Monitoring & Log Analytics

Objective Summary: To develop an easy way to implement, cost effective deployment plan for our Monitoring & Log Analytics policies and procedures

Key Subjects:

1. **Research tools that can be used to collect and analyse log data:**
    - Splunk is a popular log monitoring and analysis tool that collects, saves, examines, and reports on any sort of machine-made data, whether structured or unstructured application logs, using a multi-line interface.
    - Another tool that can be used is Mezmo which allows you to monitor and analyse log files in real-time. It is accessible in the cloud and it's possible to look up, save, and keep data from any application or system, such as Windows, Linux, AWS, Python.

2. **Redefine key assets and data categories**

    Key Assets
    - Fitness gadgets: heart rate monitors, wearable devices
    - Platforms for gamified exercise: software that includes game components.
    - Health Monitoring Systems: Tools and applications that monitor the safety of exercise.

    Data Categories
    - User Data: Health measurements and personal data.
    - Activity logs and performance metrics comprise exercise data.
    - Engagement Information: User interactions and gamification analytics.
    - Safety Information: Health Alerts, Injury Reports.

3. **Redefine Roles and Responsibilities**
    - Security experts: safeguard user information and guarantee the safety of the infrastructure and fitness application
    - Compliance: Guarantees that internal log management rules and legal requirements are followed.
    - Log Administrator: Oversees the policies for log retention, storage, and collecting.

4. **Ensure all digital assets are covered in deployment – explain how they will be covered**
    - Automated Monitoring: To quickly identify errors and problems, implement automated monitoring systems that continuously track and send alerts based on log data from all assets.
    - Frequent Audits: Update configurations whenever new assets are added and conduct routine audits to ensure that all assets are being properly monitored and logged.

5. **Cost Effectiveness:**
    - One user can utilise 500 MB of Splunk each day and it is free of charge. Splunk also has two paying options if you require more sophisticated features. In that instance, pricing is available upon request. However, Mezmo provides a 14-day free trial in addition to several paid choices and a free version as well which allows the user to test the tools before fully committing.

6. **Ease of implementation:**

    Splunk
    - Training: To facilitate learning, documentation and training materials are made available.
    - User Interface: Offers a strong, multi-line interface that is quite configurable.

    Memzo
    - Quick Installation: Quick to set up and accessible via web interface.
    - User Interface: User-friendly interface designed for real-time monitoring and log analysis.

7. **Adherence to regulatory requirements:**

    Memzo
    - HIPAA Compliance: Offers secure audit trails and logging for patient data, preserving confidentiality and logging access information.
    - Real-Time Monitoring: Assists in fulfilling regulatory requirements for logging and monitoring across multiple systems and applications by providing real-time insights and alerts.

    Splunk
    - SOC2, FedRamp, and ISO 27001 Compliance: uses strict security standards and procedures to guarantee safe data handling and protection.
    - EEOC Compliance: Complies with regulations to guarantee ethical and fair employment standards and discrimination-free hiring procedures.
    - Sector-Specific Requirements: Respects laws like GDPR, PCI-DSS, and HIPAA in order to control risks, stay out of trouble with the law, and keep customers trust.

References

Leanne Mitton, L.M. (2023). Regulatory Compliance 101: What You Need To Know. Splunk Blogs https://www.splunk.com/en_us/blog/learn/regulatory-compliance.html

Mezmo. (2024). MONITORING AND LOGGING REQUIREMENTS FOR COMPLIANCE. Regulatory Compliance. https://www.mezmo.com/learn-observability/monitoring-and-logging-requirements-for-compliance

Rafal Kuc, R.K. (2023). 15 Best Log Analysis Tools & Log Analyzers of 2024 (Paid, Free & Open-source). Sematext. https://sematext.com/blog/log-analysis-tools/ (Tools to use research)