



Resister aux attaques basées sur l'identité

L'identité est votre principale surface d'attaque.



Olivier Eyries

Co-founder & CEO

www.saporo.io



Ce que fait Saporo

Saporo réduit votre surface d'attaque liée à l'identité pour mieux résister à 80 % des attaques.

95 % des organisations utilisent Microsoft Active Directory et/ou Azure.

Main data sources



Microsoft
Active Directory



Azure



File Shares



ADCS



Entra ID



365



Usage of
Permissions



Sessions



VMs



Resources



Apps

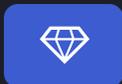
And more.

Companion data sources



okta

Les problèmes que Sapiro résout



Il est trop facile pour les attaquants d'accéder aux actifs critiques.

40%

des administrateurs fantômes peuvent être exploités en une seule étape.
proofpoint.



Absence de segmentation adéquate des identités.

80%

des cyberattaques exploitent des techniques basées sur l'identité.
CROWDSTRIKE



Le volume est tels que l'automatisation est nécessaire.

94%

des actifs critiques peuvent être compromis en quatre mouvements ou moins par des attaquants.
XM Cyber



Réduit votre surface d'attaque liée à l'identité pour mieux résister à 80 % des attaques en :

- ✓ **Découvrant automatiquement** tous les chemins d'attaque liés aux identités à grande échelle pour prioriser les risques
- ✓ **Segmentant les identités** des actifs critiques pour atténuer les violations
- ✓ **Identifiant toutes les mauvaises configurations** afin de réduire les opportunités pour les attaquants
- ✓ **Proposant des correctifs** qui gêneront le plus les attaquants tout en impactant le moins possible l'activité
- ✓ **Surveillant en continu** les changements pour empêcher la croissance de la surface d'attaque liée à l'identité

Une technologie unique et suisse

Différenciateurs

Pourquoi c'est unique

Pourquoi c'est important



Théorie des graphes

Précision de l'analyse, pas de faux positifs.

Focus sur ce que les attaquants peuvent faire.
75 % des expositions ne sont pas exploitables (a).



Couverture

Focus sur les identités à travers les systèmes.

Les attaques sont souvent transversales.
L'identité est le seul dénominateur commun.



Scalabilité

Rapidité de l'analyse, pas de crash.

Analyse continue à grande échelle.
Analysez une organisation de 250k utilisateurs en 2h.

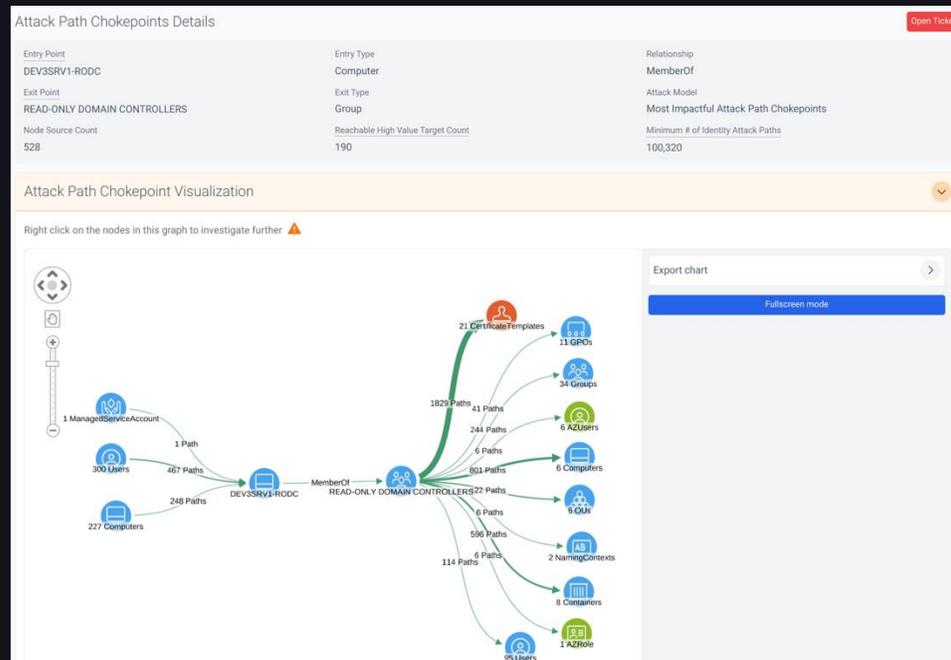
Notes:

a) [Attack path analysis – Rapid7](#)

Sécuriser l'identité: une approche transversale.



Segmenter vos annuaires et identités
(Tiering)



Trouver et corriger les misconfigurations critiques.
(ANSSI, MITRE, CIS)

Misconfigurations to resolve to increase your score from Critical to Poor

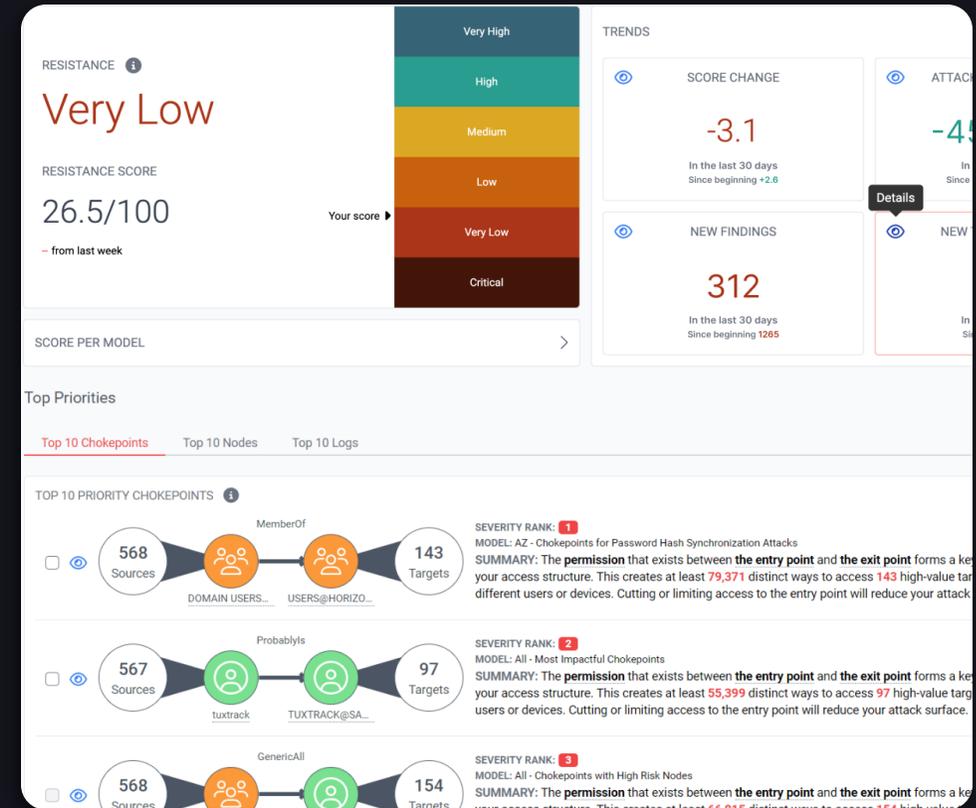
To improve your score to a higher level, you must solve all of the following misconfigurations

SEVERITY	NAME	AFFECTED NODES	PATHS TO HVT
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
critical	Kerberos pre-authentication disabled for privileged accounts	15	4,704

Mesurer votre résistance aux attaques compromettant les identités.

Si un attaquant peut devenir domain admin en moins de 5 étapes, les autres mesures défensives important peu.

Selon CrowdStrike, la durée moyenne de pénétration est de 62 minutes en 2024.



MERCI DE VOTRE ATTENTION !

Sondage de satisfaction
Merci de votre feedback



Scannez-moi

 Cyberdefense