Operational security involves monitoring and recording activities using security information and event management (SIEM) systems to analyze logs and detect suspicious activity.These systems are used to centrally analyze logs from all systems and network devices, enabling early detection and rapid response to threats.