20/12/2021

Specification for Anti-Virus Solution for Disaster Management Centre

As per the IT equipment requirements of Disaster Management Center, technical evaluation committee recommended below specification.

#	Clause	Compliance (Complied / Not Complied)	Remarks
1	General Requirements		
1.1	The bidder shall propose an Endpoint Protection Solution to secure all Endpoints of Disaster Management Centre including (but not limited to) Servers, Desktops, Laptops and Mobile Devices.		
1.2	The proposed solution should be a Leader or a Challenger in the latest Gartner Magic Quadrant for Endpoint Protection Platforms		
1.3	The proposed solution should be certified by third party testing organizations like AV-Test, AV-Comparatives, ICSA Labs, SE Labs, MRG Effitas		
1.4	All features and functionalities complied in the compliance table will be considered as the features & functionalities of the proposed version/edition of the product unless otherwise specifically mentioned under “Remarks” column.		
1.5	The bidder shall specify the Product Name, Version, and Released-date for the proposed solution.		
2	Product Features		
2.1	The proposed solution should offer the following features:		
2.1.1	Antivirus		
2.1.2	Host-based Intrusion Prevention System (HIPS)		
2.1.3	Ransom ware Protection		
2.1.4	Memory Scanner		
2.1.5	Botnet Detection and Protection		
2.1.6	Sandboxing on the Endpoint		
2.1.7	Sandboxing on the Cloud		
2.1.8	Exploit Blocker		
2.1.9	Detection of known vulnerabilities on the network level, for which a patch has not yet been released or deployed, and prevent exploitation.		

2.1.10	AI / Machine Learning		
2.1.11	Protection for Unified Extensible Firmware Interface (UEFI)		
2.1.12	Threat Intelligence		

2.1.13	Two-way Firewall with following features:		
a)	Analyze the content of network traffic and protect from network attacks. Any traffic which is considered harmful should be blocked.		
b)	Alert the user when the user connects to an unprotected wireless network or a network with weak protection.		
c)	Define a firewall profile and trusted zone for each network adapter and to each connected network.		
d)	View a list of IP addresses that have been detected as the source of attacks and add to the blacklist to block connections for a certain period of time.		
e)	Detect and block communication with malicious command and control servers		
2.1.14	Intrusion Detection (IDS) Features:		
a)	Protect against an attack that uses a rogue challenge during authentication in order to obtain user credentials.		
b)	Detection of known evasion techniques used for opening MSRPCS named pipes in SMB protocol.		
c)	Detect and block various CVEs (Common Vulnerabilities and Exposures) in the remote procedure call system developed for the Distributed Computing Environment (DCE).		
d)	Detect and block various CVEs in the RDP protocol		
e)	Detection of ARP poisoning attacks triggered by man in the middle attacks or detection of sniffing at network switch.		
f)	Detection of DNS poisoning – relieving a fake answer to a DNS request (sent by an attacker) which can point the user to fake and malicious websites.		
g)	TCP/UDP Port Scanning attack detection		
h)	Ability to block unsafe addresses after attack detection		
i)	Display notifications for incoming attacks against security holes		
2.1.15	Packet Inspection Features:		
a)	Allow/Block incoming connections to admin shares in SMB protocol		

b)	Deny SMB sessions without extended security		
c)	Deny opening of executable files on a server outside the Trusted zone in SMB protocol		
d)	Deny NTLM authentication in SMB protocol for connecting a server in/outside the Trusted zone		
e)	Check TCP connection status – see if all TCP packets belong to an existing connection. If a packet does not exist in a connection, it should be dropped.		
f)	TCP protocol overload detection		
g)	ICMP protocol message checking		
h)	Covert data in ICMP protocol detection		
2.1.16	Device Control – Centrally manage and scheduling of device permissions of users		
a)	Control and Manage all the USB ports in client PCs		
b)	Authenticate and verify USB storage devices		
c)	Allow or block by device ID		
d)	Allow or block USB flash drives and external HDDs		
e)	Allow or block Modems and Dongles.		
f)	Allow or block Firewire Storages		
g)	Allow or block CD/DVD		
h)	Allow or block Bluetooth Devices		
i)	Allow or block Smart Card Readers		
j)	Automatic encryption and decryption of data on removable media.		
2.1.17	Web Control – shall support web filter with URL, category based & centrally manage and scheduling of web access permissions of users		
a)	URL based web control (allow/block)		
b)	Pre-defined category-based web control (allow/block)		
c)	Scanning of all HTTP & HTTPS traffic for malicious content		
2.1.18	Email Protection:		
a)	Provide control of email communications over POP3(S) and IMAP(S) protocols using a plug-in for user's email client		
b)	Antispam Protection		

c)	Anti-phishing Protection		

2.1.19	Application Operation Management		
a)	Control Potentially Unwanted Applications/Grayware which could install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user.		
b)	Control Potentially Unsafe Applications which are commercial software that has the potential to be misused for malicious purposes such as remote access tools, password-cracking applications, and keyloggers.		
c)	Control Suspicious Applications include programs compressed with packers or protectors.		
d)	Anti-Stealth Feature providing the detection of dangerous programs such as rootkits, which are able to hide themselves from the operating system, and are difficult to detect using ordinary testing techniques.		
e)	Enable advanced scanning via Microsoft Anti-malware Scan Interface (AMSI)		
f)	Application modification detection (to avoid abusing rules configured for some application by another application by temporarily or permanently replacing the original application's executable file with the other applications executable file, or by maliciously modifying the original application's executable file.)		
g)	Application protocol content filtering that works automatically, regardless of the Internet browser or email client used.		
2.1.20	Full Disk Encryption		
2.2	Server Protection with all features mentioned under clauses 2.1.1 to 2.1.19		
2.3	The main features of the product should be able to be fine-tuned using multiple threshold levels rather than just enabling/disabling.		
2.4	The vendor should have their own AV Engine		
2.5	The proposed solution should offer the following functionalities:		
2.5.1	On-access scanning		
2.5.2	Real-time scanning		
2.5.3	On-demand scanning		
2.5.4	Scheduled scanning		

2.5.5	Scan compressed files		
2.5.6	All files should be scanned for malicious code when they are opened, created or run.		
2.5.7	Scan Microsoft Office Documents before they are opened.		
2.5.8	Must be able to prevent Institute systems from Zero-Day exploits & attacks and not to rely on signature-based detection and protection methods.		
2.5.9	The solution should be able to automate the endpoint prevention by autonomously reprogramming and re-tuning itself using threat intelligence gained from behavioral analysis, reputation and machine learning.		
2.5.10	Must provide an intuitive white & black listing capability that is auditable and granular that can be applied to an endpoint, group of endpoints or system-wide.		
2.5.11	Must accommodate multi-site, centralized operations architecture with efficient communication and update mechanism.		
2.5.12	Ability to load setup parameters using an .xml configuration file, or to save the current setup parameters to a configuration file		
2.5.13	Manual submission of quarantined files to cloud		
2.5.14	Automatic submission of quarantined files to cloud		
3	Performance		
3.1	The bidder must list the minimum hardware and software requirements for its endpoint agent for PCs)		
3.2	The bidder must describe the Network Load (with used MB size, eg:MB/day)		
3.3	The bidder must describe the System Footprint (on PCs)		
3.4	The bidder must describe the System Footprint (on Servers)		
3.5	The proposed solution should not rely on resource intensive detection and protection methods that can adversely affect the performance of endpoints		
3.6	All capabilities of the proposed solution must be delivered through a single endpoint agent that cannot consume more than 15% of resources of the installed device at its peak.		
3.7	The false positive threat identification should be less than 0.1% of the installed endpoints at any given time		

3.8	The proposed solution architecture should accommodate efficient distribution of updates within the site as well as to remote sites.		
4	Management		
4.1	The proposed solution must provide a consistent, functional, and centralized administrative web interface that is intuitive and easy to navigate.		
4.2	The proposed solution should facilitate both standalone on-premise management as well as cloud-based management options		
4.3	The proposed solution should not send any endpoint information out of the organization's network, in an on-premise deployment.		
4.4	The administration console should be available to any authorized IT staff on any device and any time.		
4.5	The bidder shall specify supported browsers for the central administrative console		
4.6	The proposed solution's web console should be capable of filtering events to show only security related data that is relevant and requires immediate attention.		
4.7	The proposed solution should provide easy and intuitive global search capability that provides intuitive drill-down interface to assist in investigation of suspicious activities.		
4.8	Please specify the supported deployment methods and operating systems for management console deployment.		
4.9	Please specify the compatibility with free database software like MS SQL Express, MySQL, MariaDB, Mongo DB, etc. for management console deployment.		
4.10	Solution to inter-operate with Active Directory through ADFS to provide access to system functions in addition to console's own local security database.		
4.11	The bidder shall provide an online portal for License Management		
4.12	The proposed solution shall support Role-based Access Control.		
4.13	Access to the web console should be protected with multi-factor authentication preferably from the same vendor.		
4.14	Only relevant information should be presented to the authorized console user (i.e. security trimmed) based on the user's role in the system. However, the console administrator(s) should have ultimate access to the system and all its components.		
4.15	The detected threat information should be communicated to the system administrators and designated IT staff in real-time.		

4.16	Real-time threat statistics should be displayed in graphic and numerical forms.		
4.17	Provide integrated, remote workflow that removes or reduces manual staff intervention.		
4.18	Prevent uninstall of endpoint protection agent by end-users who have elevated (high privileged) access on those systems.		
4.19	Uninstall the endpoint agent from the installed systems through the management console.		
4.20	Investigate and mitigate the potentially infected endpoints remotely.		
4.21	Provide extensive, interactive reporting with drill-down capability on captured incidents.		
4.22	Provide extensive, full auditing capabilities for every step of the system workflows.		
4.23	Provide flexible email notification capability to alert IT staff about suspicious activities that may pose security threat to the Institute assets.		
4.24	Pre-installed Policies		
4.25	Tools to remove existing EPP		
4.26	Active Directory Synchronization		
4.27	LDAP Synchronization		
5	Reporting		
5.1	The bidder shall describe Reporting Capabilities of the proposed solution.		
a)	Scheduled reports		
b)	Report by type		
c)	Pre-defined reports		
d)	Editable reports filters		
e)	Definable report time range		
f)	Editable friendly reports		
g)	Downloadable reports (PDF, PS, CSV format)		
h)	Send report by email		
5.2	The solution should provide both real-time and historical reporting capability that is Intuitive and easy to use.		
5.3	The solution should provide holistic and historic reporting of the protected endpoints (through real-time, ad-hoc and for a specific time period).		

5.4	System should have an open reporting architecture that is easy to share and export to other systems.		
5.5	The IT staff should be able to configure scheduled custom reports in addition to standard reports provided by the vendor.		
5	Supported Operating Systems		
5.1	The proposed solution should support the following operating systems at a minimum:		
5.1.1	Windows 10 (32-bit & 64-bit)		
5.1.2	Windows 8 (32-bit & 64-bit)		
5.1.3	Windows 7 (32-bit & 64-bit)		
5.1.4	Windows XP (32-bit & 64-bit)		
5.1.5	Windows Server 2008 & 2008 R2 (32-bit & 64-bit)		
5.1.6	Windows Server 2012 & 2012 R2 (64-bit)		
5.1.7	Windows Server 2016 (64-bit)		
5.1.8	Windows Server 2019 (64-bit)		
5.2	Please elaborate support for following operating systems:		
5.2.1	MacOS		
5.2.2	Debian-based Linux Desktops & Servers		
5.2.3	RedHat-based Linux Desktops & Servers		
5.2.4	Open Suse Linux Desktops & Servers		
6	Other Requirements		
6.1	Should be able to generate a Hardware Inventory (Chassis, Device information, Display, Display adapter, Input device, Mass storage, Network adapter, Printer, Processor, RAM and Sound device)		
6.2	Should be able to generate a Software Inventory		
6.3	Vulnerability Report and Patch Management		
6.4	Local updates mirror server		
6.5	Updates Scheduler		
6.6	Update Rollback		
6.7	Licensing Portal		
6.8	Licenses Manager		

6.9	The commercials should be indicated for Disaster Management Centre endpoints, and the license should be for 12 Months.		
6.10	The bidder shall provide 24x7 product support via:		
a)	Phone		
b)	Email		
c)	Remote Desktop Tools		
d)	On-site Support		
6.11	Help desk support ticket creating mechanism: (Should mention here)		
a)	Help Desk URL		
b)	Help Desk Phone Number		
6.12	Provide three references of successful deployment for similar business/institution in last year.		
6.13	The bidder must provide proof for at least two certified engineers for the proposed product.		
6.14	Manuals/Guides/FAQ/Knowledge Base		
6.15	The vendor is expected to provide timely support for project planning, deployment, problem resolution for the proposed solution.		
6.16	Training:		
6.16.1	The bidder shall propose vendor certified training enabling the engineers to configure, operate and maintain the proposed solution.		
6.16.2	This formal classroom training must cover all key-concepts specific to the proposed solution.		