cybershen

WHEN CYBERSHEN & BITRUSTEE MEET · ZTUP
ZERO-TRUST UNIFIED PLATFORM

Le Zero Trust à l'épreuve de l'IA

Une attaque pilotée par l'IA, six gestes, trois piliers.



LE CONSTAT

L’IA : une menace protéiforme

80–90 %

d’une campagne d’espionnage exécutée par une IA, presque sans intervention humaine.

ANTHROPIC, NOV. 2025 — GTG-1002

25 M$

virés après une visioconférence où tous les interlocuteurs étaient des deepfakes.

ARUP, HONG KONG, 2024

En 20 jours

trois fuites de code source et de notes internes, collées dans un chatbot public.

SAMSUNG, 2023

LE CŒUR DE L'APPROCHE

Supprimer les conditions de l'attaque

L'IA attaque en minutes. Plutôt que d'accélérer la réponse (ce qui a plusieurs limites), nous supprimons ce qui la rend possible.

SUPPRIMER LES CONDITIONS

Durcir en profondeur

On retire à l'attaque ce dont elle a besoin : surface fermée, configuration durcie, privilège retiré.

AUCUNE FENÊTRE OUVERTE

Tout verrouiller – Partout!

Une fenêtre oubliée suffit. On les traite toutes, dans un même cadre, et ce qui n'est pas permis reste fermé.

PERMETTRE ET CONTENIR

Maîtriser les usages

L'IA entre aussi par nos propres usages. Les permettre, les tracer et les maitriser est nécessaire pour ne pas les subir.



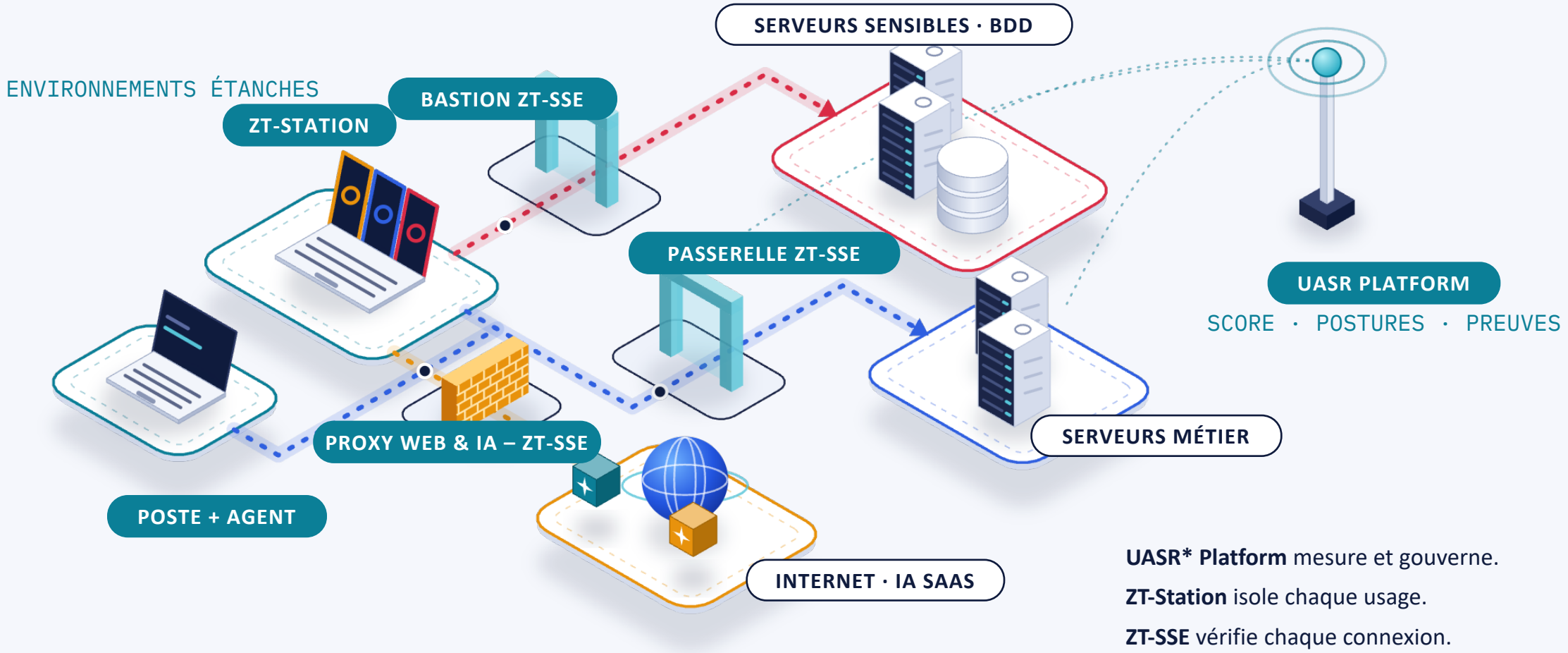




cybershen

ZTUP EN UNE IMAGE

Trois piliers, une seule boucle



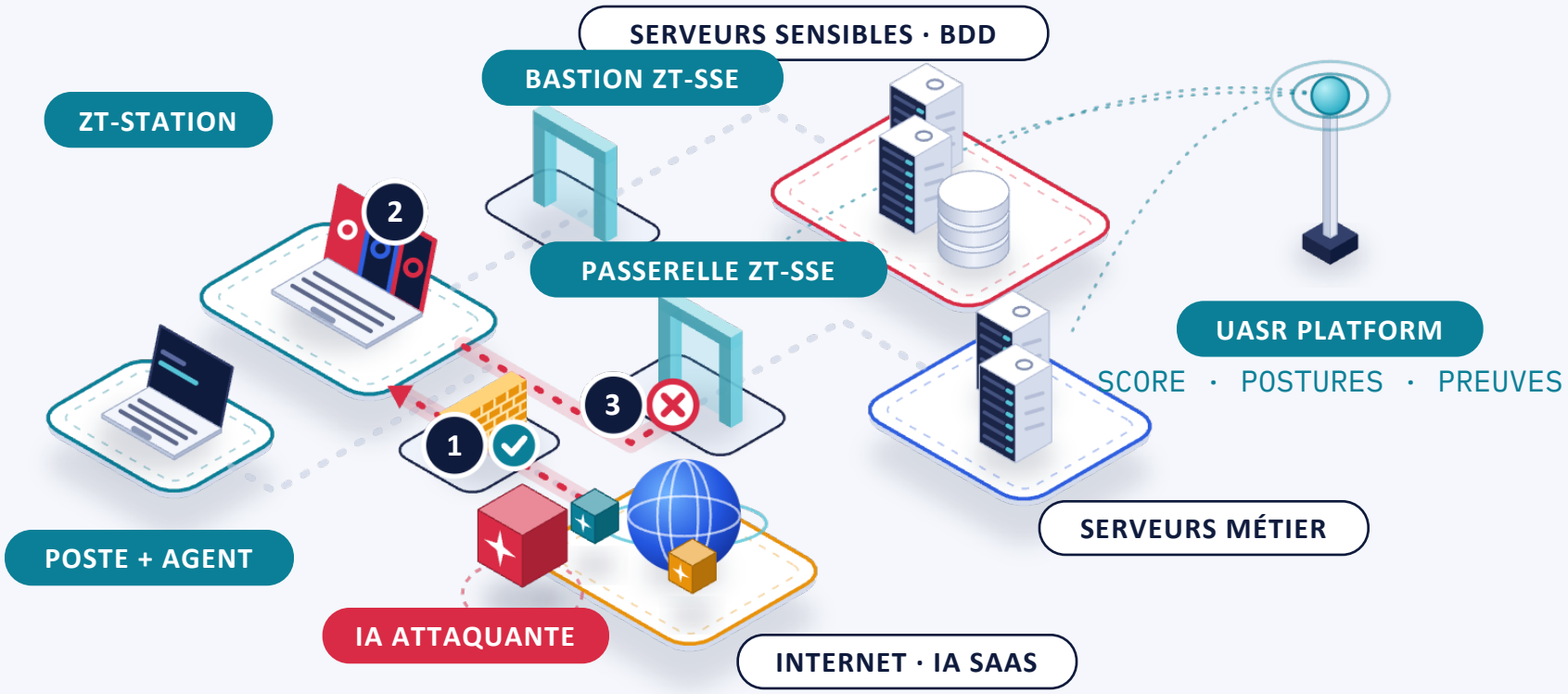
UASR* Platform mesure et gouverne.

ZT-Station isole chaque usage.

ZT-SSE vérifie chaque connexion.

LE SCÉNARIO · 1/2

L’attaque entre



1 Reconnaissance

Elle scanne votre surface. La gestion de la surface externe l’avait déjà refermée.

UASR PLATFORM

2 Hameçonnage

Le piège s’ouvre dans l’environnement bureautique, et nulle part ailleurs.

ZT-STATION

3 Rebond

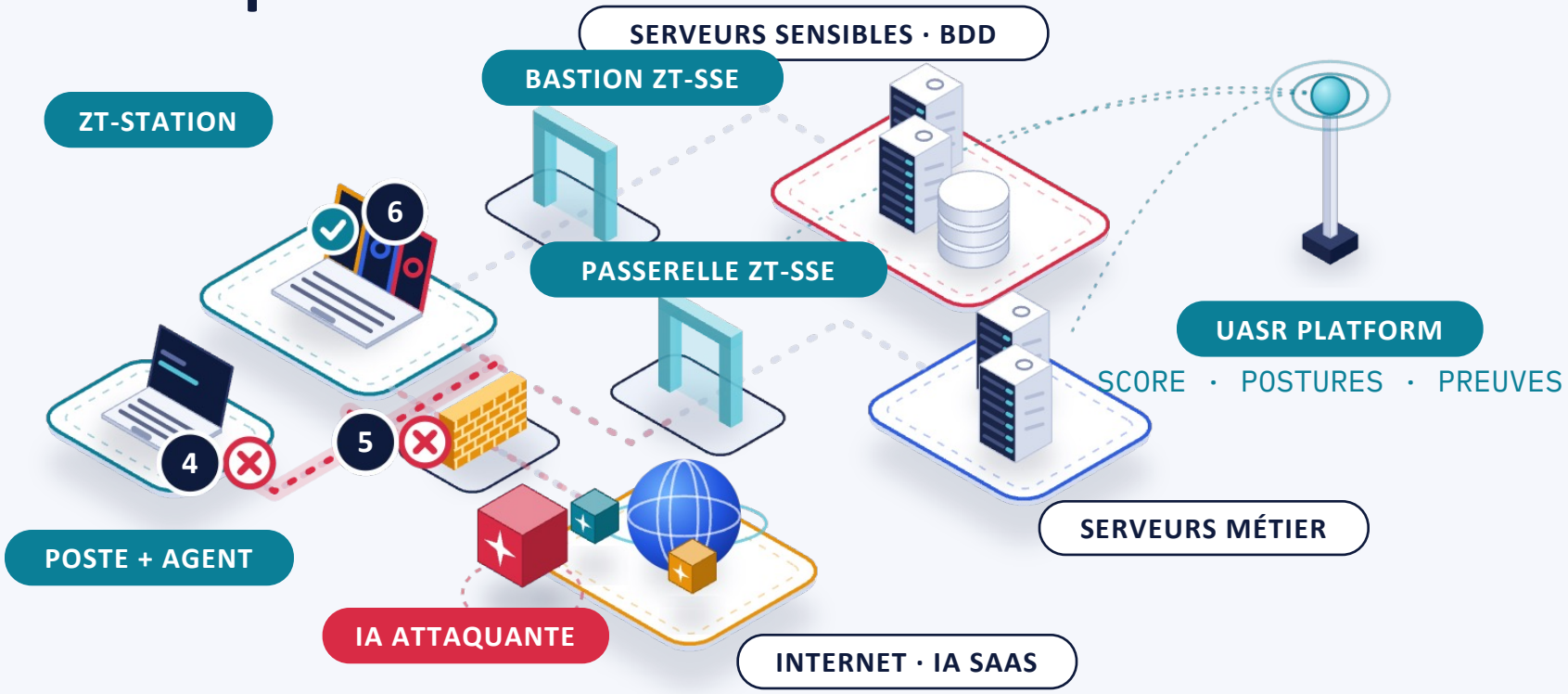
Appareil inconnu/action non autorisée, aucune règle explicite : la passerelle refuse.

ZT-SSE

cybershen

LE SCÉNARIO · 2/2

L’attaque n’avance pas



4 Propagation

Parc durci, chaque machine notée : plus rien à enchaîner.

UASR PLATFORM

5 Exfiltration

Le canal sort vers une IA publique. Bloqué au proxy.

ZT-SSE

6 Reprise

Environnement réinitialisée, et toute l’histoire dans la prevue (forensic).

ZT-STATION

cybershen

UNE SEULE ATTAQUE, TROIS PILIERS

Une défense en profondeur et adaptative

UASR PLATFORM

Voir et durcir

La porte était fermée avant l'attaque (1). Le parc était durci (4).

ZT-STATION

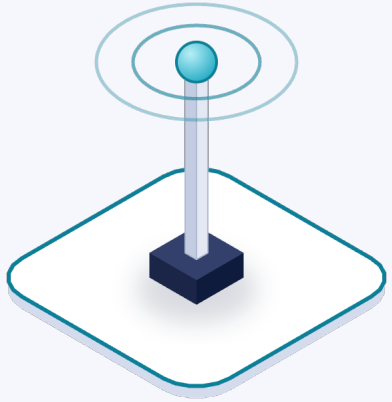
Confiner et reprendre

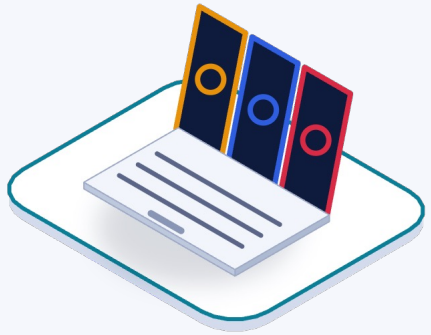
Le piège est resté dans un environnement (2). L'environnement part à l'état sain (6).

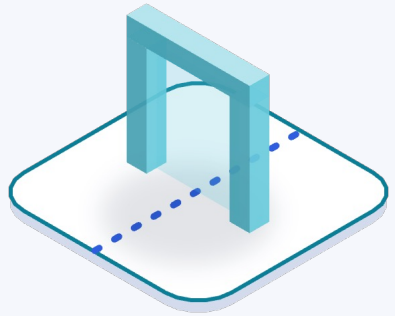
ZT-SSE

Vérifier chaque connexion

Le rebond est refusé (3). L'exfiltration vers l'IA publique est bloquée (5).







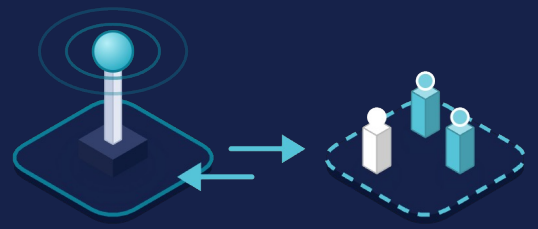
cybershen

cybershen

ZTUP · UN SCORE, UNE POLITIQUE, UN POSTE DE CONFIANCE

Humain ou IA : rien ne passe sans vérification.

Jean-François BETTE · CTO Cybershen · jean-françois.bette@cybershen.com



APPEL À COLLABORATION

Équipes de recherche

Zero Trust, IA, isolation, UEBA : nous ouvrons nos travaux aux équipes de recherche.

contact@cybershen.com