, so signal quality rises over time rather than decaying into background noise.

10 billion events a day.

That is what our SOC processes. You hear about almost none of them.

What you are actually signing up for

Sources we watch. Endpoint telemetry, identity logs, cloud signals, and network or firewall logs where available. Exact sources agreed during onboarding.

Infrastructure agnostic. Single cloud, multi-cloud, hybrid, or on-premises. We work with what you have rather than asking you to move.

Distributed operations. SOC operations run from Iceland and Poland, bringing together wider operational experience and regional threat intelligence.

Tuned to you. Detections are built for your environment during onboarding and refined continuously afterwards.

Documented for auditors. Escalation paths and regular reporting produce the evidence regulated organisations need.

What you get

- 01 Continuous monitoring.** Endpoints, identity, cloud, and network signals watched around the clock across agreed sources.
- 02 Clean triage.** We investigate enough to separate noise from real threats, with context attached.
- 03 Clear escalation.** What happened, what it means, and what to do next.
- 04 Detection tuning.** Ongoing tuning so signal quality keeps improving rather than decaying.
- 05 Regular reporting.** Documented monitoring and escalation, ready for auditors.

Who it is for

Teams building response.

Always-on visibility while you grow internal capability.

Lean security teams.

Coverage outside business hours without hiring a night shift.

Regulated organisations.

Demonstrable monitoring and escalation for auditors.

From onboarding sources to actionable escalation

01	02	03	04
Onboard. Connect agreed log sources across endpoint, identity, cloud, and network.	Monitor. Watch around the clock, with detections tuned to your environment.	Triage. Separate noise from real threats and gather the context that matters.	Escalate. Hand you a clear summary and next steps, then refine detections over time.

Why Syndis

Based in Iceland, Sweden, and Poland. Serving clients globally.

Our analysts hold offensive certifications alongside defensive ones, which means the people watching your environment know how attacks are actually built, not just how they appear in a console. Detection and response sits alongside advisory, offensive testing, and training under one contract.

CISSP

GCFA

CISM

OSCP

SC-200

CySA+

Get always-on visibility

Tell us your environment and sources. We come back with a monitoring plan. We respond to most inquiries within one business day.

■ syndis@syndis.com | Get a quote: syndis.com/soc-quote

