

# LA VISIBILITÉ : UNE NÉCESSITÉ POUR DÉTECTER LES ATTAQUES CONTRE VOS INFRASTRUCTURES

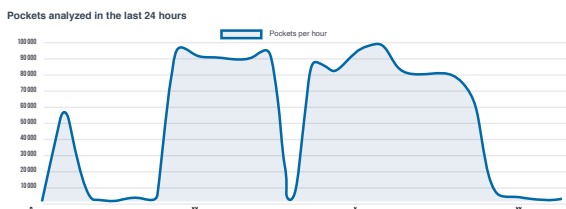
Dans le contexte actuel de cybersécurité, le nombre d'attaques informatiques augmentent constamment et vos données sont continuellement à risque. Pour maintenir son statut de partenaire de confiance, NOVIPRO a à cœur la sécurité de vos informations. Les plans de développement de la sécurité ne peuvent pas toujours être priorités.

NOVIPRO vous offre donc tranquillité d'esprit au niveau de votre sécurité d'entreprise grâce à son offre de visibilité permettant de répondre aux différentes questions essentielles:

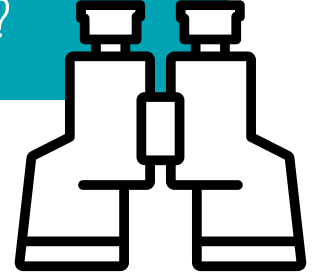
- Suis-je ciblé par des attaquants ?
- Suis-je victime de vols de données ?
- Ai-je une bonne visibilité de mon réseau ?

L'objectif des équipes d'experts de NOVIPRO est de vous accompagner dans l'optimisation de votre réponse de sécurité en cas d'incident et d'augmenter la visibilité sur votre réseau tout en minimisant l'impact sur vos opérations.

	VISIBILITÉ	PRISE EN CHARGE
Déploiement, implémentation	✓	✓
Entraînement des modèles IA	✓	✓
Détection 24/7/365	✓	✓
Contextualisation des alertes de sécurité	✓	✓
Communication vers vos équipes	✓	✓
Accompagnement dans les résolutions		✓
Prise en charge des alertes d'urgence		✓
Rapport d'activité mensuel		✓
Cyber Swat / Réponse aux incidents	OPTION	OPTION



Savez-vous si vous êtes  
victime d'une attaque  
informatique ?



## VOTRE DÉTECTION EN BREF

Les cybercriminels redoublent d'ingéniosité pour ne pas éveiller les soupçons des équipes techniques:

- Balayages externes
- Signaux faibles
- Mouvements latéraux
- Exfiltration de données
- Activités noyées dans les flux d'opération

Il est humainement impossible de surveiller tous les indicateurs de compromission. La solution de visibilité proposée utilise l'intelligence artificielle pour s'adapter en permanence et analyser les milliers d'événements recensés aussi bien sur les flux externes qu'internes afin de détecter les menaces rapidement.

### VISIBILITÉ

Les anomalies détectées sont immédiatement transmises à nos experts en cybersécurité afin qu'ils les analysent en fonction de votre structure. Les faux positifs seront éliminés et les alertes transmises ne seront que celles qui doivent être prises en charge par vos équipes. Vous serez donc en mesure d'apporter les correctifs appropriés et ce rapidement sur les éléments suivants:

- Alertes contextualisées à destination de vos experts.
- Actions de sécurisation déclenchées par nos équipes.

### PRISE EN CHARGE

Au lieu de vous transmettre les alertes nécessitant une intervention, NOVIPRO fera l'analyse, déterminera les actions à prendre et vous accompagnera dans l'application des correctifs à apporter. De plus, nous pouvons également mettre à votre disposition une équipe d'experts en sécurité pour supporter vos équipes en cas de cyberattaques.

### PROCESSUS DE DÉTECTION DES MENACES

- 1  Hackers
- 2  Création de menaces
- 3  Visibilité et IA pour détection de menaces
- 4  Transmission des menaces détectées à l'équipe NOVIPRO et traitement de la menace

