Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

1. Firewall
2. Intrusion Detection System(IDS)
3. Security Information and Event Management(SIEM) tool.

Part 2: Explain your recommendations

- Firewalls will enable the allowing or blocking of network traffic based on a set of predefined rules. An example of such a rule is to block any incoming traffic from a source with an IP address similar to that of any device on the internal network. That would indicate a potential replay attack.
- Intrusion Detection Systems(IDSs) would alert network and security administrators about potential attacks and intrusions. This would enable security professionals to stop attacks at the source before they compromised the internal network.
- Security Information and Event Management(SIEM) tools would collect and analyze log data from network devices all across the network and aggregate them to a single dashboard. This enables the SOC team to analyze log data and identify threats, common incidents and network traffic anomalies that could signify risks.