FEASIBILITY STUDY: IMPLEMENTING OPENCTI

Redback Operations

Contents

1. INTRODUCTION

Purpose of the Study

The purpose of this feasibility study is to evaluate the potential benefits and challenges of implementing OpenCTI within Redback Operations. OpenCTI, an open-source threat intelligence platform, offers capabilities that could enhance the cybersecurity posture of the organization. This study will explore how OpenCTI can be integrated into the existing infrastructure, particularly to support the various cybersecurity teams—SecDevOps, GRC, Blue Team, Red Team, and Infrastructure Team—who are engaged in both defensive and offensive operations.

Background Information on OpenCTI

OpenCTI is designed to collect, organize, and visualize cyber threat information from multiple sources, providing a unified platform for managing and analyzing threat intelligence. It supports various formats, including STIX/TAXII, and offers API integration capabilities, making it a flexible tool for threat intelligence sharing and collaboration. Given Redback Operations' emphasis on cybersecurity, including monitoring and incident response activities, OpenCTI's features could significantly enhance the team's ability to detect and respond to threats.

2. OBJECTIVES

Primary Goal

To determine whether OpenCTI can effectively support and enhance the threat intelligence capabilities of Redback Operations, aligning with the specific needs of ongoing projects and cybersecurity initiatives.

Specific Objectives

- Enhance Threat Visibility: Improve the organization's ability to detect and understand emerging cyber threats by consolidating threat data in a centralized platform.
- Improve Incident Response: Facilitate faster and more informed decision-making during incidents through real-time access to relevant threat intelligence.
- Support Collaboration: Enable seamless collaboration among different cybersecurity teams by providing a shared platform for threat data.
- Align with Organizational Growth: Ensure that OpenCTI can scale with Redback Operations as it takes on new projects and handles increasing volumes of threat data.

3. FUNCTIONAL ANALYSIS

Overview of OpenCTI's Features

- Data Aggregation: OpenCTI aggregates threat intelligence from multiple sources, including internal logs, external threat feeds, and manual inputs, into a unified database.
- Threat Visualization: The platform offers powerful visualization tools, including graphs and dashboards, to help users understand the relationships between different threats.
- Automated Sharing: OpenCTI can automate the sharing of threat intelligence across teams and systems, ensuring that all relevant parties have access to the latest information.
- Integration with Existing Tools: OpenCTI supports integration with other cybersecurity tools, such as SIEMs, through its API, allowing for automated data flow and response.

Comparison with Organizational Requirements

- Cybersecurity Team Needs:
    - Blue Team: Focused on defensive operations using tools like SIEM, Nagios, and Wazuh, OpenCTI could provide enhanced threat intelligence that integrates directly into these tools.
    - Red Team: Engaged in penetration testing and vulnerability assessments, the Red Team could benefit from the latest threat intelligence to simulate real-world attack scenarios.
    - SecDevOps: Tasked with integrating and deploying security tools, the SecDevOps team could use OpenCTI to ensure that deployed systems are aligned with the latest threat landscapes.
- Project-Specific Needs:
    - VR SunCycle and Wearable Technology Projects: These projects may involve collecting and processing sensitive data, making them potential targets for cyber threats. OpenCTI can help in identifying and mitigating such risks by providing relevant threat intelligence.

Key Features Aligned with Organizational Needs

- API Integration: Essential for integrating OpenCTI with existing tools used by various teams.
- Real-Time Threat Sharing: Supports faster incident response, which is critical for both offensive and defensive cybersecurity teams.

- Scalability: Important to ensure that OpenCTI can grow alongside Redback Operations as it expands its project portfolio and cyber operations.

4. TECHNICAL ASSESSMENT

System Requirements

- **Existing Infrastructure**: Redback Operations currently relies on virtual machines (VMs) provided through Deakin University's VPN and other remote resources. Therefore, the implementation of OpenCTI will need to leverage this existing infrastructure rather than deploying on traditional on-premises servers or cloud platforms.
- **Software Dependencies**: OpenCTI operates on Linux distributions and requires additional software such as PostgreSQL, Elasticsearch, and Redis. The technical team must assess whether these can be accommodated within the existing VM infrastructure.
- **University's VPNcture**: The network infrastructure, particularly the use of Deakin University's VPN, will need to support the secure and efficient operation of OpenCTI. This includes ensuring that data transfer between VMs and other integrated tools (like SIEM, Wazuh, and Nagios) is secure and dependable.

Compatibility

- **Existing Systems**: OpenCTI must be compatible with the tools and systems currently in use within Redback Operations, which are primarily accessed through VMs. This includes ensuring that the VMs have the necessary resources and configurations to support the platform.
- **Protocols**: OpenCTI's support for industry-standard protocols such as STIX/TAXII is crucial for its integration with Redback's existing tools and external threat intelligence feeds.

Scalability

- **Infrastructure Constraints**: Given the reliance on VMs and the university's infrastructure, scalability will depend on the available resources within this environment. The feasibility of expanding the infrastructure (e.g., increasing the number of VMs or their resources) must be assessed.
- **Organizational Growth**: As Redback Operations grows and potentially takes on more complex cybersecurity projects, the infrastructure supporting OpenCTI must be flexible enough to scale accordingly. This could involve negotiating additional resources from the university or optimizing the use of existing VMs.

Deployment Considerations

- **Leveraging Existing VMs**: Rather than deploying on new on-premises or cloud infrastructure, OpenCTI can be deployed within the existing VM environment provided by Deakin University. This approach minimizes additional costs and complexity.
- **Technical Challenges**: Potential challenges include ensuring that VMs have sufficient resources to handle OpenCTI's requirements, managing data security across VMs, and maintaining performance within the constraints of the university-provided infrastructure.

Maintenance and Support

- **Ongoing Maintenance**: Maintenance will involve managing OpenCTI within the VM environment, ensuring that software dependencies are kept up-to-date, and that performance remains optimal. The IT support team must be familiar with the VM environment and how to maintain OpenCTI within it.
- **Technical Support**: Given the open-source nature of OpenCTI, community support will be valuable, but in-house expertise will also be crucial for handling day-to-day operations and troubleshooting within the VM environment.

5. SECURITY AND COMPLIANCE

Security Features: The security assessment will need to consider the protections provided by the university's VM environment and VPN. Focus on how OpenCTI's security features, such as encryption and access controls, can integrate with or enhance the existing security measures provided by the VMs.

Compliance: Compliance considerations will be based on how OpenCTI operates within the VM environment. Ensure that the VM infrastructure meets relevant compliance standards (e.g., data residency, access control) and that OpenCTI's deployment will not introduce compliance risks.

Data Privacy: Since the VMs and VPN are provided by Deakin University, data privacy measures must align with the university's policies. Assess how OpenCTI can maintain privacy and confidentiality within this shared infrastructure.

6. INTEGRATION POTENTIAL

Compatibility with Existing Tools: The integration of OpenCTI with tools like SIEM, Wazuh, and Nagios will need to be tested within the existing VM environment. Focus on how data flows between these tools within the VMs and whether any performance or security issues arise.

API Capabilities: The API integration will need to work within the constraints of the VM environment, including any limitations imposed by the university's network setup. Consider the feasibility of API calls across VMs and through the VPN.

Interoperability: Ensure that OpenCTI's interoperability with other tools is fully functional within the VM environment, considering any potential restrictions or performance impacts imposed by the university's infrastructure.

7. USER EXPERIENCE AND TRAINING

Usability: Training programs should focus on how users can effectively operate OpenCTI within the VM environment. This includes managing the application within VMs and understanding any specific requirements related to the university's infrastructure.

Training Requirements: The training must cover not only OpenCTI's functionalities but also the specifics of using it within the VM environment. This might include how to access OpenCTI via the VPN, manage resources within VMs, and troubleshoot common issues in this setup.

Onboarding: Onboarding will need to include instructions on accessing and managing OpenCTI through the university's VM infrastructure, ensuring all users are comfortable with this environment.

8. COST-BENEFIT ANALYSIS

Initial Costs: The cost analysis will reflect savings from not requiring new on-premises hardware or cloud services. Instead, the focus will be on any costs associated with configuring and optimizing the existing VMs for OpenCTI.

Ongoing Costs: Recurring costs might include additional VM resources if needed, but there will be no expenses related to maintaining physical hardware or cloud subscriptions.

Benefits Analysis: The benefits will include leveraging existing infrastructure to minimize costs, while still gaining enhanced threat intelligence capabilities through OpenCTI. This approach could also improve ROI by avoiding the need for significant new investments in hardware or cloud services.

9. RISK ASSESSMENT

Technical Risks: Risks will center on the limitations of the existing VM environment, such as performance constraints, resource availability, and potential integration challenges. Mitigation strategies will focus on optimizing the VM environment for OpenCTI.

Organizational Risks: Organizational readiness will include ensuring that all participants are comfortable working within the VM environment and that the necessary resources (both technical and human) are available to support OpenCTI in this context.

Mitigation Strategies: Strategies will include ensuring sufficient VM resources are allocated, providing specialized training for managing OpenCTI within VMs, and working closely with the university's IT team to address any infrastructure limitations.

10. ALTERNATIVE SOLUTIONS

- **Evaluation of Alternatives**:
  - **MISP (Malware Information Sharing Platform)**: MISP is an open-source platform like OpenCTI and should be evaluated for how well it can be integrated within the existing VM infrastructure. Given its flexibility, MISP could be a viable option if it aligns well with the current environment.
  - **ThreatConnect**: A commercial platform with advanced features, ThreatConnect should be assessed for its compatibility with the VM environment. Consider whether it is more complex feature set justifies the cost and effort needed to deploy it in the existing infrastructure.
  - **Anomali**: Another commercial solution, Anomali's suitability for deployment in the VM infrastructure must be considered. Its robust capabilities may offer significant advantages, but at a higher cost and potential complexity.

Comparison

- **Features**: The feature comparison remains unchanged, focusing on the capabilities of each platform.
- **Cost**: Acknowledge that the costs related to deploying these alternatives should now also factor in any challenges or benefits associated with the VM infrastructure.
- **Suitability**: Consider how well each alternative can be integrated into the VM environment, like the evaluation for OpenCTI.

11. CONCLUSION

Summary of Findings: The conclusion will reflect the suitability of OpenCTI for deployment within the existing VM environment. Emphasize that this approach maximizes the use of current resources while still providing the desired enhancements to threat intelligence capabilities.

Recommendations: Recommend moving forward with OpenCTI, with an implementation plan that includes careful testing and optimization within the VM environment.

Next Steps: The next steps will include working with the university's IT team to ensure the VMs are properly configured for OpenCTI and planning for a pilot phase to test the deployment in this environment.