**Q1.**

**Logging** is the process of recording information about a program's execution for the purposes of debugging, monitoring, and maintaining software applications. It involves capturing events and data points that describe the state of the application, actions performed, errors encountered, and other relevant information.

Q2.

**Identify unauthorized access:** Logs reveal login attempts, both successful and failed. By tracking logins from unusual locations, strange access times, or a series of unsuccessful attempts followed by a successful one, you can pinpoint signs of unauthorized access and potential account compromises.

**Detect data breaches:** By analyzing logs, you can detect anomalous actions performed on sensitive files or data. Unexpected file changes, access from abnormal locations, or large data transfers out of your system could indicate a data breach in progress.

**Achieve compliance:** Regulatory standards like HIPAA, PCI DSS, CMMC, and others often mandate robust logging and auditing practices. Maintaining proper logs demonstrates your commitment to security and compliance readiness.

**Troubleshoot issues:** Logs are invaluable for diagnosing and resolving technical issues. By reviewing logs, you can identify the root cause of problems, such as application errors, hardware failures, or network connectivity issues. This information can help you optimize your IT infrastructure and minimize downtime.

**Debugging:** Helps developers identify and diagnose issues within the application.

**Monitoring:** Provides insights into the application's behavior and performance.

**Auditing:** Keeps a record of actions and events for security and compliance purposes.

**Q3.** **Logging is crucial for several reasons:**

**Emergency (emerg):** indicates that the system is unusable and requires immediate attention.

**Alert (alert):** indicates that immediate action is necessary to resolve a critical issue.

**Critical (crit):** signifies critical conditions in the program that demand intervention to prevent system failure.

**Error (error):** indicates error conditions that impair some operation but are less severe than critical situations.

**Warning (warn):** signifies potential issues that may lead to errors or unexpected behavior in the future if not addressed.

**Notice (notice):** applies to normal but significant conditions that may require monitoring.

**Informational (info):** includes messages that provide a record of the normal operation of the system.

**Debug (debug):** intended for logging detailed information about the system for debugging purposes.