FEASIBILITY STUDY: IMPLEMENTING OPENCTI

Redback Operations

Document Owner: Purple Team
Next Review Date: 17 June 2024
Last Modified By: Devika Sivakumar
Last Modified on: 12 May 2024

Contents

1. Introduction

- Purpose of the Study
- Background Information on OpenCTI

2. Objectives

- Define the specific goals and objectives of implementing OpenCTI within the organization.

3. Functional Analysis

- Overview of OpenCTI's features and functionalities.
- Comparison with organizational requirements and objectives.
- Identification of key features that align with organizational needs.

4. Technical Assessment

- System Requirements: Hardware, software, and network infrastructure needed to deploy OpenCTI.
- Compatibility: Evaluation of compatibility with existing systems, tools, and protocols.
- Scalability: Assessment of OpenCTI's ability to scale with organizational growth and data volume.
- Deployment Considerations: Analysis of deployment options (on-premises, cloud-based) and associated technical challenges.
- Maintenance and Support: Evaluation of ongoing maintenance requirements and availability of technical support resources.

5. Security and Compliance

- Security Features: Overview of OpenCTI's security measures to protect data confidentiality, integrity, and availability.
- Compliance: Assessment of OpenCTI's compliance with relevant regulations and standards (e.g., GDPR, NIST).
- Data Privacy: Examination of how OpenCTI handles sensitive information and ensures privacy compliance.

6. Integration Potential

- Compatibility with Existing Tools: Evaluation of OpenCTI's ability to integrate with other security tools, such as SIEM, threat intelligence feeds, etc.
- API Capabilities: Analysis of OpenCTI's API functionalities for custom integrations with internal systems.
- Interoperability: Assessment of interoperability with industry-standard formats and protocols.

7. User Experience and Training

- Usability: Evaluation of OpenCTI's user interface and user experience for security analysts and administrators.
- Training Requirements: Identification of training needs for staff to effectively utilize OpenCTI.
- Support Resources: Availability of documentation, tutorials, and user communities for assistance.

8. Cost-Benefit Analysis

- Initial Costs: Estimation of initial setup costs including licensing fees, hardware/software procurement, and implementation expenses.
- Ongoing Costs: Assessment of recurring costs such as subscription fees, maintenance, and support.
- Benefits Analysis: Identification and quantification of potential benefits, such as improved threat visibility, faster incident response, and risk reduction.
- Return on Investment (ROI): Calculation of the ROI based on cost savings and risk mitigation benefits over a specified time.

9. Risk Assessment

- Technical Risks: Identification of potential technical challenges and risks associated with implementing OpenCTI.
- Organizational Risks: Assessment of organizational readiness, change management challenges, and stakeholder buy-in.
- Mitigation Strategies: Development of strategies to mitigate identified risks and challenges.

10. Alternative Solutions

- Evaluation of alternative solutions to OpenCTI, including other open-source and commercial threat intelligence platforms.
- Comparison of features, costs, and suitability to organizational requirements.

11. Conclusion

- Summary of findings and recommendations regarding the feasibility of implementing OpenCTI.
- Next Steps: Proposed actions for moving forward, including a timeline and implementation plan.

This outline provides a structured approach to conducting a feasibility study on implementing OpenCTI within an organization. Each section can be further elaborated with detailed analysis and findings based on the specific context and requirements of the organization.