SURVEILLANCE ACTIVE (SOC)

OBJECTIFS

Détection proactive de cybermenaces et réponse sur mesure aux incidents de cybersécurité.

Approche mutualisée contre les cybermenaces, au bénéfice des organisations desservies par notre réseau.

NE LAISSEZ AUCUNE MENACE PASSER INAPERÇUE – ACCÉDEZ À UNE CYBERSÉCURITÉ PROACTIVE

Le service Surveillance active en cybersécurité propose les fonctionnalités de détection et réponse adaptées aux besoins des organisations desservies par le RISQ. Le niveau de **prise en charge d'événement est adapté selon les besoins de l'organisation** et peut varier de **l'accompagnement** lors d'un événement jusqu'à la **prise en charge complète de la détection et de la réponse** à un incident.

UNE APPROCHE DE DÉFENSE SÉCURITAIRE, STRUCTURÉE ET COLLABORATIVE

8. Adaptation et évolution continue du service pour répondre spécifiquement aux besoins uniques de chaque organisation, en fonction de l'évolution de la menace et des priorités (Conception de nouveaux cas d'usage personnalisés.)

7. Analyse approfondie des incidents, suivie de recommandations spécifiques et d'actions correctives pour renforcer la sécurité sur le long terme.

6. Réponse rapide et efficace face aux incidents de cybersécurité, incluant l'isolement des postes compromis et la réinitialisation des comptes, avec un accompagnement tout au long du processus de résolution.

5. Rencontres techniques mensuelles et participation à une communauté de pratique en cybersécurité, permettant un échange constant sur les meilleures pratiques et les défis émergents.

4. Un contact direct avec notre équipe SOC pour une prise en charge rapide des incidents et des questions urgentes à toute heure.

1. Un service mutualisé offrant un accès à des ressources technologiques avancées et à une expertise humaine certifiée en cybersécurité.

2. Identification préventive des comportements suspects et des menaces avant qu'elles n'affectent votre réseau, grâce à des outils de détection avancée.

3. Surveillance proactive et analyse en temps réel des événements suspects et des menaces, assurant une vigilance constante pour protéger vos systèmes.

Prise en compte des menaces, cyberincidents et expériences pour améliorer le service et en faire bénéficier les autres organisations qui pourraient avoir des risques ou des vulnérabilités similaires.

UNE SOLUTION TECHNOLOGIQUE COMPLÈTE

Déploiement, configuration et gestion de Microsoft Sentinel

Construisant sur les licences Microsoft des organisations, mise en place et gestion de la plateforme Sentinel pour une surveillance de sécurité optimisée, grâce à la fédération Microsoft Lighthouse, permettant une protection étendue et une gestion efficace des risques.

Surveillance des événements critiques

Mise en place de règles de surveillance personnalisées et d'alertes en temps réel pour détecter et répondre aux comportements suspects sur des systèmes variés, y compris Linux, Defender365, et les événements réseau.

Intégration et analyse de journaux actifs hors de l'écosystème Microsoft 365

Surveillance et analyse des journaux de systèmes externes pour une détection avancée des comportements suspects et des menaces, renforçant ainsi la visibilité sur l'ensemble de votre infrastructure.

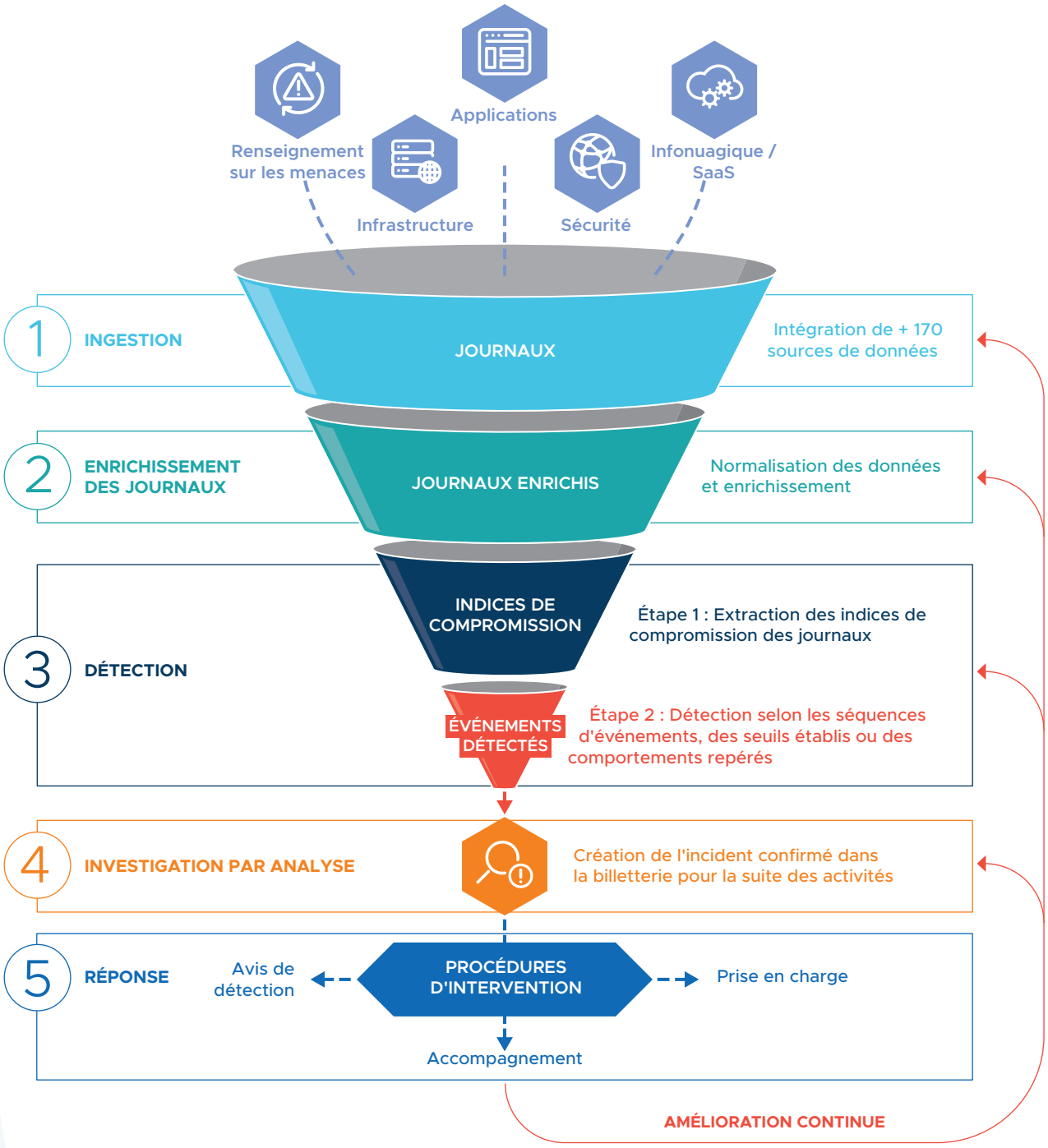
Surveillance et protection des actifs et comptes sensibles ou à hauts risques

Protection renforcée des actifs et comptes sensibles grâce à une approche différenciée de l'intervention, basée sur la criticité des ressources touchées.

Mise à profit des solutions de cybersécurité du RISQ

- ✓ Systèmes de détections des intrusions (SDI) pour une vigilance accrue contre les tentatives d'intrusion.
- ✓ Fil de menace CanSSOC, pour un suivi continu des menaces émergentes.
- ✓ Surveillance des pare-feux (RISQ Pare-feu), garantissant une défense à tous les points d'entrée.
- ✓ Protection contre les attaques par dénis de services distribué (DDoS), qui assure une défense en amont du réseau.
- ✓ Détection proactive des attaques via des technologies de déception (honeypots) pour piéger et analyser les attaquants avant qu'ils n'atteignent vos systèmes.

GESTION D'UN INCIDENT



Contactez-nous dès aujourd'hui pour en savoir plus sur ce service essentiel.

www.risq.quebec