Securing the Supernatural: Cybersecurity Implementation at the Mystery Shack

Task 3: Post-Implementation Report

Richard Le

011672979

D490 Cybersecurity Graduate Capstone

Instructor Wendy Campbell

April 30th, 2024

Contents

Section A: Policies

With the integration of Bitdefender GravityZone into The Mystery Shack's (TMS) infrastructure, new cybersecurity policies are set to be established to prevent a habitual lapse to the company's weak security posture.

First and foremost, one of the most important implemented policies is least privilege. This policy mandates that those within TMS may only access the most minimal amount of company information and resources necessary to perform their designated job functions. Access controls will be rigorously enforced, with user roles and permissions regularly reviewed and adjusted. Naturally, only a limited number of administrative privileges will be given to authorized personnel and will grant authorization at their discretion. By incorporating least privilege, we minimize the possibility of data breaches and unauthorized access by intentional and unintentional malicious actors.

As part of the Payment Card Industry Data Security Standard regulation (PCI DSS), encryption policies for both data-in-transit and data-at-rest is an obligatory requirement for data confidentiality and integrity. This policy will mandate all sensitive data including personal information, transaction details, and cardholder information, will be encrypted with up-to-date encryption protocols such as AES-256. Encryption keys will be managed securely and only managed by administrators. Data encryption ensures regulatory compliance prevents unauthorized data access by protecting confidentiality in the event of a data breach.

Since the pre-implementation security awareness among the company was low, moving forward a user awareness and training policy will be enforced. This policy compliments the introduction of the cybersecurity training platform Breach Secure Now (BSN) introduced from

the project rollout. A reference metric within the BSN platform is an Employee Security Score (ESS) which reflects a user's competent knowledge for various security awareness. An additional report is generated with the user's mistakes against recognized phishing campaigns. The user training policy will state that a user's ESS score and phishing scores must meet above a certain threshold, otherwise they are subject to additional training. Continuous failure to meet score thresholds will result in employee suspension or eventual termination. Overall, this policy enhances TSM's cybersecurity awareness and keeps employees up-to-date with recognizing emerging security threats, leading to a decrease in breaches.

Lastly, a final policy will be continuous monitoring and incident response. The introduction of Bitdefender GravityZone is a courageous endeavor, the first major cybersecurity solution implemented into the infrastructure. Thus, the reevaluation of system monitoring and incident response must take the solution into account when responding to security incidents. The policy will provide multi-layered structures regarding incident response, continuous monitoring, threat detection, and post-incident analysis utilizing Bitdefender GravityZone as a significant response tool. The policy improves the response team's ability proactive and reactive ability for security incident detection and response, leading to the decrease of company fines and damages.

A1.

The implementation of the above policies enhances cybersecurity decision-making such as strategic risk management, operational efficiency, and regulatory compliance. Bitdefender GravityZone's implementation strategizes risk management and data analysis as it provides real-time insights into threats and system vulnerabilities with its advanced library of threat information, allowing technical staff to quickly make informed decisions. This immediate responsiveness is critical for breach prevention or reducing the impact of ongoing attacks.

Additionally, Bitdefender's automation of certain routine security tasks, such as patch management and encryption key rotation allow more free time for technical staff to pivot their focus to other security concerns. An increase in operational efficiency among technical staff aids in faster response times to real-time threats or proactive security improvements. As for regulatory compliance, Bitdefender features in-house compliance features and reports allow for better insight into an organization's compliance-related activities and helps guide them towards regulatory adherence. This helps TMS maintain ongoing compliance even after the implementation project and reduces legal risks.

Section B: Cybersecurity Assurance Criteria

The Bitdefender GravityZone implementation for TMS houses numerous in-house tools for strengthening the company's security posture through automation, modernization, and adoption of industry-standard tools.

As an advanced endpoint protection platform, Bitdefender GravityZone brings extensive automation capabilities to TMS' cybersecurity efforts such as advanced threat detection and response, patch management, and policy enforcement. Bitdefender's advanced machine learning algorithms and behavioral analytics automatically detect known real-time threat signatures or patterns. This capability ensures incidents are mitigated quickly without wasting the time or effort of a manual diagnosis by a cybersecurity analyst, allowing for rapid protection against sophisticated attacks. Bitdefender's automated patch management tools detects outdated software among its agents and provisions rapid patch management to ensure all operating systems and applications are up-to-date. Next, Bitdefender's in-house tools allow for the creation of security policies and automatic enforcement amongst its agents. Example policies of Bitdefender's automatic capabilities may include strong password use, secure network configurations, or application blacklisting, thereby minimizing TMS' attack surface.

Bitdefender proactively prepares for current and future cybersecurity challenges by bridging security absences and modernizing its clients' security infrastructure. One method how Bitdefender achieves this is its advanced antimalware protection through machine learning to detect new, emerging threats. The next-generation antimalware is continuously updated with the latest industry threat signatures, allowing for TMS to expand its digital footprint without minimal fear of outdated security measures. Moreover, Bitdefender's endpoint detection and response (EDR) capabilities provide detailed visibility into threat activities and faster remediation.

Without the solution's insights, TMS cybersecurity analysts would manually need to detect and response to incidents with less knowledge into these numerous threats. An extension of this feature is Bitdefender's risk analytics and hardening of the network infrastructure. It achieves this by continuously assessing the network security posture, identifies vulnerabilities, then suggests actionable insights for hardening, thereby modernizing the overall security defenses against potential attack vectors compared to TMS' previously manual inspections.

The adoption of Bitdefender GravityZone aligns TMS with current industry standard tools and methods in cybersecurity such as compliance, infrastructure integration, and a scalable security architecture. Bitdefenders feature such as EDR, advanced threat protection, policy enforcement, and more are designed to meet and exceed the security controls detailed within NIST SP 800-53, an industry recognized document that outlines frameworks for protection of data and systems (Bitdefender, n.d.b). Such controls within the NIST 800-53 include access controls, risk management, system monitoring, etc. (Joint Task Force, 2020). The advanced encryption and automated patch management of Bitdefender aligns with PCI DSS as this standard obligates a company's use of protection of cardholder data and maintenance of a vulnerability management program (Kim & Solomon, 2021). As for the implementation of industry-standard infrastructure, Bitdefender GravityZone is designed to seamlessly integrate with any company's existing IT infrastructure whether its physical, virtual, or cloud-based due to the solution itself being cloud-based. This added flexibility allows for the integration of its industry-standard protection across all environments without compatibility issues. Additionally, the platform offers high scalability of an environment which is applicable to TMS' growing business. When companies like TMS expand, the integration of additional security tools is seamless as the necessity arises with the emerging cybersecurity landscape.

Section C: Data Collection and Implementation

As a security solution, how Bitdefender GravityZone collects digital evidence of its user agents is paramount to address for security concern and transparency. According to Bitdefender (n.d.c), within every installed user agent, the solution collects data repositories and categorizes them with the Investigation tab for forensic data, Scan Logs tab for scan details, General tab for numerous status updates of the endpoint. Bitdefender's EDR and log management records actions such as file access, network requests, system changes, and more at central repository locations in the management console for easy review (Bitdefender, n.d.b).

Any effective security solution keeps in mind the confidentiality, integrity, and availability (CIA) triad of cybersecurity principles. Naturally, Bitdefender upholds confidentiality with its enforcement of encryption and access control measures of its endpoints. The implemented encryption covers both data-at-rest and data-in-transit while the configuration of access controls is enforced through robust authentication mechanisms and policy-driven user permissions. Integrity is protected through Bitdefender's features of file integrity monitoring and continuous patch management. For example, file integrity monitoring is achieved through Bitdefender's logging of any changes made to critical system files and configurations. If any unauthorized alteration is detected, alerts are triggered for immediate investigation and remediation. The automatic system updates and patch management upholds integrity against vulnerabilities that may exploit, expose, or corrupt data on its endpoints. As for availability, Bitdefender ensures the uptime of its systems through performance and health monitoring or other security measures. The solution continuously monitoring health and performance of endpoints to proactively resolve issues related to downtime with measures such as patch

management, EDR, access controls, and more. Additionally, the solution's infrastructure is designed to be resilient against DDoS or other downtime related attacks (Bitdefender, n.d.b).

Section D: Investigation & Mitigation of Cyber Incidents

As a feature-rich endpoint protection platform, Bitdefender GravityZone's primary objective is specifically designed to investigate and mitigate cyber incidents among all clients. For TMS' implementation, they are attacked by fairly common methods and practices regularly seen amongst other organizations such as trojans, bind shells, and more. A main protection feature is the use of EDR, which continuously monitors, collects, then correlates data from all endpoints to analyze activities. After analysis, potential attacks and behaviors are matched to known security incident types through its machine learning capabilities. In the event of an incident, Bitdefender's EDR enables analysts to trace the origin of the attack, understand attacker methods, and identify the scope of its impact. Moreover, the incorporation of global threat intelligence in the solution's data library provides greater context to detected security alerts by correlating local incident data with global threats. Thereby providing enhanced insight into attack complexity ranging from simple to sophisticated and understanding attack vectors that may be indicate of larger cybercrime campaigns. Within TMS, Bitdefender will be able to protect TMS against previous attacks toward the company when they struggled to before due to its continuous machine learning and adaptation.

Methods in which Bitdefender protects TMS are through automated incident response, patch management, policy enforcement, and threat hunting. Amongst TMS' limited cybersecurity team, Bitdefender aids enhances protection and lessens technical workload with their configuration of automatic incident responses based on predefined security policies. Next, automated patch management mitigates commonly known exploits and vulnerabilities to ensure TMS systems are up-to-date with the latest security updates. Policy enforcement seconds this objective as their consistent application may enforce access control, application control, and

other settings for the reduction of TMS' attack surface, such as disabling USB ports. Lastly, threat hunting features allow the TMS cybersecurity team to find indicators of compromise amongst the network, allowing for easier identification of passive threats or ongoing breaches not yet automatically detected.

Section E: Cybersecurity Plan, Standards, or Procedures for Proposed Solution

The first developed plan for the use of Bitdefender was least privilege. Like the created policy from section A, least privilege restricts a user from accessing information or resources not required to perform their necessary job functions. Naturally, a merchandise sales employee will not have authorization to configure Bitdefender settings.

Secondly, the introduction of multi-factor authentication (MFA) guidelines will enhance overall company security and access to Bitdefender itself. By enforcing MFA through an authentication app, a malicious insider may not access Bitdefender configurations without providing proof they are amongst the IT or cybersecurity team. Similarly, this guideline enforcement through Bitdefender itself prevents malicious attackers from accessing employee resources until they bypass MFA restrictions.

The implementation of Bitdefender additionally calls for the new development of continuous monitoring and incident response plans in coordination with the solution. The collaboration of Bitdefender includes an updated, detailed incident response plan outlining procedures to utilize the solutions feature-rich environment to better detect, respond, and mitigate cyber threats. Continuous monitoring critically oversees the performance, health, and efficiency of the introduced solution which allows administrative staff and stakeholders to make an informed decision to continue using Bitdefender. The plan also includes a step-by-step playbook that includes a hierarchy of escalation, call lists, and proper responses in accordance with predefined security policies for incident response.

User training and awareness standards were developed for the post-implementation maintenance of Bitdefender as well. The novelty of Bitdefender's introduction will be a

continuous process of learning well after the completion of the implementation project, and thus the technical team must stay on top of learning Bitdefender's capabilities. Doing so enables the technical team to utilize the solution more effectively and comprehensively train eventual new technical hires using it for the first time. As for non-technical personnel, the plans to adhere above a certain ESS score, weekly trainings, micro-trainings, and phishing campaigns within the BSN training platform promotes overall security awareness. This leads to an overall decrease to common user-enabled mistakes such as phishing or malicious downloads.

E1.

The relevant regulatory frameworks or standards Bitdefender aligns with are PCI DSS, NIST 800-53, and Information Technology Infrastructure Library (ITIL) practices. As an organization that processes credit card transactions, TMS is automatically subject to PCI DSS regulations and fines regarding protection of user financial data. PCI DSS security control obligations include a secure firewall configuration, data encryption, use of non-vendor supplied default passwords, access control, a vulnerability management program, and continuous monitoring (Kim & Solomon, 2021; Johnson, Weiss, & Solomon, 2022). Bitdefender addresses these concerns through its integrated firewall configuration feature, automatic encryption of data-at-rest and data-in-transit, policy enforcement for access control and password policies, automated patch management tools, and continuous endpoint logging and reports (Bitdefender, n.d.b).

Bitdefender's aligns among numerous applicable NIST 800-53 specified controls such as access control (AC), configuration management (CM), and incident response (IR). AC control AC-2 and AC-3, account management and enforcement, outlines the need for user management for certain systems, type of access allowed, and access control enforcement (Joint Task Force,

2020). Bitdefender supports AC-2 by configuring an endpoint directly to specify granted user authorization and their access privilege. It additionally provides other functionalities such as least privilege enforcement or account creation, deletion, or modification. CM-7, least functionality, is supported through Bitdefender's ability to restrict endpoints to only essential capabilities such as disabling USB ports, unused services, or ports. Control IR-4, incident response, Bitdefender is clearly in alignment with due to their variety of investigation tools such as automatic threat detection, immediate isolation of affected systems, and more for quicker incident detection and response.

Utilizing the ITIL 4 framework provides TMS with a structured and consistent approach for the implementation project without disturbing the existing infrastructure as it aligns with business objectives. A crucial principle of ITIL is risk management, that states how a company's services must be systematic in its process of identifying, triaging, and mitigating potential risks (Ivanti, n.d.). Bitdefender achieves this through its detailed analysis and insight of risk analytics which aid cybersecurity and IT staff in the threat detection and response processes. Another key service principle under ITIL is release and deployment management, which states an organization must facilitate controlled and consistent deployment of any updates or software changes (Ivanti, n.d.). Bitdefender easily manages this through its centralized management console, allowing for scheduled updates, patches, and changes to be deployed uniformly or even after work hours to ensure all systems are minimally disturbed yet consistently protected.

E2.

As part of the implementation project, a variety of user guides, applications, tools, or installation guides were established to facilitate ease of deployment. Installation guides were the first to be created as these detailed playbooks assisted the IT team with step-by-step installation

procedures, initial configuration, and integration with existing systems. Once the team thoroughly understood the installation guide, automated tool scripts were created to streamline the installation of the solution across network endpoints. Then, custom training modules and user guides were created to complement the existing suite of Bitdefender eLearning modules and catered towards TMS' unique network environment. As part of the cybersecurity plan, a set of security policies were developed specifically for enforcement through Bitdefender GravityZone's policy enforcement feature. These policies define rules, restrictions, and procedures that all endpoints must follow to strengthen the security posture.

Section F: Post-Implementation Environment

Following the successful implementation of Bitdefender GravityZone, a review of TMS's before and after environment highlights several new processes or systems developed. As part of the Pilot Testing phase, VMware licenses were purchased to mimic the live TMS environment. Moving forward, the IT and cybersecurity team may continue to utilize the virtual environment for sandboxing new configurations, new solutions, and more. Ten Windows 10 Pro licenses were also purchased and implemented to minimize the critical risk of running EOL Windows 7 software. As for policies, MFA was introduced as an additional security measure for preventing unauthorized access to TMS resources and validating personnel identities. The new automated security operations enhance security strength through automation-supplemented workflows for threat detection, incident response, and system updates, which reduce the reliance on manual intervention and accelerate the response to threats. Continuous monitoring and incident response plans contribute to an increase in proactive and reactive threat mitigations through formal playbooks, effective role communication, and escalation lists.

F1.

Bitdefender GravityZone significantly contributes to TMS's previously meek security posture through its advanced feature-rich platform. With advanced endpoint protection, threat hunting, advanced antimalware signatures, and more, TMS quickly detects and responds to potential threats faster than ever before. The real-time analysis data correlation enhances decision-making for security analysts to evaluate more insightful conclusions of an attack. Also, the automated response capabilities of GravityZone minimize both the attack surface and attack vectors of the infrastructure, overall reducing the potential impact on the organization. On the same note, the introduction of automation streamlines routine security tasks, like updates or

patches, and reduces operational overhead among the technical staff. This extraordinary increase in operational efficiency allows the team to pivot their attention towards more strategic security tasks or optimizing resource allocation.

F2.

Within Bitdefender, a comprehensive suite of tools collects, correlates, and reports data metrics which provide granular visibility into the security landscape of TMS. Granular event logging capture detailed information about all activities and events across the network. This information is crucial for conducting forensic investigations for breaches as they help analysts create a clear timeline and scope for an incident. Additionally, Bitdefender's integration of global threat intelligence provides greater context to these security logs. This allows analysts to assess whether identified threats or incidents are isolated events or indicative of wider attack campaigns, thereby promoting more informed strategic responses and decisions. The use of behavioral analytics amongst endpoints and user monitoring helps to detect anomalies indicative of a security threat, proactively mitigating potential threats well before exploitation.

The impact of Bitdefender's gathered data demonstrates an overall net positive effect upon TMS' business processes. Firstly, collected data significantly aids in the success of incident response plan plans, thereby helping the cybersecurity team reach better metrics for key performance indicators such as recovery point objectives (RPO), recovery time objectives (RTO), mean time to detect (MTTD), and mean time to respond (MTTR). The inclusion of Bitdefender's automation features supports overall business continuity and decreases downtime as well. By minimizing disruptions from security incidents, TMS wastes less time and resources managing and recovering from potential threats and allows them to focus on core business objectives. Additionally, compliance and audit readiness will linger overhead throughout TMS'

operations. Naturally, Bitdefender serves as a constant reminder to prepare for regulatory compliance. The ability to quickly run mock compliance assessments with regulations like PCI DSS and NIST SP 800-53 reduces the risk of non-compliance penalties and helps maintain the organization's reputation for safeguarding customer data.

F3.

Summative testing results as previously discussed from Task 2 will review the overall success of the Bitdefender project and how it affected TMS' security landscape. The tools and procedures utilized were PCI DSS and NIST 800-53 audits, external penetration tests, Nessus vulnerability scans, performance reviews, and user feedback from the BSN training platform.

PCI DSS compliance resulted in 95% compliance and was determined no further action is necessary. For external penetration tests, the new TMS security configurations did not allow for any unauthorized access or privilege escalation to outsiders with a 98% network intrusion detection rate. Vulnerability scans and threat detection accuracy provided a 100% known malware detection rate for malware variants and minimal critical vulnerabilities. Reviews for system uptime and performance indicate 85% uptime, with minor slowdowns under peak load and scans completed with moderate impact on end-user operations at 90% uptime. A suggested plan of action for increasing system uptime and performance metrics closer to 100% would be to reconfigure scan times, patch management for endpoints, or hardware upgrades on endpoints. Heavily affected endpoints will have software, memory utilization, and total data usage reviewed to potentially increase performance and uptime. Onto user feedback for BSN, 80% of personnel describe positive feedback with the new security training modules. The remaining 20% are those who still are unfamiliar with the abundant scope of technology. The plan for weakness correction

here may be to ease the difficulty on testing scenarios towards these end-users, allowing them to digest and understand content better.

F4.

Risk 1: Compatibility Issues

- **Likelihood:** Moderate
- **Impact:** High
- **Description:** Even with thorough pre-implementation testing, unforeseen compatibility issues with existing hardware or custom software applications may arise. These can lead to system instability or disruptions in service, affecting operations and customer sales.
- **Mitigation:** TMS will maintain and eventually expand its VMware testing environment continuously test updates and new integrations before they are deployed in the production environment. Additional ongoing training for IT staff will be established to manage and troubleshoot compatibility issues swiftly.

Risk 2: Security Configuration Errors

- **Likelihood:** Moderate to High
- **Impact:** High
- **Description:** The implementation of a new security solution requires extensive training and experience to utilize efficiently. Technical staff will inevitably have incorrect or insecure security configurations which can lead to new vulnerabilities and exploits.
- **Mitigation:** Cybersecurity and IT personnel will conduct regular security audits and reviews to ensure all configurations adhere to best practices and compliance standards.

Ongoing training will be enforced well past the implementation project to develop Bitdefender proficiency and future training manuals for new hires.

Risk 3: User Resistance

- **Likelihood:** Moderate
- **Impact:** Moderate
- **Description:** The introduction of the BSN training platform, and ongoing Bitdefender training among technical staff is sure to be met with user resistance. The sudden enforcement of a cybersecurity culture when TMS was previously lax in security awareness will have some staff feel as if these changes overcomplicate their workflow.
- **Mitigation:**

Risk 4: Insider Threats

- **Likelihood:** High
- **Impact:** High
- **Description:** As a museum of supernatural oddities, the proprietary information employees hold is of high value to other countries, companies, or news outlets. A malicious insider may attempt to gain privilege escalation or peddle confidential information to outsiders in a selfish effort for monetary gain. If proprietary research and information is disclosed, TMS is at risk of losing a large fraction of its customer base.
- **Mitigation:** The concept of least privilege, MFA, and implementation of secure access controls through Bitdefender will be enforced. These principles prevent staff from accessing company resources they otherwise would not normally be granted, especially for the functionality of their job role. Additionally, those who are employed with TMS will have to sign a non-disclosure agreement (NDA) to prevent information leakage to

competition or other sources. If this NDA is broken, TMS will file heavy legal action against the individual.

F5.

1. **Stanley Pines, CEO**
    a. As CEO, Stanley Pines' primary needs are concerned with the overall financial health and reputation of TMS. Particularly, he wants to avoid large financial losses due to breaches, noncompliance, and a weakening public image. Bitdefender GravityZone accommodates Stanley Pines' needs by significantly increasing the overall security posture, minimizing the risk for breaches and aligning with PCI DSS compliance.
2. **Stanford Pines, CTO**
    a. Stanford Pines's needs revolve around the integrity and confidentiality of his scrutinous research data, as well as maintaining a flexible yet secure technological environment. Bitdefender offers a solution for Stanford through its advanced threat protection, data security features, and scalability features. These attributes of Bitdefender safeguard sensitive information whilst enhancing his concern for technological agility and upscaling required for research and development.
3. **Dipper & Mabel Pines, COO's**
    a. As COOs, the twins are responsible for overseeing smooth daily operations. Meaning they require an integrated solution that ensures operational continuity without disrupting the customer experience. The automated cybersecurity tools of Bitdefender evidently raise the security posture of the organization, leading to less breaches or attacks which would cause downtime. Operational continuity is met

as the noninvasive nature of Bitdefender allows it to run in the background without disruption of business services.

4. **Sooz Ramirez, CMO**
    a. Similar to Dipper & Mabel, Chief Maintenance Officer Soos requires a reliable infrastructure that experiences minimal operational disruptions or technical disruptions both digitally and physically. Bitdefender's comprehensive monitoring aids Soos' needs as it can notify him when a system's hardware is faulty, outdated, or in need of repair for certain parts. This ensures system reliability, uptime, and continuous support of business and system operations.
5. **Wendy Corduroy, HR**
    a. Wendy spearheads the ongoing initiative of employee training, security awareness culture, and compliance with security policies. As such, Bitdefender includes training modules and simulations which are crucial to educating personnel about security best practices and PCI DSS. Bitdefender's policy enforcement also ensures that systems and employees are more likely follow the more technical policy guidelines for upholding security.
6. **Mystery Shack's IT and Cybersecurity Team**
    a. As the technological backbone of TMS, this group requires the more latest, sophisticated tools to manage the security infrastructure for efficient incident response and proactive protection. Evidently, Bitdefender provides real-time monitoring, automated threat response, and detailed analytics that advantageously empower the team to manage and secure the network.
7. **Customers**

   a. The needs of TMS' customer base expect the organization to safeguard the confidentiality and integrity of their data, as well as availability of business operations for their recreation. Bitdefender meets their needs through secure encryption and data protection with AES-256. The enhanced defense and risk mitigation through Bitdefender also increases operational availability, ensuring customer trust and satisfaction.

8. **Regulatory Compliance Officers**
   a. Compliance offers require for TMS adhere to regulatory requirements such as PCI DSS or NIST 800-53 otherwise the organization fails its obligations. Bitdefender GravityZone supports compliance with standards like PCI DSS and NIST 800-53, featuring tools for audit trails and compliance reporting that facilitate regulatory adherence. Additional tools are compliance are Bitdefender's firewall configurations, data encryption, patch management, and secure access control.
9. **Financial Partners and Merchandise Suppliers**
   a. This group of stakeholders are concerned with TMS' promise to protect business transactions, data exchanges, and uphold smooth business operations. The strong encryption and transaction security features of Bitdefender safeguard all data exchanges, ensuring the integrity of financial transactions and supply chain communications between parties.
10. **Local Government and Community Leaders**
   a. The needs of this stakeholder group revolve around the overall security and integrity of local businesses to maintain community trust. If TMS were to suffer numerous breaches, confidence of the local community wavers and they fear they

could be additional targets for attack. Through the adherence of high security and compliance standards, TMS contributes to Gravity Falls' economic stability and trust through its global customer attractions and tourism. This also reinforces local government efforts for secure business promotion.

11. Cybersecurity Consultants and Vendors

a. As external advisors, this stakeholder group requires confirmation that their solutions and produce functions as expected. These needs are necessary for stakeholders to grow and promote their proprietary solutions. Bitdefender's extensively advanced security capabilities are showcased through TMS' successful implementation project. Where the company could not before, they now exhibit extraordinary security tools, thus enhancing the reputation of this stakeholder group.

Section G: Post-Implementation Maintenance Plan

After the successful completion of the implementation project, a maintenance plan is crucial for determining the ongoing success and efficiency of the cybersecurity solution. The numerous key points of the plan involve continuous monitoring, regular patch management, performance and security audits, and ongoing user training and awareness programs.

Continuous monitoring is an essential requirement of post-implementation maintenance to quickly remedy any potential misconfigurations, new threats, or anomalies among TMS. A security baseline will be established immediately after the implementation as a reference point for analytic metrics as part of the incident response plan. The in-house Bitdefender monitoring tools will provide real-time alerts and daily logs of unusual activity, prompting the cybersecurity team to quickly squash threats.

Regular patch management will now be automatically provisioned as opposed to the previously manual process by the IT team. The crucial nature of patches aid TMS in preventing known exploits, so plan involves automatic updates for all security and OS software, including Bitdefender GravityZone. The IT and cybersecurity team will incorporate a stringent update and patch management protocol within Bitdefender to constantly keep the infrastructure up to date. High-priority updates are applied immediately after release during predefined maintenance windows to minimize system downtime. Monthly checks for the update scripts and processes will be reviewed to confirm the integrity of the update process, ensuring that no critical updates are missed.

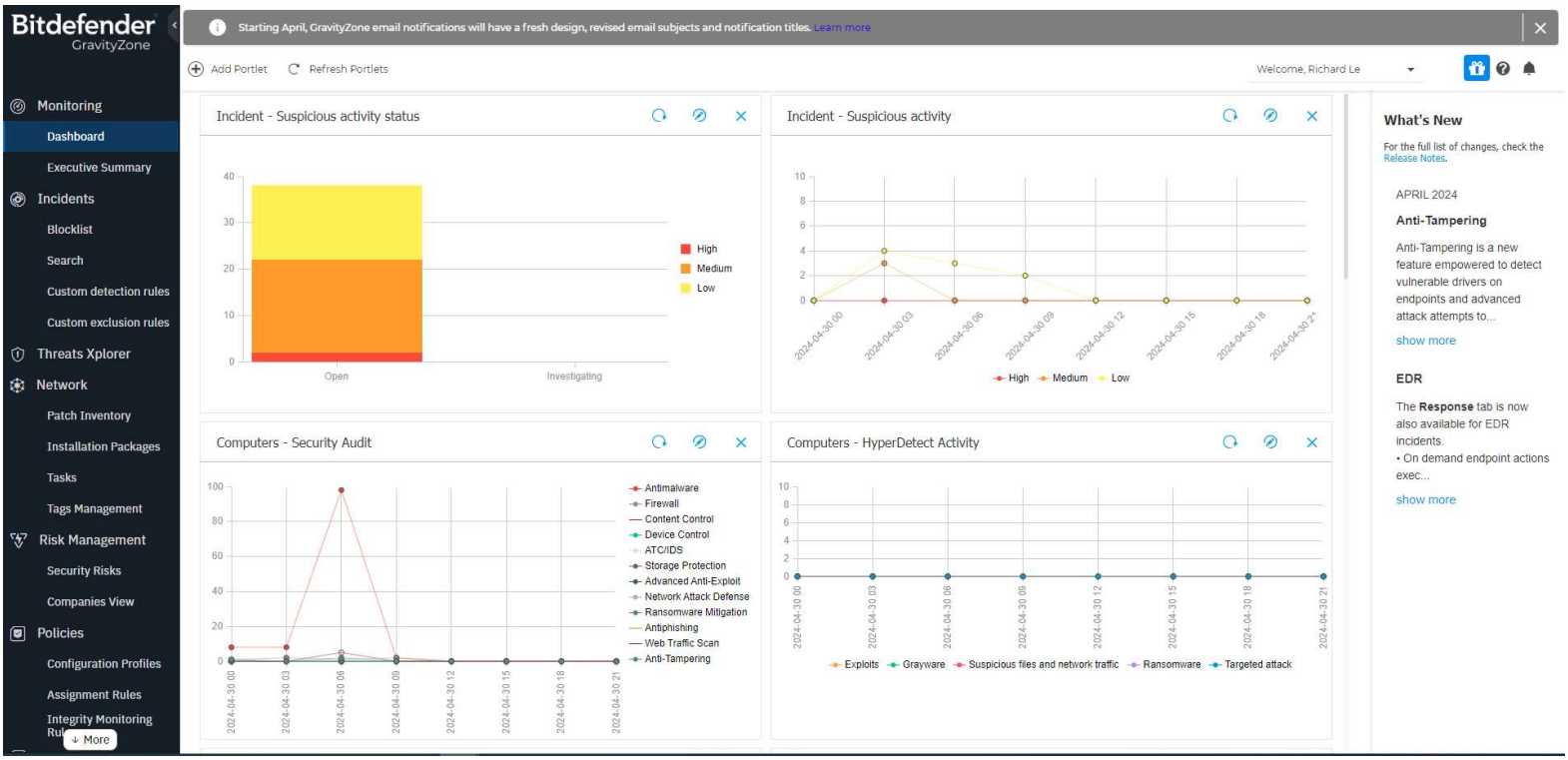
Quarterly performance and security audits will take place as a natural responsibility for the organization’s compliance with security standards and regulatory requirements. External

penetration tests will regularly be conducted to assess TMS' ability to adapt with emerging cybersecurity threats and protection against breaches. Compliance audits assist in holding the organization accountable for data protection and effective security measures. The findings from these audits and penetration reports guide the necessary adjustments in security strategies and help maintain the system's defenses against evolving cyber threats.

The nature of human error is a statistical concern among most organizations regarding security breaches. Thus, ongoing training programs between technical staff and non-technical staff are established to enhance security protocols against threats. For the technical staff, the programs will include biannual workshops, monthly security briefings, and mandatory training review from Bitdefender's eLearning platform. An eventual TMS Bitdefender guide will be established from existing knowledge and experience with Bitdefender. This aids eventual new hires utilizing the solution for the first time. As for non-technical staff, TMS will promote the ongoing use of the BSN platform, enforcing all employees to maintain an ESS score above 70%. Simulated phishing reports and training scores will be reviewed quarterly to assess individuals falling behind in their knowledge of security awareness.

Section H: Cybersecurity Artifact

The below artifact of the original project showcases the Bitdefender GravityZone dashboard. Various metrics are displayed for analysts to understand a broad scope of the infrastructure.



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

Bitdefender. (n.d.c). *Viewing Endpoint Details.* Bitdefender. https://www.bitdefender.com/business/support/en/77212-155147-viewing-endpoint-details.html

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

Ivanti. (n.d.). *What is ITIL 4?* Ivanti. https://www.ivanti.com/glossary/itil-4

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