Annexure -A

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
1	48	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 7	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.	As per RFP specification mentioned, this particular point is requesting the inclusion of predefined lists of critical system files, either for operating systems or applications (such as web servers, DNS, etc.). However, it is observed that excluding the operating system/application may potentially compromise data center security. Therefore, we kindly request the inclusion of both components—operating systems and applications—for enhanced efficacy in ensuring data center security. Clause should read as : Solution should support any pre-defined lists of critical system files for various operating systems and applications (web servers, DNS, etc.) and support custom rules as well.	As per RFP.
2	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 16	Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems	This particular point seems to duplicate point No. 13; nevertheless, we humbly request the addition of a feature for automatically recommending rules in the log analysis module based on the Server OS. Given that a significant number of ransomware attacks can be identified in the initial phases through server logs, such a feature would greatly assist organizations in securing their critical assets. Therefore, we kindly ask for the incorporation of automatic recommendation rules for log analysis. Clause should read as : Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/unassigment of rules also should have capability of pattern matching like Regular Expressions or simpler String Patterns and rule will be triggered on a match also ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.	As per RFP.

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
3	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 20	Proposed OEM should be positioned in any quadrant from latest published Gartner Magic quadrant report for Endpoint Protection.	In accordance with the guidelines outlined in the Request for Proposal (RFP), the clauses recommend a proposal from an Original Equipment Manufacturer (OEM) currently positioned in the latest Gartner Magic Quadrant. We kindly request your consideration to include either Gartner Leaders and Challengers to ensure the selection of best-of-breed products for securing crown jewels. Clause should read as: Proposed OEM must be positioned in either the Leaders or Challengers quadrant according to the latest published Gartner Magic Quadrant report for Endpoint Protection.	As per RFP.
4	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 25	Should automatically submit unknown files/suspicious object samples with OnPremise sandbox solution for simulation and create IOCs on real time basis as per sandboxing analysis and revert back to server security. Should support existing server operating OS RHEL 6.x, 7.x, 8.x, 9.x and higher, and Windows Server 2016, 2019, 2022and higher.	As per the specifications in the RFP, the clauses indicate to include sandboxing for existing operating system used in the Data Centre environemnt (RHEL 6.x, 7.x, 8.x, 9.x and higher, and Windows Server 2016, 2019, 2022and higher) to safeguard critical workloads against zero-day attacks. However, it has been observed that the term "sandboxing" is not explicitly mentioned in the second line. We kindly request your consideration in accepting this amendment to enhance the protection for your critical workloads. Clause should read as: Should automatically submit unknown files/suspicious object samples with OnPremise sandbox solution for simulation and create IOCs on real time basis as per sandboxing analysis and revert back to server security. Proposed solution should support custom sandboxing for existing server operating OS RHEL 6.x, 7.x, 8.x, 9.x and higher, and Windows Server 2016, 2019, 2022and higher for ensuring protection from zero-day and ransomware attacks.	As per Revised RFP.

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
5	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 21	Management of proposed solution should support both window as well as Linux platform	As per the RFP specifications, it's noted that the proposed management server should be compatible with both Windows and Linux operating systems. Additionally, we kindly request clarification regarding the requirement for database licensing for management server. Furthermore, we would appreciate the inclusion of MS-SQL, Oracle and PostgreSQL for logging events to non-proprietary, industry-standard databases. Clause should read as: Solution should support the logging of events to a non- proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL also management platform should support Windows & Linux operating systems.	As per RFP.
6		Suggestion/Recommendation		As per MoUD, NCIIPC, DSCI, NIST and Cert-In guidelines which recommend to adhere defence in depth layered security approach by incorporating different dedicated security layers from different OEM to avoid any single point of failure. We would request you to not allow existing network security and routing switching vendor to participate for current RFP for endpoint security requirement to avoid single point of failure inline to guidelines laid down by our governing agencies.	As per RFP.
7		Suggestion/Recommendation		Given a Datacentre environemnt, We assume that there should be an endpoint security solution already running in your environment. We would like to understand whether you are looking for integration of proposed solution with an existing endpoint solution running in your environment to achieve holistic visibility and control.	As per RFP.

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
8	48	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 7	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.	As per RFP specification mentioned, this particular point is requesting the inclusion of predefined lists of critical system files, either for operating systems or applications (such as web servers, DNS, etc.). However, it is observed that excluding the operating system/application may potentially compromise data center security. Therefore, we kindly request the inclusion of both components—operating systems and applications—for enhanced efficacy in ensuring data center security. Clause should read as : Solution should support any pre-defined lists of critical system files for various operating systems and applications (web servers, DNS, etc.) and support custom rules as well.	As per RFP.
9	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 16	Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems	This particular point seems to duplicate point No. 13; nevertheless, we humbly request the addition of a feature for automatically recommending rules in the log analysis module based on the Server OS. Given that a significant number of ransomware attacks can be identified in the initial phases through server logs, such a feature would greatly assist organizations in securing their critical assets. Therefore, we kindly ask for the incorporation of automatic recommendation rules for log analysis. Clause should read as : Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/unassigment of rules also should have capability of pattern matching like Regular Expressions or simpler String Patterns and rule will be triggered on a match also ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.	As per RFP.

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
10	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 20	Proposed OEM should be positioned in any quadrant from latest published Gartner Magic quadrant report for Endpoint Protection.	In accordance with the guidelines outlined in the Request for Proposal (RFP), the clauses recommend a proposal from an Original Equipment Manufacturer (OEM) currently positioned in the latest Gartner Magic Quadrant. We kindly request your consideration to include either Gartner Leaders and Challengers to ensure the selection of best-of-breed products for securing crown jewels. Clause should read as: Proposed OEM must be positioned in either the Leaders or Challengers quadrant according to the latest published Gartner Magic Quadrant report for Endpoint Protection.	As per RFP.
11	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 25	Should automatically submit unknown files/suspicious object samples with OnPremise sandbox solution for simulation and create IOCs on real time basis as per sandboxing analysis and revert back to server security. Should support existing server operating OS RHEL 6.x, 7.x, 8.x, 9.x and higher, and Windows Server 2016, 2019, 2022and higher.	As per the specifications in the RFP, the clauses indicate to include sandboxing for existing operating system used in the Data Centre environemnt (RHEL 6.x, 7.x, 8.x, 9.x and higher, and Windows Server 2016, 2019, 2022and higher) to safeguard critical workloads against zero-day attacks. However, it has been observed that the term "sandboxing" is not explicitly mentioned in the second line. We kindly request your consideration in accepting this amendment to enhance the protection for your critical workloads. Clause should read as: Should automatically submit unknown files/suspicious object samples with OnPremise sandbox solution for simulation and create IOCs on real time basis as per sandboxing analysis and revert back to server security. Proposed solution should support custom sandboxing for existing server operating OS RHEL 6.x, 7.x, 8.x, 9.x and higher, and Windows Server 2016, 2019, 2022and higher for ensuring protection from zero-day and ransomware attacks.	As per Revised RFP.

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
12	49	Item -1: Endpoint Detection and Remediation/Response (EDR) - Point No. 21	Management of proposed solution should support both window as well as Linux platform	As per the RFP specifications, it's noted that the proposed management server should be compatible with both Windows and Linux operating systems. Additionally, we kindly request clarification regarding the requirement for database licensing for management server. Furthermore, we would appreciate the inclusion of MS-SQL, Oracle and PostgreSQL for logging events to non-proprietary, industry-standard databases. Clause should read as: Solution should support the logging of events to a non- proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL also management platform should support Windows & Linux operating systems.	As per RFP.
13		Suggestion/Recommendation		As per MoUD, NCIIPC, DSCI, NIST and Cert-In guidelines which recommend to adhere defence in depth layered security approach by incorporating different dedicated security layers from different OEM to avoid any single point of failure. We would request you to not allow existing network security and routing switching vendor to participate for current RFP for endpoint security requirement to avoid single point of failure inline to guidelines laid down by our governing agencies.	As per RFP.
14		Suggestion/Recommendation		Given a Datacentre environemnt, We assume that there should be an endpoint security solution already running in your environment. We would like to understand whether you are looking for integration of proposed solution with an existing endpoint solution running in your environment to achieve holistic visibility and control.	As per RFP.
15	47	Annexure 1 BoM	Item 1 : EDR Item 2 - 5 : SSL	We request for allowing separate participation of each package since the products belong to completely different domains / OEMs. Package 1 : Item 1 : EDR Package 2 : Item 2 - 5 : SSL	As per RFP.
16	47	Annexure 1 BoM	Item 2 - 5 : SSL MAF & Compliance	We request you to revise the terms and conditions for Item 2 - 5 : SSL , that bidder can also submit the OEM MAF & Compliance on OEM Letterhead / On Letterhead of authorized distributor of quoted OEM with proof of authorization from OEM.	As per Revised RFP.

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
17	48	Annexure 2 Item 1 EDR	Clause 1 Proposed solution should be completely On-Premise based having single unified agent.	Proposed solution should be completely On-Premise / Cloud based having single unified agent. As EDR solution can be of on-premise or on cloud following MEITY guidelines of India data residency.	As per RFP.
18	48	Annexure 2 Item 1 EDR	Clause 4 Proposed solution should protect against distributed DoS attack and should have the ability to lock down a computer (prevent all communication) except with management server.	Proposed solution should have the ability to lock down a computer (prevent all communication) except with management server in case of ransomware attack. As Locking down individual computers wouldn't mitigate a DDoS attack, as it targets the network infrastructure rather than specific machines. Instead, the solution must have the capability to quarantine or lock down computer in case of ransomware attacks. Therefore, request to amend the changes as suggested.	As per Revised RFP.
19	48	Annexure 2 Item 1 EDR	Clause 6 It should provide automatic recommendations against existing vulnerabilities	It should provide automatic recommendations/remediation against existing or zero day vulnerabilities. As per recommendations, while helpful, rely on human action and may not be implemented promptly or consistently, leaving systems exposed to potential exploitation for longer periods. Automatic remediation minimizes response time, enhances security posture, and reduces the risk of successful attacks. Therefore, request to amend the changes as suggested.	As per Revised RFP.
20	48	Annexure 2 Item 1 EDR	Clause 9 Host IPS/EDR should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless. Solution must detect and block access to suspicious, dangerous phishing sites by scanning all form fields.	Host IPS/EDR should be capable of creating/recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule scan. Solution must detect and block access to suspicious , dangerous phishing sites by scanning all form fields. As per recommendations, while helpful, rely on human action and may not be implemented promptly or consistently, leaving systems exposed to potential exploitation for longer periods. Automatic remediation minimizes response time, enhances security posture, and reduces the risk of successful attacks. Therefore, request to amend the changes as suggested.	As per Revised RFP.

S.No.	RFP. Page No.	Rule No.	Rule Details	Query/ Suggestion/ Clarification Note:	Remark/ Response
21	48	Annexure 2 Item 1 EDR	Clause 15 Should provide recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Selecting rules, configuring policies, updating policies) provide automatic recommendation of removing assigned policies if vulnerability no longer exists	The solution must include an option for Host Isolation/quarantine to isolate specific host (access to network) that is under malware attack and poses a risk of propagation. Vulnerabilities can potentially reappear or be exploited in different ways therefore, removing an assigned policy when a vulnerability no longer exists may leave the system unprotected if the vulnerability resurfaces. It's safer to maintain security policies as a proactive measure to mitigate potential risks and to continuously monitor and update security measures even if vulnerabilities appear to be resolved. Instead solution must have the capability to automatically quarantine the infected host machine without human intervention in order to prevent malware spread across different machines.	As per Revised RFP.
22	48	Annexure 2 Item 1 EDR	Clause 22 Container security automated processes for critical security controls to protect containers and the Docker host.	Solution should safeguard developers from leaking sensitive information like passwords and keys. It should intercept git commit commands and scan modified files in repositories for security purposes. Containers have their own unique security considerations and attack surfaces that require specialized security solutions tailored for containerized environments. This clause is specific to an OEM. Therefore, request to amend the clause for wider participation.	As per Revised RFP.
23	48	Annexure 2 Item 1 EDR	Clause 23 Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless.	Host IPS/Anti-Exploit should be capable of recommending-rules/protect based on vulnerabilities with the help of virtual patching and should have capabilities to schedule scan. Host IPS will have limited capabilties based on signatures only instead solution should be capable of prevent real time attack. Request to amend the clause as suggested.	As per Revised RFP.
24	48	Annexure 2 Item 1 EDR	Clause 24 HIPS Solution Should not has the need to provision HIPS Rules from the Policy Server as the Rules should be automatically provisioned to shield vulnerabilities using virtual patching	EDR/HIPS solution should be capable of reducing the attack surface with risk assessment and Vulnerability & Patch management. Host IPS will have limited capabilties based on signatures only instead solution should be capable of prevent real time attack. Request to amend the clause as suggested.	As per Revised RFP.