Mandiant

PROTECTED THEATER - BEFORE YOU BEGIN

Before you start the Protected Theater setup, verify the hardware and networking you plan to use will support Protected Theater and that you have gathered all the required information:

1. Protected Theater requires a static IP (only the Protected Actor can use DHCP for networking).
2. For Windows: You have identified the Windows boot type, Legacy or UEFI
    a. Boot the Windows image outside of the Protected Theater.
    b. Open a command prompt.
    c. Type `msinfo32` .
    d. In the System Information window that appears, look for **BIOS Mode**, this will show either Legacy or UEFI.
3. Confirm that the recipient hardware meets the **Protected Theater Minimum System Requirements (https://docs.mandiant.com/home/msv-protected-theater--system-requirements)**.
4. Nested virtualization must be enabled on the Protected Theater image before booting.

    The Director validates nested virtualization is enabled when the Protected Theater initializes and reviews the image details

    - For VMware installs: more information is available from VMware at **https://communities.vmware.com/t5/Nested-Virtualization-Documents/Running-Nested-VMs/ta-p/2781466**. This can only be done through the web client for ESXi.
5. Reserve all guest memory for the host to improve performance. To do this in VMWare:
    a. Select the host in ESXi.
    b. Click **Actions** > **Edit Settings**.
    c. Expand the **Memory** field.
    d. Select the **Reserve all guest memory** checkbox.
    e. Click **OK**.

    If this is not possible, there is a less invasive adjustment that can be made. Information on that adjustment is available at **https://kb.vmware.com/s/article/1002586**.
6. The Protected Actor uses DHCP for networking while the Protected Theater requires a static IP.
7. An SSL certificate is used when connecting to the Protected Theater Console. When you add an SSL certificate to the Director, this same certificate will be used.

    This is only available in MSV and is not required. You can use VNC instead.
8. Protected Actor Artifacts and Services have been added to the Allow lists. For the complete list of entries, see **Windows Services for Protected Actor (https://docs.mandiant.com/home/msv-pt-windows-services)**.
9. A Windows administrative user account (local or domain) with the appropriate permissions has been created. The administrative account requires the following:
    - Must be able to sign in from the network
    - Must have the **Allow logon locally** policy applied
    - Must have User Access Control (UAC) disabled

The capabilities of Protected Theater are designed specifically to ensure a safe environment exists for the execution of endpoint control tests that are expected to be destructive to an endpoint if the control technology being tested is not effective. Care should be taken when defining Protected Theater Rules to ensure only the communication absolutely required to validate the controls being tested is allowed. Allowing more than this communication to exit the Protected Theater (e.g., Windows domain services) could expose systems beyond the Protected Theater to malicious communication and service impact.