Business Challenge

Security teams are constantly challenged with the ability to monitor their changing fleet of mobile devices and associated vulnerabilities for the organization. Without integrating the Tenable plugin with IBM Security MaaS360 with Watson, scanning and gaining additional vulnerability data becomes increasingly complex. If devices are unaccounted for or fail to have the correct policies, personal and enterprise data is at major risk.

Solution

The Tenable® plugin for MaaS360 provides a way for security teams to understand the cyber exposure of their mobile devices being managed by IBM. Tenable collects mobile device hardware and software information by importing asset lists and asset data from MaaS360 and runs its plugins against the collected data to determine vulnerabilities. Comprehensive reports are then generated for security teams to better understand their Cyber risk to help ensure compliance across their mobile environment.

Value

The Tenable plugin for MaaS360 provides the ability to:

- Gather all known information for your organizations iOS and Android devices
- Receive vulnerability information for your organizations mobile devices
- Report on vulnerability findings within Tenable for your organizations mobile devices
How It Works

1. Tenable launches Mobile Device Management Scan process.
2. Nessus® connects to MaaS360 and gathers all known information about Android and iOS devices.
3. Nessus® uses the data collected from MaaS360 to discover vulnerabilities.
4. Findings are returned to and reported within Tenable.

More Information

Tenable Installation Links:
https://www.tenable.com/products/tenable-io
https://www.tenable.com/products/tenable-sc

Configuration Documentation:
docs.tenable.com

For support please contact: community.tenable.com