Using Cloud Analytics with Caldera

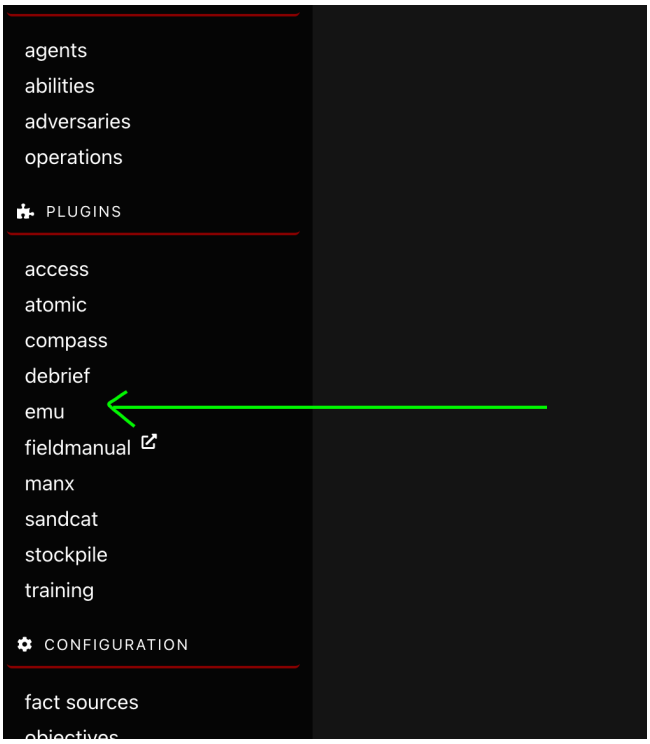
Using the emu plugin for Caldera makes it easy, but it is not obvious at all how it works. The high level process is as follows:

NOTE: Caldera 4.0.0-beta was used for the following instructions. Not tested on other versions.

Setup

Ensure EMU Plugin is Enabled

Make sure the emu plugin is enabled within Caldera. If not, navigate to *Configuration -> configuration-> Plugins*, and enable the emu plugin, and restart Caldera. When enabled, you should see `emu` on the left side menu.



Install New Advesary Emulation Plan

Option A: Install From AEP Archive

1. On the command line on the Caldera system, navigate to the following directory (`CALDERA_HOME` denotes the home directory of the Caldera installation).
    1. `cd CALDERA_HOME/plugins/emu/data/adversary-emulation-plans`
2. Copy the attached file to the Caldera system, and decompress while in the directory in the previous step.
    1. `tar -zxvf /path/to/aep1-package-caldera.tar.gz`
3. The resulting directory layout should look similar to the following:

1. 

Option B: Create Directory Layout Manually

Alternatively, you can manually recreate the same structure.

1. `cd CALDERA_HOME/plugins/emu/data/adversary-emulation-plans`
2. `mkdir -p aep1/Emulation_Plan/yaml/`
3. `cp /path/to/aep1.yaml ./aep1/Emulation_Plan/yaml/`

Activate New Adversary Emulation Plan

After completing one of the above versions, restart Caldera.

Validate

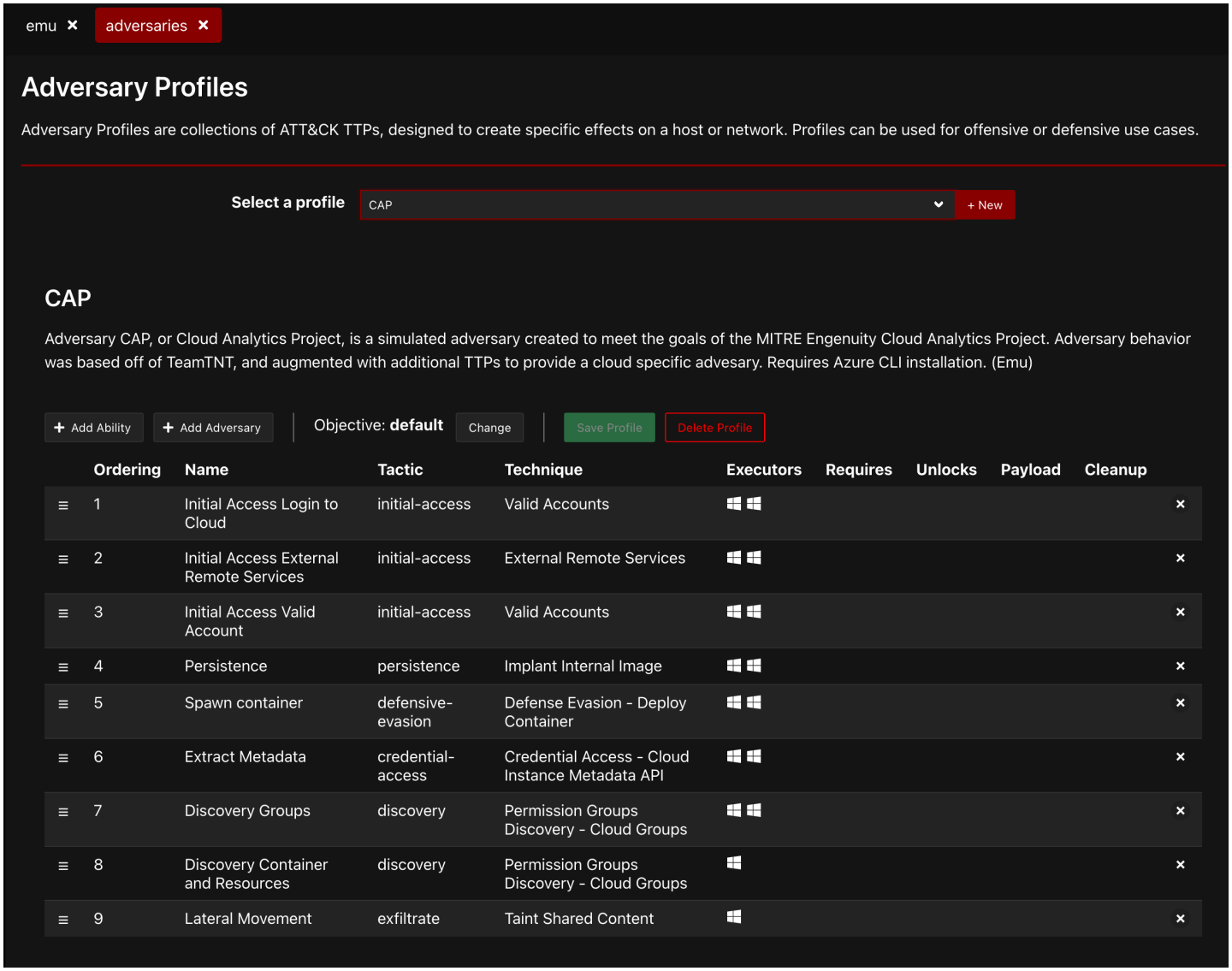
NOTE: The Cloud Analytics adversary name is currently CAP, short for Cloud Analytics Project.

Adversary Profile

Within Caldera, *Adversary Profiles* allow for collecting ATT&CK TTPs for a specific effect or scenario, such as an offensive or defensive scenario.

To validate the CAP profile is setup, within the Caldera web interface, navigate to *Plugins* -> *emu* -> *Adversaries* -> *Select a profile* -> ***CAP***.

A screen similar to the following should be displayed.



Fact Sources

Within Caldera, *Fact Sources* allow for using variables within an execution plan. Multiple fact source configurations can be setup for a profile, such as a fact source for the test environment. Along with Adversary Profiles, Fact Sources allow for executing predefined scenarios customized to a particular environment.

To validate the CAP Adversary Fact Source has been setup, within the Caldera web interface, navigate to *Configuration -> fact sources -> Select a source -> **CAP***.

A screen similar to the following should be displayed.

emu × adversaries × fact sources ×

Fact Sources

Facts are identifiable pieces of data, collected by agents or loaded when the server starts. A source is a collection of facts. Rules are boundaries to ensure specific traits cannot be used.

Select a source CAP (Emu) + Create Source

CAP (Emu)

Duplicate Delete Source

Facts (15)

+ Add Fact Find a trait or value...

Order	Origin	Fact Trait	Value	Score
0	IMPORTED	identity.app.id	unknown	1
1	IMPORTED	identity.app.pw	unknown	1
2	IMPORTED	identity.tenant	unknown	1
3	IMPORTED	cloud.resource.group	casandbox	1
4	IMPORTED	container.name	psdocker	1
5	IMPORTED	container.registry	justsomeregistry	1
6	IMPORTED	container.upstream.image	mcr.microsoft.com/powershell:latest	1
7	IMPORTED	container.upstream.image_b	docker.io/library/hello-world:latest	1
8	IMPORTED	container.upstream.image_b.tag	latest	1
9	IMPORTED	cloud.location	eastus	1
10	IMPORTED	container.image	justsomeregistry.azurecr.io/targetrepository:targettag	1
11	IMPORTED	vm.name	ca-linux-vm	1
12	IMPORTED	acr.username	justsomeregistry	1
13	IMPORTED	acr.password	secretpassword	1
14	IMPORTED	container.name_b	publicapp	1