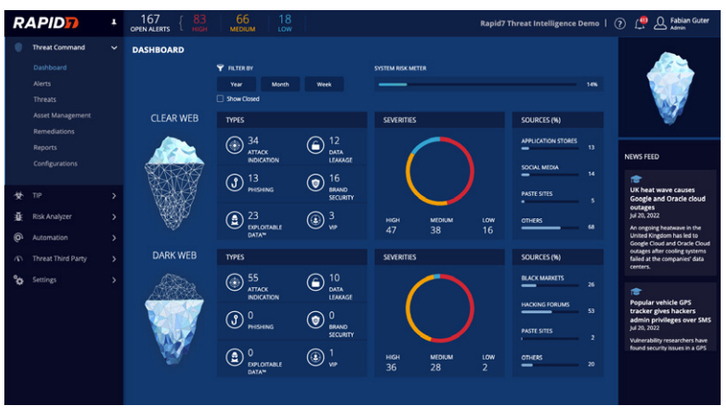
Maîtriser les menaces du web, du deep web et du darknet

Alors que de nombreuses entreprises accordent une attention accrue à la cybersécurité interne, elles savent souvent peu de choses sur ce qui se passe sur Internet sous le nom de l'entreprise. Threat Command, la solution external threat intelligence de Rapid7, permet de combler cette lacune. Threat Command détecte les faux domaines, les faux profils de médias sociaux et les données divulguées et facilite l'élimination de ces menaces externes.

Les entreprises suisses avec une marque forte sont à la pointe en matière de cybersécurité lorsqu'il s'agit de se défendre contre les menaces qui visent le réseau interne. En revanche, ce qui se passe au nom de l'entreprise sur le clear web, le deep web ou le darknet n'est souvent pas clair. Des domaines falsifiés sont-ils utilisés pour des campagnes de phishing? Existe-t-il de faux profils de médias sociaux qui nuisent à la réputation des représentants de l'entreprise? Des cybercriminels proposent-ils des données d'entreprise divulguées sur le darknet? De telles activités malhonnêtes peuvent causer d'énormes préjudices.



Les renseignements sur les menaces externes protègent les assets et la réputation

Threat Command, la solution external threat intelligence de Rapid7, s'attaque à tous ces problèmes. Une plateforme *cloud native* intuitive collecte automatiquement des informations liées à l'entreprise – même dans les zones d'Internet difficiles d'accès – et génère des analyses de risques approfondies. Grâce à son équipe d'analystes spécialisés, Rapid7 va encore plus loin: les experts effectuent des recherches ciblées sur le deep web et le darknet, détectent les menaces stratégiques et, si nécessaire, éliminent les menaces détectées – de la suppression d'un faux domaine à l'achat de données fuitées pour les rendre inaccessibles à d'autres personnes intéressées.

Une solution globale unique

La combinaison entre une plateforme cloud automatisée et l'expertise d'analystes spécialisés rend Threat Command unique en son genre par rapport aux autres solutions de protection de la réputation. Les clients ne reçoivent pas seulement des rapports standardisés, mais également des rapports sur mesure et précis ainsi qu'une assistance spécialisée de la part de l'équipe d'analystes de Rapid7 – conseils personnalisés inclus. Chez les fournisseurs qui ne proposent qu'une plateforme logicielle, les clients ou leurs partenaires de cybersécurité doivent se charger eux-mêmes de l'analyse et de la résolution des problèmes. Or, il est extrêmement difficile de trouver les spécialistes nécessaires. L'exemple d'une banque privée, qui ne dispose que de deux collaborateurs dans le domaine de la sécurité, montre clairement que même les entreprises établies ont besoin d'un soutien que le partenaire informatique existant ne peut pas fournir en raison du manque de personnel qualifié. Et les fournisseurs qui ne misent que sur des experts ne peuvent faire évoluer leurs prestations que de manière limitée.

Une mise en place rapide, des résultats rapidement obtenus

Threat Command peut être mis en place dans les 48 heures, par exemple sous forme de preuve de concept, et fournit les premiers résultats en très peu de temps sur la base d'une vaste base de données de renseignements sur les menaces externes. Il suffit au client de fournir une liste de ce qui doit être analysé – comme des noms d'entreprises et de marques, des adresses IP ou des noms de collaborateurs. Puis des analyses plus approfondies suivent dans un délai d'une à deux semaines. L'entreprise peut donc rapidement se rendre compte de l'utilité de la solution et décider si Threat Command est adapté à sa situation ou non (il y a déjà eu des clients pour lesquels aucune menace externe n'a été détectée).

Threat Command est intéressant à la fois pour les clients et pour leurs partenaires de cybersécurité. La mise en service et l'utilisation de la plateforme ne nécessitent aucune ressource technique de part et d'autre – ce qui réduit la charge de travail des équipes de sécurité existantes. Et pour les partenaires de distribution, c'est l'occasion d'acquérir de nouveaux clients ou de compléter leur offre de solutions et de services. Pour transformer les informations livrées par Threat Command en connaissances et en actes, il est toutefois nécessaire de disposer de connaissances d'experts – et celles-ci sont fournies avec Threat Command!

Une solution très demandée, des applications multiples

Threat Command suscite un vif intérêt en Suisse, tout particulièrement dans le secteur financier, important dans notre pays. Plus d'une demi-douzaine de banques utilisent déjà la solution. Les informations les plus demandées concernent les campagnes de phishing menées au nom de l'entreprise. En indiquant une plage de numéros de cartes de crédit, il est également possible de savoir si des données de cartes de crédit ont fuité. Threat Command n'est pas seulement intéressant pour le secteur financier, mais aussi pour d'autres branches fortement numérisées comme le commerce en ligne. Les cabinets d'avocats, qui ont besoin de tout savoir sur la réputation externe de leurs partenaires et de leurs collaborateurs pour des raisons évidentes, se montrent également intéressés.

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch