Continuous Monitoring/Continuous Diagnostics and Mitigation (CM/CDM)

Continuous Diagnostics and Mitigation

Continuous Diagnostics and Mitigation (CDM) are used to help ensure an ongoing state of security of federal information systems and applications. Part of CDM is manual such as conducting audit reviews, ensuring operational procedures are adhered to, and part of CDM is automated or technology based. This page seeks to help with some of the automated CDM that should occur with each federal system, such as ensuring patches are maintained and that application vulnerabilities are fixed. If you operate an external application for the NCI, that is, it is hosted outside of an NIH-managed network but is funded by, for, or on behalf of the NCI, then the NIH can help with some of your CDM requirements by running scans against your host and application. Currently, NIH can run Tenable (Nessus) scans against your network hosts (i.e., only against the host or hosts that are used to support an NCI application), and AppScan tests against your NCI web based application. With the information generated from these tools your team should be able to address weaknesses at the host/OS level and at the web application level. These remote scans are provided free of charge by the NIH with proper authorization from both your organization's security official and from the NCI ISSO. Please note, NIH does not provide a license for your own use, only a remote scan using NIH's existing license.

Read more about the External AppScan Process

Read more about the Tenable Nessus Process