Solicitation RFI FTB-1213-SIEM Replacement

Security Information and Event Management (SIEM) Project

State of California

Bid RFI FTB-1213-SIEM Replacement
Security Information and Event Management (SIEM) Project

Bid Number	**RFI FTB-1213-SIEM Replacement**
Bid Title	**Security Information and Event Management (SIEM) Project**
Bid Start Date	**Aug 27, 2012 2:07:49 PM PDT**
Bid End Date	**Sep 20, 2012 2:00:00 PM PDT**
Question & Answer End Date	**Sep 13, 2012 7:00:00 AM PDT**
Bid Contact	**Tracie Zamora** **Staff ISA** **916-845-3937** **tracie.zamora@ftb.ca.gov**
Standard Disclaimer	**The State of California advises that prospective bidders periodically check the websites, including but not limited to Bidsync, and/or other state department links for modifications to bid documents. The State of California is not responsible for a prospective bidder's misunderstanding of the bid solicitation or nonresponsive bid due to failure to check these websites for updates or amendments to bid documents, and/or other information regarding the bid solicitations. Failure to periodically check these websites will be at the bidder's sole risk.** **The information published and/or responded to on these websites is public information. Confidential questions/issues/concerns should be directed to the contact on the ad.**

Description
The FTB is surveying the marketplace for potential vendors that can provide a comprehensive Security Information Event Management (SIEM) solution.

State of California
Franchise Tax Board

August 27, 2012

To: Potential Vendors

Subject: Request for Information (RFI) Franchise Tax Board (FTB) Security Information and Event Management (SIEM) Project.

The FTB is surveying the marketplace for potential vendors that can provide a comprehensive SIEM solution. The solution must employ an alerting tool with the ability to accurately identify suspicious events by correlating log information from firewalls, intrusion detection/prevention systems, servers, and other network devices. The solution must also provide a reporting tool for producing customizable reports on all collected events and correlated information.

This RFI contains our draft requirements for the desired solution. FTB has provided a list of technical and functional items for vendors to respond to regarding their SIEM solution. Please provide detailed explanation, product specifications, literature, or other documentation of how your product/solution meets each requirement. Vendors may also provide alternatives to a requirement and provide further information to clarify response.

If you intend to respond to this RFI, please send your contact information by September 13, 2012 so we may provide any supplemental information.

IMPORTANT INFORMATION – PLEASE READ BEFORE RESPONDING TO THIS RFI

1. FTB will not reimburse vendors for any costs associated with responding to this RFI.
2. FTB has no obligation to buy or issue a solicitation as a result of this RFI.
3. Information provided in response to this RFI will not be considered when evaluating bidders responding to any future procurement.
4. Responses to this RFI will become public record, upon completion of the RFI process.
5. If future a procurement results from this RFI, vendors will have to agree to the State's terms and conditions: http://www.documents.dgs.ca.gov/pd/modellang/GPIT060810.pdf

If you are interested in responding, please submit at least one soft copy of your response by 2:00PM PDT, September 20, 2012 via e-mail to: tracie.zamora@ftb.ca.gov

Or mail your response to:

Tracie Zamora
Franchise Tax Board
Procurement and Asset Management
P. O. Box 2086, MS A-374
Rancho Cordova, CA 95741-2086

We appreciate your time and consideration in reviewing and responding to this RFI. Any questions can be directed to me at (916) 845-3937.

Tracie Zamora
Technology Acquisition Analyst
Procurement and Asset Management

Phone#916.845.3937 Fax#916.845.9627 tracie.zamora@ftb.ca.gov

Overview:

FTB is surveying the marketplace for potential vendors that can provide a comprehensive SIEM solution to upgrade or replace its existing system. The existing system is composed of two different systems. One, developed in-house, is used for the collection and reporting of audit logs collected primarily from legacy applications. The other is a commercial off-the-shelf (COTS) SIEM product, primarily used for the collection and reporting of device and application audit logs. The solution must provide secure log file collection and storage, backup, retrieval, reporting, and event alert notification. In addition to a reporting tool, the SIEM solution must provide event correlation and integrate with existing security systems at FTB, as indicated in the requirements below.

Requirements and Response:

Below is a list of technical and functional items for vendors to respond to regarding their SIEM solution. The information provided will assist FTB in making a determination on how best to move forward to replace our existing in-house system and to combine both systems into one viable and supportable COTS system. If the proposed solution does not provide the listed functionality, vendors are encouraged to propose alternative functionality the solution may provide.

To assist you in responding, we are providing the following information:

Number of active event sources: 1,000
Number of events collected daily: 300,000,000
Average events per second: 3,500
Amount of data collected daily: 175GB
Amount of data currently stored: 55TB (uncompressed)

These numbers are expected to increase significantly over the next several years with the implementation of the various phases of the Enterprise Data to Revenue (EDR) project. Total storage is expected to double within the first year while daily amounts are expected to increase from 5-10% per month over the next several years.

As FTB reviews responses from this RFI, we may request a presentation and possibly follow with a proof of concept.

FTB requests that vendors provide detailed explanations, product specifications, literature, or other documentation for each of the requirements listed below. Please provide estimated catalog pricing on product(s), estimated catalog pricing on maintenance and/or any additional or potential costs in order to meet the following requirements:

Administration

1) Describe how your solution integrates with Active Directory (AD) and list the protocols used (e.g., Lightweight Directory Access Protocol (LDAP) or Kerberos).
2) Describe the Role-Based Access Control (RBAC) functionality and granularity within your solution.
3) Describe how users and administrators access your solution such as via a browser, management console, dashboard, or other graphical user interface (GUI).
4) How many concurrent user sessions are allowed?

Technical Support/Troubleshooting

1) Describe the training and modules offered, and provide a current schedule of training available within the State of California, including the Sacramento area.
2) Attach documentation or describe your 24x7 product support offerings including telephone support and issue escalation procedures.
3) Attach documentation or describe your hardware and/or software maintenance agreements (renewable annually) for upgrades, patches, and enhancements.
4) Will you provide resources (hardware, software, and services) for FTB to conduct a proof-of-concept of your solution at no cost to the State?

5) Will you allow for acceptance testing of your solution up to 120 days prior to our acceptance of the product?
6) Does your solution include context-sensitive help functionality to provide troubleshooting and system guidance?

Technical

1) If Windows based, explain your solution's capability to become part of an existing Windows domain, or if it is necessary to create a separate, trusted domain.
2) Is integration with a centralized network time server using Network Time Protocol (NTP) supported?
3) Provide hardware and/or software product life cycles with end-of-life/support dates for your current solution.
4) Indicate whether your solution utilizes SAN or NAS mass storage solution(s), or both, and any specific requirements or recommendations.
5) Explain how your solution is designed to ensure high availability, including redundancies, and performing system and database maintenance without business interruptions.
6) Is your solution fully compatible (not interfering with normal functionality) with the following types of software? If not, please explain.
    a. Virus protection suites
    b. Automated patching software
    c. Asset management Software

Reporting

1) How does your solution automate and schedule reports on a recurring basis without manual intervention?
2) Describe how your solution integrates with Microsoft Reporting Services. Include the steps required and supported versions.
3) How are the reports displayed on-line from within the application?
4) List the graphical formats your solution can utilize to display reports.
5) Explain how your solution restricts access to reports by role (e.g., detailed user reports that should not be available to all users).
6) Describe how your solution queries Active Directory for any attribute, and incorporates them as report values.
7) Describe how your solution provides links with or is able to query other databases such as MS SQL.
8) List the formats that can be used to export reports and database data.
9) Describe how your solution provides the capability to create custom reports.
10) Explain how report column names can be customized with user provided names.
11) Describe how your solution filters report data (e.g., apply custom filters on the data and exclude specified data from the export process).
12) Describe how report columns displayed in reports can be limited (e.g., display specific columns in a report instead of all columns that may have been generated when the report was run).
13) Describe how your solution provides for report aggregation to improve overall system performance (e.g., combining output from multiple reports without having to re-run the reports).

Security

1) List the methods for providing automated alerts when logging has stopped on any given device, application, or specified alert thresholds are exceeded (e.g., SMTP, Text (SMS), SNMP v3.0).
2) When new vulnerabilities impacting your solution are discovered by your company or industry sources, how soon after the vulnerability is publicly announced, does your company provide patches, fixes, or other compensating controls?
3) If appliance based, list the hardening standards your solution complies with (e.g., National Institute of Standards and Technology (NIST)).
4) Explain how your solution provides secure collection of log file and event data utilizing open standard network protocols for encryption, utilizing at least 128 bit AES, SFTP, FTPS or HTTPS.

5) Describe how your solution provides for secure storage of collected audit data, including encryption algorithms, and how it prevents any modifications to the data.

Collection

1) List the leading vendors your solution is able to import data from as listed in the Gartner Magic Quadrant for Security Information and Event Management, May 24, 2012.
2) Describe your solution's log collection methodologies, whether push/pull technologies are used, agents or agentless, SNMP, web services, etc.
3) Provide a list of the specific event sources and log types your solution is able to securely collect and store log data from, including, but not limited to the list below. Attach appropriate product documentation if available.
    a. Operating systems
    b. Services (e.g.: DNS, DHCP)
    c. Databases
    d. Syslog
    e. Text Files
    f. VPN/Firewalls
    g. Proxy servers
    h. Badging systems
    i. Intrusion Detection/Prevention systems
    j. Mainframe SMF records
    k. Commercial off-the-shelf (COTS) products (provide listing of supported products)
    l. Custom applications
    m. Vulnerability scanning tools
4) Explain how your solution is able to integrate with or merge data from MS SQL databases.
5) What are the limitations regarding the number of event sources your solution can collect from? How does your solution prevent system performance degradation or loss of log data if too many event sources are trying to send log data to the solution at one time?
6) Describe your solution's capability to recover logs when transmission of data is abruptly terminated.
7) Is your solution capable of collecting log data from relay devices?
8) How does your solution collect audit log data from custom in-house applications?
9) Describe how your solution aggregates and normalizes variable log file formats and characteristics into central repository.
10) Describe how your solution collects log files 24/7 and provides scheduled log extracts and manual log extracts outside normal scheduling.
11) Describe how your solution identifies and provides automatic notifications when duplicate logs are received, and how it performs automated verification to ensure that log files and records being stored are not duplicative.
12) Describe how your solution collects and displays logs in near real-time.
13) How does your solution buffer logs locally when the event source is unavailable?
14) How does your solution balance collection of events between multiple collection points?
15) Does your solution have the capability of providing a single, load balanced collection point? If so, describe how this functionality works in your solution.
16) Explain how your solution is able to filter out or purge unnecessary or unwanted audited events (e.g., by specific Windows event IDs or subcategories).
17) Describe situations where events could be dropped by your solution.

Database

1) Describe how the database scales, and provides for future expansion. Describe clearly identifiable upgrade paths and provide associated costs.
2) List the tools that may be used to query the reporter database.
3) Describe how the database supports RBAC using Active Directory for user and group access controls.
4) Describe the authorization and process for access to the data store.
5) Describe how your solution performs data file compression for maximum space utilization.
6) Describe the process for archiving or purging data after it reaches or exceeds specified data retention periods.
7) Explain retention and purge period criteria (e.g., type, source, date). List any other criteria available.
8) How does your solution retrieve archived data and provide access to archived and on-line data simultaneously?

Functionality/Performance

1) Describe how your solution is able to resume data collection with the last captured event without loss of data upon system restart, or in the event that an event source loses communication with the data collector, resulting in complete, integrity-verified collected audit log data.
2) Describe the event correlation, mapping, and trend analysis capabilities of your solution, including retention and replay of correlated events.
3) Describe the high-performance metrics for your solution.
4) Describe techniques for improving performance including data indexing and the capability for the creation and application of user-defined indexes.
5) Describe how your solution provides user defined fields and the methods available for population.
6) Describe the capability of your solution to create, store, and manage custom queries created to capture, categorize, and alert on specific activity.
7) Describe how pattern recognition is accomplished, and provide for automated alerts based on rule sets such as multiple concurrent user logons, concurrent local and remote user logons, and abnormal logon attempts.
8) How much data can your solution maintain online for queries and reporting purposes? FTB has a statutory requirement to maintain up to six years of data, which could exceed 200TB (uncompressed). Explain how this amount of data can be made available for performing queries and producing reports.
9) Based on the data amount in the previous question, provide the expected response time to generate a query or report for one user (single userID).
10) Provide the expected response time to generate a query or report from collected Windows Server log files for one user (single userID) based on:
    a. 10,000,000 events _____
    b. 100,000,000 events _____
    c. 1,000,000,000 events _____
11) What is the maximum record length your solution can import and process, and how many fields can be contained within a single record? Are XML strings handled differently? Provide sample table layouts if possible.

Question and Answers for Bid #RFI FTB-1213-SIEM Replacement - Security Information and Event Management (SIEM) Project

OVERALL BID QUESTIONS

There are no questions associated with this bid. If you would like to submit a question, please click on the "Create New Question" button below.

Question Deadline: Sep 13, 2012 7:00:00 AM PDT