CYBERSECURITY 101 · eBuilder Security

SOC

A Security Operations Centre is the people, process and technology that watch your systems for cyber threats around the clock. Here is what a SOC does and why it matters.

WHAT IT IS

A SOC is the combination of people, process and technology that monitors your systems for threats around the clock, then detects, investigates and contains incidents. It is a function, not a room, so it can be run in-house, shared with a provider or bought as a service.

WHY IT MATTERS

44%

of breaches involved ransomware, the year's top attack type

Verizon DBIR, 2025

4.8 million

unfilled cybersecurity roles worldwide, so most teams cannot watch everything

ISC2, 2024

4 in 5

SOCs run around the clock, yet the typical SOC is only 2 to 10 people

SANS Institute, 2024

WHAT HAPPENED

In August 2025 ransomware at Miljödata, a Swedish HR software supplier used by about 80% of the country's municipalities, disrupted 164 municipalities and four regions. Data on more than a million Swedes was later published on the dark web. (The Record and Swedish authorities, 2025)

RED FLAGS TO WATCH FOR

You may have a monitoring gap if any of these are true.

- Your last incident was found by a customer or by luck rather than your own monitoring
- Alerts pile up unreviewed overnight and at weekends
- No one can tell you your mean time to detect or respond
- You own security tools but no one is correlating what they report
- You collect logs but no one is watching them in real time

THE ONE RULE THAT STOPS IT

Make sure someone or something is watching your systems around the clock, because you cannot report or contain an attack you never detect.

THEN BUILD THE HABIT AROUND IT

- Match your coverage to your reporting deadlines, including the 24-hour NIS2 clock
- Measure mean time to detect and mean time to respond, and drive both down

- Extend monitoring to suppliers and cloud, then rehearse the response

MYTHS AND FACTS

MYTH

A SOC is a room full of screens.

FACT

A SOC is a function. It can be an in-house team, a virtual team or an outsourced service.

MYTH

A SIEM or an EDR is a SOC.

FACT

Tools collect data but do not investigate or respond. Without people and a process they just add alerts.

MYTH

Only large enterprises need a SOC.

FACT

Smaller firms are targeted too. Ransomware featured in 88% of breaches at small and mid-sized firms in 2025 (Verizon).

THE LEGAL DUTY

Cybersäkerhetslagen, in force since 15 January 2026, brings NIS2 into Swedish law. Significant incidents must reach MCF within 24 hours of detection, then 72 hours and one month. Continuous monitoring is what makes those deadlines achievable.

GET HELP

See how a Sweden-based SOC could cover your systems around the clock.

Read the Full Article →