VECTR v8.0.0 Feature Breakdown

Table of Contents

Attack Automation

What is it?

VECTR's attack automation allows you to build individual test cases or entire campaigns as an executable. The executable can then be run on a target machine, where the test cases are run one by one, and the results logged. VECTR supports importing the log files, which will update data in the campaign dashboard for bulk execution and within individual test case panels for every test case run.

How does it work?

Documentation is provided here:
https://docs.vectr.io/vxf/configuration/

How can this feature help me?

- Import Atomic Red Team library using VECTR's data import feature and customize selected atomic tests for your environment
- Assemble automated campaigns for controls validation purposes, such as EPP/EDR and SIEM platforms
- Create new campaigns from threat intelligence sources and red team operations
- Create adversary emulation plans from threat intelligence sources, focused on TTPs suitable for automation

Support for rootless containers

What is it?

Provides additional security and allows for VECTR to run in a podman runtime environment.

How does it work?

The VECTR containers are now run with a UID/GID of 10001/10001. This allows for more granular control of what directories on the host are allowed to be written to from the container when using bind mounts. More information can be found on the FAQ page:
https://docs.vectr.io/upgrading/non-root-migration/faq/

Installation and upgrading instruction can be found on the migration page:
https://docs.vectr.io/upgrading/non-root-migration/

How can this feature help me?

See documentation links in previous section.

SSO Support

What is it?

Single Sign-On (SSO) enables the ability to offload authentication to an identity provider (IDP) of your choice.

How does it work?

You can configure any number of providers that support the following SSO protocols:
- OpenID Connect (OIDC)
- SAML2
- Azure AD

Documentation is provided here:
https://docs.vectr.io/sso/

How can this feature help me?

Allows your organization to use your existing identity provider to manage access.