



Management de la surface d'attaque grâce à la prédiction des chemins d'attaque par l'IA

Découvrez vos faiblesses de sécurité et traduisez-les en contre-mesures prioritaires

MAÎTRISEZ LES CHEMINS D'ATTAQUE POTENTIELS AVEC UNE SOLUTION PRÉDICTIVE PILOTÉE PAR L'IA

Identifier et comprendre les chemins d'attaque qu'un acteur malveillant pourrait emprunter en exploitant tout type de vulnérabilités ou de faiblesses au sein du système d'information devient une priorité absolue pour les RSSI afin de maîtriser leur surface d'attaque, de prévenir les attaques et de les arrêter avant qu'elles ne portent. La plateforme de gestion des chemins d'attaque SCUBA, alimentée par notre technologie unique d'IA brevetée, prédit et cartographie visuellement tous vos chemins d'attaque comme vu à travers les yeux d'un attaquant. Il fournit aux équipes des mesures de remédiation efficaces et prioritaires. Identifier proactivement les chemins d'attaque permet de réduire le risque sur votre activité grâce à une gestion fine des vulnérabilités et à la segmentation du réseau, afin que les équipes puissent réduire la surface d'attaque globale.

CONSTRUISEZ VOTRE RÉPONSE AVANT LES ATTAQUES AVEC DES REMÉDIATIONS PRIORISÉES

La plateforme SCUBA fournit le contexte de vos faiblesses de sécurité pour comprendre comment et où les attaquants se déplacent dans le réseau et quels sont les chemins possibles qu'ils peuvent emprunter après avoir réussi à compromettre un actif. SCUBA enrichit automatiquement ces chemins d'attaque avec les vulnérabilités les plus récentes et les métadonnées MITRE ATT&CK. Cela permet à vos équipes de prendre des mesures proactives et prioritaires recommandées par SCUBA pour perturber ces chemins avant leur exploitation, réduisant ainsi considérablement les risques sur vos actifs et informations.

PRINCIPAUX AVANTAGES

Cartographie en temps réel des chemins d'attaque et du risque opérationnel

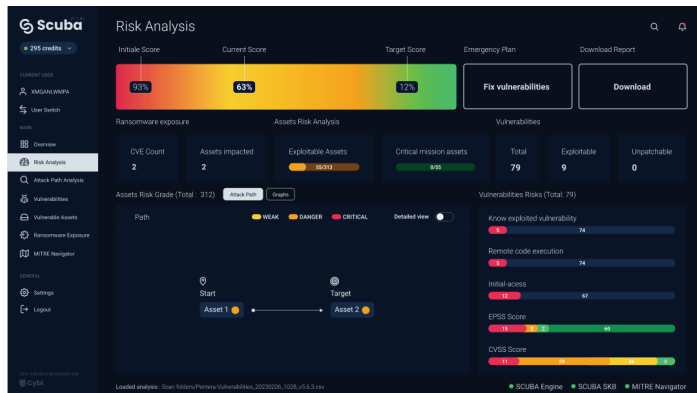
Prendre l'avantage sur les attaquants avec des stratégies de remédiation prioritaires.

Déploiement "plug and play", sans agent, autonome ou intégré
Obtention des résultats en quelques minutes.

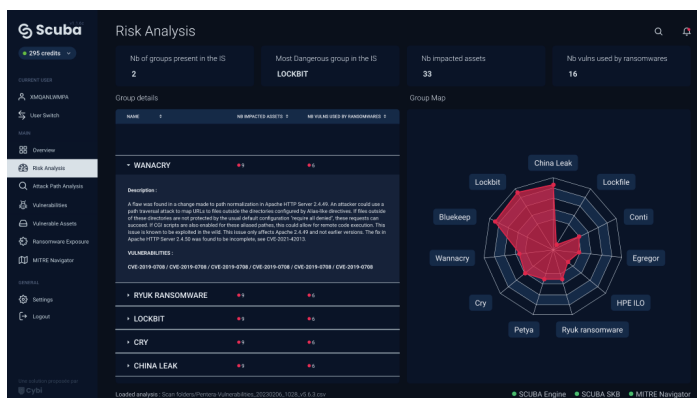
Support complet des normes de sécurité, y compris MITRE ATT&CK, NIST et CISA.

Optimisation des ressources et gain de temps

Obtenez une vue à 360° du risque cyber de vos actifs critiques par la prédiction des chemins d'attaque. Avec SCUBA, vous obtenez une vue complète et approfondie de la surface d'attaque, augmentée avec des chemins d'attaque pour mieux comprendre les attaquants, et un plan de priorisation de vos actions de remédiation.



Découvrez et priorisez proactivement les faiblesses et les vulnérabilités associées aux chemins d'attaque au sein de votre réseau Réduisez votre exposition aux attaques et aux ransomwares en suivant les conseils de remédiation étape par étape de SCUBA.



Contractez nous par e-mail avec **contact@cybi.fr**

SCUBA enrichit les actifs et les vulnérabilités avec des métadonnées telles que le score CISA KEV EPSS, les tactiques et techniques MITRE ATT&CK et les expositions potentielles liées à l'exploit de ransomware pour vous aider à prendre des décisions plus éclairées.

[illegible]

SCUBA offre la flexibilité de deux modes de déploiement. On-prem pour garder vos données sur site et sous votre contrôle. SaaS, pour que vous puissiez tirer parti du cloud. Aucun agent et aucun privilège ne sont requis. Vous pouvez utiliser votre propre scanner de vulnérabilités ou vous fier au Scanner SCUBA pour analyser vos actifs en quelques clics afin de comprendre votre exposition.

Fruit de l'alliance de chercheurs issus des laboratoires du LORIA et d'Inria (Laboratoire haute sécurité LHS) et d'entrepreneurs en Cybersécurité, Cybi est un éditeur de logiciel de cybersécurité français qui propose une technologie unique d'attack path management basée sur des moteurs d'intelligence artificielle brevetés, et permet de définir une politique d'application des patchs optimisant l'utilisation des ressources financières et humaines.