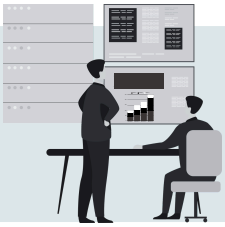
Fiche produit

Centre de Télésurveillance Cyberenity by IPgarde (SOC)

Une couverture de l'ensemble du périmètre SI de votre organisation grâce à une surveillance des menaces, des enquêtes et des mesures correctives gérées par nos analystes CTN experts.

VUE D'ENSEMBLE

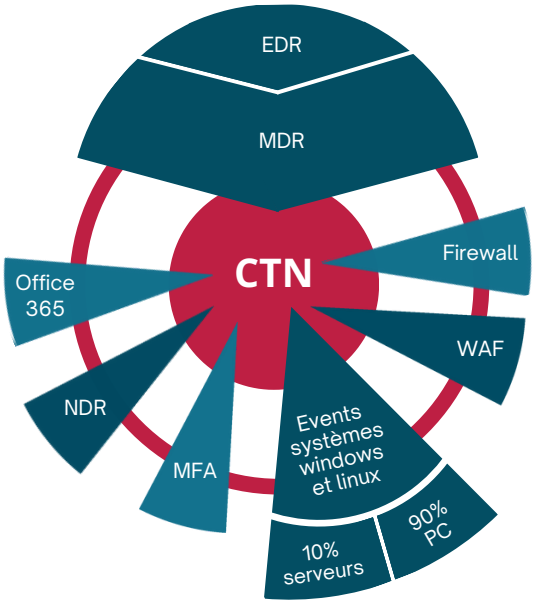
Pour les équipes de sécurité des petites et moyennes entreprises, la fourniture de **services de cybersécurité de haute qualité** et le maintien des environnements **professionnels à l'abri des menaces** nécessitent une équipe qualifiée capable **d'analyser et interpréter les signaux recueillis par l'ensemble des logiciels utilisés** pour réagir rapidement **aux alertes les plus silencieuses.** Or, de nombreuses organisations sont confrontées à **des ressources humaines limitées** et manquent de compétences approfondies en matière de cybersécurité. En outre, elles sont constamment surchargées de responsabilités en matière de triage des alertes. À cela s'ajoutent **la montée en flèche des coûts** et la complexité de la gestion de solutions multiples pour découvrir les menaces cachées, ce qui conduit à **l'inefficacité et à de longs délais de réponse aux incidents.**



Les équipes informatiques ont besoin **d'un service fiable (outils et équipes) leur assurant une couverture totale de leurs SI,** quelque soit la dangerosité, l'origine ou la sophistication de la cyber-menace.

IPgarde relève ces défis **grâce à une offre de Télésurveillance Numérique** (CTN / SOC) qui permet à vos équipes de s'appuyer à 100% sur notre équipe de cyber-spécialistes dédiée qui opère 24/7/365 pour détecter, prévenir et contrer les cyberattaques. Cette offre va plus loin qu'un MDR managé, dont le périmètre **est limité aux signaux remontés par l'EDR** ThreatDown (représentant environ **60%** du périmètre total). Le périmètre d'action du CTN Cyberenity d'IPgarde couvre aussi l'ensemble des évènements présents sur les systèmes d'exploitation des PC et des serveurs de votre organisation (**30%** du périmètre environ), mais également **les évènements provenant de logiciels** tiers comme vos Firewall / MFA / WAF ou Office 365. Vos SI sont ainsi **entièrement suivis à chaque instant par nos cyber-spécialistes,** permettant **la détection des signaux les plus silencieux** qui auraient très certainement mis plusieurs semaines à remonter avec une autre solution de cybersécurité.

ORIGINE DES LOGS TRAITÉS PAR LE CTN



DÉFIS

- **Ressources limitées pour répondre aux besoins en matière de sécurité :** 67 % des personnes interrogées font état d'une pénurie de personnel dans le domaine de la cybersécurité.[1]
- **Trop plein de signaux d'alertes :** Le grand nombre d'alertes bénignes cache les mouvements les plus faibles qui peuvent pourtant être décisifs.
- **La lenteur de la réaction permet aux attaquants de disposer de plus de temps sur vos points d'accès :** 277 jours - nombre moyen de jours pour identifier et contenir une violation.

AVANTAGES

Couvrir l'ensemble du périmètre de vos SI avec les équipes ET les outils les plus performants.

- **Un périmètre complet :** Surveillez les logs provenant de votre MDR, d'Office 365, de vos Firewall, WAF et MFA, mais aussi et surtout de l'ensemble des signaux provenant de vos systèmes d'exploitation Windows et Linux : **au niveau de vos serveurs ET de vos PC (une des seules solutions du marché à le proposer).**
- **Moins d'efforts** : Économisez les ressources de votre équipe en vous appuyant sur les analystes de sécurité experts de ThreatDown pour surveiller les activités suspectes sur vos réseaux en 24/7/365.
- **Meilleurs résultats :** Obtenez des temps de réponse et de remédiation plus rapides, à un coût nettement inférieur à celui de l'internalisation d'un service cybersécurité.

1 Rapport Malwarebytes sur l'état des logiciels malveillants.

AVANTAGES DU SOC / CTN CYBERENITY BY IPGARDE

- **Surveillance 24 heures sur 24, 7 jours sur 7 et 365 jours par an :** Nous surveillons les appareils informatiques et effectuons des enquêtes spécialisées jour et nuit, en semaine, le week-end et les jours fériés.

- **Un périmètre de détection complet :** Nos équipes surveillent les signaux malveillants provenant non seulement de l'EDR ThreatDown by Malwerbytes, mais aussi des sources autres comme O365, votre pare-feu, les évènements sur vos systèmes Windows et Linux (sur les serveurs **ET sur les postes PC**), mais également sur les NDR, MFA et WAF.

- **Des analystes CTN compétents** : Notre équipe d'experts en cybersécurité est composée de chasseurs de menaces accomplis, dotés **d'une solide expérience en matière de réponse aux incidents** et de dizaines d'années d'expérience dans le triage et l'atténuation des menaces complexes liées aux logiciels malveillants.

- **Des outils de pointe primés et reconnus** : la couverture des signaux est alimentée par la plateforme ThreatDown by Malwerbytes Endpoint Detection and Response (EDR) et enrichie par de multiples sources de renseignements sur les menaces, dont le SIEM, le SOAR, Phenix ID.

- **Grande vitesse de réaction** : Les menaces les plus importantes sont remontées en quelques minutes, quand elles pourraient prendre plusieurs semaines à être identifiées sans le CTN (une fois les malwares installés sur vos SI)

- **Options de remédiation flexibles** : Notre équipe CTN peut fournir un soutien actif à la remédiation aux menaces au fur et à mesure qu'elles sont découvertes, ou fournir des conseils très utiles aux équipes informatiques dans le cadre de leurs propres efforts de remédiation.

- **Chasse active aux menaces** : Notre équipe CTN traque les menaces invisibles en se basant sur les indicateurs de compromission (IOC) antérieurs et les activités suspectes observées sur les terminaux.

- Déploiement rapide : Le CTN est facile à installer, ce qui permet à votre équipe de **sécurité d'intégrer rapidement de nouveaux appareils informatiques à notre service MDR** 24x7 en quelques minutes.

- **Roll back de 72 heures** (restauration jusqu'à 72 h en arrière) en cas de ransomware pour vos machines Windows

COMMENT CELA FONCTIONNE-T-IL ?

Une fois les agents déployés, le service MDR est activé en quelques minutes et les analystes d'IPgarde peuvent **surveiller l'environnement du client.** Les données de détection sont intégrées dans la plateforme MDR Security Orchestration, Automation, and Response (SOAR), où elles sont **enrichies par des flux de renseignements internes et externes** sur les menaces. Ce processus **accélère** l'identification, l'analyse et le triage (**hiérarchisation** des réponses et enquêtes) des événements de sécurité. À ce stade, la plateforme MDR SOAR vérifie que les alertes d'activité suspecte **sont des menaces réelles ou des détections bénignes** et peut augmenter le niveau de gravité de certaines détections EDR sur la base de renseignements sur les menaces. Les cas qui nécessitent une remédiation sont soit complétés par l'analyste, soit guidés par le client ou le MSP s'ils ont choisi d'effectuer leurs propres actions de remédiation.

PRENDRE RDV AVEC UN REPRÉSENTANT IPGARDE POUR BÉNÉFICIER DE LA SOLUTION CTN CYBERENITY BY IPGARDE

Blog IPgarde
www.blog.ipgarde.com

IPgarde
01 77 49 24 50
contact@ipgarde.com
www.ipgarde.com