## Arrêtez de traquer les anomalies et les alertes

SECBI
AUTONOMOUS INVESTIGATION™

# AUTOMATISEZ LA DÉTECTION, L'INVESTIGATION ET LA RÉPONSE SUR LE PÉRIMÈTRE GLOBAL D'UNE ATTAQUE

Il est de plus en plus difficile de naviguer à travers les milliards d'évènements liés à la sécurité qui changent constamment de périmètre et de nature.

Les analystes des opérations de sécurité (SOC) de niveau 1 et 2 sont confrontés à une surabondance de faux positifs. Les analystes de niveau 3 et les chasseurs de menaces ne disposent pas d'outils adéquats pour obtenir des résultats dans les délais requis.

De plus, l'absence d'outils de détection complets fait que l'on rate souvent une partie ou la totalité d'un incident détecté. Il en résulte une réponse seulement partielle, causant une plus longue période de temps d'immobilisation de l'activité malveillante.

La bonne réponse doit être immédiate et exhaustive afin d'éviter de causer des dommages trop importants aux actifs de l'entreprise.

Une grande partie du processus peut et doit être automatisée pour gagner du temps et augmenter fortement la productivité des analystes.

Contrairement à la technologie traditionnelle de capture de paquets, la solution SecBI exploite le trafic réseau sans déployer d'équipement ou d'agents supplémentaires pour assurer une mise en œuvre rapide et efficace. Les résultats sont immédiats et l'utilisation du système est quasi intuitive, sans devoir s'appuyer sur les services professionnels du fournisseur.

## Entrez dans la technologie AUTONOMOUS INVESTIGATION™

La technologie Autonomous Investigation ™ est basée sur l'apprentissage automatique supervisé et non supervisé pour analyser le trafic réseau afin de détecter les menaces complexes et furtives.

Elle dévoile instantanément toute l'étendue d'une attaque, accélérant la détection et la recherche de menaces, et optimisant les réponses et la mise en place de mesures correctives. Les analystes SOC reçoivent des rapports d'attaque complets leur donnant une visibilité sur tous les points d'infection impliqués dans la même attaque. Ce rapport complet fournit aux analystes des options exploitables, telles que le blocage d'hôtes malveillants spécifiques à cet incident et l'automatisation de la réaction pour l'avenir.

Le processus de SecBI identifie les clusters malveillants et enregistre les informations sur les menaces pour une vérification externe du comportement détecté, assurant ainsi une détection plus rapide et plus précise, ce qui réduit considérablement le nombre de faux positifs.

Détectez les malwares ciblant les fichiers et le BIOS, le crypto-jacking, les attaques IoT et la prochaine menace inconnue.

- Automatisez la réponse
- Améliorez la prévention
- Amplifiez la détection

QUE COMPRENDS LA PORTÉE TOTALE D'UNE ATTAQUE?

Un rapport complet de l'incident, depuis l'infection jusqu'à l'incident malveillant global, comprenant:

TOUS LES UTILISATEURS ET TERMINAUX INFECTÉS ET AFFECTÉS

TOUS LES DOMAINES ET HÔTES MALVEILLANTS

## LE POUVOIR DE DÉTECTER L'INCONNU

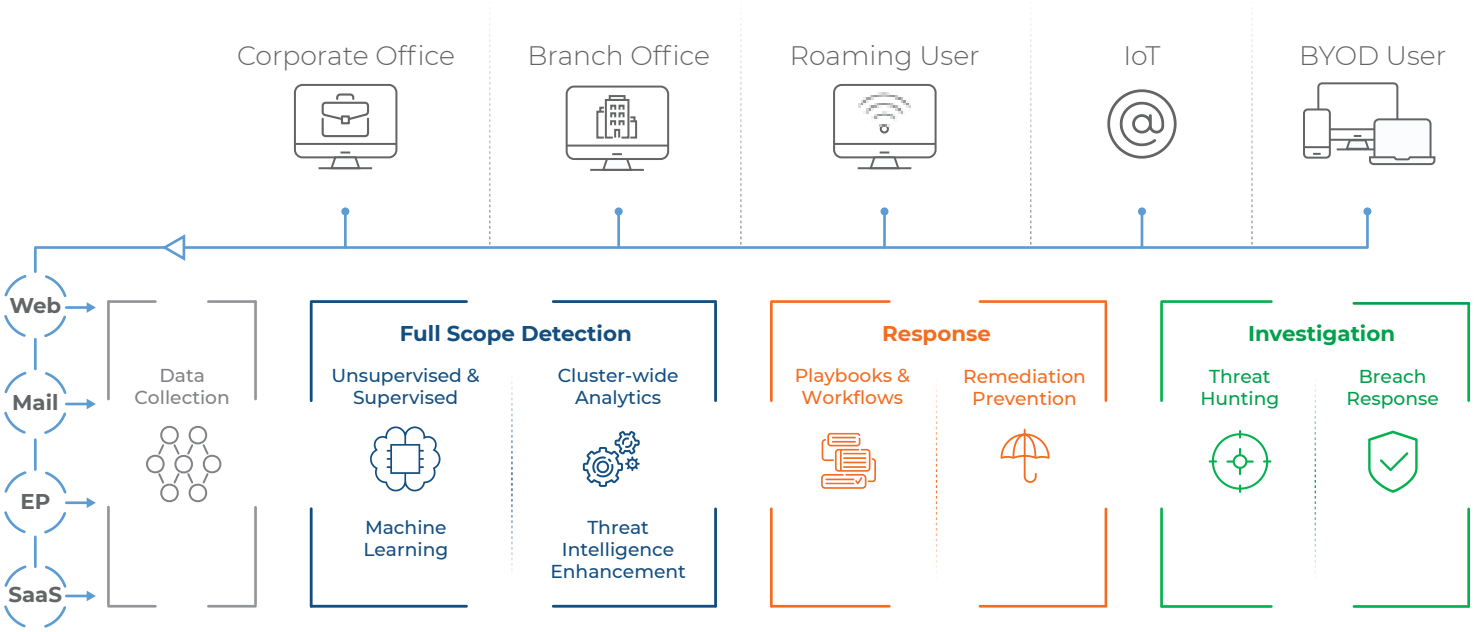
La technologie SecBI détecte et regroupe toutes les entités internes (utilisateurs, périphériques, etc.) et externes (domaines, adresses IP, serveurs C & C, points de chute, etc.) impliquées dans les communications d'un réseau compromis. L'identification d'un cluster malveillant, par opposition à une seule anomalie isolée ou à une alerte sporadique, permet une détection plus rapide et plus précise. SecBI transforme les flots d'alerte d'incidents en une liste priorisée facilitant tri, enquête et mitigation.

## VISIBILITÉ TOTALE SANS SACRIFIER LA PROTECTION DES DONNÉ

SecBI analyse le trafic réseau et les données de sécurité provenant de l'infrastructure réseau existante afin d'effectuer des analyses combinées à des renseignements sur les menaces, offrant ainsi une visibilité inégalée sur le réseau, quel que soit le cryptage.

En utilisant les métadonnées plutôt que l'inspection des paquets, SecBI offre une visibilité complète du trafic réseau sans compromettre les politiques de protection des données en utilisant des informations personnelles ou sensibles.

## DÉTECTION, RÉPONSE ET INVESTIGATION AUTOMATISÉES




## LE CHAINON MANQUANT EN CYBER DEFENSE: RÉPONSE AUTOMATISÉE ET PRÉVENTION AUGMENTÉE

Malgré le couplage intuitif d'une réponse automatisée associée à une détection précise, peu de solutions combinées sont disponibles sur le marché. Contrairement aux solutions de playbooks automatisés basées sur des anomalies isolées et des faux positifs, SecBI offre une grande valeur ajoutée en permettant une automatisation complète grâce à une technologie de détection de haut niveau basée sur un apprentissage automatique non supervisé.

Une large gamme de procédures et de playbooks automatisés est prédéfinie dans le système et permet de construire automatiquement toute l'étendue d'un incident, avec la possibilité d'injecter des réponses dans la procédure pour une réponse et une mitigation précises.

L'ajout de playbooks et de connecteurs vers les différents équipements de sécurité permet une configuration et des extensions flexibles afin de permettre une mitigation complète basée sur les playbooks via des mises à jour de stratégies et une mise en œuvre pour tous les équipements de sécurité concernés.

## CAS D'USAGE: RÉPONSE À UN INCIDENT

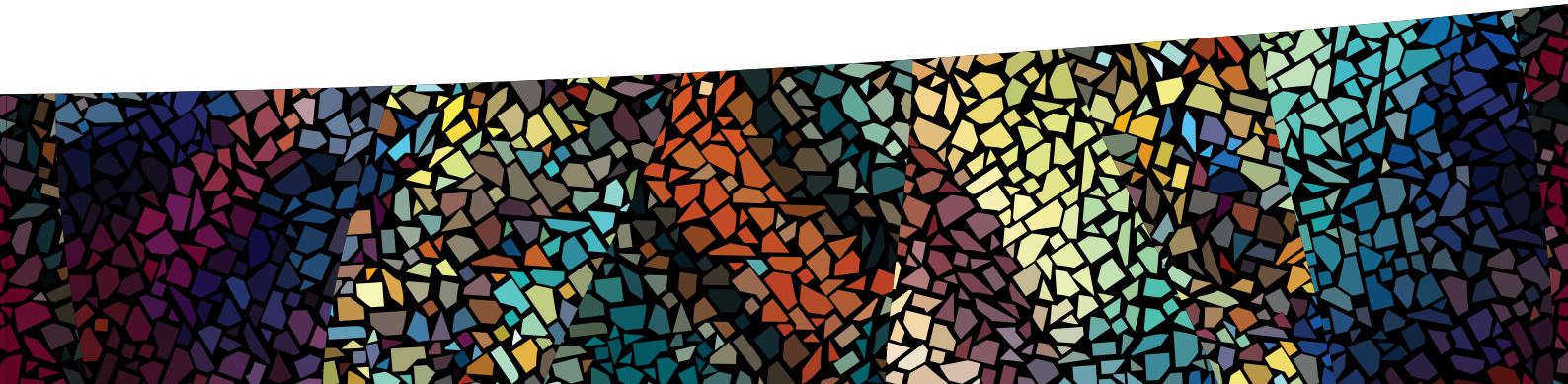
SecBI permet aux analystes de prioriser et d'enquêter sur les incidents plus efficacement. La solution SecBI aide les analystes de tous niveaux d'expérience à atteindre leurs objectifs plus efficacement dans tous les scénarios d'investigation et d'intervention. Il aide les analystes à placer les alertes dans le bon contexte, à enquêter sur les alertes hautement prioritaires dans le contexte approprié et à minimiser les risques.

## Les avantages d'Autonomous Investigation™

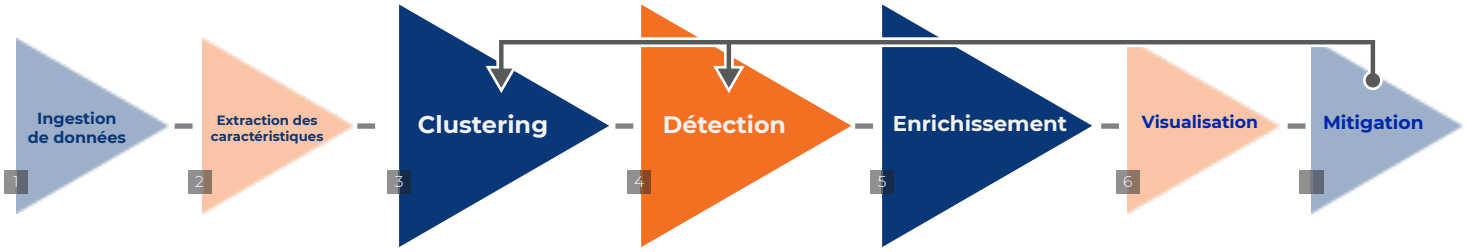
- ☑ Gain de temps pour les analystes SOC avec investigation et réponse automatisées
- ☑ Elimine la durée des infections partielles
- ☑ Pas besoin de matériel supplémentaire: ni équipements, ni agents
- ☑ Permet une réaction rapide et précise aux incidents
- ☑ Réduit le besoin en personnel de sécurité expert

## CAS D'USAGE: CHASSE AUTOMATISÉE DE MENACES

La technologie Autonomous Investigation de SecBI permet aux analystes de rechercher les menaces plus efficacement et de mieux comprendre ce qui se passe dans leur environnement. Les analyses sont intégrées à des données d'analyse forensique hautement fiables sur plusieurs niveaux, allant de métadonnées appuyant les enquêtes sur les utilisateurs ou les incidents, jusqu'aux données brutes, permettant ainsi aux analystes sécurité de tester des hypothèses. Une architecture basée sur le big-data permet à SecBI de changer d'échelle facilement et à moindre coût, en élargissant la fenêtre de recherche sur plusieurs mois et années.



## LE PROCESSUS




## SIGNES D'UNE VRAIE TRANSFORMATION DU SOC

- ☑ Amélioration drastique de la productivité des analystes
- ☑ Détection de la portée complète de chaque incident suspect
- ☑ Chasse de menaces plus rapide et plus efficace
- ☑ Réponse automatisée aux violations et prévention d'attaques futures

## DÉPLOIEMENT EN QUELQUES HEURES

La solution SecBI se déploie facilement et instantanément sans équipements ou agents supplémentaires. Le déploiement peut être effectué sur site ou dans le cloud. Votre SOC est immédiatement renforcé sans aucune modification de l'infrastructure réseau. Votre personnel SOC est rapidement formé à l'utilisation de la solution. Aucun service professionnel supplémentaire n'est nécessaire.

SECBI AUTONOMOUS INVESTIGATION™

www.secbi.com

info@secbi.com