Mandiant

SECURITY VALIDATION ACTOR OVERVIEW

Actors are the Security Validation components that let you safely perform tests in production environments. Actors are used to test the effectiveness of:

- Network Security controls
- Windows, Mac, and Linux endpoint controls
- Email controls

Network Actors

Network Actors are used to inspect network traffic (IDS, IPS, NGFW, and so on) and are installed within your business zones. These Actors can have multiple interfaces and serve as either the source or destination of a test. Two Actors send traffic between each other to see how the network control responds. Standard tests include:

- Segmentation and policy validation
- Malicious file transfer
- C2
- Data exfiltration

Endpoint Actors

The Endpoint Actor is designed to process non-destructive behaviors to test endpoint-based security solutions. This Actor is added to the target host using an executable containing an Endpoint Agent. You complete Actor registration in a manner similar to the process for Network Actors.

Endpoint Actors can be installed anywhere on your network; you do not need to have dedicated systems. Installation of the Endpoint Actor does not require IT or policy changes.

As a best practice, install Endpoint Actors on hosts for each of your gold images. You do need to install them on every system in your environment.

By default, when run, Host CLI Actions automatically select the "System account" of the host. You can create **Action User Profiles (https://docs.mandiant.com/home/msv-action-user-profiles)** to match other accounts on the Host (root, Admin, user). This matching includes local and AD accounts. When using AD accounts, you can use existing users in different GPOs. No additional configuration is required, and running Actions does not affect other active user sessions on the host.

Endpoint Actors can process many of the same behavior types as Network Actors, with a few notable exceptions:

- Cannot complete file transfers (malicious and data exfiltration) through ICMP tunneling, SSH, and secure copy
- Cannot complete file transfers (malicious and data exfiltration) through DNS tunneling or ICMP tunneling
- Cannot act as the destination Actor for an HTTPS Action (they can be the source)
- Multiple interfaces are supported in Windows environments but not Mac or Ubuntu