CYBERSECURITY 101 · eBuilder Security

AI-Native XDR

What AI XDR is, where it helps and where a human still decides, for Swedish organisations.

WHAT IT IS

AI-native XDR, or AI XDR, is extended detection and response built with machine learning at its core. It pulls signals from across endpoints, networks, identity, cloud and email, correlates them into one attack picture and speeds up investigation and response. It matters because most attacks now cross several systems, and tools that watch only one leave a blind spot at the seams.

WHY IT MATTERS

USD 5.05M

average cost of a breach that spans multiple environments, the most expensive kind

IBM Cost of a Data Breach Report, 2025

USD 1.9M

average saving per breach for organisations using AI and automation extensively in security operations

IBM Cost of a Data Breach Report, 2025

241 days

global average time to identify and contain a breach, a nine-year low

IBM Cost of a Data Breach Report, 2025

WHAT HAPPENED

In September 2023 the group known as Scattered Spider phoned MGM Resorts' IT help desk posing as an employee and had an account reset. That one call led to administrator access across Okta and Azure and the encryption of more than 100 virtual hosts. MGM's filing with the US Securities and Exchange Commission put the impact at about USD 100 million.

RED FLAGS TO WATCH FOR

The recent ransomware cases shared the same opening moves. Watch for:

- A help desk asked to reset a password or MFA under time pressure
- A privileged account reset, then a login from an unusual place
- Separate tools each showing a small anomaly that no one links together
- A vendor promising a fully autonomous SOC with zero false positives

THE ONE RULE THAT STOPS IT

Verify identity through a separate trusted channel before any help-desk password or MFA reset.

THEN BUILD THE HABIT AROUND IT

- Correlate identity, endpoint and cloud signals so one attack raises one alert, not three
- Require phishing-resistant MFA on every external-facing portal
- Keep a human in the loop for high-impact automated actions

MYTHS AND FACTS

MYTH

AI XDR replaces your security team.

FACT

No production platform runs a fully autonomous SOC. It handles triage and routine response while a human owns the high-impact calls.

MYTH

If a product says AI, the detection is AI-native.

FACT

Many tools add machine learning onto an old rules engine. AI-native means the detection core itself is the model on unified data.

MYTH

AI XDR removes false positives.

FACT

Anomaly detection trades false positives against false negatives. Good AI XDR cuts the noise but no system reaches zero.

THE LEGAL DUTY

In Sweden, Cybersäkerhetslagen (SFS 2025:1506, in force 15 January 2026) requires continuous monitoring under NIS2 Article 21.2a, with an early warning to MCF (formerly MSB) within 24 hours of a significant incident, a full notification within 72 hours and a final report within one month.

GET HELP

Talk to eBuilder Security about detection and response for Swedish organisations.

Read the Full Article →