

## Gestion de la surface d'attaque des identités

L'identité est la principale surface d'attaque. Saporor réduit considérablement votre surface d'attaque interne grâce à une meilleure segmentation des accès aux ressources critiques et à la résolution des mauvaises configurations.

**80%**

des cyberattaques exploite l'identité

**94%**

des actifs critiques peuvent être compromis facilement.

**40%**

40% des admin fantômes exploitables en une seule étape.

## Découvrez et analysez vos systèmes comme un attaquant.

Explorez et analysez votre environnement comme un attaquant. Identifiez et corrigez les accès les plus risqués. Si la majorité de vos utilisateurs peuvent devenir administrateurs en quelques étapes, cela doit être la priorité.

### Identifiez et corrigez

- **Segmenter** les identités critiques pour réduire les risques.
- **Découvrir** les chemins d'attaque à grande échelle.
- **Détecter** les mauvaises configurations pour réduire les failles
- **Surveiller** les changements pour éviter l'expansion de la surface d'attaque.

### Sources de données principales



Microsoft  
Active Directory



Azure



File Shares



ADCS



Entra ID



365



Usage of  
Permissions



Sessions



VMs



Resources



Apps



And more.

### Sources de données complémentaires



okta

**“**Saporor est un outil de défense indispensable pour toutes les organisations qui veulent avoir une longueur d'avance dans la gestion des risques au sein de leurs infrastructures de plus en plus complexes.”

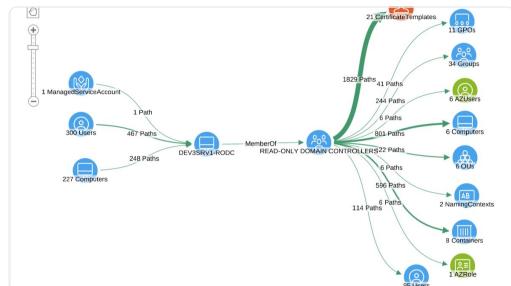
Christophe Bouillard  
CISO à Bank Mirabaud & Cie

# Résistez aux attaques basées sur l'identité



**Réduisez considérablement votre surface d'attaque des identités**

**Empêchez l'accès facile aux actifs critiques** et éliminez des millions de chemins entre utilisateurs et actifs privilégiés



Misconfigurations to resolve to increase your score from Critical to Poor			
To improve your score to a higher level, you must solve all of the following misconfigurations			
Severity	Name	Affected Nodes	Paths to HVY
critical	Dangerous ACLs expose domain controller objects (attack path)	670	181,508
critical	Dangerous control paths expose privileged user/group from standard users	271	104,406
critical	AD Credential Dumping - DCSync (indirect)	65	24,787
critical	Privileged accounts with SPN	61	20,011
critical	AD Credential Dumping - DCSync	21	8,384
critical	Dormant privileged user accounts (1 year)	24	7,392



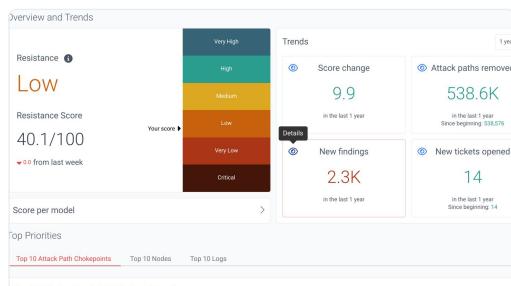
**Priorisez les ressources sur ce qui compte le plus**

**Focalisez-vous sur les risques critiques.** Saporoo corrèle les mauvaises configurations avec des référentiels (**ANSSI, MITRE, CIS**) pour prioriser les remédiations.



**Surveillance continue pour rester protégé**

**Suivez les changements à risque en temps réel.** Les mises à jour système de routine peuvent affecter votre posture de sécurité.



## Installation facile et flexible

Évolutif et sans agent, Saporoo s'installe en une heure, avec seulement un accès en lecture requis. Déployable sur site ou dans le cloud.

**Contactez-nous**  
[www.saporoo.io](http://www.saporoo.io)  
[hello@saporoo.io](mailto:hello@saporoo.io)



JURY's Favorite



#29 in 2024



Best Cyber Security