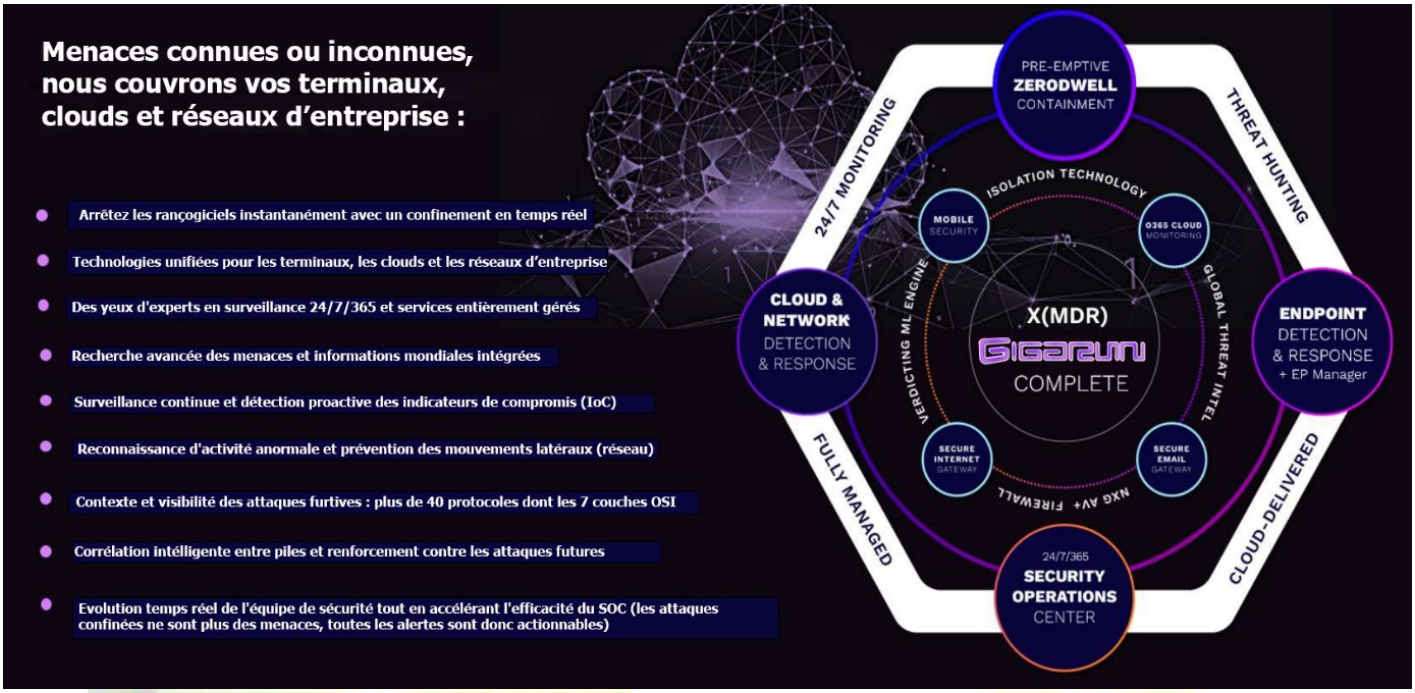


Les cyberattaques et les normes de conformité évoluant rapidement, protéger votre organisation devient de plus en plus complexe et implique l'utilisation de meilleurs outils pour vous aider à atténuer les attaques ou éventuellement à réduire leur impact.

Car un antivirus seul n'est aujourd'hui plus suffisant pour assurer votre cyberdéfense. C'est pourquoi de nombreuses organisations adoptent des outils SIEM pour sécuriser leurs systèmes, applications et infrastructures dans le cloud ou sur site.

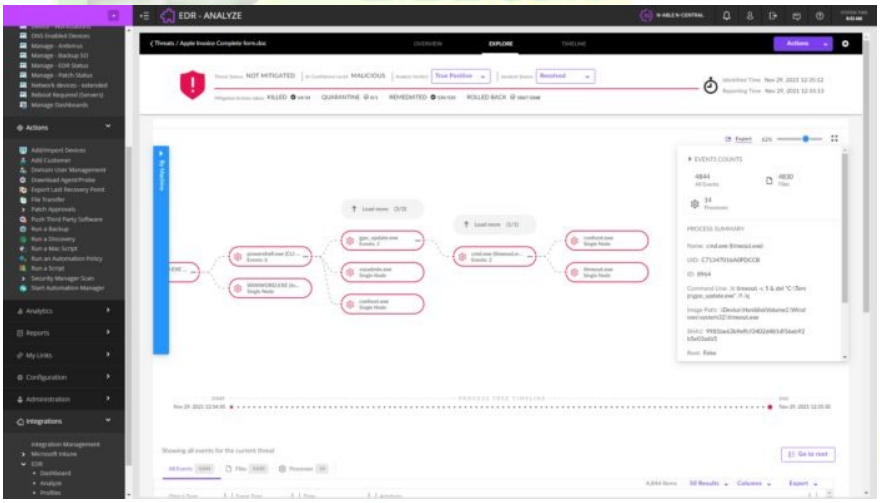
Les technologies SIEM combinent la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM) au sein d'un même système de gestion de la sécurité.

Mais même le meilleur système de protection au monde n'est désormais plus suffisant. Il faut également assurer le suivi de ces outils et de vos infrastructures par le biais d'une équipe de spécialistes de la sécurité et de la cyberdéfense afin de répondre aux attaques, empêcher les intrusions et prévenir la violation de données. Ceci 24h sur 24 et 7 jours sur 7 car les attaques les plus violentes se déroulent toujours durant les périodes les moins suivies (nuit, week-end etc…)

Face au nombre croissant d'attaques sur l'ile de la Réunion (CHU de Saint Pierre, LEAL Réunion etc…) Gigarun à mis en place un service de cybersécurité (www.cybersecure.re) Qui combine l'utilisation d'outils de cyberdéfense et le suivi permanent des appareils sous protection par une équipe de spécialistes cybersécurité. Cette équipe dédiée au suivi du Security Operation Center (SOC) assurent la supervision de la sécurité de vos actifs et intervient rapidement en cas d'incident ou d'attaque, et ceci en permanence.

La solution SIEM étant lourde, couteuse et inadaptée aux PME, notre solution SaaS Endpoint Détection and Response / Extended Detection and Response (EDR/XDR) traite les endpoints (Postes, téléphones, serveurs etc…) mais également les logs recueillis sur les divers organes du réseau (firewall, AD, mails etc…). Notre équipe SOC analyse et corrèle ces données afin de traiter efficacement les incidents à la source.

C'est une approche SIEM, implémentée au sein d'une solution cloud unifiée ou l'équipe SOC surveille les évènements en temps réel et analyse ces derniers pour traiter les véritables alertes qui seront isolées des faux positifs.



En effet les attaques se produisent en quelques minutes et secondes durant lesquelles il faut être réactif pour éviter d'en subir les conséquences néfastes. L'impact d'une attaque ne se produit pas toujours instantanément. Un intrus peut mettre un certain temps (25 jours en moyenne) à s'attarder pour prendre pied et énumérer les ressources à sa disposition pour exécuter des missions de recherche, de destruction ou d'exfiltration de données qui seront lancées de nuit ou en W-E. Le SOC intercepte et isole l'attaque avant que ses impacts et dommages intentionnels ne se produisent. C'est donc une course contre l'attaquant, et lorsqu'il s'agit d'intrus entrant dans vos points de terminaison, nous protégeons d'abord, puis nous posons des questions et identifions, détectons et rendons un verdict en second lieu.

Nous protégeons aussi nos clients dans le traitement de transactions par carte bancaire et leur évitons des amendes paralysantes dues à une compromission. Nous recherchons les informations de paiement exposées en effectuant des analyses PCI DSS et PAN.

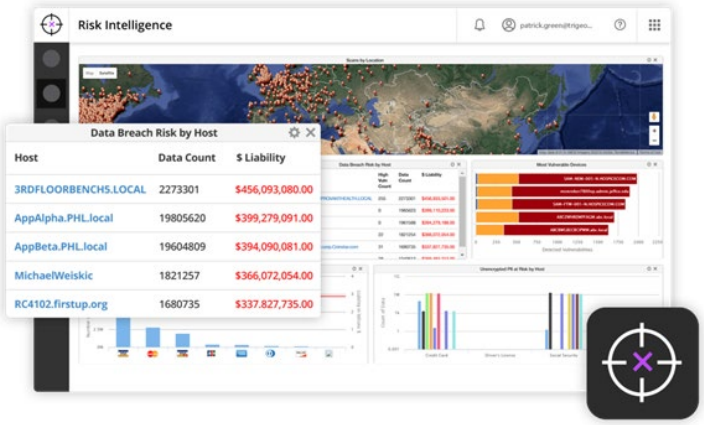
Notre outil de gestion intelligente des risques vous permettra de disposer de rapports chiffrés, à la demande, qui évaluent le coût potentiel d'une violation de données.

Il localise les données sensibles à risque sur vos réseaux et postes de travail gérés, et détermine le coût potentiel d'une violation de données.

Parmi les fonctionnalités incluses :

- Analyse approfondie des vulnérabilités
- Rapports personnalisables détaillant l'impact financier des risques

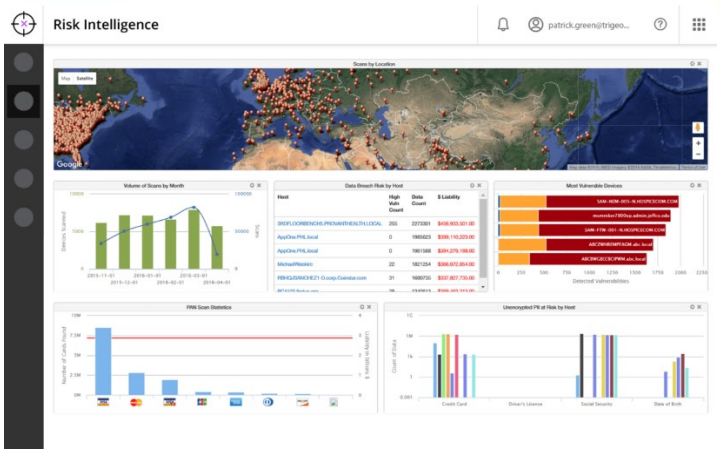
- Identification des accès utilisateur inappropriés
- Analyses PCI, DSS, PAN et PII
- Identification des données à risque
- Rapports sur les tendances de risques pour un suivi des améliorations



Convertir une liste de vulnérabilités détectées par une analyse avec une valeur financière que vous comprendrez facilement vous fera prendre la mesure de la valeur ajoutée de ce service et des rapports détaillés répertoriant :

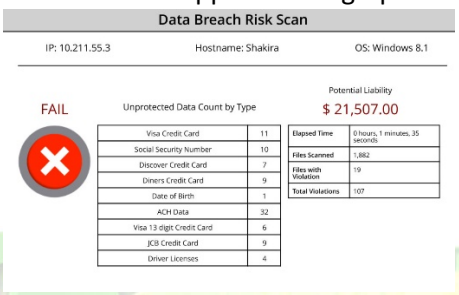
- Les informations d'identification personnelle (PII) exposées qui informent du risque de ne pas réussir un audit de conformité.

- Les rapports de tendances qui montrent la diminution des risques et l'apparition de nouvelles vulnérabilités.



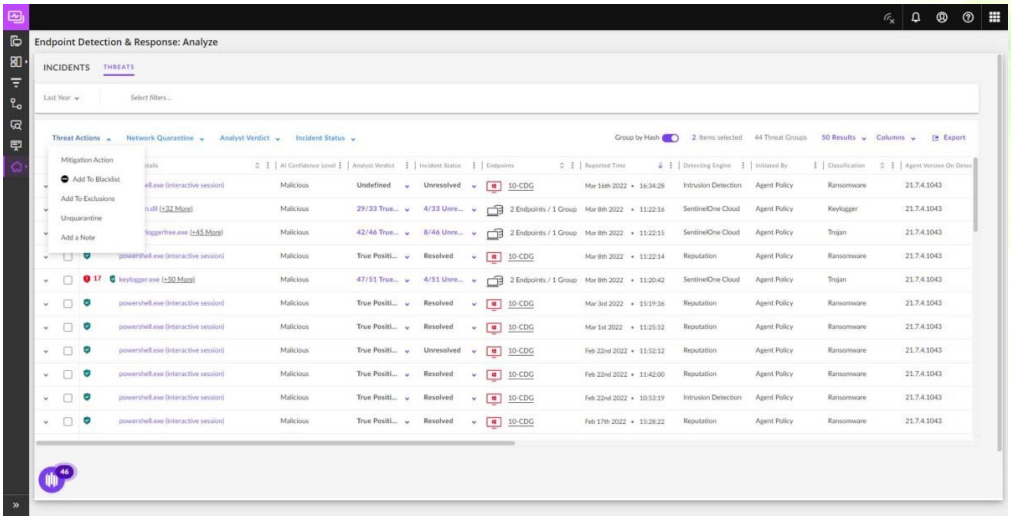
En attribuant une valeur financière à la vulnérabilité des données, nous prouvons la rentabilité de la protection des données et hiérarchisons les problèmes à résoudre en :

- Repérant les vulnérabilités PII, PAN et PCI DSS
- Évaluant les risques liés aux données sur les postes de travail, serveurs et applications SaaS.
- Estimant le coût des risques identifiés.
- Générant des rapports cartographiant la réduction des risques.



Notre SOC assure le contrôle, la détection des attaques et la réponse aux incidents ainsi que la mise en conformité de votre système d'information en assurant les services de :

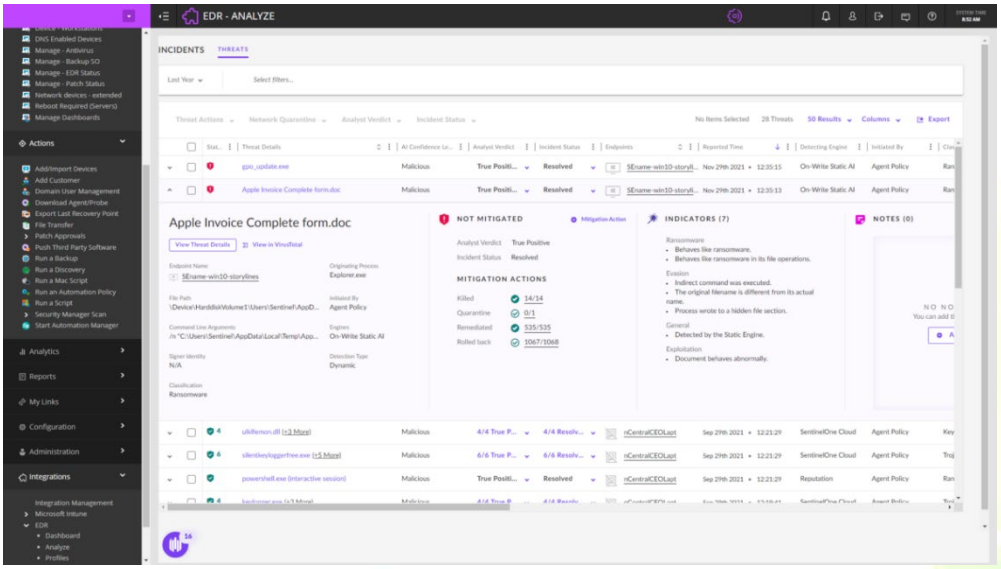
- Détection des comportements potentiellement malveillants, comme la modification de clés de registre ou le lancement de certains processus.
- Contextualisation des détections et représentation visuelle de l'attaque, avec tous les hôtes touchés
- Renseignements (threat intelligence) sur les cybermenaces existantes
- Conseils pratiques de réponse, pour aller plus loin qu'un simple descriptif basique des événements
- Blocage des attaques à distance, en isolant les hôtes touchés du reste du réseau
- Restaure les appareils (Windows uniquement) en cas d'attaque de ransomware en quelques minutes ou secondes, et non des heures



Leur intervention permet d'éviter les attaques complexes et ciblées qui sont conçues sur mesure pour attaquer un environnement spécifique. Elles sont de ce fait plus résistantes aux solutions de cybersécurité standard.

- Exploitation des vulnérabilités : les pirates informatiques cherchent à exploiter des failles de sécurité courantes présentes sur vos systèmes exposés au public. 57 % des violations de données font suite à l'exploitation de vulnérabilités connues qui auraient pu être corrigées.

- Spear phishing : extrêmement efficace et très courant, le spear phishing repose sur des communications trompeuses et ciblées. Ces communications ont pour objectif d'inciter un membre de votre entreprise à partager des informations sensibles ou de le pousser à ouvrir un fichier exécutable.
- Attaques de type "Watering hole" : le hacker recherche des vulnérabilités sur des sites web utilisés par vos employés et infecte un ou plusieurs de ces sites avec des malwares.
- Attaques Man-in-the-middle : le hacker intercepte vos communications et ne les transmet qu'après les avoir examinées, voire modifiées. Il crée l'illusion que vous parlez directement à votre interlocuteur de confiance.
- Achat d'accès : un nombre colossal d'attaques est mené en permanence sur un nombre colossal de systèmes. Les accès obtenus sont revendus sur le darknet.



Force d'identification rapide des éventuelles attaques internes ou externes, le SOC permet d'agir rapidement pour répondre aux incidents. Obtenez également une visibilité immédiate sur les applications et les services cloud potentiellement nuisibles ou indésirables.

- Identifiez automatiquement les menaces avancées, et hiérarchisez les priorités en fonction du risque encouru et du degré de criticité de l'hôte.
- Obtenez un aperçu contextualisé des attaques : visualisez toutes les détections et tous les hôtes pertinents sur une période donnée.
- Stoppez rapidement les attaques grâce à des recommandations pratiques ou à des actions de réponse ciblée, mise en œuvre plus facilement et plus rapidement car des procédures ont été établies en amont pour agir en fonction du type d'incident. La rapidité est un élément clé pour limiter les dégâts, notamment dans le cas d'une infection par un malware.
- Résolvez les cas difficiles grâce à des analyses d'incidents à la demande et à des investigations menées par des Threat Hunters de renommée mondiale.
- Réduisez vos frais de gestion grâce à une solution endpoints cloud-native à client unique.
- Externalisez le monitoring avancé des menaces chez un fournisseur de services managés certifié.
- Le service permet d'alerter nos consultants : ils accèdent ainsi immédiatement aux données de l'incident pour vous aider à le résoudre.

Évitez les pannes coûteuses, les pertes de données et les rançons. Ayez l'assurance de pouvoir gérer votre entreprise tout en faisant face aux cybermenaces en adoptant notre service SOC de cyberdéfense EDR et XDR cloud.