

Identity risk has been a critical issue lately. How do we manage our attack surface?

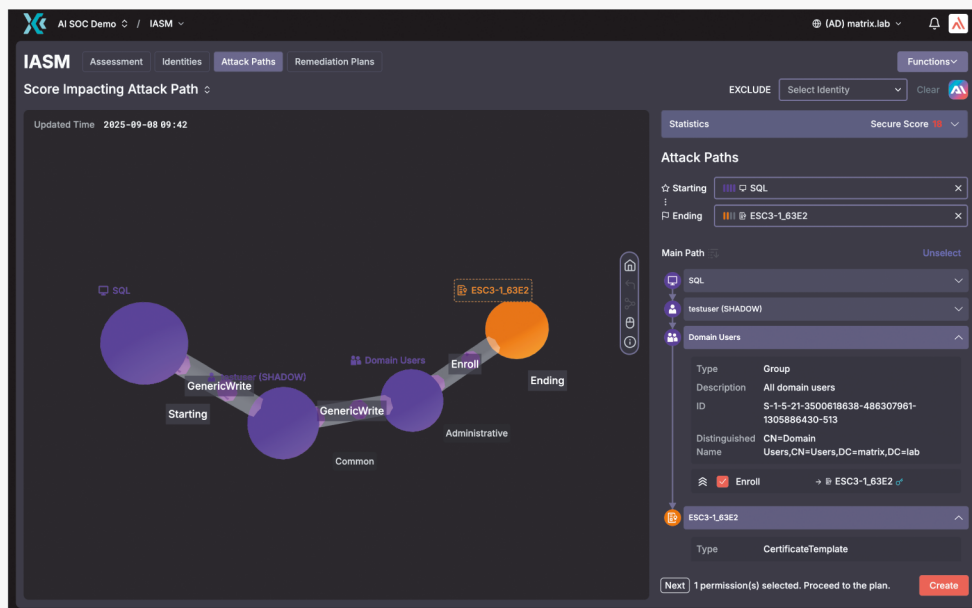
Over 40% of recent unauthorized intrusions are due to spoofing using legitimate user accounts and passwords, according to a global cybersecurity vendor.

Enterprise user account information is often traded on the black market and is popular among attackers.

It is easier to use a legitimate account to gain entry into an organization than to exploit a vulnerability.

Once an authorized user's account is obtained, various misconfigurations can be exploited to elevate privileges.

Start checking Active Directory settings as a first step for identity risk management!



Identity Attack Surface Management (IASM)

Effectively manage the processes of understanding identities within an organization, investigating risks, and implementing mitigating actions.



Visualize relationships among large numbers of complex users, devices, groups, and objects.



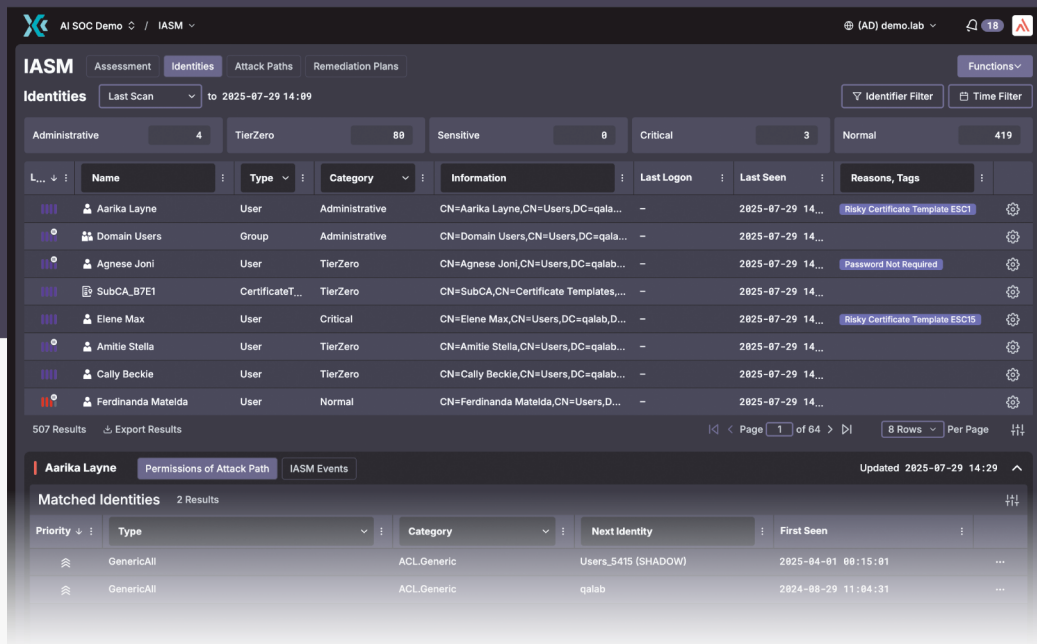
Leverage AI to inventory IDs in the enterprise, identify hidden privileged accounts, and automatically detect misconfigurations or over-authorization.



Use AI-driven attack simulations to detect attack paths exploited to elevate privileges to control privileged accounts.



Utilize CyCraftGPT to interpret intricate case contexts and rapidly gain better understanding.



Identities Last Scan to 2025-07-29 14:09

Administrative	TierZero	Sensitive	Critical	Normal
4	88	8	3	419

Name	Type	Category	Information	Last Logon	Last Seen	Reasons, Tags
Aarika Layne	User	Administrative	CN=Aarika Layne,CN=Users,DC=qala...	-	2025-07-29 14...	Risky Certificate Template ESC1
Domain Users	Group	Administrative	CN=Domain Users,CN=Users,DC=qala...	-	2025-07-29 14...	
Agnese Joni	User	TierZero	CN=Agnese Joni,CN=Users,DC=qalab...	-	2025-07-29 14...	Password Not Required
SubCA_B7E1	CertificateT...	TierZero	CN=SubCA,CN=Certificate Templates...	-	2025-07-29 14...	
Elene Max	User	Critical	CN=Elene Max,CN=Users,DC=qalab,D...	-	2025-07-29 14...	Risky Certificate Template ESC15
Amitie Stella	User	TierZero	CN=Amitie Stella,CN=Users,DC=qalab...	-	2025-07-29 14...	
Cally Beckie	User	TierZero	CN=Cally Beckie,CN=Users,DC=qalab...	-	2025-07-29 14...	
Ferdinanda Matelda	User	Normal	CN=Ferdinanda Matelda,CN=Users,D...	-	2025-07-29 14...	

507 Results Export Results

Page 1 of 64 8 Rows Per Page

Aarika Layne Permissions of Attack Path IASM Events Updated 2025-07-29 14:29

Matched Identities 2 Results

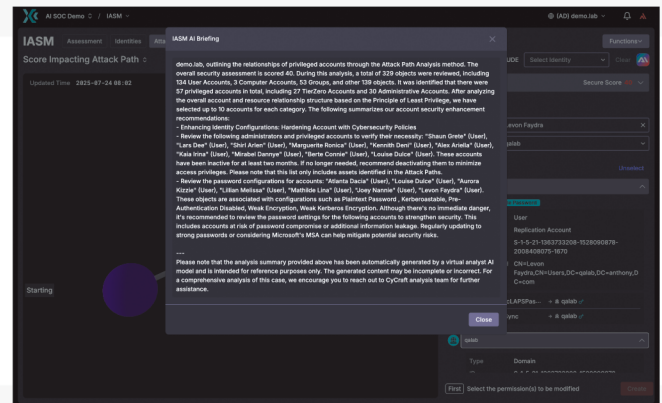
Priority	Type	Category	Next Identity	First Seen
GenericAll	ACL.Generic	Users_5415 (SHADOW)	2025-04-01 08:15:01	
GenericAll	ACL.Generic	qalab	2024-08-29 11:04:31	

XCockpit IASM Prioritizes AD Objects and Mobilizes Comprehensive Risk Management.



Case Interpretation with Generative AI

Combine the exclusively trained CyCraftGPT AI technology with our AD expertise to automatically generate incident briefings.



Our Service Procedure

Step 1

- Prepare an endpoint within the domain and execute AD information collection program.
- Upload the collected results to our cloud analysis site.

Step 3

- Quantify the security of the current configuration.
- Generate scripts for modification of configuration automatically.

Step 2

- Detect the existence of hidden privileged accounts, IDs with excessive privileges, and so on.
- Simulate attacks and identify attack paths.

Step 4

- After modifying the configuration, scan again to see if the risk has been mitigated.
- Repeat periodically to improve security posture.