FIREEYE™

SECURITY ORCHESTRATION PLAYBOOK

FIREEYE ENDPOINT SECURITY ACQUISITION

USER GUIDE (v1.0.0)

Endpoint Security Acquisition

This package contains a playbook that, when triggered, sends an email alert to a specified inbox regarding a new acquisition detected by FireEye Endpoint Security (HX). The alert will contain basic details about the acquisition and will assist the recipient in taking further action if needed. The playbook is triggered by an adapter that periodically polls FireEye Endpoint Security for new acquisitions.

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

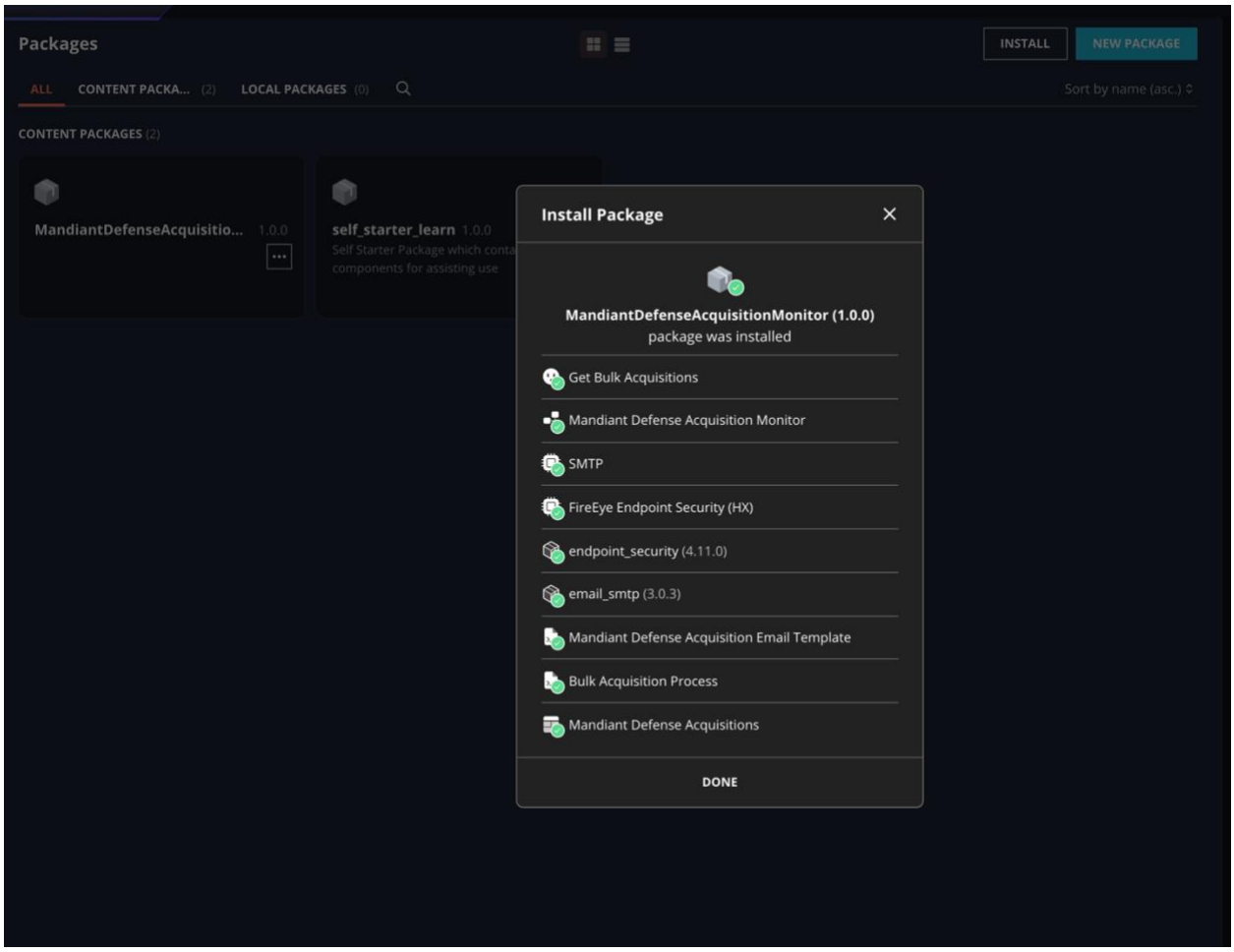

Figure 1, Package Installation

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 pictured in Figure 2.

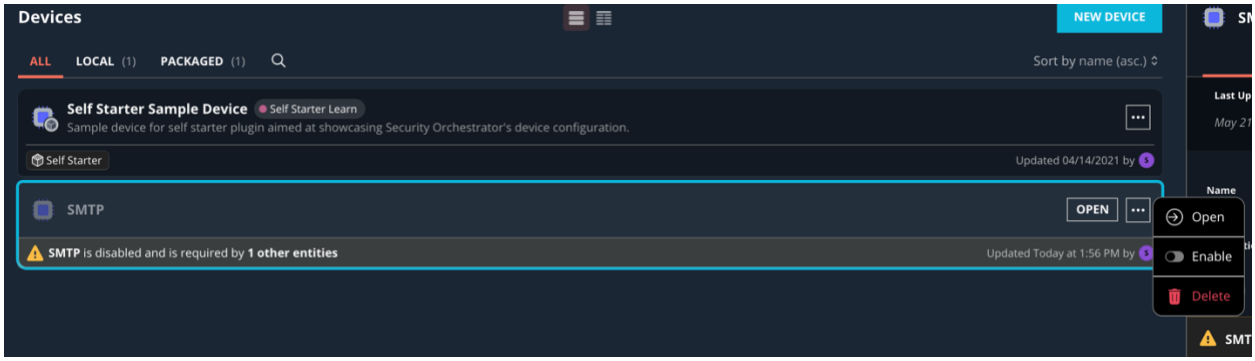

Figure 2, Enable Device

Configure and enable required Adapters by going to
Configure (left column) -> Adapters (left column) -> adapter to configure and enable (center)
Once an adapter is configured, enable it by clicking the ⋯ button to the right of the device as pictured in Figure 3.

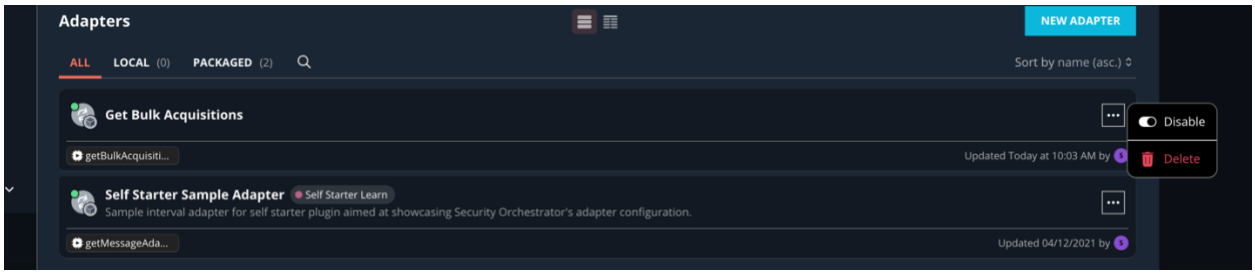

Figure 3, Enable Adapters

Required Devices:

SMTP

Required Parameters:

- Host: Host of the mail server
- Username: If required by the host, the username of the sender
- Password: If required by the host, the password of the sender
- Port: if host is not using 587
- All other parameters should be left default

FireEye Endpoint Security (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

Required Adapters:

Get Bulk Acquisitions

Require Parameters:

- None, default vales all acceptable

Playbook Parameters:

- None, triggered by Get Bulk Acquisitions adapter
- When opened, playbook should resemble Figure 4

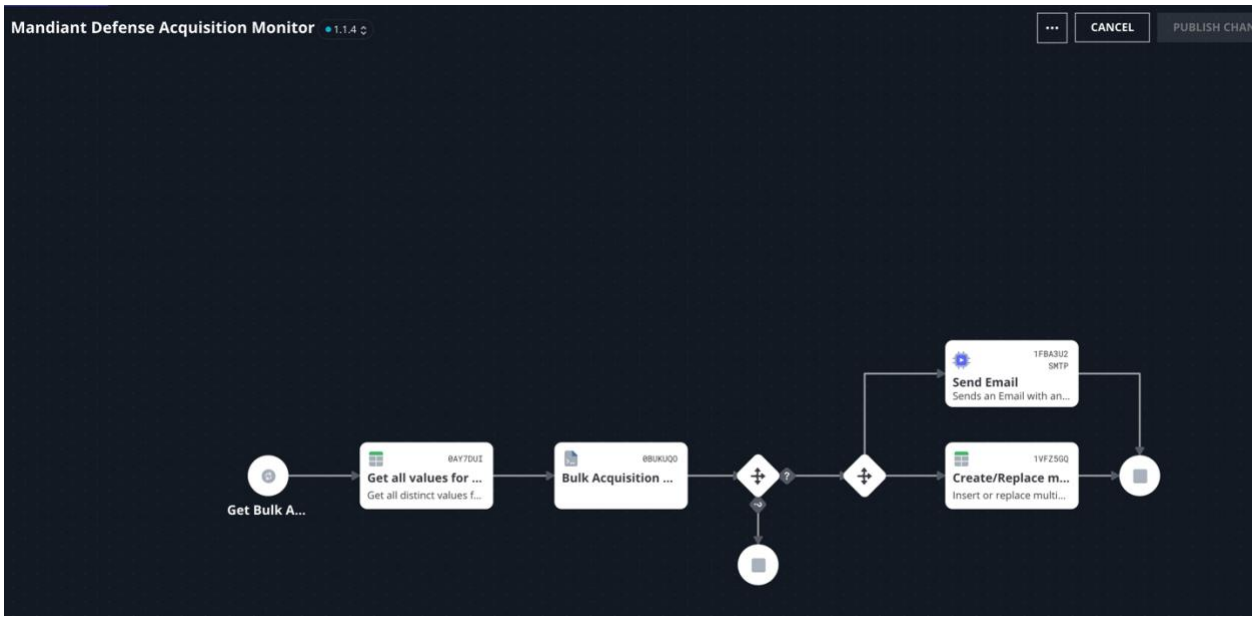

Figure 4, Mandiant Defense Acquisition Monitor Playbook