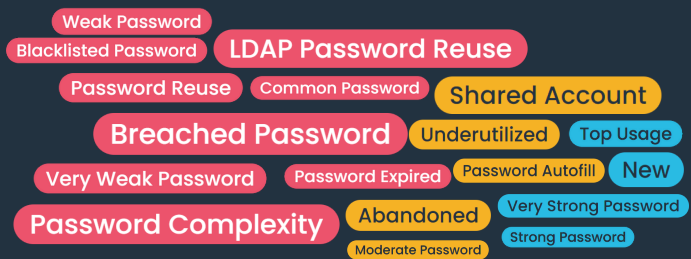


Tag Types

Scirge collects accounts and application metadata that are discovered by the Endpoint Browser Extension based on policies. Tags are associated based on password hygiene, usage trends, cloud intelligence, and correlation of events. Tags can be configured, and unique Tags can be created based on Custom criteria as well.

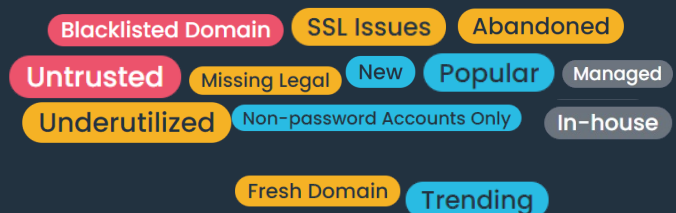
ACCOUNT TAGS

Tags relating to accounts are mainly concerned with password hygiene and usage trends. Some Tags can be customized, for example, to define password complexity, expiration, or blacklists.



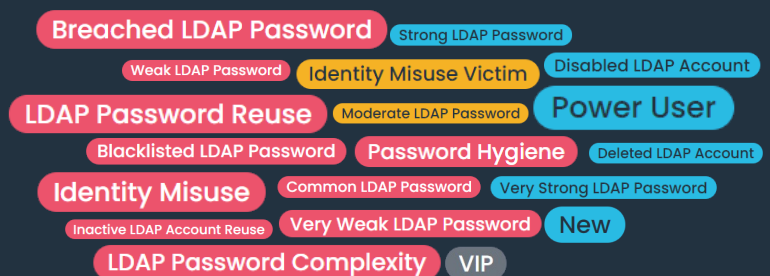
APPLICATION TAGS

Application Tags are showing usage trends and website reputation such as domain age, missing legal terms, or when they are blacklisted on spam lists.



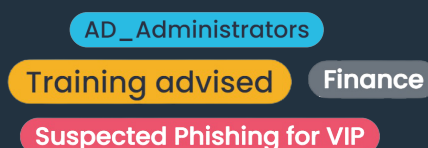
PEOPLE TAGS

People Tags show AD/LDAP-related password hygiene and account usage-related information, as well as potential signs of fraud.



CUSTOM TAGS

Custom Tags can be based on the correlation of other tags, manual assignment, and LDAP group membership.



Tags by Use Cases

Different Tags can be used to identify indicators of different risk types. Protection against account takeovers and hacking is based on password hygiene checks, while visibility and compliance are supported via complexity rules and account and application usage Tags.

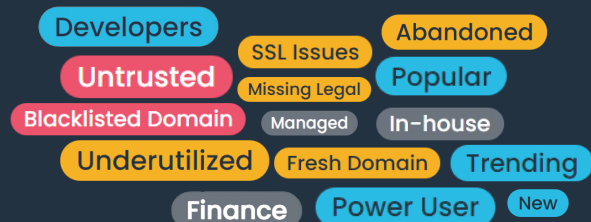
ACCOUNT AND PASSWORD PROTECTION

These tags reveal when unsecure passwords are created, or when accounts are misused from a security or compliance perspective.



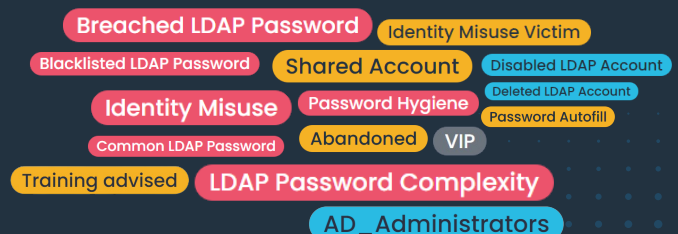
SHADOW IT DISCOVERY

Trends of application usage and indicators of risky websites are tagged for visibility into Shadow IT.



GOVERNANCE, RISK, AND COMPLIANCE

Logins on risky websites, usage of weak or shared passwords, and impersonating other employees are all indicators of misconduct and violation of regulations.



Correlations

Some Tags speak for themselves, but correlating them creates indicators that are more than the sum of its parts. These combinations can be set up using various alerting methods to warn employees or security operators, or utilized to assign additional Tags. Here are just some examples.

POTENTIAL PHISHING

Password reuse or new accounts on a recently registered, risky, or first seen domain indicates that a user may have fallen victim to a phishing attack.



HIGH RISK PASSWORD USAGE

Reusing passwords is risky enough, but when the password already has signs of weakness, it makes it crucial.



UNWANTED APPLICATIONS

Employees are concerned about getting their job done. But when Shadow IT applications emerge or are left behind, management must understand if there are any compliance risks or overheads created.



PROTECTING PRIVILEGED USERS

When accounts of high privilege user or ex-employees are utilized by other, it's an indicator of potential impersonation or internal fraud.



IDENTIFYING RISKY BEHAVIOUR

Employees with a high number of accounts with low overall password qualities, using unsanctioned password managers or shared accounts should be identified for further education.

