0DATA LAB · PAPIER 005 · JUILLET 2026

Le Système Immunitaire des Infrastructures

Hadda TIKIJJA

0DATA Lab, Rennes, France

contact@odata.fr

📄 Télécharger le PDF 🌐 Version Web

RÉSUMÉ

La cybersécurité moderne est une course à l'armement : signatures contre mutations, pare-feux contre contournements. Cette course est perdue d'avance — l'attaquant a l'initiative, le défenseur réagit. Nous proposons un changement de paradigme radical : *ne plus courir*. Au lieu de détecter des menaces, nous connaissons l'état normal. Au lieu d'ajouter des couches, nous greffons un système immunitaire vivant. Au lieu de bloquer, nous anesthésions. Nous introduisons la **cybersécurité organismique** : un modèle à trois niveaux d'immunité — innée, adaptative, collective — directement transposé de 4 milliards d'années d'évolution biologique. Nous démontrons que tout programme malveillant, par sa seule activité réseau, devient une synapse détectable. Rien n'échappe à un organisme qui se connaît.

1. Introduction

La sécurité informatique est bâtie sur un postulat implicite : l'infrastructure est un territoire à défendre. Comme une forteresse. Des murs (firewalls), des douaniers (IDS/IPS), des caméras (SIEM), des chiens de garde (EDR). Chaque nouvelle menace appelle une nouvelle couche. Chaque nouvelle couche ajoute de la complexité.

Le résultat est un paradoxe bien documenté : plus on sécurise, plus la surface d'attaque s'élargit. Un SOC moderne gère entre 15 et 40 outils. Chaque outil est un point de défaillance poten-

tiel. Chaque alerte est un signal dans un océan de bruit. Le taux de faux positifs dépasse 60% dans la plupart des déploiements [1]. Les équipes sont noyées.

Et pendant ce temps, le vide travaille.

1.1 Le Vide est un Appel

Chaque infrastructure contient des angles morts. Le switch oublié dans le placard du troisième étage. Le VLAN fantôme hérité d'un administrateur parti il y a six ans. Le serveur de test que personne n'a documenté. Le port ouvert que personne ne surveille.

Ce vide n'est pas neutre. Il n'est pas inerte. Il est une *invitation permanente à la compromission*. Un appel silencieux que l'attaquant finira par entendre.

PRINCIPE FONDAMENTAL

Le vide est un appel. La présence est une immunité.

Un organisme ne peut pas se défendre contre ce qu'il ne sent pas. La première fonction de toute immunité n'est pas de combattre — c'est de *percevoir*. Connaître son propre corps. Sentir chaque organe. Prendre le pouls. Là où il n'y a pas de présence, il y a une porte ouverte. Là où NOVA est greffée, l'infrastructure se connaît — et ce qui se connaît ne peut plus être surpris.

C'est le fondement de notre approche. Nous ne vendons pas de la sécurité. Nous ne courons pas après les menaces. Nous éliminons le vide. Nous installons la présence.

2. Positionnement

Nous ne faisons pas « de la cybersécurité en mieux ». Nous faisons autre chose. La différence n'est pas une question de performance — c'est une question de catégorie.

MARCHÉ TRADITIONNEL	0DATA
Ajouter des couches	Remplacer le modèle
Signatures d'attaques	Connaître l'état normal
Déployer des agents	Greffer un symbiote

5 à 40 outils cloisonnés	Un organisme qui apprend
Réagir après l'incident	Anticiper avant la maladie
Protéger le périmètre	Immuniser l'organisme
Bloquer la menace	Anesthésier la menace

> *On ne compare pas un oiseau à un drone. On ne compare pas un système immunitaire à un antivirus. — Principe créatif 0DATA*

Le système immunitaire biologique ne fonctionne pas par signatures. Il ne met pas à jour une base de données de pathogènes. Il connaît le *soi*, et tout ce qui n'est pas le soi déclenche une réponse. C'est ce modèle que nous transposons.

3. Fondements

3.1 Présence & Immunité

Le postulat central de la cybersécurité organismique est le suivant :

AXIOME DE LA PRÉSENCE

Soit I une infrastructure. Soit $V(I)$ l'ensemble des points de I qui ne sont pas sous observation continue.

Théorème du Vide. Pour toute infrastructure I, la probabilité de compromission non-détectée croît exponentiellement avec $|V(I)|$.

Corollaire. La réduction de $|V(I)|$ vers zéro est la condition nécessaire et suffisante de l'immunité infrastructurelle.

En d'autres termes : **le vide est un appel, la présence est une immunité.** Un organisme qui se connaît entièrement ne peut pas être surpris. Une infrastructure dont chaque organe est senti en continu ne peut pas être compromise silencieusement.

Ce principe a une conséquence opérationnelle directe. L'objectif n'est pas de « détecter 100% des menaces » — c'est une cible mouvante, infinie. L'objectif est de réduire $|V(I)|$ à zéro — une cible fixe, mesurable, atteignable. On ne court plus après les attaquants. On élimine leur terrain de chasse.

3.2 Théorème de l'Activité

THÉORÈME DE L'ACTIVITÉ

Tout programme malveillant = du code. Tout code en exécution = une activité réseau. Toute activité = une synapse dans le graphe topologique de l'infrastructure. Toute synapse hors baseline = une anomalie.

Conséquence. Dans une infrastructure sous observation continue, aucune activité malveillante ne peut exister sans générer une synapse — et aucune synapse ne peut exister sans être détectée. *Rien n'échappe.*

Ce théorème est la transposition directe du principe immunitaire biologique : le système immunitaire ne connaît pas tous les pathogènes — il connaît le *soi*. Tout ce qui n'est pas le soi déclenche une réponse. De même, NOVA ne connaît pas tous les malwares — elle connaît la *baseline* de l'infrastructure. Toute déviation est une alerte.

4. Architecture Immunitaire

Le système immunitaire biologique fonctionne sur trois niveaux. Nous transposons chacun d'eux.

4.1 Immunité Innée — Toujours Active

L'immunité innée est la première ligne de défense du corps. Elle est non-spécifique, toujours active, immédiate. Dans NOVA, elle correspond à la couche fondamentale :

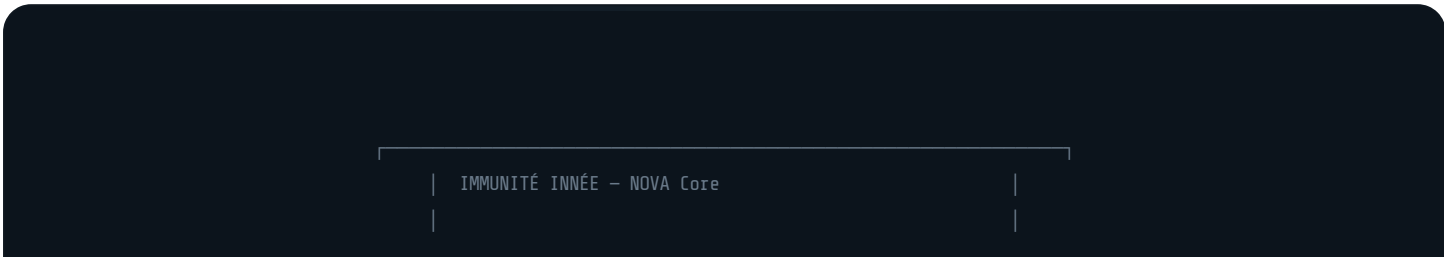

Figure 1 : La couche d'immunité innée de NOVA

4.2 Immunité Adaptative — Sur Alerte

Quand l'immunité innée détecte une anomalie, l'immunité adaptative prend le relais. Elle est spécifique, ciblée, et garde la mémoire de l'infection.

Figure 2 : La couche d'immunité adaptative

4.3 Immunité Collective — Mémoire Partagée

Le troisième niveau est le plus puissant : l'immunité collective. Quand un individu développe des anticorps contre un pathogène, toute la population peut en bénéficier — via la vaccination.

Figure 3 : La couche d'immunité collective

PRINCIPE DE L'IMMUNITÉ COLLECTIVE

Un symbiote qui apprend protège son hôte. Tous les symbiotes qui partagent protègent l'espèce. C'est la transposition directe de l'immunité grégaire : quand une fraction suffisante de la population est immunisée, le pathogène ne peut plus circuler. Dans notre modèle, **chaque greffe renforce toutes les autres**.

5. Anesthésie Numérique

5.1 Pourquoi ne pas bloquer

La réponse classique à une intrusion est le blocage : couper la connexion, isoler la machine, tuer le processus. Cette approche a un défaut fondamental : **elle informe l'attaquant qu'il a été détecté**. Le malware mute. L'attaquant change de méthode. La menace réapparaît ailleurs, sous une forme différente.

Nous proposons le contraire : **l'anesthésie**.

DÉFINITION — ANESTHÉSIE NUMÉRIQUE

L'anesthésie numérique est la redirection du trafic d'un équipement compromis vers un bac à sable vivant qui émule l'infrastructure réelle. Le programme malveillant continue de fonctionner, persuadé d'être sur l'infrastructure cible. En réalité, il est isolé, observé, et filmé. Chaque paquet qu'il émet enrichit notre connaissance de ses méthodes.

L'objectif n'est pas de gagner une bataille. L'objectif est de **gagner la guerre — pour tous les symbiotes, pour toujours**.

Figure 4 : Le cycle d'anesthésie numérique

5.2 Implémentations

OPTION	NIVEAU	TECHNIQUE	RISQUE RÉSEAU
A — ARP Miroir	L2	ARP spoofing ciblé	Modéré
B — VLAN Quarantaine	L2	Switch SNMP/API	Faible
C — DNS Hijacking	L7	Interception DNS	Très faible
D — SDN/OpenFlow	L2–L3	Reprogrammation flux	Négligeable

6. Cas Difficiles

Notre modèle immunitaire brille particulièrement sur les cas qui échappent aux approches traditionnelles.

SCÉNARIO	APPROCHE CLASSIQUE	APPROCHE ORGANISMIQUE
APT furtive Exfiltration lente, 1 Ko/jour	Seuil de détection trop bas → invisible	Synapse nouvelle (même minuscule) → hors baseline → détectée
Supply chain Logiciel légitime compromis	Signé, autorisé → exécuté	Comportement réseau change → détecté
Insider malveillant Accès légitime, usage illégitime	Authentifié → autorisé	Horaire/cible/volume atypique → détecté
Ransomware Propagation massive	Détection quand il est trop tard	Explosion de synapses anormales → isolation automatique en secondes

7. Extensions Naturelles

Le système immunitaire décrit ici est la couche de défense. Il s'inscrit dans une architecture organismique plus large qui ouvre plusieurs trajectoires naturelles.

Superposition Numérique. L'anesthésie numérique peut être étendue au concept de superposition : le malware existe simultanément dans deux états — bloqué pour le réseau réel (état « mort »), actif pour le bac à sable (état « vivant »). Comme le chat de Schrödinger, il est à la fois vivant et mort. La décohérence survient quand le malware « mesure » l'environnement et découvre le leurre. Les travaux récents en deception quantique [2,3] et en décohérence défensive [4] fournissent des ancrages théoriques prometteurs.

Symbiote Autonome. Le symbiote évolue en cinq phases : découverte → apprentissage → anomalie → contrôle → auto-analyse. Au stade 5, il vérifie sa propre intégrité et détecte les tentatives de compromission de lui-même. Un système immunitaire qui s'immunise.

Guérison Cellulaire. Au-delà de l'isolation et du rollback, l'extension vers la greffe curative — remplacer un organe compromis par un clone sain sans interruption de service — est une évolution naturelle du protocole de greffe (Papier 001).

Intégration Réglementaire. L'alignement sur NIS2, GDPR, et la certification ExpertCyber (ANSSI) est documenté dans le Papier 004.

8. Discussion

Le modèle proposé repose sur un pari fondamental : que la connaissance du *soi* — exhaustive, continue, vivante — est une meilleure stratégie de défense que la connaissance des *menaces* — partielle, datée, réactive.

C'est le pari de la biologie. Le système immunitaire ne connaît pas la liste des pathogènes existants. Il connaît le soi, et rejette le non-soi. Cette stratégie a tenu 4 milliards d'années.

Notre approche n'est pas sans défis. La qualité de la baseline est critique : une baseline polluée par une infection préexistante pourrait normaliser un comportement malveillant. C'est pourquoi la baseline est construite sur une fenêtre minimale de 7 jours, avec validation croisée par l'Institut (comparaison avec les baselines d'infrastructures similaires).

Un autre défi est la réduction à zéro du vide $|V(I)|$. Dans une infrastructure complexe, certains angles morts sont inévitables — équipements air-gap, segments isolés, dispositifs sans inter-

face réseau. La réponse n'est pas de prétendre les couvrir, mais de les *documenter*. Un angle mort connu et balisé n'est plus un vide — c'est une frontière surveillée.

L'anesthésie numérique, enfin, est une arme à double tranchant. Un bac à sable qui émule l'infrastructure réelle doit être parfaitement étanche. Une fuite du bac à sable vers le réseau réel transformerait l'observatoire en vecteur d'infection. La validation formelle de l'étanchéité du bac à sable est un travail en cours.

Tuer le malware = gagner une bataille. L'anesthésier, le comprendre, et partager cette connaissance = gagner la guerre — pour tous les symbiotes, pour toujours.

9. Conclusion

Nous avons introduit la **cybersécurité organismique** : un modèle où l'infrastructure n'est plus un territoire à défendre, mais un corps à immuniser.

Trois principes la fondent :

Le vide est un appel, la présence est une immunité. La condition nécessaire et suffisante de la sécurité n'est pas la détection des menaces, mais l'élimination des angles morts. Un organisme qui se connaît entièrement ne peut pas être surpris.

Toute activité est une synapse. Dans une infrastructure sous observation continue, aucun programme ne peut s'exécuter sans laisser de trace. Le théorème de l'activité garantit la détectabilité de toute action malveillante.

Bloquer informe, anesthésier instruit. L'anesthésie numérique transforme chaque intrusion en leçon collective. Le malware devient son propre traître — il révèle ses méthodes, ses cibles, ses infrastructures, et cette connaissance protège tous les symbiotes.

Nous ne vendons pas de la cybersécurité. Nous greffons un système immunitaire. Nous éliminons le vide. Nous installons la présence.

Ce travail est un appel. À tous ceux qui sentent que la course aux menaces est une impasse. À tous ceux qui savent que la sécurité ne se décrète pas — elle se cultive. La greffe est prête. Le corps attend.

Remerciements

À toutes les équipes infrastructure qui, chaque jour, défendent ce qu'elles ne voient pas entièrement. Aux ombres silencieuses de l'infrastructure mondiale — ce travail est pour vous.

Au Pr. D. Farmer, pour les conversations fondatrices sur la viabilité de la métaphore biologique en cybersécurité.

Ce travail est dédié aux artisans du numérique qui savent qu'un réseau n'est pas un territoire — c'est un corps.

Références

[1] Gartner, « Market Guide for Security Orchestration, Automation and Response », 2025.

[2] Y. Li et al., « Quantum Deception: Exploiting Quantum Effects for Cybersecurity Deception », arXiv:2510.11848, 2025.

[3] S. Chen et al., « Game of Travesty: Deception Strategies in Cyberspace », arXiv:2309.13403, 2023.

[4] M. Rivera et al., « Decoherence as a Defence Mechanism in Quantum-Inspired Security », arXiv:2606.24219, 2026.

[5] A. Aickelin et S. Cayzer, « The Danger Theory and Its Application to Artificial Immune Systems », arXiv:0801.3549, 2008.

[6] J. Greensmith et al., « Introducing the Dendritic Cell Algorithm », arXiv:1001.2208, 2010.

[7] H. TIKIJJA, « Digital Grafting: A Novel Paradigm for Infrastructure Evolution », 0DATA Lab, 2026. Papier 001.

[8] H. TIKIJJA, « Synthética : Taxonomie du Vivant Numérique », 0DATA Lab, 2026. Papier 002.

[9] H. TIKIJJA, « Le Système Nerveux des Infrastructures », 0DATA Lab, 2026. Papier 003.

[10] H. TIKIJJA, « La Greffe Numérique : Une Nouvelle Discipline », 0DATA Lab, 2026. Papier 004.