Test and Acceptance Plan

For

Security Information and Event Management (SIEM) Solution

Table of Contents

PART A - ACQUISITION BACKGROUND AND OBJECTIVES

1 Statement of Need

The Department of Veterans Affairs (VA), Network Security Operations Center (NSOC) serves as VA's security operation element under the Office of Information Security (OIS). The NSOC manages, protects, and monitors the cyber security posture of the entire VA enterprise, coordinates externally with government incident response centers, performs threat and vulnerability analyses, reports cyber security deficiencies, develops concept of operations or guidelines relating to cyber security incidents, performs analyses of cyber security events, maintains detailed logs and databases of VA cyber security incidents and responses, and performs the full range of functions across the spectrum of activities relating to incident management and response, vulnerability scanning, event correlation and analysis, audit log analysis, patch distribution, and remediation planning. The NSOC has a requirement to procure a non-brand name Security Information and Event Management (SIEM) solution. The solution will centralize network and security event information from the security event log aggregator.

The product shall centralize network and security event information from the security event log aggregator. The SIEM will have the following system level capabilities:

- Automated Actions
- Event Correlation and Root Cause Analysis
- Reporting and Fault Management
- Real Time Monitoring
- Forensics Analysis

2 Applicable Conditions

The systems to be tested shall be ready for testing after the Contractor has configured the systems for the VA environments.
Two systems shall be tested. They are:

1. The system and equipment for the one test lab environment
2. The system and equipment for one of the Trusted Internet Connection (TIC) Gateways environment

3 Testing

The VA will conduct testing of the proposed solution for a period of seven (7) calendar days. Testing shall include: configuration; installation; and performing routine SIEM functions as listed in the PWS and the Offeror's proposed capabilities. Specific areas of testing focus shall include: Integration with Splunk; Splunk and SIEM Solution performance; Encrypted web interface functionality; and Storage and data management functions.

4 Acceptance Criteria

The solution shall be determined to be acceptable upon successfully:

- Meeting or exceeding the VA requirements

- Meeting or exceeding the Offeror's proposed capabilities
- Remaining stable through the testing exercises
- Not requiring additional rudimentary code and/ or programming

5 Testing Completion

The VA will compile a report documenting the findings and share with the Contractor. Upon the systems being determined to be acceptable, the Contractor shall initiate delivery of all remaining SIEM components.

Upon the systems being determined to be unacceptable, the VA will return all equipment delivered to the VA by the Contractor for this acquisition, for which the Contractor shall issue a full refund.