

Cyber Response Index

T3 2026 · juillet – septembre – Solvane Énergies

N°7 · T3 2026

CONFIDENTIEL

INDICE D'EFFICACITÉ

78 / 100

NIVEAU : MAÎTRISÉ

VS TRIMESTRE PRÉCÉDENT

+6 pts

T2 2026 : 72 / 100

SUR 12 MOIS GLISSANTS

+14 pts

T3 2025 : 64 / 100

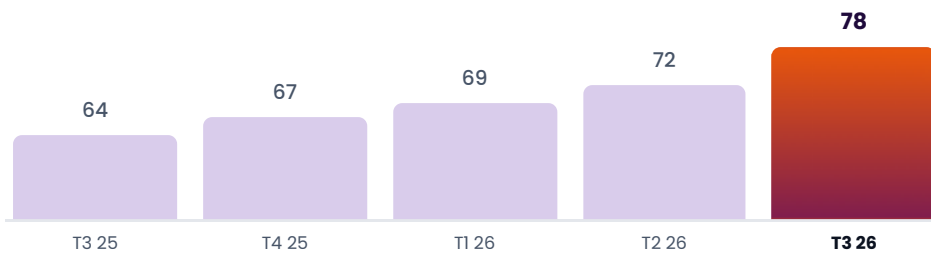
PRÉPARÉ POUR

SOLVANE
ÉNERGIES

Maquette — données fictives. Méthode de calcul identique d'un trimestre à l'autre.

Votre capacité à détecter et à stopper les attaques progresse pour le **quatrième trimestre consécutif**.

> _ Évolution de l'indice



> _ LECTURE DE L'INDICE



0 – 59 · à renforcer

60 – 79 · maîtrisé

80+ · solide

> _ DONNÉES DU RAPPORT

Rapport	N°7
Période	T3 2026
Campagnes	3
Scénarios	38
Périmètre	Postes, serveurs, messagerie, AD, IA

> _ Indicateurs opérationnels

84 %

des attaques
détectées

MTTD 6 min

61 %

des attaques
bloquées

MTTR 17 min

2 h 40

délai médian de
réaction

9

blind spots corrigés
ce trimestre

> _ Trois constats principaux

1 Défaut de surveillance sur les infrastructures
IA **NOUVEAU**

NON SURVEILLÉ

Les requêtes malveillantes adressées à l'assistant IA interne et à ses serveurs (injection de consignes, extraction de données) n'ont généré aucune alerte : ces briques ne remontent aucun journal au SOC.

2 Propagation interne

DÉTECTÉE, PEU TRAITÉE

Un attaquant qui rebondit d'une machine à l'autre est repéré, mais les alertes sont traitées en plus de 4 heures.

3 Fuite de données

NON DÉTECTÉE

L'envoi de fichiers vers un service de stockage en ligne n'a déclenché aucune alerte.

> _ Trois recommandations associées

1 Raccorder les plateformes IA au SOC

Collecter dans le SIEM les journaux des passerelles et serveurs IA, puis activer des règles de détection dédiées.

Porteur : SOC et équipe data / IA

2 Fixer un délai de réponse cible

Définir avec le SOC une procédure et un délai d'une heure pour ces alertes.

Porteur : SOC

3 Surveiller les flux sortants

Activer une règle de détection sur les volumes d'envoi anormaux vers l'extérieur.

Porteur : SOC et réseau

Périmètre testé : 3 campagnes, 38 scénarios — postes de travail, serveurs, messagerie, Active Directory et infrastructures IA. Méthode de calcul identique d'un trimestre à l'autre.
Maquette — données fictives.

Confidentiel · COMEX · Rapport trimestriel · Cyber Response Index N°7 · page 1/1