

Is intrusion detection required if centralized log correlation is in place?

PCI SSC FAQ | Article 1074 | December 2022

Although log correlation is a valuable tool in a company's information security strategy, it does not replace intrusion detection mechanisms, such as IDS/IPS. Intrusion detection mechanisms provide proactive detection of threats coming into the network by comparing network traffic against known "signatures" or behaviors of different compromise types (e.g. hacker tools, Trojans, and other malware). Intrusion-detection and/or intrusion-prevention techniques are required by PCI DSS Requirement 11. In addition, logs from the intrusion-detection and/or intrusion-prevention mechanisms should be included in the daily log reviews, as required in PCI DSS Requirement 10. Note that the use of log harvesting, parsing, and alerting tools can be used to facilitate the process by identifying log events that need to be reviewed.

Source: <https://www.pcisecuritystandards.org/faqs/1074/>