Logs are required for the monitoring of system health and security since they allow tracking activities, events, and errors in applications, services, and operating systems. Application logs, for example, provide information from the individual applications, including what happens when the applications crash or malfunction. They play a key role in problem troubleshooting and the maintenance of an application that is secure. An application crashing too many times or acting abnormally could mean malware or vulnerabilities. In Windows, these logs are in the "Application" section of the Event Viewer. On Mac, they go into `/var/log/`, and on Linux at `/var/log/application.log`. Application logs are also monitored in real time by such tools as Splunk and Graylog, generating alerts upon the detection of abnormal conditions.

On the other hand, event logs record events throughout the system, including attempted logins, permission changes, and updates to configuration. These logs are very important to monitor user activities and locate security breaches. For example, several unsuccessful login attempts may reveal a brute-force attack. Event logs are stored in the Event Viewer on Windows systems, categorized into "Security", "Application", and "System" logs. On macOS, the Console application offers access to logs; on Linux, `journalctl` or directly `/var/log/syslog` does the job. With the help of some tools like Logwatch and Windows Event Viewer, early detection of threats is possible.

Service logs show the insights into specific services such as web servers or databases, recording their startups, crashes, and general activity that may indicate vulnerabilities or ongoing attacks, such as a DDoS. Repeated server crashes may be a symptom of an attack or misconfiguration. Service logs are available in Windows under "System" logs in Event Viewer; on Linux and Mac, this can be found under /var/log/. Nagios and Zabbix monitor service logs and trigger alerts at the slightest disruption of services.

System logs in some Operating Systems usually track some major events, including the operating system boot process, kernel activities, and even hardware failures that occur; hence, they are usually useful in diagnosing OS-level problems. These logs can also help identify hardware failures or system crashes that could point to an underlying vulnerability. System logs in Windows are kept within the Event Viewer, whereas on Mac, they are stored in `/var/log/system.log`, and Linux does the same in `/var/log/syslog` or `/var/log/dmesg`. Centralizing these logs into a utility like Syslog or dmesg for Linux , or even with commercial offerings such as Splunk, produces the same effect.

Log monitoring allows for the identification of various possible threats, such as a zero-day exploit and unauthorized USB access. For example, USB logs monitor the connection of unauthorized devices that could introduce malware into your system. This normally occurs under "Security" logs within Windows and `/var/log/usb.log` on Mac/Linux. Auditd for Linux or BitLocker for Windows enhances security by adding in the monitoring of removable media access.

Sources:

CrowdStrike - Event Log Details and Uses
Logit.io - Log Types and Monitoring for Various OS
Splunk - Monitoring and Threat Detection through Logs
XpoLog - Application Log Importance and Monitoring
TechTarget - System Log Data and Security Benefits
SolarWinds - Best Practices for Log Monitoring