NéoSOC

néosoft

PME & ETI : la cybersécurité accessible, mission impossible ?

NéoSOC apporte une réponse simple, efficace et adaptée à votre budget.

Qualification des incidents critiques **en moins d'1h**.

Trois piliers pour vous protéger :
Disponibilité | Contrôle | Légitimité

- **Surveillance et détection 24/7 :**
  Une protection continue, sans interruption.
- **Visibilité complète et couverture 360°**
  de votre système d'information.
- **Expertise reconnue de Néosoft :**
  15 ans d'expérience et de nombreux clients protégés.
- **Protection proactive :**
  Premières actions de remédiation automatisées en cas d'incident.

Notre méthodologie : Une sécurité sur-mesure, du besoin à la réponse rapide.

- **Manuel qualité Néosoft :**
  Un cadre solide qui part de votre besoin réel et garantit votre satisfaction à chaque étape.
- **Trois stratégies clés, adaptées à votre environnement :**
  Stratégie d'analyse avec détection ciblée via des règles spécifiques client.
  Stratégie de collecte des données strictement nécessaires pour une analyse efficace et maîtrisée.
  Stratégie de notification : alertes ciblées et plan d'action partagé.
- **Un Service Delivery Manager dédié à votre service :**
  Une interface unique pour fluidifier les échanges.
  Une coordination claire et un suivi de la qualité.
  Une approche proactive avec pilotage et reporting.

NéoSOC

néosoft

Avec notre mode MSSP, bénéficiez d'un pilotage expert et sécurisé de votre cybersécurité, sans complexité pour vous**.**

Une tarification flexible, pensée pour vos assets et votre usage **:**

- **Offre Standard : [EDR]** Harmony Endpoint
- **Offre Essential : [EDR]** Harmony Endpoint **+** 1 à 4 briques technologiques
- **Offre Premium : [EDR]** Harmony Endpoint **+** 1 à 4 briques technologiques **+** un SIEM

Ces briques technologiques proviennent des leaders du marché : **Checkpoint**, **Tenable** et **RSA**, garantissant ainsi une protection solide et fiable.

Votre entreprise est-elle prête à faire face à la prochaine cyberattaque ?

- Avez-vous une vision claire et complète de votre parc IT ?
- Êtes-vous certain que vos protections sont vraiment efficaces ?
- Quel serait le coût réel d'une attaque sur votre production et vos finances ?
- Disposez-vous des moyens et compétences pour assurer une détection 24/7 ?