Tel. Nos.: (0674) 2375100,
FAX No.: (0674) 2510214/ 2514669,
E-mail: rfpdit@odishascb.com

ORISSA STATE CO-OPERATIVE BANK LTD.
ESTD. 1948

THE ODISHA STATE COOPERATIVE BANK LTD.
(Scheduled Bank)
Pandit Jawaharlal Nehru Marg,
Bhubaneswar – 751 001

Ref No. OSCB/DIT/ 1054*/2023-24, Date:* 19/5/23

Amendment of "Request for proposal for supply, Installation, Commissioning and Management of Hyper-Converged Infrastructure and Security software at data centre and Disaster Recovery Centre for a Period of 5 Years"

THE ODISHA STATE CO-OP. BANK LTD.
BHUBANESWAR

Amendment of “Request for proposal for supply, Installation, Commissioning and Management of Hyper-Converged Infrastructure and Security software at data centre and Disaster Recovery Centre for a Period of 5 Years”

Existing Term	Amendment
Table 1 Technical Specifications **–Software Component** OS - RHEL License with OS patching tool - 4 nodes **SIEM Tool**	**Table 1 Technical Specifications** **--Software Component** OS - RHEL License with OS patching tool - 8 nodes(4 nodes for DC and 4 Nodes for DR) support 24x7x365 days **Specification at Annexure-1**
Sl No. 12 HCI Specifications and qualifications- BOM Specifications Proposed HCI solution should have minimum 5 Banking customer references.	**Sl No. 12 HCI Specifications and qualifications- BOM specifications** Proposed HCI solution should have minimum 5 Banking customer references such as Govt/ PSU /Insurance Sector/ Banking Sector
Sl No. 14 HCI Specifications and qualifications- BOM Specifications Form Factor. : Solution can be 2U3N or 2U1N 2U2N or 1U1N	**Sl No. 14 HCI Specifications and qualifications -BOM Specifications** Form Factor. : Solution can be 2U3N or 2U1N or 2U2N or 1U1N. Rack Mount kit to be offered with security bezel with lock and chassis intrusion kit.
SL.No-51: HCI Specifications Qualified switch vendor should be in Gartner leaders QUADRANT	**SL.No-51: HCI Specifications** Qualified switch vendor should be in Gartner QUADRANT
Sl No 4 :Mandatory Credential and Pre-Qualification of Bidder The bidder should have a minimum average ann turnover of at least Rs120 Crore during the last three audite financial years (i.e. FY 2020-21, FY 2021-22 & 2022-23).	**Sl No 4 :Mandatory Credential and Pre-Qualification of Bidder** The Bidder Should have minimum average annual turnover of at least Rs.30 Crore during last 3 Financial years(i,e. FY 2019-20,FY 2020-21 & 2021-22).
Sl No 5 :Mandatory Credential and Pre-Qualification of Bidder The bidder should have booked profit and ha positive net worth in each of the last three audited financ years (i.e FY 2020-21, FY 2021-22 & FY 2022-23).	**Sl No 5 :Mandatory Credential and Pre-Qualification of Bidder** The Bidder should have booked profit and have positive net worth in each of the last three audited financial years (i.e FY 2019-20, FY 2020-21 & FY 2021-22).

THE ODISHA STATE CO-OP BANK LTD. * BHUBANESWAR *

Sl No 10 :Mandatory Credential and Pre-Qualification of Bidder 10. Bidder should have HCI solution certified expert on payroll. **Supporting Documents** A letter from HR on company letter head to be enclosed with details of HCI solution certified employees on the payroll of the Bidder / Group Company.	**Sl No 10 :Mandatory Credential and Pre-Qualification of Bidder** Bidder undertaking from HR on Company letter head that after award of the order we will ensure HCI Certification for employee or we will hire HCI solutions certified Employees on our payroll within 45 days.
Sl No 11 :Mandatory Credential and Pre-Qualification of Bidder Bidder should have executed minimum 5 orders last 5 financial years (i.e., FY 2018-19, FY 2019 - FY 2020-21 , FY 2021-22 & FY 2022-23) for supply of HCI solution to Bank / Governme Organization / PSU. At least one order should ha an order value of INR 3 Crore or more and at le one order should have the HCI solution from t Proposed OEM. Bank would need 5 customer references from the BFSI industry vertical who have implemented HCI Solution of the proposed OEM	**Sl No 11 :Mandatory Credential and Pre-Qualification of Bidder** Bidder/OEM should have executed minimum 2 orders in last 5 financial years (i.e., FY 2017-18, FY 2018-19, FY-2019-20, FY 2020-21 & FY 2021-22) for supply of HCI solution to bank / Government organization / PSU. At least one order should have an order value of INR 3 Crore or more and at least one order should have the HCI solution from the proposed OEM. Bank would need 5 customer references from the BFSI industry vertical who have implemented H Solution of the proposed OEM.
Annexure-G- BILL OF MATERIAL SERVER for DC @ Bhubaneswar and DR Faridabad with 5 years warranty and Support	**Annexure-G- BILL OF MATERIAL** SERVER for DC-4 nodes @ Bhubaneswar and DR – 4 nodes @ Faridabad with 5 years Warranty and and Support.

THE ODISHA STATE CO-OP. BANK LTD. * BHUBANESWAR *

SIEM Tool Specification at Annexure-1

The solution should be able to collect logs from different infrastructure components such as Servers, Firewalls, Databases, Applications.

The solution should normalise the logs to collect insights from the logs

Logs support should be extended to the platforms through custom apps and APIs for non-supported log formats.

The Solution should support collectors at separate locations.

The user interface to monitor and investigate events from the SIEM tool should be customizable and should provide capabilities necessary for further analysis

The solution should have ability to perform trend analysis basis the historical data collected.

Solution should enable the easy customizable dashboards and customizable dashboards based no visualizations:

- Bar chart
- Pie
- Donut
- Area Chart
- Line Chart

The Service Provider is expected to provide Threat Intelligence & Analytics feeds which can be used to detect threats & can further enhance integration with SIEM.

Vendor should have capabilities to detect access anomalies e.g. Detection of deviation in the interaction of one server with another to detect attacks such as lateral movements.

Network Threat hunting should utilize existing logs from security controls such as firewalls , IPS devices , to detect targeted attacks.

In addition to the advanced analytics capabilities solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples

- Failed login attempts
- Login attempts from suspicious locations
- Authorization attempts outside of approved list
- Vendor logins from unauthorized subnets
- Vertical & Horizontal port scans
- Traffic from blacklisted IPs
- Login attempts at unusual timings

Solution should support criticality levels of alerts from a number of security products including Firewalls, Routers ,AV etc.

The proposed solution should support collection of events through customization of connectors or similar integration for the assets that are not natively supported.

The proposed solution should be able to collect data from new devices added into the environment once onboarded, without any disruption to the ongoing data collection.

The proposed solution should have connectors to support listed devices/ applications, wherever required the vendor should develop customized connectors.

The proposed solution should support log collection from all major operating systems and their versions but not limited to Windows, Linux, Mac

The collectors should be able to store/retain both normalized & raw data for forensic purposes

The proposed solution should have capabilities to store the event data in its original format in the central log storage

The proposed solution should support multiple log collection protocols.

Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users

The Solution should have its own integrated case management to analyse the alerts.

Case management should have capabilities to set criticality of the identified alerts.

Case management should be able to conduct analysis and enrich the observables such as IP address, email, domains, urls.

The solution should have integrated vulnerability assessor to identify vulnerable operating system patches, packages and installed software

The solution should have file integrity monitoring module to keep the track of defined critical files.

THE ODISHA STATE CO-OP. BANK LTD.

Solution should be able to record the changes made to the files being monitored

The solution should be able to categories the events based on the mitre att&ck framework.

The solution should be able to parse logs generated by custom developed applications.

The solution should be able to send notification over multiple channels integration such as slack, teams, emails,

The solution should be able to integrate with third party threat intelligence sources over APIs to enrich events and

The solution should allow to create custom visualizations and graphs as per customer requirement

The solution should allow access to the raw logs for investigation and RCA activities

The solution should be able to get details from agents such as current running processes, open ports, agent ip details.

The response capabilities should be customizable with development work

The proposed solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service

The proposed solution should provide options to load balance incoming logs to multiple collector instances.

The proposed solution should support log collection from all operating systems and their versions including but not limited to Windows, Unix, Linux, etc.

The proposed solution should be able to store/retain both the log meta data and the original raw message of the event log for forensic purposes.

The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.

The proposed solution should support the following log collection protocols: Syslog over UDP / TCP, Syslog NG, JDBC

It should be possible to categorize events while archiving for example, events for network devices, antivirus, servers etc.

The proposed system should display all real time events. The proposed solution should have drill down functionality to view individual events from the dashboard

The proposed solution should allow applying filters and sorting to query data

The proposed solution should have the ability to perform free text searches for events, incidents, rules and other parameters.

The proposed system should identify the originating system and user details while capturing event data.

The proposed solution should have the ability to send notification of correlated events via well-defined methods

The proposed solution should be capable of retrieving the archived logs for analysis, correlation and reporting purpose.

THE ODISHA STATE CO-OP. BANK LTD. * BHUBANESWAR *