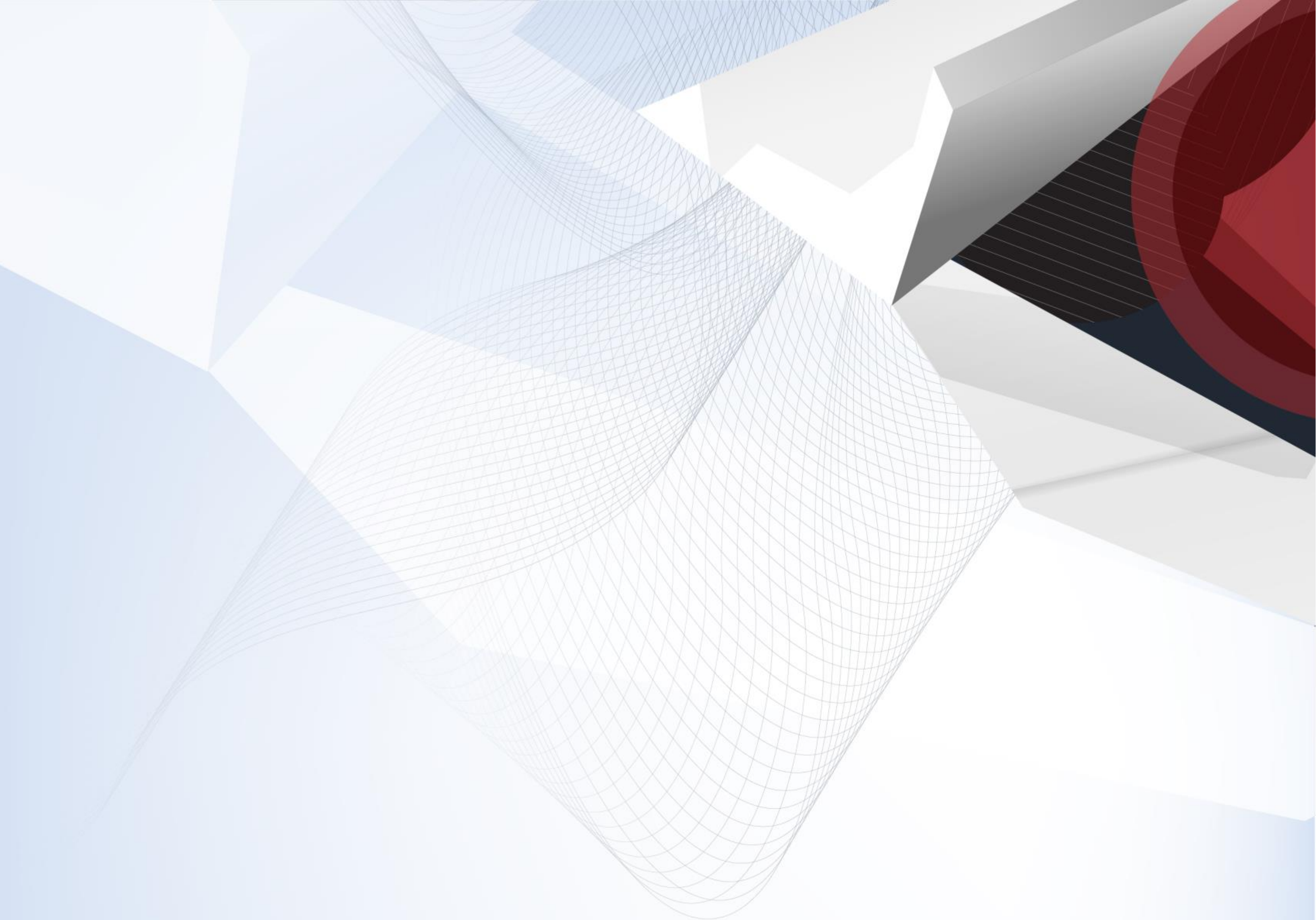


SECURITY ORCHESTRATION

FireEye Endpoint Security Containment Playbook

USER GUIDE (v1.2.0)

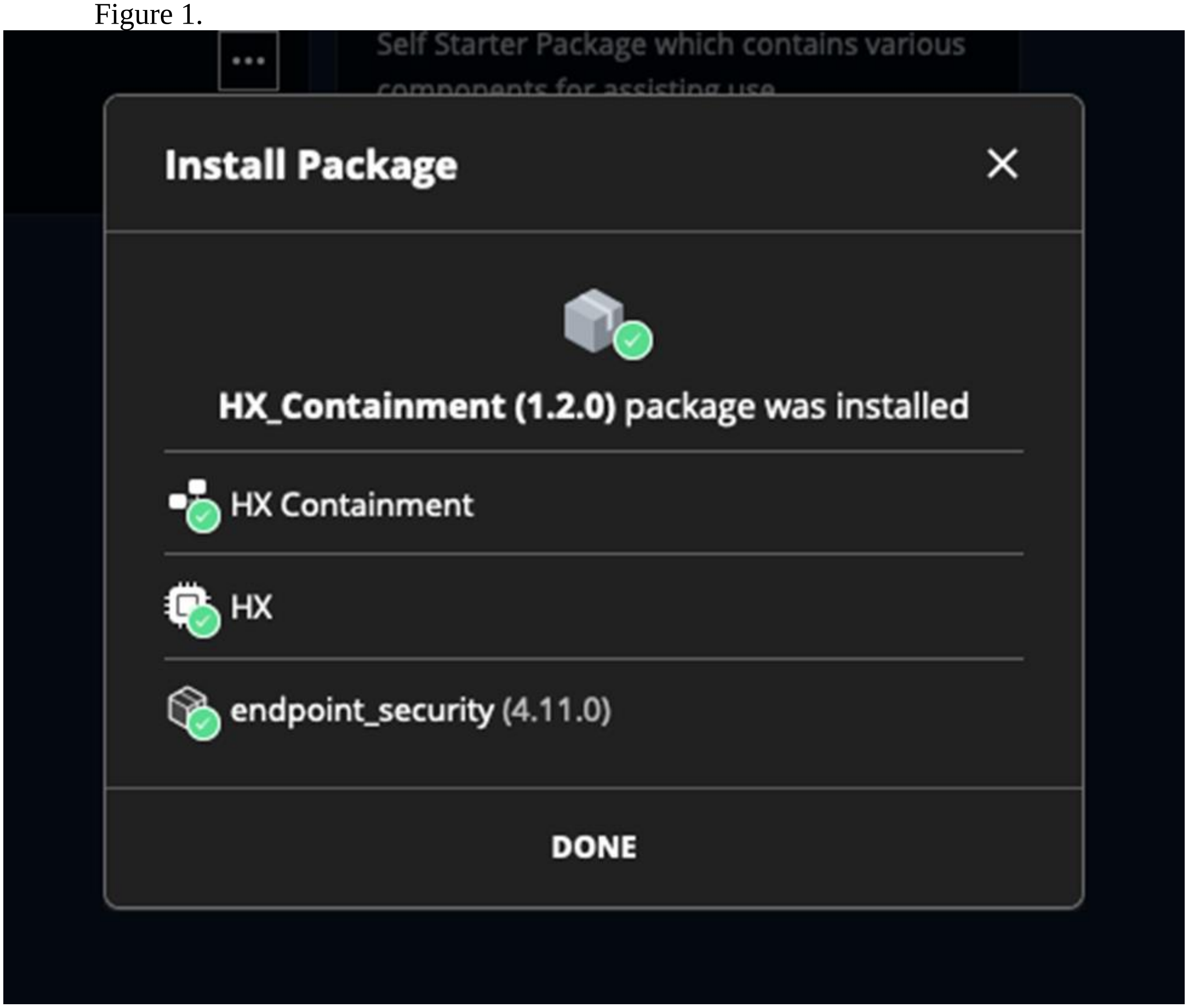
Description

This package contains a playbook that contains an endpoint via the FireEye Endpoint Security (HX) agent.

Provide a hostname, IP address, agent ID, or username of someone logged in to have the playbook request and approve containment.

Installation

Begin by installing the package fireeye.hx_containment-1.2.0 package by navigating to Manage Content (left column) -> Install (top right) -> Choose File (center), then selecting fireeye.hx_containment -1.2.0 package from your local file system. Results should resemble Figure 1.



Install Package

HX_Containment (1.2.0) package was installed

HX Containment

HX

endpoint_security (4.11.0)

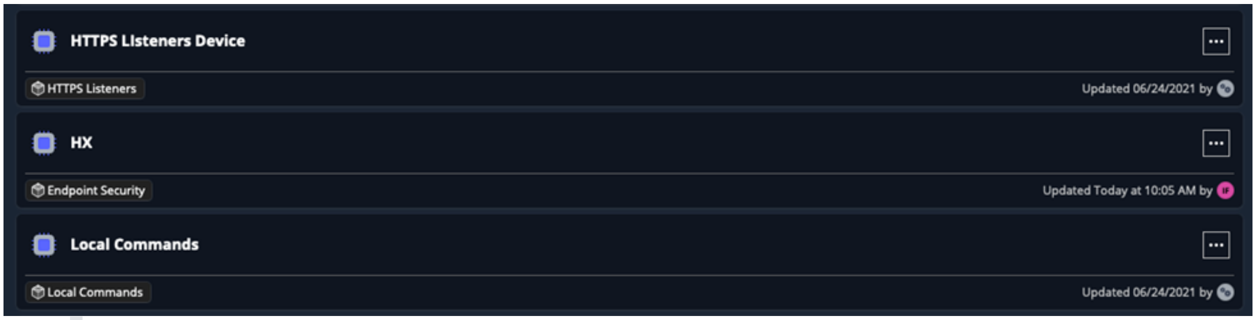
Self Starter Package which contains various
components for assisting use
×
DONE

Figure 1, Package Installation

Configuration

Configure and enable required devices by going to Configure (left column) -> Devices (left column) -> device to configure and enable (center)

Once a device is configured, enable it by clicking the ⋯ button to the right of the device as shown in figure 2.



HTTPS Listeners Device ⋯

HTTPS Listeners — Updated 06/24/2021 by

HX ⋯

Endpoint Security — Updated Today at 10:05 AM by

Local Commands ⋯

Local Commands — Updated 06/24/2021 by

Figure 2, Enable Device

To use the playbook, manually input the artifact to identify the host and execute or configure it as a sub-playbook in a larger workflow as shown in figure3.

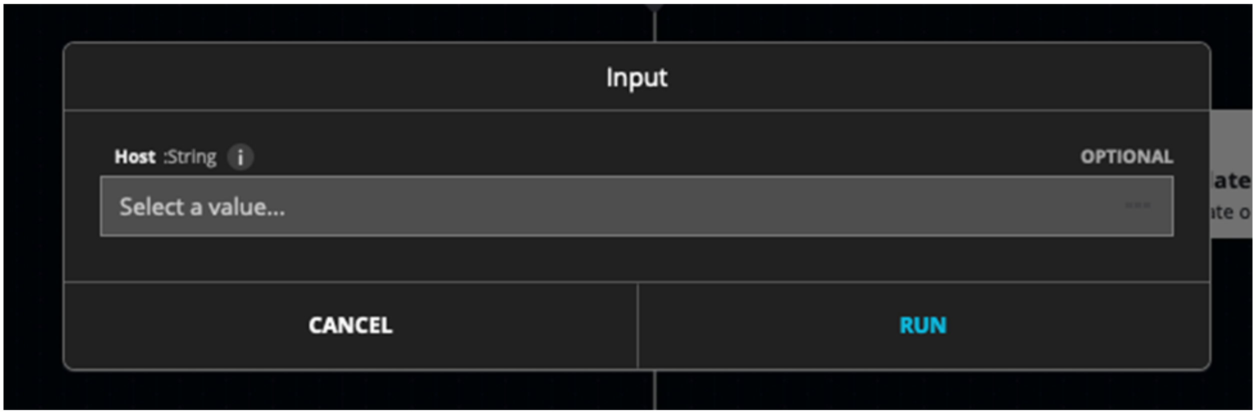


Figure 3, Playbook Inputs

Device(s):

HX

Required Parameters

- Password: Credential for the HX account
- Username: Credential for the HX account
- Host address: URL for the HX instance
- All other parameters should be left default

Playbook Parameters:

- Artifact to identify endpoint

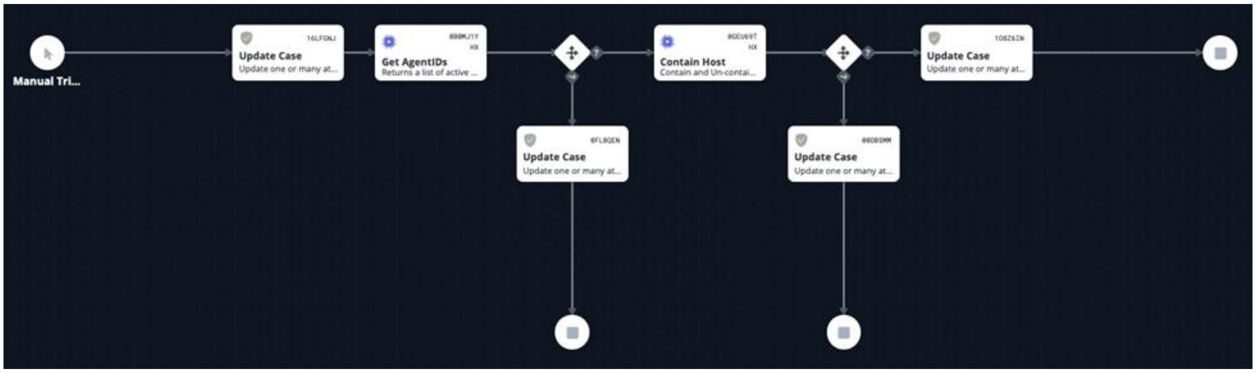


Figure 4, HX Containment Playbook