Continuous Diagnostic and Mitigation and Continuous Monitoring as a Service

TOOLS FUNCTIONAL AREAS

TOOLS FUNCTIONAL AREAS

The contractor shall offer tools to perform in the functional areas below, as required to support requirements of individual orders under this BPA.

TOOL FUNCTIONAL AREA 1 - HARDWARE ASSET MANAGEMENT

The Hardware Asset Management (HWAM) Function is to discover unauthorized or unmanaged hardware on a network. Once unauthorized or unmanaged hardware is discovered by the contractor's provided tool(s), the agency will take action to remove this hardware. Since unauthorized hardware is unmanaged, it is likely vulnerable and will be exploited as a pivot to other assets if not removed or managed.

TOOL FUNCTIONAL AREA 2 - SOFTWARE ASSET MANGEMENT

The Software Asset Management (SWAM) Function is to discover unauthorized or unmanaged software configuration items (SWCI) in IT assets on a network. Once unauthorized or unmanaged SWCI are discovered by the contractor's provided tool(s), the agency will take action to remove these SWCI. Because unauthorized software is unmanaged, it is probably vulnerable to being exploited as a pivot to other IT assets if not removed or managed. In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings; malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate itself throughout the enterprise.

TOOL FUNCTIONAL AREA 3 - CONFIGURATION MANAGEMENT

The Configuration Management (CM) Function is to reduce misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual, and operating system) and software. Once a misconfiguration of hardware devices is discovered by the contractor provided tools, the supported department / agency will be responsible to take any needed action to resolve the problem or accept the risk. Over 80% of known vulnerabilities are attributed to misconfiguration and missing patches. Cyber adversaries often use automated computer attack programs to search for and exploit IT assets with misconfigurations, especially for assets supporting Federal agencies, and then pivot to attack other assets.

TOOL FUNCTIONAL AREA 4 – VULNERABILITY MANAGEMENT

The Vulnerability Management (VUL) Function is to discover and support remediation of vulnerabilities in IT assets on a network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified. Once the contractor provided tool(s) identify these mistakes and deficiencies, the agency will take action to remove or remediate these from operational systems so that they can no longer be exploited. (An information security vulnerability is a deficiency in software that can be directly used by a hacker to gain access to a system or network).