

AI SIEM

An AI SIEM adds machine learning and behavioural analytics to a traditional SIEM. Here is what it actually improves, where it still needs people and what it means under NIS2.

WHAT IT IS

An AI SIEM is a security information and event management platform that collects and correlates log data, then uses machine learning to score anomalies and cut alert noise. It does not replace analysts. It ranks and enriches alerts so a smaller team can find the threats that fixed rules miss, and act on them faster.

WHY IT MATTERS

4.8 million

The shortfall of cybersecurity professionals worldwide, the gap AI in the SOC is meant to help close.

ISC2, 2024

76 days

How long the Equifax breach went undetected after a monitoring sensor's certificate had lapsed.

US GAO, 2018

Four months

How long the Capital One breach ran before an outside tip, not its own monitoring, surfaced it.

US OCC, 2020

WHAT HAPPENED

In late 2013 attackers stole about 40 million payment card records from the US retailer Target. Target's own malware detection flagged the exfiltration tool and raised alerts, but staff saw them and did not escalate. The technology worked and the response did not. (US Senate, 2014)

RED FLAGS TO WATCH FOR

The warning signs show up in how your team already works.

- Analysts ignore most alerts because almost all of them are noise.
- A log source could go quiet for days and no one would notice.
- You would most likely hear about a breach from someone outside.
- When a tool flags something, no one can explain why it fired.
- Detection is all fixed rules, so anything new slips through.

THE ONE RULE THAT STOPS IT

An alert only matters if someone acts on it. Make sure the few that matter reach a person who will, and that no source has quietly gone dark.

THEN BUILD THE HABIT AROUND IT

- Rank and correlate alerts so the real incident is not buried.

- Alert on silent or missing log sources, as well as on events.
- Baseline normal user and service-account behaviour, then flag deviations.
- Confirm where your logs are processed and who can be compelled to access them.

MYTHS AND FACTS

MYTH

An AI SIEM replaces your analysts.

FACT

It automates triage and correlation so analysts work the real incidents. A person still decides and responds.

MYTH

Buy it and you are protected.

FACT

It only sees what you feed it. Equifax had monitoring, but a blind sensor hid a breach for 76 days.

MYTH

Location does not matter if data stays in the EU.

FACT

Under Schrems II and the US CLOUD Act, a provider under foreign law can be compelled to hand over EU-stored data.

THE LEGAL DUTY

Continuous monitoring and incident reporting are legal duties under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with 24-hour and 72-hour reporting to MCF (formerly MSB) and boards personally accountable under Article 20.

GET HELP

eBuilder Security runs detection and response so the alerts that matter reach an analyst who acts. Read the full guide at the link below.

[Read the Full Article →](#)