



Service MDR/SOC 24/7

## Notre expertise. Votre tranquillité d'esprit

*Peu importe où les cyber-menaces se cachent, ou ce qu'elles sont, Gardien Virtuel est là pour vous protéger. Nos services gérés de détection et de réponse aux incidents de sécurité (MDR) livrés par les spécialistes de notre centre d'opérations 24/7 (SOC) permettent à votre organisation d'être proactive face aux cyberattaques pour ainsi éviter la Une des journaux et de faire partie des statistiques.*

En opération depuis 2011, le SOC de Gardien Virtuel examine méticuleusement les activités du réseau et des utilisateurs afin de détecter et d'atténuer rapidement les attaques, en surveillant continuellement les événements, les fichiers journaux, les comportements des utilisateurs et le trafic du réseau, tout en assurant la conformité avec les exigences légales et de cyber-assurance.

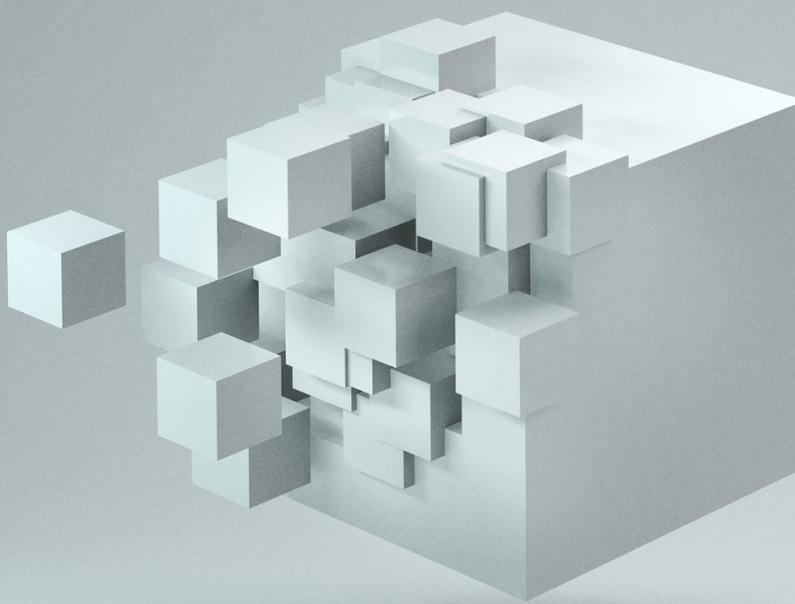
Nos experts en cybersécurité ont une connaissance approfondie du paysage actuel des menaces. Ils identifieront les attaques avancées et les risques internes en concevant des protocoles de détection et des cas d'utilisation capables d'identifier rapidement les activités suspectes en l'espace de quelques instants. Grâce à la mise en œuvre des meilleures technologies avancées telles que SIEM (Qradar),

SOAR (Revelstoke) VMDR (Qualys) et XDR (CrowdStrike et Microsoft), nos spécialistes de la sécurité répondent rapidement et efficacement aux menaces. Vous pouvez être assuré que notre équipe travaille avec des informations de la plus haute qualité possible, garantissant des résultats efficaces et efficaces pour votre surveillance et votre réponse en matière de cybersécurité.

Lorsque des événements ou des schémas suspects sont découverts, notre équipe SOC mène des enquêtes rapides et approfondies afin d'endiguer les risques pour les systèmes et les employés. Cette réponse et cette communication rapides à votre organisation minimisent les impacts potentiels des cyber-menaces sur vos opérations.

Les dangers  
sont réels.

La solution  
est simple.



Gardien Virtuel peut identifier les risques et offrir une gestion de bout en bout et continue pour aider à protéger vos systèmes et vos données contre les menaces extérieures.



### **Le service MDR/SOC 24/7 de Gardien Virtuel offre l'ensemble de fonctions de cybersécurité le plus complet :**

#### **UN SERVICE DE COUVERTURE DE CLASSE MONDIALE**

- Surveillance permanente 24 heures sur 24, 7 jours sur 7, et assistance d'un cyber analyste dédié
- Assistance 24/7 en matière de perturbation et d'endiguement des menaces
- Recommandations concrètes pour améliorer votre posture de cybersécurité (rapports, communication et collaboration tous les mois)
- Remontées d'informations détaillées avec analyse et recommandations
- Combinaison d'enquêtes automatisées rapides et humaines pour efficacité accrue du confinement des menaces et de remédiation
- Détection des menaces selon le cadre Mitre Att&ck et plusieurs flux de renseignements sur les menaces inclus

#### **COUVRIR TOUS LES ANGLES D'ATTAQUE**

- Analyse continue du comportement des utilisateurs et des entités (UEBA)
- Cas d'usage inclus dans le service : Ransomware, force brute, phishing, attaques DOS et plus.
- Couverture et visibilité multi-sources (sur site, dans les nuages, surveillance des comptes O365, etc.)
- Détections automatisées avec signatures, analyse comportementale, IOCs effets sur le réseau de sécurité
- Analyse du réseau (détection des mouvements latéraux non autorisés)

#### **ADAPTÉ À VOTRE RÉALITÉ, PERSONNALISÉ À VOS BESOINS**

- 24/7 ou soir/huit/week-end
- Protection anti-ransomware
- Surveillance du dark web
- Protection EDR des points de terminaison
- Gestion des vulnérabilités et correctifs automatisés

