| Response to Pre-Bid Queries for RFP | | | | | |
|---|---|---|---|---|---|
| RFP Ref. No. | CPCM-27/2025-26 Date: 13-Feb-2026 GEM Bid No. GEM/2026/B/7237338 | | | | |
| RFP Name | Request for Proposal (RFP) for SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION AND SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION AND RESPONSE SERVICES (MDR) | | | | |
| **Sr. No.** | **Page No.** | **RFP Clause** | **Clause Description** | **Query** | **StockHolding Remarks** |
| 1 | 13 & 36 | Technical Bid Evaluation<br>Point No. 4 | OEM solution must be positioned in the respective Leader’s quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave reports for proposed SIEM Solution | We request the authority to delete this clause in line with the Government ofIndia’s Public Pro curement (Preference to Make in India) Order, 2017, issuedby DPIIT, Ministry of Commerce & Industry, Ref. No.P-45021/2/2017-PP(BE-II) and subsequent amendments.<br>Gartner Magic Quadrant positioning is not a mandatory requirement under GoI procurement policy and restrict participation of eligible Indian OEMs. We request that Government /Defense/BFSI/ PSU / Judiciary Purchase Orders beaccepted as equivalent compliance. | No change<br>This is not a mandatory requirement for participation but a part of technical scoring criteria. |
| 2 | 10 & 35 | Eligibility Criteria<br>Point No. 8 | Bidder should have a Support office at MMRDA Region or Pune. | With reference to the clause stating that “Bidder should have a Support Office at MMRDA Region or Pune,” we respectfully request the Authority to kindly review and modify this requirement.<br>We submit that mandating an existing support office at the time of bid submission may restrict wider participation. We propose that bidders who donot presently have a support office in the MMRDA Region or Pune may be permitted to submit a declaration confirming that, upon award of the contract, they shall establish a support office within 45 days.<br>This modification will promote fair competition and broader participationwithout affecting service delivery commitments or project timelines. | No change |
| 3 | | | | Seems to be a Typo. Bidder should have Support office at Mumbai. | **Clarification:**<br>Bidder should have a Support office at MMRDA Region or Pune. |
| 4 | 24 | Transition Management (On-boarding and During-Exit) | | The RPF refers to the transition of MDR services. Could the customer please confirm which MDR/SIEM platform is currently in use (e.g., QRadar, Splunk, ArcSight, or any other)? | **Clarification:**<br>Custom built platfrom from ATOS |
| 5 | 16 | Scope of Work (SOW)<br>Solution Implementation | j) The solution should be able to handle at least 2000 sustainable EPS and scalable to 5000 Peak EPS. | The scope mentions average and peak EPS requirements. Could the customer confirm the current EPS utilization along with the types and number of onboarded log sources? | **Clarification:**<br>EPS range is already mentioned, bidder has to calibrate the  Solution as per this requirement |
| 6 | | | | Need clarity to define EPS, GB/Month and GB/Day (need correct nos yearlyt basis, what if there is an increase in usgae per year in (EPS, GB/Day, GB/Month) | **Clarification:**<br>Based on the EPS range mentioned, bidder has to calibrate the  Solution as per this requirement |
| 7 | | | | Please share indicative daily ingest volume (GB/day) | **Clarification:**<br>Based on the EPS range mentioned, bidder has to calibrate the  Solution as per this requirement |
| 8 | | General | General | Could the customer confirm the total number of log sources, along with their respective types, that they intend to integrate with the SIEM? | **Clarification:**<br>Please refer pg- 19-20 --> Security solutions to be integrated with SIEM Platform |
| 9 | | General | General | Could the customer confirm whether a SOAR platform is currently in use? If yes, please provide the total number of playbooks that will need to be migrated. | **Clarification:**<br>No SOAR platform in place |
| 10 | 16 | Scope of Work (SOW)<br>Solution Implementation | h) While, it is expected that connectors for all the standard applications and devices will be readily available with the Service Provider and connector for mostly in-house/custom built applications will need to be developed. Service Provider is be expected to develop connector for the custom built applications specifically developed for StockHolding. | The scope refers to “custom built applications.” Could the customer confirm how many such applications are currently integrated with the SIEM, and whether there are any new applications planned for integration? | **Clarification:**<br>Existing custom build applications - None<br>Future expected custom build application - Cannot be decided at this point. To be built as and when required |
| 11 | | General | General | Please provide the total number of use cases and reports currently deployed that are planned for migration. | **Clarification:**<br>Details shall be shared with winning bidder |
| 12 | | General | General | Could the customer share the daily alert volume along with a breakdown of true positives and false positives? | **Clarification:**<br>Details shall be shared with winning bidder |
| 13 | | General | General | Please clarify the total log retention requirement. Is the 180-day retention period applicable to online storage only, or does it include both online and offline storage?<br>Additionally, is there a requirement to retain logs beyond 180 days? | **Clarification:**<br>Online logs should be made available for 180 days<br>Offline logs within the platform should be made available for 2 years |
| 14 | 17 | Log Collection | Logs from all the in-scope devices and additional devices integrated as part of contract period located at the geographically dispersed location should be collected. Bidder / Vendor should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with industry best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, bidder / vendor should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement. Prepare Daily, Weekly, Monthly compliance reports. | Could the customer confirm the total number of sites and offices from which log collection is required? | **Clarification:**<br>All device logs shall be aggregated at a log collector at DC, NDR and DR site (1 each) except WAAP and EDR logs which will be ingested via API's. In the future, as and when SDWAN is implemented, the logs shall be ingested directly from the routers and switches presented at PAN-India Level (approx. 205 branches) through local breakout at branches/Centrally as the case may be.<br>Any new infra if depoyed at StockHolding in the near future, should also be onboarded in the SIEM platform. |
| 15 | 17 | Alert Generation | Solution should be capable to generate alerts, register and send/receive the same through message formats like SMTP, SMS, Syslog, and SNMP as per user configurable parameters. | The scope mentions alert generation through channels such as SMTP, SMS, Syslog, and SNMP. Could the customer confirm whether they currently have an SMS gateway available? | **Clarification:**<br>Since the platform shall be generating the SMS incase of alerts, it is expected that the bidder shall configure the SMS Gateway at their end. |
| 16 | 17 | Event viewer / dashboard / reports / incident management | Solution should provide various reports based on user onfigurable parameters and standard compliance reports like ISO27001, IT Act and regulatory reports.<br>Selected bidder will customize incident management / dashboard / reports for StockHolding and will modify the same as per the changing requirement of StockHolding. | The scope references reporting requirements such as ISO 27001. Could the customer confirm if any additional compliance reports are required apart from ISO 27001? | **Clarification:**<br>Since we are a regulated entity, any regulatory reports as per SEBI, Depositories, Stock Exchanges, PFRDA, IRDA etc. should be made available. SOC2Type2 Report shall also be made available |
| 17 | 17 | Incident Management Tool | | The scope states that the SIEM should include an integrated incident management tool. Could the customer confirm whether they require case management capabilities for tracking alerts, investigations, and the incident lifecycle? | **Clarification:**<br>Yes, case management capabilities tracking alerts, investigations, and the incident lifecycle should be available |
| 18 | 12 | Technical Bid Evaluation | | We would request you to consider SOC experience in managing 'national critical infrastructure' sector also, along with the BFSI for scoring criteria. | No change |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 19 | 44 | Technical Compliance<br>Point no. 44 | Log Archival: Logs collected from all the devices should be stored in a non-tamper able format on the archival device in a compressed form. Collection of Logs and storage should comply with the Regulatory requirement and should maintain a chain of custody to provide the same in the court of law, in case the need arises. For correlation and report generation purpose, past 180 days log data should be available online. Logs prior to 180 days period should be stored on removable media. Service Provider will ensure that retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols. | Please clarify if 90 days of online retention and upto 365 days of archival retention suits? | **Clarification:**<br>Online logs should be made available for 180 days<br>Offline logs within the platform should be made available for 2 years. Please refer EPS requirement |
| 20 | | | | As mentioned, online logs are required to be retained for 180 days, and an additional 180 days are allocated for log archival. Kindly confirm how many days the logs need to be stored beyond the total 365-day period. | **Clarification:**<br>Online logs should be made available for 180 days.<br>Offline logs within the platform should be made available for 2 years. |
| 21 | 39 | Technical Compliance<br>Point no. 18 | Alert Generation<br>Solution should be capable to generate alerts, register and send/receive the same through message formats like SMTP, SMS, Syslog, and SNMP as per user configurable parameters | Please clarify, Alert information can be shared using officials mail communication? | **Clarification:**<br>Yes. Email based communication is allowed. |
| 22 | | | | Is SMS alert mandatory | **Clarification:**<br>Yes, for high and critical alerts/incidents. |
| 23 | 9 | ELIGIBILITY CRITERIA<br>Point no. 4 | The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second).<br>Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP. | Request to relax this clause as below.<br><br>The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second).<br>Note: Bidder to submit the experience of **proposed/similar** SIEM and MDR tool only for this RFP. | No change |
| 24 | 9 | | | Please allow to submit separate PO references for SIEM and MDR services to comply this clause. | No change |
| 25 | 9 | ELIGIBILITY CRITERIA<br>Point no. 4 | | Request to reconsider removal of EPS as the only Measure to define the past experience. Our SIEM solution relies on the Number of Devices, request you to relax the requirement or alternatively quantify ....with at least one (01) deployment handling not less than 300 devices provisioned.<br>Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP. | **Change Clause:**<br>The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or minimum 1000+ devices. |
| 26 | 9 | ELIGIBILITY CRITERIA<br>Point no. 4 | | removal of EPS as the only Measure to define the past experience. Our SIEM solution relies on the Number of Devices, request you to relax the requirement or alternatively quantify Minimum number of devices to be considered as 300 devices | **Change Clause:**<br>The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or minimum 1000+ devices. |
| 27 | 12 | Technical Bid Evaluation<br>Point no. 2 | Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) each during last 05 (five) years in India<br>Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP.<br><br>• 1-3 Projects – 10 Marks<br>• 4-5 Projects – 12 Marks<br>• More than 5 Projects – 15 Marks | Request to relax this clause as below.<br><br>Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) each during last 05 (five) years in India<br>Note: Bidder to submit the relevant experience only of **the proposed/similar** SIEM and MDR tool for this RFP.<br><br>• 1-3 Projects – 10 Marks<br>• 4-5 Projects – 12 Marks<br>• More than 5 Projects – 15 Marks<br><br>**Also, Please allow to submit separate PO references for SIEM and MDR services to comply this clause.** | No change |
| 28 | 13 | Technical Bid Evaluation<br>Point no. 3 | Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India<br><br>• 1-3 Projects – 5 Marks<br>• 4-5 Projects – 7 Marks<br>• More than 5 Projects – 10 Marks | Request to relax this clause as below.<br><br>Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India<br><br>• **1-2 Projects** – 10 Marks<br>• **2-3 Projects** – 12 Marks<br>• **More than 3 Projects**– 15 Marks<br><br>**Also, Please allow to submit separate PO references for SIEM and MDR services to comply this clause.** | No change |
| 29 | 29 | Payment Terms: | SIEM Subscription + MDR Services -<br>Monthly payment post adjustment of penalties if any for that quarter after SIEM – MDR Implementation Go-Live Milestone | Request to relax this clause as below.<br><br>SIEM Subscription + MDR Services - **Advance payment** on yearly basis | **Clarification:**<br>No Change |
| 30 | 12 | Technical Bid evaluation<br>Point No. 2 | Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) each during last 05 (five) years in India Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP. | Need clarity to define EPS, GB/Month and GB/Day (need correct nos yearlyt basis, what if there is an increase in usgae per year in (EPS, GB/Day, GB/Month). | **Clarification:**<br>We have given indicative minimum 2000 EPS and scalable to 5000 EPS. Any usage upto 5000 EPS has to be borne by the bidder without any additional cost to StockHolding |
| 31 | 13 | Technical Bid evaluation<br>Point No.4 | OEM solution must be positioned in the respective Leader's quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave | OEM Solution should/platfrom should be in any Quadrant of Gartner, IDC Market share, latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave | No change<br>This is not a mandatory requirement for participation but a part of technical scoring criteria. |
| 32 | 15 | Security Information and Event Management | The SIEM solution is required to collect logs from network devices, servers, application security logs, Anti-virus, Security devices, Security solutions like VA tool etc. | Solution should be able to collect Raw logs telemetry for in-depth in AI- threat analysis  (detection logs does not provide deeper insights) | **Clarification:**<br>Log aggregator has all the device logs. It is upto Bidder to decide which type of logs to be ingested in order for SIEM platform to co-relate. |
| 33 | 15 | Expectation from Managed Detection and Response (MDR) Services: | No Half-Measures in Defending the Cyber Assets: MDR offering to provide for all six components of threat management – intelligence, analytics, SIEM, forensics, cyber incident remediation, and breach management—to protect StockHolding's critical infrastructure and networks | Solution should also provide Breach Prevention Warranty by 3rd party Cyber Insurance to provide coverage over breach management cost | **Clarification:**<br>No Change |
| 34 | 16 | Solution Implementation | a) SIEM solution shall be implemented in Service Provider's Data Centre or Cloud based. The Service Provider shall ensure that Data Centre / Cloud Service shall be hosted in India and in no circumstances data shall not move out of India during the entire contract duration. | or the SIEM Solution should be able to provide a copy of logs within the legal boundaries of India. (like EDR) | **Clarification:**<br>No Change. Platform should be hosted in India |
| 35 | | | | **Request for Clarification:**<br><br>Kindly confirm whether the SIEM licenses are required to be procured and owned in the name of Stock Holding, or if a bidder-owned licensing model is also acceptable. | **Clarification:**<br>Bidder owned licensing model is acceptable. However, tenancy shall be in the name of Stockholding |
| 36 | 24 | Service Level Agreement (SLA) and Penalty | Service Level Agreement (SLA) and Penalty | Need more time to revert bank on the SLA and Penalty clause | **Clarification:**<br>**No Change** |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 37 | 31 | Indemnify | **Indemnify:-**<br>The Bidder should hereby indemnify, protect and save StockHolding against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder in which name of StockHolding is used should be done only with the explicit permission of StockHolding. | **We propose adding an exception to the existing indemnity clause as below:-**<br>**Indemnity:-**<br>Exceptions to Indemnity<br>The Bidder shall not be liable to indemnify StockHolding for any claim or infringement arising from (i) any misuse, alteration, or unauthorized modification of the equipment or services by StockHolding; (ii) any use of the equipment or services in combination with third-party products not supplied or recommended by the Bidder; (iii) StockHolding's failure to follow the Bidder's operating instructions or specifications; or (iv) any materials, data, or specifications provided or mandated by StockHolding that result in an infringement claim. | No change |
| 38 | 31 | Termination Clause | **Termination Clause:-**<br>StockHolding reserves right to terminate the contract by giving 90 days prior written notice in advance against any of the following conditions –<br>a) If penalty amount (excluding penalty on resource management) is equal to or more than 10% of monthly contract value for consecutively 3 times in a particular year;<br>b) If penalty amount on Resource Management is equal to or more than 10% of monthly contract value for consecutively 3 times in a particular year;<br>c) If at any point of time, the services of bidders are found to be non-satisfactory; | **We propose addition to the existing clause as below:-**<br>**Termination Clause:-**<br>For Temination by the Bidder for breach:-<br>In the event StockHolding materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the StockHolding, the Bidder may terminate this defenitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the StockHolding. | No change |
| 39 | General | | Recommending new clause to RFP | **We reccomending below clause under the RFP:-**<br>**Limitation of Liability:-**<br>NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, OR LOSS OF DATA, OR INTERFERENCE WITH BUSINESS, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.<br>In no event, regardless of the form of the claim or cause of action (whether based in contract, negligence, strict liability, tort or otherwise) shall either Party's aggregate liability to the other Party under this Agreement exceed the fees actually paid under a relevant Purchase Order or Statement of Work which is subject matter of claim | No change |
| 40 | General | | We recommend including a Non-Solicitation clause in the RFP | **We recommending below clause under the RFP:-**<br>**Non-Solicitation:-**<br>During the Term of this definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, "Representatives"). Parties agree that Associates are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party. | No change |
| 41 | 36 | ANNEXURE – 3 – Technical Criteria & Compliance<br>Point No.2 | Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) each during last 05 (five) years in India<br>Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP. | We request to modify the clause as below:-<br>Projects for implementation of SIEM / MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) each during last 07 (Seven) years in India Note: Bidder to submit the relevant experience only of the SIEM / MDR tool for this RFP. | **Change Clause:**<br>Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or minimum 1000+ devices each during last 05 (five) years in India<br>Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP. |
| 42 | 36 | ANNEXURE – 3 – Technical Criteria & Compliance<br>Point No.3 | Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India | We request to modify the clause as below:-<br>Projects of SIEM/MDR services implementation in BFSI Sector in India during last 07 (Seven) years in India | **Change Clause:**<br>Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or minimum 1000+ devices each during last 05 (five) years in India<br>Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP. |
| 43 | | ANNEXURE – 3 – Technical Criteria & Compliance<br>Point No.2 & 3 | - | If a bidder has experience in implementing and managing SOC operations for global customers, with services delivered from India, will such experience be considered valid for meeting the stated qualification criteria? | Bidder to submit relevant experience as per terms and conditions of the RFP |
| 44 | 36 | ANNEXURE – 3 – Technical Criteria & Compliance<br>Point No.6 | Customer reference for proposed SIEM-MDR Solution during the last 5 years as on RFP date | We request to modify the clause as below:-<br>Customer reference for SIEM /MDR Solution during the last 5 years as on RFP date | **Clarification:**<br>No Change |
| 45 | 34 | ANNEXURE - 2 – Eligibility Criteria Point No.4 | The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second).<br><br>Note: Bidder to submit the experience of proposed<br>SIEM and MDR tool only for this RFP. | We request to modify the clause as below:-<br>The bidder must have executed a minimum of three (03) projects related to SIEM / MDR services in India during the last Seven (07) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second).<br><br>Note: Bidder to submit the experience of SIEM / MDR tool only for this RFP. | **Change Clause:**<br>The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or minimum 1000+ devices.<br><br>Note: Bidder to submit the experience of proposed<br>SIEM and MDR tool only for this RFP. |
| 46 | 29 | Terms and Conditions<br>A. Payment<br>Point No. 1 | 50% on SIEM – MDR Implementation Go-Live (Part A-600 devices to be on-boarded to the log collector)<br>50% on Remaining Device On-boarding Go-Live (Part B-600 devices to be on-boarded to the log collector) | We request to modify the clause as below:-<br>70% on SIEM – MDR Implementation Go-Live (Part A-600 devices to be on-boarded to the log collector)<br>30% on Remaining Device On-boarding Go-Live (Part B-600 devices to be on-boarded to the log collector) | **Clarification:**<br>No Change |
| 47 | | | | Revision of One-time Implementation of SIEM Platform. The Software licenses as well as Cloud Provisioning (Compute+ Storage+ Retention+ Securty measures) hence we propose to have following model,<br><br>40% of total One-time Implementation of SIEM Platform as Upfront payment.<br>30% on SIEM – MDR Implementation Go-Live (Part A - 600 devices to be on-boarded to the log collector)<br>30% on Remaining Device On-boarding Go-Live (Part B- 600 devices to be on-boarded to the log collector) | **Clarification:**<br>No Change |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 48 | | | | Request to reconsider minimum experience requirement.Minimum 3 years of experience in implementation and support for SIEM & MDR . | **Clarification:**<br>No Change |
| 49 | | | | Are there any end point devices that are to be monitored through SIEM | **Clarification:**<br>The winning bidder shall integrate with the existing EDR platform via API and ingest the logs for monitoring through SIEM |
| 50 | | | | How many devices are to be considered as critical devices out of 1200 | **Clarification:**<br>All devices are considered as critical |
| 51 | | | | The RFP mentions "Part A – 600 devices to be on-boarded to the log collector" and "Part B – 600 devices to be on-boarded to the log collector", which indicates a total baseline of 1200 devices for SIEM–MDR implementation.<br>Kindly confirm whether bidders should consider 1200 devices as the total in-scope device count for sizing, licensing, infrastructure, and commercials.<br>If yes, please provide the detailed device-wise breakup of these 1200 devices across log source categories (e.g., servers, network devices, security devices, applications, databases, endpoints, cloud platforms, etc.) to enable accurate sizing, effort estimation, and commercials. | **Clarification:**<br>1. Yes. Total devices shall be 1200<br>2. Device wise breakup shall be shared with the winning bidder |
| 52 | | | | Any requirement for onshore presence / dedicated onsite SOC resources at Stockholding for coordination, incident response? | **Clarification:**<br>Not Required. However monthly reviews shall be an onsite based meeting. |
| 53 | | | | Payment Terms: Monthly payment post adjustment of penalties if any for that quarter after SIEM – MDR Implementation Go-Live Milestone. Please confirm payment term, is it Monthly advance, net 30 days? | **Clarification:**<br>Not Required |
| 54 | | | | As per the RFP, it is mentioned that 1,200 devices/applications need to be onboarded. However, upon reviewing the current RFP inventory, the total count of devices/applications is not clearly specified.<br>Please find below the queries based on the infrastructure stack shared.Based on this detail we will able to factor the Project time lines, Deliverty & Custom parser & use cases | **Clarification:**<br>Count of devices shall be shared with the winning bidder |
| 55 | 19 | Technical Compliance<br>Brief description of how operations are performed post Implementation | e) Threat Hunting: Threat hunting advocates – "Don't wait for alerts to show up; hunt them". Output of advanced security analytics models run on the platform which is analyzed by a specialized hunting team and the data is queried further to detect threats that may have bypassed other security controls or use cases. This is security analytics in action: MSSP should apply data science and machine learning models to network, application, user, and machine data to proactively hunt for unknown and hidden threats in our environment. | **Request for Clarification:**<br>Kindly confirm the number of threat hunting exercises/programs the bidder is expected to consider under the scope. | **Clarification:**<br>It is expected to perform continous threat hunting activities - This is security analytics in action: Winning Bidder should apply data science and machine learning models to network, application, user, and machine data to proactively hunt for unknown and hidden threats in our environment. |
| 56 | 20 | Deliverables<br>Managed Detection and Response Sizing and Capabilities | Service Provider will deliver:<br>Unified Tool - One click access to program Status.<br>Access and demo will be provided during the pre-kick off discussion. | **Request for Clarification:**<br>Kindly confirm whether the customer expects a separate MIS/reporting tool to gain visibility into SOC operations, or if providing SIEM console access for SOC alert visibility will suffice.<br>Additionally, please confirm the number of user accounts that the bidder is required to provision for this purpose. | **Clarification:**<br>StockHolding expects a unified dashboard providing consolidated visibility into SOC operations, not limited to incident status, SLA performance, reporting, and executive summaries; SIEM console access alone will not be sufficient.<br>The bidder may provide either a separate MIS/reporting tool or an integrated dashboard within the SIEM/MDR platform meeting these requirements. |
| 57 | 10 & 34 | ELIGIBILITY CRITERIA (Documents to be Submitted Online)<br>Point No.7 | The bidder must have a direct partnership with the supplier of the SIEM tool. One Service Provider can bid only with one OEM as regards SIEM solution is concerned | **Request for Modification:**<br>The bidder must have a direct partnership with the supplier of the SIEM tool. ~~One Service Provider can bid only with one OEM as regards SIEM solution is concerned~~<br>**Justification:**<br>Most qualified bidders maintain partnerships with multiple Gartner Leader SIEM OEMs and have successfully delivered similar complex SOC and SIEM engagements in the past. Therefore, bidder capability should ideally be evaluated based on demonstrated technical expertise, project experience, and delivery maturity rather than being narrowly constrained by partnership structure.<br>In the interest of promoting wider participation, ensuring fair competition, and enabling the customer to receive the most technically and commercially optimal solution, we respectfully request the tender committee to consider revising this clause accordingly. | Bidder can have partnerships with multiple SIEM OEMs but can bid  with SIEM solution of any one OEM only. The bidder must have a direct partnership with the supplier of the SIEM tool. |
| 58 | 40 | Incident Management Tool,<br>Point No. 20 | The principal goal of the incident management process is to identify anomalous activities in the environment, contain those events and restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus facilitating continued service quality and availability. | The containments of events & restore normal service operations are  such capabilities typically require orchestration and automated response functionality through SOAR.<br>"Kindly confirm if there is any  requirement of SOAR solution as well." | **Clarification:**<br>No SOAR platform in place |
| 59 | 40 | Incident Management Tool,<br>Point No.  23 | Bidder should also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate/remediate, recover and learn from the incidents responded to. | The capabilities such as "contain, eradicate/remediate, recover" belong to SOAR,<br>Kinldy confirm if there is any requirement for SOAR solution. | **Clarification:**<br>No change. These activities can be executed manually as well. |
| 60 | 40 | Managed Detection and Response Services,<br>Point No.30 | Raising remediation tickets to pre-defined users with recommendations and/or response playbooks | Features such as "response playbooks" belong to SOAR,<br>Kindly confirm if there is any  requirement of SOAR solution. | **Clarification:**<br>No SOAR platform in place |
| 61 | 41 | Brief description of how operations are performed post Implementation,<br>Point No. 38 | As a part of the Standard MDR offering, Service Provider should detect, investigate and contain threats. Post that, they will send out tickets to StockHolding's SOC team for mitigation and response actions within our network. They will also provide playbooks and knowledge base to help us resolve these tickets. StockHolding's SOC team can reach back to them for query resolution but such support is provided on best effort basis. | "To contain threat", is a feature of SOAR solution.<br>Kindly confirm if there is any requirement of SOAR solution. | **Clarification:**<br>No change. These activities can be executed manually as well. |
| 62 | 38 | Solution Implementation,<br>Point 10 | The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by StockHolding as per the SOW including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations i.e. DC, DR and branch offices, etc. | Kindly mention the number of locations of DC, DR, NDR & branch offices, whose logs needs to be monitored. | **Clarification:**<br>All device logs shall be aggregated at a log collector at DC, NDR and DR site (1 each) except WAAP and EDR logs which will be ingested via API's. In the future, as and when SDWAN is implemented, the logs shall be ingested directly from the routers and switches presented at PAN-India Level (approx. 205 branches) through local breakout at branches/Centrally as the case may be.<br>Any new infra if depoyed at StockHolding in the near future, should also be onboarded in the SIEM platform. |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 63 | | | | Kindly confirm whether DC,DR & NDR are in High Availability or not. | **Clarification:**<br>This information is not relevant. Logs from devices shall be aggregated into a log collector at StockHolding end and the SIEM platform should ingest these logs |
| 64 | 13 & 36 | Annexure-3- Technical Criteria & Compliance<br>Point No.4 | OEM solution must be positioned in the respective Leader's quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave reports for proposed SIEM Solution<br>Presence of OEM Solution in Leader's quadrant/category – 10 Marks | Kindly Requesting to give Exemption or Waive Off for this Clause, This will help more Make In India startups to come forward and particpate in this opportunity<br>With Reference to Public Procurement (Preference to Make In India) Order 2019 from MeitY Point No.8:-In any procurement process, the procuring entity shall not specify any mandatory qualification criteria, any eligibility specifications or certification(s) issued by any foreign testing/security lab(s)/analyst reviews which restricts eligibility of Indian cyber security products as defined in this order. | No change<br>This is not a mandatory requirement for participation but a part of technical scoring criteria. |
| 65 | 12 & 35 | Annexure-3- Technical Criteria & Compliance<br>Point No. 2 | Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) each during last 05 (five) years in India<br>Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP.<br>• 1-3 Projects – 10 Marks<br>• 4-5 Projects – 12 Marks<br>• More than 5 Projects – 15 Mark | This clause is restricting multiple Bidders and OEMs of different make and models to participate in the tender because in each and every bid or tender, the products quoted regularly will change and the bidder always looks at the best commercial models quoted by the OEM. So it will be difficult for bidders as well as OEMs to participate in this opportunity.<br>Kindly amend this clause to " **Note: Bidder to submit the relevant experience of SIEM and MDR**' that will help multiple Bidders and OEMs to participate in this opportunity and it helps the customer also to get the best of the products available in the market to cater the requirement. | No change |
| 66 | 9 | Eligibility Criteria<br>Point No. 1 | The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of SIEM and MDR services implementation and support for the period of 7 years. | We request to cosider the experience of SIEM/ MDR/ SOC services implementation and support for the period of 5 Years. | No change |
| 67 | | | | Request to reconsider minimum experience requirement.Minimum 3 years of experience in implementation and support for SIEM & MDR . | No change |
| 68 | 9 | Eligibility Criteria<br>Point No.4 | The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second).<br>Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP. | We request to consider a min. of three (03) projects related to SIEM/ MDR/ SOC Services in India during the last five(05) years as on RFP date with at least one (01) deployment with 2000 EPS (Events Per second) | No change |
| 69 | 16 | Solution Implementation | j)The solution should be able to handle at least 2000 sustainable EPS and scalable to 5000 Peak EPS | Kindly confirm whether 5000 peak EPS licensing is required upfront or scalable during contract tenure. | **Clarification:**<br>Scalable during contract tenure. |
| 70 | 21 | Logging of Critical Devices | a) The Service Provider is required to maintain the syslog of the devices installed at DC, DR and NDR locations for a period of 180 days. | Please clarify whether 180 days refers to hot/searchable storage or includes archived storage. Also confirm expected average log ingestion per day (GB/day). | **Clarification:**<br>Online logs should be made available for 180 days<br>Offline logs within the platform should be made available for 2 years. Please refer EPS requirement |
| 71 | 20 | Managed Detection and Response Sizing and Capabilities | Integration with multiple security devices | Kindly provide log source count per category (Firewall, WAF, EDR, AD, DB, Network, etc.) for accurate EPS sizing. | **Clarification:**<br>Details shall be shared with winning bidder |
| 72 | 23 | Integration of devices in Managed detection and response along with SIEM Services | d) 24X7X365 log monitoring for in scope devices and applications. | Please confirm whether L3 investigation and forensic analysis is included within MDR scope. | **Clarification:**<br>L3 investigation is part of scope. However, Forensic analysis is out of scope |
| 73 | 23 | Threat Hunting | Advanced analytics and ML-based hunting | Kindly confirm frequency and deliverables of proactive threat hunting (monthly report, executive summary, etc.). | **Clarification:**<br>It is expected to perform continous threat hunting activities - This is security analytics in action: Winning Bidder should apply data science and machine learning models to network, application, user, and machine data to proactively hunt for unknown and hidden threats in our environment.<br>StockHolding expects a unified dashboard providing consolidated visibility into SOC operations, but not limited to incident status, SLA performance, reporting, and executive summaries; SIEM console access alone will not be sufficient.<br>The bidder may provide either a separate MIS/reporting tool or an integrated dashboard within the SIEM/MDR platform meeting these requirements. |
| 74 | 16 | Solution Implementation | n) The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days | Kindly clarify whether 180 days refers to online searchable storage or includes archived logs. Please confirm expected daily log volume in GB/day. | **Clarification:**<br>Online logs should be made available for 180 days<br>Offline logs within the platform should be made available for 2 years. Please refer EPS requirement |
| 75 | 17 | Log Collection | Logs from all the in-scope devices and additional devices integrated as part of contract period located at the geographically dispersed location should be collected. Bidder / Vendor should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with industry best practices. In case the | Secure log transfer and agent-based collection. Please confirm number of servers where agent-based collection is expected, to ensure accurate sizing. | **Clarification:**<br>Details shall be shared with winning bidder |
| 76 | | | | We will be leveraging Stockholding connectivity to transfer the logs through IPSec VPN, please confirm. | **Clarification:**<br>Yes. Connectivity shall be established via Secured Tunnel |
| 77 | 19 | e) Threat Hunting Section | Threat hunting advocates – "Don't wait for alerts to show up; hunt them". Output of advanced security analytics models run on the platform which is analyzed by a specialized hunting team and the data is queried further to detect threats that may have bypassed other security controls or use cases. This is security analytics in action: MSSP should apply data science and machine learning models to network, application, user, and machine data to proactively hunt for unknown and hidden threats in our environment. | Kindly clarify expected frequency of proactive threat hunting reports (monthly/quarterly). | **Clarification:**<br>It is expected to share the monthly report |
| 78 | 19 | d) Auto Containment Section | Service Provider's auto remediation to quickly contain threats by<br>enabling rules on firewall, NGFW, IPS, Proxy, EDR, WAF, Patch management, Routers or AD.<br>Service Provider will integrate our security devices and push rules based on predefined response playbooks, for us. Incase auto-remediation is not possible, Service<br>Provider to coordinate with StockHolding's SOC Team to manually apply the changes. | Rule push to firewall/IPS/EDR etc. Please confirm whether Service Provider will be granted rule-change privileges or actions will require prior written approval from StockHolding SOC team. | **Clarification:**<br>Yes. Access shall be provided wherever required and applicable. |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 79 | 19-20 | Security solutions to be integrated with SIEM Platform | List of integrated security systems | Kindly share estimated log source count per solution (WAF, NAC, Firewall, EDR, AD, etc.) for accurate EPS sizing. | **Clarification:**<br>Stockholding has already mentioned the EPS range, Please refer pg- 19-20 --> Security solutions to be integrated with SIEM Platform. Further Details will be shared with the winning Bidder to evaluate the estimated log size. |
| 80 | 28 | 6) SIEM – MDR Implementati on Go-Live | Go-Live of SIEM platform post integration with existing log collector and use cases (600 devices are on-boarded to the log collector) | 600 devices to be onboarded in Part A. Kindly confirm definition of 'device' (e.g., individual server, VM, network appliance, log source). | **Clarification:**<br>Device can be a security device, VM, physical server, router, switch, etc. |
| 81 | 28 | 7) Remaining Device Onboarding GoLive | On-boarding of all remaining devices in scope | Remaining devices onboarding in 24 weeks. Please confirm total number of devices expected during entire contract period. | **Clarification:**<br>Approximately 1200 |
| 82 | 22 | Log Archival Section | Logs collected from all the devices should be stored in a non-tamperable format on the archival device in a compressed form. Collection of Logs and storage should comply with the Regulatory requirement and should maintain a chain of custody to provide the same in the court of law, in case the need arises. For correlation and report generation purpose, past 180 days log data should be available online. Service Provider will ensure that retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols. | Non-tamperable storage; open standard retrieval. Kindly clarify whether WORM-compliant storage is mandatory. | **Clarification:**<br>It should be non-tamperable and immutable |
| 83 | 26 | Time to Notify customer on a High Severity Incident post first level investigation | The MDR Team will analyse alerts and create an Incident ticket for alerts that need action from the SOC Team. Such incidents will also be notified via email. The SLA for notifying High Severity Incident Tickets post first level investigation is 30 minutes after the alert is detected in MDR platform. | 30 minutes notification. Please confirm whether SLA clock starts from alert generation or from alert validation by L1 analyst. | **Clarification:**<br>SLA starts from the alert notification from the source system. |
| 84 | 27 | Time to respond to the customer for Log data requests | The SLA for retrieving log files for up to last 30 days is 6 hours from time of request SLA will be measured using formula: (Number of Log requests responded within 6 hours in a quarter) x 100 /<br>(Number of Log requests) | 6 hours retrieval for last 30 days. Kindly clarify expected maximum log size per retrieval request. | **Clarification:**<br>The log size are dynamic and cannot be predicted, Based on the EPS and Device count bidder has to analyze and make provision for such requirement |
| 85 | 28 | SIEM – MDR Implementati on Go-Live | Go-Live of SIEM platform post integration with existing log collector and use cases (600 devices are on-boarded to the log collector) | Kindly confirm whether dependencies (network readiness, access approvals) are excluded from SLA calculation. | **Clarification:**<br>Yes. SLA's exclude stockholding dependencies. |
| 86 | 24 | Transition Section | StockHolding has considered a transition period of 3 months from existing Service Provider to new Service Provider for smooth transfer of the SOC services handover process. | Kindly clarify whether existing Service Provider will provide full knowledge transfer including use cases and playbooks. | **Clarification:**<br>Stockholding will showcase the existing use cases with the winning Bidder |
| 87 | 13 | Technical Bid Evaluation<br>Point No.3 | Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India | We have successfully executed multiple end-to-end SIEM implementation and SOC enablement projects across highly regulated sectors in India, including Power Sector PSUs, Healthcare, and PFRDA, which share identical security, compliance, and operational maturity requirements as critical BFSI environments (e.g., real-time monitoring, regulatory reporting, incident management, and threat detection). These engagements involved comprehensive deployment of SIEM platforms, configuration of correlation and analytics rules, integration with distributed infrastructure, and establishment of 24×7 Security Operations Center (SOC) functions, strengthening the client's overall cybersecurity posture and aligning with stringent audit and compliance mandates. | No change |
| 88 | 13 | Technical Bid Evaluation<br>Point No.4 | OEM solution must be positioned in the respective Leader's quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave reports for proposed SIEM Solution | The RFP clause mandates that the proposed OEM solution must be positioned in the Leader's quadrant/category of the latest IDC MarketScape / Gartner Magic Quadrant / Forrester Wave for SIEM.<br>In this regard, we respectfully submit that the Authority has emphasized adoption of the "Make in India" model and promotion of indigenous cybersecurity solutions. Our proposed SIEM OEM is an Indian cybersecurity organization aligned with the Government of India's Make in India and Digital India initiatives, with proven large-scale deployments across critical and regulated sectors including PSUs, Power, Healthcare, and financial regulatory bodies such as PFRDA.<br>While global analyst reports such as Gartner, IDC, or Forrester typically evaluate large multinational vendors, emerging and indigenous Indian OEMs may not always be featured despite having strong technical capabilities, compliance alignment (RBI, CERT-In, MeitY), and successful production-grade deployments in mission-critical environments. | No change<br>This is not a mandatory requirement for participation but a part of technical scoring criteria. |
| 89 | 38 | Solution Implementation<br>Point No.2 | SIEM solution shall be implemented in Service Provider's Data Centre or Cloud based. The Service Provider shall ensure that Data Centre / Cloud Service shall be hosted in India and in no circumstances data shall not move out of India during the entire contract duration. | Kindly confirm whether MeitY empanelled cloud providers are mandatory. | **Clarification:**<br>Yes. Cloud provider should be MeitY compliant provided bidder is using 3rd party cloud service providers for hosting the SIEM platform. |
| 90 | 38 | Solution Implementation<br>Point No.8 | Build custom interfaces/ Connector for Applications. To begin with StockHolding will start with integration of critical applications. Service Provider can be asked for integrating further more applications if found critical and required by StockHolding | Kindly confirm whether there is a defined cap on the number of future application integrations included within the contract scope. | **Clarification:**<br>Existing custom build applications - None<br>Future expected custom build application - Cannot be decided today. To be built as and when required |
| 91 | 38 | Solution Implementation<br>Point No.9 | While, it is expected that connectors for all the standard applications and devices will be readily available with the Service Provider and connector for mostly in-house/custom built applications will need to be developed. Service Provider is be expected to develop connector for the custom built applications specifically developed for StockHolding. | Kindly confirm expected integration approach for custom applications (Syslog/API/Agent/DB connectors) and approximate count of in-house applications. | **Clarification:**<br>Existing custom build applications - None<br>At this moment Stockholding wants to integrate the Infra Devices for the said requirement |
| 92 | 38 | Solution Implementation<br>Point No.10 | The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by StockHolding as per the SOW including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations i.e. DC, DR and branch offices, etc. | Kindly mention the type of connectivity present with the DC DR or Branch offices | **Clarification:**<br>Details will be shared with the winning Bidder |
| 93 | 39 | Solution Implementation<br>Point No.15 | The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days | Kindly mention the amount of logs produced per day (GB/day)<br>& storage beyond 180 days? Do you need searchable logs after 180 days or shall it move to archive? | **Clarification:**<br>The log size are dynamic and cannot be predicted, Based on the EPS and Device count bidder has to analyze and make provision for such requirement<br>Searchable option should be available for logs beyond 180 days as well. |
| 94 | 16 | Solution Implementation | f) Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool. | What is the total number of User / group to be factored for ITSM sizing ? | **Clarification:**<br>This requirement is only for SIEM MDR Solution with alerts and tickets to be generated from this platform. ITSM is not part of this Solution requirement. Infuture Stockholding will need integration support from the winning Bidder for ITSM Solution deployed by Stockholding. |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 95 | 16 | Solution Implementation | m) Bidder will also supply all the necessary hardware, software and supporting accessories etc. for integration of the components supplied for CSOC. REC will supply only the Rack space, power and network points. | We understand that its managed service contract where bidder will own the license?<br>There is no supply of hardware or license to you, please confirm.<br>We request Stockholding to provide the required VMs for log collection at their DC, DR & NDR locations. | **Clarification:**<br>The required infrastructure example VM server will be made available by Stockholding for log collection purpose. |
| 96 | | | | Bidder to supply hardware for CSOC. Please clarify whether this includes log collectors, storage appliances, and HA components. | **Clarification:**<br>The required infrastructure example VM server will be made available by Stockholding for log collection purpose. |
| 97 | | | | Does Stockholding will provide the required underlying VM Infra for deployment or Log Collector | **Clarification:**<br>The required infrastructure example VM server will be made available by Stockholding for log collection purpose. |
| 98 | 16 | Solution Implementation | n) The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days | What is online and offline retention requirements for 180 days ?<br>Can we consider 90 days online and 90 days offline ? | **Clarification:**<br>Minimum 180 days is required for online. This should be seamless and searchable. Separate ticket request should not be raised by stockholding to get/check the logs.<br><br>For logs beyond beyond 180 days and upto 2 years searchable option should be available without raising any ticket |
| 99 | 21 | Logging of Critical Devices | b) he logs will be reviewed by StockHolding officials on quarterly and half yearly basis and same has to be ensured by Service Provider. | Does it mean that logs needs to be stored at Stockholding premises ?<br>In an MSSP setup, we wont be able to provide access to Stockholding for log reviews. | **Clarification:**<br>Online logs should be made available for 180 days<br>Offline logs within the platform should be made available for 2 years. Please refer EPS requirement |
| 100 | 24 | Transition Management (On-boarding and During-Exit) | Service Provider has to develop a detailed transition plan covering at least the following key areas:a) Transition Schedules, Tasks and Activities<br>b) Plan for Service Transition to new Service Provider<br>c) Transition activities like Service On-boarding, etc.<br>d) Operations and Support<br>e) Other Resources if any<br>f) Relationships to StockHolding's other Teams / Projects<br>g) Management Controls<br>h) Reporting Procedures<br>i) Risks and Contingencies- Key Risks, issues, dependencies and mitigation plans.<br>j) Transition Impact Statement and assessment<br>k) Review Process<br>l) Configuration Control<br>m) Plan Approval<br>n) Describe tools, methodologies and capabilities of the teams deployed for transition. | What is your current SIEM platform and its deployment model ? | **Clarification:**<br>Custom built platfrom from ATOS |
| 101 | | | | What is your average and peak EPS observed per month ? | **Clarification:**<br>We have given indicative minimum 2000 EPS and scalable to 5000 EPS along with the total volume of the Devices (1200) to be onboarded. Any usage increase upto 5000 EPS has to be borne by the bidder without any additional cost to StockHolding |
| 102 | | | | what is the number of log sources integrated with SIEM ? | **Clarification:**<br>We have given indicative minimum 2000 EPS and scalable to 5000 EPS along with the total volume of the Devices (1200) to be onboarded. Any usage increase upto 5000 EPS has to be borne by the bidder without any additional cost to StockHolding |
| 103 | | | | What is total number of use cases configured on SIEM ? | **Clarification:**<br>Details shall be shared with winning bidder |
| 104 | | | | What is your average number of monthly SOC incidents ?<br>Please provide bifurcation of P1, P2 & P3 incidents. | **Clarification:**<br>Details shall be shared with winning bidder |
| 105 | | | | What is the threat intel feed available ? | **Clarification:**<br>Custom built platfrom from ATOS |
| 106 | | | | What is your SOAR platform ? | **Clarification:**<br>No SOAR platform in place |
| 107 | | | | How many automation playbooks are configured ? | **Clarification:**<br>Details shall be shared with winning bidder |
| 108 | | | | what is your ITSM platform ? | **Clarification:**<br>ITSM is not part of this Solution requirement. In future Stockholding will need integration support from the winning Bidder for ITSM Solution deployed by Stockholding. |
| 109 | | | | What is your current L1, L2, L3, SME resource count in SOC ? | **Clarification:**<br>Details shall be shared with winning bidder |
| 110 | | | | Can you provide your asset inventory ? | **Clarification:**<br>Details shall be shared with winning bidder |
| 111 | 16 | Solution Implementation – Incident Management and Ticketing Tool | f) Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool. | The RFP states that the SIEM solution should have an inbuilt incident management and ticketing tool or support seamless integration with a separate ticketing tool, with capability to populate relevant incident details from SIEM alerts into the ticketing system.<br><br>Kindly clarify:<br>1. Whether the bidder is expected to provide a new ITSM / ticketing tool as part of the SIEM–MDR solution, or<br>2. Whether integration with StockHolding's existing ITSM platform is acceptable and preferred.<br>3. The current ITSM / ticketing tool used by StockHolding. | **Clarification:**<br>This requirement is only for SIEM MDR Solution with alerts and tickets to be generated from this platform. ITSM is not part of this Solution requirement. In future Stockholding will need integration support from the winning Bidder for ITSM Solution deployed by Stockholding. |
| 112 | 16 | Solution Implementation | n) The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days | Storage requirement mentions minimum 180 days. Please clarify whether 180 days refers to hot/online logs only and whether any cold/archive retention (e.g., 1 year / 2 years) is expected. | **Clarification:**<br>Online logs should be made available for 180 days<br>Offline logs within the platform should be made available for 2 years. Please refer EPS requirement |
| 113 | | | | Can Stockholding change in log Storage from 180Days to 90Days | **Clarification:**<br>No Change |
| 114 | | | | This 180Days of logs required RAW logs are the parsed logs | **Clarification:**<br>Online logs should be made available for 180 days<br>Offline logs within the platform should be made available for 2 years<br><br>All the logs should be made available in RAW log format |
| 115 | 23 | Development of Connectors for customized applications/ devices | While it is expected that connectors for all the standard applications and devices will be readily available in the collector and Log management devices, connector for mostly inhouse/custom built applications will need to be developed. | Please share the number of in-house application to estimate the number of custom connector that might require | **Clarification:**<br>Existing custom build applications - None<br>Future expected custom build application - Cannot be decided today. To be built as and when required |
| 116 | 15 | Solution Implementation | EDR/XDR tool | Please confirm whether MSSP is responsible for policy design for EDR/XDR | **Clarification:**<br>No, however if there are any suggestions for improvement same can be discussed |
| 117 | 15 | Solution Implementation | SOAR tool | Who will be responsible for author, maintain, and own SOAR playbooks/use-cases, is SOAR as well considered or will be considered lateron in scope of work | **Clarification:**<br>No SOAR platform in place |
| 118 | 15 & 44 | Solution Implementation | DR/HA for SIEM tool | Please confirm whether MSSP is responsible for building DR - Disaster Recovery or HA - High Availability setup for SIEM implementation, as on page 44 it is mentioned for only logs and not the complete SIEM setup to run on HA/DR if the primary SIEM goes down, as it may impact live monitoring, (The Service Provider is required to maintain the syslog of<br>the devices installed at DC, DR and NDR locations for a<br>period of 180 days). Please elaborate and provide more details on the same. | **Clarification:**<br>Please refer pg- 26,27,28 for the SLA and Penalty and Deploy the SIEM-MDR Solution accordingly |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 119 | 36 | General | General | Is there any specific years of experienced resources required (for L1, L2, L3, Lead, etc) as only mentioned for "The bidder should have minimum three (3) resources certified/ trained on the proposed SIEM solution". | **No change** |
| 120 | 17 | Log Correlation | Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by the bidder on regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents. | "In any case false negatives will not be permitted." - Request to rephrase as "Best-effort reduction of false negatives with continuous tuning; any material misses to be RCA'd with corrective actions and use-case updates within agreed timelines." | **Clarification:**<br>No Change |
| 121 | General | General | General | In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.<br>Please refer to Government of India office Memorandum ( F 8/78/2023) on participation of demerged entity in public procurement process. | Bidder to submit relevant supporting documents as per terms and conditions of the RFP |
| 122 | 47 | ANNEXURE - 4 - Commercial Price Bid Format | List of Applications mentioned in the RFP are as of present today and might increase in the future. Any additional applications to be on-boarded shall be at zero cost to Stockholding. | In case of efforts required to onboard additional applications, for eg. Custom development of adapters etc involves cost and should be chargeable. Please confirm the service provider will have option to charge customer for additional scope which is not defined during this bid process? | **Clarification:**<br>This has to be built in. No separate rate card or additional scope charges will be paid |
| 123 | 26 | Service Level Agreement (SLA) and Penalty | LD Penalty: 1% of One time Implementation Cost (Part A) for every week's delay beyond the SLA time period. | Request to cap LD penalty at 5% of One-time charges | No change |
| 124 | 26 | Service Level Agreement (SLA) and Penalty | Day 2 SLA Penalty | Request to cap SLA penalty at 5% of Monthly charges payable | No change |
| 125 | General | General | General | Purchase Preference to MSE OEMs available up to price within L1+X% (15%). Request to relax this clause, suggestion is to evaluate without any purchase preference for MSE | No Change |
| 126 | General | General | General | Kindly confirm if Bidder along with its affiliate including its subsidiaries can participate and can submit credentials of the parent company. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary. | Bidder to submit relevant supporting documents as per terms and conditions of the RFP |
| 127 | General | General | General | Also, please allow the bidder to use the documents from parent company for qualification on Eligibility, experience, references, etc. | Bidder to submit relevant supporting documents as per terms and conditions of the RFP |
| 128 | 26 | Service Level Agreement (SLA) and Penalty | 1. Service Provider will provide access to MDR platform and associated notification systems with the exception of "Scheduled Platform Maintenance" | Proposed solution is built on an MSSP multi-tenant platform. We request that this clause be relaxed or revised to specify access to the customer portal instead. The customer will continue to have access to our service portal, where they can view all relevant information and receive necessary notifications. | **Clarification:**<br>Access to be provided to Stockholding on the Stockholding tenancy of the SIEM platform. |
| 129 | 16 | Solution Implementation | c) Implement the SIEM tool to collect logs from the identified devices / applications / databases etc. | Can you share the list of application & names ,This will help  understand how many parser,use case need to be develpoed | **Clarification:**<br>Details shall be shared with winning bidder |
| 130 | 16 | Solution Implementation | f) Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool. | Does Stockholding need SIEM integration with your tickting tool | **Clarification:**<br>This requirement is only for SIEM MDR Solution with alerts and tickets to be generated from this platform. ITSM is not part of this Solution requirement. In future Stockholding will need integration support from the winning Bidder for ITSM Solution deployed by Stockholding. |
| 131 | 16 | Solution Implementation | g) Build custom interfaces/ Connector for Applications. To begin with StockHolding will start with integration of critical applications. Service Provider can be asked for integrating further more applications if found critical and required by StockHolding | Will this futher application integration cost need to included in current proposal, Or Should biider provide the rate card for it | **Clarification:**<br>This has to be built in. No separate rate card |
| 132 | 23 | Integration of devices in Managed detection | g) Forensics to identify the origin of threats, mitigation thereof, initiation of measures to prevent recurrence. | Does bidder need to consider forensics as part of solution | **Clarification:**<br>Detailed Forensics is out of Scope. |
| 133 | 42 | Security solutions to be integrated with SIEM Platform | Brand Protection and Monitoring Logs, Website Monitoring Service against Defacement | Name of Brand Monitoring solution & does it support SIEM Integration | **Clarification:**<br>Details shall be shared with winning bidder |
| 134 | 42 | Security solutions to be integrated with SIEM Platform | Anti-Phishing Service Logs | Make & model & Count | **Clarification:**<br>Details shall be shared with winning bidder |
| 135 | 42 | Security solutions to be integrated with SIEM Platform | Packet Analysis | Which OEM Application is used for Packet Analysis | **Clarification:**<br>Details shall be shared with winning bidder |
| 136 | 42 | Security solutions to be integrated with SIEM Platform | Database and Compute Server Audit Logs | Total Count of Database & OEMs | **Clarification:**<br>Details shall be shared with winning bidder |
| 137 | 42 | Security solutions to be integrated with SIEM Platform | End Point Protection | Make & model & Count | **Clarification:**<br>Details shall be shared with winning bidder |
| 138 | 42 | Security solutions to be integrated with SIEM Platform | Active Directory Logs | Number of AD Servers | **Clarification:**<br>Details shall be shared with winning bidder |
| 139 | 42 | Security solutions to be integrated with SIEM Platform | Oracle NSG and VMWare NSX Logs | Make & model & Count | **Clarification:**<br>Details shall be shared with winning bidder |
| 140 | 42 | Security solutions to be integrated with SIEM Platform | Application Delivery Controller (ADC) Logs | Is this application hosted on-prem or cloud | **Clarification:**<br>ADC is on-prem within Load Balancer. |
| 141 | 42 | Security solutions to be integrated with SIEM Platform | PIM, PAM, | Consider Arcon application, Just consider the number of licenes in total of User & devices | **Clarification:**<br>Query is not clear |
| 142 | 42 | Security solutions to be integrated with SIEM Platform | Routers and Switches | Make & model & Count, Count of devies | **Clarification:**<br>Details shall be shared with winning bidder |
| 143 | 42 | Security solutions to be integrated with SIEM Platform | Proxy | Please confim the Proxy is from Force Point & How many User licenses ,& Hosted On-prem or cloud | **Clarification:**<br>Forcepoint proxy on premise |
| 144 | 42 | Security solutions to be integrated with SIEM Platform | Oracle Exadata and PCA | Make & model & Count | **Clarification:**<br>1 Box - Exadata X10M and 1 Box - PCA X10M |
| 145 | 42 | Security solutions to be integrated with SIEM Platform | VMware Private Cloud | Number of VM Windows & Linux & other OS | **Clarification:**<br>Details shall be shared with winning bidder |
| 146 | 42 | Security solutions to be integrated with SIEM Platform | CISCO ISE Logs | Number of user Licesnes | **Clarification:**<br>Details shall be shared with winning bidder |
| 147 | 31 | Right to alter RFP | a. StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids.<br>b. StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that StockHolding's decision in this regard will be final and binding on all bidders. | **Request the addition of following in the clause**: "Any alteration in terms and conditions shall be notified to the bidders in advance." | No change |

| Sr. No. | Page No. | RFP Clause | Clause Description | Query | StockHolding Remarks |
|---|---|---|---|---|---|
| 148 |  | Clause 19 GeM GT&C Buyer Added Bid Specific ATC<br>Gem General Terms and Conditions | Termination | Request to amend the clause as follows: “Except if otherwise specified in a Service Schedule or COF, either Party may terminate an individual Service at the end of its Initial Term or Service Term (whichever is applicable), by providing no less than ninety (90) days advance written notice to the other Party subject to StockHolding’s payment to Bidder of any outstanding Service Fees, including connection and/or disconnection charges, for the Service(s) so terminated.<br>(b) Either Party (the “Non-Defaulting Party”) may terminate a Service upon written notice of termination to the other Party (“Defaulting Party”) if (i) the Defaulting Party breaches a material provision of this Agreement or the applicable COF and the Defaulting Party fails to cure such breach within thirty (30) days after receipt of written notice of breach from the Non-Defaulting Party; or (ii) any bankruptcy, insolvency, administration, liquidation, receivership or winding up proceeding is commenced in respect of the Defaulting Party.<br>(c) Termination of one Service will not affect the Parties rights and obligations with regard to other Services ordered under this Agreement.” | No change |