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.

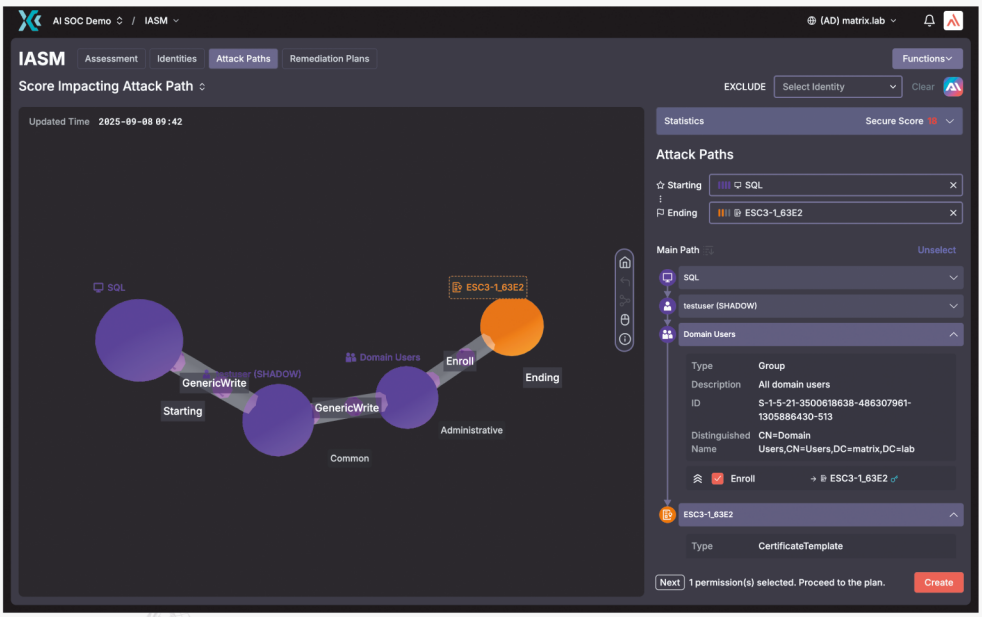
Enterprise user account information is often traded on the black market and is popular among attackers.

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!

XCOCKPIT IASM

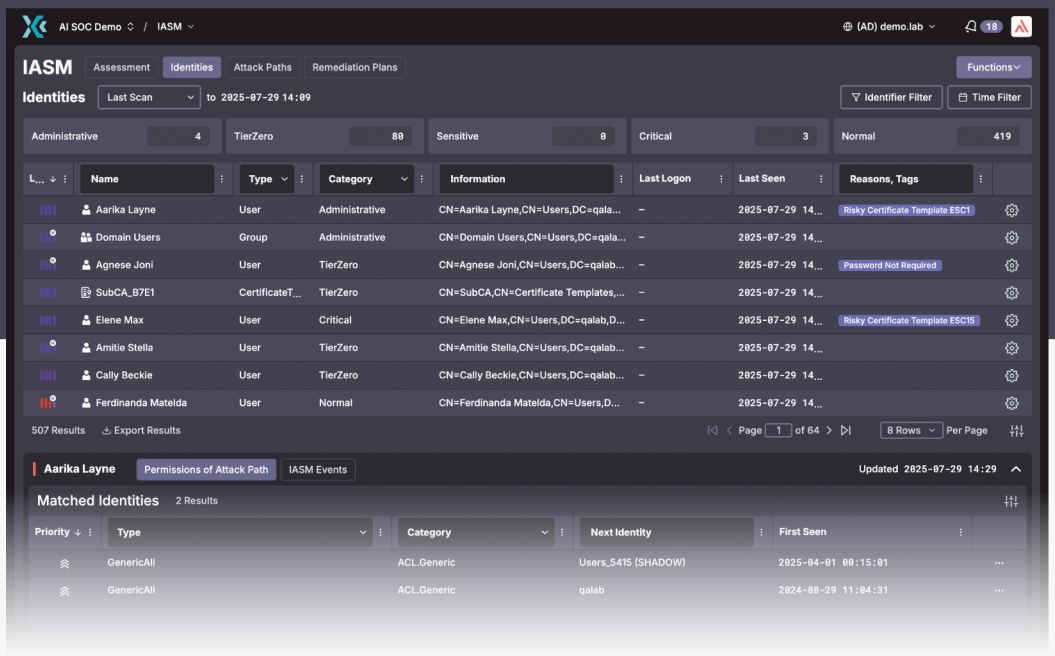


Identity Attack Surface Management (IASM)

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.

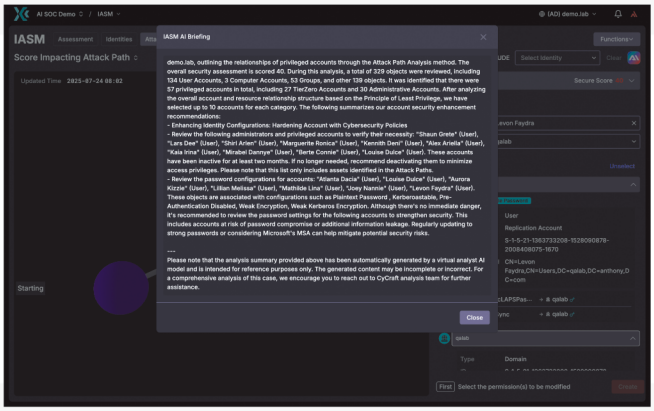
XCOCKPIT IASM



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 2

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

Step 3

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

Step 4

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