SANS Checklist:

Mobile Security Selection Criteria

Written by:

Lee Neely
SANS Instructor

Mobile Security Selection Criteria

	Requirements	Priority	Additional Info
Deployment process	Support app download from public stores	High	Official app should be available on Apple's App Store and Google Play
	Overall ease of deployment	High	Considering required actions by the end user and the admin
End user experience	Low impact on device battery usage	High	Usage should be under 3%
	Low data usage	Medium	Both on cellular network and Wi-Fi
	App maintains end user's privacy	High	Not exposing sensitive user information
	Clear display of detected threats and mitigation options	High	Provide a clear and simple display of detected threats with an advisory for mitigating them
	Provide automatic mitigation options for most threats	High	For minimizing actions required from the end user
Threat detection	**Network Threats**		
	Secure communication downgrading (SSL stripping) attack detection	High	Man-in-the-middle attack in which the device communication is downgraded from SSL to plain text
	Secure traffic decryption (SSL decryption) attack detection	High	Man-in-the-middle attack in which traffic from the end user's device is decrypted by the attacker
	Content manipulation attack detection	Medium	Attack in which the content of a web page is altered in order to manipulate the end user
	Rogue networks detection	High	Identify anomalies in public hotspots to identify rogue networks
	Ability to perform automatic mitigation on detected network threats	High	Mitigate network threats without end user intervention, keeping traffic secure without losing connectivity
	Malware		
	Detection of malicious apps based on different app properties	High	For instance, app source, requested permissions, certificate, etc.
	Detection of repackaged/fake apps	High	Detection of malicious apps that impersonate legitimate apps
	Detection of malicious apps based on signatures/known exploits	Medium	Using standard antivirus capabilities
	Ability to block malicious app installation	High	Intervene in real time to stop installation in case the app is risky
	Detection of iOS malware	Medium	Ability to detect new and existing iOS malware such as XcodeGhost and YiSpecter
	Detection of malicious profiles on iOS devices	High	Malicious profiles can be used for monitoring/controlling activity on an iOS device
	Device vulnerabilities		
	Ability to identify jailbroken or rooted devices	Medium	Detection and policy enforcement on these non-compliant devices
	Ability to identify device OS vulnerabilities	High	Present vulnerability details and risk clearly for each device
	Ability to prompt end users to upgrade their device OS version	Medium	Ability to do this as soon as the update is available (sometimes even before the formal vendor announcement arrives)

Mobile Security Selection Criteria

	Requirements	Priority	Additional Info
Management and administration	Provide visibility on detected threats and vulnerabilities	High	Present a clear, detailed description of each threat (including network and malware) and vulnerability (OS/ device configuration)
	Provide an overall risk estimate per device	High	Risk calculation should take into account current threat, device history, vulnerabilities, etc.
	Provide forensic capabilities on identified threats	Medium	Present details about the impact of each detected threat
	Provide the option to define an organization-level compliance policy	High	Devices that do not comply with the organizational policy can be blocked from using organizational resources
	Reporting	High	Provide reporting capabilities, including scheduled email reports, support for different data formats (tables, graphs) and document formats (PDF, CSV)
Other	EMM integration	High	Work with or without an existing EMM solution such as AirWatch, MobileIron and XenMobile
	SIEM integration	High	Support integration with different SIEM systems (ArcSight, McAfee ESM, Splunk, etc.) for exporting detected threats
	Provide a third-party API	Low	Provide a third-party API for retrieving device security information

See how #1 Mobile Threat Defense solution meets these criteria

SEE DEMO

About the Author

Lee Neely, a SANS mentor instructor, teaches cybersecurity courses, including the new cybersecurity management training, and Information System Security Officer training. He worked with the SANS SCORE project to develop the iOS Step-by-Step configuration guide as well as the Mobile Device Configuration Checklist included in the SEC 575 course. A senior IT and security professional at Lawrence Livermore National Laboratory (LLNL), Lee has been involved in many aspects of IT. He currently leads LLNL's new technology group, working to develop secure implementations of new technology, including developing its secure configurations, risk assessments and policy updates required for corporate and BYOD mobile devices.