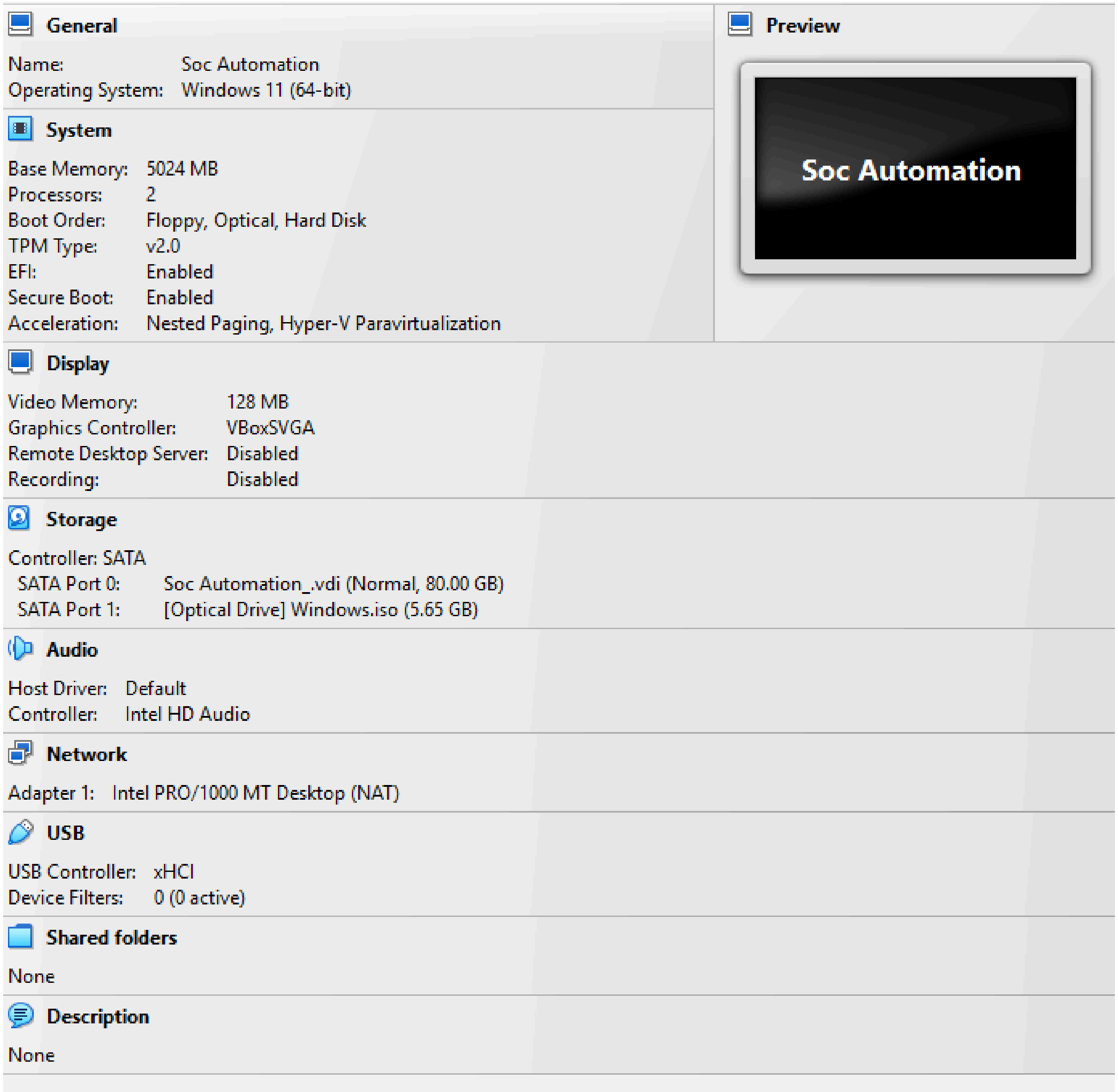
Windows 11 Virtual Machine Setup (VirtualBox)

This section describes how to create the monitored Windows 11 endpoint used for attack simulation.

Steps:

1. Install VirtualBox from virtualbox.org
2. Create a new virtual machine
   - Name: Windows 11 Lab
   - ISO Image: Windows 11 installation ISO
   - RAM: 4–8 GB
   - CPUs: 2–4
   - Storage: 60 GB
   - Enable EFI
3. Install Windows normally
4. Install VirtualBox Guest Additions
   - Enables copy/paste
   - Enables auto-resize
   - Enables drag-and-drop
5. Update Windows and reboot

The VM is now ready for Sysmon installation.



General

Name: Soc Automation
Operating System: Windows 11 (64-bit)

Preview

System

Base Memory: 5024 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
TPM Type: v2.0
EFI: Enabled
Secure Boot: Enabled
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Soc Automation_.vdi (Normal, 80.00 GB)
SATA Port 1: [Optical Drive] Windows.iso (5.65 GB)

Audio

Host Driver: Default
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: xHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None