

Cyber Response Index

Q3 2026 · July – September — Solvane Énergies

NO. 7 · Q3 2026

CONFIDENTIAL

EFFECTIVENESS INDEX

78 / 100

LEVEL: CONTROLLED

VS PREVIOUS QUARTER

+6 pts

Q2 2026: 72 / 100

OVER ROLLING 12 MONTHS

+14 pts

Q3 2025: 64 / 100

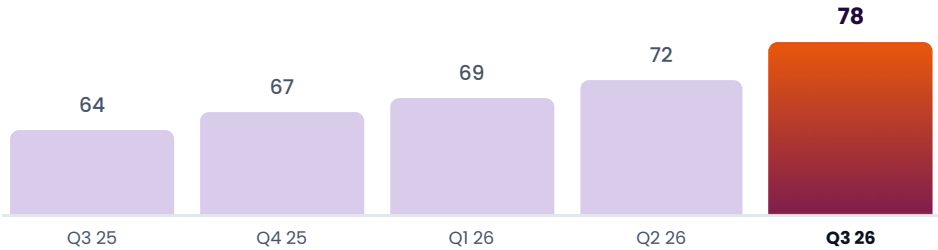
PREPARED FOR

 SOLVANE ÉNERGIES

Mock-up — fictitious data. Identical calculation method from one quarter to the next.

Your ability to detect and stop attacks has improved for the **fourth consecutive quarter**.

>_ Index trend



>_ Operational indicators

84 %

of attacks detected

MTTD 6 min

61 %

of attacks blocked

MTTR 17 min

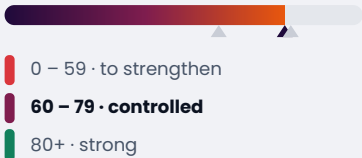
2 h 40

median response time

9

blind spots fixed this quarter

>_ READING THE INDEX



>_ REPORT DATA

Report	No. 7
Period	Q3 2026
Campaigns	3
Scenarios	38
Scope	Endpoints, servers, email, AD, AI

>_ Three key findings

1

Monitoring gap on AI infrastructure **NEW**

NOT MONITORED

Malicious requests sent to the internal AI assistant and its servers (prompt injection, data extraction) raised no alert: these components forward no logs to the SOC.

2

Lateral movement

DETECTED, SLOW RESPONSE

An attacker hopping from one machine to another is spotted, but alerts take more than 4 hours to be handled.

3

Data leakage

NOT DETECTED

Uploading files to an online storage service triggered no alert.

>_ Three matching recommendations

1

Connect AI platforms to the SOC

Collect AI gateway and server logs in the SIEM, then enable dedicated detection rules.

Owner: SOC and data / AI team

2

Set a target response time

Agree with the SOC on a procedure and a one-hour response time for these alerts.

Owner: SOC

3

Monitor outbound traffic

Enable a detection rule on abnormal outbound upload volumes.

Owner: SOC and network

Tested scope: 3 campaigns, 38 scenarios — endpoints, servers, email, Active Directory and AI infrastructure. Identical calculation method from one quarter to the next. Mock-up — fictitious data.