Feasibility Study: Integrating Hayabusa into Redback Operations' Cybersecurity Framework

Redback Operations

Version	Modified By	Approver	Date	Changes made
1.0	Devika Sivakumar		15th September 2024	Feasibility Study: Hayabusa

Contents

1. Objectives

The primary objective of this study is to evaluate the feasibility of integrating Hayabusa, a Windows forensic tool, into Redback Operations' cybersecurity ecosystem, specifically with the existing Wazuh platform. The study explores how Hayabusa can complement Redback's current tools—such as Wazuh, Suricata, Nagios, and VirusTotal—and provide forensic capabilities that are currently lacking in Redback's infrastructure.

As Redback Operations manages various projects, such as VR Sun Cycle Smart Bike, Elderly Wearable Technology, Athlete Wearable Technology, Player Tracking, and BugBox, securing sensitive project data is critical. The Cybersecurity Team, tasked with defending these projects, can leverage Hayabusa's forensic abilities to enhance incident response, particularly in post-incident investigation and root cause analysis.

2. Current Infrastructure Overview

Redback Operations uses a cloud and virtualized infrastructure supported by various cybersecurity tools to monitor, defend, and respond to security incidents across different projects. The Cybersecurity Team operates within a structured environment, utilizing:

- Wazuh as the primary SIEM for log management and real-time threat detection.
- Suricata for network intrusion detection.
- Nagios for monitoring system health and server performance.
- VirusTotal integrated with Wazuh to scan files and logs for malware.

Each project, from Project 1: VR Sun Cycle Smart Bike to Project 5: BugBox, has unique data collection, storage, and processing needs, ranging from IoT data streams to real-time player tracking systems. Given the scope and variety of these projects, the Cybersecurity Team often handles large volumes of logs, particularly from Windows-based systems. While Wazuh and Suricata do an excellent job of identifying threats in real-time, forensic analysis to determine how an attack unfolded or how a breach occurred is limited without a dedicated tool like Hayabusa.

3. Technical Feasibility: Integrating Hayabusa with Wazuh

Integrating Hayabusa with Wazuh is both technically feasible and strategic. The two tools complement each other: while Wazuh provides comprehensive log management and real-time alerts, Hayabusa dives deeper into Windows Event Logs, which are vital for incident response and forensic investigations.

Integration Points:

- Forensic Analysis: Wazuh can trigger Hayabusa to analyze specific Windows Event Logs when an alert is raised. This gives the Cybersecurity Team detailed insights into system behavior and potential misconfigurations that could have led to an incident.
- Automated Workflows: Hayabusa can be integrated into Wazuh's automated workflows. For instance, when Wazuh detects an anomaly on a Windows system, Hayabusa can be deployed to conduct deeper analysis without human intervention.
- Unified Dashboard: Data from Hayabusa can be visualized in the Wazuh dashboard, allowing analysts to view both real-time events and detailed forensic logs in one place.
- Threat-Hunting: Hayabusa provides critical forensic data that can be analyzed over time, feeding into threat-hunting strategies, and helping to identify patterns that may otherwise go unnoticed by Wazuh.

The integration does not require overhauling the existing infrastructure and can be implemented by configuring Wazuh to support custom log analysis scripts. Moreover, since the Cybersecurity Team is already proficient with Wazuh, adding Hayabusa would require minimal additional training.

4. Benefits of Adding Hayabusa

Integrating Hayabusa into Redback's cybersecurity ecosystem will provide significant benefits, particularly for the Cybersecurity Team in terms of forensic analysis and post-incident investigation.

Key Benefits:

1. Enhanced Forensic Capabilities: Hayabusa will enable the team to conduct in-depth investigations into security incidents by analyzing Windows Event Logs that go beyond what is currently visible through Wazuh's real-time alerts. This will help identify the root causes of incidents, especially for projects like BugBox, where user session data might be targeted.
2. Improved Incident Response: The Cybersecurity Team can react more effectively to threats by analyzing logs from compromised systems. For example, in Project 2: Elderly Wearable Technology, any anomaly in IoT device data transmission can be investigated for hidden attacks that evade real-time detection.
3. Integration with Wazuh for Streamlined Workflows: Hayabusa's outputs can be integrated into Wazuh's alerting mechanisms, ensuring that real-time security events and post-incident forensic data are accessible from a single pane of glass. This enhances the efficiency of incident response workflows.
4. Long-Term Threat-Hunting: By adding Hayabusa to the threat-hunting toolkit, the Cybersecurity Team can leverage forensic data to track advanced persistent threats (APTs) and study the attack patterns across projects. This is critical for projects like

Athlete Wearable Technology, where personal and performance data must be protected.

5. Alignment with Compliance Requirements: For projects dealing with sensitive data, such as Elderly Wearable Technology (Project 2) and Player Tracking (Project 4), Hayabusa's forensic capabilities will strengthen compliance with data protection standards, including GDPR and NIST 800-53.

5. Risks and Challenges

Despite the potential benefits, there are several risks and challenges associated with the integration of Hayabusa.

Performance Impact: Running forensic-level analysis on large volumes of Windows Event Logs can introduce latency, particularly in high-traffic environments such as the Player Tracking project. The team must carefully balance the depth of forensic analysis with system performance.

Data Storage and Management: With the increased logging from Hayabusa, there will be a significant growth in the volume of forensic logs that need to be stored and managed. The Cybersecurity Team will need to assess whether Redback's current data storage infrastructure can handle this additional load.

Training Needs: While Hayabusa is intuitive, the Cybersecurity Team will need to undergo training to ensure that they are able to effectively utilize its advanced forensic features. This could initially slow down operations as the team adapts to new workflows.

False Positives: Misconfigurations in log analysis or thresholds can increase the number of false positives generated by Hayabusa. This can be mitigated through careful tuning and by leveraging Wazuh's real-time event correlation to focus forensic efforts on true threats.

6. Alternative Solutions

If integrating Hayabusa presents significant challenges, alternative solutions should be considered:

- Velociraptor: An open-source alternative with a focus on endpoint monitoring and digital forensics. It provides similar benefits to Hayabusa but with a lighter footprint.
- GRR Rapid Response: A Google-developed tool optimized for large-scale forensic analysis, particularly useful if Redback's project data volumes increase in the future.
- Enhanced Wazuh Usage: Wazuh's native forensic capabilities could be further exploited, though it would not provide the deep, detailed forensic analysis that a dedicated tool like Hayabusa or Velociraptor could offer.

7. Conclusion

The integration of Hayabusa into Redback Operations' cybersecurity framework presents a significant opportunity to enhance forensic capabilities, particularly for projects that generate large volumes of data or have sensitive user information. Wazuh will continue to serve as the core SIEM tool, while Hayabusa will provide post-incident forensic analysis, ensuring a well-rounded security posture.

For Redback's Cybersecurity Team, having Hayabusa integrated into Wazuh's workflows will streamline the investigation of Windows-based systems, provide better insights into system compromises, and aid in identifying long-term threats across projects such as Athlete Wearable Technology and BugBox. While there are some risks, such as performance impacts and increased data storage needs, these can be managed with proper planning and configuration.

Overall, integrating Hayabusa into the cybersecurity infrastructure is a feasible and beneficial step toward strengthening the company's ability to respond to and investigate security incidents, ensuring the integrity and security of Redback Operations' projects.

Appendix: Playbook Maintenance and Review The integration of Hayabusa into Wazuh should be reviewed bi-annually. This review will ensure that all configurations are optimized, and that the tool remains aligned with Redback's growing infrastructure. Training should also be updated annually, ensuring all Cybersecurity Team members can leverage Hayabusa effectively in incident response and forensic workflows.