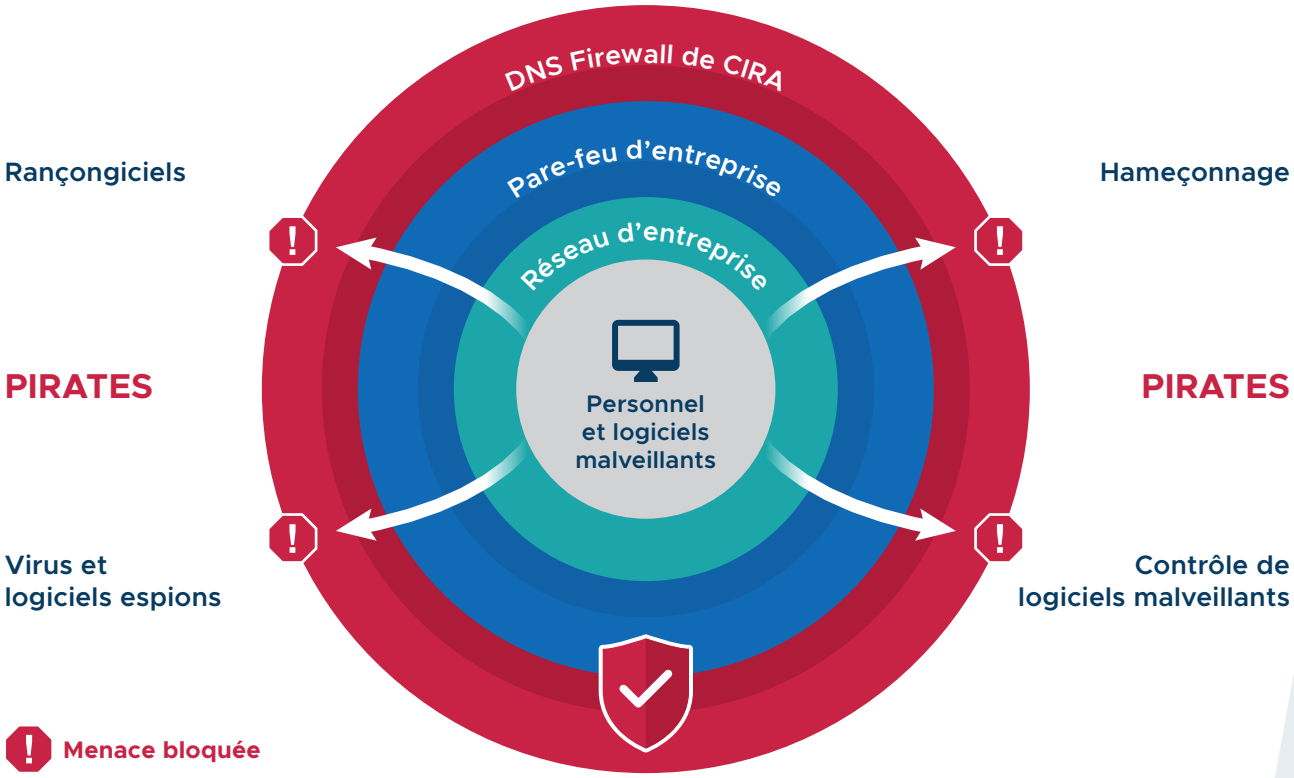
cira

DNS FIREWALL DE CIRA

Le DNS Firewall de CIRA joue un rôle essentiel dans le concept de sécurité en couches. En s'intégrant à votre stratégie de défense 360˚, le DNS Firewall de CIRA surveille et analyse votre trafic DNS. Il bloque l'accès à des sites Internet malveillants et propose un filtrage personnalisé du contenu.

OBJECTIF

Créer un environnement sécuritaire pour l'apprentissage en ligne en protégeant le réseau informatique de votre organisation contre les programmes malveillants et les attaques par hameçonnage.



DÉTECTE

Analyse les données DNS globales (historique, et en temps réel) afin de détecter les menaces à la sécurité.

SIGNALE

Repère et signale les activités malveillantes.

GÈRE

L'examen des transactions DNS permet de non seulement bloquer les menaces qui planent sur votre domaine, et les adresses IP, mais aussi l'accès aux sites Internet malveillants.

S'ADAPTE

Les politiques utilisées par les serveurs DNS sont continuellement mises à jour grâce à divers flux de menaces.

ATTÉNUE

Met en quarantaine les appareils infectés qui ont préalablement été détectés.

AUTRES AVANTAGES

- **Bloque plus de 100 000 nouvelles menaces chaque jour,** quelle que soit leur provenance (externe ou interne à votre réseau).
- **Désactive les instructions de commandement et de contrôle** de logiciels malveillants. La connexion aux serveurs de commande et de contrôle des appareils infectés sera bloquée. Le logiciel rançonneur ne pourra retrouver les clés de chiffrement et les zombies ne reçoivent plus les directives d'attaque.
- **Entièrement déployé en quelques minutes.** Aucun matériel ou logiciel n'est requis. Il suffit de changer la configuration du DNS récursif responsable de l'acheminement des requêtes vers le DNS Firewall de CIRA.
- **Propulsé par Akamai.** Les données et la science des données sont essentielles à la production d'un flux de menace. Akamai dispose d'une visibilité sur 3% des données DNS mondiales et 30% de tout le trafic Internet pour offrir une couche de protection puissante.

UNE PROTECTION DIGNE DE CONFIANCE

85 %

des menaces détectées ne l'ont pas été par les flux de détection des logiciels malveillants d'autres parties.

51 %

des logiciels malveillants de type *zero-day* passent sous le radar des solutions antivirus.

14 minutes

de la détection à l'intégration dans le flux de détection des cybermenaces.

Le programme d'initiatives financées en cybersécurité pour les CSS et CS est actuellement financé jusqu'en 2025.

INFORMATION

Pour obtenir plus d'information et pour répondre à toutes vos questions, merci de contacter le Service aux membres du RISQ à sam@risq.quebec.

Vous pouvez aussi directement contacter CIRA par courriel à info@d-zone.ca

www.risq.quebec