Securing the Supernatural: Cybersecurity Implementation at the Mystery Shack

Task 2: Project Proposal

Richard Le

011672979

D490 Cybersecurity Graduate Capstone

Instructor Wendy Campbell

April 26th, 2024

Contents

Section A: Security Problem

This report proposes the integration of the endpoint protection platform Bitdefender GravityZone into the Mystery Shack infrastructure. The Mystery Shack (TMS), based in Gravity Falls, Oregon, is a popular tourist destination known for its intriguing and mysterious exhibits, has expanded its digital and physical infrastructure to include online merchandise sales, digital ticketing, and interactive displays. As of now, they have expanded to house two small museums along with their original humble shack, the Mystery Shack. However, the existing cybersecurity measures are rudimentary and not equipped to handle sophisticated cyber threats. This poses significant risks, such as data breaches, financial loss due to transaction fraud, and the potential compromise of unique digital content and customer privacy. The lack of robust cybersecurity threatens not only the financial health of the business but also its reputation among its global customer bases. To remedy this, Bitdefender GravityZone is an advanced cybersecurity platform tailored for small to medium businesses and protects endpoints, servers, and virtual environments across various networks, including physical, virtual, and cloud-based infrastructures. It offers a comprehensive suite of security features and capabilities aimed at safeguarding organizations against a wide range of cyber threats. Such features include Advanced Threat Protection, endpoint detection and response, risk analytics and hardening, antimalware analysis, firewall and web filtering, internal monitoring and reports, machine learning, and more (Bitdefender, n.d.b).

The Mystery Shack's main adversary is the anonymous hacker known as Bill Cipher. As an advanced hacker with malintent, Bill Cipher actively targets the Shack's cybersecurity posture to compromise the company's reputation and compliance. With increasing digital transactions and storage of financial and personal information, the TMS is vulnerable to cyber threats that could lead to data breaches, identity theft, and financial fraud due to their handling of cardholder

data. The environment's unique nature, involving both online and on-site interactions, makes it a potential target for various sophisticated cyber-attacks.

The CEO Stanley Pines is a money-loving greedster, similar to the Krusty Krab's Eugene Krabs. Therefore, the need for a solution such as Bitdefender is of utmost priority to save money. According to Palatty (2023), small businesses like The Mystery Shack experience approximately 43% of all cyber-attacks annually, and of that percentage about 46% of attacks were against small businesses with less than 1,000 employees. Palatty (2023) also states that small businesses spend between a range of $826 to $653,587 to recover from cybersecurity incidents. Due to TMS' recent losses and fines following their security breaches, CEO Stanley Pines is willing to allocate an appropriate budget for the implementation project and secure future finances.

There are various root causes to TMS' weak security posture since the company is hosted in the more rural town of Gravity Falls, Oregon. The first among them is outdated systems and software. TMS has numerous systems running EOL software like Windows 7, which are vulnerable to numerous known exploits. Bitdefender's automated patch management tools that ensure all software is up-to-date, significantly reducing the risk associated with outdated systems. TMS' second root cause is a lack of comprehensive security measures such as advanced threat detection. As a solution, Bitdefender GravityZone introduces a layered defense strategy with advanced threat protection (and endpoint detection and response capabilities. These features proactively detect, prevent, and respond to sophisticated threats before they can cause harm, ensuring a robust security posture. The third root cause is limited incident response capability with only just a few cybersecurity personnel. Bitdefender offers compensating controls as its incident response capabilities include automated response features to immediately isolate affected systems and threats. A fourth root cause for the weak security is TMS' exacerbation of

poor user security practices and awareness, such as susceptibility to phishing or weak security policies. Bitdefender GravityZone can help address this by including tools for policy enforcement that ensure things such as strong password policies, or by offering comprehensive security training modules. These features of Bitdefender help educate staff on the best security practices, thereby reducing the risk of breaches due to human error.

Section B: Stakeholders

1. **Stanley Pines, CEO**
    a. As the CEO, Stanley Pines' implementation involvement will oversee the entirety of the integration project. From a strategic perspective, he will ensure the solution aligns with business goals and needs. Stanley is critically affected by any financial implications of a security breach which would include legal fines and reputational loss among customers. His influence on the project is critical because his approval is necessary for budget allocations, infrastructure approvals, and major decisions with the project scope and objectives.
2. **Stanford Pines, CTO**
    a. Stanford Pines is Stanley's twin brother, designated Chief Technology Officer (CTO), and Research Head. Stanford is the main person responsible for all technological needs, supernatural research & development, and supernatural artifacts, which are the main attractions for TMS. His implementation involvement will provide technical insight for the integration of new cybersecurity solutions with existing research data systems. Stanford is critically affected due to the sensitive nature of his research data of the supernatural. Se Gravity Falls is the only location with supernatural occurrences, compromise of Stanford's data will damage the company's proprietary assets and information. Stanford's influence on the project is critical as he manages the network infrastructure and must ensure the solution meets rigorous standards required for research integrity.
3. **Dipper & Mabel Pines, COO's**

a. Twins Dipper & Mabel Pins are the Chief Operational Officers (COO's) for TMS and are actively involved in day-to-day implementation. Their involvement would be high as their responsibility ensure that operations continue smoothly without disruption from the new security measures. For the twins, the impact of a security breach would affect them highly as they hold high stakes in upholding operational integrity and customer satisfaction for in-person and online sales. As for their influence, the influence would be high because their feedback directly affects adjustments during the implementation phase to optimize user experience and operational efficiency.

4. **Sooz Ramirez, CMO**

a. Soos Ramirez is the Chief Maintenance Officer. His implementation involvement will oversee the maintenance of digital and physical infrastructure, ensuring that Bitdefender GravityZone will be effectively integrated into existing systems. The impact of the security problem is direct as any disruptions caused by a breach or attack will affect Soos' overall maintenance of TMS infrastructure and assets. Soos' project influence will be high due as his maintenance of both physical and digital systems is crucial for the smooth implementation and ongoing management of the cybersecurity solutions. His role involves ensuring that all systems are up-to-date and functioning optimally post-implementation, minimizing downtime, and ensuring that security updates are applied consistently and correctly.

5. **Wendy Corduroy, HR**

   a. As HR, Wendy's implementation involvement will include organization and delivery of training sessions related to new security protocols, systems, and software. Her impact from the security problem involves tasks to ensure all employees are adequately trained and compliant. This directly influences how effectively the security policies are implemented. Wendy has high influence on the implementation project as she must cultivate a security-aware culture. The effectiveness of her awareness training will affect overall security compliance and effectiveness for TMS.

6. **Mystery Shack's IT and Cybersecurity Team**

   a. The IT and Cybersecurity team's involvement will be active for the setup, configuration, and monitoring of the network infrastructure. Regarding the security problem's impact, their workload is directly affected by TMS's security landscape as an increase in security issues translates to more intensive monitoring and response requirements. As for their project influence, both teams are critical for the technical understanding of the solution and its rollout. The teams must adapt and extend their existing responsibilities to include configuring Bitdefender security settings, monitoring system logs for unusual activities, and applying security patches. Their ability to quickly learn and effectively manage these additional cybersecurity responsibilities directly influences the project's success and the Shack's security posture.

7. **Customers**

   a. The implementation involvement of customers is none/indirect. During the integration project, the focus is to safeguard personal and financial data. The

impact of the security problem for customers is significant since their personal and financial data is at risk of potential breaches. The customers' project will be indirectly significant as customer trust and satisfaction are paramount for the TMS's ongoing success and reputation.

8. **Regulatory Compliance Officers**
    a. Compliance officers' implementation involvement is to ensure alignment with legal and regulatory standards, such as Payment Card Industry Data Security Standard (PCI DSS). Compliance officers' security problem impact will be medium, se they will be affected for noncompliance and issue penalties, sanctions, or fines against TMS. Their influence on the project is high as they dictate the obligatory requirements shaping the integration and framework of the proposed solution.
9. **Financial Partners and Merchandise Suppliers**
    a. The implementation involvement for financial partners and merchandise suppliers is minimal se this project is mainly the integration of a cybersecurity software tool. However, their impact from the security problem is high se the parties will be affected by potential financial disruptions and data breaches. Their project influence is minimal to moderate as these parties request robust security to maintain smooth business operations and transactions.
10. **Local Government and Community Leaders**
    a. Local government's implementation involvement is moderate. This group of stakeholders will focus on how TMS maintains security obligations and impact on local community trust. Their impact from the security problem is moderate, where

some individuals may be at risk of damage from a breach. This party is mainly concerned for overall security and operational integrity of local businesses. This groups project influence is minimal for cybersecurity.

11. Cybersecurity Consultants and Vendors

a. Cybersecurity consultants and vendors, namely Bitdefender GravityZone as the vendor, help provide specialized knowledge regarding cybersecurity solutions and implementation. This stakeholder group's impact is high from the security problem as their reputation is directly tied to the success of their security solutions. If their solutions were inadequate in protecting clients, their businesses would become damaged. This group's project influence is high as well because their provided solutions are critical for achieving the desired businesses objectives.

Section C: Historical Evidence

The first piece of historical data for TMS's security posture is a previously conducted vulnerability assessment from 2 years ago. The below vulnerability report supports the decision to implement Bitdefender GravityZone as the ideal endpoint protection platform for integration.

The Mystery Shack Vulnerability Report

The Mystery Shack conducted this vulnerability assessment as part of its efforts to enhance cybersecurity infrastructure, leading up to the integration of advanced cybersecurity solutions such as antivirus and endpoint protection services. This assessment was carried out by an external, qualified cybersecurity firm following guidelines set forth in NIST 800-30 Rev 1 to identify the following:

- Vulnerabilities using the CVSS model
- Severity
- Likelihood of occurrence

Table A. Risk Classifications

Risk Level	Description
High	The loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability may have a serious adverse effect on organizational operations, assets, or individuals.
Low	The loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, assets, or individuals.

Table B. Severity (Based on CVSS Model)

Severity Level	**Description**
Critical	Exploitation likely results in root-level compromise without needing special credentials or knowledge about victims.
High	Difficult to exploit. May result in elevated privileges or significant data loss/downtime.
Medium	Requires manipulation of victims, or attacker must be on the same local network. Limited access gained from exploitation.
Low	Exploitation requires local or physical access, having little impact on the organization.

Table C. Level of Effort

Level of Effort	Description
High	Requires a high level of effort from critical teams, involving extensive changes that may risk service downtime.
Moderate	Requires a dedicated effort from teams, potentially impacting services or causing partial outages.
Low	Requires minimal effort, generally involving updates or simple commands with no impact on production services.

Table D. System Inventory

System Components:

- **Servers:** A mix of Windows Server 2019 and Ubuntu Linux across approximately 3 virtual servers hosting various roles including:
    - Web application servers (nginx, Apache Tomcat)
    - Database server (PostgreSQL)
- **Workstations:**
    - 10 units - Windows 7
    - 10 units - Windows 10
    - 10 units - Ubuntu Linux.
- **Networking Equipment:**
    - 2 Cisco 3750X switches
    - 2 Sophos XG firewalls
    - Verizon FIOS router (CR1000A)
- **Wireless Access Points:** 10x HPE JZ337A Aruba AP-535

Table E. Risk Identification

Risk #	Vulnerability (NVT Name)	NVT OID	Severity	Risk	Level of Effort
1	Outdated Anti-Virus Software Detection		High	High	Low
2	Operating System (OS) End of Life (EOL) Detection		Critical	High	Low
3	SQL Injection Vulnerability in Web Application		Critical	High	High
4	Phishing Susceptibility Test		High	High	Moderate
5	Unauthorized Wireless Access Points		High	High	Moderate
6	Misconfigured Firewall Rules		Medium	Moderate	Moderate
7	Weak Password Policy Detection		High	High	Moderate
8	Remote Desktop Protocol (RDP) Brute Force Vulnerability		High	High	Low
9	Insecure Direct Object References		Medium	Moderate	Low

Note: The specific NVT OIDs (Object Identifiers) for some vulnerabilities have been omitted and need to be determined by the IT team based on the network's specific configuration and software details.

Company Cybersecurity Tools:

Tool Name	Purpose
Sophos XG	Network Firewall
Duo	Multi-factor Authentication
Wireshark	Network Protocol Analyzer
Nessus	Vulnerability Scanner
Active Directory	Identity and Access Management

Conclusion:

This vulnerability report identifies significant security vulnerabilities that require immediate attention to prevent potential cyberattacks. The findings should guide the future integration of a comprehensive cybersecurity solution, highlighting the critical need for enhanced antivirus and endpoint protection to safeguard the Mystery Shack's digital and physical assets.

Section D: Project Phases

D1.

The Mystery Shack will be guided by several industry-standard methodologies to ensure the security solution is robust, effective, and compliant with regulatory standards such as NIST SP 800-53, PCI DSS, the Agile Project Management methodology, and the Information Technology Infrastructure Library (ITIL). As noted by Joint Task Force (2020), NIST Special Publication 800-171 provides a comprehensive set of security controls for an organization's information systems, aiding in guidance for the overall approach in managing and mitigating cybersecurity risks. For PCI DSS, any company that processes credit cards is subject to a set of specific security requirements to protect customer cardholder data, otherwise said company is subject to legal fines (Kim & Solomon, 2021). Se TMS handles customer transactions, PCI DSS is a necessary standard for continuing secure operations. Next, the Agile Project Management (APM) method approaches the development of a project with high flexibility, iterative progress through time allotted sprints, and continuous stakeholder involvement (Drumond, 2024). TMS will orporate this method for its ability to quickly adapt to changes, especially when new cyber threats emerge daily. Lastly, ITIL is a set of practices and policies which guide IT infrastructure management, development, and operations (Kim & Solomon, 2021). ITIL practices are applicable to TMS to manage the deployment, service transition, and ongoing maintenance of Bitdefender GravityZone's services.

D2.

The integration project will be rolled out into the following key sprint phases as per the APM methodology:

Phase 1: Planning and Assessment

- **Activities**: Conduct an initial vulnerability report and penetration test to determine cybersecurity posture and identify vulnerabilities. Data classification will also be determined based on data sensitivity and criticality. A security baseline will be established using NIST SP 800-53, PCI DSS, and ITIL controls. We will also engage stakeholders to develop the project scope and objectives to be clear and actionable.
- **Duration**: 4 weeks
- **Key Deliverables**: Security assessment report, penetration test report, data classifications, project scope document, and baseline configuration.

Phase 2: Configuration and Customization

Activities: Security team will configure Bitdefender GravityZone according to the security needs identified in the assessment phase. This phase will focus on implementing security controls from NIST SP 800-53 that ensure comprehensive coverage, including access controls, information protection processes, and security ident procedures. Additional measures of this phase are the purchasing of licenses or equipment to replace EOL assets of the network infrastructure. For example, Windows 10 Pro licenses will replace any Windows 7 system. Since the network also lacks proper firewalls, budget allocations will be set to adopt new firewall equipment. Customization measures and settings will be developed to protect payment information in compliance with PCI DSS.

Duration: 3 weeks

- **Key Deliverables**: Security settings implementation report, configuration management plan, Windows 10 Pro licenses, new firewalls.

Phase 3: Pilot Testing

- **Activities**: Purchase and provision VMware virtual machine licenses to mimic the TMS live environment. This helps assess the deployment Bitdefender GravityZone and the team's effectiveness of configurations, integration with existing systems, and the overall impact on system performance. Collect feedback from pilot users to identify any issues or areas for improvement, ensuring the pilot phase helps to refine the final rollout.
- **Duration**: 3 weeks
- **Key Deliverables**: VMware licenses, replica of live environment hosted on virtual machines, pilot testing report, feedback analysis report.

- **Phase 4: Full Deployment**
  - **Activities**: Implement Bitdefender GravityZone across all organizational systems and endpoints. Conduct comprehensive training for all staff on new security protocols, emphasizing the importance of data security and the specific measures implemented. Use ITIL principles to manage the rollout effectively, ensuring minimal disruption to ongoing services.
  - **Duration**: 3 weeks
  - **Key Deliverables**: Complete system deployment report, Breach Secure Now enrollment, staff training records

- **Phase 5: Monitoring and Optimization**
    - **Activities**: Establish continuous monitoring using Bitdefender's integrated tools to ensure compliance with NIST SP 800-53 and PCI DSS controls and to adjust configurations as needed based on threat intelligence and performance data. Regularly review system performance and security logs to detect anomalies and refine security measures. Utilize ITIL's Continual Service Improvement process to make iterative improvements based on operational feedback and emerging threats. Final compliance audits and another penetration test will affirm the success of the project.
    - **Duration**: Ongoing
    - **Key Deliverables**: Performance monitoring reports, an ongoing security awareness culture, post-project penetration test results, optimization and improvement logs, and compliance reports.

Criteria for Conclusion of Implementation:

The project is deemed complete when all systems are secured and meet several key benchmarks. The first benchmark is overall security coverage with Bitdefender GravityZone integrated with all infrastructure endpoints without operational disruption. The next benchmark is staff proficiency where all employees have completed the required security training and demonstrate understanding with new security protocols. The third key criteria is adherence to regulatory compliance under NIST SP 800-53 and PCI DSS with a final confirmed compliance audit. The last criteria for conclusion will be post-implementation reviews demonstrating system performance metrics. Such metrics will include high availability and uptime, security logs

indicating effective detection, and efficient response to potential threats. with NIST SP 800-53 and PCI DSS controls, all staff are trained, and the system passes a final security audit confirming compliance.

Project Management Methodology:

The implementation project will utilize a hybrid methodology between the APM and traditional project management methodology. This approach will have iterative development where the project is broken into sprints, allowing for regular reassessment of project goals and deliverables based on ongoing feedback or testing results. The Agile approach also allows for update meetings where all involved teams gather feedback and ensure the integration meets objectives, needs and requirements. Utilizing Agile principles, the project will feature regular sprint reviews, allowing for adjustments based on stakeholder feedback and real-time insights into the project's progress. Agile will integrate with traditional project management components of a phased rollout as noted by the above phases.

D3.

For the implementation of Bitdefender GravityZone at the TMS, it is crucial to thoroughly understand and proactively manage potential risks to ensure project success. Here is an in-depth analysis of the primary risks associated with this project, their potential impacts, and the strategies for their mitigation:

1. Compatibility Issues

- **Risk Description**: Potential compatibility problems between Bitdefender GravityZone and existing hardware or software systems, particularly with legacy systems or custom applications.

- **Impact**: Technical compatibilities could lead to system malfunctions, operational delays, or the need for additional resources to resolve issues, potentially raising project costs and extending timelines.
- **Mitigation Strategies**:
    - **Pre-Implementation Testing**: Conduct thorough compatibility tests during the planning phase to identify and address any potential issues before full-scale implementation.
    - **Vendor Collaboration**: Work closely with Bitdefender support teams to understand system requirements and receive assistance in configuring the solution to fit the specific infrastructure of the Mystery Shack.
    - **Contingency Planning**: Develop alternative plans for systems that may not be compatible, consider possible upgrades or the use of bridging technologies.

2. User Resistance

- **Risk Description**: Resistance from employees who are accustomed to the current system and may be reluctant to adapt to new security processes.
- **Impact**: User resistance can slow down the adoption process, reduce the effectiveness of the new security measures, and ultimately compromise security posture.
- **Mitigation Strategies**:
    - **Engagement and Communication**: Launch a comprehensive change management program that includes regular information sessions, demonstrations,

and discussions to educate employees about the benefits of Bitdefender GravityZone.

- **Training Programs**: Implement detailed training sessions with administrative staff tailored to different user groups, focusing on how the new system will make their tasks easier and improve security.
- **Feedback Mechanisms**: Establish channels for employees to voice concerns and provide feedback on the system, ensuring that their input is considered in the ongoing optimization process.

3. Budget Overruns

- **Risk Description**: The possibility of the project exceeding the allocated budget assigned by Stanley due to unforeseen expenditures such as additional hardware requirements, extended project timelines, or the need for external consultants.
- **Impact**: Budget overruns can strain financial resources, potentially forcing project scope reductions or compromising on solution quality.
- **Mitigation Strategies**:
    - **Detailed Budget Planning**: Start with a detailed budget that includes allowances for unforeseen expenses.
    - **Regular Financial Reviews**: Conduct regular budget reviews throughout the project lifecycle to monitor spending and adjust plans as necessary.

    - **Cost Management Measures**: Implement cost control measures and prioritize expenditures to ensure the most critical elements of the implementation are funded adequately.

4. Project Delays

- **Risk Description**: Delays due to various factors such as staffing issues, delayed deliveries, extended configuration or testing phases, or unexpected technical challenges.
- **Impact**: Delays can extend the time before security benefits are realized, leaving the Shack vulnerable to potential cyber threats.
- **Mitigation Strategies**:
    - **Realistic Timeline Setting**: Establish a realistic project timeline with buffer periods to accommodate potential delays.
    - **Resource Allocation**: Ensure adequate resources are allocated from the project's initial planning, including contingency plans for staffing and technical resources.
    - **Regular Progress Monitoring**: Implement strict project monitoring and control processes to keep the project on track and address any issues promptly.

By identifying and preparing for these implementation risks, the TMS can mitigate potential negative impacts on the project. By doing so, these measures ensure a smoother transition to Bitdefender GravityZone and a stronger security posture post-implementation.

Section E: Training Approach

A detailed, comprehensive training approach is necessary for the successful implementation of Bitdefender GravityZone into the security posture. The proposed training program will be designed to equip staff members with knowledge about the new solution, full detail on how to utilize Bitdefender effectively, information on new security policies and protocols, and an overall increase in cybersecurity awareness.

Beginning with the audience, there will be designated groups based on their roles within the company and their interactions with the IT systems. With the IT and cybersecurity teams, this group will receive the most technical training that includes system management, configuration, updates, and advanced troubleshooting on the solution. As for frontline employees and physical security staff, these groups will receive cybersecurity awareness including phishing recognition, safe system use, and basic security measures. The next audience group is administrative staff, who will focus on security practices related to their daily tasks, understanding security reports or alerts, and managing data securely within the company.

The delivery methods for the training program will be distributed by Wendy, head of HR. In order to accommodate schedules, learning preferences, and job functions, a variety of delivery methods will be implemented. The first method will be interactive workshops conducted by Bitdefender GravityZone experts, where groups such as IT, cybersecurity, and administrative staff may familiarize themselves with the solution. Additionally, hands-on simulation will be conducted for practicality and enable staff to have a comprehensive understanding for utilizing Bitdefender in response to real attacks. For non-technical staff, online training modules will be provided with self-paced courses covering general cybersecurity awareness. Online training modules will be hosted through a partner platform named Breach Secure Now, a recognized

leader in cybersecurity training which features including custom phishing simulations, self-paced training modules, weekly training content, and an employee secure score for monitoring awareness (Breach Secure Now, n.d.).

Training content within the program will begin with an organization-wide email from Wendy stating the need for Bitdefender GravityZone's integration and increase in cybersecurity awareness. The first key area of training content after will be an overview of Bitdefender GravityZone, introducing its features and capabilities. The next key area will be cybersecurity best practices as education on general cybersecurity threats such as phishing, malware, and safe internet practices. An overview of operational procedures will be a training focus as well. Daily procedures such as secure login practices, data handling, and understanding security alerts will be conducted for all staff with a focus on administrative roles. For IT and cybersecurity staff, specific training will be conducted to manage deep dives into Bitdefender GravityZone configuration, troubleshooting, updating systems, and monitoring security logs. Lastly, emergency response training will be included to prepare the IT and cybersecurity team for responding to security idents. This training will establish a line of communication, steps to mitigate risks, procedural protocols, and ident documentation.

The duration of the training program will be determined based upon the phases of the implementation project. There will be an initial intensive training scheduled before and immediately after the rollout for staff directly managing Bitdefender GravityZone. This phase will consist of multiple sessions over a two-week period to ensure efficiency with the new solution. As for other non-technical staff, ongoing, regular training sessions will be scheduled quarterly to cover updates, refreshers, and training for new employees. Breach Secure Now's training modules will also be a part of this ongoing training duration, as mentioned with their

weekly training modules and phishing simulations. Moreover, ad-hoc sessions may be conducted especially after significant system updates or in response to new emerging threats. By the end of the initial training program, monitoring and evaluation data will be gathered to assess feedback on the training process.

Section F: Project Phase Resources

A variety of resources are necessary to successfully implement the project including human resources, technological requirements, financial budgets, and time allocations.

Within the Planning and Assessment phase, the first resource to address is the allocation and cost of Bitdefender GravityZone licenses. With 30 current devices in the infrastructure, we will choose to buy 50 licenses to allow for spare flexibility in case TMS introduces future new systems. According to Bitdefender (n.d.a), the cost of 50 Bitdefender GravityZone Business Security Premium licenses totals to $1508.49, a cost-effective price due to the vendor's current 30% spring sale. This business subscription is valid for 1 year, after which point the C suite will review and decide to continue utilizing its services. The rationale for selecting the Business Security Premium license is due to TMS's size as a small to medium business. Business Security Premium is engineered towards these smaller companies seeking aggressive cyber defense from sophisticated attacks. Next, would be the cost of a new vulnerability assessment and penetration test from external parties. Since the historical vulnerability report is 2 years old, it is necessary to gauge TMS' current infrastructure in order to properly plan during the stakeholder meeting. As noted by Baran (2023), the average cost of an external penetration test ranges from between $5,000 to $20,000, with price factors including network complexity, number of public-facing systems, and other infrastructure services. Regarding vulnerability assessments, Cole (2023) details how the average range of an external vulnerability assessment is between $1,000 to $10,000. Price factor variables include frequency of assessments, the option for vulnerability management, and scope of the assessment. TMS is not in demand for the add-on vulnerability management service, however the company will need regularly occurring assessments to ensure perseveration of their security posture. A last resource for this phase are the free live webinars

for Bitdefender training. According to Bitdefender (n.d.b), the company hosts free live webinars for TMS's technical team to increase their technical skill in configuration and management of the platform.

The next project phase, Configuration and Customization, will address potential upgrades for EOL hardware, EOL software, and configuration tools. The purpose of this project phase is to prepare the infrastructure for the solution's implementation. The change in network systems begins by purchasing Windows 10 Pro licenses to replace the existing Windows 7 systems. According to CDW (n.d.a), the cost of purchasing 10 Windows 10 Pro licenses is $1849.90. The team will also need to mimic the live environment to accurately test the security configurations. To achieve this, virtual machine licenses will be purchased to create the complex pilot testing environment and will be constructed by the CTO, Stanford. A total of 7 licenses, $199 each, will be purchased for the 2 web servers, 1 database server, and 4 workstations costing $1,393 (VMware, n.d.). Another necessary resource is the eLearning Bitdefender platform. There, the company posts free live webinars and online modules will constantly be referred to as the rollout is deployed so the technical teams may understand in depth any misconfigurations or errors (Bitdefender, n.d.b). Finally, the ITIL best practices will also be referenced during the implementation as these guidelines enhance operational efficiency and security.

The Pilot Testing project phase primarily is where the IT and cybersecurity teams will initially test Bitdefender GravityZone's capabilities and simulate various operational scenarios. Under the guidance of the CTO, this phase validates the security configurations and operational workflows without impacting the live environment. Since this will happen within the virtual machine environment, all required resources for this phase include the Bitdefender licenses,

VMware licenses, and Bitdefender training modules from their eLearning platform. No other resources would be necessary.

Onto the Full Development project phase, this phase encompasses the delivery of cybersecurity training and Bitdefender GravityZone rollout. For a monthly subscription, Breach Secure Now will charge TMS $99 for their training services (Breach Secure Now, n.d.). Human resources such as the CTO, IT team, and security team will manage the rollout of Bitdefender GravityZone onto company systems. As the rollout begins, the technical teams will adhere to the ITIL resource to adopt best practices and ensure a smooth transition. An additional resource is the eLearning Bitdefender platform previously mentioned in the Configuration and Customization phase. The training content will be repetitively utilized during and after deployment. Finally, the ITIL best practices will also be referenced during the implementation as these guidelines enhance operational efficiency and security.

Lastly the Monitoring and Optimization phase, the company must establish continuous monitoring using Bitdefender's integrated tools, adherence to compliance, and promote an ongoing culture of security awareness. The first required resource are the internal tools of the Bitdefender GravityZone platform, such as integrity monitoring, automated correlation and analysis, and machine learning (Bitdefender, n.d.a). These internal performance monitoring provides continuous insight for the CTO and cybersecurity team to maintain a stable security posture. Some services act as charged add-ons, but the price will vary based upon business size, infrastructure layout, and scalable demand from the business. A second resource to properly promote security awareness is the previously mentioned Breach Secure Now platform, which has weekly training and micro-training modules for employees (Breach Secure Now, n.d.). Ongoing mandatory use of the platform encourages healthier awareness among employees of popular

cyber threats to lookout for. The third resource for this phase's success is the utilization of ITIL best practices, specifically the Continual Service Improvement process to systematically evaluate and enhance operations based on feedback and emerging threats. These will aid in gathering documentation of all updates applied to the infrastructure, including security patches and system enhancements. The ITIL practices will also help with documenting optimization and improvement logs of all changes made to improve system performance and security, along with rationales based on the collected data. Furthermore, an additional post-project penetration test will be conducted to affirm the overall success of implementation and Bitdefender's defense capabilities. As such, the price is again between $5000 to $20,000 as noted by Baran (2023). A last resource for this phase is the passing of the compliance audit questionnaire. According to Glover (n.d.), any business that isn't categorized as Level 1, meaning over 6 million annual transactions, is not required to pass a compliance report with an onsite audit by a Qualified Security Assessor. Therefore, TMS's required resource is to pass the PCI DSS self-assessment, costing between $50 to $200 (Glover, n.d.). They may also need to obtain training and policy development if TMS were to not pass with $70 per employee (Glover, n.d.).

Section G: Final Project Deliverables

Once the implementation project is complete, there are various final project deliverables to ensure TMS's immediate needs are met for enhancing cybersecurity. The first among them is comprehensive software and licensing documentation, which includes a record of all license purchases, renewal dates, and compliance with software licensing agreements. Additionally, detailed network diagrams and system architecture will be updated to reflect the post-project environment.

The next set of deliverables are logs and manuals. Installation and configuration logs will detail the step-by-step setup and adjustments made, capturing issues and resolutions to serve as a reference for future maintenance or troubleshooting. Then throughout the project, an ongoing development of updated security policies and procedures manual will be created and guide daily operations or emergency responses. This manual is complemented by robust training materials and user manuals designed to facilitate the effective use of Bitdefender GravityZone for current or new hires of the IT and cybersecurity teams to reference.

Additionally, testing reports from the pilot phase and post-full development phase will offer performance benchmarks, security testing outcomes, and training feedback for staff's security awareness. The subsequent analysis provides insight for system optimizations prior to full deployment. Furthermore, the ongoing training of Breach Secure Now will promise delivery of a security aware work culture within TMS as well. More deliverables are compliance documentation and audit reports confirming adherence to NIST SP 800-53 and PCI DSS regulatory standards, ensuring the implementation meets all mandatory security frameworks.

Among the last deliverables are a project review document, where it will encapsulate feedback from stakeholders and lessons learned, providing valuable insights for continuous improvement. Finally, the project will establish continuous monitoring reports from Bitdefender GravityZone's internal monitoring tools. These tools will generate initial reports that benchmark the system's performance against security threats.

G1.

Phase	**Start Date**	**End Date**	**Duration**	**Key Resources**
Planning & Assessment	5/1/2024	5/28/2024	4 weeks	- Bitdefender licenses - Penetration test reports - Vulnerability assessment reports - Project scope document
Configuration & Customization	5/29/2024	6/18/2024	3 weeks	- Windows 10 licenses - Bitdefender licenses - VMware licenses - Bitdefender eLearning platform
Pilot Testing	6/19/2024	7/9/2024	3 weeks	- VMware licenses - Bitdefender licenses - Bitdefender eLearning platform
Full Deployment	7/10/2024	7/31/2024	3 weeks	- Breach Secure Now (BSN) subscription - ITIL best practices
Monitoring and Optimization	8/1/2024	Ongoing	Ongoing	- Bitdefender integrated monitoring tools - ITIL continuous improvement practices - Ongoing BSN training - Compliance asessors/assessments - 2nd penetration test

Section H: Project Evaluation Approach

H1.

The formative testing process occurs during the implementation or Full Deployment phase of the project. Throughout the phase, continuous checks and adjustments will be made to ensure all configurations within Bitdefender GravityZone function as intended as per project specifications. The required tools will include Bitdefender's internal real-time monitoring software, internal audits, and configuration management checks. Procedures for formative testing will focus on system configuration with Bitdefender training modules, accurate security settings, and the integration with existing infrastructure during the Pilot project phase.

In regards to summative testing, this will take place after the Pilot project phase and throughout the Monitoring and Optimization phase. Summative testing evaluates the overall success of the implementation project and state of the security posture. The testing checks if the project meets the established goals and requirements. The summative test procedures and tools will include internal Nessus vulnerability scans, performance reviews, penetration tests conducted by external experts, and compliance audits to ensure adherence to standards like PCI DSS and NIST SP 800-53. It will also include staff feedback from ongoing use of the cybersecurity training platform BSN.

H2.

Minimal Acceptance Criteria: These criteria are minimal standards that the project must meet to be considered successful. For the Bitdefender GravityZone implementation, these include:

- No critical vulnerabilities as identified by post-implementation vulnerability scans.
- All system components must comply with PCI DSS and NIST guidelines.

- System downtime during deployment must not exceed the agreed threshold.

Key Performance Indicators:

- Reduction in the number of security incidents reported.
- Compliance with all applicable regulatory requirements.
- User satisfaction rates with the new system, Employee Secure Score for cyber-training within BSN.
- System performance metrics such as response time and resource utilization.

H3.

The test cases and scenarios occurring during the Pilot Testing and Full Deployment phase are designed to mirror real-world cyber threats that TMS might face, ensuring the security solutions are robust and practical. Scenarios will include:

- Simulated phishing attacks to test the effectiveness of new training and email filtering.
- Attempted breaches using known vulnerabilities to verify the system's ability to detect and respond to attacks.
- Common malware attacks to verify Bitdefender's malware signatures and its ability to automatically remove such threats.
- Load testing to assess system performance under peak loads, which is crucial for the tourist-heavy operations of the Mystery Shack.

These scenarios are justified as they replicate potential security threats for TMS's unique environment, providing a realistic and comprehensive test of the security infrastructure.

H4.

Results from both formative and summative testing phases will be analyzed using a combination of quantitative and qualitative methods. As for the quantitative analysis, it involves statistical review of system logs, performance metrics, and incident report data. This numerical data assesses whether the implementation meets the quantitative KPI's and minimal acceptance criteria.

Qualitative analysis relies on feedback from staff and management regarding Bitdefender usability, intrusiveness, and effectiveness. The analysis also reviews findings from compliance audits and penetration test feedback to obtain expert insights for the new network security posture.

References

Baran, E. (2023, May 16). *Pricing Insights – How Much Does Penetration Testing Cost?* Blaze Information Security. https://www.blazeinfosec.com/post/how-much-does-penetration-testing-cost/#:~:text=External%20penetration%20testing%20costs%20can,access%20to%20an%20organization's%20network.

Bitdefender. (n.d.a). *GravityZone Business Security Premium.* Bitdefender. https://www.bitdefender.com/business/products/gravityzone-premium-security.html

Bitdefender. (n.d.b). *Learning @ Bitdefender.* Bitdefender. https://elearning.bitdefender.com

Breach Secure Now. (n.d.). *Partner Subscription*. Breach Secure Now. https://www.breachsecurenow.com/partner-subscription/

CDW. (n.d.a). *Windows 10 Pro - upgrade license - 1 device.* https://www.cdw.com/product/windows-10-pro-upgrade-license-1-device/3446584?pfm=srh

CDW. (n.d.b). *Sophos XGS 116/126/136 Next Generation Firewall Appliance with 5G Add-On Module.* https://www.cdw.com/product/sophos-xgs-116-126-136-next-generation-firewall-appliance-with-5g-add-on-mo/7348338?pfm=srh

Cole, N. (2023, May 8). *How Much Should a Vulnerability Assessment Cost in 2023?* Network Assured. https://networkassured.com/security/vulnerability-assessment-cost/

Drumond, C. (2024). *Agile Project Management - What is it and how to get started?.* Atlassian. https://www.atlassian.com/agile/project-

management#:~:text=What%20is%20agile%20project%20management,customer%20feedback%20with%20every%20iteration.

Glover, G. (n.d.). *How Much Does PCI Compliance Cost?* Security Metrics. https://www.securitymetrics.com/blog/how-much-does-pci-compliance-cost

Johnson, R., Weiss, M., & Solomon, M.G. (2022). *Auditing IT infrastructures for compliance* (3rd ed.). Jones and Bartlett Learning. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3370743&site=eds-live&scope=site&authtype=sso&custid=ns017578&ebv=EK&ppid=Page-__-42

Joint Task Force. (2020). *Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-53r5

Kim, D. & Solomon, M.G. (2021). *Fundamentals of information systems security* (4th ed.). Jones and Bartlett Learning. https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/detail.action?docID=6741186

Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J., & Walden, D. (2023, August 28). *Building a Cybersecurity and Privacy Learning Program.* National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/50/r1/ipd

Palatty, N. J. (2023, December 22). *51 Small Business Cyber Attack Statistics 2024 (And What You Can Do About Them).* Astra. https://www.getastra.com/blog/security-audit/small-business-cyber-attack-

statistics/#:~:text=Small%20businesses%20account%20for%2043,with%201%2C000%20or%20fewer%20employees.

SBA. (2024, April 4). *Strengthen Your Cybersecurity.* U.S. Small Business Administration. https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

VMware. (n.d.). *VMware Workstation 17 Pro.* https://store-us.vmware.com/vmware-workstation-17-pro-5709912600.html