RFP# 554-2023-0052

Managed Security Information & Event Management (SIEM) Services for Existing LogRhythm SIEM

ADDENDUM #3

Date: March 12, 2024

(1) QUESTION: Please describe the current LogRhythm architecture? Is it a single XM appliance on premise or a distributed architecture? If distributed, please describe number of System Monitors, Data Processers, AIE's and Data Indexers?
AUTHORITY RESPONSE: Single XM with 2 virtualized collectors.

(2) QUESTION: Please provide estimated end date for hardware/software support and licensing?
AUTHORITY RESPONSE: RDUAA is licensed until 3/31/25.

(3) QUESTION: What is the LogRhythm platform currently licensed for in terms of MPS (e.g., platform is licensed for 1000 MPS but only ingesting 500 MPS)?
AUTHORITY RESPONSE: 1000MPS

(4) QUESTION: What has been the average daily ingestion (MPS) over the last 6 months? If available, please provide a Log Volume by Log Source Type for the last 3 months?
AUTHORITY RESPONSE: ~300

(5) QUESTION: Is RDUAA ingesting 100% of its intended log sources? If not, what is still left to be ingested?
AUTHORITY RESPONSE: No. Devices in flux include switches and maintenance/ingestion is ongoing.

(6) QUESTION: Does RDUAA have any smart plugins deployed?
AUTHORITY RESPONSE: None with automation.

(7) QUESTION: Does RDUAA have any cyber threat intel integrations with the LogRhythm platform?
AUTHORITY RESPONSE: Several feeds/TAXII

(8) QUESTION: Please describe any required or existing custom reporting requirements?
AUTHORITY RESPONSE: No custom reporting. Our intent is to allow the selected partner to create/manage these to deliver actionable items to our analysts.

(9) QUESTION: Will RDUAA consider a multi-year (2 or 3) contract?
AUTHORITY RESPONSE: Multi-year will not be considered for this term.

(10) QUESTION: Please describe your threat hunting requirements?
AUTHORITY RESPONSE: Actionable items including hits based on perceived intrusion or behavior.

(11) QUESTION: Does RDUAA adhere to or follow any cybersecurity frameworks?
AUTHORITY RESPONSE: CIS (cross-mapping NIST in some cases).

(12) QUESTION: Please describe any custom log sources or log parses currently in product?
AUTHORITY RESPONSE: RDUAA does not have custom sources.

Thank you for your interest in doing business with our Agency and we look forward to receiving a proposal submittal from your firm.

Paul Brown

Procurement and Contracts Specialist II

END OF ADDENDUM #3