

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
1	33. Annexure – VII, Sl. No 8	34	Solution should be compatible with cloud architecture (preferably cloud native) and capable enough to integrate all the target state infrastructure, Active directory, security and endpoints components. The solution should be capable to integrate with UEBA & SOAR solutions/ modules as and when needed by the Company without any additional cost.	Target State infrastructure – here it is asked for end points components needs to be integrate with UEBA and SOAR, - are you looking for Separate UEBA Solution, if so, would like to know the no of end points you have or looking for SIEM should have capability of the same to get UEBA.	Refer the amendment.
2	Annexure – VII, Sl. No 18	18	The solution should be able to integrate with incident management and ITSM tool for incident logging and ticketing	Please let us know what is the ITSM Tool you have, or confirm if SOC Provider can use their ITSM tool	Refer the amendment.
3	Annexure – VII, Sl. No 36	36	The Proposed solution should Automatically enrich all incoming events with minimum following information. These fields should be customizable to add/modify/delete as desired by administrator): - Asset Owner, BIA & CIA - Geo-location of IP - Reputation of IP, URL, File etc. - Hash of files - Historical security incidents on same IP/same host/same user/same vulnerability/same location etc. - Threat Intelligence: (IoAs), (IoCs), and adversary's TTPs - Vulnerability information of asset. - Application Security review data. - Zone classification - Risk score of assets Bidder to Provide details on what additional enrichment options can be provided by the solution. Support for STIX-TAXII and API integration should be provided to automatically ingest IoCs in SIEM from threat intelligence vendors.	Are you looking for Risk Score for the environment?	Yes
4	Annexure – VII, Sl. No 69	69	Vendor shall build the capacity of the SIEM solution that can handle the log retention as mentioned below: · Six months – Online · Three Years – Offline Vendor should provide backup copy of logs to canfin for record and reconciliation in specified media device.	Does the 3 years Offline storage will be provided by Canfin.	Vendor should provide and manage the storage for online and offline storage. The storage should be in India only.
5	Annexure – VII, Sl. No 78	78	IT Forensic services for root cause of incident and investigations as and when required by CFHL.	Is Canfin looking for Forensic Analysis as a part of tool	Refer the amendment.
6	12.Payment Terms	15	Payment shall be released Quarterly in arrears from the date of Go live based on the devices onboarded into the solution. The devices may be onboarded in phases at discretion of the Company.	Kindly consider payment terms as Quarterly in advance. If the devices are going to be onboarded on a phased manner go live will be challenge. Hence your statement is contradictory.	Refer the amendment.
7	12.Payment Terms	15	Price shall remain fixed up to an additional of 5 assets for a period of 3 years from the date of acceptance of Purchase Order. There shall be no increase in price for any reason whatsoever and therefore no request for any escalation of the cost / price shall be entertained.	We can confirm based on the discussion with OEM	Comply with RFP terms & conditions.
8	12.Payment Terms	16	Payment for onsite resource will be released Quarterly in arrears.	Kindly consider payment terms as Monthly in arrears for onsite resource.	Comply with RFP terms & conditions.
9	29. ANNEXURE -III: PRE-QUALIFICATION CRITERIA	28	S.No. 1 The bidder must have GST registration number and should be a registered company in India as per Companies Act 1956 / 2013 and must be in existence for the last 5 years on the date of RFP	Request to kindly modify clause as below: The bidder must have GST registration number and should be a registered company in India as per Companies Act 1956 / 2013/ LLP Act 2008 and must be in existence for the last 5 years on the date of RFP	Refer the amendment.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
10	29. ANNEXURE -III: PRE-QUALIFICATION CRITERIA	28	S.No. 2 Turnover & profitability The bidder should have reported minimum annual turnover of Rs. 50 crores and should have reported profits	Request to kindly modify clause as below: Turnover & profitability The bidder should have reported average annual turnover of Rs. 50 crores and should have reported profits	Comply with RFP terms & conditions.
11	29. ANNEXURE -III: PRE-QUALIFICATION CRITERIA	28	S.No. 3 Bidders shall be the Original Equipment Manufacturers (OEM) of Solution (OR) An authorized dealer/Distributor	Request to kindly modify clause as below: Bidders shall be the Original Equipment Manufacturers (OEM) of Solution (OR) An authorized dealer/ Distributor (OR) Should have been in the business of providing SIEM services of any of the OEM	Comply with RFP terms & conditions.
12	29. ANNEXURE -III: PRE-QUALIFICATION CRITERIA	28	S.No. 4 The bidder should provide atleast one proof of having Implementation, Manage & Maintaining SIEM Solution in any Scheduled Commercial banks/NBFC/HFC/ Banks/Other companies in India during the immediate preceding for three Financial years (FY23-24, FY 22-23, FY 21-22)	Request to kindly modify clause as below: The bidder should provide atleast one proof of having Implementation, Manage & Maintaining SIEM Solution in any Central Government / State Government/ PSU/ BFSI / Large Enterprises /Scheduled Commercial banks/ NBFC/ HFC/ Banks/ Other companies in India/ Global during the immediate preceding for three Financial years (FY23-24, FY 22-23, FY 21-22)	Comply with RFP terms & conditions.
13	21. Evaluation Criterion	19	S.No. 1.A Bidder credentials, Experience and past performance on similar contracts for implementation of managed SIEM Solution to Banking/Financial/ Government departments/ PSU organization / Housing Finance/other companies	Request to kindly modify clause as below: Bidder credentials, Experience and past performance on similar contracts for implementation of managed SIEM Solution to Large Enterprises / Banking/ Financial/ Government departments/ PSU organizations / Housing Finance/other companies	Comply with RFP terms & conditions.
14	21. Evaluation Criterion	19	S.No. 1.B Past Experience of projects for managed SIEM services in BFSI sector organization/NBFC/ Scheduled Commercial Banks/ Government departments/ PSU organization/Housing Finance Company in India.	Request to kindly modify clause as below: Past Experience of projects for managed SIEM services in BFSI sector organization/NBFC/ Scheduled Commercial Banks/ Government departments/ PSU organization/Housing Finance Company/ Large Enterprises in India/ Global .	Comply with RFP terms & conditions.
15	21. Evaluation Criterion	19	S.No. 2 Quality of resources resumes to be shared with CFHL, [higher weightage for certified CCNA-Security, CEH, ITIL, CEIH, OSCP, CISSP, CISA, CPT) resources].	Request to kindly modify clause as below: Quality of resources resumes to be shared with CFHL, [higher weightage for certified CCNA-Security, CEH, ITIL, CEIH, OSCP, CISSP, CISA, CPT, CISM,CCISO/ISO 27001) resources].	Refer the amendment.
16	Indemnity			Tenderer shall indemnify and hold harmless the bidder for all Losses incurred in connection with any third-party Claim, except to the extent finally judicially determined to have resulted primarily from the fraud or bad faith of such Bidder.	Comply with RFP terms & conditions.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
17	Limitation of the Bidder's Liability towards the Purchaser			Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive, or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services	Comply with RFP terms & conditions.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
18	Non-solicitation			Bidder shall not hire employees of Tenderer or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of Tenderer directly involved in this contract during the period of the contract and one year thereafter.	Comply with RFP terms & conditions.
19			Force Majeure	1) Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. 2) For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days. 3) Unless otherwise directed by Tenderer in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. 4) In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, Tenderer and the bidder shall hold consultations in an endeavour to find a solution.	Comply with RFP terms & conditions.
20	Termination for Convenience			1) In case of termination, Tenderer shall pay the bidder for all work-in progress, Services already performed, and expenses incurred by the bidder up to and including the effective date of the termination of this Agreement. 2) Tenderer shall be entitled to terminate/cancel the purchase order at any time for the balance order quantity which is within the delivery schedule with no liability on either side and without assigning any reason thereof. However, the purchase order for the quantity which has already been offered for inspection shall not be cancelled and supply of the same shall be availed in due course of time. 3) Bidder may terminate/cancel the contract by giving a written notice of 30 days in case: a) Its invoices are not paid on time b) If Tenderer fails to comply with the terms of agreement	Comply with RFP terms & conditions.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
21	Retention of copies			On payment of all bidder fees in connection with the Contract, Tenderer shall obtain a non-exclusive license to use within its internal business, subject to the other provisions of this Contract, any Deliverables or work product for the purpose for which the Deliverables or work product were supplied. bidder retains all rights in the Deliverables and work product, and in any software, materials, know-how and/or methodologies that bidder may use or develop in connection with the Contract.	Comply with RFP terms & conditions.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
22	Non-Exclusivity			It is agreed that the services are being rendered on a non-exclusive basis and the bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.	Comply with RFP terms & conditions.
23	Section 8.Scope of Work and Clause No. 8.16	9	On quarterly basis, Bidder should conduct CTF(Capture The Flag) events within the team to enhance the knowledge levels of support team and CFHL resources.	Define the scope of activities and no.of persons to be included from CFHL	CFHL IT and security team will be part of the training for knowledge enhancement.
24	Section 8.Scope of Work and Clause No. 8.20	9	Bidder shall Transfer the knowledge to the CFHL employees about day to day operations, system/backend level troubleshooting, dashboard, creation of basic and advanced rules & analytical models, creation and customization of reports & queries etc without any additional cost to the Company	This is a SOC training requirement, this can be done only in a Captive SOC Engagement. Request you to Remove this clause.	It is related to basic training like rule creation, report creation and generation, MIS reports etc. Comply with RFP terms & conditions.
25	Section 8.Scope of Work and Clause No. 8.21	9	Bidder shall perform digital forensic investigation on need basis with complete replay of attack including the ingress and egress of payload without any additional cost. Provide complete insight into threat vector and impact analysis with detailed RCA.	This feature is not a part of SIEM solution. We need to include a NDR tool for collection of flows and playback - is this a mandatory need?	Refer the amendment.
26	Section OnSite Resource & Support	10	The selected bidder has to deploy 1 Onsite Resource at Company's Registered Office, Bengaluru for dedicated/exclusive support for proposed SIEM solution during the contract period.	Kindly confirm the resource should be L1, L2, or L3 Resource.	Please refer RFP clause 8 for scope of work and eligibility criteria for Onsite Resource.
27	Section 9. CanFin Homes Critical Asset	11	Cloud Compute Components	Kindly confirm all the listed assets are hosted on Cloud and request you to confirm Cloud Host Service provider name.	Yes. Cloud service providers - Microsoft Azure, other public clouds.
28	Section I Implementation, Manage and Maintain of SIEM Solution and Project Time lines	15	Project Timelines: Bidder is requested to complete the entire managed SIEM solution within 2 Months from the date of acceptance of Purchase Order. • Entire services have to be provided by the Bidder.	As the requirement is SaaS, there would be only integration and baselining activity.	Comply with RFP terms & conditions.
29	Section 12 Payment Terms	15	Payment will be released within 60 days from submission of relevant documents as per RFP terms.	Request CanFin to accept 30 Days payment terms submission of relevant documents as per the RFP Terms	Refer the amendment.
30	Section 14 Extension of Contract	17	However even in case, the bidder is not interested to extend the Contract for a further period, bidder shall be essentially required to execute the work at least for next 12 months' period on the same rates and terms & conditions of the Contract. CFHL has right to alter (increase or decrease) the number of resources. CFHL has right to place repeat order to the bidder for any resources mentioned in the Contract. The contract shall be co-terminus with the Purchase orders issued unless extended by CFHL.	Request Canfin to Amend the clause as "However even in case, the bidder is not interested to extend the Contract for a further period, bidder shall be essentially required to execute the work at least for next 3 months' period on the same rates and terms & conditions of the Contract. CFHL has right to alter (increase or decrease) the number of resources. CFHL has right to place repeat order to the bidder for any resources mentioned in the Contract. The contract shall be co-terminus with the Purchase orders issued unless extended by CFHL.	Comply with RFP terms & conditions.
31	Section 29. ANNEXURE -III: PRE-QUALIFICATION CRITERIAand Clause No. 4	28	The bidder should provide atleast one proof of having Implementation, Manage & Maintaining SIEM Solution in any Scheduled Commercial banks/NBFC/HFC/Banks/Other companies in India during the immediate preceding for three Financial years (FY23-24, FY 22-23, FY 21-22)	The bidder should provide atleast one proof of having Implementation, Manage & Maintaining SIEM Solution/ <u>As a Managed SIEM Service Contract</u> in any Scheduled Commercial banks/NBFC/HFC/Banks/Other companies in India during the immediate preceding for three Financial years (FY23-24, FY 22-23, FY 21-22)	Comply with RFP terms & conditions.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
32	Section 33 ANNEXURE - VII: Functional / Technical requirements: Scope fo work and Clause No.41	37	Solution should have the capabilities of IOC blocking and domain filtering.	This not feature of SIEM. We need to include SOAR Module to achieve this. Is CanFin also want to include SOAR. If Yes, What are the Technologies you want to integrate.	Refer Sl No. 40.
33	Section 33 ANNEXURE - VII: Functional / Technical requirements: Scope fo work and Clause No.64	39	Ability for quick Counter Response by integrating with devices such as firewall and AD for blocking traffic or quarantine system.	To achieve this Canfin Homes need to have EDR at their Endpoints to Quarantine. To automate it we need to includeSOAR Module. Kindly confirm if We need to include the same.	Refer the amendment.
34	Section 33 ANNEXURE - VII: Functional / Technical requirements: Scope fo work and Clause No.67	40	Solution should provision reconstructing common file formats including word document, image, Web page.	is CDR solution an additional requirement?	Refer the amendment.
35	Section 33 ANNEXURE - VII: Functional / Technical requirements: Scope fo work and Clause No.69	40	Vendor should provide backup copy of logs to canfin for record and reconciliation in specified media device.	As per the RFP Canfin homes needs SaaS based solution. if SaaS , backup will not be a possibility. This is only possible in On-Prem Soluton	Backup of logs should be provided as and when required by CFHL. Comply with RFP terms & conditions.
36	Section 33 ANNEXURE - VII: Functional / Technical requirements: Scope fo work and Clause No.77	41	During the exit of the contract or services vendor should provide logs as per retention period from their end to without any Price.	To move the logs from SaaS based service incur Cost. Request CanFin to remove the clause.	Comply with RFP terms & conditions.
37	Section 11.Deliverables & Service Level Agreements (SLAs). And Clause SLAs for Solution Uptime	12	Solution Uptime	Request Canfin homes keep the Penalty cap maximum of 10% of the monthly cost.	Comply with RFP terms & conditions.
38	Section 29. ANNEXURE -III: PRE-QUALIFICATION CRITERIA	28	Additional Point	Additional point to be included in the RFQ "SaaS Platform should be in the latest Gartners Leaders Quadrant"	Comply with RFP terms & conditions.
39	ANNEXURE - VII: Functional / Technical requirements	34	1.The proposed solution should be a Software as a Service (SaaS) based model. The management of Data Center (DC) and Disaster Recovery (DR) shall be handled by the bidder. Bidder should ensure the guaranteed uptime during the contract period.	Do bidder have to manage the devices in DC DR or only SIEM	DC and DR related to SIEM solution shall be handled by the bidder.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
40	ANNEXURE - VII: Functional / Technical requirements	37	41.Solution should have the capabilities of IOC blocking and domain filtering.	We can block IOC using logic app, but support is limited products.	As many SIEM providers having the capability of blocking of IOCs. Comply with RFP terms & conditions.
41	ANNEXURE - VII: Functional / Technical requirements	40	67.Solution should provision reconstructing common file formats including word document, image, Web page.	Need more details on reconstructing common file formats.	Refer the amendment.
42	ANNEXURE - VII: Functional / Technical requirements	40	The Log management solution (Centralized) should be placed at Canfin data centers for collection of logs from different log sources. VMs and Storage for Log collector will be provided by canfin.	In SAAS based solution logs stored in cloud in India region, autoscaling can be done	Comply with RFP terms & conditions.
43	ANNEXURE - VII: Functional / Technical requirements	40	If connectivity between log collection agents and logger is down then the Log collector agents should store the logs of at least 3 days and send them once connectivity is established. Option to inform canfin official within an hour and effort to restore log collection /pushing should be documented in SLA.	In SAAS base solution very less connectivity issue, log will stop only if customer does some changes on device level	Comply with RFP terms & conditions.
44	ANNEXURE - VII: Functional / Technical requirements	41	78.IT Forensic services for root cause of incident and investigations as and when required by CFHL.	Forensic services expected on basic or advanced level.	Refer the amendment.
45	Clause 26- PBG	25	amount equivalent to 10% of Total Cost of Ownership	Please help revise the PBG to 3%. As per communication on BG value, only 3% is being charged even by Canara Bank on RFPs	Comply with RFP terms & conditions.
46	Clause 12- Payment terms	15	Payment will be released within 60 days from submission of relevant documents	Please help release the payment within 30 days from date of submission of documents and invoice. Credit period of 30 days	Comply with RFP terms & conditions.
47	SLA	12	SLA for solution uptime	Please help reduce the penalties. Please help revise from 5%, 8%, and 15% to 3%, 5% and 8%	Comply with RFP terms & conditions.
48	SLA	12	SLA for solution uptime	Please help reduce the penalties. Please help with penalty of INR 1000 per week as per day basis is exorbitantly high	Comply with RFP terms & conditions.
49	Penalties/LD	15	Liquidated Damages for non-delivery of Services:	Please help reduce the penalties. Please help with penalty of INR 1000 per week as per day basis is exorbitantly high	Comply with RFP terms & conditions.
50	33. ANNEXURE - VII: Functional / Technical requirements:	34	Solution should provision reconstructing common file formats including word document, image, Web page.	This clause is not clear. Please elaborate in detail.	Refer the amendment.
51	33. ANNEXURE - VII: Functional / Technical requirements:	41	IT Forensic services for root cause of incident and investigations as and when required by CFHL.	IR service is not component of SOC. It can be opt additional service which have commercials involved. Please confirm if we need to bundle both SOC and IR services in this RFP.	Refer the amendment.
52	8. Scope of Work	9	Bidder shall perform digital forensic investigation on need basis with complete replay of attack including the ingress and egress of payload without any additional cost. Provide complete insight into threat vector and impact analysis with detailed RCA.	Forensics is a separate activity and might involve specialized tools, skills and may take days / weeks to investigate incidents basis complexity. Kindly factor this as an additional exercise in a retainership / man-days model. We would recommend to consider 30 man days for 3 years.	Refer the amendment.
53	8. Scope of Work -> Onsite resource and support	10	Onsite Resource should be available at the premises of the Company during working Hours on all working days of the Company during the entire contract period.	We understand 2nd and 4th Saturday would be non-working at CanFin Homes.	1 and 2nd Saturday is non working at Can Fin Homes as of now.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
54	21. Evaluation Criterion:	19	2. Quality of resources resumes to be shared with CFHL, [higher weightage for certified CCNA-Security, CEH, ITIL, CEIH, OSCP, CISSP, CISA, CPT] resources].	CEH is not relevant for this engagement. Kindly include DFIR Certifications such as CHFI.	Refer the amendment.
55	29. ANNEXURE -III: PRE-QUALIFICATION CRITERIA	28	A bidder submitting the proposal in response to this RFP who shall implement, Install, Maintain & Manage SIEM Solution for Data Center, Disaster Recovery, Company website and its related security components of the Company and meeting the following Eligibility Criteria may respond.	We understand this is a SaaS model , and shared SIEM platform can be utilized to deliver managed services	Though offering solution is in SaaS model, proposed solution instances should be dedicated to CFHL.
56	Annexure-III: Pre Qualification Criteria	28	2.Turnover & profitability The bidder should have reported minimum annual turnover of Rs. 50 crores and should have reported profits. Certified copies of Audited Financial Statements or certificate from Auditors providing the Turn Over & net profit details in at least 2 out of last 3 financial years (FY 22-23, FY 21-22, FY 20-21).	Request you amend as following - The bidder should have reported average annual turnover of Rs. 50 crores and should have reported profit in last 3 financial years (FY 22-23, FY 21-22, FY 20-21). OR Request you to provide relaxation to MSME Bidders as per GOI guidelines.	Comply with RFP terms & conditions.
57	33. ANNEXURE - VII: Functional / Technical requirements:	34	Solution should be compatible with cloud architecture (preferably cloud native) and capable enough to integrate all the target state infrastructure, Active directory, security and endpoints components. The solution should be capable to integrate with UEBA & SOAR solutions/ modules as and when needed by the Company without any additional cost.	We understand proposed solution should be able to integrate with SOAR / UEBA platform in future as and when CanFin Homes decides to procure the same. For now, UEBA / SOAR supply, installation is out of scope of bidder.	Yes
58	9		Bidder shall perform digital forensic investigation on need basis with complete replay of attack including the ingress and egress of payload without any additional cost. Provide complete insight into threat vector and impact analysis with detailed RCA.	To meet this requirement we need wiredata. And hence organization should provide authorization to collect wire data and compute resource. And also approval to use open source tools for analyzing the wire data.	The same will be provided to the successful Bidder. Refer the amendment.
59	11		Canfin Homes Critical Assets	The details of make and model of all the assests are required for parser availability check.	The same will be provided to the successful Bidder.
60	36		The solution must detect internal denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (but not limited to) ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc identify the presence of botnets in the network, identify DNS spoofing attack etc. and detect long-lived connections that may be associated with data-exfiltration.	This use case may require flow data, hope organization will provide the flow data as required.	The same will be provided to the successful Bidder.
61	40		Solution should provision reconstructing common file formats including word document, image, Web page.	Generaly This feature is part of CDR (Content DisArm and Reconstruction) solutions, please explain what is the expectation from SIEM here.	Refer the amendment.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
62	14		SLA for Any VAPT observation reported	The closure of vulnerabilities requires device management to be part of scope. We can follow with organizations IT Teams for closure. What is the expectation here.	Refer the amendment No. 3. The selected bidder shall conduct 1 instance of vulnerability Assessment & Penetration testing for the proposed solution in every year during the contract period and submit the relevant closure reports to CFHL as per the timelines stipulated. Also, CFHL may its discretion, conduct VAPT by internally or third party vendor. The bidder must comply with the vulnerabilities reported as per the time line stipulated.
63	8.29 - Other Requirements	10	Bidder should conduct security trainings for CFHL nominated persons once in six months without any additional cost to the Company. The training program would cover mutually agreed agenda on the e-security products and technologies.	Please provide a view of what trainings are expected from the bidder	Cluase is self explanatory. Bidder should conduct the training covering with proposed solution, relevant security products and technologies. However, training agenda will be mutual agreed.
64	33 - Annexure VII - Functional/Technical Requirements	34	Point no 5 - Bidder operations team should send alerts with details of mitigation steps to designated personnel of CFHL.	Please confirm if the bidder can leverage existing Service Desk? If yes, please let us know the Service desk that is operational at CFHL?	Refer the amendment No. 9.
65	33 - Annexure VII - Functional/Technical Requirements	34	Point no 6 - The Bidder should bring workflows and solutions that can automate majority of the incident response activities such as false positive management, managing white lists, escalation workflow, SLA management etc.	Please clarify what tool is expected here?	Refer the amendment No. 9.
66	33 - Annexure VII - Functional/Technical Requirements	35	Point 16 - The solution must have an incident review framework for incident management. Incident review framework to facilitate incident tracking, investigation, pivoting and closure. The solution must allow tracking of incidents from correlation rule through investigation of that event to closure with respect to the incident reporting framework. Theproposed solution should provide incident management tool.	Please clarify the tool that is expected here	Refer the amendment No. 9.
67	33 - Annexure VII - Functional/Technical Requirements	40	Point 67 - Solution should provision reconstructing common file formats including word document, image, Web page	Please elaborate on this requirement	Refer the amendment.
68	33 - Annexure VII - Functional/Technical Requirements	34	Point 8 - Solution should be compatible with cloud architecture (preferablycloud native) and capable enough to integrate all the target state infrastructure, Active directory, security and endpoints components. The solution should be capable to integrate with UEBA & SOAR solutions/ modules as and when needed by the Company without anyadditional cost.	In Point no 16, incident management tool is asked for, where as here in Point 8 SOAR is defined as optional	Refer the amendment.
69	Payment Terms:	15	Payment shall be released Quarterly in arrears from the date of Go live based on the devices onboarded into the solution.	Payment shall be released Quarterly in Advance from the date of Go live based on the devices onboarded into the solution.	Refer the amendment.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
70	Payment Terms:	15	Payment will be released within 60 days from submission of relevant documents as per RFP terms.	Payment will be released within 30 days from the date of invoice	Refer the amendment.
71	Limitation of Liability	22	In no event shall Can Fin Homes Ltd. be liable for any proven consequential, special, punitive, incidental or indirect damages.	This has to be mutual.	Comply with RFP terms & conditions.
72	Indemnity	23	The Bidder shall, at its own expense, defend and indemnify the Company against all third party claims for infringement of patent, trademark, design or copyright arising from use of proposed product/products or any part thereof. Bidder will provide infringement remedies and indemnities for third party Products, on a pass-through basis. If the company is required to pay compensation to a third party resulting from such infringement, the Bidder shall be fully responsible to pay such compensation along with all costs, damages and attorney's fees and other expenses that a court may finally award, in the event of the matter being adjudicated by a court or that be included in a Bidder approved settlement. The Company will issue notice to the Bidder of any such claim without delay and provide reasonable assistance to the Bidder in disposal of such claim, and shall at no time admit to any liability for, or express any intent, to settle the claim. The Bidder shall also reimburse all incidental costs, which the Company may incur in this regard.	This needs to be mutually discussed	Comply with RFP terms & conditions.
73	Penalties / Liquidated Damages:	15	Liquidated Damages for non-delivery of Services: Failure to complete the activities within 2 Months from the date of acceptance of Purchase Order shall attract penalty at the rate of Rs. 1000/- (excl GST) per day. However, the total penalty under this clause shall be restricted to 10% (excl GST) of the project cost.	Liquidated Damages for non-delivery of Services: Failure to complete the activities within 2 Months from the date of acceptance of Purchase Order shall attract penalty at the rate of Rs. 1000/- (excl GST) per day. However, the total penalty under this clause shall be restricted to 3% (excl GST) of the project cost.	Comply with RFP terms & conditions.
74	Functional / Technical requirements	34		Kindly requesting you to provide the sizing details of the Events Per Seconds (EPS) for the proposed SIEM solution.	Solution should have the capability at both the EPS (Events Per Second) and device levels. Current engagement is looking for device based solution. Detailed device list is mentioned in the RFP clause 9.
75	Functional / Technical requirements	37	The solution should provide Detection of lateral movement based on suspicious connections with machines in the network.	This is not a feature of SIEM. This is a NBAD feature. Kindly request you to remove the clause.	Refer the amendment.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
76	Functional / Technical requirements	39	Solution should support quick response to an ongoing incident or serious threats with remote configuration of parameters in servers/desktops, Firewalls, AD (Active Directory), IPS, WAF, Network Switches & Routers · Automated Remediation for responding to commodity threats (e.g. recall malicious mails from inboxes, block bad IPs in Firewall, Disable bad users in Active Directory, etc.) Solution should support multiple configuration parameters to servers/desktops including removal/changes to services, users, registry keys, software, and browser plugins.	This is not a feature of SIEM. This is a SOAR feature. Kindly request you to let us know if we need to propose UEBA here else requesting you to remove the clause.	Refer the amendment.
77	Functional / Technical requirements	40	Solution should provision reconstructing common file formats including word document, image, Web page.	This is not a feature of SIEM. This is a NBAD/ NDR feature. Kindly request you to remove the clause.	Refer the amendment.
78	Cloud Services	Page No 11 & 12	Cloud Service Provider and Cloud-Based SIEM Solution	What cloud service provider is currently in use for these services (such as AWS, Azure, Google Cloud)? If applicable, which cloud-based SIEM solution is intended to be implemented?	Microsoft Azure and other public cloud
79	Infrastructure	Page No 11 & 12	Existence of Simple Notifications in the Infrastructure	Are there any simple notifications maintained in the infrastructure?	Resource Monitor is in place and managed by cloud service Provider for alers & notifications based on the compute resource usage.
80	Security Endpoint	Page No 11 & 12	Presence of Security Endpoint Antivirus	Do you maintain Security endpoint antivirus?	End Point Anti virus is in place. Currently we are not integrating with the proposed solution. In future, company may decides, the same should be integrated with the SIEM solution.
81	Scalability	Page No 11 & 12	Management of Scalability for VMs	How is scalability managed for these VMs in case of increased traffic or workload?	Management of Scalability for VMs is part of our Cloud Service provider scope.
82	Windows-based VMs	Page No 11 & 12	Databases and Applications on Windows-based VMs with MS SQL	What databases and applications are hosted on the Windows-based VMs with MS SQL?	The same will be provided to the successful Bidder.
83	Infrastructure Logs	Page No 11 & 12	Location of Logs in the Infrastructure	In the infrastructure logs, where are the logs being stored or maintained?	Bidder should specify the sizing of Log collector as per Annexure VIII. Intial Log collector will be at CFHL DC and further Bidder should manage the logs from log collector to proposed solution environment.
84	Data Center Firewall	Page No 11 & 12	Security Measures for Data Center Firewall	What security measures are implemented through the firewall for the data center?	The same will be provided to the successful Bidder.
85	Firewall Protocols	Page No 11 & 12	Firewall Protocols and Restrictions	Are there specific protocols or restrictions configured on the firewall?	The same will be provided to the successful Bidder.
86	WAF Security Policies	Page No 11 & 12	Security Policies for the WAF	Are there specific security policies in place for the WAF?	The same will be provided to the successful Bidder.
87	WAF Cyber Threat Protection	Page No 11 & 12	Configuration of Web Application Firewall Against Cyber Threats	How is the web application firewall configured to protect against potential cyber threats?	The same will be provided to the successful Bidder.
88	Linux-based VMs	Page No 11 & 12	Types of Applications and Databases on Linux-based VMs	What types of applications and databases are hosted on the Linux-based VMs?	The same will be provided to the successful Bidder.
89	Linux Security	Page No 11 & 12	Security Posture Maintenance for Linux-based Components	How is the security posture maintained for Linux-based components?	The same will be provided to the successful Bidder.
90	API Gateway APIs	Page No 11 & 12	APIs Managed Through the API Gateway	What APIs are managed through the API Gateway?	The same will be provided to the successful Bidder.

Response to Pre-Bid Queries - RFP (RFP-IT-362/2023-24 dated 24/02/2024) for Managed Service Provider (MSSP) for SIEM Solution for Can Fin Homes Ltd					
Sl.No	Section & Clause Reference No.	Page No.	RFP Text	Query	CFHL Response to Bidder Queries
91	API Traffic Monitoring	Page No 11 & 12	Monitoring of API Traffic	How is API traffic being monitored?	The same will be provided to the successful Bidder.
92	Disaster Recovery	Page No 11 & 12	Disaster Recovery Measures for Cloud Components	What disaster recovery measures are in place for the cloud components?	The same will be provided to the successful Bidder.
93	Integrated Functions	Page No 11 & 12	Integration of Functions with the AP	Are there integrated any functions with API?	The same will be provided to the successful Bidder.
94	Load Balancer	Page No 11 & 12	Utilization of Load Balancer for Traffic Distribution	How is the load balancer utilized to distribute traffic across servers?	The same will be provided to the successful Bidder.