Barbara Garcia

ID: 011883626

6/26/2024

**D490 – Cybersecurity Capstone Task 3: Technology-Supported Security Solution**

**A.**

Implementing a security information and event management (SIEM) solution within Things, Inc.'s network makes the company's security infrastructure visible, resulting in improved decision-making. Making decisions without clear data is not effective. The visibility of network and server activity provided by the SIEM dashboard allows the company to visually see its security posture's status, allowing it to make thoughtful, logical decisions based on actionable data efficiently.

**A1.**

The company has adopted various new policies as part of the SIEM implementation. These include a data collection and management policy, access control policy, incident response policy, compliance, and legal policy, operation policy, threat intelligence policy, training and awareness policy, security policy, and a reporting and metrics policy.

The data collection and management policy guides how the company collects, stores, and transmits data within the SIEM solution. It includes deciding which log sources and types will be collected and data retention periods that consider regulatory requirements and storage capacity. The access control policy guides user roles, permissions, and authentication and authorization related to the SIEM implementation.

The incident response policy guides alerting and notifications, incident handling procedures, and post-incident review. The compliance and legal policy ensures that SIEM operations comply with regulations like GDPR and PCI-DS and that data protection practices comply with privacy laws. It also guides the maintenance of detailed logs of SIEM activities to support compliance.

The operation policy encompasses change management, system monitoring, backup, and recovery. The threat intelligence policy defines how the cybersecurity engineer will integrate threat feeds into the SIEM and establishes the processes the company will use for acting upon threat intelligence and suspicious activities detected by the SIEM. The training and awareness policy addresses user training to ensure SIEM users have the knowledge and skills to run the system effectively and securely, as well as ongoing education to keep staff updated on new threats, SIEM features, and best practices through continuous training and education programs.

The security policy addresses data encryption, system hardening, and regular audits and assessments. The reporting and metrics policy establishes reporting procedures for SIEM activity and performance metrics to measure the effectiveness of the SIEM.

**B.**

The SIEM implementation promotes automation in cybersecurity by using automation to aggregate and display essential log data, which saves time, increases efficiency and productivity, and makes it easier to see anomalies.

The SIEM improves security by monitoring data in transit. Things, Inc. will be able to react proactively to potential security events, often stopping them before they disrupt confidentiality, integrity, and availability. It modernizes security by using a platform that continuously improves as technology advances and allows for the implementation of SOAR to modernize further and automate security monitoring and response.

The implementation uses Splunk, an industry-standard SIEM platform, as the base for the SIEM implementation and endpoint detection and response nodes within the SIEM infrastructure, which is an industry-standard device for monitoring network activity.

**C.**

The security incident and event management program effectively addresses data collection and implementation of confidentiality, integrity, and availability.

The SIEM Collects log data such as event logs, Syslog logs, and Windows event logs, aggregates and normalizes the data so that the SIEM can parse the data and provide additional context through enrichment. The SIEM stores data for the retention period, making it available for analysis and forensic investigations. The SIEM also has search and query capabilities that enable analysts to sift through large amounts of data to find evidence needed for forensics.

The SIEM platform implements confidentiality through access controls, encryption, data masking, and comprehensive access logging and auditing. It implements integrity by hashing logs and data, using digital signatures to verify integrity, using change management controls to track configuration changes, and using integrity monitoring that generates alerts if an anomaly is detected. It implements availability by utilizing redundant hardware, software, and network components, high availability architectures with failover clustering and load balancing, regular backups, disaster recovery plans, and scalability, ensuring the solution can handle increased volume without decreasing performance.

**D.**

The SIEM implementation investigates cybersecurity incidents by aggregating data to the SIEM dashboard, which cybersecurity analysts review and analyze. The SIEM implementation mitigates data with a security operations center team that works with IT to respond to any activity that may compromise confidentiality, availability, or integrity. The team also works with IT to regularly change and update SIEM infrastructure and configuration as necessary to prevent security incidents from happening.

**E.**

Various procedures were developed for the continued operation of the SIEM solution. Essential SIEM functions for which procedures were developed include data collection and normalization, monitoring and maintenance, incident response, and evaluation and improvement.

For data collection and normalization, procedures were developed to identify and prioritize log sources, configure log sources to send logs to the SIEM system in a consistent and standardized format, and ensure that collected logs are normalized to a common format for efficient analysis and correlation. Procedures established for monitoring and maintenance include continuous monitoring of the SIEM system to ensure it is collecting and analyzing data effectively, performing regular health checks and maintenance tasks to ensure the system is operating at an optimal level, and regularly reviewing logs and alerts to identify any missed incidents or false positives.

Procedures developed for incident response include playbooks that outline the steps to take when an alert is triggered and implement automated response actions for specific types of incidents to reduce response time. Continuously improving the SIEM's performance is essential. Procedures developed for evaluation and improvement are periodic reviews of the SIEM system to identify areas for improvement, engaging in a feedback loop with the security engineer and analysts to gather insights and continuously improve the implementation, and regularly updating and upgrade the SIEM system to add new features, address vulnerabilities, and improve performance.

**E1.**

**Cybersecurity Compliance and SIEM**

The SIEM solution implemented by Things, Inc. aligns with regulatory compliance, such as PCI DSS. “The PCI DSS applies to all entities that store, process and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data.” (“PCI DSS V4.0 Quick Reference Guide,” 2022) Since Things, Inc. collects credit card payments from its customers, it must comply with PCI DSS. The SIEM implementation facilitates compliance with this standard. Requirements of this standard supported by the SIEM include log management and monitoring, regularly monitoring and testing networks, access control measures, incident response, security policies, and procedures, protecting cardholder data, and maintaining a vulnerability management program.

PCI DSS requirement ten calls for the regularly tracking and monitoring of all access to network resources and cardholder data. The SIEM system collects, stores, and analyzes logs from various sources, which helps identify unauthorized access, suspicious activities, and potential security incidents. Requirement eleven calls for Things, Inc. to regularly test security systems and processes. The SIEM tool provides continuous network traffic monitoring, which detects anomalies and potential threats and supports vulnerability assessments and penetration testing activities by analyzing and correlating logs to identify security weaknesses.

Requirement twelve of the PCI DSS calls for implementing an incident response plan. The SIEM system provides real-time alerting and automated response mechanisms for security incidents, enabling quick identification, analysis, and response to potential breaches and supporting a comprehensive incident response process. PCI DSS requirement three mandates the protection of cardholder data. The SIEM does not directly protect cardholder data. However, it monitors and alerts on access to cardholder data repositories, ensuring access to the data is authorized and logged.

**Cybersecurity Initiatives and SIEM**

The SIEM implementation has several core functions that align with cybersecurity initiatives. Security Information and Event Management (SIEM) solutions are critical in aligning with cybersecurity initiatives. The implementation team developed various standards within the SIEM implementation at Things, Inc. One of these is centralized log management, which is essential for maintaining visibility across the IT environment. Another is threat detection and incident response, where the dashboard sends alerts so the cybersecurity analysts can detect and respond to events that may indicate a security incident. The SIEM can detect suspicious activity, abnormalities, and potential security threats. The SIEM implementation supports compliance and reporting procedures by providing automated compliance reporting and auditing, ensuring that the company enforces security policies and retains logs according to regulatory requirements.

The real-time monitoring and alerts provided by the SEM solution allow security teams to respond proactively, minimizing the impact of security incidents. The SIEM's ability to integrate with other security tools, such as endpoint protection and solutions, enhances the overall security of the network infrastructure by enabling a comprehensive defense plan. The final way a SIEM solution aligns with cybersecurity initiatives is by increasing situational awareness through the dashboards and visualizations that provide insight into the company's security stance, allowing the team to understand the current threat profile, prioritize risks, and make informed decisions about security approaches.

**E2.**

Things, Inc. used various tools and applications for the SIEM implementation. A third party created some of these, and the company made others. The team did not develop any unique applications for the implementation other than those provided by the following security tools. Tools used for the implementation were Splunk to provide a SIEM platform, Jira to track security tickets, OpenVAS for vulnerability scanning, Service Desk Plus for incident response, and Apptega for compliance and reporting. The IT and security operations teams used installation guides provided by third-party tools in preparation for the deployment phase. While they used user guides provided by third-party tools, the implementation team also developed incident response playbooks that they continue to update on an ongoing basis.

**F.**

The post-implementation environment includes a revised network topology that includes endpoint detection and response nodes on each company workstation and server, as well as a central Splunk SIEM that collects logs from remote employees, cloud servers, and both corporate office networks.

**F1.**

Implementing the security incident and event monitoring platform improves the security posture of Things, Inc. by enabling the security operations center team to be prepared to respond to potential events and threats proactively rather than reactively. The SIEM platform also allows the company to be more efficient. Since the SIEM aggregates and normalizes data, the team can spend time responding to critical events immediately instead of manually poring over logs to gather the data needed to formulate a response.

**F2.**

As the team analyzed server uptime reports, event logs, and reporting from security analysts, they observed that incidents resulting in server unavailability decreased by 70%, and overall security incidents went down by 60%. The effect of the implementation on business processes is that procedures were added to daily business processes to regularly communicate SIEM data and observations on SIEM data between the security operations center team, the IT team, and the data and applications team.

**F3.**

Upon reviewing summative test results, the data review shows that 60% fewer security events occurred overall, which meets the acceptance criteria of a 50% decrease required by the summative assessment.

The plan of action to improve summative test results in the future is for the team to engage in regular reviews of SIEM performance and adjustments to enhance security monitoring effectiveness, allowing the team to improve configuration management, reduce false positives and false negatives, and train staff.

**F4.**

There are some post-implementation risks that the team needs to be aware of so that they can mitigate them. These include high operational costs, integration complexity, misconfiguration, compliance risk, and vendor lock-in.

The risk of high operational costs is high since the CEO must be able to continue to see and understand the value of the SIEM platform going forward, as there is a risk of lacking an appropriate budget allocation to continue. The impact on the organization is that budgetary restrictions can impede the project's ongoing success. This impact can be mitigated by continuing clear communication with executive stakeholders and proper budget planning for continued security monitoring operations.

The risk of integration complexity is high as the company has defaulted to more complicated than necessary infrastructure in the past. The effect on the organization is that inefficient spending can hinder the project's success and leave security gaps open that can compromise the effectiveness of the SIEM implementation. To mitigate this, the team will work hard to ensure no sprawl is involved in the implementation by carefully planning the initial launch stage and continually reviewing the SIEM implementation to ensure the team is efficient with its resources.

As the SIEM program continues to operate, the likelihood of misconfiguration is high due to the complex nature of the company's infrastructure, which makes it easier for an engineer to inadvertently leave a machine out or configure it inappropriately for its unique use. If this risk occurs, the impact on the company would be high as it could result in missed security incidents that the team does not get to respond to in time to avoid. To mitigate this risk, the team will review each other's work to ensure proper implementation and engage in appropriate initial and ongoing SIEM training.

The risk of being out of compliance is relatively low. The company falls into fewer high-risk compliance categories than others. They do not handle personally identifiable information, health information, and government data, nor do they operate in the European Union. They are only bound to a few laws and regulations. Since the company has a compliance officer who is well-trained on the SIEM's compliance tools and on using Apptega for compliance tracking and reporting, it is unlikely they will have a compliance problem. If they do, the impact on the company would be high, as it could incur fines, loss of revenue, and loss of reputation. To mitigate this, the compliance officer will use integrated SIEM compliance tools and Apptega to ensure the implementation continues to comply with relevant regulatory and legal compliance requirements.

The potential risk of vendor lock-in is high as the company is already negatively affected by it within one of its primary applications. The organization's impact is that if the company becomes stuck with the current SIEM vendor beyond when it is ideal, budget and security needs may be negatively affected. To mitigate this, the team should continually review the SIEM vendor's compatibility with the security needs, infrastructure, and budget of Things, Inc. The company should also maintain data backups in a format compatible with other SIEM providers if changing platforms becomes necessary.

**F5.**

In the project planning stage, the needs of the stakeholders involved in the SIEM implementation were identified. Through the implementation process, the needs of each stakeholder were met. The CEO needed to understand why the SIEM was required and what it does for the company. That need was met during the project stakeholder meeting, during which the rest of the implementation team presented the information to the CEO. The project manager needed a thorough understanding of the company's pre-SIEM security posture and what the company seeks to achieve from SIEM implementation. This need was met during phase one of the project, where the consultant consulted with IT and executive teams to learn more about the company's security posture before the SIEM implementation.

The security operation team needed thorough SIEM training, communication channels to collaborate with the implementation team, and the network and software resources necessary to properly set up and use the SIEM. The training portion of the implementation plan gave these stakeholders the knowledge they needed for their role in SIEM implementation. Communication channels were established in the preparation phase, and the software resources for SIEM implementation were provisioned during the pilot implementation. The IT team and network administrators needed communication channels with all departments, and they needed to have access to work closely with the SOC team during implementation. Clear communication channels were established during the initial meeting with all the project stakeholders, and they successfully used those channels to work closely with the SOC team during the implementation phase.

The compliance officer needed to know the SIEM's compliance capabilities and an understanding of what a SIEM does and how it stores and transmits data. He acquired this knowledge by consulting with the implementation team in phase one and through the Spunk training he received. The data owners and application developers needed to understand the goals of the SIEM to help guide data selection. They developed this understanding during the initial project meeting and via collaboration with the IT and SOC teams during the planning and development phase.

**G.**

One post-implementation maintenance plan for the SIEM solution is a procedure for updates, patch management, and configuration management. The company regularly updates SIEM software to the latest version to benefit from new features, performance improvements, and security patches. The company will use patch management to apply patches and updates to the underlying operating systems, databases, and other supporting software components to ensure the entire system functions optimally.

They regularly review and update detection rules, correlation policies, and alerting mechanisms to adapt to new threats and organizational changes. As part of configuration and change management, regular SIEM configuration backups will be made along with the implementation of rules and policies to facilitate quick recovery in the event of system failure.

**H. Updated Network Diagram with SIEM Implementation**

A diagram of a computer

Description automatically generated

**References**

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 6). *Computer Security Incident Handling Guide*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/61/r2/final

*Documentation - Splunk Documentation*. (n.d.). Docs.splunk.com. https://docs.splunk.com/Documentation

GDPR.EU. (2019). *Complete guide to GDPR compliance*. GDPR.eu. https://gdpr.eu/

Gillis, A. (n.d.). *What is SIEM, and Why is it Important?* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

Hughes, G. (2023, May 17). *A Framework for SIEM Implementation*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation?gad\_source=1&gclid=CjwKCAjw7NmzBhBLEiwAxrHQ-S8peHCFcnjDnTSSiUEzHdnfYwEjaJLb4veQQn6SI2isJ8GZtKQxdxoCv8MQAvD\_BwE

ISO. (2022, October). *ISO/IEC 27001 standard – information security management systems*. ISO. https://www.iso.org/standard/27001

Kent, K., & Souppaya, M. (2006a, September 13). *Guide to Computer Security Log Management*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/92/final

Kent, K., & Souppaya, M. (2006b). *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

NIST. (2023). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

PCI DSS v4.0 Quick Reference Guide. (2022). In *PCI DSS*. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI\_DSS-QRG-v4\_0.pdf

PCI Security Standards Council. (2023). *Document Library*. PCI Security Standards Council. https://www.pcisecuritystandards.org/document\_library/