2.9. Data Base Activity Monitoring

|  |
| --- |
| **Technical and Performance Specifications for Database Activity Monitoring**    **DAM – Quantity Two (2) for DC** |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Requirements | Criteria | Bidder’s Response |
| 1 | General Requirements |  |  |
| 1.1 | The vendor must exclusively provide Cyber security solutions | Mandatory |  |
| 1.2 | The vendor of the proposed solution must be leader in DAM security test for the last two Years as measured by NSS lab or Gartner Magic quadrant security effectiveness | Mandatory |  |
| 1.3 | The solution must be hard ware appliance and on premise deployment | Mandatory |  |
| 1.4 | The solution must be licensed for 6 databases (different IP address) with Core | Mandatory |  |
| 1.5 | The solution must support data protection and vulnerability assessment for databases. | Mandatory |  |
| 1.6 | The solution must support hardware and software license for three years | Mandatory |  |
| 1.7 | The solution that collect activities from database must be appliance base | Mandatory |  |
| 1.8 | The solution must come up with be in HA mode | Mandatory |  |
| 1.9 | The central reporting system must be in appliance based. | Mandatory |  |
| 2 | Functionality Requirement |  |  |
| 2.1 | The solution must provide automated discovery of both new and existing database systems and Database tables on the network | Mandatory |  |
| 2.2 | The solution should be able to support/monitor all database activities in OSs like AIX, UNIX, HP UNIX, Linux, Solaris, Windows and Databases like Oracle, MS-SQL, MySQL at a minimum. | Mandatory |  |
| 2.3 | Solution must be support asset management and change management processes. | Mandatory |  |
| 2.4 | Solution must perform data discovery and classification. | Mandatory |  |
| 2.5 | Solution must have inbuilt vulnerability assessment testing of supported databases | Mandatory |  |
| 2.6 | Solution must have a provision for custom assessments. | Mandatory |  |
| 2.7 | Solution must be to verify that default database accounts do not have “default” passwords. | Mandatory |  |
| 2.8 | Solution should provide risk score of individual databases, based on combination of security alerts, discovery results, vulnerability assessment, sensitivity & confidentiality of data stored in the database | Mandatory |  |
| 2.9 | The solution must have virtual patching capabilities (Protecting the database from known vulnerabilities without deploying a patch or script on the system) | Mandatory  Mandatory |  |
| 2.10 | The solution should Provide tools for managing and mitigating risk to data stored in databases | Mandatory |  |
| 2.11 | The Solution must have a comprehensive tracking and logging facility for users. | Mandatory |  |
| 2.12 | The solution must have an auditing process that is independent from the database platform being audited to allow for SODs | Mandatory |  |
| 2.13 | The Solution able to capture activity by a user by logging all SQL activities | Mandatory |  |
| 2.14 | The Solution must have inbuilt database security by being able to protect the DB from attacks such as database worms, denial of service attack and SQL injection. | Mandatory |  |
| 2.15 | Provide real time protection and reports to security administrators. Be able to provide real-time blocking of attacks, monitor and be able to block activities of privileged user accounts. | Mandatory |  |
| 2.16 | Provide for quarantining or blacklisting user accounts that have violated policies. | Mandatory |  |
| 2.17 | The solution must include a user rights management solution to review user rights and identify users with excessive rights. It must also be able to log user logon statistics. | Mandatory |  |
| 2.18 | The solution should have the ability to define rules and alerts | Mandatory |  |
| 2.19 | The solution should provide means to profile data activity behavior together with tools to filter noise or known false Positives. | Mandatory |  |
| 2.20 | The solution should not store sensitive data in plain text in logs generated by the application (e.g. passwords) | Mandatory |  |
| 2.21 | The solution must be scalable to accommodate future growth in number or size of servers | Mandatory |  |
| 2.22 | The solution should not materially impact any other monitoring tools already in use in the systems | Mandatory |  |
| 2.23 | The solution should provide tamper proof audit trail (including from privileged users) | Mandatory |  |
| 2.24 | Logs and audit-trail generated by the solution should not be editable by users\administrator and should be read-only | Mandatory |  |
| 2.25 | The solution must be able to do data summaries in tables, trends and charts based on standard and custom reporting policies. | Mandatory |  |
| 2.26 | The solution must have capabilities to generate scheduled reports and custom real time alerts based on incident policies through various alert delivery channels such as email. | Mandatory |  |
| 2.27 | The solution must be able to generate standards and custom reports. The reporting module must flexible with various framework-based reports, on- demand reports, and scheduled reports which can be generated in various file formats. | Mandatory |  |
| 2.28 | The solution must allow for policy configurations to identify, report/alert and block suspicious transactions and activity. | Mandatory |  |
| 3 | **Integration** |  |  |
| 3.1 | The solution must be support standard log formats which can be used to integrate to SIEMs | Mandatory |  |
| 3.2 | The solution should have option to filter the events before sending to SIEM | Mandatory |  |
| 3.3 | The solution should support integration with 3rd party antimalware to prevent infected clients from accessing sensitive data | Mandatory |  |
| 4 | **Administration and Management** |  |  |
| 4.1 | Solution should include a Web based single administration interface | Mandatory |  |
| 4.2 | The Proposed solution should have an out-of-band management capability. | Mandatory |  |
| 4.3 | Management solution should support Role-Based Access Control or multiple user roles that facilitate separation of duties. i.e. Administrator (Super-User), Manager, read only etc. | Mandatory |  |
| 4.4 | The solution should support the following authentication mechanism for accessing the solution In-built authentication in the solution  i. Kerberos authentication  ii. LDAP\ AD authentication  iii. RADIUS authentication | Mandatory |  |
| 5 | **Hardware requirement and Performance Specifications** |  |  |
| 5.1 | Dual hot-swap hard drives, Dual hot-swap  power supplies | Mandatory |  |
| 5.2 | 4 x 1G copper port | Mandatory |  |
| 5.3 | 4x10GBASE-SR | Mandatory |  |
| 5.4 | Hard drive 2 x 2TB | Mandatory |  |
| 5.5 | RAM- 16GB | Mandatory |  |
| 5.6 | OUT-OF-BAND PORT MANAGEMENT- 2 x 100/1000 Copper | Mandatory |  |
| 5.7 | Accessory’s with full kit and accessory  License three Years license for the following features   * For 6 database * Data discovery and classification * Vulnerability Assessment and user right management * Data activity monitoring and protection policy * Security analytics * High performance reporting | Mandatory |  |
| 5.8 | Deployment should be Certified professional or service from the vendor. | Mandatory |  |
| 6 | **Database Activity Management Server Hardware Specification quantity 1** |  |  |
| 6.1 | Memory 16GB | Mandatory |  |
| 6.2 | Hard drive 2TB | Mandatory |  |
| 6.3 | Management port 2\*100/1000 copper | Mandatory |  |
| 6.4 | Redundant power supply | Mandatory |  |
| 6.5 | 2\*power supply | Mandatory |  |
| 6.6 | Accessory’s with full kit and accessory | Mandatory |  |
| 6.7 | Three Year Warranty | Mandatory |  |
| 6.8 | Deployment professional level or service from the vendor | Mandatory |  |