Request for Proposal (RFP)

FOR SEQRITE EPP LICENSES RENEWAL & FOR SUPPLY, IMPLEMENTATION OF SEQRITE XDR LICENSES

SBI Capital Markets Ltd

Ref: RFP no. CO/IT/2488
Date: 29-May-2026

CO/IT/2488 **29-May-2026**

RFO FOR SEQRITE EPP LICENSES RENEWAL & FOR SUPPLY, IMPLEMENTATION OF SEQRITE XDR LICENSES

We intend to renew the existing Seqrite EPP Software subscription licenses along with supply and implementation of XDR Licenses, Quotations are invited from Authorized partners of Seqrite Enterprise Product partners for the period of one year.

Interested parties are requested to submit their Technical Bid and Commercial bid online on eTENDER.

Timelines:-

Pre-Bid Queries	**04-June-2026**
Submission of Technical & Commercial Bids	**10-June-2026 5.30 pm**

- All Bidders are requested to share their lowest commercial Bid.
- The lowest bidder shall be selected as L1 Bidder.
- SBICAPS reserves the right to conduct a Reverse Auction if the price is unreasonable.
- Further, sbicaps shall reserve the rights to negotiate with L1 Vendor
- The details of the bid and other terms and conditions are enclosed in Annexure-A.

Contact Email: procurement@sbicaps.com

Yours faithfully,

VP (IT)

Technical BID Comprises of various formats

S/N	Particulars	Details
1	Terms & Conditions of RFP	Annexure A
2	Eligibility Criteria	Annexure-B
3	Client References	Annexure-C
4	Bidders/OEM profile	Annexure-D
5	Technical Specifications	Annexure-E

ANNEXURE "A"

TERMS & CONDITIONS:

1. **Evaluation OF BID**

   The SBICAP committee shall evaluate the Technical Bids initially and the shortlisted technical bidders for Commercial Round**.**

2. **Terms & Conditions**

   - The prices quoted should be valid for 60 days.

3. **Termination**

   SBICAP shall reserves the rights to terminate the contract at the time of renewal in case product functionality and support is not satisfactory or for any other reason.

4. **PAYMENT**

   - 90% of the invoice value will be released on delivery, installation and acceptance of the equipment/software subscription.
   - 10% of the amount shall be payable against Bank Gurantee

   DELIVERY

   - New XDR Licenses and related configuration should be deployed withing 45 days from the date of Purchase Order. In the event of delayed delivery, penal charges of 2% of software subscription, amount per week or Rs 1500/- will be charged as penalty
   - The bidders shall include any delivery charges, freight charges, and in the cost while delivering the machines at different locations.

5. Scope of Work

- The successful bidder shall renew the existing EEP on prem licenses to EPP Cloud base licenses
- The OEM shall implement XDR solution for all SBICAPS users
- The proposed XDR software should be offered on Cloud and the same should resides in India.

1. Discovery-

Asset Assessment: Cataloging all targeted endpoints (Windows, Linux, macOS), cloud platforms (AWS/Azure/GCP), and network gateways

Network & Port Mapping: Mapping out required firewall exceptions, proxy requirements, and network access controls for secure outbound cloud connectivity.

Integrations Mapping: Defining API telemetry connections for active directories, email servers, and cloud resources.

2. **Core Platform & Tenant Setup**

Console Provisioning: Setting up the central cloud-native XDR management platform with complexed authentication process with enforcement of password reset along with OTP or Email based 2nd factor authentication.

Role-Based Access Control (RBAC): Granting specific security administrative, analyst, and read-only auditor permissions within the platform.

Global Exclusion Baseline: Factoring pre-existing internal application whitelists into the engine to filter out safe corporate software and avoid alert fatigue

3. **Endpoint Security & Sensor Deployment**

Universal Agent Rollout: Mass distributing unified agent software via automated platforms like Microsoft Active Directory GPO, System Center Configuration Manager (SCCM), or custom scripts.

Policy Standardization: Configuring base enforcement profiles including ransomware protection, behavioral shielding, and system asset control.

4. **Multi-Vector Telemetry Correlation**

Cloud & Identity Integration: Tying cloud audit logs directly to host actions to monitor for anomalies like unauthorized privilege jumps.

Playbook Engineering: Constructing initial automation playbooks to execute tasks like auto-quarantining a machine if a critical indicator of compromise (IOC) triggers

MITRE ATT&CK Mapping: Custom-tuning alert classification matrices so internal logs align properly against public threat hunting frameworks.

5. **Testing, Validation & Handoff**

Simulation Testing: Triggering simulated non-destructive EICAR file or safe script-based attacks to verify proper sensor recording, alerting, and auto-isolation.

As-Built Documentation: Transferring architectural infrastructure blueprints, customized playbook flowcharts, and client deployment summaries.

Knowledge Transfer: Hosting training sessions for the operational team covering fundamental platform navigation, manual alert hunting, and system log compilation.

Annual Support from Bidder and OEM-

Platform Maintenance & Hygiene

Agent Infrastructure Health: Performing recurring reviews as and when required by SBCIAOS to identify, troubleshoot, and fix broken sensors or machines out of sync.

Threat Query Refining: Adjusting detection rules, custom IOAs/IOCs, and search logic to keep pace with new global security vectors

Playbook Optimization: Periodically updating response playbooks to match evolving business processes and eliminate false alerts

Incident & Triage Assistance

Priority Escalation: Providing technical support for high-priority incidents where standard automated playbooks need manual escalation

Root-Cause Analysis (RCA): Collaborating with internal teams after a critical incident to figure out the entry point using the platform's visual attack timeline.

OEM Escalation Management: Managing technical communication with the software vendor's engineering group for underlying agent bugs or backend platform issues

Service Level Agreement (SLA) Framework

Severity	Definition	Response Time	Resolution Time
L1 Critical	Enterprise production outage or active, uncontrolled attack across network vectors	30 Mins (24/7 Support)	4 hours
L2 High	Major software failure on multiple critical assets; functional platform impairment.	2 Hours	12 Hours
L3 Medium	Local agent issues, localized software errors, or singular device disconnection, Security Audit High / Critical Severity points	4 hours	24 hours
L4 Low	Standard service requests, documentation queries, configuration updates, or whitelisting	8 hours	3 Business Days

- The Bidder shall provide L1 support onsite and remote as and when required by SBICAPS during contract period
- The OEM shall provide L2 & L3 support
- The Bidder & OEM shall enter a service contract with SBICAPS in standard format
- The vendor shall maintain, update SCD, SOP, Technical configuration/Architecture Documentations, versions for all the components on timely basis during contracted period.
- The service window for SBICAP is from 10.00 am to 6.45 pm from Monday to Friday. At emergency situations, the Vendor shall support on Public Holidays and Sundays. The OEM warranty for the product should cover for 24x7x365.
- SBICAPS shall conduct the VAPT, App Sec Audit on quarterly basis and OEM of the product should close all vulnerabilities as per the timeline mentioned below

Category	**Resolution Time**	**Penalty beyond resolution time**
High/Critical	24 hours	Rs. 2500 per day
Medium	48 hours	Rs. 500 per day
Low	72 hours	Rs. 250 per day

Annexure-B Eligibility Criteria

Sr. No.	Criteria	Compliance (Yes/No)	Remarks
1	The Bidder should be in a business of supply, delivery installation and maintenance of Security Solutions, End Point Protection including XDR for at least 3 years		Certificate of Incorporation Company PAN Card Copy GSTN certificate Copy CIN Number Copy
2	Bidder should be authorised supplier of Seqrite Products		Partnership Certificate from OEM
3	The Bidder should have yearly sales turnover of minimum Rs.1 crore and profitable during last three financial years and should be profitable (2022-23, 2023-24, 2024-2025)		Auditors Certificate with Turnover and profitability details
4	The Bidder ‘s Account should not have been declared as a Non-Performing Asset (NPA) in the Books of any bank or financial institution as on 31-Mar-2026.		Certificate from Bank/ Auditor
5	The bidder should have Active ISO 9001& ISO 27001 Certifications		Copies of Certificate
6	The OEM should have active ISO 9001 and ISO 27001 certification		Copies of Certificate
Bidders Profile and Client References			
7	Client References for Seqrite XDR and EPP		Annexure-D
8	Bidders Profile		Annexure-E

Note- Kindly upload the signed and stamped copy with evidence in a single file

ANNEXURE-C

Client References for the OEM / Partner

Customer References (at least 2) for proposed similar solution implemented solution in last 5 years for feedback purpose

S/N	**Customer Name (Reference 1)**	
1	Contact Person	
	Email Id	
	Mobile number	
2	Nature of Assignment	
3	Completion date	

S/N	**Customer Name (Reference 2)**	
1	Contact Person	
	Email Id	
	Mobile number	
2	Nature of Assignment	
3	Completion date	

Previous experience with SBI or its group companies

S/N	Customer Name	
1	Contact Person	
	Email Id	
	Mobile number	
2	Nature of Assignment	
3	Completion date	

ANNEXURE-D

BIDDERS and OEM PROFILE

1	Name of the Bidders Company				
2	Registered Office Address				
3	Year of Incorporation				
4	MD & CEO	Name			
		Telephone			
		Email			
		Designation			
5	Income tax no. GST (Attach Photostat / true copy of latest Income Tax Clearance Certificate)				
6	Company PAN				
7	Company CIN				
7	Financial Details (for last 3 years)*		2022-23	2023-24	2024-25
	a. Turnover (Rs. In lakhs)				
	b. Profit after Tax (Rs. In lakhs)				
	c. Revenue from AMC/FMS (Rs. In lakhs)				
8	Please mention partnership level with OEM		< Glod/Platinum etc.>		
9	Please confirm Bidders direct presence at Mumbai, New Delhi, Kolkata, and Chennai or presence through Channel partners/ASP at above location.		<Pls mention location names where presence is available>		
10	No. of Top 10 clients of OEM in India in BFSI/Public Sector segment, for Seqrite XDR		<Please give company Names>		
16	Total Employee strength of Bidder		<employee count>		
17	Total Employee Strength of OEM				
18	ISO Certificates ISO 9001 and ISO 27001 and other certificate details for OEM		<Pls enclose certificates>		

Declaration-- We hereby declare that all the information provided in this bidder profile submission is true and correct to the best of our knowledge and belief. We understand that any misrepresentation or incorrect information may lead to disqualification from the bidding process.

Annexure-E
Technical Specifications

EPP -Cloud

S/n	A. Antivirus Protection	Compliance Yes/NO
1	The Cloud Solution should reside in India and should have DR failover facility	Please brief
2	Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, network viruses, mixed threat attack from multiple entry points, and spyware.	
3	Provision to add whitelisted Wi-Fi SSID in Device Control Wi-Fi configuration. Endpoints will only be able to connect to whitelisted Wi-Fi SSID	
4	Must have capability to scan missing patches for non-Microsoft applications. ex: Adobe Reader, Adobe Acrobat, Adobe Flash Player, VLC, Java, Putty, Notepad++, 7-Zip, Mozilla Firefox and Mozilla Thunderbird.	
5	The proposed solution should have Virtual Patching functionality. This feature must provide a temporary shield against known vulnerabilities, effectively blocking attacks without modifying the underlying software code and providing valuable time until the official vendor patch can be deployed.	
6	Must have the capability to Control access to Personal or Corporate Google accounts.	
7	Must have the capability to Control access to YouTube videos based on their Category, Publisher etc.	
8	Must have ability to create Safelist for specific Applications to be allowed on the Endpoints. Solution should also provide the option to block some selected applications.	
9	The EPS (Endpoint Security) Console should offer enhanced control and visibility by allowing administrators to centrally manage the entire quarantine process on endpoints. Key management actions supported include Restore, Delete, Send to Lab, and Pull from Agent.	
10	The system must utilize macOS Safari, ensuring full support for integrated web security features when accessing websites over the QUIC protocol	
11	The system ensures comprehensive endpoint security through integrated Email and Web Protection. It performs real-time scanning of local inboxes to identify phishing and spam content. Additionally, it features a Category-Based Web Filtering engine that restricts access to malicious or unauthorized websites according to predefined security profiles.	

XDR Cloud

Incident Investigation		Compliance (Yes/No)
1	Incidents should be automatically generated by the backend module by correlating alerts when threat detection rules/policies is matched.	
2	Should have provision to display these incidents to the user in simple yet understandable manner.	
3	Must be able to see all Incidents in the environment in a timeline view	
4	Must see all alerts correlated to the incident in the incident details	
5	Must see all alerts associated to the incident in a timeline view	
6	Must be able to filter the Incidents based on the timeframe i.e. I should be able to filter alerts generated in last 24 hrs, last 7 days, last 30 days, 180 days	
7	As an Incident Responder/analyst, I would like to see total Incidents that I am working on.	
8	As an Incident Responder, I will be able to drill down to the component alert's details from the Incident detail's view	
9	As an IR/analyst, I should be able to see all the individual attributes corresponding to the incident, such as file hashes, process names, cmd line, registry changes, ulr access, network access etc.	
10	As an IR/analyst, I should be able to apply multiple filters in the list.	
11	As an IR/analyst, I should see clickable views to check Critical High, Medium and Low Incidents	
12	As an IR/analsyt, I should see clickable views to check various stages the incidents are in New, Investigation phase, Remediation phase and closed.	
13	All Endpoints associated to the incident must be listed	
14	All users associated to the incident must be listed	
15	The sytem should be able to raise alerts based on anomalies seen on the endpoint that deviate from the endpoint baseline, that may indicate a threat	
16	As an IR/analyst, I should be able to drill down into the endpoints belonging to the incident and see all alerts and incidents associated to the endpoints over time.	
17	As an analyst I should be able to see all unassociated/informational alerts that have been generated on the endpoints associated to the incident, I should be able to easily associate these alerts to the incident	
18	As an IR/SOC Manager, I would like to group Incidents based on type, priority, assignee, severity, status, etc	
19	As an IR/SOC Manager, I should be able to add notes to the incident, change the priority of the incident, change the name and description of the incident, change assignee and status and other functions that are required in order to comprehensively and methodically respond to the incident and track it to closure.	
20	As an IR, I should be able to view an RCA for the Incident	
21	Activity logs will record every activity done during Incident response. It will track status changes, assignee changes, notes and other changes made and also serve as an audit log	

22	Activity logs will NOT have edit option	
23	As an Administrator, I should be able to create SLAs for various stages of the Incident response	
24	As a SOC Manager/Analyst/Business owner, I should be flexibly notified about any Incidents that are create in the environment based on many criteria	
25	As an SOC Manager/Analyst, I should be able to track which incidents have passed their SLA's and are Late	
Alert analysis		
1	Must be able to raise alerts from events sourced from endpoints by matching complex event attribute rules that can span across multiple events and endpoints	
2	Must see network map in tree view to aid the analysis. E.g. : an alert is generated based on activities happening across machines in network.	
3	Must see process activity map in tree view to aid my analysis. E.g. : an alert is generated based on activities happening on one machine.	
4	Must see chain of activities to understand the flow of attack. E.g. : Scenario: file1 came via email. When file1 is executed, it dropped file2. File2 then injected code into a system process.	
5	Must see details of a process (e.g. SHA2 hash, digital signature info, etc.) to understand more about it.	
6	Must see details of an activity (e.g. registry creation) to investigate the potential attack.	
7	Must be able to zoom in & zoom out to investigate the attack. E.g. : Scenario: an alert is generated across machines. IR wants to see more of activities on one machine.	
8	Must see all activities done by a process to aid the analysis of Inicdent Responder/analyst. E.g.: Scenario: a process created registries, files, & other processes.	
9	Must see all activities done by parent & child processes to allow for deeper investigation.	
10	Must have an option to filter events in tree based on their type (e.g. process, network, registry) to keep investigation focussed.	
11	Must see alerted process – it's parent & it's children in default view.	
12	Must be able to go back in time to investigate how the attack may have started. Scenario: check parent of the alerted process. Then look for parent of the parent; continue till originated point is arrived at.	
13	Must see a colour coding scheme that would help visually distinguish between various event types.	
14	Must see a colour coding scheme that would help visually highlight alerted process and interesting events.	
15	Must see an event table with all events associate with the alert	
16	Must see critical events on a timeline view to understand how the attack progressed.	
17	Must take actions to respond to an attack. The actions will be executed on the endpoint and vary as per the activity. E.g.: Supported actions: kill process, delete a file, quarantine a file, whitelist a process, isolate endpoint	

18	Must have consolidated view of processes killed, files quarantined, Endpoints isolated by XDR	
19	Must be able to take actions on the alerted flow	
20	Must be be able to see a response for the actions executed on the endpoint.	
21	Must see brief description of the alert generated like conditions that have been hit for the generated alert.	
22	Must view the time sequence of activities performed by a process on which an alert is generated. E.g.: Example: - A process creates some files, then deletes an existing file, it then modifies another file then connects to internet, downloads another file, it then establishes connection with another machine in the network, drops a new file on that machine.	
23	Must be be able to clearly recognize the type of an activity in Timeline View. Example: - An activity can be a registry change or a network connection or a file deletion etc.	
24	Must get an option to filter the activity types in the timely sequence. Example: - I should get an option to see ONLY the network activities performed by an alerted process.	
25	There will be cases when some activities will occur at same time. As an IR/analyst, I should be able to recognise separate activities in such cases where the occurrence time is same.	
26	Must get an option to zoom in/out on the sequence of activities. It should provide an option to focus on activities occurred in a certain time frame.	
27	Must get an option to see the details of an activity in an alerted process.	
Threat Hunting:		
1	An Analyst must be able to select one or many threat indicators to perform an operation. e.g. Hunting for process name = "putty.exe" or hunting for process name = "putty.exe" AND local IP = "11.22.33.44"	
2	Must be able to use a threat indicator multiple times in a query.	
3	Must be able to add/remove/edit a threat indicator value.	
4	Must be be able to clear entire search criteria.	
5	Must be able to see a preview of search query while creating it.	
6	Must be capable of finding below Threat Indicators: 1. MD5 2. SHA2 3. Process Command Line 4. Process Path 5. IP Address 6. Process Name 7. URL, Registry keys and values	
7	Must be capable of hunting based on timeframe e.g.: last 7 days, last 30 days	
8	Must be able to perform threat hunting on the bulk IOCs	
9	Result of Threat hunting will be the list of processes in which these threat indicators are found.	
10	An analyst can associate alerts and processs found that are unassociated to Incidents that are already available in the system or create a new Incident and associate the alerts found	
11	Following information will be available in the search results: 1. Host Name of the processes 2. Related Process information (process ID, process name, process timestamp) 3. If there is/are any alert/s generated on this process and if yes, count of the alerts.	

12	Must be able to search within the threat hunting result	
13	Must be able to save a specific threat hunting query for future.	
14	An analyst must have its own list of query list just like a bookmark list in browser.	
15	Automated hunting - the system should be able to, on a periodic basis hunt for IOC's that are sources from various Threat Intelligence sources, in the complete historical alerts and processes data	
16	All threat hunting queries should be saved in history.	
17	An analyst should be able to reuse queries from threat hunting history. He may modify and run the query.	
18	System must be able to store all events data received from the various endpoints and systems for a period of up to 180 days	
Response		
1	An analyst must be allowed to take remediation action on endpoint, process, file and registry activities.	
2	A user must be able to isolate an endpoint, during which only EDR console will have access to the endpoint	
3	The system must be able to persist isolation across reboots of the endpoint.	
4	For process activity, user can take Kill action. This will kill the process which is executing but it will not delete the file that created the process.	
5	For process activity, user can take Delete action. This will kill the process in memory which is executing and will also delete the file that created this process	
6	The user can also perform Quarantine and Restore action on a file.	
7	For File and Registry activities only Delete action will be supported.	
8	Automated Response - System should be able to perform automated responses based on an Incidents property - for example, if a severe incident of a particular type is created, Incident will be able to Isolate all Endpoints associated to the Incident	
Rule Builder		
1	A rule is defined as a policy that consists of a combination of one or more threat indicators. Rule violations have to be detected by the system across all the endpoints as these occur.	
2	Using a rule/policy, the system will be able to automatically detect malicious/suspicious activities occurring in one or more endpoints in the organization and to generate a response against these detections. A rule is written to detect activities occurring on a single machine or to detect lateral movement across multiple machines.	
3	Threat indicators that have to be supported for rules are Process name, parent process name, network URL, Network Protocol, drive type, event name, registry key name, file name, etc.	
4	Must have provision to see a list of indicators to select from while writing a rule.	
5	Process: 1. Name 2. Path 3. Command Line 4. Child Process Name 5. Child Process Path 6. Child Process command line 7. Is process signed	
6	Registry: 1. Key 2. Value 3. Value data	

7	Network: 1. URL 2. Port 3. IP 4. Protocol	
8	File: 1. Name 2. Path 3. MD5 3. SHA2 4. Is file Signed 5. Drive Type	
9	Windows Event: Event ID	
10	Must be able to associate MITRE TTPs to the rule such that this gets associated to the alert.	
11	Must be able to save a rule with a name. The name will be unique for that tenant.	
12	Must be able to edit the rules..	
13	Must get a confirmation that a rule is saved successfully in the backend.	
14	Must get a notification if a rule is failed to get saved in the backend.	
15	Must be able to write custom rules like e.g. Write a rule to detect if any machine tries to access any particular IP or Write a rule to detect if a specific registry key is generated on any machine.	
16	An analyst can combine threat indicators with 'AND' & 'OR' conjunctions.	
17	Must get option to set the severity for the rule. The severity can be either High, Medium or Low and Base.	
18	Only one level of nesting is supported with support for adding brackets. E.g. Write a rule to detect if a process "powershell.exe" AND (IP = "11.22.33.44" OR IP = "33.44.55.66") is in the network.	
Dashboard		
1	An analyst will be able to see various charts/graphs , including Incident timeline, Top Incidents, MITRE attack metrices, Incident rate, affected endpoints over time, etc. All the graphs will be filterable based on various time durations, incident severity, state, etc.	
2	A SOC Manager dashboard will consist of charts related to operational efficiency and threat metrices. These will include Incident summary by state and criticality, Incident assignment status, Top Incidents, analyst load, MITRE attack metrics, Affected endpoints over time, Incident rates and false positive rates, ROI of the system, various MTTR graphs, Analyst load by incident type, and Late incidents graphs.	
3	An Admin dashboard will have graphs related to incident and alert load operations	
4	The reports can also be downloaded in PDF/Excel format.	
5	The reports can be scheduled	
While listing		
1	An IR can whitelist an alert raised on a process, command line, process path, network IP and protocol. He can select combination of these parameters to generate a whitelisting rule.	
2	These rules can be modified or deleted later.	
Playbooks		
1	As a SOC Manager, I should be able to create playbook based orchestrations that emulate various manual functions that an analyst does in the SOC, such as assignments, notifications, status updates, based on various attributes on an Incident	
2	As a SOC Manager, I should be able to create various investigation and response playbooks that automate many of the enrichment and response actions that area taken as a result of an Incident	

3	As a SOC Manager, I should be able to create both automated playbooks that are triggered when an Incident is created or updated, or manual playbooks that may be associated to various attribute types	
Extended Detection and Response		
1	The system must be able to ingest alerts and events from multiple sources, including endpoints, network firewalls emails systems such as O365 and Gmail.	
2	The system should be able to correlate alerts from multiple sources to create single incidents that show the chain of progression of an attack	
3	The system should have a connector framework that will be able to extend data, enrichment and response systems	
4	Data Retention period: The events generated on any endpoint in the network can be retained upto 180 days	
Sensor System requirements and support		
1	Microsoft Windows 11, Processor: 1 GHz or faster, RAM: min 1 GB for 32-bit or 2 GB for 64-bit	
4	Microsoft Server 2019, Windows Server 2016, Processor: 1.4 GHz Pentium or faster, RAM: 2 GB	
Add on feature		
1	A Chat bot that would respond to the FAQs at one click	
2	The Cloud Solution should reside in India and should have DR failover facility	Kindly brief
3	The Proposed solution should get integrate with IBM QRADR SIEM Solution	

ANNEXURE-F
COMMERCIAL BID FORMAT

BILL OF MATERIAL

S/N	Particulars	Qty	Year 1	Year 2	Year 3
1	Seqrite EPP Cloud 8.x Enterprise Suite (1 Year) Company Name : SBI Capital Markets Limited Product Key : 48082R7027A286179E03 Number of Users : 500 Period : 23/07/2026 to 22/07/2027 **Including OEM and Partner Support**	500			
2	Seqrite XDR Cloud License 23/07/2026 to 22/07/2027	500			
3	One Time Implementation Charges from OEM	1			

Payment Terms and Conditions

1. 100 % Payment Yearly in advance
2. 10% BG to be provided by Bidder of Product value
3. One Time cost will be payable after going live and sign off