Malware configuration and testing

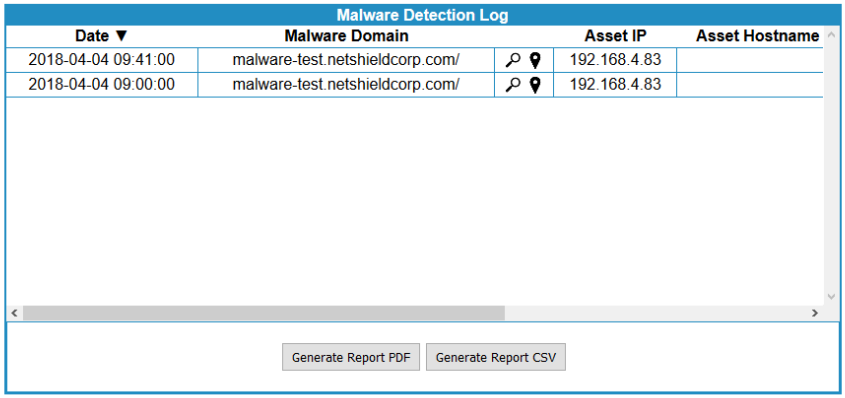
Eth 1 (MON) is used to listen to egress traffic on the uplink port of a switch. This is accomplished by connecting it to a span (Cisco) or mirror port.
It is a receive-only port, it never transmits.

An IP address is required to bind the protocol to the adapter (OS requirement) so Eth 1 (MON) can detect traffic destined for a known Command and Control or Phishing server. Always use a valid IP address that will NOT be
found on the network. Ex. 1.1.1.1/ 255.255.255.0

Before enabling malware scanning ensure the configuration is complete, Asset Detection is enabled and Eth 1 (MON) is connected.

Test malware detection is working by attempting to open the test page from an asset on the network segment under test. The URL is:
http://malware-test.netshieldcorp.com/.

An entry will be created in the Malware log.



If blocking is enabled and Malware is configured correctly the page will not be accessible and the test PC will be blocked.

If a site is blocked as TLD but the domain is not on the manual malware list then check if the site was blocked due to TLD and then removed from the manual malware list it will still be blacklisted.

You can move the site to the whitelist and that will allow access.