Request for Proposal (RFP) for Integrated Security Operations Centre (SOC), Security Incident and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR) Solution

1. Introduction

The objective of this Request for Proposal (RFP) is to engage qualified vendors in submitting a comprehensive proposal for the supply and implementation of an integrated Security Operations Centre (SOC), Security Incident and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR) solution. This solution aims to empower our organization with proactive capabilities to detect, investigate, and respond to security incidents and events effectively and efficiently.

Background

Our organization functions in a highly competitive sector, managing a substantial amount of sensitive data crucial to our business operations. Recognizing the importance of robust security measures to safeguard our data and assets from cyber threats, we also acknowledge that the ever-evolving nature of cyber threats necessitates advanced protection. Consequently, we seek a comprehensive SOC, SIEM, and SOAR solution capable of delivering cutting-edge threat detection, investigation, and response.

2. Scope of Services

The selected vendor will be responsible for the implementation and provision of ongoing SOC, SIEM, and SOAR services for a period of 2 years. The scope of services includes:

Implementation Phase

a. Solution Design and Configuration

- Design, implementation, and configuration of an integrated SOC, SIEM, and SOAR solution tailored to our organization's specific needs and requirements.

b. Integration

- Seamless integration of the SOC, SIEM, and SOAR solution with our organization's existing security tools and technologies.

c. Customization

- Customization of the solution to address our organization's unique security challenges and use cases.

Ongoing Services (2-year period)

a. SOC Services

- Continuous monitoring, analysis, and reporting of security incidents and events across our organization's network.
- Regular SOC reports and dashboards provided to our organization's management team.

b. SIEM Services

- Ongoing collection, correlation, and analysis of logs from various sources, including network devices, servers, and applications.
- Regular SIEM reports and dashboards provided to our organization's management team.

c. SOAR Services

- Continuous automation and orchestration of security workflows across various security tools and technologies.
- Development of customized playbooks and automation workflows for our organization's specific security use cases.

Training and Support Services

a. Training

- Provision of comprehensive training for our organization's SOC analysts on the use of the SOC, SIEM, and SOAR solution.
- Training delivery options to include in-person, online, or self-paced formats.
- Provision of a proposed schedule for training sessions and estimated duration for the training process.

b. Ongoing Support

- Dedicated helpdesk support and access to a dedicated account manager for our organization.
- Regular software updates and patches to ensure the solution remains up-to-date with the latest security threats and technologies.
- Periodic review meetings with our organization's management team to discuss performance, address concerns, and suggest improvements.

By providing these services, the selected vendor will help ensure the continuous protection of our organization's sensitive data and assets against evolving cyber threats during the 2-year service period.

3. Evaluation Criteria

Proposals will be assessed based on the following criteria, with each criterion carrying a weight of 25%:

Solution Quality and Fit

- How well the proposed solution meets our organization's technical requirements, integrates with our existing security tools, and addresses our specific security use cases.
    - Does the solution offer advanced threat detection and response capabilities?
    - How seamlessly does the solution integrate with our existing security tools and technologies?
    - Can the solution be customized to address our organization's unique security challenges?

Vendor Experience and Reputation

- The vendor's track record, expertise, and success in delivering SOC, SIEM, and SOAR solutions to similar organizations.
    - How many years of experience does the vendor have in providing SOC, SIEM, and SOAR solutions?
    - What is the vendor's success rate in implementing and maintaining such solutions for clients in similar industries?

- Does the vendor have any industry recognitions or awards for their SOC, SIEM, and SOAR offerings?

Implementation Approach and Timeline

- The clarity and feasibility of the proposed implementation plan, including the ability to meet project deadlines.
    - Is the proposed implementation plan clear, realistic, and achievable within the given timeframe?
    - How will the vendor ensure minimal disruption to our organization's operations during the implementation process?
    - What is the proposed timeline for project milestones and completion?

Training and Support Services

- The quality and effectiveness of the training and ongoing support provided to our organization's SOC analysts.
    - What type of training will be provided to our SOC analysts, and how will it be delivered (e.g., in-person, online, self-paced)? - What is the proposed schedule for training sessions, and how long will the training process take? - What level of ongoing support will be available to our organization after the solution is implemented (e.g., helpdesk, dedicated account manager, software updates)?
- 4. Step-by-Step Implementation Plan
    - The following is a step-by-step implementation plan for the integrated SOC, SIEM, and SOAR solution:

    Step 1: Requirements Gathering and Analysis

        - Conduct a thorough assessment of our organization's security needs, requirements, and existing security infrastructure.
        - Identify key stakeholders and involve them in the requirements gathering process.
        - Document the gathered requirements and obtain approval from the organization's management team.

    Step 2: Solution Design and Configuration

        - Design the SOC, SIEM, and SOAR solution architecture based on the approved requirements.
        - Define the necessary components, modules, and interfaces for the solution.
        - Configure the solution to meet our organization's specific needs and requirements.

    Step 3: Integration and Customization

        - Integrate the SOC, SIEM, and SOAR solution with our organization's existing security tools and technologies.
        - Customize the solution to address our organization's unique security challenges and use cases.

- Test the integrated solution to ensure seamless functionality and compatibility with our existing infrastructure.

Step 4: Deployment and Initial Training

- Deploy the integrated SOC, SIEM, and SOAR solution in our organization's environment.
- Provide initial training to our SOC analysts on the use of the solution.
- Monitor the solution's performance and address any issues that arise during the initial deployment phase.

Step 5: Ongoing Services and Support

- Provide continuous SOC, SIEM, and SOAR services as outlined in the scope of services.
- Deliver regular reports and dashboards to our organization's management team.
- Develop customized playbooks and automation workflows for our organization's specific security use cases.
- Ensure the solution remains up-to-date with the latest security threats and technologies through regular software updates and patches.

Step 6: Training and Support Services

- Provide comprehensive training for our organization's SOC analysts on the use of the SOC, SIEM, and SOAR solution.
- Offer training delivery options, including in-person, online, or self-paced formats.
- Schedule training sessions and provide an estimated duration for the training process.
- Provide ongoing helpdesk support, access to a dedicated account manager, and periodic review meetings with our organization's management team.

Step 7: Periodic Evaluation and Improvement

- Conduct periodic evaluations of the solution's performance, effectiveness, and alignment with our organization's security needs.
- Gather feedback from our organization's management team and SOC analysts to identify areas for improvement.
- Implement necessary improvements and enhancements to the solution based on the feedback and evaluation results.

By following this step-by-step implementation plan, the selected vendor will ensure the successful deployment and ongoing management of the integrated SOC, SIEM, and SOAR solution for our organization.