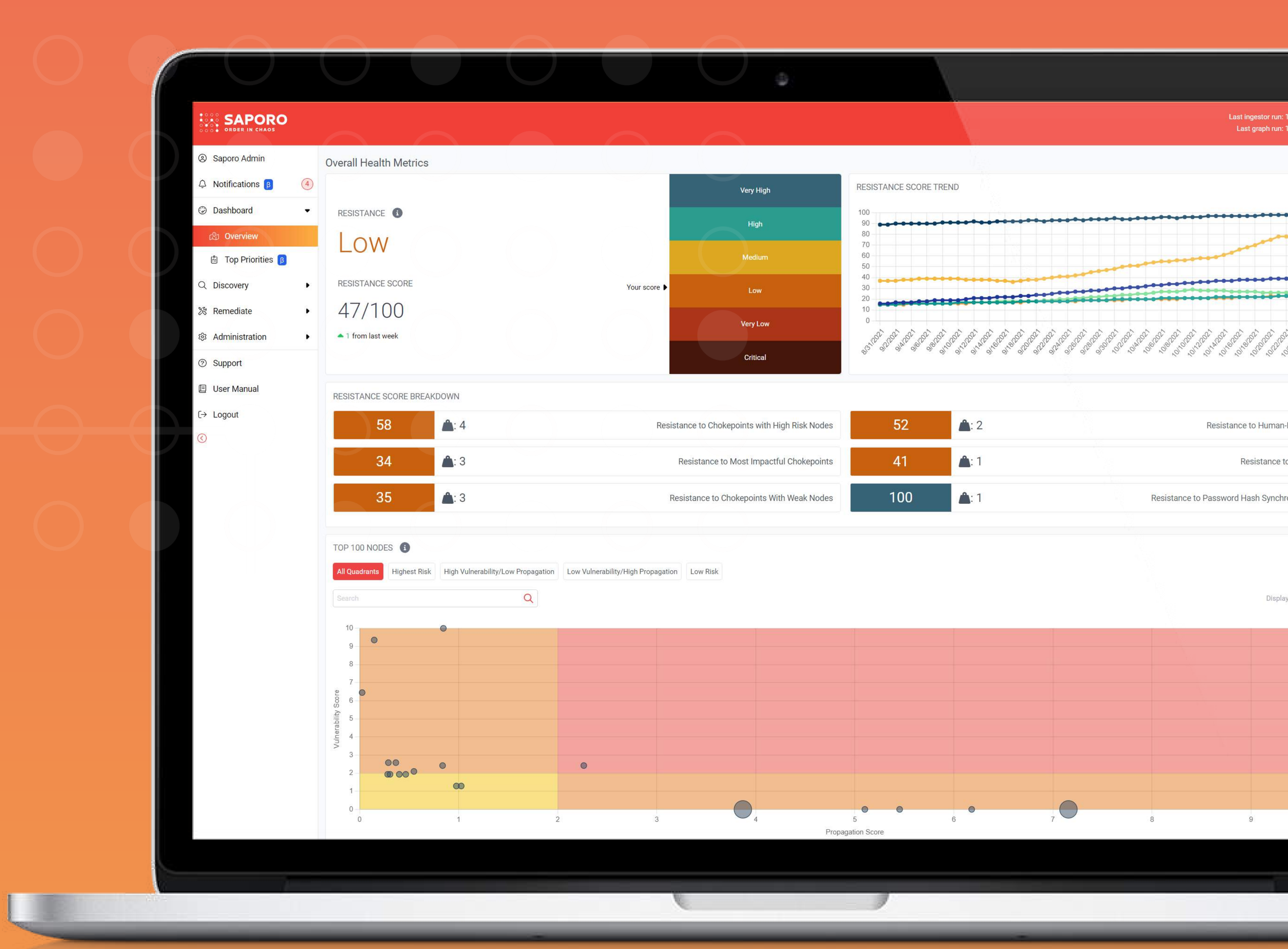
SAPORO
ORDER IN CHAOS

Découvrez vos lacunes en matière de sécurité grâce à

l'analyse des chemins d'attaque de vos identités



www.saporo.io

Qu'est-ce qu'une analyse des chemins d'attaque de vos identités ?

L'analyse approfondie des chemins d'attaque de vos identités par Saporo s'étend sur une période pouvant aller jusqu'à trois jours ouvrables, comprenant deux sessions distinctes : l'une consacrée à l'installation et l'autre à l'examen des résultats.

Ce que l'on peut attendre de notre offre de base :

Un **score de résistance** est fourni qui indique la difficulté pour un attaquant d'accéder aux actifs critiques dans votre environnement.

Les **10 principaux points névralgiques**, c'est-à-dire les endroits optimaux pour bloquer le plus grand nombre de chemins d'attaque liés à l'identité. Ce mécanisme vous permet d'identifier ce qui est le plus critique et à allouer les ressources de manière efficace.

Les **50 objets les plus dangereux** qui ont le potentiel de propager des attaques plus rapidement et plus facilement que d'autres, combinant à la fois des facteurs de vulnérabilité et de propagation élevée.

Un **rapport exploitable** contenant les résultats les plus importants et nos recommandations pour améliorer votre posture de sécurité.

Notre offre de base fournit des données provenant exclusivement d'Active Directory et comprend un modèle d'attaque. Cependant, pour les utilisateurs Azure et une gamme plus large de modèles d'attaques, nous offrons des options personnalisés. Pour plus d'informations, n'hésitez pas à nous contacter à l'adresse hello@saporo.io.

Pourquoi l'analyse des chemins d'attaque de l'identité ?

Une analyse des chemins d'attaque avec Saporo peut réduire de manière significative votre surface d'attaque interne en découvrant les dangers les plus critiques que d'autres outils et services ne verraient pas. Notre technologie innovante fournit une analyse complète pour assurer la sécurité de vos actifs critiques.

Gestion des risques
Évaluez votre niveau de risque actuel et établissez votre seuil de risque d'une manière différente. L'analyse de Saporo dépasse l'approche conventionnelle qui consiste à fournir une simple liste de vulnérabilités de sécurité. Au lieu de cela, elle met l'accent sur les risques qui ont le plus grand impact sur votre environnement, vous permettant ainsi de prendre des décisions éclairées concernant les mesures de sécurité.

Une transformation consciente des risques
Vous envisagez de migrer votre infrastructure informatique vers le cloud ? Protégez vos actifs critiques et assurez une transition en douceur en testant votre résistance aux risques de sécurité potentiels. Saporo vous aide à identifier toutes les configurations erronées qui pourraient menacer votre posture de sécurité dans le Cloud.

Effectuez-vous régulièrement des pentests ?
Bien que les pentests soient très utiles pour tester votre capacité à détecter les menaces et à y répondre, leur portée est limitée. Avec cette analyse, vous pouvez obtenir une image complète de vos risques liés à vos l'identités à travers des millions de chemins d'attaque et des centaines de problèmes de configuration communs, que vous pouvez corriger immédiatement.

C'est simple et facile à démarrer

En investissant un peu de temps dans votre sécurité dès maintenant, vous pouvez réduire considérablement votre surface d'attaque et les risques, tout en économisant un nombre important de ressources en cas d'attaque.

Nous en sommes conscients. C'est pourquoi nous avons fait de Saporo une solution rapide et évolutive.

- ☑ **L'installation se fait en quelques minutes**
- ☑ **Notre solution est sans agent et ne nécessite qu'un seul compte utilisateur en lecture seule**

Obtenez tous les avantages avec
une gestion continue de la surface d'attaque

Ne passez pas à côté de l'image complète avec Saporo fonctionnant 24/7 et fournissant des informations quotidiennes sur l'impact des configurations d'identité ! En plus de tous les avantages liés à l'analyse, notre abonnement complet offre également :

ANALYSE D'IMPACT

Adoptez les principes de la sécurité dès la conception en simulant en toute sécurité les changements avant qu'ils ne soient mis en œuvre dans un environnement de production.

LOGS

Vous pouvez désormais obtenir le contexte des alertes provenant d'autres systèmes grâce à la surveillance en temps réel de l'activité dans les répertoires pris en charge.

INTEGRATIONS

Intégrez votre solution avec Saporo en utilisant notre API ouverte ou construisez une intégration personnalisée selon vos besoins.

L'ACCÈS À TOUS LES MODÈLES

Exploitez tous nos modèles, tels que les ransomwares, les points d'étranglement pour les attaques DCSync, les points d'étranglement avec des nœuds à haut risque et bien d'autres encore.

TOUTES LES SOURCES DE DONNÉES

L'ingestion et l'analyse de données provenant de sources importantes telles que Active Directory, Azure, AWS et Okta, et d'autres encore seront bientôt disponibles.

SUPPORTED DATA SOURCES

Microsoft Active Directory · Azure · amazon web services · okta · kubernetes (Coming soon) · GitHub (Coming soon) · Google Cloud (Coming soon) · salesforce (Coming soon)