Barbara Garcia

6/18/2024

**D490 – Cybersecurity Capstone Task 2: Project Proposal**

**A.**

**A1.**

**Background**

Things, Inc. is an IoT company that owns two different brands of ‘smart’ devices that control industrial systems. It has a major security problem. Its web facing servers are having regular availability issues caused by lack of active security and event monitoring on the company’s network. Each brand has web servers that customers depend on to operate the devices. Recently, both brand’s servers have been experiencing outages that affect the users’ ability to use the smart devices. Due to the reactive posture of the company, these outages have lasted up to a few hours, which is impacting business operations. This proposed project seeks to implement a Security Incident Event Management (SIEM) platform that will proactively monitor these systems to detect potential incidents before servers are down, which will result in few incidents and less downtime when an incident occurs.

**Environment**

Things, Inc.’s technology environment is spread out geographically with patchwork infrastructure. There is considerable IT sprawl and lack of IT planning. There are servers located in at least two physical locations and in the cloud. Some are served by additional third parties on the back end of the web servers. The company employs overseas IT personnel and there is lack of communication and transparency. Web servers for both brands experience downtime regularly, which affects availability, and are often close to overloaded.

As to assets, the company has two office locations, each with their own internal network, workstations, and servers. In addition to overseas IT contractors using their personal workstations who have access to the servers, there are many remote employees within the US, each using a company laptop. The company also houses virtual servers in the cloud.

The Virtual server for brand one is running an application built on old code and are hosted by a third party with frequent outages in lag. These issues are causing them to go offline frequently. Since only server status is monitored, and not logs, the company does not act on server issues until the server is already down.

**A2.**

To avoid a catastrophic server failure that could result in loss of availability that affects the company’s reputation and costs them large amounts of money and lost business, the company should implement a SIEM solution to proactively monitor the company’s network and assets, especially essential web servers. As Jamiu Akande states in his article, “Under the eye of a SIEM solution, data from logs, apps, devices and security tools like firewalls and antivirus software come together to help organisations detect and respond to potential threats in real time.” (Akande, 2023)” Since Things, Inc is experiencing regular enough incidents to impact business operations, they need a way to reduce the amount and severity of incidents. “84% [of organisations that use SIEM] reported a measurable reduction in security breaches due to the use of their SIEM platform.” (Akande, 2023)

**A3.**

There are three main root causes to the security problems experienced by Things, Inc. The company’s IT posture is reactive, responding to events after they have already happened and impacted the company’s business operations. A second root cause is that the company is prioritizing sales and money in the moment rather than taking time and resources to engage in thorough risk analysis. The third root cause of the security problems is that there is no technical implementation within the company’s infrastructure to monitor network and server security activity in real time.

**B.**

The project has internal and external stakeholders that will be necessary for success. The stakeholders include Things, Inc’s CEO, a project manager, SOC team, the network administrator, a compliance officer, data owners, and application developers.

The CEO’s involvement will consist of approving the implementation plan and the budget for the project. He needs an understanding of why the SIEM is needed and what it will do for the company’s bottom line. The CEO is affected by the company’s current server and tool downtime and risk of greater availability incidents because he is responsible for profitability. His influence is great since he will decide if the project will move forward and how much funding will be given toward the project, which will affect whether the implementation is successful.

The project manager for the SIEM implementation will be a cybersecurity consultant hired as an independent contractor. This stakeholder will drive the implementation project based on best practices and company security goals. He or she will need a thorough understanding of the company’s current security posture and what the company seeks to achieve with the SIEM implementation. The problem affects the cybersecurity consultant in that they are now tasked with taking a large part in solving it. This person has arguably the strongest influence over the project’s implementation second only to the CEO, as he or she will bring experience from prior SIEM implementations and guide the direction of the entire project.

Another essential stakeholder group is the Security Operations Center (SOC) team, consisting of a cybersecurity engineer and three cybersecurity analysts. As to this group’s influence on the project, the engineer will help design and build the architecture for the SIEM implementation and analysts will be involved in monitoring security dashboards and providing feedback on their experiences and observations. Their needs are training, communication channels needed to collaborate with the implementation team, and the network and software resources necessary to properly set up and use the SIEM. There is not currently an SOC team in place, so these stakeholders are not currently affected by the security issue, though the severity of the server outages and the variances in network infrastructure will affect their efforts at implementing a successful SIEM program. This team collectively has a big influence on the project as they will be involved in driving design, fielding implementation and be heavily involved in ongoing operations.

Another important stakeholder group are the IT and Network Administrators. Their involvement will be coordinating log aggregation and coordinating with all departments to ensure a seamless implementation. They need open communication channels with all departments and to have access to work closely with the SOC team. This group is heavily affected by the ongoing security issues, as they currently spend much of their time reacting to incidents instead of proactively managing the company’s IT assets. They have a moderately large influence on the project, as they oversee the network and control the settings of company workstations and servers. Their collaboration will be essential to the project’s success.

The compliance officer will be involved in all parts of implementation that affect compliance with legal and regulatory requirements. They need to know the SIEM’s compliance capabilities and an understanding of what a SIEM does and how it transmits data. The compliance officer is not currently affected by the issue as there is no compliance officer currently at the company. This stakeholder will influence how data is used, transported and store and will influence all facets of the implementation that are affected by compliance.

The final stakeholder group is the data owners and application developers. This group will help determine what data will be useful to use for SIEM aggregation. They need to understand the goals of the SIEM implementation to help guide data selection. The security problem affects them in that it puts the confidentiality, integrity and availability of the data they are responsible for at risk. Their influence is moderate. Though they won’t make final decisions, they will give useful context as to what data is available for use.

**C.**

As the project team proceeds with the SIEM implementation, they will use historical data from Things, Inc. to guide decision-making. Historical data they will use includes Incident Reports from all prior server outages for both brands, incident reports from prior account takeover attacks, incident reports from other events that affected confidentiality, availability, or integrity. All logs related to prior incidents will be reviewed to guide the team as they tune the SIEM on what logs to show and alerts to trigger.

**D.**

**D1.**

SIEM solutions are used by many companies to monitor and respond to cybersecurity events. This project will use standard methodologies to guide the design and development of the SIEM implementation. These include collecting and aggregating logs, monitoring and analyzing the logs in real time, incident detection and response, integrating threat intelligence, compliance monitoring and reporting, data retention and management, user and entity behavior analytics (UEBA), integration with other security tools and continuing improvement.

**D2.**

The planning and rollout of the project will include 5 phases and will use the LEAN Methodology for implementation. LEAN was selected for this project largely because of its focus on continuous improvement and focus on collaboration and communication. The four basic steps that make up LEAN’s continuous improvement cycle are identify, plan, execute and review.

Phase one of the project is planning and preparation. During this phase, the team will define the objective and scope of the project, assess current infrastructure, and select an appropriate SIEM solution that meets the company’s current and future needs. Phase two is design and integration. During this phase, the team will design the SIEM’s architecture, determine how data will be collected, and define use cases and correlation rules. Phase three will be deployment and testing. During this phase, the team will first conduct a pilot deployment in the network at the company headquarters. To avoid service interruption, the pilot will not include essential web servers. Once the pilot implementation is successful and necessary adjustments have been made the team will deploy the solution company-wide. This phase will also include training and awareness for all staff. Phase four is monitoring and optimization, which will include continuous monitoring of the SIEM solution and the overall project, regular tuning of the SIEM and ongoing incident response and forensics. The final phase is review and maintenance. This phase is ongoing and includes regular reviews and audits of the SIEM implementation, updates and upgrades, and regular stakeholder communication.

**D3.**

Implementing a SIEM solution in a company that does not have existing monitoring infrastructure brings some risk to the organization.

One of these risks is high implementation and operational costs. Given the CEO is hesitant to spend money on projects that don’t bring direct revenue into the company, obtaining the funds necessary to properly implement the SIEM solution may prove difficult, potentially resulting an implementation that doesn’t meet the needs of the company’s infrastructure.

Another risk is integration complexity. As the company’s technical footprint is inconsistent, the project has the potential to require more resources to implement.

Misconfiguration is always a potential risk when implementing a technical solution. In this case, the likelihood is high because of the complex nature of the company’s infrastructure. The potential impact of misconfiguration is high because it could cause disruptions in systems and in inhibit the appropriate alerts populating to the dashboard.

Anytime data is being stored and transported, there are risks to being out of compliance with regulatory requirements. Since the project will employ a compliance officer, the likelihood of this risk is low. The impact if it does happen is high, as it could cost the company in terms of regulatory fines and/or loss of reputation.

Another implementation risk is vendor lock-in. Being locked into a specific vendor can make it difficult to make changes to the SIEM down the road if the vendor becomes too expensive or no longer fulfills the company’s implementation requirements. The likelihood of Things being locked into a vendor is high, given it is already affecting one of the main applications for IoT devices. The impact has the potential to be high since the company has no control over a third-party’s future decisions.

**E.**

The implementation of a SIEM solution at Things, Inc. will only be successful if its employees receive appropriate initial and ongoing training.

Depending on the audience, training needs will vary. The security operations center team will obtain need in-depth knowledge of SIEM functionalities, threat detection, incident response, and advanced analytics. The IT team and network administrators will need training that gives them understanding of SIEM integration, data collection, and log management. Compliance officers will need to gain knowledge of the SIEM’s compliance reporting features and how to generate necessary reports. Senior management will need a high-level understanding of the capabilities, benefits and ROI of the SIEM.

Training will be delivered via instructor-led training, self-paced learning, workshops, hands-on labs, documentation, and knowledge base.

The content of training will include introduction to SIEM, SIEM system setup and configuration, log management, threat detection, incident response, advanced analytics, reporting, maintenance, and optimization.

The duration of training will vary based on each employee’s duties. The SOC team will initially have two to three weeks of intensive training that also includes workshops and hands-on labs. Going forward they will participate in monthly refresher courses and advanced training sessions twice a year. Compliance officers will receive a week ong initial training that focuses on compliance features and reporting requirements. Senior management will receive one to two days of training

**F.**

Throughout the project, various resources will be necessary. It is essential to the SIEM’s success that the CEO and any other financial decision makers have a clear understanding of why the SIEM is needed, the resources that will be needed and the cost of those resources. Some phases will use resources initiated in prior stages. If no new expenses are incurred, these expenses will not be counted twice.

Phase one is the planning and preparation phase. The resources that will be needed for this are a cybersecurity deployment consultant acting as the project manager that will cost the company $50,000 MMcDaniel (2022), a compliance officer who will require an annual salary of $73,000 (Saray.com, n.d.), a vulnerability assessment via Open VAS, which will have a cost of zero dollars, an asset inventory compiled by the IT team and department managers that will incur no additional cost, and information on SIEM options for no cost.

Phase two is the design and integration phase. The resources required for this phase are a cybersecurity engineer that will cost an annual salary of $120,000 (Moore, 2016) and a SIEM platform. The company will be using Splunk at a cost of $48,000 per year. (*Splunk Pricing Insights and Buyer Guide for 2024 | Vendr*, n.d.)

Phase three is the deployment and testing phase. The resources required for this phase are the SIEM platform that was procured in phase 2, the cybersecurity consultant who was already hired in phase one, the cybersecurity engineer hired in phase two and three SOC analysts at a salary of $69,000 per year each for a total of $207,000 annually. (*SOC Analyst Salary: How Much Can You Earn as a SOC Analyst? | Cyber Security Jobs*, n.d.)

Phase four is the monitoring and optimization stage. One of the resources needed for this phase is an incident management system. The company will use ManageEngine ServiceDesk Plus Incident Management at a cost of $3,895 per year. *ManageEngine ServiceDesk plus Cloud Pricing / License Cost* (n.d.). Jira will be needed to track any incident tickets related to SIEM operations. The cost for this is $2,050 per year. (Atlassian, 2020) This phase will also require advanced SIEM training for the security practitioners. The SOC analysts will learn and achieve Splunk Certified Cybersecurity Defense Analyst Certification. The training will cost the company $1,500, *STEP | Splunk Training and Enablement Platform* (n.d.), and the exam will cost the company $130. (*Training and Certification FAQs*, n.d.) Network administrators will take the Splunk Core Certified User training. The training will cost the company $600, *STEP | Splunk Training and Enablement Platform* (n.d.), and the exam will cost $130. (*Training and Certification FAQs*, n.d.) The cybersecurity engineer will obtain Splunk Cloud Certified Admin certification. The training will cost $2,000, *STEP | Splunk Training and Enablement Platform* (n.d.), and the exam will cost $130. (*Training and Certification FAQs*, n.d.)

Phase five is the review and maintenance phase. This phase will require various resources, mostly coming from within the organization. One additional tool needed for this phase is a compliance reporting tool. The company will use Apptega for this, at a cost of $6,930 per year. (*AWS Marketplace: Apptega*, n.d.) This phase will also require a review and audit team made up of the security analysts, the cybersecurity consultant and the compliance officer. The team will review audit reports from Splunk, change logs, performance reports and incident reports that will be used as resources in this phase. A patch management program headed by the IT and network admins will also be needed for this phase.

**G.**

The project has six major milestones. The first milestone will be a meeting of the project stakeholders to plan the project and select a SIEM solution and will last one to two business days. The start date for the project is June 18th 2024 and the end date is July 30th 2024. The resources needed for this milestone are all stakeholders and data from prior incidents. The deliverable for this milestone will be the meeting minutes, including decisions made and budget approval. The second milestone is to install endpoint detection and response (EDR) nodes on the pilot workstations at the corporate home office and calibrate the SIEM dashboard. This will take two to three business days and will require the resources of Splunk, the cybersecurity engineer, the cybersecurity consultant, and the compliance officer. The deliverables for this phase will be an updated network diagram reflecting the installation of EDR nodes and the SIEM dashboard set up to monitor the pilot machines.

The third milestone is to conduct SIEM logging and monitoring of home office workstations, review results and draft report. This will take two weeks and will require the resources of Splunk, cybersecurity analysts, cybersecurity engineer, cybersecurity consultant, Jira, Apptega, and the compliance officer. The deliverables for this milestone will be the log reports and the feedback report from the monitoring team, including change recommendations. The fourth milestone is to make necessary adjustments to the SIEM system based on the pilot program report, then install EDR nodes and calibrate the SIEM dashboard for company-wide workstations and servers. The resources for this milestone are Splunk, cybersecurity analysts, Apptega, Jira, the cybersecurity engineer, the cybersecurity consultant, and the compliance officer and will last one week. The deliverables will be the updated network diagram and the SIEM Dashboard after the expanded implementation.

The fifth milestone will be a meeting of the implementation team to review results of the implementation and make any necessary adjustments. This will last one week and will require all stakeholders, SIEM dashboard data, Apptega data, Jira tickets, and incident reports. The deliverables will be the Jira reports, Apptega data, incident reports and the meeting minutes. For the sixth and final milestone, the CEO, IT manager, cybersecurity consultant, cybersecurity engineer, cybersecurity analysts, compliance officer will meet to evaluate the program and sign off on ongoing implementation if the project meets success criteria. In addition to stakeholders, this milestone will require all data and reports from the implementation as well as stakeholder feedback. This milestone will take one business day. The deliverable from this milestone will be the signed approval form with CEO and other stakeholder signatures.

**H.**

**H1.**

Assessment of the project as it progresses will be essential and consist of formative and summative assessment practices. According to EvalCommunity, “Formative evaluation is a process of gathering and analyzing feedback during the development or implantation a program, project, or product. It identifies strengths, weaknesses, and areas for improvement, with the aim of making adjustments to improve the quality and effectiveness of the program or product.” (*Understanding Formative Evaluation: Definition, Benefits, and Best Practices - EvalCommunity*, n.d.) Summative Assessment is performed at the conclusion of an assignment, test or project and compares to a standard or benchmark. (Carnegie Mellon University, 2019)

Formative procedures for this project will be to review logs ingest by the SIEM, assess the dashboard to determine if it is showing what the team needs it to show to align with security goals, and to regularly adjust SIEM settings based on performance. The tools needed for assessment are Splunk, event and incident logs, and dashboard reports.

Summative procedures will be to compare system performance, consisting of the number and severity of security incidents and any incidents that compromise confidentiality, integrity, and availability to standard benchmarks and prior company incidents. The tools needed for the summative assessment are Jira, key performance indicator (KPI) reports, Apptega data, and prior incident data.

**H2.**

During assessment, the team analyze the results and determine if they meet the minimum acceptance criteria. For the formative assessment, the acceptance criteria is that the SIEM’s current implementation is successful in reducing incidents that compromise confidentiality, integrity, and availability of company assets. The key performance indicators will be server downtime and server latency.

The summative assessment acceptance criteria is that the data reviewed during this assessment reflects 50% fewer incidents after implementation of the SIEM.

**H3.**

Given that the major security problem Things, Inc. faces is the increasingly common incidents of web servers powering IoT becoming inaccessible, the assessment criteria of monitoring this major resource will let the team know if the SIEM implementation is making a difference in this area. Since this is the largest pain point, and the servers are the largest revenue driver of the company, it makes sense to focus on this. If the SIEM implementation is successful in providing greater protection for web facing servers, it will set a framework for the company to continue to improve security on all company machines.

**H4.**

The team will use data, reports, employee feedback, and contractor observations to analyze the results of the SIEM implementation. They will comb through data, review dashboards and reports and collaborate to compare server downtime rates after implementation to server downtime rates before implementation.

**References**

Akande, J. (2023, September 27). *The Cyber Risks of an Unoptimised SIEM*. RiverSafe. https://riversafe.co.uk/resources/tech-blog/the-security-risks-of-an-unoptimised-siem/#:~:text=Inadequate%20threat%20detection

*Apptega Platform | Security and Compliance Made Easy*. (n.d.). Www.apptega.com. Retrieved June 17, 2024, from https://www.apptega.com/platform

Atlassian. (2020). *Jira Pricing - Monthly and Annual Subscription Cost per User*. Atlassian. https://www.atlassian.com/software/jira/pricing

*AWS Marketplace: Apptega*. (n.d.). Aws.amazon.com. Retrieved June 17, 2024, from https://aws.amazon.com/marketplace/pp/prodview-dujbeorjpvung

Carnegie Mellon University. (2019). *Formative vs summative assessment* . Carnegie Mellon University. https://www.cmu.edu/teaching/assessment/basics/formative-summative.html

Freeze, D. (2024, February 26). *SIEM Implementation: Strategies and Best Practices*. Cybercrime Magazine. https://cybersecurityventures.com/siem-implementation-strategies-and-best-practices/

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/s21144759

IBM. (2022). *What is Security Information and Event Management (SIEM)?* IBM. https://www.ibm.com/topics/siem

Kent, K., & Souppaya, M. (2006). *Special Publication 800-92 Guide to Computer Security Log Management Recommendations of the National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Kidd, C. (2023, October 12). *What’s SIEM? Security Information & Event Management Explained*. Splunk-Blogs. https://www.splunk.com/en\_us/blog/learn/siem-security-information-event-management.html

*ManageEngine ServiceDesk Plus Cloud pricing / license cost*. (n.d.). Www.manageengine.com. https://www.manageengine.com/products/service-desk/pricing.html

MMcDaniel. (2022, December 7). *What You Need To Know About SIEM Pricing & SIEM Costs*. PCH Technologies. https://pchtechnologies.com/what-you-need-to-know-about-siem-pricing-siem-costs/

Moore, M. (2016, April 21). *Should You Become a Cybersecurity Engineer?* University of San Diego. https://onlinedegrees.sandiego.edu/should-you-become-a-cyber-security-engineer/

Salary.com, S. built by: (n.d.). *Security Compliance Analyst Salary*. Salary.com. Retrieved June 17, 2024, from https://www.salary.com/research/salary/posting/security-compliance-analyst-salary

*SOC Analyst Salary: How Much Can You Earn as a SOC Analyst? | Cyber Security Jobs*. (n.d.). Www.cybersecurityjobs.com. https://www.cybersecurityjobs.com/soc-analyst-salary/

*Splunk Cloud Certified Admin*. (n.d.). Splunk. Retrieved June 17, 2024, from https://www.splunk.com/en\_us/training/certification-track/splunk-cloud-certified-admin.html

*Splunk Pricing Insights and Buyer Guide for 2024 | Vendr*. (n.d.). Www.vendr.com. Retrieved June 17, 2024, from https://www.vendr.com/buyer-guides/splunk#:~:text=For%20a%20team%20with%20a

*STEP | Splunk Training and Enablement Platform*. (n.d.). Education.splunk.com. Retrieved June 17, 2024, from https://education.splunk.com/Saba/Web\_spf/NA10P2PRD105/app/me/learningeventdetail

Terry, J. (2023). *What is Lean Methodology?* Planview. https://www.planview.com/resources/guide/lean-principles-101/what-is-lean/

*Training and Certification FAQs*. (n.d.). Splunk. Retrieved June 17, 2024, from https://www.splunk.com/en\_us/training/faq.html

*Understanding Formative Evaluation: Definition, Benefits, and Best Practices - EvalCommunity*. (n.d.). EvalCommunity. https://www.evalcommunity.com/career-center/formative-evaluation/#:~:text=Formative%20evaluation%20is%20a%20process

*What is SIEM?* (n.d.). Cloudflare. Retrieved June 9, 2024, from https://www.cloudflare.com/learning/security/what-is-siem/

*What is SIEM? | IBM*. (2024, April 2). Www.ibm.com. https://www.ibm.com/topics/siem#:~:text=Security%20information%20and%20event%20management